WAVECREST
COMPUTING

Cyfin® Reporter

User Manual for Version 8.2.x

www.wavecrest.net

Table of Contents

Introduction

Welcome to the Administrative Manual for Cyfin Reporter. Cyfin Reporter is a scalable log file analyzer that reads your Web-use logfiles and turns them into easy-to-read reports on employee Web use. This manual covers detailed instructions for all of Cyfin Reporter 's features. It is up to you (the administrator) whether to use the basic or advanced functionality of Cyfin's features.

If you have an earlier version of the product, it is recommended that you update to the latest version. However, if you are not quite ready to update, and depending on how long ago it has been since your last update, many instructions covered in this manual may still apply to your version of the product.

Structure and Use

The manual is structured in the order that is recommended for setting up the features. However, you can always start with using the basic setup of the product covered in the Get Started section of the manual and later use the more advanced features when you are ready. With the exception of a few sections that have a required setup screen, 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. Some of the key things you will find instructions for in this manual are how to:

- Run summarized and detailed reports
- Classify categories based on your company's Internet usage policy
- Set abuse thresholds
- Increase reporting speed with the optional internal database.

You will find that there are numbered step-by-step instructions with screen shots for each process. The instructions will guide you through the menu and the screens. You will find menu options listed like the example below:

Advanced Settings – Groups and IDs

Throughout the manual, you will also see a number of "Notes" and "Cautions" imbedded with the instructions. Pay close attention to these, as they usually contain important exceptions to the instructions. "Cautions" will apply to everyone, but "Notes" may or may not apply depending on your network and/or how you plan to use the features.

Organization for this Manual

Section 1: Get Started

This section covers all the basic setup steps you need to complete to get the product up and running. This includes installing the product, configuring your logfiles, downloading the URL list, and running reports.

Section 2: Groups and IDs

In this section, you will learn about the product's core grouping structure and the several ways that you can use grouping. This includes importing Groups and IDs from Active Directory or a text file, setting up scheduled imports, and manually adding your Groups and IDs. 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.

Section 3: Data Management

The reporting feature of this product is dependent on the logfiles. This section covers instructions on viewing your logfiles and managing the product's Data Manager. The Data Manager compresses logfiles allowing for faster reporting and long-term storage. The data can also be exported to other applications.

Section 4: Web Policy Support

Wavecrest's products were built with customizable Web policy support settings to fit any organization's needs. This section will walk you through classifying categories, creating custom categories, and setting abuse threshold policies.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

Section 5: Reporting

There are several, customizable reports available in the product and the option to use Interactive or Read-only reports. Interactive reports allow you to drill down from a higher level report to get more detailed Web-use data. This section shows you how to create high and low-level reports, schedule reports to run automatically, use interactive reporting, the Dashboard and set report preferences.

Section 6: Advanced Configuration

For those organizations that require an array configuration, this section gives instructions for how to set this up and maintain all product installations within your array.

Section 7: Administrative Features

This section contains instructions on various other administrative features, including how to create administrator and operator accounts, scheduling the download of the URL list, and downloading product updates.

Section 8: Other Features

This section briefly discusses some of the other product screens that do not need a lot of instruction, but can be helpful. These include the job queue and help screens.

Help and Contact Information

? Additional help for the product screens is also available in the product. Just click on this icon in the upper right hand corner of the interface. A window will then pop up with information about the screen and instructions on how to use it.

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 ex. 4 (U.S. and Canada).
Direct	321-953-5351 ex. 4
International	001-321-953-5351 ex. 4 (outside U.S. and Canada)
Email	
Technical Support	support@wavecrest.net
General Info	info@wavecrest.net
User Forum	
Forum	http://forum.wavecrest.net

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

Technical Considerations

1. **Will you be using an array configuration?**
   If you plan to set up an array configuration in your network, then you need to do this first before setting up any other features in your product. An array configuration allows you to manage several product installations from one "primary" product that you designate. Once the array is configured, then you will only need to configure product settings at the "primary" server. You will find the setup instructions for an array in Section 6.1 of the manual.

2. **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 Required Setup for Groups and IDs in Section 2.

3. **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's 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 Section 4.

4. **Will you run reports from raw logs or the Data Manager?**
   There are several advantages to importing the raw log data into the Data Manager. The Data Manager compresses the logfile data, which increases the reporting speed dramatically, allows you to export the data in .xml or .csv formats for use in other applications, and allows you to use the Dashboard and Interactive reporting. To learn more about the Data Manager and for instructions on how to enable it, see Section 3.

5. **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. These ratings will appear in your Web-use reports, making it easy to quickly identify when Web abuse has occurred. For instructions on setting classification ratings, see Section 4.

6. **Will you incorporate abuse thresholding?**
   This is another feature that allows you to quickly identify Web abuse in reports. Abuse thresholding allows you to set the number of "allowed visits" to each category by the individual user, group or entire enterprise. If that threshold is ever exceeded, this will be displayed via a red bar in the reports. To learn more about abuse thresholding, see Section 4.

7. **How will you distribute reports?**
   Reports can either be run manually on an ad hoc basis or can be scheduled to run daily, weekly, monthly or quarterly. Scheduled reports can either be emailed out to each groups' recipient (which you would have configured in Groups and IDs), emailed to someone you specify, or saved to a directory where managers can retrieve the report. See Section 5 on creating reports. If you plan for managers to log in and create their own reports, see the instructions for creating operator access accounts in Section 7.1.

8. **Will you create administrator and operator access accounts?**
   Administrators have full access to the product while operators are limited to only reporting. Operator 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 operator accounts, see Section 7.1.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1.0 Get Started

This section gives instructions for getting the product up and running. It involves the following simple steps:

- **Download and Install the Product** - A wizard will guide you through the process.
- **Download the URL List** - Complete this step so that you can run reports.
- **Change the Default Password** - Change the Administrator password.
- **Set up Memory Settings** - Select the amount of memory needed.
- **Configure Logfiles** - Specify what type of logfiles you have and where they are stored.
- **Set up Administrator Email** - Receive reports and status updates via email.
- **Create and Run a Site Analysis Report** - Create a high-level summary report; one that is useful for identifying suspect areas.

Be sure to complete these steps before moving on to any other sections in this manual. Many of these steps are mandatory to get the product up and running properly.

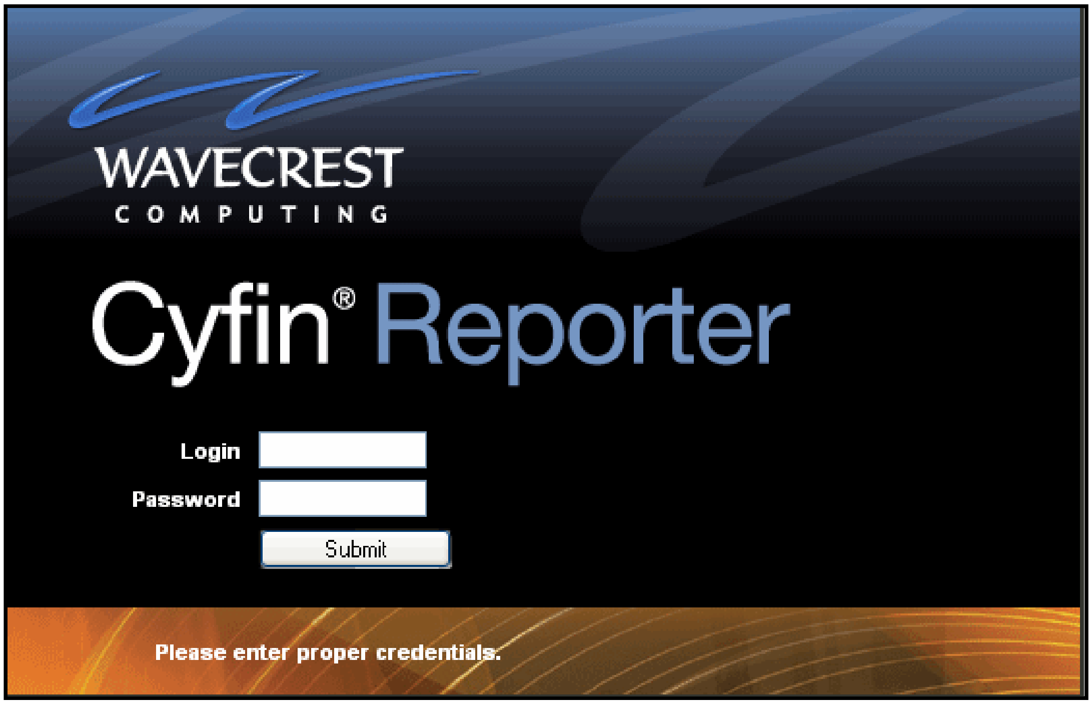
CAUTION: *If you plan on having an array configuration, skip this section and instead go to Section 6.1 on Advanced Configuration.*

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1.1 Download and Install the Product

In this step you will download and start a wizard to install the product.

1. Double-click on the executable file and simply follow the wizard's onscreen instructions.
2. After a few clicks you will find yourself at the login screen shown below.



Please enter proper credentials.

3. Log into the product using the following default credentials:
   LOGIN: admin
   PASSWORD: password

NOTE: *If the login screen does not appear, bring it up by going to* ***Start - Programs - Cyfin - Browser Interface****.*

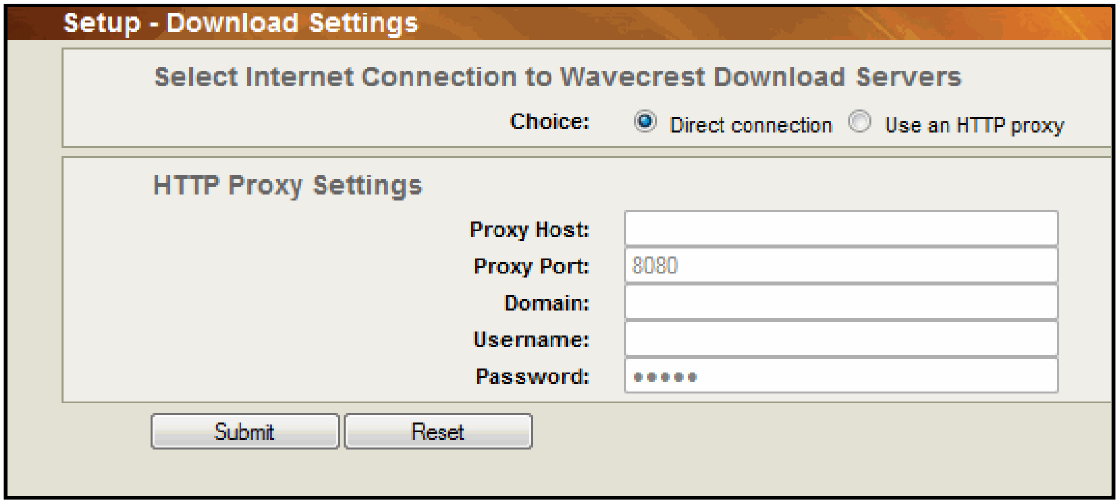
© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1.2 Download the URL List

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 your Internet traffic goes through a proxy, begin with Step 1, as you will need to configure your proxy information first. If Internet traffic does not go through a proxy, then you can skip to Step 3 for downloading the list.

1. If your Internet traffic goes through a proxy, go to the **Setup – Download Settings** screen to configure your proxy information. This will ensure that you can download the list, product updates, and also receive product news.



Setup - Download Settings

Select Internet Connection to Wavecrest Download Servers

Choice: ● Direct connection ○ Use an HTTP proxy

HTTP Proxy Settings

Proxy Host:

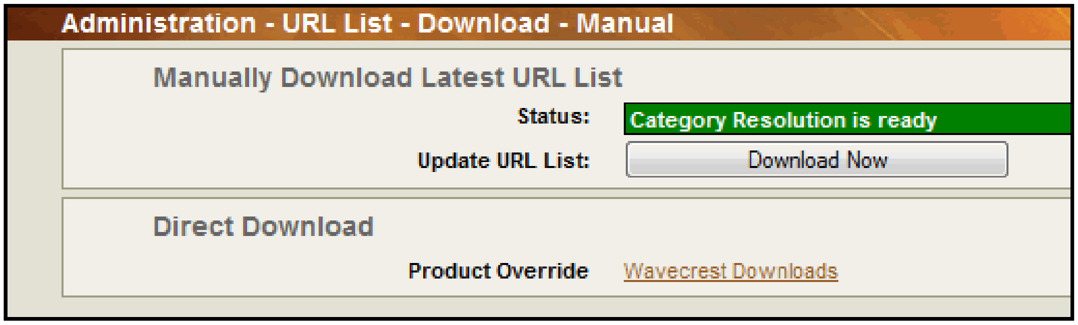
Proxy Port: 8080

Domain:

Username:

Password: •••••

2. Fill in the text-entry boxes with the correct authentication credentials, and then click **Submit**.
3. To download the list, go to the **Administration - URL List** screen and click on the **Manual** link.



Administration - URL List - Download - Manual

Manually Download Latest URL List

Status: Category Resolution is ready

Update URL List:

Direct Download

Product Override Wavecrest Downloads

4. Next, click on the **Download Now** button. You should see a progress meter screen pop up. When it indicates that the download is complete, you can close the window.

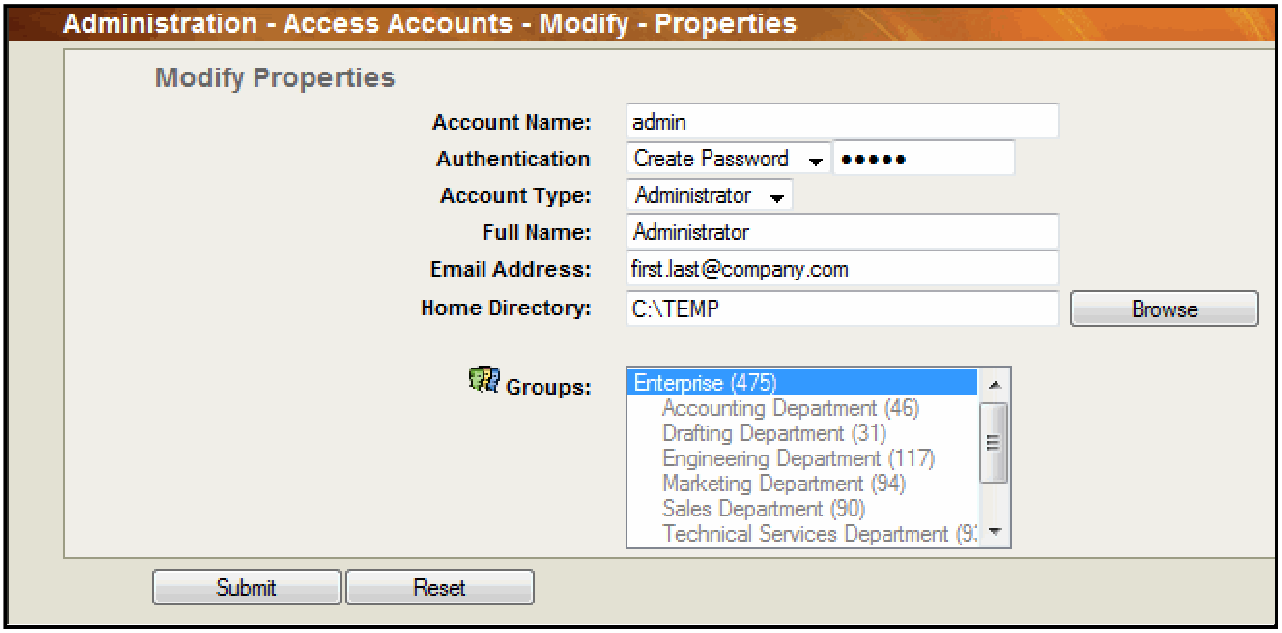
NOTE: *The Product Override link should only be used in the event that the URL list download from the product is unsuccessful. This link will take you to a Web page where you will find the URL list download and instructions for downloading from the site.*

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1.3 Change the Default Password

Once you have logged into the product and downloaded the URL list, you will want to change the default password.

1. Go to **Administration - Access Accounts** and click on the **Modify** link.
2. Click on the **admin(Administrator)** link.



Administration - Access Accounts - Modify - Properties

Modify Properties

Account Name: admin

Authentication: Create Password ●●●●●

Account Type: Administrator

Full Name: Administrator

Email Address: first.last@company.com

Home Directory: C:\TEMP

Groups:

- Enterprise (475)
- Accounting Department (46)
- Drafting Department (31)
- Engineering Department (117)
- Marketing Department (94)
- Sales Department (90)
- Technical Services Department (9:

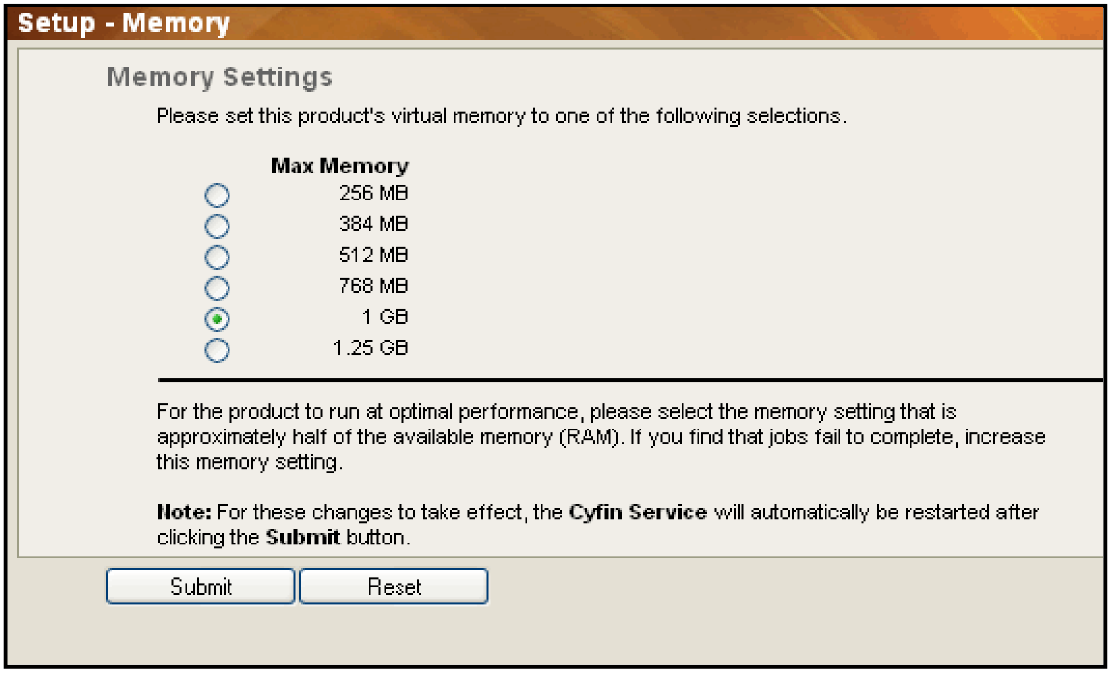
3. Type in your new password in the **Password** field.
4. At this time, you can also change the **Full Name**, **Email Address**, and **Home Directory**. Reports will be sent to the **Email Address** specified and saved to the **Home Directory** specified on this screen.
5. When you have finished making your changes, click **Submit**.

1.4 Set up Memory Settings

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 and recommended minimum is 256 MB RAM. If you start to meet your memory threshold, the product will notify you to increase your memory setting.

***NOTE:** For optimal performance, we recommend that you choose the setting that is approximately half of your available memory (RAM).*

1. To set your memory, go to **Setup** on the menu and then click the **Memory** link.



Setup - Memory

Memory Settings

Please set this product's virtual memory to one of the following selections.

	Max Memory
○	256 MB
○	384 MB
○	512 MB
○	768 MB
●	1 GB
○	1.25 GB

For the product to run at optimal performance, please select the memory setting that is approximately half of the available memory (RAM). If you find that jobs fail to complete, increase this memory setting.

Note: For these changes to take effect, the **Cyfin Service** will automatically be restarted after clicking the **Submit** button.

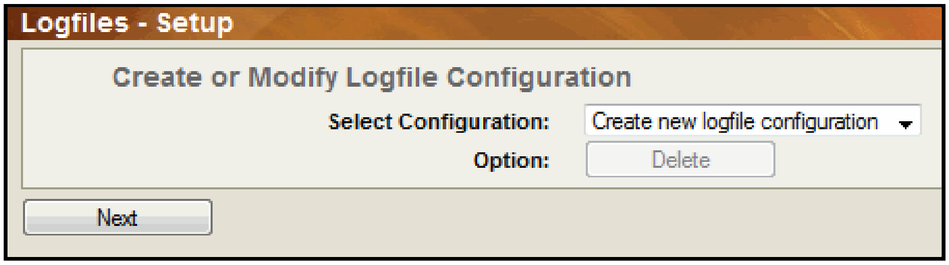
2. Check the radio button (in the "**Choice**" column) that corresponds to the appropriate amount of memory to be used, keeping in mind your available RAM.
3. Click **Submit** to apply changes, or click **Reset** to reload previous values.
4. After you click Submit, you will receive a popup asking whether you would like to restart the service. Your memory setting changes will not take affect until you restart the service.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1.5 Configure Logfiles

This process will configure the product to read your logfiles. It is from these logfiles that the product generates easy-to-read reports.

1. Begin by going to the **Logfiles - Setup** screen.

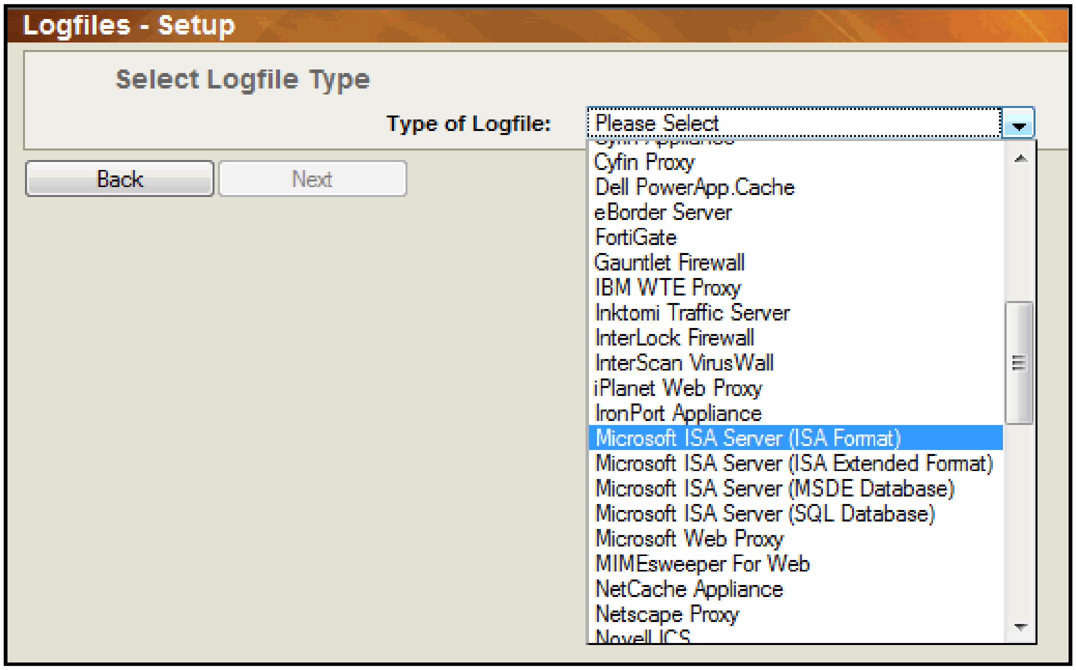


Logfiles - Setup

Create or Modify Logfile Configuration

Select Configuration: Create new logfile configuration

2. Leave the default choice *Create new logfile configuration* in the drop down box and simply click **Next**.



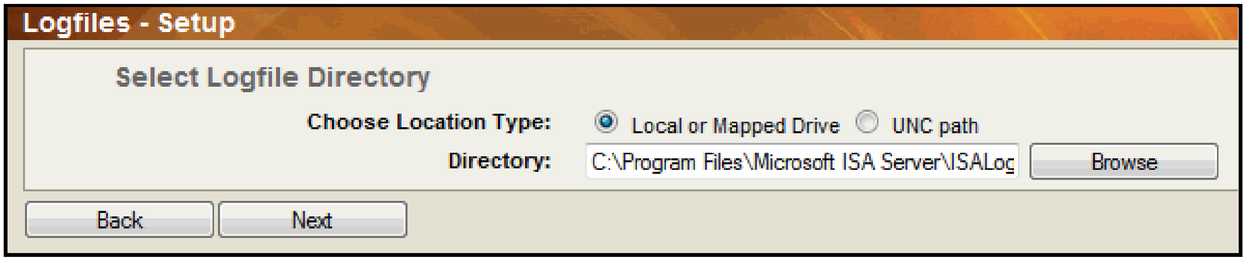
Logfiles - Setup

Select Logfile Type

Type of Logfile: Please Select

3. Use the pull down menu and select the **Type of Logfile** for your server.
   NOTE: *If you make a mistake, the product will realize it in a couple of steps and redirect you back to try again.*

4. When you have made your choice, click **Next**.



Logfiles - Setup

Select Logfile Directory

Choose Location Type: ● Local or Mapped Drive ○ UNC path

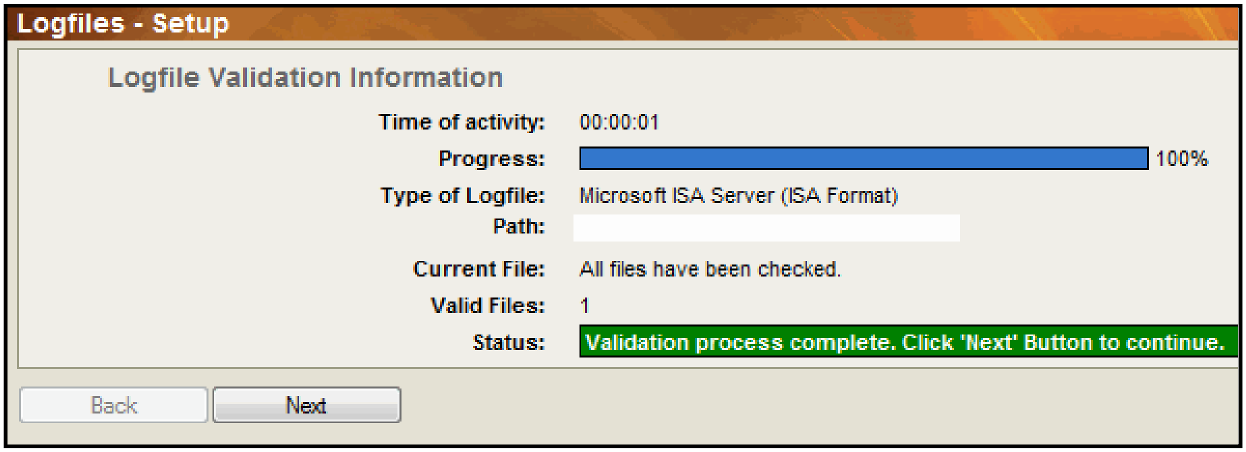
Directory: C:\Program Files\Microsoft ISA Server\ISALog

5. In this step you need to direct the product to where your logfiles are located.
   - If the logfiles are local to the machine, choose the **Local** radio button and then **Browse** to the folder containing them.
   - If the logfiles are shared elsewhere across the network, choose the **UNC Path** radio button. By doing so, the **Browse** button will be grayed out, and you need to type in the full network path to your logfiles.

6. After configuring the log file directory, click **Next.**

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

7. The product will locate and validate your logfiles in the next step. You should see a progress meter and a message indicating success on this screen.



Logfiles - Setup

Logfile Validation Information

Time of activity: 00:00:01

Progress: 100%

Type of Logfile: Microsoft ISA Server (ISA Format)

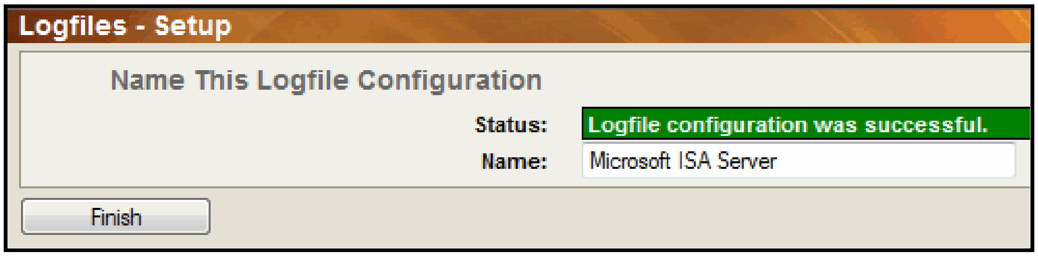
Path:

Current File: All files have been checked.

Valid Files: 1

Status: Validation process complete. Click 'Next' Button to continue.

8. When you see the green colored success message, click **Next**.
*NOTE: If there was a problem finding logfiles or validating them, an error message will appear with helpful information, and direct you to click the **Back** button to make a change.*



Logfiles - Setup

Name This Logfile Configuration

Status: Logfile configuration was successful.

Name: Microsoft ISA Server

9. When valid logfiles have been configured, the next step is to name the configuration. This is helpful for identification purposes, especially if you add more log file configurations later.

10. After typing in a name for your new log file configuration, click **Finish**.

    *NOTE: If you don't name the configuration and simply click **Finish**, the product will name the configuration the same as your logfile type.*

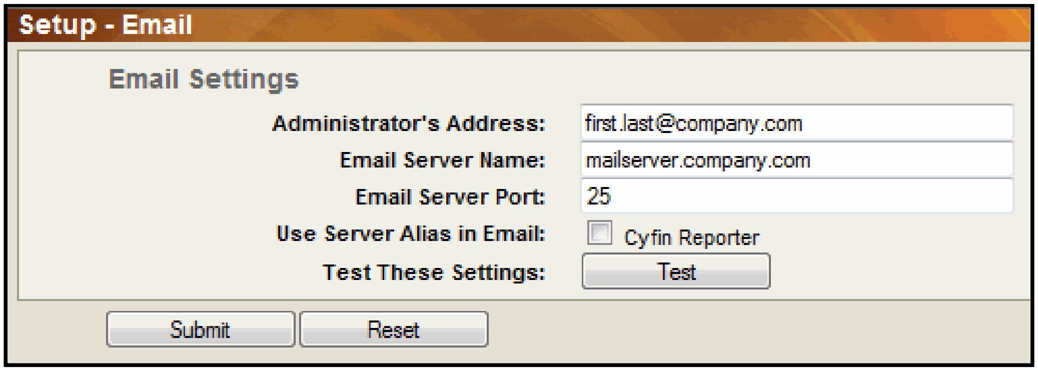
11. Finally, just close the window or click on the link displayed to add another configuration.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1.6 Set up Administrator Email

This step will let the Administrator receive all product-produced emails (e.g., error messages, fault indicators, URL list download notifications, etc.).

1. Go to the **Setup - Email** screen.



Setup - Email

Email Settings

Administrator's Address: first.last@company.com

Email Server Name: mailserver.company.com

Email Server Port: 25

Use Server Alias in Email: □ Cyfin Reporter

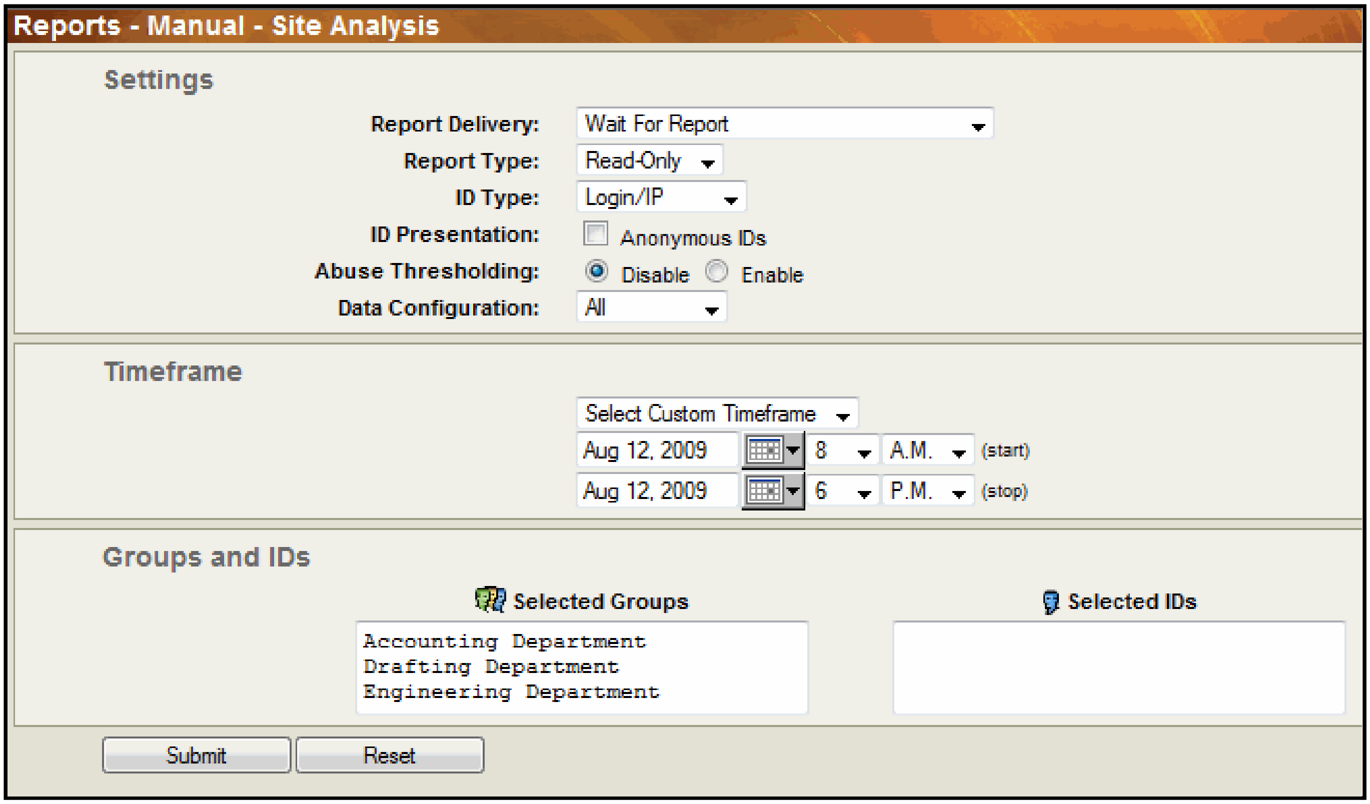
2. Fill out the screen with the Administrator's email information.
3. Click on the **Test** button to make sure the product is communicating with the email server.
4. If it is successful, then click **Submit** to save the configuration.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1.7 Create and Run a Site Analysis Report

Now that you have completed basic configuration of the product, it's time to run a report. In this step you will run a high-level read-only report against your logfile data. While this report is being run against your raw logfiles, it is recommended that you import your logfiles into the Wavecrest Database. This will increase reporting speed and allow you to use interactive reports. (See Section 3 on using the Wavecrest Database).

1. Go to the **Reports - Manual** screen.
2. Click on the first link, **Site Analysis**.



Reports - Manual - Site Analysis

Settings

Report Delivery: Wait For Report

Report Type: Read-Only

ID Type: Login/IP

ID Presentation: □ Anonymous IDs

Abuse Thresholding: ● Disable ○ Enable

Data Configuration: All

Timeframe

Select Custom Timeframe

Aug 12, 2009 8 A.M. (start)

Aug 12, 2009 6 P.M. (stop)

Groups and IDs

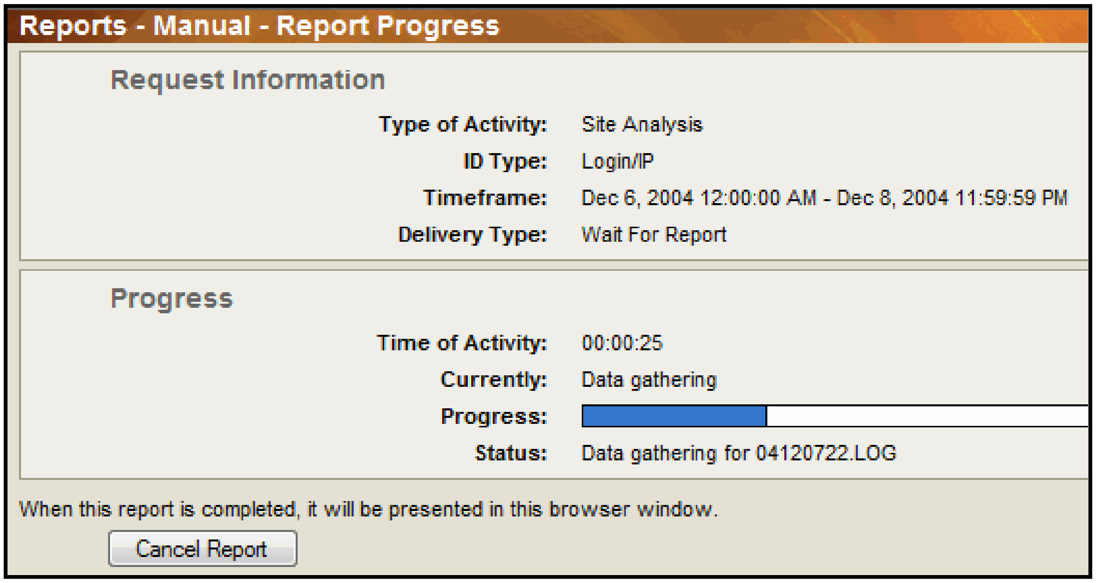
Selected Groups

Accounting Department
Drafting Department
Engineering Department

Selected IDs

3. In the **Report Type** field, *Read-Only* should be selected. (Interactive Reports will only run against logfiles imported into the Wavecrest Database. See Section 3 for instructions on importing data to the database.)
4. For basic testing purposes on this screen, use the **Timeframe** pulldown to *Select Custom Timeframe*. Date and Time field selections will appear. You need to configure a *Start Date/Time* and *Stop Date/Time* ensuring that surfing activity is included. Choose a time period that is covered by your existing logfiles, and only covers about one or two hours.
   NOTE*: If you have large amounts of Web-use data, it is recommended that you set up and use the Wavecrest Database.*
5. Leave the Enterprise group in the **Selected Groups** box, and simply click **Submit**.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.



Reports - Manual - Report Progress

Request Information

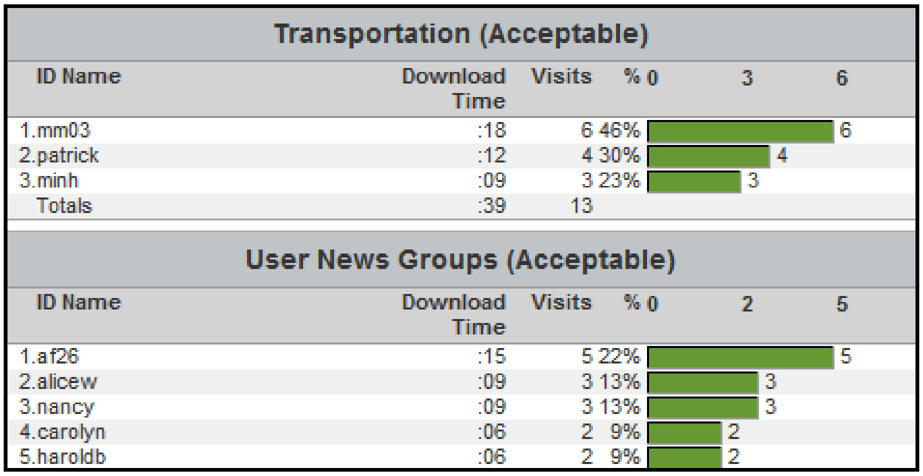
Type of Activity:	Site Analysis
ID Type:	Login/IP
Timeframe:	Dec 6, 2004 12:00:00 AM - Dec 8, 2004 11:59:59 PM
Delivery Type:	Wait For Report

Progress

Time of Activity:	00:00:25
Currently:	Data gathering
Progress:	
Status:	Data gathering for 04120722.LOG

When this report is completed, it will be presented in this browser window.

6. After your report finishes, click on the **All IDs** link that will be displayed. A sample portion of the Site Analysis report is shown below. The Site Analysis report will show you total visits by classification, category, and by user per category.



Transportation (Acceptable)

ID Name	Download Time	Visits	%	0 3 6
1.mm03	:18	6	46%	6
2.patrick	:12	4	30%	4
3.minh	:09	3	23%	3
Totals	:39	13		

User News Groups (Acceptable)

ID Name	Download Time	Visits	%	0 2 5
1.af26	:15	5	22%	5
2.alicew	:09	3	13%	3
3.nancy	:09	3	13%	3
4.carolyn	:06	2	9%	2
5.haroldb	:06	2	9%	2

7. View your report, and verify that you see user IDs along with categorized Web activity.

***NOTE**: If you do not see data on the report, try running the same report but change the ID Type to "IP Addresses." If you only get activity when running a report against IP addresses, you most likely need to configure authentication on your network to see login names. If your configured logs do not contain login names (due to a lack of network user authentication), then you will only get data on IP addresses until/unless you start authenticating login names. From that point forward, you'll be able to use Login Names as the **ID Type** in reports.*

2.0 Groups and IDs

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. (Users can be grouped in accordance with some common characteristic, usually by department. They can also be entered without grouping.) The Groups and IDs import process can be performed manually or automatically. You also have the option of managing your Groups and IDs inside the product or at your directory source.

Before using the Groups and IDs feature, you must complete the Get Started section of this manual, which covers all setup procedures to get the product running. Once you have completed 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, i.e., "Ungrouped IDs" and "VIP Group." Additional customer-specified subordinate groups and/or individual IDs can be added 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 subordinate subgroup to Enterprise. If you don't 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 customer-specified groups.
- **VIP Group.** This group is another subgroup to Enterprise. It is used to exclude designated individuals from reports. When an ID is placed in this group, his or her Web-use activity will not appear in reports.

Next, you must decide whether or not you will use grouping. Using "groups" lets you apply different Web policy settings 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 (those not previously found) in the logfiles will be placed automatically in Ungrouped IDs.
- You can import IDs into Ungrouped IDs (See Section 2.2).
- You can manually add IDs to Ungrouped IDs (See Section 2.3).

In this section, you will find instructions on:

- **Required Setup** – Completing this section is required (mandatory) before importing any Groups and IDs.
- **Importing Groups and IDs** –Import from Active Directory or a text file.
- **Adding Groups and IDs** – Manually input Groups and IDs or add them after your initial import.
- **Editing Groups and IDs** – Delete, move, and modify Groups and IDs.
- **Finding an ID** - Search for an ID, its Group, and policy settings.

2.1 Required Setup

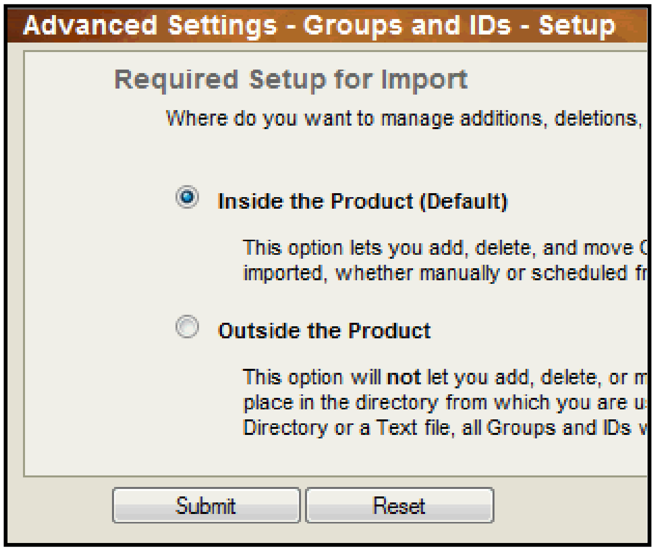
Before you begin importing Groups and IDs, you must decide where you want to modify your Groups and IDs: "Inside the Product" or "Outside the Product." Both options are discussed below.

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 or a text file. Each time Groups and IDs are imported, whether manually or scheduled from Active Directory or a text file, only new Groups and IDs will be imported. (The new Groups and IDs imported will be based on your selected groups in your import configuration setup.) Your existing Groups and IDs will not be modified.
***NOTE**: If you wish to have any users in the VIP Group, you MUST use this option.*

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 or a text file, 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.*

1. To make your selection, go to **Advanced Settings – Groups and IDs** and click on the **Setup** link.



Advanced Settings - Groups and IDs - Setup

Required Setup for Import

Where do you want to manage additions, deletions,

● Inside the Product (Default)

This option lets you add, delete, and move C
imported, whether manually or scheduled fr

○ Outside the Product

This option will **not** let you add, delete, or m
place in the directory from which you are u
Directory or a Text file, all Groups and IDs v

2. Click on the radio button to make your selection and then click **Submit** to apply your changes.

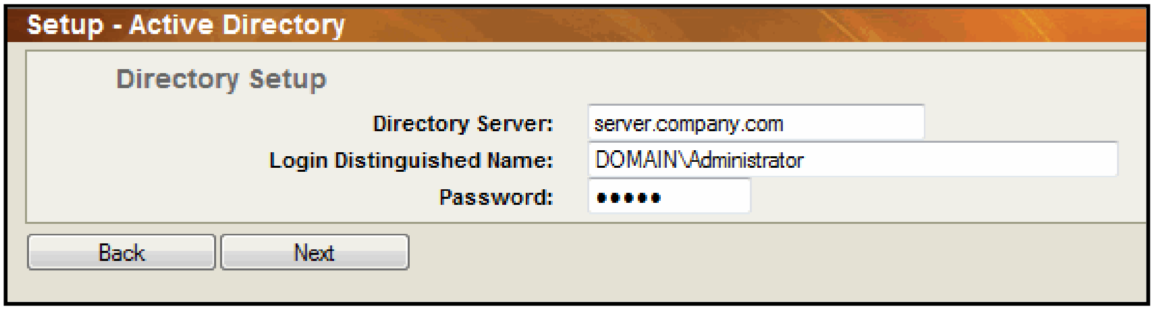
2.2 Import Groups and IDs

If you have not completed Section 2.1 Required Setup, do so first before getting started with importing Groups and IDs.

There are two ways to import your Groups and IDs. You can configure to import your Groups and IDs from (1) Active Directory or (2) a text file. If you choose to import from Active Directory, you have the option of creating a scheduled import to occur once every 24 hours.

2.2.1 Import from Active Directory

1. To create an Active Directory configuration to be imported, go to **Advanced Settings – Groups and IDs** and click on the **Active Directory** link.
2. Click on the **Setup** link. The configuration wizard will pop up.
3. Leave the default selection set at *Create new Active Directory configuration* and click **Next**.
   ***NOTE**: If you ever want to make changes to any of your configurations, use the pull-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.*
4. Now you must configure the connection to your Directory Server.



Setup - Active Directory

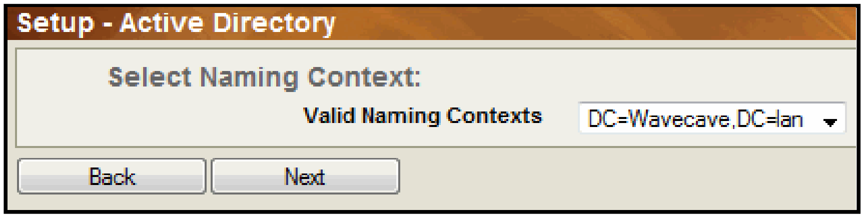
Directory Setup

Directory Server: server.company.com

Login Distinguished Name: DOMAIN\Administrator

Password: •••••

5. Enter your appropriate information in the following fields: **Directory Server**, **Login Distinguished Name**, and **Password**. Only modify the **Authentication Type** and **Port** if necessary. *Simple* is the default for Authentication Type, and *389* is the default for Port.
6. Click **Next**.
7. Both **Connection Status** and **Authentication Status** indicators should appear green. If both are green, click **Next**. If either status is red, click **Back** and double-check your Directory Setup settings.

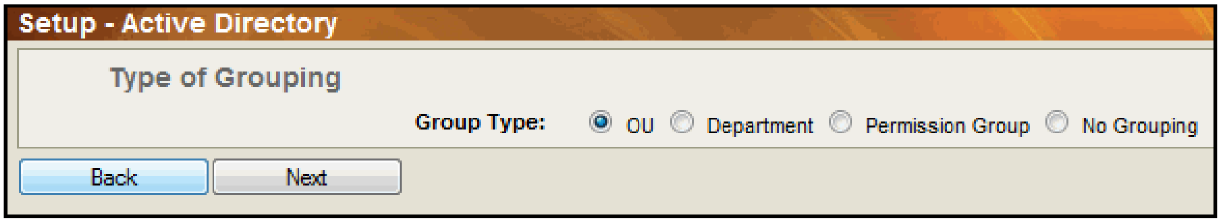


Setup - Active Directory

Select Naming Context:

Valid Naming Contexts: DC=Wavecave,DC=lan

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

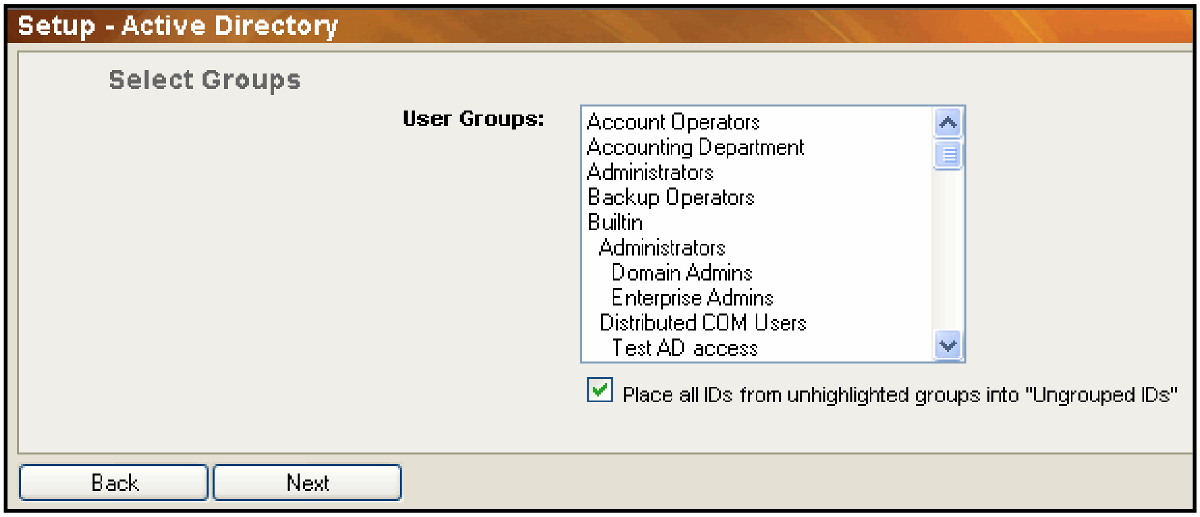


Setup - Active Directory

Type of Grouping

Group Type: ● OU ○ Department ○ Permission Group ○ No Grouping

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



Select Groups

User Groups:

Account Operators
Accounting Department
Administrators
Backup Operators
Builtin
Administrators
Domain Admins
Enterprise Admins
Distributed COM Users
Test AD access

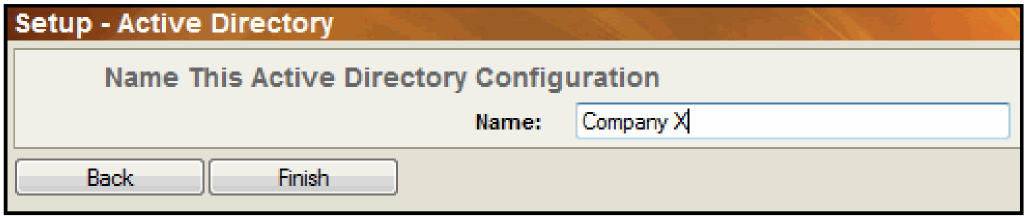
☑ Place all IDs from unhighlighted groups into "Ungrouped IDs"

10. Select the groups to be imported by clicking on them, so they are highlighted. If you want to select multiple groups, hold down the Ctrl key and click on the groups you want imported.
    ***NOTE**: If you do not highlight any **User 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.*

    Optional: Check the checkbox at the bottom of the screen if you want to place the users from the unhighlighted groups into Ungrouped IDs. 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 check the box and do not select any User Groups, all IDs will be placed in Ungrouped IDs. Also remember that if you selected to manage your Groups and IDs "outside the product," you will not be able to move any of your Groups and IDs in the product.*

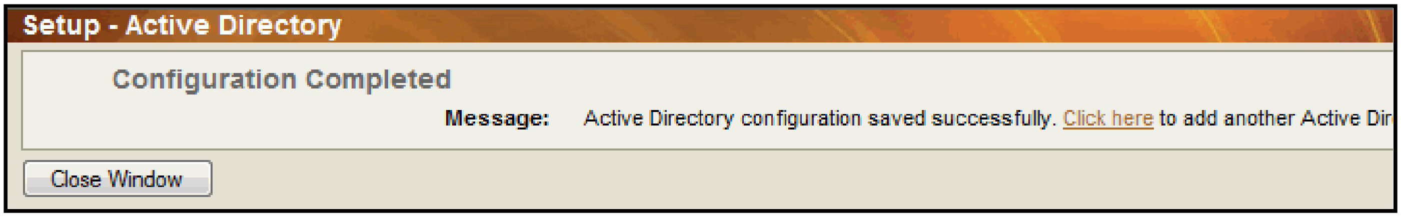
11. Once you have selected the groups that you want to import, click **Next**.



