eTrust® Audit and eTrust® Security Command Center

Implementation Guide

r8 SP2

CA Product References

This document references the following CA products:

- eTrust® Security Command Center (eTrust SCC)
- eTrust® Audit (eTrust Audit)
- *e*Trust® Antivirus (eTrust AV)
- Unicenter® Event Management Console (Unicenter EVT)

Contact Technical Support

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

Contents

Chapter 1: Security Information Management Overview

This section contains the following topics:

Introduction to SIM Systems

Network security solutions generate large amounts of information. Managing the varying levels of information, performing analysis, and managing data retention represent a technical challenge for any business. Security Information Management (SIM) systems help with these tasks, providing advanced management functions including analysis, real-time or near real-time alert or remediation capabilities, and reporting facilities.

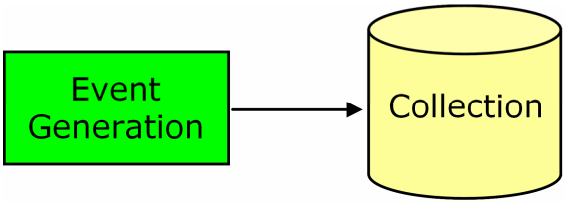
Event Generation

A basic level of security information management is configuring the event source to generate the necessary events for collection. Each application or device vendor provides documentation with instructions on what is necessary to enable event generation, shown in green in this and following illustrations.

Recording and Storing Data

A higher level of security information management is the recording of event data. Events come from security applications or devices such as network appliances, firewalls, servers, and activities on those servers. The network activities include any number of events such as logon and logoff, failed logons, messages from firewall activities, access to restricted devices or applications, and many others.

One basic use for a SIM solution stores this generated event data in a central database, as shown in the following illustration:

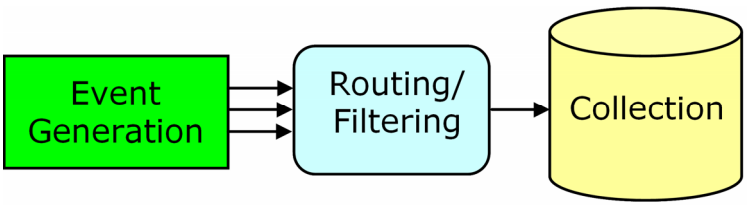


Collection provides a way to store events in a central database, and includes the processes and services that assist in that task and the storage database itself. Collection is shown in light yellow in this and subsequent illustrations.

This solution works well if your requirements only relate to event storage. However, this solution stores everything regardless of its usefulness and does not provide any means of viewing or acting on the data. It is rare for an organization to need to store *all* of its generated events. Typically, you store only certain types of events and ignore others. For example, you may not want to store information about failures to set up printers on remote desktop connections, but you would want to store information about failed logon attempts or access to restricted objects.

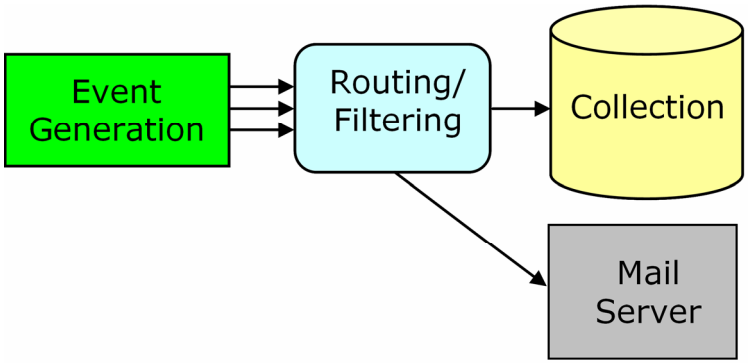
Controlling Data Flow

Another aspect of a SIM solution is a mechanism to control how much information goes into the database using routing and filtering capabilities. Some events represent more critical information that requires a person to be alerted or an automated process to be executed. After the immediate alert or action, the event can then be forwarded to a database for reference during the analysis phase. Other events can be excluded altogether because there is no meaningful information inherent in the event. The following illustration shows events being routed or filtered before they reach the collection database:



Filtering lets you control what kinds of events are stored, and which are discarded. *Routing* lets you control where events are sent and stored in a distributed network. Routing and filtering are shown in light blue in this illustration and subsequent ones.

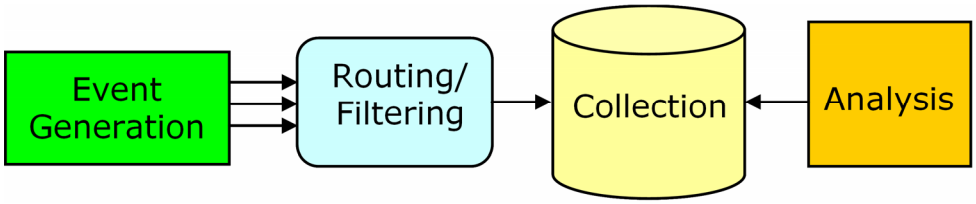
More advanced routing features let you send some information to other destinations. The next illustration shows events being sent to the database and to an SMTP mail server for email alerts after routing and filtering:



A SIM system with routing, filtering, and data collection represents a workable solution. However, there still is no means of viewing event data, analyzing the data, or gathering report information. A robust SIM solution provides management views of data (events) so that you can monitor the security network and trends and patterns in near real time.

Analyzing Collected Data

The addition of an analysis framework lets you analyze different views of your data, including viewing alerts and incidents, reviewing system status, and creating reports to demonstrate compliance. The analysis component of the SIM solution is shown in this illustration in a light orange color. The ability to view your data in a way that is relevant to your business is ultimate the outcome of a SIM solution.



These areas represent the basis of a SIM solution for managing your network's security operations and event data. Later sections will relate these areas to basic scenarios and the eTrust Audit and eTrust Security Command Center products to prepare you for their implementation.

The CA SIM Solution

This guide helps you implement both eTrust Audit and eTrust Security Command Center as a SIM solution. eTrust Audit is a SIM solution that offers security routing, filtering, and monitoring capabilities such as event aggregation, reduction, and correlation. eTrust Security Command Center is a SIM solution that offers custom reporting and management views of system activity and status.

