eTrust® Audit and eTrust® Security Command Center

Audit & SCC Release Summary

r8 SP2

CA Product References

This document references the following CA products:

- CA eTrust® Audit
- CA eTrust® Security Command Center (SCC)

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 1: New Features

This section contains the following topics:

Web-based User Interface

The eTrust Audit user interface has been updated and reorganized to reflect new functionality and improve work flow. Entirely new web-based features include:

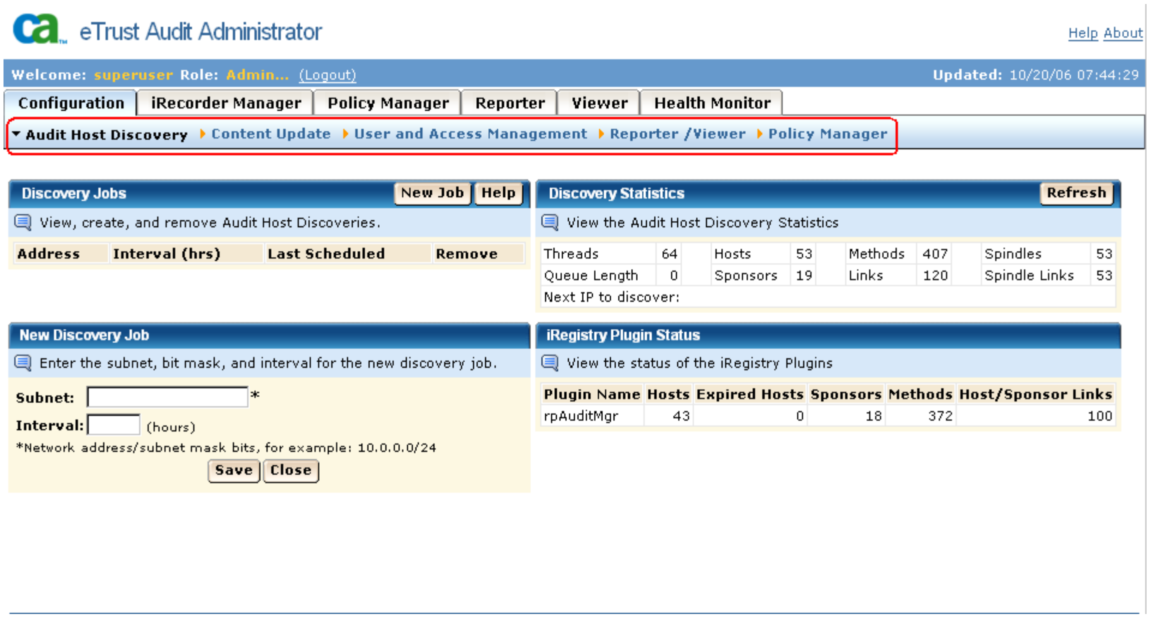
- Audit Policy Manager
- Audit Reporter
- Audit Viewer

These features replace the Win32 interfaces for all eTrust Audit components except Security Monitor, which remains a Win32 interface. The following topics illustrate some of the new interface features.

Note: The new web-based interface introduces significant changes to the Policy Manager and other administrative tasks. Before you upgrade or use the new interface, it is important to review the *eTrust Audit and eTrust Security Command Center Administration Guide*. Additional information is also available in the online help for the Audit Administrator interface and the *eTrust Audit and eTrust Security Command Center Implementation Guide*.

Updated Configuration Interface

The updated Audit Administrator configuration interface lets you complete various types of management and configuration tasks using the UI subtabs as shown in the following illustration.



Welcome: superuser Role: Admin... (Logout) Updated: 10/20/06 07:44:29

View, create, and remove Audit Host Discoveries.

Address	Interval (hrs)	Last Scheduled	Remove

View the Audit Host Discovery Statistics

Threads	64	Hosts	53	Methods	407	Spindles	53
Queue Length	0	Sponsors	19	Links	120	Spindle Links	53
Next IP to discover:							

Enter the subnet, bit mask, and interval for the new discovery job.

