Event Log Gatherer User Guide Version 1.5

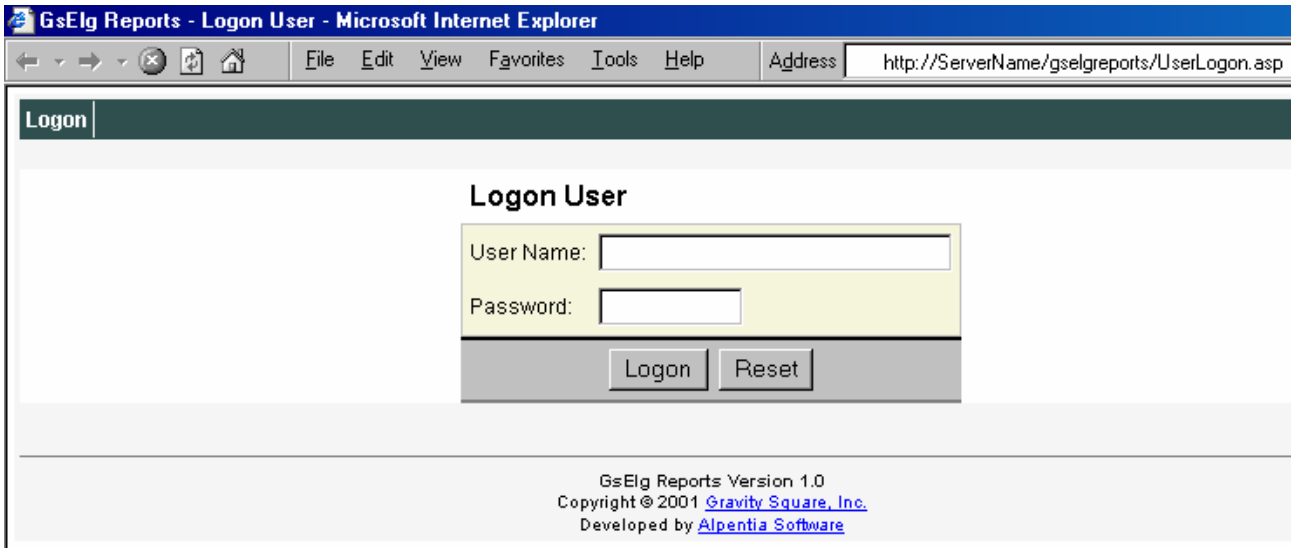
www.gravitysquare.com
info@gravitysquare.com

May 27, 2003

5041 46th Ave NE Seattle, WA 98105 **T** 206.669.8341 **F** 206.524.4159

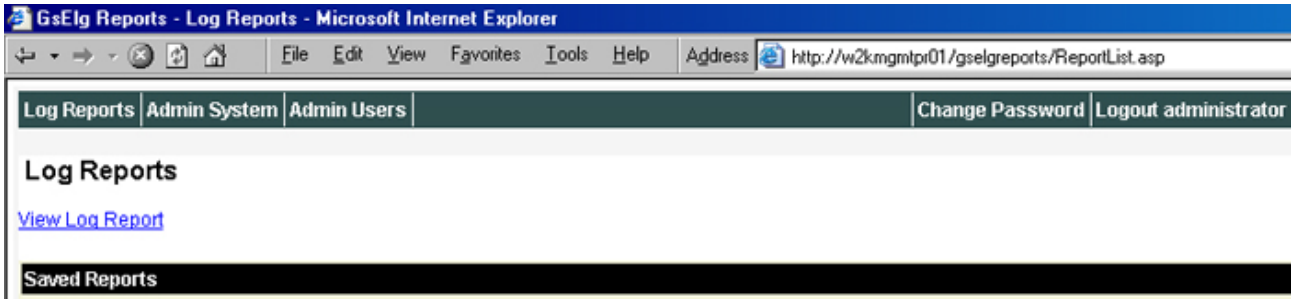
1.0 Logon

Open the web application by browsing to the logon URL: http://servername/gselgreportsweb/UserLogon.asp, and log on to the application.



