CorreLog®

Global User Alert Plug-in Software

Users Manual

http://www.correlog.com   mailto:info@correlog.com

CorreLog, Global User Alert Plug-in User Manual

No part of this manual shall be reproduced without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibilities for errors or omissions. Nor is any liability assumed for damages resulting from the use of this information contained herein.

Table of Contents

Section 1: Introduction ………….. 5

Section 2: Software Installation ………….. 9

Section 3: Software Operation ………….. 13

Alphabetical Index ………….. 21

Section 1: Introduction

This manual provides a detailed description of the CorreLog Global User Alert Plug-in software. This is an optional set of files and executables added to the CorreLog Server to provide special alerting of users, in direct support of user anomaly detection and certain security requirements.

The manual provides information on installation and usage of this software, as well as a detailed description of screens, and certain features not documented elsewhere within the CorreLog manual set.

The Global User Alert Monitor software consists of a new screen that is added to the system, located in the "Alerts > Users" tab. This new screen provides special capabilities to apply a single threshold / match pattern across a range of users. Although this capability already exists in CorreLog (within the existing Correlation and Alerts tabs) the Global User Alert Monitor can often simplify the alerting process, and create a more visible indication of the user-centric alerts that may be necessary to monitor system security. In particular, this screen may be useful in demonstrating to auditors that CorreLog is configured to satisfy certain PCI-DSS and other security requirements.

This manual is intended for CorreLog users who will operate the system, as well as system administrators responsible for installing the software components. This information will also be of interest to program developers and administrators who want to extend the range of the CorreLog system's role within an enterprise to include special user management.

Background Information

It is important to note, before discussing the Global User Alert functions herein, that CorreLog contains special elements to detect anomalous user behavior. These elements are entirely sufficient to manage insider threats and other security violations. Therefore, the Global User Alert functions are not strictly required to manage security, and exist mainly to simplify the alerting process.

Without the Global User Alert function herein, CorreLog manages anomalous user behavior by capturing specific classes of information via its "Correlation Threads" capability, and then monitoring the counts of these message over a user defined interval. This permits full visibility of anomalous behavior based upon classes of users and messages.

For example, CorreLog can monitor the "Invalid Login" message rate for a particular group of users, and when the rate changes beyond its normal limits, CorreLog can raise an alert and open a ticket. Likewise, CorreLog can monitor other aspects of user behavior (such as login rates, process startups, USB insertions, file modifications, etc.) and compare that behavior to a threshold for the class of users. The actual threshold can be determined automatically based upon past message rates via the CorreLog "Auto-Learning" function.

Standard Threads and Alerts

For a large enterprise, standard "Correlation Threads" can be created for specific classes of users. Given that the CorreLog operator can identify a message class with a fairly fixed and limited amount of deviation (such as "UNIX Admin Logon Failures", or "Windows USB Insertions") the operator simply creates a thread to capture these messages, sets an alert on the thread counter rate, and then permits the system to "auto-learn" the threshold for that class of messages.

Note that the actual number of users and messages represented by a thread can be quite large. A class of messages can represent millions of messages and thousands of different users, and still accurately detect anomalies for any user, as long as the standard deviation of the message rate is small. This is somewhat counter-intuitive to users who may not realize that the number messages received and the actual message rate is unimportant. Anomalous behavior is detected through the "deviation" in message rate, and not the magnitude of the message rate.

Best detection occurs when similar users are compared. For example, one might expect the behavior of UNIX administrators to be different from network router administrators or ordinary Windows users. Creating appropriate threads and alerts provide a complete solution for an enterprise. However, this can also result in large numbers of Correlation Threads (and alerts) based upon the many different classes of users and message types that may be received by CorreLog.

Global User Alerts: Benefits and Limitations

The Global User Alert function can reduce the number of threads on the system by specifically targeting classes of users and messages with a single configuration alert and threshold that is applied across all users. Subsequently, if any user within that class exceeds the threshold, that user is identified as anomalous.

