



IBM India Software Labs

Tivoli Security Information and Event Manager

Reporting in TSIEM

Aslam Siddiqui

Boudhayan Chakrabarty

Introduction to Reports

- **Tivoli® Security Information and Event Manager provides dozens of security compliance reports that enable you to check compliance with security policy, to verify the log collection events, and to analyze data in the Log Management Depot.**
- **The log management reports are accessed through the Log Management Dashboard.**
- **The Tivoli Common Reporting report set can be accessed through the navigation panel in the Tivoli Integrated Portal as well as through the Log Management reports.**

Tivoli Security Information and Event Manager provides many security compliance reports, including:

- **Graphic reports**
- **Event summary reports**
- **Event detail reports**
- **Trend reports**
- **Standard reports**
- **Custom reports**
- **Log management reports**
- **Compliance management module reports**
- **Tivoli Common Reporting reports**

Graphic Reports

- **Graphic reports provide visual analyses of security policy compliance activities. The purpose of graphic reports is to show you, at a glance, the status of security compliance in your organization.**
- **Examples of graphic reports include the Enterprise Overview graph, the Trend graphic, the Database Overview graphic, some of the Log Manager reports, and others**

Example of Enterprise overview and Trend graphic

Compliance Dashboard

Dashboard
Trends
Reports
Regulations
Policies
Groups
Distribution
Settings

CIFDB

Compliance Dashboard

Database AGGRDB on Server CIFDB

Enterprise Overview
Settings

Events by top event count by "Who" and "on What" from May 1, 2009 till Aug 1, 2009.

Who

GROUP00194	▶	●	●	●	●
GROUP01787	▶	●	●	●	●
GROUP03905	▶	●	●	●	●
GROUP03986	▶	●	●	●	●
GROUP04335	▶	●	●	●	●
GROUP05171	▶	●	●	●	●
GROUP05598	▶	●	●	●	●
GROUP05740	▶	●	●	●	●
Other Sources	▶	●	●	●	●
Staff	▶	●	●	●	●

Trend graphic

Percentage of Policy Exceptions from May 13, 2009 till Aug 1, 2009.
Settings

5

© 2012 IBM Corporation

Event summary reports

- **Event summary reports, or event lists, provide lists of all events that match the specified criteria. For example, you can see a list of all events that occurred during a particular time period. Event summary reports are useful for seeing what other events occurred at the same time or affected the same technological assets, or otherwise share a W7 attribute.**
- **From the event list, you can drill down to see event detail reports.**

Example of Event summary reports

Compliance Dashboard ? -

[Dashboard](#)
[Trends](#)
[Reports](#)
[Regulations](#)
[Policy](#)
[Groups](#)
[Distribution](#)
[Settings](#)

CIFDB > SELFAUDIT > All Events

All Events

Database SELFAUDIT on Server CIFDB

Setup:

Start time: Month: Day: Year: Hour: Min:

End time: Month: Day: Year: Hour: Min:

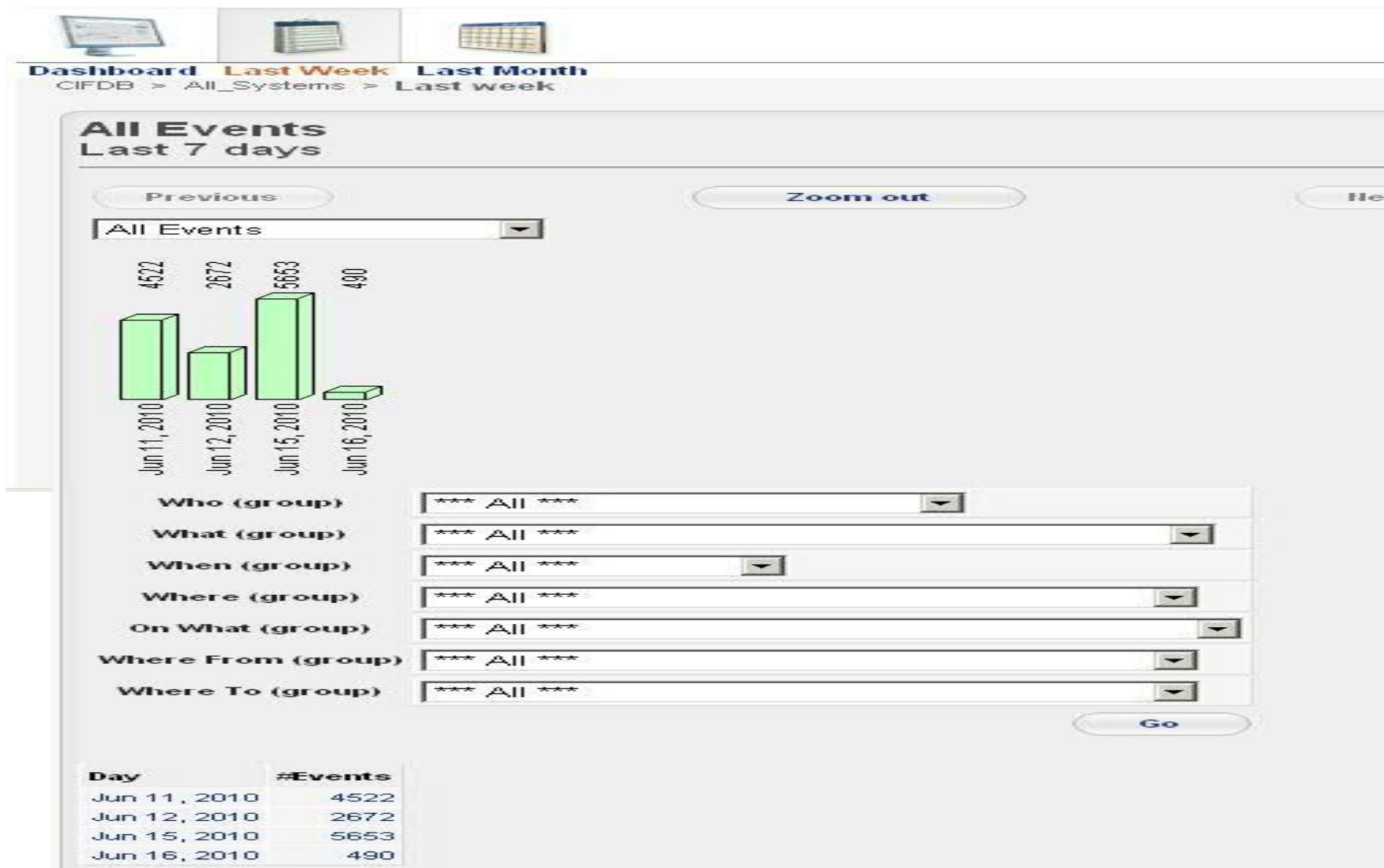
Time zone:

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where From (detail)	On What (detail)	Where To (detail)
30	9/28/12 7:00:10 PM (-1200)	1	Access : Dbinstance / Success	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	CIFADMIN	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	DBINSTANCE : - / CIFINST	cldfp21 (IBM DB2 9.5 - 9.X on Windows)
10	9/28/12 6:30:03 PM (-1200)	1	Rotate : Auditlog / Success	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	CIFADMIN	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	AUDITLOG : default / db2audit.instance.log	cldfp21 (IBM DB2 9.5 - 9.X on Windows)
10	9/28/12 6:30:08 PM (-1200)	1	Access : Dbinstance / Success	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	CIFADMIN	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	DBINSTANCE : - / CIFINST	cldfp21 (IBM DB2 9.5 - 9.X on Windows)
10	9/28/12 6:30:08 PM (-1200)	1	Convert : Auditlog / Success	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	CIFADMIN	cldfp21 (IBM DB2 9.5 - 9.X on Windows)	AUDITLOG : default / db2audit.instance.log	cldfp21 (IBM DB2 9.5 - 9.X on Windows)
	9/28/12 6:30:09 PM		Access : Dbinstance /	cldfp21 (IBM DB2 9.5 - 9.X		cldfp21 (IBM DB2 9.5 - 9.X on		cldfp21 (IBM DB2 9.5 - 9.X on

