



I P S W I T C H

User Guide
for Custom Reporting
in WhatsUp Event Analyst
v10.x

Custom Reporting In WhatsUp Event Analyst

- Custom Reporting In WhatsUp Event Analyst..... 2
- Limiting Data In Your Report With Filters 2
- Designing Your Report's Layout..... 4
- Special Syslog Fields Available for Custom Reporting 9
- Creating Custom Fields To Extract Useful Data From the Description Field of Security Events 9
- Correlating Security Events With Custom Fields 13
- Increasing Readability With Friendly Event ID Definitions 16
- Running and Scheduling Custom Reports 18
- Custom Report Output Formats: HTML and CSV 19

Custom Reporting In WhatsUp Event Analyst

In This Guide

Custom Reporting In WhatsUp Event Analyst	2
Limiting Data In Your Report With Filters	2
Designing Your Report's Layout.....	4
Special Syslog Fields Available for Custom Reporting.....	9
Creating Custom Fields To Extract Useful Data From the Description Field of Security Events	9
Correlating Security Events With Custom Fields.....	12
Increasing Readability With Friendly Event ID Definitions	16
Running and Scheduling Custom Reports	18
Custom Report Output Formats: HTML and CSV	19

Custom Reporting In WhatsUp Event Analyst

Creating custom reports with WhatsUp Event Analyst is easy, and typically only involves three steps.

Step 1 - Limiting the data returned to your report by creating a Basic or Advanced Filter in WhatsUp Event Analyst (on page 2)

Step 2 - Designing the report layout by selecting, grouping, and orienting the fields displayed in the Custom Reports Designer (on page 4)

Step 3 - Manually running the report against a filtered log source, or scheduling the report to run repeatedly (on page 18)

Limiting Data In Your Report With Filters

It is important to keep report size at a minimum, so in almost every case it is necessary to create a filter inside WhatsUp Event Analyst that limits the amount of log data your report displays. WhatsUp Event Analyst allows you to create and store basic or advanced filters to accomplish this.

Custom Reporting in WhatsUp Event Analyst

Basic Filters work against all log sources that WhatsUp Event Analyst works with, including EVT files, EVTX files, comma-delimited text files, and database tables. However, basic filters do not support advanced filtering capabilities, such as multiple field conditions, wildcards, exclusionary conditions, etc. To create a basic filter, click the **Edit** menu, and then select **Define Basic Filters**.

For more information on how to create and edit basic filters, please review that help topic in the WhatsUp Event Analyst User Guide.

Advanced filters only work against log data stored in database tables (e.g. Microsoft Access, Microsoft SQL Server, or Oracle). In contrast to Basic filters, advanced filters are much more powerful, allowing you to look for multiple possible values in a single field, create exclusionary conditions, and use wildcards. To create an advanced filter, click the **Edit** menu, and then select **Define Advanced Filters**.

For more information on how to create and edit advanced filters, please review that help topic in the WhatsUp Event Analyst User Guide.



Note: There are multiple ways to store log data in database tables in order to harness the power of advanced filters for your custom reporting needs. One way is to use Ipswitch's WhatsUp Event Archiver solution to automatically collect event log data into central database tables on a scheduled basis. Another option is to export one or more log files manually from their native format (EVT/EVTX) into database tables by using WhatsUp Event Analyst's Export menu. WhatsUp Event Analyst can export log files one at a time into Microsoft Access MDB database tables, even when Microsoft Access is not installed on the local machine. Similarly, it can read and report on the log data in Microsoft Access database tables when Microsoft Access is not installed; all that is required is to link to the Access .MDB file and table name in the *Database Table Links Manager Dialog*.

Examples Of Filters For Custom Reports:

Example 1 - Remote Access Events. Management may desire a report showing all RemoteAccess events that are recorded in the System Log. To make sure your report only displays RemoteAccess events, you can create a basic filter like so:

Source: RemoteAccess

Event Types: Information, Warning, Error

All other fields in the filter are left blank

Example 2 - Network Logons Not Related to Machine Accounts. You can create a custom report that displays all 540 Network Logon events that are not tied to machine account logons using an advanced filter like so:

Source: Security

Event ID: 540

Description DOES NOT Contain: \$

Designing Your Report's Layout

The Custom Report Designer dialog allows you to design the exact grouping, sorting, and layout of event log fields in your custom reports. When you select **Add** or **Edit** in this dialog, the Custom Report Designer dialog opens in Editor mode and displays a grid that is a visual representation of your custom report layout. To see roughly how a report will look and function after you design it, you can click the **Test** button to run it against a sample dataset. If you no longer need a particular custom report layout, click the **Delete** button to remove it from WhatsUp Event Analyst.