Subnet: *

Interval: (hours)

*Network address/subnet mask bits, for example: 10.0.0.0/24

View the status of the iRegistry Plugins

Plugin Name	Hosts	Expired Hosts	Sponsors	Methods	Host/Sponsor Links
rpAuditMgr	43	0	18	372	100

Audit Host Discovery

Lets you set up and view discovery job status for eTrust Audit Hosts.

Content Update

Lets you update Audit Administrator content by downloading template information and Message Parsing (MP) files from a CA website.

User and Access Management

Lets you configure user role assignments and access to the interface for your Audit Administrator environment.

Reporter/Viewer

Lets you configure eTrust Audit Data Sources for use by the Reporter and Viewer utilities.

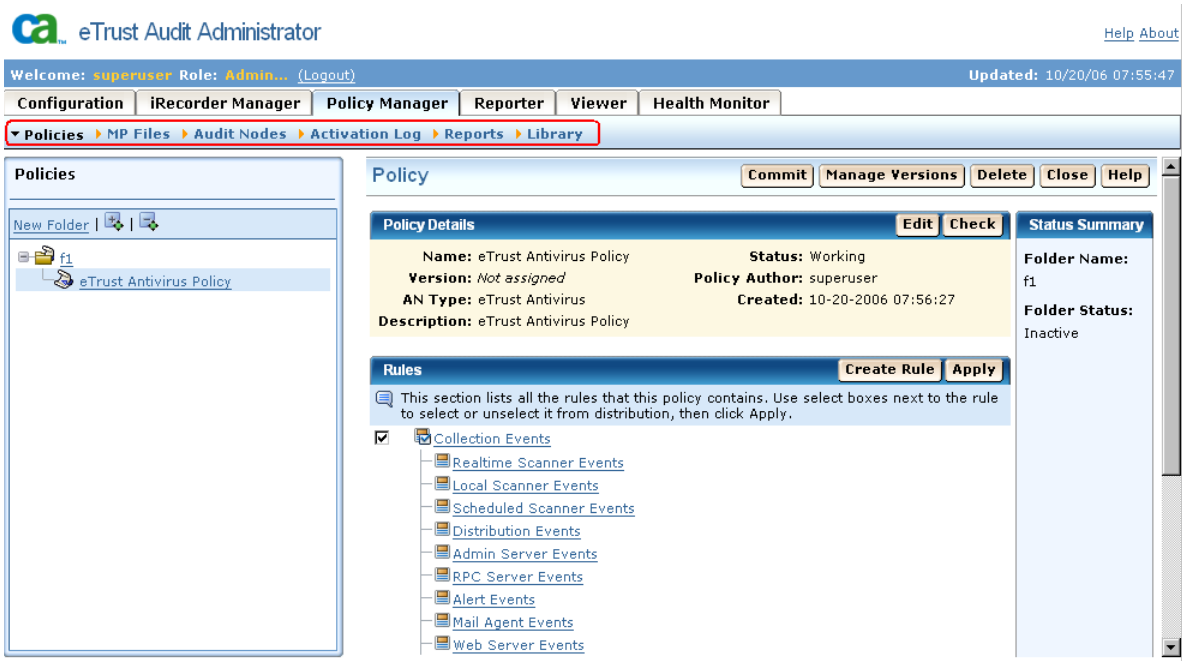
Policy Manager

Lets you perform Policy Manager administration tasks, configuring the Distribution Server and managing locked Policy Manager objects.

See the "Managing Audit Administrator" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Configuration interface. Task-based information for each of the UI subtabs illustrated here is contained in its own sub-chapter.

New Policy Manager Interface

The new Policy Manager interface lets you perform tasks related to creation and distribution of policies and MP files using the UI subtabs as shown in the following illustration.



