Burst Technology

presents

bt-LogAnalyzer

SQL Edition

User Guide

Burstek™

9240 Bonita Beach Road

Bonita Springs, FL 34135

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

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

bt-LogAnalyzer SE™ Installation and User Guide

This guide is the property of Burstek, and embodies proprietary, trade secret, and confidential information. The bt-LogAnalyzer computer program, this guide, and all other Burstek manuals are protected by trade secret and copyright laws.

The bt-LogAnalyzer computer program, this guide, and all other Burstek manuals may not be copied, reproduced, transmitted, transcribed, stored in a retrieval system, or reduced to any electronic medium or machine-readable form without the express written approval of Burstek Unauthorized copying of the program or this guide is a violation of copyright or trade secret law.

Burstek reserves the right to make changes or improvements to the software and documentation described herein at any time and without notice.

Burstek

9240 Bonita Beach Road

Bonita Springs, FL 34135

Phone: 239.495.5900 or toll free 800.709.2551
Fax: 239.495.5311

Email: support@burstek.com

Table of Contents

Welcome

Welcome to bt-LogAnalyzer, an easy-to-use application that helps you evaluate employee Web and Email use in your organization.

- **Web Reporting** - bt-LogAnalyzer provides automatic categorization (i.e. Education, Sex, Sports, Hacking, Gambling, Games, Business Services, etc.) of Websites accessed and makes it easy to identify possible issues with regard to Internet access, company risk or bandwidth consumption by generating detailed reports, summaries and graphs.
- **Email Reporting** - bt-LogAnalyzer reports on inbound, outbound and internal Email by Email addresses, volume, bandwidth and subject.

What's New in bt-LogAnalyzer SE

With bt-LogAnalyzer SE, you will benefit from reduced report generation time while enjoying all the features you have come to know and love. To cut down the time you need to create a report, we introduced the following features into our application:

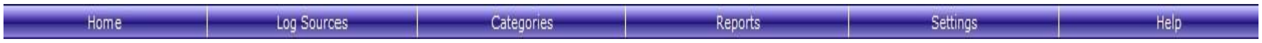
- **Log data loading**. This will prevent you from reading the same logs every time you build a report. Prior to report generation, all log data will be loaded from Log Info Sources into the bt-LogAnalyzer storage. When generating a report, bt-LogAnalyzer will contact the storage for the data, not individual logs. The storage is a Microsoft ® SQL Server database.
- **Categorization of the loaded log data**. This will help you avoid categorizing the same logs again and again when generating different reports. After loading into the storage, all the log data will be pre-categorized using the existing URL Control List. Once this is done, the reports will be generated based on the categorized log information, which will reduce the generation time dramatically.

Introduction

Navigating the Web Interface for LogAnalyzer 7

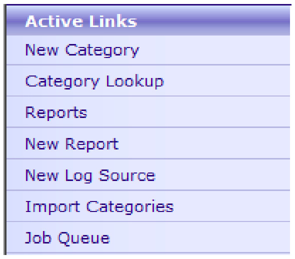
bt-LogAnalyzer's Web Interface is designed for quick access to tasks that an administrator typically performs.

Menu Bar



The Menu Bar at the top of the LogAnalyzer homepage is the primary navigation tool. Clicking on each heading will provide you with a webpage specific to that heading name. Hovering your mouse cursor over the individual Menu Bar options will display a drop down menu with basic Quick Navigation features regarding the selected Menu Item.

Active Links



Active Links Quick Nav

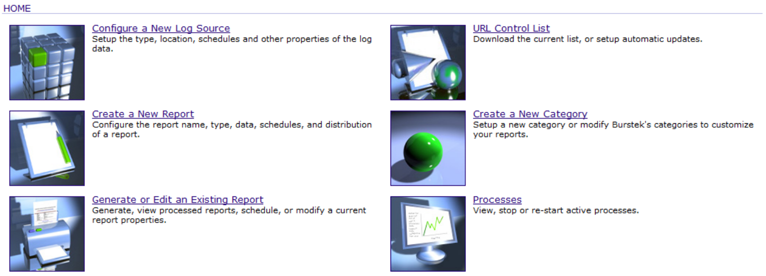
On the left side of the page are the Active Links that provide additional instant access to specific functions within the LogAnalyzer Application.

For example, clicking on the "Job Queue" link at the bottom of the list will take you directly to the Job Queue interface so that you can see any currently running tasks. The Active Links object is available on each page within LogAnalyzer providing you with the ability to quickly navigate between options.

NOTE:
The "Import Categories" link will be unavailable if you are not logged in to the console.

Home Tab

This is normally the first page you will see when accessing the LogAnalyzer interface. The links in the center of the page are quick links to common tasks within LogAnalyzer.



HOME

Configure a New Log Source
Setup the type, location, schedules and other properties of the log data.

URL Control List
Download the current list, or setup automatic updates.

Create a New Report
Configure the report name, type, data, schedules, and distribution of a report.

Create a New Category
Setup a new category or modify Burstek's categories to customize your reports.

Generate or Edit an Existing Report
Generate, view processed reports, schedule, or modify a current report properties.

Processes
View, stop or re-start active processes.

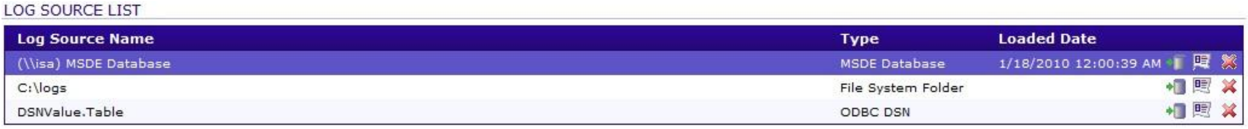
LogAnalyzer Interface Home Page

From this page you can navigate quickly to sections specific to your need such as those listed below. Each of these processes will be explained in detail later in this guide as well.

- Configure a New Log Source
- Create a New Report
- Generate or Edit an Existing Report
- Update the URL Control List or setup Automatic Updates
- Create a New Category, or modify Burstek's existing categories to suite your needs
- View, stop or re-start active process

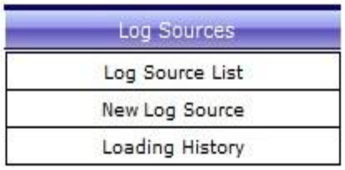
Log Sources Tab

The Log Source tab contains all the necessary links to configure how data will be imported into LogAnalyzer. You can quickly review all of your data sources and identify the last time they were loaded as well as make changes to their configuration, including deleting outdated sources.



LOG SOURCE LIST

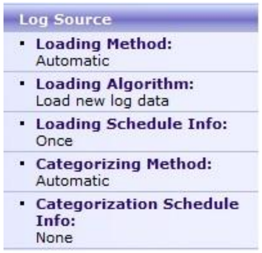
Log Source Name	Type	Loaded Date
(\\isa) MSDE Database	MSDE Database	1/18/2010 12:00:39 AM
C:\logs	File System Folder	
DSNValue.Table	ODBC DSN	



Log Source Quick Nav

The Log Sources tab has a hover menu as well as an additional navigation list on the left of the display. The Log Source hover menu provides quick access to the common areas related to log data such as your loading history. The "Log Source List" navigation links provide additional functionality specific to modifying individual Log Sources.

The 'Log Source' display list on the lower left of the page will provide you with a snapshot into each of your log sources such as their method of loading and their schedule.

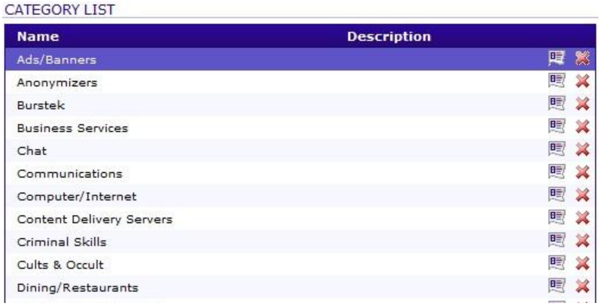


Log Source

- **Loading Method:** Automatic
- **Loading Algorithm:** Load new log data
- **Loading Schedule Info:** Once
- **Categorizing Method:** Automatic
- **Categorization Schedule Info:** None

Log Source Summary

Categories Tab



CATEGORY LIST

Name	Description
Ads/Banners	
Anonymizers	
Burstek	
Business Services	
Chat	
Communications	
Computer/Internet	
Content Delivery Servers	
Criminal Skills	
Cults & Occult	
Dining/Restaurants	

Categories List

The core of the Burstek application is its Categorization technology and by using this section of LogAnalyzer's Web page, you can modify all aspects of those categories including adding or excluding URL's.

The "Categories" interface displays Categories in a list oriented view allowing you to quickly identify and manage the required category.

As with the 'Log Sources' tab, there is a hover menu and a "Category List" navigation section. The Hover menu provides the ability to create, import, lookup existing categorized URL's and view loading history data while the "Category List" navigation provides the additional options of deleting categories, managing settings, and clearing the category load history.

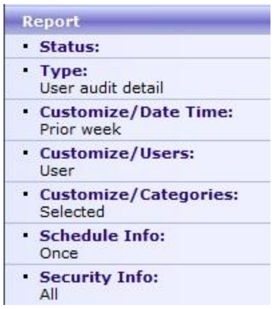
NOTE:
The Import Categories, Loading History and Clear History options will be disabled unless you are logged into the LogAnalyzer Web Interface

Reports Tab

The reports section of LogAnalyzer's interface is where you will create the reports for those requesting the data.

The "Reports" screen has three sections that you should become familiar with.

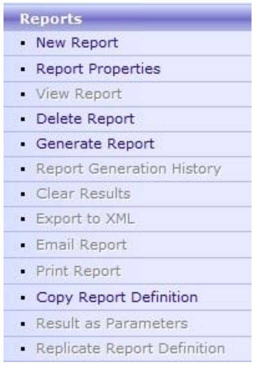
1. The Reports Display Window shows all existing reports for the environment
2. The Reports Navigation links to specific actions related to report management
3. The Report Summary provides a quick view of the selection reports details.



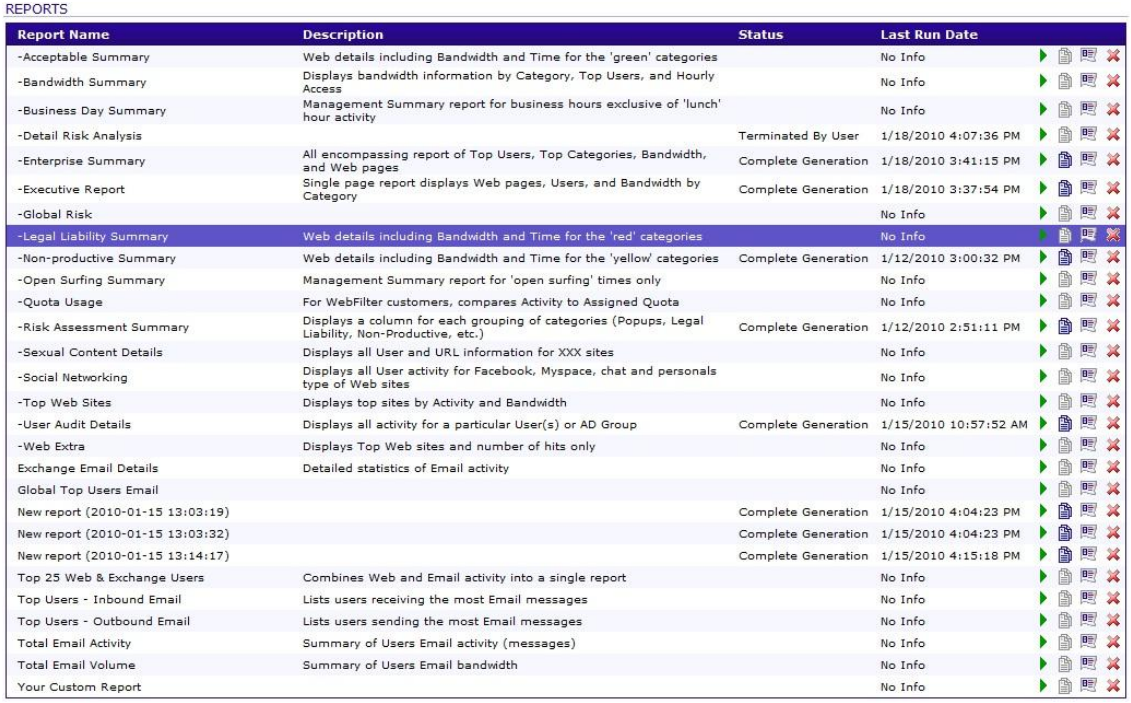
Report

- **Status:**
- **Type:** User audit detail
- **Customize/Date Time:** Prior week
- **Customize/Users:** User
- **Customize/Categories:** Selected
- **Schedule Info:** Once
- **Security Info:** All

Report Summary



Reports Navigation



REPORTS

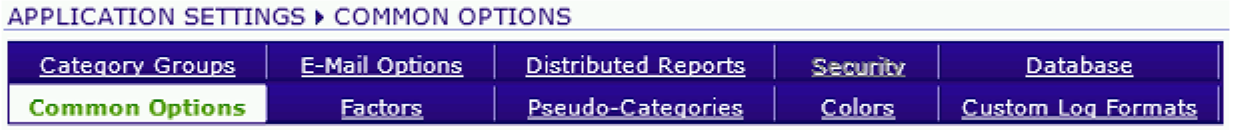
Report Name	Description	Status	Last Run Date
-Acceptable Summary	Web details including Bandwidth and Time for the 'green' categories		No Info
-Bandwidth Summary	Displays bandwidth information by Category, Top Users, and Hourly Access		No Info
-Business Day Summary	Management Summary report for business hours exclusive of 'lunch' hour activity		No Info
-Detail Risk Analysis		Terminated By User	1/18/2010 4:07:36 PM
-Enterprise Summary	All encompassing report of Top Users, Top Categories, Bandwidth, and Web pages	Complete Generation	1/18/2010 3:41:15 PM
-Executive Report	Single page report displays Web pages, Users, and Bandwidth by Category	Complete Generation	1/18/2010 3:37:54 PM
-Global Risk			No Info
-Legal Liability Summary	Web details including Bandwidth and Time for the 'red' categories		No Info
-Non-productive Summary	Web details including Bandwidth and Time for the 'yellow' categories	Complete Generation	1/12/2010 3:00:32 PM
-Open Surfing Summary	Management Summary report for 'open surfing' times only		No Info
-Quota Usage	For WebFilter customers, compares Activity to Assigned Quota		No Info
-Risk Assessment Summary	Displays a column for each grouping of categories (Popups, Legal Liability, Non-Productive, etc.)	Complete Generation	1/12/2010 2:51:11 PM
-Sexual Content Details	Displays all User and URL information for XXX sites		No Info
-Social Networking	Displays all User activity for Facebook, Myspace, chat and personals type of Web sites		No Info
-Top Web Sites	Displays top sites by Activity and Bandwidth		No Info
-User Audit Details	Displays all activity for a particular User(s) or AD Group	Complete Generation	1/15/2010 10:57:52 AM
-Web Extra	Displays Top Web sites and number of hits only		No Info
Exchange Email Details	Detailed statistics of Email activity		No Info
Global Top Users Email			No Info
New report (2010-01-15 13:03:19)		Complete Generation	1/15/2010 4:04:23 PM
New report (2010-01-15 13:03:32)		Complete Generation	1/15/2010 4:04:23 PM
New report (2010-01-15 13:14:17)		Complete Generation	1/15/2010 4:15:18 PM
Top 25 Web & Exchange Users	Combines Web and Email activity into a single report		No Info
Top Users - Inbound Email	Lists users receiving the most Email messages		No Info
Top Users - Outbound Email	Lists users sending the most Email messages		No Info
Total Email Activity	Summary of Users Email activity (messages)		No Info
Total Email Volume	Summary of Users Email bandwidth		No Info
Your Custom Report			No Info