Name This Active Directory Configuration

Name: Company X

12. Type in a **Name** for this Active Directory configuration, and click **Finish**.



Configuration Completed

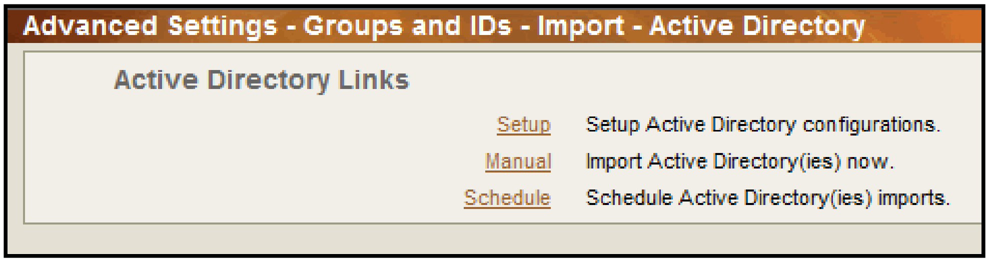
Message: Active Directory configuration saved successfully. Click here to add another Active Dir

13. You should see a successful configuration message. You now have the option to:
    a) Create another configuration by clicking on the link, or
    b) Close the window.

14. Once you have created your configuration(s), you are now ready to import.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

15. When you close the configuration wizard, you should still be at the **Advanced Settings – Groups and IDs – Active Directory** screen.



Advanced Settings - Groups and IDs - Import - Active Directory

Active Directory Links

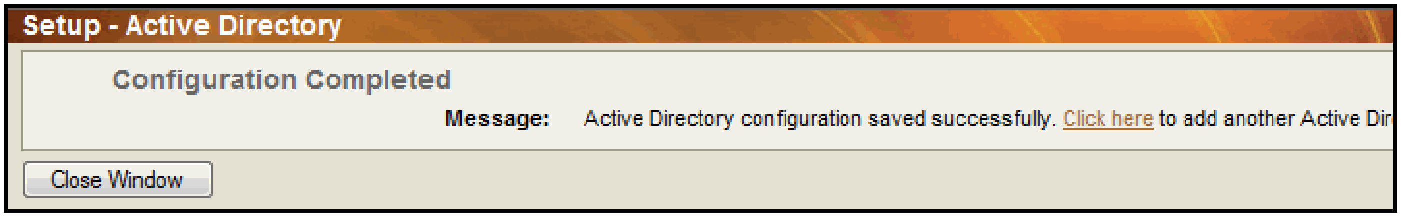
Setup Setup Active Directory configurations.

Manual Import Active Directory(ies) now.

Schedule Schedule Active Directory(ies) imports.

16. To import your configurations immediately, click on the **Manual** link.

17. If your import is successful, you should receive the following message.



Setup - Active Directory

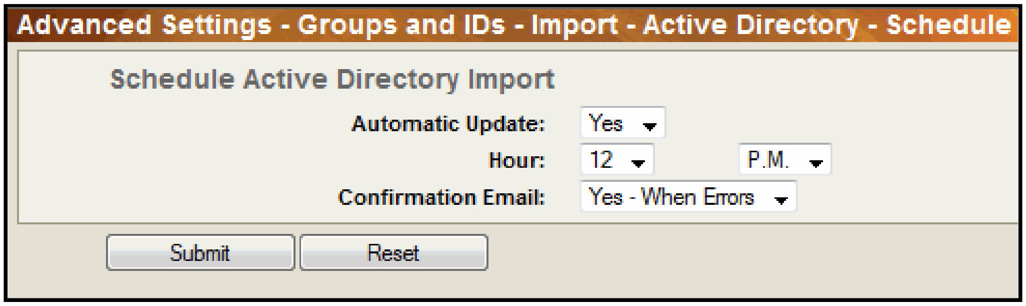
Configuration Completed

Message: Active Directory configuration saved successfully. Click here to add another Active Dir

18. Click on the link to view all of your imported Groups and IDs or close the window.

19. Every time you want to update your Groups and IDs, you will need to go to the **Advanced Settings – Groups and IDs – Active Directory** screen and click on the **Manual** link unless you schedule daily updates.

20. If you want to schedule imports to occur once every 24 hours, click on the **Schedule** link.



Advanced Settings - Groups and IDs - Import - Active Directory - Schedule

Schedule Active Directory Import

Automatic Update: Yes

Hour: 12 P.M.

Confirmation Email: Yes - When Errors

21. For the **Automatic Update** field, select *Yes*. If you ever want to stop the scheduled import, you will need to return to this screen and change the **Automatic Update** field to *No*.

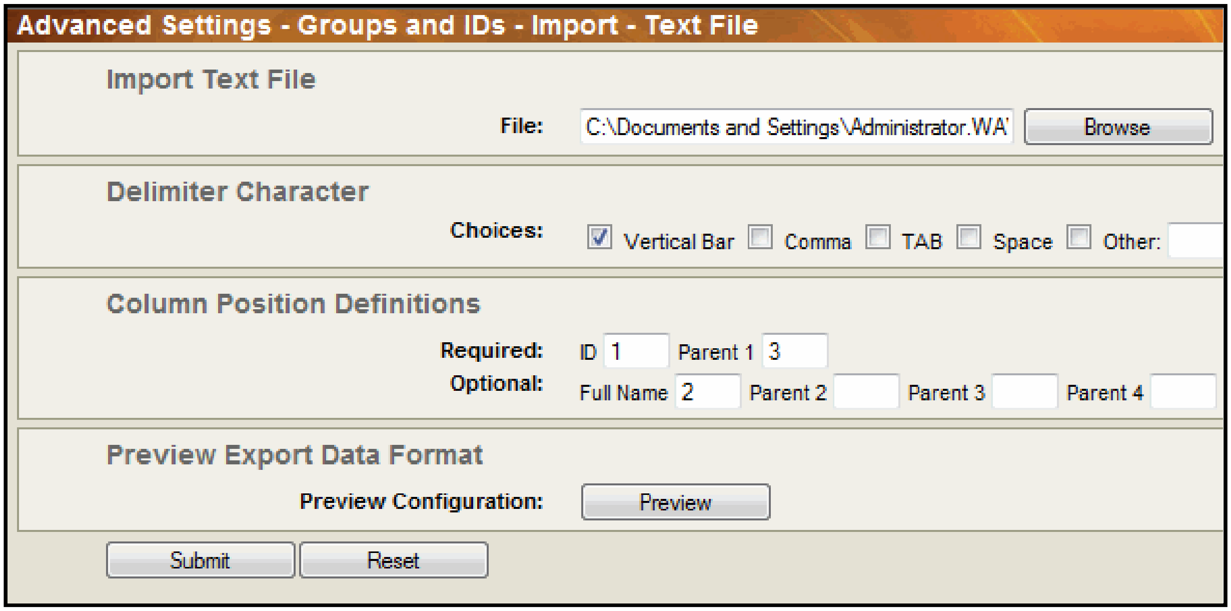
22. Select the **Hour** that you want the import to occur, and select whether or not you wish to receive a **Confirmation Email** for the import.

23. Click **Submit** to save your changes.

2.2.1 Import a Text File

For instructions on creating your text file, see Appendix A.

1. To import Groups and IDs from a text file, go to **Advanced Settings – Groups and IDs** and click on the **Text File** link.



Advanced Settings - Groups and IDs - Import - Text File

Import Text File

File: C:\Documents and Settings\Administrator.WA'

Delimiter Character

Choices: ☑ Vertical Bar □ Comma □ TAB □ Space □ Other:

Column Position Definitions

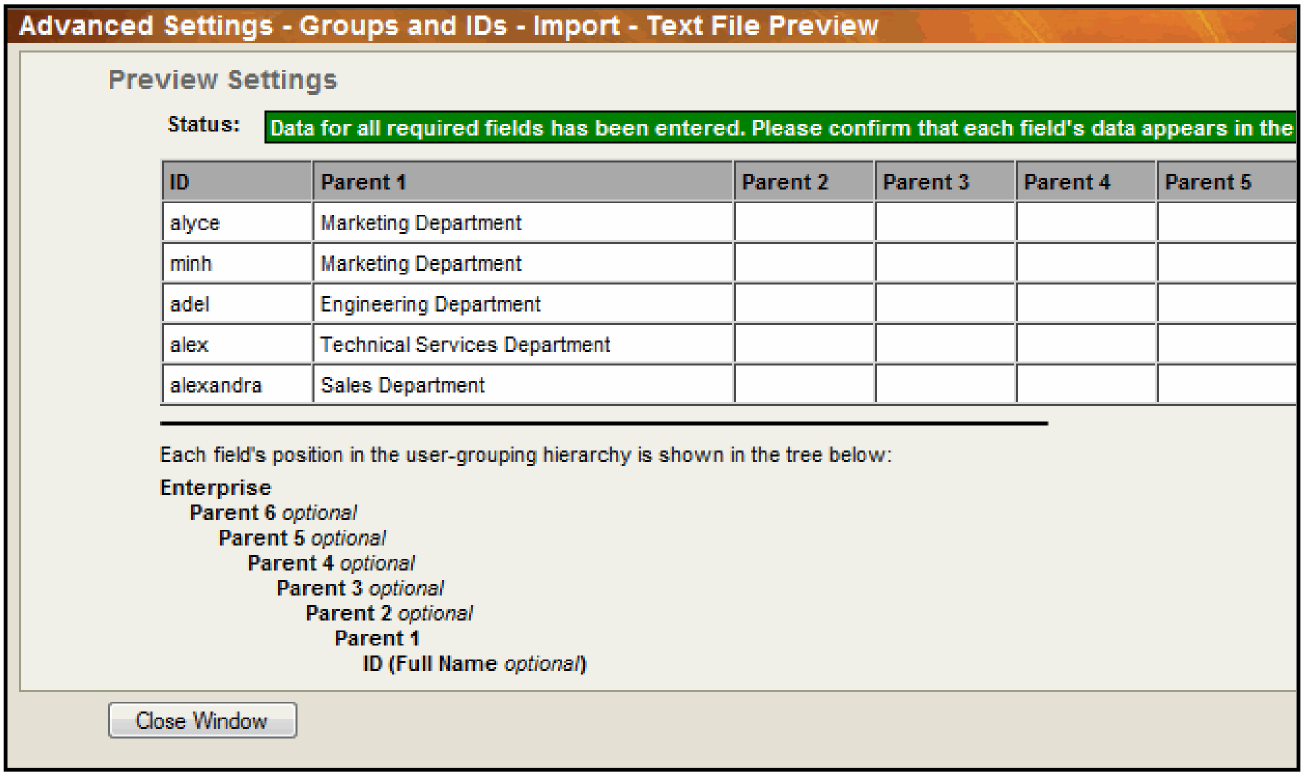
Required: ID 1 Parent 1 3

Optional: Full Name 2 Parent 2 Parent 3 Parent 4

Preview Export Data Format

Preview Configuration:

2. In the **File** field, type in the file name or click on the **Browse** button to locate the file you want to import.
3. Check the box for the **Delimiter Character** that you used in your text file.
4. For the two required data fields (columns), enter column numbers that correspond to the left-to-right column positioning of those fields in the text file. Column numbers range from 1 to 6.
5. If any of the optional data fields (columns) are used in the text file, enter column numbers that correspond to the left-to-right column positioning of those fields in the text file. Column numbers range from 1 to 6.
6. Click the **Preview Configuration** button to check that your data is in the correct columns. If it is not, close the Preview screen, retype and double-check your values for **Column Position Definitions**.



Advanced Settings - Groups and IDs - Import - Text File Preview

Preview Settings

Status: Data for all required fields has been entered. Please confirm that each field's data appears in the

ID	Parent 1	Parent 2	Parent 3	Parent 4	Parent 5
alyce	Marketing Department				
minh	Marketing Department				
adel	Engineering Department				
alex	Technical Services Department				
alexandra	Sales Department				

Each field's position in the user-grouping hierarchy is shown in the tree below:

Enterprise
  Parent 6 *optional*
    Parent 5 *optional*
      Parent 4 *optional*
        Parent 3 *optional*
          Parent 2 *optional*
            Parent 1
              ID (Full Name *optional***)**

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

7. If your data and columns are correct, close the Preview window.

8. Click **Submit** to import your Groups and IDs.
   NOTE*: Configured text file imports will occur at midnight each day.*
   CAUTION*: If you have both a text file and an Active Directory import configured, whenever an Active Directory import occurs, the text file will also import along with it.*

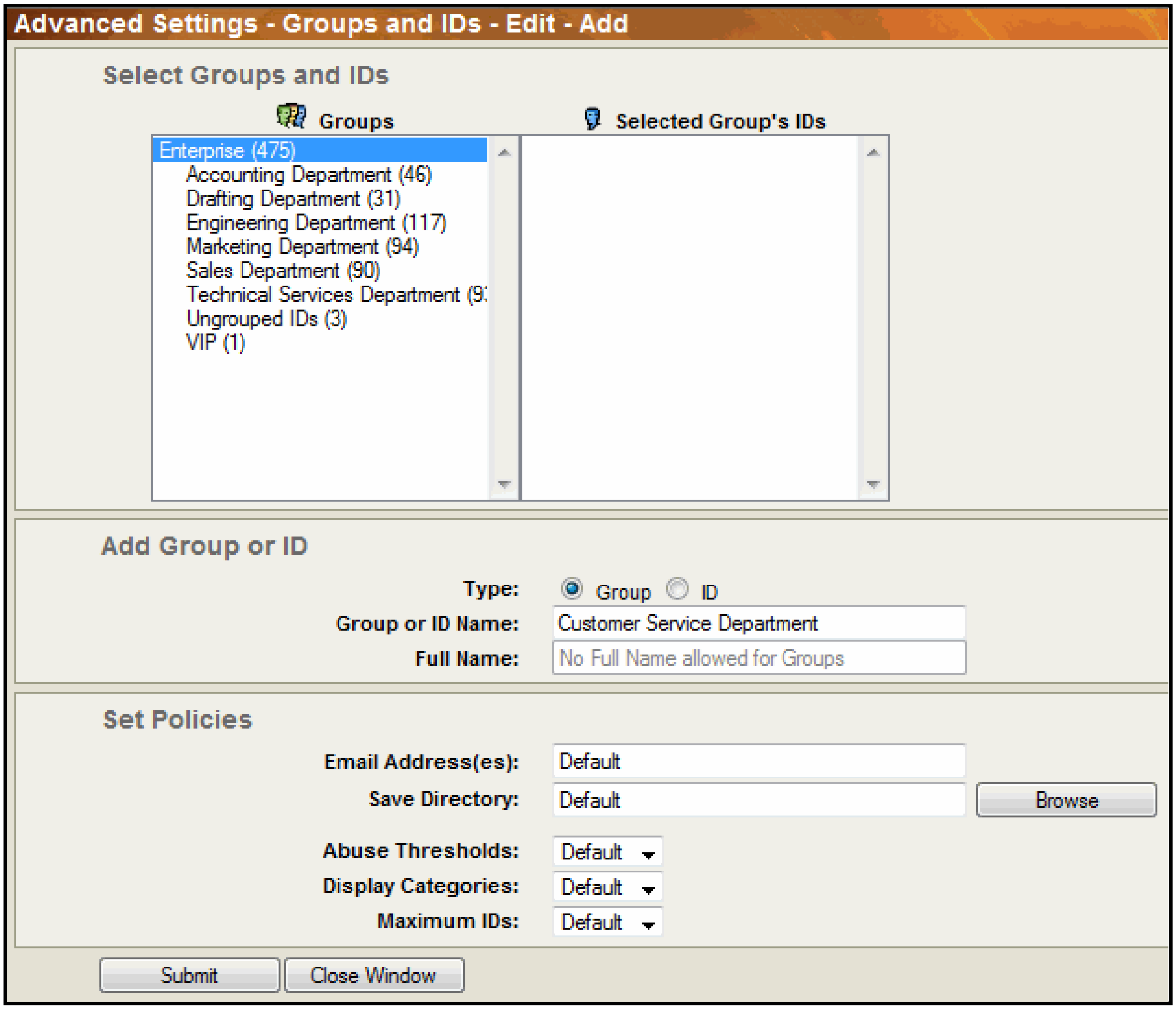
2.3 Add Groups and IDs

If you do not want to import Groups and IDs, you can manually add each Group or ID in the product. Even if you did import your Groups and IDs, you can add more, IF you chose to manage your Groups and IDs "Inside the Product" (See Section 2.1). If you chose to manage them "Outside the Product," you can only add Groups and IDs to your directory source and re-import. This screen 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.*

2.3.1 Add a Group

1. Go to **Advanced Settings – Groups and IDs** and click on the **Add** link.



Advanced Settings - Groups and IDs - Edit - Add

Select Groups and IDs

Groups

Enterprise (475)
Accounting Department (46)
Drafting Department (31)
Engineering Department (117)
Marketing Department (94)
Sales Department (90)
Technical Services Department (9
Ungrouped IDs (3)
VIP (1)

Selected Group's IDs

Add Group or ID

Type: ● Group ○ ID
Group or ID Name: Customer Service Department
Full Name: No Full Name allowed for Groups

Set Policies

Email Address(es): Default
Save Directory: Default
Abuse Thresholds: Default
Display Categories: Default
Maximum IDs: Default

2. Select the "parent" group to which you wish to add the group. In this case we will add our new group to *Enterprise*. ***NOTE**: Groups can only be added to other groups. A group can not be added to an ID.*
3. For **Type**, select the **Group** radio button.
4. In the **Group or ID Name** field, type in the name of the group (for example, "sales") you are adding.
5. The **Full Name** field will be grayed out because it cannot be used for groups.

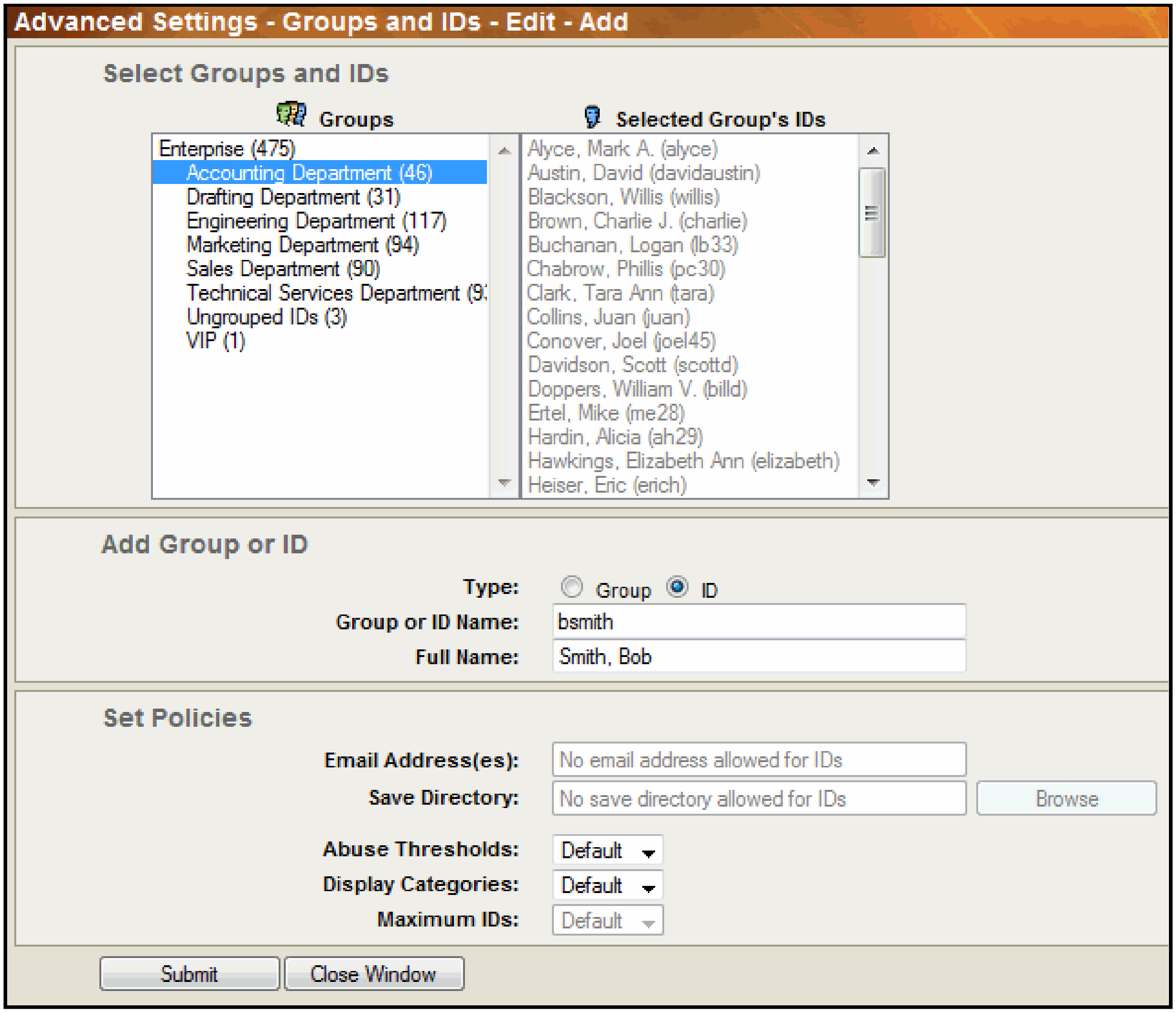
© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6. Complete the other fields.
   Email Address(es): Type in email address(es) of the person (or people) who should receive Web-use reports on the selected group.
   Save Directory: Reports will be saved to a directory of your choosing so that they can be accessed by the person (or people) who need to see them. This field is only applicable for groups.
   Abuse Thresholds: Select a policy to apply to the selected Group or ID. See Section 4 on abuse threshold policies.
   Display Categories: Select a policy to apply to the selected Group or ID. See Section 5 on display category policies.
   Maximum IDs: Select a policy to apply to the selected group. See Section 5 on maximum ID policies.

7. Click **Submit** to add the group and settings.

2.3.2 Add an ID

1. Now, we will add an ID to the group that was just created. You will remain at the **Groups and IDs - Edit - Add** screen.



Advanced Settings - Groups and IDs - Edit - Add

Select Groups and IDs

Groups
Enterprise (475)
Accounting Department (46)
Drafting Department (31)
Engineering Department (117)
Marketing Department (94)
Sales Department (90)
Technical Services Department (9
Ungrouped IDs (3)
VIP (1)

Selected Group's IDs
Alyce, Mark A. (alyce)
Austin, David (davidaustin)
Blackson, Willis (willis)
Brown, Charlie J. (charlie)
Buchanan, Logan (lb33)
Chabrow, Phillis (pc30)
Clark, Tara Ann (tara)
Collins, Juan (juan)
Conover, Joel (joel45)
Davidson, Scott (scottd)
Doppers, William V. (billd)
Ertel, Mike (me28)
Hardin, Alicia (ah29)
Hawkings, Elizabeth Ann (elizabeth)
Heiser, Eric (erich)

Add Group or ID

Type: ○ Group ● ID
Group or ID Name: bsmith
Full Name: Smith, Bob

Set Policies

Email Address(es): No email address allowed for IDs
Save Directory: No save directory allowed for IDs Browse
Abuse Thresholds: Default
Display Categories: Default
Maximum IDs: Default

Submit Close Window

2. Select the “parent” group to which you wish to add the ID. In this case we will add our new ID to *Sales*.

   NOTE*: IDs can only be added to other groups. An ID can not be added to another ID.*

3. For **Type**, select the **ID** radio button.

4. In the **Group or ID Name** field, type in the ID name (for example, "bsmith").

5. Type in the **Full Name** of the ID you are adding.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6. Complete the other fields.
   Email Address(es): Type in email address(es) of the person (or people) who should receive Web-use reports on the selected group.
   Save Directory: Reports will be saved to a directory of your choosing so that they can be accessed by the person (or people) who need to see them. This field is only applicable for groups.
   Abuse Thresholds: Select a policy to apply to the selected Group or ID. See Section 4 on abuse threshold policies.
   Display Categories: Select a policy to apply to the selected Group or ID. See Section 5 on display category policies.
   Maximum IDs: Select a policy to apply to the selected group. See Section 5 on maximum ID policies.
7. Click **Submit** to add the new ID.
8. Click the **Close Window** button when finished.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

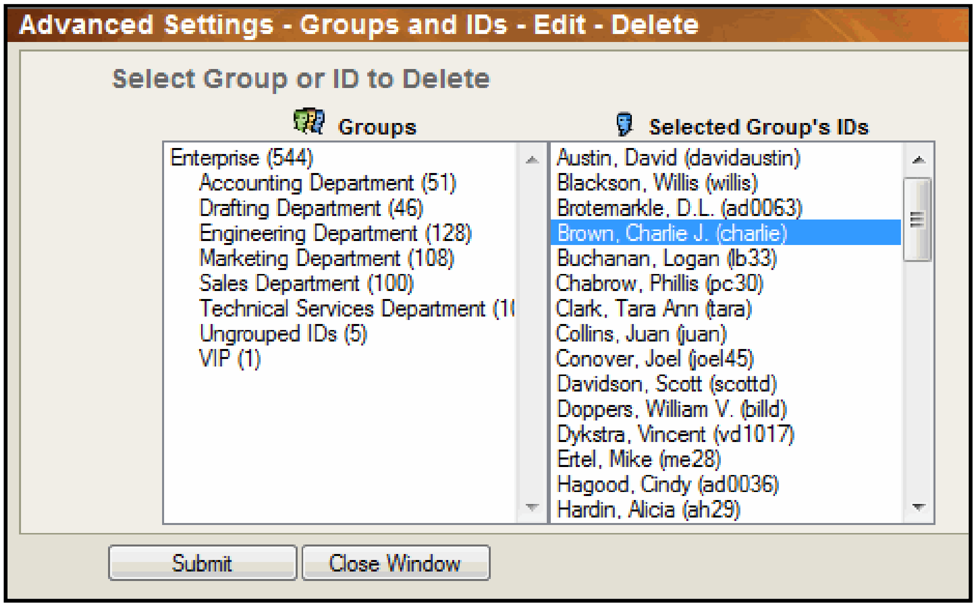
2.4 Edit Groups and IDs

In this section, you will learn how to delete, move, and modify your Groups and IDs. If you chose to manage your Groups and IDs “Inside the Product” in the Required Setup (See Section 2.1), then follow the instructions in these sections.

If you chose to manage your Groups and IDs outside the product, then you can only edit Groups and IDs in your directory source and re-import to apply your changes. However, you will be able to modify the report and policy settings for each group inside the product at the Modify screen.

2.4.1 Delete

1. Go to **Advanced Settings – Groups and IDs** and click on the **Delete** link.



Advanced Settings - Groups and IDs - Edit - Delete

Select Group or ID to Delete

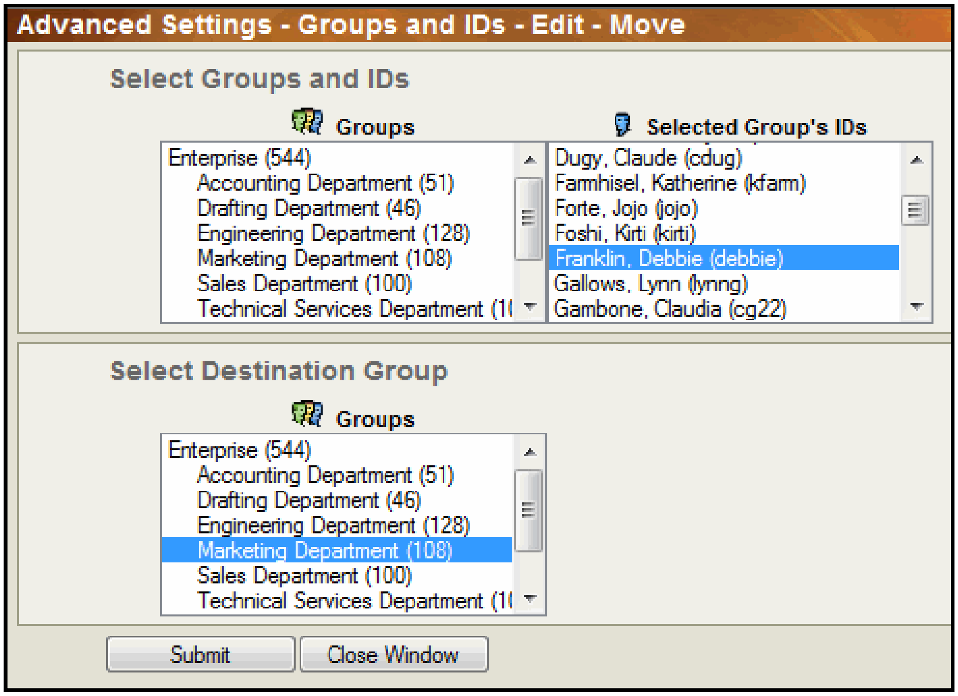
Groups	Selected Group's IDs
Enterprise (544)	Austin, David (davidaustin)
Accounting Department (51)	Blackson, Willis (willis)
Drafting Department (46)	Brotemarkle, D.L. (ad0063)
Engineering Department (128)	Brown, Charlie J. (charlie)
Marketing Department (108)	Buchanan, Logan (lb33)
Sales Department (100)	Chabrow, Phillis (pc30)
Technical Services Department (1(	Clark, Tara Ann (tara)
Ungrouped IDs (5)	Collins, Juan (juan)
VIP (1)	Conover, Joel (joel45)
	Davidson, Scott (scottd)
	Doppers, William V. (billd)
	Dykstra, Vincent (vd1017)
	Ertel, Mike (me28)
	Hagood, Cindy (ad0036)
	Hardin, Alicia (ah29)

2. Click on the Group or ID that you want to delete so that it is highlighted.
3. Click **Submit** to delete the Group or ID.
4. Close the Window when you are finished.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

2.4.2 Move

1. Go to **Advanced Settings – Groups and IDs** and click on the **Move** link.


Advanced Settings - Groups and IDs - Edit - Move
Select Groups and IDs
Groups
Selected Group's IDs
Enterprise (544)
Accounting Department (51)
Drafting Department (46)
Engineering Department (128)
Marketing Department (108)
Sales Department (100)
Technical Services Department (1(
Dugy, Claude (cdug)
Farnhisel, Katherine (kfarn)
Forte, Jojo (jojo)
Foshi, Kirti (kirti)
Franklin, Debbie (debbie)
Gallows, Lynn (lynng)
Gambone, Claudia (cg22)
Select Destination Group
Groups
Enterprise (544)
Accounting Department (51)
Drafting Department (46)
Engineering Department (128)
Marketing Department (108)
Sales Department (100)
Technical Services Department (1(
Submit
Close Window

2. Select (highlight) the Group(s) or ID(s) that you want to move. You can select more than one Group or ID at a time by holding down the CTRL key while clicking on the Groups or IDs.
   ***NOTE**: Do not select "Enterprise." It cannot be moved or made subordinate to another group.*

3. Select the Destination Group for your previously selected Group(s) or ID(s).
   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").

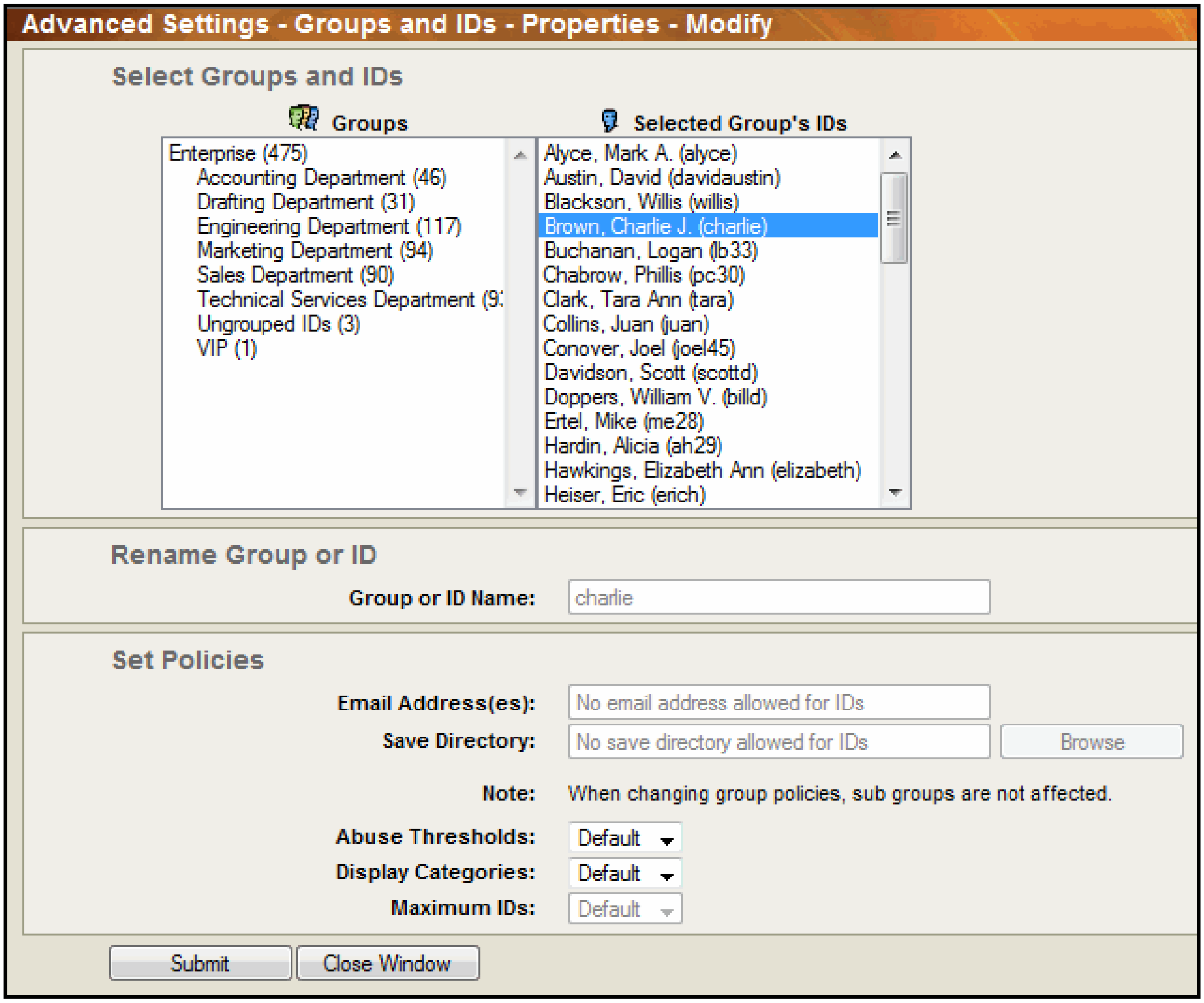
4. Click **Submit** to move the Group(s) or ID(s).

5. Close the Window when you are finished.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

2.4.3 Modify

1. Go to **Advanced Settings – Groups and IDs** and click on the **Modify** link.



Advanced Settings - Groups and IDs - Properties - Modify

Select Groups and IDs

Groups

Enterprise (475)
Accounting Department (46)
Drafting Department (31)
Engineering Department (117)
Marketing Department (94)
Sales Department (90)
Technical Services Department (9:
Ungrouped IDs (3)
VIP (1)

Selected Group's IDs

Alyce, Mark A. (alyce)
Austin, David (davidaustin)
Blackson, Willis (willis)
Brown, Charlie J. (charlie)
Buchanan, Logan (lb33)
Chabrow, Phillis (pc30)
Clark, Tara Ann (tara)
Collins, Juan (juan)
Conover, Joel (joel45)
Davidson, Scott (scottd)
Doppers, William V. (billd)
Ertel, Mike (me28)
Hardin, Alicia (ah29)
Hawkings, Elizabeth Ann (elizabeth)
Heiser, Eric (erich)

Rename Group or ID

Group or ID Name: charlie

Set Policies

Email Address(es): No email address allowed for IDs

Save Directory: No save directory allowed for IDs

Note: When changing group policies, sub groups are not affected.

Abuse Thresholds: Default

Display Categories: Default

Maximum IDs: Default

2. Select (highlight) the Group or ID that you want to modify.

   ***NOTE**: When changing group policies, sub-groups 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. Make your changes to the following fields.
   Email Address(es): Type in email address(es) of the person (or people) who should receive Web-use reports on the selected group.
   Save Directory: Reports will be saved to a directory of your choosing so that they can be accessed by the person (or people) who need to see them. This field is only applicable for groups.
   Abuse Thresholds: Select a policy to apply to the selected Group or ID. See Section 4 on abuse threshold policies.
   Display Categories: Select a policy to apply to the selected Group or ID. See Section 5 on display category policies.
   Maximum IDs: Select a policy to apply to the selected group. See Section 5 on maximum ID policies.

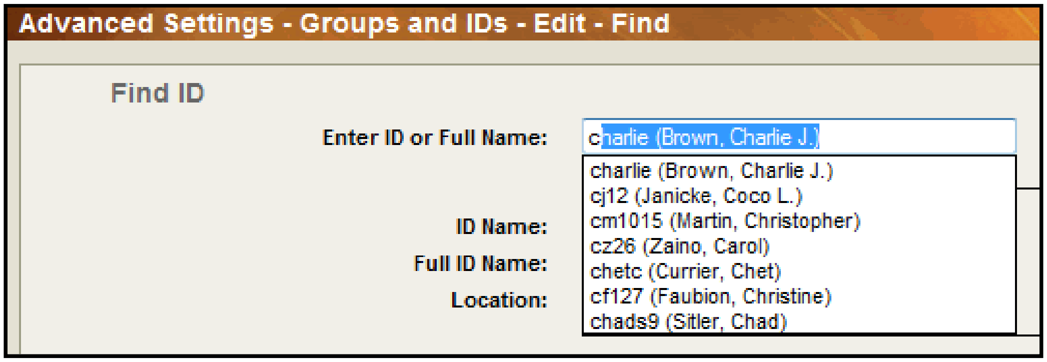
4. Click **Submit** to apply your changes, and click on the **Close Window** button when you are finished.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

2.5 Find an ID

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

1. To find an ID, go to **Advanced Settings - Groups and IDs** and click on the **Find** link.
2. Type in the user **ID** or **Full Name** of the monitored user.



Advanced Settings - Groups and IDs - Edit - Find

Find ID

Enter ID or Full Name: charlie (Brown, Charlie J.)

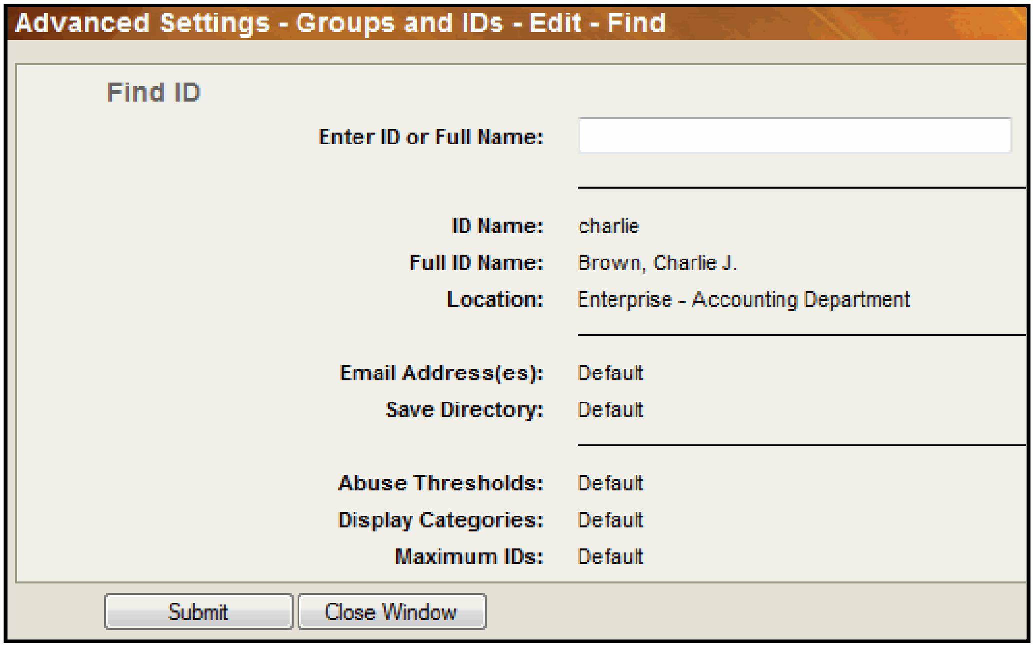
charlie (Brown, Charlie J.)
cj12 (Janicke, Coco L.)
cm1015 (Martin, Christopher)
cz26 (Zaino, Carol)
chetc (Currier, Chet)
cf127 (Faubion, Christine)
chads9 (Sitler, Chad)

ID Name:

Full ID Name:

Location:

3. Click **Submit**, and the product will retrieve the settings for that user.



Advanced Settings - Groups and IDs - Edit - Find

Find ID

Enter ID or Full Name:

ID Name: charlie

Full ID Name: Brown, Charlie J.

Location: Enterprise - Accounting Department

Email Address(es): Default

Save Directory: Default

Abuse Thresholds: Default

Display Categories: Default

Maximum IDs: Default

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

3.0 Data Management

Data Management is a key feature of this product. With Data Management, you can manage your Web-use data from your configured logfiles or import your logfiles into the optional-use Dashboard (high-level) and Mass Storage (low-level) databases and manage your data there. Even though the databases are an optional-use feature, they must be enabled if you choose to use the Dashboard and Interactive Reporting (see Section 5). It is highly recommended that you use the Data Manager if you have large amounts of Web-use data.

Before getting started with Data Management, you should have completed the Get Started section of this manual. If so, you will have already configured your logfiles. Of course, you can always come back to the logfile configuration instructions in this section if you need to change or add a configuration.

In managing your logfile data, this section will show you how to:

- **Set up the Logfile Directory** - Specify the directory location of your logfiles.
- **Set up Logfile Configurations** - Configure the product to locate and read your logfiles.
- **View Logfiles** – View your configured logfiles.
- **Revalidate Logfiles** – Revalidate any invalid logfiles.

Once you have configured your logfiles, you can begin using the Data Manager. Logfile data can be imported into the databases where it is compressed. This will reduce report-generation time by more than 95 percent (compared to methods that generate reports by reading logfiles directly). This section will show you how to:

- **Enable the Data Manager** – Turn on the Dashboard (high-level) and Mass Storage (low-level) databases.
- **Configure Dasbhoard Database** - Keep the default Derby database or configure MySQL or MSSQL.
- **Import Logfile Data into the Database** – Manually import configured logfile data or schedule the import to occur daily.
- **View Data** – View the data.
- **Export Data** – Export data to other applications.
- **Delete Data** – Delete data from the database.

To use the Data Manager, you must first enable it. Once enabled, the product automatically retrieves the previous day’s raw logfile data and stores it in the database. It does this on a daily scheduled basis. This process could be scheduled, for example, between 1:00 and 4:00 AM, or other periods of low Web usage. The product default is midnight. This way the previous day’s data will be available the following morning for report generation. The data will be permanently stored within the product to enable generation of a variety of reports, i.e., daily, weekly, monthly, quarterly, etc.

Although processing logfiles is active from the time the Data Manager feature is first enabled, the product is only designed to automatically retrieve and store “future” logfile data as it is created in daily use. (It does not automatically “go back” and retrieve data generated prior to the Data Manager being enabled.) To populate the Dashboard (high-level) and Mass Storage (low-level) databases with past configured logfile data, you can import these logfiles into the databases 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 Data Manager is report-generation speed. When the databases are used, a virtually unlimited number of authorized users can generate their own reports in minimal time. Currently only administrators can access the Dashboard.

For example, when the Data Manager is enabled, 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 Mass Storage (low-level) 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 logfile. With respect to persistence, once the configured logfile data has been imported into the Data Manager, you never have to read it again. The data remains stored and readily available for future use.

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

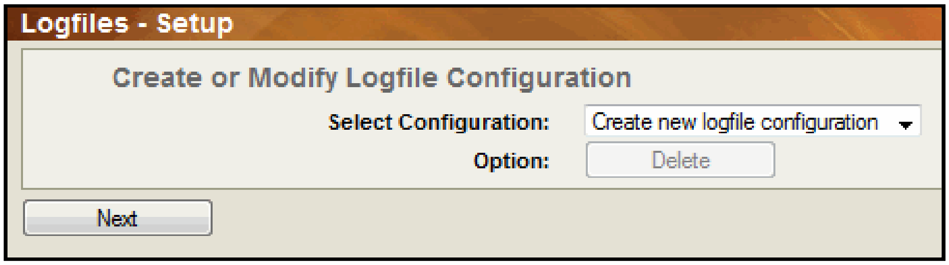
The export feature of the Data Manager has many benefits also. Data can be exported as a CSV or XML file to other applications e.g., spreadsheets, report generators, relational databases, etc. The parameters when exporting data are customizable as well.

3.1 Logfile Data

3.1.1 Set Up Logfile Configurations

Logfile configuration consists of specifying the logfile type and location.

1. Go to **Logfiles – Setup**. The **Create or Modify Logfile Configuration** wizard will come up.



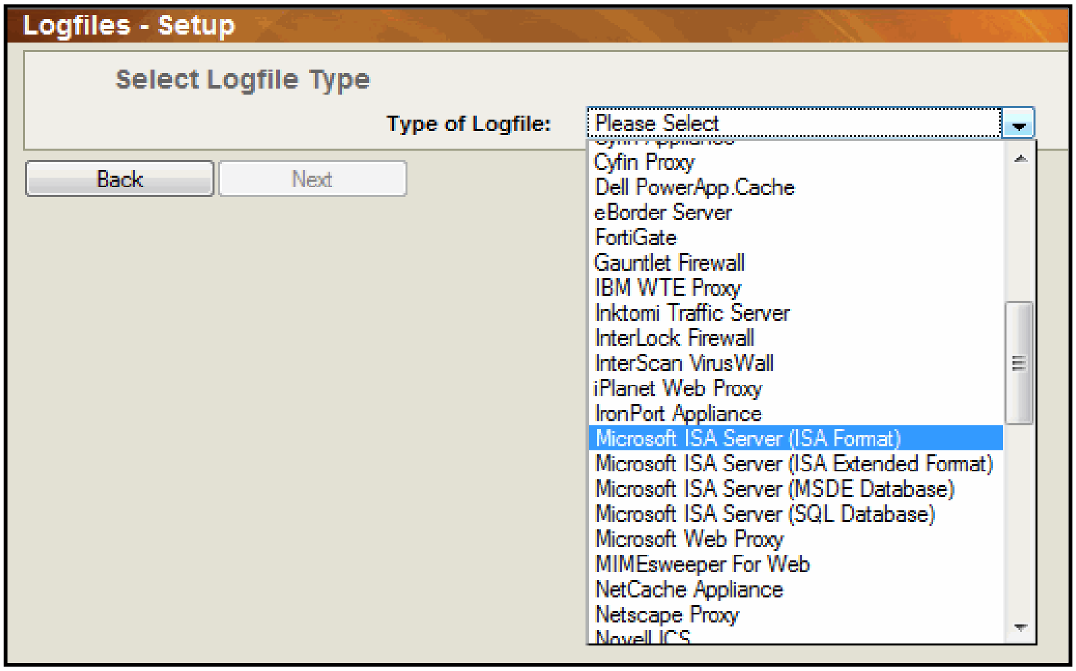
Logfiles - Setup

Create or Modify Logfile Configuration

Select Configuration: Create new logfile configuration

2. Select *Create new logfile configuration* when creating a new configuration. Otherwise, use the pull-down menu to select a previously created logfile configuration that you wish to modify.
__NOTE__: If you wish to delete a previously created logfile configuration, select that logfile configuration and click on the __Delete__ button.

3. Click **Next**.

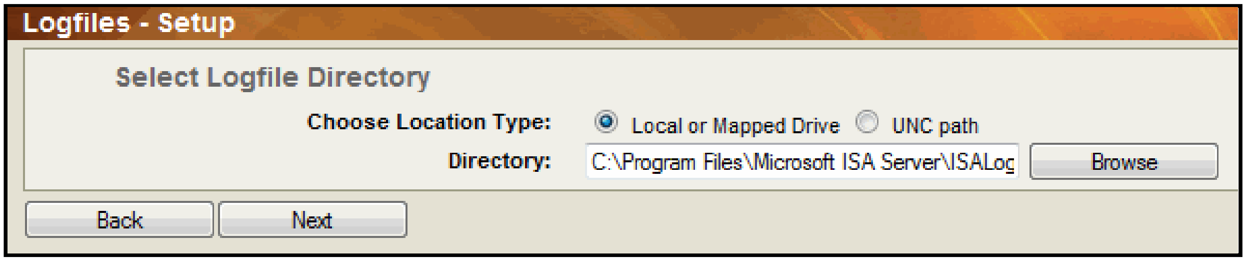


Logfiles - Setup

Select Logfile Type

Type of Logfile: Please Select

4. Select the **Type of Logfile** for your configuration and click **Next**.



Logfiles - Setup

Select Logfile Directory

Choose Location Type: ● Local or Mapped Drive ○ UNC path

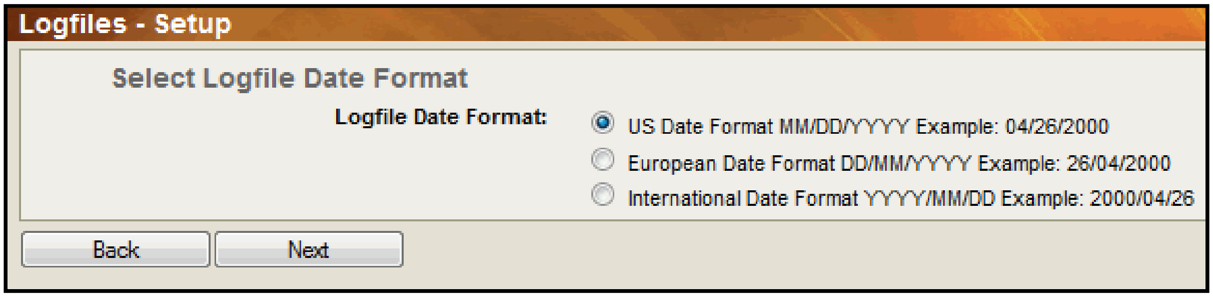
Directory: C:\Program Files\Microsoft ISA Server\ISALog

5. Select the appropriate radio button to indicate whether the logfiles are stored on a **Local or Mapped Drive** or can be accessed via a **UNC path**.

6. **Browse** to the logfile location, or (if **UNC path** was selected) type in the **Directory** path.

