eTrust® Audit

Administration Guide

r8 SP2 CR1

CA Product References

This document references the following CA products:

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

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 1: Managing Audit Administrator

Audit Administrator is the web-based user interface for eTrust Audit. As an Audit Administrator user with the Admin role, you can perform any of the following functions:

- Configure users and roles, access and distribution settings, and update content.
- Discover, query, and set up iRecorders.
- View status information based on the rate of events received from event sources using the Health Monitor.

This section contains the following topics:

Audit Host Discovery

You can set up and view discovery job status for eTrust Audit Hosts from the Configuration tab.

A discovery job lists the hosts that are running iRecorders, Health Monitor, or Post-Collection Utilities. You can select the subnets on which you want to run the discovery job and schedule how often you want the job to run.

More information

Add a Discovery Job

You can add a discovery job to determine which hosts are running iRecorders, Health Monitor, or Post-Collection Utilities.

To add a discovery job

1. Click Audit Host Discovery.

   The Discovery Jobs pane opens.

2. Click New Job at the top of the pane.

   The New Discovery Job dialog opens.

3. Enter the Subnet and Interval information, and click Save.

   The new job appears in the Discovery Jobs pane.

   Note: You must enter the information in the following format:
   Network address/subnet mask bits

   For example, you might enter a Class C subnet as follows:
   10.1.1.0/24

   and you might enter a Class B subnet as follows:
   10.1.0.0/16

You can view the details in the Discovery Statistics and iRegistry Plugin Status panes.

More information

Delete a Discovery Job (see page 10)
Host Properties (see page 11)

Delete a Discovery Job

You can delete unneeded discovery jobs.

To delete a discovery job

1. Click the **X** button in the Remove column beside the discovery job you want to remove.

   A confirmation dialog appears.

2. Click OK.

   The deleted job is removed from the Discovery Jobs pane.

More information

Add a Discovery Job (see page 10)
Host Properties (see page 11)

Host Properties

Hosts have a single *state* property. The property value depends primarily on the presence of an installed eTrust Audit client. When an Admin level user performs a Host iRecorder discovery process, the possible returned host states are as follows:

Unmanaged

Unmanaged nodes have no client component installed on them, and thus cannot receive policies or Message Parsing (MP) files from the distribution server.

Managed

Managed nodes have a client component installed, and you can control the event capture from them using the Policy Manager.

More information

Add a Discovery Job (see page 10)
Delete a Discovery Job (see page 10)

Updating Content

You can update Audit Administrator content from the Configuration tab by downloading the following information from a CA website:

iRecorder data models

Map event information into different audit fields. These audit fields along with their descriptions and possible values are called data models and are used by the Rule Builder utility.

Rule Templates

Filter and correlate events stored in the local Rule Template Library. You download rules as a package rather than individually, and newly-downloaded templates overwrite any existing templates in the library.

Visualizer Queries

Extract a subset of events from the Audit Collector database using predefined queries and display them in a table or network diagram. The Visualizer is available only on a Windows Policy Manager.

MP Files

Interpret text-format log event data. You can download the latest MP files for distribution to the eTrust Audit clients in your environment.

More information

Download iRecorder Data Models (see page 12)
Download Rule Templates (see page 13)
Download Visualizer Queries (see page 13)
Download MP Files (see page 14)

Download iRecorder Data Models

You can download the latest data models for iRecorders from a CA website.

To download data models

1. Click Content Update in the Configuration tab.

   The Content Update pane displays the default download site.

2. Enter the URL where the data model files are stored, or use the default site displayed in the Download Data Models pane.

3. Enter your User Name and Password (if required), and click Download.

   The Updated Content Status pane displays a list of data models and their download statuses.

More information

Download Rule Templates (see page 13)
Download Visualizer Queries (see page 13)
Download MP Files (see page 14)

Download Rule Templates

You can download the latest rule templates from a CA website. The downloaded templates overwrite any existing templates in the library.

To download rule templates

1. Click Content Update in the Configuration tab.

   The Content Update pane displays the default download site.

2. Enter the URL where the rule templates are stored, or use the default site displayed in the Download Rule Templates pane.

3. Enter your User Name and Password (if required), and click Download.

   The Updated Content Status pane displays a list of rule templates and their download statuses.

More information

Download iRecorder Data Models (see page 12)
Download Visualizer Queries (see page 13)
Download MP Files (see page 14)

Download Visualizer Queries

You can download the latest queries for the Visualizer from a CA website. This feature is available only on a Windows Policy Manager.

To download Visualizer queries

1. Click Content Update in the Configuration tab.

   The Content Update pane displays the default download site.

2. Enter the URL where the queries are stored, or use the default site displayed in the Download Visualizer Queries pane.

3. Enter your User Name and Password (if required), and click Download.

   The Updated Content Status pane displays a list of query files and their download statuses.

More information

Download iRecorder Data Models (see page 12)
Download Rule Templates (see page 13)
Download MP Files (see page 14)
Audit Host Discovery (see page 9)

Download MP Files

You can download the latest MP Files from a CA website.

To download MP files

1. Click Content Update in the Configuration tab.

   The Content Update pane displays the default download site.

2. Enter the URL where the MP files are stored, or use the default site displayed in the Download MP files pane.

3. Enter your User Name and Password (if required), and click Download.

   The Updated Content Status pane displays a list of MP files and their download statuses.

More information

Download iRecorder Data Models (see page 12)
Download Rule Templates (see page 13)
Download Visualizer Queries (see page 13)

Managing Users and Access

You can configure user role assignments and access to the interface for your Audit Administrator environment by completing the following tasks:

- Search, sort, or add and remove users, and assign user roles using User Management.
- Segregate the Maker and Checker roles' creation and approval rights for Policy Manager objects using Access Management.
- Configure the Embedded Identity and Access Management (EIAM) server for Global Users and User Groups using User Source Management.

More information

User Management Tasks (see page 17)
User Source Management (see page 25)
User Roles (see page 15)

User Roles

Audit Administrator provides predefined user roles with the following responsibilities and privileges:

Admin

Performs configuration tasks and defines and creates users and roles.

Maker

Creates folders, policies, MP files, and rules.

Checker

Reviews and rejects or activates policies or MP files.

Viewer

Views events using the Viewer and Health Monitor alerts and logs.

Reporter

Views and schedules reports.

For detailed information about user privileges, consult the following table.

USER PRIVILEGES	Admin	Maker	Checker	Viewer	Reporter
Create internal IAMT users	Y	N	N	N	N
Define (Create, Update, Delete) roles	Y	N	N	N	N
Associate roles to internal/global users	Y	N	N	N	N
Configure CA ftp site	Y	N	N	N	N
Configure iRecorder Auto-discovery	Y	N	N	N	N
Update Data Models	Y	N	N	N	N
Update Rule Templates	Y	N	N	N	N
Update MP	Y	N	N	N	N
View iRecorder Status	Y	N	N	N	N
Configure iRecorder	Y	N	N	N	N
Configure Distribution Server	Y	N	N	N	N
Configure Data Sources	Y	N	N	N	N
Configure Health Monitor parameters	Y	N	N	N	N
Create policy folder	N	Y	N	N	N
Create MP folder	N	Y	N	N	N
Make (Create, Update, Delete) Policy/MP	N	Y	N	N	N
Commit Policy/MP	N	Y	N	N	N
Create AN group	N	Y	N	N	N
Create AN node	N	Y	N	N	N
Associate Policy/MP to AN group	N	Y	N	N	N
Dissociate Policy/MP to AN group	N	Y	N	N	N
Disable Node	N	Y	N	N	N
Approve changes to Policy/MP and AN group	N	N	Y	N	N
Reject changes to Policy/MP and AN group	N	N	Y	N	N
View events (using Viewer)	N	N	N	Y	N
View Health Monitor alerts	N	N	N	Y	N
View Health Monitor logs	N	N	N	Y	N
Configure reports	N	N	N	N	Y
View reports	N	N	N	N	Y
Schedule reports	N	N	N	N	Y

More information:

Policy Manager Tasks (see page 37)
How Basic Maker Work Flows Progress (see page 40)
How Checker Work Flows Progress (see page 47)

User Management Tasks

You can perform user management tasks, including the following:

- Searching for users by attributes including name, role, or group membership
- Assigning or changing user roles
- Configuring user authentication policies
- Using the CA Management Database (CA-MDB) to do the following:
  - Creating users
  - Setting user contact and identification information
  - Set passwords and password policies

More information

Add a User (see page 17)
Remove a User (see page 18)
Search for Users (see page 18)
Change User Details (see page 19)
Assign or Change User Roles (see page 20)

Add a User

You can add a user. This feature is only available if you are using the internal CA Management Database (CA-MDB) to store users and credentials.

To add a user

1. Click the New User button in the Users pane. The button appears to the left of the Users folder.

   The New User pane appears.

2. Enter the required information, and click Add Application User Details.

   The Application Group Membership pane appears.

3. Assign the appropriate user roles, and click Save.

   The new user appears in the User pane with a confirmation message.

More information

Remove a User (see page 18)
Search for Users (see page 18)
Change User Details (see page 19)
Assign or Change User Roles (see page 20)
Setting Passwords or Password Policies (see page 21)

Remove a User

You can remove a user. This feature is only available if you are using the internal CA Management Database (CA-MDB) to store users and credentials.

To remove a user

1. Select the user you want to remove, and click Delete.

   A confirmation dialog appears.

2. Click OK.

   The user is removed and a confirmation message appears.

More information

Add a User (see page 17)
Search for Users (see page 18)
Change User Details (see page 19)
Assign or Change User Roles (see page 20)
Setting Passwords or Password Policies (see page 21)

Search for Users

You can search for users when using an external LDAP directory.

To search for users in an external LDAP directory

1. Click the Configuration tab, and then the User and Access Management sub-tab.
2. Click the User Management link.
3. Choose one of the following search types:
   - Select Global Users if you want to search any user irrespective of application.
   - Select Application User Details if you want to search any user for a particular application.

   The asterisk wildcard character is supported in the search value.
4. Enter your search criteria and click Go.

   If the search is successful, user names appear in the Users pane as child nodes of the Users tree. Leave the Value field empty to display all users.

Note: Except for assigning Audit Administrator user roles, the other information that appears is read-only. You can make changes to the information from your LDAP directory's user interface.

More information

Add a User (see page 17)
Remove a User (see page 18)
Change User Details (see page 19)
Assign or Change User Roles (see page 20)
Setting Passwords or Password Policies (see page 21)

Change User Details

The types of user details you can change depend upon the type of directory to which you connect. You can change details for a user only if you selected the CA Management Database (CA-MDB) in the Configuration tab's User Source Management area. If you select an external directory, global user and groups details are read-only.

Note: Changes to some areas, such as the Global User Details and Global Group Membership sections, must be made from the Embedded Identity and Access Management (eIAM) interface, or in your external directory's interface.

To change user details from the Audit Administrator

1. Search for a global or application user using a combination of attributes, comparison operators, and specific values.

   Select Global Users if you want to search any user irrespective of application. Select Application User Details if you want to search any user for a particular application. The asterisk wildcard character is supported for use in the search value.

   A list of users corresponding to the search criteria appears in the Users pane at the left and below the Search pane.

2. Click on the user name you want.

   The details display in a separate area to the right.

3. Scroll to the desired section, make changes as allowed, and click Save.

   A confirmation message appears.

More information

Add a User (see page 17)
Remove a User (see page 18)
Search for Users (see page 18)
Assign or Change User Roles (see page 20)
Setting Passwords or Password Policies (see page 21)

Assign or Change User Roles

You can assign roles to users to control their access to the eTrust Audit Administrator. To do so, you must be logged in to Audit Administrator as a user with the Admin role.

The software provides the following basic user roles (see page 15) with default access privileges as part of the installation. You can create additional roles using the Embedded Identity and Access Management (eIAM) server interface.

To assign or change user roles

1. Search for a global user using a combination of attributes, comparison operators, and specific values.

   A list of users corresponding to the search criteria appears in the Users pane at the left.

2. Click on a user name to see details for that user.

   The details display in a separate area to the right.

3. Scroll to the Application Group Membership area.

4. Click one of the entries in the Available User Groups list and then click the right arrow to copy that membership into the Selected User Groups list.

   Note: You can use the double arrows as a shortcut to copy all items to, or to remove all items from, the Selected Groups list.

5. Click Save when you finish assigning roles.

   A confirmation message appears.

More information

Add a User (see page 17)
Remove a User (see page 18)
Search for Users (see page 18)
Change User Details (see page 19)
Setting Passwords or Password Policies (see page 21)

Setting Passwords or Password Policies

Normally you set a password as part of creating a new user. If you need to change a user's password or password policies from the Audit Administrator interface, use the following procedure.

To set a password from the Audit Administrator interface

1. Log in to the Audit Administrator as an Admin level user.
2. Click the User and Access Management sub-tab and then click the User Management link.
3. Search for the desired user.
4. Scroll down to the Authentication section.
5. Click the Reset Password check box.

   Enter and confirm the new password and click Save.

More information

Add a User (see page 17)
Remove a User (see page 18)
Search for Users (see page 18)
Change User Details (see page 19)
Assign or Change User Roles (see page 20)

How to Manage Access

You can manage access to eTrust Audit by choosing whether to restrict file approval actions by enabling the segregation of duty feature, which is off by default.

If you do not enable segregation of duty, approval remains unrestricted; any user with both the Maker and Check roles may modify or approve any file. If you choose to enable segregation of duty you may choose strict segregation, or a more relaxed form called transactional.

Use the following process to enable Segregation of Duty:

1. Select the type of Segregation of Duty you want, strict or transactional.
2. Modify the policydb.conf file if you want transactional Segregation of Duty
3. Enable Segregation of Duty from the Policy Manager interface.

More information

Access Management (see page 22)
Enable Transactional Segregation of Duty (see page 23)
Set Access Management (see page 24)

Access Management

Segregation of Duty lets you control whether a single user can assume both Maker and Checker roles for the same policy or MP file. Two levels of segregation of duty checking are available, strict and transactional. By default, when you turn on the feature, eTrust Audit uses the strict level.

Transactional segregation of duty allows smaller organizations to take advantage of segregation of duty without requiring as much staff.

At either level, no single person is allowed to be both Maker and Checker for the same production change or file.

