*e*Trust® Audit

iRecorder Reference Guide for eTrust SiteMinder

r6.0 Service Pack 4 CR 03

First Edition

CA Product References

This document references the following CA products:

- *e*Trust® Security Command Center (eTrust SCC)
- *e*Trust® Audit (Audit)
- *e*Trust® SiteMinder

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: Welcome to iRecorder for eTrust SiteMinder

This section contains the following topics:

Who Should Read this Guide

This guide is for system administrators who may install the iRecorder on network servers and for security professionals who will create policies to handle eTrust SiteMinder events after the iRecorder is installed.

Note: The use of Policy Manager and the Data Tools herein refers to eTrust Policy Manager and eTrust Data Tools.

Chapter 2: How to Install and Configure the iRecorder

This section contains the following topics:

Pre-Installation Steps

Before you install the iRecorder, do the following:

- Install the iRouter component on a host where eTrust Audit Client components are installed. Because the iRouter lets iRecorders communicate with eTrust Audit, the iRecorder installation prompts for the host where iRouter is installed.

  For more details on how to install the iRouter, see the *Reference Guide*.

- Ensure that the Policy Manager and the Data Tools are installed somewhere on the network.
- Make sure there is an ODBC Data Source, which defines the database connection to the SiteMinder audit log database.

Create a System DSN For Oracle

Before installing the iRecorder, make sure that a System Data Source Name (DSN) for the eTrust SiteMinder Oracle database is properly configured.

To create a System DSN, follow these steps:

1. Click Start, Programs, Administrative Tools, and select Data Sources (ODBC).

   The ODBC Data Source Administrator dialog appears.

2. Click Add, on the System DSN tab.

   The Create New Data Source dialog appears.

3. Select Oracle in OraHome92 from the list of data source drivers, and click Finish.

   The Oracle ODBC Driver Configuration dialog appears.

4. Enter the values for the Data Source Name and Description, select the TNS Service Name from the drop down list, and click Test Connection to ensure successful connection.

   The Oracle ODBC Driver Connect dialog appears.

5. Click OK on the Oracle ODBC Driver Configuration dialog.

   The Oracle System DSN is created for eTrust SiteMinder iRecorder.

Create a System DSN For MS SQL Server

To create a System DSN for SQL Server, follow these steps:

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

   The ODBC Data Source Administrator dialog appears.

2. On the System DSN tab, click Add

   The Create New Data Source dialog appears.

3. From the list select SQL Server, and click Finish.

   The Create New Data Source to SQL Server dialog appears.

4. Enter the values for the Name and Description, select the Server from the drop down list, and click Next.

5. Select With SQL Server authentication using a login ID and password entered by the user, enter the values for Login ID as *irec_user* and its Password, and click Next.

6. Check the box for Change the default database to, select the database for the audit trail (where you wish to maintain the trace details), and click Next.

   Important! *You can use a non master database as the default database.*

7. Click Finish.

   The ODBC Microsoft SQL Server Setup dialog appears.

8. Click Test Datasource, to ensure successful connection.

   The SQL Server ODBC Data Source Test dialog appears.

9. Click OK.

   The DSN to be used for the audit trail is created.

Installation Materials

The iRecorder for eTrust SiteMinder is provided on the eTrust SiteMinder Policy Server media.

Install the iRecorder from the Media

To install the iRecorder for eTrust SiteMinder, follow these steps:

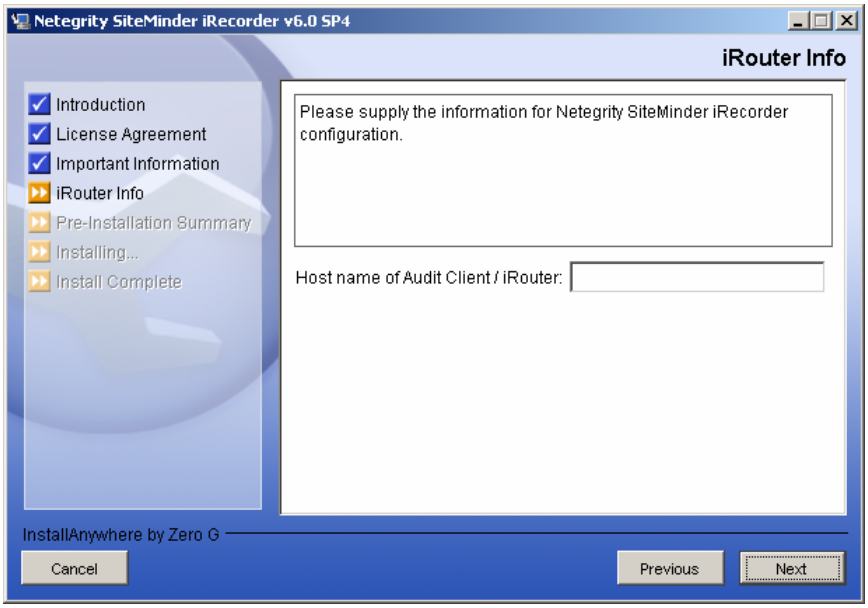
1. Click Start, Run and enter the following command:

   <media-Drive>\win32\nete-ps-irec-6.0-sp4-win32.exe

   media-Drive

   Specifies your media drive letter designation.

2. On the iRouter Info dialog, enter the hostname where the iRouter is installed. If the iRouter is on the localhost, enter localhost.



3. Continue with the installation, and click Done when the installation is completed.

Configuration and Use of the iRecorder

The following topics describe how to configure and use the eTrust SiteMinder iRecorder.

Note: The following sections include information for the various irecorders and operating systems, thus all of the data provided may not apply to your particular operating system or systems.

Start the iRecorder

The iRecorder runs as a sub-component of the iTechnology-iGateway service.