Using The Report Layout Grid To Group Data By Related Fields

For better readability and interpretation, you may want to group your report data one or more times to better correlate data related to one or more fields. To create groups in your report layout, work diagonally downwards from top-left to bottom-right in the report layout grid. You can create up to 7 levels of groupings in any report layout, but in most situations, you will seldom need more than 4 levels. For example, a grid that looks like this:

Name: Description:

Report Layout (Click buttons to cycle through field names. Press 'Help' below for more information)

Computer							
	User						
		DateTime	EventID	Description			

Computer: COMPUTER1

User: DOMAIN\UserDEF

<i>DateTime</i>	<i>EventID</i>	<i>Description</i>
4/28/2006 9:54:32 PM	7062	The DNS server encountered a packet addressed to itself on IP address 10.0.0.5.

User: None

<i>DateTime</i>	<i>EventID</i>	<i>Description</i>
4/28/2006 9:46:48 PM	3150	COMPUTER10 removed from WINS database.

Computer: COMPUTER2

User: None

<i>DateTime</i>	<i>EventID</i>	<i>Description</i>
4/28/2006 9:51:30 PM	2	The Computer Browser service failed to start.

Computer: COMPUTER3

User: DOMAIN\UserXYZ

<i>DateTime</i>	<i>EventID</i>	<i>Description</i>
4/28/2006 9:54:29 PM	7062	Document 'CorporateFinancials.xls' was printed on FastLaser10 on port LPT1.

User: NT AUTHORITY\SYSTEM

<i>DateTime</i>	<i>EventID</i>	<i>Description</i>
4/28/2006 9:48:20 PM	30	A valid time server could not be contacted.

Custom Reporting in WhatsUp Event Analyst

Notice how all the log data for a COMPUTER1 is shown first, then COMPUTER2, etc. This is because the *Computer* field is the top-most group. Similarly, within each *Computer* group, all log data related to particular users are grouped together, since the *User* field is the second-highest group.

On the other hand, a grid that looks like this:

The screenshot shows a configuration window for a report layout. At the top, there are two text boxes: 'Name: Grouping Example 2' and 'Description: Group By Computer Then EventID'. Below these is a label 'Report Layout (Click buttons to cycle through field names. Press 'Help' below for more information)'. The main area is a grid of 10 columns and 10 rows. The first row has 'Computer' in the first column. The second row has 'EventID' in the second column. The third row has 'DateTime' in the third column, 'User' in the fourth column, and 'Description' in the fifth column. The remaining cells in the grid are empty.

will group log records in your report like so:

Computer: COMPUTER1

EventID: 3150

<i>DateTime</i>	<i>User</i>	<i>Description</i>
4/28/2006 9:46:48 PM	None	COMPUTER10 removed from WINS database.

EventID: 7062

<i>DateTime</i>	<i>User</i>	<i>Description</i>
4/28/2006 9:54:32 PM	DOMAINUserDEF	The DNS server encountered a packet addressed to itself on IP address 10.0.0.5.

Computer: COMPUTER2

EventID: 2

<i>DateTime</i>	<i>User</i>	<i>Description</i>
4/28/2006 9:51:30 PM	None	The Computer Browser service failed to start.

Computer: COMPUTER3

EventID: 30

<i>DateTime</i>	<i>User</i>	<i>Description</i>
4/28/2006 9:48:20 PM	NT AUTHORITY\SYSTEM	A valid time server could not be contacted.

EventID: 7062

<i>DateTime</i>	<i>User</i>	<i>Description</i>
4/28/2006 9:54:29 PM	DOMAINUserXYZ	Document 'CorporateFinancials.xls' was printed on FastLaser10 on port LPT1.