Trend reports

- **Trend reports show security events over specific time periods.**
- **Trend reports are useful for identifying general trends in security compliance.**
- **You can drill down into the trend reports to see information about specific events.**

Example of Trend reports



Standard Reports

- **Tivoli® Security Information and Event Manager provides dozens of standard reports that enable you to view event data**
- **Standard reports are listed in the My Reports page.**
- **Standard reports can be viewed by under My Reports page by clicking the Reports icon in the Compliance Dashboard.**
- **Reports are organized in four main Report Centers, or sets of reports:**

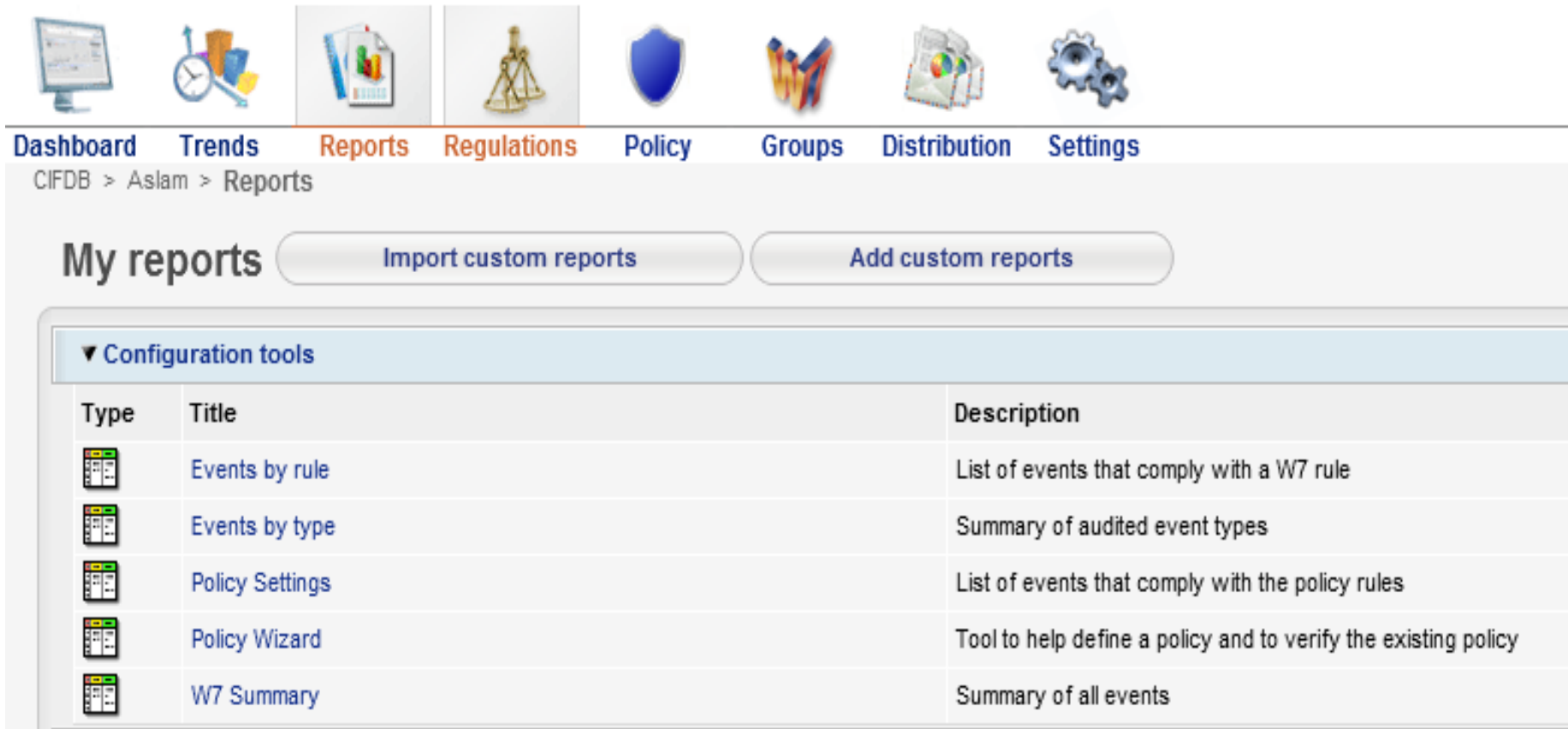
Four main Report Centers

- **Configuration tools**
- **Daily verification reports**
- **Detailed investigation reports**
- **Firewall reports**

Configuration tools

- The standard reports include the Configuration tools reports, which provide information about how events, policies, and rules are configured in Tivoli® Security Information and Event Manager.
- To show or hide the Configuration tools section, click the title bar. If the section is hidden, then it will be shown. Likewise, if the section is shown, then it will be hidden.
- There are several available Configuration tools:
 - Events by rule
 - Events by type
 - Policy Settings
 - Policy Wizard
 - W7 Summary

Example of Configuration tools








Dashboard Trends **Reports** Regulations Policy Groups Distribution Settings

CIFDB > Aslam > Reports

My reports [Import custom reports](#) [Add custom reports](#)

▼ Configuration tools

Type	Title	Description
	Events by rule	List of events that comply with a W7 rule
	Events by type	Summary of audited event types
	Policy Settings	List of events that comply with the policy rules
	Policy Wizard	Tool to help define a policy and to verify the existing policy
	W7 Summary	Summary of all events















Daily verification

- **The standard reports include the daily verification reports, which provide information about different types of security events. A security administrator might want to review the daily verification reports every day to see if any critical events occurred.**
