Wavecrest**CyBlock**®Appliance

Version 9.6.1

Secure Web Filtering and Monitoring

User**Guide**

www.wavecrest.net

904 East New Haven Avenue, Melbourne, FL 32901 USA
www.wavecrest.net

Table of Contents

Introduction

Welcome to CyBlock Appliance. CyBlock Appliance a turnkey Web security hardware solution. With reliable performance and speed, it provides powerful filtering that blocks Web sites, malware, IM, P2P, streaming, file sharing, and more. This manual covers detailed instructions for setting up blocking policies and reporting for the appliance.

Organization

The documentation follows the menu structure which is organized for ease of setup and use of the product. However, you can always start with using the basic setup of the product covered in the Getting Started Checklist and later use the more advanced features when you are ready. You do not have to read each section from beginning to end. You are welcome to skip around to find instructions for the features that are important for your organization's use. The sections are briefly described below.

Getting Started

This section is a checklist of all the basic setup steps beyond getting the appliance connected to help you get the product up and running. This includes installing the client piece on all monitored computers and configuring users' browsers.

Managing Direct Traffic

This section provides the recommended steps for managing direct traffic including setting up the DNS server.

Hybrid Deployment

The Hybrid deployment is a feature that uses CyBlock Cloud to extend Web filtering and monitoring to your cloud users. It integrates your local CyBlock installation with your cloud accounts. This section summarizes how the Hybrid deployment works.

Web Management

Wavecrest's products were built with customizable Web policy support settings to fit any organization's needs. This section will walk you through creating blocking policies, white/black lists, and a customized blocking message.

Data Management

The reporting feature of this product is dependent on the log files. This section covers instructions on viewing your log files and managing the product's Report Database. The Report Database compresses log files allowing for faster reporting and long-term storage.

User Management

In this section, you will learn about the product's core grouping structure and the ways that you can use grouping. This includes adding your groups and IDs as well as importing them from a text file or Active Directory. Even if you do not want to use grouping, you will want to read the Introduction to this section as you will still need to understand the core grouping structure and how to import or add IDs. Instructions on how to change your password for your account and manage logon accounts can also be found here.

Categorization

This section contains instructions on scheduling the download of the URL List, checking the category of any URL in the URL List, and creating custom categories and populating them with URLs that your company wants to track. You can also select the categories to display on your reports.

Real-Time Monitors

The Real-Time Monitors let you view employees' Web activity live including requests that were denied due to Web filtering and those denied due to content type filtering. You may also view current bandwidth usage data for the Enterprise.

Reports

This section shows you how to use customizable and predefined Dashboard charts, create and manage custom report templates, manage reports, schedule reports to run automatically, and create high-level and low-level reports. There are several standard reports available in the product as well as the option to use Interactive or Read-Only reports. Interactive standard reports allow you to drill down from a higher-level report to get more detailed Web-use data.

System Status

This section contains informational screens which are used to view the product's server status and its specifications, jobs in the queue, and policy-related information that you have set in the product.

Settings

This section contains instructions on updating your license information, creating a restore point, and setting report options for the way that you want report data presented.

It also covers instructions for setting up a PAC file configuration and proxy chaining to connect to another proxy upstream from the product.

Help

This section briefly describes the Profiling page used with Technical Support, how to find category descriptions, how to check for product updates, and how to accept and print the End User License Agreement.

Help and Contact Information

Additional help for the product is also available in the product. Just click **Help** in the navigation bar at the top. The product Help window will then appear in which you can search for information.

Chat assistance is also available from Customer Service or Technical Support.

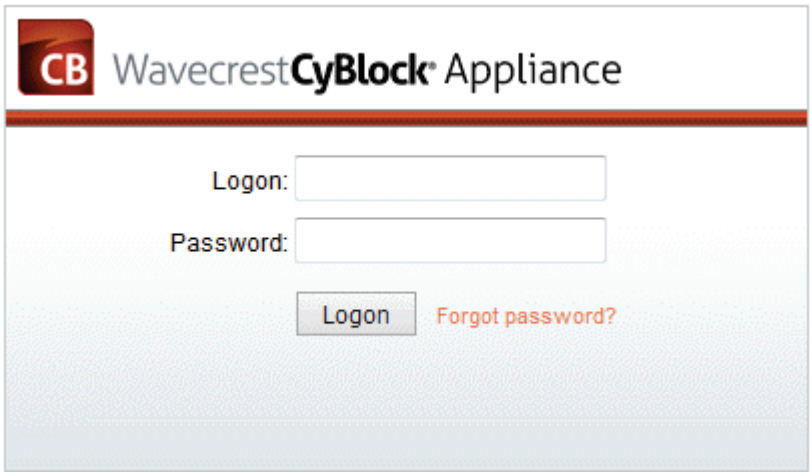
- In the product, click **Live Support** in the navigation bar at the top. The Wavecrest Live Support window opens. Enter your name and e-mail address. Select the department, type your message, and click **Start Chatting**.

If you ever need additional help beyond what is available in the manual or the product, please feel free to contact our Technical Support team.

Contact Information	
Telephone Numbers	
Toll-Free	877-442-9346, Ext. 4 (U.S. and Canada)
Direct	321-953-5351, Ext. 4
International	001-321-953-5351, Ext. 4 (outside U.S. and Canada)
E-Mail	
Technical Support	support@wavecrest.net
General Info	info@wavecrest.net

Logon

1. Log on to the product using the following default credentials:
    - **Logon** - admin
    - **Password** - password
2. Click **Logon**. The Change Your Password page is displayed.
3. After changing your temporary password, log on with your new password.



Forgot Password

If you ever forget your password, click the **Forgot password?** link on the Logon page. The Reset Password page will be displayed.

Enter your logon and click **Submit**. Your password will be reset, and you will receive a Password Reset e-mail to change your password.

Technical Considerations

1. **How will you manage groups and IDs?**

   You have two options. You can either 1) manage them at the directory source, i.e., Active Directory, or 2) manage them inside the product. If you choose to manage your groups and IDs at the directory source, you will not be able to move or edit them inside the product. If you choose to manage your groups and IDs inside the product, only new IDs will be imported from your Active Directory or text file. No moves or changes at the directory source will be imported. Instead, these changes will have to be made inside the product. To learn more about managing groups and IDs, see the Introduction and Manage Users section for User Management.

2. **What policies do you need to create and how will they apply to your users?**

   Your answers to these questions will not only help you when it is time to create your policies, but it will also help you determine how to structure your groups and IDs. For example, you may only need a single policy for the entire Enterprise or several different policies for your different groups and/or individual users. How you plan to distribute reports will also need to be taken into consideration when setting up your groups and IDs. To learn more about what your options are and what decisions you need to make before importing your groups and IDs, see Appendix A. For instructions on how to create or import your groups and IDs, see User Management.

3. **Will you import your groups and IDs from Active Directory?**

   If the answer is yes, then you have two options when creating your blocking policies.

   Option 1: You can import your groups and IDs first and then create blocking policies.

   Option 2: You can create blocking policies first to match your Active Directory policies and then import your groups and IDs. This way all of your groups and IDs will automatically be assigned to the appropriate blocking policies when you import them. If you choose to create your blocking policies first, you must use permission groups.

   NOTE: You must select to manage your groups and IDs outside the product if you choose to create your blocking policies first.

4. **Will you apply classification ratings to your categories?**

   The product offers three different classification ratings that can be applied to each category. They are acceptable, unacceptable, or neutral. You can choose to have these ratings appear in your Web-use reports, making it easy to quickly identify when Web abuse has occurred. For instructions on setting default classification ratings, see Classify Categories.

5. **How will you distribute reports?**

   Reports can either be run manually on an ad hoc basis or can be scheduled to run daily, weekly, or monthly. Scheduled reports can either be sent via e-mail to someone you specify or saved to a directory where managers can retrieve the report. See Reports for creating reports. If you plan for managers to log on and create their own reports, see the instructions for creating manager access accounts in Add Logon Account.

6. **Will you create administrator and manager access accounts?**

   Administrators have full access to the product while managers are limited to only reporting. Manager accounts can be further limited to only have access to run reports on specified users and/or groups. When creating these accounts, you also have the option to assign a new password or authenticate to Active Directory. For instructions on creating administrator and manager accounts, see Add Logon Account.

Getting Started

Getting Started Checklist

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

- **Install the Client Piece** - The client piece is installed on users' computers so that protocols will be blocked and monitored by ID.
- **Configure Users' Browsers** - Browsers must be set to go through the proxy.
- **Change the Default Password** - Change the Administrator password.
- **Enter Serial Number and Activation Key** - Complete this step to activate the product.
- **Download the URL List** - Complete this step so that you can run reports.
- **Set Up Memory Settings** - Select the amount of memory needed.
- **Set Up Groups and IDs** - Determine whether you will use grouping.
- **Configure the Report Database** - Connect to the metric server to use the Report Database.
- **Enable Logging** - Configure the appliance to log Web traffic.
- **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.
- **Set Up Administrator E-Mail** - Receive reports and status updates via e-mail.
- **Participate in OtherWise** - Optimize categorization results.
- **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 Real-Time Web Monitor** - View Web traffic live.
- **Run the Real-Time Protocol Monitor** - View protocol traffic live.
- **Create and Run a Site Analysis Report** - Create a high-level summary report–one that is useful for identifying suspect areas.

  NOTE: Be sure to complete these steps. Many of these steps are mandatory to get the product up and running properly. Click the links above to go to the instructions for a particular step. Most of these instructions are located in other sections of the manual.

Configure Users' Browsers

Your monitored users' browsers must be configured to go through the Appliance to filter and report on login names for all HTTP traffic. There are a few ways to accomplish this task and a couple of things you can do to ensure that users do not change their browser settings. For Internet Explorer, it is possible to change IE settings for all users in your domain in one step, or you can choose to change each user's IE settings individually. For Firefox, you can only change each user's browser settings individually.

You need to know the IP address of the server that the product is installed on before you begin configuring browsers. You can find the IP address of the CyBlock Appliance by going to **Settings - Network**.

Configure All Users' Browsers in Internet Explorer

These instructions will step you through defining IE settings for all users in your domain.

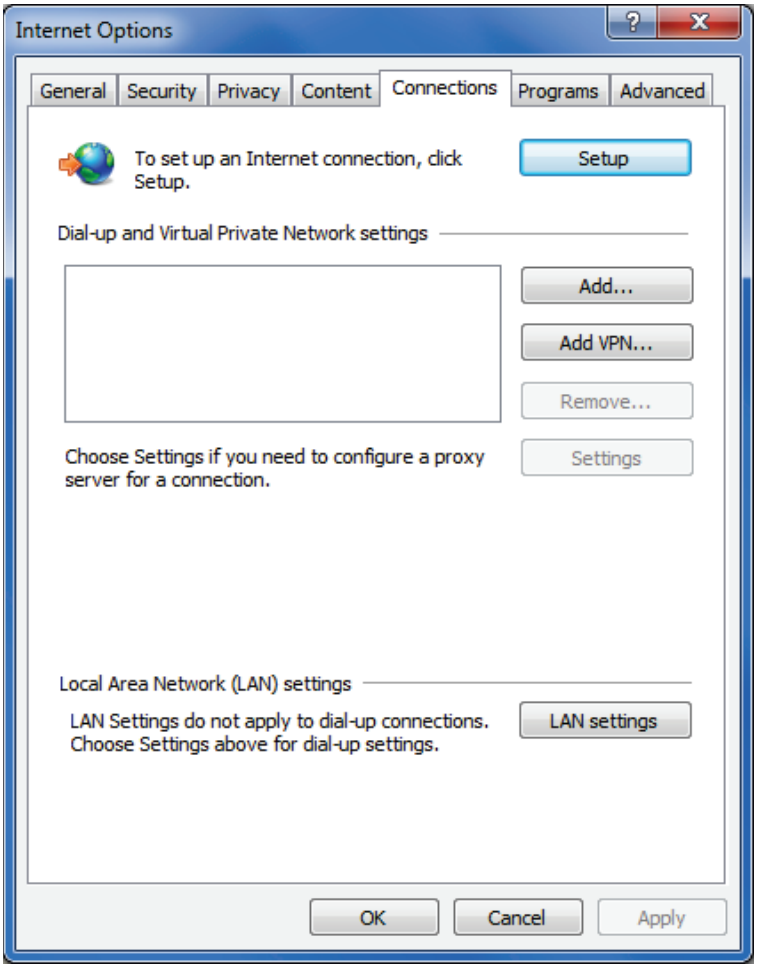
NOTE: These instructions apply **only** to Internet Explorer browsers in an Active Directory domain.

1. Go to **Programs - Administrative Tools** on your Domain Controller computer.
2. Open **Active Directory Users and Computers**.
3. Right-click the root of the domain and select **Properties**.
4. Select the **Group Policy** tab and click **Edit** for the **Default Domain Policy** GPO.
5. Go to **User Configuration - Windows Settings - Internet Explorer Maintenance**.
6. Open the **Connection** folder.
7. Right-click **Proxy Settings** and go to **Properties**.
8. Select the **Enable Proxy Configuration** check box.
9. Fill in the IP address of the Appliance.
10. Apply your changes, and the next time users open IE, their Web traffic will be logged by the Appliance.

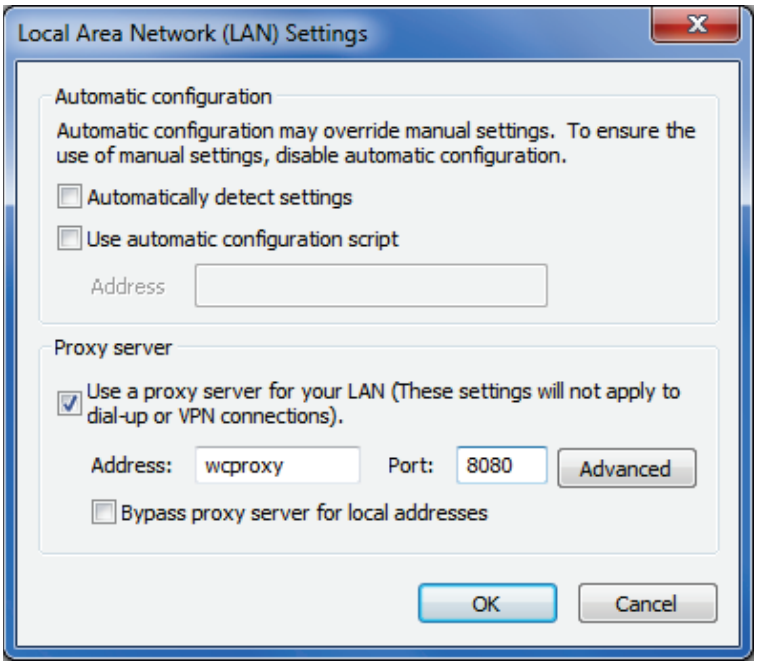
NOTE: If you are in an Active Directory domain but have difficulty changing these settings, please contact Wavecrest Support at 321-953-5351, Ext. 4 or support@wavecrest.net for assistance.

Configure a Single User's Browser in Internet Explorer

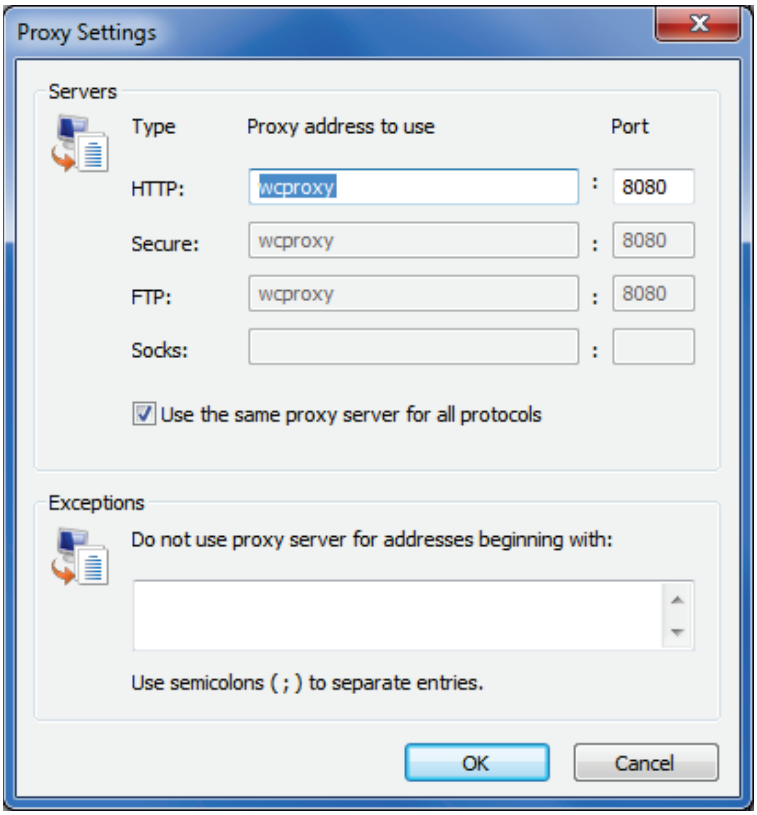
1. Begin by opening your Internet Explorer browser.
2. Click the **Tools** menu. Then, click **Internet Options**. The Internet Options dialog box will appear.



3. Next, click the **Connections** tab and then the **LAN Settings** button.



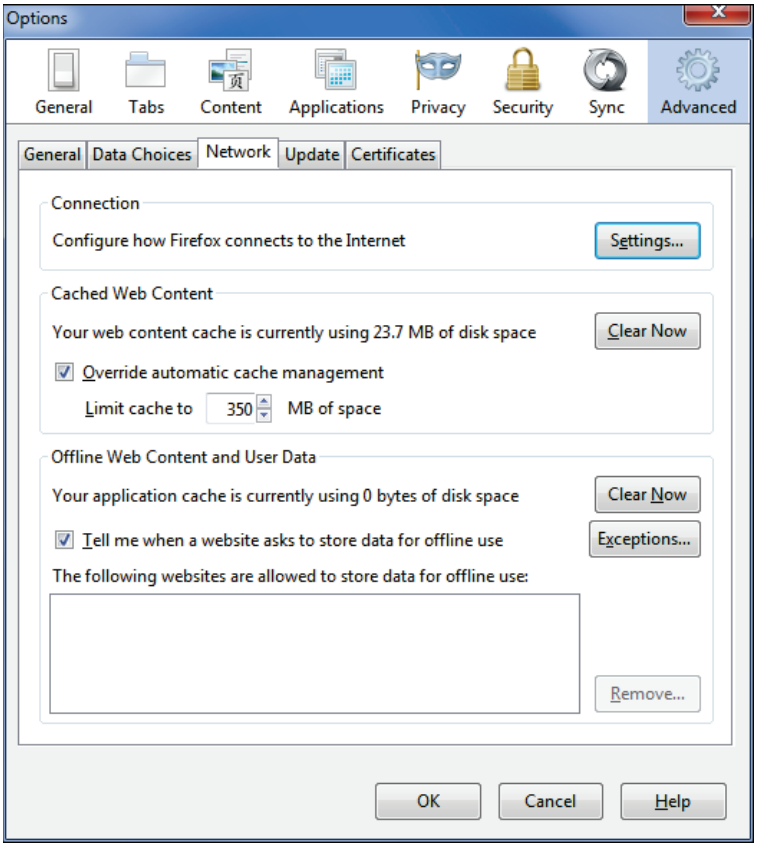
4. In the LAN Settings dialog box, select the check box in the **Proxy server** section that indicates **Use a proxy server...**
5. Clear any other check boxes on this screen.
6. In the **Address** field, type in the IP address of the Appliance.
7. If possible, leave the **Port** field alone with the default port of 8080.
8. If you click the **Advanced** button next to the **Port** field, you should see that HTTP traffic is now being routed through the server you just specified. (There should be no reason to modify this screen.)



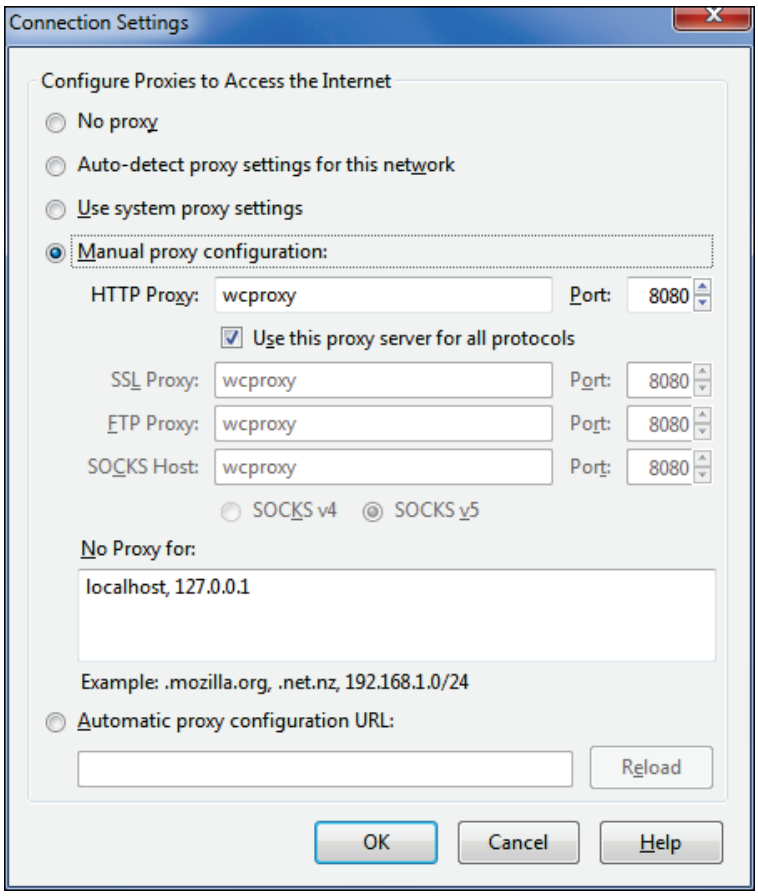
9. Click **OK** to close any open dialog boxes; doing so will save your new proxy configuration.

Configure a Single User's Browser in Mozilla Firefox

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 **Manual proxy configuration** option.
5. In the **HTTP Proxy** box, type the IP address of the Appliance. Do not change the **Port** box default of 8080.
6. Click **OK** to save changes, and exit the dialog box.

Prevent Users From Changing Browser Settings

Disable Internet Explorer's Connection Option

1. Go to **Programs - Administrative Tools** on your Domain Controller computer.
2. Open **Active Directory Users and Computers**.
3. Right-click the root of the domain and select **Properties**.
4. Select the **Group Policy** tab and click **Edit** for the **Default Domain Policy** GPO.
5. Go to **User Configuration - Administrative Templates - Windows Components - Internet Explorer**.
6. Double-click **Internet Control Panel**.
7. Go to **Properties** and select the ***enabled*** option for ***Disable the connections page***.
8. Click **OK** when are finished to save your changes. Users will no longer be able to see the **Connections** tab in their Internet Explorer browser.

Create a Firewall Rule

There is another way to ensure that all users browsing the Web go through your proxy server and not bypass it. You can configure your firewall to deny all HTTP (port 80) outbound requests except for ones coming from the IP address(es) of your proxy server(s).

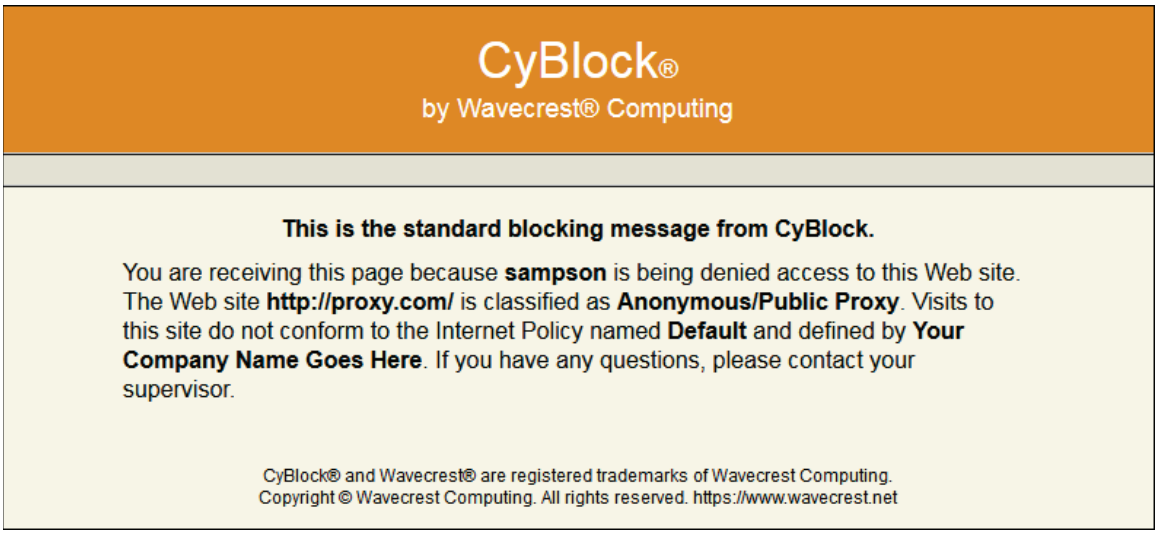
How it works: The firewall will deny all Web browsing requests except ones coming from the proxy server. This will ensure that all users browsing the Web have to go through your proxy server.

How to configure your firewall: All firewalls should support the above functionality but provide different ways of configuring this option. Please consult your firewall's admin guide for the proper settings.

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.

Managing Direct Traffic

CyBlock Appliance allows you to monitor and filter direct HTTP and HTTPS traffic via redirection. Before enforcing a blocking policy on direct HTTPS traffic, the following setup is recommended.

Setting Up Your DHCP Server

Your DHCP server needs to be configured with your appliance IP address as the DNS server for both managed and unmanaged devices.

- Managed devices are those devices that are going through the proxy for Internet connections. These devices include Windows computers and employee personal devices (BYOD).
- Unmanaged devices are devices that have not been configured with proxy settings, and are accessing the Internet using your organization's policy settings and guest network (Wi-Fi). These devices include guest laptops and iOS/Android devices.
- For managed devices inline with the appliance in your network, add the appliance IP address as the DNS server.
    - If you want to apply the DNS server update immediately, use the following command:
    - psexec.exe -accepteula \\<DESIRED_HOST> cmd /c "netsh interface ip set dns name="Local Area Connection" source=static addr=<DESIRED_DNS_IP>"

      where DESIRED_HOST is the computer name for a specific computer or * for all computers in the current domain, and DESIRED_DNS_IP is the appliance IP address.
    - The psexec command is used to quickly push the DNS server (appliance IP address) to all managed devices or to update the DNS server on those devices if a failure occurs.
    - Alternatively, if using the DHCP Lease Process, you can wait for the DNS server to be updated when the IP address lease is renewed.
- For unmanaged devices using your guest network, add the appliance IP address to the Wi-Fi DNS setting being pushed out. By applying this change, the Wi-Fi will reset all current connections. When devices reconnect, they will get the new DNS setting.
    - If manually setting the DNS server on devices, refer to the device Help documentation.

Authenticating Your Users

Ensure that authentication is set up for all users so that direct HTTP and HTTPS traffic can be properly filtered.

- For managed computers:
    - Go to Authentication Manager to set up authentication for your network.
    - Configure users' browsers using a PAC file.
    - Enable SSL Inspection to inspect direct HTTPS traffic.
- For unmanaged devices accessing your Wi-Fi network:
    - Go to Authentication - Rules to set up your IP address or range of IP addresses for your Wi-Fi network.
    - Go to Authentication - Cookie to set up your AUP Only Logon page.
    - iOS devices:
        - Once the device is connected to your Wi-Fi network, the AUP Only Logon page opens.
        - You will select the check box agreeing to the AUP and then select Logon.
        - You will then be able to access the Internet.
    - Android devices:

- Once the device is connected to your Wi-Fi network, you will need to go to the browser.
- The AUP Only Logon page will open in the browser.
- You will select the check box agreeing to the AUP and then select Logon.
- You will then be able to access the Internet.

NOTE: If the browser has open secure pages or the default home page is secure, a certificate error may occur. You may select the button to proceed, or open a new tab and navigate to an unsecure site. The AUP Only Logon page will then be displayed.

Filtering Direct HTTPS Traffic

Now you can enable filtering on direct HTTPS traffic.

- On the Settings - Proxy - Direct Traffic page, direct HTTP traffic is set to be filtered by default.
- Click the HTTPS status indicator to enable filtering on direct HTTPS traffic.
- You may enter any valid network source IP addresses to be excluded from redirection.
- You may also enter any valid destination IP addresses/domains to be excluded from redirection.

Hybrid Deployment

The Hybrid deployment is a feature that uses CyBlock Cloud to extend Web filtering and monitoring to your off-premises employees, that is, those connecting to the Internet from hotels, airports, home offices, or remote offices. It consists of two components, that is, a local CyBlock installation and CyBlock Cloud delivered as a service.

Below is a summary of how the Hybrid deployment works.

- Install one of our enterprise-level CyBlock deployment options–CyBlock Software or CyBlock Appliance.
- You will be provided with a CyBlock Cloud account from our Sales department.
- You pair your local CyBlock with your cloud account using the Hybrid Configuration page. Multiple cloud accounts can be paired.
- On the User Management - Authentication - Rules tab, a Cloud rule appears with the same authentication type as the Default rule which you can modify, but not delete.
- When configuration changes occur in your local CyBlock, they automatically sync with CyBlock Cloud. See Configurations Synced.
- The IPC Log page displays the communication messages sent between your local CyBlock and CyBlock Cloud and is used for troubleshooting purposes.
- Remote employee Web traffic is routed to the CyBlock Cloud server where the policies are applied.
- On-premises employee Web traffic is routed to your local CyBlock within your network.
- You can monitor live Web traffic of your remote employees, i.e., cloud users, on the Real-Time Web Monitor.
- Dashboard charts show cloud Web activity for the top users, groups, categories, and sites, and provide trending.
- Reports can be run to further analyze the Web usage of your cloud users.

Web Management

Introduction

This product contains several configurable features that let you correlate and optimize its support of your organization's Web usage policy. That is, you can easily configure these features to highlight inappropriate activity and block selected Web sites. In addition, if you need to, you can configure different policy settings for different suborganizations and individual users.

Before configuring these features, make sure you have completed the Getting Started Checklist. In addition, if you plan to apply different Web policies to different groups or users, be sure to complete the groups and IDs import process. See User Management.

In this section, you will find instructions on how to:

- **Apply Controls** - Allow specific YouTube videos based on your blocking policies for Web categories.
- **Filter** - Block by protocols, Web categories, content types, and search terms; create white/black lists; and customize your own blocking message.
- **Manage Bandwidth** - Create policies to control bandwidth usage by categories or groups.
- **Install CyBlock Client** - Install the client piece to block and monitor all non-HTTP protocols.

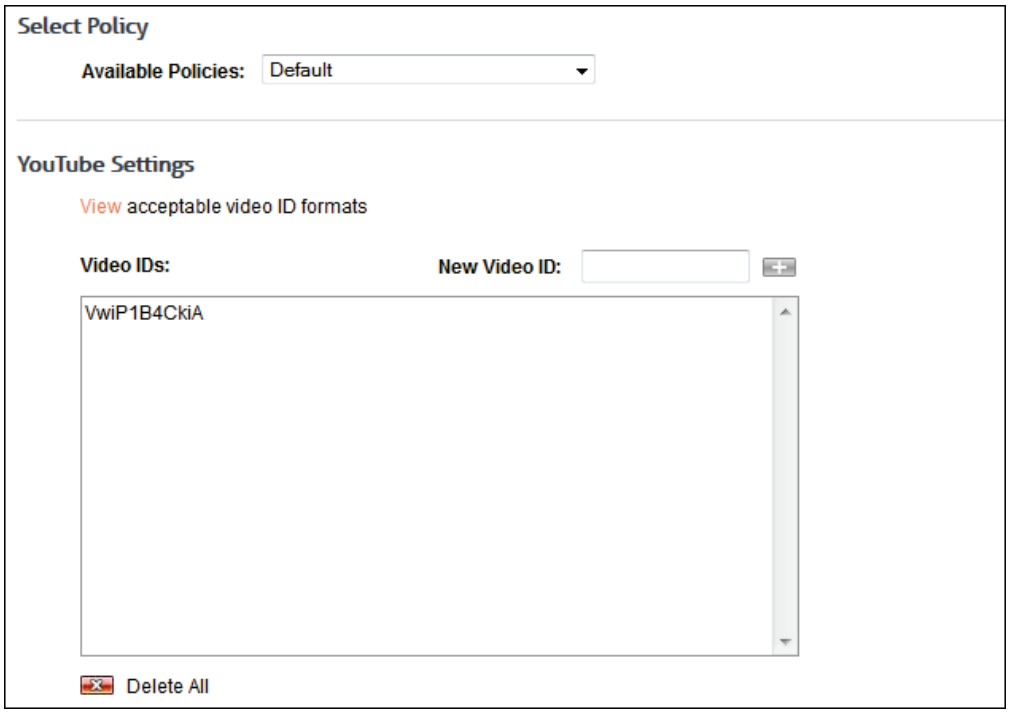
The Web Management features can be very helpful in controlling and monitoring Web usage in the workplace. By using these features, you can greatly reduce the risk of legal liability, wasted bandwidth, security threats, and lost productivity. These same features help ensure the production of clear, actionable information that management and IT staff can use to correct any deviations from the organization's policy.

Application Controls

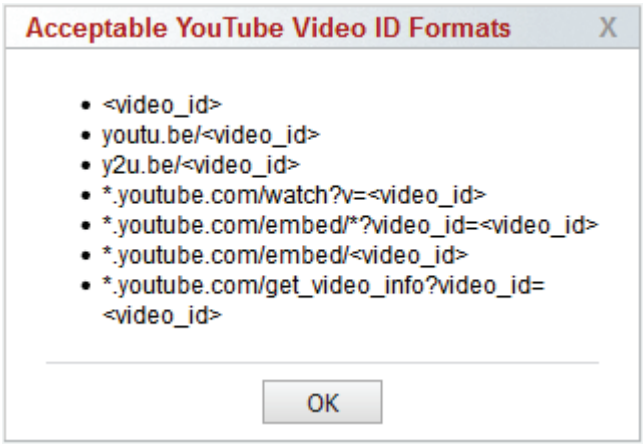
The Application Controls feature enables you to reliably fine-tune access to popular sites within social media such as YouTube. This page provides the ability to allow only specific YouTube videos based on your blocking policies for Web categories. The Video Streaming category should be blocked to enforce the selected policy.

NOTE: The allowed video will only play if users are not logged on to YouTube or any other Google app.

1. Go to **Web Management - Application Controls**. The Application Controls page is displayed.



2. Under **Select Policy**, in the **Available Policies** field, select the blocking policy that you want to associate with this allowed site.
3. Under **YouTube Settings**, click the **View** link to see the acceptable video ID formats.

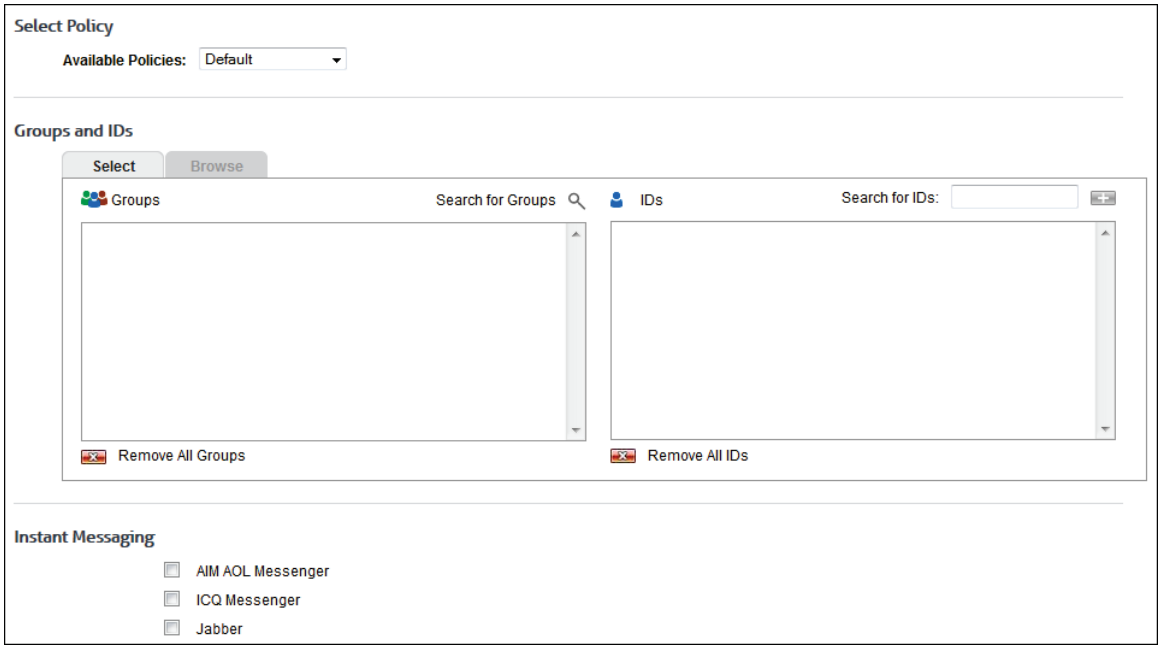


4. Click **OK**.
5. To allow a video ID, type the video ID in one of the video ID formats in the **New Video ID** field, and press ENTER. Only the video ID will be added to the **Video IDs** box.
6. To delete a video ID, hover over the corresponding line and click the red x icon. To delete all video IDs, click the **Delete All** red x icon.

Control Web Protocols

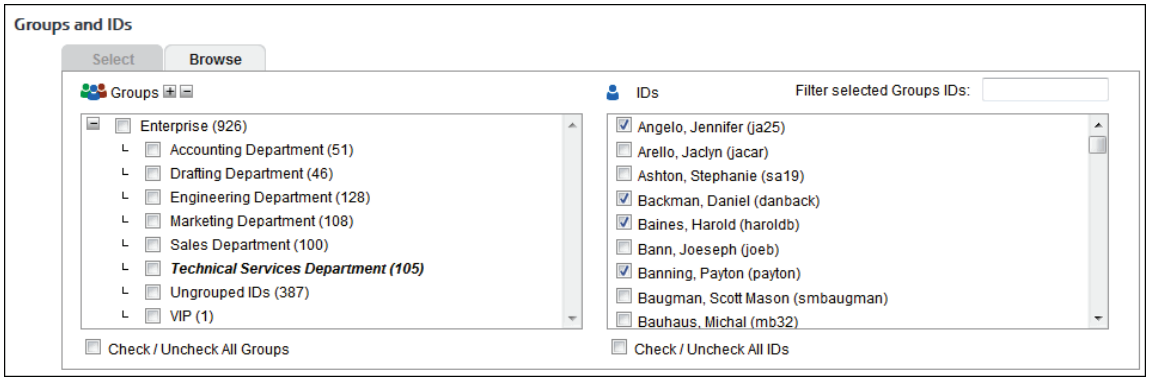
This page allows you to block non-HTTP protocols, i.e., IM, e-mail, P2P, etc. Groups and IDs can be specified for each blocking policy you create. Therefore, you can choose to have multiple blocking policies, i.e., different policies for different groups and IDs, or you can choose to have one universal policy for the entire organization.

1. Go to **Web Management - Filter - Protocols**. The Control Web Protocols page is displayed.



2. Under **Select Policy**, in the **Available Policies** field, select *Create new policy* to create a new blocking policy, or you can choose to modify or delete an existing one.
3. After selecting *Create new policy*, enter a policy name in the **Available Policies** field (for example, Policy A). If you are modifying or deleting a previously created policy, its name will appear in this field. To rename the policy, click the pencil icon. To delete the policy, click the red x icon next to the field.

   NOTE: The Default policy cannot be deleted.
4. 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.

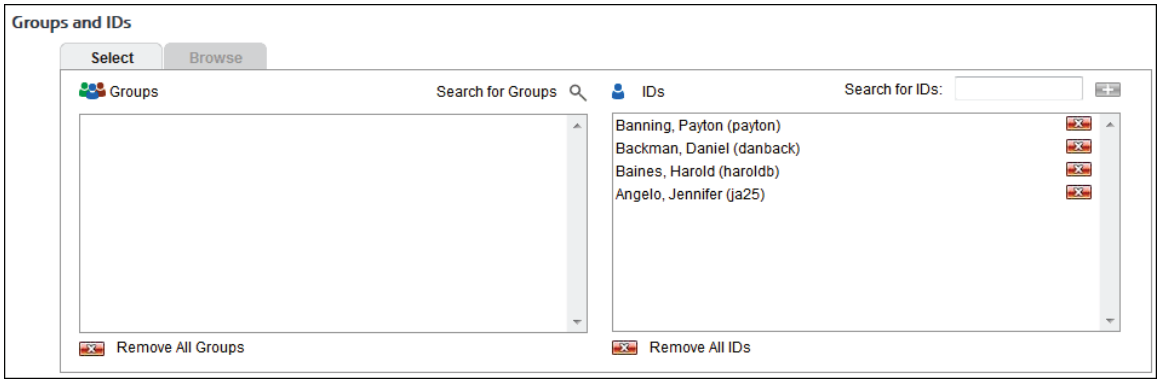


Other options include:

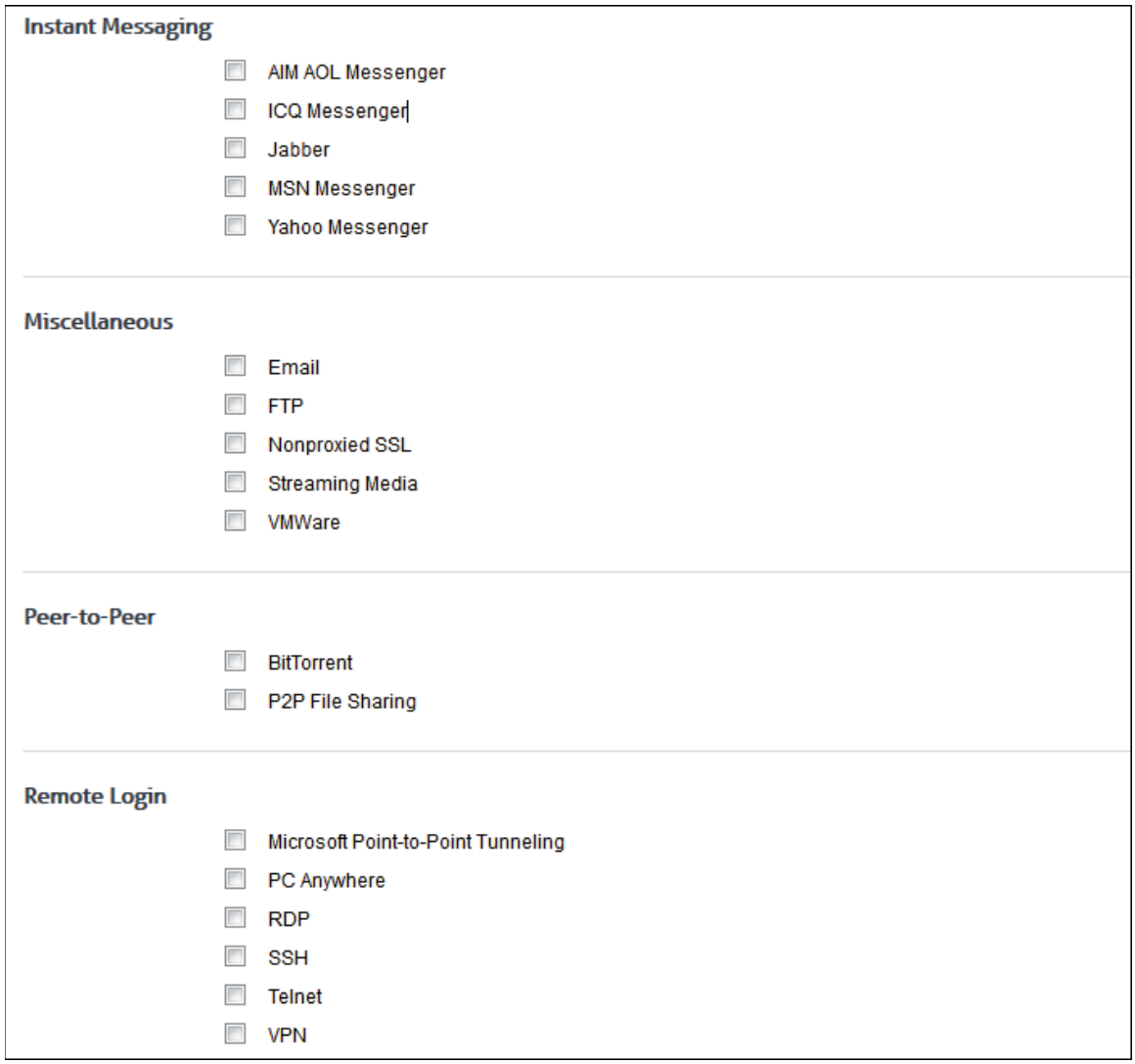
- **Expand or collapse groups:** To expand and view group tiers, click the plus icon. To expand or collapse all groups, click the plus or minus icon next to **Groups**.
- **Search for a specific ID:** If you know the ID names you want to filter, you can search for and select them using the **Filter selected 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.



5. 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.
6. Select the check boxes next to the protocols that you want to block.

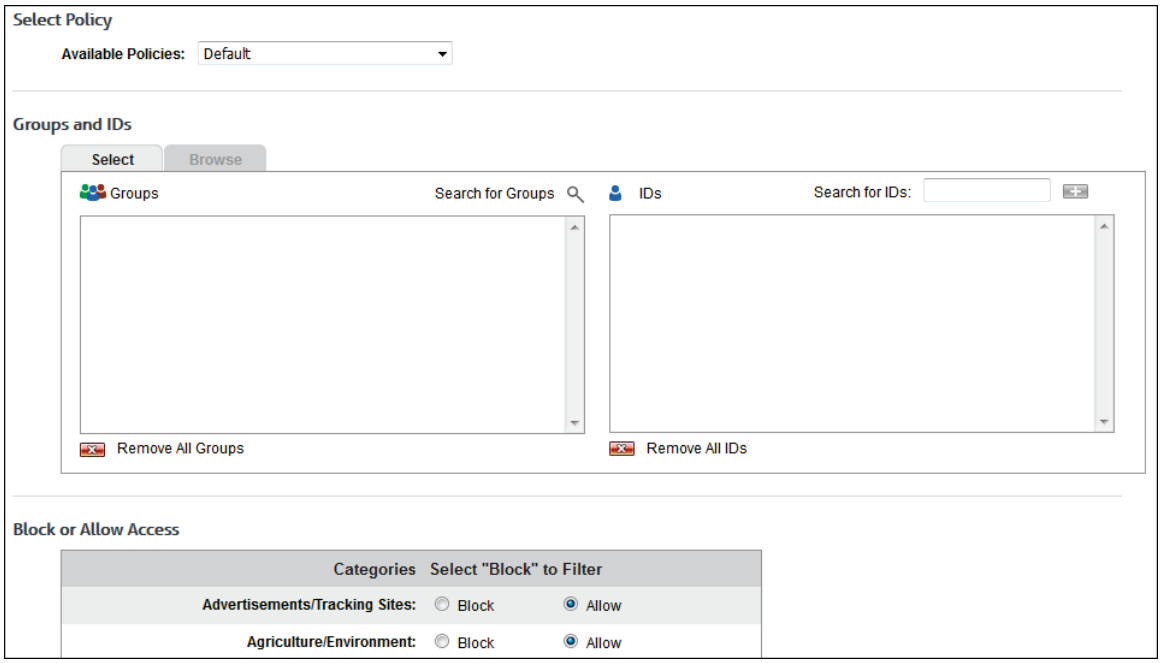


7. Click **Submit** to apply your settings.

Control Web Categories

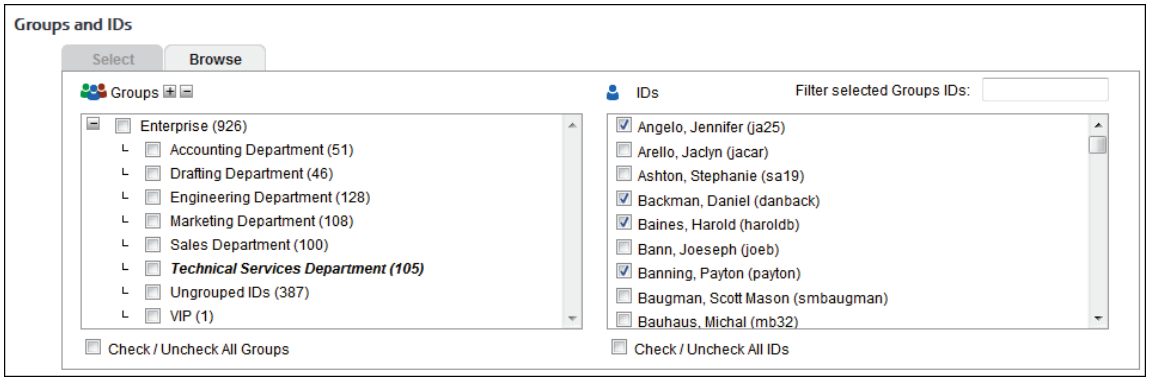
This page allows you to create, modify, and delete blocking policies for Web categories. Groups and IDs can be specified for each blocking policy you create. Therefore, you can choose to have multiple blocking policies, i.e., different policies for different groups and IDs, or you can choose to have one universal policy for the entire organization. You can also select what times of the day you want to block categories. For example, you may want to allow shopping sites during lunch, but block them for the rest of the day.

1. Go to **Web Management - Filter - Categories**. The Control Web Categories page is displayed.



2. Under **Select Policy**, in the **Available Policies** field, select *Create new policy* to create a new blocking policy, or you can choose to modify or delete an existing one.
3. After selecting *Create new policy*, enter a policy name in the **Available Policies** field (for example, Policy A). If you are modifying or deleting a previously created policy, its name will appear in this field. To rename the policy, click the pencil icon. To delete the policy, click the red x icon next to the field.

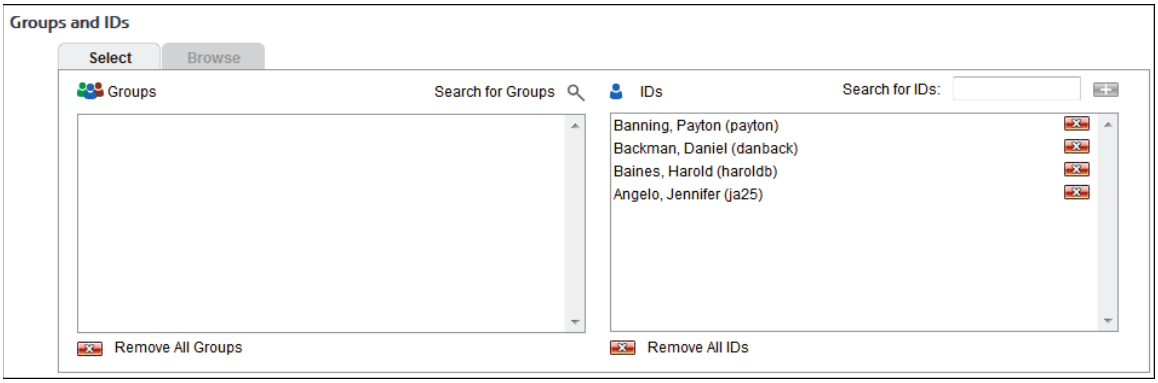
   NOTE: The Default policy cannot be deleted.
4. Under **Groups and IDs** on the Browse tab, choose groups and IDs by selecting their corresponding check box. To view IDs in a group, click the group name.



Other options include:

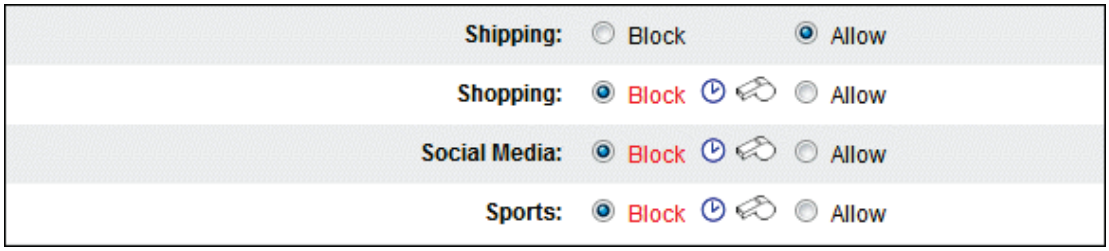
- **Expand or collapse groups:** To expand and view group tiers, click the plus icon. To expand or collapse all groups, click the plus or minus icon next to **Groups**.
- **Search for a specific ID:** If you know the ID names you want to filter, you can search for and select them using the **Filter selected 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.



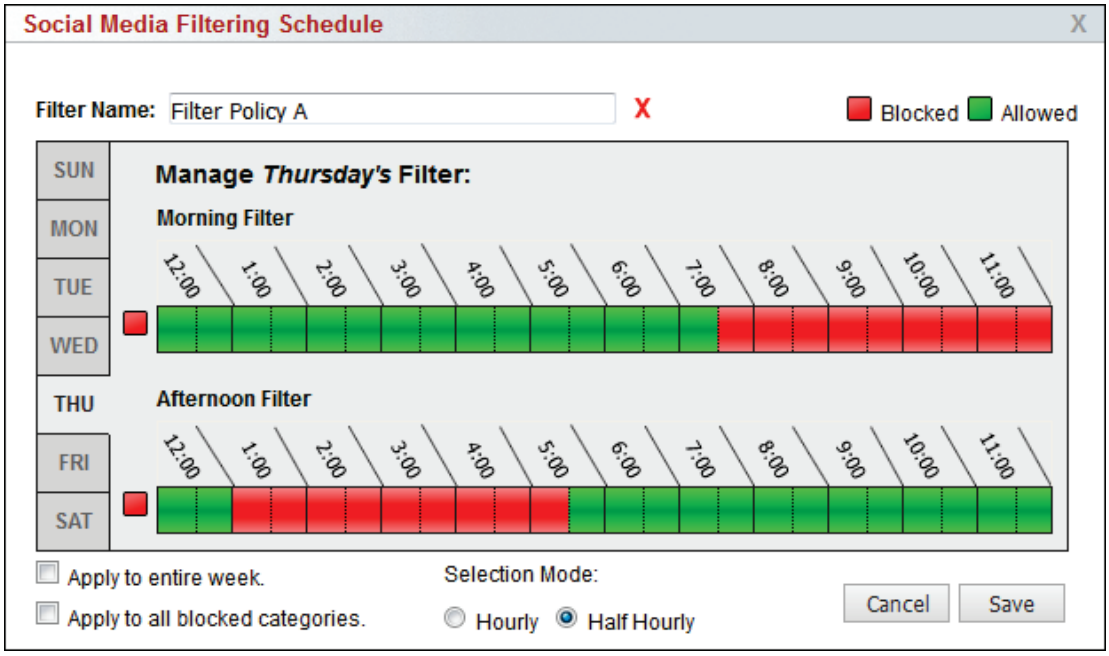
5. To delete a group or ID, click the corresponding red x icon. To delete all groups or IDs, click the **Remove All Groups** or **Remove All IDs** red x icon.
6. Under **Block or Allow Access**, apply a **Block** or **Allow** setting to each category by selecting the corresponding option.

   NOTE: If you know there are only a handful of categories to which you wish to allow access, scroll to the bottom of the page, and click **Block All**. Then, scroll up to select those categories that you want to allow (and vice versa).
7. If you apply a **Block** setting to a category, **Block** will change to the color red, and you will see a small clock icon next to it.



8. To apply blocking by 30-minute increments to the category, click the clock. The Filtering Schedule dialog box will appear.

   NOTE: By default, when you select the block option for a category, it will be blocked at all times.



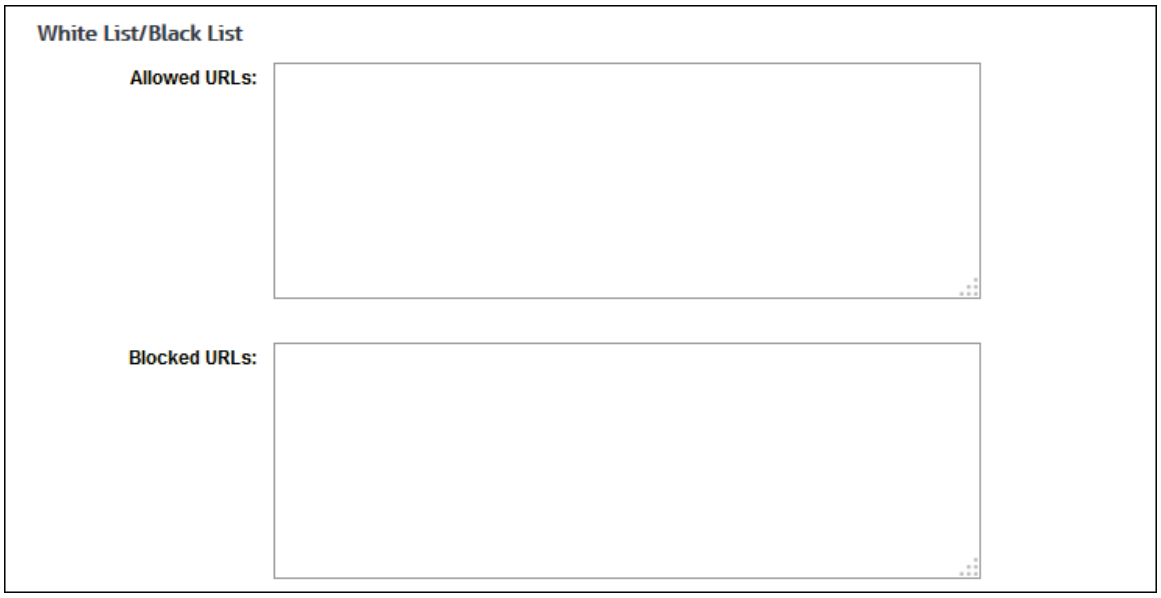
9. Click the table cells to select the times you want to allow access to that category. When you click a cell, the color will change from red to green indicating that the sites in that category can be accessed at that time. (Red = Block; Green = Allow)
10. If you want to apply these settings to all blocked categories, select the check box at the bottom.

    CAUTION: If you use this check box, your time selections will also apply to legal liability categories, e.g., Pornography, Gambling, and Hate/Crime. However, you can change the time policy for each of these categories by clicking the clock for each and changing all cells to red.

11. When you have finished making your time selections, click **Save**. If at any time you want to close the box without saving your changes, click **Cancel**.
12. Next to each blocked category a coaching icon appears.
    - Coaching allows authenticated/authorized users to override CyBlock's blocking function and to proceed to the site requested.
    - Coaching can be enabled on only categories that have been set to **Block**.
    - With coaching, traffic for the blocked category is allowed for 30 minutes and is logged in the database.
    - This traffic can be viewed on the Top Coached Traffic report.
13. If you want to enable coaching, click the coaching icon which will toggle from white (disabled) to red (enabled) . The following blocking message is displayed when coaching is enabled.

    NOTE: When using a redirect Web page for your Web Blocking Message, coaching cannot be used. When using a custom blocking message, token {6} must be included in your HTML file to enable coaching. See Web Blocking Message.

14. Under **White List/Black List**, you can create exceptions to your blocking policy. A white list can be used to allow access to specific sites while blocking all others in the corresponding category. A black list can be used to block access to specific sites while allowing all others in the corresponding category. For example, if you blocked the Search Engines category, but you wanted to allow access to Google, then you would type **.google.com* in the **Allowed URLs** box to allow access to that Web site.



15. To create a white list, in the **Allowed URLs** box, type the URL you want to allow.
16. To create a black list, in the **Blocked URLs** box, type the URL you want to block.

    NOTE: If you enter a URL that already exists in the Allowed URLs box, that URL will be removed, and the entry in the Blocked URLs box will be retained after you click **Submit**.

17. To add multiple URLs, enter the first URL and press ENTER; then enter the second URL and press ENTER. Repeat until you have included all the URLs.

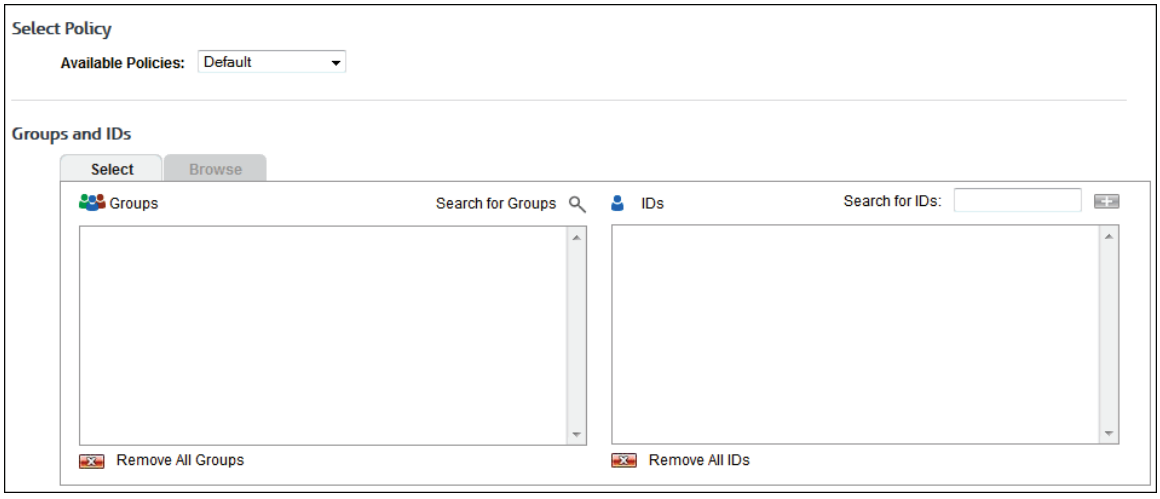
    NOTE: See Edit URLs for rules on adding wildcards in your URL entries.

18. To modify a URL, highlight the portion of the URL you would like to modify. Then type the changes.
19. To delete a URL, highlight the URL you would like to delete, and then press DELETE.
20. Click **Submit** to apply your changes.

Control Web Content Types

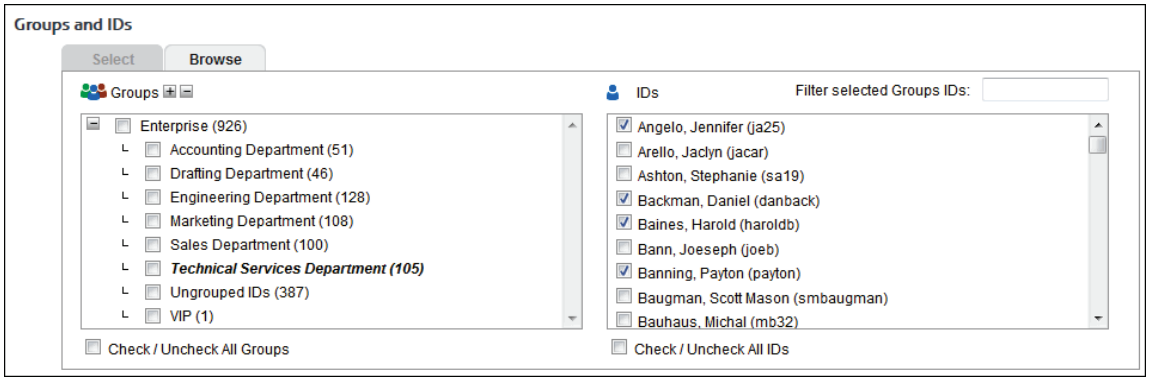
This page lets you go beyond blocking categorized Web sites. It allows you to actually block content found on Web pages. That is, it enables you to stop certain kinds of content from appearing on the Web page or being downloaded. This attribute can be used to block known file extensions (for example, .mp3).