When the GSIELG application is installed, the setup script creates a default user named 'Administrator', with password 'administrator'. Initially you must log on to the GSIELG application using this user name.

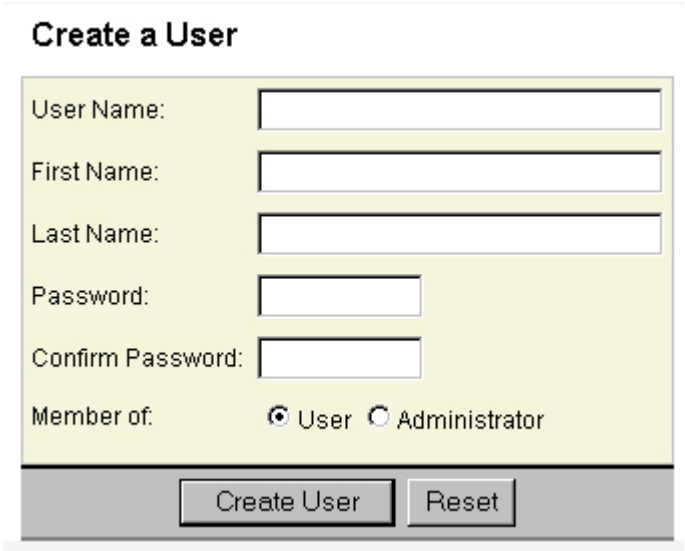
This is the main screen available upon logon:



2.0 User Administration

2.1 Creating User Logons

Users designated as GSIELG Administrators may create other user logons (other administrators or standard users). Once logged on, at the main screen select “Admin Users”, and then select “Create New User”.



Enter new user data as in the provided example:

Enter User Name:	JSmith	(this is the logon name)
Enter First Name:	John	
Enter Last Name:	Smith	
Enter Password:	**********	(this is the logon password)
Confirm Password:	**********	
Member of:		Select type of user: User or Administrator:

- Users can view event log reports only
- Administrators can view reports, add, reset, or delete other users, add servers to be monitored, set up event log record exclusions, and clear events from the database.

Select “Create User” button to create user
Select “Reset” button to clear all fields of the form

NOTE: The database stores logons and passwords in clear text. The passwords set for users in this application should not match their other passwords (for example domain or local system passwords).

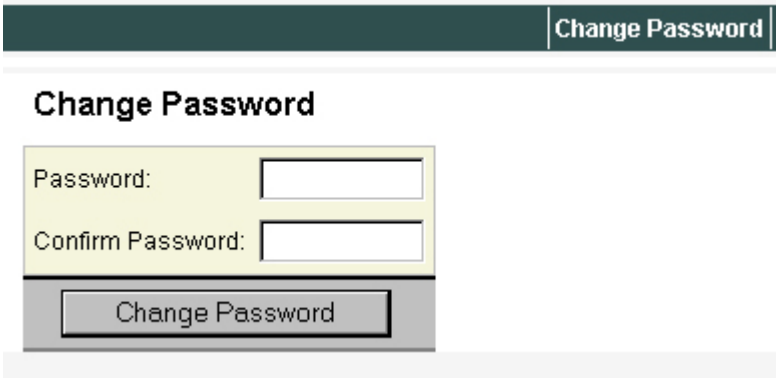
2.2 Updating Existing User Logon

Users designated as GSIELG Administrators may update existing user logons (other administrators or standard users). Once logged on under an administrator account, select “Admin Users” on the main screen, select the user to be updated, and select “Edit”. Modify user’s data and select ‘Update User’.

> **NOTE**: When editing the user logon data, select the ‘Reset’ button to reload the original data.

2.3 Changing Password

Once logged on, users and administrators may quickly change their password by selecting “Change Password” from the menu bar on the main page..



3.0 System Administration

Users designated as Administrators may manage the GSIELG application by creating, editing, and deleting other users (as described in sections above), by adding servers to be monitored by the GSIELG application, by excluding certain classes of events from being stored in the GSIELG database, and by clearing event log records from the database.

