

eTrust® Audit and eTrust® Security Command Center

Audit & SCC Release Summary

r8 SP2



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the product are permitted to have access to such copies.

The right to print copies of the documentation and to make a copy of the related software is limited to the period during which the applicable license for the Product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2006 CA. All rights reserved.

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 7

Web-based User Interface	7
Updated Configuration Interface	8
New Policy Manager Interface	10
New Reporter Interface	12
New Viewer Interface	13
New Health Monitor Interface	14
Policy Manager Change Control Support	15
Centralized Management of Message Parsing (MP) Files	15
Improved Policy Distribution	16
Audit Client Status Polling	17
Additional Client Platform Support	17
Enhanced Policy Manager Support	17
Native Packaging for Solaris and Red Hat SUSE	18
New Policy Conversion, Import, and Export Utilities	18

Chapter 2: Changes to Existing Features 19

Advanced Encryption Standard (AES) Support	19
UNIX SAPI Recorders Available Separately	20
Visualizer Supported Only on Windows	20
Client Support Changes	20
MS Access Not Supported	20
Post-Collection Utility Supported Only on Windows	21

Chapter 1: New Features

This section contains the following topics:

[Web-based User Interface](#) (see page 7)
[Policy Manager Change Control Support](#) (see page 15)
[Centralized Management of Message Parsing \(MP\) Files](#) (see page 15)
[Improved Policy Distribution](#) (see page 16)
[Audit Client Status Polling](#) (see page 17)
[Additional Client Platform Support](#) (see page 17)
[Enhanced Policy Manager Support](#) (see page 17)
[Native Packaging for Solaris and Red Hat SUSE](#) (see page 18)
[New Policy Conversion, Import, and Export Utilities](#) (see page 18)

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.

eTrust Audit Administrator [Help](#) [About](#)

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

Configuration | **iRecorder Manager** | **Policy Manager** | **Reporter** | **Viewer** | **Health Monitor**

▼ **Audit Host Discovery** > **Content Update** > **User and Access Management** > **Reporter /Viewer** > **Policy Manager**

Discovery Jobs [New Job](#) [Help](#)

View, create, and remove Audit Host Discoveries.

Address	Interval (hrs)	Last Scheduled	Remove
---------	----------------	----------------	--------

New Discovery Job

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

[Save](#) [Close](#)

Discovery Statistics [Refresh](#)

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:

iRegistry Plugin Status

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.

The screenshot displays the eTrust Audit Administrator web interface. The top navigation bar includes tabs for Configuration, iRecorder Manager, Policy Manager (selected), Reporter, Viewer, and Health Monitor. Below this, a breadcrumb trail shows Policies > MP Files > Audit Nodes > Activation Log > Reports > Library. The main content area is divided into two panels. The left panel, titled 'Policies', shows a tree view with a folder 'f1' containing 'eTrust Antivirus Policy'. The right panel, titled 'Policy', shows details for the 'eTrust Antivirus Policy'. It includes a 'Policy Details' section with fields for Name, Version, AN Type, Description, Status, Policy Author, and Created. The 'Rules' section lists various event types with checkboxes for selection. The 'Status Summary' section shows the folder name and status.

eTrust Audit Administrator [Help](#) [About](#)

Welcome: **superuser** Role: **Admin...** ([Logout](#)) Updated: 10/20/06 07:55:47

Configuration | **iRecorder Manager** | **Policy Manager** | **Reporter** | **Viewer** | **Health Monitor**

Policies > **MP Files** > **Audit Nodes** > **Activation Log** > **Reports** > **Library**

Policies

New Folder | |

f1

eTrust Antivirus Policy

Policy [Commit](#) [Manage Versions](#) [Delete](#) [Close](#) [Help](#)

Policy Details [Edit](#) [Check](#)

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

Rules [Create Rule](#) [Apply](#)

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](#)

Status Summary

Folder Name: f1
Folder Status: Inactive

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.

The screenshot shows the eTrust Audit Administrator web interface. The top navigation bar includes links for Configuration, iRecorder Manager, Policy Manager, Reporter, Viewer, and Health Monitor. The Reporter section is active, displaying a detailed report for 'Detailed CA - Top Secret Events'. The left pane shows a tree of report templates, with 'Detailed CA - Top Secret Events' selected. The right pane displays the report details, including a table of generated reports and a table of scheduled jobs.