1. Go to **Web Management - Filter - Content**. The Control Web Content Types page is displayed.



2. Under **Select Policy**, in the **Available Policies** field, select *Create new policy* to create a new blocking policy, or you can choose to modify or delete an existing one.
3. After selecting *Create new policy*, enter a policy name in the **Available Policies** field (for example, Policy A). If you are modifying or deleting a previously created policy, its name will appear in this field. To rename the policy, click the pencil icon. To delete the policy, click the red x icon next to the field.

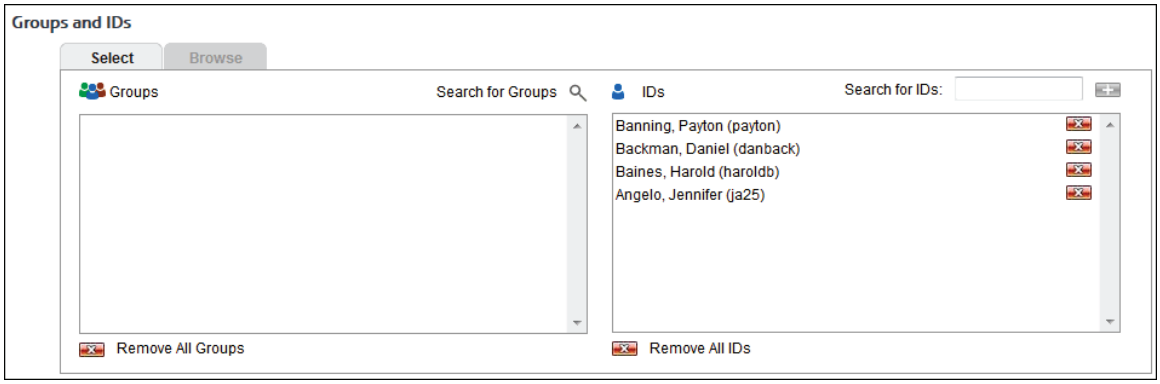
   NOTE: The Default policy cannot be deleted.
4. Under **Groups and IDs** on the Browse tab, choose groups and IDs by selecting their corresponding check box. To view IDs in a group, click the group name.



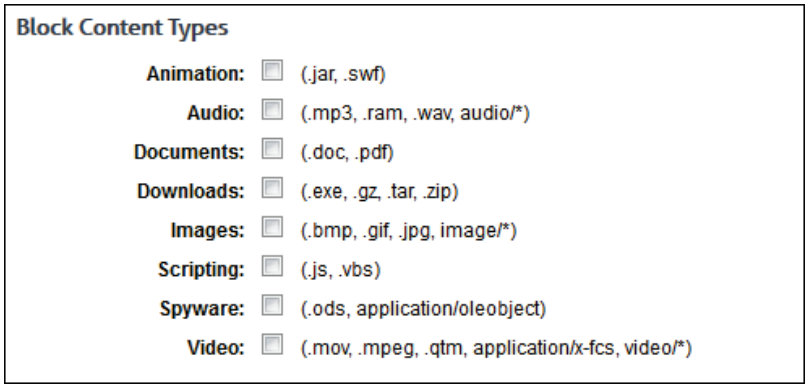
Other options include:

- **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.

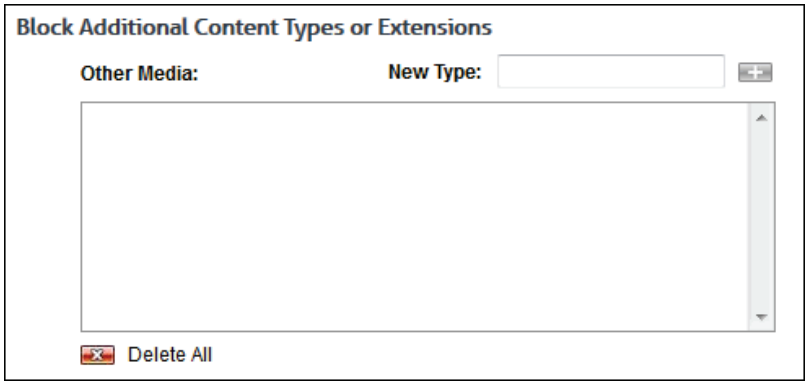
The groups and IDs that you have selected will appear on the Select tab.



5. 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.
6. Under **Block Content Types**, select the check boxes next to the content types and extensions that you want to block. Note that some content types cover all extensions with a wildcard. To block a specific extension, use the **Block Additional Content Types or Extensions** section below.

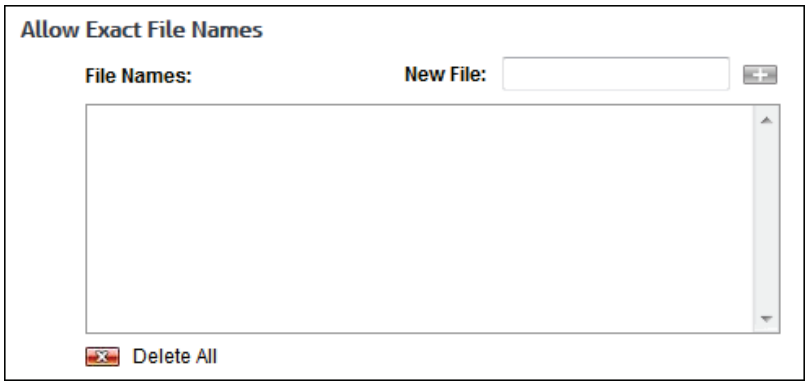


7. Under **Block Additional Content Types or Extensions**, to block additional content types or extensions, type the content type or extension in the **New Type** field, and press ENTER to add it to the **Other Media** box.

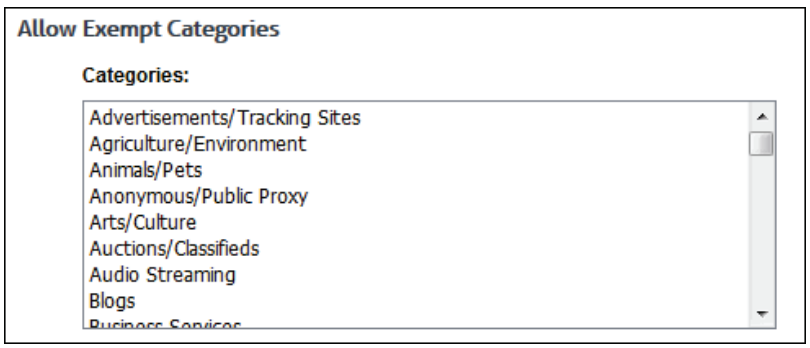


- Examples of content types include image/png, video/x-msvideo, and application/json.
- Examples of extensions include .png, .avi, and .json. Extensions entered without a period will be formatted with a period.

8. To delete a content type or extension, click the corresponding red x icon. To delete all content types and extensions, click the **Delete All** red x icon.
9. If you have blocked content types and extensions and would like to allow specific file names, under **Allow Exact File Names**, type the file name in the **New File** field, for example, reports.txt, and press ENTER to add it to the **File Names** box.



10. To delete a file name, click the corresponding red x icon. To delete all file names, click the **Delete All** red x icon.
11. If you have blocked content types and extensions and would like to allow specific categories to be exempt from blocking, under **Allow Exempt Categories**, select the first category by clicking it. Then hold down CTRL and click the additional categories you want to allow. To unselect a category, hold down CTRL and click the selected category.



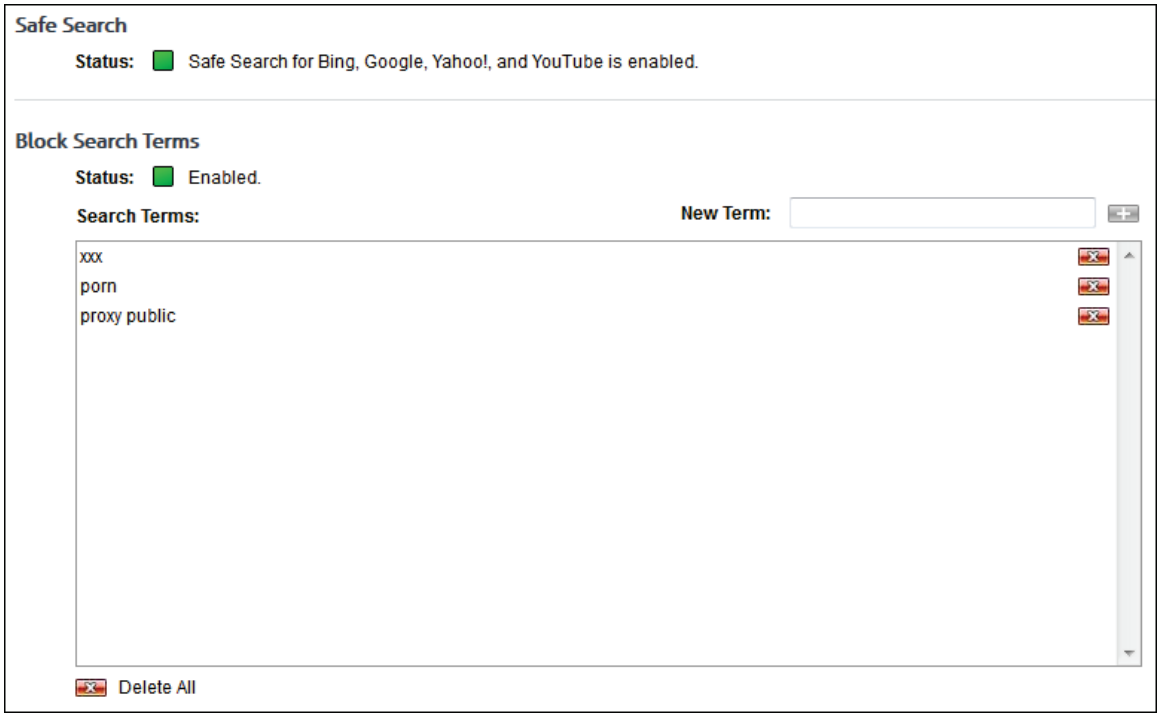
12. Click **Submit** to apply your changes.

13. If content types and extensions are entered in the browser address bar and they are blocked, the following examples of blocking messages are displayed.
    - CyBlocked Images Content
    - CyBlocked Extension
    - CyBlocked Images Extension
    - CyBlocked Documents Extension

Control Web Search Filtering

This page offers the ability to specify search terms to block in search engine results. It also allows you to force the Bing, Google, Yahoo!, and YouTube search engines to use a "strict" Safe Search setting. To use a secure connection (https://) to these sites, SSL Inspection has to be turned on for the categories in which these search engine sites reside. By default, this category is Search Engines. Enable SSL Inspection by selecting your groups and/or IDs and categories including any custom categories that contain these search engine sites. Adult content will then be filtered from search results.

1. Go to **Web Management - Filter - Web Search**. The Control Web Search Filtering page is displayed.



2. Under **Safe Search**, click the **Status** indicator to enable (green) or disable (red) safe search for Bing, Google, Yahoo!, and YouTube.
3. Under **Block Search Terms**, click the **Status** indicator to enable (green) or disable (red) the Block Search Terms feature.
4. To block a search term, type the search term in the **New Term** field, and press ENTER to add it to the **Search Terms** box.
5. To delete a search term, click the corresponding red x icon. To delete all search terms, click the **Delete All** red x icon.

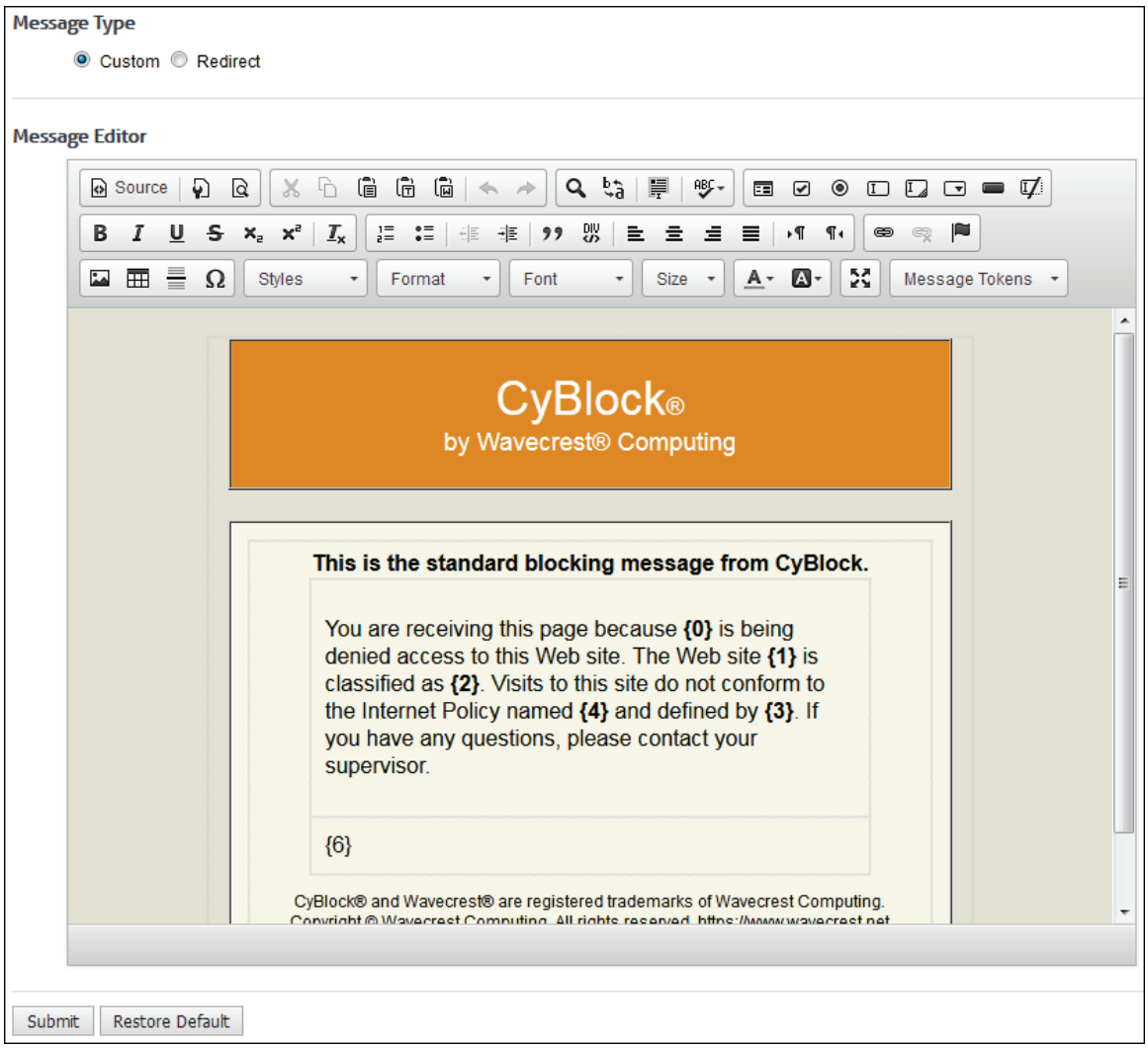
   NOTE: If the search term contains no spaces and exceeds the width of the **Search Terms** box, the red x icon will appear on top of the long search term to allow you to delete it.

Web Blocking Message

This page lets you customize a Web blocking message that will appear when a user tries to access a blocked Web site. You can use the Toolbar buttons in the Message Editor to change the formatting of the text and to add the necessary tokens in the blocking message. Or, you can specify a URL that the user will be redirected to when he or she tries to access a blocked site.

NOTE: If coaching is enabled for any categories on the Control Web Categories page, you will not be able to change the blocking message.

1. Go to **Web Management - Filter - Message**. The Web Blocking Message page is displayed.



2. Select **Custom** or **Redirect** to configure your Web blocking message.
3. If you selected **Custom**, in the **Message Editor**, the Wavecrest default blocking message is displayed. You can customize the blocking message to suit your needs.

   The following describes the available tokens, and their use within the blocking message file:

Token	Description
{0}	The user name that is being blocked.
{1}	The URL being accessed that caused the user to be blocked.
{2}	The category name that the URL is classified as.

{3} Your organization name as defined on the Update License Information page.
{4} The current filter policy name that is blocking the user.
{5} Not used for blocking messages.
{6} Coaching feature which is optional. If present and enabled on the Control Web Categories page, the user will be presented with a notice and a link to bypass the blocking message.

NOTE: To disable the Coaching feature on the Control Web Categories page, omit this token from the file.

4. If you selected **Redirect**, type the URL for the Web blocking message in the **Redirect To** field. The URL must include the protocol such as http://.

NOTE: Coaching is disabled when using a Redirect URL. See Control Web Categories.

5. Click **Submit** to apply your settings.
6. If for some reason you need to revert to the Wavecrest default blocking message, click **Restore Default**.
   - A confirmation dialog box is displayed.
   - Click **Restore Default** to restore the default message.

Bandwidth Management

Bandwidth throttling allows you to implement a restriction policy when enterprise bandwidth consumption exceeds a preestablished threshold. You can choose to implement one of two types of real-time bandwidth throttling policies:

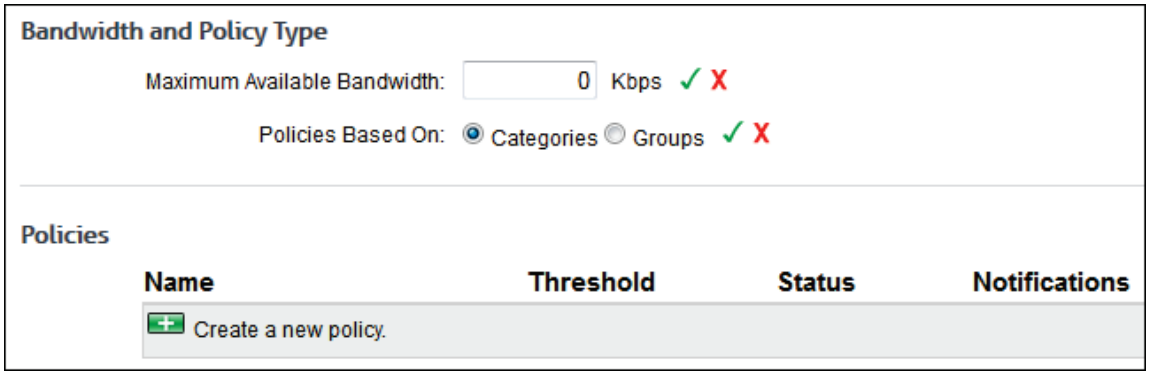
- **Category Control:** This type of policy is designed to limit bandwidth usage involving visits to sites in nonessential categories of Web sites. When this type of policy is triggered, CyBlock will impose a bandwidth cap on all visits to a specific Web category or to one or more sets of categories specified.
- **Group Control:** This type of policy is designed to restrict bandwidth available to users in designated groups when they visit high bandwidth sites (e.g., peer-to-peer file swapping and sites with video and audio). When this type of policy is triggered, CyBlock will apply a bandwidth cap to any member of a covered group visiting such sites.

You can choose to use Category Control policies or Group Control policies, but not both types at the same time.

A bandwidth throttling policy is activated when the overall enterprise bandwidth consumption exceeds a threshold level that has been set for that policy. Once activated, specific caps within the policy restrict the bandwidth that is available to users covered by that policy. For Web activity covered by the policy, bandwidth throttling slows the data transfer rate so it does not exceed the cap.

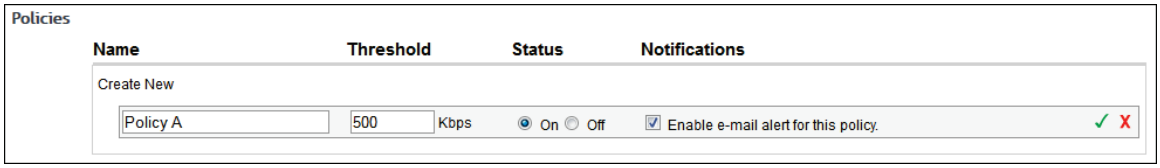
NOTE: A policy can have only *one* threshold, but it can have *multiple* caps if desired.

1. Go to **Web Management - Bandwidth**.

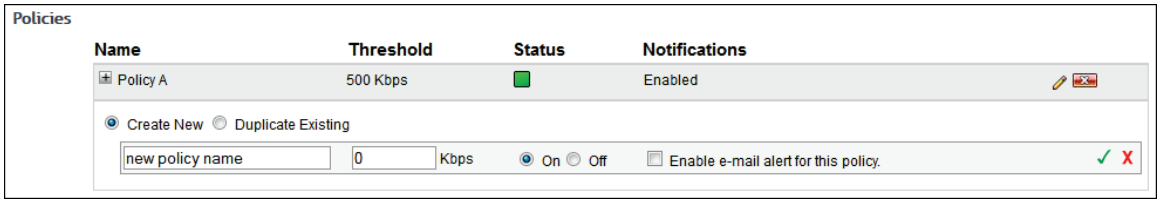


2. In the **Maximum Available Bandwidth** field, click the pencil icon, and type the total bandwidth available for Internet connection speed in your wide area network (WAN). Press ENTER, or click the green check mark. This field is for information only and does not impose restrictions on bandwidth. It works with the **Threshold** and **Cap Limits** fields in the following ways:
   - If you decrease the maximum available bandwidth to lower than the threshold, an error is displayed.
   - If you set the threshold to greater than the maximum available bandwidth, an error is displayed.
   - If the total of all cap limits exceeds the maximum available bandwidth, an error is displayed.
3. In the **Policies Based On** field, click the pencil icon, and select the **Categories** or **Groups** option. Click the green check mark.

   NOTE: If you create policies based on categories, you will have to delete all policies if you wish to change this to groups, and vice versa.
4. Under **Policies**, click the green plus icon to create a new throttling policy.

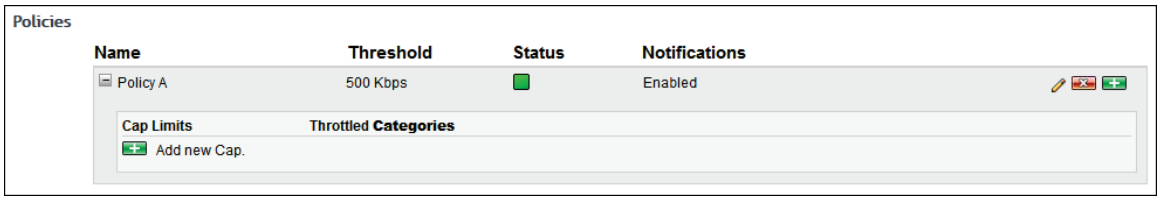


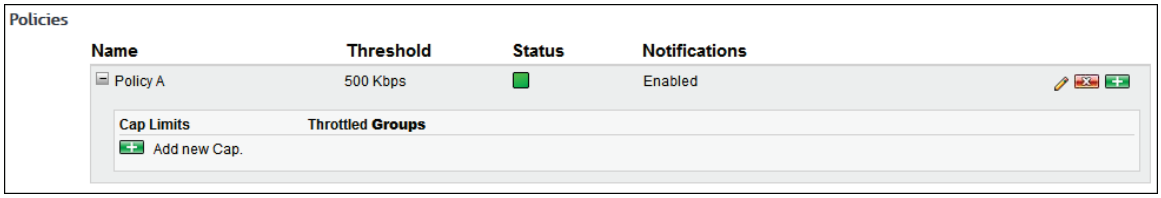
5. Enter a name for the threshold policy.
6. In the **Threshold** field, type the bandwidth threshold in kilobits per second (Kbps). When this threshold is reached, the policy is triggered, and the policy row is highlighted in orange.
7. In the **Status** field, select the **On** or **Off** option to enable or disable the policy.
8. In the **Notifications** field, select the check box if you would like an e-mail notification when this policy becomes active.
9. To save the policy, click the green check mark; or to cancel before saving, click the red x icon.
10. To turn the policy on or off, under **Status**, click the indicator to enable (green) or disable (red) the policy.
11. To edit the policy, click the pencil icon.
12. To delete the policy, click the red x icon.
13. To add a new policy, click the green plus icon.



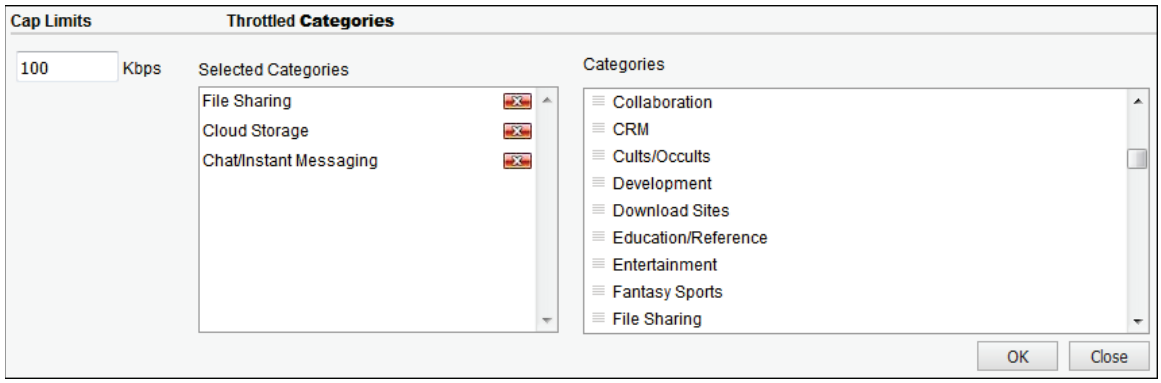
- Select the **Create New** or **Duplicate Existing** option. If you select **Duplicate Existing**, select the policy you want to duplicate from the Select Policy drop-down field.
- Complete and save the information for the new policy.

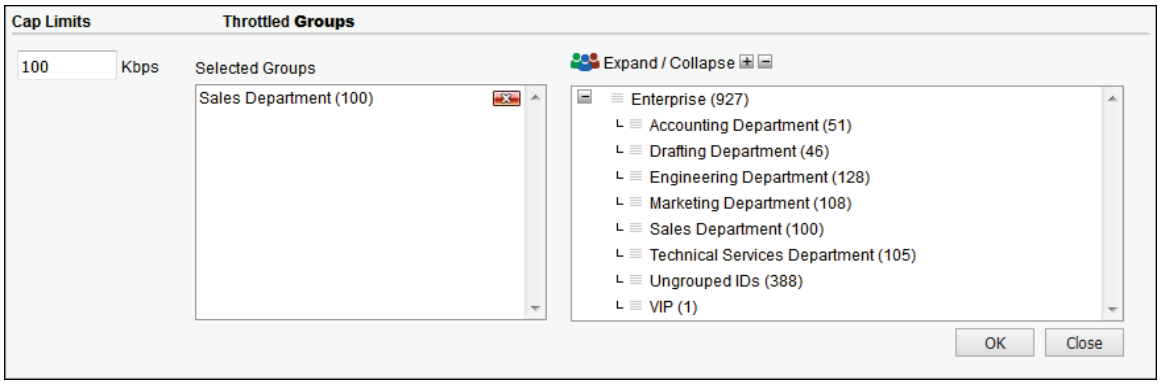
14. Use the plus icon next to the policy name to expand the policy and create, view, or edit caps. One of the following screens is displayed based on the type of policy you selected.





15. Under **Cap Limits**, click the green plus icon to create a new cap. One of the following screens is displayed based on the type of policy you selected.





16. Enter a cap limit in kilobits per second (Kbps). This limit is used to throttle the bandwidth used by the assigned categories or groups.

    NOTE: If set to 0, the category or group will be blocked when the threshold is reached, and the blocking message will be displayed.

17. Add categories or groups to which the bandwidth throttling cap applies by clicking and dragging categories or groups to the **Selected Categories** or **Selected Groups** box.

    NOTE: If you have two caps and want to add a category or group that is in cap 1 to cap 2, you will be notified that the category or group is already capped. If you choose to update caps, cap 1 will be deleted if it contains only that one category or group.

18. Click **OK** to save changes to the bandwidth throttling cap.

19. When a policy is activated, the following occurs:

    - The policy row is highlighted in orange. You can clear the alert by double-clicking the policy row and selecting **Clear Alert**. Click the green check mark to save the change.
    - An e-mail notification will automatically be sent to the administrator for each policy activated, if the policy is on and e-mail alerts are enabled.

Install CyBlock Client Piece

We recommend that you install CyBlock Client on all users' computers in order to block and monitor all non-HTTP protocols by ID (user names).

There are three ways to install CyBlock Client on your users' computers, and instructions for each of these methods are included in this section.

- Install CyBlock Client on all computers from one central location using PsExec
- Assign CyBlock Client using Active Directory GPO
- Install CyBlock Client manually

If you **do not** install the client piece on users' computers, you will not be able to block or monitor protocols by ID name or IP address. However, you can still apply a "universal" protocol blocking policy to the default ID name, "noclient," which is located in the VIP group. (The "noclient" ID can be moved out of the VIP group.) All protocol traffic viewed on the Real-Time Protocol Monitor will also show the "noclient" ID name.

Install CyBlock Client Using PsExec

NOTE: This client piece is only compatible with **Windows** computers. It will **not** install properly on **Linux or Mac** platforms.

1. Place your **cyblockclient.msi** file in a public, shared folder location to which all computers have access.
2. Download the **psexec.exe** utility as part of the **PsTools** package from the following URL:

   http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx

3. Unzip the **PsTools.zip** file.
4. From a **cmd prompt**, run the following command structure from the appropriate directory (where you have **PsTools**):

   psexec.exe * -u DOMAIN\ADMIN_ACCOUNT -p DOMAIN_ADMIN_PASSWORD msiexec /i "<SHARED PATH TO CYBLOCK CLIENT INSTALL>\cyblockclient.msi" /qn /L*v"<SHARED PATH TO CYBLOCK CLIENT INSTALL>/install.log"

Example: psexec.exe * -u WAVECREST\Administrator -p password msiexec /i "\\sharedcomputer\public\installs\cyblockclient.msi" /qn /L*v"\\sharedcomputer\public\installs\install.log"

5. In the command window, you will see the file being sent out to your domain computers.
    - You should see "**msiexec exited on.(computername)..with error code 0**" messages, indicating that the install worked with "zero errors," or "without error."
    - When the install is completed, the command prompt will sit at the "**PsTools**" directory.

NOTE: When this method is used to install CyBlock Client, it **automatically adds CyBlock Client to any Windows Firewall exceptions lists**.

Install CyBlock Client Using GPO

NOTE: This client piece is only compatible with **Windows** computers. It will **not** install properly on **Linux or Mac** platforms.

This method will assign CyBlock Client msi package "per-computer," which will install the program when the computer starts.

Create a Distribution Point

1. Log on to the server as an **Administrator**.
2. Create a shared network folder to contain the CyBlock Client msi package.
3. Set permissions on the folder to allow access to the CyBlock Client msi package.
4. Copy the CyBlock Client msi package into the folder.

Create a Group Policy Object (GPO)

1. On your Domain Controller server, open **Active Directory Users and Computers**.
2. Right-click your domain name and select **Properties**.
3. Select the **Group Policy** tab.
4. Select the GPO you want and click **Edit**.
5. Under **Computer Configuration**, expand **Software Settings**, right-click **Software Installation**.
6. Select **New** and click **Package.**
7. In the **Open** dialog box, type the full UNC path of the CyBlock Client msi package.
8. Click **Open.**
9. Click **Assigned,** and then click **OK**.
10. Close the **Group Policy** snap-in, and click **OK**.
11. Exit **Active Directory Users and Computers**.
12. The assigned CyBlock Client msi package will be installed automatically when computers start.

Prevent Users From Stopping CyBlock Client Service

1. Using an **Administrator** account, log on to a computer that has the CyBlock Client Service installed.
2. Install the **Group Policy Management Console** (GPMC). The URL to get the GPMC is:

    http://www.microsoft.com/downloads/details.aspx?familyid=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887

3. Start the **Group Policy Management MMC** (gpmc.msc).
4. Select the **OU** where you have placed the client computers.

   NOTE: If this is the *default* Computers OU, you cannot link a Group Policy Object. Instead, link it to the **domain**.
5. Right-click the **OU** and select the **Create and link a new gpo here** option.
6. Give the new GPO a name, such as *Policy to run CyBlock Client.*
7. Select the GPO itself, right-click, and select **Edit.**
8. Go to **Computer Configuration - Windows Settings - Security Settings - System Services**.
9. Select **CyBlock Client** from the list of services that appear.
10. Double-click the **CyBlock Client** service name.
11. Click **Define this policy**.
12. Change the security setting to only enable "real" admins to overrule these settings.
13. Set the **Service Startup mode** to **Automatic**.
14. Click **OK**.
15. Close the **Group Policy Management Console**.
16. Log off and by default, in 90 minutes the policy will refresh and be applied.

Install CyBlock Client Manually

You can manually install CyBlock Client on each user's computer by accessing the CyBlock Appliance browser interface.

1. Log on to the browser interface on the computer you wish to install CyBlock Client.
2. Go to **Web Management - Client**.
3. Under **Download and Install**, click the **Download** link.

Uninstall CyBlock Client Using PsExec

To uninstall CyBlock Client using PsExec, from a **cmd prompt** run the following command:

psexec.exe * -u DOMAIN\ADMIN_ACCOUNT -p DOMAIN_ADMIN_PASSWORD msiexec /x "<SHARED PATH TO CYBLOCK CLIENT INSTALL>\cyblockclient.msi" /qn /L*v"<SHARED PATH TO CYBLOCK CLIENT INSTALL>/uninstall.log"

Example: psexec.exe * -u WAVECREST\Administrator -p password msiexec /x "\\sharedcomputer\public\installs\cyblockclient.msi" /qn /L*v"\\sharedcomputer\public\installs\uninstall.log"

Data Management

Introduction

When logging is enabled, CyBlock Appliance logs all HTTP Web traffic. Reports can be run from these log files, or the log files can be imported into the Report Database where the data is compressed, which speeds up reporting. It is highly recommended that you use the Report Database if you have large amounts of Web-use data.

In managing your Web-use data, this section will show you how to:

- **Enable Logging** - Configure CyBlock Appliance to log Web traffic.
- **View Log Files** - View your configured log files.
- **Revalidate Log Files** - Revalidate any invalid log files.

NOTE: In a Hybrid deployment, your cloud log files can also be managed in the same manner as your local CyBlock log files.

Log file data can be imported into the Report Database where it is compressed. Most importantly, this will reduce report-generation time by more than 95 percent (compared to methods that generate reports by reading log files directly). This section will show you how to:

- **Configure the Report Database** - Connect to the metric sever to use the Report Database.
- **Import Log File Data into the Database** - Manually import configured log file data or schedule the import to occur daily.
- **View Data** - View the imported data.
- **Delete Data** - Delete data from the database.

To use the Report Database, you must first connect to the metric server. Once the Report Database is configured, the data will be stored for a limited time to enable generation of a variety of reports on a daily, weekly, or monthly basis.

Although processing data is active from the time the Report Database feature is first configured, the product is only designed to automatically retrieve and store “future” log file data as it is created in daily use. (It does not automatically “go back” and retrieve data generated prior to the Report Database being configured.) To populate the Report Database with past configured log file data, you can import these log files into the database manually. This data can then be used to generate reports covering past periods. Alternatively, you can select to convert all past data on the Schedule screen.

The primary benefit of using the Report Database is report-generation speed. When the database is used, a virtually unlimited number of authorized users can generate their own reports in minimal time.

For example, when the Report Database is configured, this product can run a large weekly Site Analysis report in seconds rather than hours and can run a monthly report in minutes rather than days. This dramatic reduction is made possible by storing the source data in the database.

With respect to scalability, this product can run a report based on 1 GB of data in about the same amount of time required to run a similar report by reading a 1-MB log file. With respect to persistence, once the data has been imported into the Report Database, you never have to read it again. The data remains stored and readily available for future use.

Another benefit is that the Report Database can hold immense amounts of data for long periods of time. This permits the generation of reports from the distant past if necessary.

Enable Logging

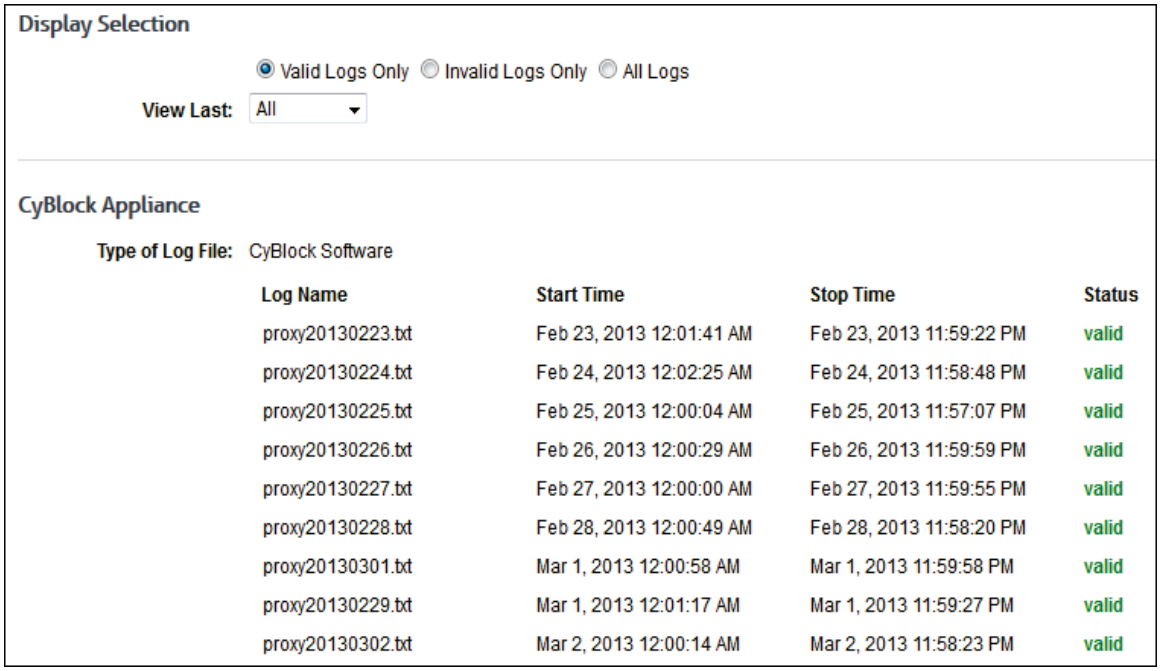
By default, CyBlock Appliance is set to log all Web traffic on-box, i.e., locally, allowing reports to be run on these local logs from the appliance interface. Most likely, you will not need to use this screen, unless you want to disable logging.

Go to **Data Management - Log Data Source - Setup** to view or make any changes to this screen.

View Log Files

This screen displays the log files that have been configured. The product uses these log files to produce reports. For each log file configuration, this screen displays the log file configuration name, type of log file, and path if applicable. For each individual log file, it displays the log name, start time, stop time, and status.

1. Go to **Data Management - Log Data Source - Viewer**, and the log files will appear on the opened page.



2. Under **Display Selection**, select an option to view valid logs only, invalid logs, or all logs.
3. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, a data configuration field is displayed to allow you to choose a configuration to view. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.
4. In the **View Last** field, select the time period of the log files you want to view. Data is displayed depending on your selections.

   Below are definitions of the information shown for each log file.

   Log File Configuration Name - The name for each configuration appears in the upper left of its displayed listing.

   Type of Log File - This is the log file source type.

Log Name - This column shows the name of validated files.

Start Time - This column shows the date and time of the first record in the log file.

Stop Time - This column shows the date and time of the last record in the log file.

Status - This column shows the status of log files for report generation purposes, using the three codes defined below.

- **Valid** - Log file can be used to generate reports.
- **Invalid** - Log file has a problem or is not compatible with report request.
- **Pending** - Validity has not yet been determined, i.e., current file has not been read yet.

Revalidate Log Files

This feature requires minimal use and instruction. If the product has not had a problem reading your configured log files, all log files should be valid, and you will not have to use this feature. If for any reason some log files are invalid, you should go to the **Data Management - Log Data Source - Revalidate** page. There the product will reexamine any "invalid" log files that were included in a configuration and may validate those that were previously invalid.

NOTE 1: For a log file to be valid, it must contain some Web-use data, i.e., it cannot be empty.

NOTE 2: If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, a data configuration field is displayed to allow you to choose a configuration to revalidate. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.

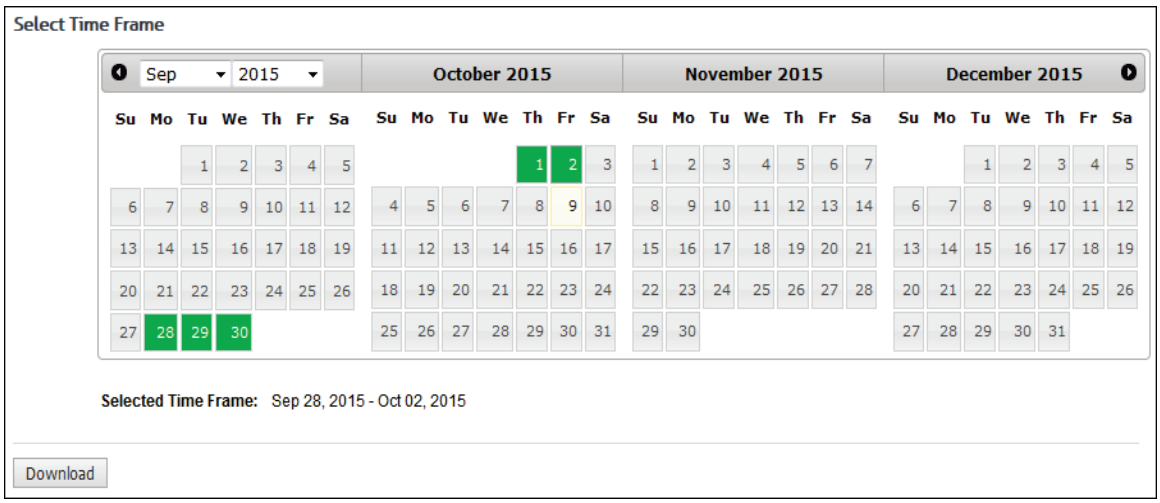
In some cases, the log files are invalid because the configuration is incorrect. If this is the case, you must fix the configuration in the **Data Management - Log Data Source - Setup** page. Once you have done so, you need to go back to **Data Management - Log Data Source - Revalidate** so that log files can be revalidated based on the revised configuration.

If your log files are still invalid, contact our Technical Support team. Our Support team is available Monday - Friday, 8:00 a.m. - 6:00 p.m. Eastern Time and can be reached by phone (321-953-5351) or e-mail (support@wavecrest.net).

Download

The Log File Download page allows you to download raw log files to a location of your choice.

1. Go to **Data Management - Log Data Source - Download**. The calendar displays the current date and allows you to select a single day or a range of days.



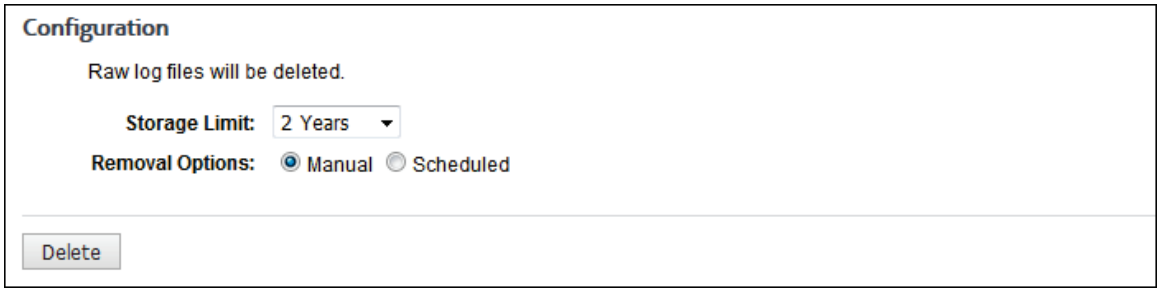
2. Click the start and stop dates of the data that you want.
3. The **Selected Time Frame** field shows the date range that you chose. If a single day was selected, that date will be displayed.
4. Click **Download**. The log files are compressed and combined into a .zip file.
5. In Firefox, a dialog box is displayed allowing you to open or save the file. Select what you would like to do with the file.

   NOTE: Other browsers may render this dialog box differently.

Log File Removal

The Log File Removal page allows you to delete raw log files from disk either at the current time or at the default scheduled time.

1. Go to **Data Management - Log Data Source - Delete**.



2. In the **Storage Limit** field, select the time period for the log files you want to retain. Log files older than this time period will be removed from disk.
3. For the **Removal Options** field, select **Manual** or **Scheduled**.
   - **Manual** - Use this option if you want to delete your raw log files at this time.
   - **Scheduled** - Use this option if you want to schedule automatic daily deletions to occur.
4. If you selected the **Manual** option, click **Delete**. A dialog box is displayed confirming the deletion. Click **Delete**.
5. If you selected the **Scheduled** option, your setting is automatically saved, and the Delete button is not available.

Report Database

The Report Database is a highly scalable database designed to store huge amounts of detailed, low-level Web-use data which is used to generate audit detail reports that provide every URL visited by a user, every category, or every domain. It also stores high-level data that is used to generate sophisticated, summary-level trending charts on the Dashboard.

To configure the Report Database, go to **Data Management - Report Database - Configuration - Settings**.

See also Settings.

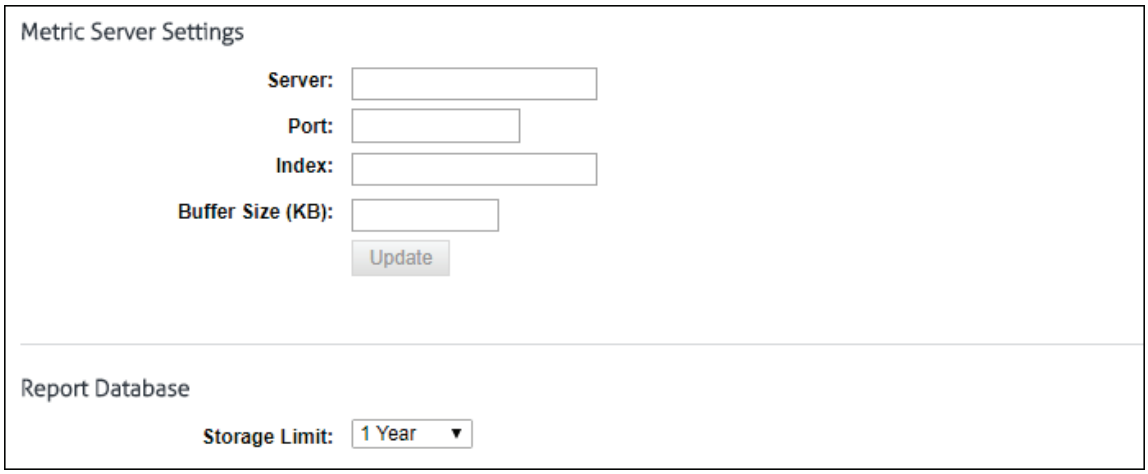
Settings

On this screen you have the ability to configure the Report Database in order to view Dashboard data and run high-level summary and audit detail reports. You can update the metric server settings as well as change the storage limit of your Web-use data.

Metric Server Settings

The metric server provides the Report Database for all Dashboard charts, summary reports, and audit detail reports, and the product must be pointed to it.

1. Go to **Data Management - Report Database - Configuration - Settings**.



2. The **Server**, **Port** and **Index** fields are prepopulated. Change the server IP address as necessary.
3. The **Buffer Size** field is also prepopulated, and you may change this if necessary.
4. Click **Update**.
5. The **Storage Limit** field is set to *3 Months* by default. You may change this if necessary, and your setting will be automatically saved. Any data older than this time period will be deleted at the default scheduled time.

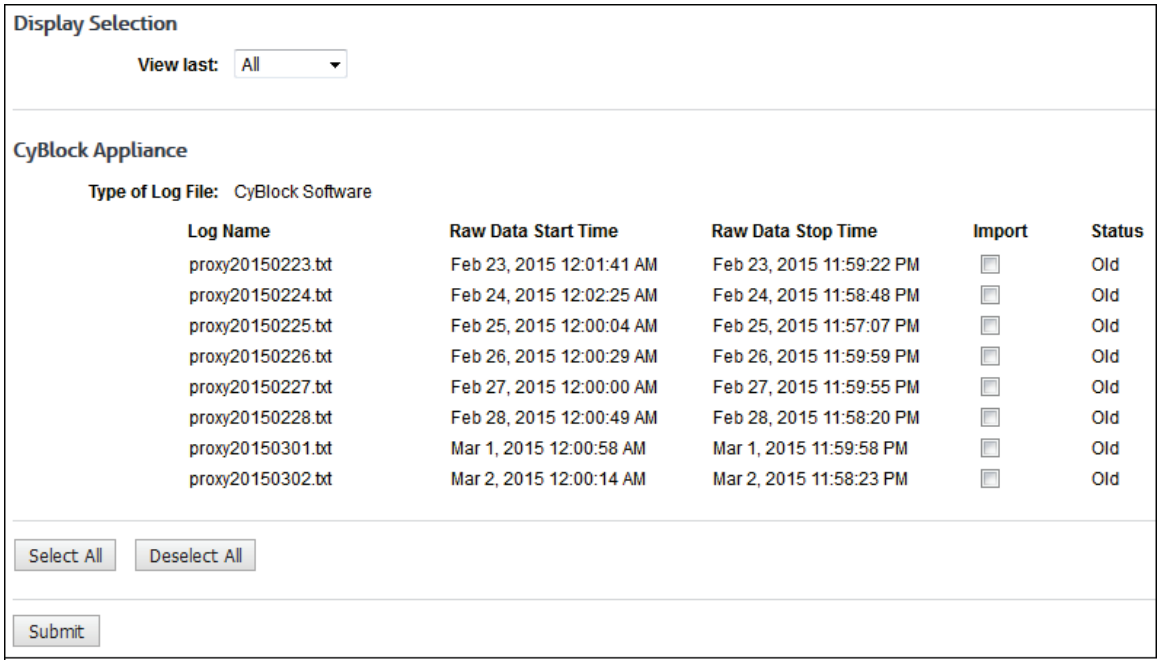
Import Log File Data

This page lets you manually import configured log files into the Report Database. When logs are available, the screen lists them and provides check boxes for selecting the logs you want to import. You can also configure the product to import the data automatically on a daily basis.

IMPORTANT: Because the process of importing data is memory intensive, we recommend increasing the product's memory setting on the **Settings - Memory** screen. As a general guideline, increase the setting to approximately half of the actual available memory on the computer.

NOTE: Importing data does not affect the original logs. This product only reads log file data; it does not modify log files in any way.

1. Go to **Data Management - Report Database - Import - Manual**. A list of logs available for importing will appear.



2. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Choose Configuration** field is displayed to allow you to choose a configuration to view. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.
3. In the **View Last** field, select the time period of the log files you want to view.
4. Select the **Import** check boxes of the logs that you wish to import. If you wish to import all of the logs, you can click the **Select All** button at the end of the log file list.

   NOTE: For a local CyBlock configuration, the **Import** check box is not displayed for the current day's log file because the proxy auto imports directly into the metric server.
5. Click **Submit** to import the logs into the database.

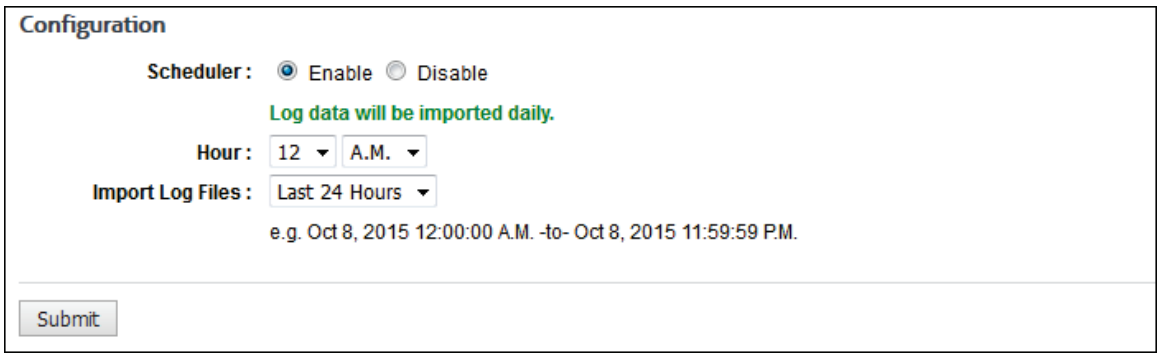
Schedule Data Import

This screen lets you schedule the import of log files into the Report Database. Be sure to configure the Report Database in order to use this feature.

IMPORTANT: Because the process of importing data is memory intensive, we recommend increasing the product's memory setting on the **Settings - Memory** screen. As a general guideline, increase the setting to be approximately half of the available memory on the machine.

NOTE: Importing data does not affect the original logs. This product only reads log file data; it does not modify log files in any way.

1. Go to **Data Management - Report Database - Import - Schedule**.

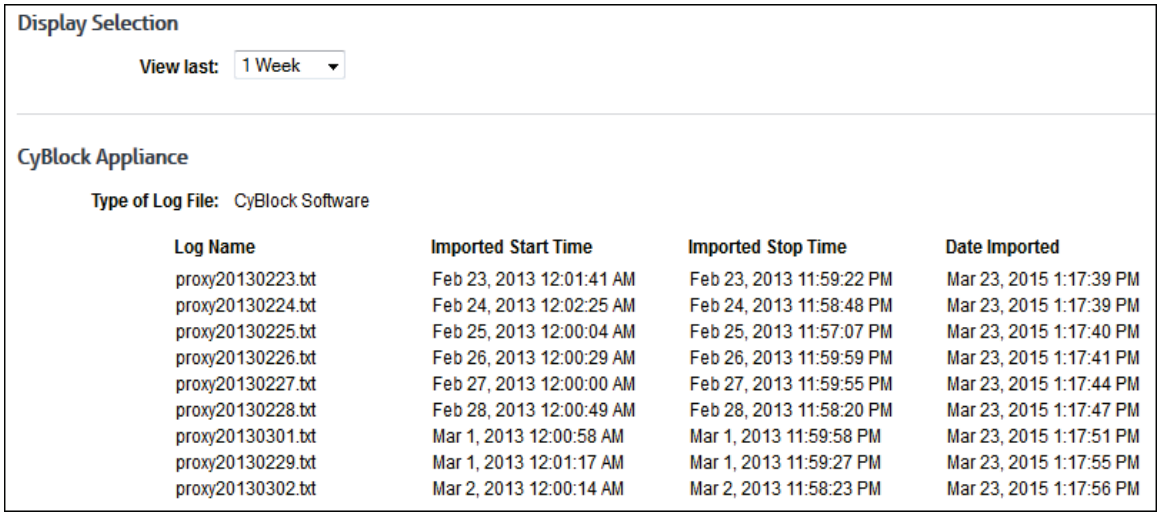


2. Select the **Enable** option to schedule the data import.
3. In the **Hour** fields, select the specific hour and time of day to begin importing data. If you have large amounts of data, you may want to schedule the data import process to run when Web traffic is low.
4. In the **Import Log Files** drop-down box, select if you want to import log files from the *last 24 hours* or if you want to import *all* log files.
5. Click **Submit** to apply your changes.

View Imported Data

This is a display-only feature. It displays the Report Database's imported log file data. For each imported data configuration, this screen displays the log file configuration name, type of log file, and path if applicable. For each log file, it displays the log file name, imported start date/time, imported stop date/time, and date imported.

1. Go to **Data Management - Report Database - Viewer**



Log Name	Imported Start Time	Imported Stop Time	Date Imported
proxy20130223.txt	Feb 23, 2013 12:01:41 AM	Feb 23, 2013 11:59:22 PM	Mar 23, 2015 1:17:39 PM
proxy20130224.txt	Feb 24, 2013 12:02:25 AM	Feb 24, 2013 11:58:48 PM	Mar 23, 2015 1:17:39 PM
proxy20130225.txt	Feb 25, 2013 12:00:04 AM	Feb 25, 2013 11:57:07 PM	Mar 23, 2015 1:17:40 PM
proxy20130226.txt	Feb 26, 2013 12:00:29 AM	Feb 26, 2013 11:59:59 PM	Mar 23, 2015 1:17:41 PM
proxy20130227.txt	Feb 27, 2013 12:00:00 AM	Feb 27, 2013 11:59:55 PM	Mar 23, 2015 1:17:44 PM
proxy20130228.txt	Feb 28, 2013 12:00:49 AM	Feb 28, 2013 11:58:20 PM	Mar 23, 2015 1:17:47 PM
proxy20130301.txt	Mar 1, 2013 12:00:58 AM	Mar 1, 2013 11:59:58 PM	Mar 23, 2015 1:17:51 PM
proxy20130229.txt	Mar 1, 2013 12:01:17 AM	Mar 1, 2013 11:59:27 PM	Mar 23, 2015 1:17:55 PM
proxy20130302.txt	Mar 2, 2013 12:00:14 AM	Mar 2, 2013 11:58:23 PM	Mar 23, 2015 1:17:56 PM

2. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Choose Configuration** field is displayed to allow you to choose a configuration to view. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.
3. In the **View Last** field, select the time period of the imported log files you want to view. You can use the Date Imported column to determine when data was imported.

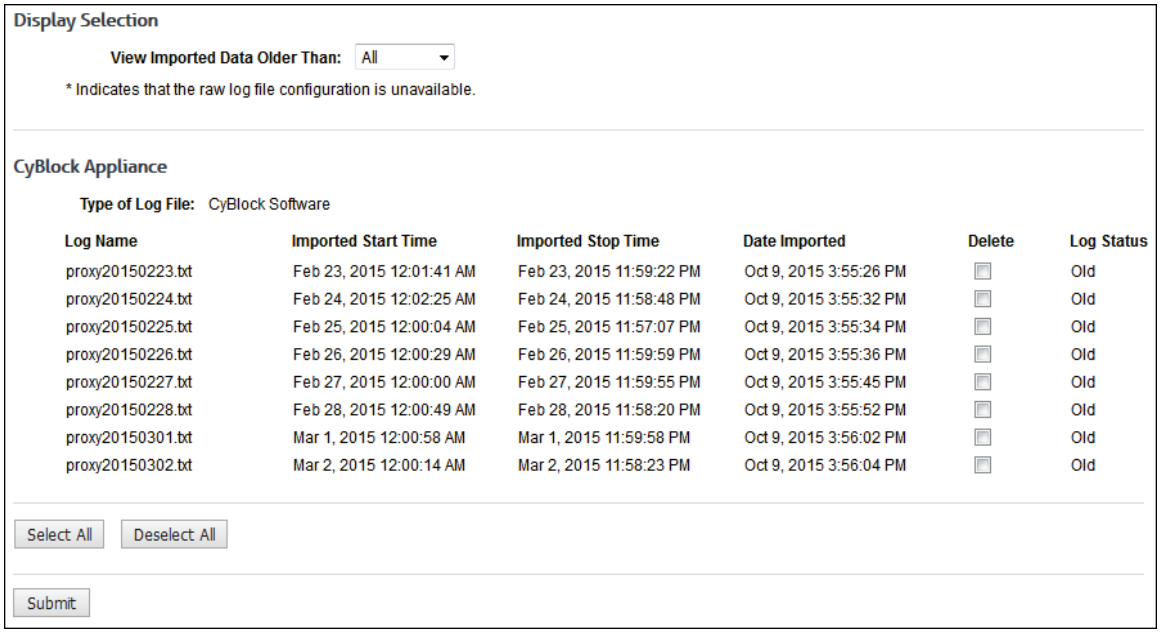
Delete Data

This feature allows you to delete database data manually. You can also schedule deletions to occur automatically once a day.

NOTE: Deleting database data does not affect logs or log file data. Wavecrest products only read and process log file data; they do not delete, alter, or distort log files in any way.

CAUTION: If you delete data from the database, you will not be able to generate Dashboard drill-down reports on that data. The product will try to reimport that data from available log files.

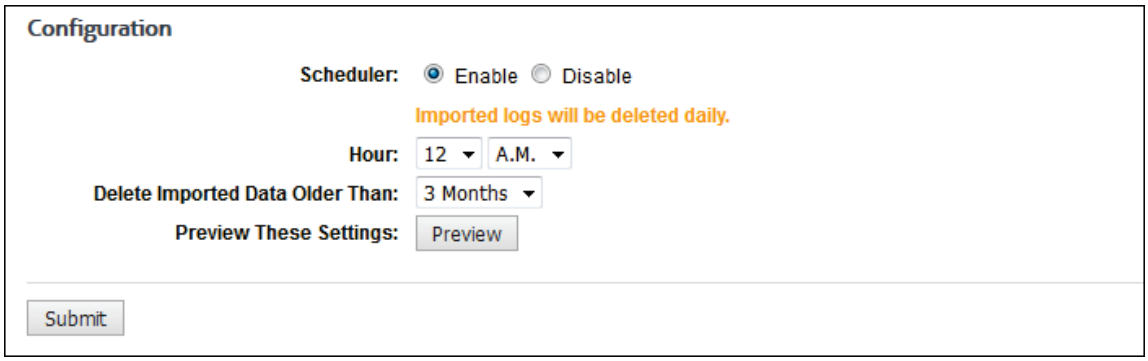
1. Go to **Data Management - Report Database - Delete - Manual**.



2. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Choose Configuration** field is displayed to allow you to choose a configuration to view. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.
3. Select the database data you want to see by using the **View Imported Data Older Than** field. You can use the Date Imported column to determine when data was imported.
4. Select the **Delete** check boxes of the imported data that you want to delete. If you want to delete all data, click the **Select All** button at the bottom of the page.
5. Click **Submit** to delete your selections.

Schedule Daily Data Removal

1. Go to **Data Management - Report Database - Delete - Schedule**.



2. Select the **Enable** option to schedule automatic daily deletions to occur.
3. In the **Hour** fields, select the specific hour and time of day to begin deleting data.
4. Using the **Delete Imported Data Older Than** drop-down box, select what old data you want deleted automatically.
5. Click **Preview** to view the data that will be deleted with these settings.
6. Click **Back** to return to the Schedule Daily Data Removal page.
7. Click **Submit** to apply your settings.

User Management

Introduction

In User Management you can input and import user ID information into the product for subsequent use in reporting and/or filtering. Users can be grouped in accordance with some common characteristic, usually by department (groups). They can also be entered without grouping (IDs). The groups and IDs import process can be performed manually or automatically. You also have the option of managing your groups and IDs (users) inside the product or at your directory source.