- **To show or hide the Daily verification section, click the title bar. If the section is hidden, then it will be shown. Likewise, if the section is shown, then clicking the title bar will hide the section.**

Daily verification reports:

- Alerts
- All Exposures
- DBA (database administrator) Activity
- Events by type
- Failed System Operations
- Failed System Services
- Failed Transactions
- Impersonation
- Logon Failure Summary

Example of Daily verification

▼ Daily verification		
Type	Title	Description
	Alerts	List of Alerts by Priority
	All Exposures	List of Exposures by Priority
	DBA Activity	List of changes to databases
	Events by type	Summary of audited event types
	Failed System Operations	List of failed operator and configuration commands
	Failed System Services	List of system processes that ended with (security) error condition
	Failed Transactions	List of failed transactions (SAP, Oracle)
	Impersonation	List of Users who caused events under another name
	Logon Failure Summary	Summary of Logon Failures
	Reconnaissance	List of actions to retrieve system information
	Restarts	List of system starts and restarts
	System Operations	Operator and system configuration activity
	System Update	List of modifications to the system
	Users	List of Users

Detailed investigation

- **The standard reports include the detailed investigation reports, which provide information about the details of security events.**
- **A security administrator might want to review the detailed investigation reports to see if any unusual or prohibited events are occurring on specific systems or performed by certain users. This is useful when investigating events.**
- **To show or hide the Detailed investigation section, click the title bar. If the section is hidden, then it will be shown. Likewise, if the section is shown, then clicking the title bar will hide the section.**

Detailed investigation reports:

- **Administration**
- **Administration per user**
- **Help Desk Activity**
- **In Period group by Users**
- **Logon History by Platform**
- **Logon History by User**
- **Object Audit**
- **Object History**
- **Out of Office Hours Activity**

