Compliant Enterprise

The Compliant Enterprise Active Control System

Release 2.0

Compliant Enterprise Reporter User's Guide

May 2007

NextLabs welcomes comments or suggestions regarding this manual or any of our product documentation. Please send an e-mail to info@nextlabs.com.

TRADEMARKS

LICENSE AGREEMENT

Published in San Mateo, CA, by NextLabs, Inc.
www.nextlabs.com
info@nextlabs.com
650.577.9101

Document Revision Number: RUG2.0-B03

Contents

Preface

Welcome to the Compliant Enterprise Active Control System, the information control platform that eliminates policy silos, controls information disclosure inside and outside the enterprise, and provides universal control over information access and use along with real-time enforcement. Only NextLabs delivers an Active Control System that can comprehensively enforce information access entitlements, protect end points while data is in use, and maintain reliable information barriers.

What's New in Release 2.0

Release 2.0 of Reporter includes the following new features and improvements over the 1.6 release:

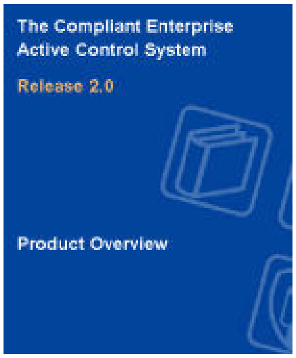
- Support for reporting on collaboration portals such as SharePoint
- Support for reporting on Linux file servers
- Support for reporting on custom obligations
- General improvements to useability and layout of the UI

Product Documentation

The Compliant Enterprise documentation set consists of eight titles: an introductory *Product Overview*; a *Getting Started Guide* with installation and configuration instructions; an *Implementation Guide* to help with strategies for auditing information use and designing policies; an administrator's guide for all enforcers and one for the system overall; user's guides for Policy Author and Reporter; and a guide to the predefined active control solutions available with release 2.0.

Product Overview

Because Compliant Enterprise is a powerful, distributed enterprise product, its components are likely to be used by a number of different users in any given organization. Even though various users may be engaged exclusively with individual components of the suite and may not be interested in any others, we strongly recommend that all users read the Product Overview carefully, in order to acquaint themselves with the high-level architecture and function of the platform as a whole.



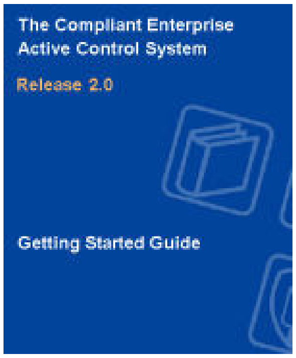
The Compliant Enterprise
Active Control System
Release 2.0
Product Overview

Getting Started Guide

The *Getting Started Guide* provides instructions on planning your system architecture and installing the Control Center and Policy Author.

The installation procedures for all policy enforcers are provided separately, in the *Enforcer Administrator's Guide*.

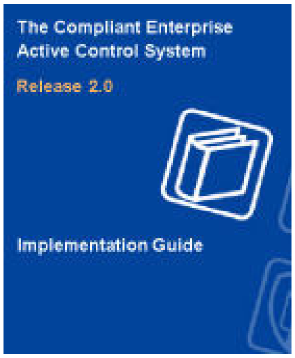
Instructions on enrolling network entities, which is required after installation, are also provided separately, in the *System Administrator's Guide*.



The Compliant Enterprise
Active Control System
Release 2.0
Getting Started Guide

Implementation Guide

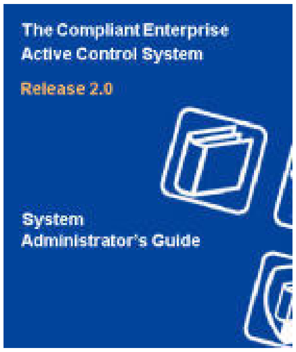
The *Implementation Guide* provides a high-level approach to designing and implementing the information control policies that best suit your enterprise's needs. It offers generic advice on analyzing your needs through information use audits, approaches to designing appropriate policies, and optimizing those policies based on ongoing monitoring.



The Compliant Enterprise
Active Control System
Release 2.0
Implementation Guide

System Administrator’s Guide

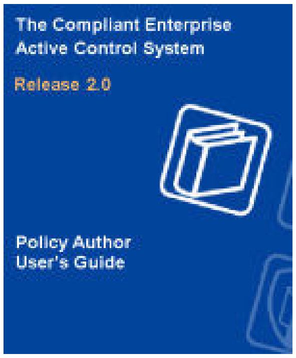
The *System Administrator’s Guide* provides information required for managing and maintaining the Compliant Enterprise system once it is set up. It provides complete instructrions on enrolling all kinds of network entities, which is required after the initial software installation. It also includes all user information for the administrative web application called Administrator, as well as for all utilities and other tools provided with the product. It is directed at the IT specialists who will be responsible for maintaining the Control Center after it has been installed.



The Compliant Enterprise
Active Control System
Release 2.0
System
Administrator's Guide

Policy Author User’s Guide

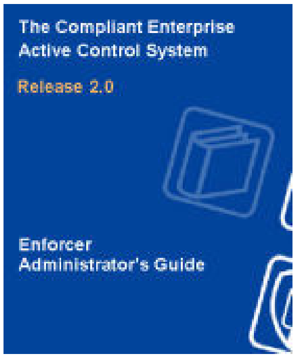
The *Policy Author User’s Guide* provides complete information on how to use Policy Author, the user interface where you build, deploy, and manage your information control policies and the library of policy components they are built upon. It is intended for the Compliant Enterprise user who will be responsible for converting generically expressed information policy goals into the specific, ACPL-based policy controls that are actually distributed to enforcement points throughout the enterprise.



The Compliant Enterprise
Active Control System
Release 2.0
Policy Author
User's Guide

Enforcer Administrator’s Guide

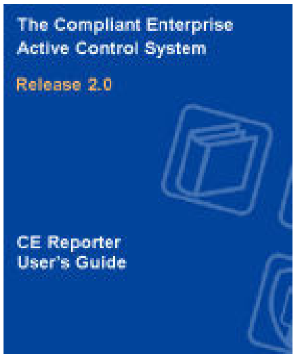
The *Enforcer Administrator’s Guide* provides information on installing, using and maintaining all the types of enforcers currently available for Compliant Enterprise: for Windows file servers, Linux file servers, Windows desktops, and SharePoint servers. It is intended for the technical specialists who will be managing the enforcers; these may be the same as the Control Center administrators, or they may be different.



The Compliant Enterprise
Active Control System
Release 2.0
Enforcer
Administrator's Guide

CE Reporter User’s Guide

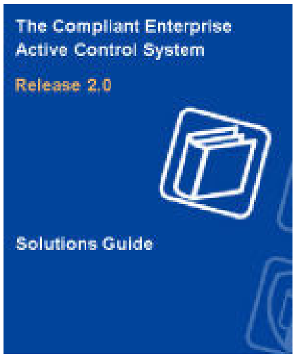
This user’s guide provides complete information on how to use Reporter, the web-based application that lets you easily generate reports on information use and access in your enterprise, and on the performance of your deployed policies. It is required reading for anyone with permission to generate or view Compliant Enterprise reports.