The main benefit to using the Global User Alert function is that each user, within a specified class of users (or all users on the system), is individually tracked using one single alert threshold and match pattern. This provides a fairly obvious indication of what users are being tracked at any given time, and how close to the specified threshold each individual user may be.

The main limitation to using Global Alerts is that it fails to identify attacks that are being launched under different user identities. For example, while the Global User Alert function can easily identify a brute force attack using multiple passwords, it cannot identify an attack using multiple user names. This limitation does not exist with the standard Correlation Thread / Alert combinations discussed earlier.

This is an important caveat that must be considered before installing and relying too heavily on the "Global User Alert" function. Although this software is very useful for detecting certain types of anomalous behavior, it is not entirely sufficient. In addition to implementing Global User Alerts, the CorreLog administrator should also make use of Correlation Threads to detect anomalous message rates that may indicate an attack across multiple user identities.

How To Use This Manual

The next section of this manual (Section 2) provides the essential information needed to install, configure, and test the Global User Alert software. Note that the only required component of the system is the configuration screen. Other information on the CorreLog server can be found in the standard "User Manual", including operation and application notes that will be of assistance in processing the alerts and tickets generated by the program, and received by the CorreLog Syslog receiver process.

Section 2: Software Installation

The CorreLog Global User Alert Monitor software is usually delivered as a self-extracting WinZip file. The installation requires minimal installation steps. Basic installation steps are as follows:

1. The operator obtains the CorreLog Global User Alert Monitor software, in self-extracting WinZip format, and executes the self-extracting WinZip file. This unzips the Global User Alert software into the existing CorreLog Windows Distribution, including all configuration data and executables

2. The operator accesses the "Alerts > Users" tab (added by the installation procedure) and configures Global User Alerts for the various users or all users, consisting of match patterns and thresholds. (These steps are described briefly in this section, with further elaboration in Section 3.)

3. The operator optionally tests the software using the "Post New Message" hyperlink found on the "Messages > Search" screen to verify the operation of the system and configuration of the Global User Alert.

Actual installation steps, as well as initial tests of the software, are documented in this section. The information needed to perform the comprehensive configuration of Global User Alert parameters is provided in Section 3, along with a description of system operation and application notes.

Administrative logins are required in order to perform the software installation. The detailed steps needed to perform the installation are provided in the sections that follow.

Installation Requirements

The Global User Alert Monitor software can be installed on a variety of platforms and operating systems, including Windows 2K, Windows 7, and Windows Vista operating systems. The following items are required.

- **Existing CorreLog Server Installation.** Prior to installing the Global User Alert Monitor software, the CorreLog Server system must be installed on a Windows platform, as discussed in the CorreLog User Reference Manual.

- **Disk Space Requirements.** The Global User Alert Monitor software requires no significant disk space beyond the normal footprint of the CorreLog server. There is generally no extra disk space load due to this software.

- **CPU Requirements**. The Global User Alert Monitor software requires very little extra CPU requirements. A single persistent process is started the CorreLog Windows platform.

Windows Installation Procedure

The CorreLog Global User Alerts package is simple to install. The user simply obtains the plug-in package, and executes the package to extract the plug-in components to the CorreLog installation. CorreLog does not need to be stopped or restarted. The specific steps needed to install and the software are as follows:

1. Login to the CorreLog Server Windows platform using an "Administrator" type login.

2. Obtain and execute the "co-n-n-n-ualert.exe" package, extracting files to the directory location where CorreLog is installed (by default the location "C:\CorreLog").

   Note: A common mistake is to extract files to some directory other than the existing CorreLog installation. The user should make sure that the location of the CorreLog server (such as C:\CorreLog or D:\CorreLog) is correctly specified.

3. Log into the CorreLog web interface using a CorreLog "admin" type login, and access the CorreLog "Alerts" screen, by clicking the new "Alerts > Users" tab at the top of the display.

   Note: This tab is added to the system during step #2 above. If the tab does not exist, the operator probably extracted the files to the wrong directory. (For specific user help, see the next section of this manual.)