- Strict segregation of duty does not allow any user with the Maker role to also be a Checker for any file or part of a file, that contains changes made or submitted by that Maker.
- Transactional segregation of duty allows the same person to be both Maker and Checker on a file or folder, provided that the person performing the Checker role was not the person who made the most recent change.

Stated another way, in transactional segregation of duty, the Maker of a policy or MP file can be a Checker in the future for an update to that same policy or MP file, and a Checker for a policy or MP file can be a Maker for an update to that same policy or MP file in the future.

More information

Enable Transactional Segregation of Duty (see page 23)
Set Access Management (see page 24)

Enable Transactional Segregation of Duty

You can enable transactional segregation of duty in the policydb.conf file, allowing a user to act as both Maker and Checker on a single file or folder in certain circumstances.

When you install eTrust Audit, the default segregation of duty style is strict, and the default setting is Off. Setting the segregation of duty option to On automatically enables the strict version. You must modify the Policy Manager configuration file if you want to use transactional segregation of duty.

To enable the transactional segregation of duty style

1. Log on to the physical Policy Manager server as a root or Administrator user and access a command prompt.
2. Navigate to the appropriate directory:

   Windows: \Program Files\CA\SharedComponents\iTechnology

   Solaris: /opt/CA/SharedComponents/iTechnology
3. Open the policydb.conf file with a text editor.
4. Locate the <iSponsor> and </iSponsor> tags and add the following line of code somewhere between the tag pair:

   <SegregationOfDuty>Transactional</SegregationOfDuty>

   Note: If this tag is not present, segregation of duty defaults to the strict version when you turn the option On. Removing the tag will restore strict segregation of duty.
5. Save the file and exit.
6. Restart the iGateway daemon or service.

   The change to transactional segregation of duty takes effect after the iGateway restart.

More information

Set Access Management (see page 24)
Access Management (see page 22)

Set Access Management

You can enforce change control for policy and MP file distribution by enabling or disabling Segregation of Duty mode. Segregation of Duty lets you control whether a single user can assume both Maker and Checker roles for the same policy or MP file.

- If Segregation of Duty is off, the same user may create as well as distribute a policy or MP file, assuming that user has both Maker and Checker roles. This is the default setting.
- If Segregation of Duty is on, a Maker and a Checker are necessary for creation and distribution of a policy or MP file. Maker and Checker roles may be assigned to the same user, but a user with both roles is restricted from acting as a Checker for a policy or MP file for which he or she was the Maker. The level of restriction depends on whether Strict or Transactional checking is enabled in your environment.

To change the Segregation of Duty state

1. Click Access Management.

   The Segregation of Duty pane appears, displaying the current segregation state.

2. Click Turn OFF or Turn ON to the toggle the state.

   A confirmation message appears.

3. Click Close to return to the configuration options pane.

   The Segregation of Duty state is changed.

More information

Access Management (see page 22)
Enable Transactional Segregation of Duty (see page 23)

User Source Management

You can configure the Audit Administrator's eIAM server to store user information internally in the CA Management Database (CA-MDB) or externally in a supported LDAP directory.

Note: If you choose the CA-MDB, you can change global user and group information and set password policies. If you choose an external directory, the global users and groups are read-only, and you can only change role assignments for access to Audit Administrator.

To reference users from an external directory

1. Click User Source Management.
2. Select Reference from an external directory.

   The external directory configuration fields appear.
3. Select the directory type you want, enter the Host Name, Port, and other required values, and click Save.

   An update confirmation message appears.
4. Click Close to return to the configuration options screen.

More information

User Management Tasks (see page 17)

Configuring Data Sources

You can configure eTrust Audit Data Sources for use by the Reporter and Viewer utilities. The Data Sources pane displays current source information. You can add a new data source, or edit or delete an existing one. You can also test a selected data source's connection.

Create a Data Source

You can create a new Reporter/Viewer data source.

To create a data source

1. Click Reporter/Viewer

   The Data Sources Configuration pane appears.

2. Click Add New DSN.

   The Create New Data Source pane appears.

3. Enter the required information and click Create.

   The new data source appears in the Data Sources pane.

   Note: You can use the Test button to test the data source's connection.

Policy Manager Configuration

You can perform Policy Manager administration tasks, configuring the Distribution Server and managing locked Policy Manager objects.

More information

Distribution Server (see page 27)
Unlock Objects (see page 29)

Distribution Server

You can configure the Policy Manager Distribution Server, controlling how it distributes approved policies and MP files to eTrust Audit clients. To do so, you must be logged in to Audit Administrator as a user with the Admin role.

You can set the following server attributes:

Node Polling Frequency

Defines the interval, in hours, minutes, and seconds, at which the server contacts event source nodes to check for policy and MP file consistency.

Default: 24 hours

Limits: Minimum 1 hour

Retry Delay

Defines the interval, in hours, minutes, and seconds, between automatic distribution retries.

Note: The Distribution Server retries failed policy distribution attempts only after all nodes have been contacted or attempted to be contacted.

Default: 30 minutes

Limits: Minimum 5 minutes

Max Retry

Defines the maximum number of redistribution attempts after a failed policy or MP file distribution.

When the Policy Manager reaches the Max Retry value for a node, it does the following:

- Stops attempts to redistribute policies or MP files to the node
- Generates an error log
- Marks the node as having exceeded Max Retry

The Checker can redistribute the same policy or MP files to available nodes that are marked as having exceeded Max Retry.

Default: 3

Max number of concurrent distribution threads

Defines the number of communication threads your distribution server uses for parallel distribution of policies and MP files.

Default: 10

Limits: 1-64

Automatically re-push Policies or MP files to tampered nodes

Defines whether the Distribution Server automatically redistributes policies or MP files to tampered nodes. A tampered node is an event source where the distribution server detects inconsistencies between the deployed policy or MP file and the parent version.

Default: Off

Note: Enforcing that only authorized MP files are in use means that you must distribute all of the required files in the same MP folder. Files present on the system but not contained in the distributed folder are deleted. For example, if your UNIX MP folder contains only the syslog.mp file, an sulog.mp file present on the system appears to be an unauthorized version. With this feature set to On, the sulog.mp file is deleted.

Active Polling

Defines whether the Distribution Server contacts event sources to check for policy and MP file consistency. The Node Polling Frequency value defines the polling rate.

Default: Off

Unlock Objects

You can unlock Policy Manager objects that have become inaccessible to users with the Maker or Checker roles.

To unlock a Policy Manager object:

1. Click Unlock Objects.

   The Unlock Policy Manager Objects pane appears, displaying a list of locked objects.

2. Select the object you want to unlock, and click Unlock.

   The object is unlocked and a confirmation message appears.
   Note: You can select and unlock multiple objects.

Chapter 2: Using iRecorder Manager

You can view a list of hosts running one or more iRecorders in the iRecorder Browser list. Select a host from the list to display the iRecorders running on the selected host and perform the following tasks:

- Start, stop, or test the selected iRecorder.
- Modify the selected iRecorder's configuration.
- View a field mapping table for the selected iRecorder.

Note: If no hosts are displayed, check the status of your discovery job on the Configuration tab, or type the host name in the Discovery Host field, and click Go.

You must be logged in to Audit Administrator as a user with the Admin role to access the iRecorder Manager.

This section contains the following topics:

iRecorder Status

You can view general statistical information for the selected iRecorder in the Status tab, which displays the View Statistics area by default. This area shows the start time, number of events sent, start/stop state, and average events per second for the selected iRecorder.

You can login to the iRecorder's host to start, stop, and test the iRecorder. To make sure the iRecorder is running, you can send a test event.

More information

Start or Stop an iRecorder (see page 32)
Test an iRecorder (see page 33)

Start or Stop an iRecorder

You can start or stop an iRecorder.

To start an iRecorder

1. Select the iRecorder you want from the iRecorder Browser list.

   The iRecorder details pane appears, displaying the Status tab.

2. Click the Login link beside the host name at the top of the iRecorder details pane.

   The host login screen appears.

3. Enter the appropriate Administrative user name and password.

   The iRecorder details pane reappears.

4. Click Start iRecorder.

   The iRecorder is started. The Status tab displays State: Running.

To stop an iRecorder

1. Select the iRecorder you want from the iRecorder Browser list.

   The iRecorder details pane appears, displaying the Status tab.

2. Click the Login link beside the host name at the top of the iRecorder details pane.

   The host login screen appears.

3. Enter the appropriate Administrative user name and password.

   The iRecorder details pane reappears.

4. Click Stop iRecorder.

   The iRecorder is stopped. The Status tab displays State: Stopped.

Note: The value, 1.#INF00, may display in the Average Events/second field when you restart an iRecorder. This indicates that the iRecorder has not run long enough (more than one second) to calculate any number of events per second before it was restarted.

More information

Test an iRecorder (see page 33)
Using iRecorder Manager (see page 31)

Test an iRecorder

You can test an iRecorder to ensure that it is running.

To send test events to an iRecorder

1. Select the iRecorder you want from the iRecorder Browser list.

   The iRecorder details pane appears, displaying the Status tab.

2. Click the Login link beside the host name at the top of the iRecorder details pane.

   The host login screen appears.

3. Enter the appropriate Administrative user name and password.

   The iRecorder details pane reappears.

4. Click Test iRecorder.

   The iRecorder generates an event with the logname eTrust Audit.

More information

Start or Stop an iRecorder (see page 32)
Using iRecorder Manager (see page 31)

iRecorder Configuration

You can view and modify the configuration of the selected iRecorder from the iRecorder Configuration tab. All of the configurable parameters for your chosen iRecorder type are displayed, along with their default values.

You can also view the configuration file for the chosen iRecorder.

More Information

Edit iRecorder Configuration File (see page 34)
View iRecorder Configuration File (see page 35)

Edit iRecorder Configuration File

You can edit the iRecorder configuration.

To edit the iRecorder configuration file

1. Select the iRecorder you want from the iRecorder Browser list.

   The iRecorder details pane appears, displaying the Status tab.

2. Click the Login link beside the host name at the top of the iRecorder details pane.

   The host log in screen appears.

3. Enter the appropriate Administrative user name and password.

   The iRecorder details pane reappears.

4. Click the Configuration tab.

   The Edit Configuration tab appears.

5. Enter your new parameter values.

   Note: Click Reset to restore the default values identified in the Description column.

6. Click Save.

   A confirmation dialog appears.

7. Click OK.

   The new configuration values are saved.

After you save your changes, you can view the XML configuration file. The file displays in the Configuration tab.

More information

View iRecorder Configuration File (see page 35)
Using iRecorder Manager (see page 31)

View iRecorder Configuration File

You can view a read-only version of the iRecorder configuration file.

To view the iRecorder configuration file

1. Select the iRecorder you want from the iRecorder Browser list.

   The iRecorder details pane appears, displaying the Status tab.

2. Click the Configuration tab.

   The Edit Configuration pane appears.

3. Click View Configuration File.

   The XML Configuration File appears.

4. Click the Close icon.

   The Edit Configuration pane reappears.

More information

Edit iRecorder Configuration File (see page 34)
Using iRecorder Manager (see page 31)

iRecorder Data Model

You can view a field mapping table containing the log name, audit and native field names, field type and description of the selected iRecorder. You can sort the Data Model view by clicking any column title.

For a larger view of the Data Model table, click the New Window icon in the upper right corner of the pane, displaying the table in a separate browser window.

More information

iRecorder Status (see page 31)
iRecorder Configuration (see page 33)
Using iRecorder Manager (see page 31)

Chapter 3: Policy Manager Tasks

Policy Manager lets you create, manage, and distribute policies and Message Parsing (MP) files. It contains the folders, policies, rules, subrules, and MP files currently defined in the Policy Manager database.

Predefined Policy Manager roles include Maker and Checker. These roles divide responsibility for the creation of policies, rules and MP files from responsibility for their review and distribution to the eTrust Audit clients. The Maker role is able to create new policies and the Checker role to reject or approve them for distribution.

The Maker and Checker roles can be assumed by different users, or the same user, depending on your segregation of duty setting. You must be logged in to Audit Administrator as a user with the Maker or Checker role to access the Policy Manager.

Note: Before users can access the Policy Manager, you must log in as the EIAM Admin user and create users (see page 17) or import external users (see page 25).

This section contains the following topics:

Policy Manager Folders and Objects

Policy Manager uses folders to organize and store policies and message parsing (MP) files. Policies or MP files must be in a folder to be created, submitted for approval, and distributed to the Audit clients. The first step in creating policies and MP files for your environment is creating folders.

Policy Manager objects are the policies, rules, subrules and MP files contained in the folders, and nodes and node groups attached to them.

More information

Folder Statuses (see page 38)

Folder Statuses

Every policy or MP folder in your Audit Administrator environment has a status, which indicates its stage in the creation or activation process. Folder statuses support change control by limiting the actions that can be taken to affect a folder or its policies or MP files, and which user roles may perform the allowed actions.

A folder's current status appears in the folder Details pane. During its creation and activation, a folder will typically pass through many of the following possible statuses:

Inactive

Indicates that the folder has no audit node (AN) groups attached. The Maker may add, edit or delete policies, rules and MP files at this stage. A newly-created folder has this status.

Attached

Indicates that the folder has one more AN groups attached. The Maker may add, edit or delete policies, rules and MP files at this stage, as well as attach or detach AN groups. A Maker may also submit Attached folders for approval by the Checker.

Locked

Indicates that the Maker submitted the folder for approval and is waiting for the Checker's review. The Maker can recall a locked folder before the Checker reviews it. The folder cannot be otherwise be affected, and retains this status until the Checker approves or rejects it.

Activated

Indicates that the Checker has approved the folder and is awaiting distribution to the eTrust Audit clients. The folder cannot be changed until it is distributed.