Name: eTrust Antivirus Policy
Version: *Not assigned*
AN Type: eTrust Antivirus
Description: eTrust Antivirus Policy
Status: Working
Policy Author: superuser
Created: 10-20-2006 07:56:27

Folder Name: f1
Folder Status: Inactive

This section lists all the rules that this policy contains. Use select boxes next to the rule to select or unselect it from distribution, then click Apply.

☑ Collection Events
- Realtime Scanner Events
- Local Scanner Events
- Scheduled Scanner Events
- Distribution Events
- Admin Server Events
- RPC Server Events
- Alert Events
- Mail Agent Events
- Web Server Events

All the main Maker and Checker tasks are completed in the Policy Manager interface.

Policies

Lets you create policy folders and policies, and review and distribute them.

MP Files

Lets you create MP folders and files, and review and distribute them.

Audit Nodes

Lets you create and search for eTrust Audit host nodes in your environment and attach them to policy or MP folders.

Activation Log

Lets you view policy and MP file activation history for your eTrust Audit environment.

Reports

Lets you access the Reporter utility from the Policy Manager window.

Library

Lets you view and create audit node types, and view rule templates.

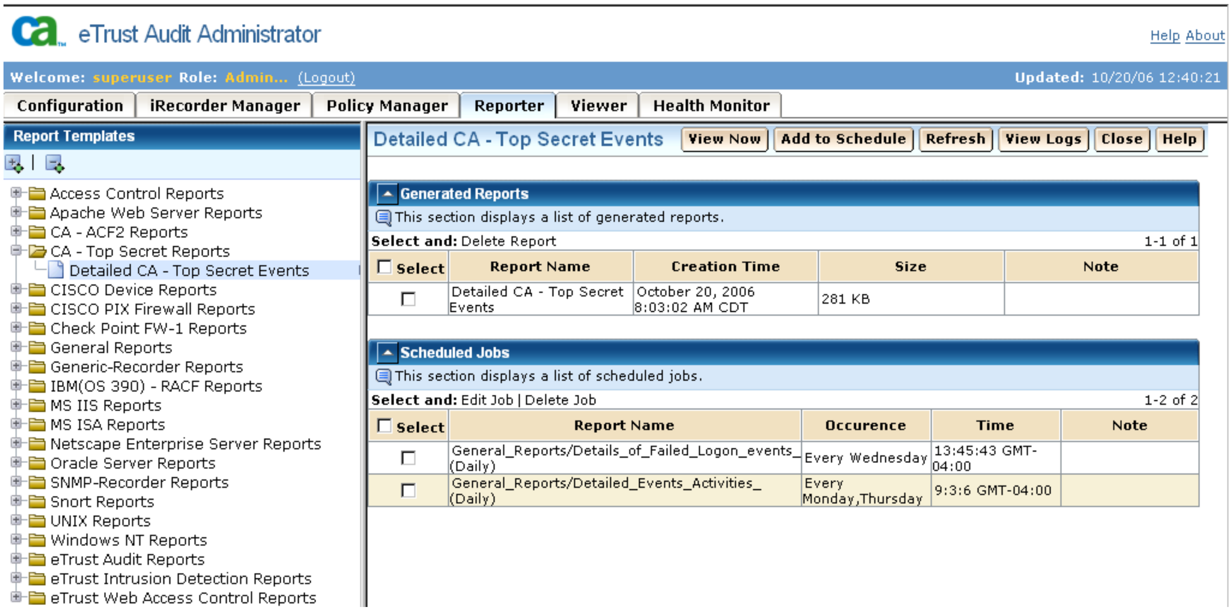
See the "Policy Manager Tasks" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide*, for more information on the new Policy Manager interface. Task-based information for each of the UI subtabs illustrated here is contained in its own sub-chapter, along with related user role information.

More information

Policy Manager Change Control Support (see page 15)

New Reporter Interface

The new Reporter utility interface lets you view selected data from eTrust Audit event databases in the form of graphic or detailed reports. It displays available report template types in a folder tree, which you can expand to view specific report templates, as shown in the following illustration.