Chapter 2: Common SIM Uses

This section contains the following topics:

Typical Scenarios

The true power of a security information management solution resides in using the collected data to achieve business objectives. Some common business objectives related to security include the following:

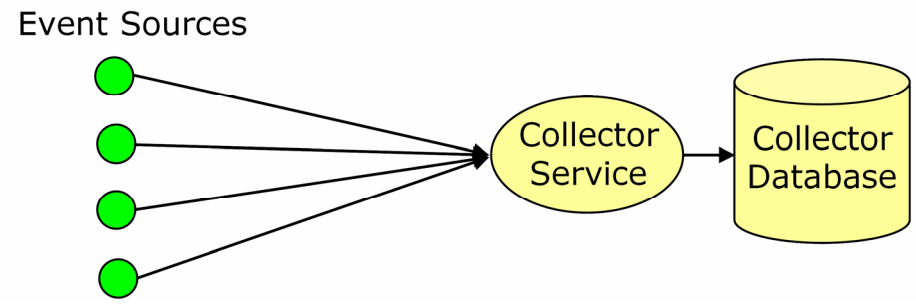
- Central data collection
- Reporting and compliance
- Status monitoring and alerts

Each of these intended uses has a different set of requirements as to data retention and handling. These requirements can affect the hardware and software structure of the SIM solution based on network and database needs.

While central data collection is part of each of the common scenarios, the actions taken on the data are different. Attempting to combine all of the scenarios would result in a SIM system that is very difficult and expensive to provision and to maintain.

Central Data Collection

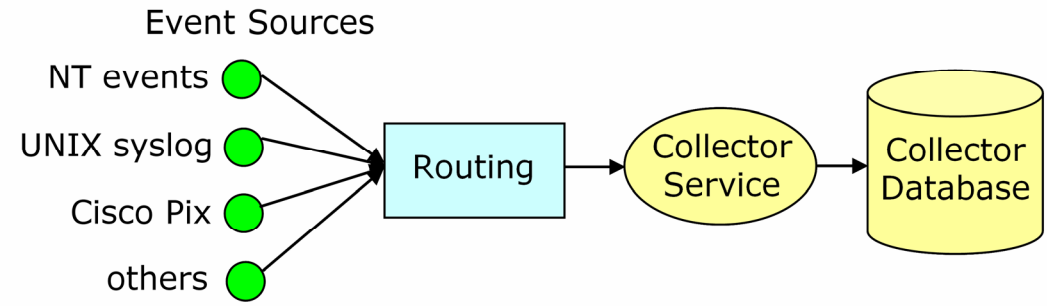
One of the most common uses for a SIM system is central data collection. Typically this is a central database, served by a commonly available, relational DBMS package, and managed by a database administrator (DBA). The illustration that follows shows a simple arrangement of event sources, a collector service or process that stores events in the database, and the collector database itself.



The event sources, shown in green, are any of a variety of devices or applications. Based on the size of the network and the volume of traffic, there may be more than one collector database (shown in yellow) to contain the events generated by the event sources. Various collection processes (also shown in yellow) support the transfer of data between event sources and the collector database. At a low level, the key operating system and database events are captured in a common format to allow further analysis.

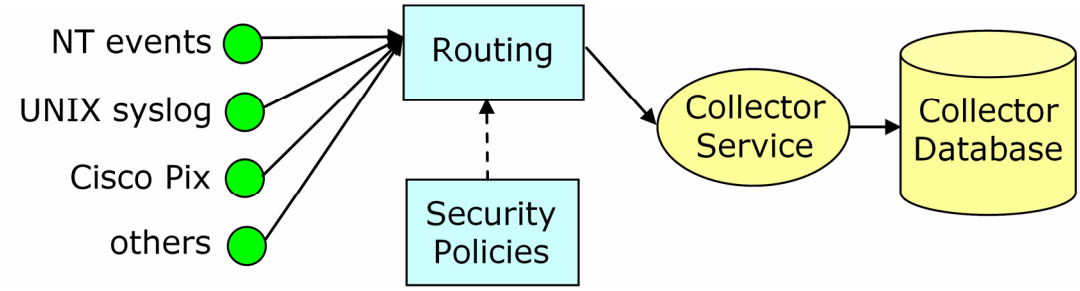
Routing Event Data

While centralized data collection is a common use, it is not usually the only service provided by a SIM solution. Additional SIM functionality, described in later scenarios, lets you use the data for specific business purposes. For example, additional routing and filtering capabilities (shown in blue) let you control which events are retained, and how they are handled. The actions taken on the event data can vary based on the SIM solutions abilities. The illustration that follows shows the routing function accepting inputs from event sources, and passing selected events to the collector database. This is a common scenario when dealing with a firewalled environment. Allowing a single server to act as a consolidation point for multiple event sources prevents multiple access points through the firewall, and better maintains the security of the environment.



Filtering Event Data

SIM system customers make the best use of centralized data collection after first carefully considering what information they actually need to retain. In large networks, the amount of data stored in the collector database can become very large. Data reduction, aggregation, and correlation are used to make automated decisions about which data to keep. Security policies can control which events are recorded by the event sources. The illustration that follows shows the interaction of security policies with the event sources and routing functions:



Ideally, you might implement the security policies across a variety of network event sources in an automated way, to control event routing. Event handling from these policies might route some event traffic to other destinations such as SMTP servers. Filtering the event data also lets you send certain types of events directly to security monitoring workstations for viewing in near real time. Using these SIM capabilities, you can create a more robust central data storage scenario.

Forensics and Detailed Analysis

SIM systems that focus on forensics and detailed analysis are a special type of central data collection scenario. This type of SIM system provides little or no monitoring or reporting as all data is collected for a given period of time. This retention timeframe is normally short as a result of the enormous volume of data collected. However, the data can be used for root cause analysis or very detailed forensic discovery of what occurred on the systems.

This scenario includes SIM solutions based on log consolidation, long term impact analysis, advanced correlation scenarios such as cross-product intrusion detection, and so forth. Such solutions require careful and detailed configuration of the collector database and a combination of security policies and custom filtering rules to accomplish the correlations.