Reports Display Window

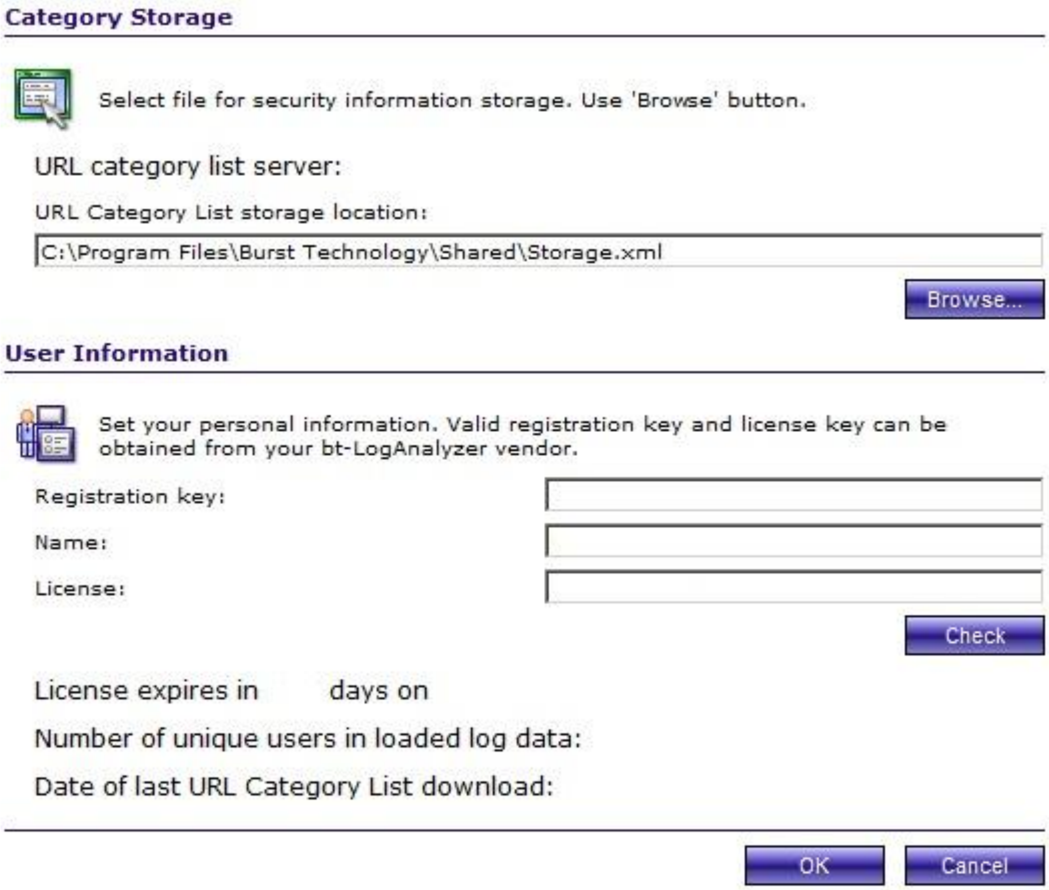
Settings Tab

The “Settings” tab of bt-LogAnalyzer SE contains all the information related to the functionality of the application. This tab also gives you the ability to Import and Export your configuration settings via the settings navigation bar to the left of the page.

A more detailed description of each of the options under the Settings category will be provided in the section “Configuring bt-LogAnalyzer SE”



For example, in “Settings -> Common Options” you can update your category list storage location as well as your registration information including license keys.



Category Storage

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

URL category list server:

URL Category List storage location:

C:\Program Files\Burst Technology\Shared\Storage.xml

User Information

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

Registration key:

Name:

License:

License expires in days on

Number of unique users in loaded log data:

Date of last URL Category List download:

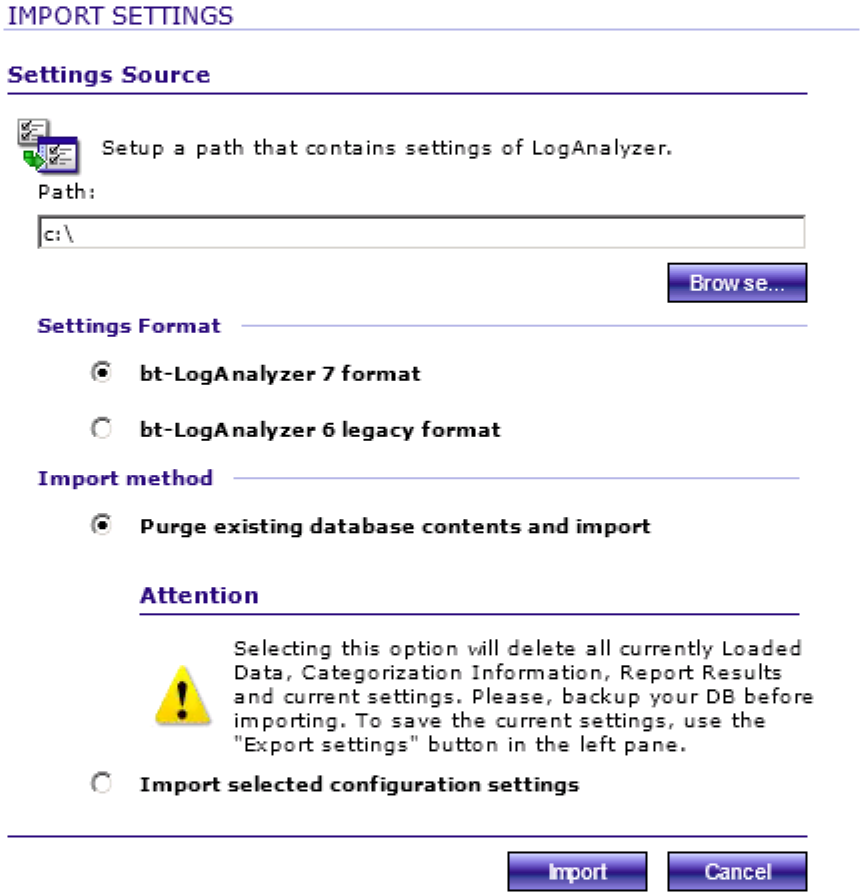
Improved Settings Import

Beginning with bt-LogAnalyzer SE^{TM} v7.1.61, the ‘Settings Import’ function has been redesigned allowing the user to import specific settings instead of an ‘All or Nothing’ approach. In previous versions of LASE, importing settings would cause the existing information loaded in the database to be automatically purged. While this can be desired in some instances, being selectable provides the user with more flexibility.

Figure 1 below, shows the **Import Settings** page. User interface login (upper-right corner) is required select the 'Import Settings' option. In this selection, the user has elected to completely purge the database and import their settings. This option is desirable when the loaded data is no longer required, and the LASE configuration is to be completely overwritten

NOTE:

Please note the 'Attention' dialog with this option selected as it confirms ALL data and settings will be deleted.



IMPORT SETTINGS

Settings Source

Setup a path that contains settings of LogAnalyzer.

Path: c:\

Settings Format

● bt-LogAnalyzer 7 format

○ bt-LogAnalyzer 6 legacy format

Import method

● Purge existing database contents and import

Attention

Selecting this option will delete all currently Loaded Data, Categorization Information, Report Results and current settings. Please, backup your DB before importing. To save the current settings, use the "Export settings" button in the left pane.

○ Import selected configuration settings

Figure 1 - Import Settings Page

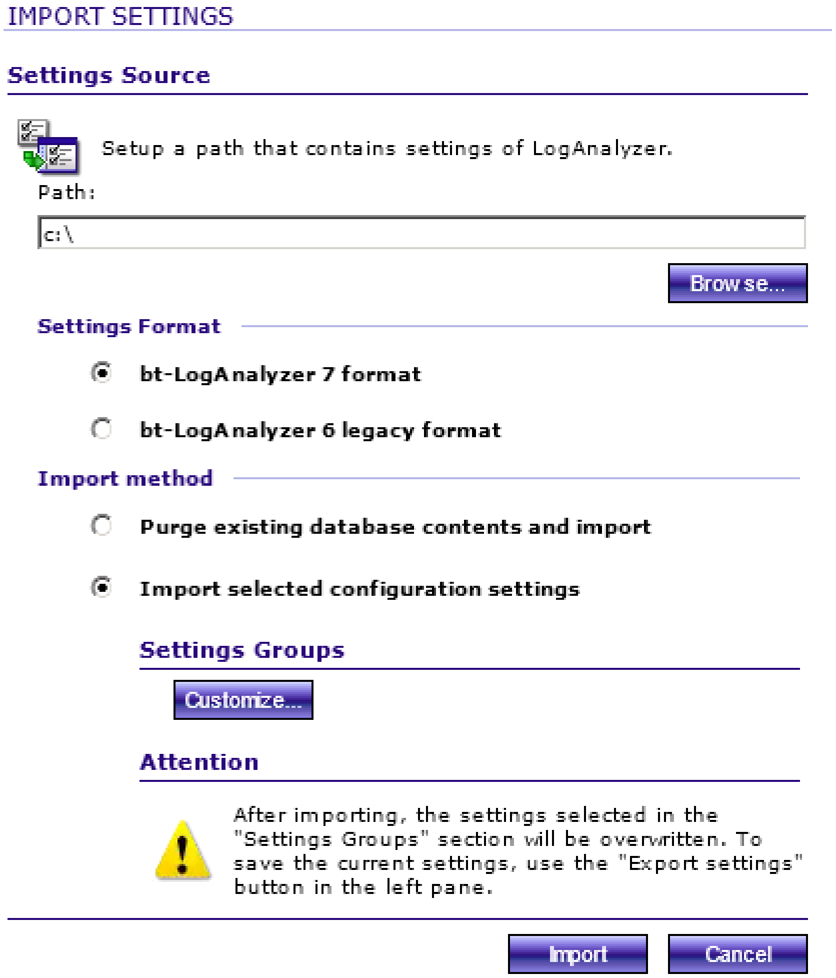
As displayed in figure 2, a 'Customize' button will appear when the 'Import selected configuration settings' option is selected. Clicking the 'Customize' button will present the screen displayed in Figure 3.

NOTE:

If you do not select a valid 'Settings Export' directory under the 'Settings Source' field, you will receive a Parsing Error stating 'AppSettings*.xml file not found'. To resolve this, enter (or browse) to the path of your Exported Settings folder and click 'Customize'.

NOTE:

It is not possible to import selective settings from bt-LogAnalyzer 6. When importing bt-LogAnalyzer 6 settings, all existing information and database contents will be purged.



IMPORT SETTINGS

Settings Source

Setup a path that contains settings of LogAnalyzer.

Path: c:\

Settings Format

● bt-LogAnalyzer 7 format

○ bt-LogAnalyzer 6 legacy format

Import method

○ Purge existing database contents and import

● Import selected configuration settings

Settings Groups

Attention

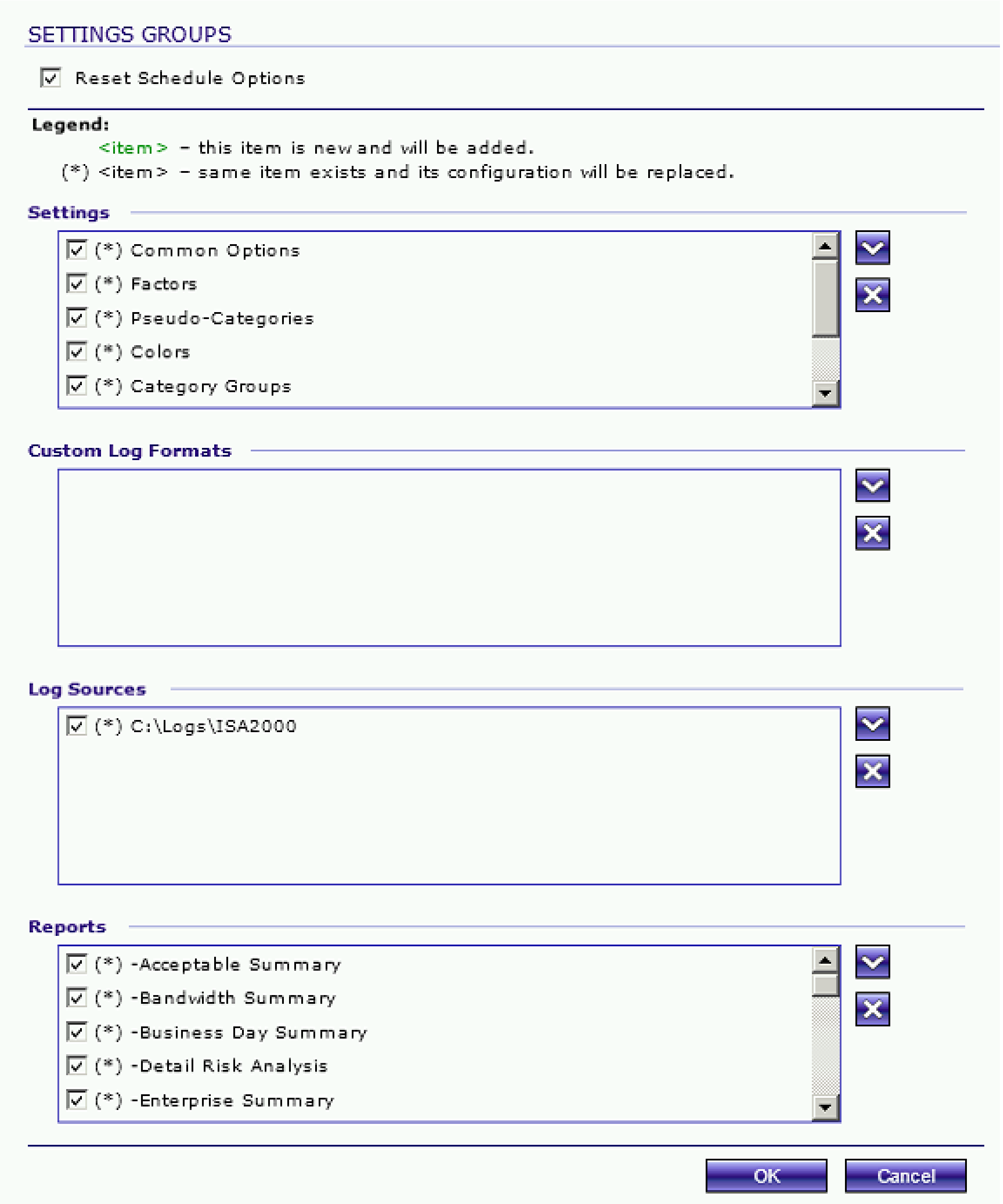
After importing, the settings selected in the "Settings Groups" section will be overwritten. To save the current settings, use the "Export settings" button in the left pane.