Generated Reports

This section displays a list of generated reports.

Select and: Delete Report 1-1 of 1

□ Select	Report Name	Creation Time	Size	Note
□	Detailed CA - Top Secret Events	October 20, 2006 8:03:02 AM CDT	281 KB	

Scheduled Jobs

This section displays a list of scheduled jobs.

Select and: Edit Job \| Delete Job 1-2 of 2

□ Select	Report Name	Occurence	Time	Note
□	General_Reports/Details_of_Failed_Logon_events_(Daily)	Every Wednesday	13:45:43 GMT-04:00	
□	General_Reports/Detailed_Events_Activities_(Daily)	Every Monday,Thursday	9:3:6 GMT-04:00	

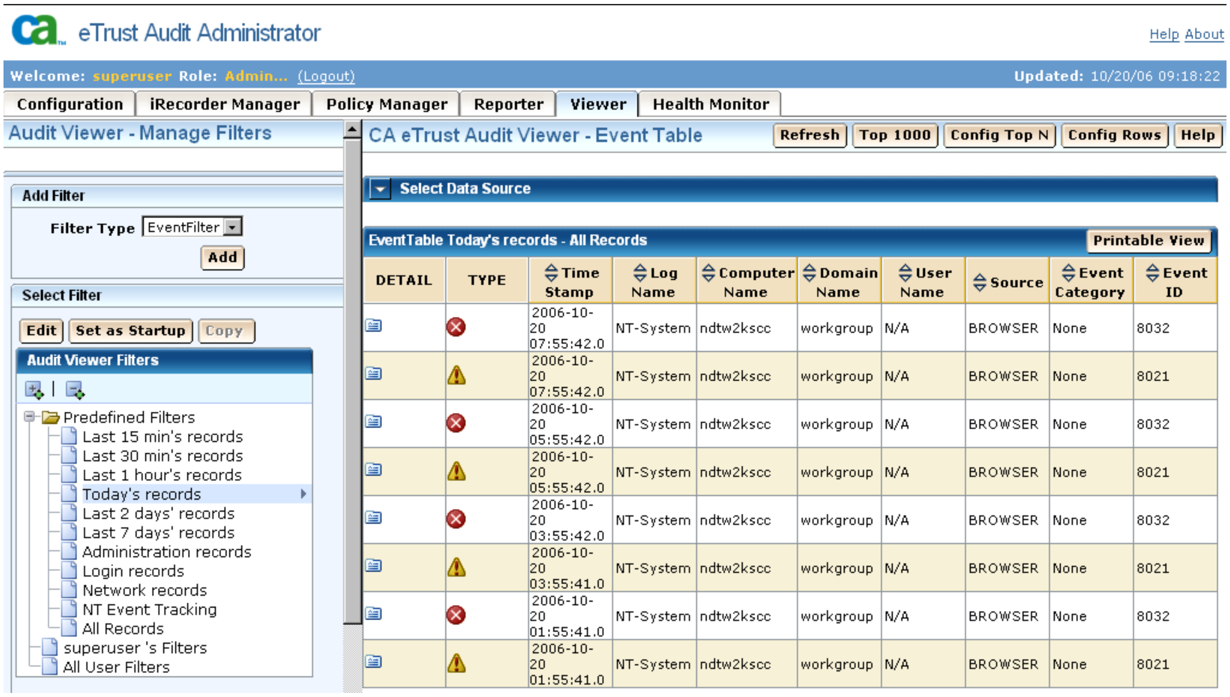
When you select a report template, it appears in the right pane, displaying any previously generated reports of that type. You can create an immediate report, schedule a new report, or view report job logs.

The Scheduled Jobs area displays all scheduled reports for your environment, regardless of their type.

See the "Using Reporter" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Reporter interface, including instructions for viewing, scheduling, and generating reports.

New Viewer Interface

The new Viewer utility interface lets you view, sort, and filter the eTrust Audit event database. It displays available filters in a folder tree, which you can expand to view specific filter details, as shown in the following illustration.