7. Click **Next**. Depending on the type of logfile selected above, the following screen may or may not appear. If it does not, please skip to step 10 below.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.



Logfiles - Setup

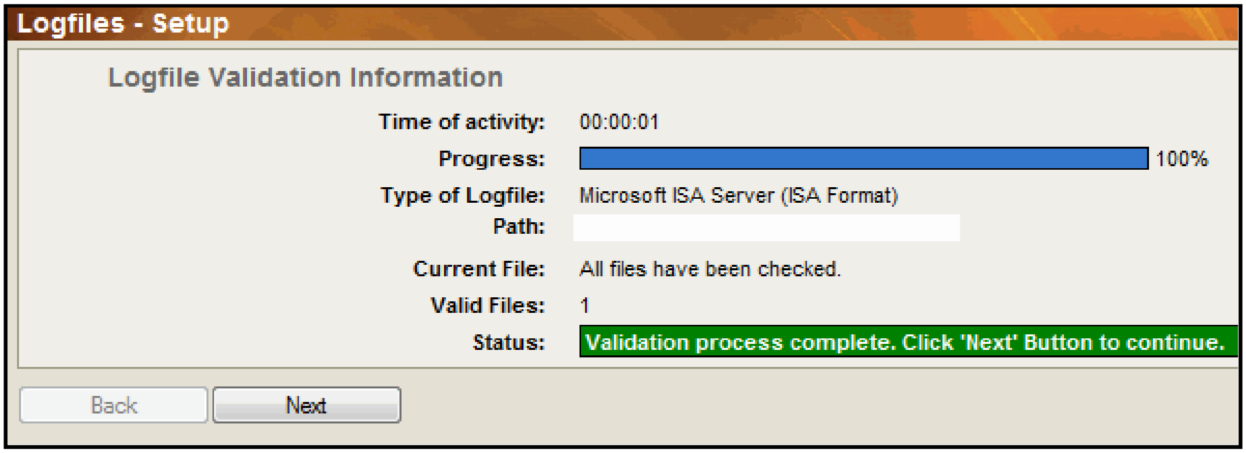
Select Logfile Date Format

Logfile Date Format:

● US Date Format MM/DD/YYYY Example: 04/26/2000
○ European Date Format DD/MM/YYYY Example: 26/04/2000
○ International Date Format YYYY/MM/DD Example: 2000/04/26

8. Select the **Logfile Date Format**. For most proxies, this action is not needed and the screen will not appear. For others such as Microsoft Web Proxy, please select the correct logfile date format, i.e., "U.S.," "European," or "International."

9. Click **Next**.



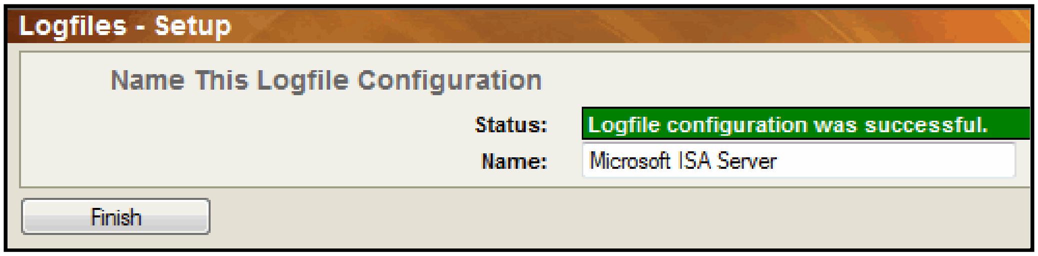
Logfiles - Setup

Logfile Validation Information

Time of activity:	00:00:01
Progress:	100%
Type of Logfile:	Microsoft ISA Server (ISA Format)
Path:	
Current File:	All files have been checked.
Valid Files:	1
Status:	Validation process complete. Click 'Next' Button to continue.

10. **Logfile Validation** should occur. When the process is complete, click **Next**.
*NOTE: If there is a problem (or error) with Logfile Validation, the screen will indicate that an error has occurred. In this case, click on the **Back** button to double check your configuration selections and make needed adjustments.*

11. You should see the 'successful configuration' message shown below and have the option to exit or create another configuration by clicking on a hyperlink.
*NOTE: If you modified a previous configuration, you must go to the **Logfiles – Revalidate** screen to validate your logfiles.*



Logfiles - Setup

Name This Logfile Configuration

Status:	Logfile configuration was successful.
Name:	Microsoft ISA Server

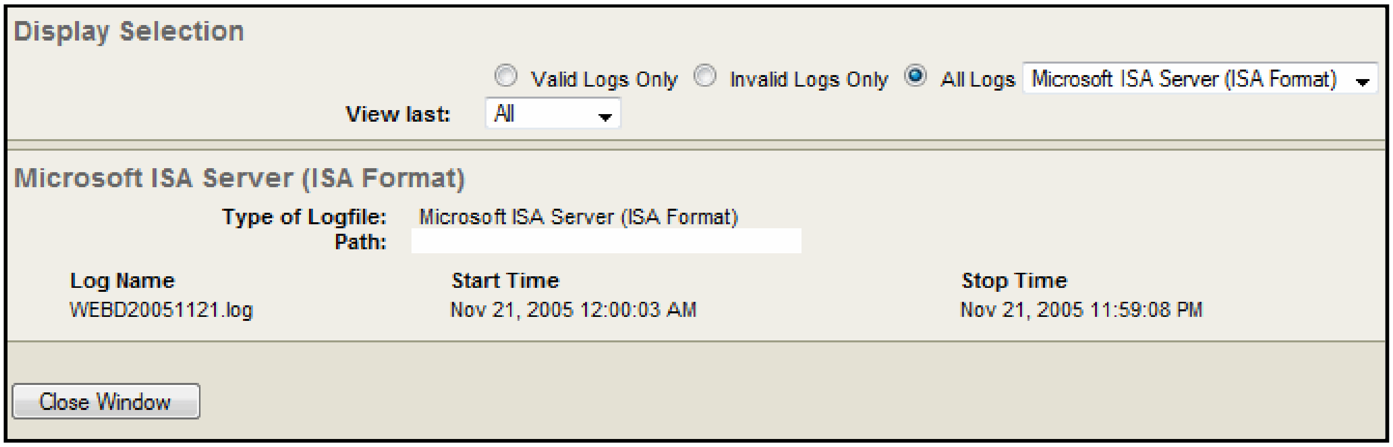
12. To exit, click on **Close Window**.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

3.1.2 View Logfile Data

This screen displays the logfiles that have been configured. The product uses these logfiles to produce reports. For each logfile configuration, this screen displays the (Configuration) Name, Type of Logfile and Path. For each individual logfile it displays the Log Name, Start Time, Stop Time and Status.

1. Go to **Logfiles – Viewer**, and the logfiles will appear on the opened screen.



Display Selection

○ Valid Logs Only ○ Invalid Logs Only ● All Logs Microsoft ISA Server (ISA Format)

View last: All

Microsoft ISA Server (ISA Format)

Type of Logfile: Microsoft ISA Server (ISA Format)
Path:

Log Name	Start Time	Stop Time
WEBD20051121.log	Nov 21, 2005 12:00:03 AM	Nov 21, 2005 11:59:08 PM

2. In the **Display Section**, use the radio button or pull down menu to select the logfile(s) you want to view. Below are definitions of the information shown for each logfile.

   Logfile Configuration Name: The name for each configuration appears in the upper left of its display listing.
   Type of Logfile: The logfile source type.
   Path: The directory path to the logfiles.
   Log Name: Name of validated file.
   Start Time: Date and time of first record in logfile. (See note below.)
   Stop Time: Date and time of last record in logfile. (See note below.)
   Status: Status of logfile for report generation purposes, using the three codes defined below.

   - **Valid**: Logfile can be used to generate reports.
   - **Invalid**: Logfile 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.

3.1.3 Revalidate Logfiles

This feature requires minimal use and instruction. If the product has not had a problem reading your configured logfiles, all logfiles should be valid, and you will not have to use this feature. If for any reason some logfiles are invalid, you should go to the **Logfiles – Revalidate** screen. There the product will re-examine any and all 'invalid' logfiles that were included in a configuration and may validate those that were previously invalid.

NOTE*: For a logfile to be valid, it must contain some Web use data, i.e., it cannot be 'empty.'*

In some cases, the logfiles are invalid because the configuration is incorrect. If this is the case, you must fix the configuration in the **Logfiles – Setup** screen. Once you have done so, you need to go back to **Logfiles – Revalidate** so that logfiles can be revalidated based on the revised configuration.

If your logfiles are still invalid, contact our technical support team. Our support team is available Monday – Friday, 8:00 am – 6:00 pm Eastern Time and can be reached by phone (321-953-5351) or email (support@wavecrest.net).

3.2 Data Manager

The Data Manager features two special-purpose databases.

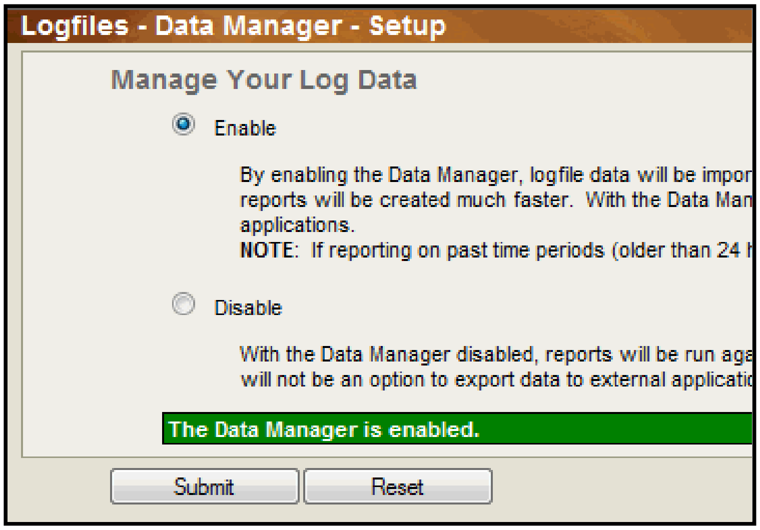
Dashboard (High-level) Database. This database is designed to meet a very different set of requirements. Its job is to store high-level data that are used to generate sophisticated summary-level trending and comparison charts on the Dashboard.

Mass Storage (Low-level) Database. This highly scalable database is designed to store huge amounts of detailed, 'low-level' Web-use data. The reports that are supported by this database include audit detail reports that provide every URL visited by a user, category or domain.

3.2.1 Required Setup

Before using the optional Data Manager, you must enable it. When you do so, the product imports your logfile data into the Dashboard (high-level) and Mass Storage (low-level) databases. These databases greatly increase the speed with which Web-use reports can be generated. With the Data Manager enabled, you can also export data to external applications.

1. Go to **Logfiles – Data Manager** and click on the **Enable** link.
2. Select the **Enable** radio button to enable the Data Manager.



Logfiles - Data Manager - Setup

Manage Your Log Data

● Enable

By enabling the Data Manager, logfile data will be impor
reports will be created much faster. With the Data Man
applications.
NOTE: If reporting on past time periods (older than 24 h

○ Disable

With the Data Manager disabled, reports will be run aga
will not be an option to export data to external applicatio

The Data Manager is enabled.

3. Click **Submit**. A screen containing instructions for importing your logfile data will pop up.

3.2.2 Settings

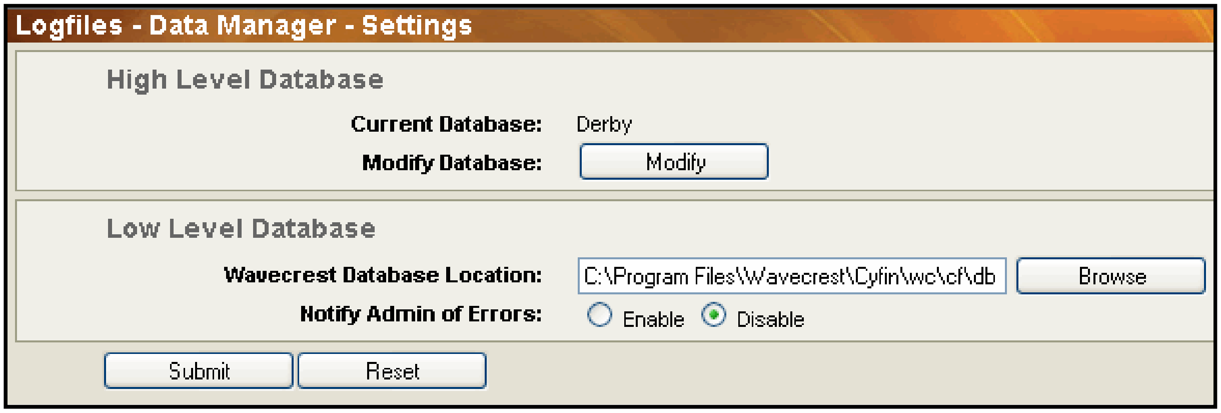
On this screen you have the ability to configure the Dashboard (high-level) database and Mass Storage (low-level) database. The Dashboard (high-level) database is necessary if you want to view Dashboard data, and the Mass Storage (low-level) database is essential to using Interactive reports and getting fast reports. With the Dashboard (high-level) database, you have the option to use the default Derby database, or configure your own MySQL or MSSQL database.

3.2.2.1 Dashboard (High-Level) Database Settings

3.2.2.1.1 Derby Configuration

The following steps to change the default Location and Bulk Insert Folder paths is optional. Derby is the default database for the Dashboard and no configuration is necessary once you have enabled the Data Manager.

1. To change the default Location and Bulk Insert Folder paths, go to **Logfiles - Data Manager** and click on the **Settings** link.



Logfiles - Data Manager - Settings

High Level Database

Current Database: Derby

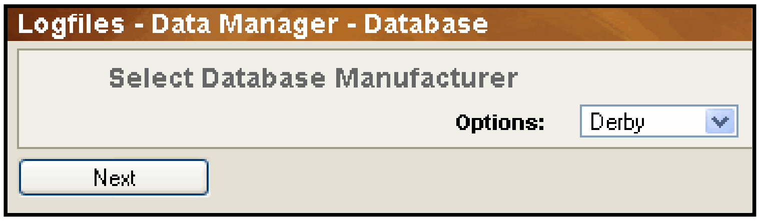
Modify Database:

Low Level Database

Wavecrest Database Location: C:\Program Files\Wavecrest\Cyfin\wc\cf\db

Notify Admin of Errors: ○ Enable ● Disable

2. Click **Modify** and a Wizard will pop up.
3. Select *Derby* as the Database Manufacturer and click **Next**.

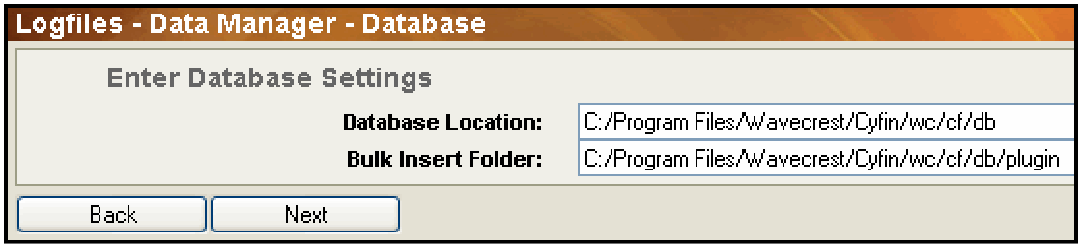


Logfiles - Data Manager - Database

Select Database Manufacturer

Options: Derby

4. A screen notifying you that the next steps are optional will appear. If you want to proceed, click **Next**.



Logfiles - Data Manager - Database

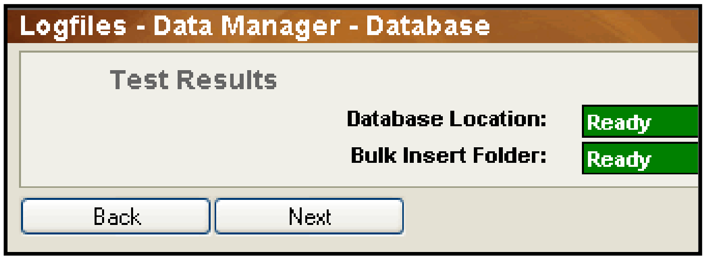
Enter Database Settings

Database Location: C:/Program Files/Wavecrest/Cyfin/wc/cf/db

Bulk Insert Folder: C:/Program Files/Wavecrest/Cyfin/wc/cf/db/plugin

5. Change the **Database Location** and/or **Bulk Insert Folder** location and click **Next**.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.



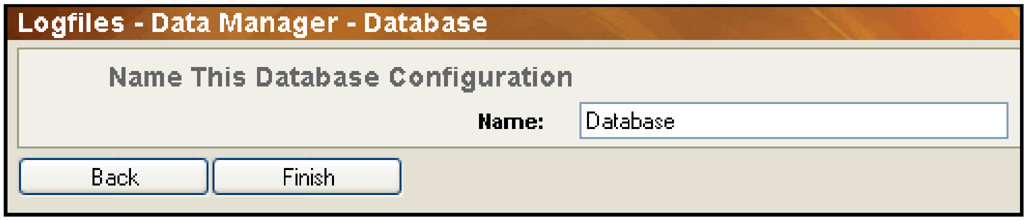
Logfiles - Data Manager - Database

Test Results

Database Location: Ready

Bulk Insert Folder: Ready

6. You should get green Ready status indicators. If so, you can go ahead and click **Next**.



Logfiles - Data Manager - Database

Name This Database Configuration

Name: Database

7. Name the database configuration and click **Finish**.

3.2.2.1.2 MySQL Configuration

The initial below instructions are for creating a new MySQL database.

If you already have a MySQL Server database created, you may proceed to the "Connect to MySQL Server" steps.

3.2.2.1.2.1 Allocate Memory to Database

1. Go to the C:/Program Files/MySQL/MySQL Server 5.x/ folder and open the file my.ini in Notepad. (This could also be called my.cnf on some systems.)
2. Edit the file by changing the **innodb_buffer_pool_size** (near the bottom of the file) value to 50% of your RAM. This is the recommended minimum. For example, if your computer has 2G of RAM, and you wish to allocate half of that to running the MySQL Server, set **innod_buffer_pool_size=1024M**.
3. Save the file.

3.2.2.1.2.2 Create Database

***NOTE**: See optional GUI instructions for the MySQL Query Browser below.*

1. Open the **MySQL Command Line Client** by going to **Programs - MySQL - MySQL Server x.x - MySQL Line Client Command.**
2. Login as the username "root".
3. Enter the command "create database Superview;"
4. To verify it was created, enter the command "show databases;" and you should see the database Superview present.
5. Restart your MySQL Service. There are two ways you can do this.
    1. Go to **Services**, right click on the **MySQL** Service and click **Restart**.

       OR
    2. Sign in to the **MySQL Administrator** and use the **Service Control** options. Click the **Stop** button and when it changes to **Start**, click it again.

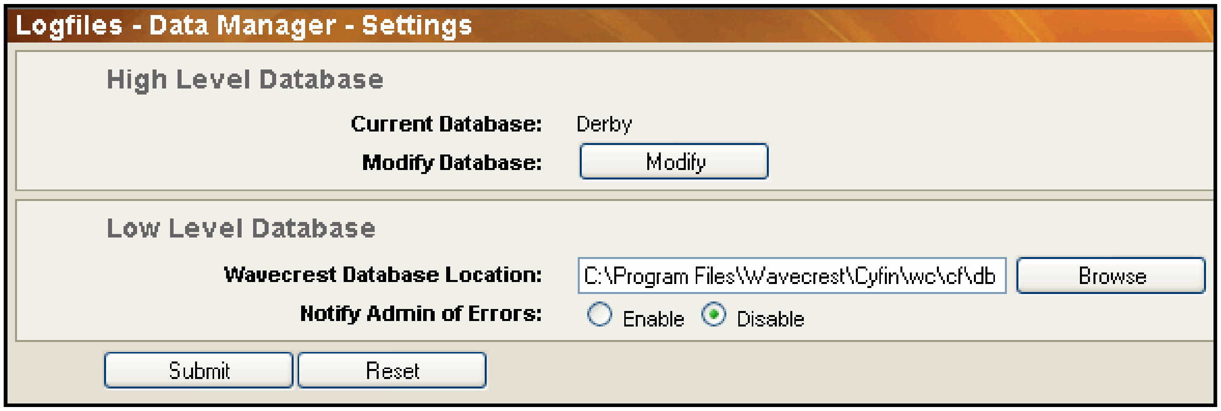
OR

1. Open the **MySQL Query Browser**.
2. Login as the username "root".
3. Right-mouse click on the **Schema Explorer** and click on **Create New Schema**.
4. In the pop-up box, enter "Superview" for the **Schma Name** and click **OK**.
5. Right-mouse click in the **Schemata** pane and click **Refresh**. You should now also be able to see the Superview database.
6. Restart your MySQL Service. There are two ways you can do this.
    1. Go to **Services**, right click on the **MySQL** Service and click **Restart**.

       OR
    2. Sign in to the **MySQL Administrator** and use the **Service Control** options. Click the **Stop** button and when it changes to **Start**, click it again.

3.2.2.1.2.3 Connect to MySQL Database

1. Go to **Logfiles - Data Manager** and click on the **Settings** link.



Logfiles - Data Manager - Settings

High Level Database

Current Database: Derby

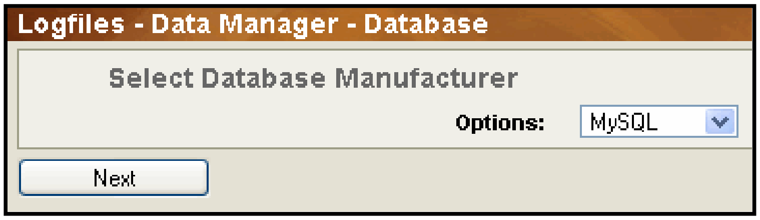
Modify Database:

Low Level Database

Wavecrest Database Location: C:\Program Files\Wavecrest\Cyfin\wc\cf\db

Notify Admin of Errors: ○ Enable ● Disable

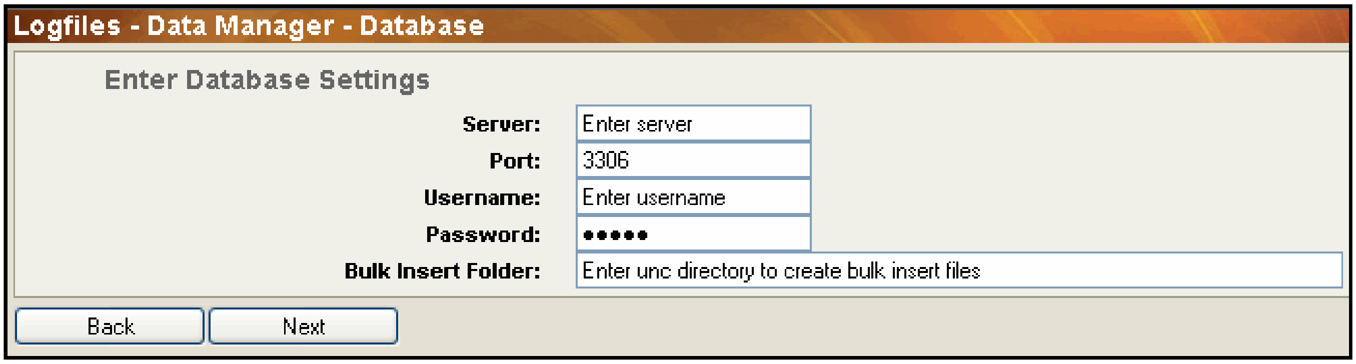
2. Click **Modify** and a Wizard will pop up.


Logfiles - Data Manager - Database

Select Database Manufacturer

Options: MySQL

3. Select *MySQL* as the Database Manufacturer and click **Next**.
4. A screen notifying you how to create a new MySQL database will appear. These will be the same instructions as above. Once you have completed them, click **Next**.


Logfiles - Data Manager - Database

Enter Database Settings

Server: Enter server

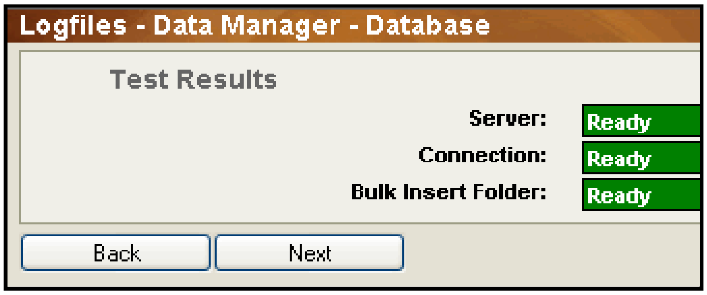
Port: 3306

Username: Enter username

Password: •••••

Bulk Insert Folder: Enter unc directory to create bulk insert files

5. Enter the **Server**, **Port**, **Username** and **Password** for your MySQL database.
6. Type in a UNC path for the Bulk Insert Folder and click **Next**.


Logfiles - Data Manager - Database

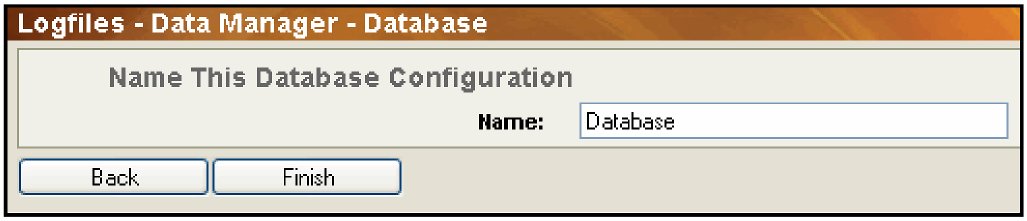
Test Results

Server: Ready

Connection: Ready

Bulk Insert Folder: Ready

7. You should get green Ready status indicators. If so, you can go ahead and click **Next**.


Logfiles - Data Manager - Database

Name This Database Configuration

Name: Database

8. Name the database configuration and click **Finish**.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

3.2.2.1.3 MSSQL Configuration

The initial below instructions are for creating a new MySQL database.

If you already have a MySQL Server database created, you may proceed to the "Connect to MSSQL Server" steps.

3.2.2.1.3.1 Setup SQL Server Authentication

1. Open the **SQL Server Management Studio**.
2. Login to your SQL server.
3. Right-mouse click on your SQL Server node instance in the **Object Explorer** and select **Properties**.
4. Select the Security page.
5. Under the Server authentication section, select **SQL Server** and **Windows Authentication** mode and then click **OK.**

3.2.2.1.3.2 Create Database Superview

1. Right-mouse click on **Databases** under your SQL Server node in the **Object Explorer** and select **New Database**.
2. In the **New Database** pop-up window, enter the database name *Superview* and then click **OK.**

3.2.2.1.3.3 Configure User Permissions

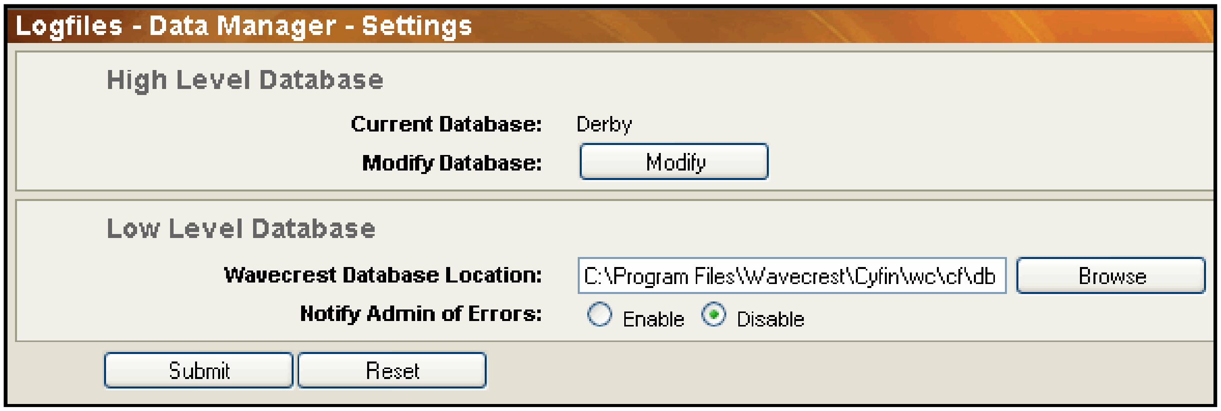
1. In your SQL Server node, expand Security in the **Object Explorer** until you see **Logins**.
2. Right-mouse click on **Logins** and select **New Login**.
3. In the **Login - New** popup window, enter *wavecrest* for the **Login name**.
4. Select the **SQL Server Authentication** radio button and enter a **Password** and **Confirm Password**.
5. Uncheck **User must change password at next login**, **Enforce password policy**, and **Enforce password expiration**.
6. Select the **Server Roles** page and ensure **public** and **sysadmin** are selected.
7. Select the **Status** page and ensure **Login** is enabled and click **OK**.
8. Close or minimize the **Microsoft SQL Server Management Studio**.

3.2.2.1.3.4 Allow TCP/IP

1. Open **Microsoft SQL Server 2008 - Configuration Tools - SQL Server Configuration Manager**.
2. Expand **SQL Server Network Configuration** and click on **Protocols for MSSQLSERVER**.
3. If **TCP/IP** is not enabled, right-mouse click and set it to **Enabled**.
4. Restart the SQL Server by selecting the server icon and clicking **Restart** for this change to take effect.

3.2.2.1.3.5 Connect to MSSQL Database

1. Go to **Logfiles - Data Manager** and click on the **Settings** link.



Logfiles - Data Manager - Settings

High Level Database

Current Database: Derby

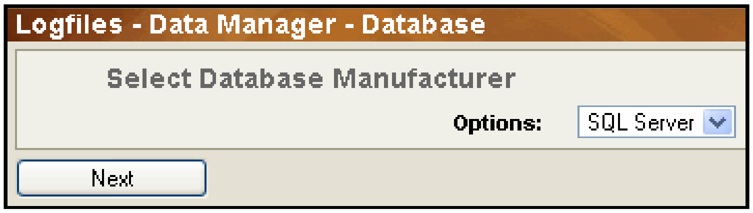
Modify Database: Modify

Low Level Database

Wavecrest Database Location: C:\Program Files\Wavecrest\Cyfin\wc\cf\db

Notify Admin of Errors: ○ Enable ● Disable

2. Click **Modify** and a Wizard will pop up.



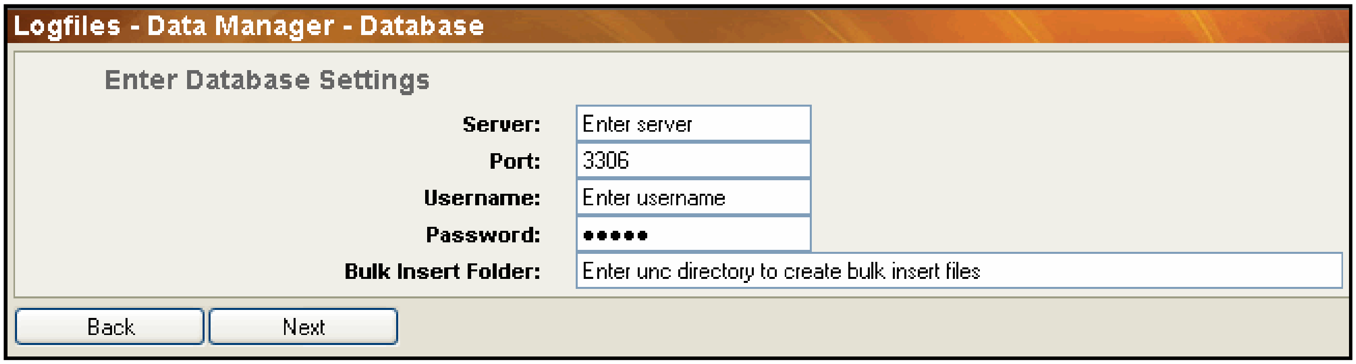
Logfiles - Data Manager - Database

Select Database Manufacturer

Options: SQL Server

3. Select *SQL Server* as the Database Manufacturer and click **Next**.

4. A screen notifying you how to create a new MSSQL database will appear. These will be the same instructions as above. Once you have completed them, click **Next**.



Logfiles - Data Manager - Database

Enter Database Settings

Server: Enter server

Port: 3306

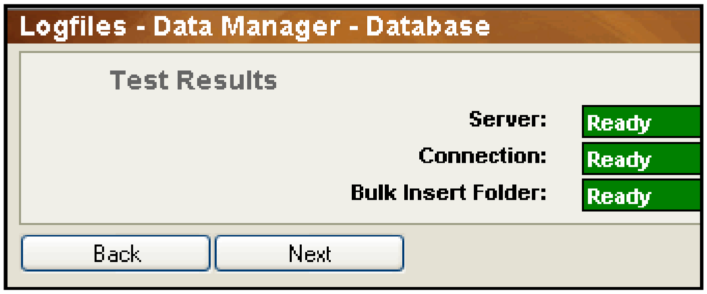
Username: Enter username

Password: ●●●●●

Bulk Insert Folder: Enter unc directory to create bulk insert files

5. Enter the **Server**, **Port**, **Username** and **Password** for your MSSQL database.

6. Type in a UNC path for the Bulk Insert Folder and click **Next**.



Logfiles - Data Manager - Database

Test Results

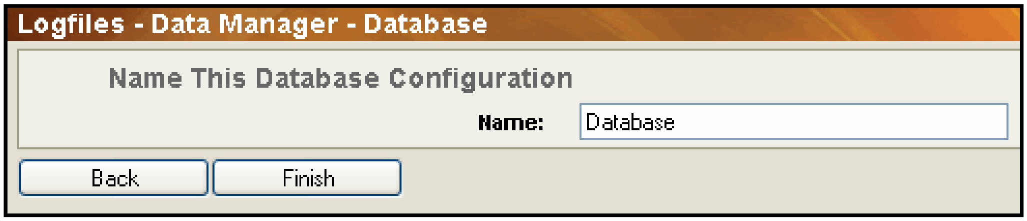
Server: Ready

Connection: Ready

Bulk Insert Folder: Ready

7. You should get green Ready status indicators. If so, you can go ahead and click **Next.**

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.



Logfiles - Data Manager - Database

Name This Database Configuration

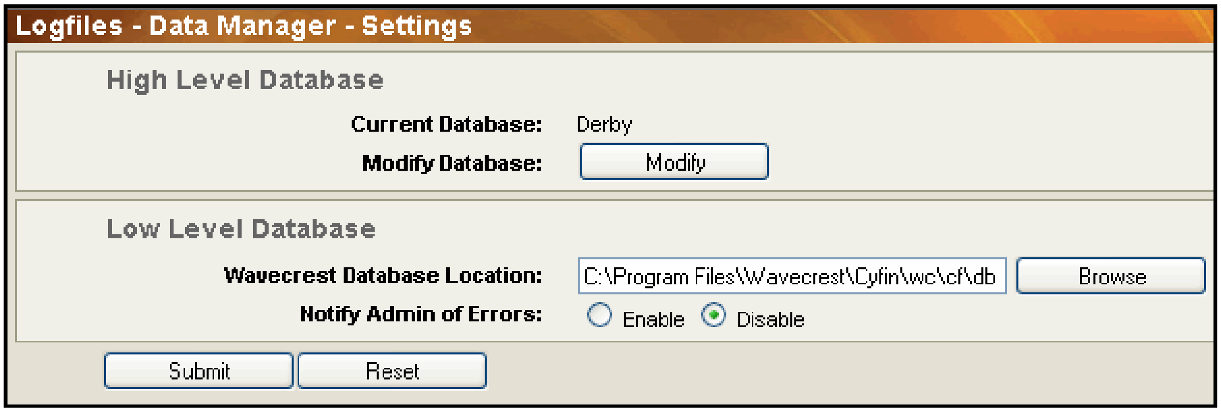
Name: Database

8. Name the database configuration and click **Finish**.

3.2.2.2 Mass Storage (Low-Level) Database

With the **Data Manager - Settings** screen, you can choose a location to store the imported data. It also lets you choose whether or not to receive email notifications of suspected data errors, if they occur during the import.

1. Go to **Logfiles – Data Manager** and click on the **Settings** link.



Logfiles - Data Manager - Settings

High Level Database

Current Database: Derby

Modify Database: Modify

Low Level Database

Wavecrest Database Location: C:\Program Files\Wavecrest\Cyfin\wc\cf\db

Notify Admin of Errors: ○ Enable ● Disable

2. Type in the path or use the **Browse** button to select the Database Location.
3. Choose whether or not to receive email notification regarding import data errors. Use the radio buttons to **Enable** or **Disable** this feature.
4. Click **Submit** to apply your settings.

3.2.3 Import Logfile Data

This section provides instructions for using the "Import Data" features within the Data Manager. These features help you import and manage logfile data very efficiently. You can configure the product to import the data automatically on a daily basis or on a manual basis.

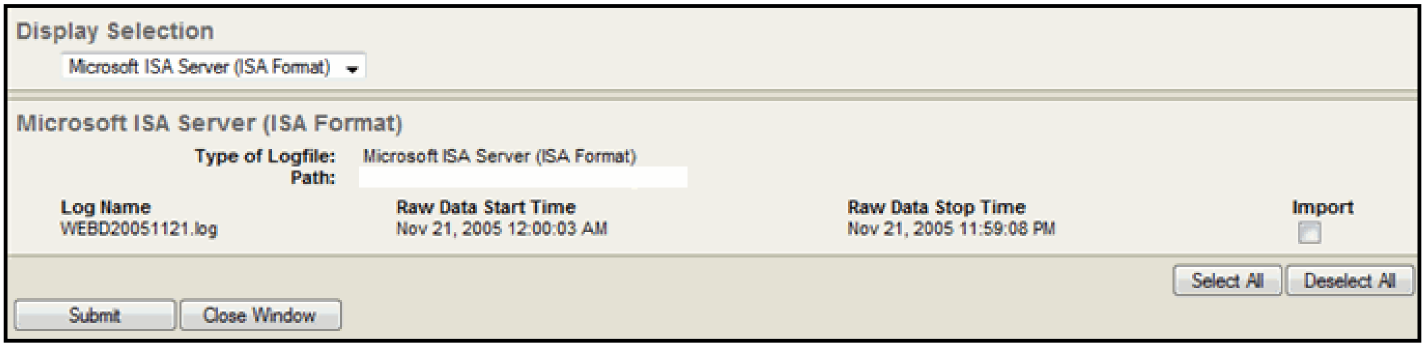
3.2.3.1 Manual Import

This screen lets you manually import configured logfiles into the Data Manager. When logs are available, the screen lists them and provides check boxes for selecting the logs you want to import.

IMPORTANT: Because the process of generating import data is memory-intensive, we recommend increasing the product's memory setting on the **Setup - Memory** screen. As a general guideline, increase the setting to approximately half of the actual available memory on the machine.
***NOTE**: Generating import data does not affect the original logs. This product only reads logfile data; it does not modify logfiles in any way.*

1. Go to **Logfiles – Data Manager** and click on the **Import Data** link.
2. Click on the **Manual** link under **Import**. A list of logs available for import will appear.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.



Display Selection

Microsoft ISA Server (ISA Format)

Microsoft ISA Server (ISA Format)

Type of Logfile: Microsoft ISA Server (ISA Format)
Path:

Log Name	Raw Data Start Time	Raw Data Stop Time	Import
WEBD20051121.log	Nov 21, 2005 12:00:03 AM	Nov 21, 2005 11:59:08 PM	□

3. Check the boxes of the logs that you wish to import. If you wish to import all of the logs, you can click on the **Select All** button at the end of the logfile list.
4. Click **Submit** to import the logs into the database.

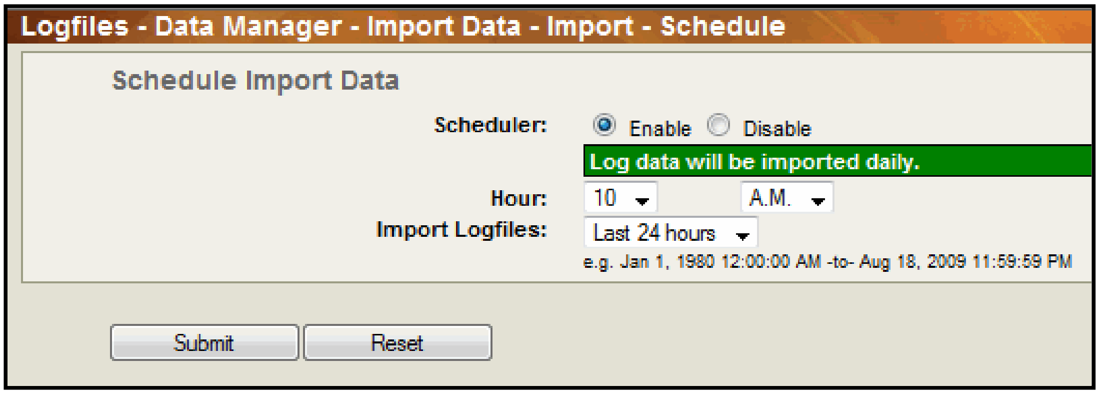
3.2.3.2 Scheduled Import

This screen lets you schedule the import of logfiles into the internal database. Be sure to enable the database in order to use this feature.

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

***NOTE**: Generating import data does not affect the original logs. This product only reads logfile data; it does not modify logfiles in any way.*

1. Go to **Logfiles – Data Manager** and click on the **Import Data** link.
2. Click on the **Schedule** link under **Import**.



Logfiles - Data Manager - Import Data - Import - Schedule

Schedule Import Data

Scheduler: ● Enable ○ Disable

Log data will be imported daily.

Hour: 10 A.M.

Import Logfiles: Last 24 hours

e.g. Jan 1, 1980 12:00:00 AM -to- Aug 18, 2009 11:59:59 PM

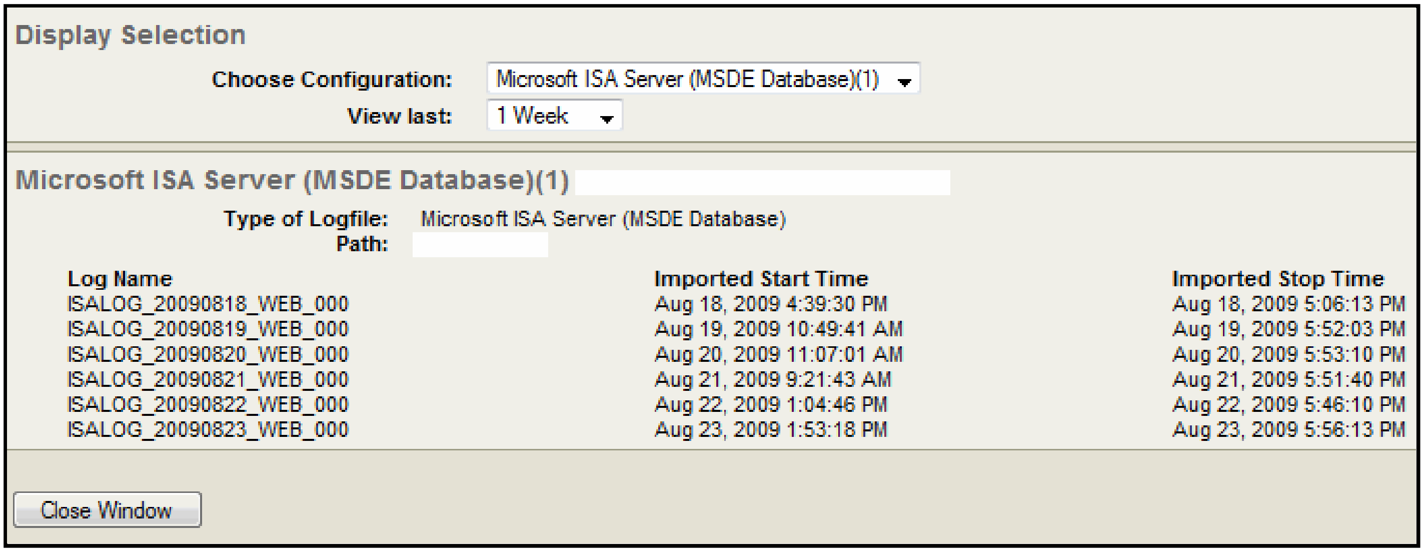
3. Select the **Enable** radio button to schedule import data.
4. Select the **Hour** to begin importing data. If you have large amounts of data, you may want to schedule the import data process to run when Web traffic is low.
5. Using the pulldown menu, select if you want to **Import Logfiles** from the *last 24 hours* or If you want to import *all* logfiles.
6. Click **Submit** to apply your changes.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

3.2.4 View Data

This is a display-only feature. It displays the Data Manager’s imported logfile data. For each import data configuration, this screen displays the (Configuration) Name, Type of Logfile and Path. For each individual logfile it displays the Log Name, Imported Start Time, and Imported Stop Time.

To view your logfiles, go to **Logfiles – Data Manager** and click on the **Import Data** link. Then, click on the **Viewer** link.



Display Selection

Choose Configuration: Microsoft ISA Server (MSDE Database)(1)

View last: 1 Week

Microsoft ISA Server (MSDE Database)(1)

Type of Logfile: Microsoft ISA Server (MSDE Database)

Path:

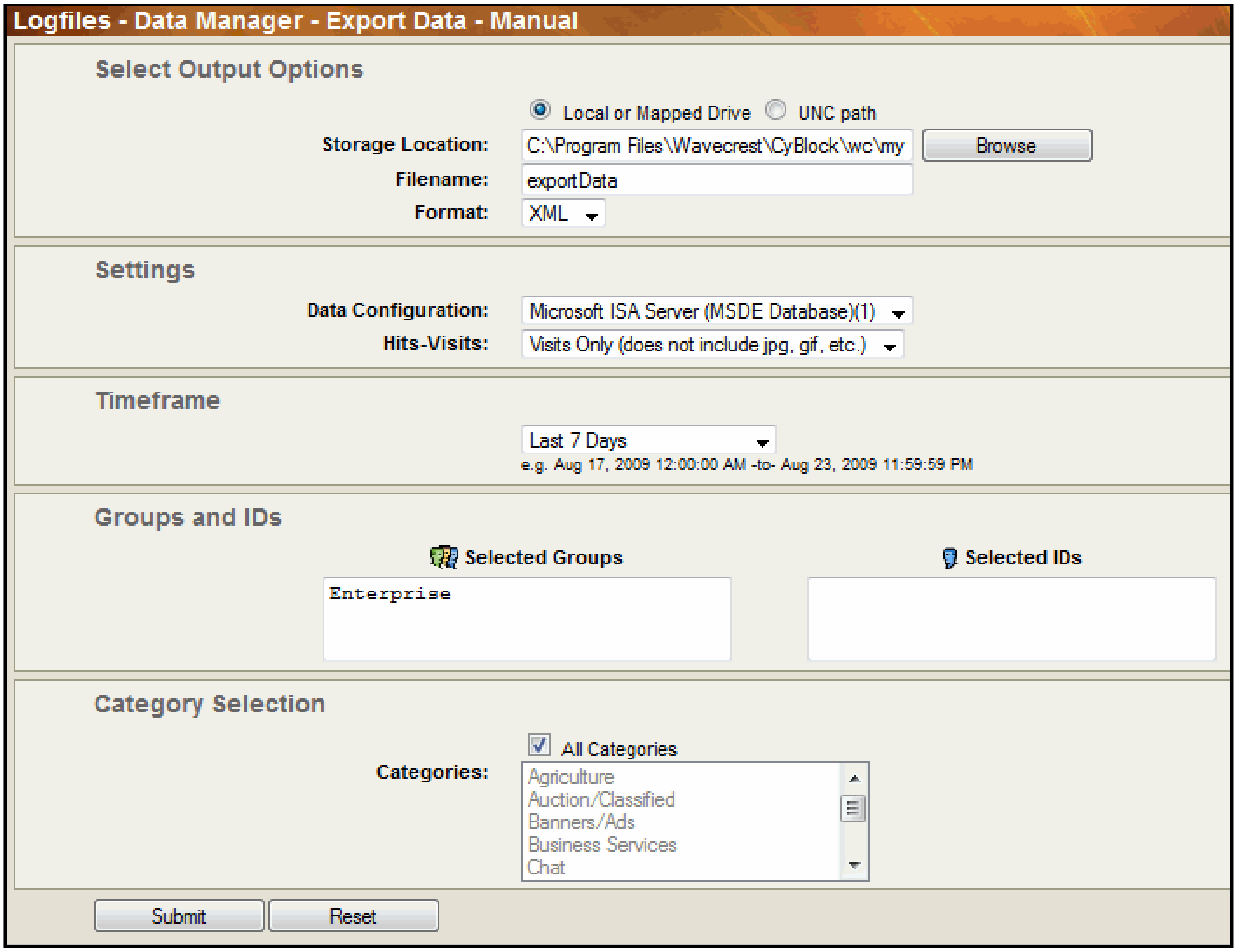
Log Name	Imported Start Time	Imported Stop Time
ISALOG_20090818_WEB_000	Aug 18, 2009 4:39:30 PM	Aug 18, 2009 5:06:13 PM
ISALOG_20090819_WEB_000	Aug 19, 2009 10:49:41 AM	Aug 19, 2009 5:52:03 PM
ISALOG_20090820_WEB_000	Aug 20, 2009 11:07:01 AM	Aug 20, 2009 5:53:10 PM
ISALOG_20090821_WEB_000	Aug 21, 2009 9:21:43 AM	Aug 21, 2009 5:51:40 PM
ISALOG_20090822_WEB_000	Aug 22, 2009 1:04:46 PM	Aug 22, 2009 5:46:10 PM
ISALOG_20090823_WEB_000	Aug 23, 2009 1:53:18 PM	Aug 23, 2009 5:56:13 PM

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

3.2.5 Export Data

With the export data feature, you can manually export data to a file for use in external applications, e.g., spreadsheets, report generators, relational databases, etc.

1. Go to **Logfiles – Data Manager** and click on the **Export Data** link.



Logfiles - Data Manager - Export Data - Manual

Select Output Options

● Local or Mapped Drive ○ UNC path

Storage Location: C:\Program Files\Wavecrest\CyBlock\wc\my

Filename: exportData

Format: XML

Settings

Data Configuration: Microsoft ISA Server (MSDE Database)(1)

Hits-Visits: Visits Only (does not include jpg, gif, etc.)

Timeframe

Last 7 Days

e.g. Aug 17, 2009 12:00:00 AM -to- Aug 23, 2009 11:59:59 PM

Groups and IDs

Selected Groups	Selected IDs
Enterprise	

Category Selection

Categories: ☑ All Categories

Agriculture
Auction/Classified
Banners/Ads
Business Services
Chat

2. Choose the ‘destination’ directory location type by clicking on the radio button for **Local or Mapped Drive** or **UNC path**.

3. Indicate a **Storage Location** for the export data. If the drive is a Local or Mapped Drive, use the **Browse** button to locate the directory for saving the export file to. If the directory is on a UNC path, type in the full address here manually.