Preliminary Checkout And Test Procedure

Detailed instructions related to usage are provided in the next section. The following steps perform a preliminary configuration and test of the system, which can be optionally performed to verify the installation is correct.

Initially, no Global User Alerts exist in the system. The operator can add and verify a new global alert as described below.

1. Access the "Alerts > Users" tab of the CorreLog server.

2. Click the "Wizard" button on the above screen to add a new Global User Alert. This will guide the operator through the steps needed to add a new configuration item to the system.

   Note: If the operator has correctly configured the software, a new user alert will appear on the top-level screen with a "gray" indication.

3. Using the "Post New Message" link on the "Messages > Search" screen, send a message that contains a valid username (appearing on the "Messages > Users" screen) and the match keyword or address. Verify that the user name appears in the list of active global alerts.

4. Repeat step #3 above to create multiple users. Verify that when the number of messages associated with a particular user exceeds the global threshold, a ticket is opened in the "Tickets" tab.

When a message matches the configured user and message patch patterns, the user name is parsed from the message and a new active alert is added to the system. (If the active alert already exists, its count is incremented.)

When the active alert reaches is threshold, a ticket is opened referencing the user selected message and the user name. This ticket appears in the "Tickets" tab (like other CorreLog Tickets) and the ticket records the threshold violation and related messages.

While the particular user alert is active, no further tickets will be opened for the alert. When the message count for the alert drops below the threshold, the active alert is removed from the system and the process can be restarted.

Section 3: Software Operation

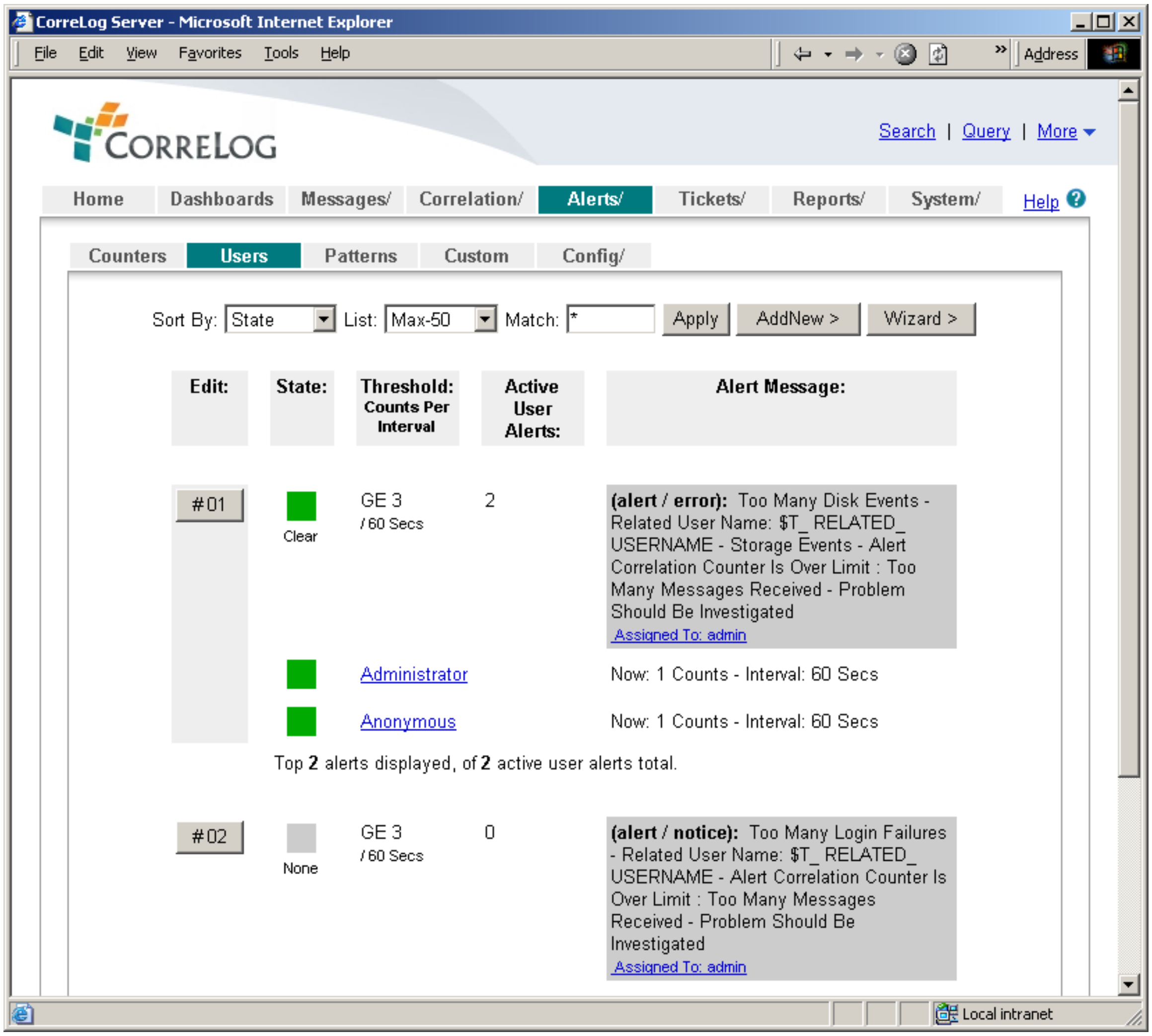
Once the CorreLog Global User Alert Plug-in software is installed, the user can add configuration items via standard "AddNew", and "Edit" buttons in a fashion similar to other CorreLog screens. This screen additionally contains a "Wizard" function that guides the user through the process of adding a new configuration item to the system.