Figure 2 - Import Settings with Custom import selected

In Figure 3, there are four separate areas containing the settings to be imported. There is also an option at the top of the page to ‘Reset Schedule Options’ and is enabled by default. This prevents schedules that may be part of imported reports or log sources from starting immediately after the import is completed.

NOTE:
Unless there is a specific need to uncheck this option, it is highly recommended to leave this enabled.

To differentiate between items that are new or items that already exist, the LASE settings are color-coded. Items listed in green text indicate that the item does not exist in the LASE configuration currently being used, and would be added by a settings import if selected. This is useful when trying to identify reports that may have been accidentally renamed or deleted. Figure 4 contains a representation for this feature. Additionally, any item with an * indicates that the item is already defined.



SETTINGS GROUPS

☑ Reset Schedule Options

Legend:

<item> - this item is new and will be added.

(*) <item> - same item exists and its configuration will be replaced.

Settings

☑ (*) Common Options
☑ (*) Factors
☑ (*) Pseudo-Categories
☑ (*) Colors
☑ (*) Category Groups

Custom Log Formats

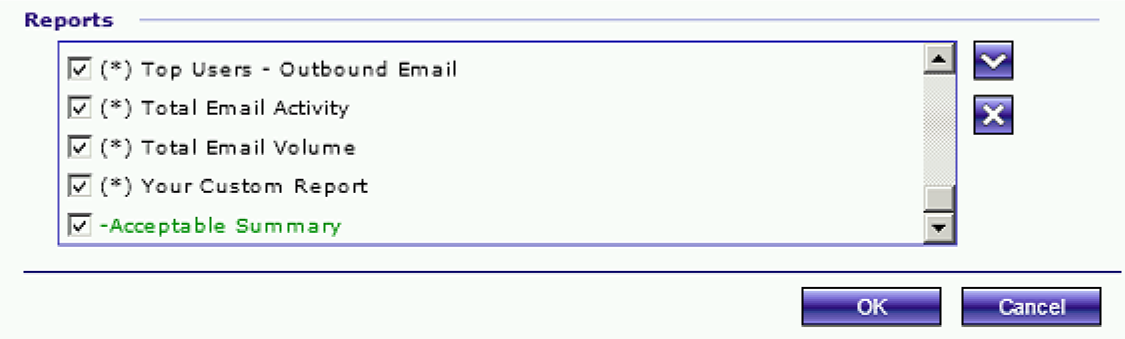
Log Sources

☑ (*) C:\Logs\ISA2000

Reports

☑ (*) -Acceptable Summary
☑ (*) -Bandwidth Summary
☑ (*) -Business Day Summary
☑ (*) -Detail Risk Analysis
☑ (*) -Enterprise Summary

Figure 3 - Custom Settings Import Option



- ☑ (*) Top Users - Outbound Email
- ☑ (*) Total Email Activity
- ☑ (*) Total Email Volume
- ☑ (*) Your Custom Report
- ☑ -Acceptable Summary

Figure 4 - Missing Report

Please also be aware of the following:

- Only items that are missing will be shown in green. Items that have different configuration settings will not be shown in a different color.
- Importing an older log source export could cause your Loading and Categorization operations to fail if it was configured for a custom log source that has since changed.
- Importing Report settings does not restore the report results. If the report results need to be restored, a database restore will be required.

The items listed above are not an exhaustive list. To guard against loss of data, the user should perform daily database backups that occur outside of loading, categorization and reporting operations.Combining database backups with scheduled 'Settings Exports' will help ensure a return to normal operations with minimal data loss should an issue occur.

Setting up Scheduled Backups 'Settings Exports'

1. From the top navigation bar, move the cursor over the 'Settings' button.
2. From the menu that appears, select 'Backup'
3. Select the 'Enable automatic settings backup' option at the top of the **Automatic Settings Backup** page.
4. Set a destination for your settings backup.

NOTE:

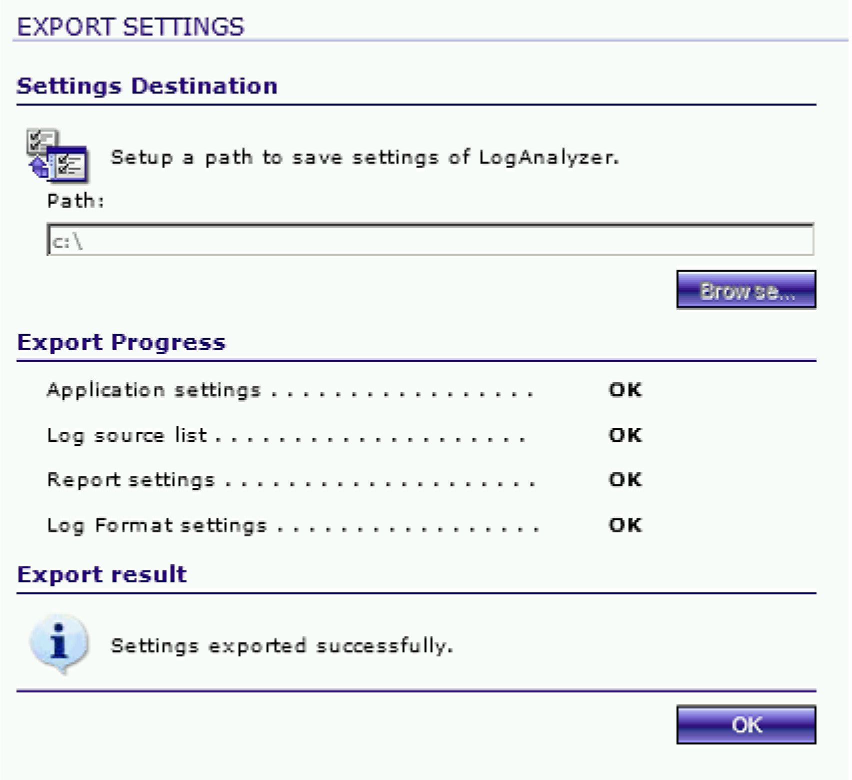
A 'Backup' or 'Settings Export' will create a folder labeled 'Exported Settings', containing a sub-folder labeled with the date/time stamp of the settings export execution date and time. The folder will contain four files.

- AppSettings<DateofExport>.xml
- LogFormatSettings<DateofExport>.xml
- LogInfoSourceSettings<DateofExport>.xml
- RepSettings<DateofExport>.xml

5. Set the time that the backup should start
6. Select the re-occurrence of the backup (Daily, Weekly, Monthly)
7. Apply your changes

Executing a Manual 'Settings Export'

1. From the top navigation bar, move the cursor over the 'Settings' button.
2. From the menu that appears, select 'Settings Export'
3. Select the path to where the settings should be stored.
4. Figure 5 shows a successful Settings Export operation



EXPORT SETTINGS

Settings Destination

Setup a path to save settings of LogAnalyzer.

Path:

c:\

Export Progress

```
Application settings . . . . . . . . . . . . . . . . .      OK
Log source list . . . . . . . . . . . . . . . . . . . .     OK
Report settings . . . . . . . . . . . . . . . . . . . .     OK
Log Format settings . . . . . . . . . . . . . . . . .       OK
```

Export result

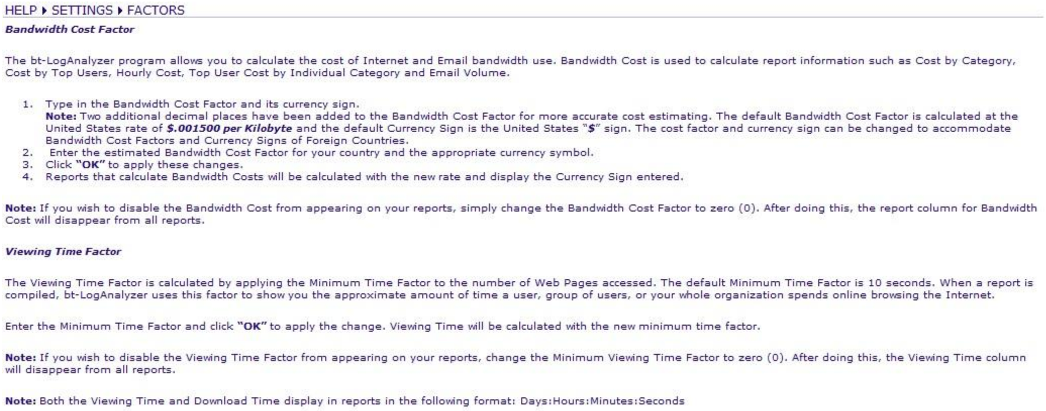
Settings exported successfully.

Figure 5 - Successful Settings Export

Help Tab

The Help button is designed to provide information on specific areas of the application that you are in. For example, clicking "Help" while in the "Settings->Factors" section of LogAnalyzer will display information specific to that section.

The contents of this user guide can also be found within the applications 'Help Menu'



HELP ▸ SETTINGS ▸ FACTORS

Bandwidth Cost Factor

The bt-LogAnalyzer program allows you to calculate the cost of Internet and Email bandwidth use. Bandwidth Cost is used to calculate report information such as Cost by Category, Cost by Top Users, Hourly Cost, Top User Cost by Individual Category and Email Volume.

1. Type in the Bandwidth Cost Factor and its currency sign.
   Note: Two additional decimal places have been added to the Bandwidth Cost Factor for more accurate cost estimating. The default Bandwidth Cost Factor is calculated at the United States rate of ***$.001500 per Kilobyte*** and the default Currency Sign is the United States "***$***" sign. The cost factor and currency sign can be changed to accommodate Bandwidth Cost Factors and Currency Signs of Foreign Countries.
2. Enter the estimated Bandwidth Cost Factor for your country and the appropriate currency symbol.
3. Click **"OK"** to apply these changes.
4. Reports that calculate Bandwidth Costs will be calculated with the new rate and display the Currency Sign entered.

Note: If you wish to disable the Bandwidth Cost from appearing on your reports, simply change the Bandwidth Cost Factor to zero (0). After doing this, the report column for Bandwidth Cost will disappear from all reports.

Viewing Time Factor

The Viewing Time Factor is calculated by applying the Minimum Time Factor to the number of Web Pages accessed. The default Minimum Time Factor is 10 seconds. When a report is compiled, bt-LogAnalyzer uses this factor to show you the approximate amount of time a user, group of users, or your whole organization spends online browsing the Internet.

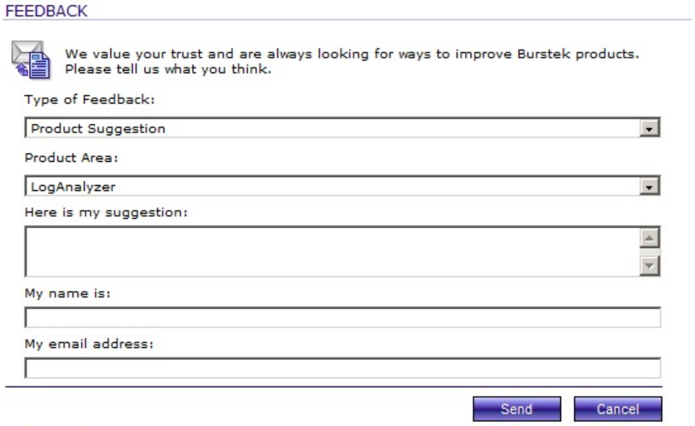
Enter the Minimum Time Factor and click **"OK"** to apply the change. Viewing Time will be calculated with the new minimum time factor.

Note: If you wish to disable the Viewing Time Factor from appearing on your reports, change the Minimum Viewing Time Factor to zero (0). After doing this, the Viewing Time column will disappear from all reports.

Note: Both the Viewing Time and Download Time display in reports in the following format: Days:Hours:Minutes:Seconds

Help Example

The "Help" tab also contains an option to provide feedback to Burstek. You can use this for :



FEEDBACK

We value your trust and are always looking for ways to improve Burstek products.
Please tell us what you think.

Type of Feedback: Product Suggestion

Product Area: LogAnalyzer

Here is my suggestion:

My name is:

My email address:

Feedback Form

- Product Suggestions
- Reporting Bugs
- Technical Support
- Sales Questions / Feedback.

Configuring bt-LogAnalyzer SE^{TM}

The bt-LogAnalyzer program supports multiple platforms, multiple log file formats, and multiple sources. You can define which log files and which source locations will be used for report generation. As a result, you are not restricted to a single directory or type of log (i.e. flat file or SQL).

Log Sources

This page presents the full list of your log sources. If a log source is displayed in red, this means that the last time the data was loaded from it, an error occurred, or the loading procces was stopped by the user.

To Display the Log Sources Properties

1. From the Log Source List, select a log source.
2. In the left pane, select **'Log Source Properties'** from the '**Log Source List'** section, or click on the properties icon of the log source. The LOG SOURCE PROPERTIES page displays.

> **NOTE:**
> If a log source is selected in the right pane, its basic properties are presented in the left pane, in the **'Load Info Source'** section.

To Add Log Sources

1. From the **Log Source List** section in the left pane, select **New Log Source**.
2. The NEW LOG SOURCE page displays. Follow the instructions on this page.

To Change Log Sources

1. From the Log Source List, select a log source you wish to edit.
2. In the left pane, select **Log Source Properties** from the **Log Source List** section, or click on the icon of the log source. The LOG SOURCE PROPERTIES page displays.
3. Change the Log Source information as desired and click "**Test**" to make sure the bt-LogAnalyzer Program can access the log files.
4. Click "**OK**" to change the log source type.

To Delete Log Sources

1. From the Log Source List, select a log source you want to delete.
2. In the left pane, select **Delete Log Source** from the **Log Source List** section.

> **NOTE:**
> You can also remove the log source from the list by clicking its ✖ icon

3. The bt-LogAnalyzer will prompt you to delete the selected item from the list.
4. Click "**Yes**" to delete the selected item.

To Manually Load Data from Log Sources into bt-LogAnalyzer Storage

1. From the Log Source List, select a log source you want to load data from.
2. In the left pane, select **Load Data** from the **Log Source List** section. The LOG SOURCES > LOAD DATA MANUALLY page displays. Follow the instructions on this page.

> **NOTE:**

You can also load data from a log source by clicking its icon

To Categorize Data Loaded into bt-LogAnalyzer Storage

1. From the Log Source List, select a log source to categorize its data.
2. In the left pane, select **Categorize Data** from the **Log Source List** section.
3. Click "**OK**" to confirm data categorization.

You can check on the categorization progress in two ways:

- By viewing the list of active processes to make sure the process is running
- By exploring the loading history, which presents the complete load/categorization details and results.

You can also view the list of active processes, click on **Job Queue** in the **Active Links** section in the left pane.

NOTE:
The **Loading History** option under **Categories** is specific to the categories section.

Manual Resolution of User's Names

This operation is relevant to MS Exchange Server logs only and allows for the uniform representation of user names in reports. Normally, this is done automatically, on data loading from a Log Source, but can also be done manually by using this option.

1. From the Log Source List, select a log source.
2. In the left pane, select **Resolve User's Names** from the **Log Source List** section.
3. Click "**OK**" to confirm.

To View Loading History

To view the loading history, which presents the complete load details and results, click on **Loading History** in the **Log Source List** section in the left pane and select the brief loading history icon or select the **Loading History Detail** in the quick launch section.