4. Type in a **Filename** for the export. ***NOTE**: If you leave a default name in this box, any previous information written to a file of that name in the same location will be overwritten.*

5. Use the **Format** pull-down menu to select either *CSV* or *XML* file format.

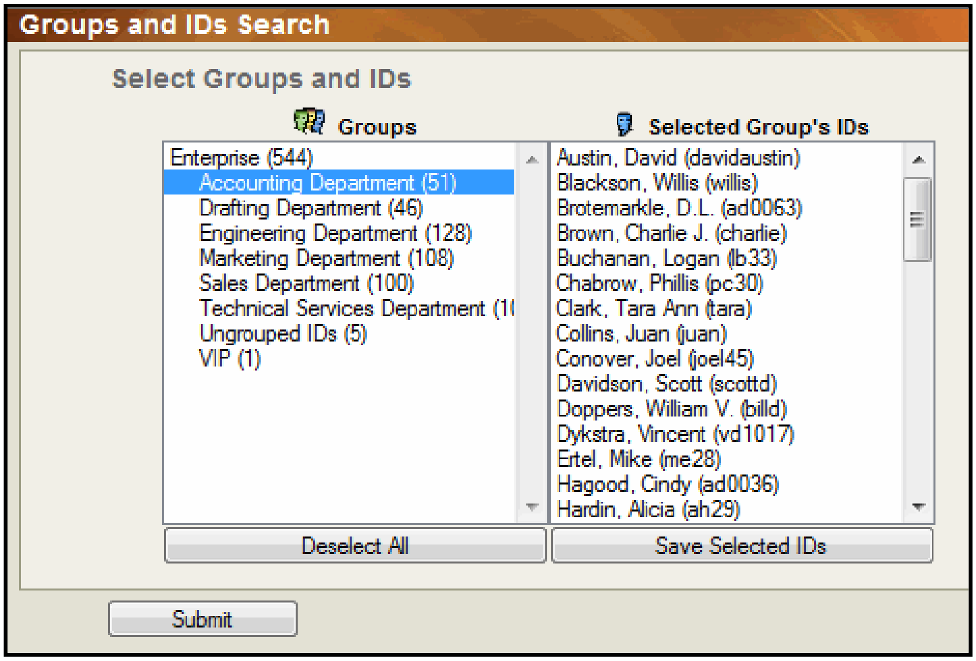
6. In the **Data Configuration** field, you can choose to export a single logfile configuration or all logfile configurations.

7. Use the **Hits-Visits** pull-down menu to select whether you want all hits and visits exported or just visits.

8. Select the **Start Date/Time** and **Stop Date/Time** for the data you want to export.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

9. Choose the Groups and/or IDs whose data you want to export. If you know the Groups and/or IDs whose data you want exported, you can type them in the appropriate text boxes. Alternatively, click on the **Search** button to select the Group(s) and/or ID(s). The following screen will pop up in a separate window.



Groups and IDs Search

Select Groups and IDs

Groups

Enterprise (544)
Accounting Department (51)
Drafting Department (46)
Engineering Department (128)
Marketing Department (108)
Sales Department (100)
Technical Services Department (1(
Ungrouped IDs (5)
VIP (1)

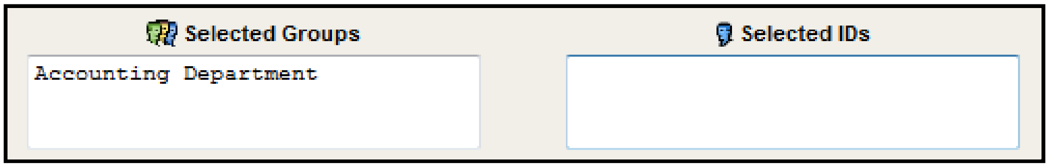
Selected Group's IDs

Austin, David (davidaustin)
Blackson, Willis (willis)
Brotemarkle, D.L. (ad0063)
Brown, Charlie J. (charlie)
Buchanan, Logan (lb33)
Chabrow, Phillis (pc30)
Clark, Tara Ann (tara)
Collins, Juan (juan)
Conover, Joel (joel45)
Davidson, Scott (scottd)
Doppers, William V. (billd)
Dykstra, Vincent (vd1017)
Ertel, Mike (me28)
Hagood, Cindy (ad0036)
Hardin, Alicia (ah29)

10. Several options are available for selecting Groups and IDs whose data you want exported. You can select one Group or ID or you can select multiple Groups and/or IDs.

- **Selecting a Group or ID**: If you are only selecting one Group or ID, select that Group or ID by clicking on it so that it is highlighted, and click **Submit**.
- **Selecting more than one Group**: If you are selecting multiple Groups, hold down the control key and click on the Groups you want, then click **Submit**.
- **Selecting more than one ID**: If you are selecting multiple IDs, hold down the control key and click on the IDs to select them. If the IDs you want to select are in more than one group, when you are finished selecting the IDs in a Group, you must click the **Save Selected IDs** button before moving on to the next Group to select additional IDs. When you are finished selecting all of your IDs, click on the **Submit** button.
- **Selecting both Group(s) and ID(s)**: If you are selecting IDs and Groups (or even one ID and one Group), you must select your IDs first, making sure you click on the **Save Selected IDs** button after making your ID selections in each Group. When you have finished selecting the ID(s), then make your Group selection(s). Click **Submit** when you have finished.

The Groups and IDs that you have selected will appear in the **Groups and IDs** field.



Selected Groups

Accounting Department

Selected IDs

***NOTE**: You can delete a Group or ID in the **Groups and IDs** field by highlighting the Group or ID and hitting the Delete key on your keyboard.*

11. Select the **Categories** that you want to include in your export data. If you want data for all categories exported, select the **All Categories** check box.

12. Click **Submit** to export the data.

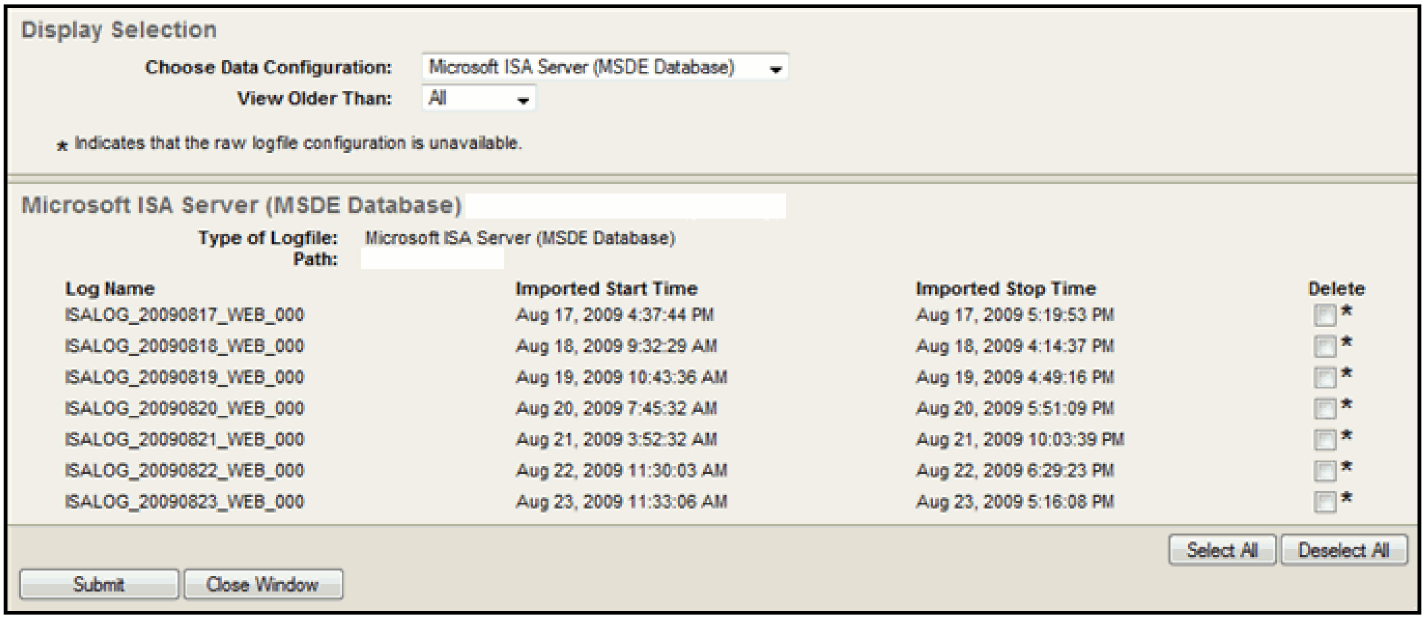
© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

3.2.6 Delete Data

This feature allows you to delete database data. You can delete data manually or schedule for deletions to occur automatically once a day.
***NOTE**: Deleting database data does not affect logs or logfile data. Wavecrest products only read and process logfile data; they do not delete, alter or distort logfiles in any way.*

3.2.6.1 Manually Delete Data

1. Go to **Logfiles – Data Manager** and click on the **Import Data** link.
2. Click on the **Manual** link under **Delete**.



Display Selection

Choose Data Configuration: Microsoft ISA Server (MSDE Database)
View Older Than: All

★ Indicates that the raw logfile configuration is unavailable.

Microsoft ISA Server (MSDE Database)

Type of Logfile: Microsoft ISA Server (MSDE Database)
Path:

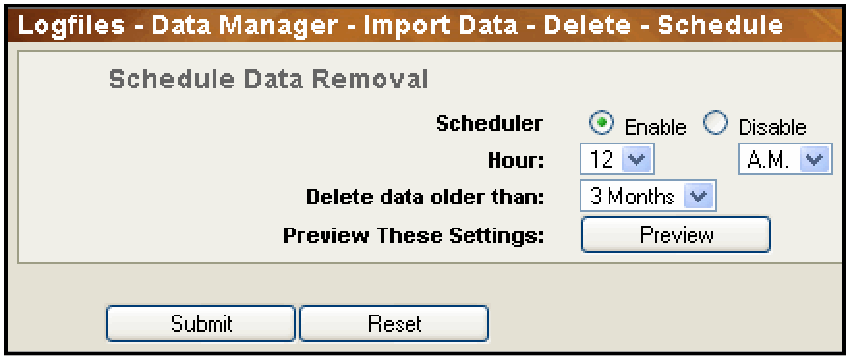
Log Name	Imported Start Time	Imported Stop Time	Delete
ISALOG_20090817_WEB_000	Aug 17, 2009 4:37:44 PM	Aug 17, 2009 5:19:53 PM	□ ★
ISALOG_20090818_WEB_000	Aug 18, 2009 9:32:29 AM	Aug 18, 2009 4:14:37 PM	□ ★
ISALOG_20090819_WEB_000	Aug 19, 2009 10:43:36 AM	Aug 19, 2009 4:49:16 PM	□ ★
ISALOG_20090820_WEB_000	Aug 20, 2009 7:45:32 AM	Aug 20, 2009 5:51:09 PM	□ ★
ISALOG_20090821_WEB_000	Aug 21, 2009 3:52:32 AM	Aug 21, 2009 10:03:39 PM	□ ★
ISALOG_20090822_WEB_000	Aug 22, 2009 11:30:03 AM	Aug 22, 2009 6:29:23 PM	□ ★
ISALOG_20090823_WEB_000	Aug 23, 2009 11:33:06 AM	Aug 23, 2009 5:16:08 PM	□ ★

3. Select the **Data Configuration** you want to view or select *All*. (This option will only be available if you have more than one data configuration.)
4. Select the database data you want to see by using the **View Older Than** pulldown menu.
5. Select the check boxes of the imported data that you want to delete. If you want to delete all data, click on the **Select All** button at the bottom of the screen.
6. Click **Submit** to delete your selections.

***CAUTION**: If you delete data from the database, you will not be able to get Dashboard reports on that data.*

3.2.6.2 Schedule Automatic Data Deletion

1. Go to **Logfiles - Data Manager** and click on the **Import Data** link.
2. Click on the **Schedule** link under **Delete**.



Logfiles - Data Manager - Import Data - Delete - Schedule

Schedule Data Removal

Scheduler ● Enable ○ Disable
Hour: 12 A.M.
Delete data older than: 3 Months
Preview These Settings: Preview

3. Select the **Enable** radio button to schedule for automatic deletions to occur.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

4. Select the **Hour**.
5. Using the **Delete data older than** pulldown menu, select what old data you want deleted automatically.
6. Click **Submit** to apply your settings.

CAUTION*: You will not be able to get Dashboard reports from any data deleted from the database.*

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

4.0 Web Policy Support

This product contains several configurable features that let you correlate and optimize its support to your organization's Web usage policy. That is, you can easily configure these features to customize the format and content of the product's reports, highlight inappropriate activity, and if applicable, block selected Web sites (CyBlock products only). In addition, if you need to, you can configure different policy settings for different sub-organizations and individual users.

Before configuring these features, make sure you have completed the Get Started section of this manual. 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 (Section 2 of the manual).

The following sections provide instructions for configuring these features:

- **Classify Categories** – Rate categories for acceptability based on your company's Web usage policy.
- **Custom Categories** – Create up to 12 custom categories for tracking Web sites of interest to your company.
- **Abuse Thresholds** – Set abuse thresholds to help you quickly detect Web abuse.

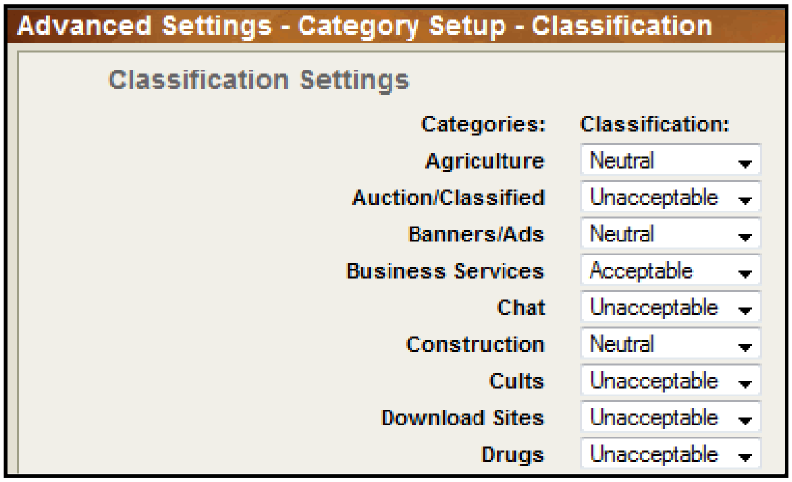
All Web policy support features are optional, but they can be very helpful in controlling and monitoring Web usage in the workplace. By using these features, you can greatly reduce the risk of legal liability, wasted bandwidth, security threats, and lost productivity. These same features help ensure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

4.1 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. Your classification settings will appear next to each category or URL on reports, making it easy for you to detect when Web abuse has occurred. ***NOTE****: For descriptions of each category, go to* ***Advanced Settings – Category Setup*** *and click on the* ***Descriptions*** *link.*

NOTE*: You can make changes to the classifications, but you cannot disable the "Classification" feature altogether.*

1. Go to **Advanced Settings – Category Setup** and click on the **Classification** link.

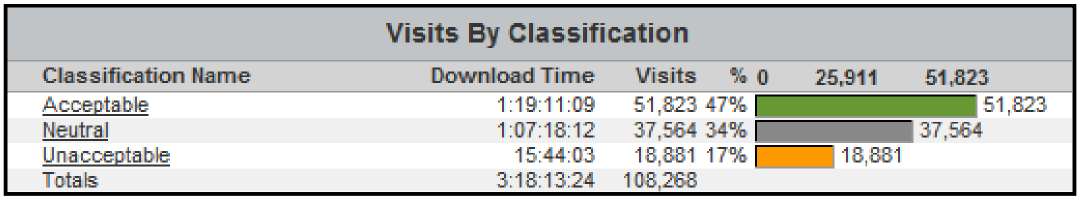


Advanced Settings - Category Setup - Classification

Classification Settings

Categories:	Classification:
Agriculture	Neutral
Auction/Classified	Unacceptable
Banners/Ads	Neutral
Business Services	Acceptable
Chat	Unacceptable
Construction	Neutral
Cults	Unacceptable
Download Sites	Unacceptable
Drugs	Unacceptable

2. Use the drop down menus next to each category to classify each as *Neutral*, *Acceptable*, or *Unacceptable*.
3. 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.



Visits By Classification

Classification Name	Download Time	Visits	%	0 25,911 51,823
Acceptable	1:19:11:09	51,823	47%	🟩 51,823
Neutral	1:07:18:12	37,564	34%	▨ 37,564
Unacceptable	15:44:03	18,881	17%	🟧 18,881
Totals	3:18:13:24	108,268		

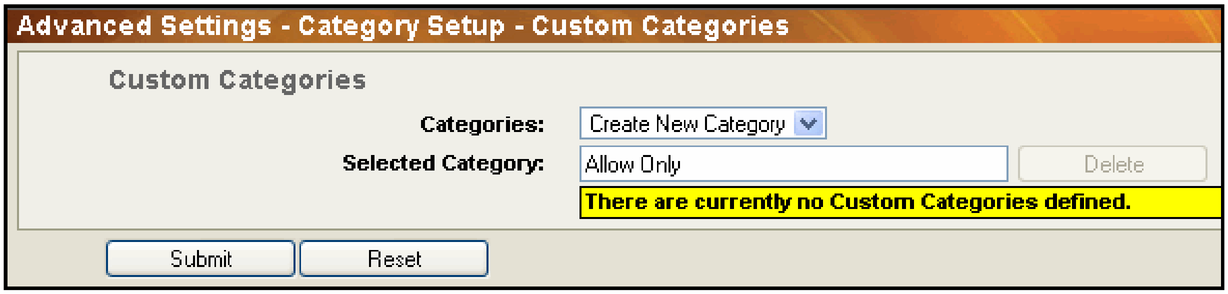
Note that each site is color coded based on the classification settings you made.
Green = Acceptable, Orange = Unacceptable, Gray = Neutral

4.2 Custom Categories

In addition to the 74 standard categories, you can create several custom categories for additional monitoring. Just like any other category, they can be viewed, be classified, and have an abuse threshold. Custom categories can be used for a variety of reasons, e.g., to create a white list, block additional Web sites or track employees' use of company intranet sites.

For the appliance, the custom categories accessible from the CyBlock Appliance interface are strictly for blocking purposes. Custom categories accessible from the Cyfin Reporter interface are for logging and reporting purposes.

1. To create a custom category, go to **Advanced Settings – Category Setup** and click on the **Custom Categories** link.



Advanced Settings - Category Setup - Custom Categories

Custom Categories

Categories: Create New Category

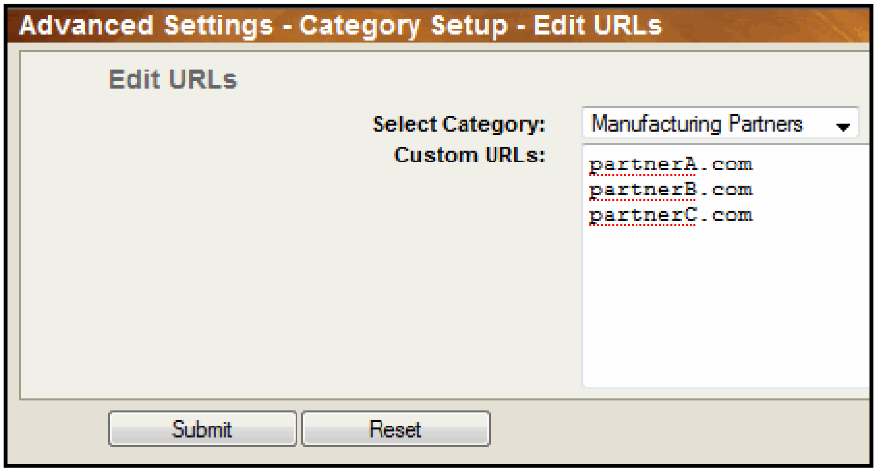
Selected Category: Allow Only

There are currently no Custom Categories defined.

2. Select *Create New Category*.
3. Type in a new name for the custom category in the **Selected Category** field. The name cannot exceed 50 characters.
4. Click **Submit**.

   NOTE*: If you know you want to create more than one custom category, repeat steps 1 through 4 until you have created names for all the categories you want to create.*

5. If you ever want to delete a custom category, select the category in the **Categories** field and click **Delete**.
6. Now that you have named your custom categories, you must add URLs to them.
7. Go to **Advanced Settings – Category Setup** and click on the **Edit URLs** link.



Advanced Settings - Category Setup - Edit URLs

Edit URLs

Select Category: Manufacturing Partners

Custom URLs:

```
partnerA.com
partnerB.com
partnerC.com
```

8. Using the **Select Category** pull down menu, select the custom category you just created.
9. In the text entry area for **Custom URLs**, type in the URLs.
   NOTE*: To add multiple URLs, simply type in the first URL and hit Enter; then type in the second URL and hit Enter, etc. Repeat until you have finished.*

(Optional) Add Wildcard Entries. You can use wildcards to add multiple URLs simultaneously. For example, let's assume that your organization has an intranet with multiple Web sites that use the organization's main Web site name as part of their URLs (e.g., ford.com). The main site name could be at the end, beginning, or middle of the intranet Web site names. Examples of wildcards used in such cases include:

- Intranet site name ends with ford.com/---------------------- enter *.ford.com/
- Intranet site name starts with http://www.ford------------- enter http://www.ford.*
- Intranet site name contains .ford------------------------------- enter *.ford.*

When you make wildcard entries such as these, this product will simultaneously add all of the applicable sites to the selected category.
CAUTION*: Adding wildcard URLs to the category could cause a performance slowdown.*

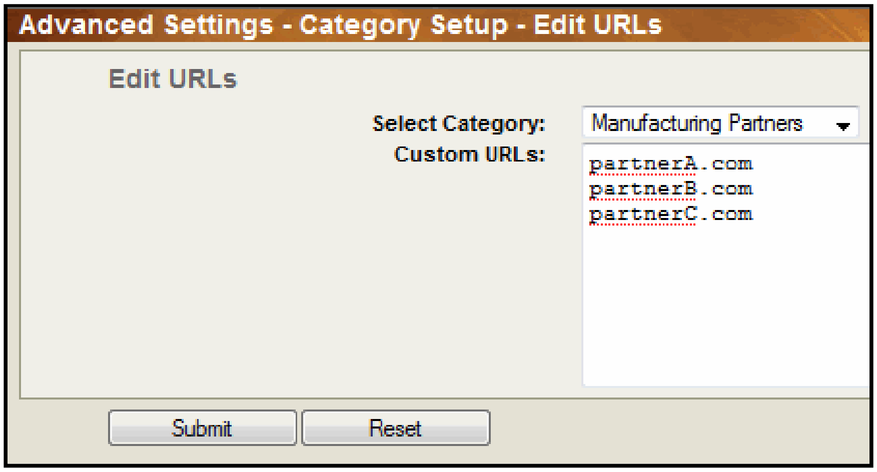
10. Click **Submit** to add the URLs.

4.3 Edit URLs in Categories

You can edit URLs in both standard and custom categories. More specifically, you can populate any of the categories with URLs of your own choosing.

***NOTE**: Your changes will override any future list downloads.*

1. Go to **Advanced Settings – Category Setup** and click on the **Edit URLs** link.



Advanced Settings - Category Setup - Edit URLs

Edit URLs

Select Category: Manufacturing Partners

Custom URLs:

```
partnerA.com
partnerB.com
partnerC.com
```

2. Using the **Select Category** pull down menu, select the category you want to edit.
3. **Add URLs**. In the text entry area for **Custom URLs**, type the URLs.
   ***NOTE**: To add multiple URLs, simply type in the first URL and hit **Enter**; then type in the second URL and hit **Enter**, etc. Repeat until you have included all the URLs.*

   (Optional) Add Wildcard Entries. You can use wildcards to add multiple URLs simultaneously. For example, let's assume that your organization has an intranet with multiple Web sites that use the organization's main Web site name as part of their URLs (e.g., ford.com). The main site name could be at the end, beginning, or middle of the intranet Web site names. Examples of wildcards used in such cases include:

   - Intranet site name ends with ford.com/--------------------- enter *.ford.com/
   - Intranet site name starts with http://www.ford------------ enter http://www.ford.*
   - Intranet site name contains .ford----------------------------- enter *.ford.*

   When you make wildcard entries such as these, this product will simultaneously add all of the applicable sites to the selected category.
   ***CAUTION**: Adding wildcard URLs to the category could cause a performance slowdown.*

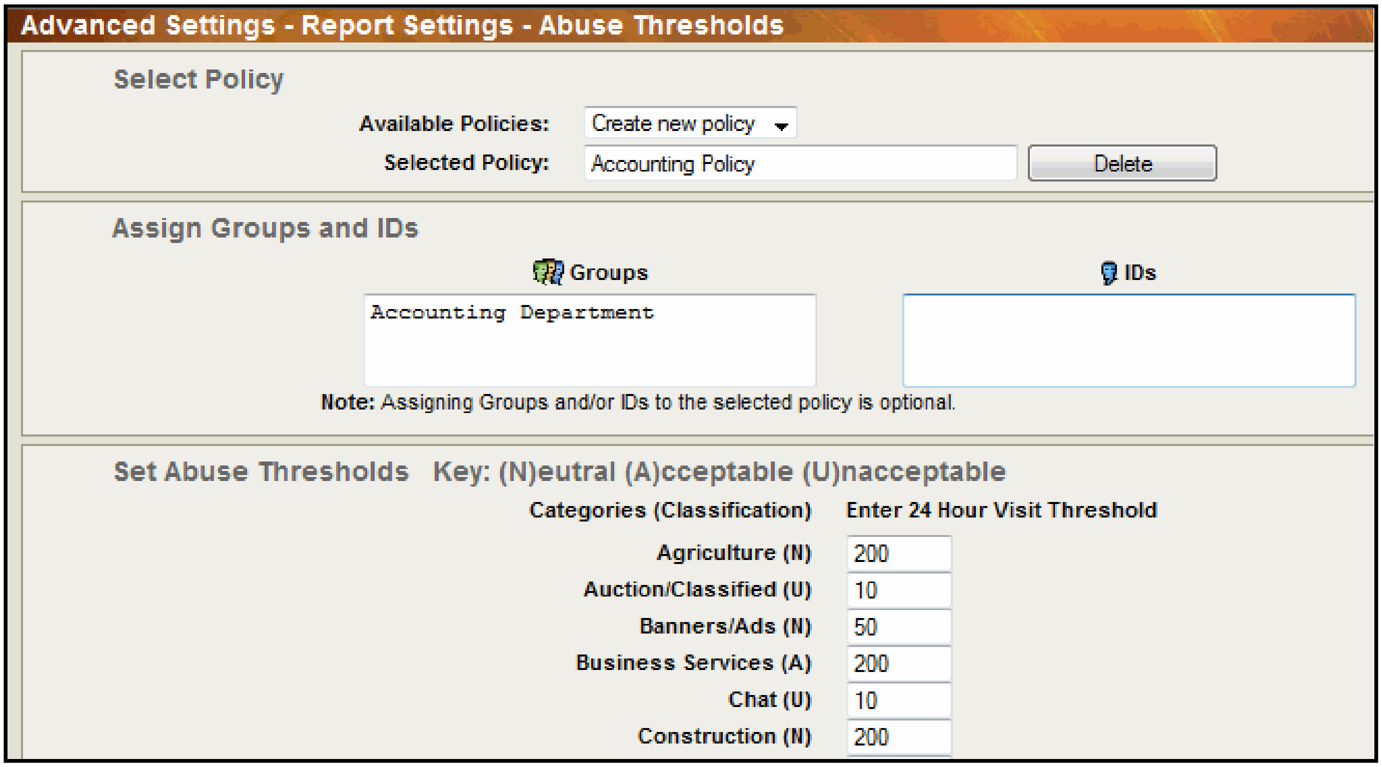
4. **Modify URLs**. Highlight the portion of the URL you would like to modify. Then type the changes.
5. **Delete URLs**. Highlight the URL you would like to delete and then hit the Delete key on your keyboard.
6. Click **Submit** to apply your changes.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

4.4 Abuse Thresholds

You can create and assign abuse threshold policies to users, groups, or the entire organization. Thresholding shows abuse that has occurred based on a customer-specified number of allowable (Web site) visits in a 24-hour period. The abuse threshold values are shown via bar graphs in reports.

1. Go to **Advanced Settings – Report Settings** and click on the **Abuse Thresholds** link.



Advanced Settings - Report Settings - Abuse Thresholds

Select Policy

Available Policies: Create new policy

Selected Policy: Accounting Policy

Assign Groups and IDs

Groups: Accounting Department

IDs:

Note: Assigning Groups and/or IDs to the selected policy is optional.

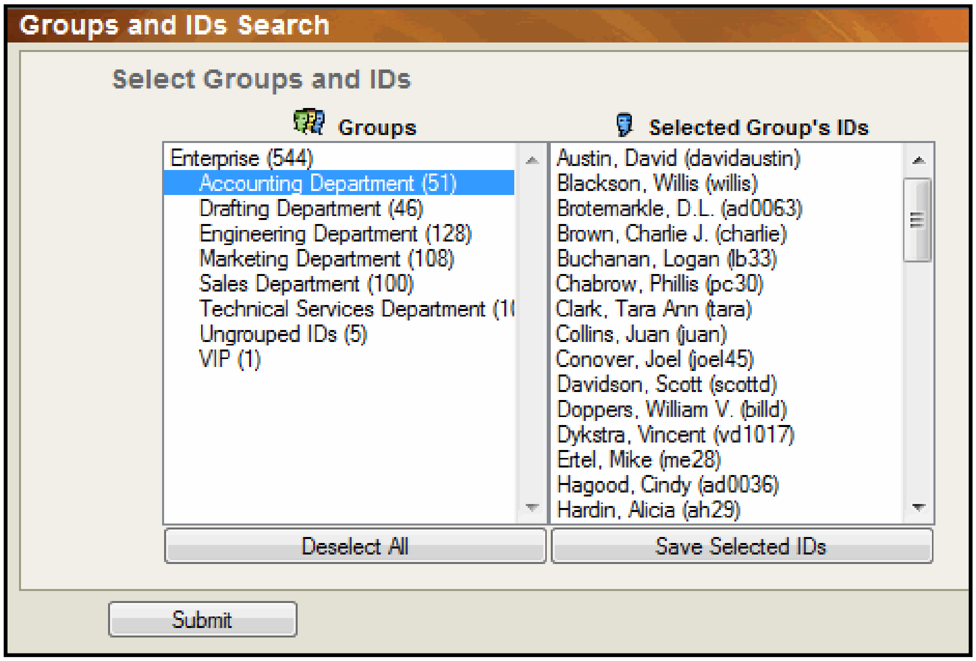
Set Abuse Thresholds Key: (N)eutral (A)cceptable (U)nacceptable

Categories (Classification)	Enter 24 Hour Visit Threshold
Agriculture (N)	200
Auction/Classified (U)	10
Banners/Ads (N)	50
Business Services (A)	200
Chat (U)	10
Construction (N)	200

2. Use the **Available Policies** pull down menu to select a policy. If you are creating a new policy, select *Create new policy*.

3. Enter a policy name in the **Selected Policy Box**.
*NOTE: This is also where you would delete a policy by clicking on the **Delete** button.*

4. Assign Groups and/or IDs to the block policy. If you know the Groups and/or IDs that you want assigned, you can type them in the appropriate text boxes. Otherwise, click on the **Search** button to select the applicable Group(s) and/or ID(s). The following screen will pop up in a separate window.



Groups and IDs Search

Select Groups and IDs

Groups:

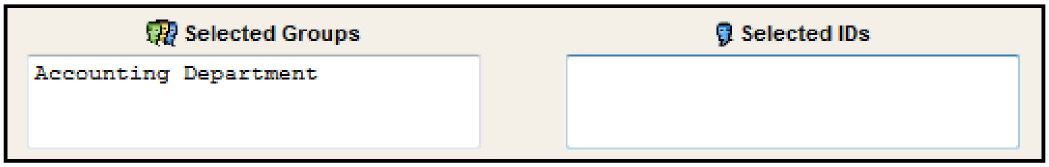
Enterprise (544)
Accounting Department (51)
Drafting Department (46)
Engineering Department (128)
Marketing Department (108)
Sales Department (100)
Technical Services Department (1
Ungrouped IDs (5)
VIP (1)

Selected Group's IDs:

Austin, David (davidaustin)
Blackson, Willis (willis)
Brotemarkle, D.L. (ad0063)
Brown, Charlie J. (charlie)
Buchanan, Logan (lb33)
Chabrow, Phillis (pc30)
Clark, Tara Ann (tara)
Collins, Juan (juan)
Conover, Joel (joel45)
Davidson, Scott (scottd)
Doppers, William V. (billd)
Dykstra, Vincent (vd1017)
Ertel, Mike (me28)
Hagood, Cindy (ad0036)
Hardin, Alicia (ah29)

5. Several options are available for selecting Groups and IDs. You can select one Group or ID, you can select multiple Groups or IDs, or you can select multiple Groups and IDs.
   - **Selecting a Group or ID**: If you are only selecting one Group or ID, select that Group or ID by clicking on it so that it is highlighted, and click **Submit**.
   - **Selecting more than one Group**: If you are selecting multiple Groups, hold down the control key and click on the Groups you want so that they are highlighted, then click **Submit**.
   - **Selecting more than one ID**: If you are selecting multiple IDs, hold down the control key and click on the IDs to select them. If the IDs you want to select are located in different Groups, you must click the **Save Selected IDs** button before moving on to the next Group to select additional IDs. If you do not do this, your previous selections will be lost. When you are finished selecting all of your IDs, click **Submit**.
   - **Selecting both Group(s) and ID(s)**: If you are selecting Groups and IDs (or even one Group and one ID), you must select your IDs first. Be sure to click on the **Save Selected IDs** button after making your ID selections in each Group. When you have finished selecting the ID(s), then make your Group selection(s). Click **Submit** when you have finished.

   The Groups and IDs that you have selected will appear in the Assign Groups and IDs field.



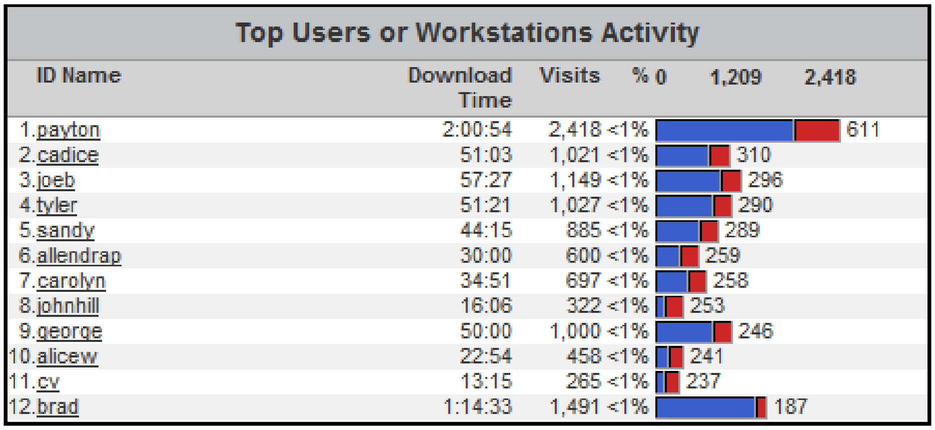
Selected Groups	Selected IDs
Accounting Department	

__NOTE__: You can delete a Group or ID in the __Assign Groups and IDs__ field by highlighting it and hitting Delete on your keyboard.

6. Next to each category, type in the number of Web page visits allowed to each category (before they are considered abuse) in a 24 hour period.

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

   Below is an example of a report that was run with abuse thresholding enabled.



Top Users or Workstations Activity

ID Name	Download Time	Visits	%	0 1,209 2,418
1.payton	2:00:54	2,418	<1%	611
2.cadice	51:03	1,021	<1%	310
3.joeb	57:27	1,149	<1%	296
4.tyler	51:21	1,027	<1%	290
5.sandy	44:15	885	<1%	289
6.allendrap	30:00	600	<1%	259
7.carolyn	34:51	697	<1%	258
8.johnhill	16:06	322	<1%	253
9.george	50:00	1,000	<1%	246
10.alicew	22:54	458	<1%	241
11.cv	13:15	265	<1%	237
12.brad	1:14:33	1,491	<1%	187

The blue in the bar graph represents the allowed visits, and the red shows where the user exceeded the threshold.

__NOTE__: When you "enable" abuse thresholding in a report, it stays enabled in all subsequent reports unless you "disable" it.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.0 Reporting

With this product, you can run high and low-level reports, schedule reports to run regularly, set report preferences, and review report policies. (For a complete listing of reports and their definitions, please see Appendix B.) You also have the option to use interactive reporting. Interactive reports allow you to drill down to get more detailed results on employee Web use by simply clicking on the report's elements, e.g., categories, ID names, and classification ratings. (To use Interactive Reporting, the Wavecrest Database must be enabled so that reports will run against Web-use data in the database. Interactive Reporting will not work if reports are run from the raw logfiles.)

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 internal intranet sites in your organization. The reports will show how often - and how - some of these sites are being used by your employees.

Before running any reports, be sure to complete the Get Started section of this manual. The Get Started section covers the required setup needed to start running reports. You also need to be familiar with the section on Web Policy Support (Section 4) 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.

In addition, if you plan to schedule reports, you must first make sure that you have (a) attached an email address to the Groups or IDs you wish to schedule reports for, (b) configured a directory for the reports to be saved in, or (c) both. You will find instructions on how to do this in Section 2.4.3 Modify Groups and IDs.

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

- **Set Report Preferences** – Set up interactive reports, select a filename format, create a custom header, change the report language, and more.
- **Dashboard** - Provides top and trend charts of Web activity by visits, hits or bytes and by users, groups, categories and classifications.
- **Run Reports** – Covers instructions on how to manually run three different types of reports: High-level Summaries, Detailed Audits, and Additional Manager Reports.
- **Schedule Reports** – Instructions for scheduling a report and modifying or deleting previously scheduled reports.
- **Use Interactive Reports** - Covers how to retrieve and use interactive reports.
- **Review Report Policies** – Lets you view summarized information of your policy settings.

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 operator accounts. Individuals with operator accounts can access the product, but only to 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 operator accounts, see Section 6.

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.

The Review Report Policies screen gives you a handy overview of your report policies. You will be able to view Groups and IDs that can be reported on, abuse threshold settings, category classification and blocking (CyBlock products only), etc. At a glance, you will be able to quickly see if any setting is missing or needs to be changed.

In addition to knowing how to run reports, it is important to understand several factors that affect the accuracy of reporting. For more information on this topic, i.e., data accuracy, the difference between “Hits” and “Visits,” and using reliable metrics, read the following white papers on our Web site at http://www.wavecrest.net/editorial /whitepapers.html.

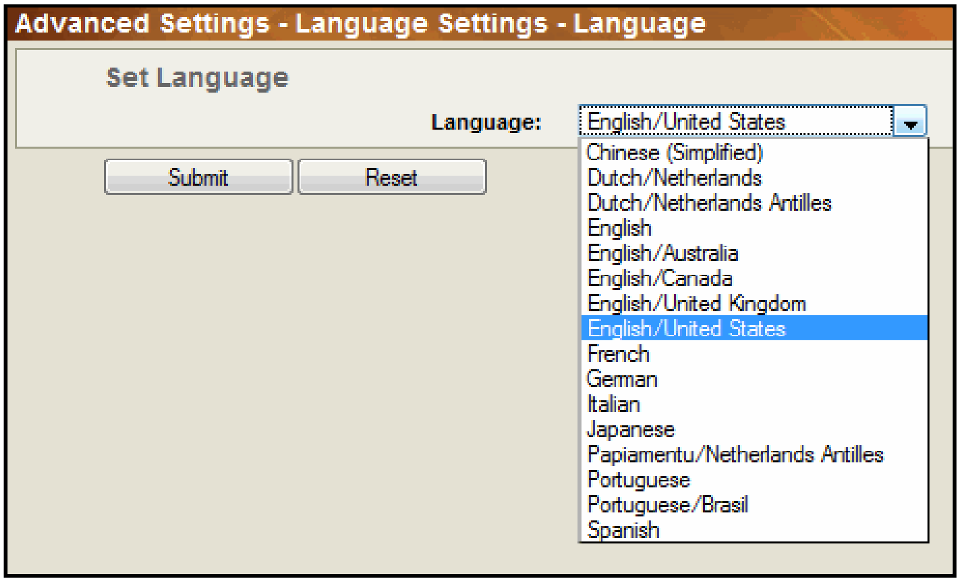
5.1 Report Preferences

To let you further customize your reports, this product contains several options that will affect how your reports will look and what information will be included in them. These options are explained below.

5.1.1 Language Settings

This screen lets you select the language to be used in reports.

1. Go to **Advanced Settings – Language Settings**.



Advanced Settings - Language Settings - Language

Set Language

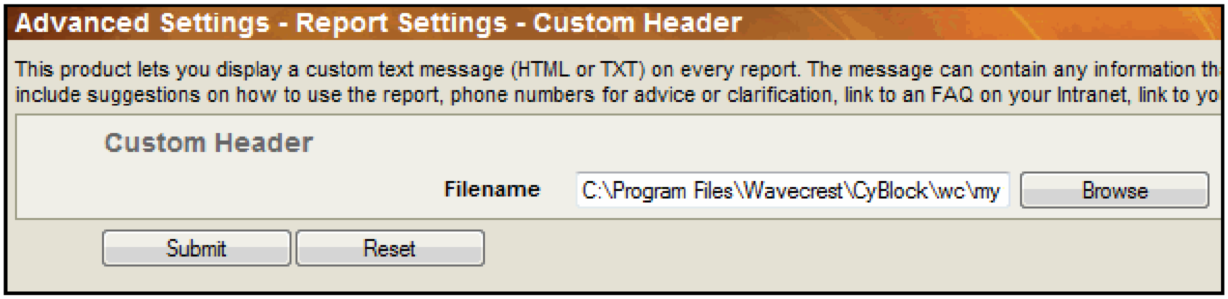
Language: English/United States

2. Select the **Language** that you want to be used in reports.
3. Click **Submit** to apply your selection.

5.1.2 Custom Header

This screen lets you display a custom header message (HTML or TXT) on every report. The message can contain any information that might be helpful to the recipient of the report. Examples include suggestions on how to use the report, phone numbers for advice or clarification, link to an FAQ on your Intranet, link to your usage policy, etc

1. To use this feature, you must first create a header message.
2. Create the message as a .TXT file, and take note of the path you decide to use for the file. When creating the message, utilize **HTML** tags if you need them. ***NOTE**: The default text file path for Cyfin products is wc/cf/db/custom.txt; for CyBlock products, it is wc/cyblock/db/custom.txt.*
3. Go to **Advanced Settings – Report Settings** and click on the **Custom Header** link.



Advanced Settings - Report Settings - Custom Header

This product lets you display a custom text message (HTML or TXT) on every report. The message can contain any information th
include suggestions on how to use the report, phone numbers for advice or clarification, link to an FAQ on your Intranet, link to yo

Custom Header

Filename C:\Program Files\Wavecrest\CyBlock\wc\my

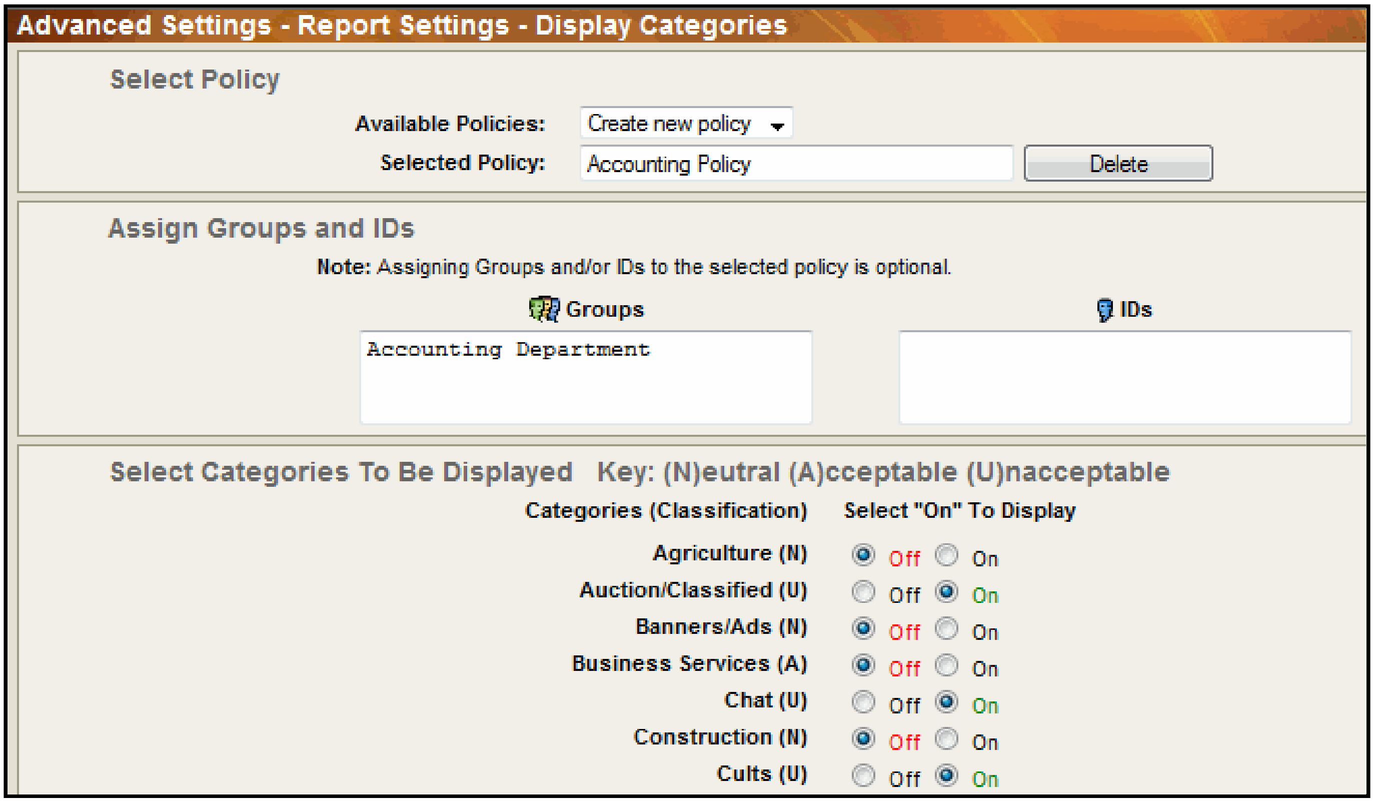
4. Enter the complete path to the .TXT file you created in the **Filename** text entry box, or use the **Browse** button to find the file.
5. Click **Submit** to apply your selection. The message will appear automatically in all reports that are subsequently generated.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.1.3 Display Categories

This screen lets you create, edit and delete Display Categories "policies." That is, it lets you establish settings that specify which content category tables are to be displayed in reports. These policies can be applied to Groups or IDs as you see fit (See Section 2 to read more about Groups and IDs).

1. Go to **Advanced Settings – Report Settings** and click on the **Display Categories** link.



Advanced Settings - Report Settings - Display Categories

Select Policy

Available Policies: Create new policy

Selected Policy: Accounting Policy

Assign Groups and IDs

Note: Assigning Groups and/or IDs to the selected policy is optional.

Groups: Accounting Department

IDs:

Select Categories To Be Displayed Key: (N)eutral (A)cceptable (U)nacceptable

Categories (Classification)	Select "On" To Display
Agriculture (N)	● Off ○ On
Auction/Classified (U)	○ Off ● On
Banners/Ads (N)	● Off ○ On
Business Services (A)	● Off ○ On
Chat (U)	○ Off ● On
Construction (N)	● Off ○ On
Cults (U)	○ Off ● On

2. Use the pull-down menu to select an **Available Policy** to modify, or leave the default selection *Create new policy*.

3. If you chose a previously created policy, its name will display in the **Selected Policy** text field. If you are creating a new **Display Categories** policy, type in a name for it.
NOTE: You can also delete a Display Categories policy by clicking on the ***Delete*** *button.*

4. **Assign Groups and IDs** to the policy. This step is optional. You can create a policy and assign Groups and IDs at a later time. If you wish to apply a universal policy to all users, select Enterprise.

5. **Select Categories to Be Displayed** in reports by selecting the *On* radio button. For categories not to be displayed, select the *Off* radio button.

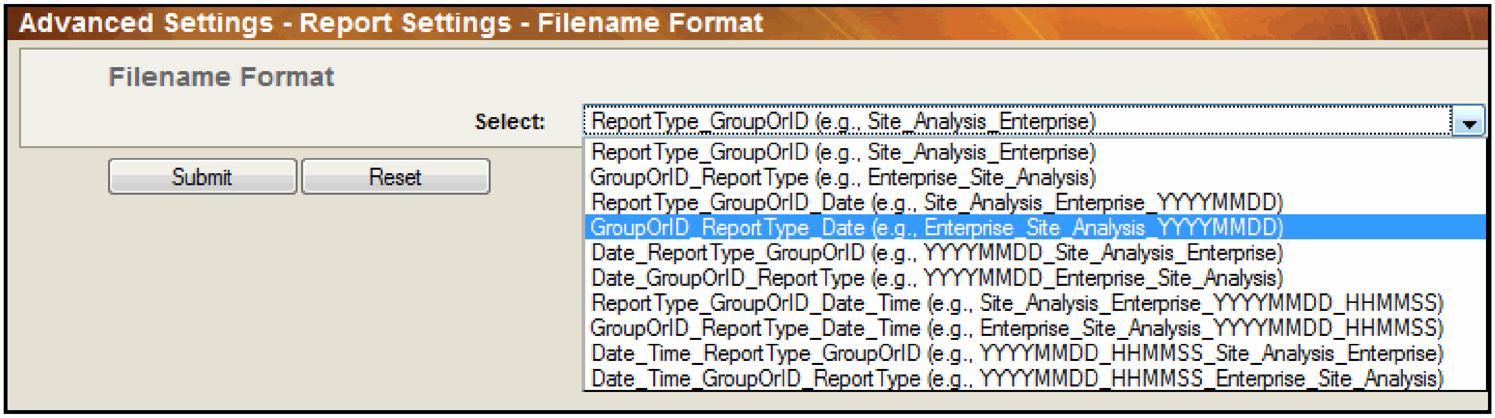
6. Click **Submit** to apply your changes.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.1.4 Filename Format

This screen lets you choose a filename format for saving reports. The available formats are made up of various combinations of the date, time, group or ID, and report type.

1. Go to **Advanced Settings – Report Settings** and click on the **Filename Format** link.



Advanced Settings - Report Settings - Filename Format

Filename Format

Select: ReportType_GroupOrID (e.g., Site_Analysis_Enterprise)

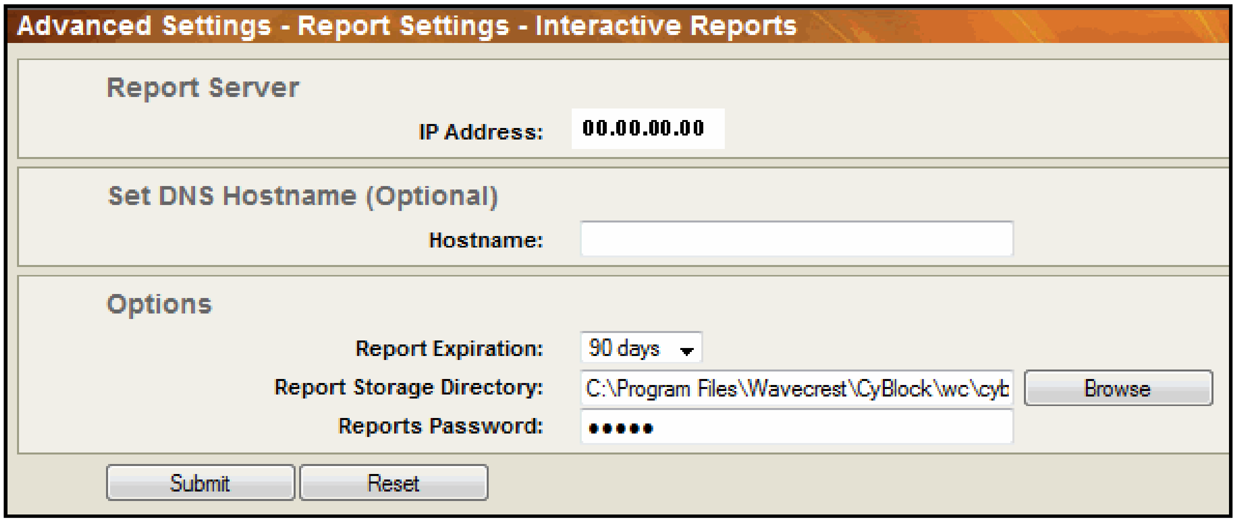
ReportType_GroupOrID (e.g., Site_Analysis_Enterprise)
GroupOrID_ReportType (e.g., Enterprise_Site_Analysis)
ReportType_GroupOrID_Date (e.g., Site_Analysis_Enterprise_YYYYMMDD)
GroupOrID_ReportType_Date (e.g., Enterprise_Site_Analysis_YYYYMMDD)
Date_ReportType_GroupOrID (e.g., YYYYMMDD_Site_Analysis_Enterprise)
Date_GroupOrID_ReportType (e.g., YYYYMMDD_Enterprise_Site_Analysis)
ReportType_GroupOrID_Date_Time (e.g., Site_Analysis_Enterprise_YYYYMMDD_HHMMSS)
GroupOrID_ReportType_Date_Time (e.g., Enterprise_Site_Analysis_YYYYMMDD_HHMMSS)
Date_Time_ReportType_GroupOrID (e.g., YYYYMMDD_HHMMSS_Site_Analysis_Enterprise)
Date_Time_GroupOrID_ReportType (e.g., YYYYMMDD_HHMMSS_Enterprise_Site_Analysis)
Submit
Reset

2. Select the filename format that you prefer from the **Select** pull-down menu.
3. Click **Submit** to apply your selection.