Rejected

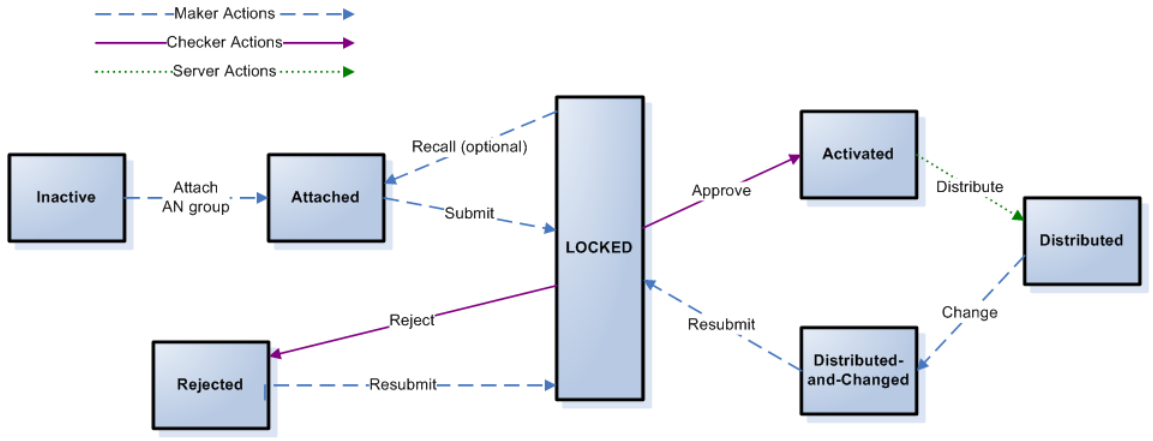
Indicates that the Checker has rejected the folder. The Maker may add, edit or delete policies, rules and MP files at this stage, as well as attach or detach AN groups. The Maker can also resubmit Rejected folders for approval by the Checker.

Distributed

Indicates that the distribution server has deployed the folder and its policies or MP files to the client computers. The Maker may add, edit or delete policies, rules and MP files at this stage, as well as attach or detach AN groups. A Checker can also marked a distributed folder for deletion.

Distributed-and-Changed

Indicates that the Maker has changed a distributed folder or its contents. The Maker must resubmit a distributed-and-changed folder to the Checker for approval in order to return it to distributed status.



How Basic Maker Work Flows Progress

If you have the Maker role, you can create and submit policies and MP files to a Checker for review and distribution. You can also edit distributed policies, or mark them for deletion, and submit those changes for review.

Users with the Maker role have the following basic work flows:

1. Creating Audit Nodes and Groups (see page 44)
2. Creating and Submitting a Policy (see page 42)
3. Creating and Submitting an MP File (see page 43)

Each of these work flows contain additional procedures you follow to complete the steps shown here. For a detailed discussion of how a Maker and Checker interact with policies, see Working with Versions.

Access Management

Segregation of Duty lets you control whether a single user can assume both Maker and Checker roles for the same policy or MP file. Two levels of segregation of duty checking are available, strict and transactional. By default, when you turn on the feature, eTrust Audit uses the strict level.

Transactional segregation of duty allows smaller organizations to take advantage of segregation of duty without requiring as much staff.

At either level, no single person is allowed to be both Maker and Checker for the same production change or file.

- Strict segregation of duty does not allow any user with the Maker role to also be a Checker for any file or part of a file, that contains changes made or submitted by that Maker.
- Transactional segregation of duty allows the same person to be both Maker and Checker on a file or folder, provided that the person performing the Checker role was not the person who made the most recent change.

Stated another way, in transactional segregation of duty, the Maker of a policy or MP file can be a Checker in the future for an update to that same policy or MP file, and a Checker for a policy or MP file can be a Maker for an update to that same policy or MP file in the future.

More information

Enable Transactional Segregation of Duty (see page 23)
Set Access Management (see page 24)

Set Access Management

You can enforce change control for policy and MP file distribution by enabling or disabling Segregation of Duty mode. Segregation of Duty lets you control whether a single user can assume both Maker and Checker roles for the same policy or MP file.

- If Segregation of Duty is off, the same user may create as well as distribute a policy or MP file, assuming that user has both Maker and Checker roles. This is the default setting.
- If Segregation of Duty is on, a Maker and a Checker are necessary for creation and distribution of a policy or MP file. Maker and Checker roles may be assigned to the same user, but a user with both roles is restricted from acting as a Checker for a policy or MP file for which he or she was the Maker. The level of restriction depends on whether Strict or Transactional checking is enabled in your environment.

To change the Segregation of Duty state

1. Click Access Management.

   The Segregation of Duty pane appears, displaying the current segregation state.

2. Click Turn OFF or Turn ON to the toggle the state.

   A confirmation message appears.

3. Click Close to return to the configuration options pane.

   The Segregation of Duty state is changed.

More information

Access Management (see page 22)
Enable Transactional Segregation of Duty (see page 23)

How to Create and Submit a Policy

A policy includes several basic objects, and must reside in a policy folder. You can add multiple policies to a policy folder. Each policy can have multiple rules, and each rule can have one or more actions. eTrust Audit contains a basic Rule Library, and also provides a Rule Wizard to create your own custom rules.

To create a basic policy and submit it for review and distribution, you must complete the following steps:

1. Create a Policy Folder (see page 48)
2. Create a Policy (see page 51)
3. Create a Policy Rule (see page 53)
4. Add Actions to a Rule (see page 55)
5. Check a Policy Folder (see page 60)

   This step is optional, but provided so that you can check your syntax for errors prior to committing the policy.
6. Attach a Policy Folder to an Audit Node Group (see page 58)

After you have created your policy and its subordinate objects, you take the following actions in order:

1. Commit the Policy (see page 59)

   The Commit function compiles the policy, checking syntax as it goes.
2. Select the policy for activation (see page 60).

   Though the Maker action link is labeled Activate, the true activation processing occurs after the Checker approves the policy.
3. Submit the Policy Folder (see page 61)
4. Recall the Policy Folder (see page 62)

   You can take this optional step to perform additional work as needed. You can only recall a folder before review by the Checker. Recall is the only action a Maker can take on a policy folder after it is in Locked status.

How to Create and Submit an MP File

Message parsing (MP files) contain instructions for eTrust Audit Client and iRecorders on how to interpret text-format event data as events occur. MP files work with policies to capture specific event data for handling in the SIM system, and must reside in an MP folder.

To create and submit an MP file, you must complete the following steps:

1. Create an MP Folder (see page 68)
2. Add an MP File (see page 70)
3. Check an MP Folder (see page 75)

   This step is optional, but provided so that you can check your syntax for errors.
4. Attach an MP Folder to an Audit Node Group (see page 73)

   The Audit Node group type must be set to MP file for this work flow.

After you have created your MP folder and file, you take the following actions in order:

1. Commit the MP File (see page 74)
2. Select the MP File for activation (see page 75)
3. Submit the MP Folder (see page 77)
4. Recall the MP Folder (see page 62)

   You can take this optional step to perform additional work as needed. You can only recall a folder before review by the Checker. Recall is the only action a Maker can take on an MP folder after it is in Locked status.

How to Create Audit Nodes and Groups

Audit nodes (ANs) and audit node groups are at the most basic level of your SIM system. You must have at least one policy distributed to one or more ANs to capture events. To submit policies and MP files for review and distribution, you must attach an AN group to the appropriate folder, allowing eTrust Audit to apply the policies or MP files to the nodes in that group.

To create and populate an AN group, you must complete the following procedures:

1. Create an Audit Node (AN) Group (see page 83) to contain one or more audit nodes.

   The group type is important, as you must select whether the group is for policies or MP files.

2. Create an Audit Node (see page 86) manually, or by using one of the other methods available:

   During its installation, the eTrust Audit Client automatically registers with the Policy Manager. Registration creates an entry in the Policy Manager database for both the host and an audit node. Using these pre-defined entries, you can use the second method to create ANs with the Add an Existing Audit Node (see page 88) procedure.

   You can use the third method, Create Multiple Audit Nodes (see page 87), to discover and add nodes using search criteria you specify.

How Advanced Maker Work Flows Progress

If you have the Maker role, you can make changes that affect distributed policy or MP folders, or audit nodes attached to distributed folders. Making a change to the objects contained in a distributed folder (see page 38) creates a new version of those objects. When you change a distributed folder, you must resubmit it for approval by the Checker before the changes become effective.

Users with the Maker role have the following advanced work flow areas:

- Audit Node-related changes (see page 45)
- Policy-related changes (see page 45)
- MP file-related changes (see page 46)

Each of these work flow areas contains procedures you follow to complete specific tasks.

How to Change Attached Audit Nodes

You can make the following changes to the AN groups or audit nodes attached to distributed policy or MP folders:

- Create audit node types (see page 92)
- Edit audit node types (see page 93)
- Delete audit node types (see page 93)
- Edit node group definitions (see page 84)
- Add nodes to an AN group (see page 88)
- Remove nodes from an AN group (see page 89)
- Deactivate or activate a node (see page 89)
- Disable or enable a node (see page 88)

How to Change Distributed Policies

You can make the following changes to distributed policies or policy folders:

- Add a policy (see page 51) to the folder
- Remove a policy (see page 64) from the folder
- Deactivate or reactivate a policy (see page 63)
- Edit rule actions (see page 56)
- Delete a rule (see page 57)
- Revert to a different policy version (see page 64)
- Delete a policy folder (see page 50)

How to Change Distributed MP Files

You can make the following changes to distributed MP files or folders:

- Add an MP file (see page 70) to the folder
- Edit an MP file (see page 71)
- Remove an MP file (see page 78) from the folder
- Deactivate or reactivate a distributed MP file (see page 76)
- Revert to a different MP file version (see page 78)
- Delete a distributed MP folder (see page 70)

Note: Making changes to distributed MP files may have unintended effects when certain distribution server features are in use. For more information, read the description of the Distribution Server (see page 27) feature, Automatically re-push Policies or MP files to tampered nodes.

How Checker Work Flows Progress

If you have the Checker role, you can review and approve or reject policy and MP folders submitted by a Maker. Any time a new folder is submitted, or a changed folder is resubmitted, the Checker approves it to allow distribution to the clients, or rejects it, returning it to the Maker.

Any change to a folder which affects its status (see page 38) requires the Maker to submit it to the Checker for review. This includes changes to the folder's attached AN groups, such as addition or deletion of audit nodes. The Checker then approves or rejects the changed folder.

For example, a Maker who wants to delete a submitted folder marks the folder for deletion and submits it to the Checker, who then uses approve to complete the deletion, or reject to return the folder undeleted.

Users with the Checker role have the following policy work flow:

- Approve a Policy Folder (see page 66)
- Reject a Policy Folder (see page 66)
- Reject a Policy (see page 67)

When a Checker approves a policy folder, the Policy Manager Distribution Server settings determine when the policies are distributed to the Audit Nodes. Maker and Checker users can review the activation log to check on a policy's activation status.

Users with the Checker role have the following MP file work flow:

- Approve an MP Folder (see page 80)
- Reject an MP Folder (see page 80)
- Reject an MP File (see page 81)

Policies

You can perform most Maker and Checker tasks (see page 37) from the Policies pane. This pane shows your policy folders and committed policy folders created by other Makers in a tree structure, displaying a detailed view when you expand a folder. When you select a folder, policy, or rule, it opens in the Details pane.

From the Policies pane, you can create, modify, or delete any of the following:

- Policy folders
- Policies
- Rules
- Audit Node (AN) groups
- Audit Nodes

You can use only alphanumeric characters, spaces, underscores, plus or minus signs, and apostrophes for the policy folder, policy, and rule names.

More information

Create a Policy Folder (see page 48)
Create a Policy (see page 51)
Create a Policy Rule (see page 53)
Add Actions to a Rule (see page 55)
Submit a Policy Folder (see page 61)

Create a Policy Folder

You must create folders to contain your policies. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To create a policy folder

1. Click New Folder in the Policies pane.

   The Folder Details pane appears.

2. Enter the Folder Name and Description, and click OK.

   The new folder appears in the Details pane.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Edit a Policy Folder

You can edit an existing policy folder. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To edit a policy folder

1. Select the folder you want to edit.

   The selected folder appears in the Details pane.

2. Click Edit.

   The Edit Policy Folder pane appears.

3. Enter your changes to the folder Name and Description, and click Save.

   The edited folder appears in the Details pane.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Delete a Policy Folder

You can delete an active or attached (see page 38) policy folder before it has been submitted for approval. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To delete a Policy Folder

1. Select the folder you want to delete.

   The selected folder appears in the Details pane.

2. Click Delete.

   A confirmation message appears.

3. Click OK.

   The deleted folder is removed from the folder display.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Delete a Distributed Policy Folder

You can mark a distributed (see page 38) policy folder for deletion, submitting it to the Checker's queue for final deletion. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

This is the only way you can delete a folder that contains a distributed policy.

To mark a policy folder for deletion

1. Select the folder you want to delete.

   The selected folder appears in the Details pane.

2. Select the policy or policies you wish to delete, and click Submit.

   The folder is removed from the list of available folders.

   Note: You may delete another Maker's distributed folder.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Create a Policy

You can create a new policy to control your eTrust Audit clients. Create a policy by choosing its Audit Node (AN) type, or by copying an existing policy. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To create a new policy by AN type

1. Select the folder in which you want to create the new policy.
2. Click Create Policy in the Details pane.

   The New Policy pane appears.
3. Click Create a new policy based on AN Type.
4. Enter Name and Description, and select the AN type you want.
5. Click Save.

   The new policy appears in the Details pane, listing any rules the policy contains.

To create a new policy from an existing policy

1. Select the folder in which you want to create the new policy.
2. Click Create Policy in the Details pane.

   The New Policy pane appears.
3. Click Create a policy from an existing policy.
4. Select the policy you want to copy from the Use an Existing Policy display.

   Note: You can select Save actions to retain the original policy's actions for your new policy.
5. Click Save.

   The new policy appears in the Details pane, listing any rules the policy contains.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Check a Policy

After creating a custom policy or modifying an existing policy, you can check for syntax errors in the policy language. This allows you to make any necessary changes before you commit the policy.

To check a policy

1. Select the policy you want to check

   The selected policy appears in the Details pane.

2. Click Check at the top of the Policy Details pane.

   The Folder Compilation Results pane appears, displaying details.

3. Click OK.

   The Details pane reappears, displaying the policy you checked.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Delete a Policy

You can delete a policy from active or attached (see page 38) policy folder before it is submitted for approval. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To delete a policy

1. Access the policy you want to delete by expanding its folder and choosing the appropriate policy

   The selected policy appears in the Details pane.

2. Click Delete.

   A confirmation dialog appears.

3. Click OK.

   The deleted policy is removed from the folder display, and a confirmation message appears in the Details pane.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Create a Policy Rule

You must create rules for your policies. Creating rules is an important configuration task because the default rule under which eTrust Audit operates is to ignore all events. If you do not specify a rule for handling a given event type, eTrust Audit takes no action. You must specify rules for all event types that you want to monitor.

To create rules, you must be logged in to Audit Administrator as a user with the Maker role.