Log Sources – Common Options Page

bt-LogAnalyzer supports multiple log sources and multiple locations. For example, your company could have an ISA Server in New York that has SQL logs, a WatchGuard appliance utilizing PostgreSQL in Chicago and a Squid Cache Server in Los Angeles that has flat log files. LogAnalyzer can point to all or any combination of the log files and create a single consolidated report. Output can be either HTML or XML and can be automatically scheduled, Emailed or saved.

NOTE:
If you did not enter a network user name and password during the installation of bt-LogAnalyzer, you will need to edit the log on properties of the bt-LogAnalyzer Service in Windows so that a network user, not a local user, is running the Service or you will not be able to create or edit Log Sources located on the network.

Log Source Type

The Log Info Source Type is either: **File System Folder**, **ODBC DSN** (if the logs are located on an SQL server), **MSDE Database**, or **WatchGuard PostgreSQL Database.**

File System Folder

1. If you selected ***File System Folder***, click the "**Browse**" button to select the folder.

> **NOTE:**
> Only local system drives and UNC paths are available. You cannot select a mapped drive or browse network folders.

2. Select the folder and click "**OK**."
3. Select the date format from the drop down list.

> **NOTE:**
> If you are using Microsoft Servers (ISA, Proxy, Exchange) use ***Auto-detect*** for the Date and Log Files format.

4. Select the Log Files format from the drop down menu. Options include:

    - Auto detect – MS
    - bt-WebFilter
    - MS ISA Server
    - MS Proxy Server
    - W3C Extended
    - Cisco Cache Engine
    - iPlanet Proxy
    - Squid Cache
    - Net Cache
    - Inktomi Traffic Server
    - CacheOS W3C Compatible
    - BorderManager
    - Exchange 5.5
    - Exchange 200x
    - MailSweeper
    - XML Report Results

5. Click the radio button to select **Use all Files** or **Use Selected Files**.
6. If you choose the **Use Selected Files** option, click the select button to display the **Select Log Files** dialog.
7. Click the check box to select the log files to be analyzed. Click the ✓ button or ✕ button on the right of the screen to select or deselect all. After you have selected the log files, click "**OK**."
8. Click "**Test**" to make sure the bt-LogAnalyzer Program can access the log files.
9. Click "**Apply**" to add the log source type.

ODBC DSN

1. If you selected ***ODBC DSN*** as your log source type, enter the DSN Value.

NOTE:
You can enter either the IP Address or the DSN Name

2. Enter the table.
3. Enter the user name.
4. Enter the password to access log files.
5. Click “**Test**” to make sure the bt-LogAnalyzer Program can access the log files.
6. Click “**Apply**” to add the log source type.

MSDE Database

1. Select this option to read from the ISA Server’s local log files.

NOTE:
bt-LogAnalyzer is not recommended to be installed on the same server as your Microsoft ISA Server. If you select this options you will need to load the **Remote Log Data Loader** on the ISA server.

2. Click on the **‘Advanced Tab’** and select **‘Use remote server for this Log Source’** under **‘Remoting’**
3. Click **“Test”** to make sure the bt-LogAnalyzer program can access the remote database
4. Click **Apply** to save the changes.

WatchGaurd PostgreSQL Database

1. Select this option to read from WatchGuard PostreSQL Databases
2. Enter the **‘Server’** name
3. Enter the **‘Port’**
4. Enter the **‘User name’** and **‘Password’**
5. Enter the **‘Database’**
6. Click **‘Test’** and **‘Apply’** to add the log source

Log Source – Advanced Page

There are two options under the **‘Advanced’** tab in the Log Source Properties.

- If **Authentication Mode** is turned on, bt-LogAnalyzer will exclude log entries for anonymous user IDs from license counts, but will include them in reports. If it is turned off, anonymous user IDs will not be counted or included in reports.
- The second option, if turned on, will drop domain names from the front of user names in the reports unless a domain is specifically listed in the log file. Otherwise the default domain name will be shown.

Remoting

This is used to identify the name of the remote server that contains the **‘Remote Log Data Loader’** installation. (See “Remote Log Data Loader Installation” in the bt-LogAnalyzer installation guide)

Log Sources – Loading Page

Loading Method

1. Select a loading method: either **Manual** or **Automatic**. To do this, click the radio button.
   If you select **Manual**, you will have to initiate data loading from the log source manually, by clicking on **Load Data** in the **Load Info Source List** section in the left pane.
   If you select **Automatic**, the data will be loaded from the log source into the LogAnalyzer storage when a report generation starts, or according to a schedule, or both. Automatic loading on report generation start is the default setting.

   > **NOTE:**
   > If you select **Automatic**, you will still be able to load log source data manually. If you select **Manual**, you will not be able to load the data automatically.

2. Select either **On report generation start**, or **According to schedule**, or both.
3. If you selected **According to schedule**, define when and how often the data will be loaded into the storage.

To Set Schedule Options:

1. In the **Start loading at** field set the date and time you wish to begin loading the data.
2. Under **Recurrence Schema**, select from one of the following options by clicking the radio button next to the selection:

   1. Once
   2. Every day
   3. Weekly
   4. Once a month.

3. If you select the **Weekly** option, select the day of the week you wish to load the data. Click the ⌄ button or ✖ button on the right of the screen to select or deselect all, respectively.
4. If you select the **Once a month** option, define the day of the month to load the data.

Loading Algorithm

1. Select a loading algorithm.
   - If you select **Load new log data**, only the data that has not been previously loaded will be copied to the storage.
   - If you select **Delete all previously loaded log data and load all log data**, all the data downloaded from the log source will be removed from the storage and then the complete contents of the log source will be re-loaded into the storage.
2. If you selected **Load new log data**, you can choose to delete the old log data from the storage. To do this, check the **Delete all previously loaded log data** box.

After you have selected your Method and Algorithm options, click the **Apply** button to apply them.

Log Sources – Categorization Tab

Pre-Categorization Method

1. Select a pre-categorization method: (The default is automatic categorization on log data loading)
   - **Manual -** If you select **Manual**, you will have to initiate categorization of the log data in the storage manually, by clicking on **Categorize Data** in the **Load Info Source List** section in the left pane.

- **Automatic -** If you select **Automatic**, the data will be categorized when a report generation starts, or according to a schedule, or both.

> **NOTE:**
> If you select **Automatic**, you will still be able to categorize log source data manually.

2. Select either **On report generation start**, or **According to schedule**, or both.
3. If you selected **According to schedule**, define when and how often the data will be categorized.

To Set Schedule Options:

1. In the **Start categorization at** field set the date and time you wish to begin categorizing the data.
2. Under **Recurrence Schema**, select from one of the following options by clicking the radio button next to the selection:
   - Once
   - Every day
   - Weekly
   - Once a month.
3. If you select the **Weekly** option, select the day or days of the week you wish to categorize the data. Click the ⌄button or ☒button on the right of the screen to select or deselect all, respectively.
4. If you select the **Monthly** option, select the day of the month you wish to categorize the data.
5. If you select the **Once a month** option, define the day of the month to categorize the data.
6. After you have selected your options, click the **Apply** button to apply them.

Category List

This page displays the bt-LogAnalyzer URL Control List which contains approximately 60 predefined categories. To navigate the list, click on page numbers at the bottom of the page.

The following options are available to work with the categories:

- **New Category**
- **Category Properties**
- **Delete Category**
- **Import Categories**
- **Loading History**

New Category

This option allows you to add a new category to the list. For example, you may wish to create a new category called "Intranet" to be able to determine how much time employees spend on the intranet and how much it costs the company.

When creating a new Category, you will see three customization sections:

- Common Options – This is where you will provide the name and description for your new category
- Included URLs - URLs that explicitly belong to a category. For example, an investment firm may wish to add the URL for their corporate newsletter as an included URL in the category Financial.

> **NOTE:**
> Best Practice guideline is to create URLs with wildcard masks. I.E. to add the URL http://www.burstek.com you would enter *.burstek.com* AND *//burstek.com*. The use of these two filters provides the highest match probability.

- Excluded URLs – URLs that you want to explicitly remove from a category. The Best Practice guideline applies to these URLs as well.

Category Properties

Use this option if you want to change an existing category's properties to customize it. For example, you may wish to customize a category such as "Local" and add URLs for local weather, news and radio. You can access the categories properties by selecting the appropriate category and clicking on the icon or by selecting the **Category Properties** link in the navigation side bar.

To Delete a Category

This option allows you to delete a category. Select the desired category and click the ✖ icon or select the **Delete Category** link in the navigation side bar

Category Lookup

This option allows you to lookup URLs in the URL Control List to determine their category (or categories, if an URL is included in more than one). Enter the URL exactly or using best practice guidelines.

Import Categories

Use this option if you want to import or update the Control List. The bt-LogAnalyzer program URL Control List is updated daily by Burstek. You can choose to automatically update your Control List on a daily, weekly or monthly basis.

- Common Information - With this page, you can download an updated URL Control List from the Internet and integrate it into bt-LogAnalyzer. You can also import updates previously downloaded from the Internet and saved to a local path.

NOTE:
If you have added or modified URL Control List categories, the categories you have added or modified will not be overwritten by automatic updates.

To Download Updates from the Internet

1. Select the **Check for updates via Internet** radio button. The default World Wide Web Location displays.
2. Select either **Download and accept updates immediately** or **Download and save updates to local path**.
3. If you selected **Download and save updates to local path**, specify the location. To do this, use the **Browse** button.
4. Press **"Apply"** to apply the options or "**OK**" to apply and go to the categories list.

To Import Updates from a Local Path

1. Select the Import updates from local path radio button.
2. Select a file to import the update from. To do this, use the **Browse** button.
3. Press **Apply** to import the update.

NOTE:
When you import updates, either from the Internet or from a local path, the updates are copied to the Category Server.

- Automatic Updates - The bt-LogAnalyzer program URL Control List is updated daily by Burstek. You can choose to automatically update your Control List on a daily, weekly, or monthly basis

NOTE:
Due to the dynamic nature of the Internet, Burstek recommends that you update your URL

Control List on a ***Daily*** basis.

1. Check the **Enable Automatic Update** option.
2. Enter the time and click the radio button next to the **Every Day**, **Every Week** or **Every Month** update option.
3. Enter the Run Automatic Updates login and password, if necessary**.** This will enable you to automatically download Control List updates if you require authentication for permission to download files.

NOTE:

This may be needed if the machine is behind a proxy server that requires authentication. This login and password will allow the **Run Automatic Updates** component to pass through the proxy server. If the proxy server allows anonymous access, the login and password can be omitted.

4. Click "**Apply**" to apply the options or "**OK**" to apply and go to the categories list. The URL Control List will be updated automatically according to the schedule you have selected.

- Notification Delivery - Specify individuals who will receive notification when the URL Control List is updated.
  1. To add a new recipient, use the **New recipient** option in the **Notification recipient** section in the left pane.
  2. To change an existing recipient's properties, use the Recipient properties option in the Notification recipient section in the left pane, or the 📋button.
  3. To delete a recipient, use the Delete recipient option in the Notification recipient section in the left pane, or the ✖button.
  4. Check the Enable notification of URL Control List Auto Download success, or Enable notification of URL Control List Auto Download failure, or both.
  5. When done, click "**Apply**" to apply the options or "**OK**" to apply and go to the categories list.

Loading History

This option allows you to view the details of category import to the Category Server and category loading into the LogAnalyzer database. The bt-LogAnalyzer program URL Control List is updated daily by Burstek.

Categories Loading History :

This page displays the results of Control List imports to the Category Server and Control List URL load operations. The following information is also available:

- **Import type**. This is either import of the URL Control List to the Category server or loading of the categories to the LogAnalyzer database.
- **User**. This displays the user who initiated the action.
- **Date of Change**. This is the date a new update of the URL Control List appeared on the Burst Technology Website.
- **Date of Load**. This is the date the update was loaded into the LogAnalyzer database.
- **Success**. The checked box indicates the success of the action.

To import the URL Control List to the Category Server, use **Import to Category Server** in the **Category Loading** section in the left navigation pane.

To load categories to the LogAnalyzer database, use **Load URL Control List** in the **Category Loading** section in the left navigation pane.

Reports

The strength of the bt-LogAnalyzer software is the ease with which you can automatically generate and distribute Standard and Customized reports.

The REPORT LIST page displays the list of reports and allows you to perform various actions with the reports. The following actions are available from the Report List section in the left pane:

New Report

Allows you to create a new report.

Report Properties

Displays the current report properties. This can also be done by pressing the report's ▤ button. The PROPERTIES page consists of six tabs: Common Options, Advanced, Customize, Schedule, Distribution, and Security. When you select a report from the list, basic report properties are presented in the Report section in the left pane.

> **NOTE:**
> The Security tab is only visible when Active Directory Organizational Unit support has been enabled during the installation process

Delete Report

Deletes the selected report from the list. This can also be done by pressing the ✖ button.

Generate Report

Allows you to generate a previously selected report. To stop a report generation process, click Process List in the Active Links section in the left pane, and follow the instructions on the PROCESS LIST page. You can also start report generation by clicking the 📄 button.

Report Generation History

Provides information on when the selected report was generated, and whether report generation was successful.

Clear Results

You can clear the results and regenerate the report.

Export to XML

Allows you to export reports in XML format.

NOTE:
To export reports to HTML, click Version for Print and save the report HTML from your browser; or click Send to Mail Recipient and choose to send the report as an HTML attachment.

Send to Mail Recipient

Allows you to Email the report.

Print Report

Allows you to print a report. After previewing the print version (this is the latest available version of the report), press the Print button in your browser.

Copy Report Definition

Allows you to create a duplicate copy of a report.

Result as Parameters

Allows you to use the report result as filtering conditions for further report generation.

Replicate Report Definition

Allows you to push a report out to a replication server.
To refresh the list of reports to show the latest report results, press the Refresh button in your browser.
To view the latest report of the selected type, click its 📄 button.

Standard Reports

The bt-LogAnalyzer program has fourteen Standard Web Reports and Seven Standard Email Reports.

Standard Web Reports

- Acceptable Summary
- Bandwidth Summary
- Business Day Summary
- Enterprise Summary
- Executive Summary
- Legal Liability Summary
- Non-productive Summary
- Open Surfing Summary
- Quota Usage
- Risk Assessment Summary
- Sexual Content Details
- Top Web Sites
- User Audit Details
- WebExtra

Standard Email Reports

- Exchange Email Details
- Top 25 Web & Exchange Users
- Top Users - Inbound Email
- Top Users - Outbound Email
- Total Email Activity
- Total Email Volume

Customized Reports

The bt-LogAnalyzer application allows you to generate an unlimited number of customized Web reports, e.g. Intranet, Local, Streaming Media and Social Networking sites such as Facebook and Twitter. Any of the standard Web and Email reports can be customized to meet your business requirements.

Reports – Common Options

The Common Options tab allows you to enter the Report Name and Description. You can also select the type of report and the details you wish to display. Other option is Maximum Report Lines.

To Set Common Options:

1. From the Common Options tab, enter the report name and a description of the information contained in the report.
2. Select the type of report, global or user audit detail.
3. Click the check box next to the report information to be included. Click the ⌄ button or ☒ button on the right of the screen to select or deselect all.

> **NOTE:**
> Detail reports are used when you wish to display URLs.

4. Set the remaining report options. (See Appendix for Descriptions of Report Types)
5. **Maximum Report Lines:** - You can set the maximum number of users that will appear on a global report or the maximum number of lines that will appear on a detail report. Click the check box to set this option. Type the number of users or lines you want to appear on the report.
6. Press **Apply** to save your options

Global Report Options:

The following Web and Email reporting options are available when generating global reports.