Setting up groups and IDs is a step in the Getting Started Checklist, which covers all setup procedures to get the product running. To complete this step in the product setup, you need to understand the product's grouping structure, which is discussed below.

The product consists of a core grouping structure for groups and IDs that can be used as is or expanded to fit your organization and its policies. The core structure cannot be deleted or changed. It contains a single top-level group called "Enterprise" and two subordinate groups called "Ungrouped IDs" and "VIP." You can add additional subordinate groups and/or individual IDs to Enterprise if desired.

The functions of these core groups are as follows:

- **Enterprise** - The Enterprise group encompasses all monitored users, specifically those Internet and/or intranet users whose IDs are made available to the product. For example, if Enterprise is specified during the setup of a report, all monitored users who accessed Web sites during the requested time frame will be included in the report. This will occur whether or not the user population has been subdivided into lower-level groups.
- **Ungrouped IDs** - This group is a subgroup to Enterprise. If you do not need user-grouping, all users can be placed in the Ungrouped IDs group. In that case, there would be no need to set up additional groups. On the other hand, if user-grouping is set up, Ungrouped IDs can be used as a "holding area" for IDs until they can be moved into your specific groups.
    - **AUP_Guest** - This ID is assigned when a guest user accepts the AUP on the AUP Only logon page to access your network.
- **VIP** - This group is another subgroup to Enterprise. It is used to exclude designated individuals from reports and applies a default blocking policy of "Allow All." When IDs are placed in this group, users' Web activity will not appear in reports, and users will be allowed full access to Web categories, Web content, and protocols unless the default policy is changed.
    - **Bypassed** - This ID is assigned when a user accesses a Web application that has been bypassed by the proxy and no login name is retrievable from the cache. See Bypass Authentication and Login Name Caching for more information on managing bypassed Web applications.
    - **Direct** - When bypassing URLs using a PAC file, this ID is assigned to any user accessing that URL through the CyBlock Appliance.

Next, you must decide whether or not you will use grouping. Using groups lets you apply different Web policy and report settings for each group. Even if you wish to use a universal Web-use policy for the entire company, you may wish to have individual department or division reports run and sent to their respective managers only. Grouping is also recommended if upper management or administrators want to see employee Web-use activity.

If you choose not to use grouping, we recommend that you place all of your users in Ungrouped IDs. You can populate Ungrouped IDs three different ways.

- When high-level reports such as Site Analysis are run, all new IDs in the log files (those not previously found) will be placed automatically in Ungrouped IDs.
- You can import IDs into Ungrouped IDs.
- You can manually add IDs to Ungrouped IDs.

In this section, you will find instructions on how to:

- **Configure Authentication** - Use different types of proxy authentication, specify if Web applications that fail to authenticate will be automatically or manually bypassed, create a cookie authentication or AUP Only page for your users to log on to your network, manage Web applications that do not authenticate, and manage login name caching for bypassed sites.
- **Edit Users** - Manually add groups and IDs or add them after your initial import, as well as delete, move, and modify groups and IDs.
- **Manage Users** - Specify how users will be managed. Completing this section is required (mandatory) before importing any groups and IDs.
- **Import Users** - Import from Active Directory or a text file.
- **Search Users** - Search for an ID, its group, and its policy settings.
- **Logon Accounts** - Change the password for accounts; and add, edit, and delete accounts.

Authentication Manager

The Authentication Manager is a feature that allows you to use different types of proxy authentication to support your organization, which may include your main office, remote users, and branch offices. You can choose to use NTLM authentication, cookie authentication, AUP only, or a combination of all three mixed with no authentication, or turn off authentication entirely. You can also create rules for various network definitions, such as an individual IP address, a range of IP addresses, and a host name.

Authentication is set to NTLM by default where login names are used for reporting and filtering. When authentication is enabled, you can automatically or manually bypass Web applications that fail to authenticate. You can also set up login name caching to cache the user name and IP address of every authenticated user. In conjunction with bypass authentication, the cache is used when connection requests are made, or it can be disabled to authenticate all connection requests.

When cookie authentication is enabled, a cookie is used to confirm that the user has been authenticated. The default length of time that the cookie will persist is 30 days. When a user enters a URL in the browser, he will be required to log on and accept your organization's Acceptable Use Policy (AUP) if this option is configured on the Authentication Manager - Cookie tab. A cookie will be created with this logon information, and the user will not be prompted again until the cookie expires.

The AUP Only option is used mainly by organizations, such as hotels, restaurants, airports, and those with guest networks, that do not require their customers to log on with credentials, but do require them to accept their AUP for liability reasons. The logon page presented to the user is configured on the Cookie tab.

You may want to disable authentication if you have servers that users are not logging on to or your network does not support login names. IP addresses will then be used for reporting and filtering.

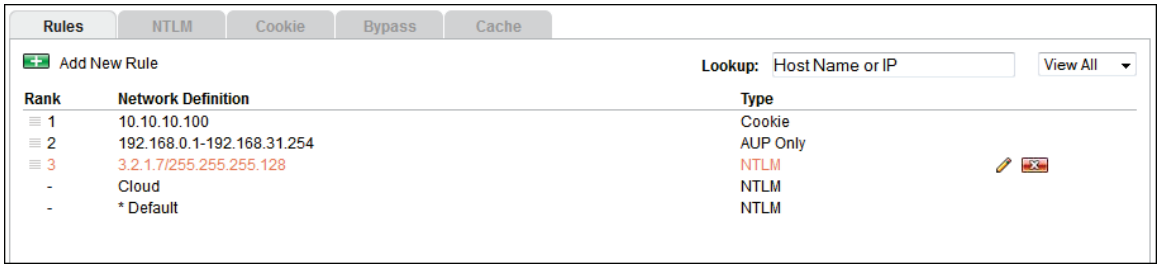
To configure proxy authentication, begin by creating your authentication rules.

Authentication Rules

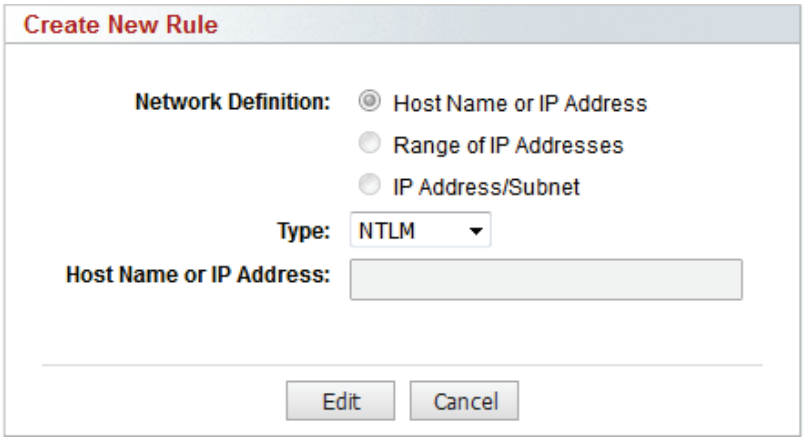
The Rules tab allows you to create authentication rules for various network definitions, such as an individual IP address, a range of IP addresses, and a host name. You may set authentication to NTLM, Cookie, AUP Only, or Disabled.

NOTE: If you are a Hybrid customer, a Cloud rule will be displayed when your CyBlock installation is paired with your CyBlock Cloud account on the Settings - Hybrid page. This rule is set to the authentication type of the Default entry and can be modified, but not deleted.

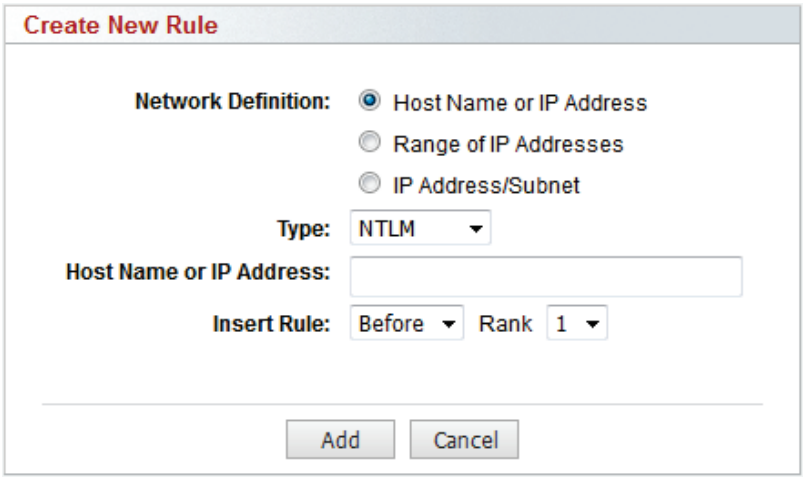
1. Go to **User Management - Authentication**. The Rules tab is displayed.



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 deleted.
3. To change the default authentication, hover over the rule line and click the pencil icon.

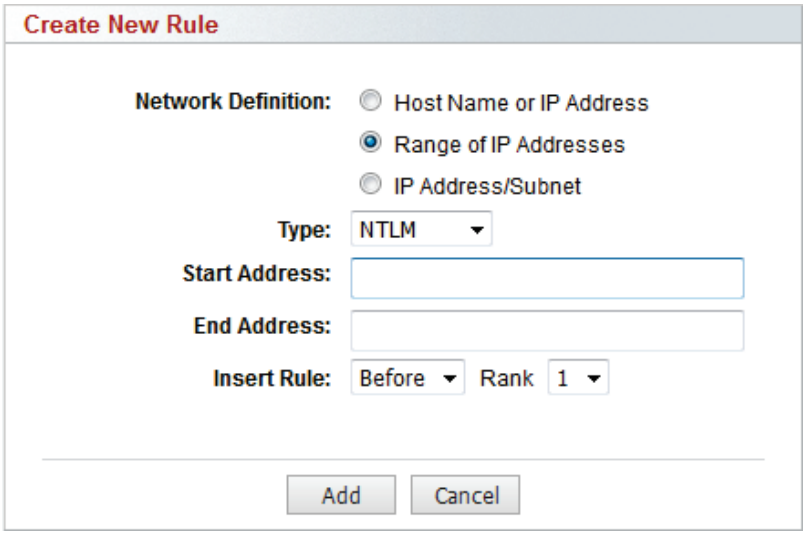


4. In the dialog box, you may only change the **Type** field. Select an authentication type from *NTLM*, *Cookie*, *AUP Only*, and *Disabled*. Click **Edit**.
5. To create a rule, click the **Add New Rule** green plus icon.

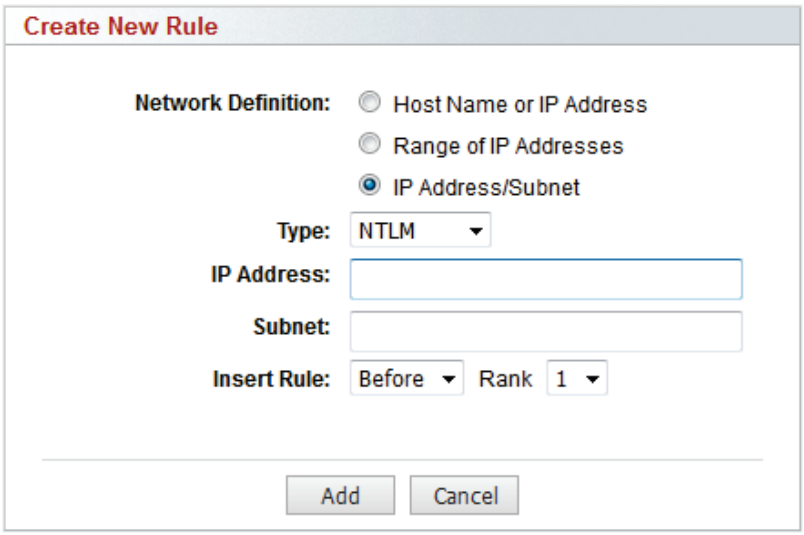


6. For the **Network Definition** field, select **Host Name or IP Address**, **Range of IP Address**, or **IP Address/Subnet**.
7. In the **Type** field, select *NTLM*, *Cookie*, *AUP Only*, or *Disabled*.
8. Complete the fields as follows:
    - If you selected **Host Name or IP Address**, type the 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.



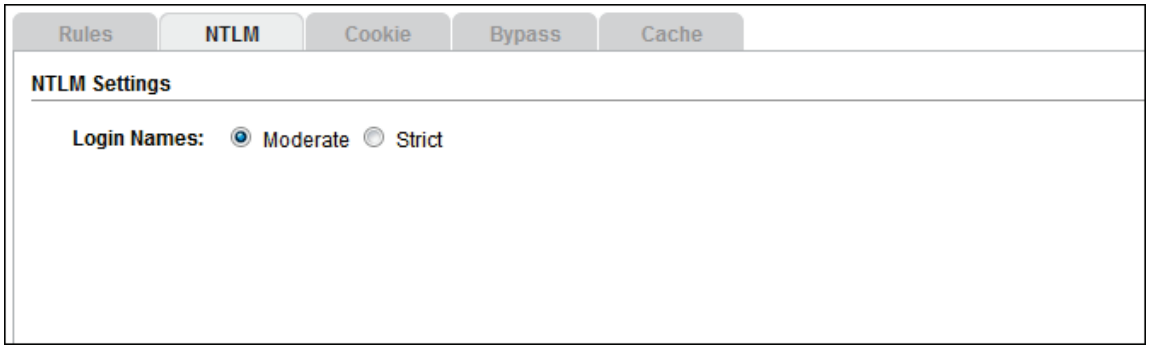
9. The **Insert Rule** fields allow you to specify where the new rule should appear in the list. Select *Before* or *After* and the rank number of an existing rule.
10. Click **Add**. Continue adding more rules as necessary. If a new rule overlaps an existing rule, a message will be displayed.
11. To 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*.

NTLM Authentication

In Moderate or Strict mode, NTLM authentication is enabled, i.e., login names are used for reporting and filtering, and the product is operating in an automatic bypass mode (see Bypass Authentication to learn more). This means that when a Web application fails to authenticate more than a set number of times, the product automatically takes action to work around the problem by bypassing authentication. The main reason a Web application may fail is because it was not designed to work with proxy authentication. This is why our CyBlock products include an automatic bypass feature that can *manage* it satisfactorily in real time so that mission-critical Web application operations can be sustained.

On this tab, you specify whether Web applications will be allowed or blocked if they fail to authenticate and are automatically bypassed.

1. Go to **User Management - Authentication** and click the **NTLM** tab.



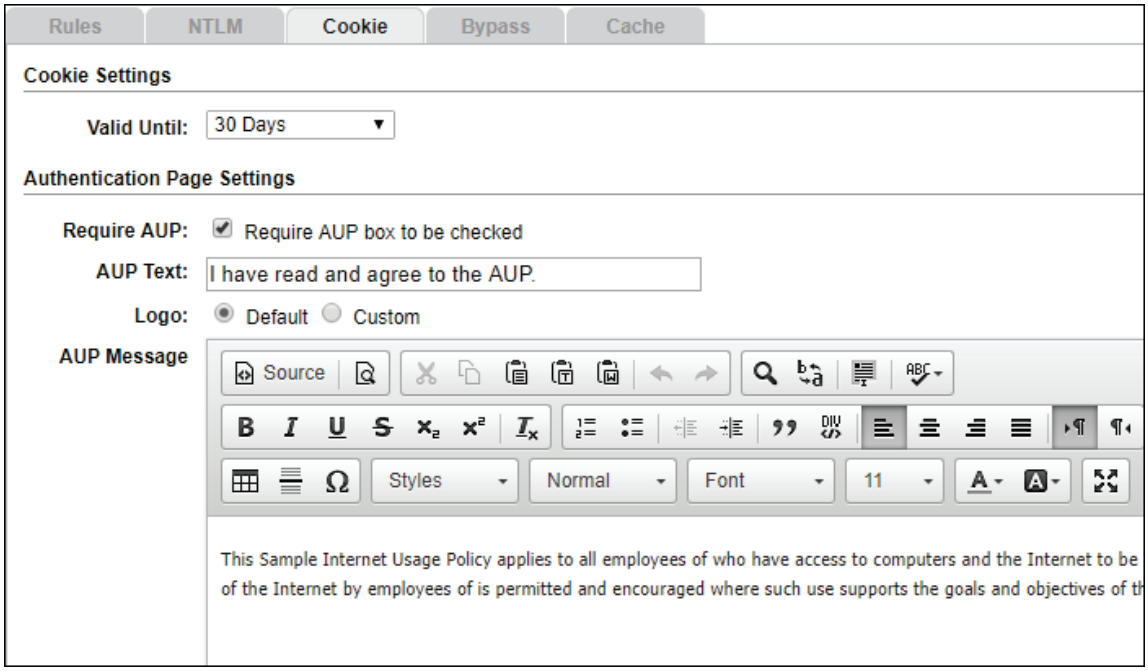
2. For **Login Names**, select **Moderate** or **Strict**.
    - **Moderate** - This is the default mode. In this mode, the cache is first checked for the Active Directory user name. If it is not in the cache, the "bypassed" user name is applied, and the Web application is allowed.
    - **Strict** - In this mode, the cache is also checked for the Active Directory user name. If it is not in the cache, the Web application is blocked. Administrators use "Strict" to validate users in their network.

    NOTE: User names are what most administrators prefer to display in reports, but if you have servers that users are not logging on to or your network does not support login names, you can change the setting to *Disabled* on the Rules tab. This will only log the IP addresses of users, not user names.

Cookie Authentication

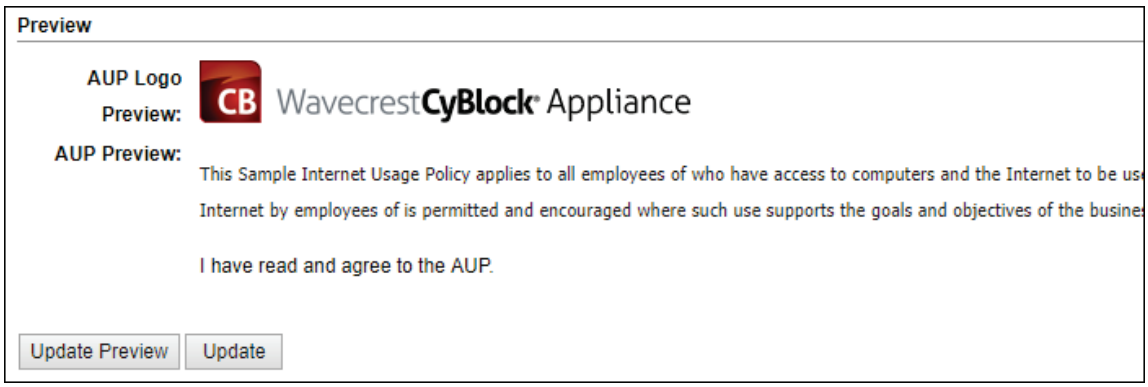
On this tab you define how long the cookie will persist and specify and preview the details of your cookie authentication logon page. This tab is also used to customize the AUP acceptance text, add the AUP text, and specify a logo for the AUP Only logon page.

1. Go to **User Management - Authentication** and click the **Cookie** tab.



2. Under **Cookie Settings**, in the **Valid Until** field, select the length of time that the cookie should persist. The default is 30 days.
3. Under **Authentication Page Settings**, select the **Require AUP** check box if you are requiring users to accept the AUP by selecting a check box.

   NOTE: If an AUP Only rule is being applied for guests accessing your network, accepting the AUP will always be required.
4. In the **AUP Text** field, type the text that you would like displayed next to the AUP check box.
5. For **Logo**, select **Default** or **Custom**.
   - **Default** - The CyBlock logo is selected by default. Anytime you want to use the default logo, select this option.
   - **Custom** - Select this option to customize your logo. The file can be placed in the ...\wc\jetty\interface folder, or it can be a URL. In the **Path** field, enter */file name* if the file is in the ...\interface folder or the full URL of the file including the protocol. If using a URL, also add this URL on the Authentication Manager - Bypass tab so that it will bypass authentication.
   - The logo should be 310x38 pixels and will be set to these dimensions if not this size.
6. In the **AUP Message** editor, type the text of the AUP.
7. Click **Update Preview** to preview the logo and AUP text for the logon page.



8. Click **Update** to save your changes.

Create Account/Forgot Password for Cookie Authentication

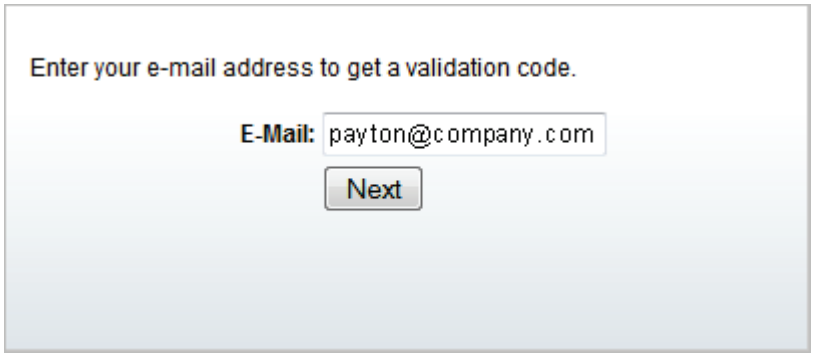
Cookie authentication requires an account for each user who wants to access the Internet through your network. When a user tries to access a Web site, a cookie authentication logon page is displayed that will allow users to create an account or reset their password if forgotten. When entering their credentials, you can require users to agree to the company's AUP before continuing on.

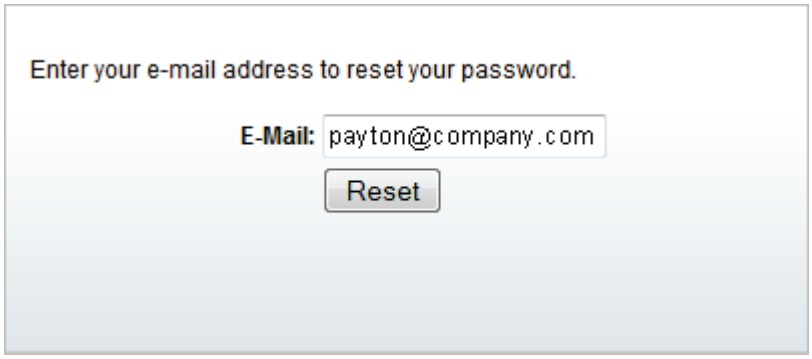
The length of time that the cookie will persist is established on the Authentication Manager - Cookie tab. On this tab, you can also create the cookie authentication logon page. To use cookie authentication, users must have an e-mail address entered in Groups and IDs.

1. When you access a Web site, the following screen is displayed.

2. In the **E-Mail** field, enter your e-mail address.
   - If you are creating an account, click **Create Account**.
   - If you are resetting your password, click **Forgot Password**.

   One of the following screens is displayed based on the link you clicked.

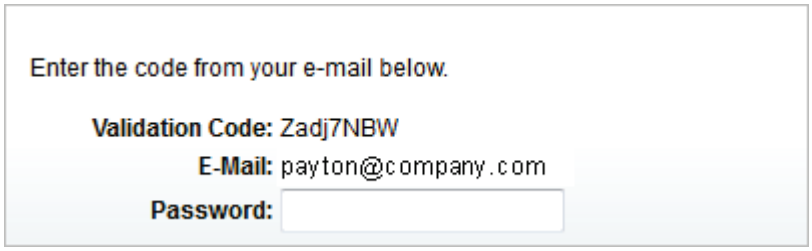




3. Continue with one of the following:
   - If you are creating an account, click **Next**.
   - If you are resetting your password, click **Reset**.

   A screen is displayed with a **Validation Code** input field.

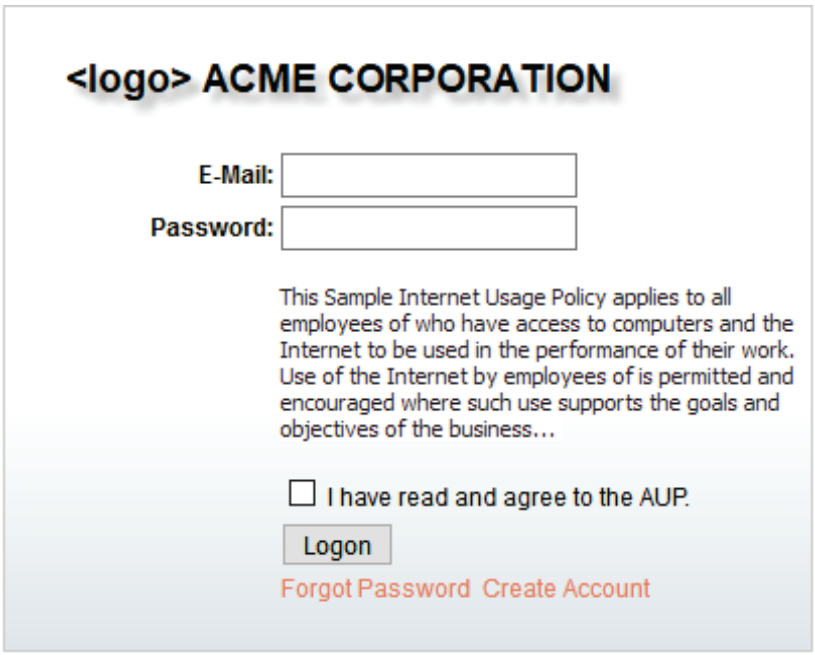
4. You will receive an e-mail message with a validation code and a link to enter a new password.
5. In the e-mail message, click the link. The **Validation Code** field will be populated with your code. Alternatively, you may return to the validation code screen to enter your code.



6. Enter your new password.
7. Select the check box to indicate that you have read and agree to the AUP.
8. Click **Continue**. A message is displayed indicating that your account is created or updated, and you are redirected to the Web site that you were trying to access.

AUP Only Logon Page

When an AUP Only rule is being applied, a logon page is presented to users requiring no user credentials. This page can be customized on the Authentication Manager - Cookie tab. You can include your company logo, enter the AUP text, and specify the text for the AUP check box.



Bypass Authentication

Bypass authentication uses automatic and manual techniques to prevent proxy authentication problems from interrupting Web application usage. It does this by automatically detecting problems and then employing "bypass" authentication techniques. While "detection and bypass" is its top priority, it also attempts (with a high success rate) to recover user names for reporting and filtering purposes–user names that otherwise would be lost when authentication is bypassed.

Bypass Authentication Process

Bypass authentication is operational any time NTLM or cookie authentication is enabled. Bypass authentication includes automatic and manual capabilities. It functions automatically to detect and then solve proxy authentication problems that users may encounter while working with Web applications. It provides manual capabilities that enable the product administrator to:

- Monitor potential and actual authentication problems.
- Take actions to prevent service interruption problems.

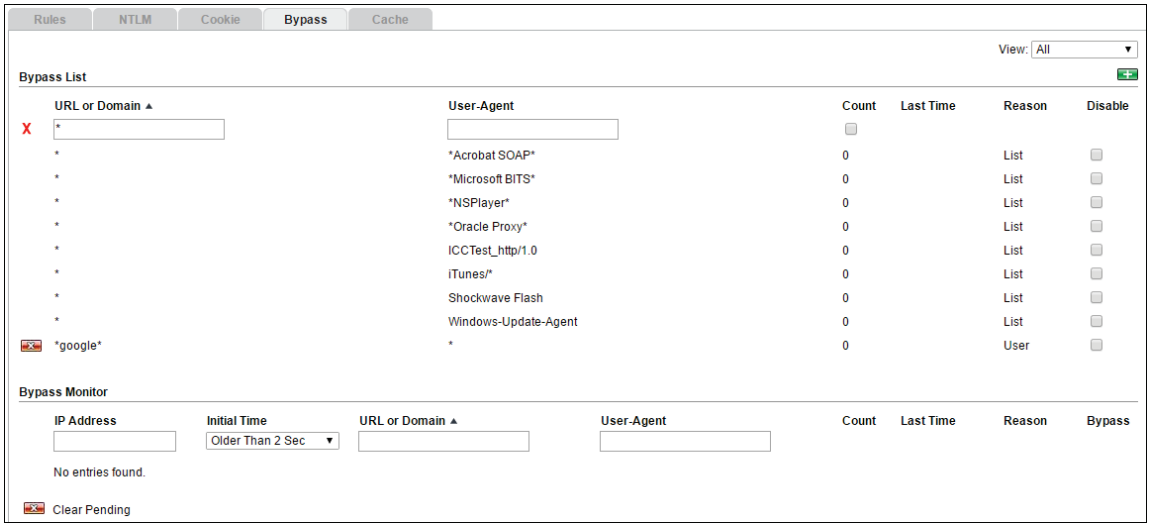
Definitions and Functionality

- **User-Agent (UA)** - The user-agent is a characteristic identification string in a header field that is used to identify the Web client. The function of the UA/Web client is to communicate via HTTP with Web servers that host Web applications.
- **URL/User-Agent (URL/UA) Combination** - Provided when a Web application failure occurs, a URL/UA combination is a two-part information element that includes the user-agent data discussed above and the URL that identifies the Web server that the client is attempting to connect with. When both data points are present, the combination clearly identifies and characterizes the client-server connection in a Web application process.
- **Bypass Monitor** - A list that records and temporarily stores the names of URL/UA combinations that fail to authenticate. Note that individual failures of a single combination are not listed separately in the Bypass Monitor, i.e., each combination is listed only once. If multiple failures occur, they are aggregated and summed as they occur. (See **Bypass Monitor Counter**.) It provides the ability to transfer entries to the Bypass List.
- **Bypass Monitor Initial Time** - The time in seconds that a URL was first challenged prior to the current time, e.g., 30 seconds ago. That is, if "Older Than 30 Sec" is selected, the filter will show entries older than 30 seconds.
- **Bypass Monitor Retention Period** - The Bypass Monitor storage period is 10 minutes. If a combination is still in the list when the period expires, it is automatically deleted. The administrator can delete it manually at any time.
- **Bypass Monitor Counter** - For each URL/UA combination on the Bypass Monitor list, failures are counted as they occur. When the count exceeds a set threshold and the minimum time is exceeded, the record is moved to the Bypass List.
- **Bypass List** - A list that stores the names of URL/UA combinations that are downloaded automatically with the daily Wavecrest URL List, are manually added by the administrator, or have exceeded the count threshold in the Bypass Monitor. Once a combination is on this list, the Web application that it identifies is exempt from authentication, i.e., authentication is “bypassed.” The storage period for this list has no limit.

  NOTE: If the product service is restarted, the **Count** field for each URL/UA combination in the Bypass List will be reset to 0. If a bypassed entry is edited, the **Count** and **Last Time** fields are reset for that entry.

- **Last Time** - This is the last date/time that the URL/UA was bypassed for authentication when in the Bypass List or the date/time that the last failed attempt occurred when located in the Bypass Monitor.
- **Reason** - The reason the URL/UA is bypassed or pending action. This column is mainly to help Technical Support troubleshoot any issues, but a few definitions include:
  -
  - **List** - The bypassed entry is included in the Wavecrest URL List.
  - **User** - The bypassed entry was added by the administrator.
  - **Closed** - The client decided to close the connection.
  - **401** - Access to the URL/domain requires user authentication, which has not yet been provided or has been provided, but failed authorization tests.

1. Go to **User Management - Authentication** and click the **Bypass** tab.



2. In the **View** field, select the entries you want to display, that is, *Bypass List*, *Bypass Monitor*, or *All*. For each view, a scroll bar is displayed if the number of entries overflows that section.

Bypass List

1. To filter the entries by URL/domain, type the URL/domain in the **URL or Domain** field.
2. To further refine the filter, you may enter a user-agent and/or select the **Count** check box. When **Count** is selected, only the number of successful attempts, greater than 0, is displayed. By default, the **Count** column shows all successful attempts including 0.
3. To clear the filter, click the **Clear Filter** red x icon.
4. To add a bypassed entry, click the green plus icon. Enter the **URL or Domain** and **User-Agent** fields in the dialog box, and click **Add**.
5. To edit a bypassed entry, place the mouse pointer over the URL/domain or user-agent that you want to edit and click that entry. Make your changes in the dialog box, and click **Modify**.
6. You can use wildcard entries to cover multiple URLs/domains and user-agents. Wildcards are denoted with a *. Examples of wildcard use with URLs/domains include:
   - URL name ends with ford.com/ - enter **.ford.com/*
   - URL name starts with http://www.ford - enter *http://www.ford.**
   - URL name contains .ford - enter **.ford.**
   - User-agent exists, but no URL/domain exists - enter *

   NOTE: The above examples also apply to the **User-Agent** field.
7. To delete a bypassed entry, click the red x icon next to that entry.

   NOTE: If there is no icon next to the bypassed entry, this means it is part of the Wavecrest URL List and cannot be deleted.
8. To disable a bypassed entry, select the corresponding check box in the **Disable** column.
9. To sort the bypassed entries, click the **URL or Domain**, **User-Agent**, or **Last Time** column title to sort by that column. An arrow is displayed next to the column title when you hover over it indicating that the column is sortable. The default sort is by **URL or Domain** in ascending order.

Bypass Monitor

1. To filter the entries by IP address, type the IP address in the **IP Address** field.

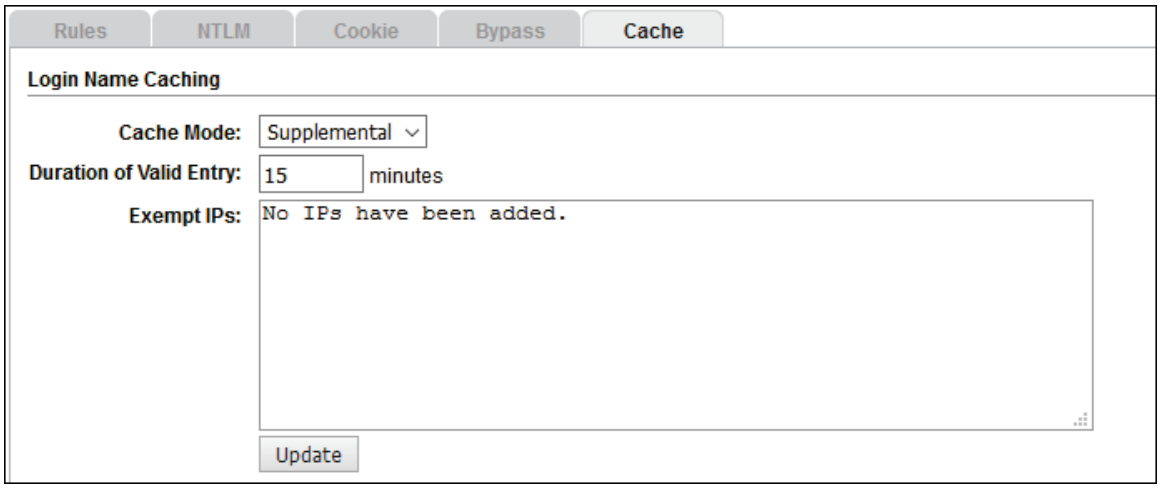
2. To further refine the filter, you may select an option in the **Initial Time** field, enter a URL/domain, and/or enter a user-agent.
3. To clear the filter, click the **Clear Filter** red x icon.
4. To transfer entries from the Bypass Monitor to the Bypass List, select the corresponding check box in the **Bypass** column to move the entry to the Bypass List.
5. To sort the entries, click the **Initial Time**, **URL or Domain**, **User-Agent**, or **Last Time** column title as previously described.
6. To clear the Bypass Monitor, click the **Clear Pending** red x icon to immediately remove all entries from this section.

Login Name Caching

Login name caching is a "holding location" (e.g., memory) that CyBlock products use to temporarily record the unique user name and IP address of every authenticated request for Internet access. If the product is configured to bypass a URL/User-Agent entry and login name caching is enabled, the product will be able to authenticate users with the cache versus using the user name of "bypassed."

This tab is used when NTLM or cookie authentication is enabled and also with the entries on the Authentication Manager - Bypass tab.

1. Go to **User Management - Authentication** and click the **Cache** tab.



2. In the **Cache Mode** field, select one of the following options:
   - *Primary* - In this mode, cache is used when connection requests are made. If a cache entry is not found or is invalid, authentication occurs and user names are added to the cache.
   - *Supplemental* - This option is the default. If authentication fails or an entry in the Bypassed list is accessed, the cache is used before the user name “bypassed.”
   - *Disabled* - In this mode, cache is never used, and all connection requests are authenticated. Entries in the Bypassed list are given the user name “bypassed.”
3. In the **Duration of Valid Entry** field, type the number of minutes in which you want login name caching to refresh. Since first added, cache entries will be available for this length of time in cache before they are cleared. The default is 15 minutes.
4. In the **Exempt IPs** field, enter any IP addresses to exclude from login name caching.
   - Wildcards (e.g., asterisk (*)) in IP addresses are not matched and should not be used.

- If Cache Mode is *Supplemental* and multiple users are using the same IP address at the same time (e.g., a server) within the duration entered above, the IP address will be automatically added to this list.

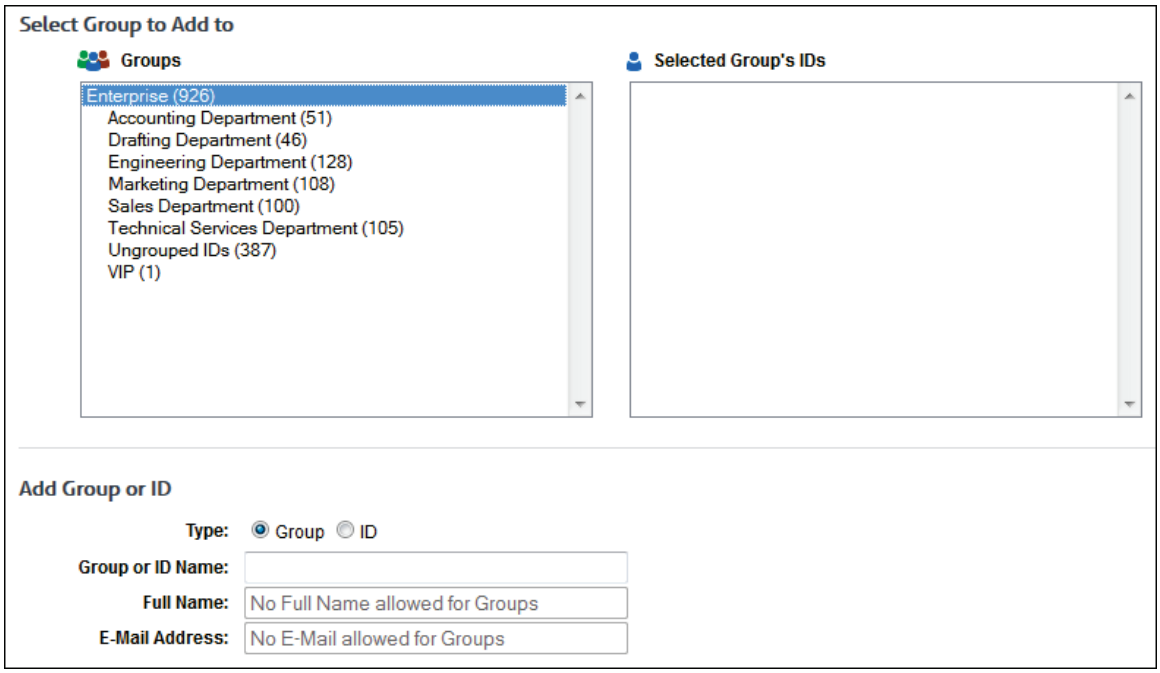
5. Click **Update** to save your changes.

Add Group or ID

If you do not want to import groups and IDs, you can manually add each group or ID in the product. Even if you imported your groups and IDs, you can add more if you chose to manage your groups and IDs inside the product (see User Management - Import Users - Manage). If you chose to manage them outside the product, you can only add groups and IDs to your directory source and reimport. This page will not be available to you.

NOTE: If you plan to have groups, we recommend that you create all groups first before creating the IDs to go in each group.

1. Go to **User Management - Edit Users - Add**. The Add Group or ID page is displayed.



2. In the **Groups** box, select the "parent" group to which you wish to add the group (for example, Enterprise).

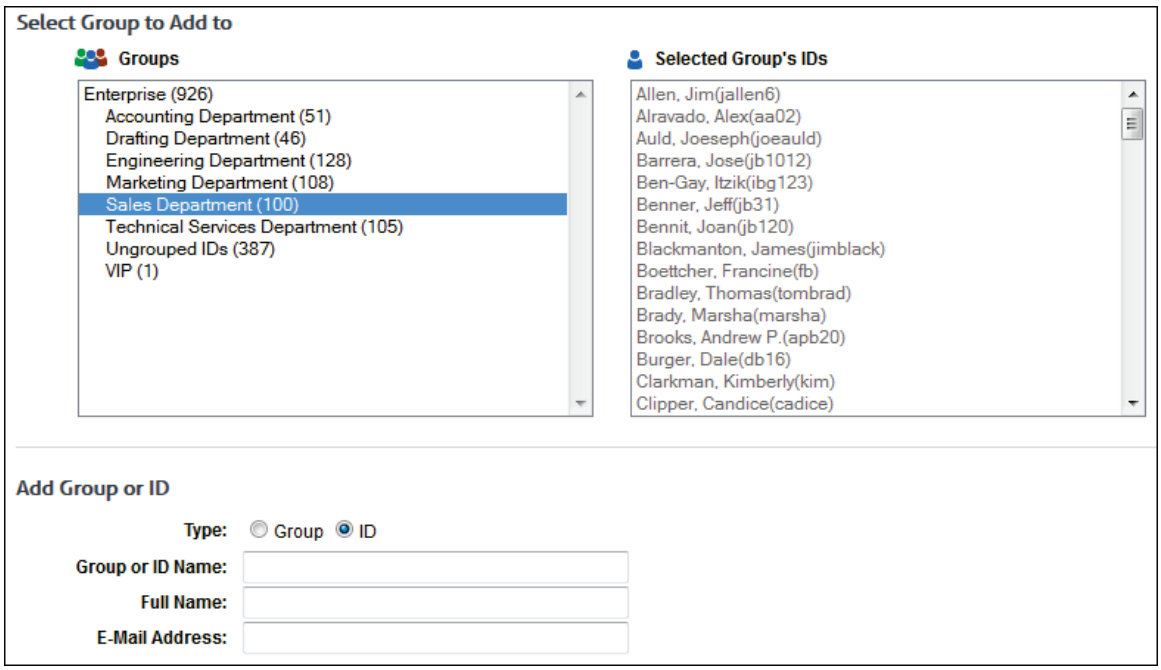
   NOTE: Groups can only be added to other groups. A group cannot be added to an ID.

3. Under **Add Group or ID**, complete the following fields:
   - **Type** - Select the **Group** option.
   - **Group or ID Name** - Type the name of the group you are adding (for example, Sales).
   - **Full Name** - This field will be unavailable because it does not apply to groups.
   - **E-Mail Address** - This field will be unavailable because it does not apply to groups.
4. Under **Policies**, complete the following fields:
   - **Web Categories** - Select a blocking policy to apply to the selected group or ID. See Control Web Categories.

- **Web Content** - Select a blocking policy to apply to the selected group or ID. See Control Web Content Types.
- **Protocols** - Select a blocking policy to apply to the selected group or ID. See Control Web Protocols.

5. Click **Submit** to add the new group.
6. To add an ID to a group, select the group in the **Groups** box to which you wish to add the ID.

   NOTE: IDs can only be added to groups. An ID cannot be added to another ID.

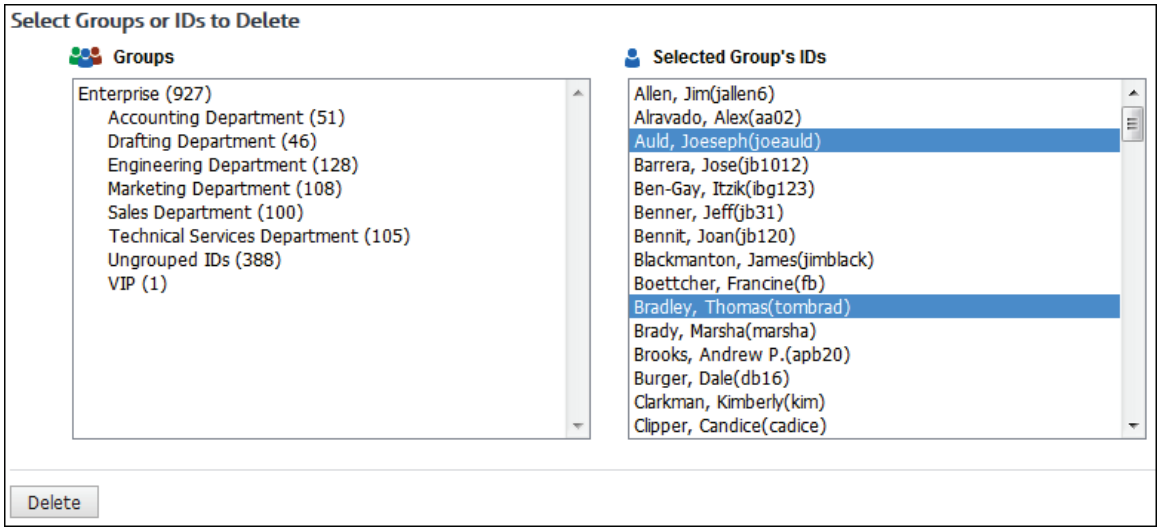


7. Under **Add Group or ID**, complete the following fields:
   - **Type** - Select the **ID** option.
   - **Group or ID Name** - Type the ID name (for example, bsmith).
   - **Full Name** - Type the full name of the person you are adding.
   - **E-Mail Address** - Type the e-mail address that will be used for cookie authentication for this person.
8. Complete the remaining fields as described above.
9. Click **Submit** to add the new ID.

Delete Groups or IDs

This page allows you to delete one or more groups or IDs. Each deletion of a group or ID is performed one at a time.

1. Go to **User Management - Edit Users - Delete**. The Delete Groups or IDs page is displayed.

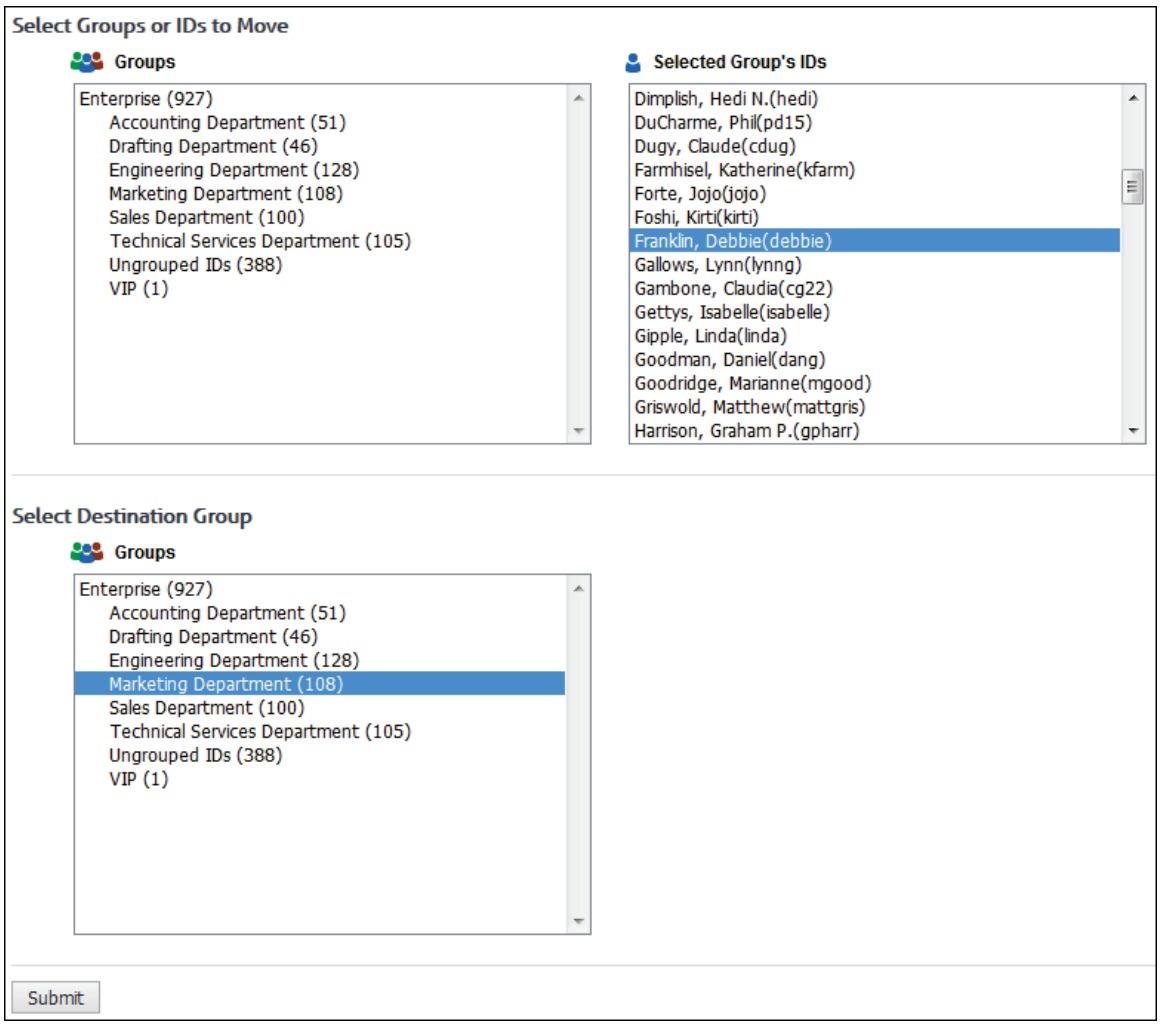


2. Under **Select Groups or IDs to Delete**, click the group or ID that you want to delete so that it is highlighted.
   - To select consecutive groups or IDs, click the first group or ID. Then hold down SHIFT and click the last group or ID you want to delete.
   - To select nonconsecutive groups or IDs, click the first group or ID. Then hold down CTRL and click the additional groups or IDs you want to delete.
   - To unselect a group or ID, hold down CTRL and click the selected group or ID.
3. Click **Delete** to delete the group or ID.

Move Groups or IDs

This page allows you to move one or more groups to another group and move one or more IDs from one group to another group.

1. Go to **User Management - Edit Users - Move**. The Move Groups or IDs page is displayed.



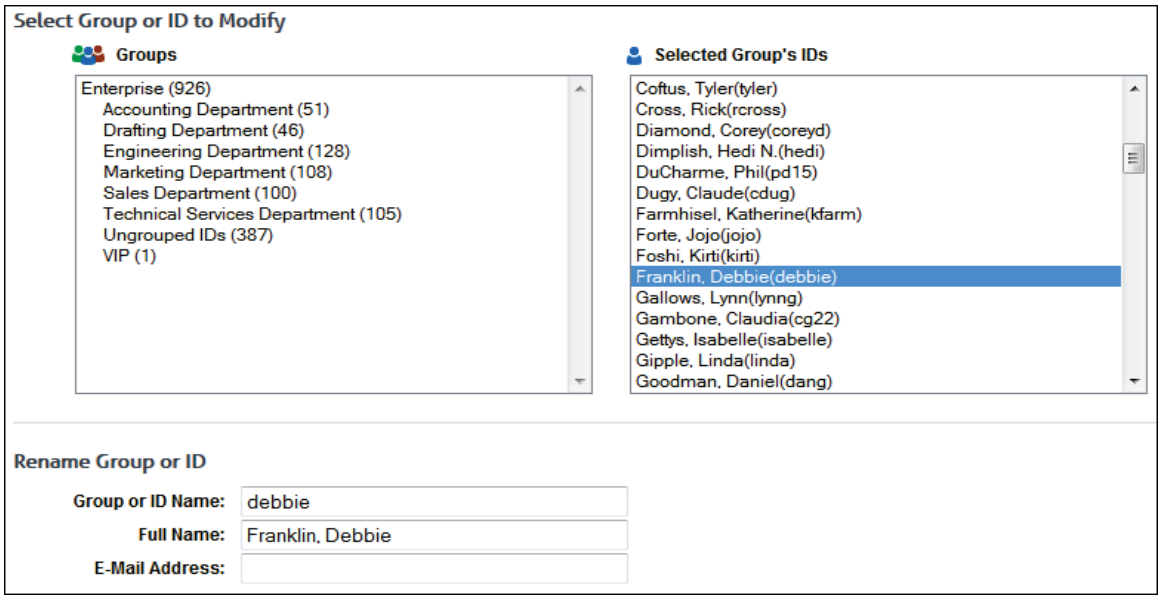
2. Under **Select Groups or IDs to Move**, click the group or ID that you want to move so that it is highlighted.
   - To select consecutive groups or IDs, click the first group or ID. Then hold down SHIFT and click the last group or ID you want to move.
   - To select nonconsecutive groups or IDs, click the first group or ID. Then hold down CTRL and click the additional groups or IDs you want to move.
   - To unselect a group or ID, hold down CTRL and click the selected group or ID.

   NOTE: Do not select *Enterprise*. It cannot be moved or made subordinate to another group.
3. Under **Select Destination Group**, click the group to which you want to move your previously selected group or ID.

   NOTE: The destination group must be different from the group to be moved. Also, a "parent" group (such as Ungrouped IDs) cannot be moved into one of its subordinate "child" groups (for example, a newly created group under Ungrouped IDs named "Sales").
4. Click **Submit** to move the group or ID.

Modify Group or ID

1. Go to **User Management - Edit Users - Modify**. The Modify Group or ID page is displayed.



2. Under **Select Group or ID to Modify**, click the group or ID that you want to modify so that it is highlighted.

   NOTE: When changing group policies, subgroups are not affected; it only changes the policy for IDs in the selected group. Therefore, if you want to change a policy for a group's subgroups, you must change the policy for each subgroup.

3. Under **Rename Group or ID**, make changes to the group name, or ID name and person's full name as necessary. If modifying a group, the **Full Name** and **E-Mail Address** fields will be unavailable because they do not apply to groups.
4. Make your changes to the remaining fields as described in Add Group or ID.
5. Click **Submit** to apply your changes.

Manage Users

Before you begin importing groups and IDs, you must decide where you want to modify your groups and IDs: Inside the Product or Outside the Product. Both options are discussed below.

Inside the Product (Default)

This option lets you add, delete, move, or modify groups and IDs within the product after an import from Active Directory, Text file, and/or Metric Server. Each time Groups and IDs are imported, whether manually or scheduled, only new IDs will be imported. (The new groups and IDs imported will be based on your selected groups in your import configuration setup.) Imported users that already exist in the group "Ungrouped IDs" will be moved to their respective new groups. All other users will not be modified.

Outside the Product

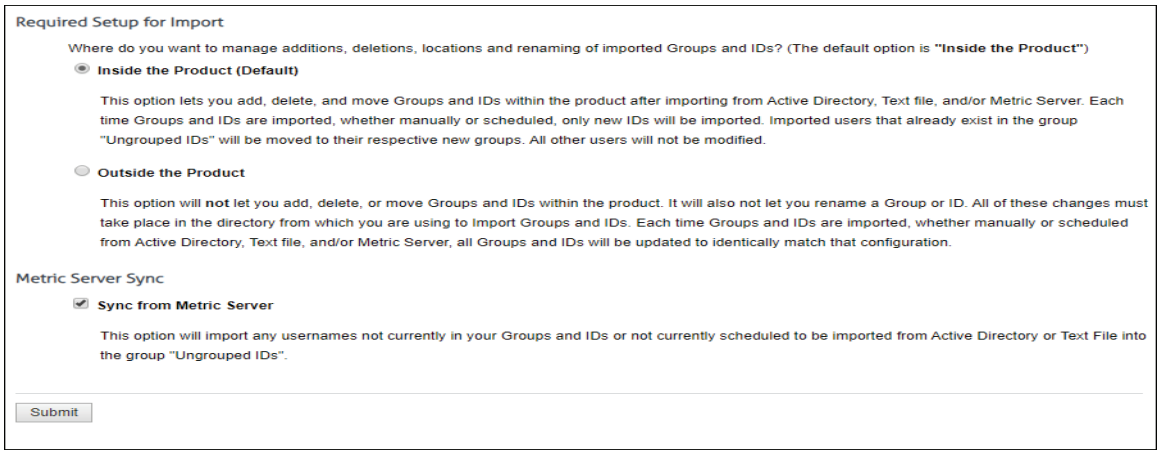
This option will not let you add, delete, or move groups and IDs within the product. It will not let you rename a group or ID in the product. All of these changes must take place in the directory from which you are importing groups and IDs. Each time groups and IDs are imported, whether manually or scheduled from Active Directory, Text file, and/or Metric Server, all Groups and IDs will be updated to identically match that configuration.

NOTE: The Inside the Product option is the default because most administrators will not use the same grouping method from the directory source for the product. Most of the time, the directory source is grouped according to your network setup and not according to how you want to apply Web-use policies.

Metric Server Sync

This option, enabled by default, will import any usernames found in the metric server and not currently in your Groups and IDs or not currently scheduled to be import from Active Directory or Text File into the group "Ungrouped IDs".

1. To make your selection, go to **User Management - Import Users - Manage**.

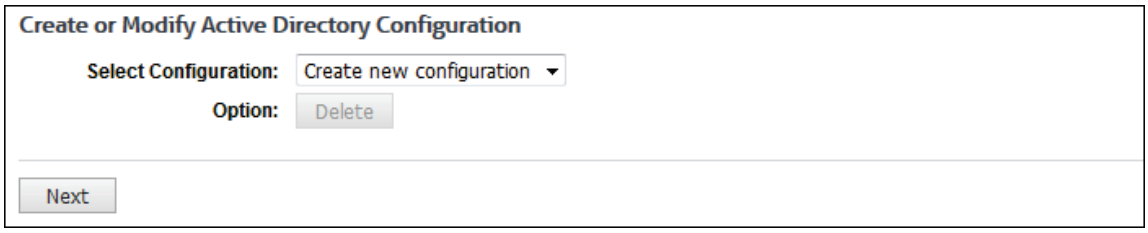


2. Select **Inside the Product** or **Outside the Product**.
3. Check the Sync from Metric Server box if you wish to import the usernames from the metric during each import. Uncheck the box if you wish to disabled this feature.
4. Click **Submit** to apply your change.

Active Directory Setup

If you have not completed the Manage Users section, do so first before getting started with importing groups and IDs. When you import from Active Directory, you have the option of creating a scheduled import to occur once every 24 hours.

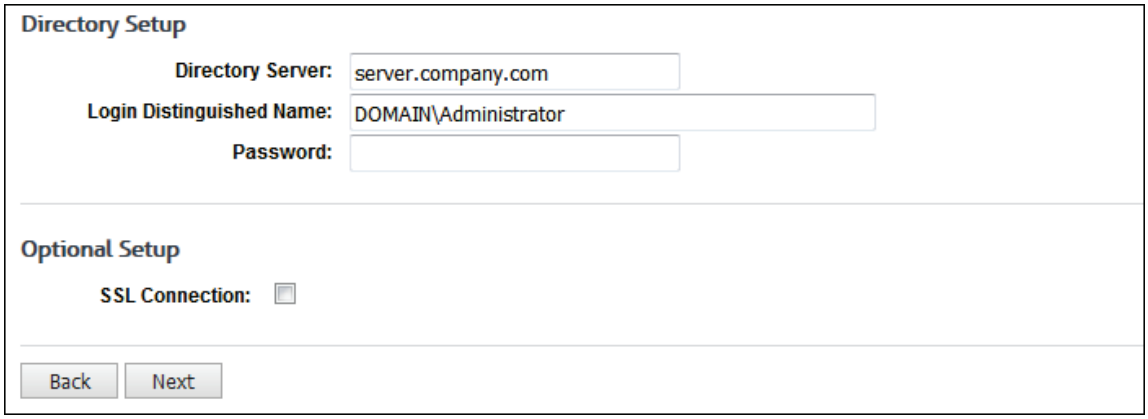
1. To create an Active Directory configuration to be imported, go to **User Management - Import Users - Active Directory - Setup**.



2. Leave the default selection set at *Create new configuration* and click **Next**.

   NOTE: If you ever want to make changes to any of your configurations, use the drop-down arrow, select the configuration that you want to change, and click **Next**. Make your changes where needed. Make sure you go through the entire wizard to submit your changes.

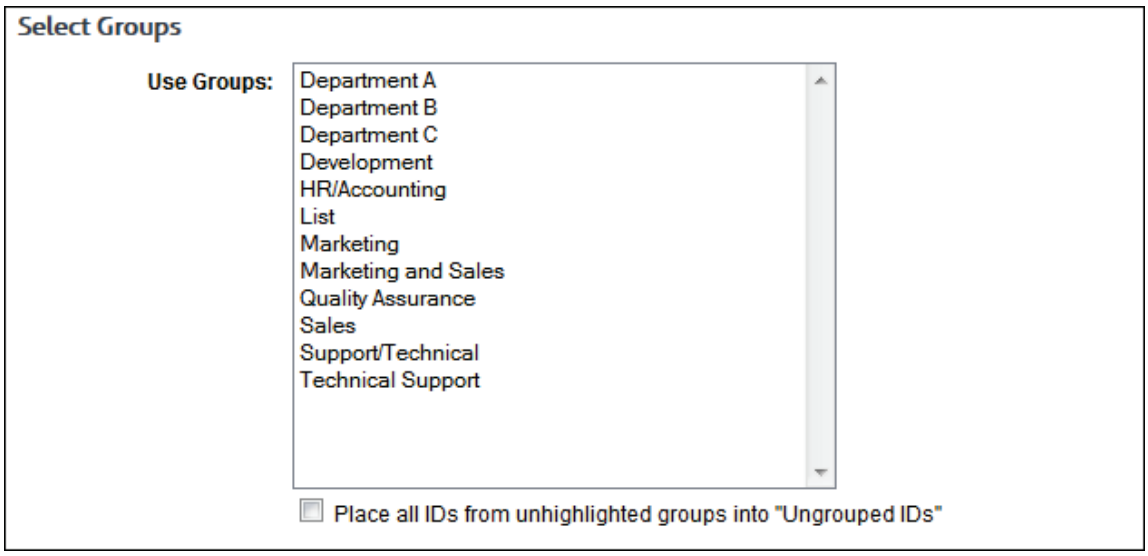
3. Now you must configure the connection to your Directory Server.