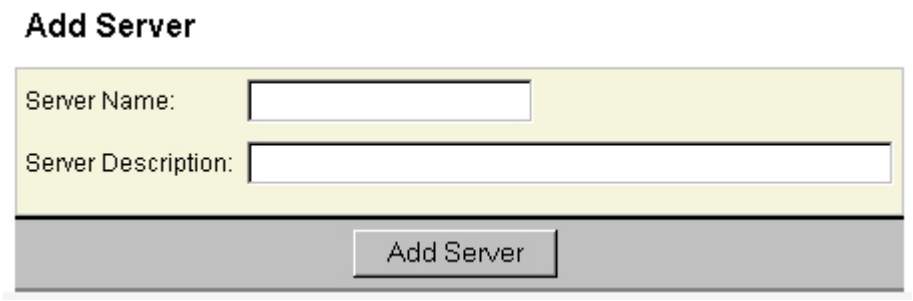
3.1 Monitored Servers Management

Once the database, COM+ application and Web components are setup, compatible Windows systems (servers) can be selected to have their event log records moved to and monitored by the GSIELG application.

Administrators can configure servers to be monitored by selecting the ‘Admin System’ option from the menu bar, and then selecting “Setup Server List’. All servers currently monitored by the GSIELG application will be displayed on this page, and administrators may add new servers to the list or remove servers from the application’s configuration.

3.1.1 Adding Server

To add a server to the list of monitored servers, select the 'Add a Server' link. This displays the 'Add Server' page:

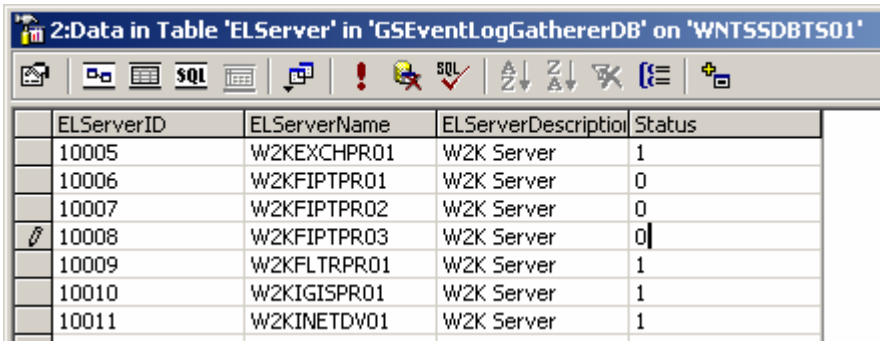


Enter the host name of the target server (enter only host name; no backslashes or FQDN), add a simple description of the server, and click 'Add Server'. This action will enter the server's name into the database and mark it as active. The GSIELG Service will pull events from this server into the database beginning with the next service cycle.

3.1.2 Removing Server

Administrators can remove servers from the application's monitoring be selecting "Setup Server List' page, locating the server to be removed, and clicking on its corresponding 'Remove' link. Servers that have been removed will no longer be monitored by GSIELG application and all corresponding event log records will be deleted from the database.

> **NOTE:** A server monitored by the GSIELG application is marked with a status of "1" in the database. Administrators may temporarily mark a server as inactive (exclude it from monitoring, but keep it and all of its event log records in the database) by manually editing the "status" field in the ELServer table of the GSEventLogGathererDB database. Change the status from 1 to 0 in the row where the server name corresponds to the target server. This is an advanced operation that requires table-wise write permissions, and should only be performed by administrators who are familiar with SQL Server.