To start the iRecorder on Windows, start the iGateway service using one of the following methods:

- Use the Services Management GUI (Start, Control Panel, Services or Administrative Tools, Services).
- Issue the following command:

```
net start igateway
```

Stop the iRecorder

The iRecorder runs as a sub-component of the iTechnology-iGateway service.

To stop the iRecorder on Windows, stop the iGateway service using either of the following methods:

- Use the Services Management GUI (Start, Control Panel, Services or Administrative Tools, Services).
- Issue the following command:

```
net stop igateway
```

How to Configure the iRecorder

iRecorder configuration parameters are kept in a configuration file usually located in the iTechnology installation directory. The iRecorder configuration parameters are automatically set during iRecorder installation and do not require any changes for the normal operation of the iRecorder.

The iRecorder configuration file for eTrust SiteMinder is named SmRecorder.conf. The versions for the operating systems are in the following directories:

- Windows: *Drive*:\Program Files\CA\SharedComponents\iTechnology

If you do want to modify any parameters, you must do the following:

1. Stop the iTechnology iGateway service (or daemon) before making the changes.
2. After making the changes, restart the service for changes to take effect.

You can change the following tags:

DSN

Specifies the ODBC Data Source that defines the database connection to the SiteMinder audit log database.

User

Specifies the user name of a database account with permission to access SiteMinder audit log database.

Password

Specifies the password of the database account.

Note: By default, contents of the Password element are encrypted. When you specify a clear-text password, you must prefix the actual password with the characters 'c ' ('c' and a space). This allows the iGateway to read the password as clear-text, encrypt the password, and write the encrypted form to the SmRecorder.conf at next startup.

PollInterval

Specifies the time in seconds the iRecorder will sleep before checking if there are new records in the SiteMinder Audit Logs database tables to be processed.

Default: 10 seconds

Sample Configuration File for eTrust SiteMinder

The following is a sample SmRecorder.conf configuration file; it is included for information only. You do not need to change any parameter for the iRecorder for eTrust SiteMinder:

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
    <Name>SmRecorder</Name>
    <ImageName>SmRecorder</ImageName>
    <ISType>DSP</ISType>
    <DispatchEP>iDispatch</DispatchEP>
    <PreLoad>true</PreLoad>
    <Version>8.0.4.050119</Version>
    <DSN>dsnname</DSN>
    <User>username</User>
    <Password>c password</Password>
    <PollInterval>10</PollInterval>
    <SupportInfo>SiteMinder Audit iRecorder</SupportInfo>
    <DebugLevel>ISP_FILE</DebugLevel>
    <LastRecordRead Log="Object">0</LastRecordRead>
    <LastRecordRead Log="Access">0</LastRecordRead>
</iSponsor>
```

Enable Debugging

You can configure the iRecorder to send debugging information to a debugging application or to a file. To enable debugging and log debug information to a file, follow these steps:

1. Stop the iRecorder by stopping the iTechnology iGateway Service.
2. Edit the iRecorder configuration file by adding the following <DebugLevel> tag between the <iSponsor> tags:

   ```
   <DebugLevel>{level}</DebugLevel>
   ```

   where {level} is one of the following:

   ISP_NOLEVEL

   Disables debugging.

   ISP_FILE

   Prints all debug messages to a debug application as well as writing it to a log file, irecordername.log, in the same directory as the iRecorder. The debug file may grow very quickly; to avoid possible disk space shortage, we recommend turning off the debugging option as soon as possible by replacing ISP_FILE by ISP_NOLEVEL.
3. Save the configuration file.
4. Start the iRecorder by restarting the iTechnology iGateway Service.
5. Send the debug file to Computer Associates Customer Support for further analysis.

Add and Manage Policies

You can add pre-packaged template policies to your Policy Manager and then use the Policy Manager to create your own custom rules. You can then activate and distribute them to function on routers throughout your enterprise.

Add the Default Policy for eTrust SiteMinder to the Policy Manager

To create a policy for the eTrust SiteMinder iRecorder, you must add the default policy template for eTrust SiteMinder to the Policy Manager.

Note: If you do not have an eTrust SiteMinder Policy, you must import the policy template for eTrust SiteMinder to the Policy Manager.

To add the default template, follow these steps:

1. On the eTrust Audit Policy Manager server, open the following file:

   `[eTrust Auditinstall]\bin\pmu_template_exchange.exe.`

   where [eTrust Auditinstall] is the directory where eTrust Audit is installed.

   The Import/ Export Policy dialog appears:

2. Select Import policy template from binary file, and click Next.

   You are asked for the policy file name for your iRecorder.

3. Enter the path where the following file is located, which is a policy file made exclusively for eTrust SiteMinder:

   eTrust_SiteMinder.ptf

   The policy file is installed along with the iRecorder at this location:

   `<Drive:>\Program Files\CA\SharedComponents\iTechnology\eTrust_SiteMinder.ptf.`

   Note: If there is no specific ptf file (eTrust_SiteMinder) available, default policies already exist in the Policy Manager that you can use for eTrust SiteMinder. You can skip this procedure.

4. Click Next.

   A dialog appears that describes the chosen policy file.

5. Click Next again.

   A dialog appears and asks whether you want to create the policy in the default policies section.

6. Click Yes and click Next.

   A dialog appears that asks you for the name of the subpolicy for eTrust SiteMinder.

7. Enter **(none - use default)** as the name of the inserted subpolicy, and click Finish.

   The default policy is loaded into the Policy Manager.

Create an AN Group

Now you must create an Audit Node (AN) Group, a group of network nodes that become available targets to which you can apply your policies.

To create an AN group, follow these steps:

1. Open the eTrust Audit Policy Manager if it is not already open.
2. On the left pane, click Audit Nodes.
3. Right-click the Targets node, and from the pop-up menu, choose New Group.
4. Enter SiteMinder for the new group name.
5. Click OK.

Select an AN Type

Now you must create an Audit Node (AN) Type for the AN group you just created, which sets the kind of events the group of nodes will be handling.

To create an AN type, follow these steps:

1. Open the eTrust Audit Policy Manager if it is not already open.
2. On the left pane, click Audit Nodes.
3. Right-click the SiteMinder group (which you created in the last step) and from the pop-up menu choose New AN.
4. Enter the host name of the iRouter that you configured the iRecorder to communicate with.
5. Select the AN type as SiteMinder.
6. Enter a description for the AN node.
7. Click OK.
8. Repeat steps 3 through 7 for each iRouter in your network that communicates with an iRecorder for eTrust SiteMinder.

Create a Policy Folder

Now you can create a policy folder to hold the policies available for deployment onto your Audit Nodes (AN).

To create a policy folder, follow these steps:

1. Open the eTrust Audit Policy Manager if it is not already open.
2. On the left pane, click Policies.
3. From the main menu bar, click File, New.
4. Select Policy Folder (this should be the only available option) and name the folder SiteMinder.
5. Click Finish.

Copy the Default Policies

Now you have your new SiteMinder policy folder, so you can copy the prefabricated default policies from the template folder to your own new folder to use them. Using this method allows you to add rules and actions to your own policies without affecting the default policies.

To copy a policy, follow these steps:

1. Open the eTrust Audit Policy Manager if it is not already open.
2. On the left pane, click Policies.
3. Expand the Default Policies folder to display the eTrust SiteMinder default policy folder.
4. Copy the policies in the eTrust SiteMinder default folder and then paste them into the new policy folder you just created, named SiteMinder.

Add Actions to the Rules

Policies are made up of rules, and you can add actions to the rules in your own policies.

To add actions to a rule, follow these steps:

1. Open the eTrust Audit Policy Manager.
2. On the left pane, click Policies.
3. Expand your SiteMinder folder to display the policies in it.

   An action must be defined for each rule.
4. Right-click the rule, and from the pop-up menu click Properties.
5. On the Action tab, select Collector action.
6. Click Add, and enter the host name or IP address of the eTrust Audit Collector.
7. Repeat Steps 5 and 6 for the Security Monitor action.
8. Click OK.

   In the tree view, the icon for the rule turns from a white bell to a blue bell.