The Compliant Enterprise
Active Control System
Release 2.0
CE Reporter
User's Guide

Solutions Guide

The *Solutions Guide* provides detailed information on customizing and using the pre-designed Active Control Solutions that are included with Compliant Enterprise: for Information Entitlements, for Endpoint Data Protection, and for Business Information Barriers.



Current Versions

Documents distributed in PDF format can become obsolete as subsequent versions are released. If you would like to check whether you are using the most current version of this or any manual, check the Document Control Number (DCN) at the bottom right of the inside cover, then click here to view a table of the most current versions of all Compliant Enterprise manuals. If the version listed in that table is later than the one in this manual, contact info@nextlabs.com to request the more recent version.

Release Notes

The release notes for each release of Compliant Enterprise are available directly on the installation CD, from the link on the splash screen or from the Docs directory. They describe any features or changes that could not be included in the documentation, and provide a list of known problems with the current version, along with suggested workarounds when appropriate.

Feedback

Feedback from Compliant Enterprise users is a valuable resource in helping our Product Information group provide you with the highest quality documentation as our product line develops. To this end, we would appreciate any comments you have on this manual or on any other Compliant Enterprise documentation; please send all feedback to info@nextlabs.com.

1 Using Reports

This chapter describes all the features of Compliant Enterprise Reporter, the web application that allows you to easily generate reports of document access and use, and policy enforcement, throughout your enterprise. It is organized into the following sections:

- Introducing Reporter
- About Reports (page 12)
- Running Reports (page 20)
- Using Reports (page 22)
- Sample Reports (page 26)

Introducing Reporter

Reporter is a Web-based application that is used to run reports about policy enforcement and document activities logged by Compliant Enterprise in its Activity Journal. The reports can be customized to answer a wide variety of questions such as who is using certain documents, what types of enforcement are taking place, what activity occurred within a given department, and so on.

This application is intended for use by whoever is responsible for monitoring and reporting on compliance, gathering statistics about document usage, and investigating any suspected incidents of information mishandling. This may include administrators, IT staff, managers, executives, and auditors, or any other authorized personnel.

Starting Reporter

To start Reporter, perform the following procedure:

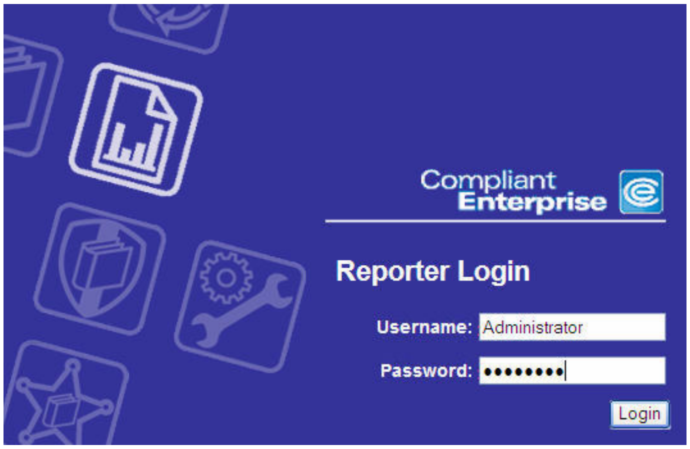
1. In your Web browser, enter the URL where Reporter is installed in your network. Typically, the URL is in the form https://*hostname*/reporter. If you do not know the URL, ask your Compliant Enterprise system administrator.

   Note: If you are using Firefox as your Web browser you cannot access Reporter unless you enable TLS 1.0 (under Tools, Options, Advanced). This is not required with Internet Explorer.

   When you successfully connect to Reporter, the Login page displays.

2. Type a valid user name and password. If you have not been assigned a user name, see your system administrator.

You can also use the built-in login name *Administrator*, along with the password that was set for the Administrator account during software installation.



Compliant Enterprise

Reporter Login

Username: Administrator

Password: ••••••••

Figure 1-1: Reporter Login Window

3. Click the Login button, and Reporter's main window displays.

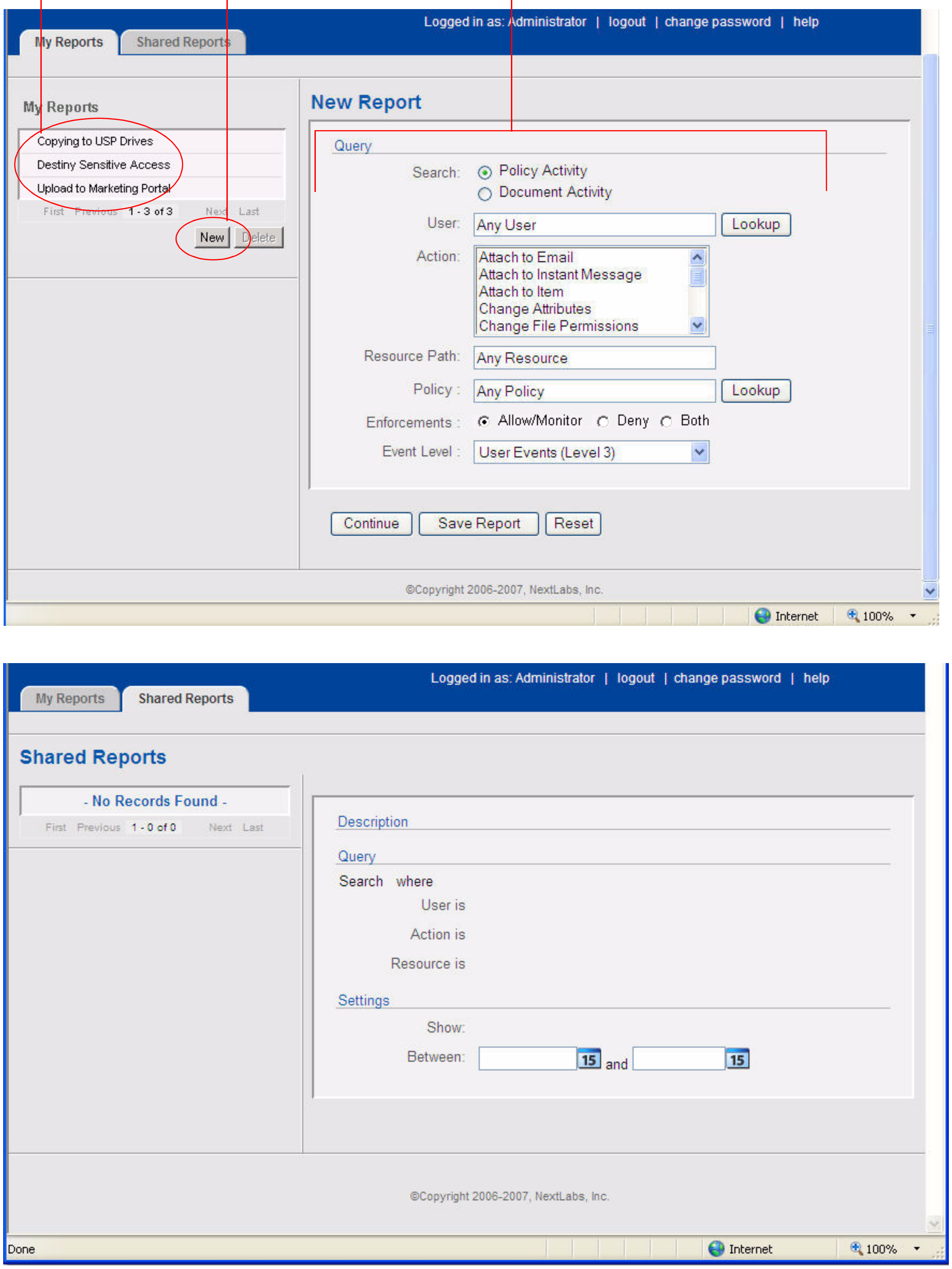
Using Reporter

Reporter's main window is divided into two tabs, My Reports and Shared Reports.