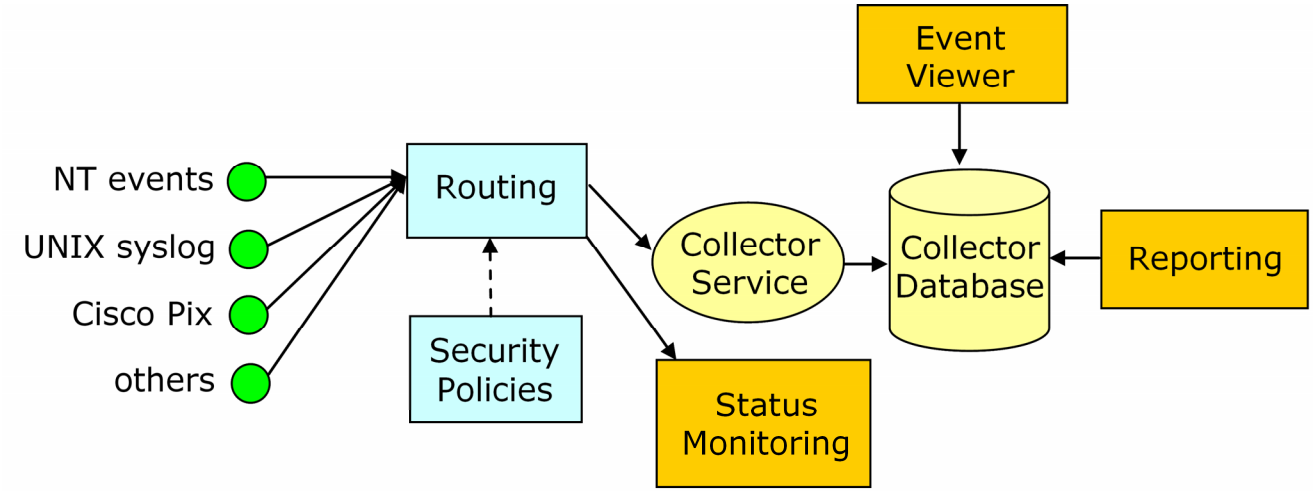
SIM implementations focused on forensics and analysis are not maintainable for long periods without large investments in hardware, software, and personnel to manage the system. Based on the large amount of data inherent in these solutions, we recommend that they be developed in a separate environment from the normal, day-to-day operations. This ensures the ability to provide adequate alerting and daily reports while retaining the capability of forensic analysis.

Reporting and Compliance

SIM systems focusing on compliance support specific requirements as determined by a set of standards. The requirements of the standard can be internally defined or they can be external standards, such as the Health Insurance Portability and Accountability Act (HIPAA) or Sarbanes-Oxley (SOX) regulations. This type of SIM implementation may or may not need detailed event data depending on the requirements. A SIM system might facilitate compliance by offering the following:

- Consolidation of server logs and security events in a common collector database
- Storage of disparate information types in a common format
- A network monitoring and evidence collection capability to support evidentiary requirements related to federal regulations
- Predefined and automated reporting of a variety of system security events

Compliance-based SIM systems include solutions based on consolidated reporting or visualization (data collected from complementary software combinations), and compliance reporting. Such systems may also include monitoring of system status in near real time. The illustration that follows shows the basic central data collection scenario with additional functionality (shown in orange) for reporting, and viewing of event data and system status.



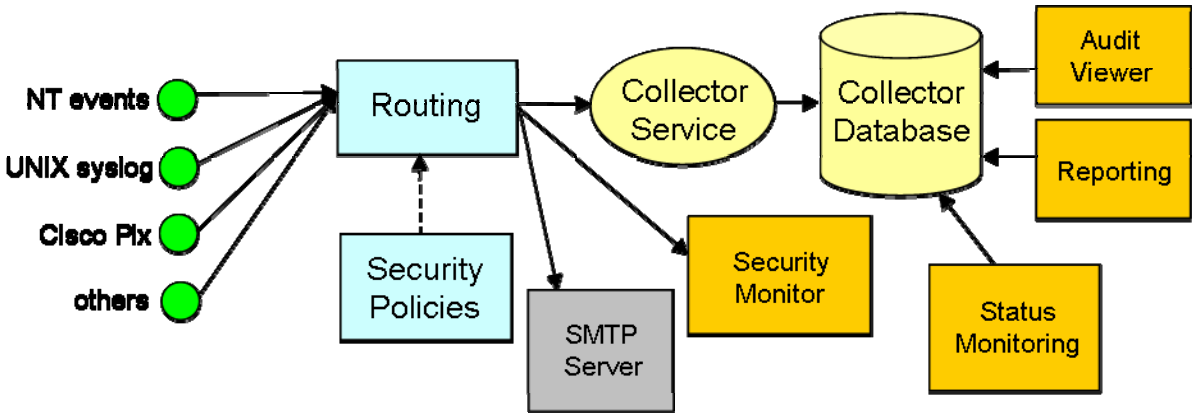
Status Monitoring and Alerts

SIM systems focusing on alerts provide monitoring of events with summary reports of specific criteria for given timeframes. Specific events can trigger alert notifications to various destinations for timely handling. Alerts may be based on different types of events from devices and applications in the network, including operating systems, firewalls, servers, databases, and reports on policy compliance and network device status. Some of the most common events that trigger alerts include the following:

- Multiple failed logon attempts
- Antivirus (AV) alerts
- Intrusion detection signature violations
- High volumes of firewall activity from a single source IP address

The illustration that follows shows an event flow with a combination of routing and filtering handled by security policies. Event traffic flows to the central database and to mail servers, security monitors, and web interfaces.

The security monitor receives events that require immediate attention. The SMTP server handles email and pager alerts for emergency notifications. The collector database contains a tailored set of events from which trends and patterns can be analyzed and reported.



SIMs that focus on status monitoring and alerts include solutions such as Network Security Monitoring (NSM), Security Operations Centers (SOCs), Daily Reports Trend Analysis, and so forth. The solution focuses mainly on day-to-day operations activities with very short perspectives and timeframes.

Event detail is not needed for this system and data can be aged to provide less granularity as the data ages. This approach provides the best use of database space while retaining the metrics needed for demonstrating ROI.