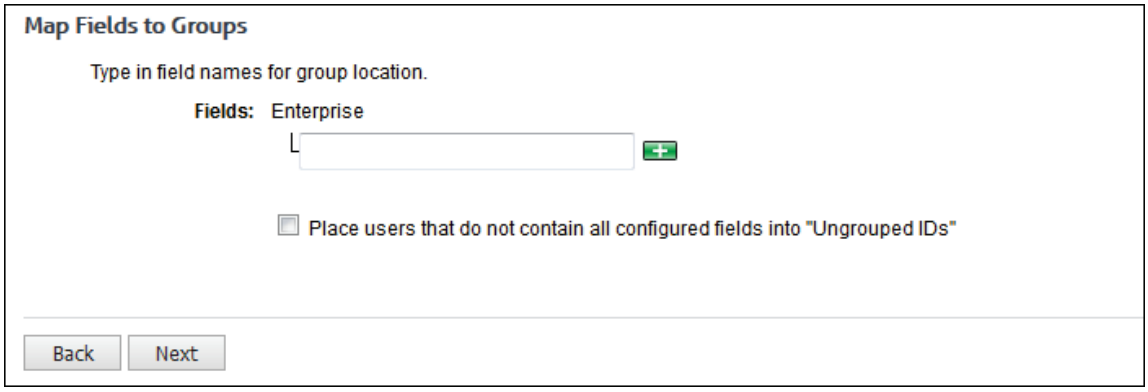
4. Enter your appropriate information in the following fields: **Directory Server**, **Login Distinguished Name**, and **Password**.
5. To import from Active Directory using an SSL connection, select the **SSL Connection** check box.
6. Click **Next**.
7. Both **Connection Status** and **Authentication Status** indicators should appear green on the Active Directory Test Results screen. If both are green, click **Next**. If either status is red, click **Back** and double-check your Directory Setup settings.

8. Select the **Valid Naming Contexts** and click **Next**.

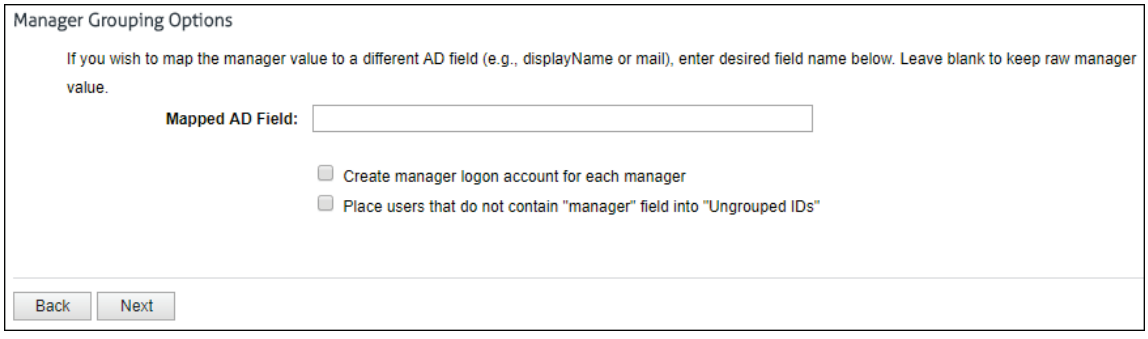
9. Select the proper grouping type (such as Department or Manager) and click **Next**.



10. If you selected **Fields**, you will see the Map Fields to Groups screen. Enter the name of each field. To add a new field, click the green plus icon.



11. If you selected **Manager**, you will see the Manager Grouping Options screen where you can map the raw manager value to a different AD field that is more user-friendly.



- For **Mapped AD Field**, type the AD field to map to. If the AD field does not exist, the distinguished name (DN) is used, that is, the raw manager value. Ensure that the AD field is unique; otherwise, the imported groups and IDs will not be properly assigned to the correct manager.
- To create a logon account for each manager, select **Create manager logon account for each manager**. When this option is selected and AD is imported, a job is submitted to the job queue, and the AD logon accounts are imported. Go to **User Management - Logon Accounts** to view the added accounts.

- If you want to place users that do not contain the Manager field into Ungrouped IDs, select **Place users that do not contain "manager" field into "Ungrouped IDs"**.

12. If you selected **Permission Group**, you will see the **Resolve for policy names** check box on the Select Groups screen.

    NOTE: If you created blocking policies for your groups and IDs to import into, you **MUST** select the **Resolve for policy names** check box in order for your groups and IDs to import into the correct blocking policies that you created previously.

13. On the Select Groups screen, select the groups to be imported by clicking them, so they are highlighted. If you want to select multiple groups, hold down the CTRL key and click the groups you want imported.

    NOTE 1: If you do not highlight any groups, all groups and IDs will be imported. This is the preferred option if you want all new groups and IDs imported with each import. Otherwise, only new IDs in your selected groups will be imported, and you will have to go back to your import configuration and select any new groups so that they will also be included in the import.

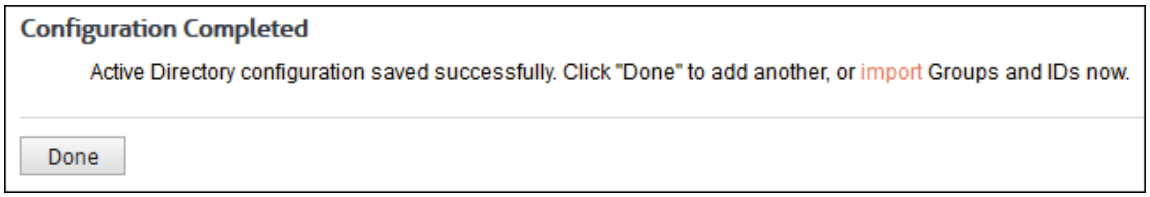
    NOTE 2: If you want to place the users from the unhighlighted groups into Ungrouped IDs, select **Place all IDs from unhighlighted groups into "Ungrouped IDs"** at the bottom of the screen. This option can be helpful, i.e., it will use the Ungrouped IDs group as a "holding tank" while you decide where to assign certain IDs.

    CAUTION: If you select the check box and do not select any groups, all IDs will be placed in Ungrouped IDs. Remember that if you are managing your groups and IDs outside the product, you will not be able to move any of your groups and IDs in the product.

    Also, if you select this check box, any IDs from the unhighlighted groups will be sent to Ungrouped IDs, which will not fall under your preconfigured blocking policies for the Permission Group selection.

14. Once you have selected the groups that you want to import, click **Next**.

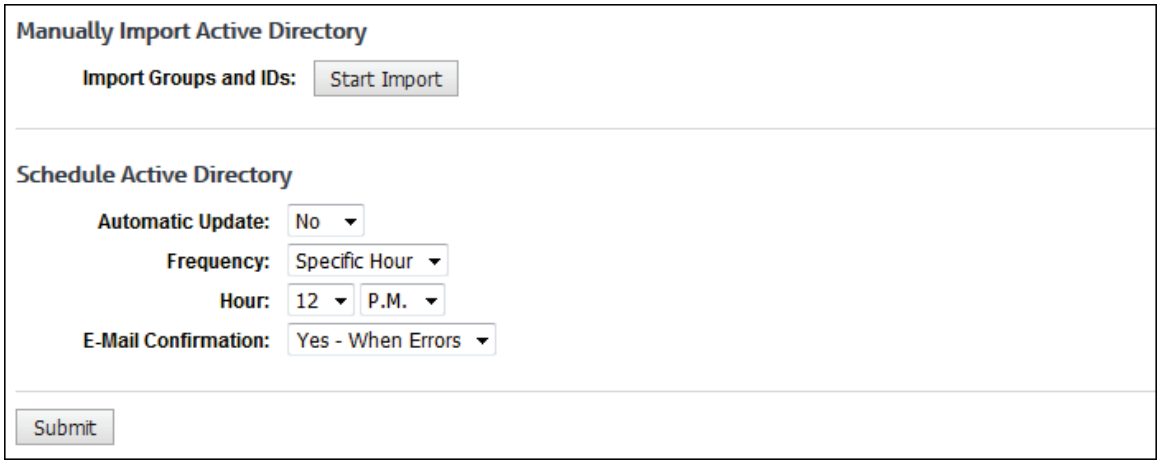
15. In the **Name** field, type a name for this Active Directory configuration, and click **Next**.
16. You should see a successful configuration message. You now have the option to create another configuration by clicking **Done** or import groups by clicking the **import** link.



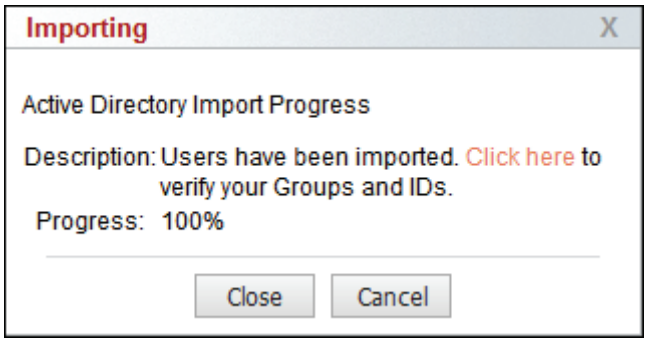
Import Users From Active Directory

This page allows you to import your Active Directory groups and IDs, and logon accounts manually or schedule an import on an hourly basis or at a specific hour every 24 hours.

1. To import users from your Active Directory configurations, go to **User Management - Import Users - Active Directory - Import**.



2. To receive an e-mail confirmation of a manual import, make a selection in the **E-Mail Confirmation** field, and click **Submit**.
    - If importing AD logon accounts, you will also receive an e-mail confirmation when the selection is *Yes - Always*.
    - If logon accounts already exist, no e-mail confirmation will be sent.
3. To import the groups and IDs, and logon accounts manually, click **Start Import**. If your import is successful, you should receive the following message.



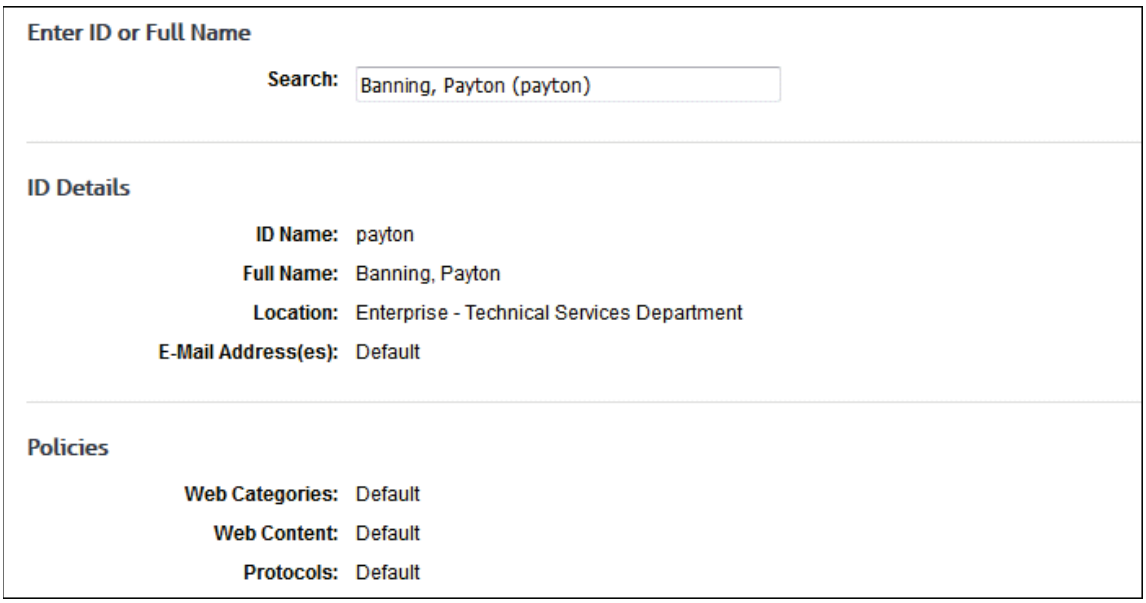
4. Click the link to view all of your imported groups and IDs, or close the window.
5. Every time you want to update your groups and IDs, you will need to click **Start Import** unless you schedule daily updates.
6. To schedule an import, in the **Automatic Update** field, select *Yes*. If you ever want to stop the scheduled import, you will need to return to this page and change the **Automatic Update** field to *No*.
7. In the **Frequency** field, select *Hourly* or *Specific Hour* if you want to schedule imports to occur every hour or at a certain hour respectively.
8. If you selected the Specific Hour option, in the **Hour** fields, select the specific hour and time of day that you want the import to occur every 24 hours. For both Hourly and Specific Hour options, the import will take place at the top of the hour.
9. In the **E-Mail Confirmation** field, select whether or not you wish to receive an e-mail for the import. An e-mail confirmation for logon accounts will only be received when the selection is *Yes - Always*.
10. Click **Submit** to save your changes.

Search for an ID

For any reason, if you need to quickly find a group to which an ID is assigned or view the policy settings for a user ID, this page will give you a quick view of that information.

1. Go to **User Management - Search Users**. The Search for an ID page is displayed.
2. Under **Enter ID or Full Name**, in the **Search** field, begin typing the ID or name of the monitored user. Users with a matching ID or name will be displayed in a drop-down box.

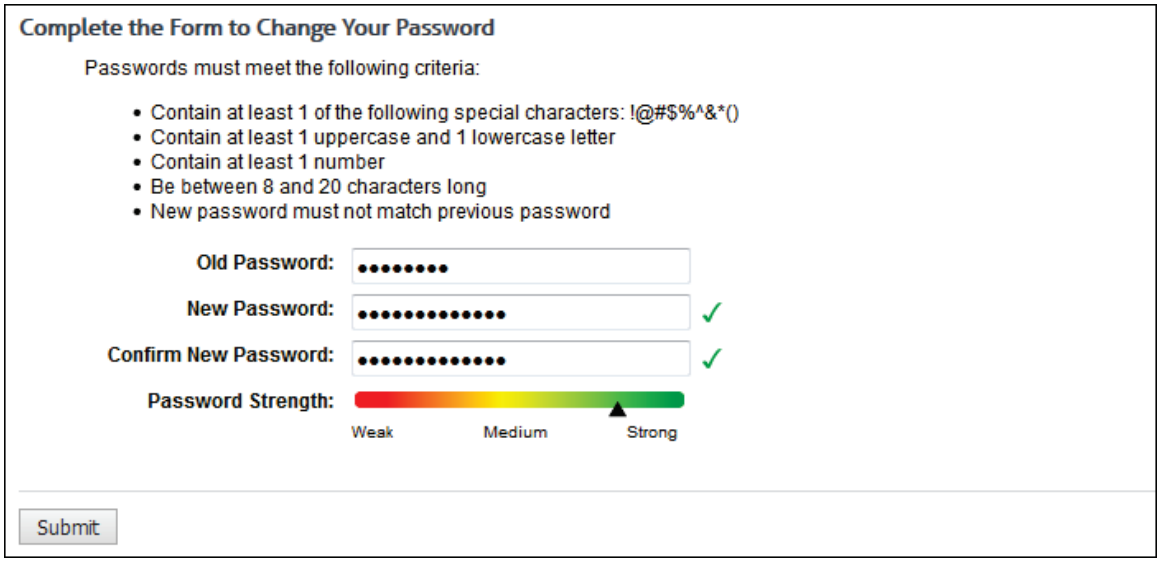
3. Click the entry that you want to view. The details for the ID are displayed including group location and policy settings.



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 and using the Generate New Password option.
   - When logged on as an administrator, clicking the key icon on the Logon Account Management pages.
   - When editing a logon account and using the Generate New Password option.

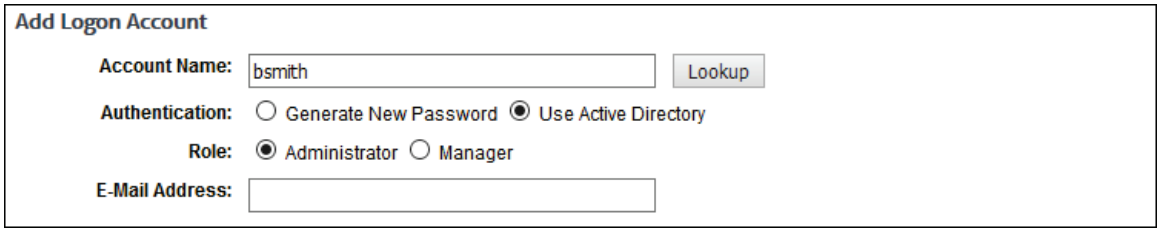


2. In the **Old Password** field, type the current password for the account.
3. In the **New Password** field, type the new password for the account. As you type the new password, a red x will display to the right of the field and change to a green check mark when the password criteria have been met. 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.

Add Logon Account

Logon accounts can be issued with an Administrator role for admins or a Manager role for managers. The Administrator role has full access to and control of the product. The Manager role only has access to a limited menu that lets managers create, run, and review reports.

1. To add a logon account, go to **User Management - Logon Accounts**.
2. Click the **Add New Logon Account** green plus icon. The Add Logon Account page is displayed.

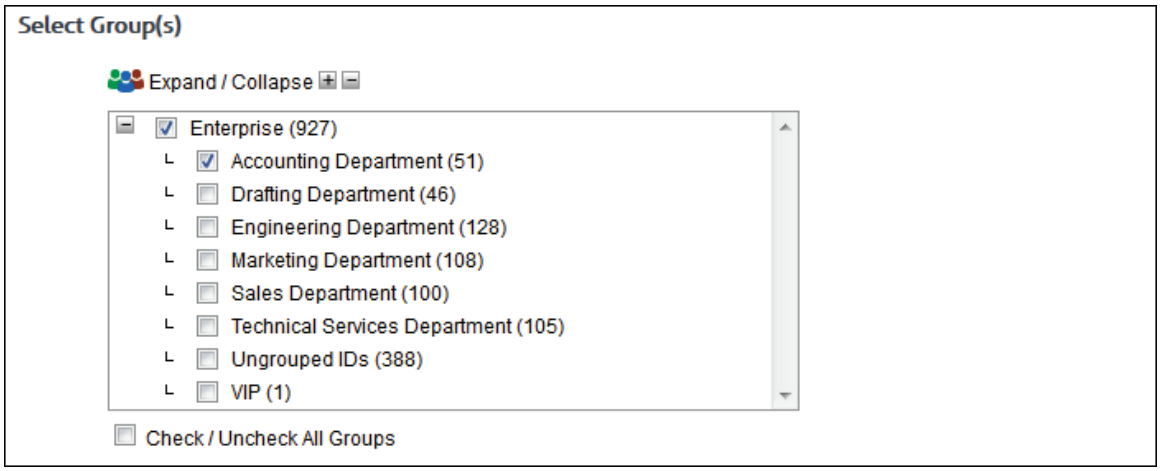


3. In the **Account Name** field, type the unique account name or logon name to be used by the account user. If you plan to use the Active Directory Authentication option, make sure the account name matches the Active Directory account name exactly.

   NOTE: The "admin" account name already exists in the product.

4. In the **Authentication** field, select one of the following options:
   - **Generate New Password** - This option generates the default password "password" if the mail server is not configured in the product. If the mail server is configured, an Account Created e-mail will be sent with logon information, and the account user will be prompted to change the password after logging on.
   - **Use Active Directory** - This option is only available if an Active Directory configuration exists. Click **Lookup** and the **Full Name** and **E-Mail Address** fields will be populated for the Active Directory account name you entered.
5. In the **Role** field, select **Administrator** or **Manager** for the logon account you are creating.
6. In the **E-Mail Address** field, type the account user's e-mail address that will receive reports. When creating a report, this address is displayed in the **Recipients** field when the **Report Delivery** field is set to *E-Mail*.
7. In the **Home Directory** field, click **Browse** to locate the directory that was set up for the account user to store reports in. You may also type the directory path. When creating a report, this path is displayed in the **Save Directory** field when the **Report Delivery** field is set to *Save*.
8. Under **Select Group(s)**, select the groups for which the account user will be authorized to create and view reports and perform other functions (if applicable).
   - If the account user has an Administrator role, *Enterprise* is selected as the group and cannot be changed.
   - If the account user has a Manager role, any group can be selected.

   NOTE: The list box displays the (optional) user-grouping structure created during groups and IDs setup. See User Management to learn how to set up groups and IDs.

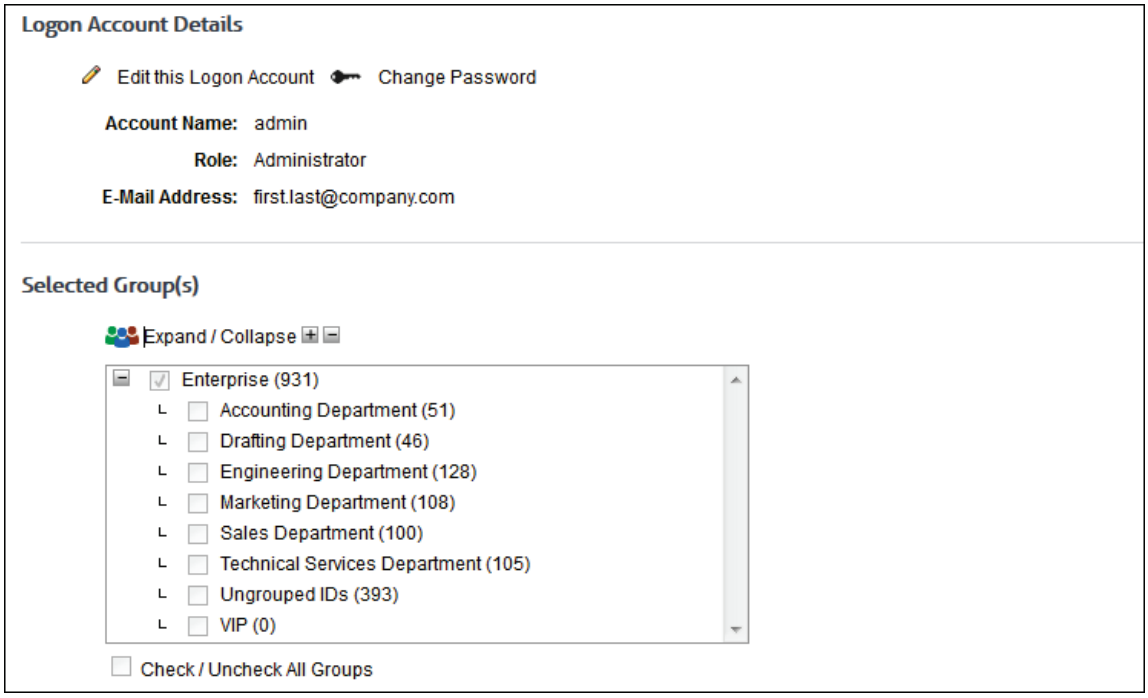


9. Click **Add** to create the account.

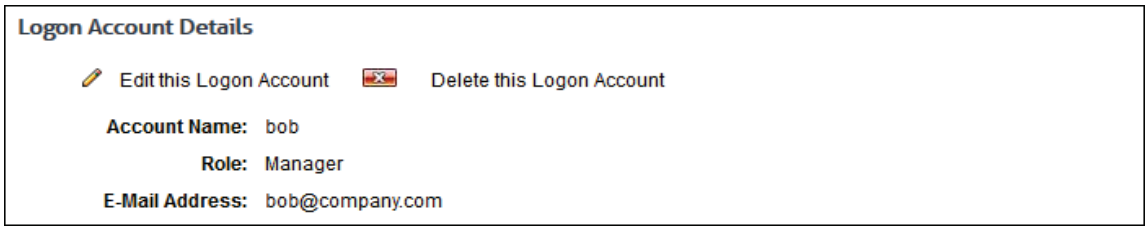
View Logon Account

You may view the details of a logon account before editing or deleting it.

1. Go to **User Management - Logon Accounts**.
2. Click an account in the list. The Logon Account Details pages is displayed with icons at the top of the page.



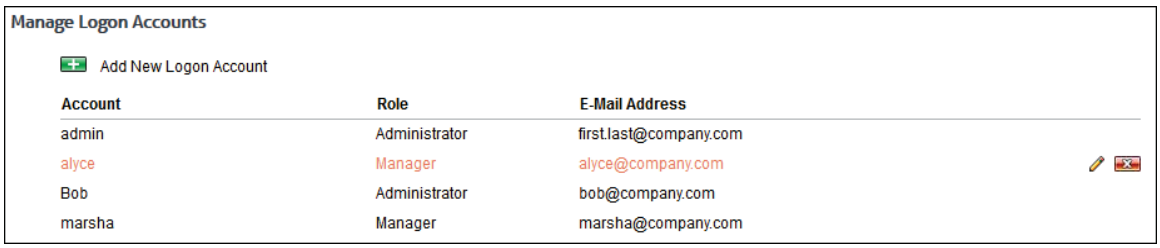
3. For the "admin" account, you may edit the account by clicking the pencil icon to go to the Edit Logon Account page. You may also change the password for the account by clicking the key icon to go to the Change Your Password page. The account cannot be deleted. Also, additional administrators cannot delete their account if they are currently logged on.
4. For all other accounts, you may edit the account by clicking the pencil icon to go to the Edit Logon Account page. You may also delete the account by clicking the red x icon.



Edit Logon Account

This page lets you modify a previously established logon account.

1. Go to **User Management - Logon Accounts**.
2. Hover over an account to display available icons.



3. Click the pencil icon for the account you wish to modify. The Edit Logon Account page is displayed.

4. In the **Account Name** field, the account name or logon name is display only and is not modifiable.
5. In the **Authentication** field, select one of the following options:
   - **Use Current** - This option allows you to keep the existing password for the account.

     NOTE: For Active Directory account names, this option is not available.
   - **Generate New Password** - This option resets the existing password to "password" if the mail server is not configured in the product. If the mail server is configured, a Password Reset e-mail will be sent, and the account user will be prompted to change the password after logging on.
   - **Use Active Directory** - This option is only available if an Active Directory configuration exists. Click **Lookup** and the **Full Name** and **E-Mail Address** fields will be updated with any changes to the Active Directory account name.

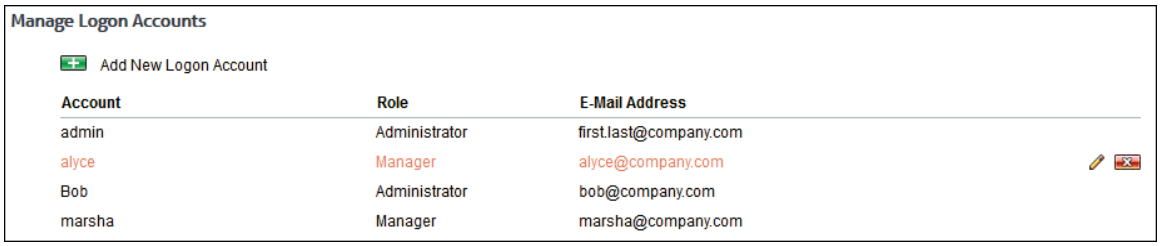
     NOTE: For the "admin" account name, this option is not available.
6. Make your changes to the remaining fields as described in Add Logon Account.
7. Click **Update** to apply your changes.

Delete Logon Account

You can delete previously established logon accounts.

NOTE: The "admin" account cannot be deleted. Also, additional administrators cannot delete their account if they are currently logged on.

1. Go to **User Management - Logon Accounts**.
2. Hover over an account to display available icons.



3. Click the red x icon for the account you wish to delete. A dialog box is displayed confirming the deletion.
4. Click **Delete**.

Categorization

Introduction

The Categorization features allow you to manage the URL List, check the categories of URLs, and customize categories.

In this section, you will find instructions on how to:

- **Manage the URL List** - Change the version of the list, download the list manually or schedule a download, and repair the list.
- **Check URLs** - Verify the category of any URL in the list.
- **Classify Categories** - Rate categories for acceptability based on your company's Web-usage policy.
- **Edit URLs** - Create an unlimited number of custom categories and populate both standard and custom categories with URLs for tracking Web sites of interest to your company.
- **Display Categories** - Select the categories to display on your reports.

URL List Options

To let you customize the categorization used in the product, this page contains options that will affect which and how categories are loaded into the product. Click Update to apply your changes in each section.

1. Go to Categorization - URL List - Options
2. Under List Version
    a. Choose the version of the list you'd like the product to load.

       The current Wavecrest URL List version is 10. If you ever experience difficulties with the URL List, contact Technical Support. Go to **Categorization - URL List - Version** to see the version of your list.

Download the URL List

The Wavecrest URL List is updated daily. In order to receive these daily updates, you must either download the URL List manually or configure the product to download it automatically once a day.

This step will ensure that you have the latest Wavecrest URL List, which will include the most recent categorized URLs and aid in accurate filtering and reporting.

If you are required to use a proxy for all HTTP connections, begin with configuring your proxy information first. Go to **Settings - Internet Connection**. If Internet traffic does not go through a proxy, then you can skip to downloading the list since **Direct connection** is the default selection. When trying to download the list, the product always tries the HTTP first, and if that fails, then it tries the FTP connection.

1. Go to **Categorization - URL List - Download**.

2. If the URL List is expired (older than 45 days), the **Status** message will be red stating that the list is expired. If the URL List is about to expire (older than 30 days), the **Status** message will be yellow and will state how many days old your list is. If you get either of these messages, you should download the URL List immediately. These messages will also appear when you log on. If your latest list was downloaded within 30 days, the **Status** message will be green.

   NOTE: To avoid the risk of having the list expire, it is recommended that you schedule the URL List to automatically download daily.

3. To download the latest version of the list, select the **Manual** option.

4. Click **Download Now**. A dialog box will appear that will show the download's progress percentage and will close when the list is fully downloaded.
5. To download the list daily, select the **Daily** option.

   NOTE: If you ever want to disable the scheduled download, change the **Download** field to **Manual**. This will turn off the automatic update.

   - In the **Hour** fields, select the specific hour and time of day that you want the automatic update to occur. The list will be downloaded within the scheduled hour.
   - In the **E-Mail Confirmation** field, select whether or not you wish to receive an e-mail confirming that the URL List download was successful.

6. Click **Download and Schedule** to download the list and schedule it to be downloaded daily.
7. Click **Schedule** to only schedule the list to be downloaded daily.

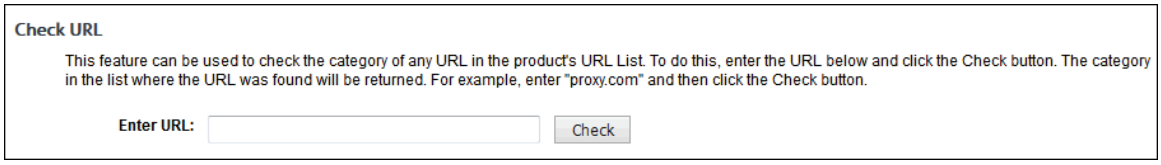
URL List Repair

If you ever experience difficulties with the Wavecrest URL List, Technical Support may ask you to repair the list. Only if instructed to do so, go to **Categorization - URL List - Repair**, and follow Technical Support's instructions.

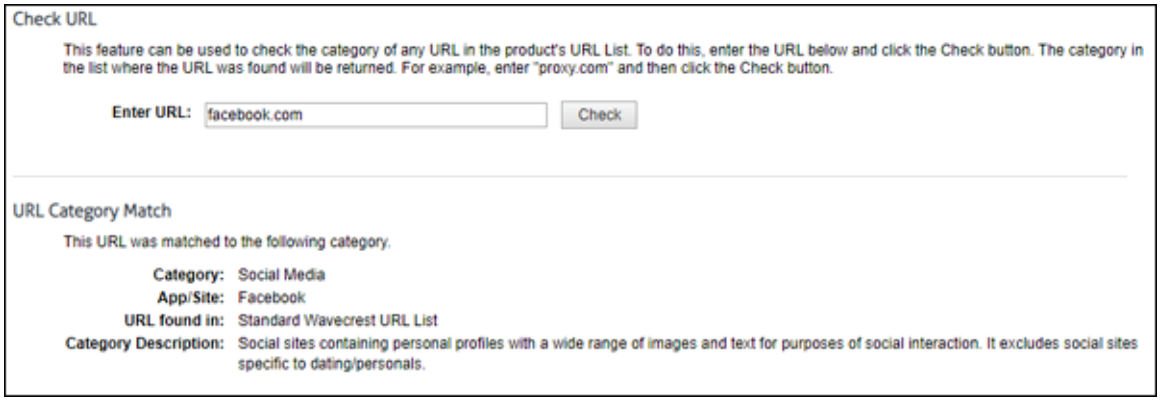
Check URL

This feature can be used to check the category of any URL in the Wavecrest URL List. It is particularly useful after you create a custom category because you can verify that the URLs you entered in the custom category have been correctly assigned to that category.

1. Go to **Categorization - Check URL**. The Check URL page is displayed.



2. In the **Enter URL** field, type the URL that you want to check.
3. Click **Check**. Category information for the URL is displayed.

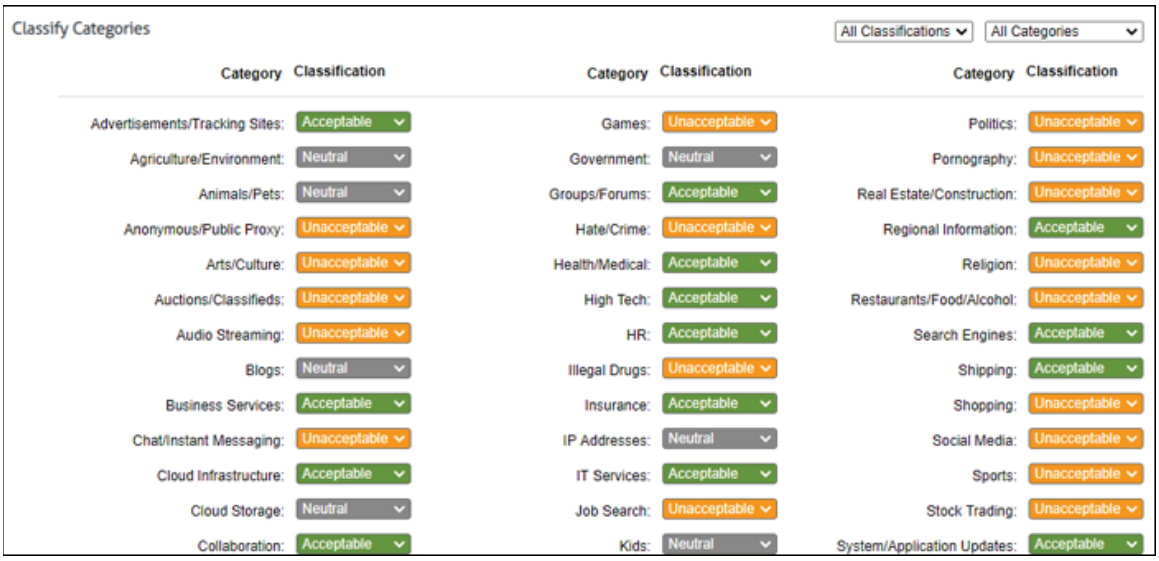


Classify Categories

By classifying categories, you are assigning an acceptability rating to each Web-use category. Categories can be rated as Acceptable, Unacceptable, or Neutral in accordance with your organization's Internet usage policy. Initially, each category has a default classification which you can accept if you like, but you will probably want to change some of these to conform to your policy. These classification settings will be used for reports.

NOTE: For descriptions of each category, go to **Help - Category Description**.

1. Go to **Categorization - Customize - Classification**.



2. Use the drop-down box next to each category to classify each as *Neutral*, *Acceptable*, or *Unacceptable*.
3. In the upper right hand corner, There are two drop-downs to limit which categories are displayed for modification. The first drop-down is to limit the categories listed by Classification. The options are All Classifications, Acceptable, Neutral, and Unacceptable. The second drop-down is to limit the category listing by the type of category. The options are All Categories, Custom Categories, or Standard Categories.
4. Click **Submit** to apply your changes. The report below is an example of how classifying your categories can help you quickly see which site visits were acceptable, unacceptable, or neutral.

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	

Note that each site is color-coded based on the classification settings you made.

Green = Acceptable, Orange = Unacceptable, Gray = Neutral

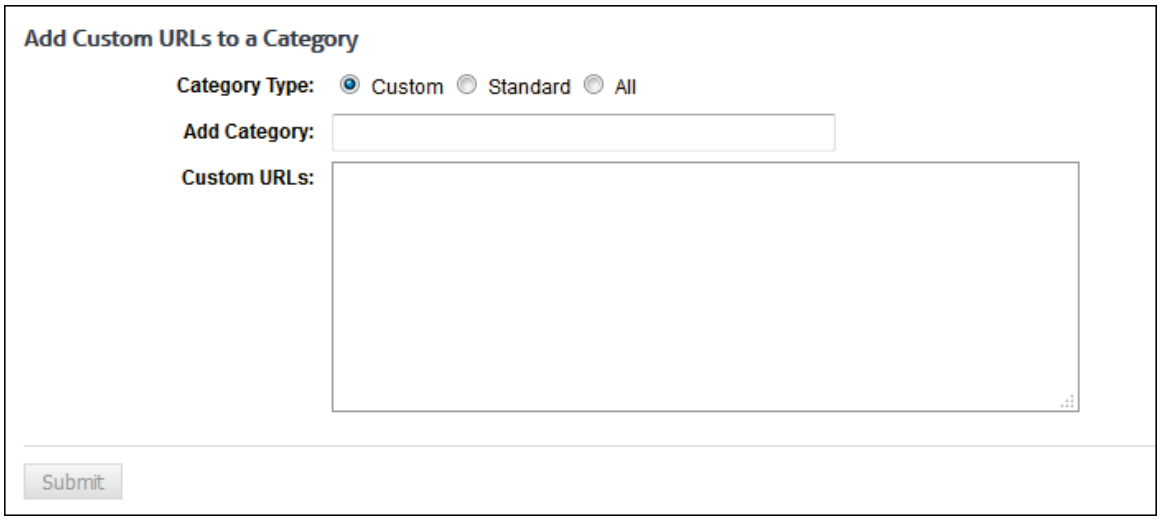
Edit URLs

In addition to 70+ standard categories, you can create an unlimited number of custom categories for additional filtering using this page. Custom categories can be used for a variety of reasons, e.g., to block additional Web sites or track employees' use of company intranet sites. This page also allows you to populate both standard and custom categories with URLs of your own choosing.

NOTE: Your category and URL changes will override any future list downloads by Wavecrest.

NOTE: If using SSL Inspection, custom categories are inspected by default.

1. Go to **Categorization - Customize - URLs**. The Edit URLs page is displayed.



2. For **Category Type**, the **Custom** option is selected by default initially to allow you to create a custom category. The **Standard** option allows you to select a standard category. The **All** option shows both custom and standard categories and permits you to create a custom category.
3. If no custom categories exist, in the **Add Category** field, type the category name. The name cannot exceed 50 characters.
4. If custom categories exist, in the **Select Category** field, select *Create Custom Category* to create a new custom category, or you can choose to modify or delete an existing one.
5. After selecting *Create Custom Category*, enter a category name in the **Add Category** field. If you are modifying or deleting a previously created category, its name will appear in the **Select Category** field. To rename the category, click the pencil icon. To delete the category, click the red x icon next to the field.

   NOTE: Standard categories cannot be deleted.
6. To add URLs to a selected category, in the **Custom URLs** box for custom categories or **Supplemental URLs** box for standard categories, type the URLs.

   NOTE 1: If you add a URL that already exists in another category, the URL will be removed from the other category.

   NOTE 2: To add multiple URLs, enter the first URL and press ENTER; then enter the second URL and press ENTER. Repeat until you have included all the URLs.

   (Optional) Add Wildcard Entries. You can use wildcards to add multiple URLs simultaneously. This can be done with domain matching, domain and path matching, or parameter matching.

   a. **Wildcards With Domain Matching.** This URL matching method categorizes Web sites whose pages all contain the same type (category) of content, e.g., Shopping, News, and Sports. In these relatively simple cases, one category applies to the entire site. Under this method, if the Web log entries are in any of the following formats and the URL List contains a matching URL, the product will categorize the visit on the basis of the domain name.

      - www.mydomain.com
      - *.mydomain.com
      - www.mydomain.*
      - *.mydomain.*

NOTE: For this method to work, and as reflected in the examples, the entry in the URL List must contain a complete domain name element. That is, the domain name between the periods (dots) must be complete and must not be augmented with an asterisk or any other character. For example, the list must not contain *mydomain*.com* or **mydomain.com*.

b. **Wildcards With Domain and Path Matching.** This URL matching method categorizes Web site visit-attempts at the path level. This method enables individual pages to be categorized. If the URLs visited (as documented in the Web logs) are in any of the following formats and there is a corresponding entry in the URL List, the product will categorize the visit on the basis of the domain name and path.

- www.mydomain.com/path/*
- www.mydomain.com/*/path/*
- *.mydomain.com/*/path/*
- *.mydomain.com/path/

NOTE 1: For this method to work, the entry in the URL List must contain a complete path element. That is, the path element between the forward slashes must be complete and must not be augmented with an asterisk or any other character. For example, the list must not contain */path*/*.

NOTE 2: As indicated at the end of the fourth example above, the asterisk is not always required, i.e., an exact path can be entered. However, as indicated in all four examples, forward slashes are always required.

c. **Wildcards With Parameter Matching.** This method adds parameter matching to the two methods defined above (domain alone and domain-plus-path). It focuses more on syntax found in URL parameters than on content of the site being evaluated by the product. The parameter method works as follows. If the Web log entries are in any of the formats listed below, the product will categorize the visit on the basis of (a) the domain name plus the parameter, or (b) domain name plus path and parameter. Note that the first three bullets are examples of the former (no path included).

- www.mydomain.com/*?keyword=value
- www.mydomain.com/?keyword=value
- www.mydomain.com/?id=*
- www.mydomain.com/?id=*&sr=* (example of multiple pairs)
- *.mydomain.com/*/path/*?id=*

NOTE 1: Parameter matching always requires the use of "?". If a question mark is placed at the end of the domain or the path, the URL List will perform this matching method.

NOTE 2: The "/" is also required for this method. However the "&" is optional and is only needed when more than one "keyword=value" pairing is involved (as indicated above). Note that the "&" is added between pairs, and the pairs do not have to be in any particular order.

Rules for Custom URLs. The rules for entering custom URLs include:

- Protocols such as http:// and https:// are not necessary and are removed when the entry is saved.
- Entries consisting of only *, ., and / are not allowed (e.g., *.*).
- Spaces in the middle of the domain name are not allowed.

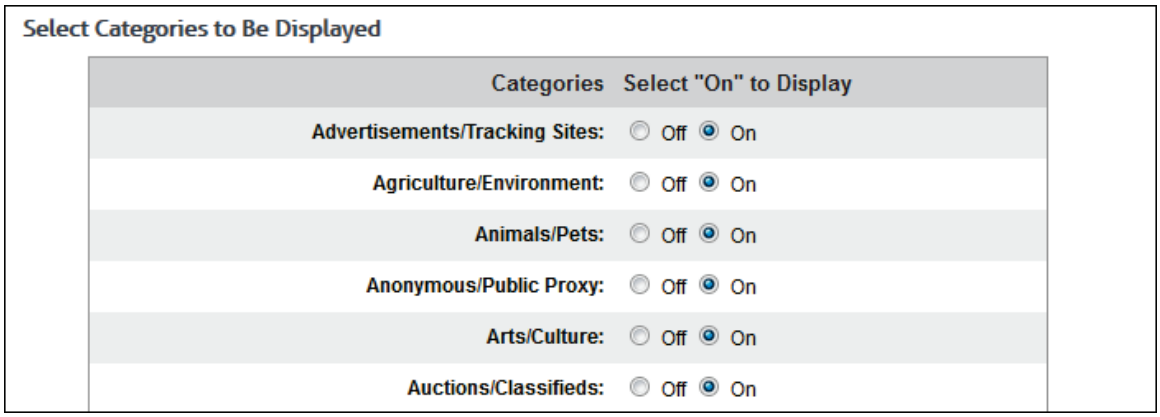
- In the domain name, * can only be preceded and/or followed by . or / (e.g., *.mydomain.*/). Incorrect domain entries such as *google* and goo*gle.com are saved as *.google.* and google.com respectively.
- In the path, * can only be preceded and/or followed by / (e.g., *.mydomain.com/*/path/*). Incorrect path entries are not saved and need to be reentered correctly.

7. To modify a URL, highlight the portion of the URL you would like to modify. Then type the changes.
8. To delete a URL, highlight the URL you would like to delete, and then press DELETE.
9. Click **Submit** to apply your changes.

Display Categories

This page lets you select the categories to display on your reports. If categories are turned off, they do not appear on reports, and they are not available as category selections for reports. By default, all categories are turned on including custom categories.

1. Go to **Categorization - Customize - Categories**. The Display Categories page is displayed.



2. Under **Select Categories to Be Displayed**, apply an **Off** or **On** setting to each category by selecting the corresponding option.

   NOTE: If you want only a few categories displayed on reports, scroll to the bottom of the page, and click **All Off**. Then scroll up to select **On** for those categories that you want to turn on (and vice versa).

3. Click **Submit** to apply your changes.

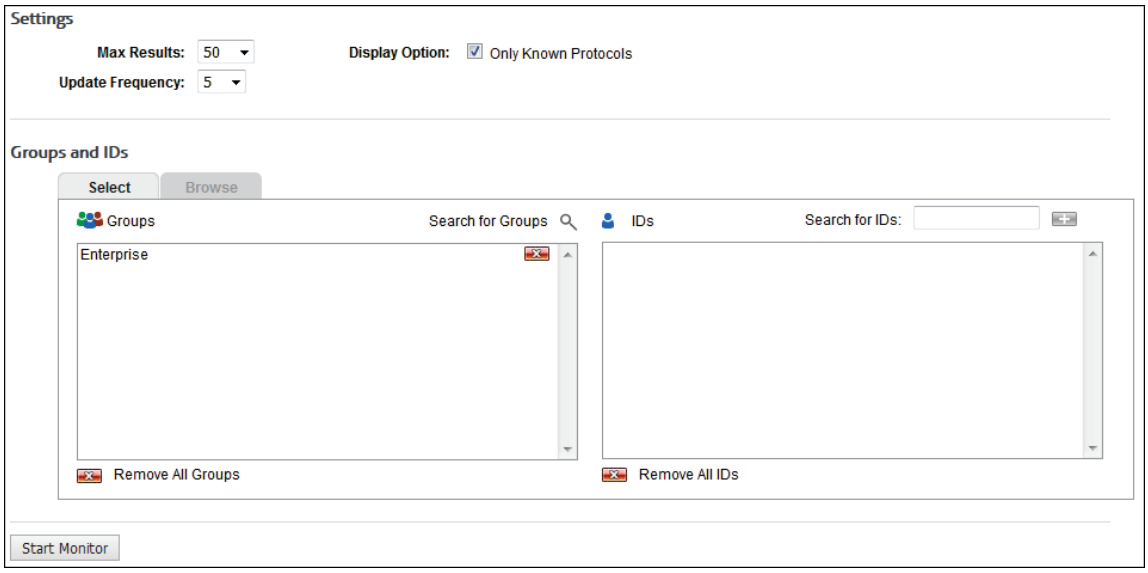
   NOTE: If all categories are set to **Off**, the Submit button is disabled.

Real-Time Monitors

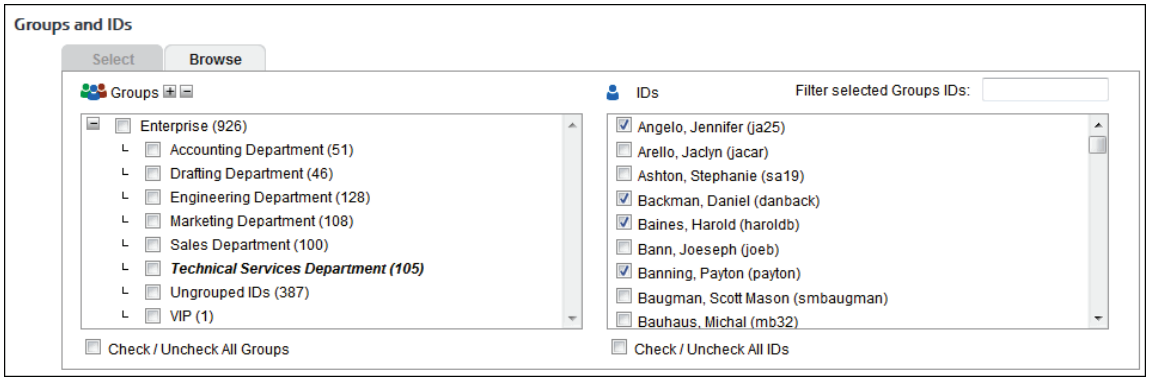
Real-Time Protocol Monitor

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

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



2. Under **Settings**, in the **Max Results** field, select the maximum number of entries you want to see on the Real-Time Protocol Monitor. Any entries 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 Option**, select **Only Known Protocols** to see only the protocols identified by the product. If this option is not selected, a hyphen (-) is shown on the monitor for protocols not identified by the product.
5. 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.

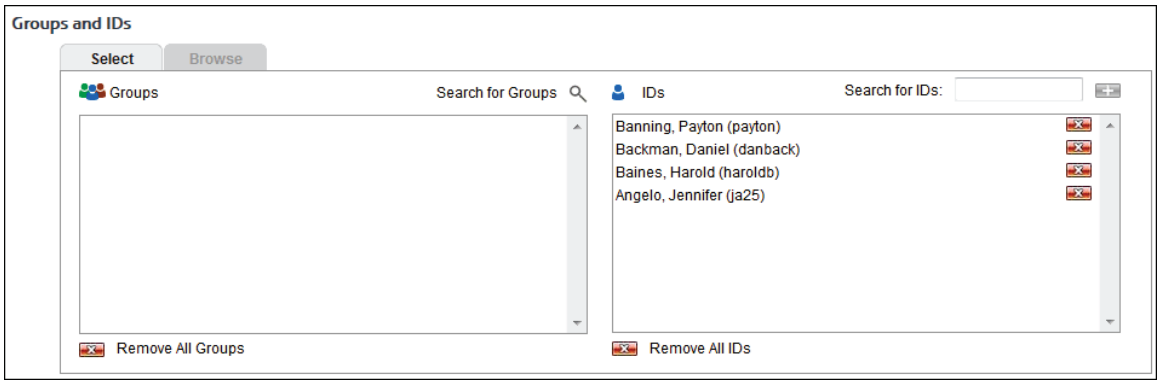


Other options include:

- **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.

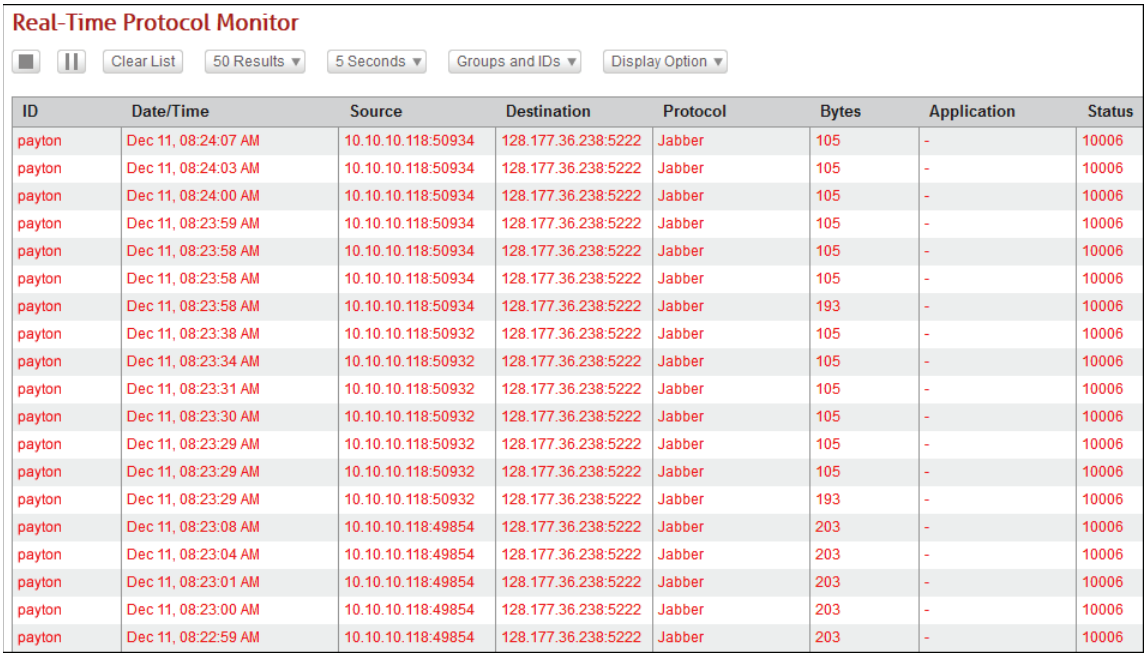
The groups and IDs that you have selected will appear on the Select tab.



6. 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.
7. 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 Ungrouped IDs.
   - If authentication is enabled and the ID is an IP address or an IP address with a wildcard, all user names for that IP address will be displayed in the monitor 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.
8. Click **Start Monitor** to run the Real-Time Protocol Monitor. The Real-Time Protocol 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 Protocol Monitor page as when you initially accessed the page.
     - If you do not click **Stop** and navigate away from the Real-Time Protocol 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, groups and IDs, and known protocols. The monitor will continue updating.
     - If no groups or IDs are selected, *Enterprise* is selected by default.

9. The monitor displays the following information:
    - The **ID** column displays the user name making the request.
    - The **Date/Time** column is sorted in descending order.
    - The **Source** column displays the source IP address and port from where the request originated.
    - The **Destination** column displays the destination IP address and port being requested.
    - The **Protocol** column displays the protocol blocked for protocol filtering. If the protocol has not been identified by the product (unknown), a hyphen (-) is shown.
    - The **Bytes** column indicates the size of the packet.
    - The **Application** column displays the Internet application that generated the packet request, if any.
    - The **Status** column shows a protocol flag that is used by Technical Support for troubleshooting purposes.
    - Packets that were denied due to protocol filtering are displayed in red.

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



Real-Time Protocol Monitor

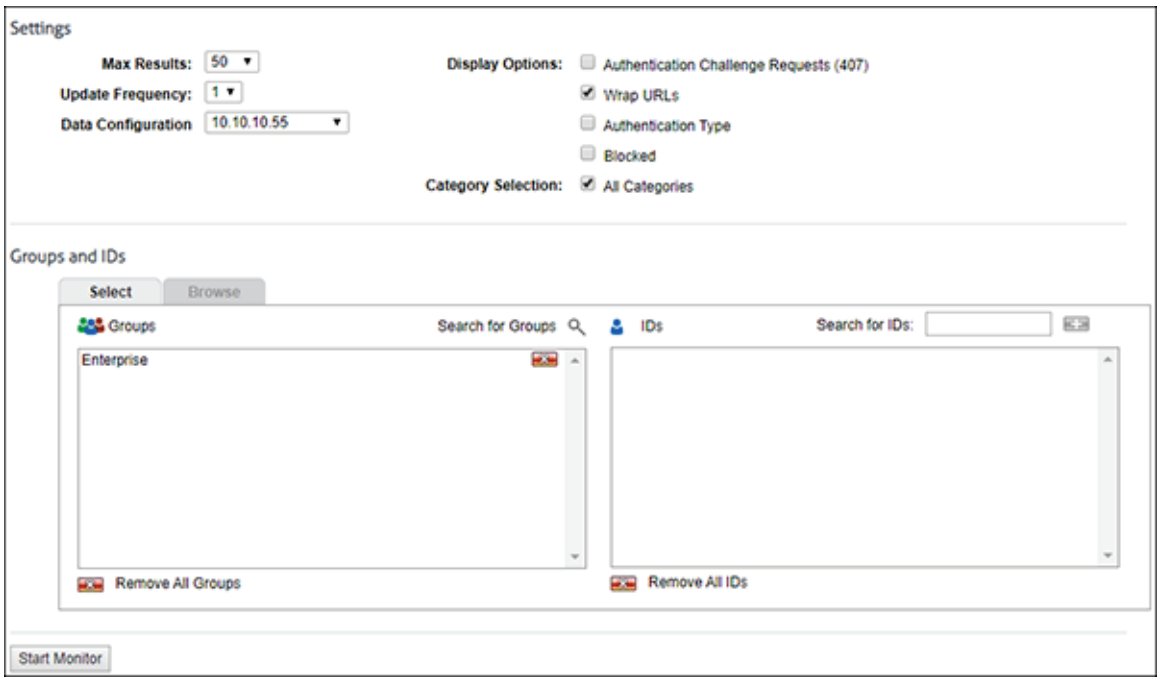
Clear List | 50 Results | 5 Seconds | Groups and IDs | Display Option

ID	Date/Time	Source	Destination	Protocol	Bytes	Application	Status
payton	Dec 11, 08:24:07 AM	10.10.10.118:50934	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:24:03 AM	10.10.10.118:50934	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:24:00 AM	10.10.10.118:50934	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:59 AM	10.10.10.118:50934	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:58 AM	10.10.10.118:50934	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:58 AM	10.10.10.118:50934	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:58 AM	10.10.10.118:50934	128.177.36.238:5222	Jabber	193	-	10006
payton	Dec 11, 08:23:38 AM	10.10.10.118:50932	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:34 AM	10.10.10.118:50932	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:31 AM	10.10.10.118:50932	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:30 AM	10.10.10.118:50932	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:29 AM	10.10.10.118:50932	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:29 AM	10.10.10.118:50932	128.177.36.238:5222	Jabber	105	-	10006
payton	Dec 11, 08:23:29 AM	10.10.10.118:50932	128.177.36.238:5222	Jabber	193	-	10006
payton	Dec 11, 08:23:08 AM	10.10.10.118:49854	128.177.36.238:5222	Jabber	203	-	10006
payton	Dec 11, 08:23:04 AM	10.10.10.118:49854	128.177.36.238:5222	Jabber	203	-	10006
payton	Dec 11, 08:23:01 AM	10.10.10.118:49854	128.177.36.238:5222	Jabber	203	-	10006
payton	Dec 11, 08:23:00 AM	10.10.10.118:49854	128.177.36.238:5222	Jabber	203	-	10006
payton	Dec 11, 08:22:59 AM	10.10.10.118:49854	128.177.36.238:5222	Jabber	203	-	10006

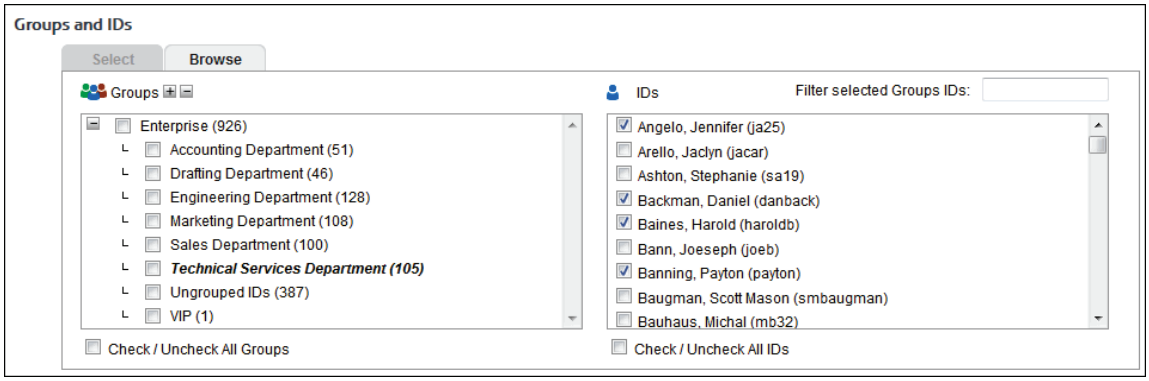
Real-Time Web Monitor

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 in your network. In a Hybrid deployment, the Real-Time Web Monitor can also display the Web traffic of your remote employees, i.e., cloud users.

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



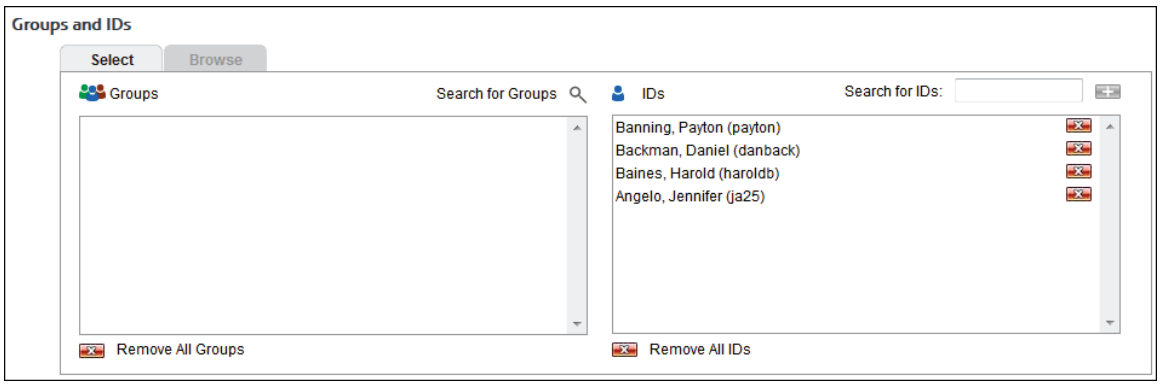
2. Under **Settings**, in the **Max Results** field, select the maximum number of URLs you want to see on the Real-Time Web Monitor. Any URLs that exceed this number are dropped from the list of results.
3. In the **Update Frequency** field, select how frequently you want the screen to update in seconds.
4. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Data Configuration** field is displayed to allow you to select the log data source of the Web traffic that you wish to view. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration or local CyBlock configuration.
5. For **Display Options**, select **Authentication Challenge Requests (407)** to see these entries.
6. 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.
7. Select **Authentication Type** to see the type of proxy authentication for each user.
8. Select **Blocked** to only see requests that have been denied.
9. 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.
10. 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.

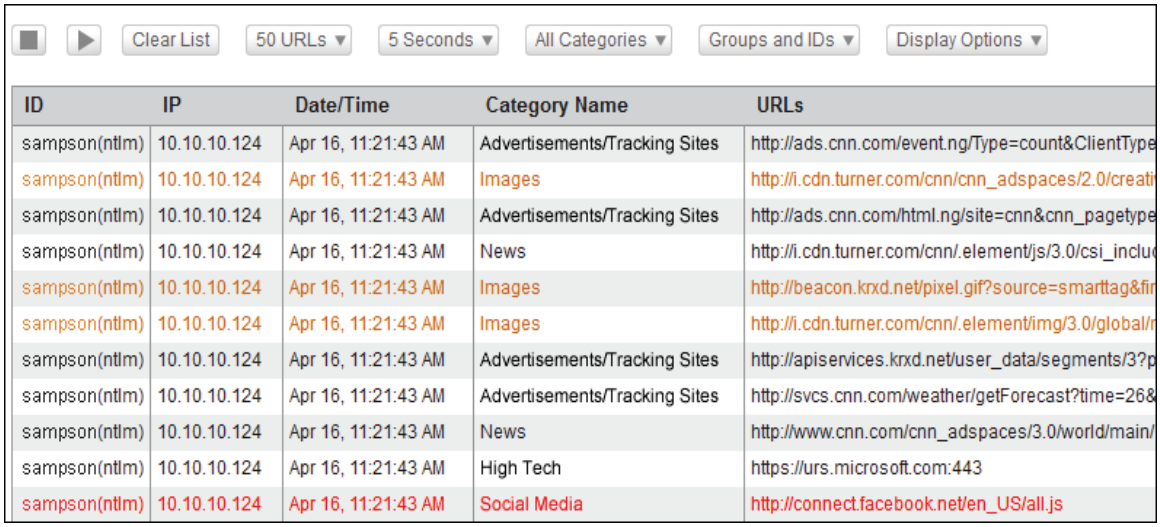
The groups and IDs that you have selected will appear on the Select tab.