- **My Reports:** lists the names of reports that have been defined and saved by the user who is currently logged in, and provides an editing area where these reports can be modified and additional reports can be created.
- **Shared Reports**: lists all reports available for all Reporter users. Reports display here if their creator designated them as shared when they first created and saved them. Shared reports can be run from this screen, but not edited.

As Figure 1-2 shows, each tab is divided into two panes. The left pane is used for navigation. It shows a list of all the user-defined, saved reports that are currently available. The selection in this pane determines what is displayed in the right pane. To view the definition of a particular report, click its name in the list. To view controls for defining a new report, click New.

The right pane displays details of the definition of the report. In the My Reports tab, this pane provides controls to edit, delete, or run a report. In the Shared Reports tab, only a control to run the report is provided, since the shared reports are not open to editing by other users.



Select an existing report

Create a new report

Define or edit report query

Logged in as: Administrator | logout | change password | help
My Reports
Shared Reports
My Reports
Copying to USP Drives
Destiny Sensitive Access
Upload to Marketing Portal
First Previous 1 - 3 of 3 Next Last
New
Delete
New Report
Query

Search: ● Policy Activity ○ Document Activity

User: Any User

Action: Attach to Email, Attach to Instant Message, Attach to Item, Change Attributes, Change File Permissions

Resource Path: Any Resource

Policy : Any Policy

Enforcements : ● Allow/Monitor ○ Deny ○ Both

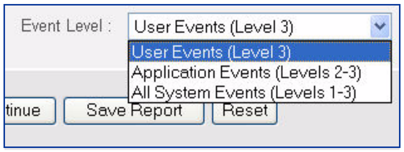
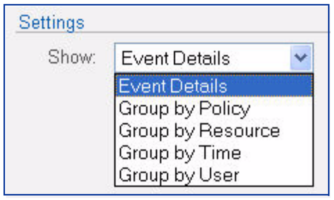
Event Level : User Events (Level 3)

Figure 1-2: The Reporter Main Window

About Reports

In Compliant Enterprise, a *report* is a formatted view of a particular set of information extracted from the Activity Journal. You define a report by specifying the *query criteria*—that is, one or more filters for the data contents you want in the report—and the *runtime report settings*, which determine how the report will actually run. Table 1-1 shows the available options for both these categories of settings.

Table 1-1: Report Definition Settings

Setting	Description
Query Criteria	
Search	For Policy Activity, the report will show all qualified instances of policies being enforced, consistent with the other query criteria For Document Activity, the report will show all activity in the system, consistent with the other query criteria—whether any policies were involved or not.
User	Specifies one or more users or groups whose activity this report will show. Click on the Lookup button to open the search window, where you can select from all currently defined users and groups.
Action	Specifies one or more actions on which to filter this report. The scroll list shows all currently defined actions; press Ctrl to select more than one from the list. Note that the actions available to filter by are different for Policy Activity and Document Activity reports. For details, see Table 1-2 and Table 1-3. Also, because policies involving Paste actions do not support logging obligations, instances of their enforcement will not be included in any reports.
Resource	Specifies a resource path on which to filter this report. Note that you can filter only by location (path)-based resources, not by file property-based ones.
Policy	Specifies one or more policies on which to filter this report. Click on the Search icon to open the search window, where you can select from all currently defined policies.
Enforcements	Allows you to filter on enforcements: Allow\Monitor, Deny, or both.
Event Level	Allows you to select the level of event verbosity your report will contain: • User-level events only (default) • Application- and user-level events • All system, application, and user-level events  Event Level : User Events (Level 3) User Events (Level 3) Application Events (Levels 2-3) All System Events (Levels 1-3) tinue Save Report Reset As a rule, you should leave this setting at the default, User Events only.
Runtime Report Settings	
Between	Defines the start and end dates of the time interval this report will cover. Click on the calendar icon to choose a date, or type it manually.
Show	Specifies the report display format: either an Event Details (tabular grid) or one of the grouped bar charts as described in Table 1-4 (page 20).  Settings Show: Event Details Event Details Group by Policy Group by Resource Group by Time Group by User

When you run a report, Reporter compares the information currently in the Activity Journal to the report criteria, selects the matching information (if any), calculates the totals, and displays the results in the format you have selected.

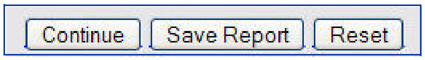
Once you define and save a report, it is listed in Reporter's navigation list. The report's creator can modify or delete the definition of the report; if the report is shared, others can run it and view the results, but cannot modify or delete it.

Creating a New Report

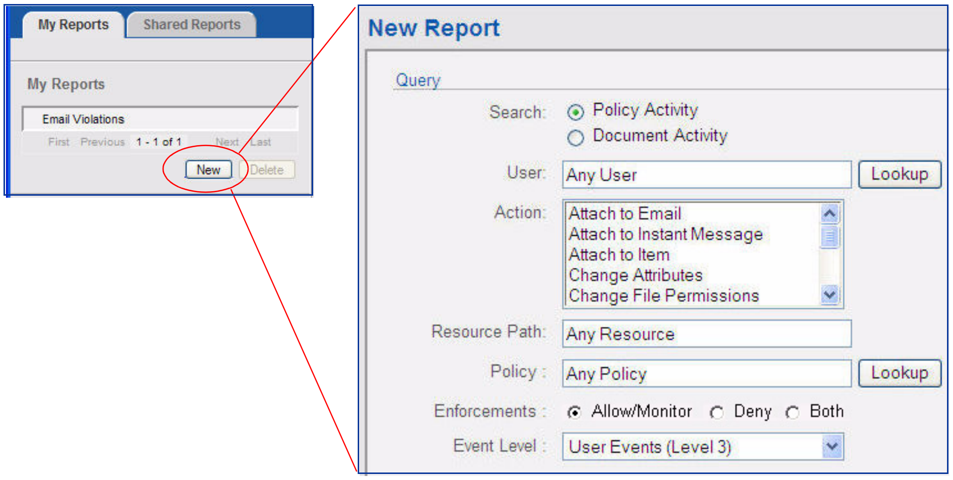
Whenever you create a new report, you must designate it as one of two types:

- **Policy Activity Report**: Provide information that is directly related to enforcement of policies. For example, you could generate a report listing all users who tried to open documents that are restricted by a currently deployed policy.
- **Document Activity Report**: Provide information that is automatically recorded in the Activity Journal by Compliant Enterprise but is not necessarily related to policy enforcement. For example, you can generate a report of all cases when someone stopped a Desktop Enforcer, or read its log files; or when users logged in and out. The exact type of information available depends on the Document Activity Audit Level of the relevant enforcer profile(s).