EventTable Today's records - All Records

DETAIL	TYPE	Time Stamp	Log Name	Computer Name	Domain Name	User Name	Source	Event Category	Event ID
🗎	✖	2006-10-20 07:55:42.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8032
🗎	⚠	2006-10-20 07:55:42.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8021
🗎	✖	2006-10-20 05:55:42.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8032
🗎	⚠	2006-10-20 05:55:42.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8021
🗎	✖	2006-10-20 03:55:42.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8032
🗎	⚠	2006-10-20 03:55:41.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8021
🗎	✖	2006-10-20 01:55:41.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8032
🗎	⚠	2006-10-20 01:55:41.0	NT-System	ndtw2kscc	workgroup	N/A	BROWSER	None	8021

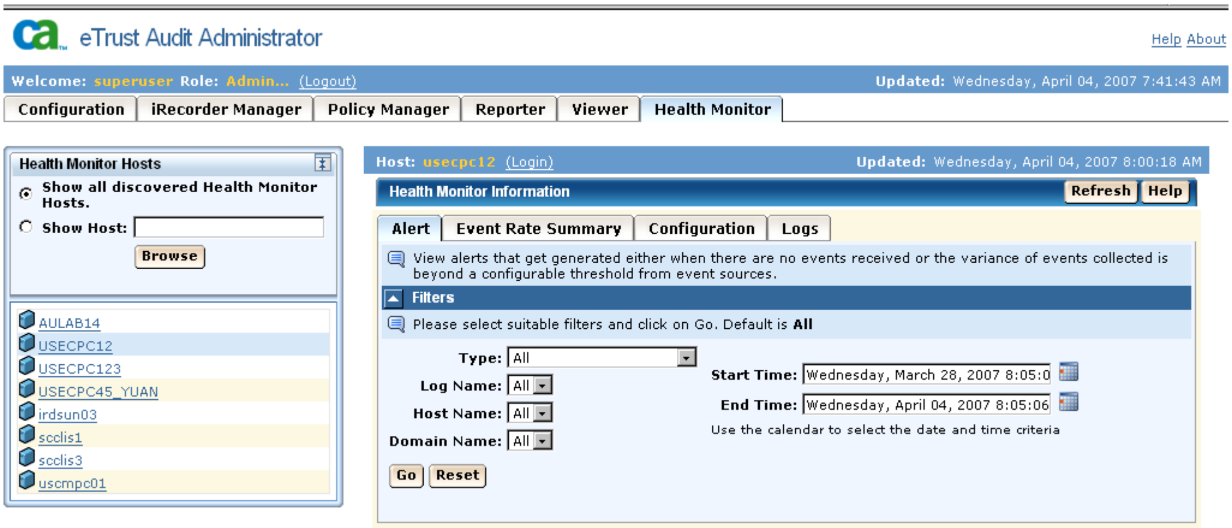
You can add new filters of your design or edit existing filters.

Events matching the qualifications of the filter you select appear in the Event Table pane. You can configure how many rows or events you want the table to display, and sort the events by any attribute other than Detail or Type. You can click the detail icon for any event to open an expanded view in a new window.

See the "Using Viewer" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Viewer interface, including instructions for viewing and filtering events.

New Health Monitor Interface

The new Health Monitor Utility lets you search and display Health Monitor hosts in your environment, as shown in the following illustration.



Welcome: superuser Role: Admin... (Logout) Updated: Wednesday, April 04, 2007 7:41:43 AM

● Show all discovered Health Monitor Hosts.

○ Show Host:

Host: usecpc12 (Login) Updated: Wednesday, April 04, 2007 8:00:18 AM

View alerts that get generated either when there are no events received or the variance of events collected is beyond a configurable threshold from event sources.