You can create rules in the following ways:

- Copying a rule from an existing policy
- Using a rule template from the pre-installed library
- Using the Rule Builder to create a custom rule

To create a rule from an existing policy

1. Select the policy to which you want to add a rule.
2. Click Create Rule in the Rules area of the Policy pane.

   The Create a Rule pane appears.
3. Click Copy a rule from existing policies.

   The Copy a Rule from the Policy Library screen appears, displaying the available policies and rules in the Browse Rules pane.
4. Select the rule you want to copy, and click Copy.

   The new rule appears in the Rules area of the Policy pane. You may now add actions to the rule.

   Note: A rule copied from an existing rule does not contain its actions. You must add actions to the copy of the rule to handle the events.

To create a rule using the Rule Template Library

1. Select the policy to which you want to add a rule.
2. Click Create Rule in the Rules area of the Policy pane.

   The Create a Rule pane appears.
3. Click Use the Rule Template Library.

   The Rule Template Wizard appears.
4. Complete the wizard, and click Finish.

   The new rule appears in the Rules area of the Policy pane. You may now add actions to the rule.

To create a rule using the Rule Builder

1. Select the policy to which you want to add a rule.
2. Click Create Rule in the Rules area of the Policy pane.

   The Create a Rule pane appears.
3. Click Use the Rule Builder in the Create a Rule screen.

   The Rule Builder Wizard appears.
4. Complete the wizard, and click Finish.
5. Expand your chosen folder to confirm creation of the new rule. It should appear in the policy's rule list.

   Creation of the rule is complete. You may now add actions to the rule.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Add Actions to a Rule

You can add actions to a newly-created or previously existing rule. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To add an action to a rule

1. Select the rule to which you want to add an action.
2. Click Edit in the Details pane.

   The Edit a Rule wizard opens.
3. Complete the wizard, and click Finish.

   The edited rule appears in the Rules area list of selectable rules.
4. Select the rule and click Apply.

   The applied rule appears in the rules pane. You may now commit the policy to which the rule belongs.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Edit a Policy Rule

You can edit an existing policy rule's attributes, including:

- Name
- Description
- Rules script
- Actions

To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To edit a rule

1. Access the rule you want to edit by expanding its folder in the Policies pane and choosing the appropriate policy.

   The policy appears in the Details pane, displaying its rules.

2. Click the rule you want to edit.

   The rule appears, with its actions displayed, in the Details pane.

3. Click Edit.

   The Edit Rule wizard appears.

4. Complete the wizard, and click Finish.

   The edited rule appears in the Details pane.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Delete a Policy Rule

You can mark an active policy rule for deletion by the Checker. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To delete a policy rule

1. Access the rule you want by expanding its folder in the Policies pane and choosing the appropriate policy.

   The policy appears in the Details pane, displaying its rules.

2. Click the rule you want to mark for deletion.

   The rule appears, with its actions displayed, in the Rule pane.

3. Click Delete.

   A confirmation dialog appears.

4. Click OK.

   A message appears, confirming that the rule is marked for deletion.

   When the folder containing this rule is resubmitted, the Checker can approve the deletion, which makes the rule inactive. A Maker user can still access the rule, if necessary, using Manage Versions (see page 64).

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Attach a Policy Folder to an Audit Node Group

You can attach a policy folder to an Audit Node (AN) group, allowing eTrust Audit to apply the policies in the folder to the event sources in the chosen node group. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To attach a folder to an AN group

1. Select the folder you want to attach to an AN group.
2. Click the Attach/Detach button in the AN Groups and Nodes pane.

   A list of the available AN groups appears.
3. Click the Attach link for the AN Group you want, or click Create AN Group to create and attach a new AN group.

   Note: If you use the Create AN Group button, you must still attach nodes (see page 83) to the new AN group.

   A confirmation message appears, and the name of your policy folder appears in the Associated Policy Folder column.
4. Click Close to return to the Policy Folder pane.

   The new AN group appears in the AN Groups and Nodes area.

If the folder is distributed (see page 38), you may attach a group to it without approval. You must then submit the folder to the Checker to approve the attachment, and to distribute the policy to the nodes in the newly attached group upon approval.

Note: If you add a group to a distributed folder, the original configuration is not retained and no new version of the policies in the folder is created.

Detach a Policy Folder from an Audit Node Group

You can detach a policy folder from an Audit Node (AN) group. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To detach a folder from an AN group

1. Select the folder you want to detach from an AN group.
2. Click the Attach/Detach button in the AN Groups and Nodes pane.

   A list of the available AN groups appears.
3. Click the Detach link for the AN Group you want to detach.

   A confirmation message appears, and the Detach link for the policy folder changes to an Attach link.
4. Click Close to return to the Policy Folder pane.

   If the folder is distributed (see page 38), you may now submit the folder to the Checker to approve the detachment.

More information

Audit Nodes (see page 82)
Policies (see page 48)
Policy Manager Tasks (see page 37)

Commit a Policy

After you have finished creating a policy you can commit it, making it available for submission. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To commit a policy

1. Select the policy you want to commit.

   Selectable rules for the policy are displayed in the Details pane.

   Note: Your policy must contain selectable rules to be committed.
2. Select the rules you want and click Commit.
3. Enter an annotation and click OK.

   A confirmation message appears.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Select a Policy for Activation

Before you submit a policy folder, you can activate the individual policies in the folder. A folder must have at least one active policy in order to be submitted. You must be logged in to Audit Administrator as a user with the Maker role to activate a policy.

To select a policy for activation

1. Select the folder that contains the policy you want to activate.

   The folder appears in the Details pane, displaying its policies.

2. Select the policy you want to activate, and click the Activate link.

   The policy is selected for activation, and a confirmation message appears. You may now submit the policy folder to a Checker.

   Note: You can select multiple policies for activation.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Check a Policy Folder

Before you submit a folder for approval and distribution, you can test for syntax errors in all the policies contained in the folder.

To check a policy folder

1. Select the folder you want to check

   The selected folder appears in the Details pane.

2. Click Check at the top of the Details pane.

   The Folder Compilation Results pane appears, displaying details.

3. Click OK.

   The Details pane reappears displaying the folder you checked .

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Submit a Policy Folder

After you have created a folder, added or created policies and attached it to an Audit Node group, you can submit the completed folder. Submitting the folder makes it visible to the Checker, who is responsible for reviewing and approving the folder before the Distribution Server deploys it to the appropriate eTrust Audit clients.

You must be logged in to Audit Administrator as a user with the Maker role to submit a policy folder.

To submit a folder

1. Select the folder you want to submit

   The folder appears in the Details pane.

2. Select the policies you want to submit in the Policies pane.

3. Click Submit.

   The Annotation dialog appears.

4. Enter an annotation, and click OK.

   A confirmation message appears. The submitted folder appears in the Details pane, displaying a status of Locked (see page 38).

   Note: You can use the Recall button if a submitted policy folder requires additional changes. This is the only Maker action that affects a Locked folder.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Recall a Folder

You can recall a folder you have submitted, to make changes or additions before it is reviewed. This is the only Maker action that can affect a locked (see page 38) folder. You can only recall a folder before the Checker approves or rejects it.

To recall a folder

1. Select the submitted folder you want to recall.

   The folder appears in the Details window.

2. Click Recall.

   An annotation dialog opens.

3. Enter an annotation describing the reason for the recall, and click OK.

   The recalled folder appears in the details window displaying a confirmation message.

More information

Policies (see page 48)
MP Files (see page 68)
Policy Manager Tasks (see page 37)

Deactivate or Reactivate a Distributed Policy

You can change a distributed (see page 38) policy folder by deactivating or reactivating its policies. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To deactivate or activate policies

1. Select the distributed folder you want to modify.

   The folder appears in the Details pane, displaying its current status.

2. Select the policy you want in the Policies pane, and click one of the following:

   Activate

   Marks the policy for activation so it can be distributed to the eTrust Audit clients, or redistributed if it was previously deactivated.

   Deactivate

   Marks the policy for deactivation. When deactivated, the policy is removed from the eTrust Audit clients to which it has been distributed.

   Undo

   Returns the policy to its current status, removing the change marking.

   A confirmation message appears.

   Note: You can select multiple policies for activation or deactivation.

3. When you have completed the policy changes you want, click Submit.

   The modified folder is resubmitted to the Checker for approval.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Delete a Distributed Policy

You can change a distributed (see page 38) policy folder by deleting its policies. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To delete a distributed policy

1. Select the distributed folder you want to modify.

   The folder appears in the Details pane, displaying its current status.

2. Select the policy you want in the Policies pane, and click Delete.

   A confirmation dialog appears.

3. Click OK.

   A confirmation message appears. The policy is marked for deletion.

   Note: You can select multiple policies for deletion.

4. When you have completed the policy changes you want, click Submit.

   The modified folder is resubmitted to the Checker for approval.

   Note: You can use the Undo link to remove the deletion marking.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Revert to a Different Policy Version

You can revert to a different version of any policy in a distributed folder (see page 38). To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To revert to a different policy version

1. Select the policy with whose versions you want to work.

   The policy appears in the Policy Details pane, displaying its name and current version.

2. Click Manage Versions.

   The Policy Version Management pane appears.

3. Select the version you want to revert to, and click Save.

   The selected version appears in the Policy Details pane along with a confirmation message. You may now submit the policy folder for approval by the Checker.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Compare Policy Versions

You can compare any two versions of a policy in a distributed folder (see page 38). To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To compare policy versions

1. Select the policy with whose versions you want to work.

   The policy appears in the Policy Details pane, displaying its name and current version.

2. Click Manage Versions.

   The Policy Version Management pane appears.

3. Select any two policy versions and click Compare.

   The Compare Versions pane appears, displaying a change summary and the policy code, highlighted to show changes.

4. Click Close.

   The Policy Version Management pane reappears.

More information

Policies (see page 48)
Policy Manager Tasks (see page 37)

Approve a Policy Folder

You can review a policy folder submitted by a user with the Maker role and approve it for distribution, or to confirm changes made by the Maker. Approval transfers the folder to the Distribution server's queue for deployment to the eTrust Audit clients. You must be logged in to Audit Administrator as a user with the Checker role to approve a policy folder.

To approve a policy folder

1. Select the folder that contains the policy you want to approve.

   The Policy Folder pane appears.

2. Click Approve.

   A confirmation message appears.

3. Click OK.

   The approved folder appears in the Policy Folder pane.

More information

How Checker Work Flows Progress (see page 47)
Policies (see page 48)
Policy Manager Tasks (see page 37)

Reject a Policy Folder

You can review a policy folder submitted by a Maker and reject it if modifications are required or any changes are not permissible. Rejection returns the entire folder and its policies to the Maker's display for updates and resubmission. You can also reject a single policy (see page 67) in a folder.

You must be logged in to Audit Administrator as a user with the Checker role to reject a policy folder.

To reject a policy folder

1. Select the folder that you want to reject.

   The Policy Folder pane appears

2. Click Reject.

   An annotation dialog appears.

3. Enter an annotation describing the reason why the folder is being rejected, and click OK.

   The rejected folder is removed from the list of available folders displayed in the Policies pane. The Maker may now make appropriate changes to the policies in the folder and resubmit it.

More information

How Checker Work Flows Progress (see page 47)
Policies (see page 48)
Policy Manager Tasks (see page 37)

Reject a Policy

You can review a policy submitted by a Maker and reject it if modifications are required or any changes are not permissible. Rejecting by policy differs from rejection by folder (see page 66) by marking the individual policy as rejected rather than the entire folder, making it easier for the Maker to determine where additional work is required.

You must be logged in to Audit Administrator as a user with the Checker role to reject a policy.

To reject a policy

1. Select the folder that contains the policy you want to reject.

   The Policy Folder pane appears

2. Click the policy you want to reject in the Policies area.

   The Policy Details pane appears.

3. Click Reject.

   An annotation dialog appears, titled with the name of the policy you are rejecting.

4. Enter an annotation describing the reason why the policy is being rejected, and click OK.

   The rejected policy and its parent folder are removed from the list of available folders displayed in the Policies pane. The Maker may now make appropriate changes to the policy and resubmit its folder.

More information

How Checker Work Flows Progress (see page 47)
Policies (see page 48)
Policy Manager Tasks (see page 37)

MP Files

eTrust Audit uses message parsing (MP) files to read text-format log event data.

You can perform Maker and Checker tasks (see page 37) related to MP files from the MP Files pane, which shows your message parsing (MP) folders. The panel also shows committed MP folders created by other Makers in a tree structure, displaying a detailed view when you expand a folder. When you select an MP file it opens in the Details pane, showing the MP files in the selected folder, the AN Groups to which the folder is attached, and any folder annotations.

From MP Files, you can create, modify, or delete the following:

- MP folders
- MP files

You can use only alphanumeric characters, spaces, underscores, plus or minus signs, and apostrophes for the MP folder and file names.

More information

Create an MP Folder (see page 68)
Add an MP File (see page 70)
Attach an MP Folder to an Audit Node Group (see page 73)
Submit an MP Folder (see page 77)

Create an MP Folder

You must create folders to contain your message parsing (MP) files. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To create an MP Folder

1. Click MP Files, and click New Folder in the MP Files pane.

   The Folder Details pane appears.

2. Enter the Folder Name and Description, and click OK.

   The new folder appears in the Details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Edit an MP Folder

You can edit an existing MP folder. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To edit an MP Folder

1. Click MP Files, and select the folder you want to edit.

   The selected folder appears in the Details pane.

2. Click Edit.

   The Edit MP file pane appears.

3. Enter your changes to the folder Name and Description, and click Save.

   The edited folder appears in the Details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Delete an MP Folder

You can delete an active or attached (see page 38) MP folder before you submit it for approval. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To delete a Policy Folder

1. Select the folder you want to delete.

   The selected folder appears in the Details pane.

2. Click Delete.

   A confirmation message appears.

3. Click OK.

   The deleted folder is removed from the folder display.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Delete a Distributed MP Folder

You can mark a distributed (see page 38) MP folder for deletion, moving it to the Checker's queue for final deletion. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

This is the only way you can delete a folder that contains a working MP file.

To mark an MP folder for deletion

1. Select the folder you want to delete.

   The selected folder appears in the Details pane.

2. Select the MP files you wish to delete, and click Submit.

   The folder is removed from the list of available folders.

   Note: You may delete another Maker's distributed folder.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Add an MP File

You can add an MP file to your eTrust Audit environment in one of the following ways:

- Use Policy Manager to import a manually-created MP file
- Copy an existing MP file

You must be logged in to Audit Administrator as a user with the Maker role to add an MP file.