Note that, by default, no global user alarms are configured. The operator must add one or more configuration items in order to use the system, as described herein. This activity will generally require detailed knowledge of the objectives for the organization, as well as an understanding of basic CorreLog operation. Detailed notes about CorreLog usage may be found in the standard "CorreLog System User Manual", and "CorreLog Screen Reference Manual", both of which are available from the "Home" screen of CorreLog after logon to the web interface.

This section provides a description of these optional software elements, their usage, and other considerations, including screenshots and explanation of all configuration values. Information in this section will normally be sufficient to perform all operational activities associated with this optional software. Further details and application information may be available from standard CorreLog support.

Global User Alert Monitor Screen

As part of the Windows installation, a new tab is created in the "Alerts" section of the CorreLog web interface, which permits the operator to configure various parameters associated with one or more Global User Alerts. This screen is visible to all users, but only CorreLog "admin" type logins may add or edit the alert specifications. The screen is depicted below:


CorreLog Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CORRELOG
Search | Query | More
Home Dashboards Messages/ Correlation/ Alerts/ Tickets/ Reports/ System/ Help
Counters Users Patterns Custom Config/
Apply AddNew > Wizard >
Local intranet

Sort By: State List: Max-50 Match: *

Edit:	State:	Threshold: Counts Per Interval	Active User Alerts:	Alert Message:
#01	🟩 Clear	GE 3 / 60 Secs	2	**(alert / error):** Too Many Disk Events - Related User Name: $T_ RELATED_ USERNAME - Storage Events - Alert Correlation Counter Is Over Limit : Too Many Messages Received - Problem Should Be Investigated Assigned To: admin
	🟩	Administrator		Now: 1 Counts - Interval: 60 Secs
	🟩	Anonymous		Now: 1 Counts - Interval: 60 Secs

Top **2** alerts displayed, of **2** active user alerts total.

Edit:	State:	Threshold: Counts Per Interval	Active User Alerts:	Alert Message:
#02	□ None	GE 3 / 60 Secs	0	**(alert / notice):** Too Many Login Failures - Related User Name: $T_ RELATED_ USERNAME - Alert Correlation Counter Is Over Limit : Too Many Messages Received - Problem Should Be Investigated Assigned To: admin

The above depiction shows a standard CorreLog screen, incorporating an "AddNew" button to add new monitors, and "Edit" buttons associated with each Global User Alert configuration item. Zero or more Global User Alerts can be added to the system. Each global alert may have zero or more active user alerts, depicted beneath the main alert. If any user exceeds the configured threshold, the indicator turns from green to red, and a ticket is opened for the user (with the text specified by the operator and depicted to the right of the screen.)