Please select suitable filters and click on Go. Default is **All**

Type: All

Log Name: All

Host Name: All

Domain Name: All

Start Time: Wednesday, March 28, 2007 8:05:0

End Time: Wednesday, April 04, 2007 8:05:06

Use the calendar to select the date and time criteria

You can select any of the available hosts displayed in the left pane to view Alert, Event Rate Summary, or Log information from the appropriate tab. You can also control the settings of the selected Health Monitor using the Configuration tab.

See the "Using Health Monitor" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Health Monitor interface, including instructions for viewing and filtering alerts, log records, and setting configuration parameters.

Policy Manager Change Control Support

eTrust Audit Policy Manager supports change control features through the new Maker and Checker roles, which are pre-defined in the Embedded Identity and Access Manager (EIAM) Tool Kit.

These roles divide responsibility for the creation of polices, rules and Message Parsing files from responsibility for their review and distribution to the clients. Users with the Maker role are able to create new policies and users with the Checker role to reject or approve them.

The Maker and Checker roles can be assumed by different users, or the same user, depending on your chosen configuration.

See the Managing Users and Access section of the "Managing Audit Administrator" chapter in thee*Trust Audit and eTrust Security Command Center Administration Guide* for more information on change control support through user roles. Additional information is available in the "Policy Manager Tasks" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide*.

Note: Policy Manager's internal user management is not available in this release. It is replaced by the EIAM Tool Kit.

Centralized Management of Message Parsing (MP) Files

Message Parsing (MP) files are used by several generic Audit Recorders or iRecorders to read text-format log event data. MP Files are managed in the same way as policies; both have the same level of acknowledgement, logging, version control and reporting support.

MP files are attached to Audit Node (AN) groups for distribution by Policy Manager, using the same improved distribution system as policies.

See the MP Files section of the "Policy Manager Tasks" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on MP files.

Note: MP files are created or modified manually and then imported into Policy Manager for version control and distribution.

More information

Improved Policy Distribution (see page 16)

Improved Policy Distribution

SP2 release includes broad improvements to policy distribution protocols. The following list summarizes these enhancements:

1. Policies and MP files are both distributed by the policy distribution protocol.
2. The maximum number of distribution threads can be configured in the user interface. The default number of threads is 10, and can be increased to a maximum setting of 64.
3. When policy files whose names include spaces are distributed to clients running on UNIX, the spaces are converted to underscores, automatically complying with UNIX naming standards.
4. eTrust Audit clients store policy version information in the Policy Manager database.
5. The Disable Node Retry feature allows a Maker to select a node or multiple nodes and exempt these nodes from all automatic policy/MP redistribution.
6. Automatic activation and enforcement is supported for policy/MP files delivered by the Policy Manager without any service restart requirements.

See the Distribution Server section of the "Managing Audit Administrator" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on policy distribution. More information on the Policy Manager database can be found in the Installing Databases chapter of the *eTrust Audit and eTrust Security Command Center Implementation Guide*.

More information

Centralized Management of Message Parsing (MP) Files (see page 15)

Audit Client Status Polling

This feature adds policy and MP file version control, enabling automatic validation of deployed policies or MP files. This allows you to recover from any changes to those policies or MP files.

Policy Manager periodically tests for any difference in status or version between active policies or MP files on the distribution server and those distributed to clients. If a difference is detected, Policy Manager generates an event, and gives you the option to redistribute the correct policy or MP file version.

See the Distribution Server section of the "Managing Audit Administrator" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on client polling. Additional information on policy and MP file version control is available in the Polices and MP Files sections of the "Policy Manager Tasks" chapter.

Additional Client Platform Support

The eTrust Audit client is now supported on additional platforms, including Solaris. For a full list of supported platforms, see the eTrust Audit *Readme.*

Enhanced Policy Manager Support

eTrust Audit Policy Manager now supports MS SQL Server 2000 and 2005 on Windows and Oracle 10g on Solaris 10. For a full list of supported databases, see the eTrust Audit *Readme.*

Migration scripts are provided to upgrade MS Access Policy Manager databases to Oracle 10g or MS SQL Server Policy Manager databases. See the Introduction to the "Installing Databases" chapter of the *eTrust Audit and eTrust Security Command Center Implementation Guide* for more information on databases.