Example of Detailed Investigation

▼ Detailed investigation		
Type	Title	Description
	Administration	List of administrative actions
	Administration per user	List of administrative actions by user
	Help Desk Activity	List of helpdesk security commands (enable/disable user)
	In Period group by Users	List of Users with events inside the specified Period groups
	Logon History by Platform	List of Platforms with Logon Events
	Logon History by User	List of Platform Users with Logon Events
	Object Audit	List of important Objects to Audit
	Object History	List of all Objects with events
	Out of Office Hours Activity	List of logons outside office hours
	Platform Events Summary	Summary of events reported by platform
	Platform History	List of all Platforms with events
	Platform events summary with message details	Summary of events reported by platform with message details
	Suspect by Object Group	List of Object Groups with Suspect Event
	Suspect by Platform	Platform summary with columns for the suspect event numbers
	User Audit	User Audit by Activity
	User History	List of All Platform Users with Events
	User audit by Object group	User activities on object groups
	Users by Event type	Summary of Users by Selected Event Type

Firewall

- **The standard reports include the Firewall reports, which provide information about firewall activity.**
- **A security administrator might want to review the Firewall reports to see if any breaches or unusual or prohibited activity are occurring on the firewall. This is useful when investigating events.**
- **To show or hide the Firewall reports section, click the title bar. If the section is hidden, then it will be shown. Likewise, if the section is shown, then clicking the title bar will hide the section.**

Firewall reports

- **Firewall Activity**
- **Firewall Overview**
- **Firewall Server Initiated Connections**
- **Firewall Suspects**

Example

▼ Firewall reports		
Type	Title	Description
	Firewall Activity	Summary of events and policy exceptions
	Firewall Overview	Active Web browsers, drops, weird sources, and low port usage
	Firewall Server Initiated Connections	Summary of server-initiated connections
	Firewall Suspects	Summary of suspects by policy exceptions, port scans and host scans

Customization of Reports

- **Report Editor can be used to create your own custom reports under the My Reports page and for any Compliance Management Modules that are installed.**
- **Custom reports include the following types of reports:**
 - **Event lists.**
 - **Summary reports.**
 - **Top- N report, where N is the number of events in a given time period.**
 - **Threshold reports.**

Viewing custom reports

- You can view custom reports in the My Reports page by clicking the Reports icon in the Compliance
- Example



The screenshot shows the IBM Compliance Dashboard interface. At the top, there is a breadcrumb trail: "Security Information Management" > "Compliance Dashboard". Below this, a navigation bar contains icons for Dashboard, Trends, Reports (highlighted), Regulations, Policy, Groups, Distribution, and Settings. The breadcrumb trail continues as "CIFDB > Aslam > Reports".

The main content area is titled "My reports" and includes two buttons: "Import custom reports" and "Add custom reports". Below these buttons is a section titled "Configuration tools" which contains a table of reports.


Type	Title	Description
	test	TSIEM test
	Events by rule	List of events that comply with a W7 rule
	Events by type	Summary of audited event types
	Policy Settings	List of events that comply with the policy rules
	Policy Wizard	Tool to help define a policy and to verify the existing policy
	W7 Summary	Summary of all events

Below the table, there is a section titled "Daily verification".

Creating custom reports using Report Editor

- **Open the Reports page.**
- **Click Add custom reports. The Report Editor opens.**
- **Specify the report parameters.**
- **When you have finished defining the report, you can either: Click Save to save the report in the Report page.**
- **Click Save & Show to save the report in the Reports page and also run the report and show the report results.**

Report Editor

- **Report Editor to create custom reports and to modify existing standard reports and custom reports**
- **The Report Editor streamlines the process of creating custom reports and adding the custom reports to either the My Reports page or to a compliance management module.**
- **To open the Report Editor: Open the My Reports page.**
- **Click Add custom reports. You can also open the Report Editor by selecting an existing custom report and clicking the pencil icon** 

Continued..

- **Specifying the General Information**

The General Information section of the Report Editor specifies the title of the report and the report center in which the report is displayed and provides a general description of the report.