To add an MP file by importing

1. Click MP Files.
2. Select the folder to which you want to add a new file, and click New MP File.

   The New MP file pane appears.

3. Select Create an MP File by selecting an AN type and import the MP File.
4. Browse to locate the MP file you want, enter Name and Description, and select AN type.
5. Click Save.

   Your new MP file appears in the Details pane.

To create an MP file from an existing MP file

1. Click MP Files.
2. Select the folder to which you want to add a new file, and click New MP File.

   The New MP file pane appears.
3. Select Create an MP File from an existing MP File.

   The Use an Existing MP File pane becomes available.
4. Select the MP file you want from the list of available files displayed, and click Copy.

   Your new MP file appears in the Details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Edit an MP File

You can edit an MP File. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To edit an MP file

1. Access the MP file you want to edit by expanding its folder in the MP Files pane, and choosing the appropriate file.

   The MP file appears in the Details pane.
2. Click Edit.

   The Edit MP file pane appears.
3. Make your desired changes to the MP File Name, Description, or Contents, and click Save.

   The edited file appears in the Details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Check an MP File

After creating a custom MP file or modifying an existing MP file, you can check it for syntax errors. This allows you to test an MP file and make any necessary changes before you commit it.

To check an MP file

1. Select the MP file you want to check

   The selected MP file appears in the Details pane.

2. Click Check at the top of the MP File Details pane.

   A confirmation message appears in the Details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Delete an MP File

You can delete an MP File. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To delete an MP file

1. Access the MP file you want to delete by expanding its folder in the MP Files pane, and choosing the appropriate file.

   The MP file appears in the Details pane.

2. Click Delete.

   A confirmation dialog appears.

3. Click OK.

   The deleted file is removed from the folder display, and a confirmation message appears in the Details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Attach an MP Folder to an Audit Node Group

You can attach an MP folder to an Audit Node (AN) group, allowing eTrust Audit to apply the files in the folder to the event sources in the chosen node group. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To attach a folder to an AN group

1. Select the folder you want to attach to an AN group.
2. Click the Attach/Detach button in the AN Groups and Nodes pane.

   A list of the available AN groups appears.
3. Click the Attach link for the AN Group you want, or click Create AN Group to create and attach a new AN group.

   Note: If you use the Create AN Group button, you must still attach nodes (see page 83) to the new AN group.

   A confirmation message appears, and the name of your policy folder appears in the Associated Policy Folder column.
4. Click Close to return to the MP Folder pane.

   The new AN group appears in the AN Groups and Nodes area.

If the folder is distributed (see page 38), you may attach a group to it without approval. You must then submit the folder to the Checker to approve the attachment, and to distribute the policy to the nodes in the newly attached group upon approval.

Note: If you add a group to a distributed folder, the original configuration is not retained and no new version of the MP files in the folder is created.

Detach an MP Folder from an Audit Node Group

You can detach an MP folder from an Audit Node (AN) group. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To detach a folder from an AN group

1. Select the folder you want to detach from an AN group.
2. Click the Attach/Detach button in the AN Groups and Nodes pane.

   A list of the available AN groups appears.
3. Click the Detach link for the AN Group you want to detach.

   A confirmation message appears, and the Detach link for the policy folder changes to an Attach link.
4. Click Close to return to the MP Folder pane.

   If the folder is distributed (see page 38), you may now submit the folder to the Checker to approve the detachment.

More information

Audit Nodes (see page 82)
MP Files (see page 68)
Policy Manager Tasks (see page 37)

Commit an MP File

After you have finished creating an MP file, you can commit it, making it available for submission. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To commit an MP file

1. Click MP Files, and select the MP file you want to commit.

   The chosen MP file appears in the Details pane.
2. Click Commit.

   An annotation dialog appears.
3. Enter an annotation, and click Save.

   The committed file appears in the Details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Select an MP File for Activation

Before you submit an MP folder, you can activate the individual files in the folder. A folder must have at least one active MP file in order to be submitted. You must be logged in to Audit Administrator as a user with the Maker role to activate a file.

To activate an MP file

1. Select the folder that contains the MP file you want to activate.

   The folder appears in the Details pane, displaying its MP files.

2. Select the MP file you want to activate, and click the Activate link.

   The MP file is selected for activation, and a confirmation message appears. You may now submit the policy folder.

   Note: You can select multiple MP files for activation.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Check an MP Folder

Before you submit an MP for approval and distribution, you can check all the files contained in the folder for syntax errors.

To check an MP folder

1. Select the folder you want to check

   The selected folder appears in the Details pane.

2. Click Check at the top of the Details pane.

   A confirmation message appears in the details pane.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Deactivate or Reactivate a Distributed MP file

You can change a distributed (see page 38) MP folder by deactivating or reactivating its MP files. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To deactivate or activate MP files

1. Select the distributed folder you want to modify.

   The folder appears in the Details pane, displaying its current status.

2. Select the file you want in the MP files pane, and click one of the following:

   Activate

   Marks the file for activation so it can be distributed to the eTrust Audit clients, or redistributed if it was previously deactivated.

   Deactivate

   Marks the file for deactivation. When deactivated, the file will be removed from the eTrust Audit clients to which it has been distributed.

   Undo

   Returns the MP file to its current status, removing the change marking.

   A confirmation message appears.

   Note: You can select multiple policies for activation or deactivation.

3. When you have completed the changes you want, click Submit.

   The modified folder is resubmitted to the Checker for approval.

Note: Deactivate always removes the MP File or Policy and does *not* put anything in its place - it is a remove-only action. Replacement with the desired MP folder or policy is manual. If you want to replace the removed file with another file, you must distribute the replacement file through another version or another policy. There is no roll-back functionality.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Submit an MP Folder

After you have created a folder, added MP files, and attached it to an Audit Node group, you can submit the completed folder. Submitting the folder makes it visible to the Checker, who is responsible for reviewing and approving the folder before the Distribution Server deploys it to the appropriate eTrust Audit clients.

You must be logged in to Audit Administrator as a user with the Maker role to submit an MP folder.

To submit a folder

1. Click MP Files, and select the folder you want to submit.

   The folder appears in the Details pane

2. Select the MP files you want to submit in the MP Files pane.

3. Click Submit.

   A confirmation message appears. The submitted folder appears in the Details pane, displaying a status of Locked (see page 38).

   Note: You can use the Recall button if a submitted MP folder requires additional changes. This is the only Maker action that affects a Locked folder.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Delete a Distributed MP File

You can change a distributed (see page 38) MP folder by deleting its MP files. To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To delete a distributed MP file

1. Select the distributed folder you want to modify.

   The folder appears in the Details pane, displaying its current status.

2. Select the file you want in the MP files pane, and click Delete.

   A confirmation dialog appears.

3. Click OK.

   A confirmation message appears. The policy is marked for deletion.

   Note: You can select multiple MP files for deletion.

4. When you have completed the changes you want, click Submit.

   The modified folder is resubmitted to the Checker for approval.

   Note: You can use the Undo link to remove the deletion marking.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Revert to a Different MP File Version

You can revert to a different version of any MP file in a distributed folder (see page 38). To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To revert to a different MP file version

1. Select the MP file whose versions you want to work with.

   The file appears in the MP File Details pane, displaying its name and current version.

2. Click Manage Versions.

   The MP File Version Management pane appears.

3. Select the version you want to revert to, and click Save.

   The selected version appears in the MP File Details pane along with a confirmation message. You may now submit the MP folder for approval by the Checker.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Compare MP File Versions

You can compare any two versions of an MP file in a distributed folder (see page 38). To do so, you must be logged in to Audit Administrator as a user with the Maker role.

To compare MP file versions

1. Select the file whose versions you want to work with.

   The file appears in the MP File Details pane, displaying its name and current version.

2. Click Manage Versions.

   The MP File Version Management pane appears.

3. Select any two versions and click Compare.

   The Compare Versions pane appears, displaying a change summary and the MP file code, highlighted to show changes.

4. Click Close.

   The MP File Version Management pane reappears.

More information

MP Files (see page 68)
Policy Manager Tasks (see page 37)

Approve an MP Folder

You can review an MP folder submitted by a user with the Maker role and approve it for distribution, or to confirm changes made by the Maker. Approval transfers the folder to the Distribution server's queue for deployment to the eTrust Audit clients. You must be logged in to Audit Administrator as a user with the Checker role to approve an MP folder.

To approve an MP folder

1. Select the folder that contains the MP file you want to approve.

   The MP Files pane appears.

2. Click Approve.

   A confirmation message appears, displaying activation details.

3. Click OK.

   The approved MP folder appears in the MP Files pane.

More information

How Checker Work Flows Progress (see page 47)
MP Files (see page 68)
Policy Manager Tasks (see page 37)

Reject an MP Folder

You can review an MP folder submitted by a Maker and reject it if modifications are required or any changes are not permissible. Rejection returns the folder to the Maker's display for updates and resubmission. You can also reject a single MP file (see page 81) in a folder.

You must be logged in to Audit Administrator as a user with the Checker role to reject an MP folder.

To reject an MP folder

1. Select the MP folder that you want to reject.

   The MP Files Folder pane appears.

2. Click Reject.

   The annotation script dialog appears.

3. Enter an annotation describing the reason why the folder is being rejected, and click OK.

   The rejected folder is removed from the available folders displayed in the MP files pane. The Maker may now make appropriate changes to the files in the folder and resubmit it.

More information

How Checker Work Flows Progress (see page 47)
MP Files (see page 68)
Policy Manager Tasks (see page 37)

Reject an MP File

You can review an MP file submitted by a Maker and reject it if modifications are required or any changes are not permissible. Rejecting by MP file differs from rejection of an MP folder (see page 80) by marking the individual file as rejected rather than the entire folder, making it easier for the Maker to determine where additional work is required.

You must be logged in to Audit Administrator as a user with the Checker role to reject an MP file.

To reject an MP file

1. Select the folder that contains the MP file you want to reject.

   The MP Folder pane appears

2. Click the file you want to reject in the MP Files area.

   The MP File Details pane appears.

3. Click Reject.

   An annotation dialog appears, titled with the name of the file you are rejecting.

4. Enter an annotation describing the reason why the file is being rejected, and click OK.

   The rejected MP file and its parent folder are removed from the list of available folders displayed in the MP Files pane. The Maker may now make appropriate changes to the file and resubmit its folder.

More information

How Checker Work Flows Progress (see page 47)
MP Files (see page 68)
Policy Manager Folders and Objects (see page 37)

Audit Nodes

Before you can create an Audit policy, you must identify the event sources you want the policy to target. To do this, create an audit node group (AN group), which represents the computers to which the event sources send their events, and then identify the audit nodes (specific computers) that are part of that group.

To create, modify, or delete an AN group or add, edit or delete nodes, you must be logged in to Audit Administrator as a user with the Maker role.

You can view and modify AN group details from the following Policy Manager sub-tabs:

Audit Nodes

Lets you perform AN tasks, including adding new nodes, and enabling or disabling existing nodes. You can view Nodes by:

- AN Group
- Host
- AN Type

Policies

Lets you perform Policy Folder tasks, including AN group attachment and creation.

MP Files

Lets you perform MP Folder tasks, including AN group attachment and creation.

Library

Lets you create, delete, and edit custom AN types.

Note: An Audit Node is a host running the eTrust Audit Client software. Computers running SAPI Recorders or iRecorders and sending events to a remote eTrust Audit Client should not be configured as Audit Nodes. However, you should configure the host that you want to process their events as an Audit Node.

More information

Create an Audit Node (AN) Group (see page 83)
Create an Audit Node (see page 86)
Disable or Enable an Audit Node (see page 88)
Deactivate or Reactivate a Node (see page 89)
Delete an Audit Node (see page 90)

Create an Audit Node (AN) Group

You must create AN Groups to contain your eTrust Audit Client nodes.

To create a new audit node (AN) group

1. Select Audit Nodes.

   The Audit Nodes pane appears.

2. Click New Group at the top of the Audit Nodes pane.

   The New Audit Node Group pane appears.

3. Select Type, enter Name and Description for your new AN group, and click Save.

   The new group appears in the Audit Node Group pane, displaying a confirmation message.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Edit an Audit Node Group

You can edit an AN group itself, or modify it by deleting a node (see page 90) from the group.

To edit an audit node group

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group you want to edit.

   The Audit Node Group pane appears.

3. Click Edit in the Details area.

   The Edit Audit Node Group pane appears.

4. Enter your changes to Name or Description, and click Save.

   The edited group appears in the Audit Node Group pane displaying a confirmation message.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Edit Audit Node Group Definitions

You can add definitions to a node group, setting default actions for any nodes associated with that group.

To edit Audit Node group definitions

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group to which you want to add actions.

   The Audit Node Group pane appears

3. Click the Edit button at the top of the Definitions area.

   A list of actions types appears, with a Server Name field for each action.

4. Enter a server name beside each action you want to define for this AN group, and click Save.

   The new definition appears in the Definitions area of the Audit Node Group pane.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Delete an Audit Node Group

You can delete an Audit Node (AN) group which contains no attached nodes.

To delete an audit node group

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group you want to delete.

   The Audit Node Group pane appears.

3. Click Delete.

   A confirmation dialog appears.

4. Click OK.

   The deleted group is removed from the Audit Nodes pane.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Mark an Audit Node Group for Deletion

You can mark an Audit Node (AN) group attached to a policy or MP folder for deletion.

To mark an audit node group for deletion

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group you want, and click Delete.

   The group is marked for deletion. The deletion takes effect when the folder to which the group is attached is submitted and approved by the Checker.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Create an Audit Node

You can manually create an audit node to identify a specific computer for your AN group.

To create a new audit node

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group to which you want to add a node.

   The Audit Node Group pane appears.

3. Click Create Audit Node.

   The New Audit Node pane appears.

4. Enter the Host Name.

   Note: If you are manually creating a node to specify a registered eTrust Audit Client, the Host Name must match the registered Client name exactly, to avoid update errors.

5. Select the Audit Node Type you want

   Note: If the AN Type you want to use does not exist, you can create a new Audit Node Type (see page 92).

6. (Optional) Enter a Description for the new node.

7. Click Save.

   The new node appears in the Audit Node Group pane, displayed with any other nodes in the group.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Create Multiple Audit Nodes

You can create multiple audit nodes at one time by searching for available host computers, which are registered but are not yet used in your Audit Administrator environment. You can register a host computers during the eTrust Audit Client installation.