	ELServerID	ELServerName	ELServerDescriptio	Status
	10005	W2KEXCHPR01	W2K Server	1
	10006	W2KFIPTPR01	W2K Server	0
	10007	W2KFIPTPR02	W2K Server	0
	10008	W2KFIPTPR03	W2K Server	0
	10009	W2KFLTRPR01	W2K Server	1
	10010	W2KIGISPR01	W2K Server	1
	10011	W2KINETDV01	W2K Server	1

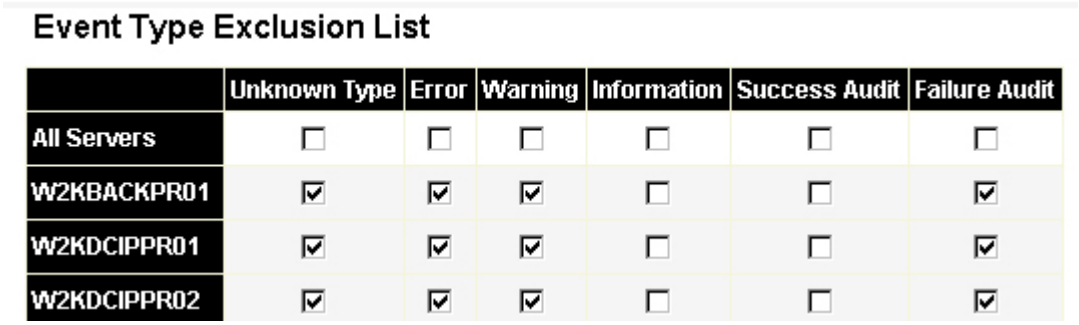
3.2 Event Exclusion Configuration

By default, the application will display the following event types for each server entered into the database:

Error
Warning
Information
Success Audit
Failure Audit
Unknown Type

Of these error types, Information and Success Audit can likely be excluded from the database repository. Inclusion of these error types, which are the most frequently generated, can cause the database to grow rapidly to several gigabytes in size, and can make the application less responsive and difficult to administer. These or other event types can be filtered from the event logs via configuration of the Event Type Exclusion List:

Select ‘Admin System’, and then ‘Setup Event Exclusion List’:



The row marked “All Servers” allows an administrator to make changes that will cascade throughout the list to all servers set up in the database. Servers may also be administered separately, so that only those event types required from each server are included in the database.

Make any changes required and then select the ‘Submit Changes’ button.

3.3 Clear Event Log Entries

Once event log entries or records are pulled from the monitored servers, they will remain in the database until manually cleared by a GSIELG administrator. In general, it is recommended to periodically clear older event log records and keep the database size small. Clearing the logs is done on a system-wide basis, rather than server-by-server.

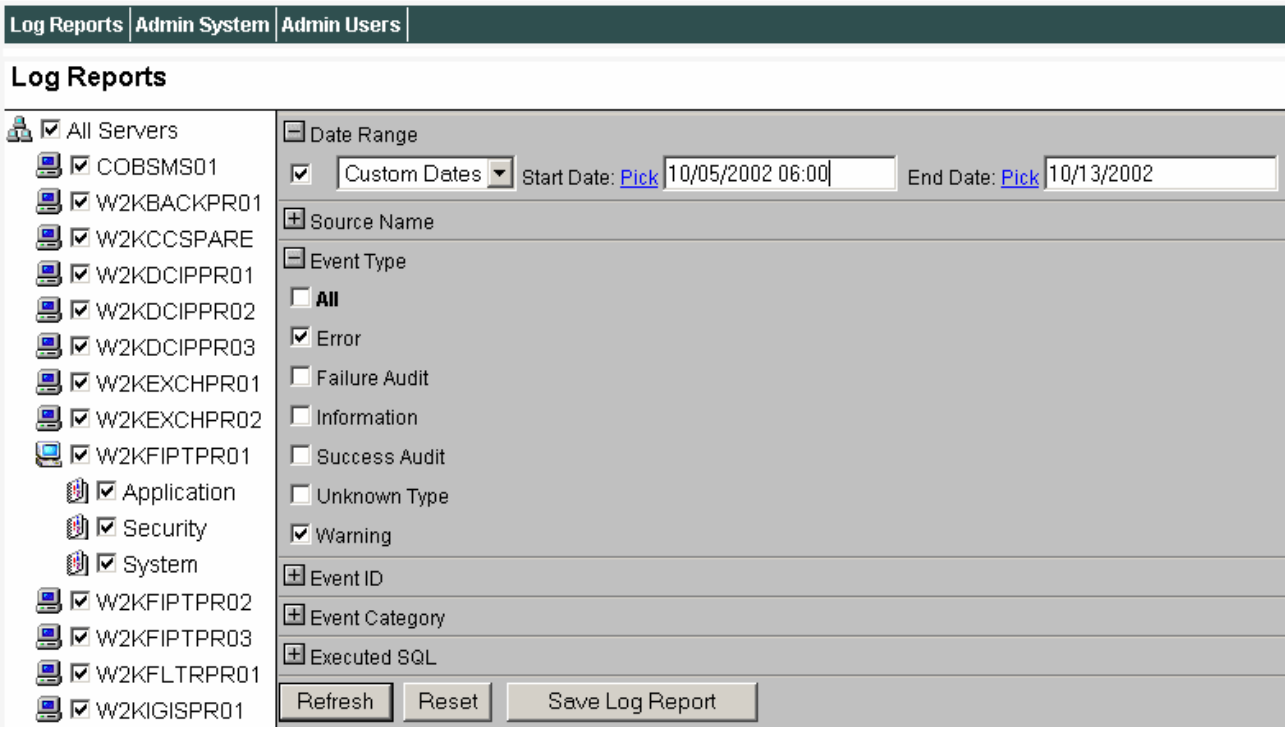
Select ‘Admin System’, and then ‘Clear Log Entries’:

This will remove permanently all database entries for all servers that are older than this date.

> **NOTE:** the database application permanently removes entries from server event logs once the server is set up in the database. Clearing these log entries will remove them permanently, and in order to view them again, the database will have to be restored from backup.

4.0 Running Reports – Viewing Event Log Records

To view event log records pulled from the servers, set up in the GSIELG application, select the "View Log Reports" link from the Log Reports menu option.



In this window, the user may select the servers to view, based on several criteria:

All or Specific Servers

Event Log Type:

- Application
- Directory Service
- DNS Server
- File Replication Service
- Security
- System

Date Range:

- Custom Dates (user define date and time interval)
- Last Hour
- Today
- Last 24 Hours
- Last 7 Days
- This Month
- Last 30 Days

Source Name:

- Event Source Names vary based on services and applications running on each server.

Event Record Type:

- All
- Error
- Failure Audit
- Information
- Success Audit
- Unknown Type
- Warning

Event ID's:

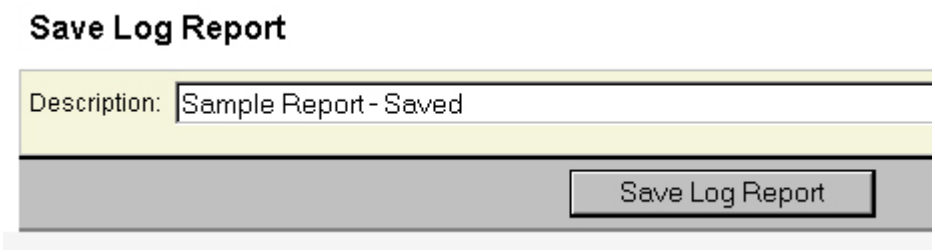
- Filtered events based on specific event ID (inclusion or exclusion)

Event Category:

- Event Categories vary based on services and applications running on each server.