Chapter 3: Understanding SIM Structure in Typical Scenarios

This section contains the following topics:

eTrust Audit and eTrust Security Command Center in Basic Scenarios

This section helps you understand how eTrust Audit and eTrust Security Command Center work together to enable SIM solutions in the following scenarios:

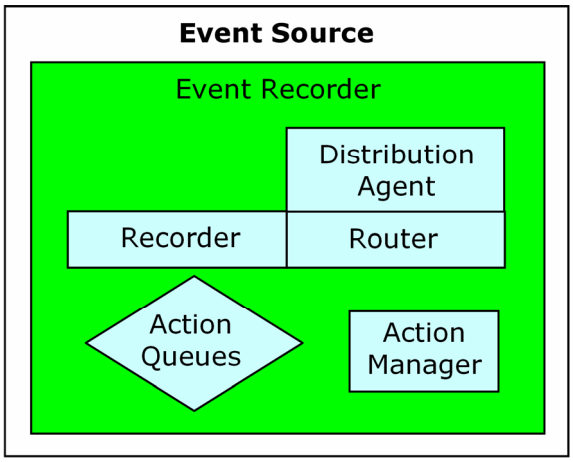
- Central data collection
- Reporting and compliance
- Status monitoring and alerts

Basic eTrust SIM implementations start with event recorders that capture events from event sources, which can include a variety of devices or applications. Typically a device or application has installed on it, or with it, an eTrust Audit Client, a SAPI Recorder, or an iRecorder, collectively referred to as event recorders. You can also install only the recorder component on an unmanaged event source, and have the eTrust Audit client installed on a remote computer. In this case, events flow from the recorder to the client for further processing. The eTrust Audit client contains other components described later in this section.

A recorder is essentially a log, file, and data reader that captures events and sends them to a router and action manager for handling. For example, a UNIX server generates events that are stored in log files by the syslog daemon. If you install an eTrust Audit client on the UNIX server, the eTrust Audit syslog recorder captures the events from the log files and forwards them to the other client components for processing.

How Captured Events Are Processed

Captured events follow a specific path as they are processed. Understanding this path is important to understanding how your SIM solution works, and how to plan for and configure it. The following illustration shows the basic eTrust Audit client components installed on an event source:

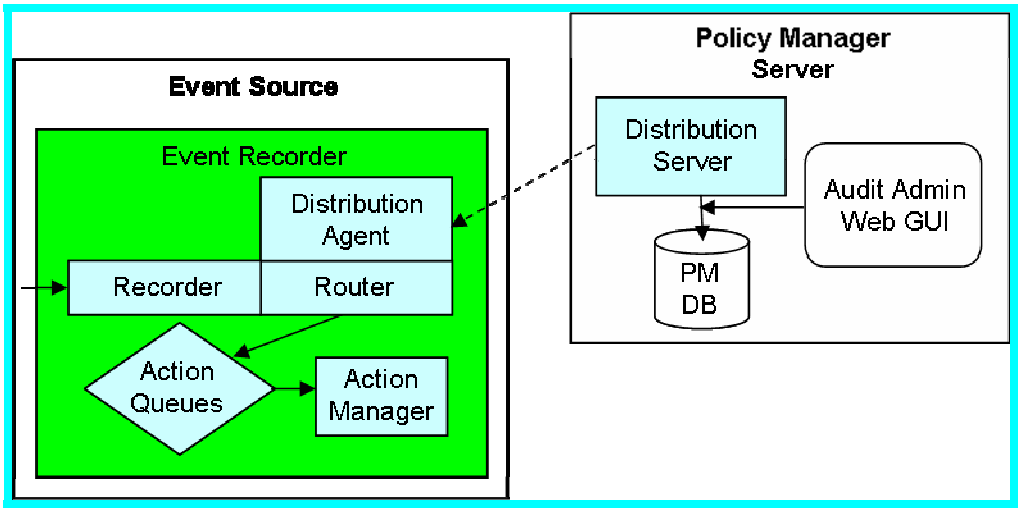


The eTrust Audit client is installed on an event source (in green) and contains routing and filtering components (shown in blue).

Within the client, events generated by a server or device are picked up by proprietary event recorders. Events are processed according to policies that you create, distribute, and manage from a central policy manager server. A policy tells the router which events to process. No events are processed further by a router until you define *and* distribute a policy.

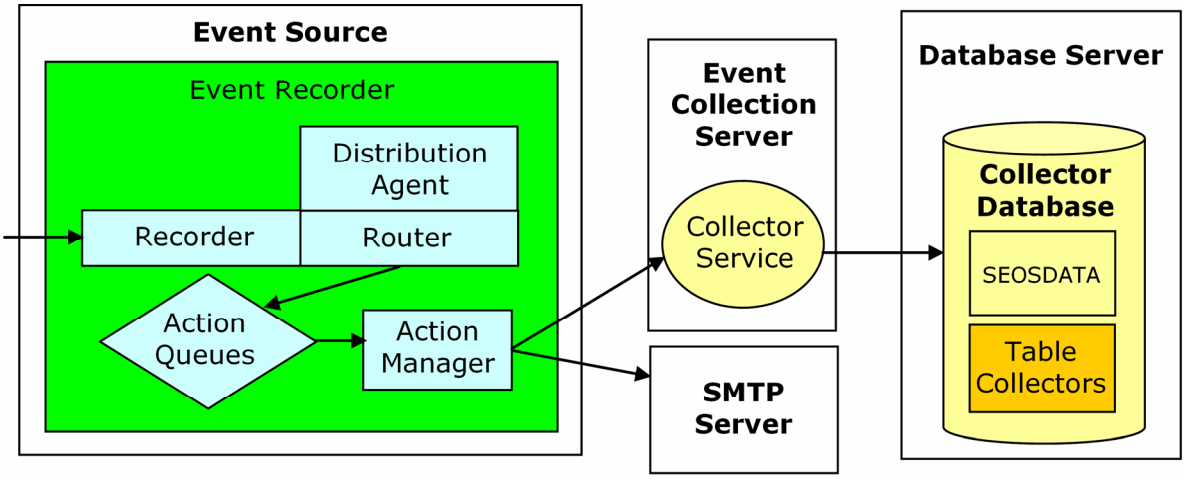
A router component sends the event to a series of action queues based on the policies defined in and distributed by the policy manager for processing. The action manager performs the actions as defined by the rules that were matched in the router and manages the flow of events from the queues.