> **NOTE:**
> The Email reporting options for outbound, inbound and internal Email volume and bandwidth are new.

Number of Web Pages per Category - Represents the number of one-category documents downloaded by a user or a group of users. Measured by the number of web pages downloaded per category.

Risk Analysis - A table representing a breakdown of websites visited into five default risk categories: Business Related, Legal Liability, Non-Business, Pop-ups, and Security Risk.

Cost by Category - Represents the cost of one-category documents downloaded by a user or a group of users. The bt-LogAnalyzer program allows you to calculate the cost of Internet and Email bandwidth use.

Number of Users per Category - Represents the number of users who visited URLs for a particular category.

Top Users Activity Web Pages - Represents the most active users in the system. Top Users Activity is measured in number of downloaded documents per user.

Top Users - Denied Activity - Represents the most active users who tried to gain access to forbidden sites. User Activity is measured in amount of the downloaded documents per user.

Top Users - Category Activity -The number of user(s) visits per category. (The category must be specified as a report filter.)

Top Users - Category Volume - The most active users in the system. Top Users – Category Volume is measured in kilobytes per user.

Top Users – Volume - The most active users in the system. Top Users - Volume is measured in kilobytes per user.

Top Web Sites - Represents the most visited web sites. (The users and/or groups must be specified as a report filter.)

Top Web Sites by Bandwidth - Represents the most visited web sites by Bandwidth. (Bandwidth is measured in total kilobytes.)

Web Access - Hourly Activity - Hourly Activity is measured in web pages accessed per hour. (The users and/or groups must be specified as a report filter.)

Web Access - Hourly Bandwidth - Displays the hourly bandwidth used to access web sites. (Bandwidth is measured in total kilobytes.)

Web Access - Results Summary - Lets you complete all report types of the global group at one time. (The users and/or groups must be specified as a report filter.)

Top Users - Volume Quota - This option is used in conjunction with bt-WebFilter. Volume Quotas are assigned in bt-WebFilter and the results are displayed according the percent of quota used.

Top Users - Time Quota - This option is used in conjunction with bt-WebFilter. Time Quotas are assigned in bt-WebFilter and the results are displayed according the percent of quota used.

Top Users - Total Email Activity - Lists the most active users (total number of Emails sent and received) Email activity is defined as percentage of user transferred Emails compared to all transferred Emails.

Top Users - Total Email Volume - Lists the most active users by volume (number of kilobytes sent and received) Email Volume is defined as percentage of user Email volume compared to the volume of all transferred Emails.

Top Users - Outbound Email Activity - It represents the most active users who have the highest number of sent Emails. Outbound Email Activity is defined as percentage of user sent Emails compared to the total number of all sent Emails.

Top Users - Outbound Email Volume - It represents the most active users who have the highest volume (measured in kilobytes) of sent Emails. Outbound Email Volume is defined as percentage of user sent Emails compared to the total volume of all sent Emails.

Top Users - Inbound Email Activity - It represents the most active users who have the highest number of received Emails. Inbound Email Activity is defined as percentage of user received Emails compared to the total number of all received Emails.

Top Users - Inbound Email Volume - It represents the most active users who have the highest volume (measured in Kilobytes) of received Emails. Inbound Email Volume is defined as percentage of user received Emails compared to the total volume of all received Emails.

Top Outbound Email Addresses - The most popular outbound Email addresses that occur among sent Emails. It is defined as percentage of the number of sent Emails to a particular outbound address compared to the number of all sent Emails.

Top Inbound Email Addresses - The most popular originating Email addresses that occur among received Emails. It is defined as percentage of received Emails originating from a particular address compared to the number of all received Emails.

User Audit Detail Options:

The following Web and Email reporting options are available when generating user audit detail reports.

Number of Web Pages per Category - Represents the number of one-category documents downloaded by a user or a group of users. Measured by the number of web pages downloaded per category.

Cost by Category - Represents the cost of one-category documents downloaded by a user or a group of users. The bt-LogAnalyzer program allows you to calculate the cost of Internet and Email bandwidth use.

Download Time by Category - Represents the amount of time spent downloading documents by category.

Top Web Sites - Represents the most visited web sites. (The users and/or groups must be specified as a report filter.)

Top Web Sites by Bandwidth - Represents the most visited web sites by Bandwidth. (Bandwidth is measured in total kilobytes.)

Web Access - Hourly Activity - Hourly Activity is measured in web pages accessed per hour. (The users and/or groups must be specified as a report filter.)

Web Access - Hourly Denied Activity - Hourly Denied Activity is measured in web pages denied access per hour. (The users and/or groups must be specified as a report filter.)

Web Access - Hourly Bandwidth - Hourly Bandwidth is measured in kilobytes per hour. (The users and/or groups must be specified as a report filter.)

Web Access - Results Summary - Lets you complete all report types of the global group at one time. (The users and/or groups must be specified as a report filter.)

Web Page Details - List the URL visited and the date/time of visit, the IP Address of the machine and the category of the URL. Note: The user and/or group should be specified as a report filter. If not, the report will be built for all users found in the log files and the user name will be listed for each record.

Top Users - Total Email Activity - Lists the most active users (total number of Emails sent and received) Email activity is defined as percentage of user transferred Emails compared to all transferred Emails.

Top Users - Total Email Volume - Lists the most active users by volume (number of kilobytes sent and received) Email Volume is defined as percentage of user Email volume compared to the volume of all transferred Emails.

Top Users - Outbound Email Activity - It represents the most active users who have the highest number of sent Emails. Outbound Email Activity is defined as percentage of user sent Emails compared to the total number of all sent Emails.

Top Users - Outbound Email Volume - It represents the most active users who have the highest volume (measured in kilobytes) of sent Emails. Outbound Email Volume is defined as percentage of user sent Emails compared to the total volume of all sent Emails.

Top Users - Inbound Email Activity - It represents the most active users who have the highest number of received Emails. Inbound Email Activity is defined as percentage of user received Emails compared to the total number of all received Emails.

Top Users - Inbound Email Volume - It represents the most active users who have the highest volume (measured in Kilobytes) of received Emails. Inbound Email Volume is defined as percentage of user received Emails compared to the total volume of all received Emails.

Top Outbound Email Addresses - The most popular outbound Email addresses that occur among sent Emails. It is defined as percentage of the number of sent Emails to a particular outbound address compared to the number of all sent Emails.

Top Inbound Email Addresses - The most popular originating Email addresses that occur among received Emails. It is defined as percentage of received Emails originating from a particular address compared to the number of all received Emails.

Email Details - List the number of sent and received Emails and the originating address of received Emails as well as the destination address of sent Emails.

Reports – Advanced

Different Advanced Report options will be available depending on if you are running a Global report or a User Audit Detail Report.

Resolve user names - This option allows you to specify the actual user name be displayed rather than their domain/logon name. Click the check box to select this option.

Include IPs to Web Page Details report - This option allows you to specify IP address of the computer used to access the Web page as well as the users domain and logon name. Click the check box to select this option.

Show Email subjects - this option allows you to show the Email subject line in Email details reports.

Suppress distribution lists - this option allows you to suppress Email distribution lists.

Hide Report Synopsis and Report Parameters sections - This option allows you to hide the report synopsis (I.E. Record Counts) and the report selection parameters section of a report so that you hide the data.

Run this report at remote servers - this option tells the report to also run on your remote bt-LogAnalyzer server(s). After setting this option, you should replicate the report definition, i.e. push the report definition to the remote servers. This can be done from the REPORT LIST page. For the instructions on how to setup the Virtual Report Server, please see the APPLICATION SETTINGS – DISTRIBUTED REPORTS page.

Limit 'Number of Web Pages per Category' report to display "X" items - this option allows you to limit the number of specific Web page details shown for each category to only what you specify.

Risk Analysis Report:

Bandwidth - displays a bar on the Risk Analysis chart showing the number of kilobytes per risk category.

Web Pages - displays a bar on the Risk Analysis chart showing the number of Web pages visited per risk category.

Download Time - displays a bar on the Risk Analysis chart showing the actual amount of time spent downloading pages within each risk category.

Apply Thresholds to the Report - this option allows you to specify whether to apply a threshold to the report or not. You can setup a default report threshold and then separate thresholds to some or all categories. For example, to recognize that an accident has happened, you may want to specify that a user needs to visit 4 sites that are categorized as "Gambling" before it shows up on a report because anything less than that could be accidental views. To define individual thresholds for some or each category, press **Categories**.

After you have set all of the **Advanced** options, click the "**Apply**" button to apply these options.

Reports – Customize

The **Customize** tab allows you to set the rules which will define the subset or records to analyze.

You can set the date and time intervals to be filtered, select the categories to be included in the report, select the individual user(s) and/or group(s) to be included in the report, and specify which reports are to be filtered.
To start setting a filter, either press its **Edit** button or click its icon.

Customize Date Time

The Date/Time filter option allows you to specify the date and the list of hourly intervals to be filtered. For example, you may wish to find out how many Websites are visited on Monday from 9-10AM and from 1- 2PM.

To Specify the Date Interval to be Filtered:

Specify the date interval to be filtered: **Prior day**, **Prior week**, **Prior month**, or **Custom**. If you selected **Custom**, specify the start and/or end dates of the interval.

To Specify the Hourly Interval(s) to be Filtered:

1. Click the check box next to the hour interval to select the interval. Click the ⌄button or ☒button on the right of the screen to select or deselect all.

   > **NOTE:**
   > The default is 24 hours (i.e. leave all unchecked).

2. Click "**Apply**" to apply these options or "**OK**" to apply and go to the CUSTOMIZE page.

Reports - Customize Categories

bt-LogAnalyzer allows you to select all categories or specify which individual categories to include in a report.

To Select the Categories to be Filtered:

1. Click the radio button to automatically select All categories or Select Individual Categories.

2. If you chose Select Individual Categories, specify the categories to be filtered. Click the check box next to the category to select the category. Click the ⌄ button or ☒ button on the right of the screen to select or deselect all.

3. Click "Apply" to apply these categories or "OK" to apply and go to the CUSTOMIZE page.

Exclude No Pseudo Categories - this is the default report option. When this is selected, all pseudo categories will be displayed on your reports.

Exclude Selected Pseudo Categories - use this option to exclude one or more pseudo categories from your reports. When a pseudo category is excluded, any Websites that would have fallen into the excluded pseudo category will be sorted into the general Control List categories they reside in.

Reports - User Filter

You can specify which users or groups of users to include in a report. You can also specify which users or groups of users to exclude from a report.

To Specify Which Users and/or Groups are to be Filtered:

Click the radio button to select All users or Individual users, groups, organizational units, IP mask or IP range.

To Add Individual Users, Groups, Organizational Units, IP Masks/IP Ranges, or E-mails:

1. To add individual users and/or groups to the list, click New Users and Groups in the Individual Users & Groups section in the left pane. The SELECT USERS AND GROUPS page displays.

2. To add an organizational unit to the list, click New Organizational Units in the Individual Users & Groups section in the left pane. The SELECT ORGANIZATIONAL UNITS page displays.

3. To add an IP mask or IP range, click New IP Mask or IP Range in the Individual Users & Groups section in the left pane. The SELECT IP MASK OR IP RANGE page displays.

4. To add an E-mail, click New Email in the Individual Users & Groups section in the left pane. The SELECT EMAIL page displays.

To Delete Individual Users, Groups, Organizational Units, IP Masks or IP Ranges, or E-mails:

1. Select an item you wish to delete from the list and click Delete Individual in the Individual Users & Groups section in the left pane, or press its button.

2. Click “OK” to confirm deletion.

3. On the USER FILTER page, click "Apply" to apply the changes or "OK" to apply and go to the CUSTOMIZE page.

To Specify Exceptions (identify which users, groups, organizational units, IP masks or IP ranges, or e-mails are to be excluded from a report):

1. To specify exceptions to the individual users and/or groups, click the New Users and Groups button in the Exceptions section in the left pane. The SELECT USERS AND GROUPS page displays.

2. To specify exceptions to the organizational units, click New Organizational Units in the Exception section in the left pane. The SELECT ORGANIZATIONAL UNITS page displays.

3. To specify exceptions to the IP masks or IP ranges, click New IP Mask or IP Range in the Exception section in the left pane. The SELECT IP MASK OR IP RANGE page displays.

4. To specify individual E-mail exceptions, click New Email in the Exception section in the left pane. The SELECT EMAIL page displays.

To Delete Individual Users, Groups , Organizational Units, IP Masks, or IP Ranges from the Exceptions List:

1. Select an item you wish to delete from the list and click Delete Individual in the Exception section in the left pane, or press its button.
2. Click “OK” to confirm deletion.
3. On the USER FILTER page, click "Apply" to apply the changes or "OK" to apply and go to the CUSTOMIZE page.

Reports - Customize Reports

You can also specify which reports results are to be filtered. For example, you can run a report to generate the top 25 users, and then filter it with a report for the top 25 Websites. This would give you the top 25 Websites visited by the top 25 users.

To Specify Which Report Results are to be Filtered:

1. Click the check box next to a report to select the report.
2. Click “Apply” to apply these Report Filter options.

Reports - Customize Log Sources

One of the strengths of bt-LogAnalyzer that separates it from the competition is the ability to support multiple log file formats and point to multiple log files in multiple locations, and combine them into a single report. There may be instances, however, when you do not want to include all log source files or all log file formats in a report. For example, you may have three ISA servers each with a different log source and you may want to report against one server only or you may want to create a Denied Activity report that contains only Denied Activity Log Sources.

NOTE:
In order to create a report that contains Denied Activity Log Sources, you must have the bt-WebFilter product installed and bt-WebFilter Logging must be turned on.

To Select Individual Log Info Sources:

1. The log sources that are displayed were previously defined. To add a log source, select **Log Sources**> **Log Sources List** from the menu and click **New Log Source** in the left pane.
2. Click the radio button to select ***All log sources*** or ***Select individual log sources***.
3. If you selected individual log sources, specify which log sources will be used to create the report. Click the check box next to the individual log to select the log source. Click the down arrow button to select all or the X button to deselect all.
4. Click “**Apply**” to apply these log sources.

Reports - Schedule

The Schedule tab allows you to define when and how often a report will be generated.

To Set Schedule Options:

1. In the Start Report Generation field, set the date and time you wish to begin generating the report.

2. Under Recurrence Schema, select one of the following options by clicking the radio button next to the selection:

   - Generate every day
   - Generate once
   - Generate weekly
   - Generate once a month.

3. If you select the Generate weekly option, select the day or day of the week you wish to generate the report. Click the ☑ button or ☒ button on the right of the screen to select or deselect all.

4. If you select the Generate monthly option, select the day of the month you wish to generate the report.

5. After you have selected your schedule options, click the “Apply” button to apply the schedule.

Reports - Distribution

The Distribution tab allows you to specify who will receive a copy of the report via Email and automatically Emails the generated report to the individuals listed. You can also specify the Email attachment format (embedded or HTML attachment).

To Add Names to the Distribution List:

1. Click ‘New Recipient’ in the **Report Recipients** section in the left pane.

2. The **Recipient’s Email Information** page displays.

3. Enter the recipient’s name and E-mail address. You must do this for each user.

TIP!

If you have mail enabled distribution groups, add the email address for that group to send the email to multiple users.