Attach the Policy to an AN Group

Once you have rules created, you can attach the policy to the AN group you created.

To attach a policy to an AN group, follow these steps:

1. Open the eTrust Audit Policy Manager if it is not already open.
2. On the left pane, click Policies.
3. From the tree view, expand the SiteMinder policy folder.
4. Right-click the SiteMinder policy folder and from the pop-up menu click Attach AN Group.
5. Select the SiteMinder AN group, and click OK.

Activate the Policy

Now that your rules are assigned to AN groups, you can activate them.

To activate a rule, follow these steps:

1. Open the eTrust Audit Policy Manager if it is not already open.
2. On the left pane, click Policies.
3. From the tree view, expand the SiteMinder policy folder.
4. Click on the icon for the rule.

   The icon turns from a blue bell to a red bell.
5. Right-click the SiteMinder policy folder and from the pop-up menu click Activate.

   A confirmation dialog appears.
6. Click Yes.

Verify the Rule Is in Effect

To verify the rule in effect, follow these steps:

1. Open the eTrust Audit Policy Manager.
2. On the left pane, click Audit Nodes.
3. Select the SiteMinder group, and verify for each AN that there are no errors.

   If there are no errors, a key icon appears beside the name of an AN.

How Event Route Testing Works

The basic flow of events is this:

1. Events that match a policy rule occur on the host system where the iRecorder is installed.
2. Events are sent to the iRouter, which sends the events to the router.
3. Policy rules sent to the router are checked to see if the events are sent to the Action Manager or discarded.
4. Events that match policy rules with actions are reviewed by the Action Manager and the action is taken.
5. In the case of this event, the Action Manager sends the event to the Security Monitor.

Test Event Routing for eTrust SiteMinder

To test event routing (and verify that the iRecorder is installed properly and sending events to eTrust Audit), follow these steps:

1. Install eTrust Audit iRouter component on a host where eTrust Audit Client components are installed.
2. Install the iRecorder component on the Windows host.
3. Verify that <Program Files>\CA\SharedComponents\iTechnology folder contains the following files:

   ```
   SmRecorder.dll
   SmRecorder.conf
   ```

4. Install eTrust Audit iRouter component on a host where eTrust Audit Client components are installed.
5. Start the eTrust Audit Policy Manager and define a policy for eTrust SiteMinder events received by the host where iRouter and the other eTrust Audit Client components are installed.
6. Create a test policy with a rule that sends all events to the eTrust Audit Security Monitor (no filter with Action set to Security Monitor).

   If there is no defined policy (rule and action), eTrust Audit ignores the events. For more information about how to create a policy, see *eTrust Audit Management Guide*.
7. Make sure the eTrust SiteMinder Policy Server is running and log in as an administrator to the SiteMinder administration console.
8. Verify that events are generated on the eTrust Audit Security Monitor.

iRecorders also support standard iTechnology SDK tools (like TestHarness and Spin interface) to query the iRecorder for current status and configuration information. For more details about these tools, see the *iTechnology SDK Reference Guide*.

Chapter 3: eTrust Audit Field Mapping

This section contains the following topics:

eTrust Audit Fields

Fields in eTrust SiteMinder events are captured by the iRecorder and mapped to a standard set of normalized fields. eTrust Audit requires all iRecorders to follow a standard Data Model and Taxonomy. The iRecorder maps the native eTrust SiteMinder fields into fields in the eTrust Audit Collector database.

Mandatory Fields

Mandatory fields are a fixed set of fields that are added to each event processed by any iRecorder. The following table describes the values that are assigned to the mandatory fields in the eTrust SiteMinder.

Field	Default Value	Description
Taxonomy	<Category>.<System>.<Action>.<Result>.<Severity>	For details, see About Taxonomy Fields (see page 24).
Date	Time when the event is received by the iRecorder	The timestamp of the event in time_t format(number of seconds since 1/1/1970 12am UTC).
TimeZone	Timezone of the iRecorder host	Local time zone of the event in number of seconds. Local time zone is the difference between the local time and UTC. For example, if the event is recorded in the US East Coast, the TimeZone during daylight saving time it will be –14400 (or -4 hours), for other times it will be –18000 (or –5 hours.)
Src	SiteMinder	Name of the component (device, application, or product) that generated the event.

Field	Default Value	Description
Log	Sm Access for runtime access control events Sm Object for administrative/management events	Logical name of the system/device/file (if any) where the events were stored by original issuer.
Location	None	Hostname or IP address of the Source system
Recorder	SmRecorder	Name of the recorder that captured the event. Specified in the source code of iRecorder.
RecorderHost	Unknown	FQDN (fully qualified domain name) of the host running the iRecorder. Consists of a host and domain name, including top-level domain. For example, www.webopedia.com is a fully qualified domain name. www is the host, webopedia is the second-level domain, and.com is the top level domain. A FQDN always starts with a host name and continues all the way up to the top-level domain name, so www.parc.xerox.com is also a FQDN.

Taxonomy Fields

The following table provides field names, possible values, and descriptions that can appear in the Taxonomy field:

Field Name	Possible Values	Description
Category	Network Security	Hardcoded
	Host Security	
	Data Access	
	Network Access	
	System Access	
	Policy Compliance	
System	OS, VPN	Depends on the type of event being generated.

Field Name	Possible Values	Description
Action	Object Access Card Swipe Manual Action Authorize Encrypt	The name action that caused an event to be generated.
Result	S, F, N	S: Success F: Failure N: None
Severity	I, W, C, F	I: INFORMATIONAL: General information about system operation W: WARNING: Functionality might be affected C: CRITICAL: Immediate action required F: FATAL: The system has become unstable

About Normalized Fields

Normalized fields are eTrust Audit field names that are mapped or translated from the native event field names according to the classification of the iRecorder. Normalized fields are common across all products in the same classification. The Taxonomy field, one of the mandatory fields, defines the classification for this iRecorder.