11. 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.
12. 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 Ungrouped IDs.
    - If authentication is enabled and the ID is an IP address or an IP address with a wildcard, all user names for that IP address will be displayed in the monitor 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.

13. 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, authentication type, and blocked. 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.
14. 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.
    - In a Hybrid deployment, if sync communication is temporarily stopped, your CyBlock installation and cloud account are unpaired, or the pairing cloud server is down for some reason, an error is displayed.

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

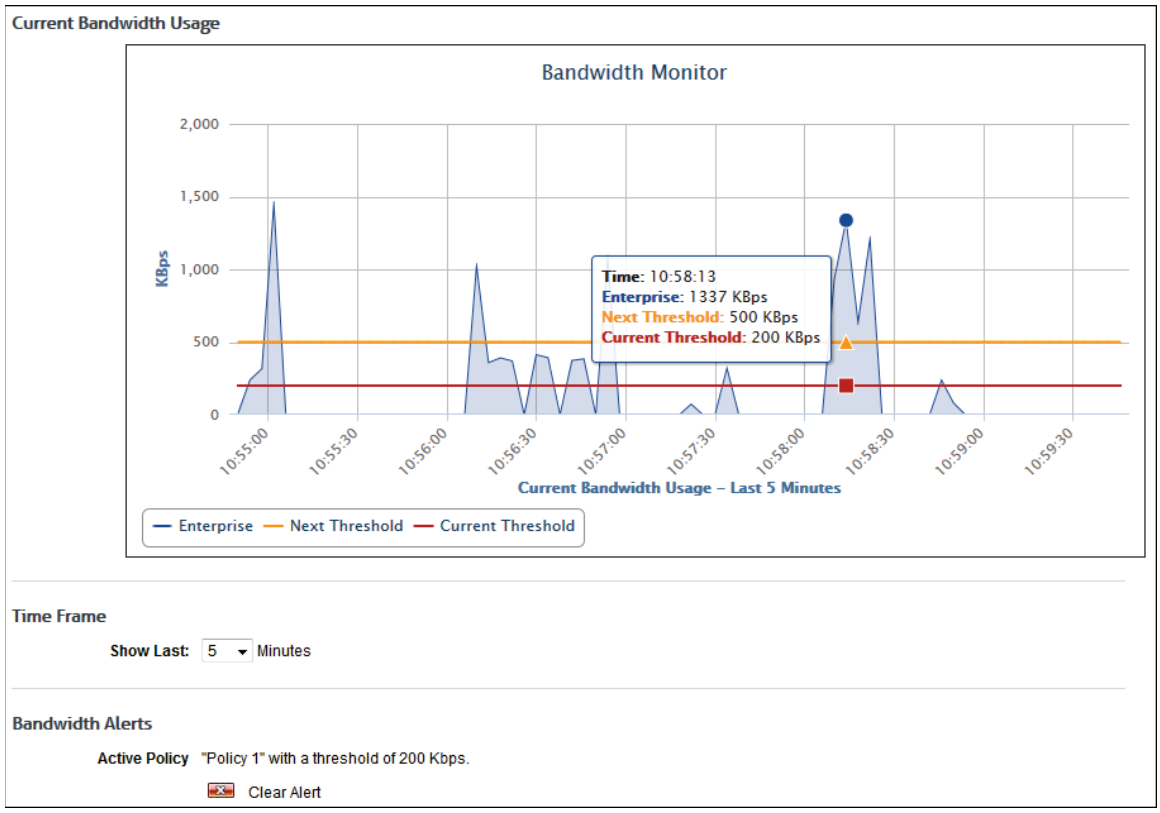


ID	IP	Date/Time	Category Name	URLs
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Advertisements/Tracking Sites	http://ads.cnn.com/event.ng/Type=count&ClientType
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Images	http://i.cdn.turner.com/cnn/cnn_adspaces/2.0/creati
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Advertisements/Tracking Sites	http://ads.cnn.com/html.ng/site=cnn&cnn_pagetype
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	News	http://i.cdn.turner.com/cnn/.element/js/3.0/csi_inclu
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Images	http://beacon.krxd.net/pixel.gif?source=smarttag&fir
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Images	http://i.cdn.turner.com/cnn/.element/img/3.0/global/r
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Advertisements/Tracking Sites	http://apiservices.krxd.net/user_data/segments/3?p
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Advertisements/Tracking Sites	http://svcs.cnn.com/weather/getForecast?time=26&
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	News	http://www.cnn.com/cnn_adspaces/3.0/world/main/
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	High Tech	https://urs.microsoft.com:443
sampson(ntlm)	10.10.10.124	Apr 16, 11:21:43 AM	Social Media	http://connect.facebook.net/en_US/all.js

Real-Time Bandwidth Monitor

This page provides current bandwidth usage data for the Enterprise for the last 5, 10, or 15 minutes.

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



2. Hover your mouse over each point to see the exact number of kilobytes per second.
3. If you want to zoom in, click and drag from left to right or from right to left on the chart. Click **Reset zoom** to return to the original view.
4. Under **Time Frame**, use the **Show Last** field to select whether you want to display the last 5, 10, or 15 minutes of bandwidth usage. The chart will update automatically based on your selection.

5. Under **Bandwidth Alerts**, the following is displayed:
    - If no bandwidth policy is activated, the **Active Policy** field will show "No bandwidth policies are currently active."
    - If a bandwidth policy is activated, the **Active Policy** field will show the policy name with its associated threshold. Click the red x icon to clear the alert. The **Active Policy** field will continue to show each policy as it is activated.
6. A notification e-mail will automatically be sent to the administrator if e-mail alerts are enabled in the policy.

Reports

Introduction

With this product, you can get a quick overview of Web activity from Dashboard charts, run high-level and low-level reports, and schedule reports to run regularly. (For a complete listing of Wavecrest's standard reports and their definitions, see Appendix B.) You also have the option to use Interactive Reporting when using the HTML report format. Interactive reports allow you to get more detailed results on employee Web use by clicking the report's elements, e.g., group, user, and category.

Running reports allows you to analyze employee Web use so that you can easily identify instances of Web abuse that can drain productivity, pose a legal liability threat, or threaten network security. Reports can also be useful if you use one or more custom categories to monitor intranet sites in your organization. The reports will show how often and how some of these sites are being used by your employees.

If you have a Hybrid deployment, you can get a quick overview of the Web activity of your remote employees, i.e., cloud users, from the Dashboard as well as run reports on their Web activity. Cloud log files are imported nightly similar to local logs, and reports would be current as of the previous day. To get a report with the current day's cloud data, go to Settings - Hybrid, perform a manual sync, and then run the report. Manager accounts would have to see their administrator for the current day's cloud data.

Before running any reports, be sure to complete the Getting Started Checklist. The Getting Started Checklist covers the required setup needed to start running reports. You also need to be familiar with the section on Web Management as reporting goes hand-in-hand with that section. This product is designed so that you can customize it according to your organization's Web policy. As a result, the reports you receive will reflect that policy. This makes it easier for you to detect Web abuse quickly when viewing your reports.

Also before running reports, be sure to set report options as well as the categories that you want displayed on the report. You may also want to view your policy settings to see if any setting is missing or needs to be changed.

In this section, you will find instructions on how to:

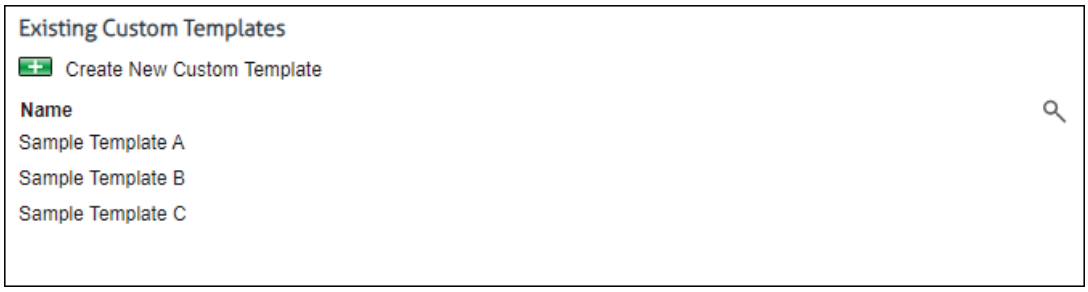
- **Create and Manage Report Templates** - Provides instructions on how to create and manage custom report templates if you have specific report requirements and want to build your own report.
- **Manage Reports** - Provides instructions for managing recently run and scheduled reports, including running, editing, duplicating, scheduling, and deleting.
- **Run Reports** - Covers how to run the following different types of reports: High-Level Summary, Audit Detail, IT, Cloud Services, and Custom Template.
- **Use Interactive Reports** - Covers how to retrieve and use Interactive reports.
- **View Dashboard Charts** - Provides customizable and predefined Top and Trend charts of Web activity on users, groups, categories, classifications, sites, and traffic by visits, hits, bytes, time online, and more.

Typically, you will manually run reports that are not needed on a regular basis. Otherwise, we suggest that you set reports to run automatically by scheduling them. This will save a tremendous amount of time. Another way to save time, especially for IT administrators, is to assign manager accounts. Individuals with manager accounts can access the product, but with only a limited menu that lets them run reports on the groups and users that they have been authorized to review. To read how to set up manager accounts, see Add Logon Account.

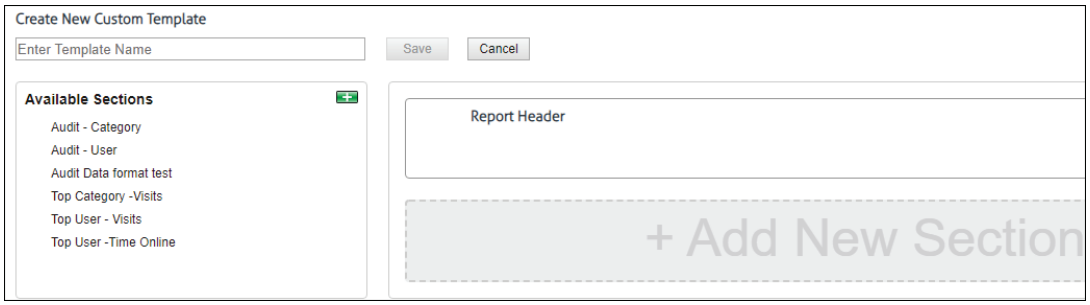
In addition, you can use the Interactive Reporting feature. With Interactive reports, report recipients can quickly drill down from higher-level reports to more detailed audit reports on a specific user, category, or classification rating without having to go back in the product to run a manual report.

Create a Custom Report Template

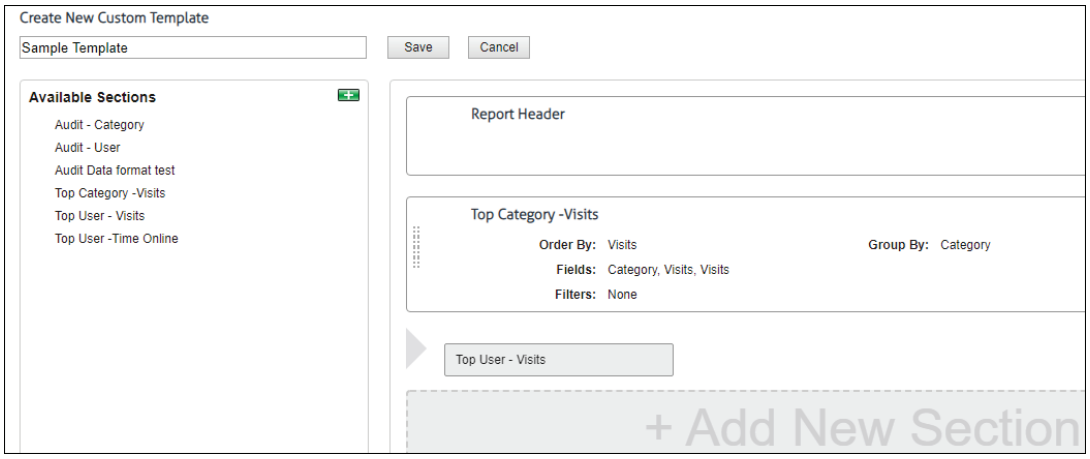
1. Go to **Reports - Templates**. The Templates page is displayed.



2. To create a custom report template, click the **Create New Custom Template** green plus icon. The **Create New Custom Template** page is displayed.



3. Enter a name for the template in the text box.

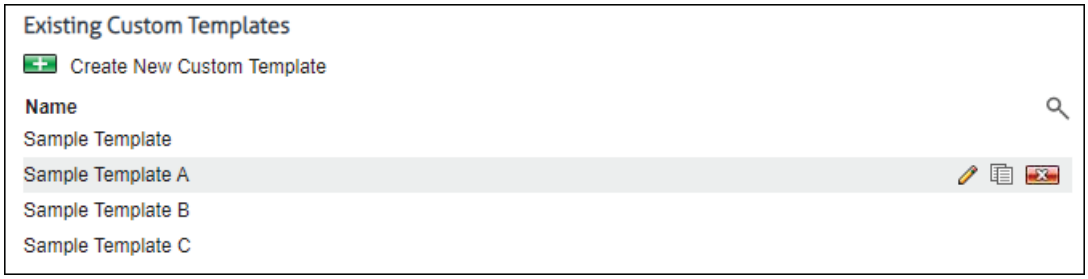


4. Next, add sections to the template in the right panel.
   - Under **Available Sections**, hover over the section you want to add, and click and drag it to the **Add New Section** area in the right panel. When a right arrow is displayed, release the mouse, and the new section will be added to the template.
   - Continue adding sections as necessary.
5. To reorder the sections, click and drag a section to its new location. When a right arrow is displayed, release the mouse, and the section will be moved to that location.
6. To delete a section from the template, hover over the section and click the red x icon.
7. Click **Save**. The new custom template is displayed on the **Existing Custom Templates** page.
8. Go to **Reports - Manager** to run the report for the custom template.

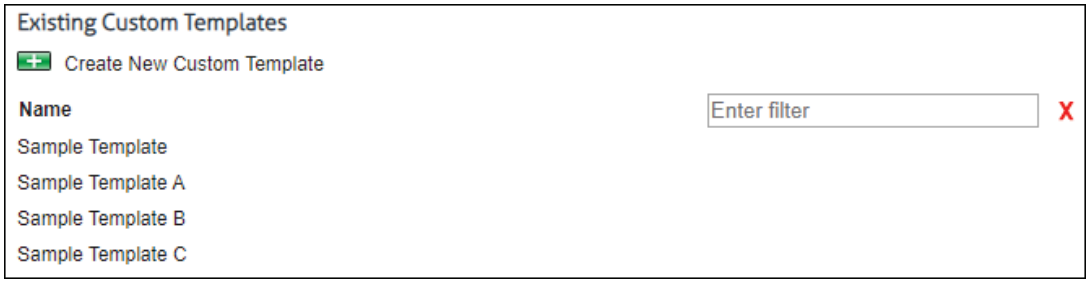
Manage Existing Custom Report Templates

You may edit, duplicate, and delete existing custom report templates. You can also quickly find a specific template by filtering the visible template entries.

1. Go to **Reports - Templates**. The Existing Custom Templates page is displayed.



2. To filter the list of templates, click the magnifying glass icon (**Filter View**). A text box is displayed.

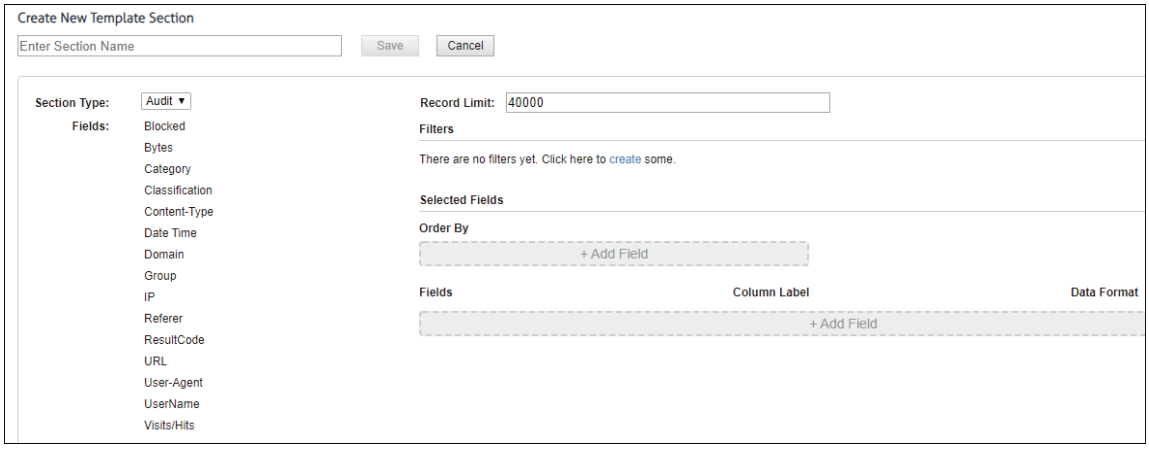


3. In the text box, enter what you want to search for. As you begin typing, templates with a matching name will be displayed in the list.
4. To cancel the filter, click the red x icon.
5. To edit a custom template, hover over the template name and click the pencil icon (**Edit Template**). The Edit Custom Template page is displayed where you may want to change the template name, or add, reorder, and delete sections in the template. See Create a Custom Report Template for details.
6. To duplicate a custom template, hover over the template and click the duplicate icon (**Duplicate Template**). The Create New Custom Template page is displayed. Make changes to the template name and sections in the template as desired.
7. To delete a custom template, hover over the template and click the red x icon (**Delete Template**). A dialog appears to confirm the deletion. Click **OK** and the template is removed from the list.

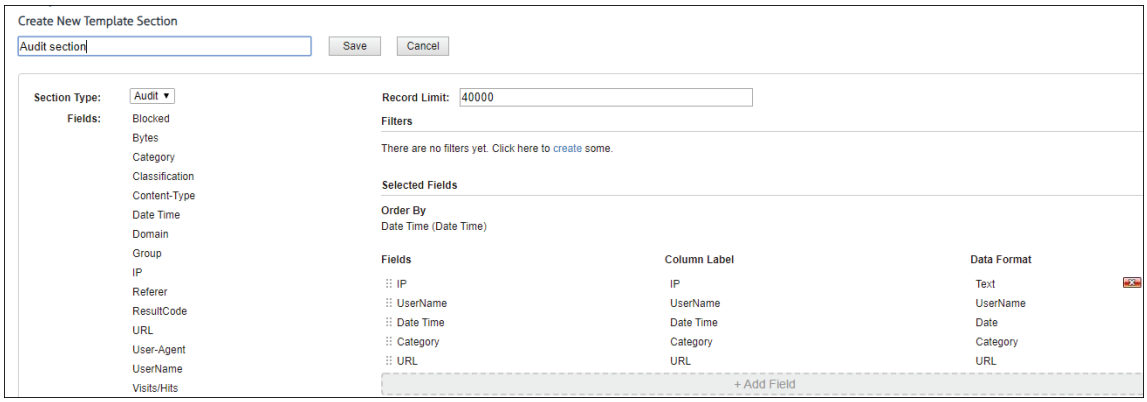
   NOTE: If you run a report from a custom template and then delete the template, the report will show as "Report Template Not Found!" in the Recently Run Reports section on the Manage Reports page. If you schedule a report to run from a custom template and then attempt to delete the template, you will be notified that the template is in use. In order to remove the template, you must first delete the report from the Scheduled Reports section on the Manage Reports page.

Create a New Report Template Section

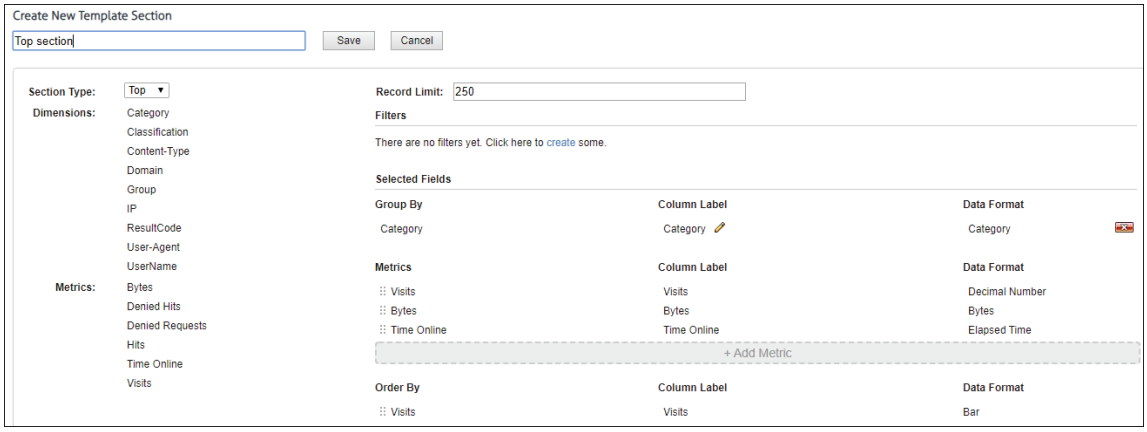
1. From the Create New Custom Template or Edit Custom Template page, click the **Create New Section** green plus icon to the right of **Available Sections**. The Create New Template Section page is displayed.



2. Enter a name for the section in the text box.
3. For **Section Type**, select **Audit** or **Top**.
    - An Audit section type gives you detailed information (i.e., many data fields) sorted by one field.
    - A Top section type is designed to group the data (e.g., by category) and provide quantitative measurements of the data (e.g., time online, number of visits), sorted by one field.
4. If you selected **Audit**, add fields to the **Order By** and **Fields** areas in the right panel.



    - Click and drag a field (e.g., Date Time) from the left panel to the **Order By Add Field** area in the right panel. The field is also copied to the **Fields** area below.
    - To add more fields, click and drag each field to the **Fields Add Field** area. When a right arrow is displayed, release the mouse, and the new field will be added to the section. Continue adding fields as necessary.
5. If you selected **Top**, add dimensions and metrics to the **Group By**, **Metrics**, and **Order By** areas in the right panel.

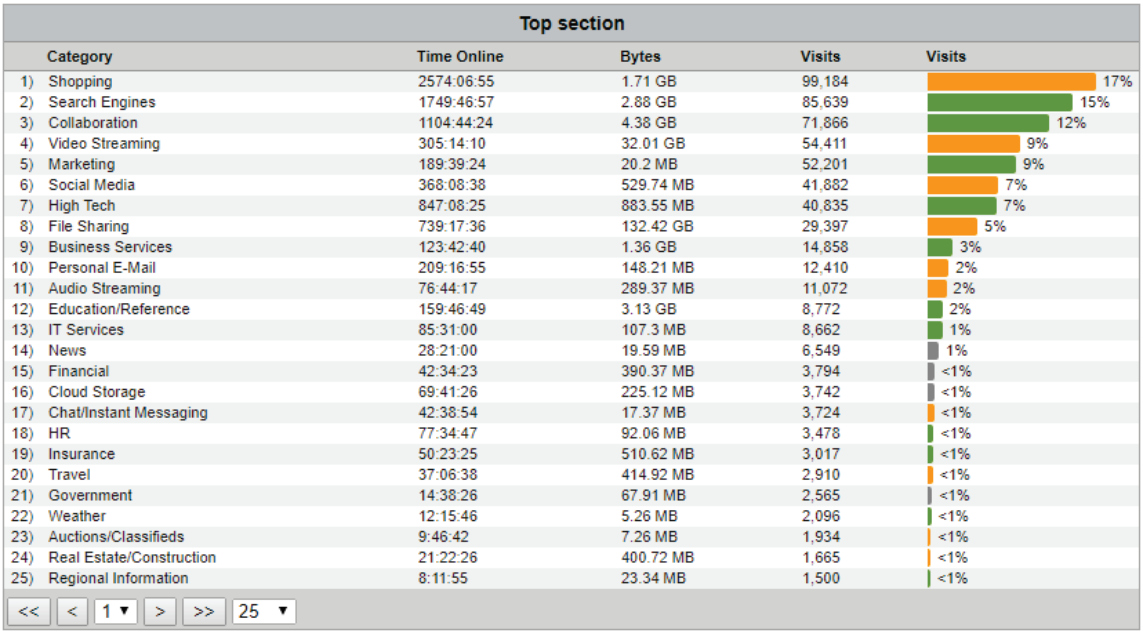


- Click and drag a dimension (e.g., Category) from the left panel to the **Group By Add Dimension** area in the right panel.
- Click and drag metrics (e.g., Time Online, Bytes) to the **Metrics Add Metric** area. When a right arrow is displayed, release the mouse, and the new field will be added to the section.
- Click and drag a metric (e.g., Visits) from the left panel to the **Order By Add Metric** area in the right panel.

6. To reorder the fields, click and drag a field to its new location. When a right arrow is displayed, release the mouse, and the field will be moved to that location.
7. To delete a field from the section, hover over the field and click the red x icon.
8. To edit a column label, hover over the label and click the label when the pencil icon appears. Type the change in the text box, and then click the green check mark.
9. To edit the data format, hover over the format type and click the format type when the pencil icon appears. Select another format type from the drop-down list. In the **Order By Add Metric** area, the format type is "Bar" by default and cannot be changed.
10. To set a limit on the number of records to display on the report, type the number in the **Record Limit** field. The maximum number of entries for a Top report is 250, and for an Audit is 40,000. The settings are in place to manage browser response times in rendering the data.
11. To filter the data, under **Filters**, click the **create** link. The Create Section Filters page is displayed.
    - Click the **Add New Filter** green plus icon. You may choose to include or exclude categories or networks.
    - In the **Type** field, select *Include* or *Exclude*.
    - In the **Field** field, select *Categories* or *Network*
    - In the **Categories or Networks** list respectively, click the category or network you want to include or exclude so that it is highlighted.
        - To select consecutive entries, click the first category or network. Then hold down SHIFT and click the last category or network.
        - To select nonconsecutive entries, click the first category or network. Then hold down CTRL and click the additional entries.
        - To unselect a category or network, hold down CTRL and click the selected entry.
    - Click **OK**.
    - To edit the filter, click the pencil icon. To delete the filter, click the red x icon.

12. Click **Save**. The new report template section is displayed under **Available Sections**.

    Below is an example of the results of a Top section in a custom template.



Top section

	Category	Time Online	Bytes	Visits	Visits
1)	Shopping	2574:06:55	1.71 GB	99,184	17%
2)	Search Engines	1749:46:57	2.88 GB	85,639	15%
3)	Collaboration	1104:44:24	4.38 GB	71,866	12%
4)	Video Streaming	305:14:10	32.01 GB	54,411	9%
5)	Marketing	189:39:24	20.2 MB	52,201	9%
6)	Social Media	368:08:38	529.74 MB	41,882	7%
7)	High Tech	847:08:25	883.55 MB	40,835	7%
8)	File Sharing	739:17:36	132.42 GB	29,397	5%
9)	Business Services	123:42:40	1.36 GB	14,858	3%
10)	Personal E-Mail	209:16:55	148.21 MB	12,410	2%
11)	Audio Streaming	76:44:17	289.37 MB	11,072	2%
12)	Education/Reference	159:46:49	3.13 GB	8,772	2%
13)	IT Services	85:31:00	107.3 MB	8,662	1%
14)	News	28:21:00	19.59 MB	6,549	1%
15)	Financial	42:34:23	390.37 MB	3,794	<1%
16)	Cloud Storage	69:41:26	225.12 MB	3,742	<1%
17)	Chat/Instant Messaging	42:38:54	17.37 MB	3,724	<1%
18)	HR	77:34:47	92.06 MB	3,478	<1%
19)	Insurance	50:23:25	510.62 MB	3,017	<1%
20)	Travel	37:06:38	414.92 MB	2,910	<1%
21)	Government	14:38:26	67.91 MB	2,565	<1%
22)	Weather	12:15:46	5.26 MB	2,096	<1%
23)	Auctions/Classifieds	9:46:42	7.26 MB	1,934	<1%
24)	Real Estate/Construction	21:22:26	400.72 MB	1,665	<1%
25)	Regional Information	8:11:55	23.34 MB	1,500	<1%

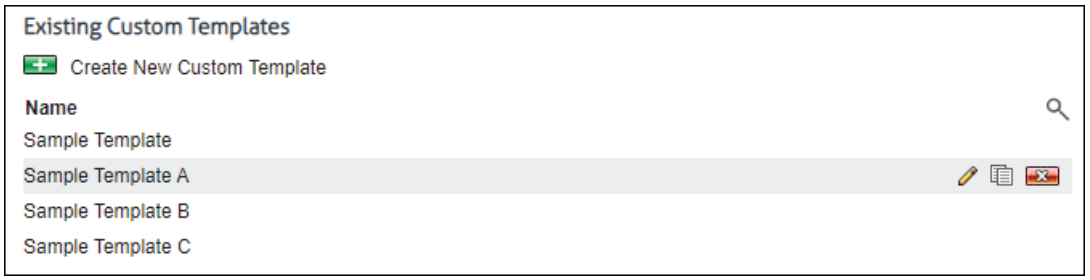
<< < 1 > >> 25

    The pagination icons at the bottom of the results allow you to page through the records. The first drop-down box indicates the number of pages; the second drop-down box allows you to set how many records to view per page, i.e., 10, 25 (default), 50, and so on.

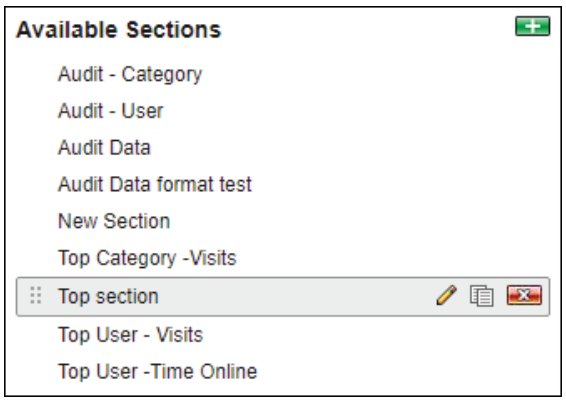
Manage Existing Report Template Sections

You may edit, duplicate, and delete existing report template sections.

1. Go to **Reports - Templates**.



2. Click the **Create New Custom Template** green plus icon, or click the pencil icon to edit an existing custom report template.
3. To edit a report template section, hover over the section and click the pencil icon (**Edit**). The Edit Template Section page is displayed where you can change the section name, record limit, and filter, and add, reorder, and delete fields in the section. See Create a New Report Template Section for details.

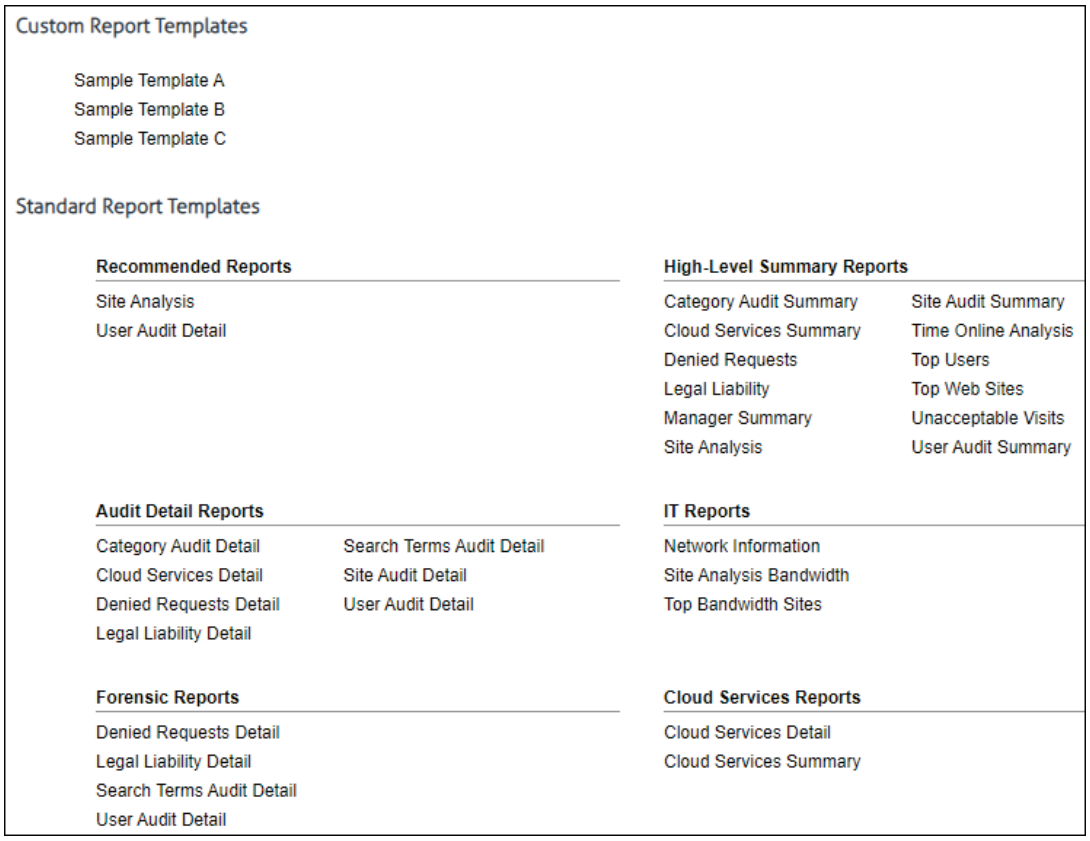


4. To duplicate a report template section, hover over the section and click the duplicate icon (**Duplicate**). The Create New Template Section page is displayed. Make changes to the section as desired.
5. To delete a report template section, hover over the section and click the red x icon (**Delete**). A dialog appears to confirm the deletion. Click **OK** and the section is removed from the list.

   NOTE: If you add a section to a custom template and then delete the section, you will be notified that the section will also be removed from the template.

Report Selection

1. Go to **Reports - Manager**. The Report Selection page is displayed if no recently run or scheduled reports exist, that is, you are a first-time user or have deleted all reports.

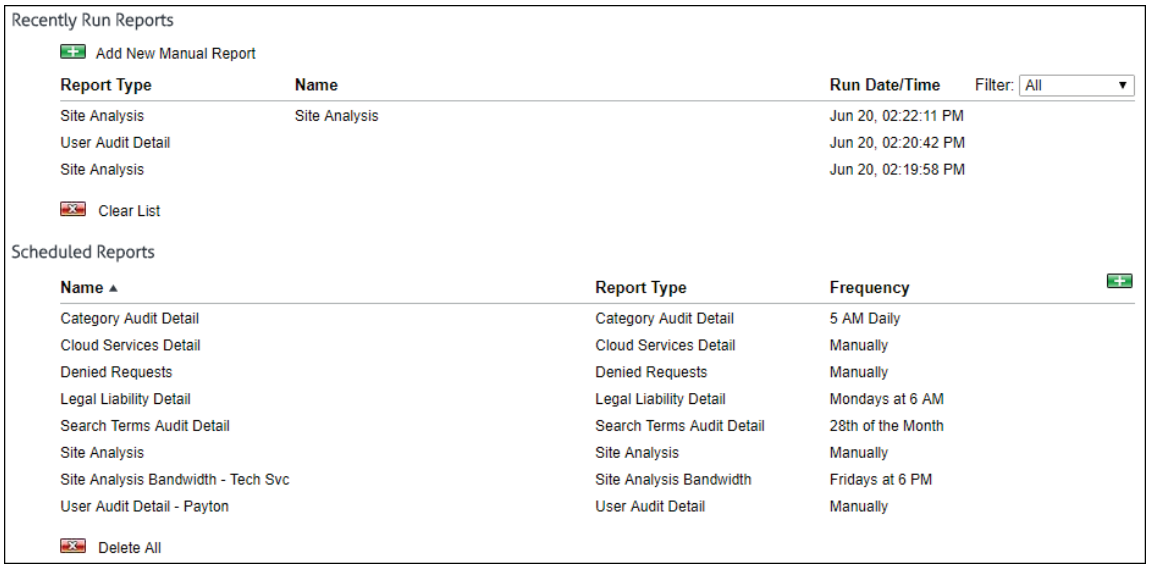


2. The **Custom Report Templates** section is blank if you are a first-time user. Otherwise, any created custom report templates are displayed.
3. The **Standard Report Templates** section shows the default report templates provided with the product.
    a. To see a description of a report, hover over the report name, and then hover over the question mark icon that appears beside it. A short description of the report is displayed.
    b. To create a report, click the report name. The Create Report page is displayed. See Run a High-Level Summary Report or Run an Audit Detail Report for instructions on how to run reports.

NOTE: A Back button is displayed only if you arrived at this page by clicking a green plus icon on the Manage Reports page to create a report.

Manage Reports

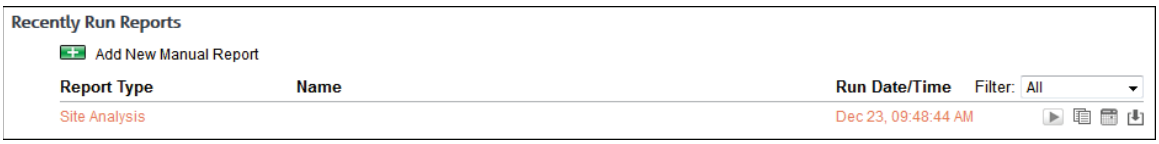
Go to **Reports - Manager**. The Manage Reports page is displayed if recently run or scheduled reports exist.



Recently Run Reports

This section shows reports (from standard and custom templates) that were run manually and through scheduling. Reports can be run at the present time (that is, unscheduled) as well as scheduled or set up to run at a later time. Unscheduled reports have no report name; whereas, scheduled reports have a saved name. Up to ten reports are displayed in this list and are sorted by run date/time in descending order.

1. To create a report, click the **Add New Manual Report** green plus icon. The Report Selection page is displayed where you can select the type of report you want to create.
2. Hover over a report line to display available icons.



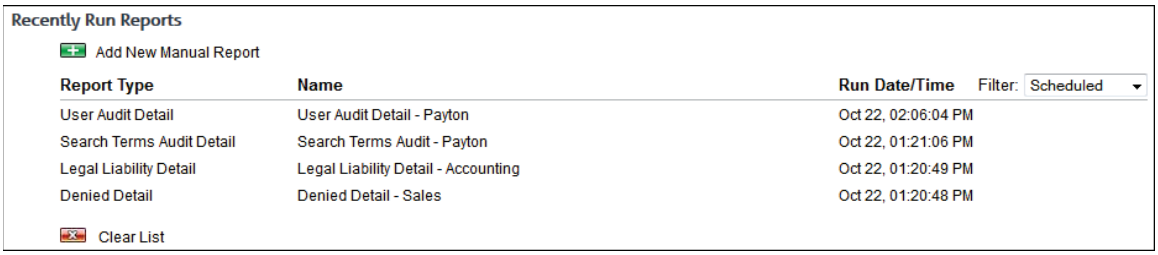
3. To run a report, click the play icon. The report runs and is displayed at the top of the list with *Running* in the **Run Date/Time** column indicating that it is processing.

- If there are many reports running, you will see *Running* for one report and *Pending* for the remaining reports indicating that they are in the queue to be processed.
- If a report has failed to run for any reason, you will see *Failed to run.* The report will not run, and you will receive an e-mail if *E-Mail* was selected for the report delivery.
  - A duplicate icon will be available for you to rerun the report with different settings if necessary.
  - A view details icon will allow you to view the reason that the report failed to run and the report parameters used.

4. To create an exact copy of an unscheduled report, click the duplicate icon. The Create Report page is displayed where you can make changes to the settings and run the report.
5. To create an exact copy of a scheduled report, click the duplicate icon. The Create Report page is displayed where you can make changes to the settings and schedule the report. Be sure to enter a different name for the report.
6. To schedule a report, click the calendar icon. The calendar icon is available for only unscheduled reports. The Create Report page is displayed where you can make changes to the settings and schedule the report.
7. To view the report, click the view icon. If multiple reports were generated depending on how you ran the report, a list is displayed with links. Click the link for the report you want to view. When you are finished with the report, click **Back to List** to return to the list of reports, or click **Close** to close the window.

   NOTE: If you run a report from a custom template and then delete the template, only the view icon will be available. The icons to run, duplicate, or schedule the report will not be available.

8. To change the view of the recently run reports, select *Scheduled* or *Unscheduled* in the **Filter** field. The default is *All*. If you selected *Scheduled* or *Unscheduled*, the last ten scheduled or unscheduled reports will be displayed.

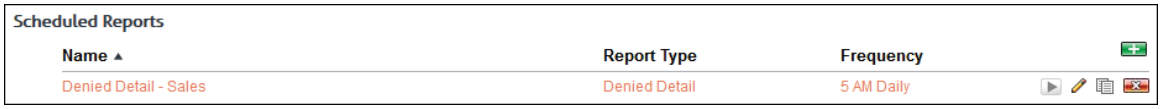


9. To clear the list of recently run reports, click the **Clear List** red x icon.
   - A dialog box is displayed confirming the removal of all recently run reports including any pending reports.
   - Click **Clear List**. The list is cleared, and a message indicates that there are no recently run reports.

Scheduled Reports

This section shows reports (from standard and custom templates) that were scheduled to run automatically at a specific time and those that were set up to run manually as needed. An unlimited number of reports can be displayed in this list and are sorted by name in ascending order.

1. To schedule a new report, click the green plus icon to the right of the **Frequency** column. The Report Selection page is displayed where you can select the type of report you want to create.
2. Hover over a report line to display available icons. You can also hover over the data in the **Frequency** column to display the next run date/time for a report.



3. To run a report, click the play icon. The report runs and is displayed in the **Recently Run Reports** section with *Running* in the **Run Date/Time** column indicating that it is processing. If there are many reports to be processed, you will see *Pending* indicating that the report is in the queue.
4. To edit a report, click the pencil icon. The Edit Report page is displayed where you can modify the settings of the scheduled report.
    - On the Edit Report page, a Delete button is available to allow you to delete the report.
    - The deleted report will be removed from the Scheduled Reports list. If it exists in the Recently Run Reports list, only the name will be removed indicating that it is no longer a scheduled report.
5. To create an exact copy of a report, click the duplicate icon. The Create Report page is displayed where you can make changes to the settings and schedule the report. Be sure to enter a different name for the report.
6. To sort the list of reports, click the column title to sort by that column. An arrow is displayed next to the column title when you hover over it indicating that the column is sortable.

    NOTE: The **Frequency** column is sorted using the current date/time as the point of reference. In ascending order, *Manually* is displayed at the bottom of the list.
7. To delete a report, click the red x icon on the report line. The deleted report will be removed from the Scheduled Reports list. If it exists in the Recently Run Reports list, only the name will be removed indicating that it is no longer a scheduled report.
8. To delete all reports, click the **Delete All** red x icon.
    - A dialog box is displayed confirming the deletion of all scheduled reports.
    - Click **Delete All**. The reports are deleted, and a message indicates that there are no scheduled reports.

NOTE: When all recently run reports and scheduled reports have been removed, the Report Selection page will be displayed.

Run a High-Level Summary Report

High-level reports give summarized information on employee Web use including the Web activity of your remote employees, i.e., cloud users, in a Hybrid deployment. 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:

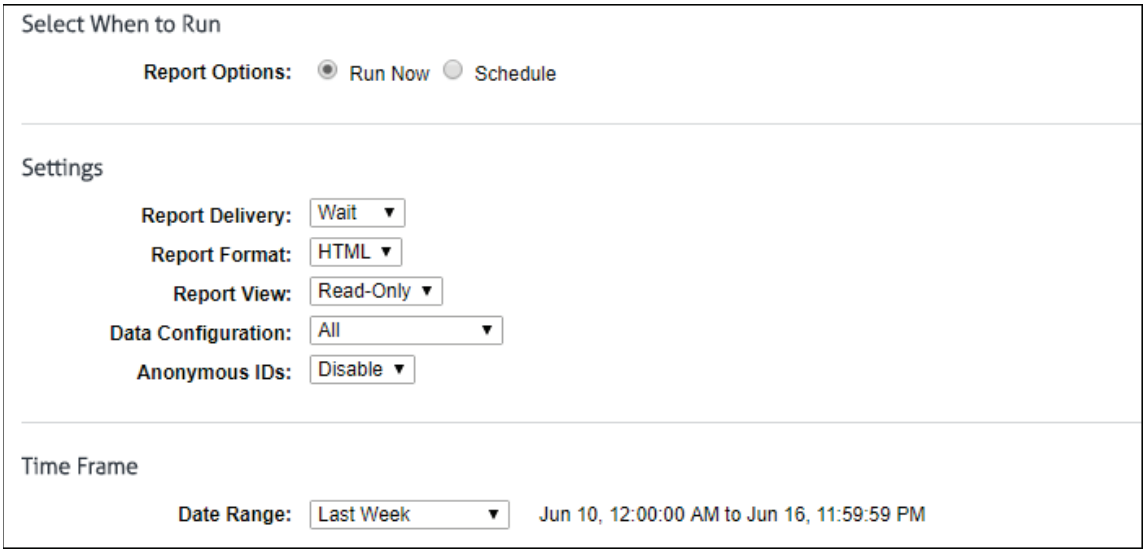
- Total visits by acceptability classification (acceptable, unacceptable, neutral)
- Total visits by content category (Shopping, Pornography, etc.)
- Total visits by group
- Total visits by user
- Total visits by user, per category

NOTE: For descriptions of all high-level reports, see Appendix B.

1. Go to **Reports - Manager**. The 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 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**, in the **Report Delivery** field, select one of the following options:
   - *Wait* - This option is available for only the **Run Now** option. After the report runs, you can view, save, and print it. The report is saved with a universally unique identifier (UUID) in the file name, e.g., 14ec2d98-346f-4cb5-806a-f85f7b74f1e1.html.
   - *E-Mail* - This option allows you to specify e-mail addresses to which you want to send the report. In the **Recipients** field, enter a valid e-mail address. 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. The report is sent in the file name format that you specified in Report Options.

5. In the **Report Format** field, select *HTML* or *PDF*.

   NOTE: If you select *PDF*, you will only have the option to get a Read-Only report (selected in the **Report View** field below).

6. In the **Report View** field, select *Read-Only* or *Interactive* if available.

7. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Data Configuration** field is displayed to allow you to choose a configuration to include in the report. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.

   NOTE: Cloud log files are imported nightly similar to local logs, and reports would be current as of the previous day. To get a report with the current day's cloud data, go to Settings - Hybrid, perform a manual sync, and then run the report. Manager accounts would have to see their administrator for the current day's cloud data.

   NOTE: You can verify that cloud log files have been transferred by going to **Data Management - Log Data Source - Viewer**.

8. If you have a network segment configured, The Network field is displayed to allow you to choose a specific network to include in the report. Select a network or all networks. If no networks are configured, a link to the Network Segment config screen is provided.

9. In the **Anonymous IDs** field, select *Enable* if anonymous IDs are turned on in the product and you want to display IDs anonymously on the report.

   NOTE: This field is not available if the **Report View** field is set to *Interactive*.

   NOTE: If anonymous IDs are turned off in the product on the Settings - Reports - Options page, existing reports with anonymous IDs enabled will not generate anonymized reports.

10. 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.

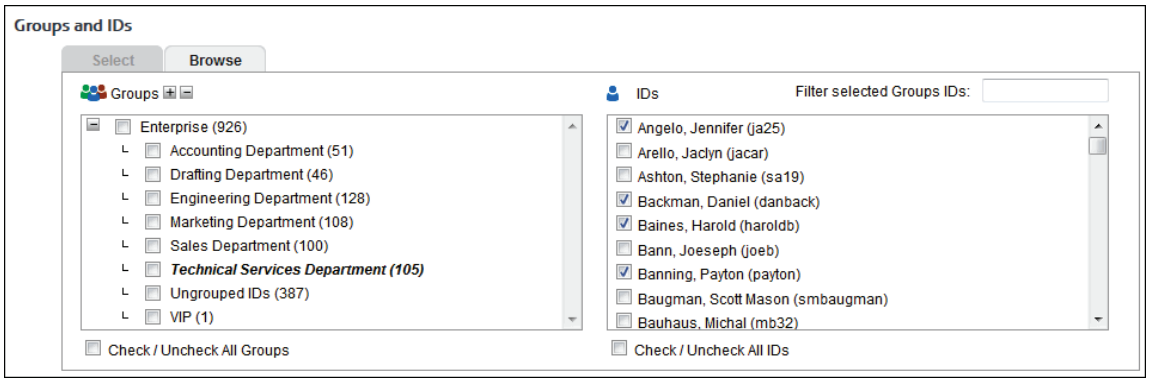
    - All predefined time frames end at 11:59:59 P.M., except *Previous 24 Hours* which ends one second before the current hour.
    - When scheduling a report, the **Date Range** options are based on the **Frequency** selection, that is, they are less than the frequency. For example, you cannot schedule 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*.
    - 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.

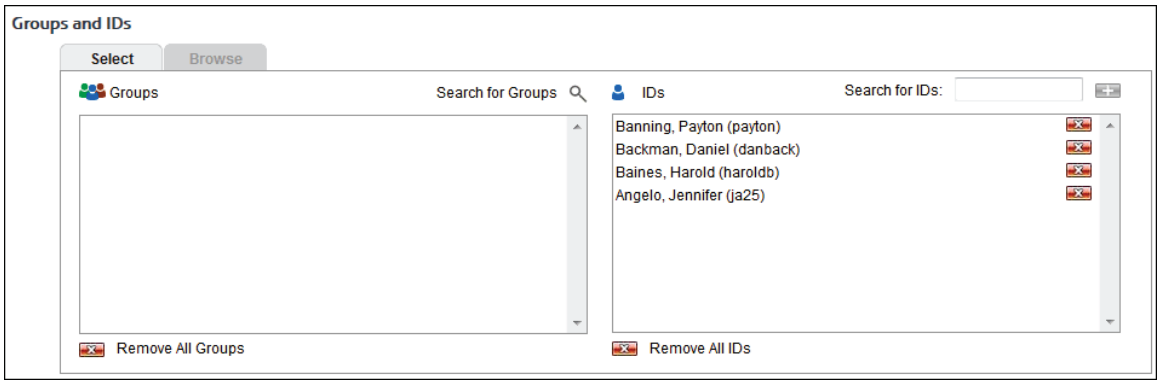
11. Under **Groups and IDs** on the Browse tab, choose groups and IDs by selecting their corresponding check box. To view IDs in a group, click the group name.



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.

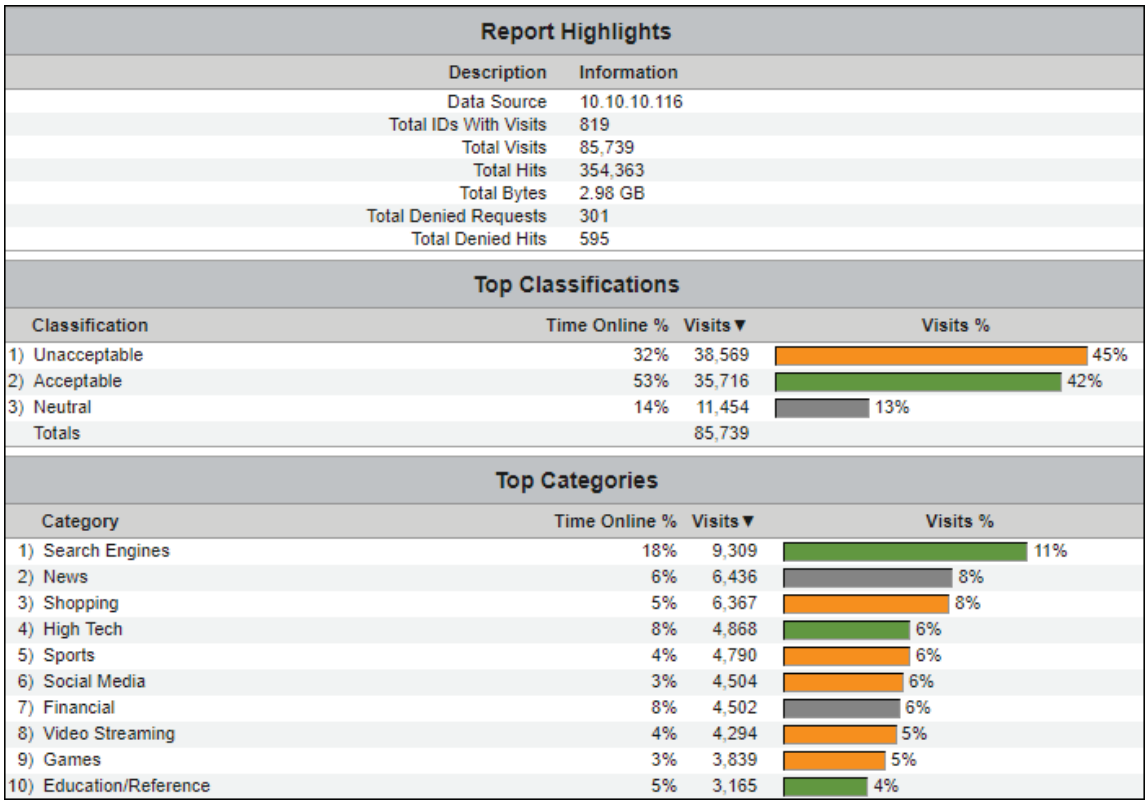
The groups and IDs that you have selected will appear on the Select tab.



12. 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.
13. 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.

14. Click **Run Now**.
    - Depending on how long the report takes to run, you may see a progress meter.
    - If one report was generated, it opens in a Report Results page where you can view, save, and print it.
    - If multiple reports were generated depending on how you ran the report, a Reports List page is displayed with links. Click the link for the report you want to view. When you are finished with the report, click **Back to List** to return to the list of reports, or click **Close** to close the window.
15. If you selected the **Schedule** option, the **Schedule and Run** and **Schedule** buttons are available.
    - Click **Schedule and Run** to schedule and deliver the report.
    - Click **Schedule** to only schedule the report.
16. 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%

Run an Audit Detail Report

Audit detail reports (or low-level reports) are designed to give detailed information on individual employee Web use including the Web activity of your remote employees, i.e., cloud users, in a Hybrid deployment. These reports show the actual URLs visited.

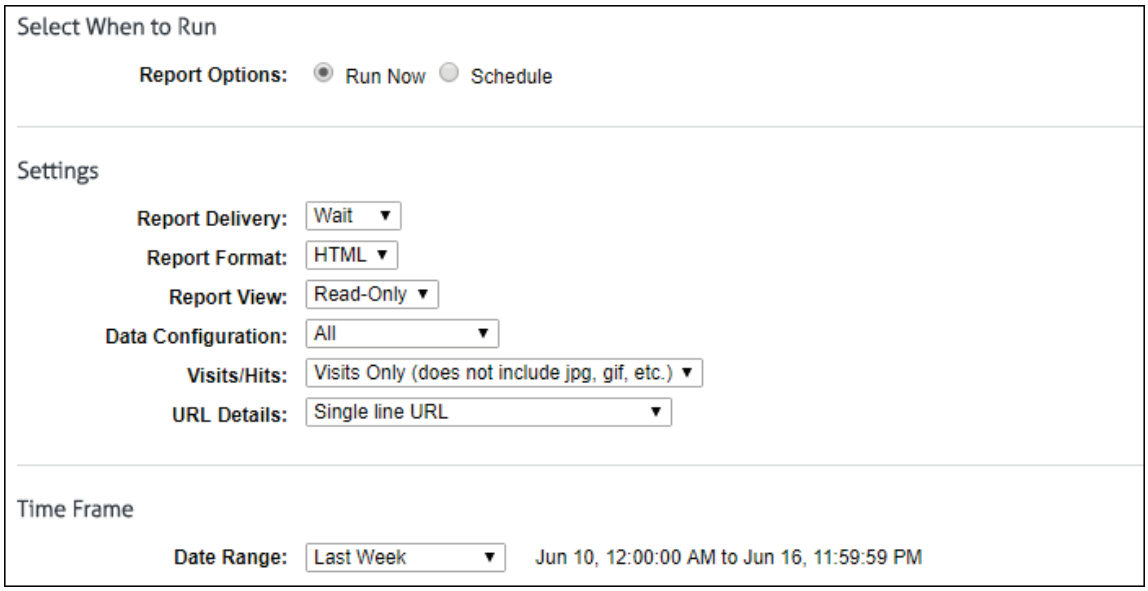
This section provides instructions on running a User Audit Detail report, but these instructions will work for any audit detail report you wish to run. The User Audit Detail report focuses on a single user. Every visit made by the user is listed separately in the main body of the report, and visits are listed chronologically by date and time.

NOTE: For descriptions of all audit detail reports, see Appendix B.

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 **Audit Detail Reports**, click **User Audit Detail**. 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 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**, in the **Report Delivery** field, select one of the following options:

- *Wait* - This option is available for only the **Run Now** option. After the report runs, you can view, save, and print it. The report is saved with a universally unique identifier (UUID) in the file name, e.g., 14ec2d98-346f-4cb5-806a-f85f7b74f1e1.html.
- *E-Mail* - This option allows you to specify e-mail addresses to which you want to send the report. In the **Recipients** field, enter a valid e-mail address. 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. The report is sent in the file name format that you specified in Report Options.

5. In the **Report Format** field, select *HTML* or *PDF*.

   NOTE: If you select *PDF*, you will only have the option to get a Read-Only report (selected in the **Report View** field below).

6. In the **Report View** field, select *Read-Only* or *Interactive* if available.
7. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Data Configuration** field is displayed to allow you to choose a configuration to include in the report. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.

   NOTE: Cloud log files are imported nightly similar to local logs, and reports would be current as of the previous day. To get a report with the current day's cloud data, go to Settings - Hybrid, perform a manual sync, and then run the report. Manager accounts would have to see their administrator for the current day's cloud data.

   NOTE: You can verify that cloud log files have been transferred by going to **Data Management - Log Data Source - Viewer**.

8. If you have a network segment configured, The Network field is displayed to allow you to choose a specific network to include in the report. Select a network or all networks. If no networks are configured, a link to the Network Segment config screen is provided.
9. In the **Visits/Hits** field, select whether you want visits only or all hits displayed on the report.

   NOTE: Choose *Visits Only* if you want the report to count and show only true visits, i.e., actual user clicks. Doing so will exclude all other types of hits, e.g., banners, ads, and audio. Choose *All Hits* if you want reports to show all types of hits, solicited or unsolicited.

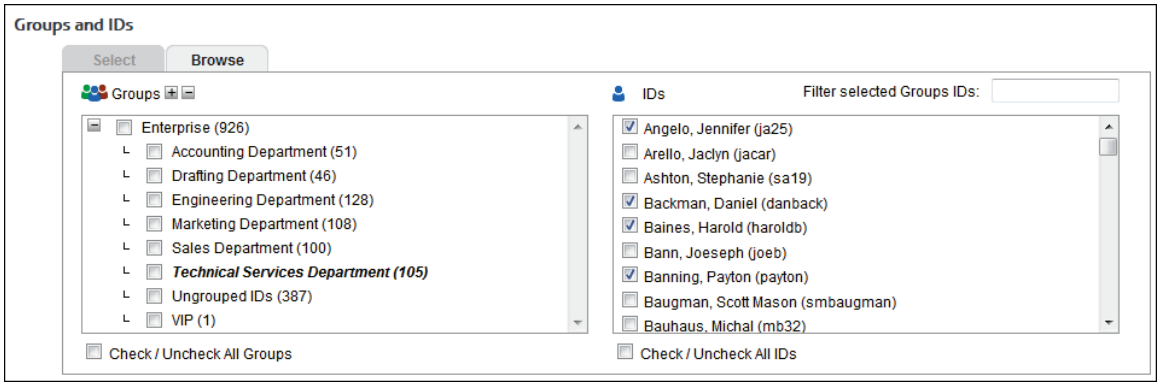
10. For **URL Details**, choose how you want the URLs to display on the report. The default setting is *Single line URL*, which means that URLs will be truncated if they are longer than one line. If full URLs are needed, you can choose *Full URLs*. This means that the full URL will be shown, even if it takes two or three lines to display it. *Text* is another option in which URLs will be wrapped and in plain text format.
11. 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*.
    - 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.

12. 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.

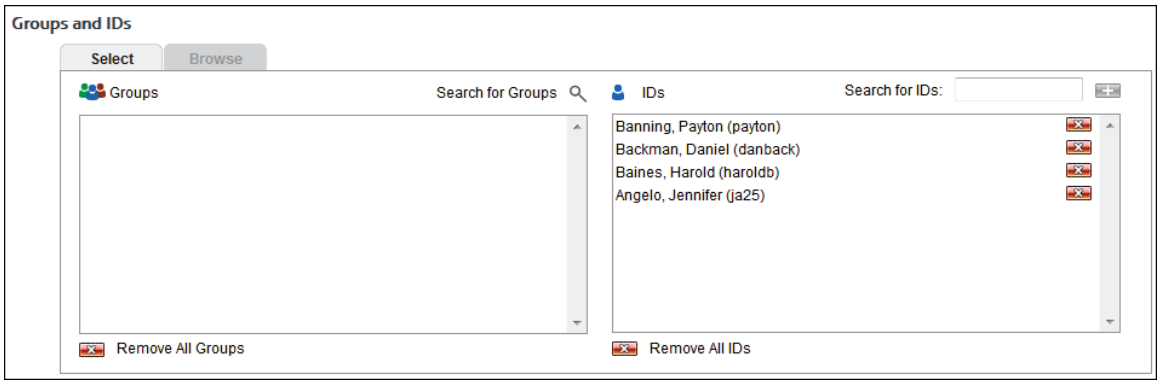
    CAUTION: You cannot run a User Audit Detail report on the Enterprise group. You can run the report on other groups, but this means a User Audit Detail report will run on each user in the selected group.



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.



13. 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.
14. 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.
15. Click **Run Now**.
    - Depending on how long the report takes to run, you may see a progress meter.
    - If one report was generated, it opens in a Report Results page where you can view, save, and print it.
    - If multiple reports were generated depending on how you ran the report, a Reports List page is displayed with links. Click the link for the report you want to view. When you are finished with the report, click **Back to List** to return to the list of reports, or click **Close** to close the window.
16. If you selected the **Schedule** option, the **Schedule and Run** and **Schedule** buttons are available.
    - Click **Schedule and Run** to schedule and deliver the report.
    - Click **Schedule** to only schedule the report.
17. Click **Back** to return to the previous page.

    Below is an example of a User Audit Detail report. The data may be filtered by IP address if more than one exists for the user, by category, and by URL.

170)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:09:26 PM	Video Streaming	http://youtube.com/fido-1/1
171)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:09:33 PM	Video Streaming	http://youtube.com/fido-1/1
172)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:09:37 PM	Video Streaming	http://youtube.com/fido-1/r
173)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:09:43 PM	Video Streaming	http://youtube.com/fido-1/1
174)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:09:47 PM	Video Streaming	http://youtube.com/fido-1/1
175)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:09:52 PM	Video Streaming	http://youtube.com/fido-1/1
176)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:10:10 PM	High Tech	http://hpcc998.external.hp.
177)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:10:24 PM	Social Media	http://linkedin.com/fido-1/2
178)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:10:39 PM	Video Streaming	http://youtube.com/fido-1/3
179)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:11:08 PM	Video Streaming	http://youtube.com/fido-1/3
180)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:11:13 PM	Video Streaming	http://youtube.com/fido-1/1
181)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:11:17 PM	Video Streaming	http://youtube.com/fido-1/1
182)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:11:24 PM	Video Streaming	http://youtube.com/fido-1/1
183)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:11:38 PM	High Tech	http://hpcc920.external.hp.
184)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:12:02 PM	High Tech	http://www.hp.com/go/sear
185)	10.10.30.166	Banning, Payton (payton)	Jul 23, 2017 12:12:24 PM	High Tech	http://hpcc866.external.hp.