4.1 Saving Event Log Reports

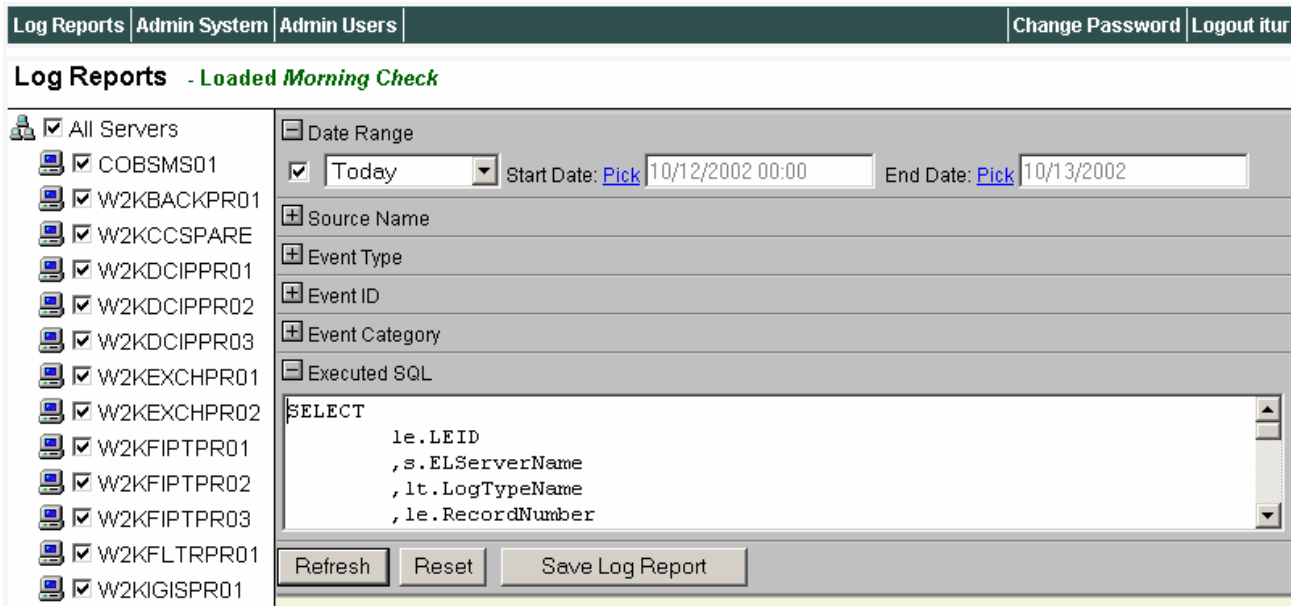
Reports based on specific criteria can be saved by using the “Save Log Report” button. This allows reports to be generated and displayed at a later time without requiring the user to select the parameters again.



Once these report queries are saved, they appear under “Saved Reports” on the main page, and are displayed immediately upon logon.

4.2 Report Query Export

GSIELG reports are build based on SQL queries and can be exported. Exported report queries can be copied directly from the Log Reports and executed directly from the SQL Query Analyzer, or any application capable of executing SQL queries against SQL or MSDE database. You can use this feature to export saved reports and, for example, provide them to other users of the GSIELG application or run them from within MS Access to print a report hardcopy.



5.0 Creating and Generating Alerts

5.1 Notification System Setup

For sending email notifications the ELG can use either SMTP or MAPI based SQL Mail services. Decide which email mechanism ELG will use and perform the following preparation steps:

1) SMTP
    a. Make sure that SMPT services are installed and enabled on the SQL Server workstation.
    b. Make sure your SMTP system is well secured and doesn't allow for mail relaying by unauthorized devices or users
    c. You can test the SMTP mail using steps provided in the following MS Knowledge Base article: http://support.microsoft.com/default.aspx?scid=kb;en-us;153119

2) MAPI based SQL Mail
    a. Follow the steps described in MSDN online article: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adminsql/ad_1_server_2ecs.asp

5.2 Notification Event Setup

The Event Log Gatherer (ELG) application can be configured to send email notifications of specific events, based on criteria defined by administrators. These criteria include:

- **Server**
    - All servers, group of servers, or a single server
- **Event Source**
    - All processes, group of processes, or a single process running on servers specified
- **Event Type**
    - All types, Error, Failure Audit, Information, Success Audit, Unknown Type, Warning
- **Event ID**
    - The specific numeric ID of an event
- **Event Category**
    - The category of event as defined on each server managed