For either type of report, you have the option of creating for a single use, or saving it so it can be reused later.



1. On the My Reports tab, click the New button. This will display the query definition controls in the Report Definition pane, as shown in Figure 1-3.



Search: ● Policy Activity ○ Document Activity

User: Any User

Action: Attach to Email, Attach to Instant Message, Attach to Item, Change Attributes, Change File Permissions

Resource Path: Any Resource

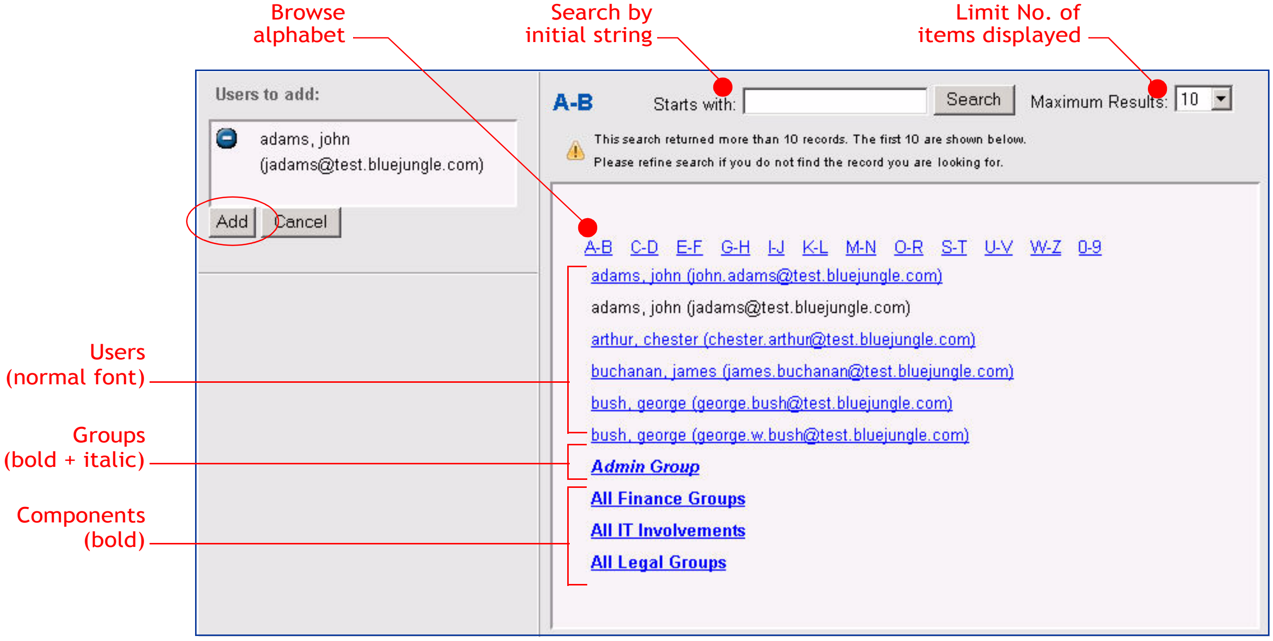
Policy : Any Policy

Enforcements : ● Allow/Monitor ○ Deny ○ Both

Event Level : User Events (Level 3)

Figure 1-3: The Report Definition Pane

2. For Search, choose the type of data you want to include in the report: Policy Activity or Document Activity.
3. For User, specify one or more users, groups, or user components you want to filter the report by. You can type these in manually; if you type more than one, separate them by commas. However, it is more reliable to use the selection tool (click the Lookup button), which displays the Users Search Window, where you can browse through all users and groups currently defined in your Information Network Directory (see Figure 1-4).



adams, john (jadams@test.bluejungle.com)

This search returned more than 10 records. The first 10 are shown below.
Please refine search if you do not find the record you are looking for.

adams, john (john.adams@test.bluejungle.com)
adams, john (jadams@test.bluejungle.com)
arthur, chester (chester.arthur@test.bluejungle.com)
buchanan, james (james.buchanan@test.bluejungle.com)
bush, george (george.bush@test.bluejungle.com)
bush, george (george.w.bush@test.bluejungle.com)
Admin Group
All Finance Groups
All IT Involvements
All Legal Groups

Browse alphabet

Search by initial string

Limit No. of items displayed

Users (normal font)

Groups (bold + italic)

Components (bold)

Figure 1-4: Users Search Window

This window lets you browse for users, groups, and user components. Select an intem in the list to display it in the Users to Add field at upper left; click the Add button when you are finished.

4. For Action, select the action or actions you want to show in this report. The list of available actions is not customizable, and the contents differ depending on whether you selected Policy Activity or Document Activity. (For details, see Table 1-2 and Table 1-3.)
5. For Resource, type the network path of the resource you want to filter by. Note that you can only filter by location (path)-based resources, not by those based on file properties.
6. For Policy Activity reports only: Specify one or more Policies, using the Lookup button to open a search window similar to the User search window. You can also type policy names manually; for more than one, separate them by commas.

7. For Policy Activity reports only: For Enforcements, specify the type of enforcement effects you want the report to focus on:
    - **Allow\Monitor**: Instances when the policy permitted the user to perform the action covered by the policy. Note that the report results always depend on what information was logged. If the policy does not have any On Allow logging obligation specified, then this report will not return any On Allow data whether you check this box or not.
    - **Deny**: Instances when the policy did not allow the user to perform the action.
8. Event Level: As a rule, you should leave this setting at the default, User Events only. This setting significantly reduces the amount of system “noise”—application- or system-level events that are accurately logged, but are generally not helpful in monitoring your policy or user activity. Higher verbosity levels are likely to include significant volumes of event traffic that is not directly useful for standard policy monitoring purposes.
9. If you do not need to save the report, click Continue. If you want to save the report, click Save Report. This opens the Save screen, as shown in Figure 1-5.
10. Provide a Name and Description for this report, and check the Is Shared box if you want other people to be able to run this report. All reports with this checkbox enabled will be available to other Reporter users, on their Shared Reports tab. When you log in, they appear on the My Reports tab.
11. Click Save Report again, and the new report name is added to the navigation list.

About Action Filters for Reports

As we mentioned, a different set of actions is available for filtering reports, depending on whether you choose Policy Activity or Document Activity type. All definitions of both sets of actions are provided in Table 1-2 and Table 1-3.

Table 1-2: Policy Activity Reports: Action Filters

Action	Report will include all instances of:
Attach to E-Mail	Users attaching any file covered by the policy to an e-mail message.
Attach to IM	Users attaching any file covered by the policy to an instant message.
Attach to Item	Users attaching any file covered by the policy to any kind of portal content, such as a list or a library; or uploading a file to a library or list.
Change Attributes	Users changing attributes of any file covered by the policy.
Change File Permissions	Users changing any of the security properties of any file covered by the policy.