To Change or Edit Names or Email Addresses on the Distribution List:

1. Select the name of the person in the distribution list whose name or Email information you wish to change.

2. Click the Individual properties option in the **Report Recipients** section in the left pane or select the ☰ icon next to the recipients name.

3. The **Recipient’s Email Information** page displays allowing you to make the necessary changes.

To Delete Names from the Distribution List:

1. Select the name on the distribution list you want to delete.

2. Click **Delete Individual** in the **Report Recipients** section in the left pane or select the ✖icon.

3. Press OK to confirm.

The name will be removed from the list.

Email Format

bt-LogAnalyzer allows you to Email the report in HTML format or send the report as an attachment to an Email in HTML format.

Click the radio button to select “HTML” or “HTML Attachment”.

> **NOTE:**
> The “Report is Delivered as a Separate Attachment to the Email being sent**.**

Save to Folder:

You can specify that a copy of the report be saved to a specific folder.

1. Click the “Browse” button to select the folder name and path, or type the folder name and path in the path field.
2. A copy of the report will be saved to the folder specified.

> **NOTE:**
> You cannot save to a mapped network, only to a UNC path

3. When done, click the **“Apply”** button to save the changes.

Reports - Security

The **Security** tab allows you to specify which individual users or Active Directory Organizational Units will be allowed to read and generate a specific report. Select **Only Members of the Following Organizational Units** and click on the **Select OU** option to select which users or organizational units will have rights to either read or generate this specific report.
To delete an organizational unit from the list, select it and then click on **Delete OU** in the **Organizational Units** section in the left pane (or press the ✖ button).

Settings

Settings - Common Options

The bt-LogAnalyzer application allows you to determine the location for report and Control List storage.

URL Control List Storage - This is the location on the network or server of the STORAGE.XML file. This file contains the category information. The default file location is:

C:\Program Files\Burstek\Shared\Storage.xml

User Information

When you purchase the product, the bt-LogAnalyzer program requires that you enter a name and license key.

1. Enter the name.
2. Enter the license key.

NOTE:
The name and license key will be provided by Burstek.

3. After you have entered the user information, click the **"Check"** button to ensure that you have a valid name and license key. (If the user information is invalid, contact Burstek.)

4. If you have a valid name and license key, click the **"OK"** button to apply these options.

Settings – Category Groups

Category groups are primarily used to help condense and clarify report data into risk potential for the organization. For example, when viewing a Risk Assessment report, all Websites are first broken into contextual categories (URL Control List Categories). These categories are then sorted into seven Category Groups for:

Corporate Intranet - Websites that are part of the organization's intranet**.**

Job Search – Websites related to job hunting resources

Legal Liability - Websites that can potentially pose a legal liability to an organization (e.g.: XXX or Gambling sites).

Non-Business - General sites that are not actively related to work (e.g.: entertainment sites).

Security Risk - Websites that contain content that can be potentially damaging to company or its equipment (e.g.: Spyware, Viruses, Illegal File Sharing/P2P).

Social Networking – Websites promoting social interaction

Streaming Media - On-line movie delivery sites

To Add a Category Group:

1. Click New Category Group in the Category Groups section in the left pane. The **CATEGORY GROUP PROPERTIES** page displays.
2. Follow instructions on the **CATEGORY GROUP PROPERTIES** page.

To Make Changes to a Category Group:

1. Select a category group from the Category Groups List.
2. Click Category Group Properties in the Category Groups section in the left pane, or the ▤ button. The **CATEGORY GROUP PROPERTIES** page displays.
3. Follow instructions on the **CATEGORY GROUP PROPERTIES** page.

To Delete a Category Group:

1. In the Category Groups List, click on the category group you wish to delete and then click Delete category group in the Category Groups section in the left pane, or press the ✖ button.
2. Press OK to confirm.
3. The category group will disappear from the list. Click "OK" to save your changes.

Settings – Category Group Properties

Define category group properties:

1. Give the new category group a name and enter a description if desired.
2. From the **Category Group Content** box, check off the content you wish to include in your new group. Only content not used in another category will appear as available.
3. Click “**OK**” to save your new category group.

Settings – Email Options

The bt-LogAnalyzer program Email Options tab allows you to set up parameters to enable report Emailing.

NOTE:

The MS Exchange server field is responsible for login-to-Email and back translation. bt-LogAnalyzer uses this translation in Email reports to get user logins based on their Emails and vice versa. Leave the MS Exchange server field blank if you are using Active Directory.

1. Enter the Email address.
2. Enter the name of the SMTP server (IP address or DNS). This is the mail server the bt-LogAnalyzer will use to Email reports.
3. Click “OK” to set these options.

Email Domains - Enter your organization’s Email domain(s) to help distinguish between inbound or outbound Emails.

To Add Email Domains:

1. Click the New Email Domain option in the Email Domain section in the left pane.
2. After entering the domain properties, press OK to save the changes.

To Edit an Email Domain Properties:

1. Select an Email domain from the list under Email Domains.
2. Click the Email Domain properties option in the Email Domain section in the left pane, or the button.
3. When done with editing the properties, press “OK” to save the changes.

To Delete an E-mail Domain

1. Select an Email domain from the list under Email Domains.
2. Click the Delete Email Domain option in the Email Domain section in the left pane, or the ✖ button.
3. Press OK to confirm.

Settings - Factors

Bandwidth Cost Factor

The bt-LogAnalyzer program allows you to calculate the cost of Internet and Email bandwidth use. Bandwidth Cost is used to calculate report information such as Cost by Category, Cost by Top Users, Hourly Cost, Top User Cost by Individual Category and Email Volume.

1. Type in the Bandwidth Cost Factor and its currency sign.

> **NOTE:**
>
> Eight decimal places are available to the Bandwidth Cost Factor for more accurate cost estimating. The default Bandwidth Cost Factor is calculated at the United States rate of ***$.001500 per Kilobyte*** and the default Currency Sign is the United States “***$***” sign. The cost factor and currency sign can be changed to accommodate Bandwidth Cost Factors and Currency Signs of Foreign Countries.

2. Enter the estimated Bandwidth Cost Factor for your country and the appropriate currency symbol.
3. Click **“OK”** to apply these changes.
4. Reports that calculate Bandwidth Costs will be calculated with the new rate and display the Currency Sign entered.

> **NOTE:**
>
> If you wish prevent the Bandwidth Cost from appearing on your reports, simply change the Bandwidth Cost Factor to zero (0). After doing this, the report column for Bandwidth Cost will disappear from all reports.

Viewing Time Factor

The Viewing Time Factor is calculated by applying the Minimum Time Factor to the number of Web Pages accessed. The default Minimum Time Factor is 10 seconds. When a report is compiled, bt-LogAnalyzer uses this factor to show you the approximate amount of time a user, group of users, or your whole organization spends online browsing the Internet.

1. Enter the Minimum Time Factor
2. Click **“OK”** to apply the change.
3. Viewing Time will be calculated with the new minimum time factor.

> **NOTE:**
>
> If you wish to prevent the Viewing Time Factor from appearing on your reports, change the Minimum Viewing Time Factor to zero (0). After doing this, the Viewing Time column will disappear from all reports.

> **NOTE:**
>
> Both the Viewing Time and Download Time display in reports in the following format: Days:Hours:Minutes:Seconds

Settings – Pseudo-Categories

Pseudo Categories are used to track information contained in Websites that is not directly related to the Website or information in a Website that may not be pertinent to you. For example, if you visit a hunting and fishing site and they have a banner ad for an assault rifle, the banner ad could be tracked in a pseudo category such as multimedia or banner ads. It will not appear as a visit in the Weapons Category. You can define a list of pseudo-categories for report generation and you can add, change or delete Pseudo-categories.

To add a Pseudo-category:

1. Click **New Pseudo-Category** in the **Pseudo-Categories** section in the left pane.
2. Follow the instructions on the PSEUDO-CATEGORY PROPERTIES page that appears.

To Change a Pseudo-category

1. From the **Pseudo-Categories** tab, select the pseudo-category you wish to change.
2. Click **Pseudo-Category Properties** in the **Pseudo-Categories** section in the left pane, or press the ▤ button of the pseudo-category.
3. Follow the instructions on the PSEUDO-CATEGORY PROPERTIES page that appears.

To Delete a Pseudo-Category

1. From the **Pseudo-Categories** tab, select the pseudo-category you wish to delete and click **Delete Pseudo-Category** in the **Pseudo-Categories** section in the left pane, or press the ✖button of the pseudo-category.
2. Press **OK** to confirm.

Settings – Pseudo-Category Properties

To Add a New Pseudo-Category Mask

1. Enter the pseudo-category name.
2. Type a description of the type of information contained in the pseudo-category.
3. Click **New** Pseudo-**Mask** in the **Pseudo-Category** section in the left pane, or the **New Pseudo-Mask** link on the page, to specify a list of pseudo-category elements. Element types can be a file extension, a MIME type, a URL mask, or a bt-WebFilter Category.
4. Follow the instructions on the PSEUDO-MASK PROPERTIES page. Once you have added all of the pseudo mask properties, click “**OK**” to add the pseudo-category to the list.

To Change a Pseudo-Category Content

1. Select a pseudo-mask under **Pseudo-Category Content**.
2. Click Pseudo**-Mask Properties** in the **Pseudo-Category** section in the left pane, or press the ▤button. Follow the instructions of the PSEUDO-MASK PROPERTIES page.

To Delete a Pseudo-Mask

1. Select a pseudo-mask under **Pseudo-Category Content**.
2. Click **Delete Pseudo-Mask** in the **Pseudo-Category** section in the left pane, or press the ✖button. Follow the instructions on the PSEUDO-MASK PROPERTIES page.

Settings – Pseudo-Mask Properties

Define pseudo-mask properties:

1. Click the radio button to specify the type of pseudo-category element you want to add.
2. From the drop down menu, select the **File Extension**, **MIME-type** or **bt-WebFilter Category**. If you selected a **URL mask**, enter the mask information.
3. Click "**OK**" to add the pseudo mask.

Settings – Distributed Reports

Distributed Report Processing feature allows bt-LogAnalyzer users to process reports on multiple machines and aggregate the processing into one report. This feature provides the following benefits:

- Multiple servers can run reports against their own logs. This distributes the time taken to generate reports lowering Network Bandwidth.
- Reports can be run more frequently, again reducing the length of time required to produce final reports.
- Only the summary of the report is sent back by the Remote Server to the Virtual Report Server reducing Network Bandwidth.
- Distributed Report Processing feature provides a transparent ("LAN-like") communications over Local Area Networks and Virtual Private Networks.
- Replicate your customized URL Control List out to all your Remote LogAnalyzer servers in your organization.

For example, you may wish to create an Enterprise Summary report for your organization that is comprised of multiple locations, you can use distributed reporting to have each site's server generate its own portion of the report and submit it to the primary server for compilation. You can even have bt-LogAnalyzer send an Email notification when the report is done compiling!

Prior to using the Distributed Report Processing feature, bt-LogAnalyzer needs to be installed on the Remote Report Server (the server that will process the summary submitted by the Remote server into one report) and on all the Remote servers. Each server will also need to have their Log Sources defined.

Remote Report Server Setup

1. Add the names of your remote servers where bt-LogAnalyzer is installed. To do this, click New Distributed Server in the Distributed Server section in the left pane.

> **NOTE:**
> The Distributed Report Processing Timeout defaults to 60 minutes. If the primary bt-LogAnalyzer server is unable to reach the remote server in 60 minutes, it will stop attempting to reach that server and will complete the requested report without the information provided by that server.

2. Select URL Control List replication mode: automatic replication or manual replication.
3. If you selected Manual replication, press Replicate to push the Control List onto the remote servers.
4. Click "OK" to save your settings.

> **NOTE:**
> To setup a report for distributed processing, check the Run this report at remote servers box on the Advanced tab of this report properties (see the REPORT PROPERTIES – ADVANCED page).

Settings - Security

Select an organizational unit:

1. Specify the domain you wish to add organizational units from. Type in your user name and password to log on to the domain, and press Login. The organizational units of the domain will be listed under Organizational Units

   > **NOTE:**
   > By default, this section lists organizational units of the domain you are currently logged on to.

2. Select organizational units you wish to add by checking their boxes. If, when you expand the unit, you wish to display its users and select from them, check the Show Users box. Select individual users, if necessary.
3. Press the “OK” button.

Settings - Colors

The Colors tab allows you to define color settings used for report generation. The following are the default colors: blue for all categories that are directly related to your business, green for all categories that are acceptable, yellow for categories that are non-productive and red for categories that are unacceptable.

🟩 Local, Intranet and categories defined by user

🟨 Non-productive (non business related)

🟥 Unacceptable (sites that pose a potential risk for your organization)

By default, the page displays the full list of categories. When a category is added to the URL Control List, it appears automatically on the Colors list with the default color.

To Set the Default Color

To set the color to be assigned automatically to newly added categories, use the Select button next to Default color.

To Set/Change the Category Color Properties

1. Select a category from the list. To navigate the list, use the page links at the bottom of the page.
2. Click Select Color in the Colors section in the left pane, or press the category’s 🗒 button to view the color chart. Follow the instruction on the SELECT COLOR page.

To Set the Category Color to Default Value

1. Select a category from the list. To navigate the list, use the page links at the bottom of the page.
2. Click Set Default Color in the Colors section in the left pane, or press the category's ✖button. Follow the instruction on the SELECT COLOR page.
3. To save the changes, click "OK".

Settings - Database

bt-LogAnalyzer use three separate databases. The database page will display the relevant information regarding the database file size and free space. The three databases are:

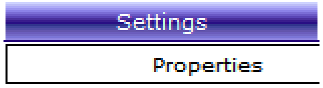
1. LAEE_Data – Contains all data imported from the log sources
2. LAEE_Reports – Once a report is generated, the results are stored here for quick access
3. LAEE_Settings – Contains all configuration information.

Settings - Custom Log Format

bt-LogAnalyzer SE^{TM} v.1.61 now has the ability to configure custom log formats, allowing users to report on log file formats not previously included in the software. To utilize this feature, the custom log format must first be defined and tested to ensure proper log file field mapping.

To define a custom log format:

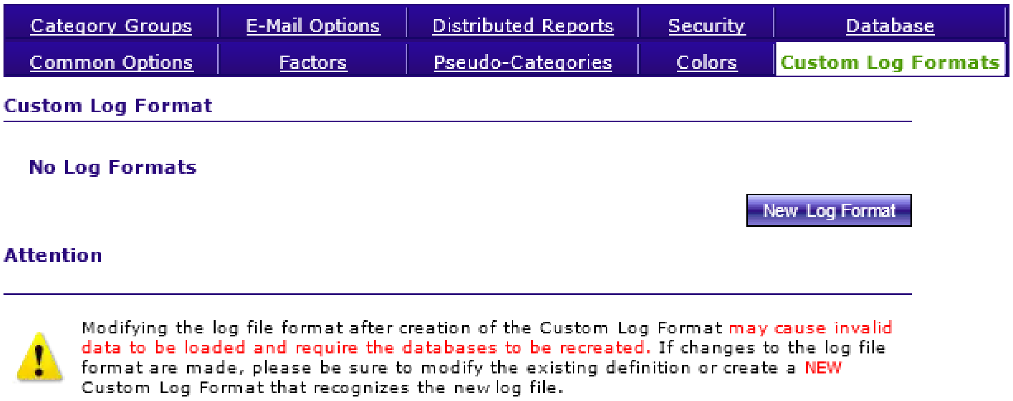
1. Navigate to the **Settings | Properties** menu item in the bt-LogAnalyzer SE^{TM} user web interface.