Normalized Fields for eTrust SiteMinder

The following table shows the normalized fields for eTrust SiteMinder:

Audit Field	SiteMinder Field	Field Type	Description
Timestamp	sm_timestamp	Date	Date/time that event was generated at the SiteMinder Policy Server, including the timezone.
Identity	sm_username	String of size 512	SiteMinder username
Resource	sm_resource (Access)	String of size 4096	The resource being accessed and/or modified.
	sm_objname (Admin)		
rowid	eventid	Long	The row ID of the event in the SiteMinder audit database

About Product-Specific Fields

Product Specific fields are native event fields that are not mapped or translated by the iRecorder. These fields are sent to eTrust Audit with a minor change: all characters in the field names that are not letters, digits or underscores are converted to underscores. To avoid name clashes with other products or with eTrust Audit itself (for example, the Status field), these fields are also prefixed by the product name followed by an underscore, such as eVM_, cisco_, ccure_.

Product-Specific Fields for eTrust SiteMinder

The following table shows the product-specific fields for eTrust SiteMinder:

Runtime / Access Control

The following data fields are product specific for eTrust SiteMinder Runtime/Access Control (Sm Access log) fields:

Audit Field	SiteMinder Field	Field Type	Description
Category ID	sm_categoryid	Integer	Event category
Hostname	sm_hostname	String of size 255	Hostname of the SiteMinderPolicy Server generating the event.
Session ID	sm_sessionid	String of size 255	SiteMinder Session ID
Agent Name	sm_agentname	String of size 255	Name of the SiteMinder agent processing the request.
Realm Name	sm_realmname	String of size 255	Name of the SiteMinder realm the accessed resource is part of.
Realm ID	sm_realmoid	String of size 64	Object ID of the SiteMinder realm the accessed resource is part of.
Client IP	sm_clientip	String of size 255	IP address of the client making the request.
Domain ID	sm_domainoid	String of size 64	Object ID of the SiteMinder domain the accessed resource is part of.
Auth Directory Name	sm_authdirname	String of size 255	Name of the user directory the user was authenticated in.
Auth Directory Server	sm_authdirserver	String of size 512	Server name of the user dir. the user was authenticated in.

Auth Directory Namespace	sm_authdirnamespace	String of size 255	Namespace, that is type, of the user directory the user was authenticated in.
Server Method	sm_action	String of size 255	The type of access, ie the request method/type.
Message Text	sm_status	String of size 1024	Additional information about the state of the request.
Error	sm_reason	Integer	Result code of the request (zero is success, non-zero an error).
ErrorCode	(none, derived from sm_reason)	Textual description of the result of the request.	
Transaction ID	sm_transactionid	String of size 255	SiteMinder transaction ID
Domain Name	sm_domainname	String of size 255	Name of the SiteMinder domain the accessed resource is part of.
Impersonator Name	sm_impersonatorname	String of size 512	For impersonated sessions, the user name of the impersonating user.
Impersonator Directory Name	sm_impersonatordirname	String of size 255	For impersonated sessions, the name of the user directory the impersonating user was authenticated in.

Admin/Management

The following data fields are product specific for eTrust SiteMinder Admin/Management (Sm Object log) fields:

Audit Field	SiteMinder Field	Field Type	Description
ResourceClass	sm_categoryid	Integer	Type of object
Hostname	sm_hostname	String of size 255	Hostname of the SiteMinder Policy Server generating the event.
Session ID	sm_sessionid	String of size 255	SiteMinder Session ID
Object ID	sm_objoid	String of size 64	Object ID of the object being modified.
Field Description	sm_fielddesc	String of size 1024	Description of the object data being modified.
Domain ID	sm_domainoid	String of size 64	Object ID of the SiteMinder domain the modified object is part of.

Appendix A: eTrust Audit Overview

This section contains the following topics:

eTrust Audit Overview

As the system administrator for a server onto which the iRecorder is being installed, you need to know a few basics about eTrust Audit so that you can understand the relationship of the iRecorder you are about to install on your system and the eTrust Audit system operating in your enterprise.

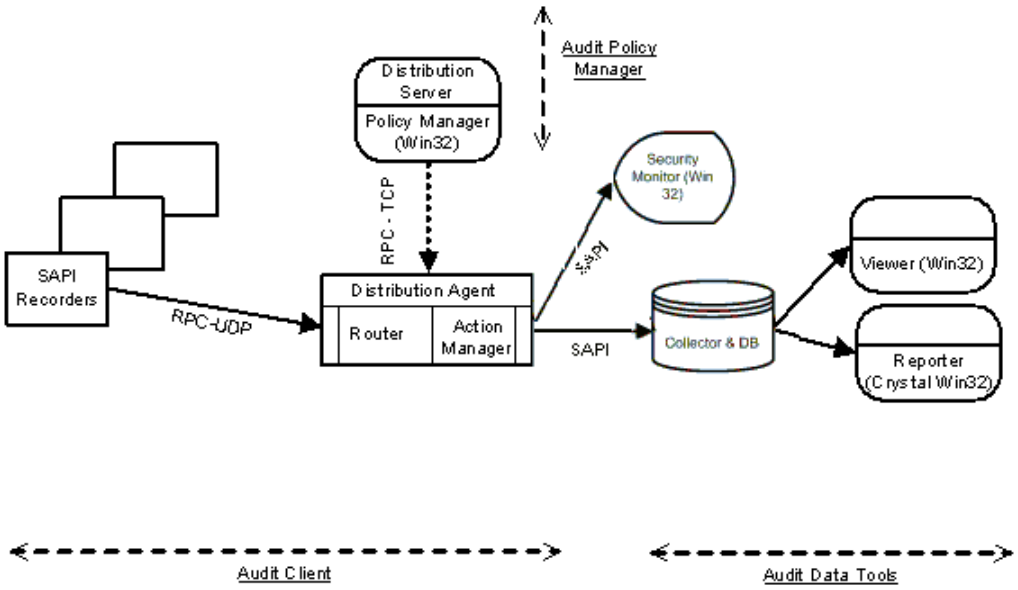
eTrust Audit is a system that enables security managers to identify and capture security-related events on systems throughout the enterprise. After the events are captured they can be reviewed, stored, or acted on based on policies. The iRecorder that you are about to install receives the events from the application or device. Based on an eTrust Audit policy, the iRecorder ignores the event or routes it through the remaining components of eTrust Audit.

The major components of eTrust Audit follow:

- Client
- Data Tools
- Policy Manager

While these components can be installed on the same host (if it runs Windows NT, 2000, XP, or 2003), it is more likely that these components are distributed among several different hosts throughout your enterprise.

The following diagram shows the relationship among the three components:



eTrust Audit uses Sun Remote Procedure Calls (RPC) to exchange data between the components of the Client and the Policy Manager. In addition, the components of the Data Tools, Collector, Viewer, and Reporter use ODBC to communicate with the underlying database (Microsoft Access, Microsoft SQL Server, or Oracle).

Audit Client

The Client component receives events and processes them based on policy rules. It is comprised of the following subcomponents:

- Recorder
- Router
- Action Manager
- Distribution Agent

How the Client Processes Events

The subcomponents of the Client process events as follows:

1. A Send API Recorder (SAPI Recorder) receives events. The SAPI Recorders receive events from sources such as other eTrust products, Unicenter, Check Point FW 4.1, UNIX syslog, Windows NT event log, SNMP, Oracle, Sybase, and IBM DB2.
2. The SAPI Recorders send the events to the Router, which filters the events according to policy rules.

   The policy rules state what to do with the events. For example, the rules can create state variables for further correlation, event consolidation, and data reduction. They can also generate new events that will be resubmitted to the Router and will go through the same filtering policy rules as the original events.