Custom Reporting in WhatsUp Event Analyst

If you want to output a sorted table of log records without any grouping at all, you can create a grid that looks like this:

Name: Description:

Report Layout (Click buttons to cycle through field names. Press 'Help' below for more information)

Computer	User	EventID	Date Time	Description			

which will display a sorted table of log records like this:

Computer	User	EventID	DateTime	Description
COMPUTER1	None	3150	4/28/2006 9:46:48 PM	COMPUTER10 removed from WINS database.
COMPUTER2	None	2	4/28/2006 9:51:30 PM	The Computer Browser service failed to start.
COMPUTER3	DOMAINUserXYZ	7062	4/28/2006 9:54:29 PM	Document 'CorporateFinancials.xls' was printed on FastLaser10 on port LPT1.
COMPUTER3	NT AUTHORITY\SYSTEM	30	4/28/2006 9:48:20 PM	A valid time server could not be contacted.
COMPUTER4	DOMAINUserABC	2699	4/28/2006 9:46:48 PM	Illegal Operation Error in Program mstcewer.exe
COMPUTER5	DOMAINUserABC	123	4/28/2006 9:54:36 PM	Performance information invalid.
COMPUTER6	DOMAINUserABC	3	4/28/2006 9:38:18 PM	Successful logon for UserABC - IP Address 10.64.0.10.
COMPUTER6	DOMAINUserDEF	2	4/28/2006 9:38:18 PM	Logon failure from UserDEF - IP Address 10.64.0.2.

Orienting Fields In The Report Layout

In most custom report layouts, you will have at least one or more group levels, followed by an end row containing the remaining fields. Therefore, most custom report layouts have a grid orientation like the ones shown below.



Arrangement of fields in grid with one group applied



Arrangement of fields in grid with two groups applied

Custom Reporting in WhatsUp Event Analyst

The final row in any report layout is the data row, displaying only the data elements you want shown within the final grouping level. You explicitly control the data elements which show up in your custom report - *only the fields that you actually place in the grid will be shown in the actual custom reports.*

Report Layout (Click buttons to cycle through field names. Press 'Help' below for more information)

EventID	User	Description	DateTime	Computer	<- The Data Row		

In addition, log data in the final data row of the report is automatically sorted alphabetically from left to right. Therefore, the order of fields in the data row is very important; if you want your data row to first be sorted chronologically by the date and time when the event occurred, make sure the DateTime field is the left-most field in the data row.