5.1.5 Interactive Reports

This screen lets you establish settings for interactive reports, such as how long to keep reports, where to store them, and changing the password needed to retrieve the reports.

1. Go to **Advanced Settings - Report Settings** and click on the **Interactive Reports** link.



Advanced Settings - Report Settings - Interactive Reports

Report Server

IP Address: 00.00.00.00

Set DNS Hostname (Optional)

Hostname:

Options

Report Expiration: 90 days

Report Storage Directory: C:\Program Files\Wavecrest\CyBlock\wc\cyb

Reports Password: •••••

2. In the **IP Address** field, select the IP address to be used for reporting if a pulldown menu is present. If the IP address is plainly displayed with no available pulldown menu, the product found the 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 hostname, type it in the **Hostname** 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 type in a DNS hostname that external computers will recognize.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

4. Select the **Report Expiration** using the pulldown. Interactive reports will no longer be accessible past the number of days you select.

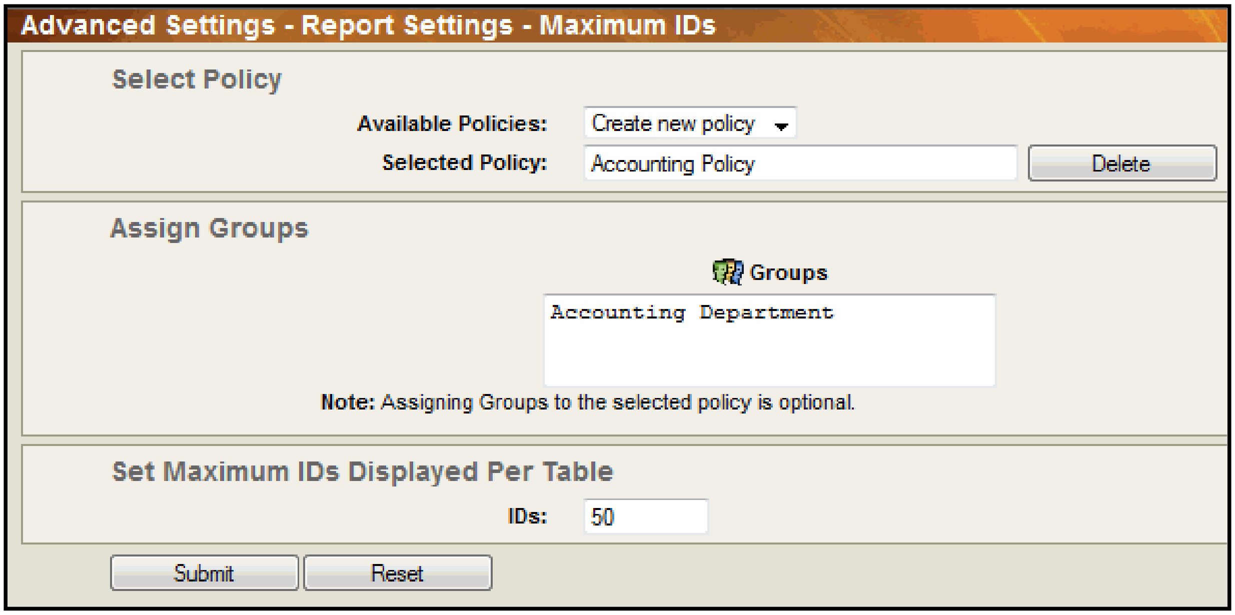
5. In the **Report Storage Directory** field, a default location will appear, but this can be changed. To change the directory location where Interactive reports will be stored, either use the **Browse** button to select the location or type the directory location path in the field. If it is a UNC path, you must type it in the field.

6. Type in 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" (no quotes).

5.1.6 Maximum IDs

This screen lets you establish Maximum IDs "policies." These policies will dictate the maximum number of IDs to be displayed in report tables.

1. Go to **Advanced Settings – Report Settings** and click on the **Maximum IDs** link.



Advanced Settings - Report Settings - Maximum IDs

Select Policy

Available Policies: Create new policy

Selected Policy: Accounting Policy

Assign Groups

Groups

Accounting Department

Note: Assigning Groups to the selected policy is optional.

Set Maximum IDs Displayed Per Table

IDs: 50

2. Use the pull-down menu to select an existing Maximum IDs policy or select *Create new policy*.

3. If you chose a previously created policy, the name of that policy will display in the **Selected Policy** text field. If you are creating a new policy, type in a name for it.
__NOTE__: You can also delete a previously selected Maximum IDs policy by clicking on the __Delete__ button.

4. Assign **Group(s)** to the policy. This step is optional. You can create a policy and assign Group(s) at a later time. If you wish to apply a universal policy to all users, select Enterprise.

5. Type in the **Maximum Number IDs** you wish to appear in reports. This must be a number between 1 and 250. The default is 25.

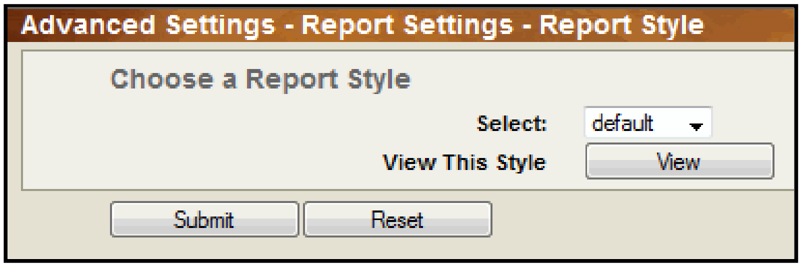
6. Click **Submit** to apply your changes.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.1.7 Report Style

This screen lets you choose the style in which you want your reports to be displayed.

1. Go to **Advanced Settings – Report Settings** and click on the **Report Style** link.



Advanced Settings - Report Settings - Report Style

Choose a Report Style

Select: default

View This Style

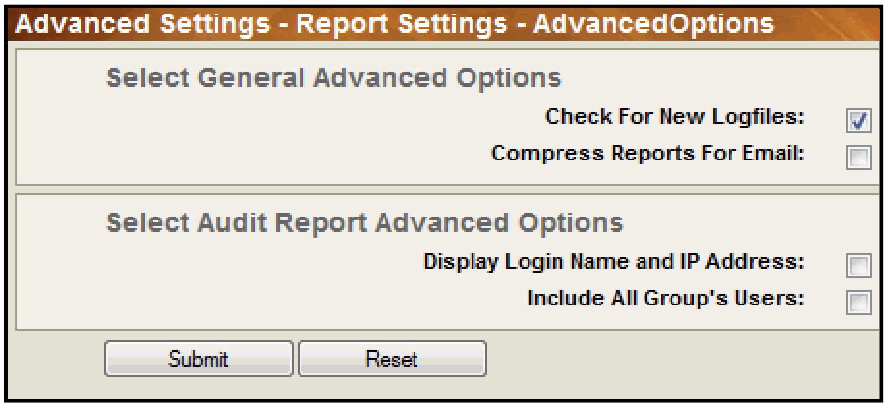
2. You can choose from two report styles: *classic* and *default*. Use the **View** button to review each style, and then **Select** the style you prefer.
3. Click **Submit** to apply your selection.

5.1.8 Advanced Options

The advanced options screen offers the following options for your reports.

- **Check For New Logfiles.** Before running a report, the product will check for any new logfiles. This option is selected by default.
- **Compress Reports For Email.** This compresses the report attachment for read-only reports in an email as a .zip file.
- **Display Login Name and IP Address.** Select this option if you want to see both the login name and IP address for each record in the report.
- **Include All Group's Users.** This will display a user ID even if there is no data for that ID in a User Audit Detail or Category Audit Detail report.

1. Go to **Advanced Settings - Report Settings** and click on the **Advanced Options** link.



Advanced Settings - Report Settings - AdvancedOptions

Select General Advanced Options

Check For New Logfiles: ☑

Compress Reports For Email: □

Select Audit Report Advanced Options

Display Login Name and IP Address: □

Include All Group's Users: □

2. Select the check box for any of the advanced options you would like to enable.
3. Click **Submit** to save your changes.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

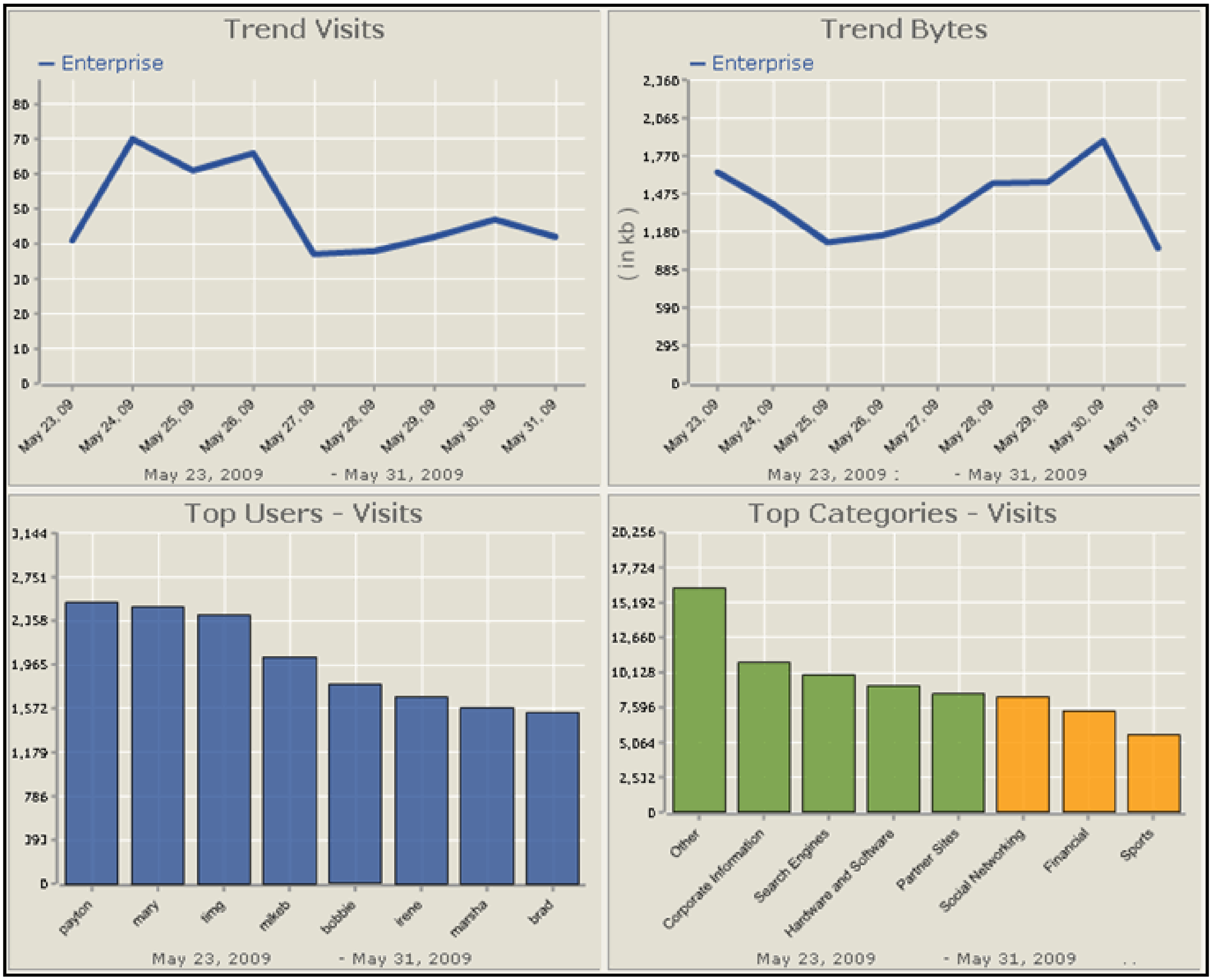
5.2 Dashboard Reports

The Dashboard Reports allow you to get a quick overview of the Enterprise's Web activity several different ways. The Dashboard consists of of three sections.

- Home - Provides an overview of the Enterprise's Web activity.
- Top - Provides reports on the top users, groups, categories, classifications and sites by visits, hits or bytes.
- Trend - Provides trends on the users, groups, categories or classifications you specify.

***NOTE**: To print any of the charts, simply click on the print icon in the top right had corner above the chart.*

1. Before opening Dashboard reports, you must enable the Data Manager and import logfile data into the Data Manger. For instructions on using the Data Manager, see Section 3.0 on Data Management.
   ***NOTE**: Adobe Flash 10 Player is required to view Dashboard reports.*
2. To open the Dashboard, go to **Reports - Dashboard**.
3. The Home screen of the Dashboard will open with four overview charts displayed. These charts represent data for the entire Enterprise over the last 7 days. You will see a Visits Trend Report, Bytes Trend Report, Top Users Report and Top Categories Report.

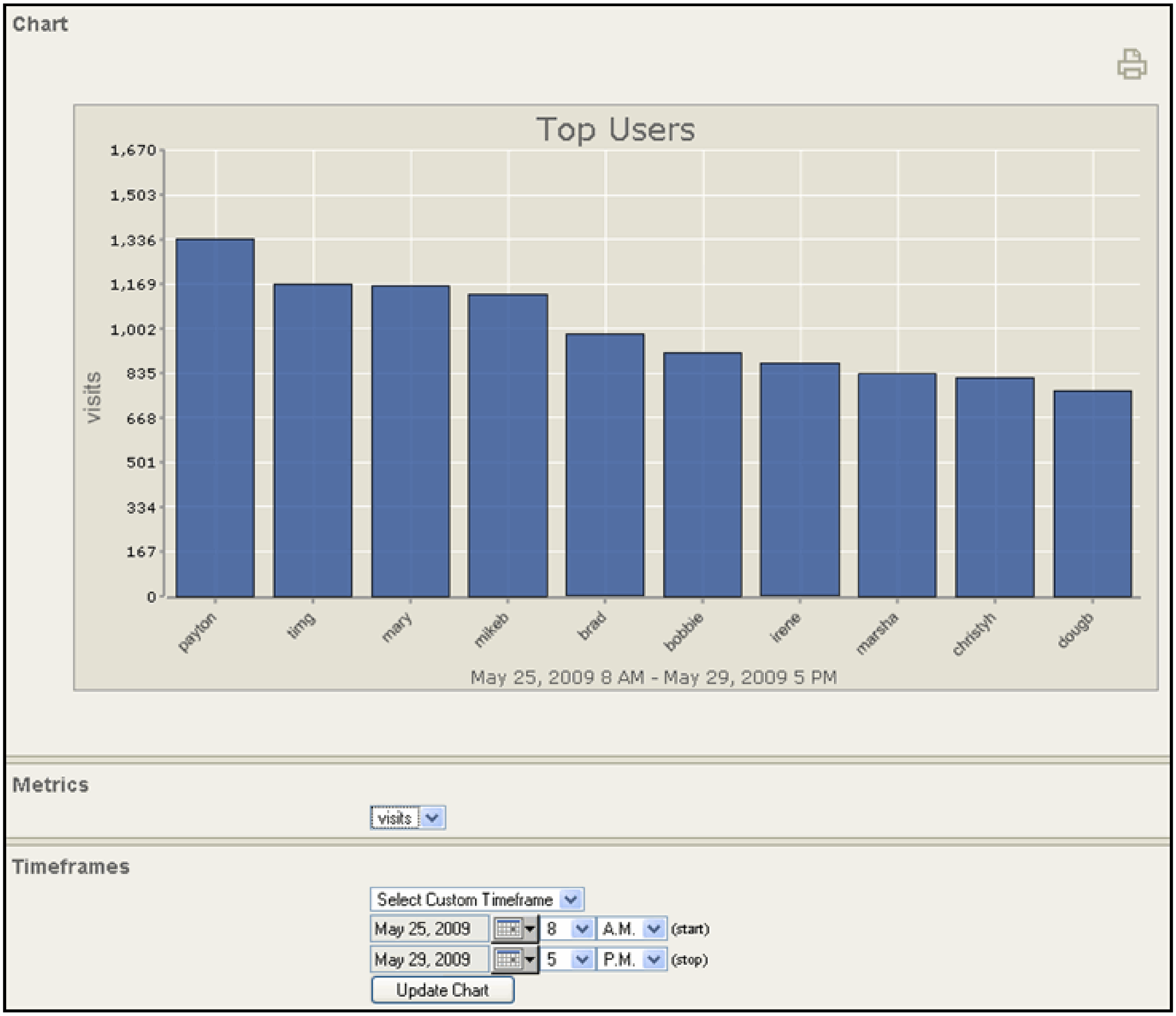


© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.2.1 Top Reports

These reports show Web use for the top users, groups, categories, classifications, and sites for the entire enterprise by the metric and timeframe specified. For the purpose of the manual, only a Top Users report is shown, but all Top reports have the same customizable features.

1. Go to **Top - Users**.
2. A chart with your top 10 users will automatically load with the default metric of "Visits" and the default timeframe of "Last 7 Days."



Metrics

visits

Timeframes

Select Custom Timeframe

May 25, 2009 8 A.M. (start)

May 29, 2009 5 P.M. (stop)

3. Use the **Metrics** pull-down to change the metric you are viewing. You can view data by visits, hits or bytes.
4. Use the **Timeframes** pull-down to select a different timeframe.

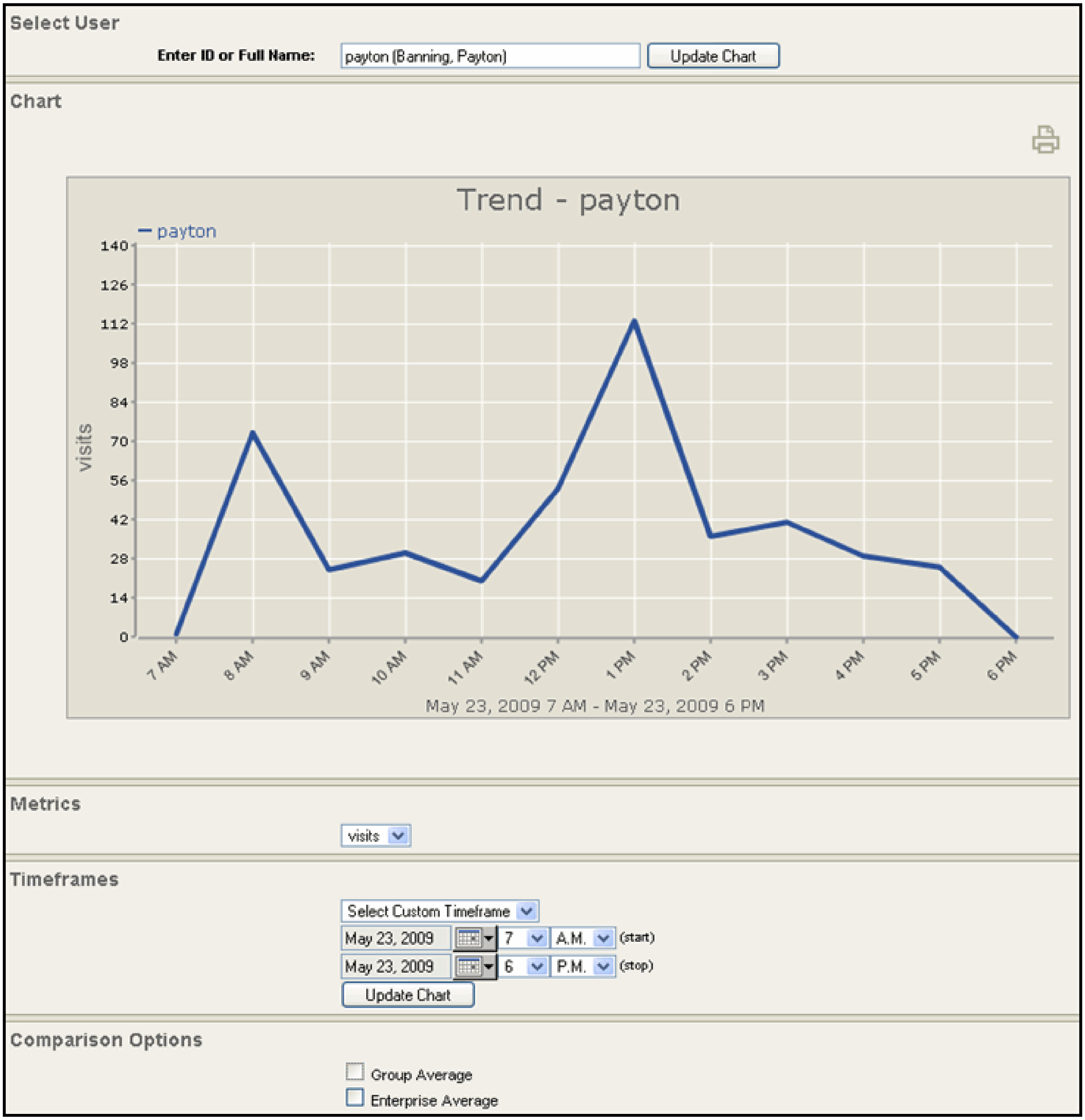
NOTE*: If you have an Array configured, you will also see a Data Configuration option. This allows you to chart only the data from the selected server in your array.*

5.2.2 Trend Reports

Trend reports allow you to view a selected user, group, category or classification data in hourly or daily increments for the specified timeframe, i.e., last 24 hours, yesterday, last 7 days, last week or last month.

5.2.2.1 Users

1. Go to **Trend - Users**.
2. In the **Select User** text field, enter in the ID or full name of the person you want to report on. As you type, you will begin to see a selection of IDs and names. If you see the ID or name that you are looking for, you can select that user.
3. Click **Update Chart**, and the chart will automatically load with the default metric of "visits" and timeframe of "last 7 days."



Select User

Enter ID or Full Name: payton (Banning, Payton)

Chart

Metrics

visits

Timeframes

Select Custom Timeframe

May 23, 2009 7 A.M. (start)

May 23, 2009 6 P.M. (stop)

Comparison Options

□ Group Average

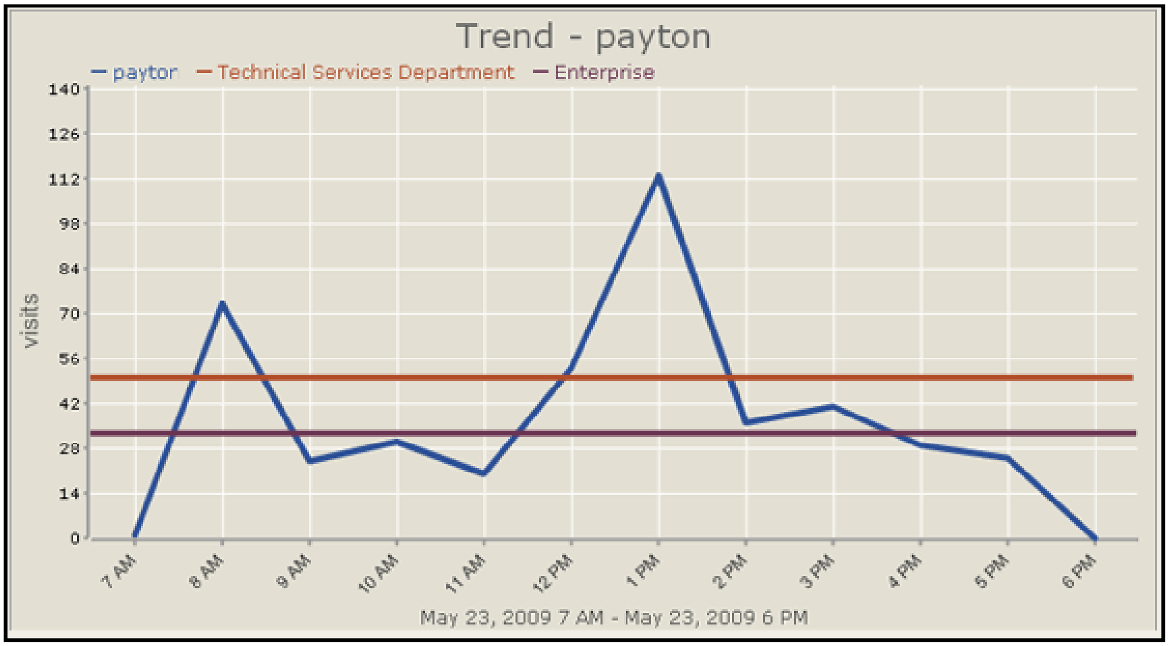
□ Enterprise Average

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

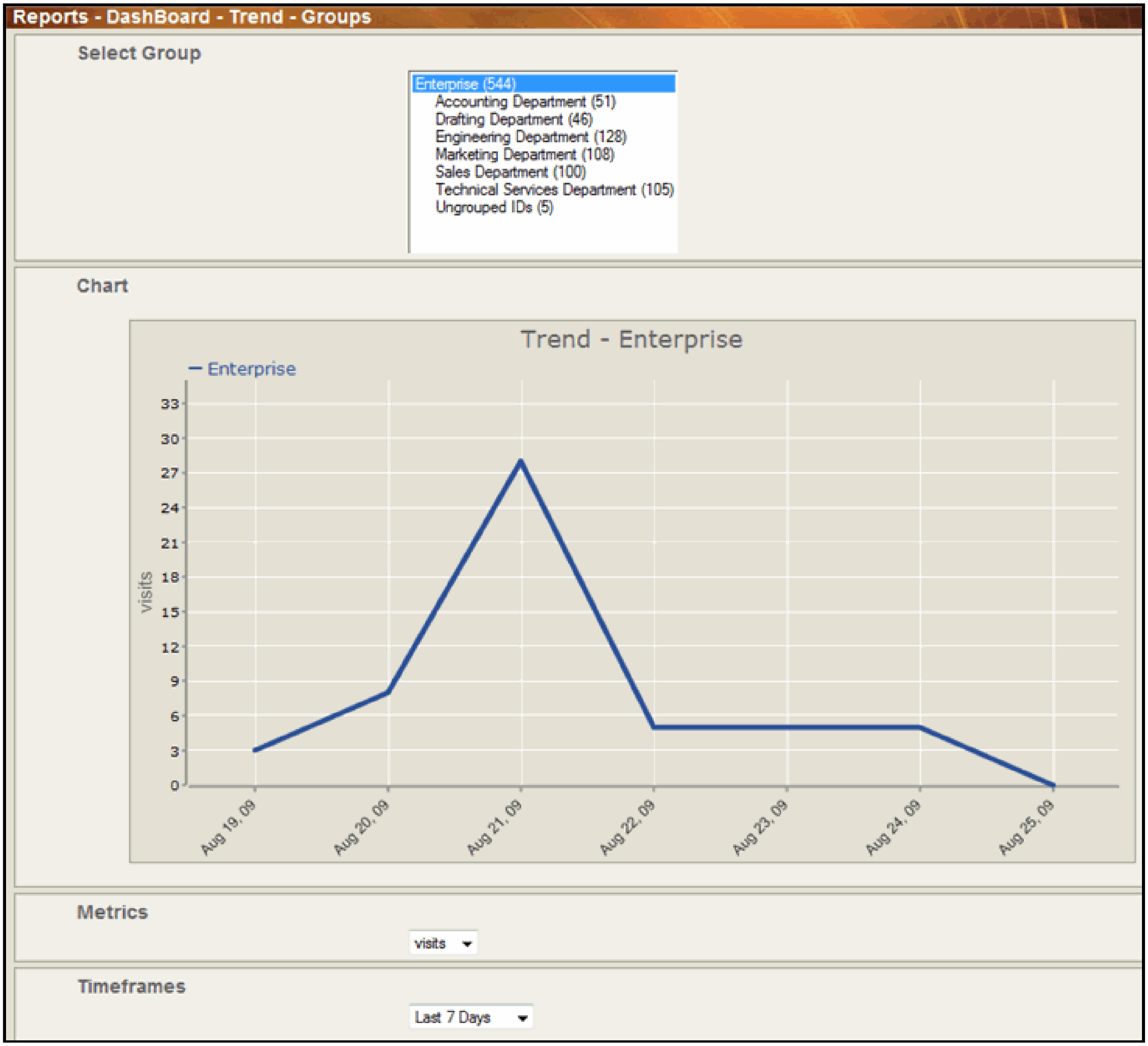
4. Use the **Metrics** pull-down to change the metric you are viewing. You can view data by visits, hits or bytes.
5. Use the **Timeframes** pull-down to select a different timerframe to view.
6. In the **Comparison Options** section, select to compare a user's data to his/her Group Average and the Enterprise Average by simply clicking the corresponding check boxes.

   ***NOTE**: If you have an Array configured, you will also see a Data Configuration option. This allows you to chart only the data from the selected server in your array.*

   Following is an example of a User Trend Report compared to the Group and Enterprise Average.



1. Go to **Trend - Groups**.
2. Select a group, and the chart will automatically load with the default metric of "Visits" and timeframe of "Last 7 Days."



Reports - DashBoard - Trend - Groups

Select Group

Enterprise (544)
Accounting Department (51)
Drafting Department (46)
Engineering Department (128)
Marketing Department (108)
Sales Department (100)
Technical Services Department (105)
Ungrouped IDs (5)

Chart

Metrics

visits

Timeframes

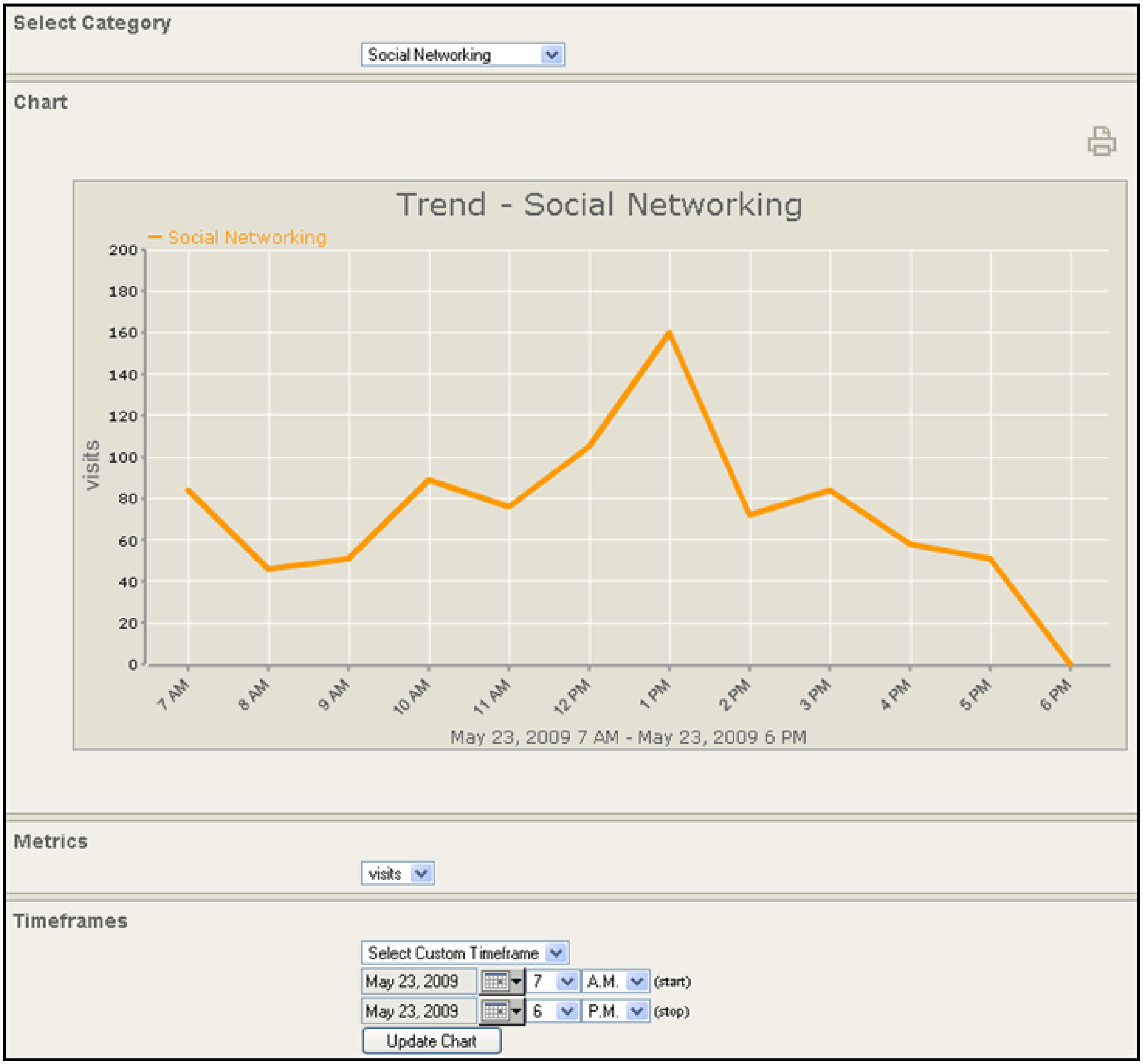
Last 7 Days

3. Use the **Metrics** pull-down to change the metric you are viewing, and the chart will automatically reload to reflect your selection. You can view data by visits, hits or bytes.
4. Use the **Timeframes** pull-down to change the timeframe, and the chart will automatically reload to reflect your selection.

__NOTE__: If you have an Array configured, you will also see a Data Configuration option. This allows you to chart only the data from the selected server in your array.

5.2.2.3 Categories

1. Go to **Trend - Categories**.



Select Category

Social Networking

Chart

Metrics

visits

Timeframes

Select Custom Timeframe

May 23, 2009 7 A.M. (start)

May 23, 2009 6 P.M. (stop)

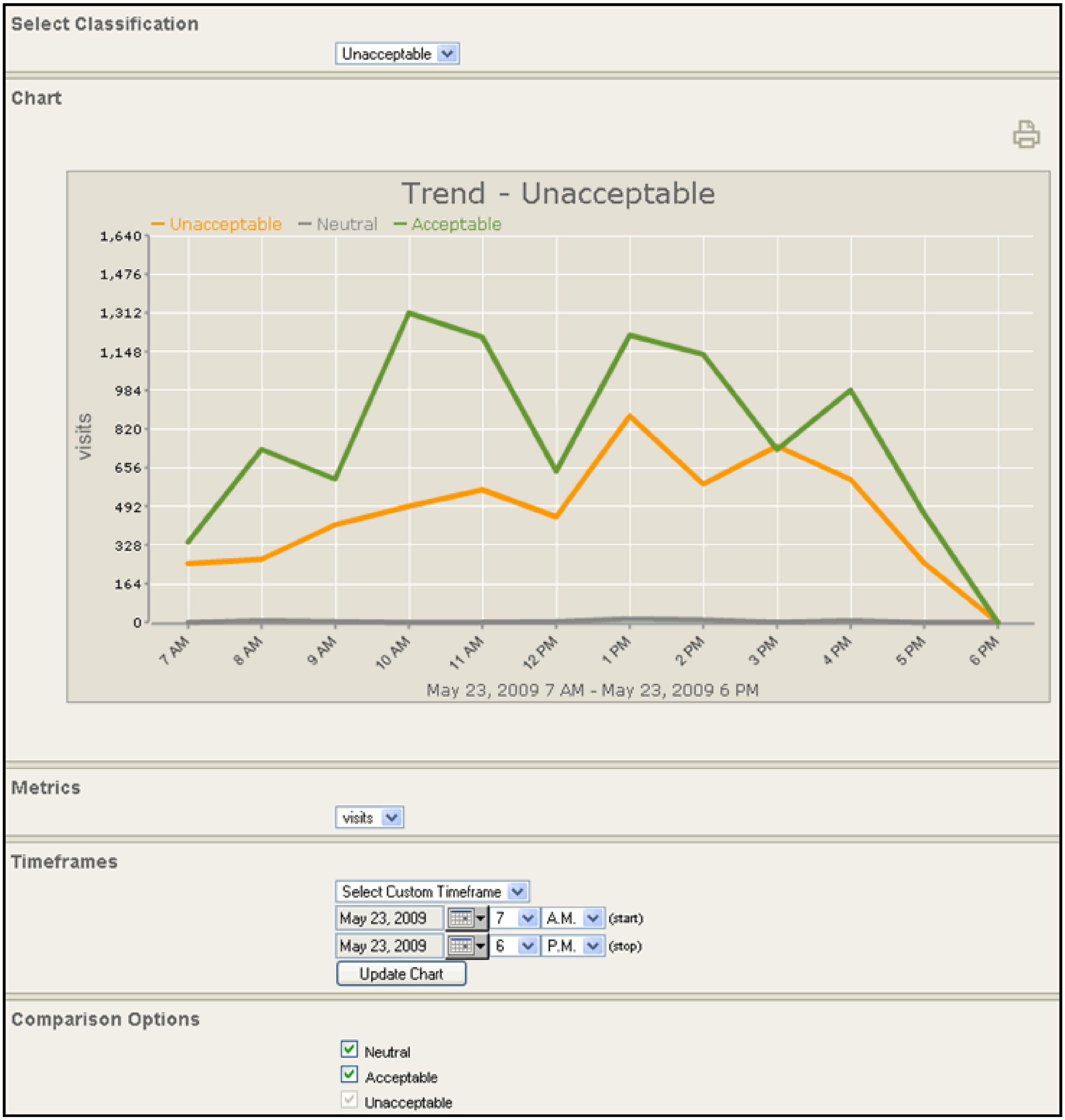
2. Select a Category, and the chart will automatically load with the default metric of "visits" and timeframe of "Last 7 Days."

3. Use the **Metrics** pull-down to change the metric you are viewing, and the chart will automatically reload to reflect your selection.. You can view data by visits, hits or bytes.

4. Use the **Timeframes** pull-down to change the timeframe, and the chart will automatically reload to reflect your selection.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

1. Go to **Trend - Classifications**. When this screen opens, a chart will automatically load showing you Unacceptable Visits for the Last 7 Days.



Select Classification

Unacceptable

Chart

Metrics

visits

Timeframes

Select Custom Timeframe

May 23, 2009 7 A.M. (start)

May 23, 2009 6 P.M. (stop)

Comparison Options

☑ Neutral

☑ Acceptable

☑ Unacceptable

2. To change the Classification, use the pull-down menu to make your selection.
3. Use the **Metrics** pull-down to change the metric you are viewing. You can view data by visits, hits or bytes.
4. Use the **Timeframes** pull-down to change the timeframe.
5. In the **Comparison Options** section, you can select to compare acceptable, unacceptable and neutral classifications by simply clicking the corresponding check boxes.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.3 Run a High-level Summary Report

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

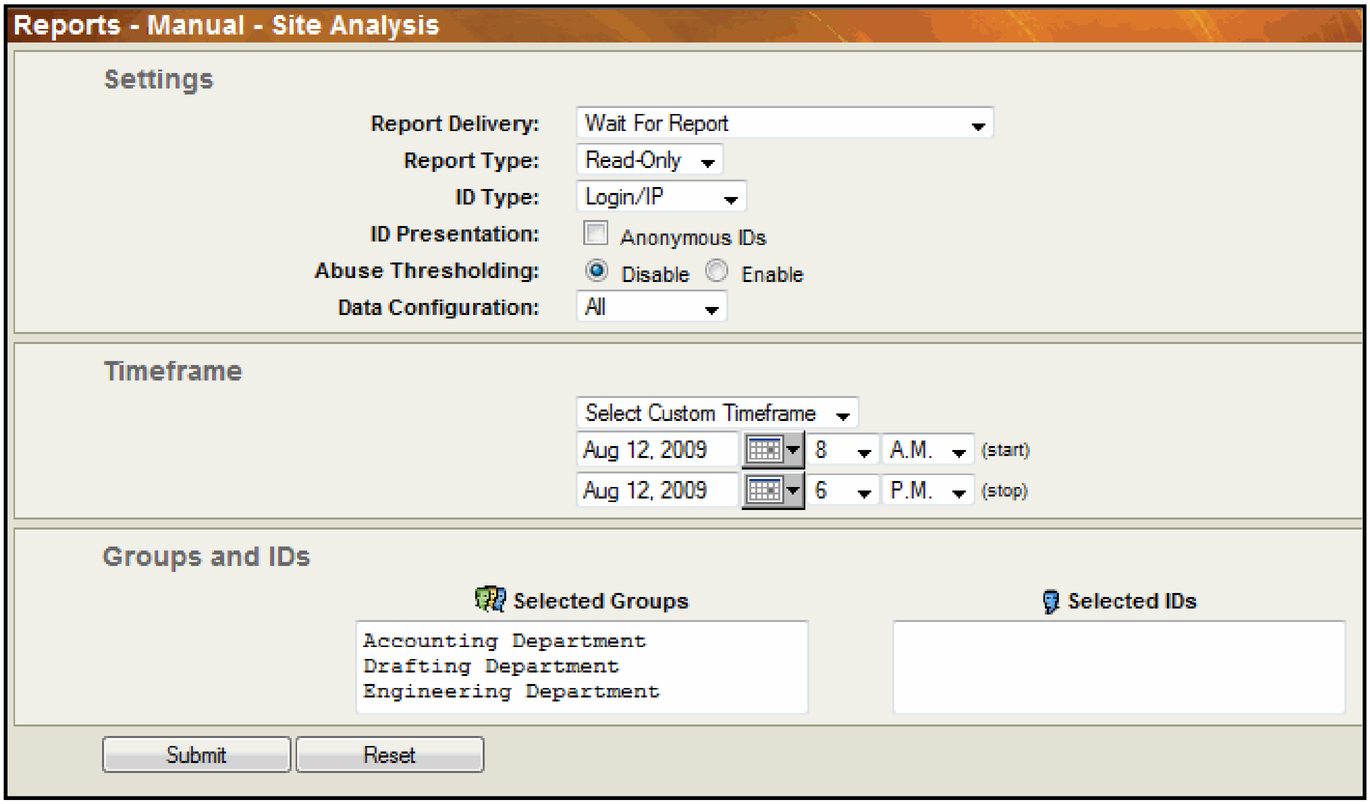
This section covers how to run a Site Analysis report, one of the more popular high-level reports. This report depicts the same Web site visits in three different ways:

- Total visits by 'acceptability' classification (acceptable, unacceptable, neutral)
- Total visits by content category (shopping, pornography, etc.)
- Total visits by user, per category.

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

As indicated above, for purposes of this manual, we will select Site Analysis, but these instructions will work for any high-level report you wish to run.

1. Go to **Reports – Manual**, and click on the high-level report that you would like to run.



Reports - Manual - Site Analysis

Settings

Report Delivery: Wait For Report
Report Type: Read-Only
ID Type: Login/IP
ID Presentation: □ Anonymous IDs
Abuse Thresholding: ● Disable ○ Enable
Data Configuration: All

Timeframe

Select Custom Timeframe
Aug 12, 2009 8 A.M. (start)
Aug 12, 2009 6 P.M. (stop)

Groups and IDs

Selected Groups

```
Accounting Department
Drafting Department
Engineering Department
```

Selected IDs

2. For **Report Delivery**, use the pull-down arrow to choose how the report will be delivered. You can choose to wait for the report, have it emailed, or saved to a directory.

3. Select the **Report Type**: *Interactive* or *Read-only*. (Read more about Interactive reports below.)
   ***NOTE**: Interactive reports can only be run against data imported into the Wavecrest Database. They can not be used when running reports against the raw logfiles. For steps on how to use the Wavecrest Database and its advantages, see Section 3.*

4. Choose the **ID Type** to be displayed.

5. For **ID Presentation** in the report, you can choose to display IDs anonymously. Check the *Anonymous IDs* checkbox to do so.

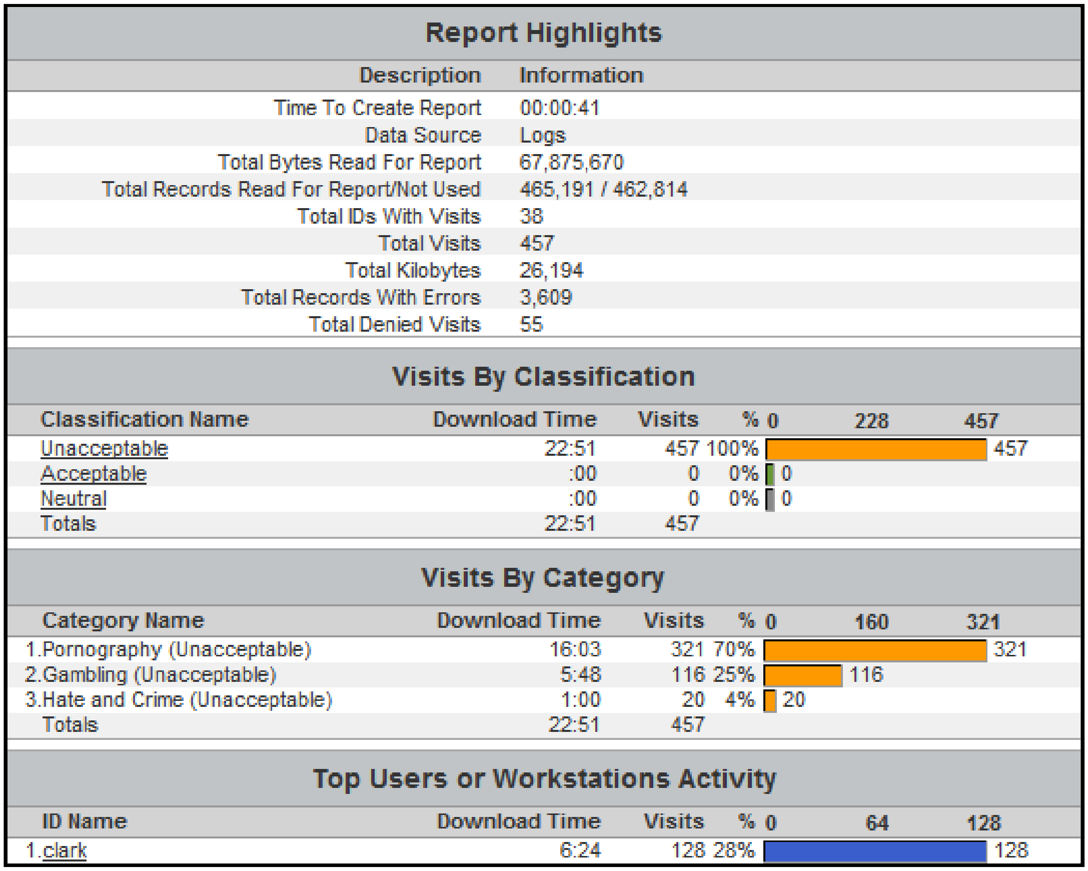
6. If you have set **Abuse Thresholding** and want it to display on the report, click the **Enable** radio button.

7. In the **Data Configuration** field, you can choose to select a single data configuration to include in the report, or you can choose to include all of them.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

8. Choose the **Timeframe** for your report. Use the pull-down to select either a predefined timeframe, or select *Custom* and set a **Start Date/Time** and **Stop Date/Time**.
9. Select the **Group(s) and ID(s)** that you wish to show in the report.
10. Click **Submit** to run the report.
11. If you selected *Enter other Email to Receive Report(s)* or *Select Other Directory to Save Report(s)* in the **Report Delivery** field, you will see a popup screen with a text box to type in the email address or directory path. In this case, enter the information, click **Submit**, and the report will run.

    Below is an example of a Site Analysis report.



Report Highlights

Description	Information
Time To Create Report	00:00:41
Data Source	Logs
Total Bytes Read For Report	67,875,670
Total Records Read For Report/Not Used	465,191 / 462,814
Total IDs With Visits	38
Total Visits	457
Total Kilobytes	26,194
Total Records With Errors	3,609
Total Denied Visits	55

Visits By Classification

Classification Name	Download Time	Visits	%	0 228 457
Unacceptable	22:51	457	100%	457
Acceptable	:00	0	0%	0
Neutral	:00	0	0%	0
Totals	22:51	457		

Visits By Category

Category Name	Download Time	Visits	%	0 160 321
1.Pornography (Unacceptable)	16:03	321	70%	321
2.Gambling (Unacceptable)	5:48	116	25%	116
3.Hate and Crime (Unacceptable)	1:00	20	4%	20
Totals	22:51	457		

Top Users or Workstations Activity

ID Name	Download Time	Visits	%	0 64 128
1.clark	6:24	128	28%	128

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.4 Run a Detail Audit Report

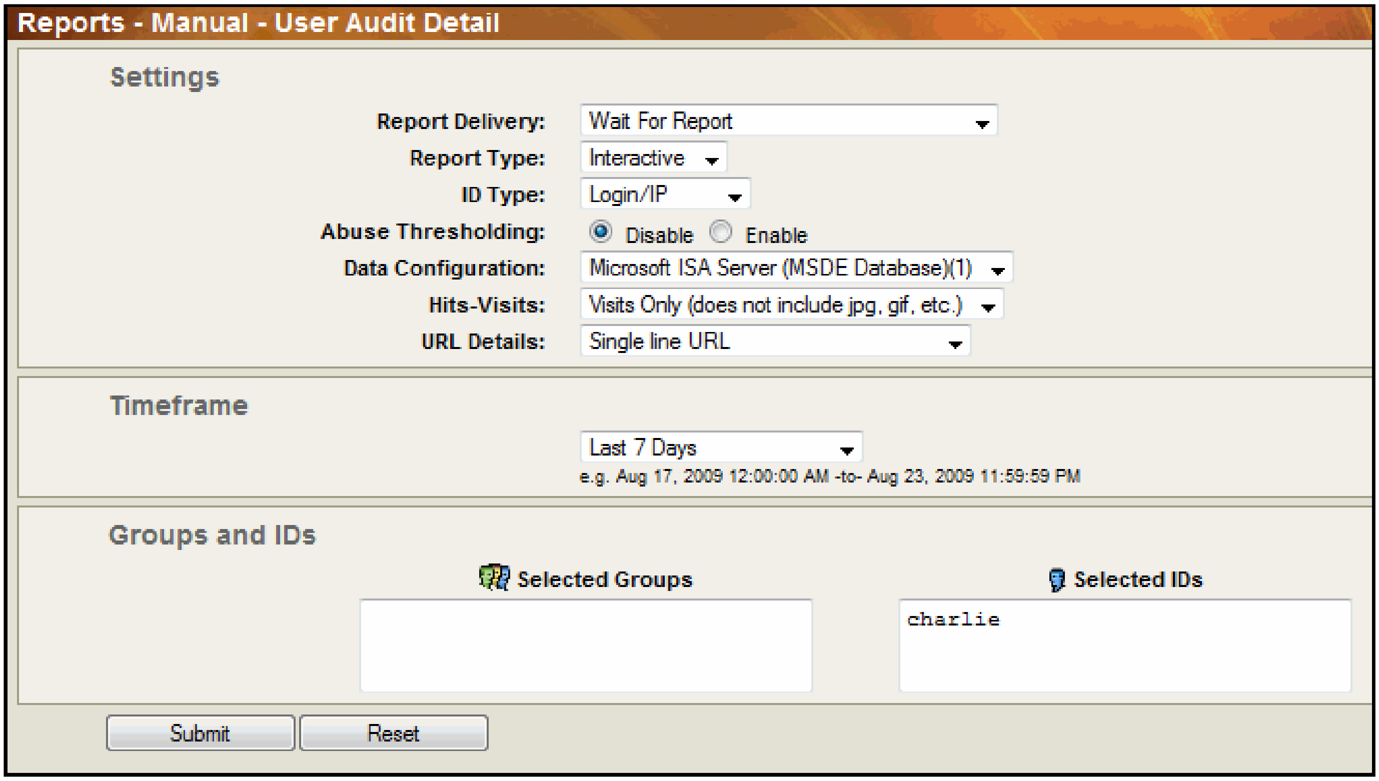
Detail Audit reports (or low-level reports) are designed to give detailed information on individual employees' Web use. These reports show the actual URLs visited.

