CA Audit

iRecorder Integration Guide for CA Identity Manager

CA Product References

This document references the following CA products:

- CA Audit
- CA Security Command Center

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: Introduction

This section contains the following topics:

Overview

CA Audit iRecorder captures events generated by an application, normalizes the events, and routes these events to CA Audit for further processing. The iRecorder can capture events from physical devices, applications, databases, or operating systems.

The iRecorder for CA Identity Manager harvests the event data generated by CA Identity Manager and submits the normalized event data to CA Audit for further analysis and reporting. It supports normal auditing and Fine Grained Auditing (FGA).

Who Should Read This Guide

This guide describes how to integrate the iRecorder for CA Identity Manager into your CA Audit environment. It is for system administrators who install the iRecorder and for Security Information Management (SIM) professionals who create policies to handle CA Identity Manager events after the iRecorder is installed.

This guide provides product-specific configuration and reference information. It does not include detailed installation and testing instructions; that information is provided in the *eTrust Audit and eTrust Security Command Center Implementation Guide.*

Note: For more information about CA Audit, including creating and managing policies, see *eTrust Audit and eTrust Security Command Center Implementation Guide* or the *eTrust Audit and eTrust Security Command Center Administration Guide.*

Chapter 2: Installing and Configuring the iRecorder

This section contains the following topics:

How to Install the iRecorder

The process for downloading and installing an iRecorder involves the following steps:

1. Download the CAZIPXP.EXE utility, the iRecorder package, and the supported iGateway package from the CA Support Online website as follows:
   - Install the iGateway package.
   - Unzip the downloaded iRecorder package.
   - Move the files to the target system manually, if necessary.
2. Install the iRecorder on a specific platform or platforms.

   Note: If you perform a silent install, create a response file.
3. (Optional) Change the iRecorder's configuration files.
4. Create or import, and then distribute, policies to capture events as follows:
   - Import the iRecorder's default policy file to the Policy Manager database.
   - Update the default policy or create a new one.
   - Distribute the policy to audit nodes.
5. Test the iRecorder events from the Policy Manager.

   Note: See the eTrust Audit *and eTrust Security Command Center Administration Guide* or the Policy Manager online help for more information.

Configure the iRecorder

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

To configure the iRecorder for additional tasks such as capturing debug information, or changing the log directory, you can modify the parameters in the configuration file.

To configure the iRecorder

1. Enter the following command to stop the iTechnology iGateway service (or daemon) before making the changes.

   Windows:

   ```
   net stop igateway
   ```

   UNIX:

   ```
   sh S99igateway stop
   ```

2. Open the iRecorder configuration file (eAC.conf), edit the parameters as required, and save the file.

3. Enter the following command to restart the iGateway service (or daemon) for changes to take effect:

   Windows:

   ```
   net start igateway
   ```

   UNIX:

   ```
   sh S99igateway start
   ```

   The iRecorder starts collecting events based on the parameters set in the configuration file.

Note: The configuration parameters of the iRecorder can be changed using the Audit Administrator iRecorder Manager, which also provides features such as discovery of iRecorders on a particular host, testing, or stopping/starting iRecorders. See the "Using iRecorder Manager" chapter of the *CA Audit and eTrust Security Command Center Administration Guide* for more information.

Configuration Parameters

You can configure the following configuration parameters in the IdentityMinder.conf:

DebugLevel

Allows the iRecorder to send debugging information to a debugging application or a file.

Note: You must add this parameter to capture the debug information and send the debug file to CA Technical Support for further analysis.

Example:

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

In this example, {level} is one of the following:

ISP_NOLEVEL

Disables debugging.

ISP_TRACE

Prints all the debug messages that include trace, warning, and error messages into a debugging application.

ISP_WARNING

Prints all the debug messages that include warning and error messages into a debugging application.

ISP_ERROR

Prints the debug messages that include only error messages into a debugging application.

Note: The ISP_TRACE, ISP_WARNING, and ISP_ERROR tags do not log messages to a file.

ISP_FILE

Prints all debug messages to a debug application as well as writes them to a log file, IdentityMinder.log, in the same directory as the iRecorder. The debug file may grow very quickly. To avoid possible disk space shortage, we recommend disabling the debugging option by replacing ISP_FILE by ISP_NOLEVEL. ISP_FILE writes only ERROR messages to the log file.

Examples: Commands for printing messages

The following are examples of commands to print messages:

- Warning and trace messages:

  ```
  <DebugLevel LogLevel="WARNING">ISP_FILE</DebugLevel>
  ```

- Warning and error messages:

  ```
  <DebugLevel LogLevel="TRACE">ISP_FILE</DebugLevel>
  ```

  Note: By default, the iRecorder records the errors in the IdentityMinder.log file, which is in the same directory as the iRecorder. The debug_level setting is ignored.

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 CA Identity Manager

You can verify that the iRecorder is installed properly and sending events to eTrust Audit by testing event routing.