To create multiple audit nodes

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group to which you want to add nodes.

   The Audit Node Group pane appears.

3. Click Create Multiple Audit Nodes.

   The Define Nodes pane appears.

4. Select the host type you want, and enter or select optional filter information including:

   Name

   Sets your search for an exact name match only; you cannot use wildcard characters.

   State

   Sets your search for a managed host (one with an eTrust Audit Client installed), an unmanaged host (one without an eTrust Audit Client installed), or any host.

5. Click Search.

   Any hosts matching your search criteria appear in the Hosts pane.

6. Select the host or hosts you want to add, and click Save.

   The Audit Node Group pane reappears, displaying a confirmation message and the new node or nodes.

More information

Audit Nodes (see page 82)
Using iRecorder Manager (see page 31)

Add Existing Audit Nodes

You can search for existing nodes to add to an AN group. An existing node is a node that has already been used in your Audit Administrator environment.

To add existing nodes

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group to which you want to add a node.

   The Audit Node Group pane appears.

3. Click Add Existing Nodes.

   The Add Existing Audit Nodes pane appears.

4. Enter the filter information you want, and click Search.

   Any nodes matching your search criteria appear in the Hosts pane.

5. Select the node or nodes you want to add, and click Save.

   The Audit Node Group pane reappears, displaying a confirmation message and the new node or nodes.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Disable or Enable an Audit Node

You can disable or enable an audit node in an AN group. Disabling a node prevents all policy or MP file distribution to that node, but does not affect any policies or MP files already running on the node. Enabling a node allows distribution to resume.

To disable or enable a node

1. Select the AN group containing the node you want to disable or enable.

   The group appears in the Details pane, displaying its attached nodes.

2. Select the node or nodes you want, and click Disable or Enable.

   A confirmation message appears, and the node state display is changed. The state change takes effect when the folder to which the group is attached is submitted and approved by the Checker.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Deactivate or Reactivate a Node

You can deactivate or reactivate a node. Deactivation prevents all policies on the specified node from working. Reactivation returns policies on the node to an active status.

To deactivate or reactivate a node

1. Select the AN group containing the node you want to deactivate or reactivate.

   The group appears in the Details pane, displaying its attached nodes.

2. Select the node or nodes you want, and click Deactivate or Reactivate.

   A confirmation message appears. The deactivation or reactivation takes effect when the folder to which the group is attached is submitted and approved by the Checker.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Remove an Audit Node From a Group

You can remove an audit node from an AN group.

To remove a node from an AN group

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group containing the node you want to remove

   The Audit Node Group pane appears, displaying a list of attached nodes.

3. Select the node you want to remove and click the Remove link.

   A confirmation dialog appears.

4. Click OK.

   The Audit Node Group pane appears, displaying a confirmation message.

   Note: You may select and delete multiple nodes at once.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Delete an Audit Node

You can mark an audit node attached to a distributed (see page 38) folder for deletion.

To delete an audit node

1. Click Audit Nodes.

   The Audit Nodes pane appears.

2. Select the AN group containing the node you want to delete.

   The Audit Node Group pane appears, displaying a list of attached nodes.

3. Select the node you want to delete, and click the Delete link.

   A confirmation dialog appears.

   Note: You may select and delete multiple nodes at once.

4. Click OK to confirm the deletion.

   The deleted node is marked for deletion. The deletion takes effect when the folder to which the group is attached is submitted and approved by the Checker.

   Note: You can use the Undo link to remove the deletion marking.

More information

Audit Nodes (see page 82)
Policy Manager Tasks (see page 37)

Activation Log

You can view the Policy Manager Activation Log, displaying the status of policy and MP file distributions. You can be logged in to Audit Administrator as either a Maker or Checker to view the Activation Log.

You can filter the activation log view by activation event time, by status values using the Status check boxes, or by the following attributes:

- Operation Type
- AN Name
- Folder Name
- Activation Message Text

Using the Not check box beside any of the attribute fields sets the filter to search for any attribute value other than the one you enter in the field.

More information

Policies (see page 48)
MP Files (see page 68)
Policy Manager Tasks (see page 37)

Library

You can view Audit Node Types and Rule Templates in the Audit Administrator Library. You can add custom AN types and edit or delete them. You cannot modify or delete Rule Templates.

More information

Audit Node Types (see page 92)
Rule Templates (see page 94)

Audit Node Types

You can view a list of predefined node types in the Node Types pane. You can also create your own custom node types, and edit or delete those node types. When you create nodes for your environment, you specify one of the predefined or custom AN types for each.

Note: Each event's Log field matches to an AN Type. If you gather events from custom sources and specify a non-standard Log name then you must create a matching custom AN Type to be able to filter those events. The Generic AN Type is the only one that does not perform matching based on the Log field.

You must be logged in to Audit Administrator as a user with the Maker role to create, edit, or delete node types.

Note: Both Maker and Checker users can view node types.

More information

Create a Node Type (see page 92)
Edit a Node Type (see page 93)
Delete a Node Type (see page 93)

Create a Node Type

You can create a custom audit node type.

To create a node type

1. Click Node Types.

   The Audit Node Types pane appears.

2. Click New Node.

   The New Audit Node Type pane appears.

3. Enter Name and Description, and click Save.

   The new node type appears in the Audit Node Type pane.

More information

Edit a Node Type (see page 93)
Delete a Node Type (see page 93)
Policy Manager Tasks (see page 37)

Edit a Node Type

You can edit custom node types. You cannot edit the predefined Audit Administrator node types.

To edit a node type

1. Click Node Types.

   The Audit Node Types pane appears.

2. Select the node type you want to edit.

   The chosen node appears in the Audit Node Type pane on the right side of the window.

3. Click Edit.

   The Edit Audit Node Type pane appears.

4. Enter your changes to Name and Description, and click Save.

   The edited node type appears in the Audit Node Type pane on the right side of the window.

More information

Create a Node Type (see page 92)
Delete a Node Type (see page 93)
Policy Manager Tasks (see page 37)

Delete a Node Type

You can delete custom node types. You cannot edit the predefined Audit Administrator node types.

To delete a node type

1. Click Node Types.

   The Audit Node Types pane appears.

2. Select the node type you want to delete.

   The chosen node appears in the Audit Node Type pane on the right side of the window.

3. Click Delete.

   A confirmation dialog appears.

4. Click OK.

   The deleted node type is removed from the Audit Node Types pane.

More information

Create a Node Type (see page 92)
Edit a Node Type (see page 93)
Policy Manager Tasks (see page 37)

Rule Templates

You can view predefined rule templates in the Template Library pane, which displays the rules grouped by type. You cannot edit the rule templates, which are used to create new rules (see page 53).

To view rule templates

1. Click Rule Templates.

   The Rule Templates appear in a tree view, sorted by type.

2. Expand the folder for the rule type you want to view.
3. Select a rule from the list of rule templates in the tree view.

   A detailed description of the selected rule appears in the Details pane, including its category and current version.

More information

Policy Manager Tasks (see page 37)

Chapter 4: Post-Collection Utility (PCU) Tasks

The Post-Collection Utility (PCU) provides a set of tools for defining policies. To access the Post-Collection Utility, you must be logged in to Audit Administrator as a user with the Admin role. The Post-Collection Utility is available only to Windows users.

Using the Post-Collection Utility, you can perform the following tasks:

- Expand eTrust Audit event data into individual entries using Load Policies
- Build logical views so that all expanded data is selectable, using View Policies
- Manage the size and contents of the Collector database using Prune Policies
- Detect event tampering by digitally signing and verifying signatures on collected events using Tamper Policies

When you access the Post-Collection Utility, a list of discovered Post-Collection Utility hosts appears in the PCU Browser pane. Select a host from the list to display the status of the PCU jobs running on that host.

This section contains the following topics:

Log on to a PCU Host

You can log on to the Post-Collection Utility host as a local administrator and perform any of the following tasks:

- Start a stopped job.
- Stop a running job.
- Remove a job from the Post-Collection Utility.
- Define a new job.

To log on to a PCU host

1. Select the host you want to log in to from the PCU Browser pane.

   The host details pane appears, displaying current jobs in the View Details area.

2. Click the Login link beside the host name at the top pane.

   The host log in screen appears.

3. Enter the appropriate Administrative user name and password.

   The View Job details display reappears.

More information

Start or Stop a Job (see page 96)
Load Policies (see page 97)
View Policies (see page 98)
Prune Policies (see page 100)
Sign and Verify Policies (see page 100)

Start or Stop a Job

You can start or stop a post-collection utility job.

To start or stop a job

1. Log in to the PCU host where the job you want exists.

   The View Jobs pane appears.

2. Click Start or Stop in the Start/Stop column for the chosen job.

   The new job status appears in the Status column.

Load Policies

You can use Load policies to expand the MSGTEXT field into individual entries. These entries can be converted in database columns through views and are then used in normal SQL queries or customized reports through external reporting tools.

You can define a new policy job using the New Job wizard. The wizard lets you define a job using an existing PCU policy template or by downloading a new one. Click New Job in the View Jobs pane to start the New Job wizard and complete the wizard fields, including the following information:

- Job name, type, and description for viewing its status.
- Initial Start Time. If no start time is specified, the job is started manually.
- ODBC data source (using Data Source Name, User Name, and Password).
- Job details for the following job parameters:
  - Run once
  - Burst load
  - Persistent job
  - Clean start
  - DB poll interval
  - Burst load, Burst load interval, and Burst count

    Note: Use Burst load to break event processing for the number of seconds specified in the Burst load interval to avoid locking the database while processing historical events.
- Job filters for database events.

The Post-Collection Utility creates a Load job as follows:

- Identifies the job by the name and description specified in the Job Information pane.
- Starts the job at the time specified in the Job Information pane.
- Connects to the ODBC data source defined in the Job Information pane.
- Selects each SEOSDATA event that is greater than the last processed ID and that matches the criteria specified in the filters.
- Keeps track of last SEOSDATA.ENTRYID that was processed for future jobs.
- Parses the MSGTEXT field into multiple entries, consisting of the following:
  - ENTRYID of event specified in SEOSDATA.entryid
  - Column name from MSGTEXT field

  - Value from MSGTEXT field
- Adds each entry as a row into the new AuditExtendString table.
- If running in burst mode, waits for the Burst Load Interval, then commits the Select operation.
- Waits for the DB Poll Interval and runs the same job again.

View Policies

After you run a load job to expand the SEOSDATA.MSGTEXT field into multiple entries in the AuditExtendString table, you can create view policies to construct logical views of the data.

You can create views as follows:

- Based on the event's LOGNAME, containing all possible column names. You can create this view automatically.
- Based on the event's taxonomy, containing all possible column names. You can create this view automatically.
- Based on the filters and columns provided in the policy. You must create a custom view to sort by filters and columns.

After you submit the view policy job, PCU constructs a view job as follows:

- Gives it the name and description specified so that you can view its status.
- Starts at the time you specified for Initial Start Time, or when you start the job the manually if you did not specify an initial start time.
- Repeats at the interval in seconds you set in the DB Poll Interval.

The view job runs as follows:

- Connects to the ODBC data source (using Data Source Name, Type, User Name, and Password)
- Processes each SEOSDATA event that is greater than the last processed ID **and** matches the criteria specified in the filters as follows:
  - If you do not specify filters/columns, PCU automatically constructs logical views on all SEOSDATA and AuditExtendString data. The views are named:

    AUD_VIEW_LOG_{logname}

    AUD_VIEW_TAX_{taxonomy}
  - If you provide filters/columns, PCU constructs a single custom logical view, selected by the filters provided, and including/excluding the columns provided. The view is named AUD_VIEW_CUST_{viewname}.
- Joins the two tables using AuditExtendString.entryid and SEOSDATA.ENTRYID. The new table contains the following:
  - All of the columns of the original SEOSDATA
  - Each expanded AuditExtendString.{column} as {column_v}

Prune Policies

You can use Prune policies to automatically discard events older than a specified date. Prune policies help you manage the size of the collector database.

Using the submitted prune policy, PCU constructs a prune job as follows:

- Gives it the name and description specified in Name and Description so that you can view its status.
- Starts at the time you specified for Initial Start Time, or when you start the job manually if you did not specify an initial start time.
- Repeats at the interval in seconds you set in the DB Poll Interval.

The prune job runs as follows:

- Connects to the ODBC data source (using Data Source Name, Type, User Name, and Password)
- Finds all SEOSDATA entries that meet the following criteria:
  - Created more than "Prune days" ago
  - Meet the criteria specified in the filters
- Stops if you select Test Prune Policy
- Processes each SEOSDATA entry found

The prune job does the following:

- Deletes SEOSDATA event
- Deletes AuditExtendString entries where AuditExtendString.entryid matches SEOSDATA.entryid
- Deletes AuditSign entry where AuditSign.entryid matches SEOSDATA.entryid

Sign and Verify Policies

You can use Tamper Policies to detect post-collection event tampering. The two types of tamper policies follow:

Sign Policies

Assigns a digital signature to new incoming events.

Verify Policies

Verifies previously signed events periodically using the digital signature.

Sign Policies

Use Sign Policies to initially apply a digital signature to incoming events.

Using the submitted sign policy, the PCU constructs a sign job as follows:

- Gives it the name and description specified in Name and Description so that you can view its status.
- Starts at the time you specified for Initial Start Time, or if you did not specify an initial start time, when you start the job the manually.
- After the job completes, it will run again when the value in DB Poll Interval seconds is reached.

The sign job runs as follows:

- Connects to the ODBC data source (using Data Source Name, Type, User Name, and Password)
- Processes each SEOSDATA event that meets the following criteria:
  - Greater than the last processed ID
  - Has not been previously signed
  - Meets the criteria specified in the filters
- Keeps track of last SEOSDATA.ENTRYID that was processed

The sign job does the following:

- Uses the data in the original event to generate an MD5 hash.
- Uses the PCU private key (generated at first install of the PCU) to digitally sign the MD5 hash.
- Creates an entry in the AuditSign table, consisting of the following information:
  - The event's ENTRYID specified in SEOSDATA.entryid
  - The digital signature
  - The date the event was signed
  - The original event's values in the SEOSDATA columns COMPUTERNAME, USERNAME, and LOGNAME
  - Verified set to 1 in order to mark the event as NON-TAMPERED
  - Verifydate set to the date the event was signed

Verify Policies

Use verify policies to verify previously signed events periodically.