Settings Properties Selection

2. Select the **Custom Log Formats** tab.

NOTE:
It is important to understand that either modifying the log file format which uses the custom log format, or modifying the custom log format mapping after data has been loaded can cause invalid data to be loaded into the LogAnalyzer databases.

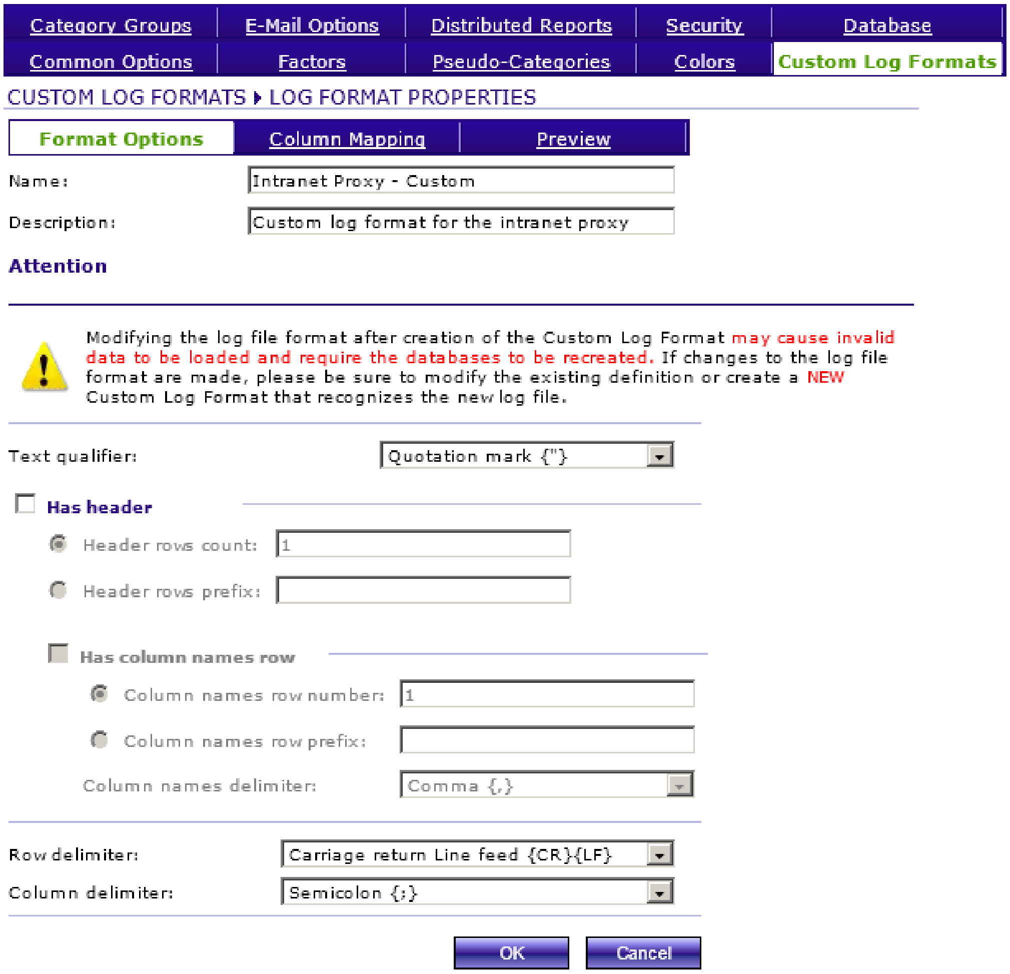


No Log Formats

Modifying the log file format after creation of the Custom Log Format may cause invalid data to be loaded and require the databases to be recreated. If changes to the log file format are made, please be sure to modify the existing definition or create a NEW Custom Log Format that recognizes the new log file.

Custom Log Format option

3. Select the **New Log Format** button to configure and create your new custom log format.



Name: Intranet Proxy - Custom

Description: Custom log format for the intranet proxy

Modifying the log file format after creation of the Custom Log Format may cause invalid data to be loaded and require the databases to be recreated. If changes to the log file format are made, please be sure to modify the existing definition or create a NEW Custom Log Format that recognizes the new log file.

Text qualifier: Quotation mark {"}

☐ Has header

● Header rows count: 1

○ Header rows prefix:

☐ Has column names row

● Column names row number: 1

○ Column names row prefix:

Column names delimiter: Comma {,}

Row delimiter: Carriage return Line feed {CR}{LF}

Column delimiter: Semicolon {;}

Custom Log Format – Format Options Page

4. Name and describe the new custom log source as desired, then configure the options needed: (See descriptions below)
   - **Text qualifier:** The text qualifier is used as a string parameter to wrap text containing special characters that can be otherwise treated as delimiters.
     Example, if no text qualifier is specified for a custom log source which uses a comma (,) as a column delimiter, then the following record may not be loaded as desired:

     127.0.0.1, 2012-05-05, "Lorem ipsum dolor sit amet, consectetur adipiscing elit."

     Result without a text qualifier specified:

127.0.0.1	2012-05-05	"Lorem ipsum dolor sit amet	consectetur adipiscing elit."

     Result with a text qualifier specified as quotation marks ("):

127.0.0.1	2012-05-05	Lorem ipsum dolor sit amet, consectetur adipiscing elit.

   - **Has header** – (check box) – Select this option if the log files contain header information
     - **Header rows count** - (option) – number of rows before first log entry in file.
     - **Header rows prefix** - (option) – alternative to **Header rows count:** parameter. Instead of determining header rows by a preset number, header rows are determined by a prefix. Row will be identified as a header row if prefixed with the configured string sequence.
   - **Has column names row** – (check box): If applicable, LASE will be able to automatically detect column meanings by their names.
     - **Column names row number** - (option) – numeric value. LASE assumes that row with number defined by this parameter (default is 1), contains delimited column names. User must specify column meanings in **Column Mapping** tab (by using the auto-mapping feature, or manually).
     - **Column names row prefix** - (option) – alternative to **Column names row number:** parameter, instead of finding column names row by row number, LASE will try to find row that starts with string value of this parameter and read the rest of the row as column names. Example value - "**#** Fields: "
     - **Column names delimiter** – String parameter which specifies which delimiter will be used to separate column names in header row. Available options are:
       - Semicolon {;}
       - Colon {:}
       - Comma {,}
       - Tab {t}
       - Space {s}
       - Vertical Bar {|}
   - **Row delimiter -** determine which symbol is used to split rows in log file. Available options are:
     - {CR}{LF}
     - {CR}
     - {LF}
   - **Column delimiter** – determine which symbol is used to split columns in log file. Available options are:
     - Semicolon {;}
     - Colon {:}
     - Comma {,}
     - Tab {t}
     - Space {s}

    - Vertical Bar {|}

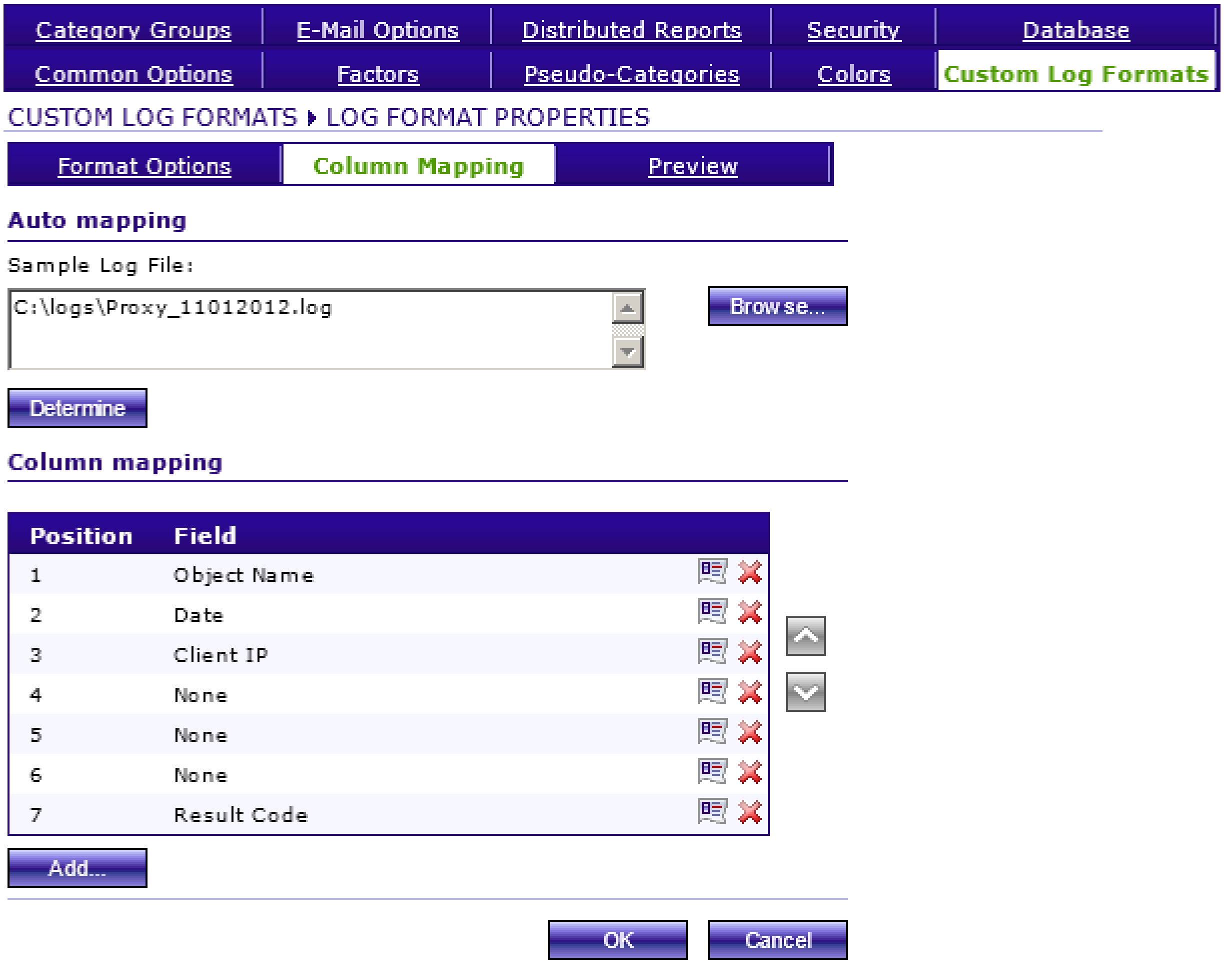
5. Once the **Format Options** tab has been configured, select the **Column Mapping** tab and configure the correct column mapping for the custom log format.
    - If the **Has header** and **Has column names row** checkboxes were selected on the **Format Options** tab, then the **Auto mapping** feature will be available. This feature allows a user to have LogAnalyzer automatically suggest the column types by testing a valid log data file.
        - Included below, is a table listing header column names which will auto-map to their respective fields in LASE:

- **Column name in log data file header**	**Field in LASE**
ClientIP, src_ip, %Ses->client.ip%, src, c-ip	Client IP
ClientUserName, src_user, %Req->vars.pauth-user%, user, usr, cs-username	Client username
logDate, date	Date
logTime, time	Time
GmtLogTime, [%SYSDATE%]	Date and time
Processingtime, %Req->vars.xfer-time%, time-taken	Processing time
Bytessent, sent_bytes, %Req->vars.p2r-cl%, sent, cs-bytes	Bytes sent
Bytesrecvd, rcvd_bytes, %Req->vars.p2c-cl%, %Req->headers.content-length%, %Req->vars.r2p-cl%, rcvd, sc-bytes	Bytes received
protocol, proto, cs-protocol	Protocol name
Operation, s-operation	Operation name
uri, %Req->reqpb.uri%, cs-uri, cs-url	Object name
"%Req->reqpb.proxy-request%"	Proxy request
mimetype, cs-mime-type	Object mime
Resultcode, rc, %Req->srvhdrs.clf-status%, result, sc-http-status, sc-status	Result code
s-hostname, cs-host, dstname	Uri host
cs-uri-stem	Uri stem
cs-uri-path	Uri path
cs-uri-query, arg	Uri query
cs-uri-scheme	Uri scheme

NOTE:

The **Object name** Field is synonymous with **URL**, which is a valid field in LASE. **URL** is not included in the above table because there is no auto-mapping pointer for this field. Assuming the correct header column name, the **Object name** LASE field would be mapped for a column containing a full URL.

- **To run the auto mapping feature:**
  1. Select the log file to be tested by clicking the **Browse…** button, then selecting the desired file, and clicking **OK**.
  2. Once the sample log file has been selected, click the **Determine** button. The Column mapping section should then display the resulting columns of the auto map feature.



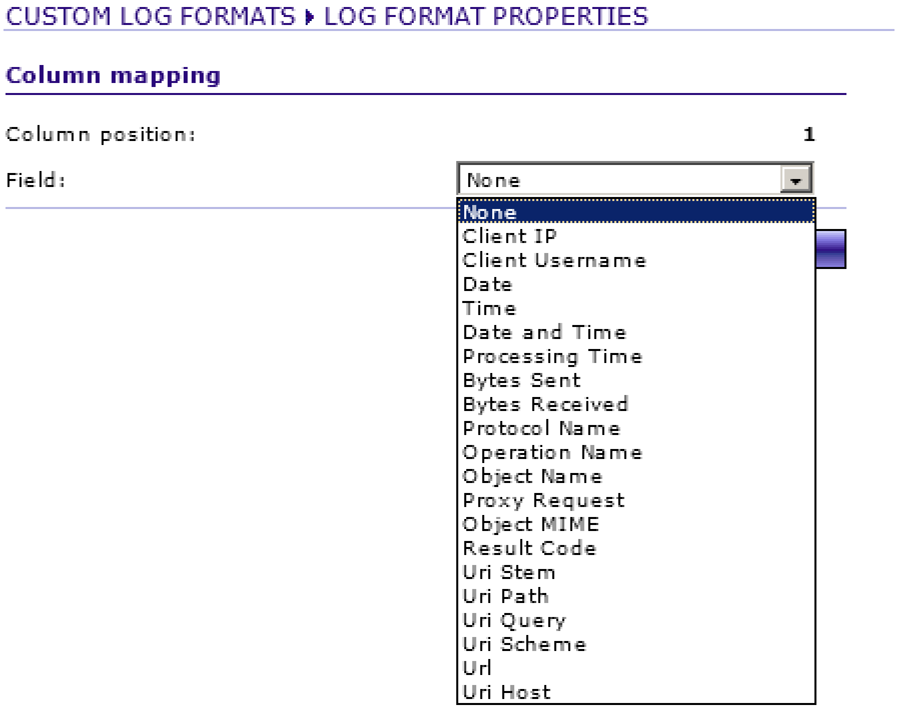
Sample Log File: C:\logs\Proxy_11012012.log

Position	Field
1	Object Name
2	Date
3	Client IP
4	None
5	None
6	None
7	Result Code

Custom Log Formats – Column Mapping Page

NOTE:
The auto-mapping results can be modified by manually configuring the column mapping after the auto-map feature has been used.