The screen provides several elements, described below.

- **Screen Controls**. The screen contains standard dialog buttons at the top, permitting the user to match alert messages and text, and permitting the user to add new alerts (via the "AddNew" button, or the "Wizard" button.)

- **Edit Button.** Beneath the Screen Controls are zero or more global alert specifications, where each specification has a numbered "Edit" button. The user can modify or delete any global user alert by clicking this button.

- **State Indicator.** Each global user alert specification has a status indicator, colored as follows: "Gray" indicates there are currently no active user alerts for the specification; "Green" indicates there are one or more active user alert instances, but all alert instances are below the configured threshold; "Red" indicates there are one or more active user alert instances that are above the alert threshold. This state indicator rolls up the state indications for each active user alert, described below.

- **Threshold.** Each global user alert specification displays the configured threshold and interval (specified when the operator created the alert.) This threshold indicates the maximum number of messages for ANY active user during a configured time interval before a ticket is opened for the user and a message is sent back to the event log.

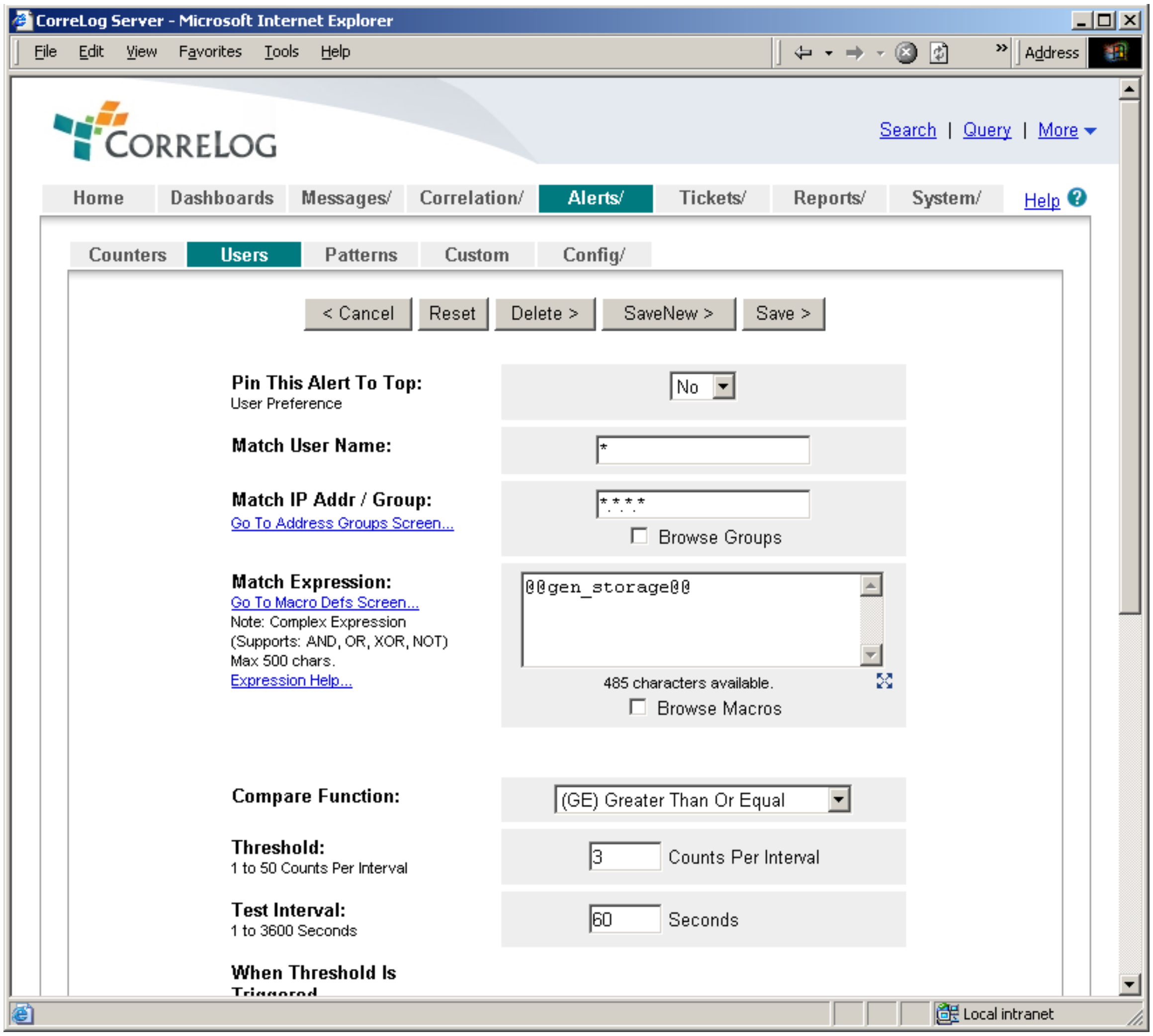
- **Active User Alerts.** Each global user alert specification displays the number of active user alerts, i.e. the number of users currently being tracked by the global user alert. If the value is zero, the "State Indicator" (above) will be "Gray", otherwise the state indicator will be either "Green" or "Red", depending upon whether a threshold has been violated for any of the active user alerts.