Table 1-2: Policy Activity Reports: Action Filters (Continued)

Action	Report will include all instances of:
Copy	Users copying any file, or contents of any file, covered by the policy, or inserting one file into another.
Create/Edit	Users either editing an existing file covered by the policy, or creating a new file in any location covered by the policy.
Delete	Users deleting any file covered by the policy.
Export	Users export a spreadsheet or datasheet from a collaboration portal covered by the policy.
Move	Users moving any file covered by the policy from its current location to any other location.
Open	Users opening any file or portal content item covered by the policy .
Print	Users printing any file or portal content item covered by the policy .
Rename	Users changing the name of any file or portal content item covered by the policy .

Table 1-3: Document Activity Reports: Action Filters

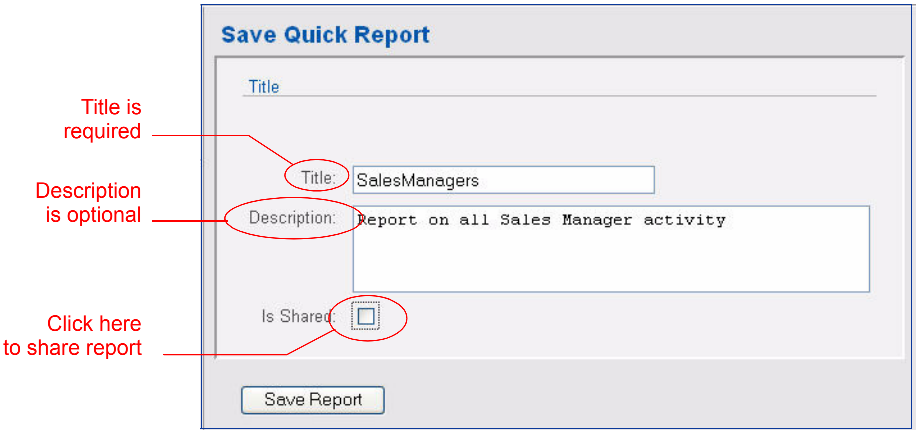
Action	Report will include all instances of:
Abnormal Enforcer Shutdown	Any Policy Enforcer shutting down under any circumstances other than by the standard use of the shutdown executable.
Attach to E-Mail	Users attaching any file covered by the policy to an e-mail message.
Attach to IM	Users attaching any file covered by the policy to an instant message.
Attach to Item	Users attaching any file covered by the policy to any kind of portal content, such as a list or a library; or uploading a file to a library or list.
Change Attributes	Users changing attributes of any file
Change File Permissions	Users changing any of the security properties of any file
Copy	Users copying any file or file contents, or any portal content, or inserting one file into another.
Create/Edit	Users either editing an existing file, or creating a new file in any location.
Delete	Users deleting any file
Enforcer Binary File Access	Users opening any binary files associated with any policy enforcer in the system.
Enforcer Configuration File Access	Users opening any configuration file of any policy enforcer in the system.
Enforcer Log File Access	Users opening any log file of any policy enforcer in the system.
Enforcer Shutdown (normal)	Any policy enforcer shutting down for normal reason.
Enforcer Startup	Any Policy Enforcer starting up.
Export	Users export a spreadsheet or datasheet from a collaboration portal.
Move	Users moving any file covered by the policy from its current location to any other location.
Open	Users opening any file covered by the policy. *Note:* When you deploy policies with Deny Open effects, you may see some unexpected reporting behavior regarding other actions for which Open is implied. See "About Implied Actions" (page 24).

Table 1-3: Document Activity Reports: Action Filters (Continued)

Action	Report will include all instances of:
Policy Bundle Authentication Failed	Policy bundle failed authentication.
Policy Bundle Authentication Succeeded	Policy bundle was successfully authenticated.
Policy Bundle File Access	Any user or process opening any bundle file.
Print	Users printing any file, either to hard copy or to a print file.
Rename	Users assigning a new name to a file or portal content item.
User Login	Users logging in to any PC in the system.
User Logout	Users logging out of any PC in the system.

Saving Reports

When you are defining a report, your work is not automatically saved. If you want to save the report for repeated use, or to share it with other users, you have to click the Save Report button before you stop work. Once a report is saved, you can find the report later in the list on the My Reports tab, as well as in the Shared Reports tab if you designated it as shared. Note that the Description field is optional, but it is highly recommended that you provide a clear description, especially if you plan to share the report with other users.



Title: SalesManagers

Description: Report on all Sales Manager activity

Is Shared: □

Title is required

Description is optional

Click here to share report

Figure 1-5: The Save Report Screen

Report Definition Syntax

There are a few important points to bear in mind about the syntax of report criteria.

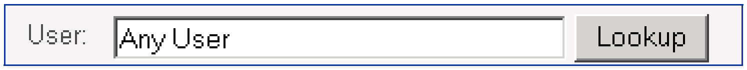
- If you put filters in multiple fields (such as User and Action), the criteria are combined with a logical AND: all criteria must be true for the data to match.
- If you put multiple values in a single field, the values within the field are combined with an OR: only one of the criteria needs to be true, for that particular field.

These are the same principles that apply to component and policy definition in Policy Author.

Filtering by User

You can filter the data by individual user name, or by user component. For example, you might include the user name Erik Tomchek as well as the user component ProductManagers, as follows: erik.tomchek@bluejungle.com, ProductManagers.

To ensure correct syntax, use the Lookup button to open the User Search Window, as shown in Figure 1-4 on page 14. Browse here to display and choose users, groups, or components; groups are indicated in bold italic, and component names are shown in bold.



User: Any User

You can also type query criteria directly. Bear in mind the following guidelines:

- You can list several search terms. Separate the items in a list with commas.
- The query is not case sensitive; *ProductManagers* and *productmanagers* will have the same effect.
- To type an individual user name, use the unique display name of the user; often, this is the user's e-mail address, but this can vary depending on the configuration of your system. To find out what format is used in your system, open the search window to choose the first user, and take note of the format that appears in the User field after you close the dialog.
- In specifying users, groups or components you can use the wildcard "*****", which matches zero or more characters including the backslash folder separator "\".

Filtering by Actions

You can filter the data by user actions (such as create, modify, send e-mail). You can select several actions from the list. The available choices vary depending on whether you are querying on policy activity or document activity. For the action filters available for policy reports, see Table 1-2 on page 15; for activity reports, see Table 1-3 on page 16.

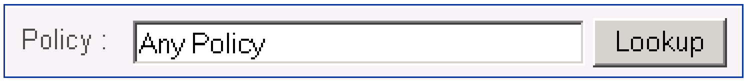
Filtering by Resources

You can filter the data by document directory (network path) only. You must type query criteria directly into the Resource field, using the following guidelines:

1. You can list several paths. Separate the items in a list with commas.
2. The query is not case sensitive: c:\ProgramFiles\* and c:\PROGRAMFILES\* will have the same result.
3. You can query on document directories only, not file names.
4. In specifying paths and file names, you can use the wildcard "*", which matches zero or more characters including the backslash folder separator "\".

Filtering by Policy

If you are querying on policy activity, you can filter the data by policy name. To ensure correct syntax, use the Lookup button.