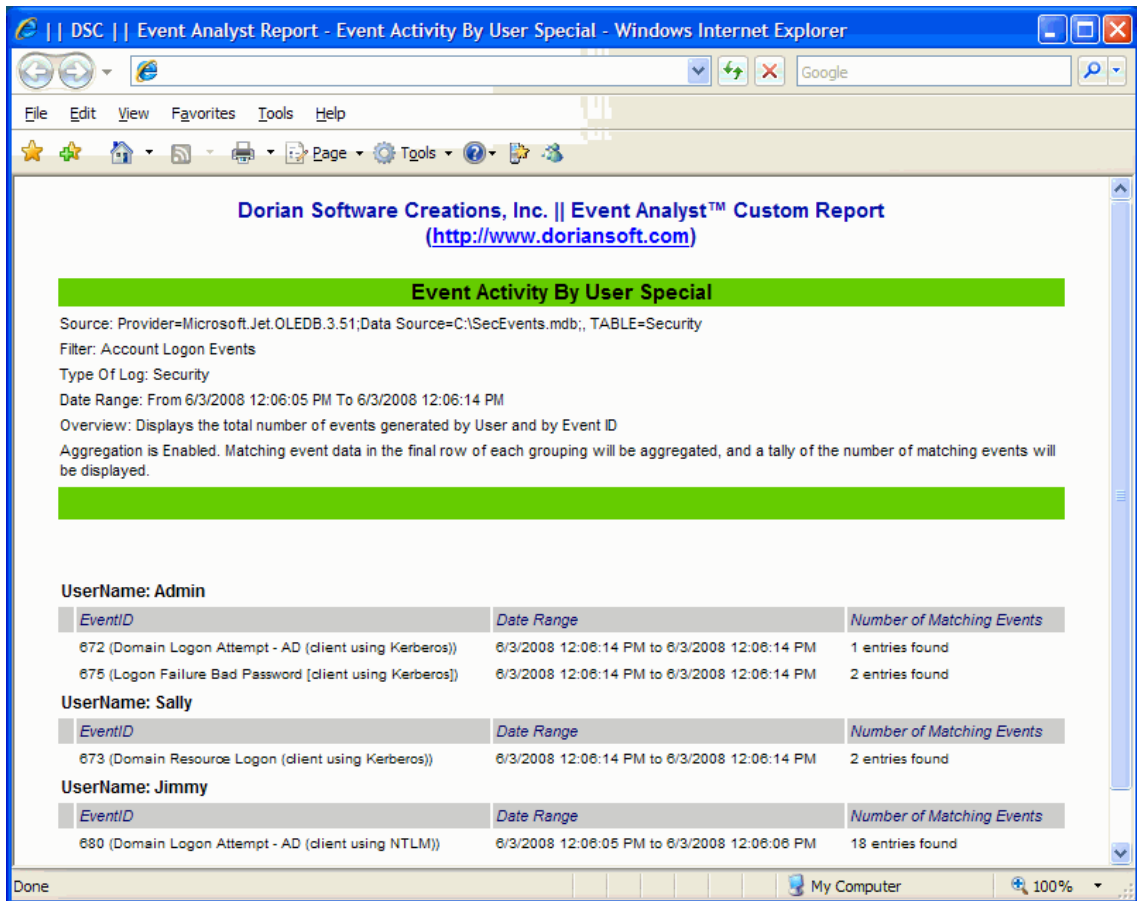
Aggregating Related Events In Your Report To Minimize Report Size

Below the report layout grid is a check box marked **Create a summary report by aggregating matching event data on the lowest report level.** If you check this option, WhatsUp Event Analyst automatically aggregates all events whose fields in the data row (see above) match exactly. This is useful if you expect a filter paired with a custom report to return a lot of data, and if you are primarily concerned with trends in that data, as opposed to seeing all the individual events returned by the filter.

For example, if you want to see a breakdown of how many events a particular user has generated in the Security log, you could first create an advanced filter that looks for a range of Event IDs over a particular set of days.

Custom Reporting in WhatsUp Event Analyst

The resulting report should look something like this:



The screenshot shows a web browser window titled "DSC || Event Analyst Report - Event Activity By User Special - Windows Internet Explorer". The page content includes the following information:

Dorian Software Creations, Inc. || Event Analyst™ Custom Report
(<http://www.doriansoft.com>)

Event Activity By User Special

Source: Provider=Microsoft.Jet.OLEDB.3.51;Data Source=C:\SecEvents.mdb;; TABLE=Security
Filter: Account Logon Events
Type Of Log: Security
Date Range: From 6/3/2008 12:06:05 PM To 6/3/2008 12:06:14 PM
Overview: Displays the total number of events generated by User and by Event ID
Aggregation is Enabled. Matching event data in the final row of each grouping will be aggregated, and a tally of the number of matching events will be displayed.

UserName: Admin

EventID	Date Range	Number of Matching Events
672 (Domain Logon Attempt - AD (client using Kerberos))	6/3/2008 12:06:14 PM to 6/3/2008 12:06:14 PM	1 entries found
675 (Logon Failure Bad Password [client using Kerberos])	6/3/2008 12:06:14 PM to 6/3/2008 12:06:14 PM	2 entries found

UserName: Sally

EventID	Date Range	Number of Matching Events
673 (Domain Resource Logon (client using Kerberos))	6/3/2008 12:06:14 PM to 6/3/2008 12:06:14 PM	2 entries found

UserName: Jimmy

EventID	Date Range	Number of Matching Events
680 (Domain Logon Attempt - AD (client using NTLM))	6/3/2008 12:06:05 PM to 6/3/2008 12:06:06 PM	18 entries found

Notice how matching field data in the data row is automatically being aggregated. Specifically, instead of showing you individual dates, the report displays a date range instead for all of the matching events. In addition, a final column is added to the data row called Number of Matching Events, so you can quickly see the level of activity for a given user and given event activity. This technique can aid an administrator in spotting important trends when the volume of events for any particular user is much greater or less than the others.