Using the submitted verify policy, the PCU constructs a verify job as follows:

- Gives it the name and description specified in Name and Description so that you can view its status.
- Starts at the time you specified for Initial Start Time, or if you did not specify an initial start time, when you start the job the manually.
- After the job completes, it runs again when the value in DB Poll Interval seconds is reached.

The verify job runs as follows:

- Connects to the ODBC data source (using Data Source Name, Type, User Name, and Password)
- Processes each AuditSign entry that meets the following criteria:
  - Was not processed in the last Verify min hours
  - Was initially signed less than Verify max days ago
  - Is currently considered NON-TAMPERED
  - Meets the criteria specified in the filters

The verify job does the following:

- Uses the data in the original event to generate an MD5 hash.
- Uses the PCU private key (generated at first install of the PCU to digitally sign the MD5 hash.
- Compares the digital signature to the sig column in the AuditSign table as follows:
  - If the signature matches, mark the event as NON-TAMPERED (AuditSign verified column set to 1)
  - If the signature does not match, mark the event as TAMPERED (AuditSign verified column set to 0)

Chapter 5: Using Visualizer

The Visualizer allows you to run standard queries on data processed by the Post-Collection Utility or drawn from eTrust Security Command Center table collectors. You must be logged in to Audit Administrator as a user with the Admin role to access the Visualizer. The Visualizer is available only to Windows users.

When you access the Visualizer, a list of available queries appears, organized by type. These queries let you to generate reports or graphs using selection criteria predefined by the query, and filtered further by values that you set.

Using Visualizer, you can perform the following tasks:

- Generate queries for display in table or graphic form
- Display sample queries in graphic form

Note: You can download queries for the Visualizer from a central website.

This section contains the following topics:

Generate Visualizer Queries

You can generate visualizer queries using the list of downloaded queries in the Query Browser. You must select the query type, specify parameters for your query, and choose whether to display the query output in table or graphic form.

To generate a query

1. Expand the list of Query categories in the Query Browser pane, and select a query from the list.

   A description of the selected query appears in the Details pane.

2. Select the database you want to query from the ODBC Source drop-down list.
3. Enter your database user name and password.
4. Enter the maximum number of rows or lines that you want displayed in the query report.
5. Select additional search criteria in the applicable fields or drop-down lists.
6. (Optional) Click Save as Default to save the selected database for future use.
7. Click View Report to display the query in table *or* Graph Results to display the query in graph form.

   Your query report appears in the chosen format.

More information

Display Sample Graphic Queries (see page 105)
Using Visualizer (see page 103)

Display Sample Graphic Queries

You can view sample query graphs in the Sample List.

To view a sample query

1. Click Visualizer Samples.

   The Sample List pane appears.

2. Select a sample query.

   A description of the selected query displays in the Details pane.

3. Click Show Graph.

   The File Download dialog appears.

4. Click Open to display and view the graphic query.

   The Analyzer toolbar and graphic query appear.

5. (Optional) Click Save to save the sample query to a specified file location.

   The Save As dialog appears.

6. (Optional) Select the file location to which you want to copy the query file, and click Save.

   The query file is saved.

More information

Generate Visualizer Queries (see page 104)
Using Visualizer (see page 103)

Chapter 6: Using Reporter

Audit Reporter 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.

You must be logged in as a user with the Reporter role to access the Reporter interface.

For details on specific Reporter tasks, see the following More information list.

This section contains the following topics:

View a Report

You can generate a report for immediate viewing. These immediate reports can be created at any time, as opposed to regularly-scheduled reports that are generated at a specific preset time.

To view a report

1. Select the template you want to use for the report from the Report Templates pane.

   The chosen report type appears in the Details pane.

2. Click View Now.

   The Preview Report Options pane appears.

3. Select the Filter, report time range, and database source you want for the report.

   If the Database source has not been preconfigured, the User ID and password fields and the Test button appear.

4. (Optional) Enter the User ID and password, and click Test to verify the new database connection.

   A confirmation message appears.

5. Click Preview.

   The report appears in a new window. A confirmation message appears in the Preview Report Options pane.

More information

Schedule a Report (see page 114)
Review a Generated Report (see page 116)
View Report Logs (see page 116)

How to Create and Use Custom Report Templates

You can create custom report templates using the Crystal Reports package. After you create your custom template, you can import that template, and use it with the eTrust Audit Reporter.

Creating custom reports involves the following basic steps:

- Creating a valid report template
- Copying your custom templates to a new folder accessible to eTrust Audit
- Generating or scheduling a report from the Reporter user interface, as usual

Create a Crystal Reports Template

You can create a custom report template for use with Crystal Reports by setting mandatory parameters, and adding additional optional parameters if your custom report requires filters. If the mandatory parameters are not defined in the report template file (.rpt), the report template will not be available for selection in the Audit Administrator interface.

To create an eTrust Audit r8 SP2-compatible report template

1. Create a report template as usual, using Record Selection Formula (not SQL WHERE clause).

   Note: Before proceeding, we recommend that you test the new report template to ensure it satisfies your requirements properly.

2. Add the following mandatory String (static) type parameters, defining their values in the template itself:

   ETA_Title

   Defines the name of the report as you want it to appear in the eTrust Audit Reporter tree. This value usually also appears in the report itself.

   ETA_ProductName

   Defines the report subtitle. This value should be set to "eTrust Audit".

   ETA_DataType

   Defines the Data Source Names that are compatible with the report. For eTrust Audit r8 SP2 this value should be "policy" or "event".

3. (Optional) Add any of the following filter parameter pairs you want to the report template's ETA_Filter formula. Do not specify initial values for these parameters in the template. The values are set by the report end user in the eTrust Audit Reporter interface. You can omit any filter values that are not required from the report template.

   Note: The following field names are case-sensitive.

   ETA_IsUsername

   Indicates whether the report will be filtered by username. The value is set to "true" if the user specifies a username filter in the Reporter interface. This parameter must be a Boolean (static) type.

   ETA_Username

   Contains the username filter value, if a username filter is specified in the Audit Reporter web interface. This parameter must be a String (static) type.

ETA_IsHost

Indicates whether the report will be filtered by computer name. The value is set to "true" if the user specifies a computer name filter in the Reporter interface. This parameter must be a Boolean (static) type.

ETA_Host

Contains the computer name filter value, if a computer name filter is specified in the Audit Reporter web interface. This parameter must be a String (static) type.

ETA_IsTimeDuration

Indicates whether the report will be filtered by time range. The value is set to "true" if the user specifies a time range filter in the Reporter interface. This parameter must be a Boolean (static) type.

ETA_TimeDuration

Contains the time range filter value, if a time range filter is specified in the Audit Reporter web interface. This parameter must be a Date-Time (static, allow range values) type.

ETA_IsTodDuration

Indicates whether the report will be filtered by time-of-day. The value is set to "true" if the user specifies a time-of-day filter in the Reporter interface. This parameter must be a Boolean (static) type.

ETA_TodDuration

Contains the value of the time-of-day filter, if a time-of-day filter is specified in the Reporter interface. This parameter must be a Time (static, allow range values) type.

The following example of the ETA_Filter formula shows all four filter parameter pairs:

```
// user filter
(
    if {?ETA_IsUsername} then
        {SEOSDATA.USERNAME} = {?ETA_Username}
    else
        1=1
) and

// host filter
(
    if {?ETA_IsHost} then
        {SEOSDATA.COMPUTERNAME} = {?ETA_Host}
    else
        1=1
) and

// time filter
(
    if {?ETA_IsTimeDuration} then
        {SEOSDATA.TIMSTAMP} in {?ETA_TimeDuration}
    else
        1=1
) and

// tod filter
(
    if {?ETA_IsTodDuration} then
        Time({SEOSDATA.TIMSTAMP}) in {?ETA_TodDuration}
    else
        1=1
)
```

4. (Optional) If you included filter parameter pairs, reference the filters in the ETA_Filter formula by using a logic AND, as illustrated in this example:

   (

   {SEOSDATA.LOGNAME} = 'eTrust AC' or … and (…)

)

   and {@ETA_Filter}

   You must complete this step in order for the filters to function.

5. Save your custom report file.

Add a Custom Report Template to the Template Directory

You can copy a custom report template to the eTrust Audit Templates directory, making it available for selection in the interface. By default, all reporter templates files are stored in the Templates directory.

To copy a custom report template to the templates directory

1. Access a command prompt.
2. Navigate to the Templates directory.

   For Windows systems, the default path is:

   [Audit root]\dat\Reports\Templates

   For UNIX systems, the default path is:

   [Audit root]/dat/Reports/Templates directory.

3. Create a new directory to contain your custom template.

   The folder name that you choose will display in the Reporter's list of report templates after you restart the Reporter.

   Note: You can only use alphanumeric characters and underscores for custom report directory names.

4. Copy your custom template to the newly-created folder.
5. Restart the Reporter and Viewer Web Server.

This causes the Reporter to pick up the new template folder and templates as part of its initialization.

Use a Custom Report

You can use a custom template to generate an eTrust Audit report in the normal fashion.

To use a custom report

1. Access the Audit Administrator.
2. Log in to the Reporter application.
3. Locate your templates folder in the list of Report templates.
4. Expand the folder node and select your custom template.
5. Generate or schedule the report in the normal way.

Schedule a Report

You can schedule a regular report and set options including how often the report is generated, its output format, and filtering.

To schedule a report

1. Select the type of report you want to schedule from the Report Templates pane.

   The chosen report type appears in the Details pane.

2. Click Add to Schedule.

   The Schedule Report pane appears.

3. Select scheduling options, which include the following:

   Schedule

   Defines the day when you want the report to be created. Selecting Every or Next from the Period menu enables the Days menu, letting you select a day of the week or date of the month for the report generation. You can select multiple days or dates.

   Select Filter

   Defines predefined or custom filtering for your report. Selecting custom filtering causes the Custom Events area to appear, allowing you to select detailed From and To times for the report span.

   Note: Policy Manager reports do not support filtering.

   Query Time

   Enables an additional level of report filtering, allowing you to select From and To times for the report query, and specify the query target by User Name and/or Computer Name.

4. Select the database source you want for the report.

   If the Database source has not been preconfigured, the User ID and password fields, and the Test button appear.

5. (Optional) Enter the User ID and password, and click Test to verify the new database connection.

   A confirmation message appears.

6. Click OK.

   The Schedule Report pane closes, and the new report appears in the Scheduled Job pane.

More information

Edit a Scheduled Report (see page 115)
Delete a Scheduled Report (see page 115)

Edit a Scheduled Report

You can edit a scheduled report.

To edit a scheduled report

1. Select the report you want to edit in the Scheduled Jobs pane, and click Edit Job.

   The Update Scheduled Job pane opens.

2. Make your changes, and click Update.

   The edited report appears in the Scheduled Jobs pane.

More information

Delete a Scheduled Report (see page 115)
Using Reporter (see page 107)

Delete a Scheduled Report

You can delete a scheduled report.

To delete a scheduled report

1. Select the report you want to delete in the Scheduled Jobs pane, and click Delete Job.

   A confirmation dialog appears.

2. Click OK.

   The deleted report is removed from the list in the Scheduled Jobs pane.

More information

Edit a Scheduled Report (see page 115)
Using Reporter (see page 107)

Review a Generated Report

You can review previously-generated reports by type.

To review a generated report

1. Select the type of report you want to view from the Report Templates pane.

   The chosen report type appears in the Details pane, displaying a list of generated reports.

2. Click the title of the report you want to view in the Report name column.

   The report appears in a new window.

More information

Delete a Generated Report (see page 116)

Delete a Generated Report

You can delete a generated report.

To delete a generated report

1. Select the report you want to delete in the Generated Reports pane, and click Delete Report.

   A confirmation dialog appears.

2. Click OK.

   The deleted report is removed from the list in the Generated Reports pane.

More information

Using Reporter (see page 107)

View Report Logs

You can view a list of all scheduled Reporter jobs that have already executed. To view report jobs, click View Logs at the top of the Detailed Events pane. The Log Details window appears, displaying a list of all eTrust Audit Reporter jobs.

Note: Immediate reports (see page 107) are not logged. Only scheduled report jobs appear in the Log Details list.

More information

View a Report (see page 107)
Schedule a Report (see page 114)
Review a Generated Report (see page 116)

Chapter 7: Using Viewer

You can view, sort, and filter the eTrust Audit event database using the Viewer. You must be logged in as a user with the Viewer role to access the Viewer.

This section contains the following topics:

Add a Filter

You can add a custom filter to your Audit Administrator environment. The new filter may be one of the following types:

Event Filter

Searches the database by event category, qualifying the search by the Event details you select.

Field Filter

Searches the event database by field contents, qualifying the search by the Field details you select.

You can make either type of filter available to you only (current user), or to all users.

More information

Add an Event Filter

You can add an event filter to search the database by event category.

To add an event filter

1. Select Event Filter in the Add Filter pane, and click Add.

   The Event Filter window appears

2. Enter a Filter Name, and select whether you wish the new filter to be available to you only or to all users.

3. (Optional) Set filter field information including:

   View From

   Defines the start of the time span searched by the filter. Selecting Events On allows you to specify a date and time for the beginning of the search.

   Default: First Event

   View Through

   Defines the end of the time span searched by the filter. Selecting Events On allows you to specify a date and time for the end of the search.

   Default: Last Event

   Event Types

   Defines which event categories the filter will search. Clearing an event category removes it from consideration by the filter.

   Fields

   Defines specific attributes to which the filter applies. You can enter a value for any or all of the following attributes to narrow the filter search:

   - Domain
   - Computer
   - LogName

Event Category

Defines event categories you want the filter to consider. You can select any or all of the following categories and enter or select additional qualifying details:

- Admin
- Login
- Network
- Resource
- Tracking
- Other

You can select either of the following event categories, but not enter additional qualifying details:

- Trusted Program
- Startup/Shutdown

4. (Optional) Click the Sql button to display the SQL language your filter choices create. The SQL pane appears, showing the filter language grayed out. You can copy and paste the SQL into the advanced SQL pane to manually edit it.
5. Click Save.

   The new filter appears in the Audit Viewer Filters pane.

More information

Add a Field Filter (see page 122)
Using Viewer (see page 119)

Add a Field Filter

You can add a field filter to search the database by field contents.

To add a field filter

1. Select Field Filter in the Add Filter pane, and click Add.

   The Field Filter window appears.