Policy : Any Policy

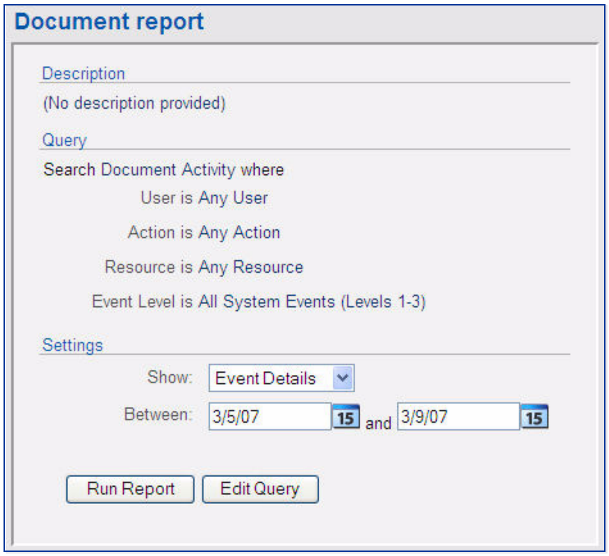
You can also type policy names directly, using the following guidelines:

- You can list several search terms. Separate the items in a list with commas.
- The query is not case sensitive: *PolicyA* and *policyA* will return the same results.
- If you use folders to organize policies, you must type the full folder path to the policy.
- To query on policy names, you can use the wildcard "*", which matches zero or more characters including the backslash folder separator "\".

Running Reports

You can run any report that you created, and any reports that other report authors have designated as shared. To run a report,

1. Select the name of the report you want to run. The details about that report appear in the Report Summary pane, as shown in Figure 1-6.



Document report

Description

(No description provided)

Query

Search Document Activity where

User is Any User

Action is Any Action

Resource is Any Resource

Event Level is All System Events (Levels 1-3)

Settings

Show: Event Details

Between: 3/5/07 and 3/9/07

Figure 1-6: The Report Summary Pane

2. For the Show setting, select an output format for the report. Table 1-4 provides information on all available formats.

Table 1-4: Available Report Formats

Format	Description
Event Details	A tabular (row and column) presentation of all data that matches the report criteria. No totals are calculated (except for the total number of records).
Group by Policy	A bar chart that shows totals for each policy included in the report.
Group by Resource	A bar chart that shows totals for each document included in the report.
Group by Time	A bar chart that shows totals for several periods of time within the specified report period. If the report period is one month or less, the data is totaled by day. If the time period is more than a month, the data is totaled by month.
Group by User	A bar chart that shows totals for each user included in the report.

3. For the Between setting, specify a start date and an end date to define the *report period*—that is, the interval of time covered by this report (see below).
4. Click Run Report. When Reporter finishes generating the report, it displays the results in the format you selected.

Time Zones

The report period is determined using the time zone where the Control Center is installed, not the time zone where you are running Reporter or the time zone where the events you are querying on occurred. Therefore, you might want to add one day to the beginning or end of your time period, depending on the time difference between the location of the Reporter application and the location where the events you are interested in occurred.

For example, suppose your Control Center is installed in New York, but you are running Reporter in California, three time zones to the west, and your query is on users in California. Your query will return three hours of data from the night before the first date in your time range (in California time), and will not include the last three hours of data on the final day of the range.

Using Reports

After you run a report, Reporter displays the results in your web browser.

If the report query matches more than 200 records, only the first 200 are shown in the report, though the total number of records is displayed. In such cases, you may want to refine your query to further restrict the data so that fewer than 200 records are returned. For example, query on a shorter time period—say, a week instead of a month.

Report Types

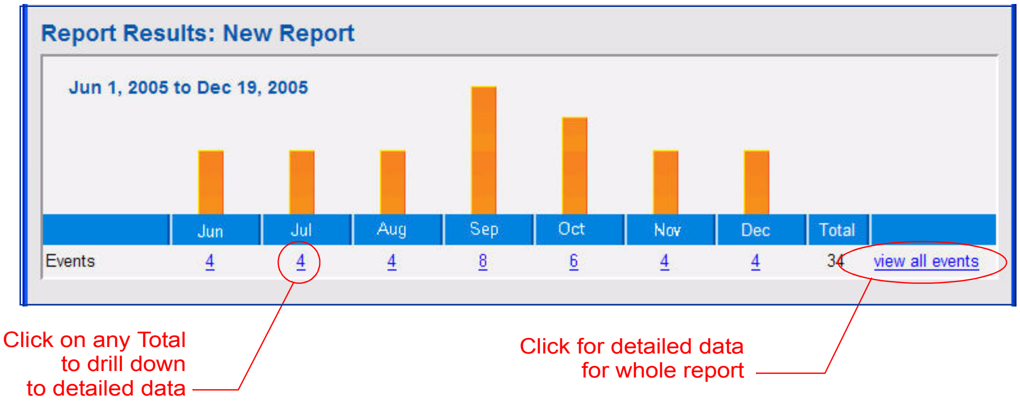
There are two general types of reports:

- **Grouped Format** reports are displayed as bar charts that summarize data grouped by policy, resource, time, or user;
- **Tabular** reports are displayed as tables, displaying event details in row and columns.

Grouped Format Reports

In the grouped report formats, the total for each group (day, month, user, policy, or document) is displayed as a hypertext link, which you can click to see details about the data included in that total. The details are displayed using the same tabular format as the Event Details style of report.

As Figure 1-7 shows, an additional link, View All Events, is also available. You can click on it to display details about all the data in the report.



Report Results: New Report

Jun 1, 2005 to Dec 19, 2005

	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total	
Events	4	4	4	8	6	4	4	34	view all events