- **Specifying the Report Layout**

The Report Layout section of the Report Editor specifies the type of report, the columns used in the report, and the charts used in the report.

- **Selecting the Data Criteria**

The Data Criteria section of the Report Editor specifies the types of events and any conditions of the events that are displayed in the report.

Specifying the General Information

▼ General Information

Title*:

Description:

Report Center*: Standard Report Center

Regulation Resource Center

Help Text:

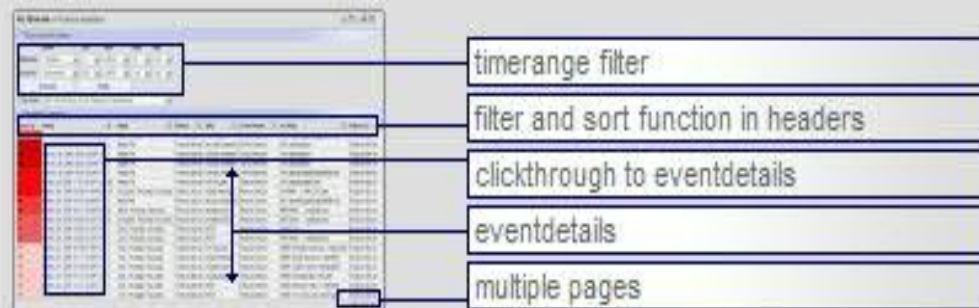
Specifying the Report Layout

Report Layout

Report Type

Select the types of report you would like to create. Mouse over the name to see an example.

- Event List
- Summary Report
- Top-N Report
- Threshold Report



a W7 normalized event list supporting drill through to underlying event detail.

Selecting the Data Criteria

Data Criteria

Event Selection

Select the types of events you would like to see. Only events that fall in all selected categories will be shown.

- Events
- Policy Exceptions
- Special Attention Events
- Failures
- Successes

The diagram shows four overlapping ovals: 'failures' (left), 'successes' (right), 'attentions' (bottom), and 'exceptions' (top). The intersection of 'failures', 'successes', and 'attentions' is shaded and labeled 'exceptions'. A larger oval encompassing all four is labeled 'all events'.

Conditions

Create the conditions of the events that you want to see in this report. Within every line-item you can compare a field with multiple values using a comma between the items. For the multiple line-items there is an AND-relation.

Field - Value	Field - Field
Compare a field with values	
field	
When group	↩
When items	
When group	
Who items	
Who group	
Who detail	
Who: Logon name	
Who: Real name	
Aspect	
What items	
What group	
What detail	
What: Verb	
<input type="button" value="Add"/> <input type="button" value="Clear"/>	

List of Conditions

Continued..

- Click on **Save and Show** .
- Once done you can see **Custom report** under **Reports Tab**

Compliance Dashboard

Dashboard Trends **Reports** Regulations Policy Groups Distribution Settings

CIFDB > Aslam > Reports

My reports

▼ Configuration tools

Type	Title	Description
	test	TSIEM test
	Events by rule	List of events that comply with a W7 rule
	Events by type	Summary of audited event types
	Policy Settings	List of events that comply with the policy rules
	Policy Wizard	Tool to help define a policy and to verify the existing policy
	W7 Summary	Summary of all events

Importing Custom reports into the "My Reports" page

- **Open the Reports page.**
- **Click Import custom reports. A field displays.**
- **Click Browse to use a file browser to select a report.**
- **Click Import to import the selected report. The report is displayed in the Reports page in the section specified in the report.**

Example of Importing Custom Reports



Dashboard Trends **Reports** Regulations Policy Groups Distribution Settings

CIFDB > Aslam > Reports

My reports

Select the file of the custom report you want to import

Distributing Reports

- **We can automatically distribute reports as email messages to a defined set of recipients by creating a distribution task on the Automated Report Distribution page.**
- **To access the Distribution configuration page: Open the Compliance Dashboard.**
- **Click the Distribution icon. The Automated Report Distribution page opens, where you can define distribution tasks and specify recipients.**