- **Alert Message.** Each global user alert specification displays the alert message that is sent back to the event log and used as the text of the ticket. The operator configures the specific alert message when the global user alert is created, and applies to any tickets created by any active user alert instance. The "assignee" of the ticket is displayed at the bottom of each configured message.

- **Active User Alert Instances.** Beneath the above values, each global user alert specification will have or more different active user alerts, where each active user alert instance contains its own state indicator, and an indication of the current counts. If any count is above the threshold, the state indicator is red (indicating that a ticket has been opened for the instance) otherwise the state indicator is green.

Global User Alert Editor Screen

The user adds a new global user alert via the "AddNew" button, or modifies an existing user alert via the "Edit" button of the top-level screen. The Global User Alert Editor Screen is a standard CorreLog dialog, similar to the standard alert editor, containing "Cancel", "Reset", Delete", "SaveAs", and "Save" buttons. An example of the Global User Alert edit screen is depicted below.



Pin This Alert To Top: User Preference	No
Match User Name:	*
Match IP Addr / Group:	*.*.*.* □ Browse Groups
Match Expression: Note: Complex Expression (Supports: AND, OR, XOR, NOT) Max 500 chars.	@@gen_storage@@ 485 characters available. □ Browse Macros
Compare Function:	(GE) Greater Than Or Equal
Threshold: 1 to 50 Counts Per Interval	3 Counts Per Interval
Test Interval: 1 to 3600 Seconds	60 Seconds
When Threshold Is Triggered	

The above screen is accessible only to CorreLog "admin" type users, and cannot be accessed via regular "user" or "guest" accounts. The screen contains many of the same familiar elements found within the "Correlation Thread" and "Alert Counters" screens, permitting the user to pin the alert to the top of the screen, match messages, specify a compare value and test interval, and specify the text of a ticket that is generated when the threshold is violated. The screen provides the ability to suggest alert messages, and assign tickets to system users.

Each of these fields is explained as follows:

- **Pin This Alert.** This select menu allows the operator to pin interesting global user alert specifications to the top. This setting is identical to the "Pin" functions found in other CorreLog screens. The "Pin" facility is useful to watch specific user alerts. On the top-level screen, pinned items are sorted and displayed before non-pinned items. Items are pinned only in the operator's personal user preferences (and are not pinned within other CorreLog logins.

- **Match User Name.** This input item allows the operator to specify a range of users to match. The input consists of a single keyword or wildcard that must match the user associated with any processed message.