Note: It is important to always include the DateTime field as the last field in the data row of any report that uses aggregation. When you do so, custom reports generated by WhatsUp Event Analyst display a date range for matching events, which greatly enhances report readability.

Selecting / Cycling Through Fields in the Grid

In order to create the report layout you want in the grid, you can repeatedly click the buttons in the grid to cycle through all the event log field names available. Once a field name is displayed on a button, you will not be able to choose that same field name again unless you clear it from the other button.

Saving and Testing Your Custom Report

Once you have all your fields laid out on the grid appropriately, you can save and test your custom report. Make sure to give your custom report a name and description, and then click the **Save** button. After your report is saved, you can click the **Test** button to get an idea about how your report will look. WhatsUp Event Analyst runs your custom report against a small set of fictitious log data and allows you to view the results immediately.

Special Syslog Fields Available for Custom Reporting

If you are using WhatsUp Event Archiver to collect syslog messages into a central ODBC database like Microsoft SQL Server, you can access the special additional fields found in those syslog database tables for your custom reports. The following four fields can be selected when designing a custom report layout:

- **SLHostName.** Represents the hostname of the syslog device that logged the message.
- **SLIPAddress.** Represents the source IP address of the syslog device that logged the message.
- **SLPriorityCode.** Represents the three-digit priority code found in any syslog message.
- **SLRFCHeader.** Holds the full RFC 3164 header of the syslog message, if the syslog device sending the message is RFC3164 compliant.

In addition to the above fields, the Category field displays the Facility and Severity Code of the syslog message (e.g. Kernel.Emergency) and the Description field displays the entire syslog message contents.

Creating Custom Fields To Extract Useful Data From the Description Field of Security Events

Beginning in Version 7 of WhatsUp Event Analyst, you can extract useful data values from the Description field of virtually all events recorded in the Windows Security event log. It is important to note that you can do this regardless of the current format the log data is in. In other words, WhatsUp Event Analyst can parse out useful data values from security log data in EVT format, EVTX format, WhatsUp Event Archiver-generated comma-delimited text files,

Custom Reporting in WhatsUp Event Analyst

and WhatsUp Event Archiver/WhatsUp Event Alarm/WhatsUp Event Analyst-generated central database tables.

Almost all Windows security events have subvalue name / subvalue data pairs that are parsable by WhatsUp Event Analyst's custom reporting engine. Let's start reviewing some examples:

Example 1 - Event ID 592 - A new process has been created

Event Type: Success Audit

Event Source: Security

Event Category: Detailed Tracking

Event ID: 592

Date: 5/28/2008

Time: 2:48:17 PM

User: DOMAIN\Jim

Computer: ATLAS

Description:

A new process has been created:

New Process ID: 1652

Image File Name: C:\WINDOWS\system32\eventvwr.exe

Creator Process ID: 2016

User Name: Jim

Domain: DOMAIN

Logon ID: (0x0,0xF0744)

In the above example, there are 6 subvalues present in the Description field of the event: New Process ID, Image File Name, Creator Process ID, User Name, Domain, and Logon ID

Example 2 - Event ID 540 - Successful Network Logon

Event Type: Success Audit

Event Source: Security

Custom Reporting in WhatsUp Event Analyst

Event Category: Logon/Logoff

Event ID: 540

Date: 5/28/2008

Time: 2:51:44 PM

User: DOMAIN\Jim

Computer: ATLAS

Description:

Successful Network Logon:

User Name: Jim

Domain: DOMAIN

Logon ID: (0x0,0x1186972)

Logon Type: 3

Logon Process: Kerberos

Authentication Package: Kerberos

Workstation Name:

Logon GUID: {ed1c734d-721b-5d80-a4b1-561637f71713}

In the above example, there are 8 subvalues present in the Description field of the event: User Name, Domain, Logon ID, Logon Type, Logon Process, Authentication Package, Workstation Name, and Logon GUID.