This section provides instructions for running a User Audit Detail report, one of the more popular drill-down reports. A 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 Detail Audit reports, see Appendix B.*

As indicated above, for purposes of this manual, we will use User Audit Detail, but these instructions will work for any detail audit report you wish to run.

1. Go to **Reports – Manual**, and click on the detail audit report you wish to run.



Reports - Manual - User Audit Detail

Settings

Report Delivery: Wait For Report

Report Type: Interactive

ID Type: Login/IP

Abuse Thresholding: ● Disable ○ Enable

Data Configuration: Microsoft ISA Server (MSDE Database)(1)

Hits-Visits: Visits Only (does not include jpg, gif, etc.)

URL Details: Single line URL

Timeframe

Last 7 Days

e.g. Aug 17, 2009 12:00:00 AM -to- Aug 23, 2009 11:59:59 PM

Groups and IDs

Selected Groups

Selected IDs

charlie

2. For **Report Delivery**, use the pull-down arrow to choose how the report will be delivered. You can choose to wait for the report, have it emailed, or saved to a directory.

3. Select the **Report Type**: *Interactive* or *Read-only*. (Read more about Interactive reports below.)
   ***NOTE**: Interactive reports can only be run against data imported into the Wavecrest Database. They can not be used when running reports against the raw logfiles. For steps on how to use the Wavecrest Database and its advantages, see Section 3.*

4. Choose the **ID Type** to be displayed.

5. If you have set **Abuse Thresholding** and wish for it to display on the report, click the **Enable** radio button. (For more information on abuse thresholding, see Section 4).

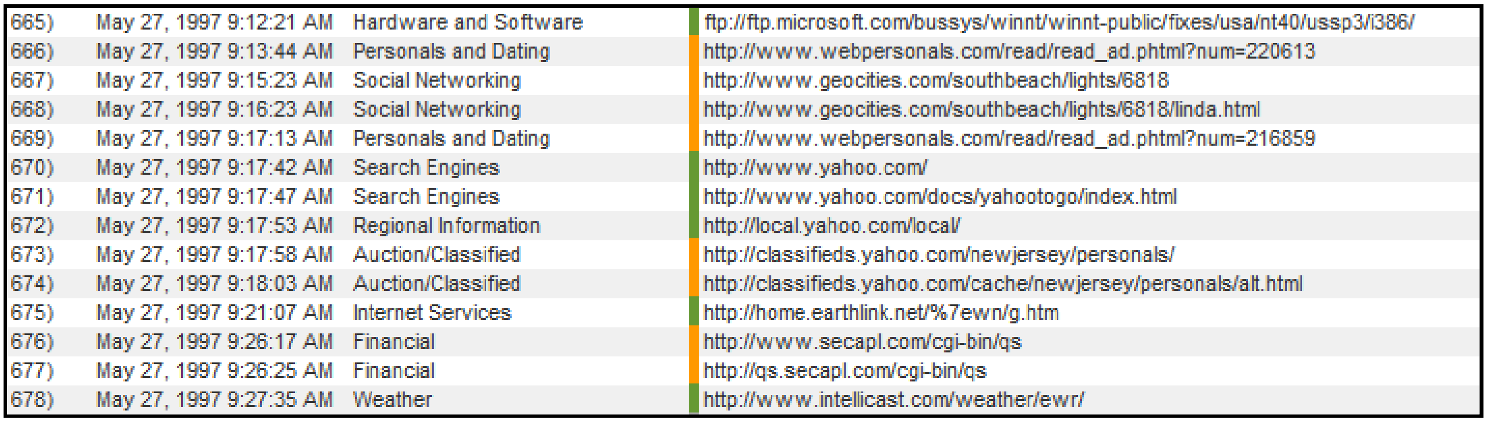
6. In the **Data Configuration** field, you can choose to select a single data configuration to include in the report, or you can choose to include all of them.

7. Select whether you want **All Hits** or **Visits Only** 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, audio, etc. Choose All Hits if you want reports to show all types of hits, solicited or unsolicited.*

8. For **URL Details**, choose how you want the URLs to display in the report. The default setting is *Single Line URL*, which means that URLs will be 'snipped' if they are longer than one line. If full URLs are needed, you can choose *Full URLs (wrapped when necessary)*. This means that the full URL will be shown, even if it takes two or three lines to display it.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

9. Choose the **Timeframe** for your report. Use the pull-down to select either a predefined timeframe, or select *Custom* and set a **Start Date/Time** and **Stop Date/Time**.
10. Select the **Group** or **ID** that you wish to show in the report.
    ***CAUTION**: You cannot run a User Audit Detail report on the "Enterprise" group. You can run the report on other groups, but remember that this means a user audit detail report will run on each user in the selected group.*
11. Click **Submit** to run the report.
12. If you selected *Enter other Email to Receive Report(s)* or *Select Other Directory to Save Report(s)* in the **Report Delivery** field, you will see a popup screen with a text box to type in the email address or directory path. In this case, enter the data, click **Submit**, and the report will run.



665)	May 27, 1997 9:12:21 AM	Hardware and Software	🟩	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3/i386/
666)	May 27, 1997 9:13:44 AM	Personals and Dating	🟧	http://www.webpersonals.com/read/read_ad.phtml?num=220613
667)	May 27, 1997 9:15:23 AM	Social Networking	🟧	http://www.geocities.com/southbeach/lights/6818
668)	May 27, 1997 9:16:23 AM	Social Networking	🟧	http://www.geocities.com/southbeach/lights/6818/linda.html
669)	May 27, 1997 9:17:13 AM	Personals and Dating	🟧	http://www.webpersonals.com/read/read_ad.phtml?num=216859
670)	May 27, 1997 9:17:42 AM	Search Engines	🟩	http://www.yahoo.com/
671)	May 27, 1997 9:17:47 AM	Search Engines	🟩	http://www.yahoo.com/docs/yahootogo/index.html
672)	May 27, 1997 9:17:53 AM	Regional Information	🟩	http://local.yahoo.com/local/
673)	May 27, 1997 9:17:58 AM	Auction/Classified	🟧	http://classifieds.yahoo.com/newjersey/personals/
674)	May 27, 1997 9:18:03 AM	Auction/Classified	🟧	http://classifieds.yahoo.com/cache/newjersey/personals/alt.html
675)	May 27, 1997 9:21:07 AM	Internet Services	🟩	http://home.earthlink.net/%7ewn/g.htm
676)	May 27, 1997 9:26:17 AM	Financial	🟧	http://www.secapl.com/cgi-bin/qs
677)	May 27, 1997 9:26:25 AM	Financial	🟧	http://qs.secapl.com/cgi-bin/qs
678)	May 27, 1997 9:27:35 AM	Weather	🟩	http://www.intellicast.com/weather/ewr/

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.5 Run a Site Analysis Bandwidth Report

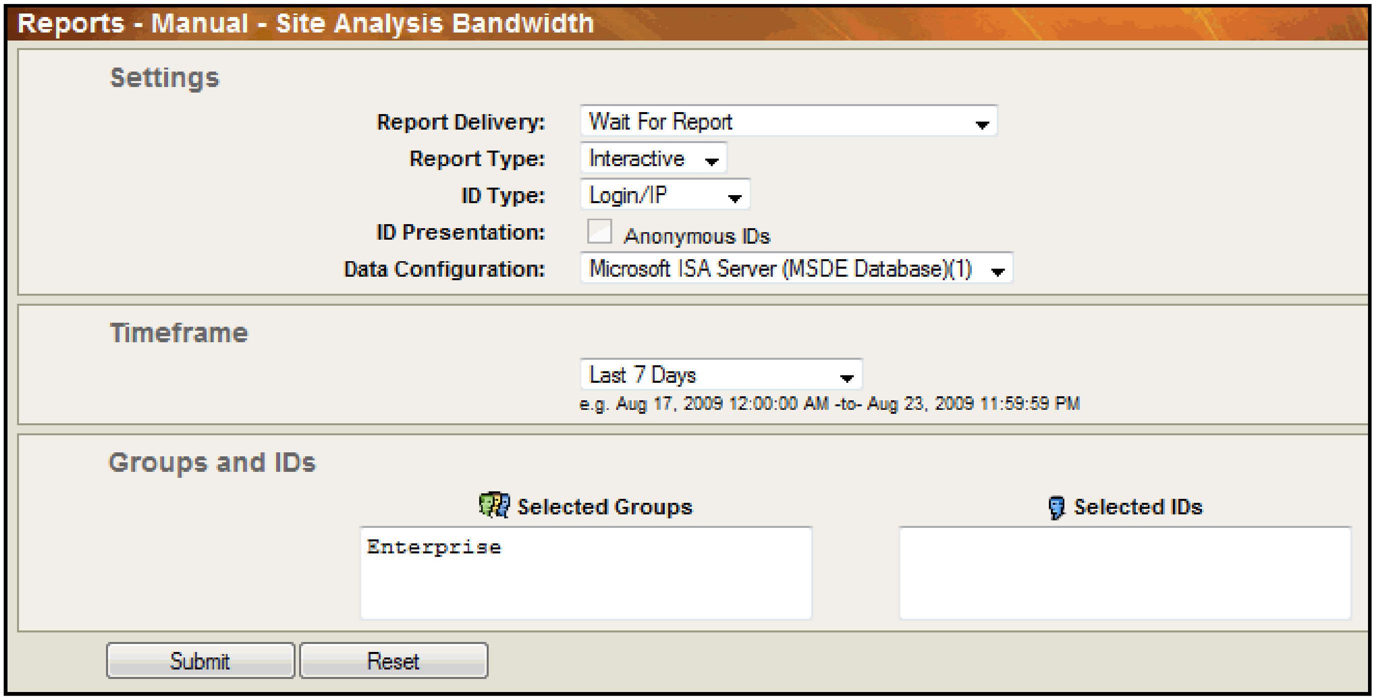
The Site Analysis Bandwidth report is one of the Additional Management Reports provided by the product. These reports, which supplement the high and low-level reports discussed above, cover the areas that managers, HR and IT find useful when managing employee Web use.

The Site Analysis Bandwidth Report is similar to the Site Analysis report, but it focuses on bandwidth consumption instead of Web site content. It breaks down bandwidth usage first by acceptability classification, then by category within each classification, and then by user within each category.

***NOTE**: For descriptions of all Additional Management Reports, see Appendix B.*

To run your report, follow the steps below. These instructions will work for any Additional Management Report you wish to run.

1. Go to **Reports – Manual** and click on the **Site Analysis Bandwidth** link under **Additional Management Reports**.



Reports - Manual - Site Analysis Bandwidth

Settings

Report Delivery: Wait For Report

Report Type: Interactive

ID Type: Login/IP

ID Presentation: □ Anonymous IDs

Data Configuration: Microsoft ISA Server (MSDE Database)(1)

Timeframe

Last 7 Days

e.g. Aug 17, 2009 12:00:00 AM -to- Aug 23, 2009 11:59:59 PM

Groups and IDs

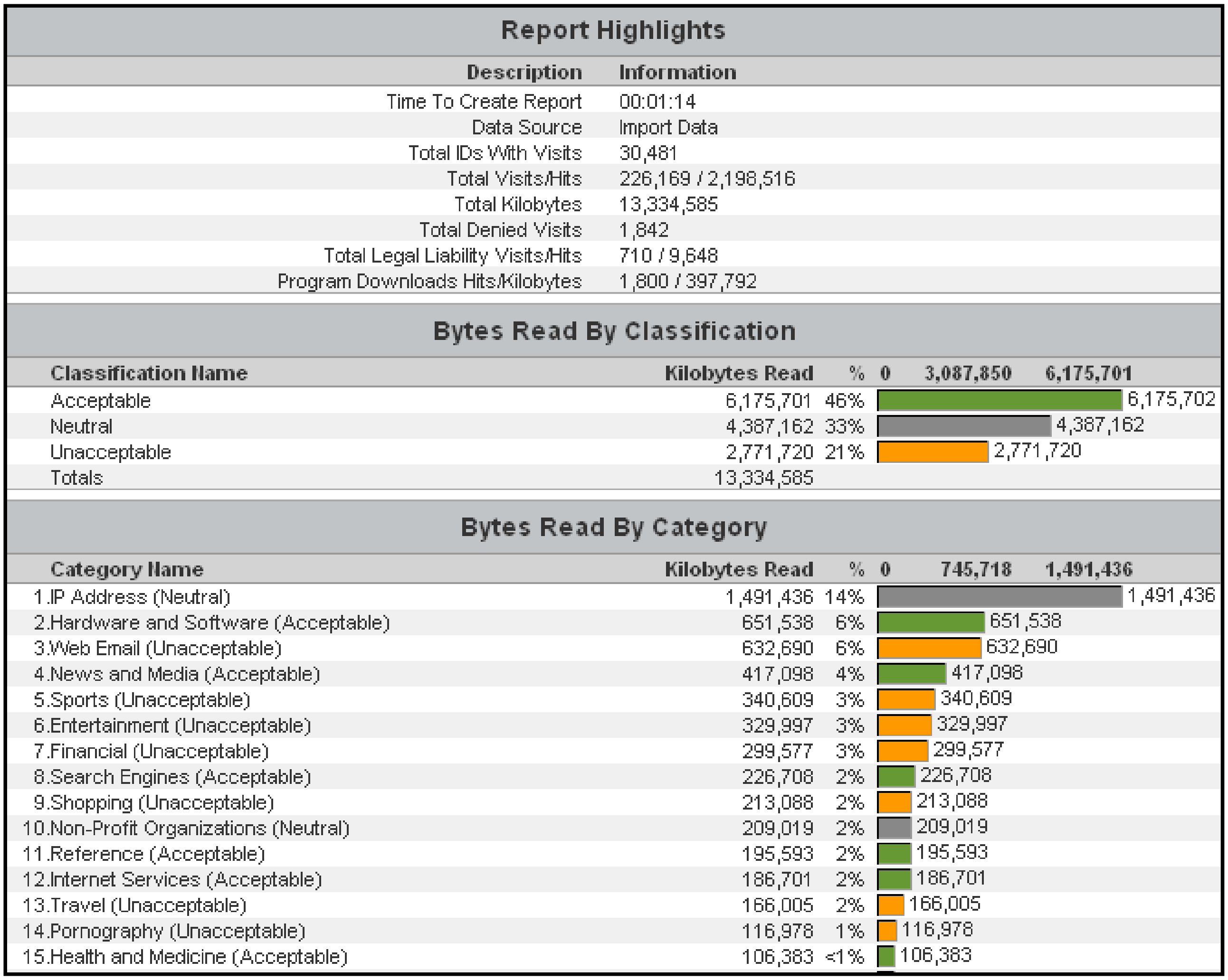
Selected Groups: Enterprise

Selected IDs

2. For **Report Delivery**, use the pull-down arrow to choose how the report will be delivered. You can choose to wait for the report, have it emailed, or saved to a directory.
3. Select the **Report Type**: *Interactive* or *Read-only*. (Read more about Interactive reports below.)
   ***NOTE**: Interactive reports can only be run against data imported into the Wavecrest Database. They can not be used when running reports against the raw logfiles. For steps on how to use the Wavecrest Database and its advantages, see Section 3.*
4. Choose the **ID Type** to be displayed.
5. For **ID Presentation** in the report, you can choose to display IDs anonymously. Check the *Anonymous IDs* checkbox to do so.
6. In the **Data Configuration** field, you can choose to select a single data configuration to include in the report, or you can choose to include all of them.
7. Choose the **Timeframe** for your report. Use the pull-down to select either a predefined timeframe, or select *Custom* and set a **Start Date/Time** and **Stop Date/Time**.
8. Select the **Group(s) and ID(s)** that you wish to show in the report.
9. Click **Submit** to run the report.
10. If you selected *Enter other Email to Receive Report(s)* or *Select Other Directory to Save Report(s)* in the **Report Delivery** field, you will see a popup screen with a text box to type in the email address or directory path. In this case, enter the data, click **Submit**, and the report will run.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

Below is an example of a Site Analysis Bandwidth report.



Report Highlights

Description	Information
Time To Create Report	00:01:14
Data Source	Import Data
Total IDs With Visits	30,481
Total Visits/Hits	226,169 / 2,198,516
Total Kilobytes	13,334,585
Total Denied Visits	1,842
Total Legal Liability Visits/Hits	710 / 9,648
Program Downloads Hits/Kilobytes	1,800 / 397,792

Bytes Read By Classification

Classification Name	Kilobytes Read	%	0 3,087,850 6,175,701
Acceptable	6,175,701	46%	6,175,702
Neutral	4,387,162	33%	4,387,162
Unacceptable	2,771,720	21%	2,771,720
Totals	13,334,585		

Bytes Read By Category

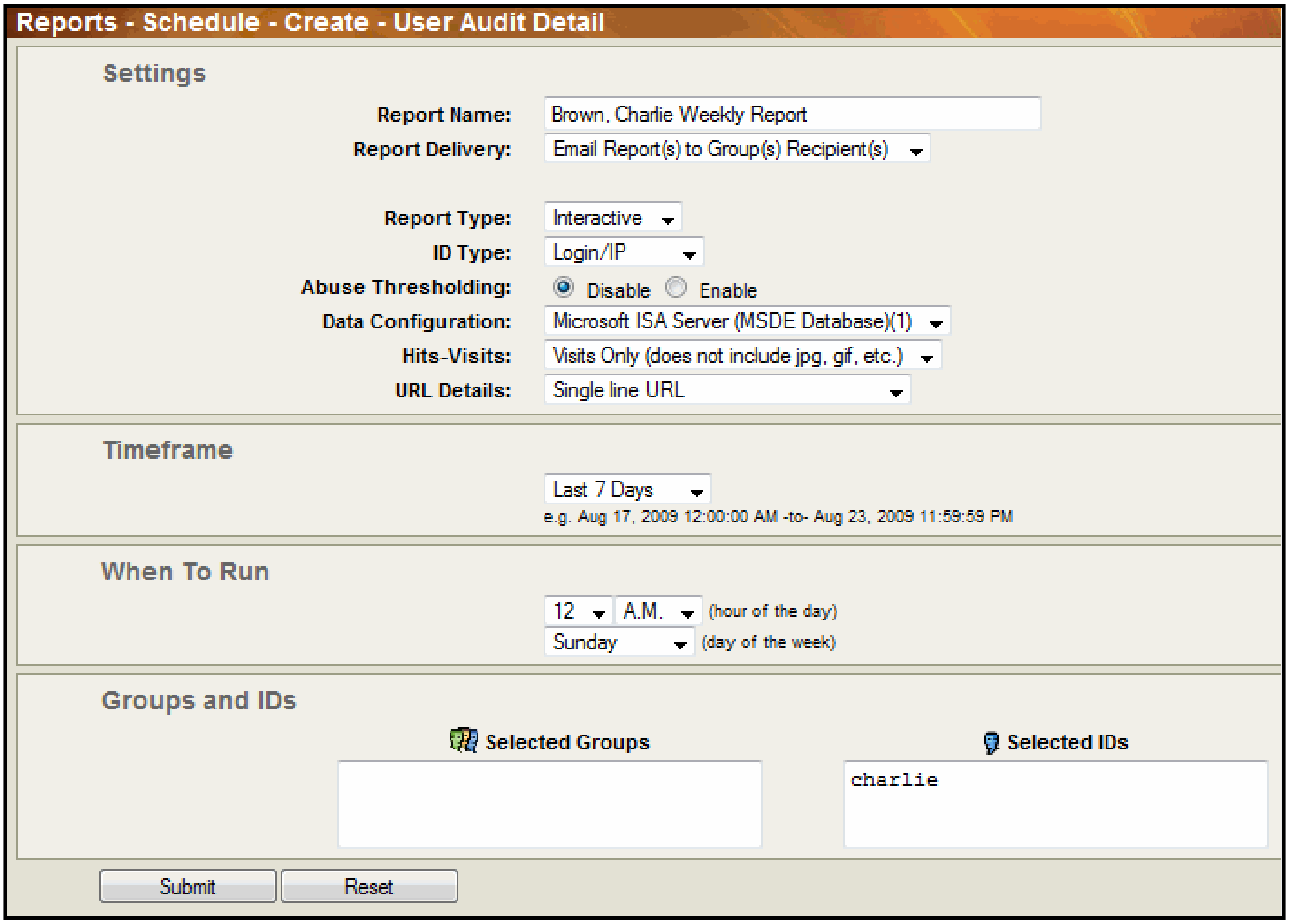
Category Name	Kilobytes Read	%	0 745,718 1,491,436
1.IP Address (Neutral)	1,491,436	14%	1,491,436
2.Hardware and Software (Acceptable)	651,538	6%	651,538
3.Web Email (Unacceptable)	632,690	6%	632,690
4.News and Media (Acceptable)	417,098	4%	417,098
5.Sports (Unacceptable)	340,609	3%	340,609
6.Entertainment (Unacceptable)	329,997	3%	329,997
7.Financial (Unacceptable)	299,577	3%	299,577
8.Search Engines (Acceptable)	226,708	2%	226,708
9.Shopping (Unacceptable)	213,088	2%	213,088
10.Non-Profit Organizations (Neutral)	209,019	2%	209,019
11.Reference (Acceptable)	195,593	2%	195,593
12.Internet Services (Acceptable)	186,701	2%	186,701
13.Travel (Unacceptable)	166,005	2%	166,005
14.Pornography (Unacceptable)	116,978	1%	116,978
15.Health and Medicine (Acceptable)	106,383	<1%	106,383

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

5.6 Schedule Reports

Reports can be scheduled to run daily, weekly or monthly and can be sent to the recipient's email address or saved to a directory that the recipient can access.

1. Go to **Reports – Schedule** and click on the **Create** link.
2. Choose the type of report you wish to schedule and click on that report's link. For purposes of this manual, we will schedule to run a **User Audit Detail** report.



Reports - Schedule - Create - User Audit Detail

Settings

Report Name: Brown, Charlie Weekly Report
Report Delivery: Email Report(s) to Group(s) Recipient(s)

Report Type: Interactive
ID Type: Login/IP
Abuse Thresholding: ● Disable ○ Enable
Data Configuration: Microsoft ISA Server (MSDE Database)(1)
Hits-Visits: Visits Only (does not include jpg, gif, etc.)
URL Details: Single line URL

Timeframe

Last 7 Days
e.g. Aug 17, 2009 12:00:00 AM -to- Aug 23, 2009 11:59:59 PM

When To Run

12 A.M. (hour of the day)
Sunday (day of the week)

Groups and IDs

Selected Groups

Selected IDs
charlie

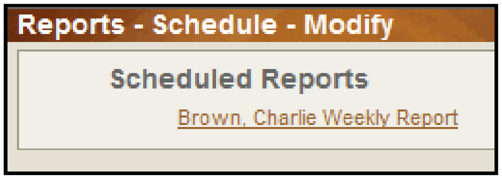
3. In the **Report Name** field, type in a name for the report.
   NOTE: *If you do not give the report a name, it will be given a default name.*
4. For **Report Delivery**, use the pull-down arrow to choose how the report will be delivered. For scheduled reports, you can have the report emailed to the group(s) recipient(s) or saved to a directory that the group(s) recipient(s) can access. You also have the option to enter one or more email addresses to receive the report. If you select this option, a text box will appear where you can enter them. If you are entering more than one email address, separate each with a comma or semicolon.
5. Select the **Report Type**: *Interactive* or *Read-only*.
   NOTE: *Interactive reports can only be run against data imported into the Wavecrest Database. They can not be used when running reports against the raw logfiles. For steps on how to use the Wavecrest Database and its advantages, see Section 3.*
6. Choose the **ID Type** to be displayed
7. If you have set **Abuse Thresholding** and want it to display on the report, click the **Enable** radio button.
8. In the **Data Configuration** field, you can choose to select a single data configuration to include in the report, or you can choose to include all of them.
9. Select whether you want **All Hits** or **Visits Only** 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, audio, etc. Choose All Hits if you want reports to show all types of hits.*

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

10. For **URL Details**, choose how you want the URLs to display in the report. The default setting is *Single Line URL*, which means that URLs will be 'snipped' if they are longer than one line. If full URLs are needed, you can choose *Full URLs (wrapped when necessary)*. This means that the full URL will be shown, even if it takes two or three lines to display it.
11. Choose the **Timeframe** for your report.
12. Select the **When To Run** time for the report.
13. Select the **Group** or **ID** that you wish to show in the report.
    ***CAUTION**: You cannot run a User Audit Detail report on the "Enterprise" group. You can run the report on other groups, but remember that this means a user audit detail report will run on each user in the selected group.*
14. Click **Submit** to set the report to run at its scheduled time.

5.6.1 Modify Scheduled Reports

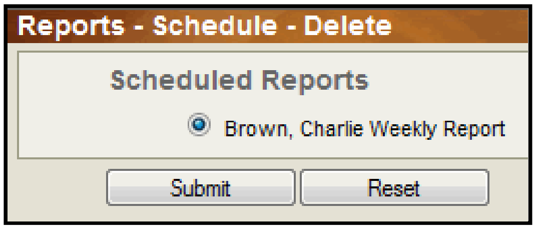
1. Go to **Reports – Schedule** and click on the **Modify** link.
2. Click on the scheduled report you wish to modify.



3. Make your modifications and click **Submit** to apply your changes.

5.6.2 Delete Scheduled Reports

1. Go to **Reports – Schedule** and click on the **Delete** link.
2. Select the radio button for the report you wish to delete.

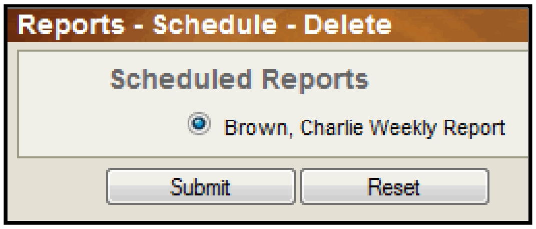


3. Click **Submit** to apply your deletions.

5.6.3 Run a Scheduled Report

This option allows you to run a scheduled report at any time.

1. Go to **Reports – Schedule** in the Cyfin Reporter interface and click on the **Run Now** link.
2. Go to **Reports – Schedule** and click on the **Run Now** link.



3. Click on the report you wish to run, and it will begin processing.

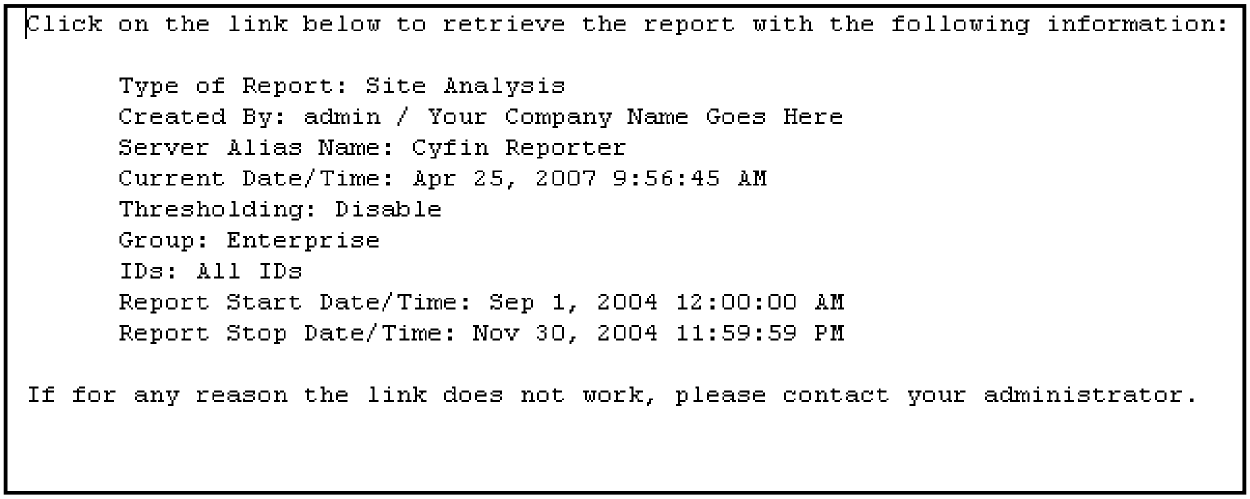
5.7 Using Interactive Reports

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

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.

To use Interactive Reporting, you must enable the Wavecrest Database. Interactive Reports can only be run against data imported into the Wavecrest Database. They can not be used when running reports against the raw logfiles. For steps on how to use the Wavecrest Database, see Section 3.

1. When an Interactive Report is emailed to a recipient or saved in the directory, the recipient will receive a link (or two links depending on your server settings) to the report.