The following illustration shows the event flow through the client and the control flow from the policy manager server. Solid lines depict event flow, while dashed lines show control flow.



Each client has its own distribution agent for receiving policies from the policy manager's distribution server component. This arrangement lets the policy manager server function as a single point of control for policy distribution to both individual clients and client groups. The policy manager has its own internal database, and there is also a separate interface for creating and distributing policies.

During production, the action manager can send events to several possible locations based on the policies you define. The destinations can include SMTP servers, SNMP traps, a file, or other applications including Security Management. The following illustration shows a very simple arrangement of components that provide for event flows to an event collection server, and then to a central Collector database. Events designated as alerts can also flow to an SMTP mail server for email notifications.



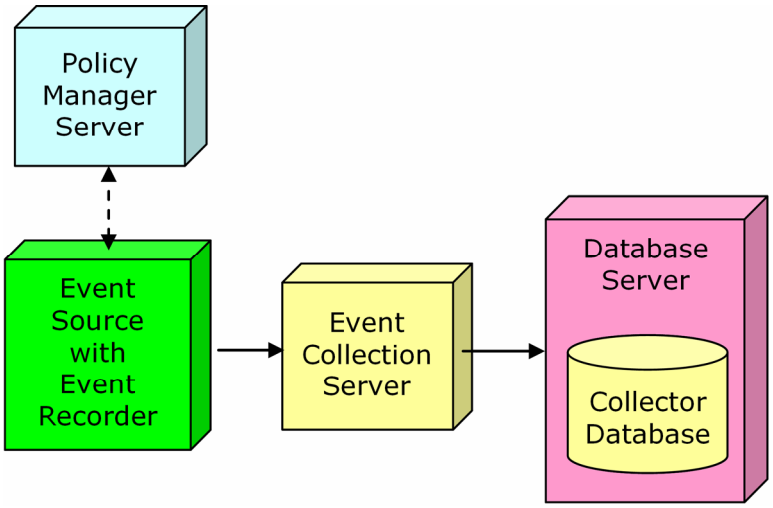
This illustration, combined with the policy manager components in the previous diagram, describes the essential components in a central data collection scenario. SIM solutions with very high event volumes that use a central database to store events may benefit from having more than one event collection server defined. Each event collection server transports events to the dedicated database server, sharing the load and increasing throughput.

In the Collector database, the primary database table is called SEOSDATA. Higher volume SIM implementations, and solutions that focus on reporting, will also benefit from the use of table collectors, a feature of eTrust Security Command Center. Table collectors are shown in this illustration as an orange color within the collector database. You can read more about table collectors in the section on Database Planning (see page 36).

Some of the scenarios make use of additional features of both eTrust Audit and eTrust Security Command Center for specific SIM needs. The additions can include the use of separate computers for filtering and displaying events, monitoring security in near real-time, sending events to an SMTP server for email notifications, and other management functions. The additions may also include the installation of specific components from both products on the same server.

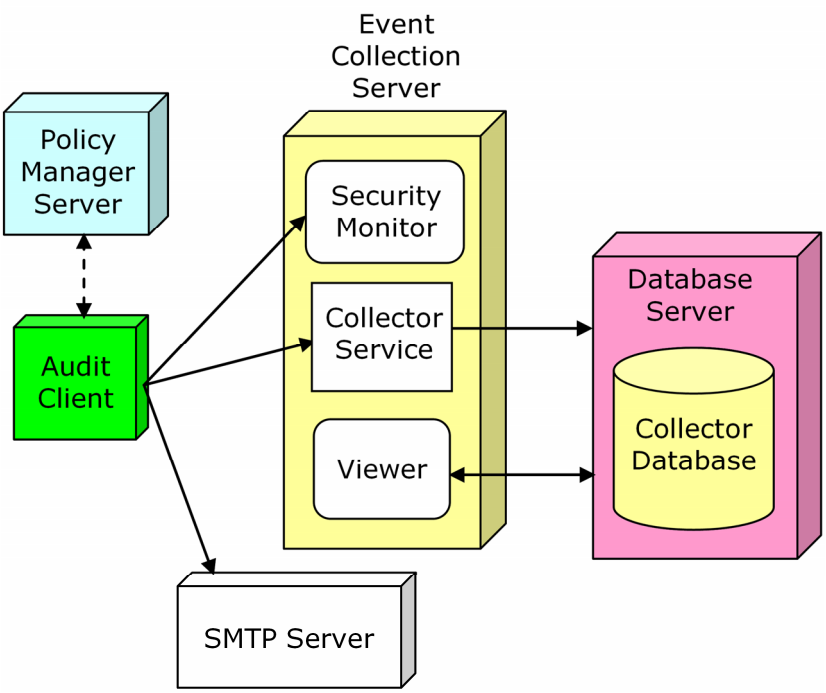
Enabling Central Data Collection

Almost all SIM solutions use central data collection as an integral part of the functionality. The eTrust Audit product provides almost all of the functionality for this solution. A very simple SIM solution contains a policy manager server for control, one or more event sources (eTrust Audit clients), an event collection server, a database server, and a central Collector database.



The database (DBMS) should be located on a dedicated server. The separate event collection server supports a Collector service and other data tools. Separation of these two machines provides better performance. For very large networks with high event volumes, a storage network array such as a Storage Area Network (SAN) may be a better alternative for event storage.