To test event routing

1. Install the iRecorder component on a UNIX host. CA Identity Manager should be installed on the same host.
2. Install eTrust Audit iRouter component on a host where eTrust Audit Client components are installed.
3. Verify that /opt/CA/SharedComponents/iTechnology contains the following files: IdentityMinder.so and IdentityMinder.conf
4. Start the eTrust Audit Policy Manager and define a policy for CA Identity Manager events received by the host where iRouter and the other eTrust Audit Client components are installed.
5. 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).
6. If there is no defined policy (rule and action), eTrust Audit ignores the events. You can find more details about how to create a policy in the *CA Audit Management Guide*.
7. Start Identity Manager and make sure Auditing is enabled. For details, see *CA Identity Manager Administration Guide*.
8. Execute a View User task.
9. 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 on these tools, see the iTechnology SDK Reference Guide.

Chapter 3: CA Audit Field Mapping

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

About Mandatory Fields

Mandatory fields are a fixed set of fields that are added to each event processed by any iRecorder. The following information describes what values are assigned to the mandatory fields in the CA Identity Manager.

Field name	Description	Identity Manager Value
Taxonomy	Taxonomy field is defined as Category.System.Action.Result.Severity	IdentityManagement.{System }.{Event name}.S{Severity} For example: IdentityManagement.Object Management.CreateGroupEvent.S
Date	The timestamp of the event. The format is in time_t (number of seconds since 1/1/1970 12am UTC).	Time stamp on the event
TimeZone	This field shall contain 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 shall be –18000 (or –5 hour) in Winter and during daylight saving time it shall be –14400 (or -4 hour)	This is calculated automatically from the Date field.
Src	Src (Source) is the name of the component (device, application, or product) that created the event.	Identity Manager Environment name For example: neteauto

Log	Log identifies the logical name of the auditing device where the events are picked up. For example, on a UNIX system, several applications (Sources) may write to Syslog. In this case, the Source would be the application name and the Logname would be Syslog.	CA Identity Manager
Location	Location identifies the hostname or IP address of the Identity Manager Server.	@ actual. This is automatically determined by the iRecorder
Recorder	This field provides the name of the recorder that captured the event.	CA Identity Manager iRecorder
RecorderHost	The FQDN of the host running the iRecorder. This is different than the Location field as the iRecorder can be installed remotely. However the Identity Manager iRecorder is not designed to be operated remotely, this will be same as the Location.	@ actual This is automatically determined by the iRecorder
Version	Version keeps track of the version of the recorder that captured the event.	iRecorder version. This is automatically determined by the iRecorder.

About the Taxonomy Field

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

Field Name	Possible Values	Description
Category	Identity Management	Hardcoded
System	Object Management Relationship Management	Depends on the type of event being generated.
Action	See the *Administration Guide*	The name of the Identity Manager Event that generated this record

Field Name	Possible Values	Description
Result	S, F, N	Success: S Failure: F None: N
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 This can be configured in the CA Identity Manager Audit configuration XML using the CA Identity Manager management console.

Normalized Fields

Normalized fields are CA 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.

Fields for Object Management System

The following table shows the fields for Object Management System:

Field Name	Description
AdminID	Uniquename of initiator of the request.
AdminUniqueName	Long/Friendly Name, typically the login name.
ObjectType	Type of the Object the event is about.
ObjectID	uniqueID of the Object (User, Group, Role….).
ObjectUniqueName	Long description of the object
AttrType	Any type identifier for the attribute being modified. This attribute is optionally populated.
AttrName	Name of the attribute being audited. This attribute is optionally populated.

AttrOldValue	Old value of the attribute being audited. This attribute is optionally populated.
AttrNewValue	New value of the attribute being audited. This attribute is optionally populated.
EventInfo	CA Identity Manager event description. This attribute is optionally populated.

Fields for Relationship Management System

The Action in the taxonomy will tell the exact relationship between the Object and the Container.

Field Name	Description	Example
AdminID	Uniquename of initiator of the request.	uid=admin1, ou=people,o=security.com
AdminUniqueName	Long/Friendly Name, typically the login name.	Admin1
ObjectType	Type of the contained Object.	USER, GROUP, ROLE
ObjectID	System token/uniqueID of the Object (User, Group, Role….).	uid=user1, ou=people,o=security.com
ObjectUniqueName	Long description of the object	user1
ContainerType	Type of the Container Object.	GROUP, ROLE, ORG
ContainerID	System token/uniqueID of the Container Object (User, Group, Role….).	cn=User, ou=groups,o=security.com
ObjectUniqueName	Long description of the object	User
EventInfo	This attribute is optionally populated.	None

Product-Specific Fields

Product Specific fields are native event fields that are not mapped or translated by the iRecorder. These fields are sent to CA 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 CA 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 CA Identity Manager

The following table shows the product-specific fields for CA Identity Manager:

Field name	Description	Example
transactionid	Transaction GUID. This is the Access control transaction Siteminder Started.	123-qwwer-12asd-1212
Eventname	Name of the event	ModifyUserEvent
eventstate	State of the event when logged.	APPROVED, COMPLETED Totally 7.
taskoid	Unique ID of the Identityminder Task that this event is associated with.	25-1234-asdf-12as-4561
taskname	The Name of the IdentityMinder Task that the event is associated with.	Modify User