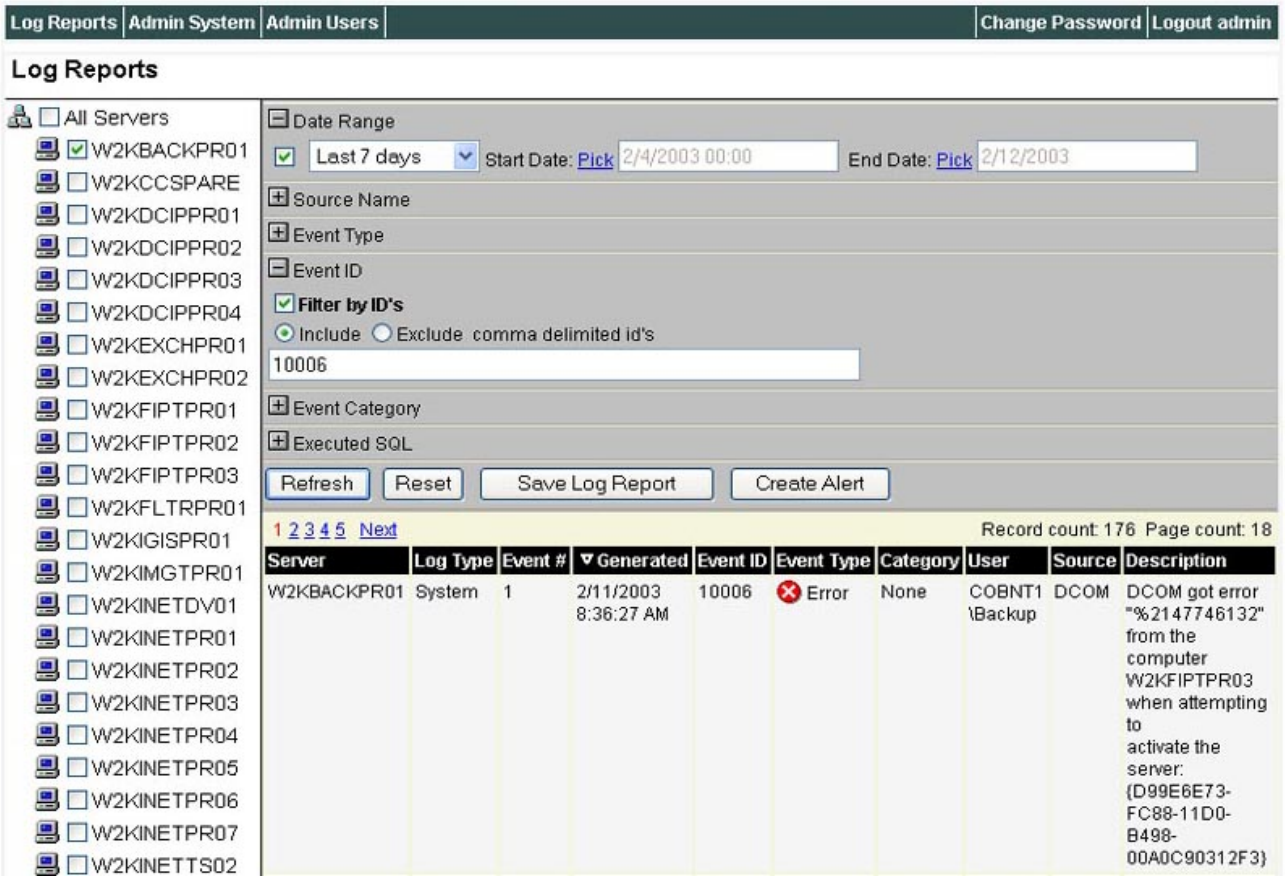
Administrators can use any combination of these criteria to receive email notifications of events. This can be done after creating a set of events on the Log Reports page, or by selecting the Admin System link and then selecting Alerts.

Alerts can be configured to be sent to multiple administrators and each administrator can receive alerts on an individual schedule. This allows a single alert to be defined on a specific event, and that alert will be sent to the administrator on duty at the time specified.