3. After the Router filters the events, they are submitted to the Action Manager, which takes actions such as sending the events using email, forwarding events to another Router and Action Manager, forwarding events to the Security Monitor, storing the events in the Collector database, and sending events to Unicenter.

For the Router and Action Manager to function, the most current version of the policy rules has to be available on the Client system. The Distribution Agent component receives policy rules from the Policy Manager.

Supported Platforms

The Client component runs on the following platforms:

- Windows 2000, XP, and 2003
- AIX
- HP-UX
- Solaris
- Tru64 UNIX
- UnixWare
- Linux

Audit Data Tools

The Data Tools component lets you store and display events received directly from the Action Manager or from the database. The following subcomponents comprise the Data Tools:

Collector

Collects events from the Action Manager and stores them in the Collector Database.

Viewer

Displays events from the Collector database based on specific selection criteria.

Reporter

Generates reports on events.

Security Monitor

Provides a near real-time display of events received directly from the Action Manager.

How the Data Tools Process Events

The subcomponents of the Data Tools process events depending on how the Action Manager routes the events to the Data Tools, and on where the events are stored:

- If the Action Manager sends the events to the Collector, which stores the events in its database, administrators can view the events using the Viewer or generate reports using the Reporter.
- If the Action Manager sends the events to the Security Monitor, administrators can view and act on events in near real time.

Supported Platforms

The subcomponents of the Data Tools can run on the following platforms:

Collector Database

The database engine can be Microsoft SQL Server, Oracle or Microsoft Access. eTrust Audit does not include Microsoft SQL Server or Oracle. However, it includes a Microsoft Access database, which we do not recommend if you plan on collecting large numbers of events. The databases run on a variety of platforms as follows:

- Windows NT, 2000, XP, and 2003
- AIX
- HP-UX
- Solaris

Viewer, Reporter, and Security Monitor

The Viewer, Reporter, and Security Monitor are all Windows-based applications and require Windows NT, 2000, or XP.

Audit Policy Manager

The Policy Manager lets administrators activate and modify default policy rules provided with eTrust Audit. It also lets administrators write new policy rules. The policy rules specify filters for the events that are received at designated Routers, called Audit Nodes (AN) in the Policy Manager interface. Administrators can even define groups of ANs so that they can distribute policy rules to a number of systems. For example, you might create an AN group comprised of all systems where the eTrust Antivirus application is running.

After the Router receives the policy rules, it works independently of the Policy Manager to filter events until the Policy Manager distributes a new version of the policy rules.

The Policy Manager component includes the following:

- Policy Manager GUI
- Distribution Server, a Windows service that distributes policies to the ANs (routers)
- Default policies, a set of pre-built policies based on Log Names.

  You can add other policies to this set by importing custom policies using the pmu_template_exchange.exe command.

How the Policy Manager is Involved in Event Processing

While default policy rules are provided and available for use after you install eTrust Audit, you must activate and distribute them to make them take effect on the servers where you have installed Clients. Therefore, to begin receiving events on any Client, an administrator must do the following:

1. Create ANs and AN groups.
2. Modify default policy rules (or create new ones) and associate the policy rules with an AN group.
3. Activate the policy rules.
4. Distribute the policy rules to the appropriate Clients.

Based on the rules, events are filtered and routed to the various other components of eTrust Audit.

See the *Audit Management Guide* for information on how to create a policy, define groups of ANs, and distribute policies to AN groups.

About Supported Platforms

The Policy Manager runs on Windows 2000, XP, and 2003.

About Improving Security and Network Communications

In today's security-conscious environment, the eTrust Audit system encounters security-related obstacles as enterprises try to deploy it across large networks. The flexible implementation possibilities available with eTrust Audit let you install the Client components on various systems. For example, you might install recorders on remote systems and the rest of the Client components on a centralized server that routes events from a number of recorders. If any of these recorders are outside your firewall, you might experience some of the following problems:

- The RPC protocol is rarely permitted across firewalls because it uses dynamic TCP/UDP ports. RPC also lacks the secure communications standards that other protocols, such as TCP or HTTPS provide.

  eTrust Audit uses RPC to send events to the Router, deliver policies from the Policy Manager, and forward events to Collector and Security Monitor (OCRA). If any of these components are deployed across a firewall, the system may fail due to the firewall blocking RPC traffic. One solution is to use fixed TCP ports and open these ports on the firewall. However, the question of data protection against network spoofing or tampering remains open.

- Guaranteed delivery is enforced in OCRA but not in SAPI, thus running the risk of losing original events.

- Secure delivery through encryption is assured with OCRA but not with SAPI, which is the route taken by the events from the Recorder to the Router. This problem becomes critical when the Recorder is separate from the Router, where most often the Recorder is located outside the intranet and is thus unguarded against spoofing.

- There is no provision to ensure events are not tampered with during their journey from the Recorder to the Router.

Appendix B: iTechnology Overview

This section contains the following topics:

iTechnology Overview

iTechnology is a CA technology based on web standards such as HTTP, HTTPS, HTML, XML, and SSL. It provides a framework to create and deploy web services across the Internet.

The building blocks of iTechnology are as follows:

iGateway (see page 38)

A web server

iSponsor (see page 39)

A web service loadable by iGateway

iClient (see page 42)