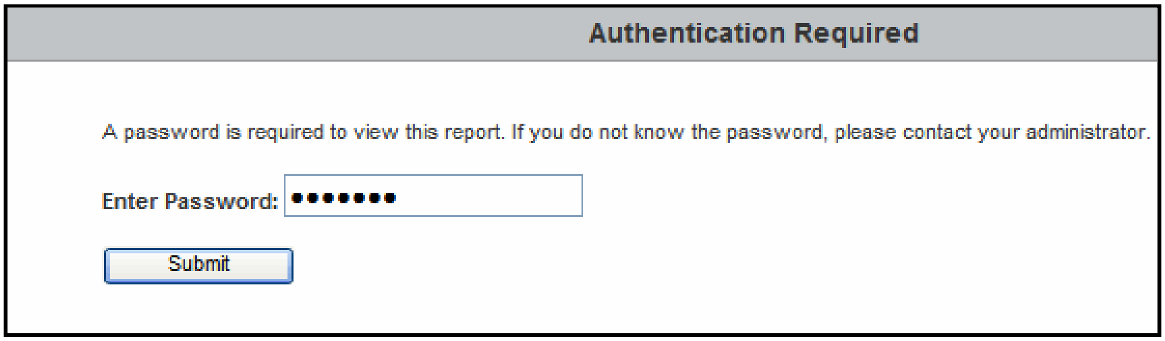


```
Click on the link below to retrieve the report with the following information:

      Type of Report: Site Analysis
      Created By: admin / Your Company Name Goes Here
      Server Alias Name: Cyfin Reporter
      Current Date/Time: Apr 25, 2007 9:56:45 AM
      Thresholding: Disable
      Group: Enterprise
      IDs: All IDs
      Report Start Date/Time: Sep 1, 2004 12:00:00 AM
      Report Stop Date/Time: Nov 30, 2004 11:59:59 PM

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

2. To open the report, click on 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 **Report Settings - Interactive Reports** screen.



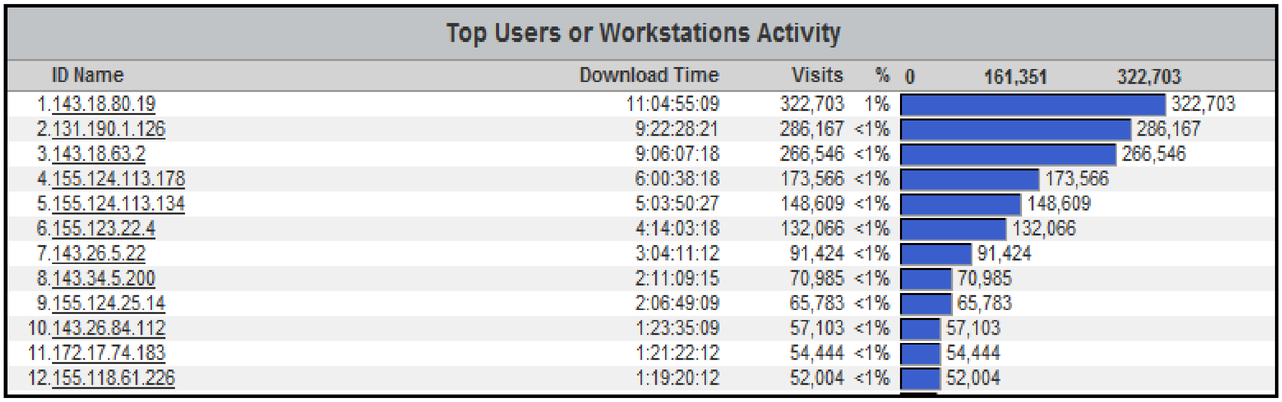
Authentication Required

A password is required to view this report. If you do not know the password, please contact your administrator.

Enter Password: ••••••••

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

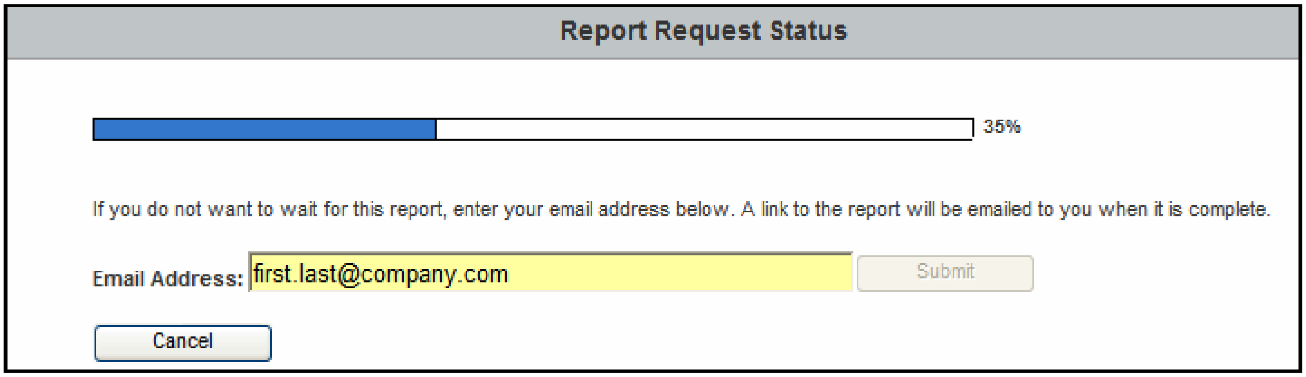
3. If you received a Site Analysis report, it would appear like the report below.



Top Users or Workstations Activity

ID Name	Download Time	Visits	%	0 161,351 322,703
1.143.18.80.19	11:04:55:09	322,703	1%	322,703
2.131.190.1.126	9:22:28:21	286,167	<1%	286,167
3.143.18.63.2	9:06:07:18	266,546	<1%	266,546
4.155.124.113.178	6:00:38:18	173,566	<1%	173,566
5.155.124.113.134	5:03:50:27	148,609	<1%	148,609
6.155.123.22.4	4:14:03:18	132,066	<1%	132,066
7.143.26.5.22	3:04:11:12	91,424	<1%	91,424
8.143.34.5.200	2:11:09:15	70,985	<1%	70,985
9.155.124.25.14	2:06:49:09	65,783	<1%	65,783
10.143.26.84.112	1:23:35:09	57,103	<1%	57,103
11.172.17.74.183	1:21:22:12	54,444	<1%	54,444
12.155.118.61.226	1:19:20:12	52,004	<1%	52,004

4. From here, you may decide that you want to drill-down to get more detail on a user's Web activity. Click on the user's ID (or for this example, the IP address). By clicking on **143.18.80.19**, you have submitted a request to get a User Audit Detail report on that particular user. The below progress meter will appear. If there are any other jobs in the queue, this screen will indicate how many jobs are in the queue.



Report Request Status

35%

If you do not want to wait for this report, enter your email address below. A link to the report will be emailed to you when it is complete.

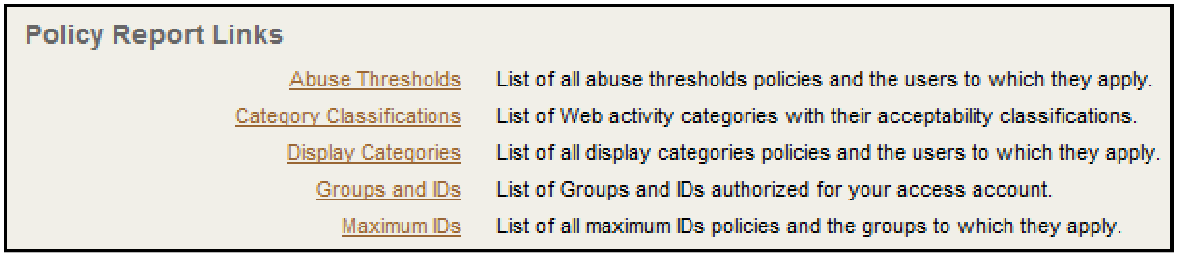
Email Address: first.last@company.com

5. If there is a lot of data or if there are multiple jobs in the queue and you do not want to wait for the report, you have the option of entering your email address to have the report emailed to you when it is complete.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

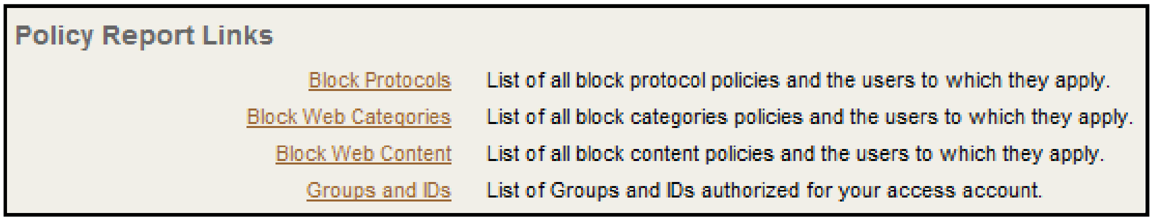
5.8 Review Report Policies

If you ever want to review your report settings, you can do so at the **Reports – Policy** screen.



Policy Report Links

Abuse Thresholds	List of all abuse thresholds policies and the users to which they apply.
Category Classifications	List of Web activity categories with their acceptability classifications.
Display Categories	List of all display categories policies and the users to which they apply.
Groups and IDs	List of Groups and IDs authorized for your access account.
Maximum IDs	List of all maximum IDs policies and the groups to which they apply.



Policy Report Links

Block Protocols	List of all block protocol policies and the users to which they apply.
Block Web Categories	List of all block categories policies and the users to which they apply.
Block Web Content	List of all block content policies and the users to which they apply.
Groups and IDs	List of Groups and IDs authorized for your access account.

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

- The **Abuse Thresholds** link indicates how many visits are acceptable before 'abuse' is considered to have occurred.
- The **Category Classifications** link shows the acceptability classifications (ratings) that your organization has assigned to the Web activity categories. NOTE: These can be default settings.
- The **Display Categories** link indicates which category tables will be displayed in reports.
- The **Groups and IDs** link indicates the groups and users that you can create reports on.
- The **Maximum IDs** link indicates how many user IDs will appear in category tables of reports.

6.0 Advanced Configuration

Wavecrest products offer an advanced Array Configuration option for those organizations that need to have multiple installations of Cyfin Reporter to help manage large amounts of logfiles. This allows an organization to manage all configurations and run reports from one location, i.e., the "Primary."

As shown in figure 1 below, an array configuration allows for the workload to be distributed and processed on the "Cyfin Secondary" servers while all reports and administrative functions are managed on the "Cyfin Primary" server. This configuration greatly reduces the amount of time it takes to process large amounts of logfiles. In order for the array to work, the logfiles must be located on a shared network storage drive so that they can be distributed amongst the Cyfin secondaries for quick processing to the Wavecrest database, which must also be located on a shared drive.

***NOTE:** If you already have existing import data, prior to moving an array scenario, we recommend that you save copies of the data (.war files) to a 'safe' location first. Likewise, if you have an array in production but decide to disband it, you should save copies of your import data first. This way you can place it where you want after the array is disbanded.*

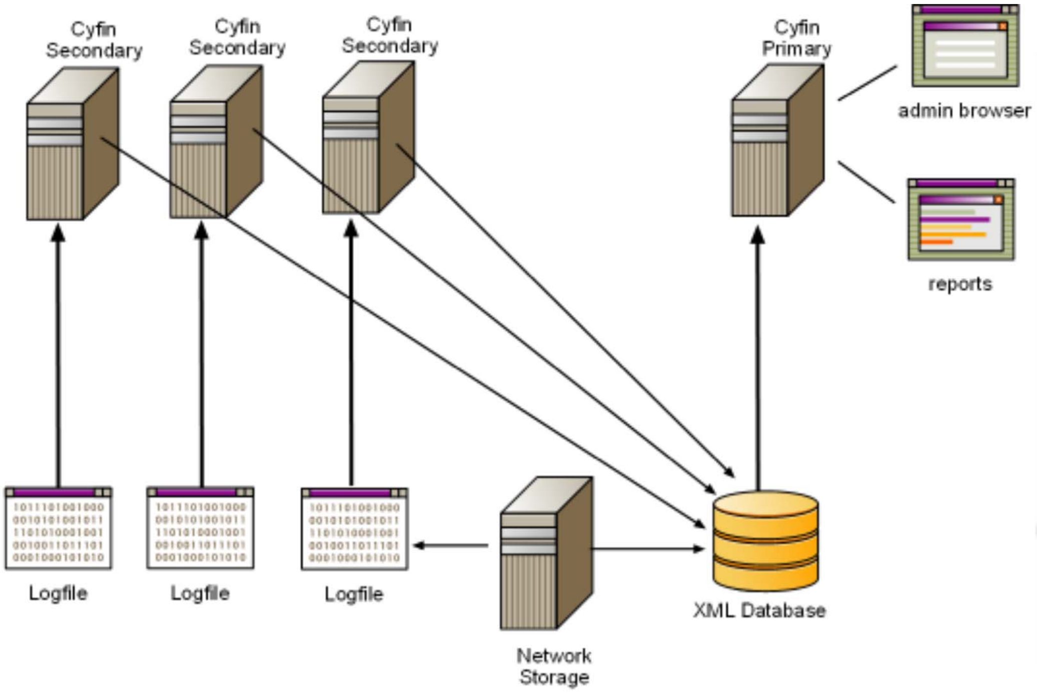


Figure 1: Array Configuration for Cyfin Reporter

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6.1 Array Configuration

This section covers instructions as if you were installing the products for the very first time, so it includes a few extra steps for those that may have already configured when the product was originally installed. However, you still may want to double check those settings to make sure they are configured to how you want them and to ensure that the product is running seamlessly after setting up the array.

You will find that some configurations must be done on the primary server and secondary servers before adding your secondaries to the array. This is why you will find that the instructions are in the following order:

- Designating and Setting Up the Primary Server
- Designating and Setting Up the Secondary Servers
- Completing the Array Setup on the Primary Server

Before getting started with the product installations, be sure to decide which server will be your primary and which servers will be your secondaries. If you plan to upgrade the software on your primary server, uninstall the Cyfin or CyBlock software on your secondary servers, and download a new product install.

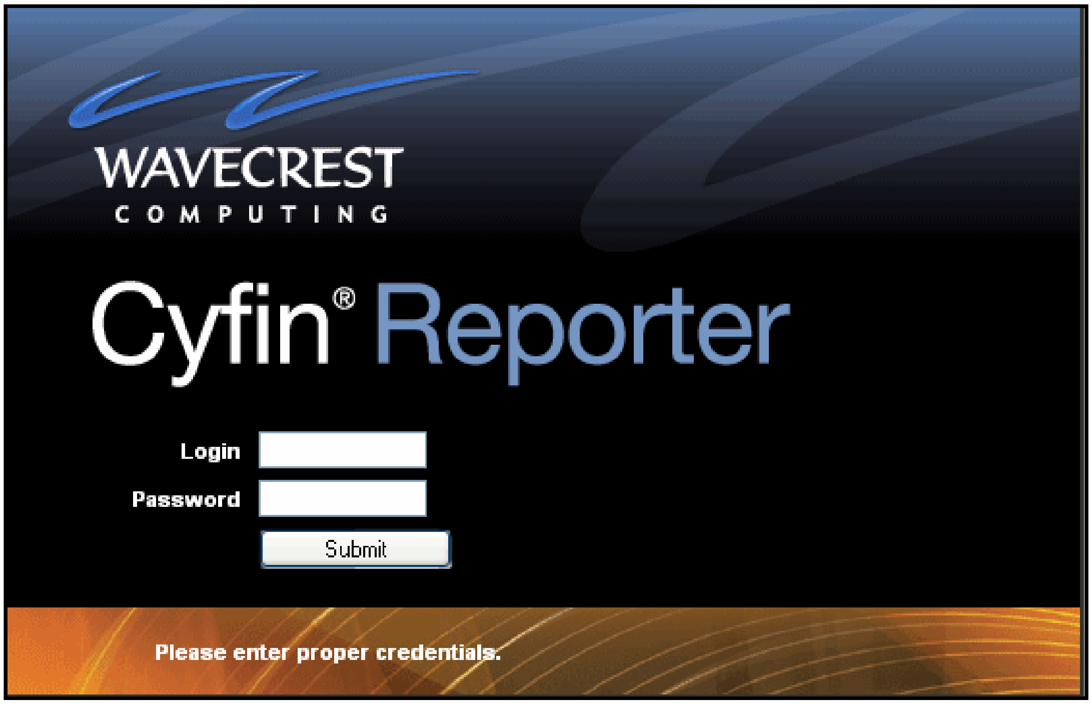
CAUTION: *If you already have a successful installation in production and are using the Data Manager feature, it is highly recommended that you save copies of your import data (.war files) to a 'safe' location before continuing.*

CAUTION: *If you ever decide to disband an array, remember to manually save import data (.war files) to a 'safe' location first. After you've taken machines out of an array scenario, you will then be able to place the import data where you see fit.*

6.1.1 Designate and Set up the Primary Server

6.1.1.1 Install the Product on the Primary Server

1. Double-click on the executable file and simply follow the wizard's onscreen instructions.
2. After a few clicks you will find yourself at the login screen shown below.



Please enter proper credentials.

3. Log into the product using the following default credentials:
LOGIN: admin
PASSWORD: password
NOTE: *If the login screen does not appear, bring it up by going to* ***Start - Programs - Cyfin - Browser Interface****.*

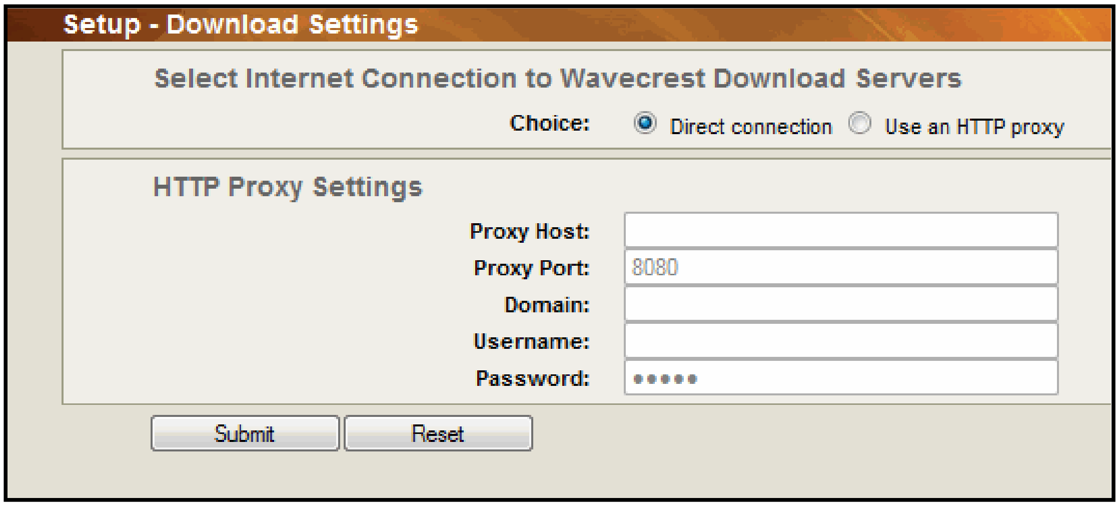
© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6.1.1.2 Download the URL List

This step will ensure that you have the latest Wavecrest URL List, which will include the most recent categorized URLs.

If you are required to use a proxy for all http connections, begin with Step 1, as you will need to configure your proxy information first. If Internet traffic does not go through a proxy, then you can skip to Step 3 for 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. If your Internet traffic goes through a proxy, go to the **Setup – Download Settings** screen to configure your proxy information. This will ensure that you can download the list, product updates, and also receive product news.



Setup - Download Settings

Select Internet Connection to Wavecrest Download Servers

Choice: ● Direct connection ○ Use an HTTP proxy

HTTP Proxy Settings

Proxy Host:

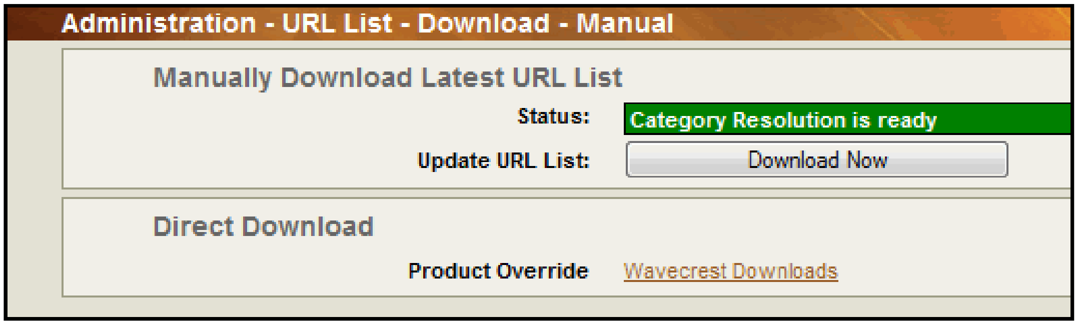
Proxy Port: 8080

Domain:

Username:

Password: •••••

2. Fill in the text-entry boxes with the correct authentication credentials, and then click **Submit**.
3. To download the list, go to the **Administration - URL List** screen and click on the **Manual** link.



Administration - URL List - Download - Manual

Manually Download Latest URL List

Status: Category Resolution is ready

Update URL List:

Direct Download

Product Override

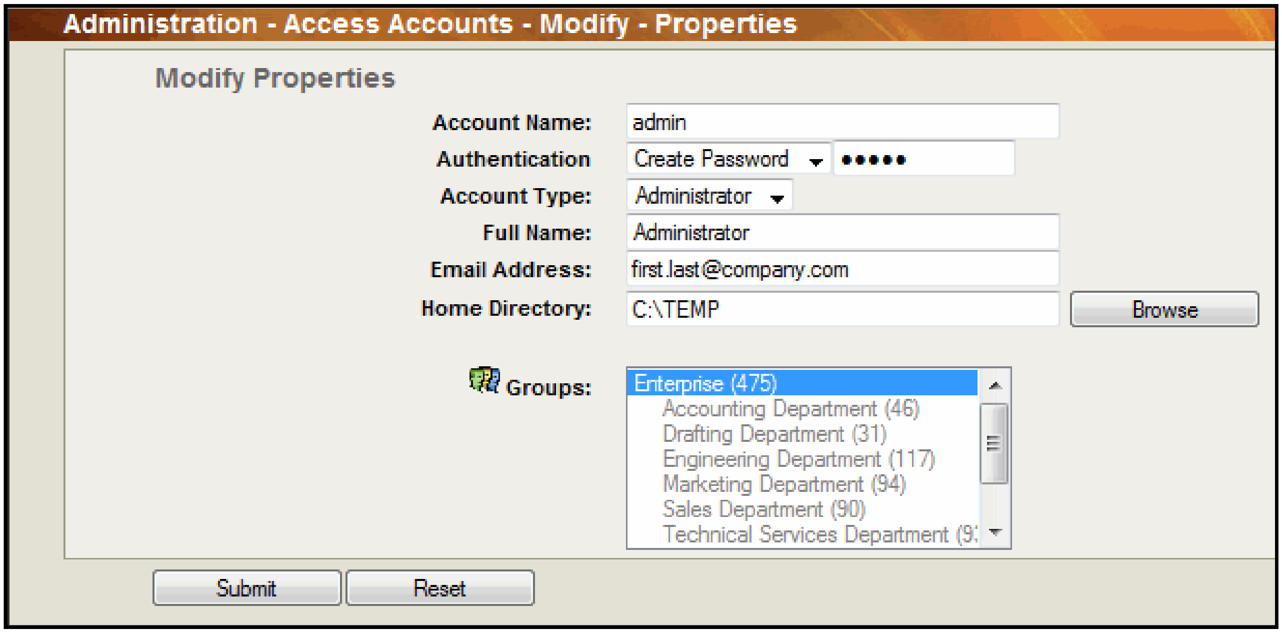
4. Next, click on the **Download Now** button. You should see a progress meter screen pop up. When it indicates that the download is complete, you can close the window.

NOTE: *The Product Override link should only be used in the event that the URL list download from the product is unsuccessful. This link will take you to a Web page where you will find the URL list download and instructions for downloading from the site.*

6.1.1.3 Change the Default Password

Once you have logged into the product, you will want to change the default password.
NOTE*: This administration account and password must be made exactly the same on all secondary servers in the array*.

1. Go to **Administration - Access Accounts** and click on the **Modify** link.
2. Click on the **admin(Administrator)** link.



Administration - Access Accounts - Modify - Properties

Modify Properties

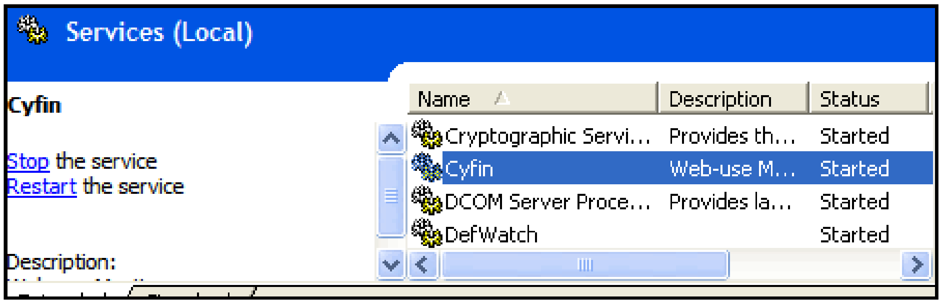
Account Name:	admin
Authentication	Create Password ●●●●●
Account Type:	Administrator
Full Name:	Administrator
Email Address:	first.last@company.com
Home Directory:	C:\TEMP
Groups:	Enterprise (475) Accounting Department (46) Drafting Department (31) Engineering Department (117) Marketing Department (94) Sales Department (90) Technical Services Department (9

3. Type in your new password in the **Password** field.
4. At this time, you can also change the **Full Name**, **Email Address**, and **Home Directory**. Reports will be sent to the **Email Address** specified and saved to the **Home Directory** specified on this screen.
5. When you have finished making your changes, click **Submit**.

6.1.1.4 Configure a Network Account for the Product Service

This step is necessary so that the Primary server can send logfile data to the Secondary servers.

1. Go into the **Control Panel**, open **Administrative Tools** and then open **Services**.
2. Right click on the product name and then click on **Properties**.



Services (Local)

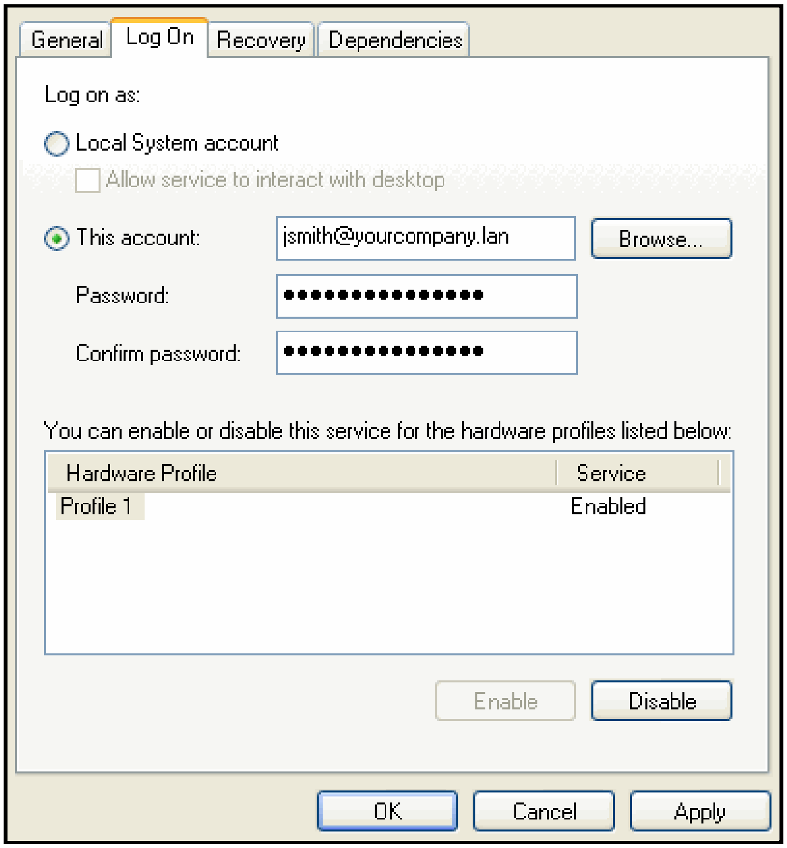
Cyfin

Stop the service
Restart the service

Description:

Name	Description	Status
Cryptographic Servi...	Provides th...	Started
Cyfin	Web-use M...	Started
DCOM Server Proce...	Provides la...	Started
DefWatch		Started

3. Select the **Logon** tab.



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: jsmith@yourcompany.lan

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

You can enable or disable this service for the hardware profiles listed below:

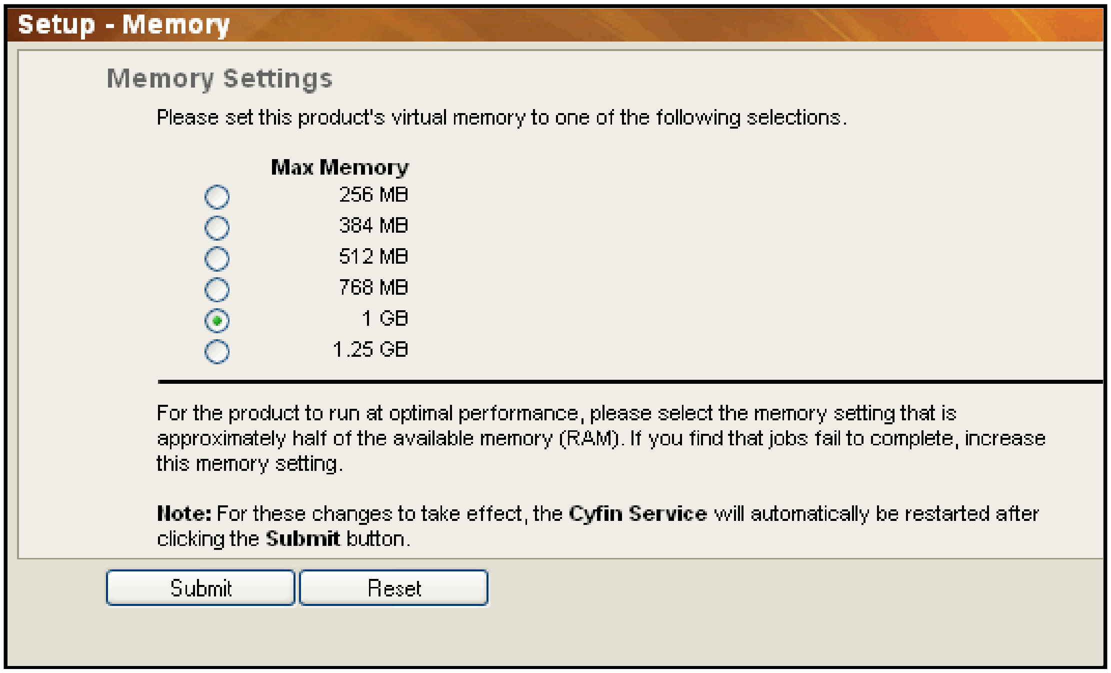
Hardware Profile	Service
Profile 1	Enabled

4. Select the radio button for **This Account** and enter a valid network account with read and write permissions.
5. Click **Apply** and then **Ok**.
6. In the Services window, right click on the product again and **Restart** the service.

6.1.1.5 Set up Memory Settings

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. For optimal performance, we recommend 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 **Setup** on the menu and then click the **Memory** link.



Setup - Memory

Memory Settings

Please set this product's virtual memory to one of the following selections.

Max Memory

○ 256 MB
○ 384 MB
○ 512 MB
○ 768 MB
● 1 GB
○ 1.25 GB

For the product to run at optimal performance, please select the memory setting that is approximately half of the available memory (RAM). If you find that jobs fail to complete, increase this memory setting.

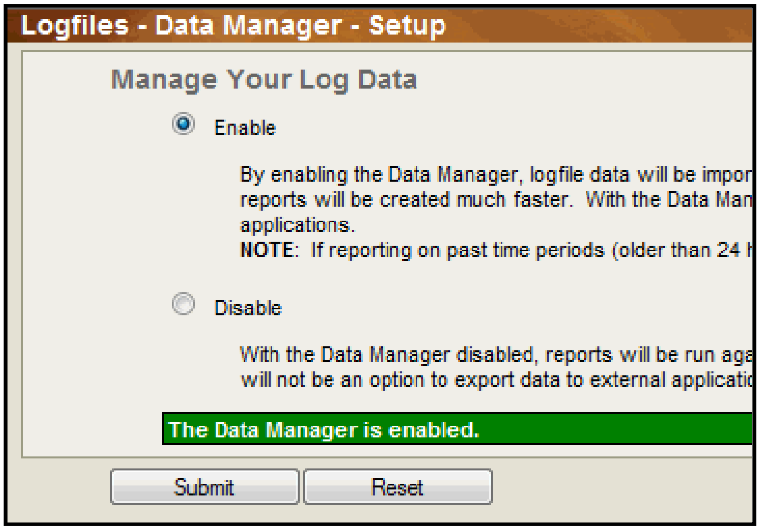
Note: For these changes to take effect, the **Cyfin Service** will automatically be restarted after clicking the **Submit** button.

2. Check the radio button (in the "**Choice**" column) that corresponds to the appropriate amount of memory to be used, keeping in mind your available RAM.
3. Click **Submit** to apply changes, or click **Reset** to reload previous values.
4. After you click Submit, you will receive a popup asking whether you would like to restart the service. Your memory setting changes will not take affect until you restart the service.

6.1.1.6 Enable the Data Manager

The Data Manager must be enabled when using an array configuration.
***NOTE**: If this is not a new installation and you already have this feature in operation, you can move on to the next step.*

1. Go to **Logfiles – Data Manager** and click on the **Enable** link.
2. Select the **Enable** radio button to enable the Data Manager.



Logfiles - Data Manager - Setup

Manage Your Log Data

● Enable

By enabling the Data Manager, logfile data will be impor
reports will be created much faster. With the Data Man
applications.
NOTE: If reporting on past time periods (older than 24 h

○ Disable

With the Data Manager disabled, reports will be run aga
will not be an option to export data to external applicatio

The Data Manager is enabled.

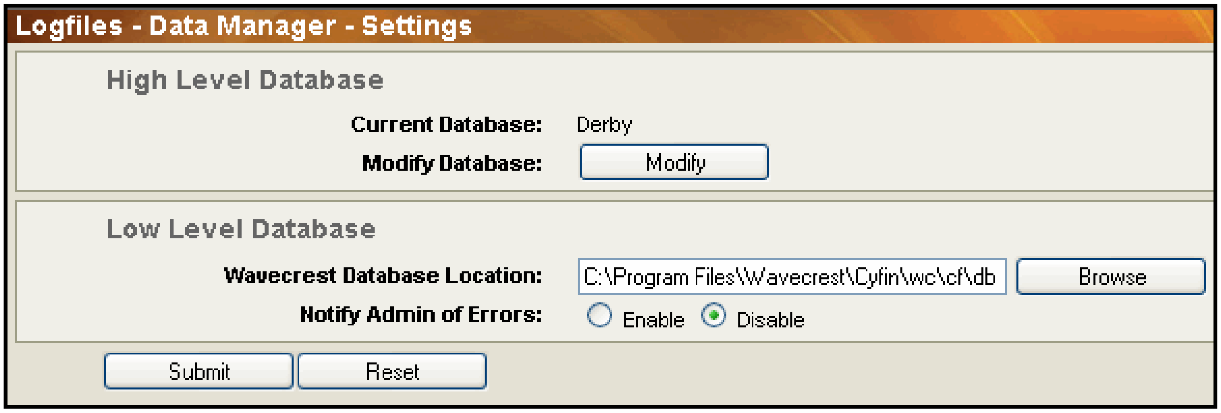
3. Click **Submit**. A screen containing instructions for importing your logfile data will pop up. At this time you will not have any logfiles to import. You must finish the steps to configure your array before any logfiles will be available.

6.1.1.7 Set the Import Data Storage Location

The Import Data storage location needs to be on a shared network drive so that all servers in the array will be able to find the imported data. If that is not the case on an already configured Cyfin install, we recommend that you save copies of all import data (.war files) to a 'safe' location as a backup precaution. Then, change the locally configured storage path to a shared network drive location. Place copies of any pre-existing (pre-Array) import data in the new shared location. We recommend that you also keep backup copies of pre-existing import data elsewhere for a short amount of time to ensure that no data is lost.

NOTE: *Test results have proven that having this location at a different physical hard disk than the logfile configuration you set above results in much faster import time. We recommend this setup because in this scenario you're reading from one hard disk and writing to another.*

1. Go to **Logfiles – Data Manager** and click on the **Settings** link.



Logfiles - Data Manager - Settings

High Level Database

Current Database: Derby

Modify Database:

Low Level Database

Wavecrest Database Location: C:\Program Files\Wavecrest\Cyfin\wc\cf\db

Notify Admin of Errors: ○ Enable ● Disable

2. Type in the path of the shared network drive in the **Wavecrest Database Location** field.
3. Choose whether or not to receive email notification regarding import data errors. Use the radio buttons to **Enable** or **Disable** this feature.
4. Click **Submit** to apply your settings.

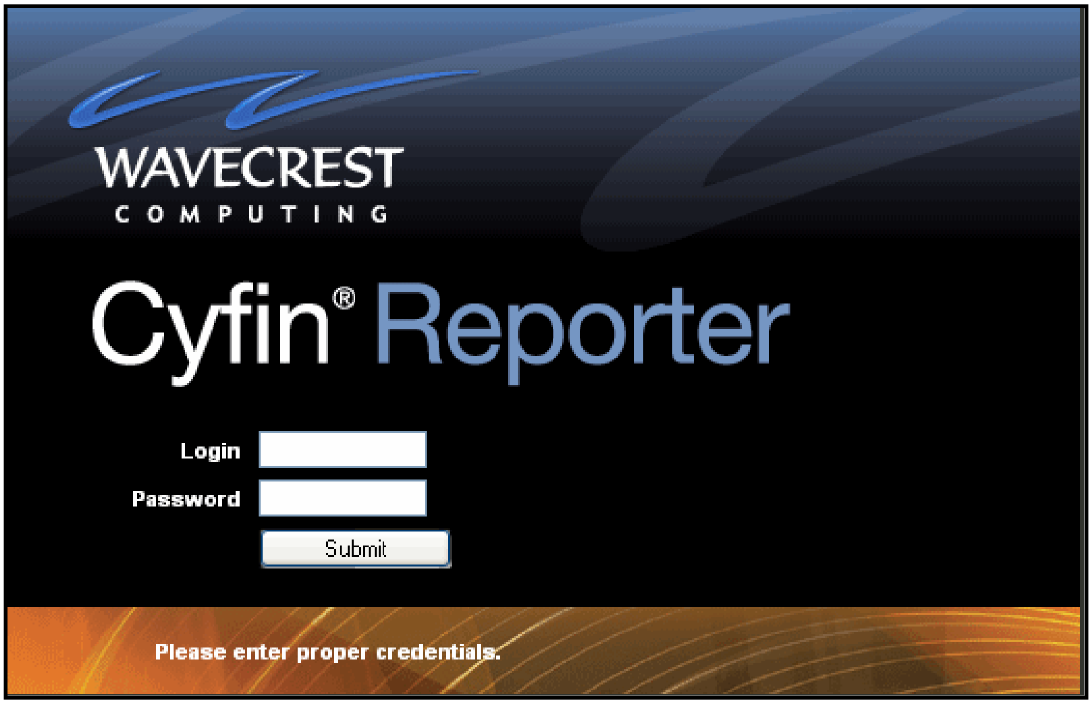
NOTE: *Only for **Smartfilter customers** (if not, ignore this step). Change the **supplemental URL list** directory. This path must be a shared UNC location. Manually configure it on the **Administration - URL List - Supplemental List** screen.*

6.1.2 Designate and Set up Secondary Servers

Be sure to follow each step in this section for every secondary server install.

6.1.2.1 Install the Product on the Secondary Servers

1. Double-click on the executable file and simply follow the wizard's onscreen instructions.
2. After a few clicks you will find yourself at the login screen shown below.



Please enter proper credentials.

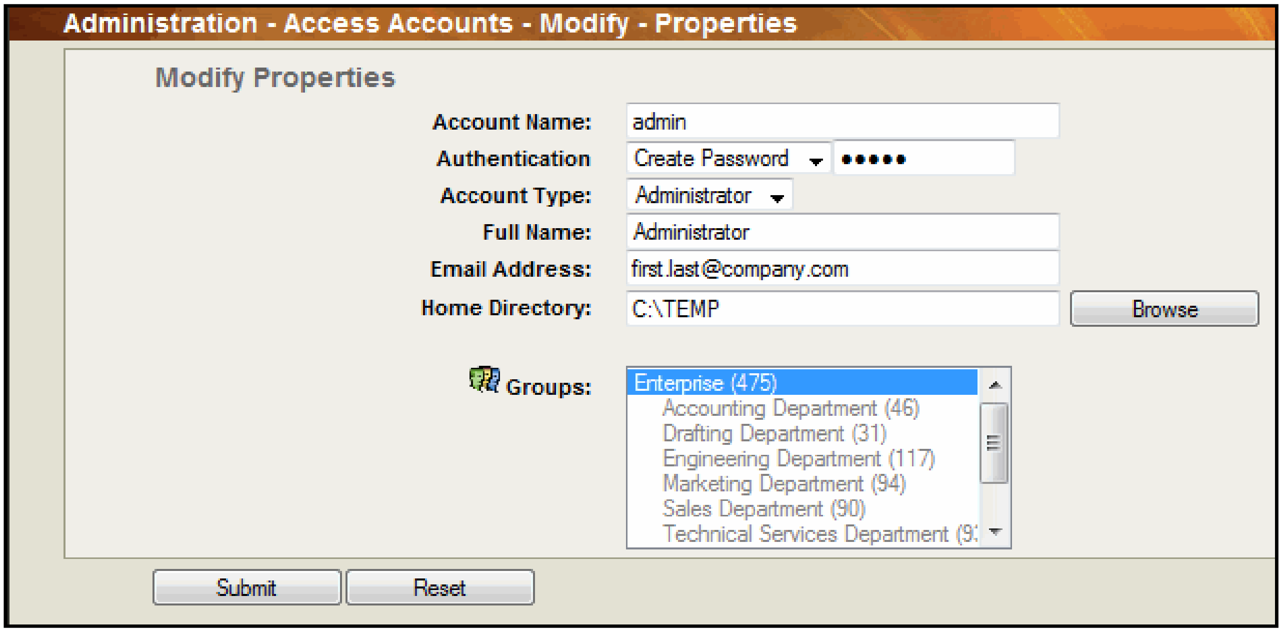
3. Log into the product using the following default credentials:
   LOGIN: admin
   PASSWORD: password

NOTE: *If the login screen does not appear, bring it up by going to* ***Start - Programs - Cyfin - Browser Interface****.*

6.1.2.2 Change the Default Password

Once you have logged into the product on the secondary servers, you will need to change the default password to match that of the primary. The accounts and passwords for all products in the array must be the same.

1. Go to **Administration - Access Accounts** and click on the **Modify** link.
2. Click on the **admin(Administrator)** link.



Administration - Access Accounts - Modify - Properties

Modify Properties

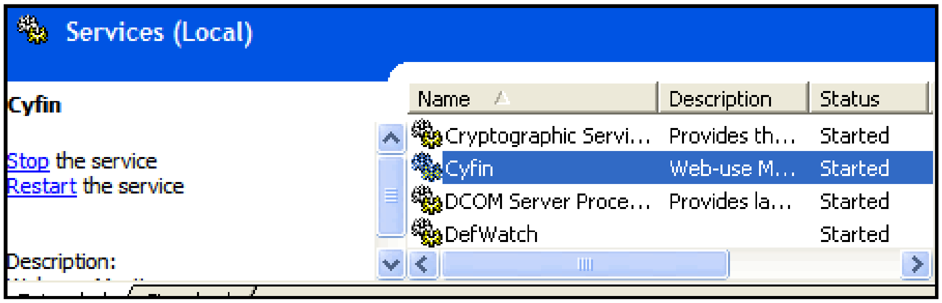
Account Name:	admin
Authentication	Create Password ●●●●●
Account Type:	Administrator
Full Name:	Administrator
Email Address:	first.last@company.com
Home Directory:	C:\TEMP
Groups:	Enterprise (475) Accounting Department (46) Drafting Department (31) Engineering Department (117) Marketing Department (94) Sales Department (90) Technical Services Department (9:

3. Type in your new password in the **Password** field. This must **exactly match** the password you set on the Primary.
4. When you have finished making your changes, click **Submit**.

6.1.2.3 Configure a Network Account for the Product Service

This step is necessary so that the secondaries can receive logfile data from the primary.

1. Go into the **Control Panel** and open **Administrative Tools** and then open **Services**.
2. Click on the product name so that it is highlighted.
3. Right click on the product name and go into **Properties**.



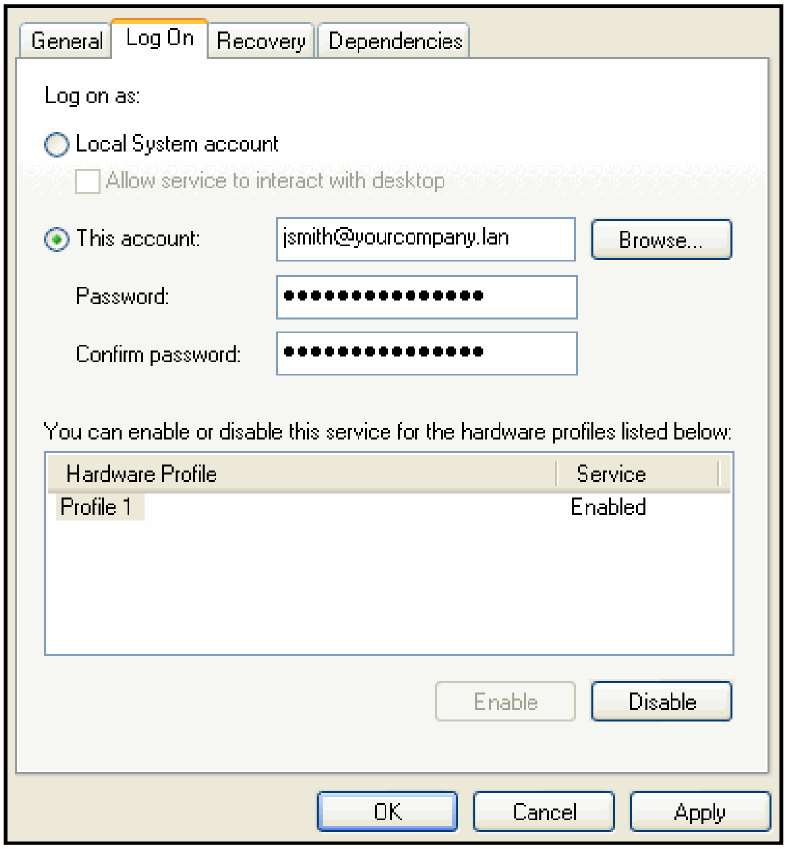
Cyfin

Stop the service
Restart the service

Description:

Name	Description	Status
Cryptographic Servi...	Provides th...	Started
Cyfin	Web-use M...	Started
DCOM Server Proce...	Provides la...	Started
DefWatch		Started

4. Select the **Logon** tab.



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: jsmith@yourcompany.lan

Password: •••••••••••••••

Confirm password: •••••••••••••••

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

5. Select the radio button for **This Account** and enter a valid network account with read and write permissions.
6. Click **Ok**.
7. In the Services window, right click on the product again and **Restart** the service.

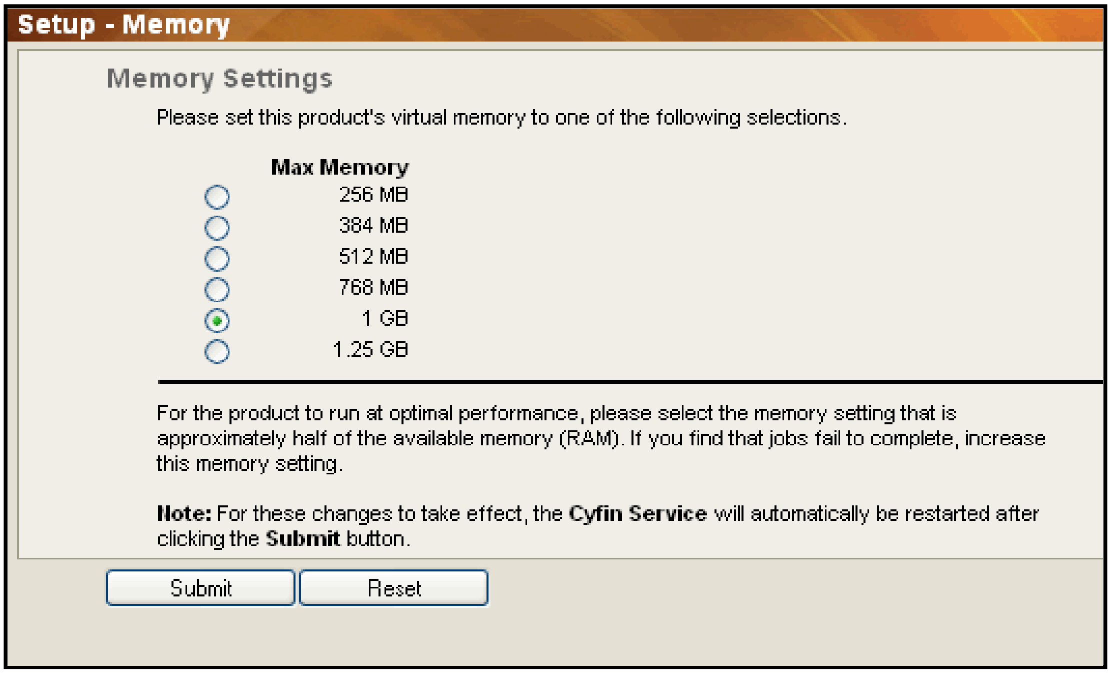
© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6.1.2.4 Set up Memory Settings

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 on new installs is 256MB. We recommend that you set the memory to be at least half of the available RAM on the machine. If you start to meet your memory threshold, the product will notify you to increase your memory setting.

NOTE: *For optimal performance, we recommend that you choose the setting that is approximately half of your available memory (RAM).*

1. To set your memory, go to **Setup** on the menu and then click the **Memory** link.



Setup - Memory

Memory Settings

Please set this product's virtual memory to one of the following selections.

Max Memory

○ 256 MB
○ 384 MB
○ 512 MB
○ 768 MB
● 1 GB
○ 1.25 GB

For the product to run at optimal performance, please select the memory setting that is approximately half of the available memory (RAM). If you find that jobs fail to complete, increase this memory setting.

Note: For these changes to take effect, the **Cyfin Service** will automatically be restarted after clicking the **Submit** button.

2. Check the radio button (in the "**Choice**" column) that corresponds to the appropriate amount of memory to be used, keeping in mind your available RAM.
3. Click **Submit** to apply changes, or click **Reset** to reload previous values.
4. After you click Submit, you will receive a popup asking whether you would like to restart the service. Your memory setting changes will not take affect until you restart the service.

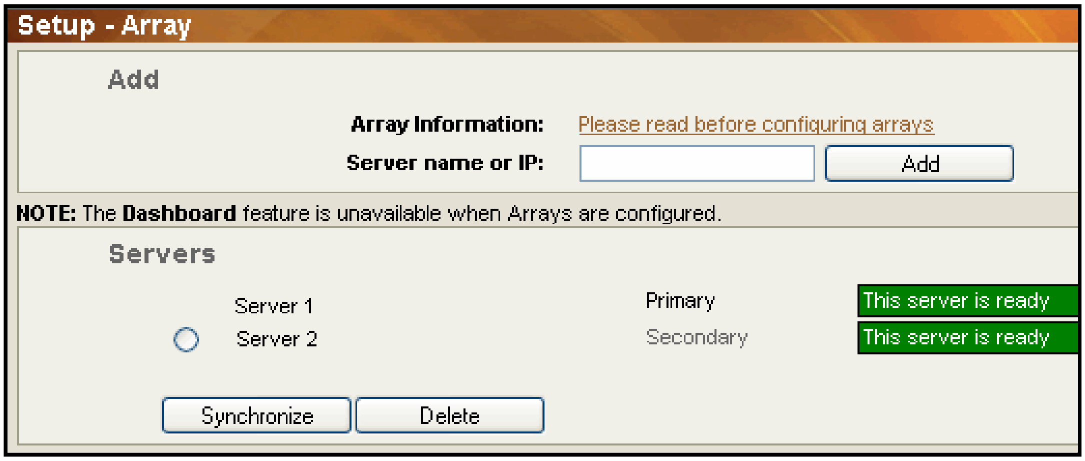
© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6.1.3 Complete Set up on the Primary Server

6.1.3.1 Add Secondary Servers to the Array

1. On the Primary, go to **Setup - Array**.
   CAUTION: *This screen will be accessible from all of your product installations, but only use this screen from the installation on your primary server. Do not use this screen on any of your secondary installations.*

2. Add a secondary server to the array by typing in the **Server Name or IP Address** in the text field and click **Add**. You should immediately see the primary server name or IP address and the secondary server name or IP address listed in the **Server** section as shown below. Repeat this step until you have added all of your secondary servers to the array.



Setup - Array

Add

Array Information: Please read before configuring arrays

Server name or IP: [ ] Add

NOTE: The **Dashboard** feature is unavailable when Arrays are configured.

Servers

	Server 1	Primary	This server is ready
○	Server 2	Secondary	This server is ready

Synchronize Delete

3. Now you are ready to begin setting up the product on your primary server. Before you do this, make sure that all of your secondary servers in the array have a status of **Ready** as shown in the image above. If they do not have a **Ready** status, the settings in the product installations on those servers will not be updated.

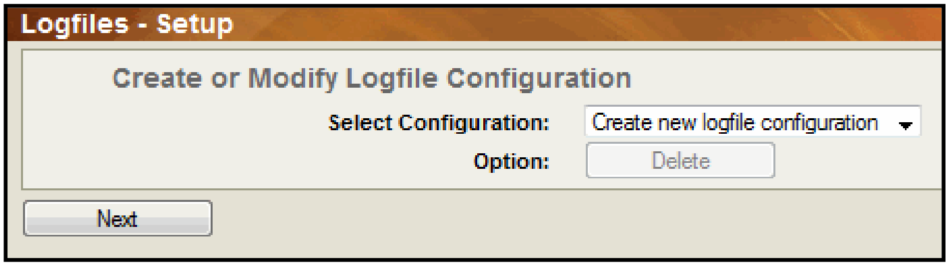
4. As you add secondary servers, each one is automatically synchronized with the Primary when added. As long as the secondary servers remain active with a status of Ready, they will be automatically updated to match the configuration on the Primary. However, if a secondary is ever "down" for a period of time or gets "out of sync" with the Primary, simply select that server's radio button and click the **Synchronize** button. If you ever need to synchronize all machines in the array, simply click the **Synchronize** button.

5. If at any time you want to delete a server in the array, select that server's radio button and click **Delete**. To delete all servers from the array, just click Delete without selecting a radio button.

6.1.3.2 Configure Logfiles

This process will configure the product to read your logfiles.

1. Begin by going to the **Logfiles - Setup** screen.



Logfiles - Setup

Create or Modify Logfile Configuration

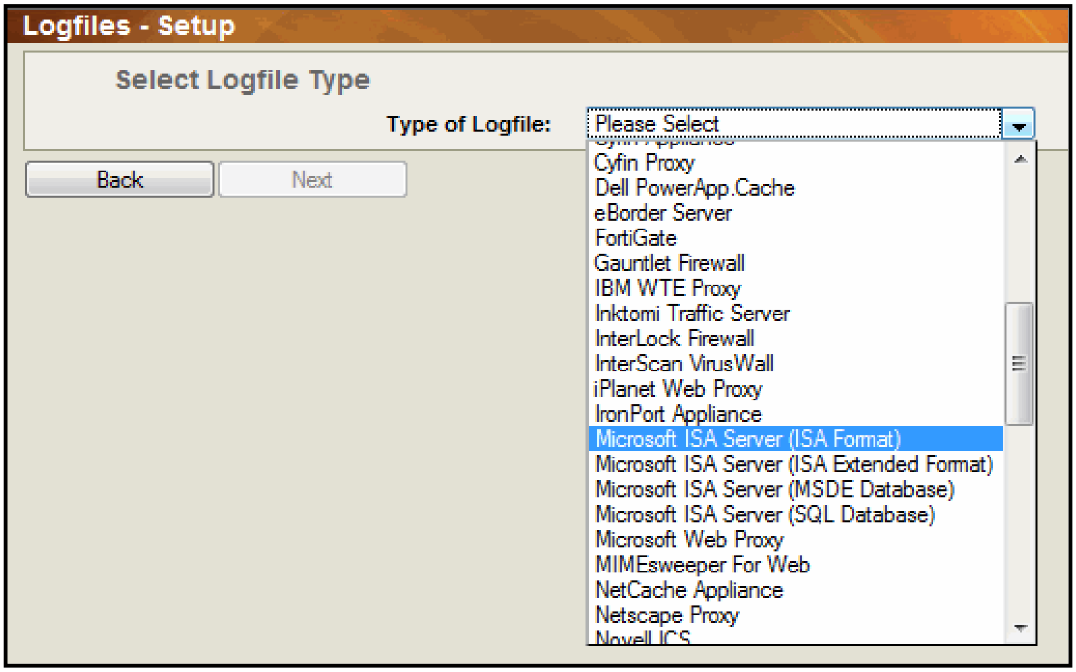
Select Configuration: Create new logfile configuration

Option: Delete

Next

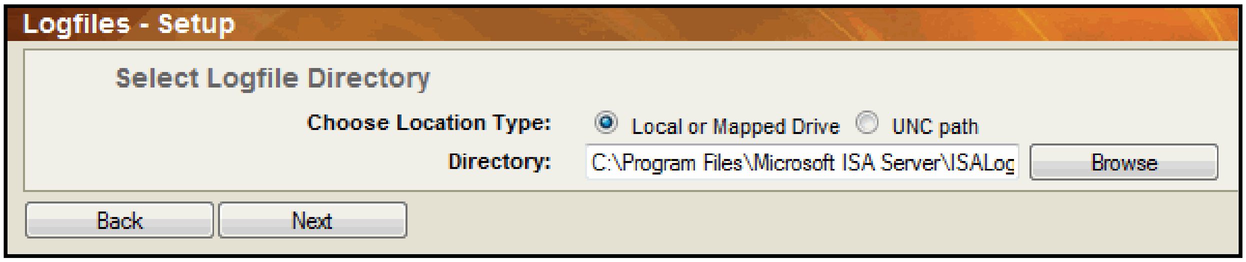
2. Leave the default choice *Create new logfile configuration* in the drop down box and simply click **Next**.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.



3. Use the pull down menu and select the **Type of Logfile** for your server.
   NOTE: *If you make a mistake, the product will realize it in a couple of steps and redirect you back to try again.*

4. When you have made your choice, click **Next**.

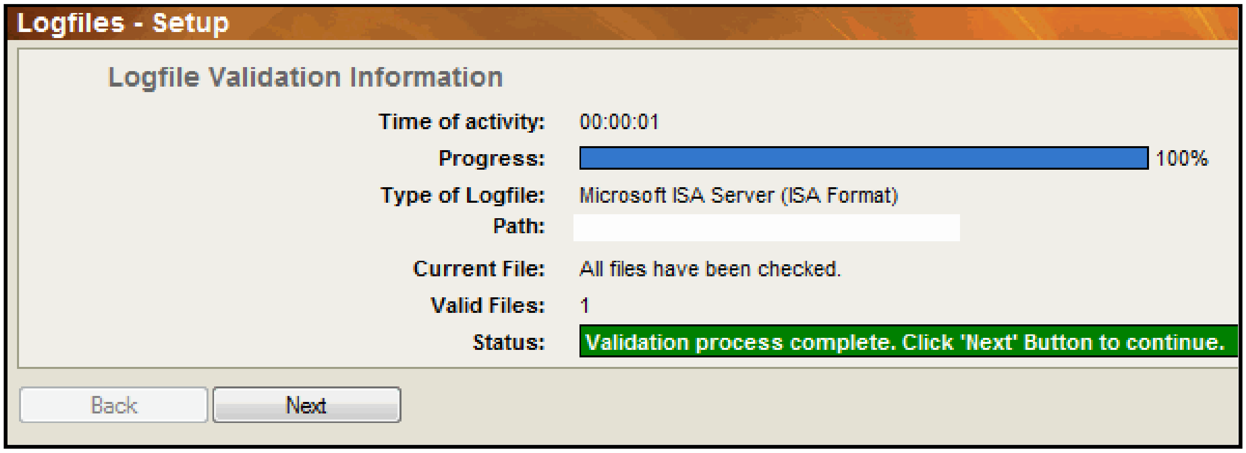


Choose Location Type: ● Local or Mapped Drive ○ UNC path

Directory: C:\Program Files\Microsoft ISA Server\ISALog

5. Configure the logfile directory and click **Next**.
   NOTE: *Remember that secondary servers must "share" their log folders for the Primary server to access the logfiles across the network.*

6. The product will locate and validate your logfiles in the next step. You should see a progress meter and a message indicating success on this screen.



Time of activity: 00:00:01

Progress: 100%

Type of Logfile: Microsoft ISA Server (ISA Format)

Path:

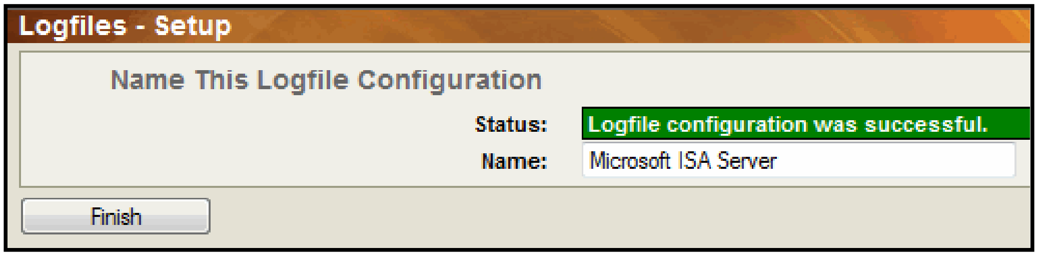
Current File: All files have been checked.

Valid Files: 1

Status: Validation process complete. Click 'Next' Button to continue.

7. When you see the green colored success message, click **Next**.
   NOTE: *If there was a problem finding logfiles or validating them, an error message will appear with helpful information, and direct you to click the **Back** button to make a change.*

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.



Logfiles - Setup

Name This Logfile Configuration

Status: Logfile configuration was successful.

Name: Microsoft ISA Server

8. When valid logfiles have been configured, the next step is to name the configuration. This is helpful for identification purposes, especially if you add more log file configurations later.
9. After typing in a name for your new log file configuration, click **Finish**.

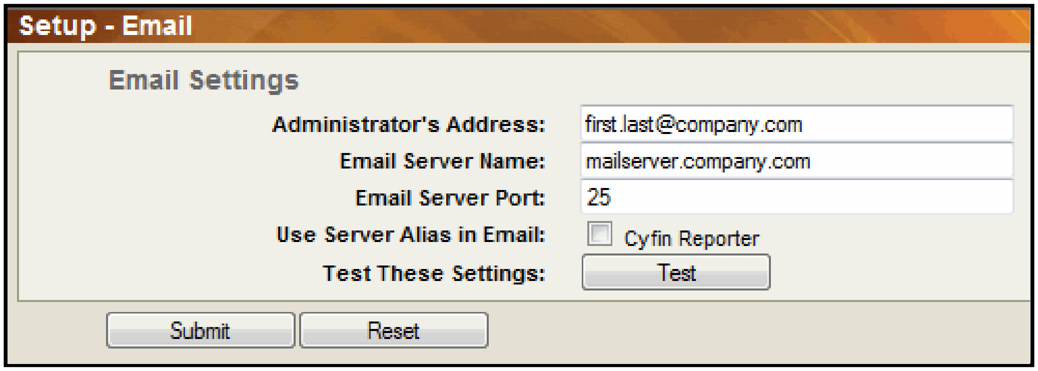
   ***NOTE:** If you don't name the configuration and simply click **Finish**, the product will name the configuration the same as your logfile type.*
10. Finally, just close the window or click on the link displayed to add another configuration.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6.1.3.3 Set up Administrator Email

This step will let the Administrator receive all product-produced emails (e.g., error messages, fault indicators, URL list download notifications, etc.).

1. Go to the **Setup - Email** screen.



Setup - Email

Email Settings

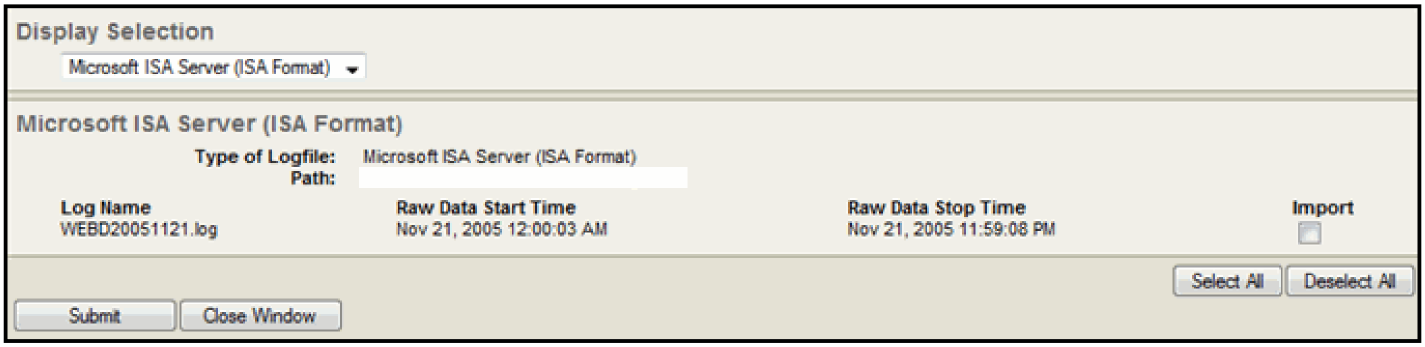
Administrator's Address: first.last@company.com
Email Server Name: mailserver.company.com
Email Server Port: 25
Use Server Alias in Email: □ Cyfin Reporter
Test These Settings:

2. Fill out the screen with the Administrator's email information.
3. Click on the **Test** button to make sure the product is communicating with the email server.
4. If it is successful, then click **Submit** to save the configuration.

6.1.3.4 Import Data into the Data Manager

Before you can run reports, you must import logfiles into the Data Manager. These instructions show you how to manually import data. You may also set up a regular scheduled import. You can find instructions for setting up a scheduled import in Section 3.2.

1. Go to **Logfiles – Data Manager** and click on the **Import Data** link.
2. Click on the **Manual** link under **Import**. A list of logs available for import will appear.



Display Selection

Microsoft ISA Server (ISA Format)

Microsoft ISA Server (ISA Format)

Type of Logfile: Microsoft ISA Server (ISA Format)
Path:

Log Name	Raw Data Start Time	Raw Data Stop Time	Import
WEBD20051121.log	Nov 21, 2005 12:00:03 AM	Nov 21, 2005 11:59:08 PM	□

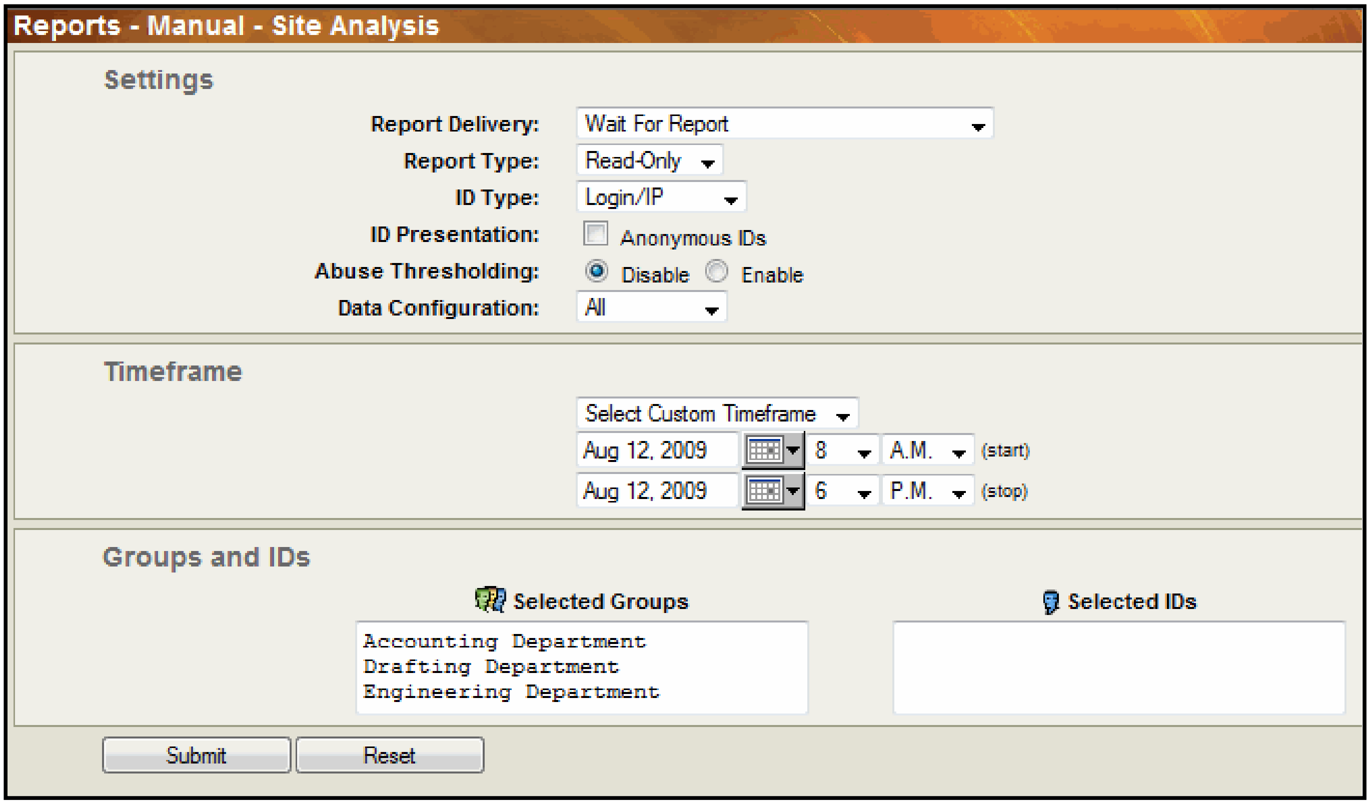
3. Check the boxes of the logs that you wish to import. If you wish to import all of the logs, you can click on the **Select All** button at the end of the logfile list.
4. Click **Submit** to import the logs into the database.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

6.1.3.5 Create and Run a Site Analysis Report

Now that you have completed basic configuration of the product, it's time to run a report.

1. Go to the **Reports - Manual** screen.
2. Click on the first link, **Site Analysis**.



Reports - Manual - Site Analysis

Settings

Report Delivery: Wait For Report

Report Type: Read-Only

ID Type: Login/IP

ID Presentation: □ Anonymous IDs

Abuse Thresholding: ● Disable ○ Enable

Data Configuration: All

Timeframe

Select Custom Timeframe

Aug 12, 2009 8 A.M. (start)

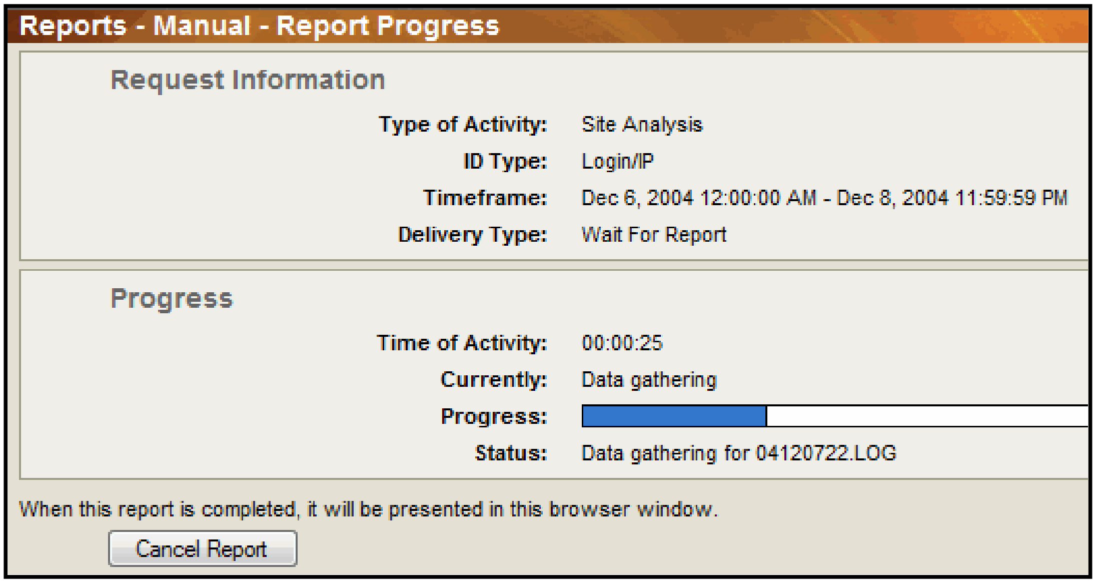
Aug 12, 2009 6 P.M. (stop)

Groups and IDs

Selected Groups: Accounting Department
Drafting Department
Engineering Department

Selected IDs:

3. In the **Report Type** field, select either *Read-only* or *Interactive*.
4. In the **ID Type** field, select *Login/IP* to ensure that you will see some data in your report.
5. Notice that on this screen shot, there is a **Data Configuration** field. This field will only appear if you have more than one logfile configuration. It allows you to filter your report data down to a single configuration.
6. For basic testing purposes on this screen, use the **Timeframe** pulldown to *Select Custom Timeframe*. Date and Time field selections will appear. You need to configure a *Start Date/Time* and *Stop Date/Time* ensuring that surfing activity is included. Choose a time period that is covered by the data you imported into the Data Manager, and only covers about one or two hours.
7. Leave the Enterprise group in the **Selected Groups** box, and simply click **Submit**.



Reports - Manual - Report Progress

Request Information

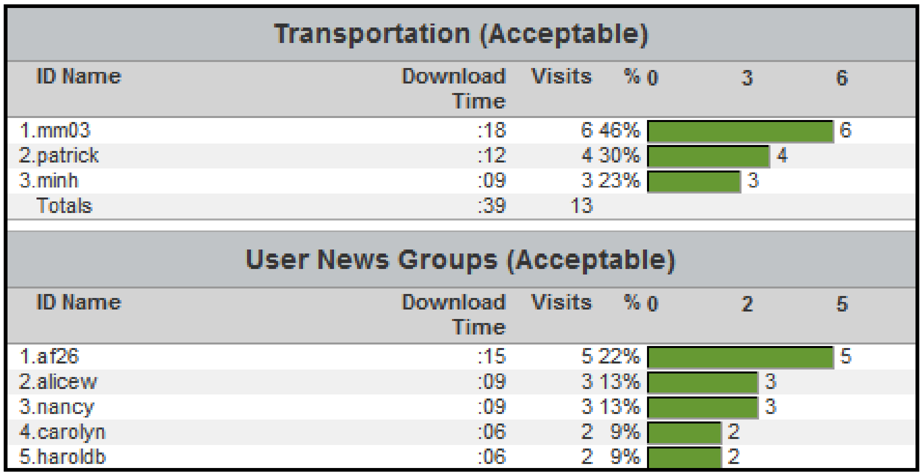
Type of Activity:	Site Analysis
ID Type:	Login/IP
Timeframe:	Dec 6, 2004 12:00:00 AM - Dec 8, 2004 11:59:59 PM
Delivery Type:	Wait For Report

Progress

Time of Activity:	00:00:25
Currently:	Data gathering
Progress:	
Status:	Data gathering for 04120722.LOG

When this report is completed, it will be presented in this browser window.

8. After your report finishes, click on the **All IDs** link that will be displayed. A sample portion of the Site Analysis report is shown below. The Site Analysis report will show you total visits by classification, category, and by user per category.



Transportation (Acceptable)

ID Name	Download Time	Visits	%	0 3 6
1.mm03	:18	6	46%	6
2.patrick	:12	4	30%	4
3.minh	:09	3	23%	3
Totals	:39	13		

User News Groups (Acceptable)

ID Name	Download Time	Visits	%	0 2 5
1.af26	:15	5	22%	5
2.alicew	:09	3	13%	3
3.nancy	:09	3	13%	3
4.carolyn	:06	2	9%	2
5.haroldb	:06	2	9%	2

9. View your report, and verify that you see user IDs along with categorized Web activity.

***NOTE**: If you only get activity on IP addresses, you most likely need to configure authentication on your network to see login names. If your configured logs do not contain login names (due to a lack of network user authentication), then you will only get data on IP addresses until/unless you start authenticating login names. From that point forward, you'll be able to use Login Names as the **ID Type** in reports.*

7.0 Administrative Features

This section covers additional administrative features to be used and maintained by the product's administrator. Before getting started on this section, be sure to complete the Getting Started section of the manual first. It contains vital instructions that need to be completed before moving on to creating accounts or scheduling the download of the URL list.

Administrative Features includes instructions on how to:

- **Create, Modify, and Delete Administrator and Operator Accounts** – Instructions on how to manage administrator and operator accounts.
- **Download the URL List** – Covers how to manually download the list and schedule it for download daily.
- **Download Product Updates** – Instructions on how to check for updates and download them when needed.
- **Check Product News** – Learn how to read product news and change the settings.

As mentioned previously in Reporting, assigning operator accounts to those that need reports regularly can save IT administrators considerable time and effort. Individuals with operator accounts can access the product, but only via a limited menu that lets them run reports on the groups and users that they have been authorized to review. They cannot make or change administrative settings.

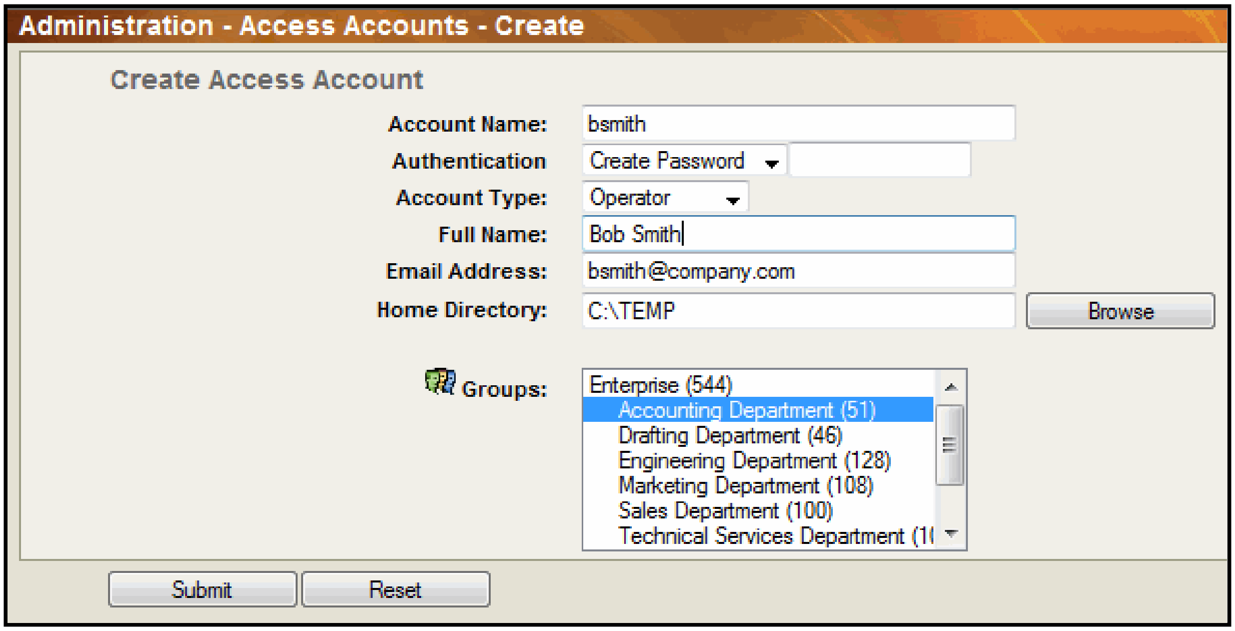
It is important to maintain the latest downloads of the product's URL list and upgrades. Keeping the list current and preventing it from expiring will reduce the number of Web sites listed in the “Other” (unidentified) category. Taking advantage of upgrades will keep the product running smoothly.

Finally, product news will let you know if there are any new critical product releases or current Internet issues that may affect your Web-use management policies.

7.1 Create Administrator and Operator Accounts

Two types of accounts can be issued: administrator accounts and operator accounts. Administrator account users have full access to and control of the product. Operator account users only have access to a limited menu that lets them create, run and review reports.

1. To create an administrator or operator account, go to **Administration – Access Accounts** and click on the **Create** link.



Administration - Access Accounts - Create

Create Access Account

Account Name: bsmith

Authentication: Create Password

Account Type: Operator

Full Name: Bob Smith

Email Address: bsmith@company.com

Home Directory: C:\TEMP

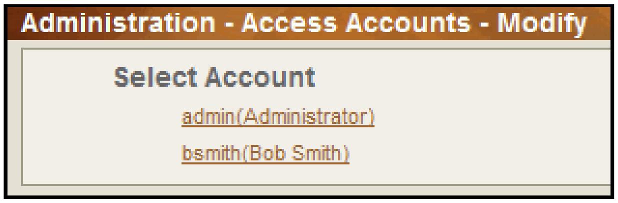
Groups:
Enterprise (544)
Accounting Department (51)
Drafting Department (46)
Engineering Department (128)
Marketing Department (108)
Sales Department (100)
Technical Services Department (1(

2. Type in the **Account Name** (or login name) to be used by the account owner. If you plan to use the Active Directory Authentication option make sure the account name matches the Active Directory account name exactly.
3. In the **Authentication** field, select *Use Active Directory* or *Create Password*. If you select *Create Password*, a text box will appear where you will type in a password for the account.
4. Use the pull-down arrow to choose either *Administrator* or *Operator* for the type of account you are creating.
5. Type in the **Full Name** of the account user.
6. Type in the **Email Address** of the account user. For operator accounts, reports covering Groups selected during the report-creation process will be sent to this email address. This email address overrides the default administrator email account entered during product setup. It also serves as the “From” address when the account owner is logged in and chooses to email reports to other recipients.
7. Type in or browse to the **Home Directory** that has been set up for the account owner to store reports in.
8. Select the **Group(s)** for which the account owner will be authorized to create and view reports and perform other functions (if applicable). To select more than one group, hold down the Ctrl key and click on each **Group**.
   NOTE*: The text box displays the (optional) user-grouping structure created during Groups and IDs setup. You can learn how to set up Groups and IDs in Section 2 of the manual.*
9. Click **Submit** to create the account.

7.2 Modify Administrator and Operator Accounts

This feature lets you modify a previously established administrator or operator account.

1. Go to **Administration – Access Accounts** and click on the **Modify** link.



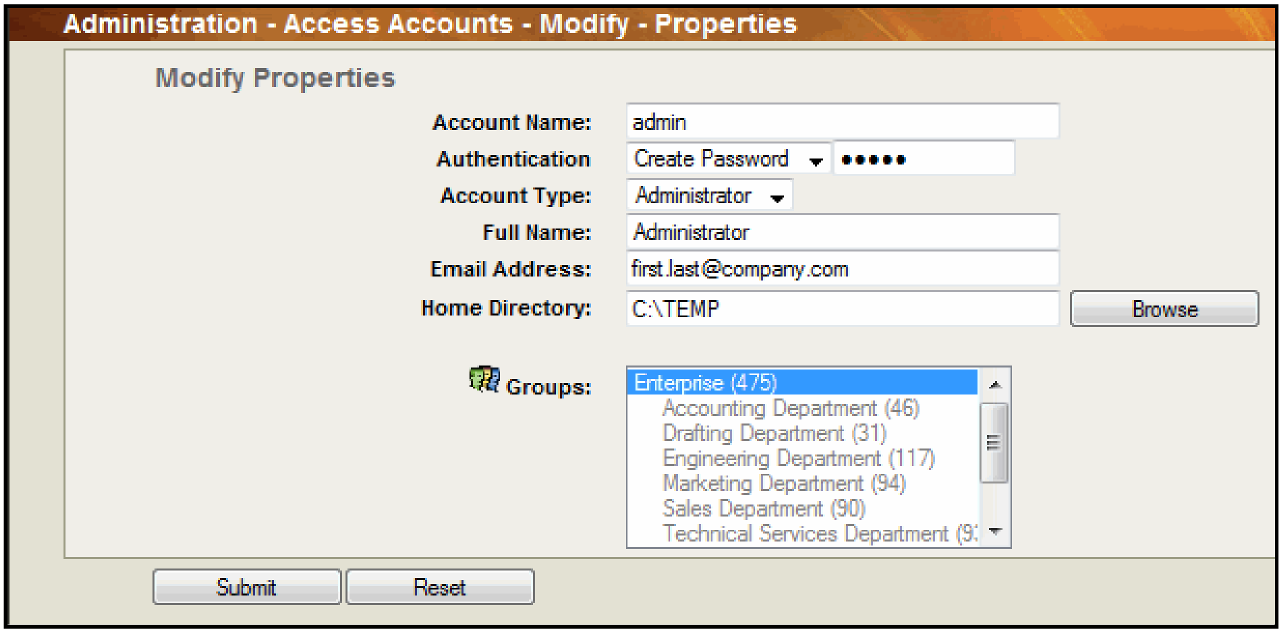
Administration - Access Accounts - Modify

Select Account

admin(Administrator)

bsmith(Bob Smith)

2. Click on the account you wish to modify.



Administration - Access Accounts - Modify - Properties

Modify Properties

Account Name: admin

Authentication: Create Password ●●●●●

Account Type: Administrator

Full Name: Administrator

Email Address: first.last@company.com

Home Directory: C:\TEMP

Groups:

Enterprise (475)

Accounting Department (46)

Drafting Department (31)

Engineering Department (117)

Marketing Department (94)

Sales Department (90)

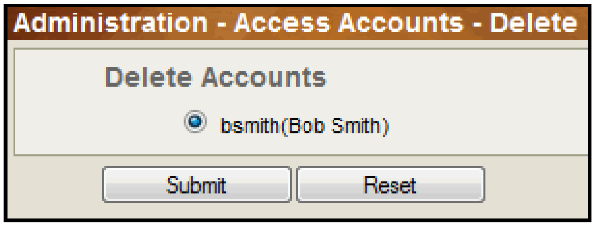
Technical Services Department (9:

3. Make your changes and click **Submit** to apply them.

7.3 Delete Administrator and Operator Accounts

Delete previously established administrator or operator accounts.
NOTE: *The administrator account cannot be deleted if he/she is currently logged in.*

1. Go to **Administration – Access Accounts** and click on the **Delete** link.



● bsmith(Bob Smith)

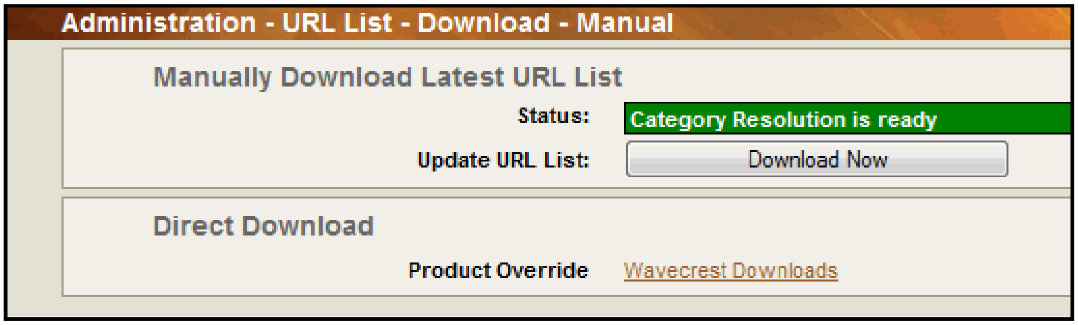
2. Select the radio button for the account that you wish to delete and click **Submit**.

7.4 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.

7.4.1 Manual Download

1. Go to **Administration – URL List** and click on the **Manual** link.



Administration - URL List - Download - Manual

Manually Download Latest URL List

Status: Category Resolution is ready

Update URL List: Download Now

Direct Download

Product Override: Wavecrest Downloads

2. If the URL list is expired (older than 45 days), the **status** bar will be red with a message stating that the list is expired. If the URL list is about to expire (older than 30 days), the **status** bar 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 in. If your latest list was downloaded within 30 days, the status bar will be green as shown above.
__NOTE__: To avoid the risk of having the list expire, we recommend that you schedule the URL list to automatically download daily. See Section 6.4.1 for instructions on scheduling the download.

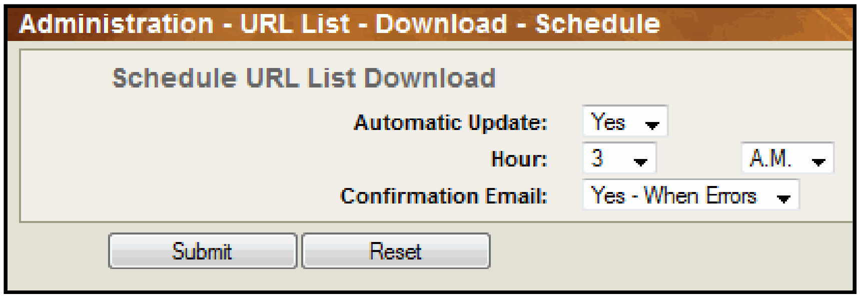
3. Click on the **Download Now** button to download the latest version of the list. A screen will pop up with a **Download Progress** bar will show the download's progress percentage.

4. You will receive a confirmation statement in the **Textual Progress** area when the list is fully downloaded. When this occurs, you can close the window.

NOTE: *The Product Override link should only be used in the event that the URL list download from the product is unsuccessful. This link will take you to a Web page where you will find the URL list download and instructions for downloading from the site.*

7.4.2 Schedule Download

1. Go to **Administration – URL List** and click on the **Schedule** link.



Administration - URL List - Download - Schedule

Schedule URL List Download

Automatic Update: Yes

Hour: 3 A.M.

Confirmation Email: Yes - When Errors

2. Use the pull-down arrow to select *Yes* in the **Automatic Update** field to enable the scheduled download.
__NOTE__: If you ever want to disable the scheduled download, change the __Automatic Update__ option to No and click __Submit__. This will turn off the automatic update.

3. Choose the **Hour** that you want the automatic update to occur by using the pull-down arrows.

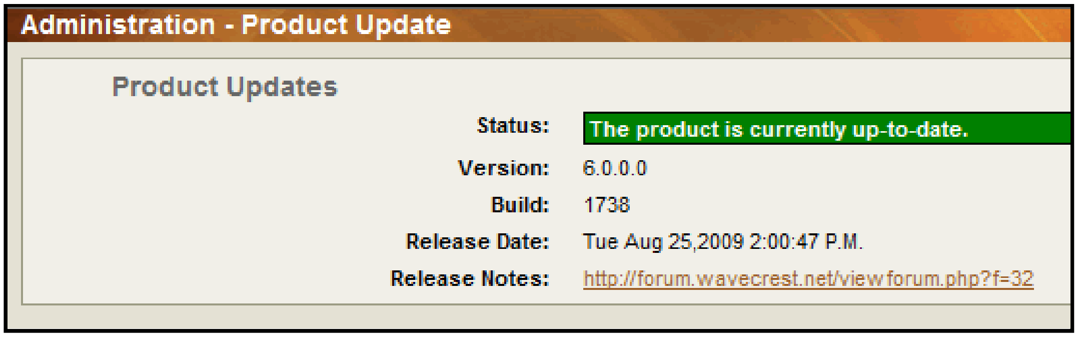
4. If you would like a **Confirmation Email** to be sent to the administrator confirming that the URL list download was successful, select *Yes*. If not, select *No*.

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

7.5 Download Product Updates

Use the Product Update screen to check for new product versions and download the latest release.

1. Go to **Administration – Product Update**. This screen will tell you if there are any current updates to the version of your product.



Administration - Product Update

Product Updates

Status: The product is currently up-to-date.

Version: 6.0.0.0

Build: 1738

Release Date: Tue Aug 25,2009 2:00:47 P.M.

Release Notes: http://forum.wavecrest.net/viewforum.php?f=32

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

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

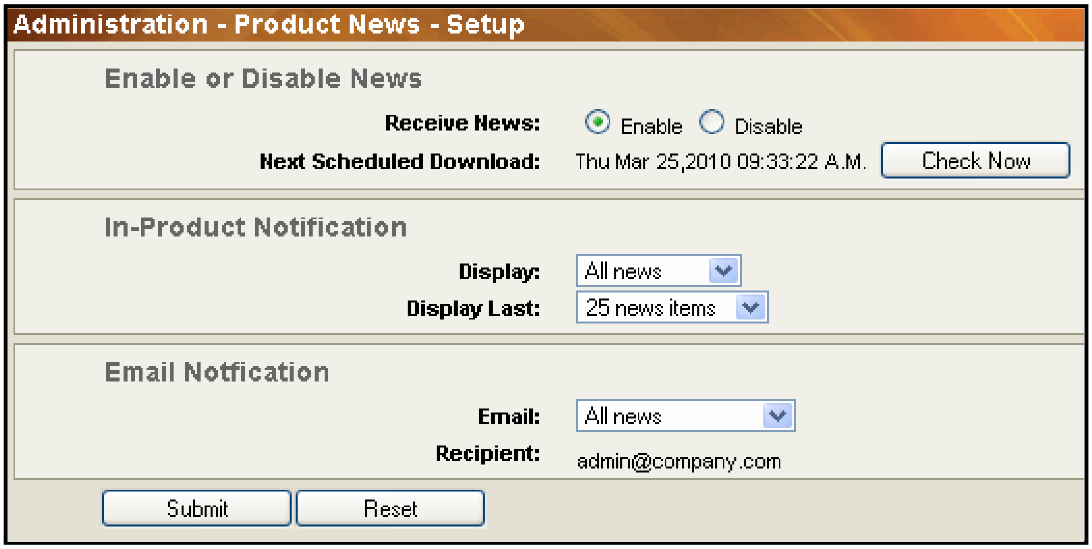
7.6 Check Product News

The Product News system allows you to receive critical information on new product updates and relevant news items that may affect your Internet management policies. The default news settings lets you receive news items in the product and displays the last 25 news items received.

You will know you have a new news item to read when the displayed yellow icon appears in the right-hand corner of the interface. Click on the icon to view the new news item. Once you have read the news item, the icon will disappear.

You also have the option of getting an email notification when there is new product news.

1. To change your news settings, go to **Administration – Product News** and click on the **Setup** link.



Administration - Product News - Setup

Enable or Disable News

Receive News: ● Enable ○ Disable

Next Scheduled Download: Thu Mar 25,2010 09:33:22 A.M.

In-Product Notification

Display: All news

Display Last: 25 news items

Email Notfication

Email: All news

Recipient: admin@company.com

2. If you do not want to receive news through the product, you can choose to disable it by clicking on the **Disable** radio button.
   NOTE*: If you decide to disable product news, you must remember that only the administrator will receive these critical updates via email. Critical news items will also be posted on the technical support forum.*

3. The Next News Download is the date and time that the product will automatically check for new news. If you want to check for news immediately, click the **Check News** button.

4. Select whether you want notifications for **All news** or only **Critical news**.

5. You can also choose how many news items you want displayed when viewing your news. Use the pull-down arrow to make your selection.

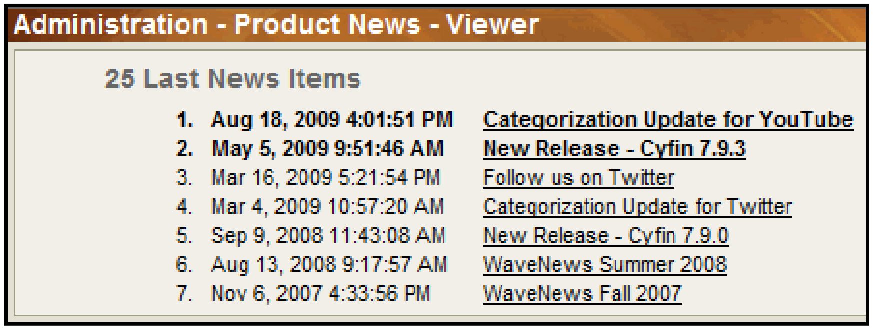
6. Select whether you want to receive email notifications for any new product news. You can select to receive notifications for **All news**, **Critical news** or **Do not email news**.

7. The **Email Address** is the administrator's email configured at the **Setup - Email** screen.

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

To view your news:

1. Go to **Administration – Product News** and click on the **Viewer** link.



Administration - Product News - Viewer

25 Last News Items

1.	**Aug 18, 2009 4:01:51 PM**	**Categorization Update for YouTube**
2.	**May 5, 2009 9:51:46 AM**	**New Release - Cyfin 7.9.3**
3.	Mar 16, 2009 5:21:54 PM	Follow us on Twitter
4.	Mar 4, 2009 10:57:20 AM	Categorization Update for Twitter
5.	Sep 9, 2008 11:43:08 AM	New Release - Cyfin 7.9.0
6.	Aug 13, 2008 9:17:57 AM	WaveNews Summer 2008
7.	Nov 6, 2007 4:33:56 PM	WaveNews Fall 2007

2. Click on the links to read each news item.

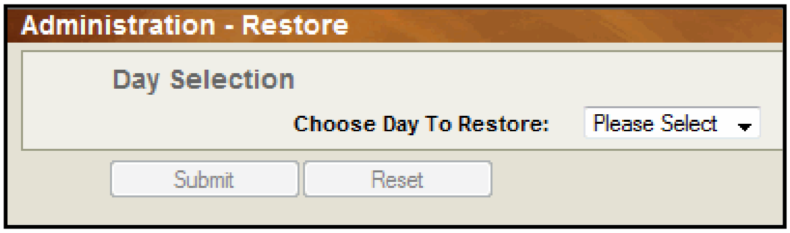
7.7 Restore

The restore option allows you to go back (or restore) your previous settings in your product from a previous day. You can restore settings up to 31 days back.

***NOTE:** This feature is not available if you are using the Array feature.*

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

1. Go to **Administration - Restore**.



Administration - Restore

Day Selection

Choose Day To Restore: Please Select

2. Select a day from which to restore settings.
3. Click **Submit**. At this point the service will automatically restart.

8.0 Other Features

8.1 Quick Start

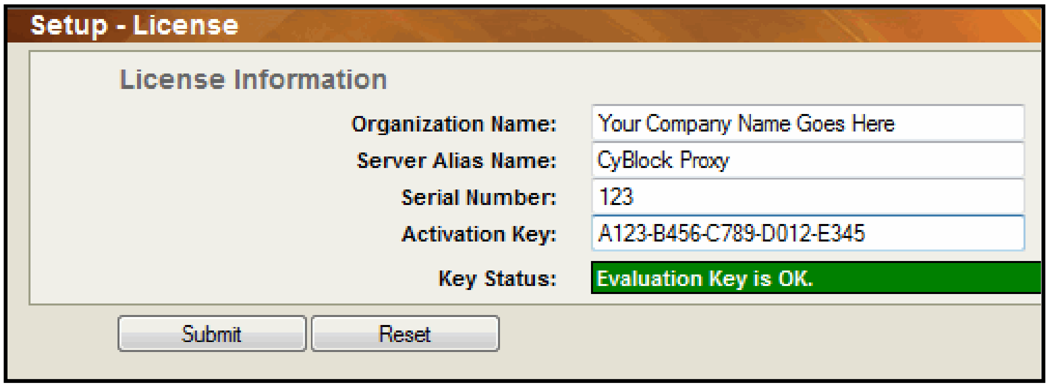
Quick Start provides you with links to the most basic setup screens that you need to get the product up and running. Below the basic setup is a link to this Administrative Guide for the product that will step you through getting the product started. It also contains detailed instructions on some of the product's features.

8.2 License

You will need to enter your product license after you purchase or renew the product license.

***NOTE**: The default evaluation key is valid for 30 days after install.*

1. To enter your license information, go to **Setup** and click on the **License** link.



Setup - License

License Information

Organization Name:	Your Company Name Goes Here
Server Alias Name:	CyBlock Proxy
Serial Number:	123
Activation Key:	A123-B456-C789-D012-E345
Key Status:	Evaluation Key is OK.

2. Enter your organization's name in the **Organization Name** text entry box.

3. Enter the server name (or its 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. Enter your serial number in the **Serial Number** text entry box 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. Enter your activation key in the **Activation Key** text entry box. (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 changes, or click **Reset** to reload previous values.
   ***CAUTION**: If you click **Reset**, the current changes will not be saved, the previous setup will be reset, and all changes will be lost.*

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

8.3 Job Queue

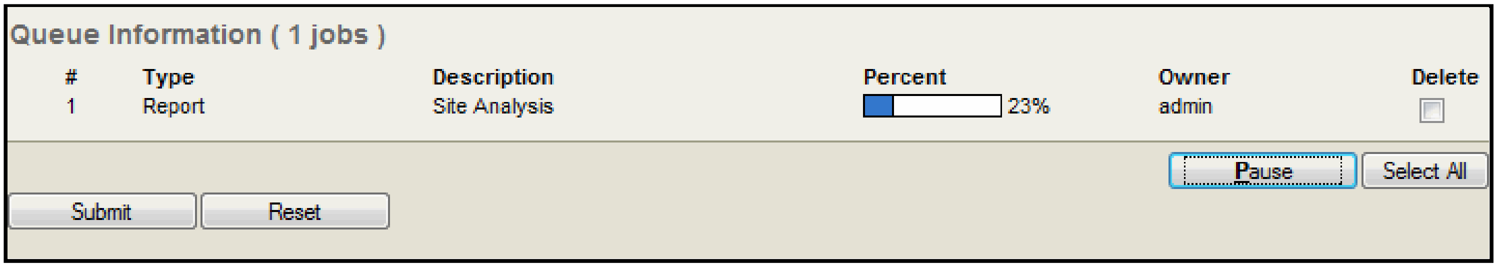
The job queue displays a prioritized list of jobs in process. If there are no open jobs, when you go to the job queue, the screen will be blank and a message indicating the system is currently idle will appear.

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 **Administration – Job Queue**.
2. You will see the list of jobs and their status on the screen.



Queue Information (1 jobs)

#	Type	Description	Percent	Owner	Delete
1	Report	Site Analysis	23%	admin	□

3. If you want to delete any of the jobs, check the **Delete** box and then, click **Submit**.
   NOTE*: Administrators can delete any job in the job queue. Operators can delete only the types of jobs that are authorized in their accounts, i.e., typically reports.*

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

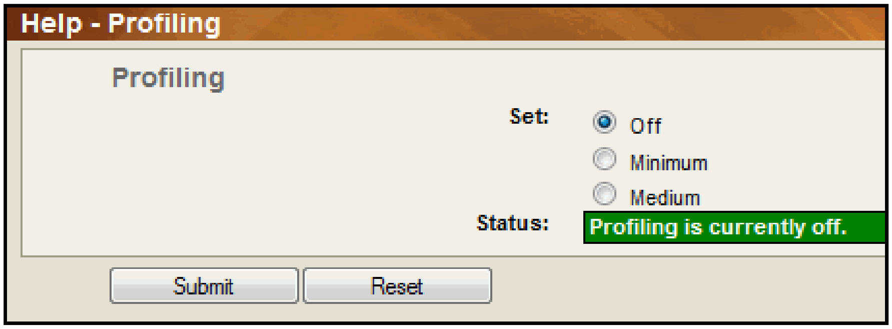
8.4 Help

8.4.1 Documentation

This area provides links to various documents that help you with the product and Web-use management in general. It includes links to this Administrative Manual, product support, Wavecrest's Web site and other helpful documents. Get to this screen by going to **Help - Documentation** on the menu.

8.4.2 Profiling

If you ever experience difficulties that can't be resolved via on-line Help, Technical Support may ask you to activate the product's "profiling" mode via the Profiling screen. When profiling is activated, the product will generate a considerable amount of data to help Technical Support resolve the issue. When the data is generated, it will be sent to a special file (sprofile.htm) for subsequent transmission to Technical Support via email (support@wavecrest.net). If you are ever asked to turn on profiling, go to **Help – Profiling** and follow Tech Support's instructions.



Set: ● Off ○ Minimum ○ Medium

Status: Profiling is currently off.

8.4.3 Support Forum

On our technical support forum, you can connect with some of our 3,500 customers. You can peruse the forum for helpful tips in using the product, or you can post your own questions and comments. If you go to **Help – Support Forum** on the menu, it will take you directly to the forum.

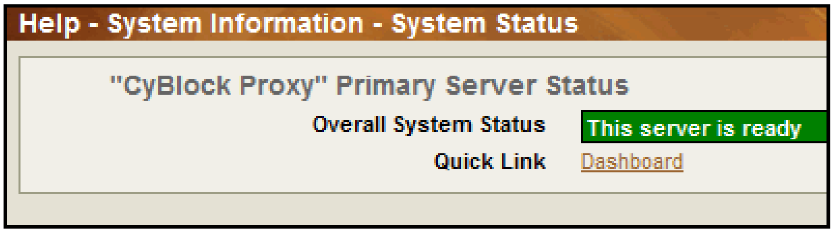
8.4.4 System Information

8.4.4.1 System Status

System Status tells you whether or not the product's Application Server is ready. If the Overall System Status message is colored green (OK), you can click on the dynamic Quick Link which will take you directly to the **Reports - Manual - Site Analysis** screen. There you can quickly generate a sample Site Analysis Report.

If the Overall System 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 System Status, go to **Help – System Information** and click on the **System Status** link.


Help - System Information - System Status
"CyBlock Proxy" Primary Server Status

Overall System Status: This server is ready

Quick Link: Dashboard

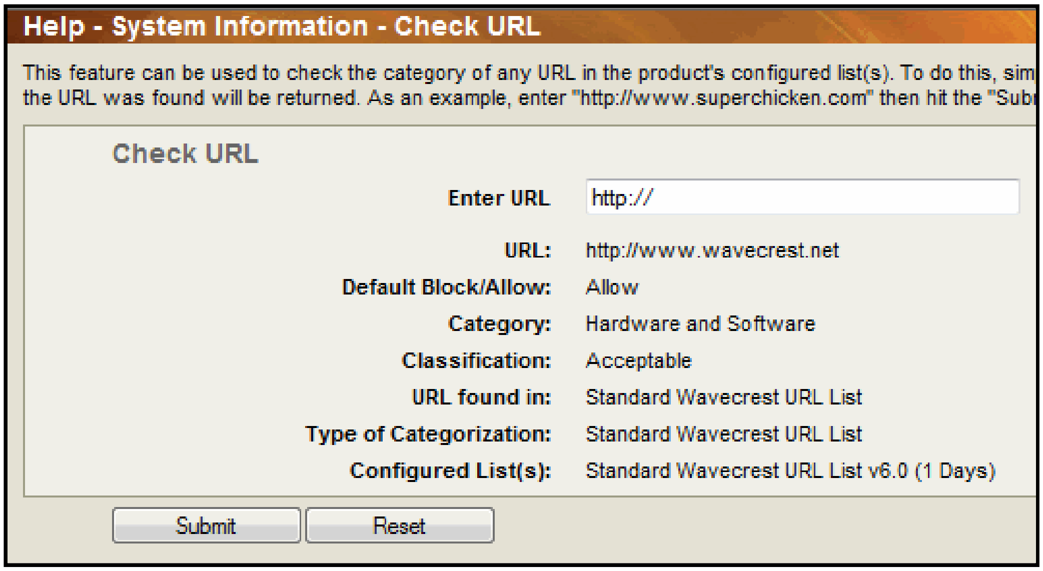
8.4.4.2 Server Information

Server Information 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, report language, etc. 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 **Help – System Information** and click on the **Server Information** link.

8.4.4.3 Check URL

This feature can be used to check the category of any URL in the product's configured list(s). It is particularly useful after you create a custom category. It enables you to verify that the URLs you entered in the custom category have been correctly assigned to that category.

1. Go to **Help – System Information** and click on the **Check URL** link.
2. Enter the URL you want to check.
3. Click **Submit** and the other fields will fill in with information about the URL.



Help - System Information - Check URL

This feature can be used to check the category of any URL in the product's configured list(s). To do this, sim
the URL was found will be returned. As an example, enter "http://www.superchicken.com" then hit the "Subr

Check URL

Enter URL: http://

URL: http://www.wavecrest.net

Default Block/Allow: Allow

Category: Hardware and Software

Classification: Acceptable

URL found in: Standard Wavecrest URL List

Type of Categorization: Standard Wavecrest URL List

Configured List(s): Standard Wavecrest URL List v6.0 (1 Days)

8.4.4.4 Sample Reports

Sample Reports lets you quickly generate a sample Site Analysis report and a sample User Audit Detail report. These reports can help you become familiar with the "look and feel" of all of the product's reports. To view these sample reports, go to **Help – System Information** and click on the **Sample Reports** link. Then, click on the link for the report you want to see.

8.4.5 About

If you go to **Help – About** on the menu, you will get a description of the product, the version you are currently using, and the release date of the version you are using. It also includes a link to Wavecrest's Web site.

© Copyright 1996-2010 Wavecrest Computing. All rights reserved.

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 semi-automatically. 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 simply 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, work location, etc. 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. 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, User ID, etc.) 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's Active Directory (AD) is a popular example.

How Wavecrest Products Interact with Active Directory

General. Wavecrest products' 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 section.
* create a hierarchical Groups & 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), immediate parent organization, etc. 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, "Sales" in England, etc.), 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, access control, etc. 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 multi-tier 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 don't 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's used in IT to control network access. MS Active Directory is a good example. In such cases, the directory's UserIDs will exactly match those that Wavecrest products find in the network logfiles. However, it's 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 does. 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 doesn't, the customer 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 whether or not 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 Groups and IDs "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 Groups and IDs "inside the product," only new IDs will be imported.*

Using the Product's Active Directory Setup Wizard. In order to import Active Directory users and groups, 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 Groups and IDs "outside the product." However, if you chose to manage them "inside the product," only new users will be imported. For step-by-step instructions of the wizard, see Section 2.2.1 on Importing Groups and IDs 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 Groups and IDs "outside the product," all Groups and IDs will be updated according to the directory source. However, if you chose to manage Groups and IDs "inside the product," only new IDs will be imported.

Semi-automated 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, table, etc.).
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/cb/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 simply be left empty (no character spaces please). 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, Accounting, etc.
* **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 **Advanced Settings - Groups and IDs - Import - Text File** screen. The process consists of a few simple data entries. See Section 2.2.2 for detailed instructions on importing your 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, space, etc.

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
wilsonp|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 delimit-characters with nothing in between. This tells the product that there is no full name.