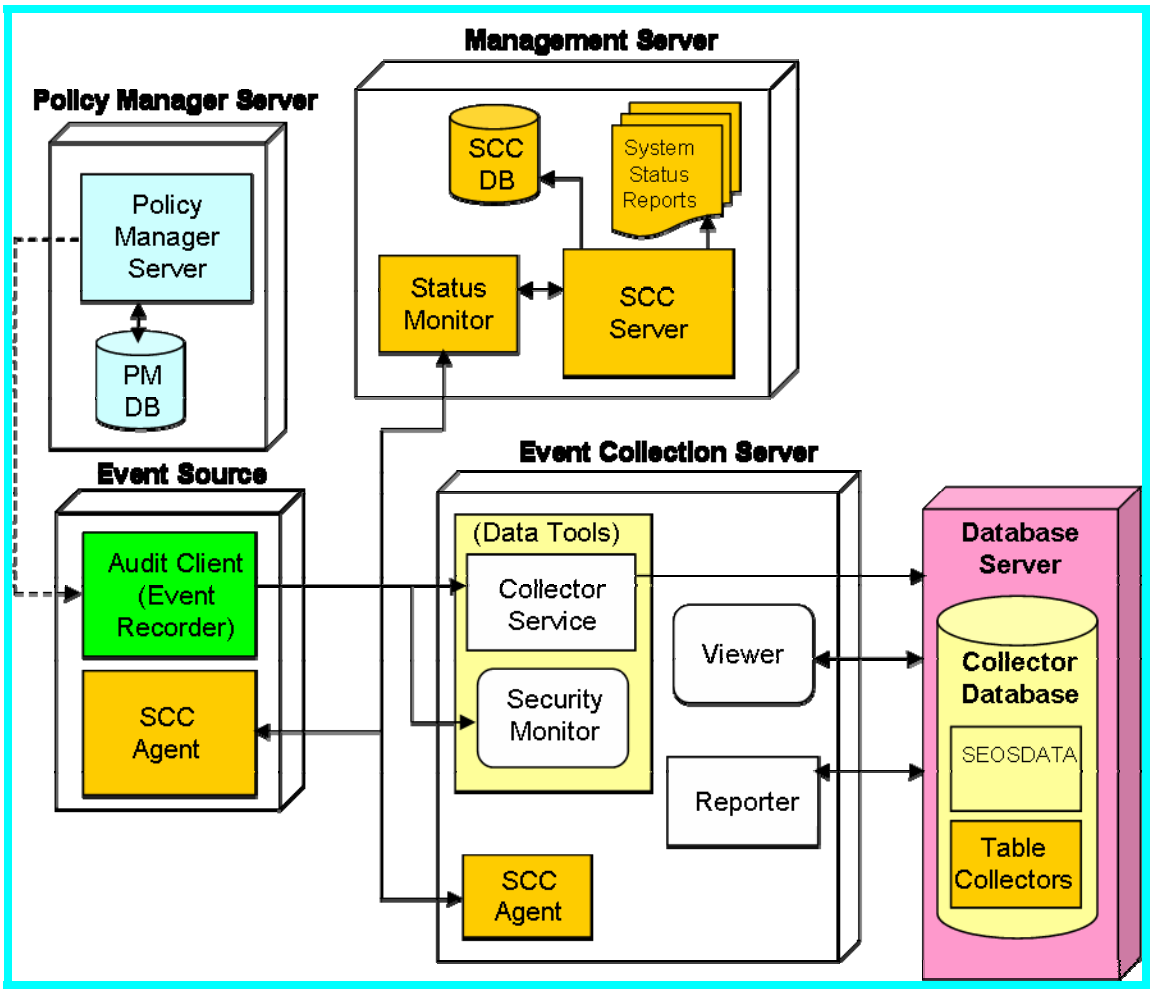
While this SIM solution is workable, events flow only to a central database, and there is no capability to monitor particularly severe events or see specific types of events as they occur. A more realistic central data collection solution appears in the following illustration:



The viewer provides a way to filter events in the database as needed. The security monitor allows you to designate which events you need to see in near real time, and monitor the status of eTrust Audit itself. The Collector service and security monitor are part of the eTrust Audit Data Tools installation package. The viewer is part of its own installation package. The policy manager and the eTrust Audit clients are also in separate installation packages. The Data Tools (yellow), Policy Manager (blue), and eTrust Audit client components (green) comprise the eTrust Audit *core* components.

Creating a Reporting and Compliance Solution

Building upon the central data collection scenario, additional functionality in eTrust Audit and eTrust Security Command Center adds reporting and additional management layers. The illustration below shows the additional functionality used to support a reporting and compliance solution:



The illustration shows separate servers for the Policy Manager and the SCC Server components. Since the SCC Server resides only on Windows servers, the UNIX Policy Manager must reside on a separate server.

However, the policy manager server has a relatively low throughput, so you can install the SCC Server component on the same physical computer, if you are using the Windows platform. This effectively creates a single management server for administering the SIM solution, allowing both policy distribution and use of the SCC Server's management functions from a single point. The additional functionality provided by SCC is shown in orange in this illustration.