Native Packaging for Solaris and Red Hat SUSE

All install packages on Solaris and Linux are now in native packaging format:

- pkg on Solaris
- RPM on Linux

See the *eTrust Audit and eTrust Security Command Center Implementation Guide* for additional installation information. You can consult the chapters on installing various components including Databases, Data Tools, and the Policy Manager.

New Policy Conversion, Import, and Export Utilities

During administration of your r8 SP2 Policy Manager database, you may from time-to-time need to import or export policies. You may also need to convert Windows system PTF files to XML for use with older iRecorders and SAPI Recorders.

For example, if you download an iRecorder and you want to import its default policies to the r8 SP2 Policy Manager database, it may not have an XML policy file supplied with it. In that case, you would need to convert the supplied .ptf file to XML using this utility, and then import the new XML file to the Policy Manager database.

You can use the following utilities to convert policy files to XML, and to import and export policy files:

acptf2xml

Converts Windows PTF policy files to XML format.

acxml2pmdb

Imports XML policy files to the r8 SP2 Policy Manager database.

acpmdb2xml

Exports policy files from the r8 SP2 Policy Manager database to XML files.

See the "Importing, Exporting, and Converting Policies" chapter in the *eTrust Audit and eTrust Security Command Center Reference Guide* for more information.

Chapter 2: Changes to Existing Features

This section contains the following topics:

A main feature of this eTrust Audit release is a new web-based interface (see page 7), so there are significant changes to the Policy Manager and other administrative tasks. Before you upgrade or use the new interface, it is important to review the *eTrust Audit and eTrust Security Command Center Administration Guide*. Additional information is also available in the online help for the Audit Administrator interface and the *eTrust Audit and eTrust Security Command Center Implementation Guide*.

Advanced Encryption Standard (AES) Support

The eTrust Audit Policy Manager distribution server is in frequent contact with eTrust Audit client computers in order to distribute new or changed policies or MP files, receive alerts, or generate reports. You can also configure the distribution server to poll the client computers and automatically redistribute policy or MP files to any node where the software detects version or status changes.

eTrust Audit supports AES 256 for Policy Manager server/client communication, replacing AES 128 as the default encryption method and providing more secure communication for your environment.

See the Distribution Server section of the "Managing Audit Administrator" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on file distribution and client/server contact.

UNIX SAPI Recorders Available Separately

UNIX Supplementary SAPI Recorders, including Oracle, Sybase, DB2, and Apache recorders, are not included in the basic eTrust Audit package for UNIX. These recorders are now available separately as standalone installation packages.

See http://supportconnect.ca.com (http://supportconnect.ca.com) for a full list of available UNIX SAPI recorders.

Visualizer Supported Only on Windows

The Audit Administrator Visualizer utility allows you to run standard queries on data processed by the Post-Collection Utility or drawn from eTrust Security Command Center table collectors. The Visualizer is available only to Windows users.

See the "Using Visualizer" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the Visualizer interface, including instructions for generating and displaying Visualizer queries.

Client Support Changes

For the eTrust Audit client r8 SP2 release, certain platforms are no longer supported. For a full list of supported platforms, see the eTrust Audit *Readme.*

More information

Enhanced Policy Manager Support (see page 17)

MS Access Not Supported

With the eTrust Audit enhancement to database support, MS Access is no longer supported for the Collector and Policy Manager databases. Migration scripts are provided to upgrade MS Access Policy Manager databases to Oracle 10g or MS SQL Server Policy Manager databases.

Post-Collection Utility Supported Only on Windows

The Post-Collection Utility (PCU) provides a set of tools for defining policies, managing the collector database, and detecting event tampering. The Post-Collection Utility is available only to Windows users.

See the "Post-Collection Utility (PCU) Tasks" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the Visualizer interface, including instructions for generating and displaying Visualizer queries.