- **Match IP Addr / Group.** This input item is a standard CorreLog IP address or wildcard or group name. This input item allows the operator to specify a range of devices to match. The processed message must match the specified IP address, wildcard, or CorreLog group name.

- **Match Expression.** This input item is a standard CorreLog match expression containing a keyword, wildcard, logical combination of keywords and wildcards, macro definitions, or logical combination of macro definitions. This field has the exact same syntax as the match expression found on the "Correlation > Threads" edit screen.

- **Compare Function.** This input item is the compare function to use with counts. This field has the exact same syntax as the compare function found on the "Alerts > Counters" edit screen.

- **Threshold.** This input item is the threshold for the alert. In conjunction with the Compare Function (above) this input specifies the maximum count of messages during the test interval (below) before the alert is fired, causing a ticket to be opened on the system. The maximum count is 50, which is the maximum number of related messages for any alert. This field has the exact same syntax as the threshold found on the "Alerts > Counters" edit screen.

- **Test Interval.** This input item is the interval (in seconds) to tabulate message counts for active user alerts. The value indicates the maximum time that the alert will be triggered, and the minimum time that another ticket for a user alert can be opened. This field has the exact same syntax as the test interval found on the "Alerts > Counters" edit screen.

- **Send Alert Message.** This input item is the text of the message sent back to CorreLog, and the text of the ticket that is opened when the alert threshold is violated. The operator can click the "Suggest" button to suggest an alert message. Note that this Send Alert Message is quite non-specific, and should be carefully tailored to reflect the alert condition, most likely based upon the match expressions discussed earlier. (See additional notes below.)

- **Insert Variable.** This input item allows the operator to add a variable to the "Send Alert Message" (above). The "Suggest" button always adds the "Related User" field to identify the username associated with any open ticket. Additionally, the operator may add other variables, such as the device name, related message, etc.

- **Alert Facility.** This select menu allows the operator to select the facility associated with the "Send Alert Message", when the user alert instance triggered. The default facility is "alert", but the operator can modify this value here.

- **Alert Severity.** This select menu allows the operator to select the severity associated with the "Send Alert Message", when any user alert instance is triggered. The operator can modify this value here.

- **Ticket Assignee.** This is the name of the ticket operator that is assigned the ticket. By default, the Ticket Assignee is the name of the currently logged in user, however the value can be set to any other user or ticket group name. The special "disabled" user prevents a ticket from being opened (but still permits a message to be sent back to the event log for further correlation.) The syntax of this field is identical to the "Assignee" value found on the "Alerts > Counters" screen.

Suggest Message Button

As part of the edit screen, the operator must supply a text message associated with the alert condition. This text message is applied to all active alert instances that are triggered, and should be edited by the user to completely describe the alert condition.

Note that the default text supplied by the "Suggest" button will probably not be adequate to fully describe the alert condition, or sufficient for the ticket assignee to understand the circumstances of the alert. The operator should manually modify the "Send Alert Message" to make the alert condition more clear.

For example, the user will typically click the "Suggest" button to suggest a message, and then modify the text to describe the alert condition, such as "Too Many User Logins", or "Too Little Process Activity", or some other distinguishing text.

Note that this behavior is slightly different from the standard "Alerts > Counters" button in that there is no counter name to qualify the message. Hence, it is usually necessary to provide extra text to the suggested message in order to identify the particular alert condition. Also, note that the "Related User" is always added to the message by default, to identify the particular user that the alert relates to. The operator can insert additional messages using the "Insert" button on this screen.

Creating Threads, Tickets, and Alerts

The messages sent by the Global User Alert Monitor are identical to the messages sent by the Alerts > Counters" screen, and other internal CorreLog messages. This permits the messages generated by this facility to be correlated like any other message. The basic steps are provided below.

1. The operator creates a thread to tabulate the messages sent by the system using the "Correlation > Threads > Add New" screen. This screen is used to collect all the messages of a particular type (such as all messages with "Global User Alert" in their content.)