Distribution of Reports as email messages

- **In the Automated Report Distribution page, configure the sender e-mail in the Email Settings section.**
- **In the Manage Users section, specify the email addresses of recipients. Recipients must be defined as users in Tivoli Security Information and Event Manager.**
- **After you have configured the send email address and specified the email addresses of report recipients, click Add distribution task.**

Configuring email settings

- **The Edit Automated Distribution Task page opens, where you can create a schedule for Tivoli Security Information and Event Manager to send reports on a recurring basis.**
- **Before you can add a distribution task, you must first configure the settings for the sender email account and the mail host.**
- **Optionally, you can specify a notification email address, which contains information about every report that is sent by the automated report distribution.**

Configuring email settings(continued)..

- **To configure the email settings: Open the Compliance Dashboard.**
- **Click the Distribution icon. The Automated Report Distribution page opens, where you can define distribution tasks and specify recipients.**
- **Expand the Email Settings section and specify the sender email address and the notification email address.**
- **Next, specify the recipient addresses in the Addresses section**

Example

✦ Email Settings

✦ Sender

These settings will be used by every Automated Report Distribution task.

From email name:

From email address:*

Reply-to email address:

Mail-host:*

* Required field

✦ Notification

Every Automated Report Distribution task will send a notification email to this address. A notification email contains details of every report sent by Automated Report Distribution, including successes, failures, or empty reports. If left empty, a notification will not be sent.

Notification email address:

Managing users

- **Before you can add a distribution task, you must specify the email addresses of the report recipients.**
- **To specify users: Open the Compliance Dashboard.**
- **Click the Distribution icon. The Automated Report Distribution page opens, where you can define distribution tasks and specify recipients.**

Managing users(continued)..

- **Expand the Manage Users section and specify the email addresses of the people to whom reports will be sent.**
- **Click Save.**
- **The Manage Users section lists the names of Tivoli® Security Information and Event Manager users.**
- **In order for Tivoli Security Information and Event Manager to send users reports by email, you must specify a valid email address is required for each recipient. If the email address field is left empty, then reports cannot be sent to that user.**

Example of Manage users

Manage Users

User Name	E-mail Address
 CIFNEWUSER	<input type="text" value="cifauditor@tsiemwm.com"/>
 CIFOWNER	<input type="text" value="ibm-tsiem@tsiemwm.com"/>

Save Cancel

Adding a distribution task

- **To create a distribution task: Open the Compliance Dashboard.**
- **Click the Distribution icon. The Automated Report Distribution page opens.**
- **Click Add distribution task. The Edit Automated Report Distribution Task page opens, where you can define or modify a distribution task.**
- **In the General Information section, configure the email message and specify the report format. If you want to send reports on a regular basis, configure a schedule for when the distribution task will run.**

Add a distribution task (continued)..

- **In the Reports section, select which report or reports to send.**
- **In the Address section, select which users to send the reports to. Click Save.**
- **The Edit Automated Report Distribution Task closes, and the distribution task is listed on the Automated Report Distribution page.**

Example

Edit Automated Report Distribution Task

General Information

Email

Title:*

Body:*

* Required field

Report Format: PDF CSV

Also send reports when they contain no data:

Schedule

Start date: month day year
 October 17 2012

Run time: hour minutes
 18 : 51

Recurrence: Inactive Daily Weekly Monthly

This distribution task is set to inactive and will not run

Reports

Report	Database	Load Schedule	Action
-- There are no reports selected for this Distribution Task. --			
<input type="text" value="Select a report..."/>			

Addresses

User Name	E-mail Address	Action
-- There are no users selected for this Distribution Task. --		
<input type="text" value="Select a username..."/>		

General Information section

- **When you add a distribution task, you must provide some general information about the email message, report format, and report schedule**
- **You can specify this information in the General Information section of the Edit Automated Report Distribution Task page.**

Email

- **In the Email section of the General Information section, specify the following parameters: Title Subject line of the email.**
- **For example, title might include the name of the report. This field is required. Body Message of the email. For example, the body might include the name of the report and why it is being sent to the recipient and any follow-up actions that the recipient might take. This field is required.**

Report Format

- **Specifies whether the report is sent in PDF format or in CSV format.**
- **By default, PDF is selected.**
- **Also send reports when they contain no data**
Specifies whether to send empty reports. By default, this option is not selected.