A stand-alone web client

Event Plugin (see page 43)

A DLL used by iControl to handle specialized tasks such as converting formats, applying filters, sending events to a database

iRouter (see page 43)

Middleware that routes events from iRecorders to the eTrust Audit router

iGateway

iGateway is a web server that runs as a Windows service or UNIX/Linux daemon process. Its purpose is to receive requests and send replies using the HTTP protocol. It also supports the HTTPS protocol for data protection against eavesdropping and tampering over the Internet. The format of request and reply is HTML and XML. The iGateway sends the requests using HTTP GET, HTTP POST, or SoapAction.

iGateway receives requests from any of the following sources:

- Web browser
- iGateway (iGateways can receive requests from other iGateways)
- iReflect
- iClient
- A local iSponsor (for unsolicited event sending)

The iGateway redirects these requests to its underlying web services called iSponsors. Based on the request, appropriate replies in XML or HTML format are built by iSponsor and sent back to the requester using the iGateway.

All network communications use the TCP iTechnology port 5250. In a protected environment, open this port in the firewalls and border routers to permit iTechnology communications. This is similar to permitting HTTP traffic through firewalls (port 80).

iSponsor

An iSponsor is a dynamically loadable library that preloads at startup or loads on-demand when a request is routed to the specific iSponsor. It is a plug-in to iGateway. It exposes selected application programming interfaces (APIs) to iGateway when loaded.

Requests to an iSponsor specify which service it needs from iSponsor. The specified service includes the API, a set of methods instructing how the software should communicate with other software, and the parameters. iGateway invokes the appropriate methods and passes the parameters to the corresponding iSponsor. The iSponsor's methods return an HTML or XML response. The response is forwarded to the requester. An iSponsor can have a plug-in that sends data to a non-iTechnology application or device. The sending protocol depends on the application or device and is not necessarily HTTP.

All iSponsors implement two standard methods:

describe

Returns the sponsor's name and version.

define

Returns all the methods defined in the sponsor.

Also, each iSponsor can implement other methods to support the specific functionalities of that iSponsor.

You can create an iSponsor using the iTechnology Software Development Kit (SDK) or the iRecorder SDK. Use the iRecorder SDK to create iRecorders only. For more information about these SDKs, see the *eTrust Audit Reference Guide*.

Examples of iSponsors

Examples of iSponsors include the following:

iRegistry

Scans a specified portion of an Internet network for active iGateway hosts and lists existing iGateway hosts on the network. iRegistry includes a plug-in to store discovered iGateway hosts in a repository. This iSponsor is included in the iGateway or iRecorder distribution.

iAuthority

Acts as a trusted Central Authority for registered iGateways. It distributes and revokes digital certificates for authentication and authorization of trusted iGateways. A valid digital certificate distributed by iAuthority must accompany any request to privileged methods in an iSponsor. The iSponsor can reject the request if the privileges granted by the certificate are not sufficient to run a method. iAuthority is included in the iGateway or iRecorder distribution.

iControl (see page 41)

Plays a central role in the iTechnology event management system. This iSponsor regulates the flow of unsolicited data, specifically the flow of audit events from the iRecorder to the router. iControl can include plug-ins called Event Plugins, a type of web service. iControl is included in the iGateway or iRecorder distribution.

iRecorder (see page 45)

Harvests events from sources such as applications, databases, devices, log files, and operating systems. These events are then sent through iControl.

iReflect (see page 42)

Behaves like an iSponsor but is not loaded by iGateway. iReflect is a dynamically loadable library that registers itself with iGateway. It communicates between non-iTechnology applications and iGateway.

Spindle

Serves web pages.

iControl

iControl is a critical component for the iRecorder. All event traffic must pass through iControl.

Features of iControl include the following:

Persistent Connection

HTTP and HTTPS are typically used as short-lived connections for a single request-reply communication. This means that when a reply is received, the connection is terminated. Persistent connection does not perform well with a constant flow of events, which can deplete system resources in terms of connections and may trigger a false alarm of denial-of-service on intermediary routers or firewalls.

You can configure iControl to use persistent or long-lived connections to send all events through one connection to the remote iControl. This method of sending is more efficient in terms of significant throughput and more economical in terms of system resources. Configure this option using the EventUsePersistentConnections parameter.

Use of HTTPS

You can enforce HTTPS use in iControl by setting the EventUseHttps parameter. HTTPS encrypts data before sending it over HTTP, ensuring data privacy.

Event Signing

Event signing guarantees that an event is not tampered with during its transit to the remote iControl. You can turn event signing off using the IgnoreSignature parameter.

Guaranteed Delivery

Events sent from the iGateway host are guaranteed to reach the specified destination. Events are temporarily stored in local storage in case the destination is temporarily unavailable. These events are removed from local storage only when the events reach their intended destination.

Bridge to eTrust Audit (iRouter)

When iRouter is installed, an event plug-in called epAudit is attached to iControl. This plug-in receives events from iControl, converts XML format into SAPI calls, and sends the converted events to the local eTrust Audit router using the SAPI protocol.

When iControl sends events, it can use two methods: push or pull.

Event Pushing or Routing

In push method, the sender iControl initiates the communication and sends events to the destination host, called the RouteEventHost. The iRecorder installation script prompts and sets this configuration parameter in the iControl.conf file.

Event Pulling or Storing