2. The operator creates an Alert for the thread counter using the "Alerts > Users > Add New" screen. This alert will send a Syslog message back to the main list of messages when one or more messages are received during an interval of time. As is always the case, when an alert is triggered, a single message is sent back to CorreLog, and a single ticket is opened while the alert is set. (See additional notes below.)

3. The operator optionally identifies an "Assignee" for the alert via the "Alerts > Users > Add New" screen. This causes a ticket to be opened on the system, and assigned to a particular user or a ticket group. The user can assign a ticket to any existing user, or ticket group.

4. The operator optionally adds a "Ticket Action" to the system, which sends e-mail (or performs some other action) when a new ticket is opened on the system, providing a real-time indication that a timeout threshold of the Global User Alert Monitor software has been violated. This message will typically contain the descriptive text entered by the operator when the alert was created, which may be slightly (or totally) different than the originating Global User Alert Monitor message.

Further information on how to correlate messages, and use the CorreLog ticketing system can be found in the "CorreLog System Users Manual" and "Screen Reference Manual". Additional help is available by contacting CorreLog support.

For Additional Help And Information…

Detailed specifications regarding the CorreLog Server, add-on components, and resources is available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com

Alphabetical Index

A

Access / 11
Action / 19
Active / 15
Activity / 18
Actual / 9
Adapter / 21
Addnew / 13 14 15 16
Addr / 17
Admin / 6
Administrative / 9
Administrator / 10
Alert / 5 6 7 9 10 11 13 14 15 16 17 18 19 21
Alerts / 5 6 7 9 10 11 14 15 17 18 19
Alphabetical Index / 20
Anomalous / 6
Assignee / 18 19
Auto-learning / 6

B

Background / 6
Basic / 9
Beneath / 15
Benefits / 7
Best / 6

Button / 15 18
Button, Suggest Message / 18

C

Cancel / 16
Checkout / 11
Click / 11
Compare / 17
Controls / 15
Correlation / 5 6 7 16 17 19
Correlog / 5 6 7 9 10 11 13 14 16 17 19
Counters / 16 17 18 19
Creating / 6 19

D

Delete / 16
Detailed / 11 13
Disk / 10
Distribution / 9

E

Editor / 16
Existing / 10
Expression / 17

F

Facility / 18
Failures / 6
Function / 17

G

Global / 5 6 7 9 10 11 13 14 16 19 21
Gray / 15
Green / 15
Group / 17

H

Home / 13
How To Use This Manual / 7

I

Index / 20
Index, Alphabetical / 20
Indicator / 15
Information / 6 13
Installation / 9 10
Installation, Software / 9
Installation, Windows Procedure / 10
Instances / 15
Interval / 17
Introduction / 5 5
Invalid / 6
Items / 17

L

Limitations / 7
Little / 18
Logins / 18
Logon / 6

M

Manual, How To Use This / 7
Message / 9 11 15 17 18
Message, Suggest Button / 18
Messages / 9 11

N

Name / 17

O

Operation / 13
Operation, Software / 13

P

Page / 21
Pci- / 5
Plug-in / 5 13
Post / 9 11
Preliminary / 11
Procedure / 10 11

Procedure, Windows Installation / 10
Process / 18

R

Reference / 10 13 19
Related / 18 19
Repeat / 11
Requirements / 10
Reset / 16

S

Save / 16
Saveas / 16
Search / 9 11
Server / 5 10
Severity / 18
Software / 9 13
Software Installation / 9
Software Operation / 13
State / 15
Suggest / 17 18
Suggest Message Button / 18
Syslog / 7 19
System / 13 19

T

Threads / 6 7 17 19
Threshold / 15 17
Ticket / 18 19
Tickets / 11 19

U

User / 5 6 7 9 10 11 13 14 15 16 17 18 19 21
Users / 5 9 10 11 19

V

Variable / 18
Verify / 11
Vista / 10

W

Windows / 6 9 10 14
Windows Installation Procedure / 10
Winzip / 9
Wizard / 11 13 15