```
smithj||Engineering
doej||Accounting
wilsonp||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 sub-classes an IP Address range for a region or district. In this case, Full Names are not used. Notice the two delimit-characters; 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 screens found in the Advanced Settings/Groups and IDs Edit Links menu, which contains the options Add, Move, and Delete. Typically, although not necessarily, the groups in a hierarchical structure consist of the various departments and sub-departments within a company.

Configure and Populate the Groups. Once the design is complete, the administrator can configure it into the product and assign users to the various groups, e.g., departments. He or she can perform both of these tasks in the Advanced Settings/Groups and IDs screens by following the simple 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.

Cautionary Note. To run a detailed User Audit report on a specific ID or IP address, the covered user's ID must already be present within the product.

Methodology. Using the Reports/Manual menu, 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 out. ***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 such exist.*

Appendix B: Report Descriptions

High-level Summary Reports

1. Acceptable Visit Report

Features. This report depicts Web-use activity only within categories classified or rated as "Acceptable." By category, it shows total number of visits made by individual users. Users are identified but individual sites are not.

Benefits. Management can quickly determine the amount of Acceptable activity. This can be done by individual category or on a summary basis for all Acceptable categories.

2. All User Summary Report

Features. This is a tabularized report that depicts each user's activity from a high-level "acceptability" perspective. For each user, this report shows the total number of visits that have been classified as "acceptable", "unacceptable", and "neutral." Extraneous hits (banners,ads, etc.) are not counted. All users are listed, not just the top 25. Individual sites visited are not shown.

Benefits. This reports presents management with a "quick-look" view of the number of acceptable and unacceptable visits made by each individual user.

3. Legal Liability Report

Features. This report contains only Legal Liability Web activity. Only visits to the Cults, Drugs, Gambling, Hate and Crime, Pornography, and Public Proxy categories are presented. Information is presented by category and by individual user. Individual sites are not separately identified.

Benefits. As indicated above, only "Legal Liability" Web-use is presented. This means that smaller, more focused reports are available to facilitate analyses, investigations and audits related to legal liability issues.

4. Neutral Visit Report

Features. This report provides Web-use only for categories classified as "Neutral."

Benefits. Management can quickly determine the level and type of "Neutral" activity.

5. Site Analysis Report

Features. This report depicts the same Web site visits three different ways:

- Total visits by classification (acceptable, unacceptable)
- Total visits by category (shopping, pornography, etc.)
- 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 three different perspectives, i.e., "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.

6. Top Users Report

Features. This report lists the top users by visits, hits, and bytes read. If Abuse Thresholding is enabled, it will also show the user names that go over the threshold settings.

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.

7. Unacceptable Visit Report

Features. This report depicts Unacceptable activity only. It does this in several ways. The report first provides an uncategorized total of visits to Unacceptable sites. It also provides a section, subdivided by category, that lists each individual visitor and the number of visits that each made within each category. The report depicts Web activity consisting of visits to sites in categories classified as "Unacceptable."

Benefits. This type of report supports "Management by Exception" techniques. That is, the report itself analyzes the activity and presents management with only the "unacceptable" visits.

Detail Audit Reports

8. Category Audit Detail Report

Features. This report is similar to the "User Audit Detail" report. However, it focuses on a single category instead of a single user. That is, it provides a detailed analysis of all covered users' Web activity in a particular category that you select, e.g., pornography. All URLs, including sub-pages as well as home pages (sites), are sorted by user.

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.

9. Category Audit Summary Report

Features. This report is similar to the "User Audit Summary" report. However, instead of analyzing a particular user's activity, it provides a synopsized audit on a particular category. Web sites are NOT sorted by user in this report. Only URLs are displayed.

Benefits. This report is very useful for quick-look determination of whether or not Web-access abuse is taking place in a particular category, e.g., pornography. If the information tells you that a true problem exists, you can drill down deeper and pinpoint the source via a Category Audit Detail Report or a User Audit Detail Report.

10. Site Audit Detail Report

Features. This report focuses on specified Web site(s) by either hits or visits. Every hit or visit made to the specified URL(s) are listed separately by user. Hits or visits are listed chronologically by date and time. Information included for each hit or visit consists of the user, category and full URL.

Benefits. Management has a complete yet concise view of all users that visited the specified Web site(s). This information can be used for personnel appraisal purposes, usage audits, etc.

11. User Audit Detail Report

Features. This report focuses on a single user. Every visit made by the user is listed separately in the main body of the report. Visits are listed chronologically by date and time. Information included for each visit consists of the site's category and full URL. A summary total of visits by category is also provided.

Benefits. Management has a concise but complete view of every URL the user has clicked. This information can be used for personnel appraisal purposes, usage audits, etc.

12. User Audit Summary Report

Features. This report lists all the Web sites visited by a single user during the reporting period. The report indicates each listed site's category and the 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 evaluating an individual user's Web activity.

Additional Management Reports

13. Custom Categories Report

Features. This report depicts Web-use in Custom Categories only (if configured). That is, it shows which users visited which custom categories. It does not identify individual sites.

Benefits. This report provides very reliable Web-use information focused strictly on subjects of specific interest to the enterprise, specified by the enterprise itself. For example, management can use this information to determine if users are properly using particular Intranet sites, HR sites, supplier sites, customer sites, etc.

14. Denied Visits 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 sites are not. Each attempt is displayed in the category attempted. "Denied" attempts 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 blocking at the proxy is used, this report can verify that it's working. It also indicates the number and type of blocked attempts. This report is a very useful supplementary tool for individual user audits.

15. Network Information Report

Features. This report depicts total visits per category, hourly total visits and total kilobytes read. No individual IDs or sites are identified in this report. It also shows download times (see definition in appendix to report).

Benefits. This report is a powerful tool for Network Administrators. It serves as a valuable aid for managing bandwidth utilization.

16. Site Analysis Bandwidth Report

Features. Similar in structure to "Site Analysis" report, this report focuses on bandwidth consumption instead of visits. It breaks down bandwidth usage first by acceptability classification, then by category within each classification, and then by user within each category.

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 depiction is very helpful for managing bandwidth usage and advising management on corrective action measures.

17. Top Bandwidth Sites Report

Features. This report shows, by kilobytes, category and actual URL, the top bandwidth-consuming site visits made during the reporting period by the selected group. Each site's category is shown alongside the kilobyte consumption for the site.   The list is sorted in descending numerical order by the highest bandwidth consumption; this enables quick determination of site effect on bandwidth. Individual user ID's are not shown on this report. Hyperlinks to all visited Web sites are provided to facilitate further analysis.

Benefits. This report gives you a quick view of the top Web sites consuming the most bandwidth in your network during the reporting period.

18. Top Web Sites Report

Features. This report shows, by Web site, the number of visits made during the reporting period by the selected group. Each site's category is shown alongside the number of visits made. The list is sorted in descending numerical order by the number of visits; this enables quick determination of site "popularity." Individual user ID's are not shown on this report. Hyperlinks to all visited Web sites are provided to facilitate further analysis.

Benefits. This report "highlights" the Web sites that were visited most by the audited group during the reporting period.

19. Top Non-Categorized Sites Report

Features. This report shows all unidentified hit activity, i.e., all URLs that were routed to the "Other" category. This is the only report that includes ALL activity, not just bona fide visits. Therefore, the report reflects all "extraneous" images, banners, ads, multimedia items, etc., as well as bona fide visits. For each URL listed, the report shows the number of hits and the full domain name. Individual user ID's are not shown. The list is sorted in descending numerical order by number of hits. Hyperlinks to all web sites are also provided.

Benefits. This report can be used by administrators to help identify any intranet sites that perhaps should be added to a "Company Intranet" custom category. A further benefit can be derived from this report by sending it to Sites@wavecrest.net for research by the Wavecrest staff. Upon receipt, the staff will identify, research and categorize the "Other" URL's and incorporate them into the Wavecrest® URL List. Inclusion of these URL's in the Wavecrest® URL List will greatly improve future reports.

Appendix C: Glossary of Terms

Abuse. A level of Web use in a designated content category that is unacceptable to the customer's organization. Automatic abuse-detection is an optional feature within this product's reporting system. It is based on customer-specified criteria, i.e., a specified number of visits in a 24-hour period. If abuse-detection is chosen, the customer decides which categories to monitor and the levels (thresholds) at which usage becomes abusive. (See also **Abuse Thresholds**)

Abuse Thresholds. The levels at which Web usage becomes abusive within designated categories. Abuse Thresholds are set by the customer's organization on the basis of its Web access policy or guidelines. The numeric threshold refers to a specified number of visits allowable within a 24-hour day. Refer to Visit and Hit definitions to get a better understanding.

Acceptable Use Policy (AUP). A customer's set of guidelines and restrictions governing employees' access to the Internet and/or organizational intranets and extranets.

Access Accounts. Accounts that grant access to the product for functional or administrative purposes. Two types of accounts are available: Administrator and Operator. Administrators have full access to all functional and administrative features. Operators can only create and retrieve reports.

Attributes. Configurable "settings" and/or "features" within the product that perform specific Web policy support and report preference functions. (See also **Web Policy Support** and **Report Preferences**)

Category. A set of URLs with similar content. Examples include shopping, sports, pornography, entertainment, financial, etc.

Classification. An "appropriateness" rating assigned to a category, i.e., Acceptable, Unacceptable or Neutral. Customers specify the classifications.

Denied. A term that 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," etc.

Domain. A "name" that is part of a URL (Web page address). More readable and memorable than a numerical address. An example is www.amazon.com.

Download Time. Approximate or average time for a Web page to load in the browser, i.e., the time span between when a user clicks on a hyperlink and the page loads in the browser. As used in this product's reports, Download Time is derived by multiplying (a) the smallest average amount of time required to download a typical Web page by (b) the number of visits. Please note that it is not possible to calculate the amount of time a user was on-line or viewing a particular page. Our Download Time approach is intended to indicate the minimum amount of time the user was on the Web. This should not be the primary data point on which to establish abuse. We suggest you use the visit count (total visits); this is a more accurate indicator of abuse. (See definition of Visit for more detail.)

> ***NOTE****: The default used in the product for Download Time is set to 3 seconds. This can be changed if desired. Please contact Wavecrest Support for details.*

Enterprise. A term that denotes the total set of users covered by this product. If the total set is organized by the customer into a hierarchy of groups for more segmented or differentiated coverage, the term "enterprise" refers to the top level of the hierarchy.

Group. A collection of users who share a common characteristic. In one example, the users in a group all belong to a particular department of an organization or company. The department name or number is the common characteristic. Groups can be based on a number of different characteristics, such as: organizational assignment, work location, job classification, mission or project assignment, etc. A "group" can consist of many users, or it can consist of only one user. In this product, groups are assigned names for identification purposes; if the group is a single user, his or her ID is the group name.

> ***NOTE**: Any group created in the product must contain at least one user. If it does not, the group will not appear the next time the product is opened.*

Hit. A typical Web page is made up of many different elements (i.e., text, images, banner ads, audio, flash, etc.). When you click on a URL and a Web page is being loaded in your browser, each of those elements is downloaded separately. As a result, clicking on a single URL can generate multiple logfile entries, one for each element downloaded. Each of these “downloads” represents a “hit.” On average, 70% of all hits are elements downloaded as a result of a user clicking on a hyperlink. Put another way, a hit count represents all elements downloaded during a user’s session, but this has no direct correlation to the number of Web pages the user actually requested or visited. To present the most accurate representation of the level of human Web-use activity, this product distinguishes extraneous hits from actual clicks, i.e., visits. (Please refer to the definition of Visit for more information on this subject)

ID. A login name or IP address that this product uses to identify users.

Import Data. As used in current versions of this product and its documentation, the term Import Data refers to the product's optional-use "internal database" which, when enabled, can automatically retrieve and store logfile information in a more compressed and organized format. The chief advantage of this approach is greatly reduced report-generation time, compared to report-generation processes that read logfiles directly.

LDAP. Lightweight Directory Access Protocol (LDAP). An interoperability standard for deploying directory-based applications and solutions. As used in this product and its documentation, the term LDAP generally refers to the product's ability to import user ID information automatically and manually from an LDAP-based directory, e.g., Microsoft's Active Directory (AD).

List. Wavecrest URL List. Also sometimes referred to as a “control list,” the Wavecrest URL list is an updatable categorized database of Web site URLs that is built into Wavecrest products. The product compares the URLs of visit attempts with the URLs in the list in order to categorize actual or attempted visits to Web sites. (See definition of Category)

Operator. A product user that has been granted a limited-access Operator account. Operators can create and retrieve Web-use reports but they cannot make administrative setup or configuration changes. Setup and configuration functions are limited to individuals that have been granted Administrator accounts.

Policy Settings. Modifiable settings that govern how this product is applied to users or groups of users and how it displays information in reports. Examples of these settings include: Category Classification, Abuse Thresholds, Display Categories, and Maximum IDs. Another example of a Policy Setting is the Block Categories setting in our filtering products. See also Report Preferences.

Report Preferences. Several customizable attributes within the product that help to streamline reports and dictate where they are sent or saved. Examples of these attributes include: Language, Full Name, Email Address, and Save Directory.

Ungrouped IDs. A hard-coded subfolder within the product's Groups and IDs feature. The subfolder is called the "Ungrouped IDs" group. It can be used to store user ID information. If the customer doesn't set up a customized user-grouping structure, all users can be placed in the Ungrouped IDs group and simply left there—in which case it serves as the main ID storage area. On the other hand, if the customer sets up his own user-grouping structure, Ungrouped IDs can be used as a holding area for user IDs until they can be moved into the proper groups.

The Ungrouped IDs group can be populated with IDs in several ways:

- By Running Reports. When high-level reports such as Site Analysis are run, IDs that are found in the logfiles for the requested time-frame are automatically assigned to Ungrouped IDs.
- Via Automatic Imports. Ungrouped IDs can be populated during automated ID import processes if the customer has not set up a grouping scheme. (If a grouping scheme has been created, the IDs are imported into their assigned specific groups.)
- Manually. The Ungrouped IDs group can be populated manually.

***NOTE**: Low-level reports such as User Audit Detail, which cover a single user, cannot be created unless the user’s ID has been assigned to a group. Consequently, if the ID is not in a customer-created group, it must be in the Ungrouped IDs group.*

URL. Universal Resource Locator. The full address of a Web page. Includes protocol designator (e.g., http), domain name (e.g., www.amazon.com), and directory or file name (e.g., /index.html).

User. A computer user whose access to Internet and intranet Web sites is monitored by this product. For reporting and/or filtering purposes, the user's ID must be available to the product via logfiles or other means, e.g., importation from an LDAP-based directory or a manual entry process.

VIP Group. A built-in group that is used by administrators to exclude certain individuals (VIPs) from reports. When an ID is assigned to this group, his or her Web-use activity will not appear in reports.

Visit. The act of clicking on a URL or hyperlink to request that a Web page or other object be downloaded. The typical Web page contains many different elements that are downloaded separately. (Refer to Hit for complete understanding.) To gauge the level of Web-use activity, this product emphasizes Visit counts. Unlike Hits, “Visits” counts how many Web pages a user actually requested, not all the elements downloaded as a result of those requests. Put another way, a hit count represents all elements downloaded during a user’s session, but this has no direct correlation to the number of Web pages the user actually visited or attempted to visit. In sum, to present the most accurate representation of the level of Web-use activity, this product distinguishes between extraneous hits and actual clicks. Furthermore, this product has an optional visit filter that is enabled by default.

Visit Filter. Feature which further differentiates between actual visits and hits, making for a more accurate depiction of visits. The visit filter is enabled by default, but it can be disabled upon request.

Web Policy. A term that is synonymous with AUP (Acceptable Use Policy). See also Web Policy Support.

Web Policy Support. Web policy support refers to how this product helps enforce an organization's AUP (Acceptable Use Policy). Some of the attributes that help to accomplish this include: Category Classification, Edit URLs, Name Custom and Abuse Thresholds.

***NOTE**: An additional example in our filtering products is the Block Categories setting.*

XML. *Extensible Markup Language*. A widely used interoperability standard. As used in earlier versions of this product and its documentation, the term XML generally refers to the product's optional-use "Data Manager " which, when enabled, can automatically retrieve and store logfile information in XML format. The chief advantage of this approach is greatly reduced report-generation time, compared to report-generation processes that read logfiles directly.

Cyfin® Reporter
Build Date: 02 April 2010

Wavecrest Computing
2006 Vernon Place
Melbourne, FL 32901
Toll-free: 877-442-9346
Voice: 321-953-5351
Fax: 321-953-5350

www.wavecrest.net