Run an IT Report

The Site Analysis Bandwidth report is one of our IT reports. These reports, which supplement the high-level and low-level reports, cover the areas that IT personnel find useful when monitoring Web usage and network resources. In a Hybrid deployment, they cover the Web usage of your remote employees, i.e., cloud users.

This section provides instructions on running a Site Analysis Bandwidth report, but these instructions will work for any IT report you wish to run. The report is similar to the Site Analysis report, but it focuses on

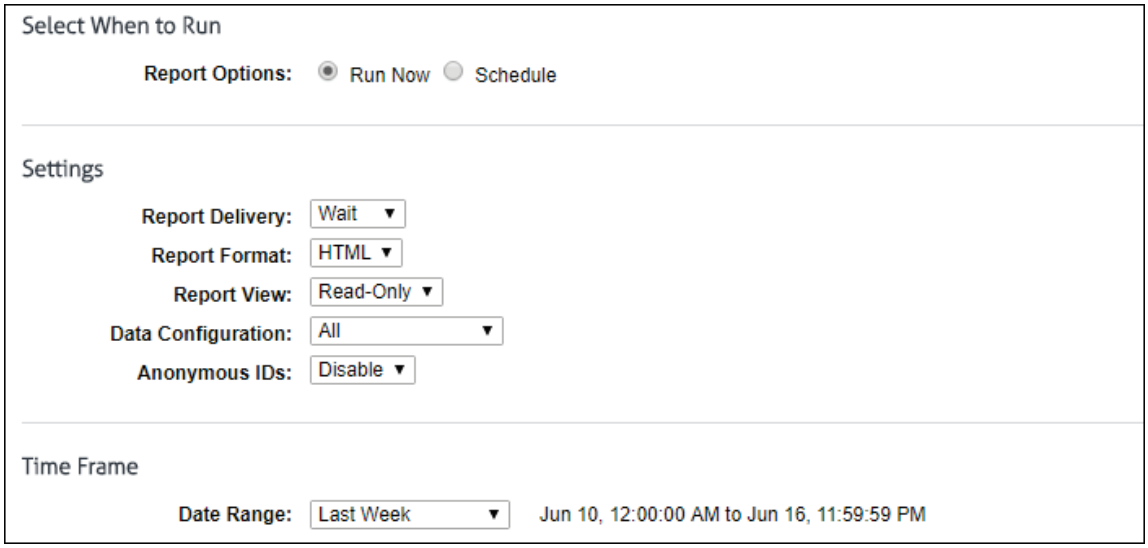
bandwidth consumption instead of Web site content. It breaks down bandwidth usage by acceptability classification, category, group, user, and user within each category.

NOTE: For descriptions of all IT reports, see Appendix B.

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 **IT Reports**, click **Site Analysis Bandwidth**. 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 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**, in the **Report Delivery** field, select one of the following options:

- *Wait* - This option is available for only the **Run Now** option. After the report runs, you can view, save, and print it. The report is saved with a universally unique identifier (UUID) in the file name, e.g., 14ec2d98-346f-4cb5-806a-f85f7b74f1e1.html.
- *E-Mail* - This option allows you to specify e-mail addresses to which you want to send the report. In the **Recipients** field, enter a valid e-mail address. 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. The report is sent in the file name format that you specified in Report Options.

5. In the **Report Format** field, select *HTML* or *PDF*.

   NOTE: If you select *PDF*, you will only have the option to get a Read-Only report (selected in the **Report View** field below).

6. In the **Report View** field, select *Read-Only* or *Interactive* if available.
7. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Data Configuration** field is displayed to allow you to choose a configuration to include in the report. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.

   NOTE: Cloud log files are imported nightly similar to local logs, and reports would be current as of the previous day. To get a report with the current day's cloud data, go to Settings - Hybrid, perform a manual sync, and then run the report. Manager accounts would have to see their administrator for the current day's cloud data.

   NOTE: You can verify that cloud log files have been transferred by going to **Data Management - Log Data Source - Viewer**.

8. If you have a network segment configured, The Network field is displayed to allow you to choose a specific network to include in the report. Select a network or all networks. If no networks are configured, a link to the Network Segment config screen is provided.
9. In the **Anonymous IDs** field, select *Enable* if anonymous IDs are turned on in the product and you want to display IDs anonymously on the report.

   NOTE: This field is not available if the **Report View** field is set to *Interactive*.

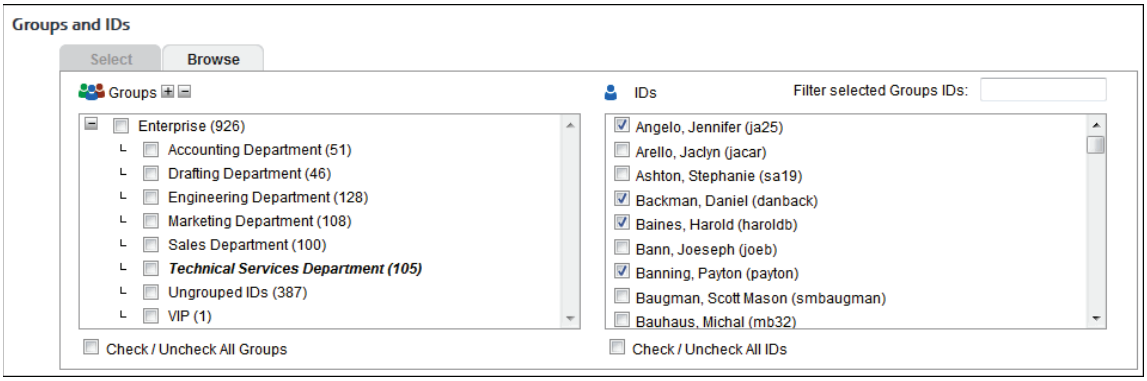
   NOTE: If anonymous IDs are turned off in the product on the Settings - Reports - Options page, existing reports with anonymous IDs enabled will not generate anonymized reports.

10. 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*.
    - 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.

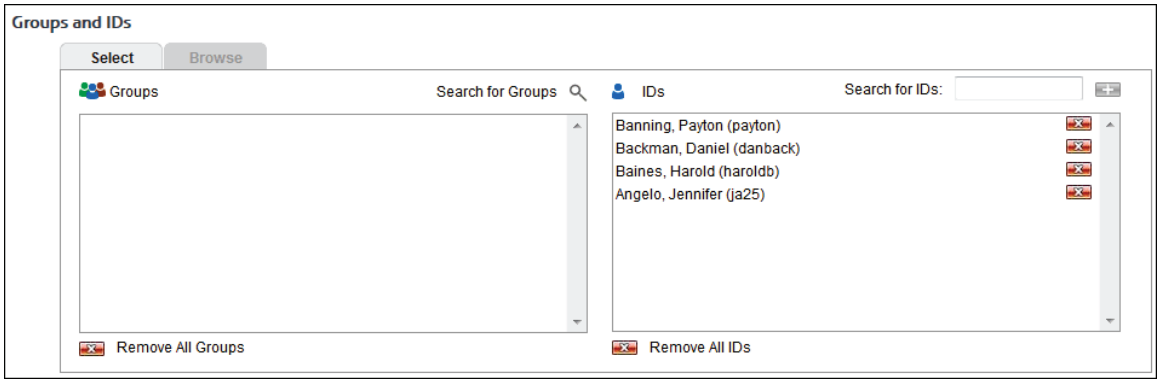
11. Under **Groups and IDs** on the Browse tab, choose groups and IDs by selecting their corresponding check box. To view IDs in a group, click the group name.



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.



12. 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.
13. 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.

14. Click **Run Now**.
    - Depending on how long the report takes to run, you may see a progress meter.
    - If one report was generated, it opens in a Report Results page where you can view, save, and print it.
    - If multiple reports were generated depending on how you ran the report, a Reports List page is displayed with links. Click the link for the report you want to view. When you are finished with the report, click **Back to List** to return to the list of reports, or click **Close** to close the window.
15. If you selected the **Schedule** option, the **Schedule and Run** and **Schedule** buttons are available.
    - Click **Schedule and Run** to schedule and deliver the report.
    - Click **Schedule** to only schedule the report.
16. Click **Back** to return to the previous page.

    Below is an example of a Site Analysis Bandwidth report.

Report Highlights

Description	Information
Data Source	10.10.10.116
Trend Start Date/Time	Jul 15, 2017 8:00:01 PM
Trend Stop Date/Time	Jul 23, 2017 8:00:00 PM
Total IDs With Visits	778
Total Visits	73,945
Total Hits	303,072
Total Bytes	2.46 GB
Total Denied Requests	265
Total Denied Hits	498

Top Classifications

Classification	Trend Bytes	Bytes ▼	Bytes %
1) Acceptable	341%	1.35 GB	55%
2) Unacceptable	265%	876.71 MB	35%
3) Neutral	318%	259 MB	10%
Totals		2.46 GB	

Top Categories

Category	Trend Bytes	Bytes ▼	Bytes %
1) High Tech	417%	305.72 MB	13%
2) Search Engines	568%	208.06 MB	9%
3) IT Services	1681%	193.25 MB	8%
4) News	301%	138.59 MB	6%
5) Games	303%	137.34 MB	6%
6) Education/Reference	408%	137.15 MB	6%
7) Video Streaming	379%	123.27 MB	5%
8) Audio Streaming	277%	104.6 MB	4%
9) Sports	296%	77.97 MB	3%
10) Financial	429%	77.54 MB	3%

Run a Cloud Services Report

Cloud services reports show employee Web use of cloud services including the Web activity of your remote employees, i.e., cloud users, in a Hybrid deployment. Cloud service Web activity includes visits to sites in the Audio Streaming, Cloud Infrastructure, Cloud Storage, Collaboration, CRM, Development, File Sharing, HR, Personal E-Mail, Video Streaming, and VoIP Services categories.

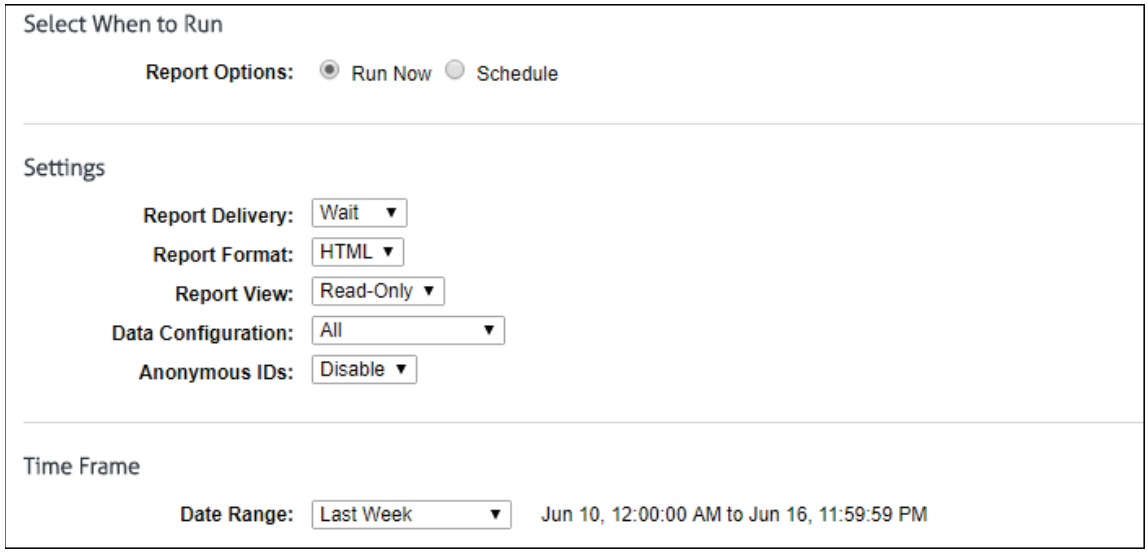
This section covers how to run a Cloud Services Summary report which is a high-level cloud services report. For instructions on running a low-level cloud services report such as the Cloud Services Detail report, see Run an Audit Detail Report.

NOTE: For descriptions of all reports, see Appendix B.

1. Go to **Reports - Manager**. The 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 **Cloud Services Reports**, click **Cloud Services Summary**. 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 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**, in the **Report Delivery** field, select one of the following options:
   - *Wait* - This option is available for only the **Run Now** option. After the report runs, you can view, save, and print it. The report is saved with a universally unique identifier (UUID) in the file name, e.g., 14ec2d98-346f-4cb5-806a-f85f7b74f1e1.html.
   - *E-Mail* - This option allows you to specify e-mail addresses to which you want to send the report. In the **Recipients** field, enter a valid e-mail address. 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. The report is sent in the file name format that you specified in Report Options.
5. In the **Report Format** field, select *HTML* or *PDF*.

   NOTE: If you select *PDF*, you will only have the option to get a Read-Only report (selected in the **Report View** field below).
6. In the **Report View** field, select *Read-Only* or *Interactive* if available.
7. If you have a Hybrid deployment and CyBlock is paired with your cloud accounts, the **Data Configuration** field is displayed to allow you to choose a configuration to include in the report. The cloud configuration selections show as your pairing cloud servers and contain the domain cloud.cyblock.com. You may select your cloud configuration, your local CyBlock configuration, or all configurations.

   NOTE: Cloud log files are imported nightly similar to local logs, and reports would be current as of the previous day. To get a report with the current day's cloud data, go to Settings - Hybrid, perform a manual sync, and then run the report. Manager accounts would have to see their administrator for the current day's cloud data.

   NOTE: You can verify that cloud log files have been transferred by going to **Data Management - Log Data Source - Viewer**.
8. If you have a network segment configured, The Network field is displayed to allow you to choose a specific network to include in the report. Select a network or all networks. If no networks are configured, a link to the Network Segment config screen is provided.
9. In the **Anonymous IDs** field, select *Enable* if anonymous IDs are turned on in the product and you want to display IDs anonymously on the report.

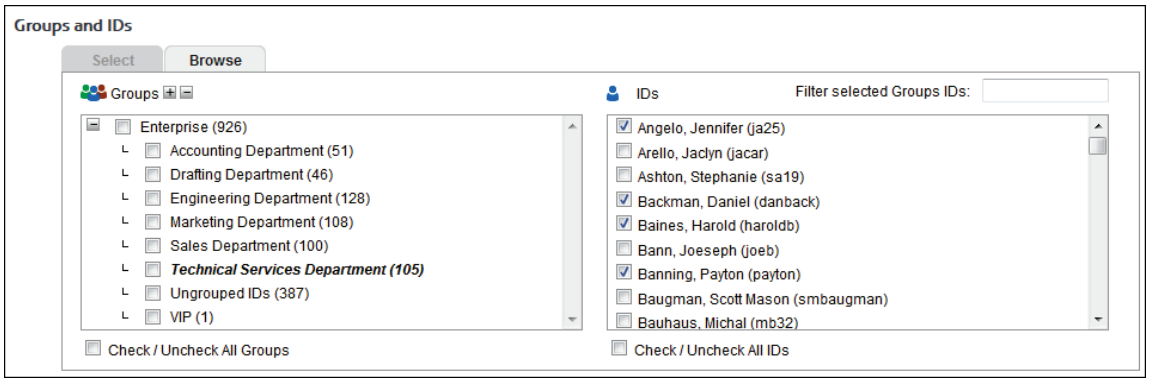
   NOTE: This field is not available if the **Report View** field is set to *Interactive*.

   NOTE: If anonymous IDs are turned off in the product on the Settings - Reports - Options page, existing reports with anonymous IDs enabled will not generate anonymized reports.
10. 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*.
    - 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.

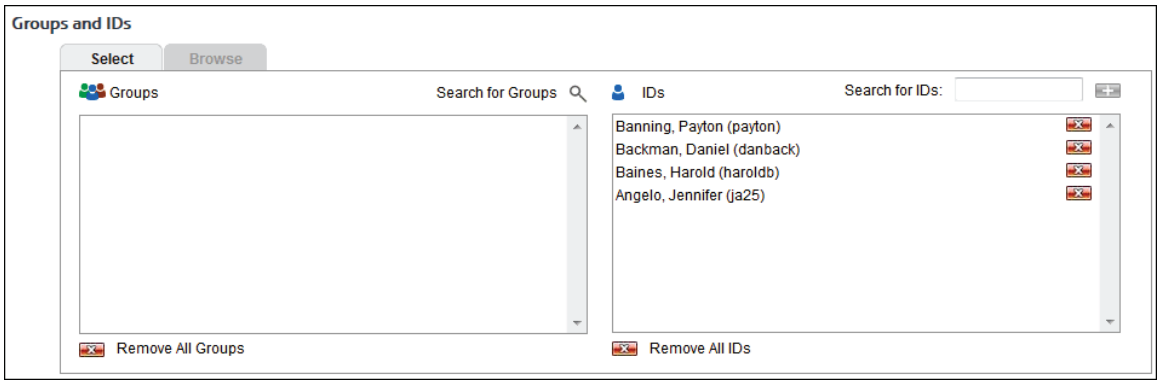
11. Under **Groups and IDs** on the Browse tab, choose groups and IDs by selecting their corresponding check box. To view IDs in a group, click the group name.



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.



12. 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.

13. 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.
14. Click **Run Now**.
    - Depending on how long the report takes to run, you may see a progress meter.
    - If one report was generated, it opens in a Report Results page where you can view, save, and print it.
    - If multiple reports were generated depending on how you ran the report, a Reports List page is displayed with links. Click the link for the report you want to view. When you are finished with the report, click **Back to List** to return to the list of reports, or click **Close** to close the window.
15. If you selected the **Schedule** option, the **Schedule and Run** and **Schedule** buttons are available.
    - Click **Schedule and Run** to schedule and deliver the report.
    - Click **Schedule** to only schedule the report.
16. Click **Back** to return to the previous page.

    Below is an example of a Cloud Services Summary report.

Report Highlights

Description	Information
Data Source	10.10.10.116
Total IDs With Visits	289
Total Visits	8,158
Total Hits	27,649
Total Bytes	372.82 MB
Total Denied Requests	74
Total Denied Hits	138

Top Classifications

Classification	Time Online %	Visits ▼	Visits %
1) Unacceptable	86%	7,432	91%
2) Acceptable	13%	683	8%
3) Neutral	<1%	43	<1%
Totals		8,158	

Top Categories

Category	Time Online %	Visits ▼	Visits %
1) Video Streaming	60%	4,328	53%
2) Audio Streaming	18%	2,381	29%
3) Personal E-Mail	7%	723	9%
4) Collaboration	13%	683	8%
5) Cloud Storage	<1%	43	<1%
Totals		8,158	

Run a Custom Template Report

Running a custom template report is similar to running an audit detail report with a few differences. These differences are explained in this section. See Run an Audit Detail Report for the majority of the instructions.

Settings

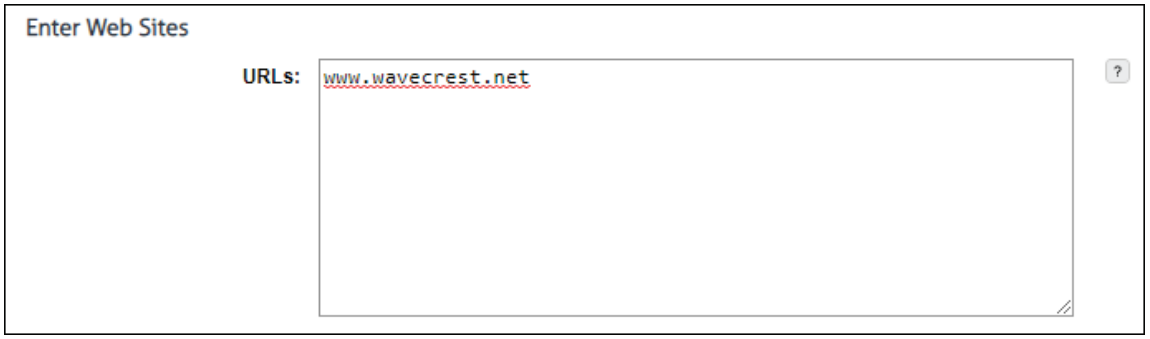
The report settings for a custom template are shown below.

- **Report Format** - The CSV format is included as an additional report output.
- **Report View** - The **Report View** options work as follows:
  - If **Report Delivery** is *Wait*, **Report Format** is *CSV*, and **Report View** is either *Read-Only* or *Interactive*, the Report Results page displays a link to save your CSV report. Close the report viewer and the Report Results page after the file is saved.
  - If **Report Delivery** is *E-Mail*, **Report Format** is *CSV*, and **Report View** is *Read-Only*, an e-mail is sent to the recipient with the .csv file attached.

    NOTE: To ensure that a large .csv file is not blocked by your server, go to **Settings - Reports - Options** and select **Compress Reports for E-Mail** to send the report as a .zip file.
  - If **Report Delivery** is *E-Mail*, **Report Format** is *CSV*, and **Report View** is *Interactive*, an e-mail is sent to the recipient with a link to the Report Results page. You can then save your report. A password is needed to display the Report Results page.
- If you have a network segment configured, The Network field is displayed to allow you to choose a specific network to include in the report. Select a network or all networks. If no networks are configured, a link to the Network Segment config screen is provided.

Enter Web Sites

The report can be restricted to only contain information for one or more Web sites (domains). Enter the desired domain(s) in the text box. This field is optional.

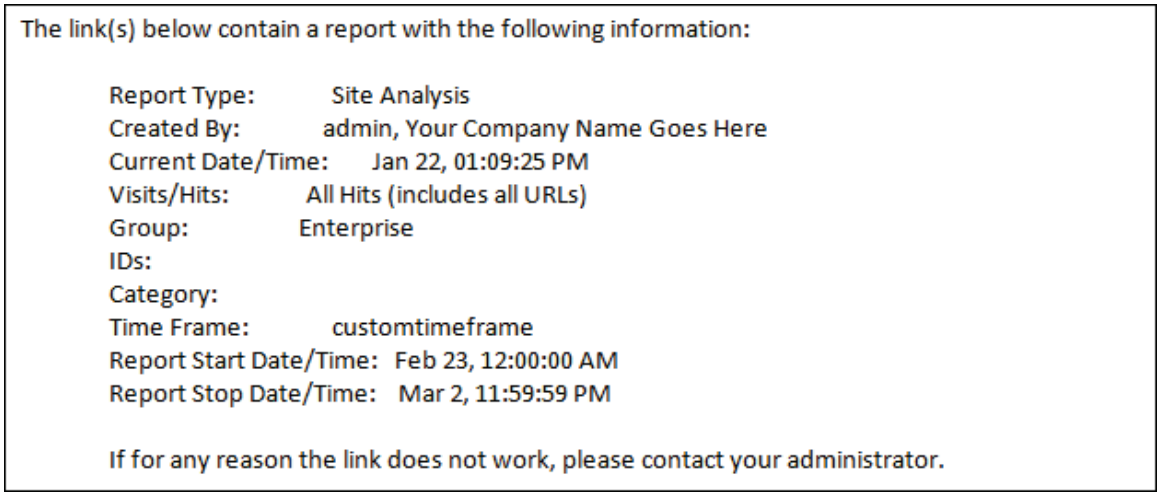


Using Interactive Reports

Interactive Reporting allows users to get more detailed information on employees' Web use by clicking a report's elements. For example, from a high-level report, such as Site Analysis, you can click a user, and a User Audit Detail report will automatically begin running on the user. You can also click a category or group.

They are also delivered differently. For example, instead of receiving an attachment of the report, recipients will receive a link. A password is needed to retrieve the reports because they are password protected.

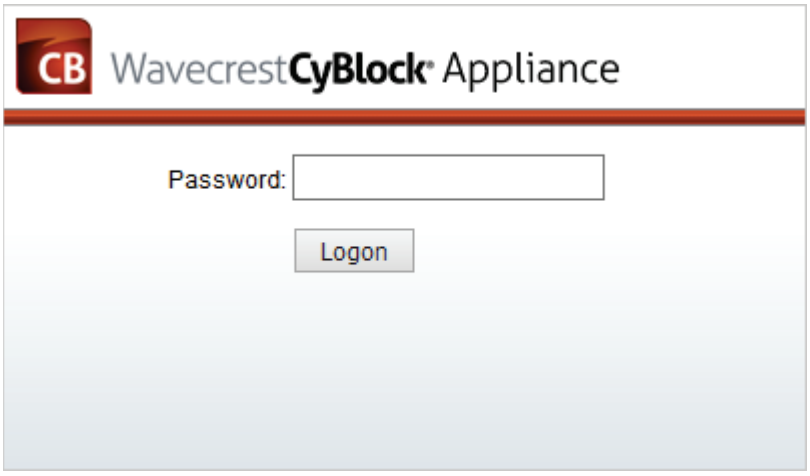
1. When an Interactive report is sent via e-mail to a recipient, the recipient will receive a link (or two links depending on server settings) to the report.


The link(s) below contain a report with the following information:

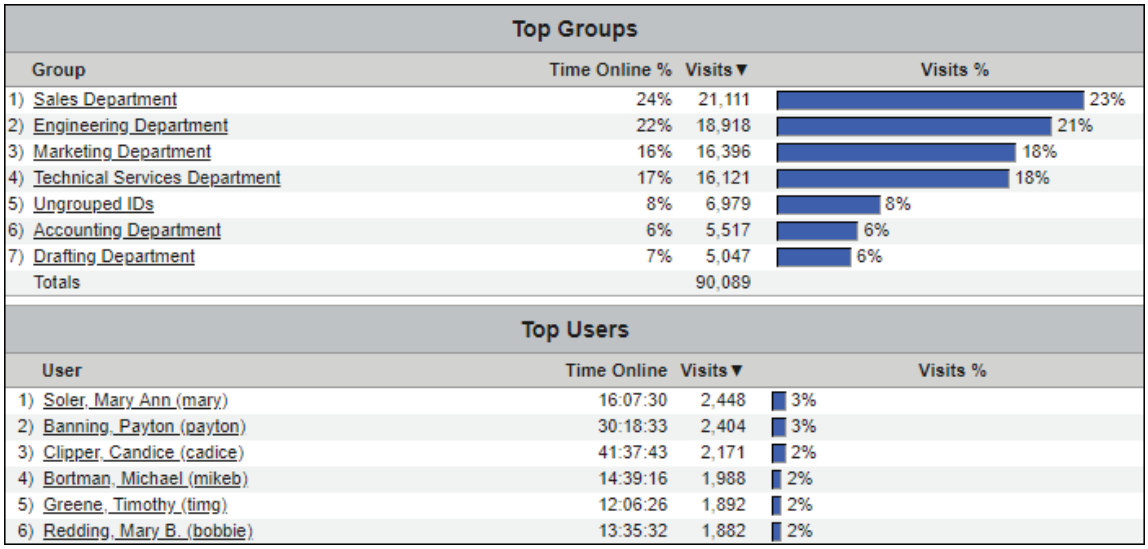
Report Type: Site Analysis
Created By: admin, Your Company Name Goes Here
Current Date/Time: Jan 22, 01:09:25 PM
Visits/Hits: All Hits (includes all URLs)
Group: Enterprise
IDs:
Category:
Time Frame: customtimeframe
Report Start Date/Time: Feb 23, 12:00:00 AM
Report Stop Date/Time: Mar 2, 11:59:59 PM

If for any reason the link does not work, please contact your administrator.

2. To open the report, click the appropriate link. You will then be asked to enter a password to retrieve the report. The default password is *password*. This password can be changed on the Settings - Reports - Interactive Reports screen.



3. In addition to viewing the report, you can save and print it. The report is saved with a universally unique identifier (UUID) in the file name, e.g., 14ec2d98-346f-4cb5-806a-f85f7b74f1e1.html.
4. If you received a Site Analysis report, it would appear like the report below.



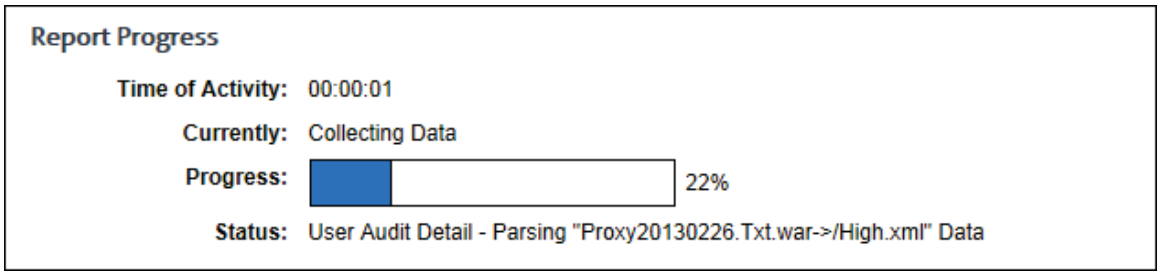
Top Groups

Group	Time Online %	Visits ▼	Visits %
1) Sales Department	24%	21,111	23%
2) Engineering Department	22%	18,918	21%
3) Marketing Department	16%	16,396	18%
4) Technical Services Department	17%	16,121	18%
5) Ungrouped IDs	8%	6,979	8%
6) Accounting Department	6%	5,517	6%
7) Drafting Department	7%	5,047	6%
Totals		90,089	

Top Users

User	Time Online	Visits ▼	Visits %
1) Soler, Mary Ann (mary)	16:07:30	2,448	3%
2) Banning, Payton (payton)	30:18:33	2,404	3%
3) Clipper, Candice (cadice)	41:37:43	2,171	2%
4) Bortman, Michael (mikeb)	14:39:16	1,988	2%
5) Greene, Timothy (timg)	12:06:26	1,892	2%
6) Redding, Mary B. (bobbie)	13:35:32	1,882	2%

5. From here, you may decide that you want to get more details on a user's Web activity. Click the user. By clicking the user, you have submitted a request to get a User Audit Detail report on that particular user. The below progress meter will appear.



6. All reports will be displayed as recently run reports on the Manage Reports page.

Using Report Filters in Audit Reports

In audit detail reports, report filters allow you to filter data by IP address, user, category, and URL. The filters are located in the Audit Detail section of the report. If only one IP address, user, or category exists in the report, the corresponding filter field will not be displayed. For example, a Category Audit Detail report provides data on one category at a time, and therefore, the category filter field will not be displayed.

NOTE: The number of URLs in the report may affect the speed at which data is retrieved. Please wait while the data is loading.

NOTE: This feature is available for only the English language report settings.

The following filters are available depending on the report:

- The IP address filter field shows the selection *All* and all IP addresses in the report. When you make a selection, the report shows only the data for that IP address.
- The user filter field shows the selection *All* and all users in the report. When you make a selection, the report shows only data for that user.
- The category filter field shows the selection *All* and all categories in the report. When you make a selection, the report shows only data for that category.
- In the URL text field, enter the URL text to filter on. You do not have to type the full URL. The report shows only data with URLs containing the entered text.

Below is an example of a Category Audit Detail report.

Audit Detail for "Pornography"

	IP Address	User	Date Time	URL
	All	All		
1)	10.10.40.1	Wills, Michael E. (mikew)	Jul 24, 2017 10:46:19 AM	D- http://www.diamond-dolls.com/
2)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:07:47 PM	D- http://www.free-pics.com/index.html
3)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:07:59 PM	D- http://www.freepics.com/
4)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:08:13 PM	http://www.jjay.com/
5)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:08:28 PM	D- http://www.comdigi.com/alex/
6)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:11:27 PM	D- http://www.p-net.net/
7)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:11:43 PM	http://www.oad.com/
8)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:12:47 PM	http://www.oad.com/oad.html
9)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:14:48 PM	http://www.oad.com/xxx.html
10)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:24:06 PM	D- http://amateurerotica.com/links.htm
11)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:25:25 PM	http://www.oad.com/xxx.html
12)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:26:37 PM	http://www.oad.com/past.html
13)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:26:53 PM	http://www.oad.com/xxx.html
14)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:32:13 PM	http://www.oad.com/xxx.html
15)	10.10.20.89	Barrol, Thomas V. (tom)	Jul 24, 2017 8:37:38 PM	http://www.oad.com/xxx.html

Below is an example of a Denied Requests Detail report.

Audit Detail for "Denied Requests"

	IP Address	User	Date Time	Category	URL
	All	All		All	
1)	10.10.20.185	Seimer, Mark O. (markse)	Jul 23, 2017 8:09:43 PM	IT Services	D- http://www.aa.net/~
2)	10.10.20.8	Collins, Juan (juan)	Jul 23, 2017 8:59:01 PM	High Tech	D- http://emwl.oyster.c
3)	10.10.20.8	Collins, Juan (juan)	Jul 23, 2017 9:12:06 PM	Nonprofit Organizations	D- http://www.rand.org
4)	10.10.20.8	Collins, Juan (juan)	Jul 23, 2017 9:13:02 PM	Nonprofit Organizations	D- http://www.rand.org
5)	10.10.40.1	Wills, Michael E. (mikew)	Jul 24, 2017 9:13:23 AM	Noncategorized/Other	D- http://www.wrestle.
6)	10.10.40.1	Wills, Michael E. (mikew)	Jul 24, 2017 10:46:19 AM	Pornography	D- http://www.diamon
7)	10.10.40.1	Wills, Michael E. (mikew)	Jul 24, 2017 10:50:40 AM	Noncategorized/Other	D- http://www.fantasy
8)	10.10.90.1	sd001	Jul 24, 2017 11:19:25 AM	Financial	D- http://www.fabian.c
9)	10.10.30.33	Rite, Bobbie W. (bobbie86)	Jul 24, 2017 11:36:49 AM	Noncategorized/Other	D- http://www.comsoc
10)	10.10.30.33	Rite, Bobbie W. (bobbie86)	Jul 24, 2017 11:39:07 AM	Noncategorized/Other	D- http://happy.comso
11)	10.10.30.33	Rite, Bobbie W. (bobbie86)	Jul 24, 2017 11:39:49 AM	Noncategorized/Other	D- http://happy.comso
12)	10.10.30.33	Rite, Bobbie W. (bobbie86)	Jul 24, 2017 11:39:55 AM	Noncategorized/Other	D- http://www.comsoc
13)	10.10.40.1	Wills, Michael E. (mikew)	Jul 24, 2017 11:53:41 AM	Noncategorized/Other	D- http://www.vangar.c
14)	10.10.40.1	Wills, Michael E. (mikew)	Jul 24, 2017 1:17:51 PM	Health/Medical	D- http://www.femalen
15)	10.10.30.51	Wall, Stephen (stevenw)	Jul 24, 2017 1:39:10 PM	Anonymous/Public Proxy	D- http://anonymizer.c

Below is an example of a User Audit Detail report.

Audit Detail for "timg"

	IP Address	User	Date Time	Category	URL
				All	
1)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:19 AM	Sports	http://espn.com/fido-1/bid-24/num
2)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:23 AM	Sports	http://espn.com/fido-1/bid-24/num
3)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:27 AM	Sports	http://espn.com/fido-1/bid-24/num
4)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:32 AM	Sports	http://espn.com/fido-1/bid-24/num
5)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:36 AM	Sports	http://espn.com/fido-1/bid-24/num
6)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:40 AM	Sports	http://espn.com/fido-1/bid-24/num
7)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:44 AM	Sports	http://espn.com/fido-1/bid-24/num
8)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:50 AM	Sports	http://espn.com/fido-1/bid-24/num
9)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:54 AM	Sports	http://espn.com/fido-1/bid-24/num
10)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:42:58 AM	Sports	http://espn.com/fido-1/bid-24/num
11)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:43:02 AM	Sports	http://espn.com/fido-1/bid-24/num
12)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:43:06 AM	Sports	http://espn.com/fido-1/bid-24/num
13)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:43:12 AM	Sports	http://espn.com/fido-1/bid-24/num
14)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 12:43:17 AM	Sports	http://espn.com/fido-1/bid-24/263
15)	10.10.30.192	Greene, Timothy (timg)	Jul 23, 2017 1:43:22 AM	Sports	http://espn.com/fido-1/bid-24/663

Visualizer

The dashboard features have been moved to the Visualizer. This is a newly-built reporting feature that provides leading edge dashboard building capabilities. For assistance with the Visualizer, help is available within it's user interface or by accessing help articles through https://kb.wavecrest.net/category/visualizer/:

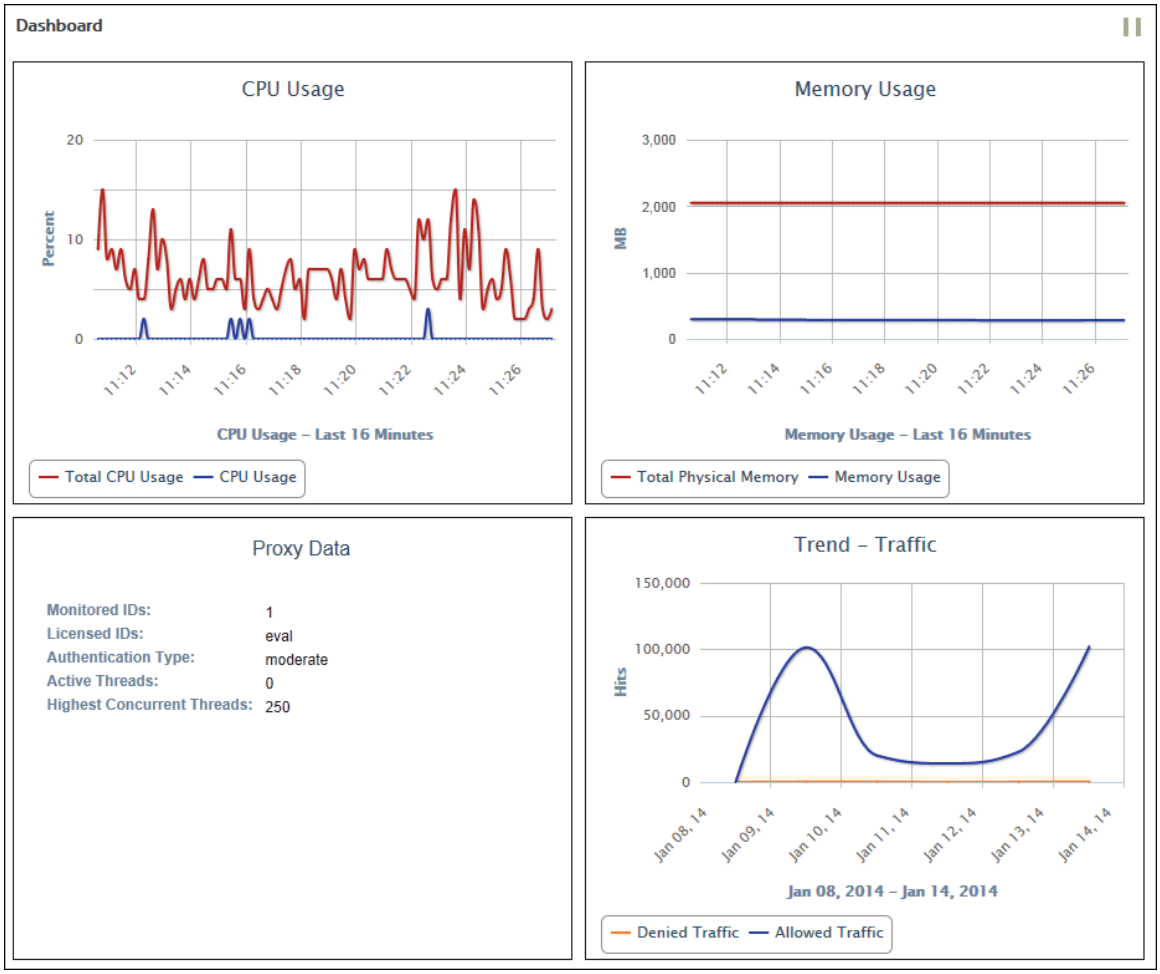
System Status

Dashboard

This screen contains administrator-level information about CPU usage, memory usage, proxy information, and current traffic trends.

- The CPU Usage chart shows the total CPU usage as well as current CPU usage.
- The Memory Usage chart shows the total physical memory as well as current memory usage.
- The Proxy Data area shows the monitored IDs, licensed IDs, authentication mode set for login names, active threads, and highest concurrent threads.
- The Trend - Traffic chart shows **Denied and Allowed traffic.** Denied traffic (or hits) refers to a failed attempt to access a Web site. For the most part, this occurs because the user is not authorized to access the site, i.e., his access has been blocked. However, a "denied" indication can also be caused by technical anomalies, e.g., "page not found by server." **Allowed traffic** (or hits) refers to all successful attempts to access a Web site. This is shown for local logging only.

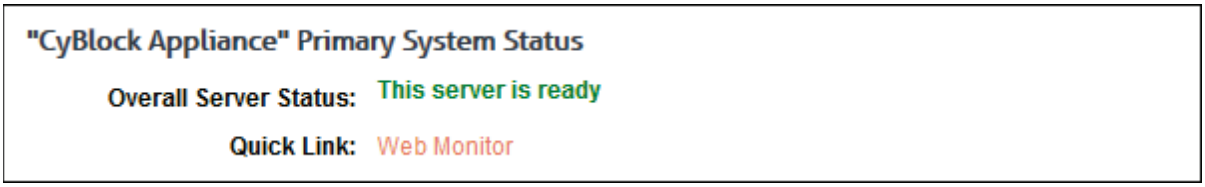
1. To access this screen, go to **System Status - Dashboard**.
2. If you want to zoom in, click and drag from left to right or from right to left on the chart. Click **Reset zoom** to return to the original view.



Server Status

The Server Status page tells you whether or not the product's application server is ready. If the Overall Server Status message is colored yellow or red, the Quick Link will take you to the specific screen that relates to the error condition. There you can quickly resolve the issue.

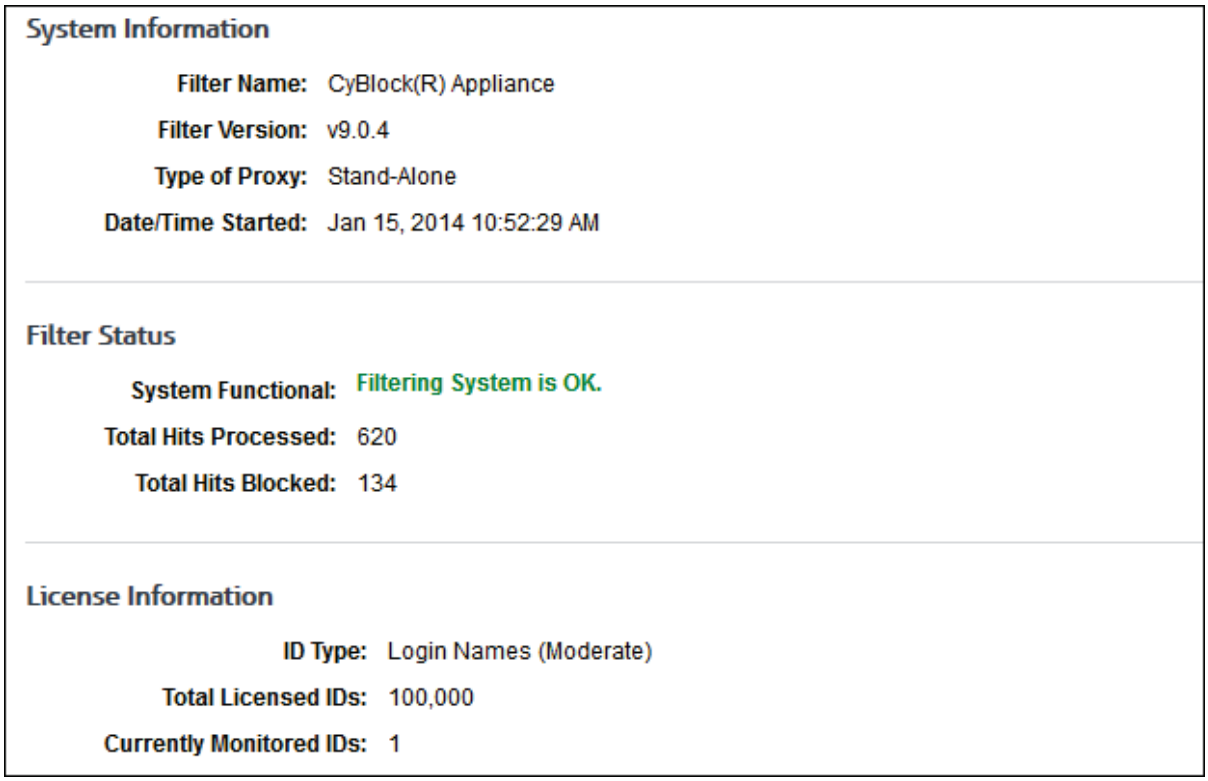
To check your server status, go to **System Status - Server**.



Filter Status

The Filter Status page provides information relating to the product's filter feature. Included are Filter Name, Filter Version, Type of Proxy, Operating System, System Functional (Yes or No), Total Hits Processed, Total Hits Blocked, and License Information.

To view your filter status, go to **System Status - Filter**.



Server Information

The Server Information page provides important items of information about the product's application server. Included are the type and version of application server, type of proxy server or firewall, installation directory path, virtual memory size, license information, and report language. Several of these informational items are derived from one-time setup actions. Others were developed during the installation process.

To view your server information, go to **System Status - Server Information**.

Proxy Information

This page is not intended for everyday use. It is a troubleshooting aid to be used only when you are in contact with Wavecrest Technical Support personnel. Technical Support will ask you to open it if the need arises. The screen provides the following information about proxy thread usage:

- Overall thread usage
- Internal connections to the proxy
- Active proxy connections to Web servers
- Keep-Alive connections to Web servers

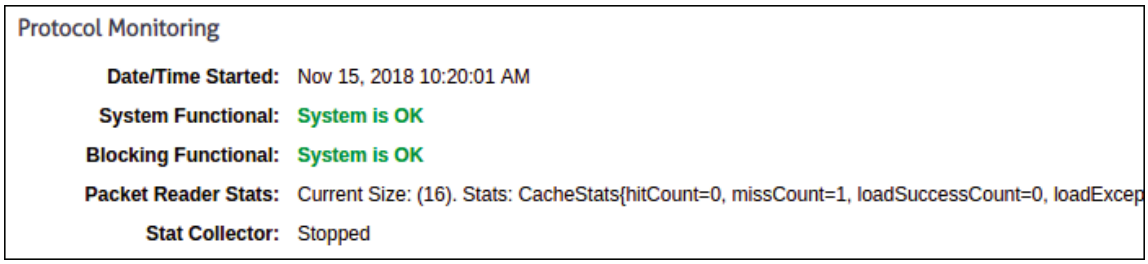
Technical Support can analyze and use this information to identify problems.

To access this screen, go to **System Status - Proxy Information**.

Protocol Status

The Protocol Status page shows the status of protocol monitoring on the appliance.

To view this status, go to **System Status - Protocol**.



Job Queue

The Job Queue page displays a prioritized list of jobs in process. If there are no open jobs, when you go to the job queue, the page will be blank, and a message indicating the system is currently idle will appear.

The job queue automatically assigns priorities and performs the jobs in a sequence that reflects those priorities. This design ensures that reports are based on the latest available data.

The job queue runs one job at a time. A job that is running will always be at the top of the list, and a progress meter will show percent completion.

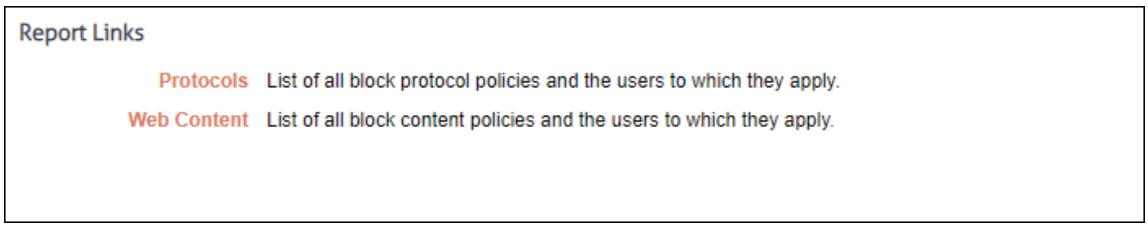
When a new job is initiated, the product automatically places it in the queue in accordance with its priority. Lower priority jobs are "bumped down" if appropriate.

1. To check the job queue, go to **System Status - Job Queue**. You will see the list of jobs and their status on the page.
2. If you want to delete any of the jobs, click the red x icon. To delete all jobs in the queue, click the **Delete All** button.
3. To pause the queue from refreshing, click **Pause**.

   NOTE: This does not pause the job from running.
4. Click **Restart** to get the queue refreshing itself again and to see the current status of job(s) running.

Policy Reports

If you want to review your policy settings, you can do so on the **System Status - Policy** screen.



This screen contains links to policy-related information that you have set in the product.

- The **Protocols** link indicates which protocols are allowed and which are blocked.
- The **Web Content** link indicates what content types and/or file extensions are to be blocked.

Login Cache

This page displays user names that are cached when login name caching is enabled. Login name caching is enabled when the Cache Mode field is set to *Primary* or *Supplemental* on the Authentication Manager - Cache tab. The IP address and computer name for the user are also displayed.

To view cached user names, go to **System Status - Login Cache**.

IPC Log

The Intra-Product Communication Log page displays the communication messages sent between your CyBlock products, for example, your local CyBlock Software or Appliance installation and CyBlock Cloud, or CyBlock Directory Agent and CyBlock Cloud. It is used by Technical Support for troubleshooting purposes.

1. To view messages, go to **System Status - Messages - IPC**.
2. If you have more than one cloud account, in the **Hybrid Configuration** field, select the configuration for the messages that you want to view.
3. To expand long messages, click the **More** link next to the message. To collapse long messages, click the **Less** link.

Update Log

The Update Log page displays the dates and times of the URL List and product updates.

To view this information, go to **System Status - Messages - Update**.

Event Log

The Event Log page shows the product event errors and messages on various processes such as scheduling reports, importing data, and updating the URL List. It shows legacy and new messages and is used by Technical Support for troubleshooting purposes.

To view this information, go to **System Status - Messages - Event**.

Profiling Log

The Profiling Log page shows debugging information from the profile file related to the product. It shows legacy and new messages and is used by Technical Support for troubleshooting purposes.

To view this information, go to **System Status - Messages - Profiling**.

Redirect Log

The Redirect Log page shows the source and destination IP addresses of redirected HTTPS traffic. It is used by Technical Support for troubleshooting purposes.

To view this information, go to **System Status - Messages - Redirect**.

DNS Log

The DNS Log page displays the DNS proxy requests for direct HTTP and HTTPS traffic. It shows the host name to IP address resolutions. It is used by Technical Support for troubleshooting purposes.

To view this information, go to **System Status - Messages - DNS**.

Web Categories Policy Report

This screen displays the configured Web Categories filter policies. These policies are used to control Web access to the internet. The policies are listed by their name with the content of the policy in a collapsed field underneath. For each individual policy, this screen displays the blocked Categories (grouped by the configured timeframe for each category), the white listed URLs, the black listed URLs, Allowed YouTube videos, and the assigned Groups and IDs. To simplify sharing the content of this screen, a print stylesheet has been applied that removes the menu and the display options section.

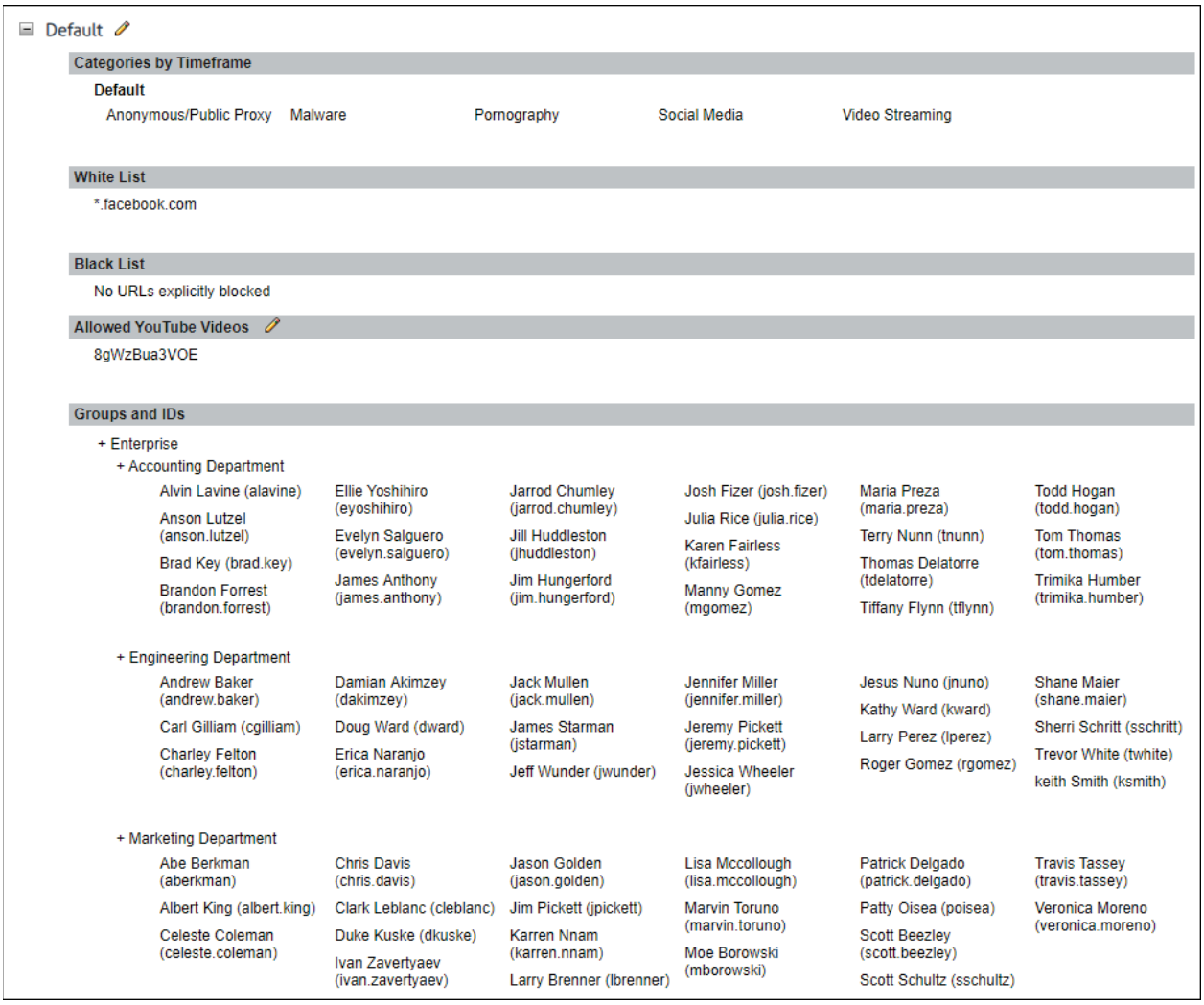
1. Go to System Status - Policy Reports **- Web Categories**, and the policies will appear on the opened page.

2. Under **Display Selection**, select a filter option to display the Categories and Groups and IDs, only the Categories or only the Groups and IDs information. The Categories portion includes the blocked categories, white listed URLs, black listed URLs and Allowed YouTube Videos.

3. In the Unassigned Policies select whether or not you wish to view or hide policies that do not have any Groups and IDs assigned to them. This is helpful to reduce the content on the screen to only active policies.

Below are definitions of the information shown for each policy. Use the Expand all button to quickly open all policies for viewing.

Each policy's name is listed at the top with a expand icon and an edit pencil. The expand icon will display the policies information below. The edit icon will take you to the Web Management - Filter - Web Categories screen with the selected policy preloaded for modification. This screen has a link back to the Web Categories Policy Report screen to quickly toggle between each screen.



Categories by Timeframe - This section displays the name of the Timeframe in bold and the category names that are assigned to that blocked timeframe configuration below.

White List - This section displays any URLs that are always allowed

Black List - This section display any URLs that are always blocked

Allowed YouTube Videos - This section displays any videos that have explicitly been allowed using the Web Management - Application Controls screen. The edit icon next to this section will take you to the referenced policy in the Application Control screen. A link back to the Policy Report screen has been added to the Application Control screen.

Groups and IDs - This section shows any group and/or ids that are assigned to this policy. For reference, the group path is displayed for each assigned group and/or id. Groups that are listed only for reference are italicized.

Settings

Introduction

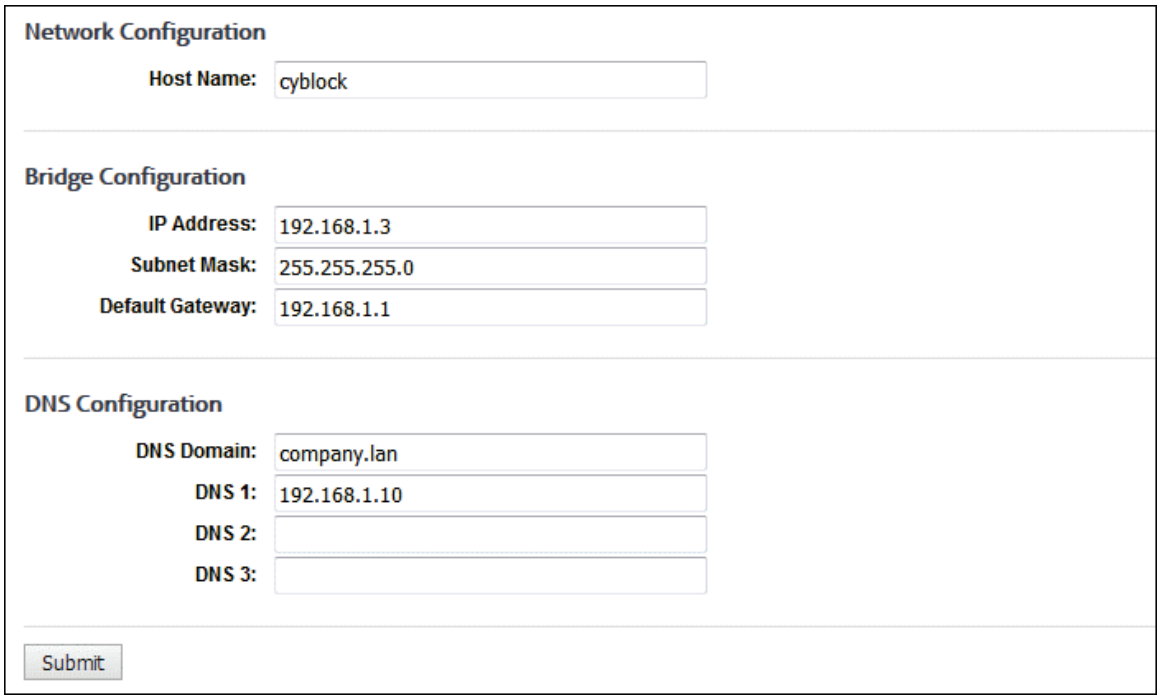
This section provides instructions on performing certain administrative tasks and setting up various features in the product, such as:

- Network settings
- License information
- Internet connection to Wavecrest download servers
- Product e-mail address
- Restore points
- Restart and shutdown
- Proxy chaining
- PAC file configuration
- SSL certificates
- SSL inspection
- Direct traffic
- Hybrid configuration
- Report options

Network Settings

This page allows you to configure CyBlock Appliance for your network.

1. Go to **Settings - Network - Configuration**.



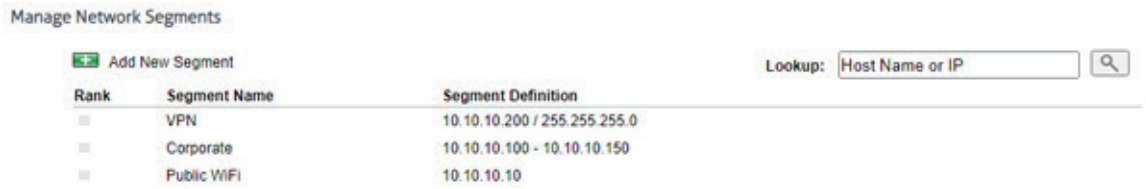
2. Under **Network Configuration** in the **Host Name** field, type a "friendly" name for the appliance.
3. Under **Bridge Configuration**, enter the IP address for CyBlock Appliance, subnet mask, and default gateway IP address of your network.

4. Under **DNS Configuration**, enter the domain name including DNS suffix, IP address of your primary DNS server, IP address of your secondary DNS server if you have one, and so on.
5. Click **Submit**.

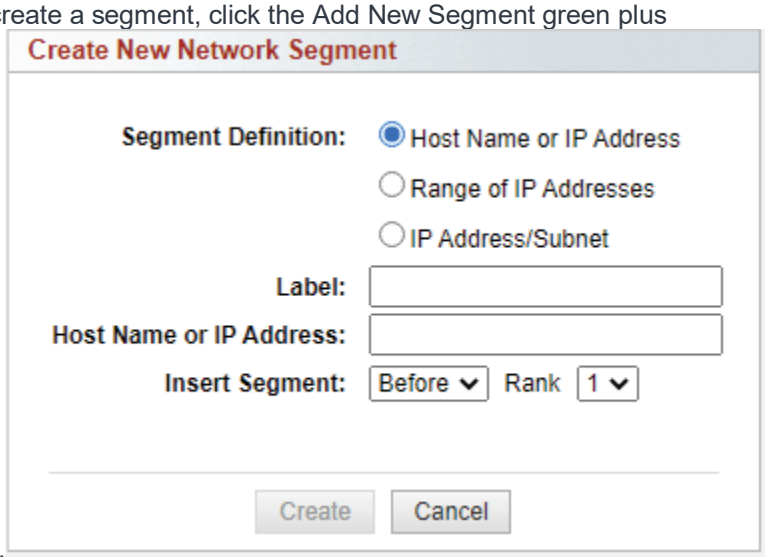
Network Segments

The Network Segments screen allows you to create labels for various network definitions, such as an individual IP address, a range of IP addresses, and a host name. This label can be used in reporting by restricting data to a specific network definition or comparing the different definitions against each other in the dashboard charts. Entries that match multiple definition is given the label of the highest rank definition.