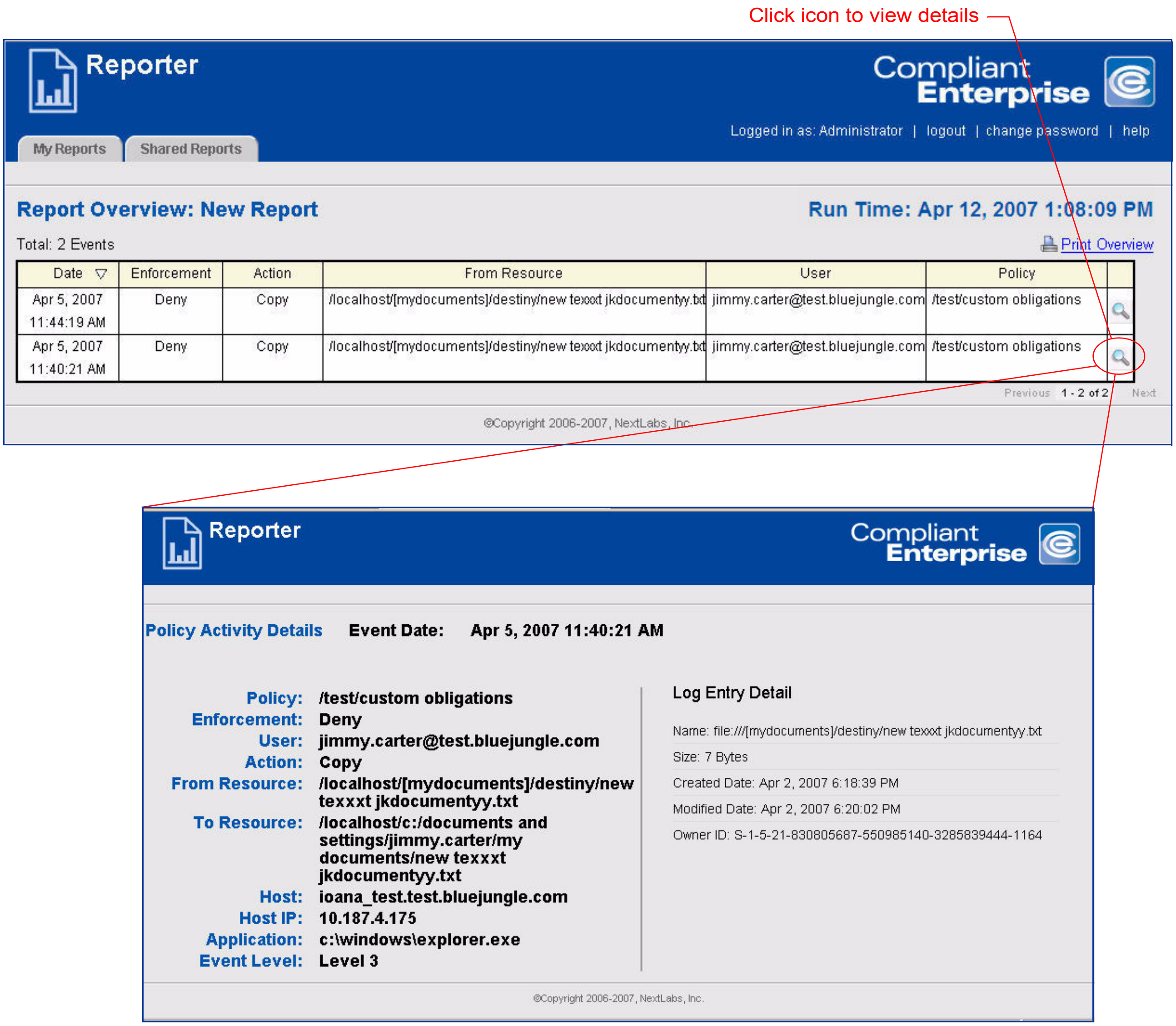
Click on any Total to drill down to detailed data

Click for detailed data for whole report

Figure 1-7: Drilling Down in a Grouped Format Report

Tabular Reports

Tabular reports, like the example in Figure 1-8, display a grid data resulting from the specified query, with each row representing one enforcement instance or other event. You can click on the magnifying glass at the end of the row to display all details about each event, as shown.



Click icon to view details

Reporter
Compliant Enterprise
Logged in as: Administrator | logout | change password | help
My Reports
Shared Reports

Report Overview: New Report

Run Time: Apr 12, 2007 1:08:09 PM

Total: 2 Events

Date ▽	Enforcement	Action	From Resource	User	Policy	
Apr 5, 2007 11:44:19 AM	Deny	Copy	/localhost/[mydocuments]/destiny/new texxxt jkdocumentyy.txt	jimmy.carter@test.bluejungle.com	/test/custom obligations	🔍
Apr 5, 2007 11:40:21 AM	Deny	Copy	/localhost/[mydocuments]/destiny/new texxxt jkdocumentyy.txt	jimmy.carter@test.bluejungle.com	/test/custom obligations	🔍

©Copyright 2006-2007, NextLabs, Inc.

Policy Activity Details Event Date: Apr 5, 2007 11:40:21 AM

Policy:	/test/custom obligations
Enforcement:	Deny
User:	jimmy.carter@test.bluejungle.com
Action:	Copy
From Resource:	/localhost/[mydocuments]/destiny/new texxxt jkdocumentyy.txt
To Resource:	/localhost/c:/documents and settings/jimmy.carter/my documents/new texxxt jkdocumentyy.txt
Host:	ioana_test.test.bluejungle.com
Host IP:	10.187.4.175
Application:	c:\windows\explorer.exe
Event Level:	Level 3

Log Entry Detail

Name: file:///[mydocuments]/destiny/new texxxt jkdocumentyy.txt

Size: 7 Bytes

Created Date: Apr 2, 2007 6:18:39 PM

Modified Date: Apr 2, 2007 6:20:02 PM

Owner ID: S-1-5-21-830805687-550985140-3285839444-1164

©Copyright 2006-2007, NextLabs, Inc.

Figure 1-8: Using Tabular Reports

Report Anomalies

Bear in mind that reports can show unexpected results at times, that may seem to reflect incorrect behavior of policies, but in fact are a result of some of the ways Windows works internally.

About Implied Actions

When Windows Explorer handles file operations, it sometimes performs several actions sequentially in a way that is not visible to the user. For example, when you run Copy on a file, Explorer first opens it, then reads the content, then writes a copy to the new location. Similarly, in order to print a file, Explorer must first open it, then send it to the print server. In fact, most of the actions you deal with in policies also involve Open in this way, as what might be called an *implied action*.

Because Open is a very common implied action, you may see some reporting anomalies whenever you deploy several policies, one of which involves a Deny Open or Allow Only Open effect. For example, suppose you have a Deny Open policy deployed, then deploy a second policy with a Deny Print effect, test it for a while, and run a report on the test activity. The test behavior will seem correct—printing is blocked, as intended—but the report will not show any instances where Print actions were denied; instead it shows many cases of Open actions being blocked. This can seem like an error in the policy or in the report, but it actually reflects the fact that, because the actions implicitly triggered the Deny Open policy, they were blocked by that rather than by the Deny Print policy.

Bear in mind that if you encounter this kind of seeming anomaly regarding actions in your reports, it is likely that some kind of implied action (involving Open, specifically) is the cause.

Preview Activity

When you use the Preview feature in Policy Author to preview document-type components, Policy Author internally performs a Read action on the underlying documents in order to display information about them in Preview pane. This may lead to unexpected reporting results if, for example, you have deployed policies that prohibit users from reading these document resources. Even though the policy is correctly blocking this activity by users, your report may show instances of Read actions—those performed in the course of Preview. This can be confusing at times, since there is no way Reporter can distinguish between actions performed internally by Policy Author, and those actually performed by users.

Querying by User Groups

Activity Journal data for an individual cannot be queried based on some group until that individual is enrolled as a member of that group. This can produce cases that seem to indicate errors in reporting. For example, let’s say Tanya is enrolled as a member of the Active Directory user group “QA Team” on July 25, and that information is propagated to Compliant Enterprise by an automatic update that same evening. If an analyst runs a monthly report on the QA group’s activity, none of Tanya’s activity before the 26th will be included in the report, only her activity from the 26th to the 31st. In other words, when you query on a group, Compliant Enterprise filters the log data not on each user per se, but on the *user while a member of that group*.

If you encounter a report that seems to show this kind of gap in a user's activity, this is a likely cause. You can test it by running a different report based on individual users, actions or resources, rather than groups. If this is done in our example, all of Tanya's activity for the whole month will be included in the report.