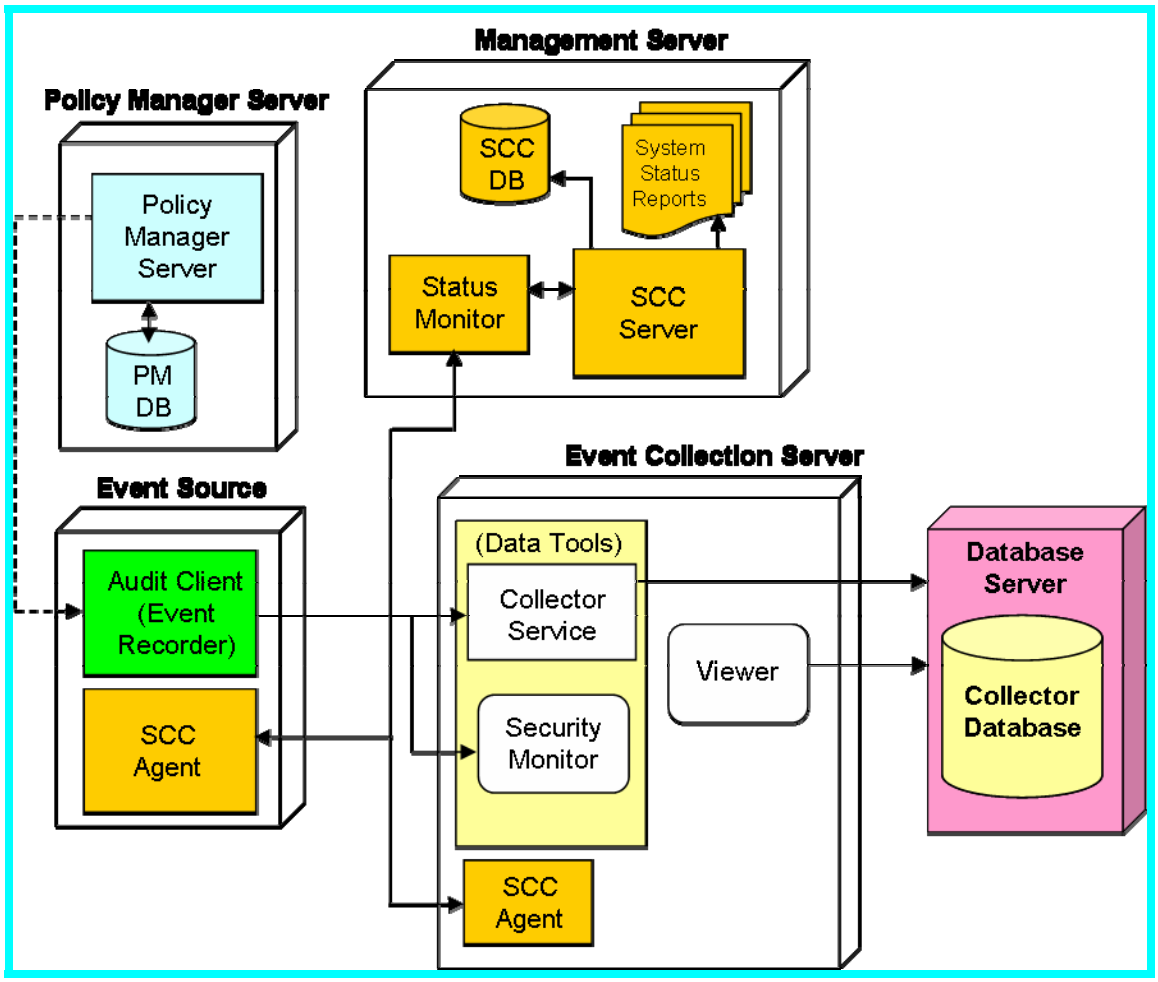
The SCC Server offers web-based integration with CA and third-party security application's event data, administration, and reporting tools. It also provides a status monitoring interface for analysis of critical processes running on the application servers. Through the use of SCC agents, the SCC Server's status monitor discovers and monitors services, processes, and daemons running on your product servers. It lets you create customized views of the security status in your enterprise. You can organize these views by application or by area of responsibility. For example, you can also create high-level status views for your Chief Executive Officer or Chief Security Officer. Drill-down capabilities provide them with access to the details, if and when they need them. You can create extremely detailed views for the security administrators who need immediate access to detailed status of the security enterprise.

Also as part of the SCC Server functionality, the SCC log viewer provides web-based access to event data using role-related views. As a web-based viewer, the log viewer component completes the ability to provide a single point of web-based access to your security enterprise. Filtered views of event data are also available from the event collection server, where the eTrust Audit viewer allows near real-time monitoring of events. The reporter, which also exists on the event collection server, lets you gather data from the collector database. This lets you create reports as required by a number of compliance regulations.

The SCC Server also maintains a small database for its internal operations. You must plan for and install this Microsoft SQL Server database as part of the SCC Server installation.

Enabling Status Monitoring and Alerts

Building upon the central data collection scenario, this SIM solution focuses more on the near real-time tracking of events and trends than on producing reports. While the reporting functions in eTrust Audit and eTrust Security Command Center are still available for use, they are not shown in the following illustration.



The policy manager server provides control over event processing through policies you create and distribute with the policy manager, as in other scenarios. On the management server, the SCC Server's web-based integration, status monitoring interface, and log viewer allow near real time monitoring of events, services, processes, and daemons running on your product servers. Since the SCC server is supported only on Windows platforms, the policy manager and SCC server components can reside on the same Windows server, if desired.

You can use role-related visualizations and filters to tailor your views of the security status and events in your enterprise. You can organize these views by application or by area of responsibility. This permits you to review different levels of event severity in different ways, or by different people, based upon their roles in the organization.

You can configure specific types of events as alerts for routing to SMTP servers, security monitor consoles, event viewers, or to table collectors in the collector database for recent trend and pattern analysis. Being able to display, sort, and filter events from the collector database allows you to review certain types of events as needed.

Chapter 4: Planning Your SIM Implementation

This section contains the following topics:

Introduction

Implementation planning for a SIM solution involves the following areas:

- Pre-installation considerations
- Database planning
- Network management planning

Having a current network topology helps you understand where the event nodes are located in relation to the eTrust Audit and eTrust Security Command Center components. Data must flow from the event sources through the event recorders to various destinations for later storage, viewing, or analysis. All data flows using the TCP and UDP protocols. You must modify any routers/firewalls that are between systems to support the data communication between systems.

If CA Technical Services assists with your implementation, the following documents may be available from your CA TS representative to support the development of your deployment plan:

- An architecture overview helps you understand the business drivers that instigated the implementation of the SIM solution, and to navigate the current security architecture.
- The results from the events-per-day volume analysis helps you define the size of the Collector database, and helps you to understand the critical nature of a properly configured database.
- The architecture specification defines in detail the security devices to be connected during the implementation. Additionally, this document should have enough information about the stakeholders for the successful implementation of the SIM solution.

Pre-installation Considerations

There are several guidelines to follow as you consider the various possible deployment options for eTrust Security Command Center. The installation steps vary by environment. You should consider carefully the information in the following sections:

- Available environments
- Prerequisites

Available Environments

You can install eTrust Audit and eTrust Security Command Center components according to the following table:

	Windows	UNIX	Linux
eTrust Audit Client	Yes	Yes	Yes
eTrust Audit Data Tools	Yes	Yes	No
eTrust AuditViewer and Reporter	Yes*	Yes* (Solaris 10 only)	No
eTrust Audit Policy Manager	Yes (Windows with MS SQL Server)	Yes (Solaris 10 with Oracle 10g only)	No
eTrust Security Command Center Server	Yes	No	No
eTrust Security Command Center Agent	Yes	Yes	Yes

* Viewer and Reporter on Windows use the Tomcat web server. Viewer and Reporter on Solaris 10 use either the Tomcat or the IBM WebSphere Application Server combines with a support Web Server.