1. Go to Settings - Network - **Segments**. The segment screen is displayed.

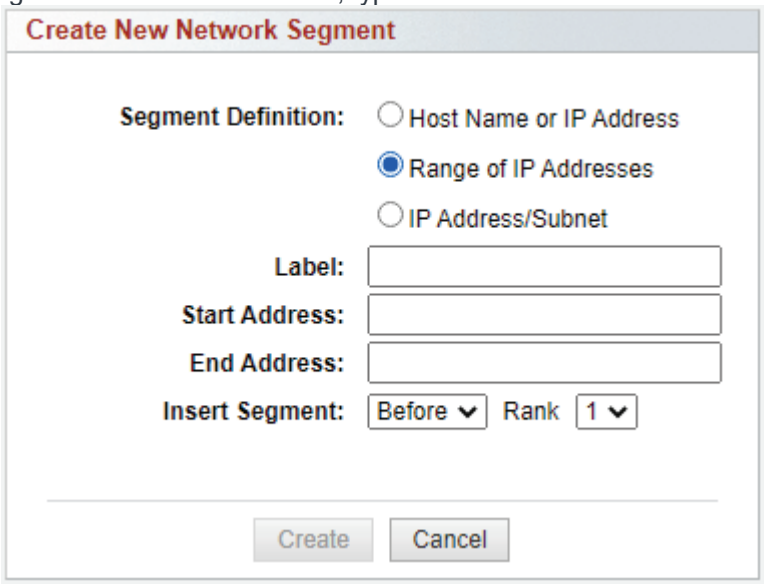


2. To create a segment, click the Add New Segment green plus icon.

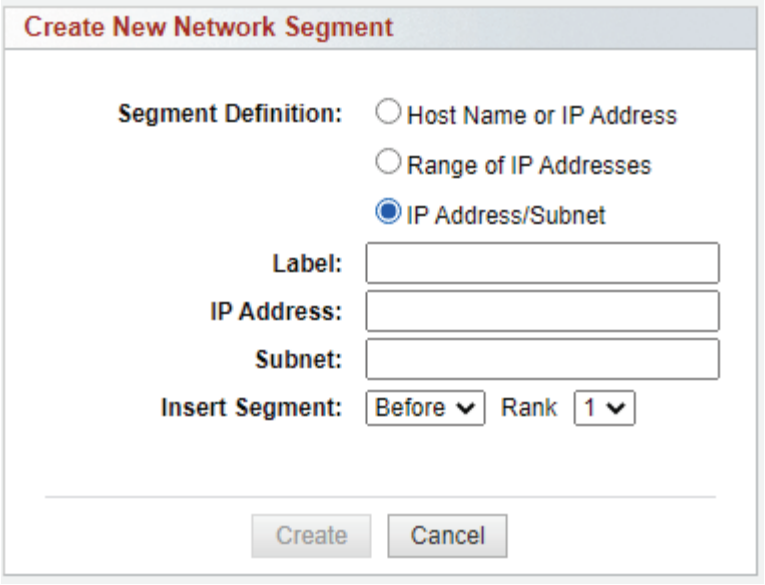


3. For the Segment Definition field, select Host Name or IP Address, Range of IP Address, or IP Address/Subnet.
4. In the Label field, type in the name of the segment.
5. Complete the fields as follows:
    - If you selected Host Name or IP Address, type the host name or IP address in the Host Name or 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.



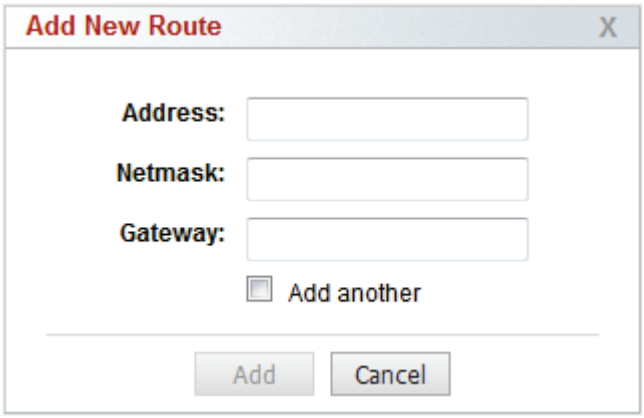
6. The Insert Segment fields allow you to specify where the new segment should appear in the list. Select Before or After and the rank number of an existing segment.
7. Click Add. Continue adding more segments as necessary. If a new segment overlaps an existing segment, a message will be displayed.
8. To sort the segments, click the drag icon and drag the segment to where you want it.
9. To edit a segment, hover over the corresponding line and click the pencil icon.
10. To delete a segment, hover over the corresponding line and click the red x icon.
11. If you have a long list of segments, you may search for a host name or IP address by entering it in the Lookup field and pressing ENTER. Click Back to Segments list to return to the list of segments.

Static Routes

This page allows you to configure static routes for CyBlock Appliance in order to route traffic from your different networks appropriately.

1. Go to **Settings - Network - Static Routes**.

2. Click the green plus icon to add a static route.



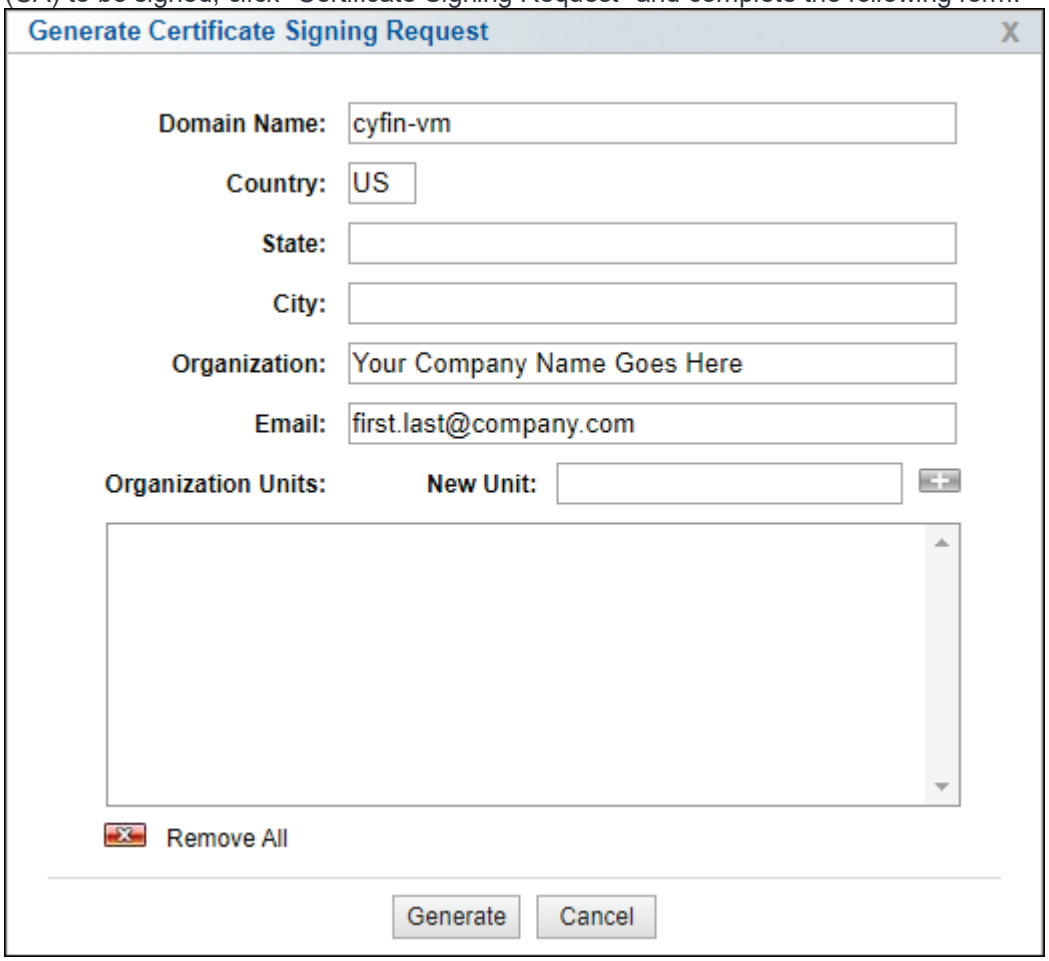
3. In the dialog box, enter the IP address for the network, netmask, and default gateway IP address of your network.
4. Select the **Add another** check box if you want to add another static route at this time.
5. Click **Add**. Continue adding more static routes as necessary.
6. To edit a route, hover over the corresponding line and click the pencil icon. Click **Update** after making the change.
7. To delete a route, hover over the corresponding line and click the red x icon. To delete all routes, click the **Delete all routes** red x icon.
8. Click **Submit**. Changes will be applied, and a message box indicating the configuration update is complete will be displayed.
9. Click **Close**.

Secure Browser Interface

This page allows you install a SSL certificate and to create a secure connection (HTTPS) to your browser interface.

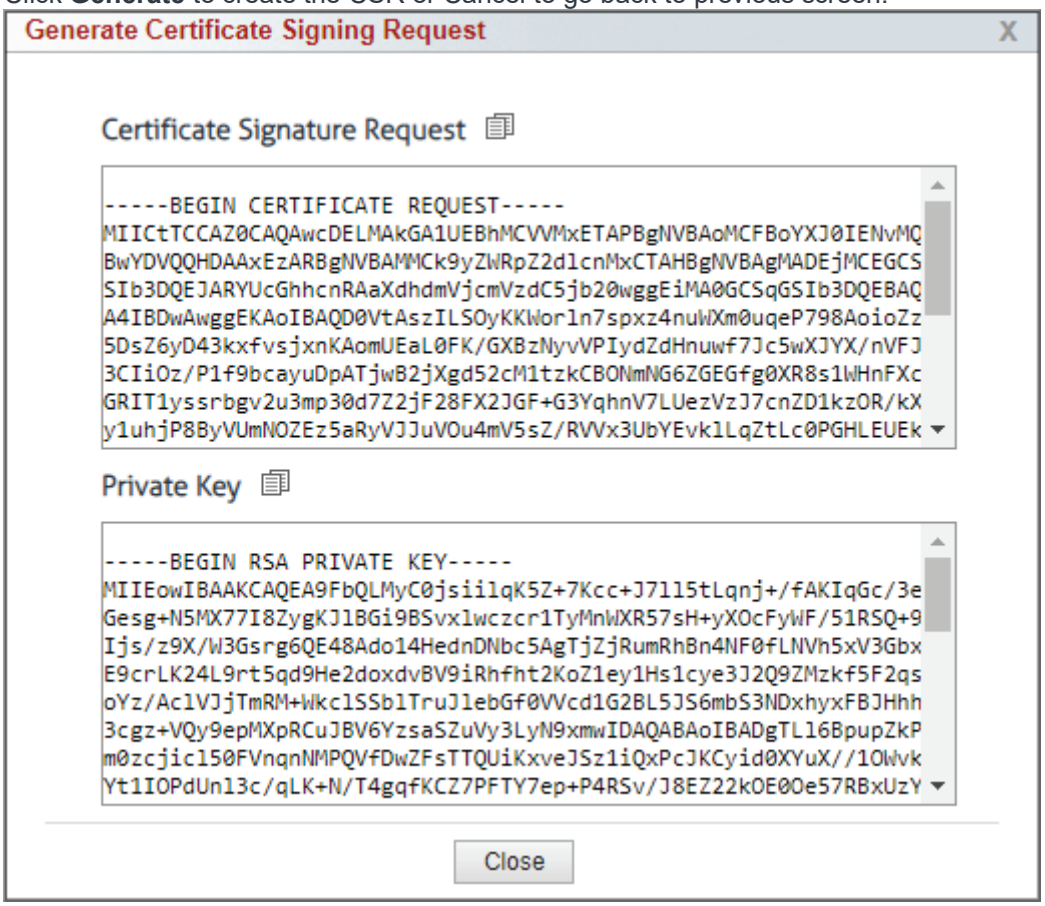
1. Go to **Settings - Secure Interface**.
2. The product includes by default a private Wavecrest certificate that you can use internally or you have the option to add your own custom certificate.
3. To download the Root Certificate Authority click "Wavecrest Certificate". Refer to the Wavecrest Certificate Installation Guide for instructions on how to install/distribute the certificate.

4. If you wish to create a Certificate Signing Reuqest (CSR) to send to your Certificate Authority (CA) to be signed, click "Certificate Signing Request" and complete the following form.



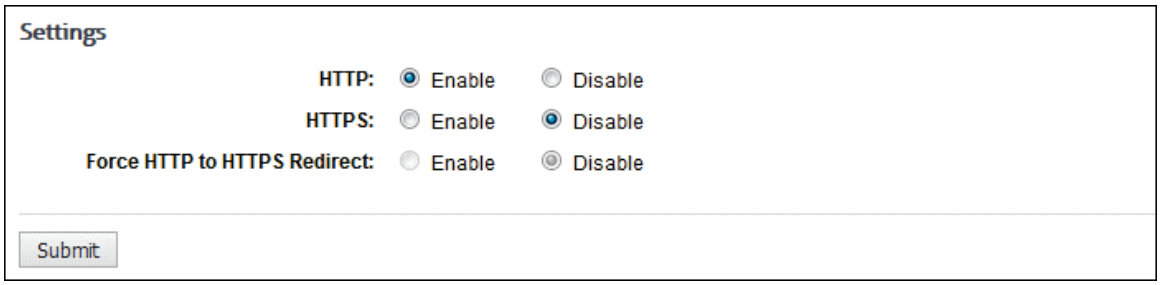
1. Enter the full domain of the server in the **Domain Name** field. This field is required.
2. In the **Country** field, enter the 2 digit country code where this server resides.
3. If applicable, in the **State** field, enter the state in which the server resides.
4. If applicable, in the **City** field, enter the city in which the server resides.
5. In the **Organization** field, enter your organization name. The default value is pulled from the information on the License screen.
6. In the **Email** field, enter the email of the person in charge of the server. The default value is the email associated with the current login.
7. In the **Organization Units**, add any departments or groups that this server belongs to (eg. IT Group) by typing the name of the Unit in the text field next to **New Unit** and hitting the + icon. Multiple units can be added in order to create a nesting effect (eg. Security Audit unit under IT unit). Use the Remove All button to delete all entries in the Organization Units box.

8. Click **Generate** to create the CSR or Cancel to go back to previous screen.



9. The CSR and private key are provided in PEM format. Foward the CSR to your CA for signing. Save the private key in a secure location and hit the **close** button. Once the CA returns the signed certificate, click on **Settings - Secure Interface** and click on the edit icon next to **Current Certificate**. Select Custom under **Certificate Type** and paste the signed certificate in the **Certificate Data(PEM)** section and append the private key at the bottom of the certificate. Click on Install to configure the certificate in the product.

5. To create a custom certificate using the PEM format click the edit pencil icon and choose **Custom**.
6. Changes to the installed certificate will result in a service restart.
7. To configure the browser interface connection type, go to **Settings**.



8. For **HTTP**, the **Enable** option is selected by default. Select **Disable** to not use an HTTP connection.
7.

8. For **HTTPS**, select **Enable** to use a secure browser connection.

9. You can enable both HTTP and HTTPS connections to test that the certificate file is correct.

10. If both HTTP and HTTPS are enabled, the **Force HTTP to HTTPS Redirect** field becomes available. Select **Enable** to redirect HTTP communication to HTTPS.

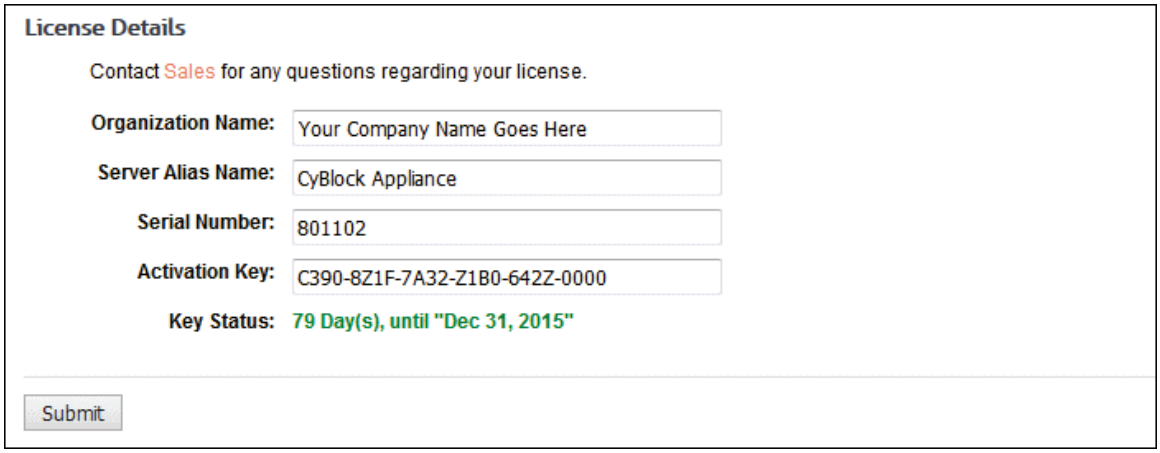
11. Click **Submit**. A dialog box appears indicating that changing secure browser settings will result in an automatic service restart.

12. Click **Continue** to restart the service.

Update License Information

This page allows you to enter your product license after you purchase the product, or renew your product license. If at any time you want to contact Sales, click the **Sales** link to send an e-mail.

1. Go to **Settings - License**. The Update License Information page is displayed.



2. In the **Organization Name** field, type the organization name that you would like to use.

3. In the **Server Alias Name** field, type the server name (or IP Address) that the product will use.

   NOTE: This is merely the server's "friendly" alias name. It has no bearing on product actions.

4. In the **Serial Number** field, type your serial number if you have purchased the product. (This can be found on the certificate provided at time of purchase. During product evaluation, the serial number default setting should not be changed.)

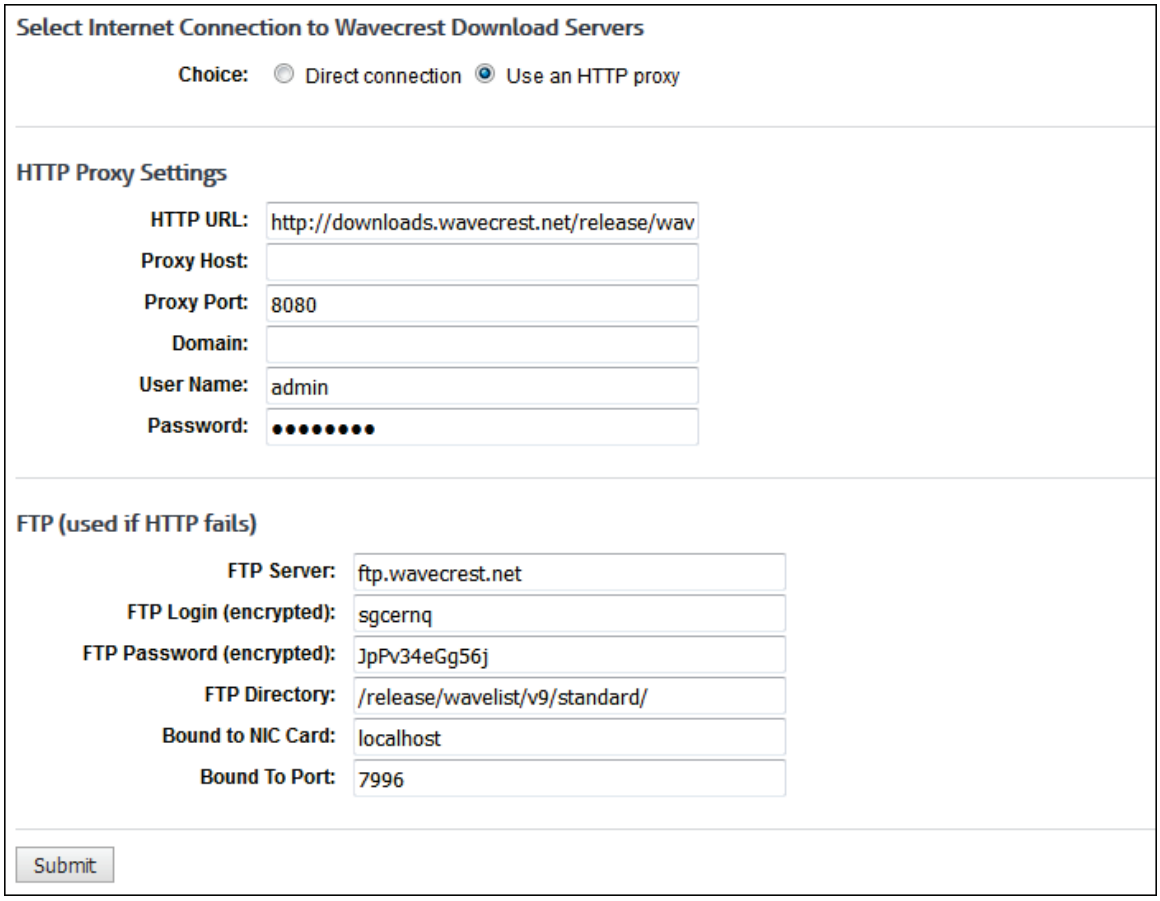
5. In the **Activation Key** field, type your activation key. (This can be found on the certificate provided at time of purchase. During product evaluation, the activation key default setting should not be changed.)

6. Click **Submit** to apply your changes.

Internet Connection

If your Internet traffic goes through a proxy, this page allows you to configure your proxy information. This will ensure that you can download the list and product updates. When trying to download the list, the product always tries the HTTP connection first, and if that fails, then it tries the FTP connection.

1. Go to **Settings - Internet Connection**.

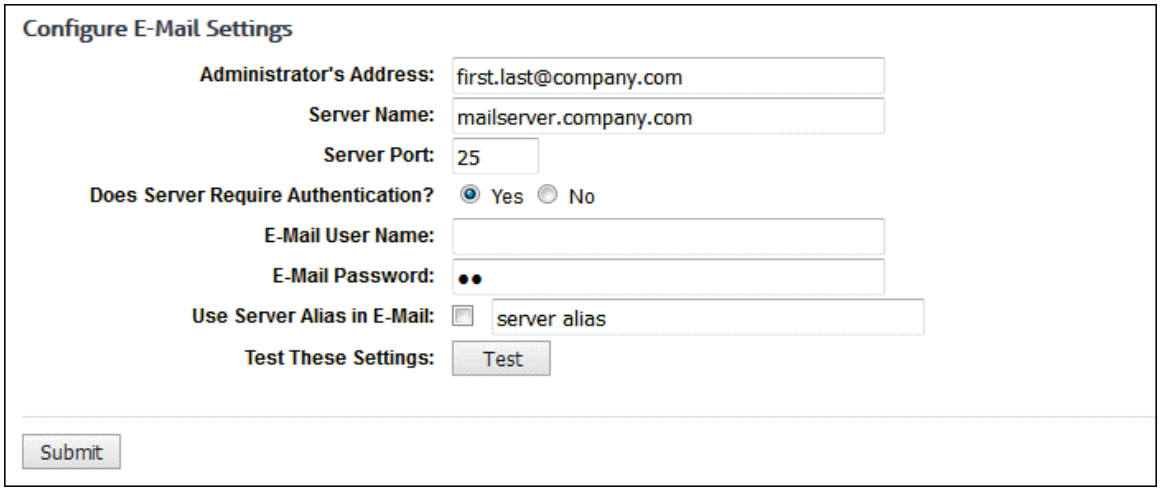


2. Fill in the fields with the correct authentication credentials, and then click **Submit**.

Set up Administrator E-Mail

This page allows the Administrator to receive all product e-mail messages (e.g., error messages, fault indicators, and URL List download notifications).

1. Go to **Settings - E-Mail**.



2. Fill out the screen with the Administrator's e-mail information. If the e-mail server requires authentication, enter the user name and password for the e-mail server logon account.

3. Click the **Test** button to make sure the product is communicating with the e-mail server.
4. If it is successful, then click **Submit** to save the configuration.

Restore or Download a Restore Point

Restore a Restore Point

The restore feature allows you to go back to (or restore) the previous configuration settings in your product from a previous day. You can restore settings up to 31 days back. The backup is done nightly and only keeps the last 30 days.

The restore/download feature allows you to transfer all configuration settings to another installation of the product. Transfers of configuration settings are only supported for the same product type, for example, CyBlock Software to CyBlock Software. Transfers across products are not allowed.

NOTE: When you restore settings, the product service automatically restarts.

1. Go to **Settings - Restore Points - Manage**.

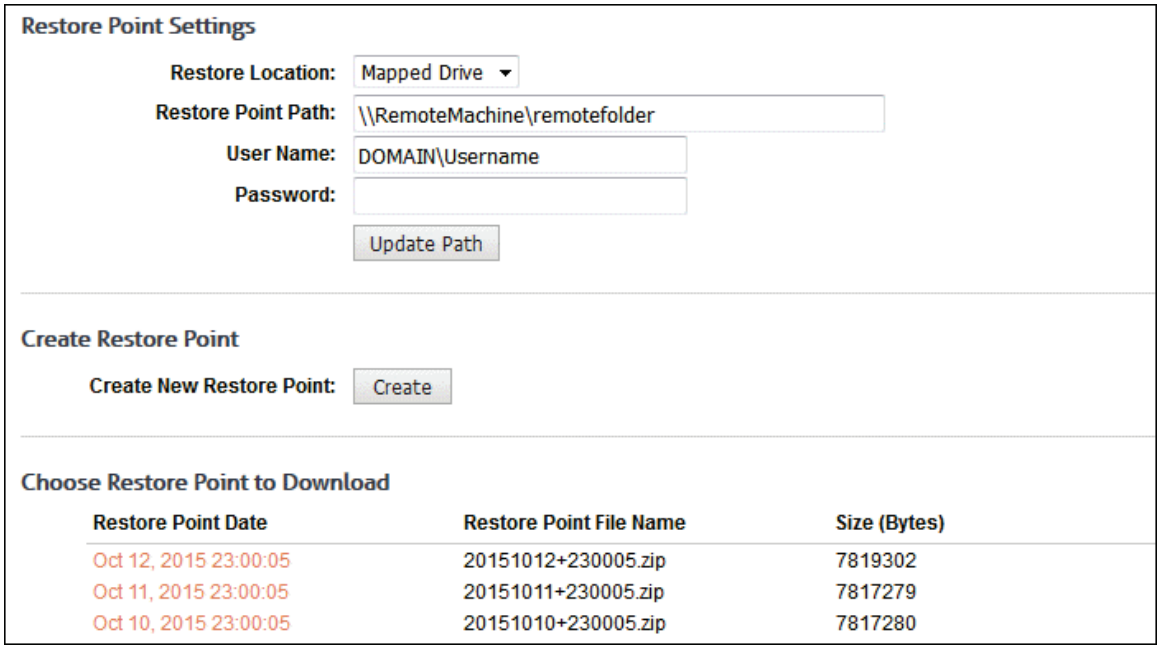
2. In the **Choose Day To Restore** drop-down box, select a day from which to restore settings.
3. Select the type of restore you would like to perform, that is, **Full** or **Configuration Only**.
   - **Full** - This option allows you to transfer configuration settings from one product type to the same product type with the same restore point path on the same computer.
   - **Configuration Only** - This option allows you to transfer configuration settings to a different restore point path on the same computer or to a different computer.
4. Click **Submit**. At this point, the service will automatically restart.

Download a Restore Point

The download feature allows you to download a restore point to a location of your choosing as a backup. You can download a restore point from the last 31 days. The restore/download feature allows you to transfer all configuration settings to another installation of the product. Transfers of configuration settings are only supported for the same product type, for example, CyBlock Software to CyBlock Software. Transfers across products are not allowed.

NOTE: When you restore settings, the product service automatically restarts.

1. Go to **Settings - Restore Points - Download**.



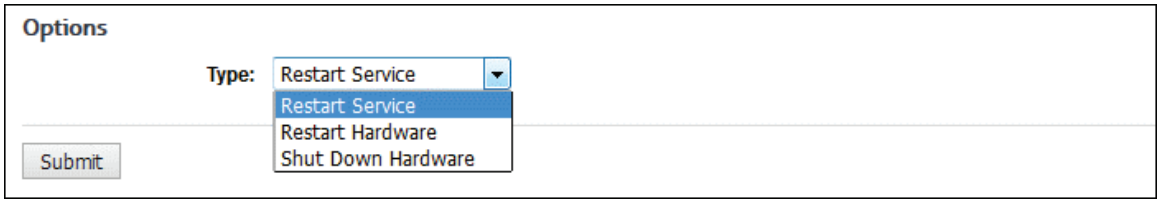
2. Under **Restore Point Settings**, in the **Restore Location** field, select *Appliance* or *Mapped Drive* for the location of the backup files.
   - If you select *Appliance*, the backup files are created in a folder on the appliance.
   - If you select *Mapped Drive*, the backup files are created in a directory that you specify. In the **Restore Point Path** field, type the UNC path of the restore point including the fully qualified domain name. The IP address can also be entered and is recommended. If required, enter your user name and password for the credentials for the mapped drive.
   - Links to the backup files are displayed under **Choose Restore Point to Download**.
3. Click **Update Path** to reload the new restore point path.
4. If you wish to create a new restore point, click **Create** under **Create Restore Point**. A link for the new restore point is displayed under **Choose Restore Point to Download**.
5. To download a restore point, click the link for the restore point in the **Restore Point Date** column.

   NOTE: The file name is in the format yyyymmdd+hhmmss.zip. Older restore points with file name ##.zip will still be displayed; however, they are not transferable and should not be used.
6. Save the file to a location of your choosing.

Restart or Shutdown

Depending on whether your product deployment is a VM or non-VM, this page allows you to restart the service for the product as well as restart or shut down the appliance or VM if necessary.

1. Go to **Settings - Restart or Shutdown**. For CyBlock Appliance, Cyfin VM, and CyBlock VM, the first screen applies. For a non-VM Cyfin or CyBlock Software deployment, the second screen applies.

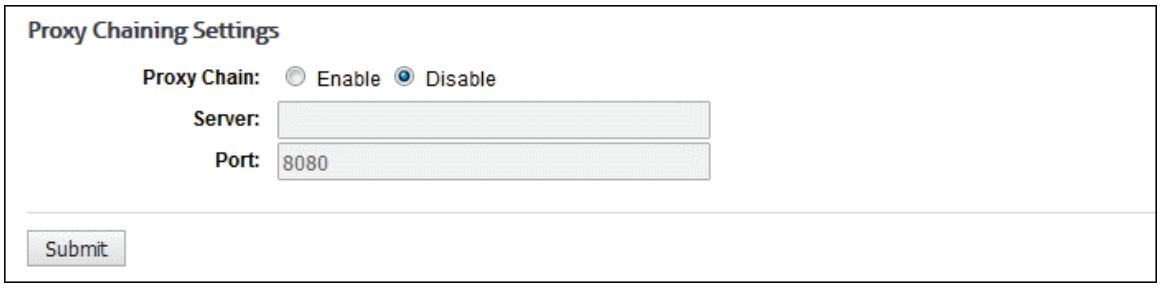


2. In the **Type** field, select one of the following options:
   - *Restart Service* - This option restarts the CyBlock process on the appliance as well as restarts the VM product service.
   - *Restart Hardware* - This option restarts the operating system on the appliance for networking as well as restarts the VM.
   - *Shut Down Hardware* - This option powers off the appliance as well as shuts down the VM.
3. Click **Submit**. You will be prompted twice to confirm the restart or shutdown.
4. For a non-VM deployment, click **Restart** to restart the service for the product. You will be prompted twice to confirm the restart.

Proxy Chaining

Proxy chaining allows organizations to chain CyBlock Appliance to another proxy upstream of it. For example, if a company is required to go through a "corporate" proxy, it can still filter and monitor Web use locally with CyBlock Appliance. The workstations to be monitored go through CyBlock Appliance first to determine if the request is allowed based on the set filtering policy. If the site is allowed, CyBlock Appliance then passes the request to the proxy upstream of it. However, if the site is configured to be blocked, then CyBlock Appliance returns the blocked message.

1. Go to **Settings - Proxy - Chaining**.



2. For **Proxy Chain**, select **Enable** to turn on proxy chaining.
3. In the **Server** field, enter the upstream proxy's name or IP address.
4. In the **Port** field, the default port is 8080. You should not need to change the port number unless the port is not available.
5. Click **Submit**.

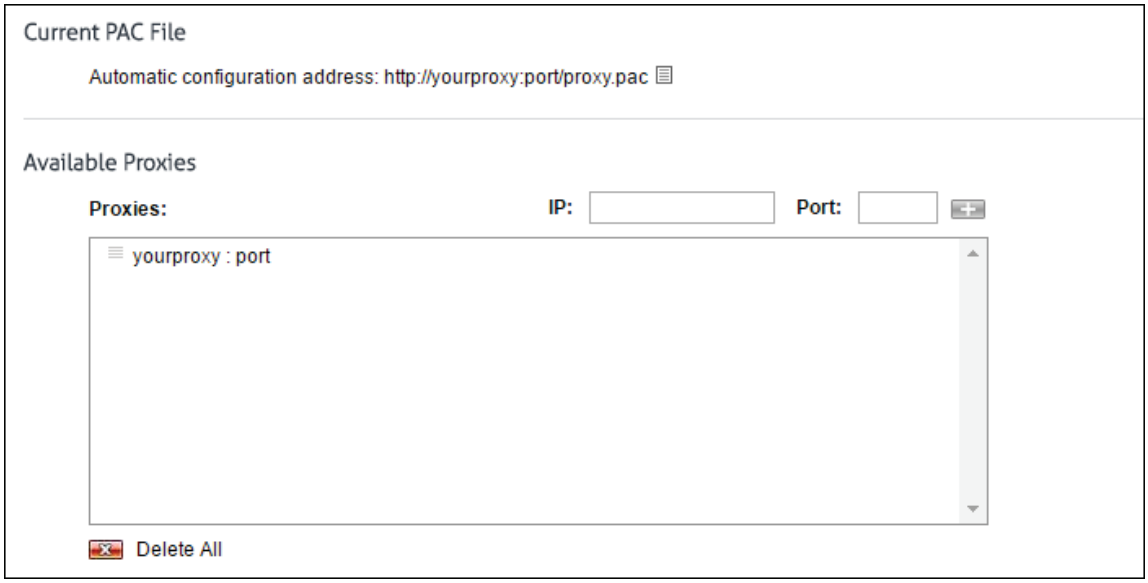
NOTE: If for any reason you need to turn off proxy chaining, return to this page, select the **Disable** option, and click **Submit**.

PAC File Configuration

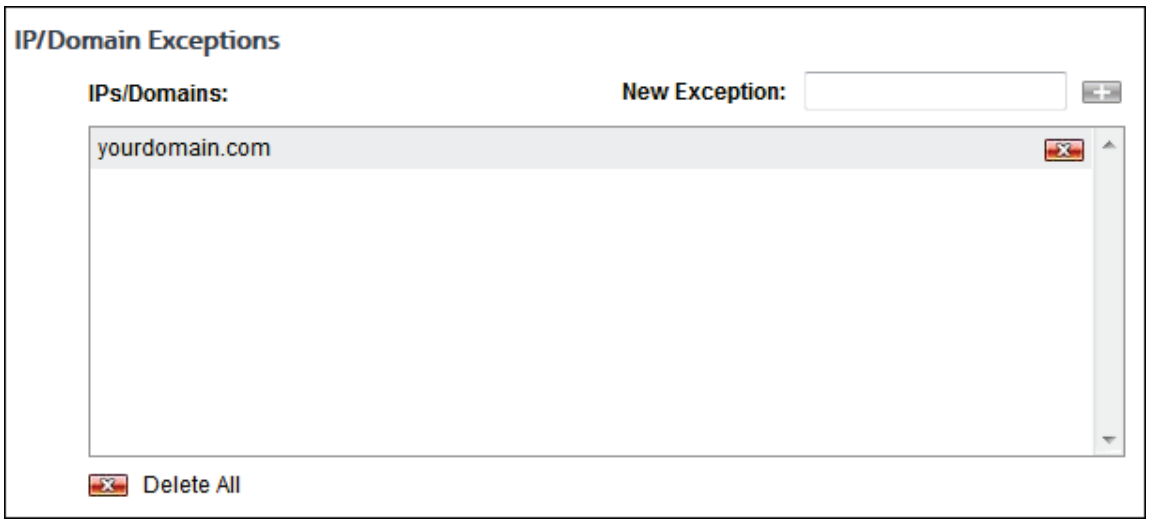
The PAC file can be used for two reasons:

- To redirect traffic to a different proxy or proxies should the first one fail.
- To specify domains to completely bypass the proxy, i.e., go direct.

1. Go to **Settings - Proxy - PAC File**. The PAC File Configuration page is displayed.



2. Under **Current PAC File**, your PAC file URL is displayed. Enter this URL in your users' browser settings.
3. To view your current PAC file, click the page icon. The PAC file text is displayed. Click **Close**.
4. Under **Available Proxies**, the **Proxies** box displays your proxy server (IP address or host name) and proxy port.
5. To add a proxy server, type the IP address in the **IP** field and the proxy port in the **Port** field and press ENTER.
6. To sort the proxies, click the drag icon and drag the proxy to where you want it.
7. To delete a proxy, hover over the corresponding line and click the red x icon. To delete all proxies, click the **Delete All** red x icon.
8. Under **IP/Domain Exceptions**, to exclude domains from going through the proxy, type the domain in the **New Exception** field, for example, yourdomain.com, and press ENTER to add it to the **IPs/Domains** box.



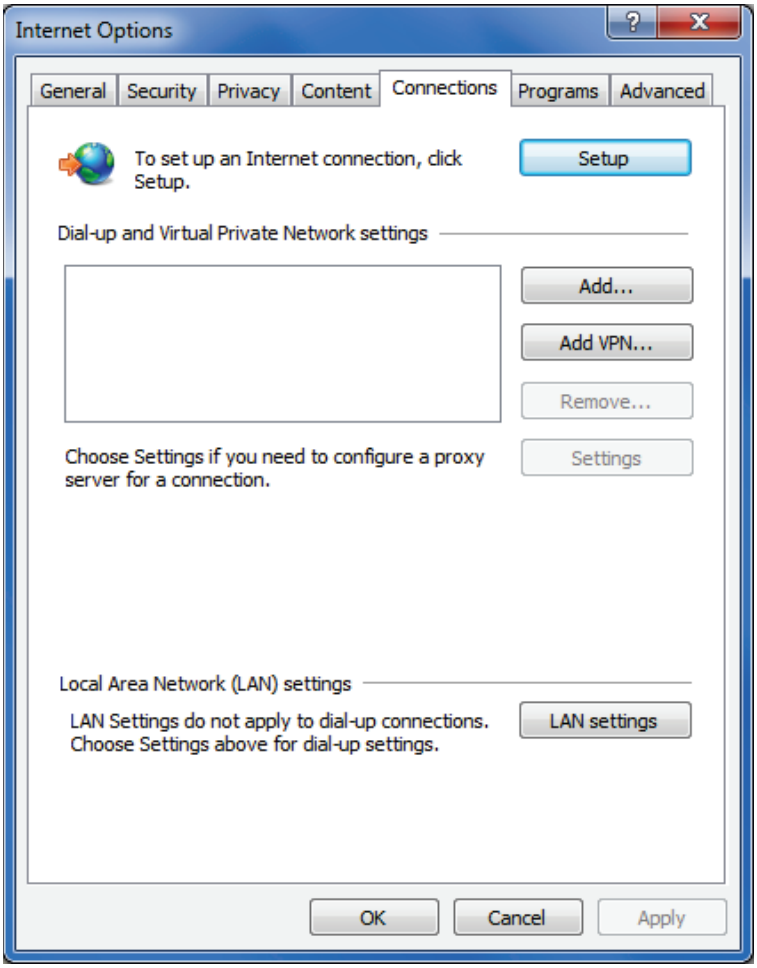
   - "www" is not necessary and is removed when the entry is added.

- Domains are inherently wildcarded by default. However, you can exclude specific domains, for example, example.yourdomain.com, if needed.

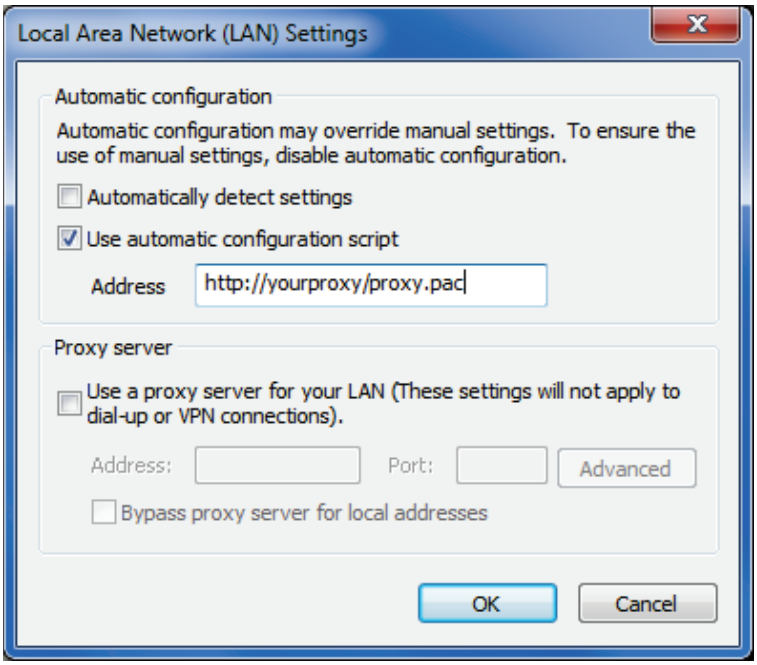
9. To delete a domain, hover over the corresponding line and click the red x icon. To delete all domains, click the **Delete All** red x icon.

Set Internet Explorer Browser Settings Using the PAC File

1. Begin by opening your Internet Explorer browser.
2. Click the **Tools** menu. Then, click **Internet options**. The Internet Options dialog box will appear.



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



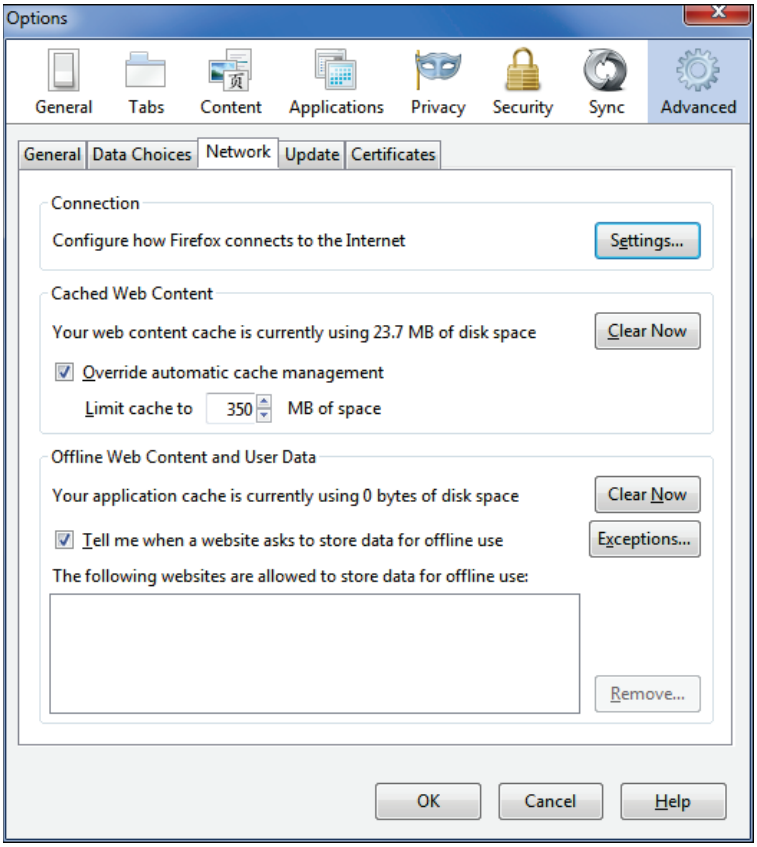
4. Select the **Use automatic configuration script** check box.
5. Type the PAC URL (located on the **Settings - Proxy - PAC File** screen) in the **Address** field.
6. Click **OK** to save your settings.

Push PAC File Configuration to IE Browsers With GPOs

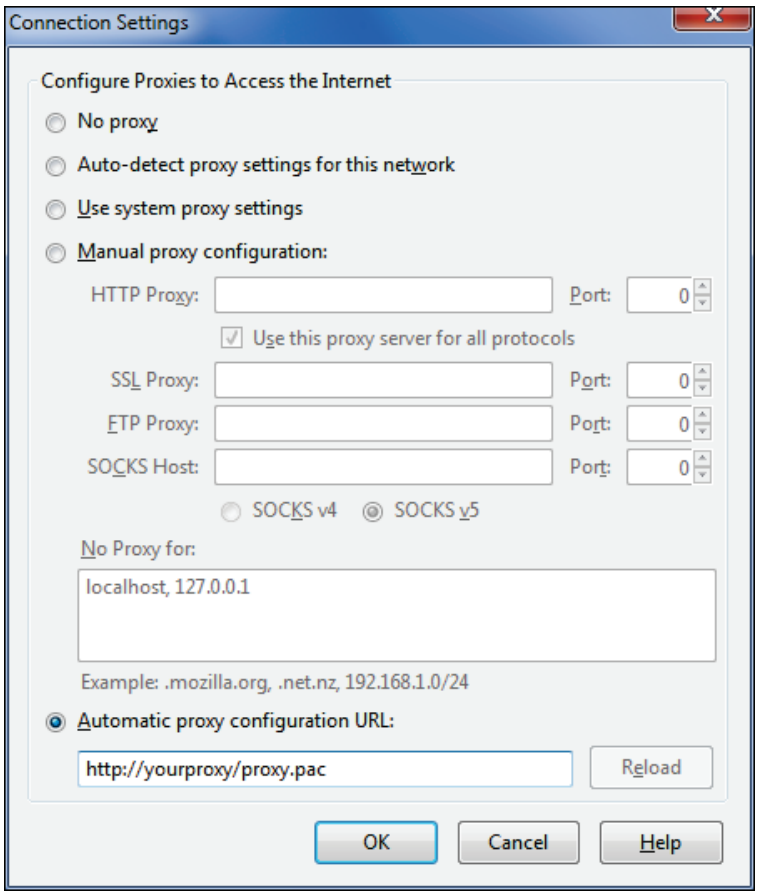
1. Open **Active Directory Users and Computers**.
2. Right-click the root of the domain and select **Properties**.
3. Select the **Group Policy** tab and edit the **Default Domain Policy GPO**, which contains several settings that pertain to IE configuration.
4. Go to **User Configuration - Windows Settings - Internet Explorer Maintenance**. In this area, you can edit the same configuration settings that you access in IE through the **Tools - Internet Options** menu.
5. Open the **Connections** folder.
6. Right-click **Automatic Browser Configuration** and select **Properties**.
7. If applicable, clear the **Automatically Detect Configuration Settings** check box.
8. Select the **Enable Automatic Configuration** check box.
9. It is optional to configure an interval (time to reload policy) for the GPO in the next box.
10. Skip the “Auto-config URL (.INS file)” section.
11. In the **Auto-proxy URL (.JS, .JVS, or .PAC file)** text field, enter the PAC URL (located on the **Settings - Proxy - PAC File** screen) for the auto-configuration.

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**.



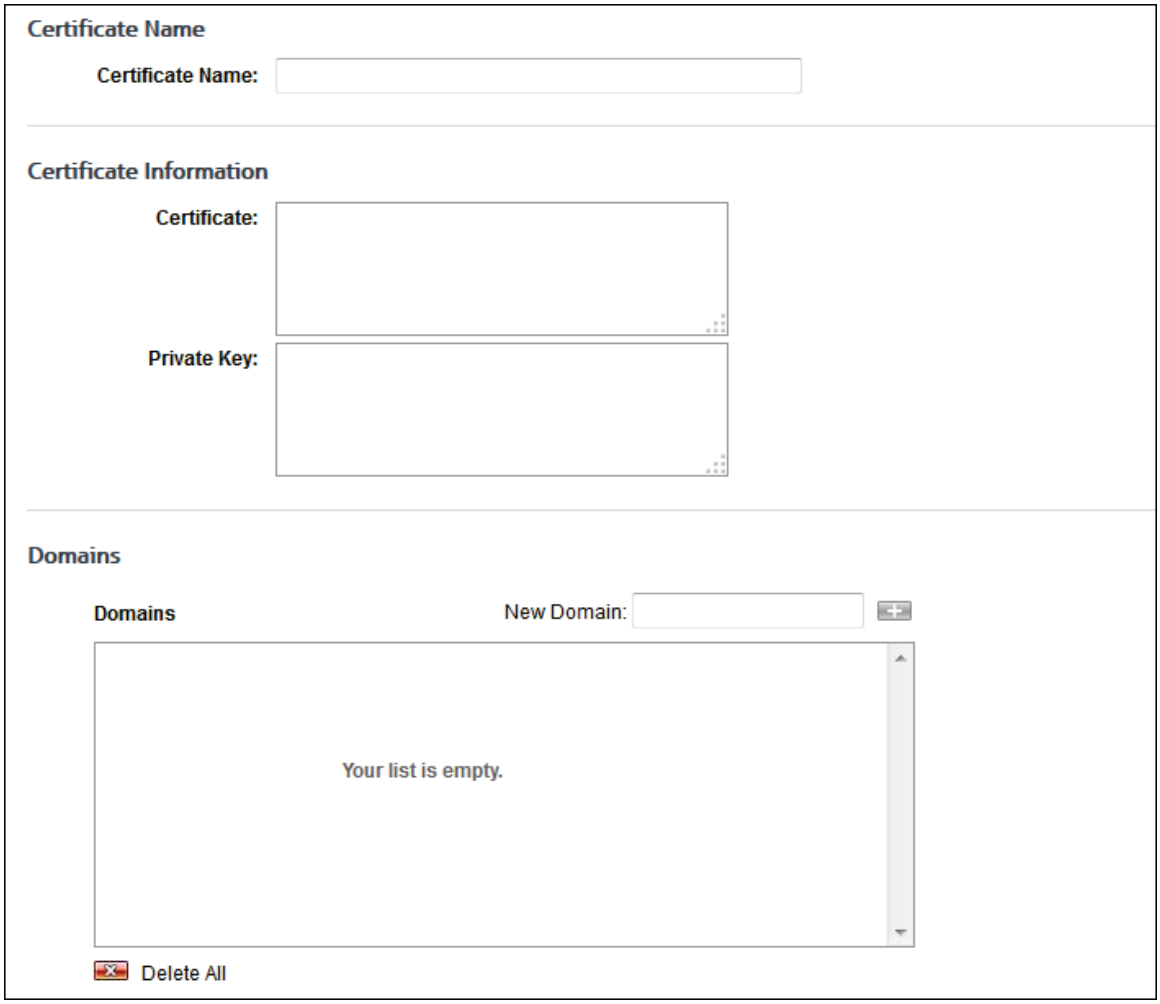
4. Select the **Automatic proxy configuration URL** option.
5. Type the PAC URL (located on the **Settings - Proxy - PAC File** screen) in the **Automatic proxy configuration URL** field.
6. Click **OK** to save your settings.

SSL Certificates

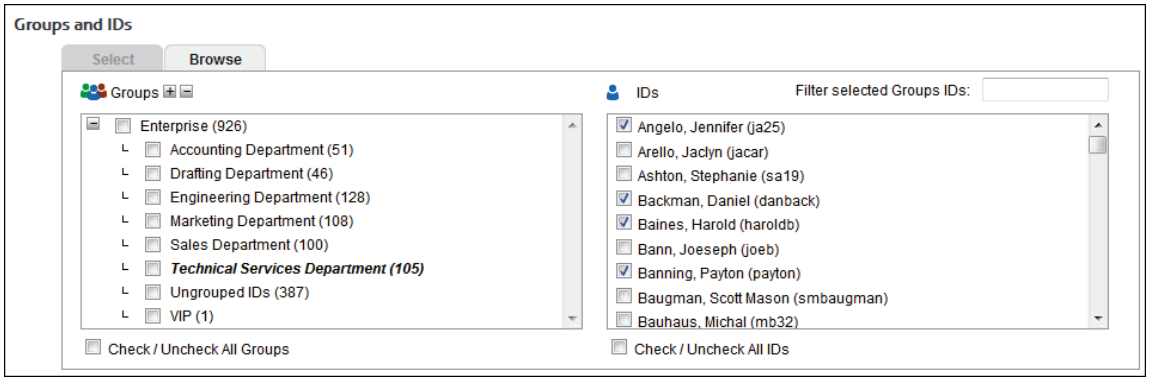
This screen allows you to install client authentication certificates for the proxy to use when in SSL inspection mode. The proxy uses these certificates to identify clients (Web applications) to Web servers so that HTTPS traffic can be inspected. The certificate string and private key string must be unique and are stored in a proprietary data format.

For each certificate, you must assign at least one domain and one group/ID. You can also enable/disable, edit, view, and delete a certificate.

1. To add a certificate, go to **Settings - Proxy - SSL Certificates**.
2. Under **Manage SSL Certificates**, click the green plus icon to add a certificate.



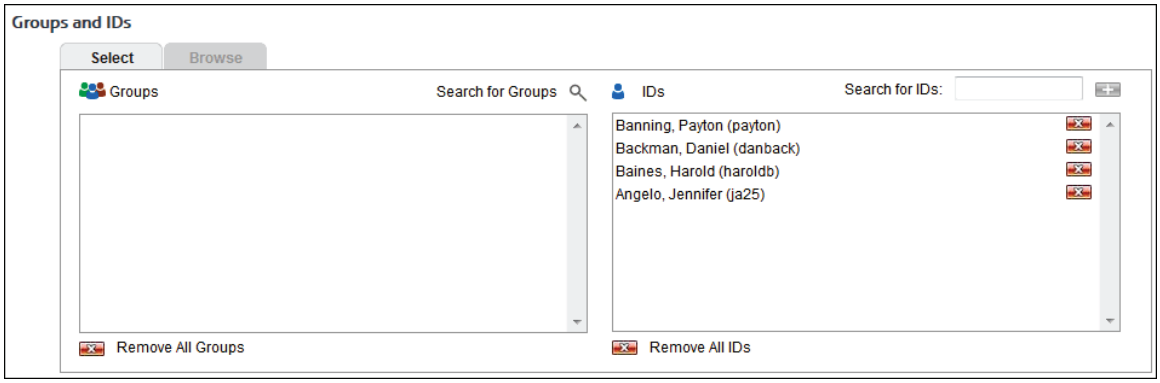
3. In the **Certificate Name** field, type the name of the certificate.
4. Under **Certificate Information** in the **Certificate** field, enter the unencrypted PEM certificate string with no password embedded.
5. In the **Private Key** field, enter the unencrypted PEM private key string with no password embedded.
6. Under **Domains**, to assign a domain to the certificate, type the domain in the **New Domain** field, and press ENTER to add it to the domain list.
7. To delete a domain, click the corresponding red x icon next to the domain. To delete all domains, click the **Delete All** red x icon.
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.



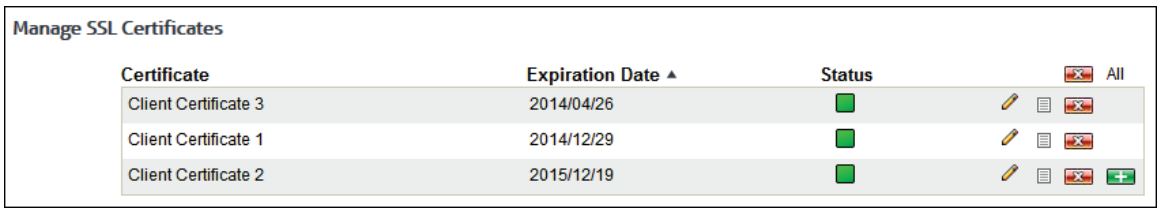
Other options include:

- **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. Click **Add Certificate** at the bottom of the screen. The certificate is added to the list of certificates.



11. To sort the certificates, click the column title to sort by that column. An arrow is displayed next to the column title when you hover over it indicating that the column is sortable. The default sort is by **Expiration Date** in ascending order.
12. To turn a certificate on or off, click the **Status** indicator to enable (green) or disable (red) the certificate.

13. To edit a certificate, click the pencil icon. You may only change the certificate name, domains, and groups/IDs. Click **Update Certificate** to submit your changes.
14. To view a certificate, click the page icon. The certificate text is displayed. Click **Back** to return to the list of certificates.
15. To delete a certificate, click the red x icon. A dialog box is displayed requesting confirmation of the deletion. Click **Delete**. To delete all certificates, click the **All** red x icon, and then click **Delete**.

SSL Inspection

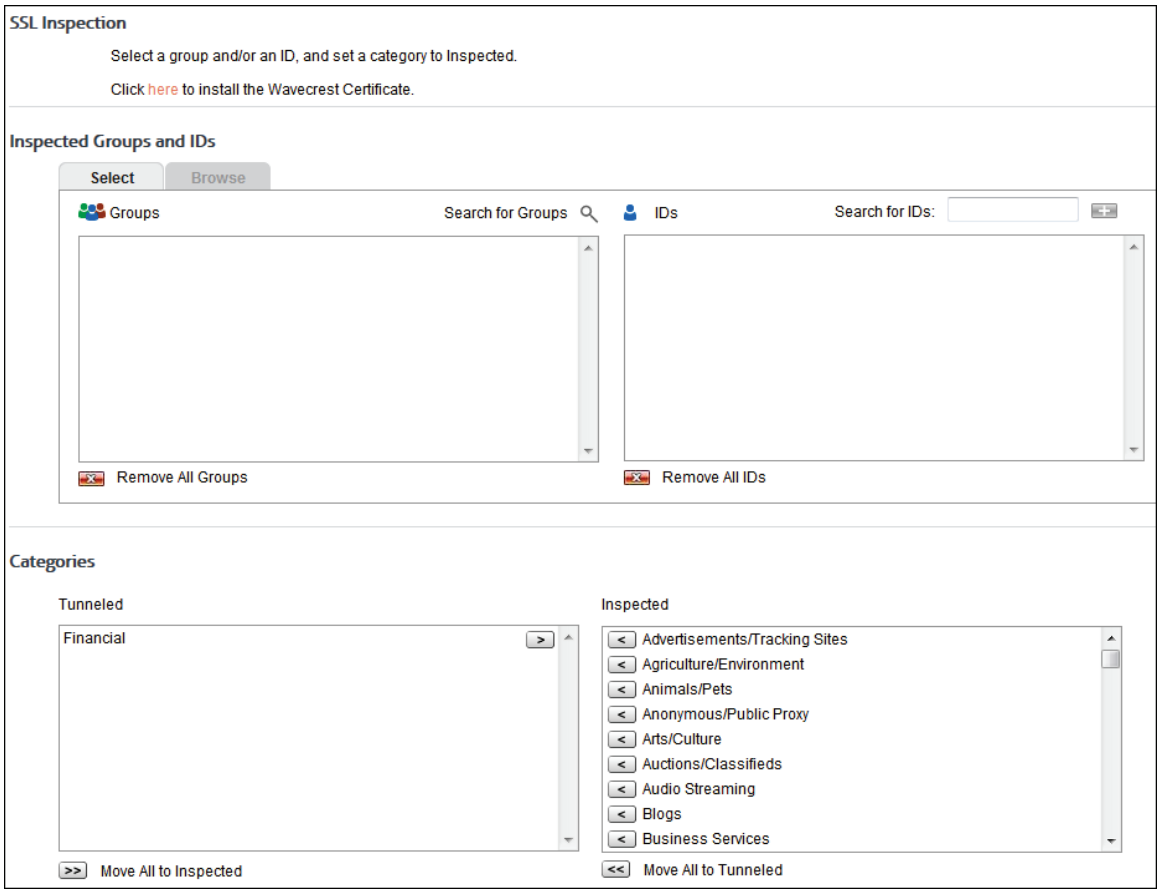
IMPORTANT: By enabling SSL Inspection, applications using HTTPS communication and not utilizing Windows Certificate Stores for certificate validation may encounter errors. Contact Technical Support for assistance.

This screen allows you to inspect SSL-encrypted traffic (that is, HTTPS activity) through the proxy server. By default, no groups are selected, and all categories except Financial are set to be inspected including custom categories. The Financial category is the only category set to Tunneled by default. Tunneled traffic is SSL-encrypted traffic that passes through the proxy server without being inspected.

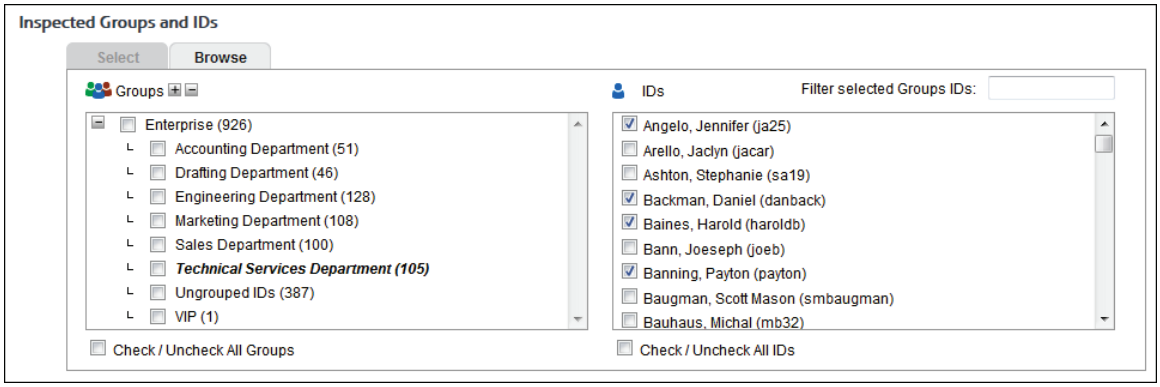
For inspection to occur, you will need to select a group and/or an ID, and set a category to Inspected. Inspected SSL traffic can be viewed in the Real-Time Web Monitor and in audit reports.

NOTE: Before using SSL Inspection, the Wavecrest Certificate must be installed. The certificate can be installed from this screen.

1. To inspect SSL traffic, go to **Settings - Proxy - SSL Inspection**.



2. To install the Wavecrest Certificate, click the link under **SSL Inspection**. Refer to the Wavecrest Certificate Installation Guide for instructions on how to install/distribute the certificate.
3. Under **Inspected Groups and IDs** on the Browse tab, choose groups and IDs whose traffic you want to inspect. To view IDs in a group, click the group name.

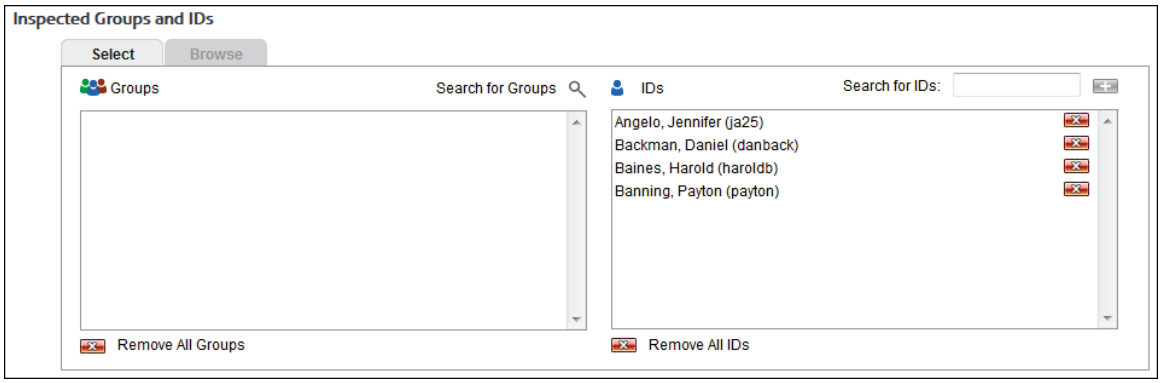


4. On the Browse tab, choose groups and IDs by selecting their corresponding check box.
    - The groups with a selected check box will be inspected.
    - To select specific IDs, click the group name. The IDs associated with that group are displayed in the **IDs** box.
        - Select the check box for each ID that you want to inspect.
        - If only IDs are to be inspected, ensure that the check box for the group is cleared, that is, the check mark is removed.
        - If the group check box is still selected, all IDs whether selected or not will be inspected.