- If the Auto-mapping feature will not be used, the log file columns can be manually configured. **To manually configure the column mapping:**
  1. Click the **Add…** button, located under the **Column mapping** section.



CUSTOM LOG FORMATS ▸ LOG FORMAT PROPERTIES

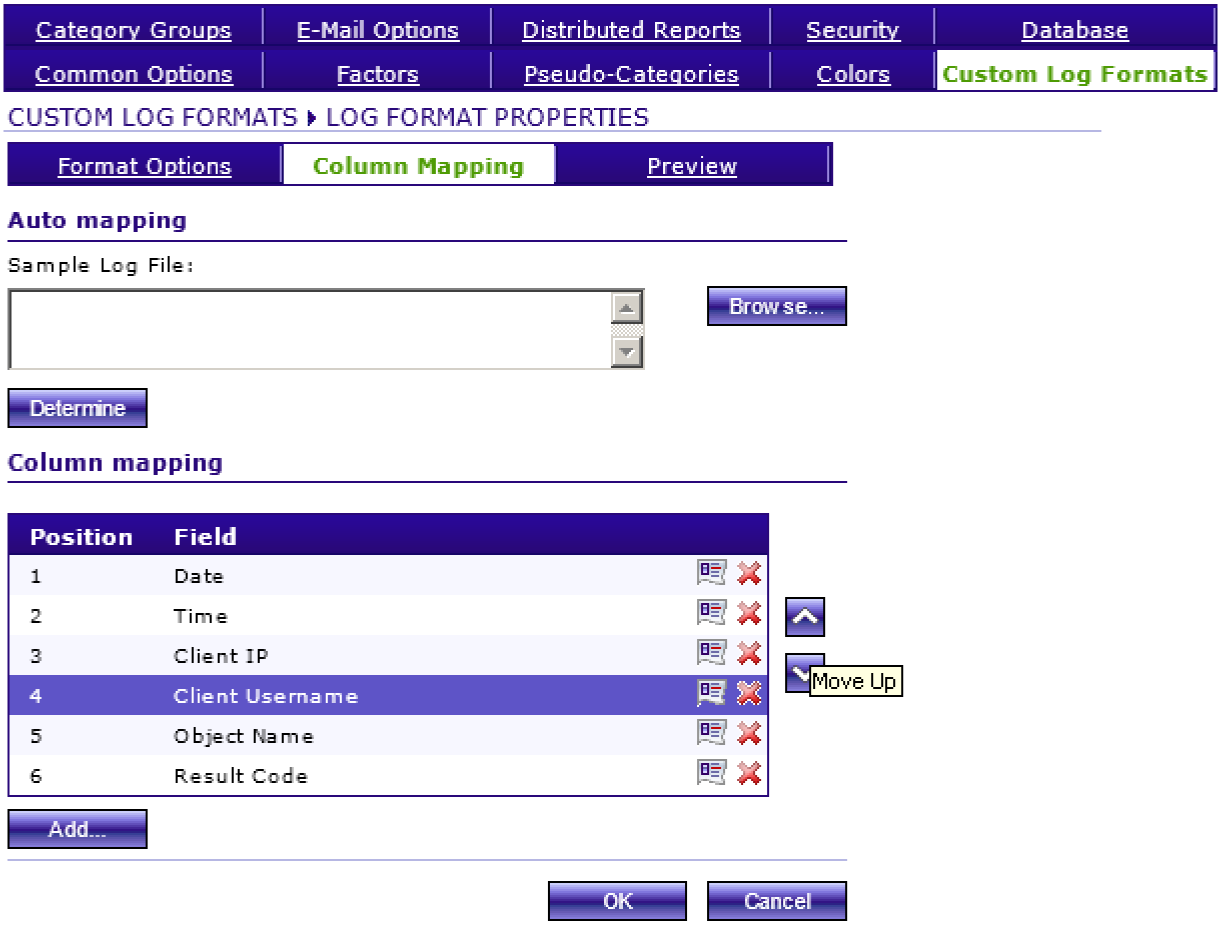
Column mapping

Column position: 1

Field: None

Custom Log Formats – Column Mapping Drop Down List

1. Select the necessary column type which is included in the log file, then click **OK**.
2. Add the additional columns until all log file columns have been added to the **Column mapping** section.
3. The position of the column mapping can be changed by selecting the desired column item, then clicking the **Move Up** or **Move Down** arrow buttons.



Position	Field
1	Date
2	Time
3	Client IP
4	Client Username
5	Object Name
6	Result Code

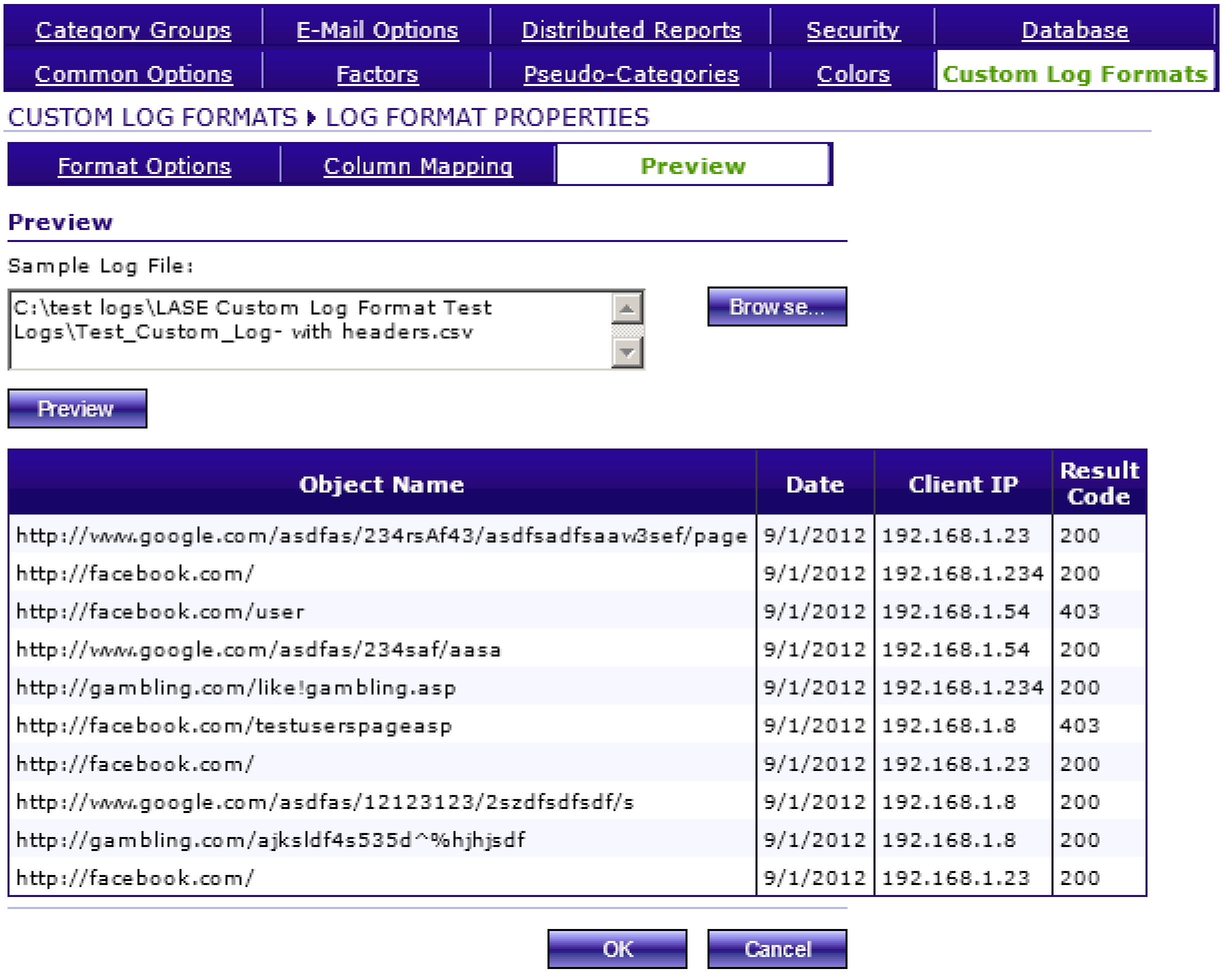
Custom Log Formats – Column Mapping Example

NOTE:

There are 4-6 required fields for any log file (excluding Exchange logs) that LogAnalyzer can successfully report on. The minimum required fields (no particular order is necessary) are included below:

- **Client IP**
- **Date and Time** OR
    a. **Date** AND **Time** (if date and time not combined into a single field, then two separate fields are required for accurate reporting).
- **Result Code**
- **URL** (or **ObjectName**) OR
    a. **UriHost** AND **UriPath** AND **UriQuery** OR
    b. **UriScheme** AND **UriStem** AND **UriQuery**

6. Once the column mapping has been configured for the custom log file format, navigate to the **Preview** tab to ensure proper log format configuration. **To test your custom log format against the newly-configured custom log format:**
    1. Select your log file by using the **Browse…** button, then click **OK**.
    2. Once the desired log file has been selected, click the **Preview** button.



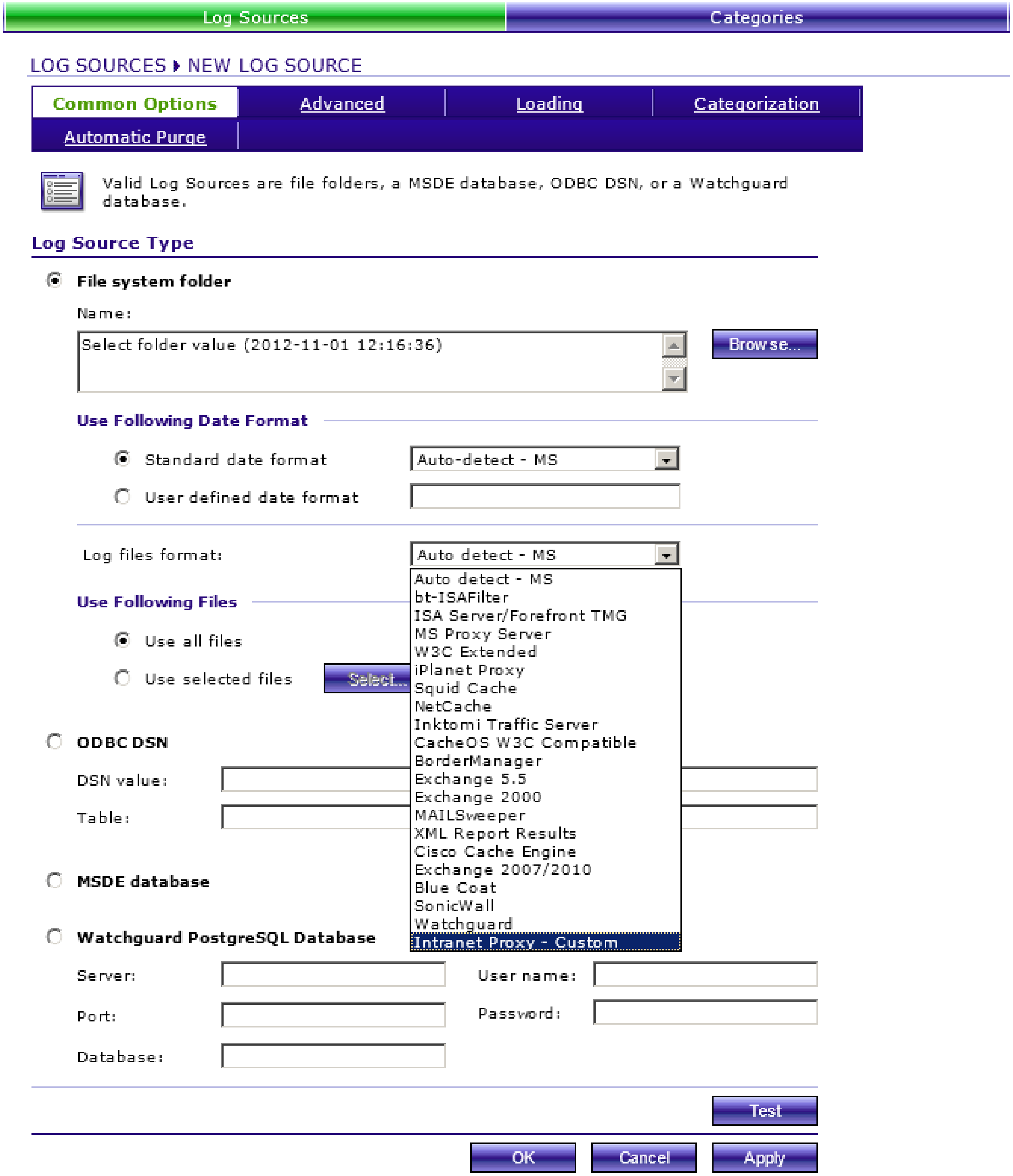
Sample Log File: C:\test logs\LASE Custom Log Format Test Logs\Test_Custom_Log- with headers.csv

Object Name	Date	Client IP	Result Code
http://www.google.com/asdfas/234rsAf43/asdfsadfsaaw3sef/page	9/1/2012	192.168.1.23	200
http://facebook.com/	9/1/2012	192.168.1.234	200
http://facebook.com/user	9/1/2012	192.168.1.54	403
http://www.google.com/asdfas/234saf/aasa	9/1/2012	192.168.1.54	200
http://gambling.com/like!gambling.asp	9/1/2012	192.168.1.234	200
http://facebook.com/testuserspageasp	9/1/2012	192.168.1.8	403
http://facebook.com/	9/1/2012	192.168.1.23	200
http://www.google.com/asdfas/12123123/2szdfsdfsdf/s	9/1/2012	192.168.1.8	200
http://gambling.com/ajksldf4s535d^%hjhjsdf	9/1/2012	192.168.1.8	200
http://facebook.com/	9/1/2012	192.168.1.23	200

Custom Log Formats – Preview Option

3. Verify that the correct content is included in each column, and that the content is complete.
4. If the log file column data seems to be mapped correctly, click **OK** to save and close the custom log format properties page.

Once the Custom Log Format has been properly configured and tested, it can then be used as a log format for the related log source. The custom log format can be found in the **Log files format:** drop-down option of the log source properties page.



LOG SOURCES ▸ NEW LOG SOURCE

Valid Log Sources are file folders, a MSDE database, ODBC DSN, or a Watchguard database.

Log Source Type

● File system folder

Name:

Select folder value (2012-11-01 12:16:36)

Use Following Date Format

● Standard date format: Auto-detect - MS

○ User defined date format:

Log files format: Auto detect - MS

- Auto detect - MS
- bt-ISAFilter
- ISA Server/Forefront TMG
- MS Proxy Server
- W3C Extended
- iPlanet Proxy
- Squid Cache
- NetCache
- Inktomi Traffic Server
- CacheOS W3C Compatible
- BorderManager
- Exchange 5.5
- Exchange 2000
- MAILSweeper
- XML Report Results
- Cisco Cache Engine
- Exchange 2007/2010
- Blue Coat
- SonicWall
- Watchguard
- Intranet Proxy - Custom

Use Following Files

● Use all files

○ Use selected files

○ ODBC DSN

DSN value:

Table:

○ MSDE database

○ Watchguard PostgreSQL Database

Server:

User name:

Port:

Password:

Database:

Log Source Common Options – Selecting the new Custom Log Source