In pull method, the sender iControl waits for the destination to call before it sends events. During this interval, it stores the events for the destination in StoreEventHost. The destination iControl retrieves the events from the sender or RetrieveEventHost. You can configure an iRecorder to set the StoreEventHost if you use the pull method. The pull method is most suitable for network environments with outgoing traffic only.

iReflect

An iReflect is a “detached” iSponsor. It is loaded by a non-iTechnology application instead of iGateway. It behaves like an iSponsor in the following ways:

- It is a dynamically loadable library like an iSponsor.
- After it is loaded by the application, it registers with the local iGateway and exposes its methods.
- It receives HTTP and HTTPS requests from the local iGateway and returns responses to it.
- Because an iReflect must be able to receive requests from its local iGateway at any time, it runs a thread that continuously listens on iTechnology port 5250.

One example of an iReflect used to send events to eTrust Audit is the Unicenter Event Management iRecorder.

iClient

iClient acts as a Web browser. It sends requests to an iGateway and receives replies from it. However, an iClient cannot receive requests from an iGateway and it cannot publish its internal methods for an iGateway to use. Therefore, you can deploy an iClient component as a dynamically loadable library to be loaded by a non-iTechnology application or as a standalone program.

Event Plug-in (EP)

The Event plug-in is a DLL used by iControl to handle specialized tasks such as converting formats, applying filters, sending events to a database, and so on. Examples of the Event plug-ins include the following:

EPAudit Plug-in

When the EPAudit plug-in is configured, all events received by iControl are sent to the EPAudit plug-in to be delivered to the Router. Functions of EPAudit plug-in include the following:

- Convert events from XML format to eTrust Audit SAPI format.
- Submit events to the eTrust Audit Router component running on the localhost.

EPUnicenter Plug-in

When the EPUnicenter plug-in is configured, all events received by iControl are sent to the EPUnicenter to be delivered to the Event Management component of Unicenter. Functions of the EPUnicenter plug-in include the following:

- Convert events from XML format to Unicenter Event Management format.
- Submit events to the Event Management component running on the localhost.

EPDebug Plug-in

When the EPDebug plug-in is configured, all events received by iControl are sent to the EPDebug to be delivered to any Debug Viewer running on the localhost.

iRouter

The iRouter is a middleware component that sits between the iRecorders and the eTrust Audit Router (a client component). It receives events in XML format from iRecorders and forwards those events to the eTrust Audit Router using Submit API. For more information, see the *eTrust Audit Reference Guide*.

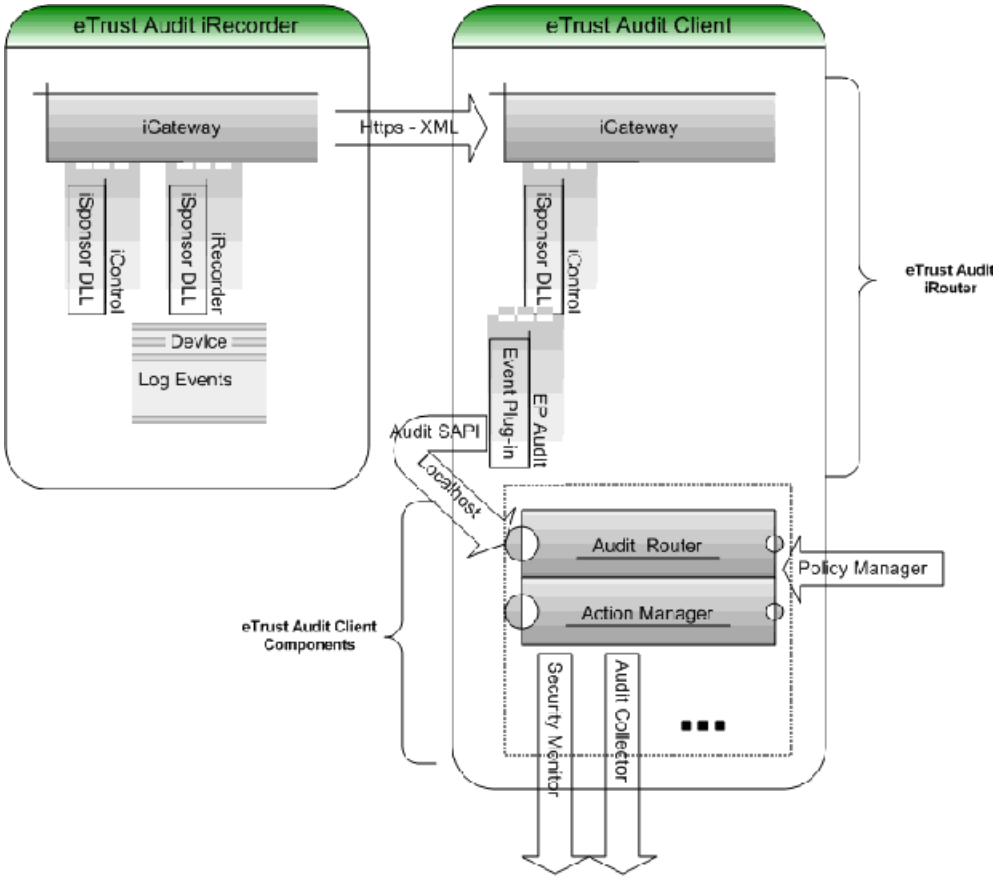
Note: You must install the eTrust Audit iRouter on the same host as the eTrust Audit Router. The iRouter and Router cannot communicate if installed on two separate hosts. You can install iRecorders and the iRouter on the same host or on separate hosts.

iRecorders and iRouters

Recorders are subcomponents packaged with eTrust Audit client components. These predefined recorders use the eTrust Audit Submit API (SAPI) to send log events to a Router and Action Manager for further processing as defined in the Policy Manager.

iRecorders are eTrust Audit client components developed using the iRecorder SDK, which is based on iTechnology SDK. iRecorders, like recorders, send log events to a Router and Action Manager for event processing. They require an intermediate component, an iRouter, which is installed on an existing eTrust Audit Client. The iRouter provides a bridge between the iRecorder and the eTrust Audit Client.

The following illustration shows the flow of information from the iRecorder to the eTrust Audit client components.



Role of the iRecorder

An iRecorder is a special type of iSponsor that sends unsolicited data, such as events, to an event management system such as eTrust Audit. Like a recorder, you deploy the iRecorder on or near the system that reports events in order to harvest them easily. Unlike recorders, iRecorders can receive events from physical devices, applications, databases, or operating systems. Sources and systems are usually located on the same host.

After it harvests events from the source, the iRecorder assigns an event classification (taxonomy) to events from similar sources, and maps information in the events as field-value pairs to a normalized data model. A common taxonomy and data model permit correlation from different sources.

The field-value pairs are packed in an XML string and sent to the iRouter. The iRouter converts the XML string into SAPI events and sends them to the local router. Events are processed and forwarded to the Action Manager and then to the Security Monitor or collector, according to the corresponding policy rules installed on the iRouter host.

The iRecorders contain a set of predefined policies to be imported in the eTrust Audit Policy Manager as part of the default policies. For more information, see the *eTrust Audit Management Guide*.

Role of the iRouter

The iRouter is the bridge that links the HTTP-based iTechnology components with eTrust Audit. The iRouter converts data it receives in XML format to the SAPI protocol and sends the converted event to a router. For more information, see the *eTrust Audit Reference Guide*.

An iRouter consists of the following components:

iGateway

Receives events from local iRecorders, remote iGateways, or remote iClients.

iControl

Receives events from an iGateway and routes them to another iGateway or to event plug-ins.

epAudit

Receives events from iControl, parses them into field-value pairs, and sends them to the local Audit router using SAPI.

Note: For the iRouter to properly send events to an existing eTrust Audit implementation, you must install the iRouter on the same system with eTrust Audit Router.

iRecorder and iRouter Installation

Deploying iRecorders in an eTrust Audit environment requires the following actions:

- Install the eTrust Audit system.
- Install the iRouter on the same system as the Router.
- Import any predefined policies distributed with your iRecorder to the Policy Manager.
- Activate and distribute the policy rules to the Routers and iRouters.

Note: You must install the iRouter before you install an iRecorder, as the installation of the iRecorder requires the host address of the iRouter.

Index