    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 icons next to **Groups**.
    - **Searching for a specific ID:** If you know the ID names you want to select, 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.



5. 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.

6. Under **Categories** in the **Inspected** box on the right, all custom and standard categories except Financial are displayed for inspection by default.
7. To exempt SSL traffic from inspection, click the left arrow icon in the **Inspected** box to move categories to the **Tunneled** box. These categories will bypass inspection and will not appear in the **Inspected** box. You can also click the double left arrow to move all categories to the left so that no categories will be inspected.
8. To inspect tunneled SSL traffic, click the right arrow icon in the **Tunneled** box to move categories to the **Inspected** box. These categories will be inspected and will appear in the **Inspected** box. You can also click the double right arrow to move all categories to the right so that all categories will be inspected.
9. Under **Domain Exceptions**, add any domains that you want tunneled, that is, exempted from inspection.

10. In the **New Exception** field, type the domain and press ENTER. Your entry is added to the **Domains** box. The list of domains to be tunneled also includes specific entries from the Wavecrest URL List.

    (Optional) Add Wildcard Entries. You can use wildcards to add multiple URLs simultaneously. This can be done with domain matching.

    Wildcards With Domain Matching. This URL matching method categorizes Web sites whose pages all contain the same type (category) of content, e.g., Shopping, News, and Sports. In these relatively simple cases, one category applies to the entire site. Under this method, if the Web log entries are in any of the following formats and the URL List contains a matching URL, the product will categorize the visit on the basis of the domain name.

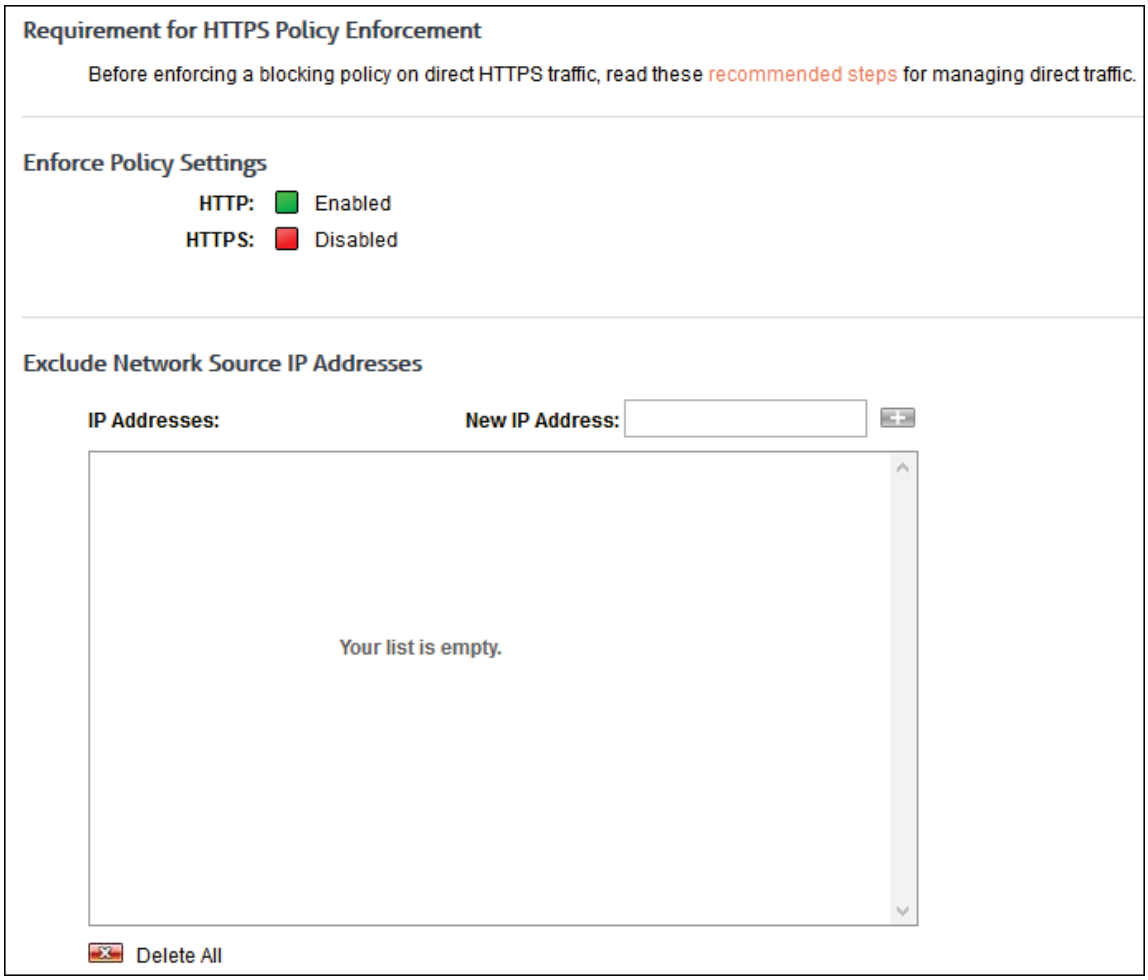
    - www.mydomain.com
    - *.mydomain.com
    - www.mydomain.*
    - *.mydomain.*

11. To delete a domain, click the red x icon next to that entry. To delete all domains, click the **Delete All** red x icon. Note that domain entries from the URL List cannot be deleted.
12. Click **Submit** to apply your changes.
    - A message indicating "successfully updated" is displayed briefly above the Submit button.
    - If an error is encountered, a message indicating that there was an error is displayed.

Direct Traffic

Managing direct HTTP and HTTPS traffic requires that the traffic be redirected in order for the proxy to monitor and filter the Web traffic. This page allows you to enforce policy settings on direct HTTP and HTTPS traffic, exclude network source IP addresses from being redirected, and also exclude destination IP addresses/domains from going through the proxy. The proxy will see all Web traffic regardless if a proxy port is set in the browser. Users will be displayed with different IP addresses but have the same ID of "direct." If cookie authentication is being used, user names can be obtained.

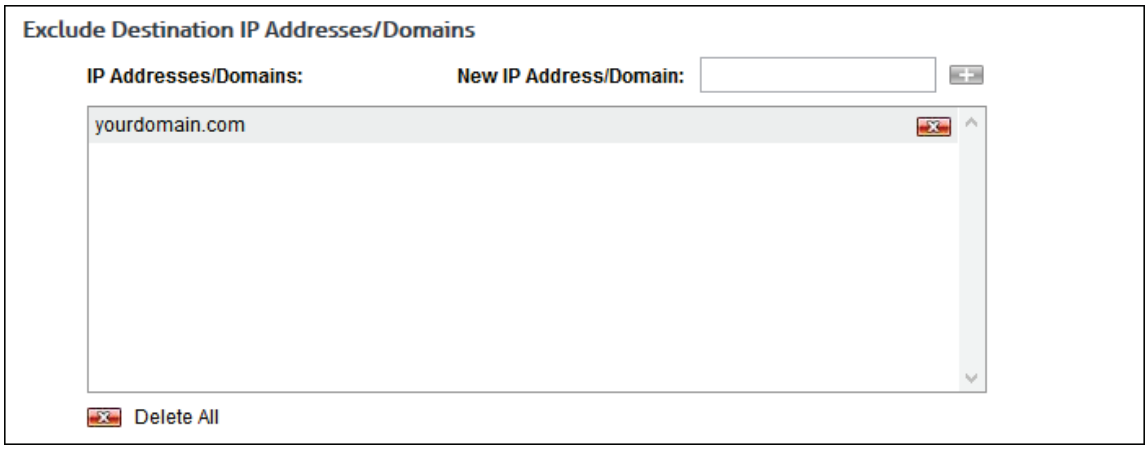
1. Go to **Settings - Proxy - Direct Traffic**.



IMPORTANT: Before proceeding further, read the recommended steps on managing direct traffic. It contains information on setting the DNS server.

2. Under **Enforce Policy Settings**, the **HTTP** status indicator is enabled (green) by default to apply policy settings to direct HTTP traffic.
3. If you are sure that the DNS server is properly set up, click the **HTTPS** status indicator to apply policy settings to direct HTTPS traffic. The indicator is disabled (red) by default.
4. Under **Exclude Network Source IP Addresses**, to exclude a network source IP address from being redirected, type the IP address in the **New IP Address** field, and press ENTER to add it to the **IP Addresses** box.
5. To delete an entry, click the corresponding red x icon. To delete all entries, click the **Delete All** red x icon.

6. Under **Exclude Destination IP Addresses/Domains**, to exclude a destination IP address/domain from going through the proxy, type the IP address in the **New IP Address/Domain** field, and press ENTER to add it to the **IP Addresses/Domains** box.



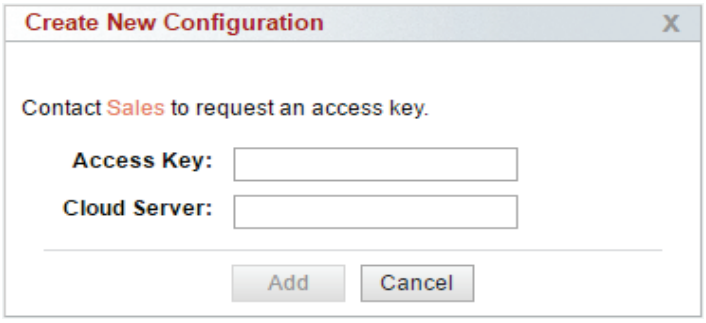
   - The IP addresses/domains listed here are used in the PAC file and are also shown on the PAC File Configuration page as exceptions.
   - "www" is not necessary and is removed when the entry is added.
   - If you are not using the PAC file, enter specific domains to exclude, for example, example.yourdomain.com. With direct traffic, domains are not wildcarded.

7. To delete an entry, hover over the corresponding line and click the red x icon. To delete all entries, click the **Delete All** red x icon.

Hybrid Configuration

This page allows you to pair your local CyBlock installation with your CyBlock Cloud account after you receive your access key. If you have more than one cloud account, those accounts can also be paired. Pairing allows the configuration changes in your local CyBlock instance to be automatically synced with your cloud accounts. It also allows you to run reports on your cloud users. If you do not have an access key, click the **Sales** link to send an e-mail to Sales.

1. Go to **Settings - Hybrid**. The Hybrid Configuration page is displayed.
2. To create a configuration, click the **Add New Configuration** green plus icon.



3. If this is the first configuration being created, the Sales link is displayed in the Create New Configuration dialog box.
4. In the **Access Key** field, enter the access key that is assigned to your CyBlock Cloud account. You should have received an e-mail notification with this information.
5. In the **Cloud Server** field, enter the cloud server provided by Sales or in your CyBlock Hybrid Account Created e-mail. This is the pairing server to which your CyBlock installation is connected.

6. Click **Add**. An icon is displayed indicating that pairing is occurring.
7. If the pairing is successful, you will see the cloud server information, the status "Paired," and available icons.
    - Sync communication is enabled between CyBlock and your cloud account.
    - On the User Management - Authentication - Rules tab, a Cloud rule is created with the same authentication type as the Default rule which you can modify, but not delete.

8. To manually sync changes with your cloud account, click the **Sync** icon.
    - The status "Syncing" is displayed.
    - If the sync is successful, the previous status "Paired" is displayed.
    - If the sync fails, an error message and the previous status "Paired" are displayed.
    - When running reports, you will need to perform a manual sync first to get the current day's cloud data.
9. To temporarily stop all communication between CyBlock and your cloud account, click the **Stop** icon.
    - Sync communication is disabled between CyBlock and that cloud account.
    - The stop icon toggles to a play icon allowing you to resume sync communication. Note that log messages created while communication is stopped are not transmitted when communication resumes.
    - After resuming communication, it is recommended that you perform a manual sync.
10. To delete the pairing between CyBlock and your cloud account, click the **Delete** red x icon.
    - You will be prompted twice to confirm the deletion.
    - After confirming the deletion, all communication is ended between CyBlock and that cloud account.
    - You will need to contact Sales to request a new access key.
    - The Cloud rule mentioned above is removed from the Rules tab.
11. If you have created more than one configuration and want to manually sync changes with all cloud accounts, click the **Sync All** icon.

Configurations Synced

When configuration changes occur in CyBlock, they are automatically synced with your cloud accounts. Synchronization applies to the following configurations:

Web Management

- **Application Controls** - This includes any allowed YouTube videos associated with the applied policy.
- **Filter - Categories** - This includes the groups and IDs and categories to be blocked and white/black list of URLs associated with the applied policy.
- **Filter - Content** - This includes the groups and IDs, content types, extensions, and exact file names to be blocked as well as exempt categories associated with the applied policy.
- **Filter - Web Search** - This includes the Safe Search setting and search terms to be blocked.

- **Filter - Message** - This includes the custom Web blocking message or Redirect URL being used.

User Management

- **Authentication - Rules** - This includes the authentication type for the Cloud rule.
- **Authentication - Cookie** - This includes the session time and authentication logon page settings excluding the logo. Changes to the logo are not synced with your cloud account at this time. Your cloud account uses the default CyBlock Cloud logo. The authentication passwords for users are also synced.
- **Edit Users** - This includes adding, deleting, moving, and modifying groups and IDs.
- **Import Users** - This includes importing groups and IDs from Active Directory.

Categorization

- **Customize - URLs** - This includes custom categories with their custom URLs.

Settings

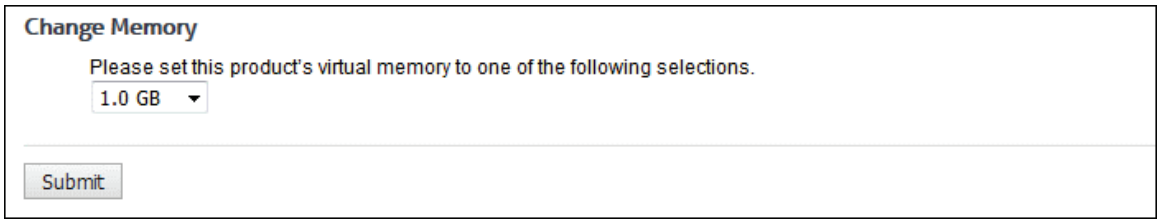
- **Proxy - SSL Inspection** - This includes the groups and IDs and categories to be inspected as well as the domains to be tunneled.
- **Hybrid** - This includes IP/domain exceptions.

Memory Settings

NOTE: This screen does not apply to the VM deployment. Memory is set on the virtual machine.

You must configure the maximum amount of memory that the product will use to perform its operations. The memory setting helps optimize overall system performance and precludes unnecessary degradation of system speed. The default setting is 512 MB. For optimal performance, it is recommended that you choose the setting that is approximately half of your available memory (RAM). If you start to meet your memory threshold, the product will notify you to increase your memory setting.

1. To set your memory, go to **Settings - Memory**.

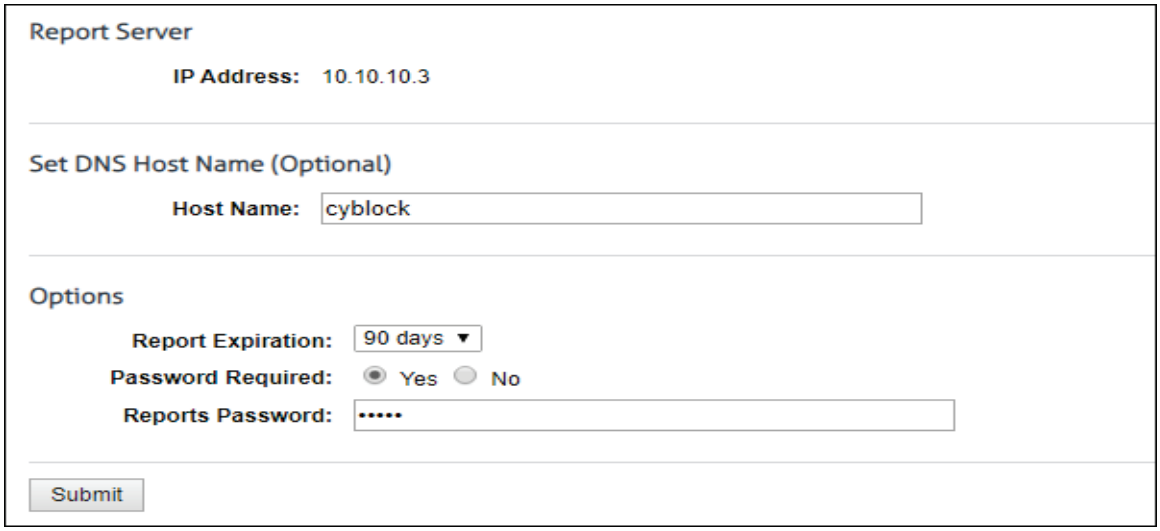


2. Use the drop-down box to select the appropriate amount of memory to be used keeping in mind your available RAM.
3. Click **Submit** to apply the change.
4. After you click **Submit**, you will receive a dialog box asking whether you would like to restart the service. Your memory setting change will not take effect until you restart the service.
5. Click **OK** to continue.

Interactive Reports

This page lets you establish settings for Interactive reports, such as the length of time to keep reports and a required password that should be changed to retrieve the reports.

1. Go to **Settings - Reports - Interactive Reports**.



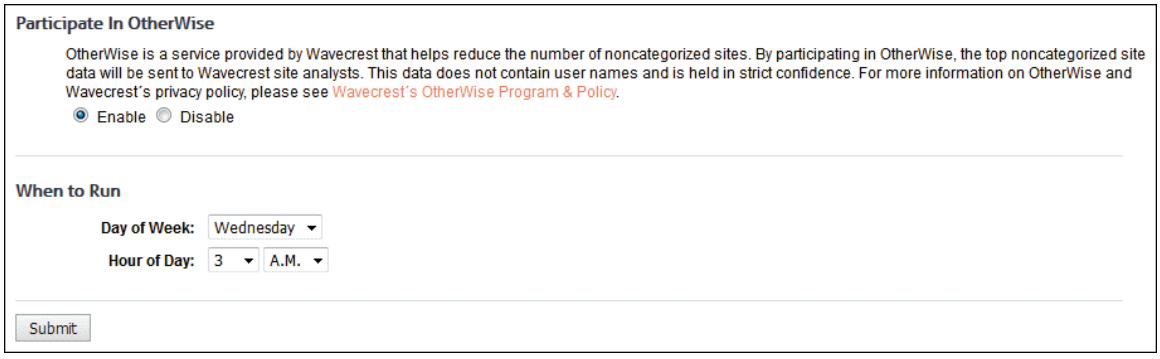
2. In the **IP Address** field, select the IP address to be used for reporting if a drop-down box is present. If the IP address is plainly displayed with no available drop-down box, the product found one NIC IP address, and no further action is required.
3. This step is optional. If you want to identify an additional report server DNS host name, enter it in the **Host Name** field. This additional server can be used for internal or external use.

   Example: If you have external users, you may want them to be able to access Web-use reports. In this case, you would use this field to enter a DNS host name that external computers will recognize.
4. Select the **Report Expiration** using the drop-down box. Interactive reports will no longer be accessible past the number of days you select.
5. Type a password in the **Reports Password** field. This password must be used by anyone trying to access an Interactive report. The default password is *password*.
6. Click **Submit** to apply your changes.

Participate in OtherWise

OtherWise is a service provided by Wavecrest that helps reduce the number of noncategorized sites. By participating in OtherWise, the top noncategorized site data will be sent to Wavecrest Computing site analysts. This data does not contain user names and is held in strict confidence. For more information on OtherWise and Wavecrest´s privacy policy, please see Wavecrest´s OtherWise Program & Policy in Appendix C.

1. Go to **Settings - Reports - OtherWise**.



2. Select **Enable** to participate in OtherWise and have top noncategorized site data sent to Wavecrest site analysts. No user names are included, and all data will be held in strict confidence.
3. Select the day of the week and hour of the day you want your OtherWise data processed and sent to Wavecrest site analysts. Your Top Noncategorized Sites report will also be displayed as a recently run report on the Manage Reports page where you can view it.
4. Click **Submit** to save your changes.

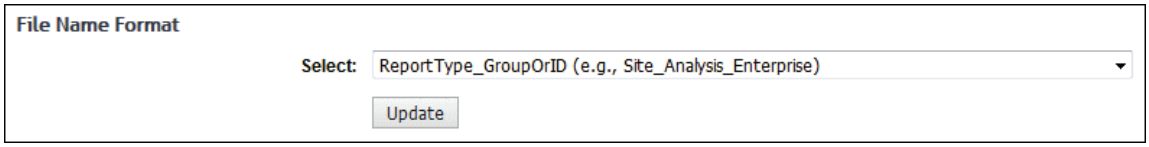
Report Options

To let you further customize your reports, this page contains several options that will affect how your reports will look and what information will be included on them. Click **Update** to apply your changes in each section.

1. Go to **Settings - Reports - Options**.
2. Under **Audit Report Advanced Options**, select **Include All Groups' Users** to display a user ID even if there is no data for that ID in a User Audit Detail or Category Audit Detail report.
3. The **Maximum Hyperlinked URLs** field determines whether URLs are hyperlinked in audit detail reports.
   - If this field is greater than or equal to the number of report URLs, all URLs are hyperlinked.
   - If this field is less than the number of report URLs, no URLs are hyperlinked.
   - Enter a number to display hyperlinked URLs in an audit report.

4. For **Visit Filter**, the **Enable** option is selected by default and set to 3 seconds.
   - With the Visit Filter turned on, a URL visit will not be counted more than once in reports within a specified time period. In the **Value** field, type the time period in seconds that you would like this to occur.
   - If you do not want to use this feature, select the **Disable** option. The **Value** field will display "-1" meaning turned off and will be unavailable. When you turn the Visit Filter back on, the **Value** field is reset to "3."

5. Under **File Name Format**, you may choose a file name format for e-mailing reports. The available formats are made up of various combinations of the date, time, group or ID, and report type. This format is used if *E-Mail* is selected for the report delivery when creating reports.
6. In the **Select** field, choose the file name format that you prefer.



7. Under **General Advanced Options**, **Check for New Log Files** is selected by default. This means that before running a report, the product will check for any new log files. If you want to turn off this feature, clear the check box.
8. Select **Anonymous IDs** to display the Anonymous IDs field when creating reports. By making this field available, you can then choose to show IDs anonymously in any applicable report you are running. This option applies to the following reports:
    - All High-Level Summary Reports excluding Top Web Sites
    - Category Audit Detail
    - Search Terms Audit Detail
    - Site Audit Detail
    - Site Analysis Bandwidth
9. Select **Compress Reports for E-Mail** to compress the report attachment for read-only reports in an e-mail as a .zip file.

10. Under **Maximum IDs**, in the **Maximum IDs Displayed Per Table** field, type the maximum number of IDs that you wish to appear on reports. This must be a number between 1 and 250. The default is 25. If the number entered is not in the range, the Update button will be disabled.

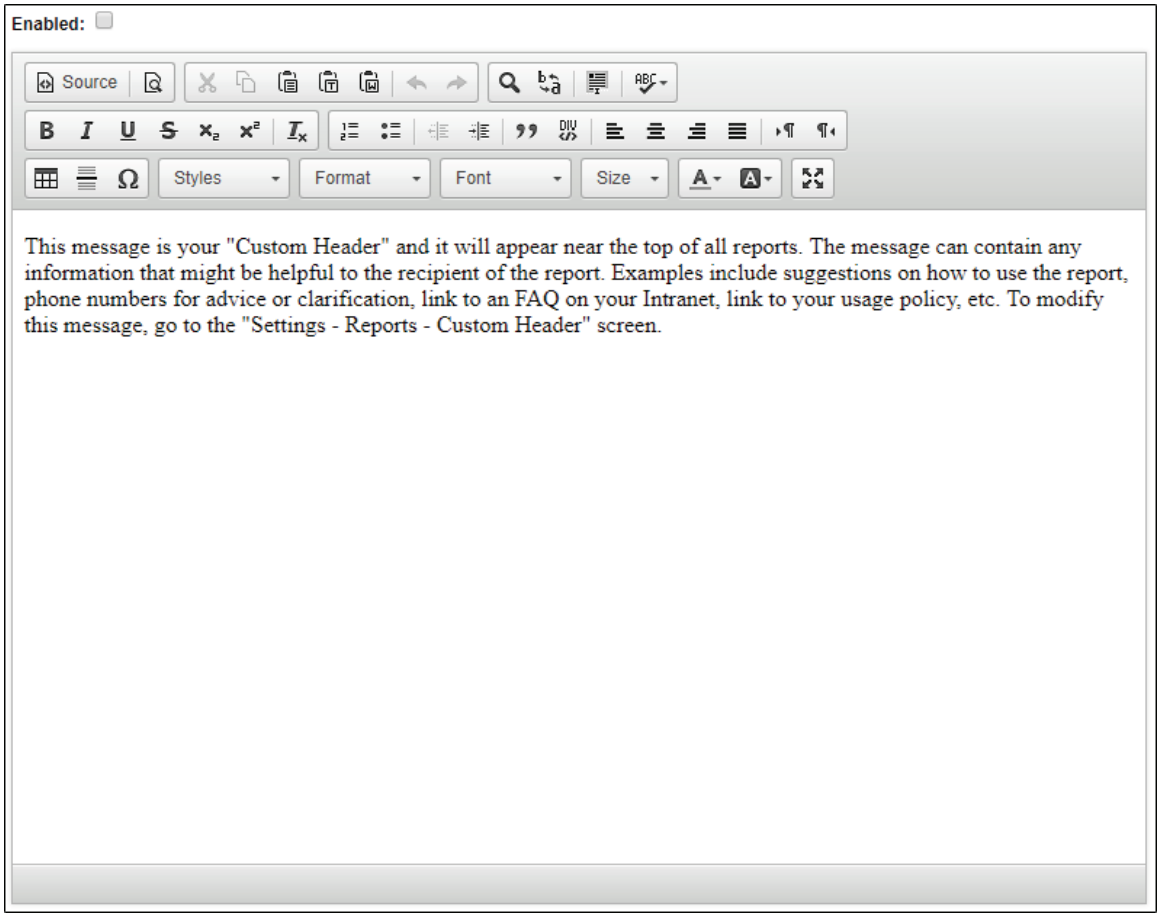
11. Under **Language Settings**, select the language that you want to be used in reports.

12. Be sure to click **Update** in every section in which you made changes.

Custom Report Header

This page lets you customize a message that will appear at the top of every standard report that is ran. You can use the Toolbar buttons to change the formatting of the text. You can also enable or disable the message from appearing when running new reports by toggling the Enabled checkbox.

1. Go to **Settings - Reports - Custom Header**. The Custom Header Message is displayed.



2. Check the **Enabled** checkbox to have the message added to reports or uncheck the box to not include message in reports.
3. Customize the default header message to suit your needs. When the message is changed to be blank, the default message is returned. If you wish to not show message, uncheck the **Enabled** box instead.

Help

Profiling

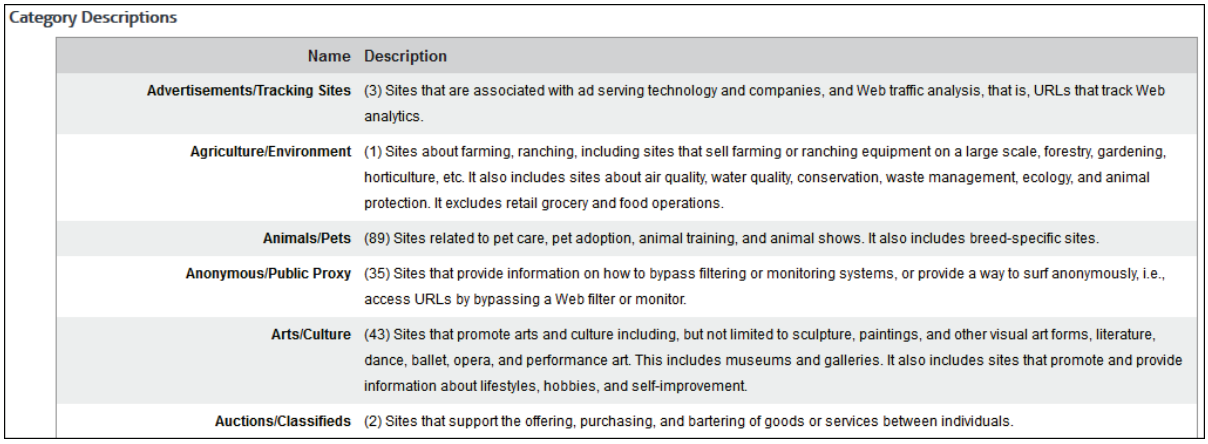
If you ever experience difficulties that cannot be resolved via online Help, Technical Support may ask you to activate the product's "profiling" mode via the Profiling page. When profiling is activated, the product will generate a considerable amount of data to help Technical Support resolve the issue. Any information sent to Wavecrest will be held in strict confidence and destroyed after the issue has been resolved. When the data is generated, it will be sent to a special file (sprofile.htm) for subsequent transmission to Technical Support via e-mail (support@wavecrest.net).

If you are ever asked to turn on profiling, go to **Help - Support - Profiling** and follow Technical Support's instructions.

Category Descriptions

This page provides a description of each category as well as a category index for Technical Support purposes.

Go to **Help - Category Description**. The Category Descriptions page is displayed.

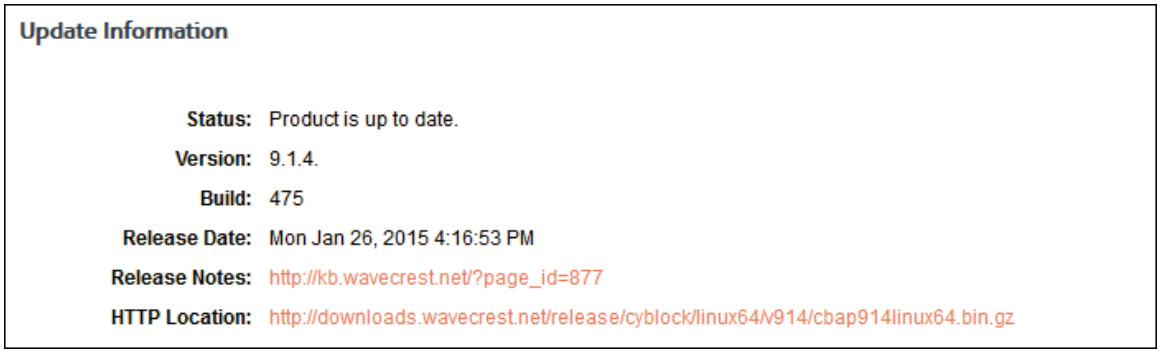


Name	Description
Advertisements/Tracking Sites	(3) Sites that are associated with ad serving technology and companies, and Web traffic analysis, that is, URLs that track Web analytics.
Agriculture/Environment	(1) Sites about farming, ranching, including sites that sell farming or ranching equipment on a large scale, forestry, gardening, horticulture, etc. It also includes sites about air quality, water quality, conservation, waste management, ecology, and animal protection. It excludes retail grocery and food operations.
Animals/Pets	(89) Sites related to pet care, pet adoption, animal training, and animal shows. It also includes breed-specific sites.
Anonymous/Public Proxy	(35) Sites that provide information on how to bypass filtering or monitoring systems, or provide a way to surf anonymously, i.e., access URLs by bypassing a Web filter or monitor.
Arts/Culture	(43) Sites that promote arts and culture including, but not limited to sculpture, paintings, and other visual art forms, literature, dance, ballet, opera, and performance art. This includes museums and galleries. It also includes sites that promote and provide information about lifestyles, hobbies, and self-improvement.
Auctions/Classifieds	(2) Sites that support the offering, purchasing, and bartering of goods or services between individuals.

Check for Product Updates

Use this page to check for new product versions and download the latest release.

1. Go to **Help - Check for Updates**. This page will tell you if there are any current updates to the version of your product.



2. The **Status** message will let you know if there are any new updates or if your product is currently up to date. If updates are available, click **Update Now** to upgrade the product.

   NOTE: While the product is updating, the service will be down for a very short time.

End User License Agreement

This page allows you to accept and print the License Agreement.

1. Go to **Help - EULA**. The End User License Agreement page is displayed.
2. If the License Agreement has not been accepted, as you scroll down to the bottom of the text, the Accept button will become available.
3. If the License Agreement has not been accepted, choose whether to opt in or out of the OtherWise Program by using the checkbox in the "Participate in OtherWise" section. Once the license is accepted, the checkbox for opting in or out of the OtherWise Program is removed. To modify participation, go to "Settings - Reports - OtherWise
4. Click **Accept**. Once the License Agreement is accepted, the Accept button will no longer be visible.

   NOTE: If the License Agreement is not accepted, manager accounts will receive an error message when they attempt to log on.
5. Click **Print** to print the License Agreement. You may return to this page at any time to view or print it.

Appendix A - Groups and IDs

Introduction to Groups and IDs

General. Groups and IDs is a feature that is used to input and/or import users' ID information into the product for subsequent use in reporting and/or filtering processes. As discussed later, the groups and IDs input/import process can be performed manually, automatically, or in some cases semiautomatically. Optionally, this feature can also be used to custom-group the IDs for more advanced usage.

Using the Product's Default Grouping Arrangements. You may not need or want to group your users in any particular way. For example, you may always want to see all users in high-level reports (e.g., Site Analysis), and/or you may want to apply policy settings uniformly to all users. The core grouping capability is designed to accommodate this universal approach. To implement, you do not need to take any special measures. All users are placed in the Ungrouped IDs group (a subgroup of Enterprise), and you designate Enterprise as the controlling group for all report formats and policy settings.

Using the Product With Customer-Specified Grouping Arrangements. Using the simplified universal approach discussed in the preceding section may not always be satisfactory. For example, management may want reports that only cover Web usage in particular departments or divisions. They may also want reports that cover personnel at specific locations, or they may want to see activity by all personnel who have a particular job classification. And, very importantly, they may want reports that show a single user's Web-access activity. In cases like these, user-grouping is essential.

NOTE: Although grouping by department is the most popular approach, groups can be based on any characteristic or parameter that applies to the users in the workforce, e.g., job title, salary level, and work location. All groups must contain at least one user in order to be reported on.

Augmenting the Core Grouping Arrangement. The groups and IDs core grouping capability can be easily augmented to accommodate a variety of requirements to monitor and/or control Web activity by groups or users. To take advantage of this capability, the overall user ID population must be subdivided into logically structured groups. This will take the form of a hierarchical structure under Enterprise.

Customized User-Grouping. Wavecrest products were designed with customized user-grouping in mind. Our products enable you to input (or import) the user population. If desired, the user population can be subdivided into a single or multi-tiered hierarchical grouping structure. This capability lets you set up, apply, and monitor different policies for different organizational units, i.e., divisions, departments, geographic areas, individual users, etc. It also lets you (a) use block/allow settings to govern Web access (Wavecrest's CyBlock products only), (b) vary report formats for different recipients, and (c) restrict the distribution of group-level or individual user reports on a "need to know" basis. Such restriction increases managerial efficiency by segmenting the reports and providing recipients with only the information they actually need. It also prevents distribution of extraneous, undesired information, and it helps maintain users' privacy.

Planning Ahead. For customers that want to set up a customized grouping arrangement, we recommend that management or HR first design the grouping structure. This should be done before the network administrator begins the product setup process. That way, the administrator will have a clear blueprint of management's expectations when he or she starts the setup process. Designing the scheme is not difficult. There are many "models" that organizations can choose from. The most common grouping scheme is an organization chart.

Multiple Approaches to the Management of Groups and IDs. Wavecrest products offer several alternative ways to set up and manage groups and IDs (users). These include fully automated, partially automated, and strictly manual approaches. These alternatives are discussed below.

Fully Automated Grouping Using Active Directory

Overview. For large ID populations, it is best to use automated processes to create groups and assign IDs. Wavecrest products provide this capability. Our products can import groups and IDs into the product

from directories, databases, or spreadsheets on other servers. This capability can save extensive amounts of time and manual data entry. These savings can be realized if network users' information (e.g., employee name, employee number, organizational affiliation, network privileges, and user ID) has already been organized and set up. For example, many organizations enter their computer users' unique identification and security data by department into a database in an Active Directory Server or a Domain Server. So long as each "database" record contains a unique user ID and a unique group (department) designator, the product can import the data en masse into groups and IDs.

Active Directory. The use of "directory services" for network management purposes is common in larger organizations. Microsoft Active Directory (AD) is a popular example.

How Wavecrest Products Interact with Active Directory

General. The groups and IDs import feature is optional functionality. It can be used in conjunction with Active Directory to automatically:

- Import relevant user information from the directory into the product's groups and IDs structure.
- Create a hierarchical groups and IDs tree in the product.
- Assign the IDs to the appropriate groups in the tree.

Once you have Active Directory configuration(s) set up, the import feature can also be used to manually import IDs into the product immediately.

CAUTION: Using Active Directory to implement automated grouping is a powerful and efficient concept. However, for the concept to be successful, the directory must have fields that contain appropriate employee-related information needed by the product, e.g., user ID, full name (if used), and immediate parent organization. The fields must be structured in a logical, hierarchical "chain of command" manner, and all groups and subgroups (i.e., organizational units or OUs) must have unique identifiers or labels. A unique identifier can be a department number or a department name–or any other type of designation–so long as there are no duplicates in the assigned database OU field. In large organizations where like functions in different locations may have the same name (e.g., "Sales" in Germany and "Sales" in England), the name should be augmented with a prefix or suffix to provide differentiation. For example, in this case, the two functions could be named "Ger.Sales" and "Eng.Sales." Assignment of unique department numbers to the various workgroups is also an effective solution. Most directories are already designed in this hierarchically structured manner for related reasons, e.g., group policy administration, network security administration, and access control. In such cases, the import feature will work smoothly and quickly.

For purposes of this discussion, we assume (a) the customer's Active Directory contains such information, and (b) "groups" will represent departments, divisions, etc. in a hierarchical organization.

Figure 1 below is a hypothetical illustration of such information.

UserID	FullName	member of	member of	member of	member of
53801	Smith, John	Accounting	BuickMfg	Domestic	GeneralMotors
27498	Brown, Jane	Sales	ChevroletMfg	Domestic	GeneralMotors
41749	Doe, Oscar	QualityControl	CadillacMfg	Domestic	GeneralMotors
25998	Ray, Tom	Accounting	BuickMfg	International	GeneralMotors
37494	Gill, Ann	Production	ChevroletMfg	International	GeneralMotors
26487	Barr, Phil	Engineering	CadillacMfg	International	GeneralMotors

Figure 1. Example of Groups and IDs Information

Field Definitions. In this example, columns 1 and 2 are devoted to the individual employees, and columns 3-6 illustrate the departmental or organizational hierarchy. Column 3 is the lowest level in the

hierarchy and is the employee's immediate parent organization. Columns 4 through 6 represent increasingly higher levels in the organizational hierarchy.

Hierarchical Considerations. Figure 1 illustrates a hypothetical multitiered case involving the maximum number of hierarchical levels–four. Fewer columns can be used if fewer levels of hierarchy (or none at all) are needed.

For example, only three columns of data are mandatory for a two-level, IDs-only, no-full-names approach. One of the three columns is used for some form of user ID, one for the users' first-level parent(s), and one for second-level parents. Such an approach would use columns 1, 3, and 4 in Figure 1.

Only two fields are mandatory for a single-tier approach. These are the columns that provide user ID and immediate parent information. In Figure 1, these would be columns 1 and 3. However, two fields alone cannot support a multi-tier approach or provide for full names in reports.

Column Numbers and Names. Wavecrest products do not require that the columns be positioned or named exactly as shown in the example in Figure 1. As long as the proper types of information are provided, other left-to-right positioning schemes and column names will also work.

Use of Full Name. Although Figure 1 shows full names as well as user IDs, the use of full names is optional.

User ID Considerations. In some cases, the customer's directory will be one that is used in IT to control network access. Active Directory is a good example. In such cases, the directory's user IDs will exactly match those that Wavecrest products find in the network log files. However, it is possible that a different type of LDAP-based directory, e.g., one used for HR or payroll purposes, may be more suitable for Web-use management purposes. If this is the case, it may identify employees differently than the access control directory. For example, it may use employee numbers or social security numbers to identify employees. In such cases, the customer may need to insert another field in the "HR/Payroll" directory to duplicate the user IDs found in the access control directory.

Ensuring Compatibility Between the Product and the Directory. As mentioned above, in some cases for grouping purposes, the information in the directory will already be appropriate. That is, the directory will contain some form of user ID, and it may contain columns denoting the group to which each employee belongs and each group's progressively higher organizational levels. If it does not, you can easily correct the situation by inserting additional columns to fully accommodate the necessary information.

Implementing the Active Directory Import Process. Some or all of the employee-related information discussed above and illustrated in Figure 1 can be imported into the product on an automatic or manual basis. In both cases, the Active Directory Setup wizard must first be used to configure your domain(s).

NOTE: A manual import will occur immediately upon clicking the link, placing the IDs into the groupings you specify first using the Active Directory Setup wizard. During that setup, you have the option to place any IDs into Ungrouped IDs. An automatic import will obtain groups and IDs on a scheduled basis. If you chose to manage your users outside the product, i.e., at the directory source, all groups and IDs will be updated according to your directory source. However, if you chose to manage users inside the product, only new IDs will be imported.

Using the Product's Active Directory Setup Wizard. In order to import Active Directory groups and IDs, you must first use the Active Directory Setup wizard to configure your domain(s). After configuration is complete, groups and IDs can be imported automatically into the product on a scheduled basis every 24 hours. Each time this occurs, the entire groups and IDs tree in the product will be rebuilt according to the hierarchical structure reflected in your specified Active Directory configuration if you chose to manage your users outside the product. However, if you chose to manage them inside the product, only new users will be imported. For step-by-step instructions for the wizard, see Import Users From Active Directory.

Manual Import. When a manual import occurs, IDs will be imported into the product immediately. The process will import groups and IDs per your specified configuration. If you chose to manage your users outside the product, all groups and IDs will be updated according to the directory source. However, if you chose to manage users inside the product, only new IDs will be imported.

Semiautomatic Grouping Using a "Text File" Method

General. If Active Directory is not available, groups and IDs information can be imported from any database or spreadsheet that contains the proper data, i.e., user ID and organizational assignment information. Personnel records in HR or payroll records in Finance may suffice. In brief, the data is exported from the source to an "import file" in the Wavecrest product.

Methodology for Exporting the Data Into the Import File. Listed below are the basic steps for creating an import file and exporting the required data into it. The more complex steps are discussed in more detail later.

1. Select your data source (e.g., spreadsheet, database, or table).
2. Ensure that the data source contains–as a minimum–a column for user ID, a column to accommodate an optional full name for each ID, and at least one parent column. If the parents have higher-level parents, additional columns will be needed. The columns do not need to be in any particular left-to-right order.
3. Export the source data to the Wavecrest product as an Excel spreadsheet. Each row (record) in the spreadsheet will represent one user ID.
4. Save the spreadsheet as text to a file named …\wc\cf\db\import.cfg for Cyfin or ...\wc\cyblock\db\import.cfg for CyBlock. This is the import file.
5. Confirm that the file has been imported properly and contains the correct items of information. Also note the type of delimiter being used to separate the data items. The delimiter may be a comma or space, for example.
6. Restart the product. Once this is done, the product's server automatically duplicates the imported group structure and assigns the IDs to the correct groups.

A Typical Import File. A typical import file will consist of the following columns:

- **ID**. ID is the login name to a proxy server, firewall, caching appliance, etc. It can also be an IP address or a domain name.
- **Full Name (Optional)**. This is the ID's full name, spelled out. This field/column is required, but if full names are not to be used, it can be left empty (that is, no character spaces). See examples below. If this field is used, then all reports will display the full name alongside the user's IP address or login name.
- **Group Name**. This is the name of the group (e.g., department) to which the ID is assigned, e.g., Sales, Engineering, or Accounting.
- **Parent Groups 2, 3, and 4 (Optional)**. These columns will contain the names of increasingly higher-level groups, if applicable.

NOTE: These particular import file requirements are essentially the same as those discussed earlier for Active Directory.

Configuring Wavecrest Products to Work With the Import File. After the import file is created, the administrator needs to ensure that the product engine is configured to work with the data in the file. That is, the administrator needs to "tell" the product (a) which piece of user information is in which column and (b) the type of delimiter being used. This is done in the **User Management - Import Users - Text File** screen. The process consists of a few simple data entries. For detailed instructions, see Import Users From Text File.

Examples of Import Files. Some examples of import files are shown below. Although we use the vertical pipe character as the delimiter in all of these examples, the delimiter can also be other acceptable characters, e.g., comma or space.

1. The following example shows a typical group import file with login names, full names, and group names.

smithj|Smith, Joe|Engineering
doej|Doe, John|Accounting
wilsona|Wilson, Alvarez|Sales

2. The following example is Microsoft Proxy specific. Assume your organization has Microsoft domains set up for each department. For this example, assume there are three departments, each with its own Microsoft domain. The Sales Department's domain is SALES, the Accounting Department's domain is ACCT, and the Engineering Department's domain is ENG. The following group import file would result in separate reports for each department or domain.

SALES*||Sales Department
ACCT*||Accounting Department
ENG*||Engineering Department

3. The following example illustrates a case in which full names are not used. Notice the two delimiters with nothing in between. This tells the product that there is no full name.

smithj||Engineering
doej||Accounting
wilsona||Sales

4. The following example fits an organization that does not authenticate users at a proxy server or a firewall, but has fixed IP addresses and uses full names.

123.10.3.8|Meyers, Peter|Sales,New York
123.10.3.9|Ellen, Susan|Sales,California
9.2.3.8|Bene, Jorge|Sales,Brazil

5. The following example fits an organization that subclasses an IP address range for a region or district. In this case, full names are not used. Notice the two delimiters; this tells the product that there is no full name.

34.5.224.*||Washington Elementary School
34.5.225.*||Adams Middle School
34.5.226.*||Grover High School

6. The following example demonstrates how to set up a group import file for an organization that uses domain names for its workstations. In this case full names are not used. An example of full domains could be joe.eng.NY.company.com.

*.eng.NY.company.com||Engineering-New York
*.eng.CA.company.com||Engineering-California
*.drafting.company.com||Drafting-Corporate Headquarters

7. The following example could be used for an organization that uses a department number as part of a login name. For example, the Sales Department has a department number of 2001, and the Marketing Department has a department number of 694. An example of login names for the Sales Department could be joe2001 and jim2001, and the Marketing Department could have users sue694 and alice694.

*2001||Sales Department
*694||Marketing Department

8. Suppose an Internet Service Provider (ISP) manages Internet activity for many small businesses. The following example demonstrates an ISP configuration for delivering a grouped-report to each business.

45.23.190.*||Real Secure Systems
*.hotpeppers.com||Hot Peppers and More
123.45.48.*||Jacobs Manufacturing
88.1.2.*||The Graphic Arts Center
*.vbooks.com||Virtual Books, Inc.

Summary. As indicated earlier, once the import file has been built and the administrator restarts the Wavecrest product server, it finds the file automatically and begins to use its information. As a result, the server automatically duplicates the imported group structure and assigns the IDs to the correct groups.

Manual Management of Groups and IDs

General. Manual management of groups and IDs involves manually creating, moving, renaming, deleting, and updating groups and IDs.

In this case the product administrator first configures a hierarchical organizational tree in the product. This is done via the User Management menu, which contains the Edit Users menu items Add, Delete, and Move. Typically, although not necessary, the groups in a hierarchical structure consist of the various departments and subdepartments within a company.

Configure and Populate the Groups. Once the design is complete, the administrator can configure it in the product and assign users to the various groups, e.g., departments. He or she can perform both of these tasks in the **User Management** screens by following the instructions for data entry. Once this is done, the administrator (or other authorized individual) can then request reports.

Using a (High-Level) Site Analysis Report to Import IDs

General. Wavecrest's products can run high-level reports such as Site Analysis without previously inputting the IDs of the covered users. This approach automatically inputs IDs of users that were active during the specified time frame of the requested report. This approach has the added benefit of producing a very useful high-level screening report while simultaneously entering applicable IDs into the product. All users imported in this manner are placed into Ungrouped IDs.

NOTE: To run a User Audit Detail report on a specific ID or IP address, the covered user's ID must already be present within the product.

Methodology. Using the **Reports - Manager** screen, create and run a manual Site Analysis report. As mentioned above, this approach automatically inputs IDs of users that were active during the specified time frame of the requested report. The imported IDs will then remain in the product for subsequent use even after the Site Analysis report is closed.

NOTE: If IDs have been previously inputted, running the Site Analysis report will only bring in "new" IDs. These will be placed in the Ungrouped IDs group from where they can be moved to other defined groups if they exist.

Appendix B - Report Descriptions

Recommended Reports

The reports in this group include Site Analysis and User Audit Detail which are described later in this appendix.

High-Level Summary Reports

Category Audit Summary Report

Features. This report provides a synopsis of users' Web activity in a single category that you select. It lists all visited Web sites (domains), and the time online, bytes read, and number of visits for each, but does not list individual users. A hyperlink to each domain is provided.

Benefits. This report is very useful for a quick-look determination of whether or not Web-access abuse is taking place in a particular category, e.g., Pornography.

Cloud Services Summary Report

Features. This report shows the Web activity of users accessing cloud services. By user, it indicates the time online and number of visits to sites in the Audio Streaming, Cloud Infrastructure, Cloud Storage, Collaboration, CRM, Development, File Sharing, HR, Personal E-Mail, Video Streaming, and VoIP Services categories. Information is presented by category, group, and user. A hyperlink to each user is provided to allow management to further review the sites that were visited.

Benefits. This report can be used to identify cloud service usage patterns to enable new cloud services, better manage cloud subscriptions, and highlight anomalous activity. It can be used to reduce the risk posed by both approved and unapproved cloud services, enabling the safe and cost-effective implementation of cloud services.

Denied Requests Report

Features. By category, this report shows which users were denied access to Web sites or a page on a Web site. Individual users are identified, but specific URLs are not. Each denied request is displayed in the category requested. Denied requests for a Web page can signify the user may not be authorized to receive the page, the page may not have been found by the Web server, or the page may have been blocked for access.

Benefits. If you have Web filtering enabled, this report can verify that it is working. It can also be used to identify users who may be engaging in excessive attempts to visit inappropriate or unauthorized sites. This report is also a useful supplementary tool for individual user audits.

Legal Liability Report

Features. This report shows Web activity that could lead to legal liability. By user, it indicates the time online and number of visits to sites in the Anonymous/Public Proxy, Cults/Occults, Fantasy Sports, Gambling, Hate/Crime, Illegal Drugs, Malware, and Pornography categories. Information is presented by category, group, user, and user within the category. Individual sites are not separately identified.

Benefits. This tightly focused report facilitates analyses, investigations, and audits related to actual or potential legal liability issues. Results can be used to prompt further investigation or trigger immediate corrective action.

Site Analysis Report

Features. This report depicts Web site visits by user, group, or Enterprise from the following different perspectives. Time online percentage and time online are also provided.

- Total visits by classification (Acceptable, Unacceptable, Neutral)

- Total visits by category (Shopping, Pornography, etc.)
- Total visits by group
- Total visits by user
- Total visits by user, per category

NOTE: Individual sites are not identified in this report.

Benefits. The Site Analysis report looks at the same visits from different perspectives, such as acceptability, category volume, and user visits within categories. It can be used by all levels of management and by network administrators to perform audits and analyses of activity in either broad or focused areas.

Site Audit Summary Report

Features. This report lists the top groups and users who visited a particular site. The report can be run for more than one site and shows the total time online and number of visits made by the user, as well as the time online percentage and total visits by hourly activity. A hyperlink to each user is provided to allow management to further review the sites that were visited.

Benefits. This report can be used by administrators to get a quick, summarized look at Internet activity by Web site. It lists the users with the highest volume of activity.

Time Online Analysis Report

Features. The report shows the amount of time spent accessing Web sites by user, group, or Enterprise from the following different perspectives. The total number of visits is also provided.

- Total time online by classification (Acceptable, Unacceptable, Neutral)
- Total time online by category (Video Streaming, Sports, etc.)
- Total time online by group
- Total time online by user
- Total time online by user, per category
- Time online by hour

NOTE: Individual sites are not identified in this report.

Benefits. The report highlights the top users who spent the most time online during the reporting period and can prompt further investigation. Managers and IT administrators can quickly see which categories had the most volume of activity and address any potential issues, such as productivity loss, bandwidth slowdowns, and policy noncompliance.

Top Users Report

Features. This report lists the most active users in terms of time online, visits, denied hits, hits, and bytes read.

Benefits. This report can be used by administrators to get a quick, summarized look at Internet activity on the network. It lists the users with the highest volume of activity, be it acceptable or otherwise. This report is an excellent screening tool and can be used to prompt drilldown and further investigation.

Top Web Sites Report

Features. This report shows all visited Web sites (domains), and the category, time online, bytes read, and number of visits for each. The list is sorted in descending order by time online which enables quick determination of site "popularity." Individual user IDs are not shown on this report, but hyperlinks to all visited Web sites are provided to facilitate further analysis.

Benefits. This report highlights the Web sites that were most visited during the reporting period. If these visits are inappropriate, you can use this information to prompt deeper investigation. You may also

consider including the offending sites in your blocking regimen if you have one of our Web security products.

Unacceptable Visits Report

Features. The report depicts Web-use activity only within categories classified as "Unacceptable." By category, it shows the total time online and number of visits made by individual users. Users are identified, but individual sites are not. The report also summarizes unacceptable visits by top categories, groups, users, and hourly activity.

Benefits. Managers and administrators can quickly evaluate and see patterns of unacceptable activity by user and category. The latter can be done by individual category or at a higher level by a consolidation of all unacceptable categories. If excessive unacceptable activity is indicated, the reviewer can quickly drill down to other reports for further detail.

User Audit Summary Report

Features. This report lists all the Web sites visited by a single user during the reporting period. For each listed site, the report indicates the category, time online, bytes read, and number of visits made to it. A hyperlink to each site is provided to facilitate further review by management.

Benefits. Management is provided with reliable information to use in analyzing, evaluating, or investigating an individual user's Web activity.

Audit Detail Reports

Category Audit Detail Report

Features. This report provides a detailed analysis of users' Web activity in a particular category that you select, e.g., Pornography. All URLs are listed for each user who visited that category. The report also provides the time online percentage, total visits, and total time online for the top groups, users, and hourly activity in this category.

Benefits. This report is very useful for identifying the most active users and the most heavily visited sites and pages in a selected category. This makes it an excellent tool for conducting detailed audits and investigations of possible misuse of Web-access resources.

Cloud Services Detail Report

Features. This report shows the specific URLs of cloud services by user, that is, visits to only the Audio Streaming, Cloud Infrastructure, Cloud Storage, Collaboration, CRM, Development, File Sharing, HR, Personal E-Mail, Video Streaming, and VoIP Services categories.

Benefits. Management has a complete and concise view of every cloud service URL the user has clicked. This information can be used for cloud usage audits, identifying the most active users and the most heavily visited sites.

Denied Requests Report

Features. This report shows the specific URLs to which users were denied access by user. Each request is displayed in the category requested. Denied requests for a Web page can signify the user may not be authorized to receive the page, the page may not have been found by the Web server, or the page may have been blocked for access.

Benefits. If you have Web filtering enabled, this report can verify that it is working. It also indicates the number and type of blocked requests, i.e., Denied, and is a very useful supplementary tool for individual user audits.

Legal Liability Detail Report

Features. This report shows the specific URLs of legal liability Web activity by user, that is, visits to only the Anonymous/Public Proxy, Cults/Occults, Fantasy Sports, Gambling, Hate/Crime, Illegal Drugs, Malware, and Pornography categories that pose a legal liability risk.

Benefits. The report provides only legal liability Web use. This means that smaller, more focused reports are available to facilitate analyses, investigations, and audits related to legal liability issues.

Search Terms Audit Detail Report

Features. This report shows search terms that users entered on popular search sites such as Google. For each search term, it shows the IP address, user, date/time, and search engine.

Benefits. This report indicates the number of search terms entered during the reporting period and can be used as a tool to aid in forensic investigations.

Site Audit Detail Report

Features. This report focuses on Web activity associated with one or more Web sites. Every hit or visit made to the specified URLs is listed separately for all users. Hits or visits are listed chronologically, and information included for each hit or visit consists of the IP address, user, and full URL. The report also provides the time online percentage, total visits, and total time online for the top groups, users, and hourly activity.

Benefits. Management has a complete yet concise view of all users that visited the specified Web sites and the resultant activity (hits or visits). This information can be used for personnel appraisal purposes, usage audits, etc.

User Audit Detail Report

Features. This very detailed report focuses on a single user. Every visit made by the user is listed separately in chronological order. Information for each visit consists of the site's category and full URL. Each URL is hyperlinked so the site or page can be quickly accessed for review if desired. A summary total of visits, time online, and bytes read are also provided by category and hour activity.

Benefits. Management has a concise but complete view of every URL the user has clicked. This information can be used for personnel appraisal purposes, incident investigations, usage audits, etc.

IT Reports

Network Information Report

Features. This report depicts the total hits, trend in bytes, and total bytes by acceptability classification, category, group, IP address, and hourly activity. No individual users or sites are identified in this report.

Benefits. This report is a powerful tool for network administrators. It serves as a valuable aid for managing and controlling bandwidth usage. By not showing users, it keeps the focus on bandwidth usage via hits, trend in bytes, and bytes, making it easier for administrators to quickly identify potential network performance problems.

Site Analysis Bandwidth Report

Features. Similar in structure to the Site Analysis report, this report focuses on bandwidth consumption instead of visits. It breaks down bandwidth usage by acceptability classification, category, group, user, and user within each category, showing the trend in bytes and total bytes.

Benefits. This report provides IT personnel with a comprehensive, categorized picture of how and when Web access is being used, and it does so while identifying the most active users in each category. This data is very helpful for managing bandwidth usage and advising management on corrective measures.

Top Bandwidth Sites Report

Features. This report shows the top bandwidth-consuming site visits made by the selected group. Each site's category is shown with the byte consumption for the site. The list is sorted in descending order by bandwidth consumption, enabling quick determination of the category and domain affecting bandwidth. Individual users are not shown on this report. Hyperlinks to all visited Web sites are provided to facilitate further analysis.

Benefits. This report quickly identifies the Web sites that consumed the most bandwidth in your network during the reporting period. If the consumption is unwarranted, you can use this information to prompt deeper investigation, or you can include the offending sites in your blocking regimen if you have one of our Web security products.

Forensic Reports

The reports in this group are audit detail reports that could be of interest to corporate IT forensic personnel, law enforcement agencies, anyone in the legal community, and forensic criminal investigators. These reports include Denied Requests Detail, Legal Liability Detail, Search Terms Audit Detail, and User Audit Detail which were described earlier in this appendix.

Cloud Services Reports

The reports in this group show employee Web use of cloud services including the Web activity of your remote employees, i.e., cloud users, in a Hybrid deployment. Cloud service Web activity includes visits to sites in the Audio Streaming, Cloud Infrastructure, Cloud Storage, Collaboration, CRM, Development, File Sharing, HR, Personal E-Mail, Video Streaming, and VoIP Services categories. The reports include Cloud Services Detail and Cloud Services Summary which were described above.

Appendix C - OtherWise Program & Policy

The OtherWise Program - What is It?

OtherWise is a voluntary, confidential, and free program under which we partner one-on-one with participating customers to steadily improve the quality, coverage, and usability of Cyfin or CyBlock. The goal is to maximize the number and percentage of Web sites that the software identifies and categorizes.

Overview of the OtherWise Process - How Does OtherWise Work?

On a voluntary basis, participating customers enable the product to automatically send noncategorized site data to Wavecrest headquarters on a weekly basis. (Customers can select the day of the week and the hour of the day that the data will be processed.) Our personnel then research, identify, and categorize the most popular of the unidentified sites and update the Wavecrest URL List (categorization database) accordingly. (We update the list daily.) After the customer downloads the daily list update, the sites in question will be identified and categorized.

NOTE: No user names are included in the data sent to Wavecrest.

Dealing with Intranet and Extranet Sites

We occasionally find that many of the URLs included in the OtherWise data represent the customer's internal intranet (and possibly extranet) sites. Because we cannot access these sites, we cannot research and categorize them. Consequently, we may return a list of these particular sites to the participating customer and suggest that they enter them into one or more custom categories which they can create themselves. Cyfin and CyBlock permit the establishment of custom categories which customers can use to track Web use activity involving sites that are of particular or unique interest to them only; intranet sites are the most common of such sites.

Results

Customers that use our highly personalized OtherWise service have reported significant reductions in the number and percentage of unidentified Web visits.

Confidentiality

Wavecrest Computing is fully committed and obligated to protecting the privacy and confidentiality of our customers' information especially information that pertains to or identifies individual employees or other users whose data flows through our systems. Our commitment and assurance are documented and enforced in several ways. One of those is close adherence to the provisions of Section A.15 of our End User Sales Agreement, quoted below:

> *"Only authorized Company employees with a need to know use or handle information collected from individual customers. Client records are regarded as confidential and will not be divulged to any third party unless legally required to do so by the appropriate authorities. The Company retains no client records produced by the product; the only records retained are those pertaining to the sale itself and contact information. Wavecrest Computing will not sell, share, or rent your personal information to any third party or use your e-mail address for unsolicited mail. Any emails sent by this Company to Customer will only be in connection with the provision of agreed services and products. We constantly review our systems and data handling processes to ensure the privacy and confidentiality of Customers' information."*

Equally if not more important, by virtue of our being a preapproved provider of software to the U.S. Government (via General Services Administration (GSA) contract GS-35F-0212L), we are subject to the provisions of a federal statute known as The Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31, 1974). This statute establishes a Code of Fair Information Practice that governs the

collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies and may be available to Government contractors. Under penalty of law, the Privacy Act prohibits the unauthorized disclosure of information from a system of records absent the written consent of the subject individual.

The confidentiality provisions of the Privacy Act and our End User Sales Agreement are included in Wavecrest administrative and personnel policies. Our staff is oriented and trained in these policies and the processes that are designed to implement and enforce them. Willful violation of these policies is cause for immediate termination and–depending on the circumstances–possible criminal or civil legal action. In our history, this has never been necessary, and no customer has ever informed us of any issues in this regard.

Your Part in the OtherWise Program

If you choose to participate, it's easy. Simply enable OtherWise on the **Settings - Reports - OtherWise** screen. The product will then send us noncategorized site data on a weekly basis automatically. (You can accept the default day/time the report will run, or you can set your own weekly schedule.) As mentioned above, we may return a list of local/intranet sites that we were unable to access for categorization purposes. If you wish to track your users' activity to these sites, you can enter them into one or more custom categories, and the traffic will be identified in subsequent reports.

Wavecrest**CyBlock**®Appliance

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