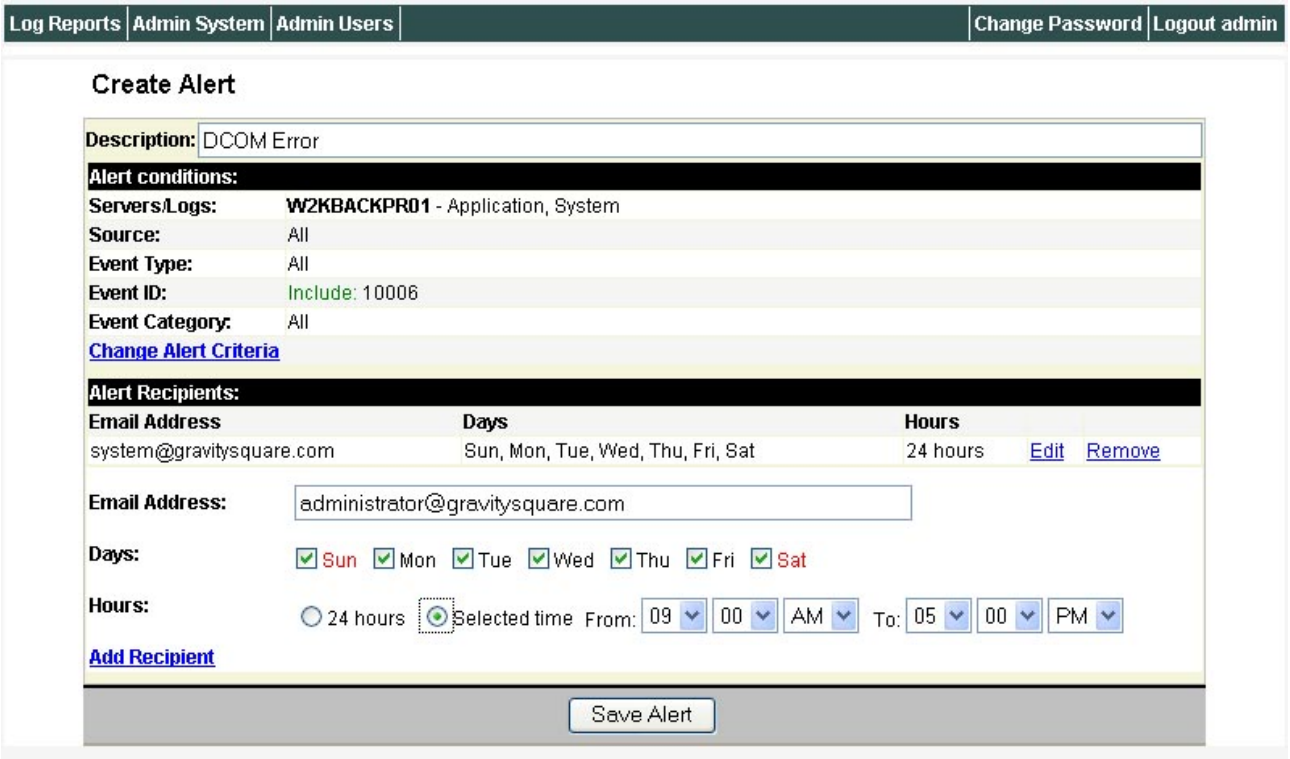
No limit to the number of alerts is defined in the system.

You can define the events which will trigger the alert generation and notification using the following steps:

- Open the application and log on using an administrator account.
- Select the Log Reports page, and then View Log Reports.
- Using graphical query building mechanism select events you want to trigger the alerting and notification e server for the test alert.



- Select Create Alert button.



- Once the Create Alert page is displayed, enter a name for the Alert.
- Within the Create Alert page, enter an email address for the recipient of the alert.
- Set the days of the week and the times during which emails should be delivered to the recipient. The default is 24/7.
- Select the Add Recipient link to enter the recipient information into the alert definition.
- Save Alert.

At this point the alert is defined. When the next collection cycle of the application includes the defined event ID from the defined server, the recipient included in the alert will receive email notification that the event was detected.

Multiple recipients may be defined for each alert, with specific times defined for each recipient.