Creating and Selecting Custom Fields

You can create custom fields to parse out subvalue data in security events. When the Custom Report Designer is in Editor Mode, click **Create Custom Field** to define a new custom field, or click **Select Custom Field** to make available a custom field that is already being used in other reports.

When creating a new custom field, enter three key pieces of information:

The **Short Name** is a 9 character or less abbreviation for the custom field that is parsed out of the description. This abbreviated name is selectable and positionable in the Report Layout Grid when you are designing a Custom Report.

The **Field To Search For In Description** is the subvalue name as it appears in the Description of a security event. These subvalue names are always followed by colons. For instance, in

Custom Reporting in WhatsUp Event Analyst

Example 1 above, *New Process ID:* and *User Name:* are examples of valid subvalue names. Make sure you always enter the subvalue name **exactly** as it appears in the Description field.

In some security events, the same subvalue name can appear more than once in the Description. For instance, the 4624 successful Logon event in Microsoft Windows Vista contains two Account Name and Account Domain subvalue names in the Description. Use the **Occurrence** setting to select the appropriate subvalue name in the Description if it appears more than once.

Once you have defined a new custom field, you can make it available for use in the custom report you are designing by clicking the **Select Custom Field** button. All custom fields that are checked in this dialog are available for use in your custom report, and all custom fields that are not checked are unavailable. As a convenience to the report designer, all custom fields that are being used in other, previously-defined custom reports are automatically made available for use in new reports.



Note: Once a custom report is deleted, all custom fields used in that custom report definition are similarly removed from WhatsUp Event Analyst, unless other custom reports remain that still use those custom fields.

Once one or more custom fields have been made available to the current custom report you are designing, you can click through the various fields on grid buttons to locate and use that custom field.

Missing Custom Fields

In some cases, the subvalue in the Description field that a Custom Field is targeting may not be present. This can happen for a variety of reasons:

- There may be a mixture of events with the same Event ID but from different operating system versions in the database table you are reporting against. In many cases, each subsequent release of a Microsoft operating system (e.g. from Windows NT 4.0 to Windows 2000, Windows 2000 to Windows 2003, etc) contains more subvalues in the description field of events that share the same Event ID.
- If you query a database table using an Advanced Filter that targets multiple Event IDs, some events may have different subvalues in their Description than others.

In all cases, if subvalue data cannot be found in one or more of the events being processed in the custom report, WhatsUp Event Analyst substitutes the phrase Field Not Present in the report. If the Description field itself is in an unrecognizable and unparseable format, WhatsUp Event Analyst substitutes the phrase Unparseable Description.

Correlating Security Events With Custom Fields

In many cases, different security events share some of the same subvalue names in their Description field. For instance, in Windows 2003 server, several different logon events record the IP address of the client computer attempting the logon. For example, let's look at Event IDs 529, 672, 673, and 675 from a Windows 2003 server:

Event ID: 529

Description: Logon Failure:

Reason: Unknown user name or bad password

User Name: JSmith

Domain: DORIAN

Logon Type: 3

Logon Process: NtLmSsp

Authentication Package: NTLM

Workstation Name: VISTANOTE2

Caller User Name: -

Caller Domain: -

Caller Logon ID: -

Caller Process ID: -

Transited Services: -

Source Network Address: 10.32.0.33

Source Port: 0

Event ID: 672

Description: Authentication Ticket Request:

User Name: Admin

Supplied Realm Name: DORIAN

Custom Reporting in WhatsUp Event Analyst

User ID: %S-1-5-21-2514599881-2511992268-3252698249-500}

Service Name: krbtgt

Service ID: %S-1-5-21-2514599881-2511992268-3252698249-502}

Ticket Options: 0x40810010

Result Code: -

Ticket Encryption Type: 0x17

Pre-Authentication Type: 2

Client Address: 10.32.0.33

Certificate Issuer Name:

Certificate Serial Number:

Certificate Thumbprint:

Event ID: 673

Description: Service Ticket Request:

User Name: Admin

User Domain: DORIAN.COM

Service Name: COMPUTER\$

Service ID: %S-1-5-21-2514599881-2511992268-3252698249-1003}

Ticket Options: 0x40810000

Ticket Encryption Type: 0x17

Client Address: 10.32.0.33

Failure Code: -

Logon GUID: {f8a905c9-feb6-ba68-f2ba-7beb46baf9dc}

Transited Services: -

Event ID: 675

Description: Pre-authentication failed:

Custom Reporting in WhatsUp Event Analyst

User Name: Admin

User ID: %S-1-5-21-2514599881-2511992268-3252698249-500}

Service Name: krbtgt/DORIAN

Pre-Authentication Type: 0x2

Failure Code: 0x25

Client Address: 10.32.0.33

All of these logon events record an "Address:" subvalue corresponding to the client computer's actual IP address, and a "User Name:" subvalue corresponding to the supplied user credentials. Because of this, we can create a custom report with custom fields that take advantage of the shared subvalues, and correlate all logon activity by Client IP and then by User Name.

Example: Correlating Logon Activity By Client IP Address and User Name

- 1 Click the **Edit** menu, and then select **Define Advanced Filters**.
- 2 Click **Add** to create a new advanced filter.
- 3 Type a **Filter Name** and **Filter Comment**, and then choose the database type your advanced filter will target.
- 4 Select the **Event ID** tab, enable filtering on Event ID, and enter the Event IDs relating to logon activity you wish to correlate. You can click the "..." button to select these Event IDs by their friendly definition. Save your advanced filter and close the Advanced Filter Builder dialog.
- 5 Click the **Reports** menu, and then select **Custom Report Designer**.
- 6 Click **Add** to create a new custom report layout.
- 7 Click **Create Custom Field**.
- 8 Create the **Address** custom field to parse out Client IP addresses from all logon events.
- 9 Click **OK**.
- 10 Click **Create Custom Field** again, and then create the **UserName** custom field to parse out the user name from all logon events.
- 11 Click **OK**.
- 12 Give your custom report a name, description, and orient the report fields as shown in the grid.
- 13 Click **Save** and then close the **Custom Report Designer**.
- 14 Click the **File** menu, and then select **Open Database Table Links**.
- 15 Choose the database table link containing the Security events you wish to correlate.
- 16 Click **Filters** to select the Advanced Filter you created in Step 4.
- 17 Select the Advanced Filter you created in Step 4, and then click **Apply**.
- 18 Click **Build Report**.

- 19 Choose the custom report you created in Step 10, and then click **Run Report**.
- 20 When the report is complete, click **View HTML** to view your report in a web browser. The output should look similar to what is shown below.

Address: 10.32.0.33

UserName: Admin

<i>DateTime</i>	<i>TypeOfEvent</i>	<i>EventID</i>
6/3/2008 12:06:14 PM	Failure Audit	675 (Logon Failure Bad Password [client using Kerberos])
6/3/2008 12:06:14 PM	Failure Audit	675 (Logon Failure Bad Password [client using Kerberos])
6/3/2008 12:06:14 PM	Success Audit	672 (Domain Logon Attempt - AD (client using Kerberos))

UserName: Admin@DORIAN.COM

<i>DateTime</i>	<i>TypeOfEvent</i>	<i>EventID</i>
6/3/2008 12:06:14 PM	Success Audit	673 (Domain Resource Logon (client using Kerberos))
6/3/2008 12:06:14 PM	Success Audit	673 (Domain Resource Logon (client using Kerberos))

UserName: JSmith

<i>DateTime</i>	<i>TypeOfEvent</i>	<i>EventID</i>
6/3/2008 12:06:05 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:05 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)
6/3/2008 12:06:06 PM	Failure Audit	529 (Logon Failure - Unknown user name or bad password)

Increasing Readability With Friendly Event ID Definitions

You can increase the readability of your custom reports by creating one or more Friendly Event ID Definitions inside WhatsUp Event Analyst. A Friendly Event ID Definition is simply a short phrase that correlates to a particular Event ID number, indicating the typical meaning of that Event ID. WhatsUp Event Analyst already comes with quite a few Friendly Event ID Definitions, most of which are related to the Security Log. However, you can create your own inside the Friendly Event ID Manager Dialog, found under the **Reports Menu > Manage Friendly Event ID Definitions**.