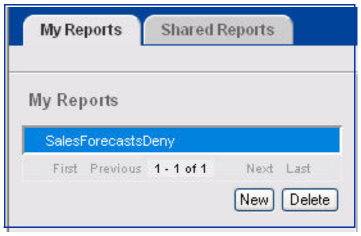
Modifying Reports

As your organization changes over time, you might want to change an existing report to include new categories of data. You may also decide to modify a report definition to make it a shared report, so that it is available for others to use.

To modify a report, select the report name to display the Report Details pane, then click the Edit Query button. When you have finished your changes, click the Save Report button.

Deleting Reports

You can delete any report listed on the My Reports tab; simply select the report and click the Delete button on the Report Summary pane. Reports cannot be deleted from the Shared Reports tab; everything there is read-only.

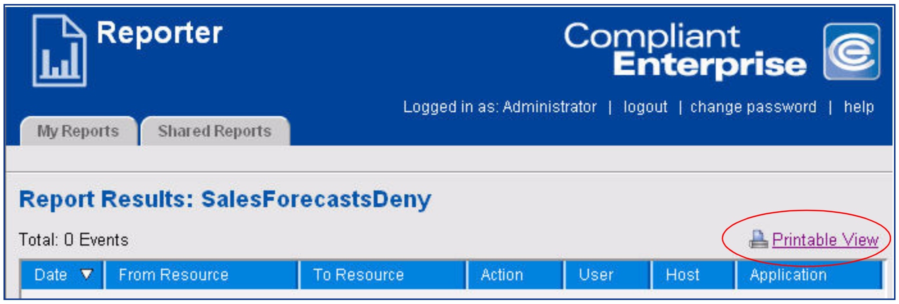


Printing Reports

You can print both types of reports. To print a bar chart, use your browser's standard print command—typically File, Print.

To print a tabular report:

1. Click the Printable View link, to the upper right of the table. The report reappears with web-based navigation controls and links removed. All the data is shown in one page, to a maximum of 200 records.



Report Results: SalesForecastsDeny

Total: 0 Events

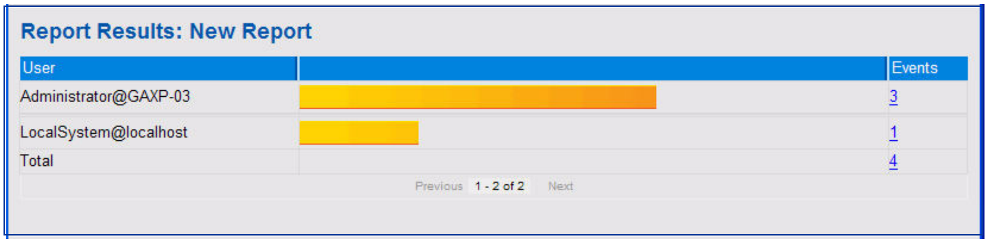
Date ▼	From Resource	To Resource	Action	User	Host	Application

Figure 1-9: Printing a Tabular Report

2. Set the "scale to fit" option in your browser.
3. Use your browser's standard print command to print the page.

Sample Reports

The following figures provide samples of two grouped format reports and one tabular report.

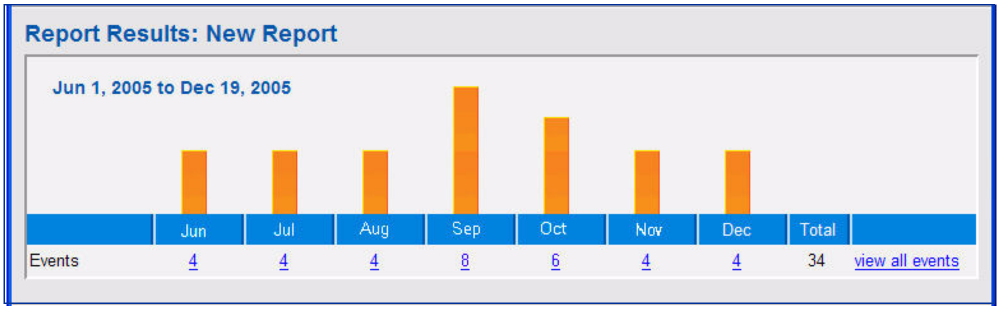


Report Results: New Report

User		Events
Administrator@GAXP-03		3
LocalSystem@localhost		1
Total		4

Previous 1 - 2 of 2 Next

Figure 1-10: Grouped by User Report

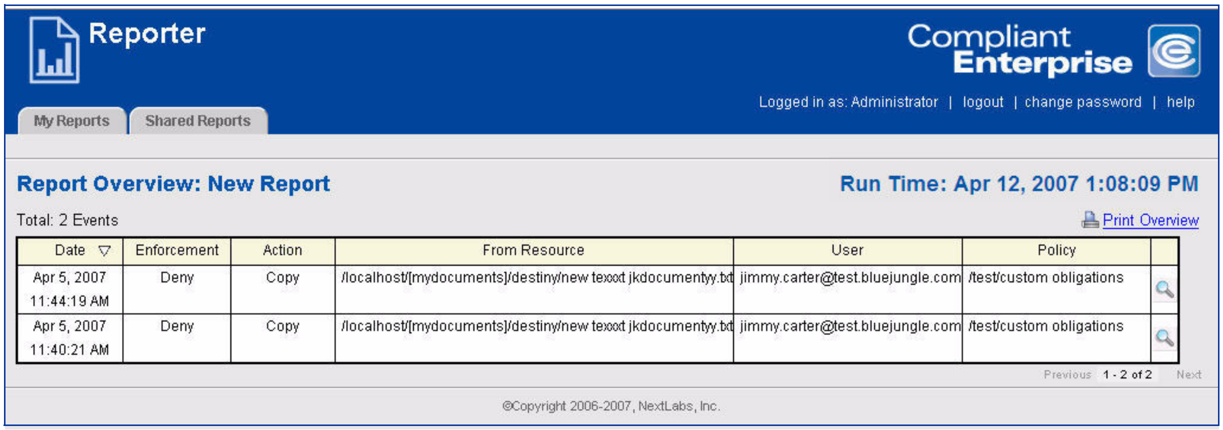


Report Results: New Report

Jun 1, 2005 to Dec 19, 2005

	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total	
Events	4	4	4	8	6	4	4	34	view all events

Figure 1-11: Grouped by Time Report



Reporter
Compliant Enterprise
Logged in as: Administrator | logout | change password | help
My Reports
Shared Reports

Report Overview: New Report

Run Time: Apr 12, 2007 1:08:09 PM

Total: 2 Events

Print Overview

Date ▽	Enforcement	Action	From Resource	User	Policy	
Apr 5, 2007 11:44:19 AM	Deny	Copy	/localhost/[mydocuments]/destiny/new texxxt jkdocumentyy.txt	jimmy.carter@test.bluejungle.com	/test/custom obligations	🔍
Apr 5, 2007 11:40:21 AM	Deny	Copy	/localhost/[mydocuments]/destiny/new texxxt jkdocumentyy.txt	jimmy.carter@test.bluejungle.com	/test/custom obligations	🔍

Previous 1 - 2 of 2 Next

©Copyright 2006-2007, NextLabs, Inc.

Figure 1-12: Event Details Report (Tabular)

Index