Schedule

- **In the Schedule section of the General Information section, specify the following parameters:**
Start date The date when Tivoli® Security Information and Event Manager begins to send reports.
- **Use the month, day, and year menus to select the date. Run time** The time when Tivoli Security Information and Event Manager starts the distribution run, that is, begins to send the reports. **Use the hour and minutes menus to select the time.**

Schedule(continued)..

- **Recurrence Specifies how often the distribution task runs. Options include: Inactive - The distribution task does not run.**
- **Daily - The distribution task runs every day.**
- **Weekly - The distribution task runs every week.**
- **Monthly - The distribution task runs every month.**

Example



Dashboard > Distribution > Edit Task

Edit Automated Report Distribution Task

▼ **General Information**

▼ **Email**

Title:*

Body:*

*** Required field**

Report Format: PDF CSV

Also send reports when they contain no data:

▼ **Schedule**

Start date: month: day: year:














Run time: hour: minutes:

Recurrence: Inactive This distribution task is set to inactive and will not run
 Daily
 Weekly
 Monthly

Reports

- **The Reports section of the Edit Automated Distribution Task page lists the selected reports in a table.**
- **The column headings include: Report Title of the report. Database Name of the Reporting Database that the report reports on.**
- **Load Schedule The load schedule for the selected Reporting Database, if any. Action Icon to remove the report from the list.**

Example

▼ Reports			
Report	Database	Load Schedule	Action
 ISO 27001 (11.2.4) Supervision and review	Bond	Never	
 W7 Summary	Bond	Never	
 Firewall Activity	SELFAUDIT	Working Days: 18:37	
 ISO 27001 (15.1.4) Data access	Bond	Never	
 ISO 27001 (12.4.3) Source code access	Test123	Never	
 System Operations	SELFAUDIT	Working Days: 18:37	
 Object History	▼	Select a database...	▼

Specifying Report recipients

- **Before you add a distribution task, you must specify the names and email addresses of the report recipients.**
- **This information can be specified in the Manage Users section of the Automated Report Distribution page.**
- **Addresses-The Addresses section of the Edit Automated Distribution Task page lists the selected recipients in a table. The column headings include:**

Specifying Report recipients(continued)..

- **User Name –Name of the Tivoli® Security Information and Event Manager user to whom the reports will be sent.**
- **Email Address -Email address of the Tivoli Security Information and Event Manager user to whom the reports will be sent.**
- **We can only send automated distribution tasks to Tivoli Security Information and Event Manager users (that is, users who have a registered user name in Tivoli Security Information and Event Manager).**

Example









Addresses

User Name	E-mail Address	Action
-- There are no users selected for this Distribution Task. --		
<input type="text" value="Select a username..."/>		

Save Cancel

Example of Automated report distribution

Report Distribution ?













Dashboard
Trends
Reports
Regulations
Policy
Groups
Distribution
Settings

Dashboard > Distribution

Automated Report Distribution

Add distribution task

▼ Distribution Task

Title	Run time	Recurrence	Start date	Action
 Test1	3:24:00 PM GMT-12:00	Every 1 day(s)	Apr 15, 2013	  
 Test144444	3:24:00 PM GMT-12:00	Every 1 day(s)	Apr 15, 2013	  
 Wow	3:24:00 PM GMT-12:00	Every 1 day(s)	Apr 15, 2013	  

Demo on Reporting

Questions/Comments!!!!