Report Templates

- Access Control Reports
- Apache Web Server Reports
- CA - ACF2 Reports
- CA - Top Secret Reports
 - Detailed CA - Top Secret Events
- CISCO Device Reports
- CISCO PIX Firewall Reports
- Check Point FW-1 Reports
- General Reports
- Generic-Recorder Reports
- IBM(OS 390) - RACF Reports
- MS IIS Reports
- MS ISA Reports
- Netscape Enterprise Server Reports
- Oracle Server Reports
- SNMP-Recorder Reports
- Snort Reports
- UNIX Reports
- Windows NT Reports
- eTrust Audit Reports
- eTrust Intrusion Detection Reports
- eTrust Web Access Control Reports

Detailed CA - Top Secret Events View Now Add to Schedule Refresh View Logs Close Help

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
<input type="checkbox"/>	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	Occurrence	Time	Note
<input type="checkbox"/>	General_Reports/Details_of_Failed_Logon_events_(Daily)	Every Wednesday	13:45:43 GMT-04:00	
<input type="checkbox"/>	General_Reports/Details_of_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.

The screenshot shows the eTrust Audit Administrator web interface. The top navigation bar includes tabs for Configuration, iRecorder Manager, Policy Manager, Reporter, Viewer, and Health Monitor. The main content area is titled "Audit Viewer - Manage Filters" and "CA eTrust Audit Viewer - Event Table".

On the left, the "Add Filter" pane shows a "Filter Type" dropdown set to "EventFilter" and an "Add" button. Below it, the "Select Filter" pane shows a tree view of "Audit Viewer Filters" with options like "Predefined Filters", "Last 15 min's records", "Last 30 min's records", "Last 1 hour's records", "Today's records", "Last 2 days' records", "Last 7 days' records", "Administration records", "Login records", "Network records", "NT Event Tracking", "All Records", "superuser's Filters", and "All User Filters".

The main "Event Table" pane displays a table of events. The table has columns: DETAIL, TYPE, Time Stamp, Log Name, Computer Name, Domain Name, User Name, Source, Event Category, and Event ID. The table shows 10 rows of events, all from "NT-System" on "ndtw2kscc" in the "workgroup" domain, with "BROWSER" as the source and "None" as the event category. The event IDs range from 8032 to 8021.

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

The screenshot displays the eTrust Audit Administrator web interface. At the top, the header shows the user is logged in as 'superuser' with the role 'Admin...'. Below the header is a navigation bar with tabs: Configuration, iRecorder Manager, Policy Manager, Reporter, Viewer, and Health Monitor. The main content area is divided into two panes. The left pane, titled 'Health Monitor Hosts', contains a search section with radio buttons for 'Show all discovered Health Monitor Hosts.' and 'Show Host:'. Below this is a list of hosts: AULAB14, USECPC12, USECPC123, USECPC45_YUAN, irdsun03, scclis1, scclis3, and uscpc01. The right pane, titled 'Host: usecpc12 (Login)', shows the 'Health Monitor Information' section. It includes a 'Refresh' button and a 'Help' link. Below this are tabs for 'Alert', 'Event Rate Summary', 'Configuration', and 'Logs'. The 'Alert' tab is selected, showing a message: '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.' Below the message is a 'Filters' section with a dropdown for 'Type' set to 'All', and input fields for 'Log Name', 'Host Name', and 'Domain Name', all set to 'All'. There are also 'Start Time' and 'End Time' fields with calendar icons, and 'Go' and 'Reset' buttons.

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 policies, 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 the *eTrust 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 Policies 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:

[Advanced Encryption Standard \(AES\) Support](#) (see page 19)

[UNIX SAPI Recorders Available Separately](#) (see page 20)

[Visualizer Supported Only on Windows](#) (see page 20)

[Client Support Changes](#) (see page 20)

[MS Access Not Supported](#) (see page 20)

[Post-Collection Utility Supported Only on Windows](#) (see page 21)

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.