2. Enter a Filter Name, and select whether you wish the new filter to be available to you only or to all users.

3. (Optional) Set filter field information including:

   View From

   Defines the start of the time span searched by the filter. Selecting Events On lets you specify a date and time for the beginning of the search.

   Default: First Event

   View Through

   Defines the end of the time span searched by the filter. Selecting Events On lets you specify a date and time for the end of the search.

   Default: Last Event

   Event Types

   Defines which event categories the filter searches. Clearing an event category removes it from consideration.

   Details

   Defines the value of the event fields you want the filter to search. Selecting the Not check box sets the filter to search for any value other than the one you have entered in the corresponding field. For example, entering UNIX in a field and selecting the Not check box will set the filter to search the given field for any value which is not UNIX.

4. (Optional) Click the Sql button to display the SQL language your filter choices create. The SQL pane appears, showing the filter language grayed out. You can copy and paste the SQL into the advanced SQL pane to manually edit it.

5. Click Save.

   The new filter appears in the Audit Viewer Filters pane.

More information

Add an Event Filter (see page 120)
Using Viewer (see page 119)

Edit a Filter

You can edit an existing user only filter. You cannot edit the predefined filters provided with Viewer, or filters created for all users.

To edit a filter

1. Select the filter you want to edit in the Audit Viewer Filters pane, and click Edit.

   The Event Filters pane for the selected filter appears.

2. Make your changes, and click Save.

   The edited filter appears in the Audit Viewer Filters pane.

More information

Add a Filter (see page 119)
Run a Temporary Filter (see page 123)
Set a Startup Filter (see page 124)
Copy a Filter (see page 125)
View Event Details (see page 126)

Run a Temporary Filter

You can set up and run a temporary filter to view events in your environment immediately, without creating a new filter or using a pre-existing filter. You can create a temporary filter from an event filter or a field filter. You can modify, discard, or save a temporary filter after you run it.

To run a temporary filter

1. Select Event Filter or Field Filter in the Add Filter pull-down menu, and click Add.

   The Event Filter or Field Filter window appears.

2. Set the filter values you want, and click Run.

   The appropriate events appear in the Event Table pane of the main Viewer window.

   Note: The Event Filter or Field Filter window does not close, letting you make further changes as needed. You may have to move or minimize it to view your temporary filter results.

3. (Optional) To retain the filter for future use, enter a name in the Event Filter or Field Filter window, and click Save.

   The Event Filter or Field Filter window closes, and the new filter appears in the Audit Viewer Filters list.

More information

Add a Filter (see page 119)
Edit a Filter (see page 123)
Set a Startup Filter (see page 124)
Copy a Filter (see page 125)
View Event Details (see page 126)

Set a Startup Filter

You can set a startup filter, which appears in the Event Table pane when you open the Audit Viewer.

To set a startup filter, select the filter you want in the Audit Viewer Filters pane and click Set as Startup. A confirmation message appears in the Select Filters area. The selected filter will appear as the startup filter.

Note: After you have set a startup filter, the application requires that one be used. You may replace your chosen startup filter with another, but you must have a filter set as startup.

More information

Add a Filter (see page 119)
Edit a Filter (see page 123)
Run a Temporary Filter (see page 123)
Copy a Filter (see page 125)
View Event Details (see page 126)

Copy a Filter

You can create a user filter by copying an existing filter.

To copy a filter

1. Select the filter you want, and click Copy.

   The Copy Filter dialog appears.

2. Enter a new Name, and select whether you wish the new filter to be available to you only or to all users.

3. Click OK.

   A confirmation message appears in the Copy Filter dialog.

4. Click Close.

   The Copy Filter dialog closes and the new filter appears in the User Filters folder of the Audit Viewer Filters pane.

More information

Add a Filter (see page 119)
Edit a Filter (see page 123)
Run a Temporary Filter (see page 123)
Set a Startup Filter (see page 124)
View Event Details (see page 126)

View Event Details

You can view details of an individual event from the filter Event Table pane.

To view event details

1. If the Data Source you want is not loaded, click the down arrow at the top of the Select Data Source pane.

   The Select DSN pull-down menu appears.

2. Select the DSN you want from the Select DSN pull-down menu, and click Load.

   A confirmation message appears.

3. Select the filter whose events you want to view in the Audit Viewer Filters pane.

   The Event Table pane opens, displaying events for your chosen filter.

4. In the Detail column, click the information icon for the event you want to view.

   The Event Details window appears.

5. (Optional) Use the Next or Prev arrows to scroll through the available events.

6. Click Close when you are finished viewing event details.

More information

Add a Filter (see page 119)
Edit a Filter (see page 123)
Run a Temporary Filter (see page 123)
Set a Startup Filter (see page 124)
Copy a Filter (see page 125)

Chapter 8: Using Health Monitor

The Health Monitor allows you to view your eTrust Audit Data Tools event sources.

Health Monitor provides status information based on the rate of events received from each of the event sources, and an Action Summary so that you can track changes to your alert configurations.

Using the Health Monitor, you can perform the following tasks:

- Display a list of the available Health Monitor hosts.
- View generated alerts for the selected host, using filters to sort the list.
- View event rate summaries for the selected host and filter them with any combination of log, host, and domain names.
- View and modify scan, alert, and database information for the selected host.
- View log table information including scan history and configuration changes.

To access the Health Monitor you must be logged in to Audit Administrator as a user with the Admin role.

This section contains the following topics:

Display Health Monitor Hosts

You can display a list of available Health Monitor host computers.

To display Health Monitor hosts

1. Click the Health Monitor tab.

   The Health Monitor hosts pane appears.

2. Do one of the following to display the discovered hosts:

   - Click Show all discovered Health Monitor hosts. This is the default selection.
   - Click Show Host and enter a specific host name.

3. Click Browse.

   A list of Health Monitor hosts or the named host appears.

4. Select the named host, or a host name from the list of discovered hosts displayed in the Health Monitor Hosts browser list, to view the alerts for that host.

More information

Alert (see page 129)
Event Rate Summary (see page 130)
Configuration (see page 131)
Logs (see page 137)

Alert

You can set up filters to screen generated alerts. If you find a particular alert of interest, you can retrieve event rate summary information for it. In the Configuration pane, you can configure alert constraints and filter alerts using the following monitoring conditions.

Health Monitor alert columns include the following category:

Alert Type

Defines the Alert type. Only a single No Events From Source alert is generated by each instance of event gathering failure. After the Health Monitor detects this alert for a specific event source, it stops generating the alert until it receives another incoming event. After the Health Monitor recognizes a new event from that same source, an alert is generated the next time a No Events From Source condition is met. This prevents redundant alerts when an event source becomes unavailable for an extended period of time.

You can also filter alerts by Log Name, Host Name, Domain Name, or time of occurrence.

Click a display column header to sort the result data by the contents of that column. Sort is automatically disabled if there are more than 200 result items.

More information

Display Health Monitor Hosts (see page 128)
Event Rate Summary (see page 130)
Configuration (see page 131)
Logs (see page 137)

Event Rate Summary

The Event Rate Summary view shows you alert event details across a range of alert types. You can see summaries for all of the log names across all host and domain names, or a single log name for a single computer in a given domain.

The summary includes the following information:

Type

Identifies the event type: Events Per Second (EPS) or Event Count (Event)

Last Scan

Identifies the number of events (or EPS throughput) recognized by the last scan.

High/Low Threshold

Identifies the maximum and minimum number of events (or throughput) recognized within a single scan interval. These values are maintained for the life of the Health Monitor.

Total Events

Identifies the number of events received from the indicated event source (host computer and log name) since the start of event gathering. This value is accumulated for the life of the Health Monitor.

Click Show Timestamps to see the time stamps for each of the following event types in the summary view:

- Last Scan
- High Threshold
- Low Threshold
- Total Events

More information

Display Health Monitor Hosts (see page 128)
Alert (see page 129)
Configuration (see page 131)
Logs (see page 137)

Configuration

You can view and modify your Health Monitor configuration by accessing the following areas:

- Scan Configuration (see page 131)
- Alert Configuration (see page 133)
- Database Server Info - displays read-only reference information

More information

Scan Configuration (see page 131)
Alert Configuration (see page 133)

Scan Configuration

You can view and set scan configuration values, including the following:

Event Scan Interval

Defines the interval between event scans. You can set the interval in any combination of days, hours, minutes.

Note: The Event Scan Interval and Alert event thresholds (see page 133) are interrelated. To obtain accurate alert occurrences, you must know the high and low event thresholds for the scan interval you intend to set. For example, if you expect to receive a high threshold of 300 events in a one minute span, and you want to set the scan interval for five minutes, set the high event threshold to 1500.

More information

Edit Scan Configuration (see page 132)

Edit Scan Configuration

You can edit scan configuration parameters for the selected Health Monitor host.

To edit scan configuration values

1. Select the host you want from the Health Monitor Hosts pane.

   The selected host's details appear in the Health Monitor Information pane.

2. Click the Login link beside the host name at the top of the Health Monitor Information pane.

   The host log in screen appears.

3. Enter the appropriate user name and password.

   The Health Monitor Information pane reappears.

4. Click the Configuration tab, and click Edit in the Scan Configuration area.

   Editable value fields appear.

5. Enter your changes, and click Save.

   The view returns to read-only status, displaying the edited configuration values in the Scan Configuration area along with a confirmation message.

   Note: You can also enable or disable scan configuration values individually by selecting or clearing the Enabled check box.

More information

Using Health Monitor (see page 127)

Alert Configuration

You can view or set various types of alerts (see page 134) for individual event sources, including:

High event count Threshold

Defines the high alert count threshold. If the number of events during the chosen scan interval exceeds this number, Health Monitor triggers an alert.

Default: 600

Low event count Threshold

Defines the low alert count threshold. If the number of events during the chosen scan interval falls below this number, Health Monitor triggers an alert.

Default: 0

Note: The Events Per Second (EPS) value for a given scan interval is rounded to the nearest whole number before it is compared to your chosen EPS specification for alert purposes.

No Event Interval Alert

Defines the no event alert threshold in any combination of days, hours, and minutes. If the specified time elapses without any events being received by Health Monitor, an alert is triggered.

Default: 1 Hour

Note: The Alert event thresholds and Event Scan Interval (see page 131) are interrelated. To obtain accurate alert occurrence, you must know the high and low event thresholds for the scan interval you intend to set. For example, if you expect to receive a high threshold of 300 events in a one minute span, and you intend to set the scan interval for five minutes, the high event threshold should be set to 1500.

You can target alerts for a specific log name (log type) or specific log name and computer name combination. You must specify both the host and domain name to identify a single computer.

More information

Add an Alert (see page 134)
Edit an Alert (see page 135)
Delete an Alert (see page 136)

Add an Alert

You can add an alert to a Health Monitor host.

To add an alert

1. Select the host you want from the Health Monitor Hosts pane.

   The selected host's details appear in the Health Monitor Information pane.

2. Click the Login link beside the host name at the top of the Health Monitor Information pane.

   The host log in screen appears.

3. Enter the appropriate user name and password.

   The Health Monitor Information pane reappears.

4. Click the Configuration tab, and click Edit in the Alert Configuration area.

   Editable value fields appear.

5. In the Add New Log Configuration Entry area, select the Log Name.

   Note: You can also select Other and type a different log name if the name you want does not appear in the list.

6. (Optional) Type a valid host name for a specific event source in the Host Name field.

7. (Optional) Type a valid domain name in the Domain Name field. This is the domain for the computer named in the Host Name field.

8. Click Add.

   The new entry appears in the Alert Configuration area, displaying the default no event interval, alert type and threshold settings.

9. (Optional) Set the No Event Interval values for this alert, if needed.

10. (Optional) If you are creating a count or threshold alert, set the alert Type in the drop-down list:
    - Select EPS to track events by average events per second.
    - Select Event to track the actual number of events that occurred during the scan interval.
11. (Optional) Set the Low and High Threshold values.

    Note: A low threshold value of zero is the same as no event and requires the creation of a No Event Interval.
12. Click Save.

    The view returns to read-only status and displays the new alert parameter at the bottom of the list. The changes take effect the next time an event scan takes place.

    Note: Saving a new alert also updates the Health Monitor configuration log with any changes.

More information

Edit an Alert (see page 135)
Delete an Alert (see page 136)

Edit an Alert

You can edit alert parameters for a Health Monitor host.

To edit an alert

1. Select the host you want from the Health Monitor Hosts pane.

   The selected host's details appear in the Health Monitor Information pane.
2. Click the Login link beside the host name at the top of the Health Monitor Information pane.

   The host log in screen appears.
3. Enter the appropriate user name and password.

   The Health Monitor Information pane reappears.
4. Click the Configuration tab, and click Edit in the Alert Configuration area.

   Editable value fields appear.
5. Enter your changes and click Save.

   The view returns to read-only status in the Alert Configuration area, and a confirmation message appears.

More information

Add an Alert (see page 134)
Delete an Alert (see page 136)

Delete an Alert

You can delete an obsolete or unneeded alert.

To delete an alert

1. Select the host you want from the Health Monitor Hosts pane.

   The selected host's details appear in the Health Monitor Information pane.

2. Click the Login link beside the host name at the top of the Health Monitor Information pane.

   The host log in screen appears.

3. Enter the appropriate user name and password.

   The Health Monitor Information pane reappears.

4. Click the Configuration tab, and click Edit in the Alert Configuration area.

   Editable value fields appear.

5. Locate the alert you want to delete, and click the trash can icon at the end of the row.

   A confirmation dialog appears.

6. Click Yes.

7. Click Save.

   The view returns to read-only status and a confirmation message appears. The changes take effect the next time an event scan takes place.

   Note: Saving the view also updates the Health Monitor configuration log with any changes.

More information

Add an Alert (see page 134)
Edit an Alert (see page 135)

Logs

You can track changes to the Health Monitor configuration using the Logs view. The logs are independent of alert events that may occur during normal network operations scanning, and provide internal tracking and accountability for the Health Monitor configuration itself.

Click Filters to set filter parameters. You can filter the Logs view in a variety of ways; from scan and configuration changes based on a specific user, or all users, to changes made within specific time frames, or any combination of these parameters.

More information

Display Health Monitor Hosts (see page 128)
Alert (see page 129)
Event Rate Summary (see page 130)
Configuration (see page 131)

Index

A

C

D

E

F

H

I

L

M

P

R

S

T

U

V

W