Custom Reporting in WhatsUp Event Analyst

After a Friendly Event ID is defined, WhatsUp Event Analyst displays your friendly definition alongside the event identifier number in custom reports, if you choose to enable this functionality. For example, a custom report that was grouped by Event ID field would now have friendly definitions shown alongside the Event IDs in parentheses:

528 (Successful logon)

Event Record Data 1

Event Record Data 2

Event Record Data n...

538 (User logoff)

Event Record Data 1

Event Record Data 2

Event Record Data n...

Also, you can use the Friendly Event ID Manager dialog to select one or more events by name when building an Advanced Filter inside WhatsUp Event Analyst.

Manage Mode

Add. Adds a new Friendly Event ID definition.

Edit. Allows you to edit an existing Friendly Event ID definition.

Delete. Deletes the currently selected definition.

Close. Closes the Friendly Event ID Manager.

Use Friendly Event IDs in custom reports to make them more descriptive. If this option is checked, matching friendly descriptions of certain Event IDs is placed in parentheses beside the Event ID numbers in custom reports. If this option is unchecked, no mapping is performed in custom reports.

Add/Edit Mode

Event ID. Enter the event identifier number for the event to which you want to associate a friendly definition.

Log Type. Select the log type in which this event identifier is found.

Source. Select the source with which this identifier is associated.

Friendly Definition. Enter descriptive text that explains the meaning/purpose of this event.

OK. Click this button to add this definition to the Friendly Event ID database, or to save changes to an existing definition.

Cancel. Abandons an adding or editing operation.

Event ID Chooser Mode

OK. Returns the Event IDs you have chosen (e.g. checked) to the Advanced Filter Builder dialog.

Cancel. Closes the dialog without returning any Event IDs.

Running and Scheduling Custom Reports

After you have designed a filter and a custom report layout, you can run your custom report immediately against a log source, or schedule it to be produced automatically on a recurring basis.

Running Custom Reports Manually

How To Report Against Active (Live) Event Logs, Saved Event Log Files (EVT/EVTX), or Comma-Delimited Text Files

- 1 In WhatsUp Event Analyst, click the **File** menu, and then select **Connect To Computer Log**, **Open Saved EVT/EVTX File**, or **Open Comma-Delimited Text File**.
- 2 Select the log you want to open, and then click **Show Results in Window**.
- 3 With the log records now displayed in a window, click the **Edit** menu, and then select **Apply a Filter**.
- 4 Select the basic filter you defined for use with your custom report, and then select **Apply**.
- 5 With the filter applied to your log source, click the **Reports** menu, and then select **Run a Report Now**.
- 6 Select the custom report you want to run from the list, and then select **Run Report**.
- 7 After the report is finished, select **View HTML** or **View CSV** depending on what output format you want to review the data in.

How To Report Against Log Records in Database Tables

- 1 In WhatsUp Event Analyst, click the **File** menu, and then select **Open Database Table Links**.
- 2 Select the appropriate database table link, log type, and then click the **Filters** button to apply the basic or advanced filter appropriate for the custom report you are preparing.
- 3 Click **Build Report**.
- 4 Select the custom report you want to run from the list, and then select **Run Report**.
- 5 After the report is finished, select **View HTML** or **View CSV**, depending on what output format you want to review the data in.

Producing Custom Reports on a Scheduled Basis

For more information on how to instruct WhatsUp Event Analyst to produce your custom reports on a scheduled basis, please review the Report Scheduler and Report Scheduling Configuration dialog help topics in the WhatsUp Event Analyst Help and Users Guide.

Custom Report Output Formats: HTML and CSV

Just like WhatsUp Event Analyst's pre-built reports, your custom reports can be produced in both HTML and CSV (comma-delimited text) formats.

If your custom report contains a limited number of records (e.g. less than 10000), the HTML version of the report may be the best way to review the data. The HTML version of the report displays the grouping levels just as you defined them in your custom report layout, enhancing its readability.

However, if your report contains a lot of records (e.g. 10000 or greater), or if you wish to do your own further analysis of the result set in a spreadsheet program like Microsoft Excel, working with the CSV version of the report is ideal. The CSV version of your custom report contains just the raw, extracted field information which you can further group, sort, and manipulate in programs external to WhatsUp Event Analyst.