Refer to the Readme file, or the operating system support matrix for eTrust Audit and eTrust Security Command Center on the http://supportconnect.ca.com (http://supportconnect.ca.com) website, for further details of specific operating system versions support for the product components.

Later sections of this guide describe the installation process you follow to install each of the product components. The installation process, and the available components, differs slightly for each environment.

Prerequisites

Refer to the Readme file, or the operating system support matrix for eTrust Audit and eTrust Security Command Center on the http://supportconnect.ca.com (http://supportconnect.ca.com) web site, for the latest system hardware and software requirements and a list of supported operating systems for each product component.

DVD-ROM Access

You will need access to a DVD-ROM reader as the installation media is available only on DVD. If a DVD-ROM reader is not available on the computer, then you need access to a network share of the installation media.

Install a Collector Database

You should install an underlying Oracle or Microsoft SQL Server collector database before installing the eTrust Audit or eTrust Security Command Center components. Instructions are provided in Installing Databases (see page 57).

When you use Microsoft SQL Server as your collector database, the eTrust Audit Data Tools create specific database tables for you as you install the components. Installation of the Data Tools for an Oracle database on Windows systems also creates specific database tables. If you use an Oracle database on UNIX systems, you must create these tables manually.

Event Log Access

You need access to the following areas and their related event logs:

- Administrator access to the computers that will have software installed
- Remote access to all remote computers
- Firewall administrator access (if there are firewalls between the components that need to be reconfigured, or if the firewalls will be event sources)
- Access to the event logs for security infrastructure devices and operating systems
- Access to the databases to be included in the implementation

Database Planning

The success of Security Information Management systems depends on database planning. The key factor for database planning is performance. Database size has the most profound effect on performance, and is affected directly by the number of events collected. You must decide what information you need to keep and what you can discard. That information, coupled with an accurate event volume analysis, helps you determine database size and tuning requirements, and thus performance. Organizations only rarely need to keep every event generated in the network. By carefully tailoring the amount of data kept, along with the maximum record size, you can create an effective SIM solution with reasonable storage needs.

You should allocate a dedicated event database server. This improves performance and provides a central point of management for the database. Minimum memory requirements for efficient operation vary by DMBS type and operating system, but generally are a minimum of 2 GB of RAM.

SIM solutions generally become one of the three largest databases in a company, so you should plan accordingly. For larger companies, start with plans for a 100 GB to 1 TB database. For smaller companies, plan for a 10 GB to 25 GB database, depending on your retention needs. If you need longer retention times, increase the size of the database.

Database Size

The following are the primary factors that affect database size:

- Event size
- Number of events
- Retention rate, including backup and recovery and how data is stored (RAID scheme)
- Number of table collectors

UDP packet-size limits reduce the maximum record size for an event to 8 KB. However, you do not have to plan for a record size that large. Using a smaller record size means that you know the average size, in bytes, of the event messages that you intend to log. The record sizes you select for table collector columns must be large enough to contain the largest fields date for the specific events that will be contained in that table collector. You also need to know the approximate number of events-per-second at peak times. At 8 KB per event with high event volumes, database sizes can become large very quickly.

CA Technical Services can provide a detailed Events Per Day (EPD) volume analysis to use as a basis for database planning and strategy. Event volume analysis is critical to proper database planning, and should be measured and verified carefully. Proper planning increases initial success and saves both time and money during implementation.

For event retention, you can configure your databases to grow in specifically measured amounts or as a percentage of the overall database. Be careful when using growth by percentage, as the newly-allocated amount may exceed your disk capacity if the database is already large. For example, 10% of 200 MB is not large when compared to 10% of 500 GB.

The recommended RAID Scheme is RAID 0+1, as this provides the best performance as well as fault tolerance.

Supported DBMS License Level

It is recommended that you use the Enterprise versions of the Oracle or Microsoft SQL Server DBMS products for your collector database. The enterprise versions offer advanced features you can use to tailor the performance of your SIM solution. These features include database partitioning, replication, and other tuning techniques. Event volume is the driver for decisions regarding the use of these features. As event volume increases, so too should the number of collector databases and the number of database partitions.

Basic Tuning

In general, the SEOSDATA table in the collector database is tuned for INSERT operations. Databases may have different tuning parameters and features. At a certain level, tuning for insert means not creating indexes (or at least large numbers of indexes). You should use table collectors for reporting. Create additional indexes for them as required by your reporting needs.

Be sure that you do not exceed the physical memory on the computer, or the database will have to begin swapping memory to disk. This decreases the performance of the system. While this may seem elementary, in production, large network environments can produce enormous amounts of information.

Some additional temporary space helps the eTrust Audit application run more efficiently.

DBMS Type	Initial Temporary Database Space
Oracle databases	250 MB
Microsoft SQL Server databases	1 MB

You should plan for 10% of the total database size as temporary database space. SELECT statements executed against the collector database use the temporary database space to build the temporary return set. The faster the disk allocated for the temporary database space, the faster will be the performance of SELECT statements.

In some cases you can turn off the DBMS Rollback feature, since you are tuning the database to facilitate INSERT operations, but this requires use of a tool such as CA Brightstor® ARCserve® Backup to do regular backups of the database.

Database Backup and Recovery

You should purchase and use an application for database backup and recovery like CA Brightstor® ARCserve® Backup.

Your backup plan should include the collector database and any table collectors you define, as well as the portal database that supports the Server, and the CA Common Services database used by the eTrust Security Command Center status monitor. The CA Common Services database is installed when you install the SCC Server.

It may not always be possible to do a cold backup (where the database is shut down during backup operation). Hot backups are generally automated to allow efficiency in handling backup in sections of the database while maintaining data integrity. Hot backups include processing tablespaces, data files, archived re-do logs, and the control file depending upon your selected database type.

Database Performance

Evolving SIM systems require storage of larger numbers of events and longer event retention rates. To support these larger implementations, the first step in implementing a solution is to define and configure a database solution to store the events.

You can use several strategies and techniques to increase performance of the database. These techniques include the following:

- Using table collectors, whenever possible
- Partitioning the SEOSDATA table, as well as any defined table collectors
- Separating data storage areas for the SEOSDATA table and any defined table collectors
- Using a pruning strategy that allows for minimal data within the SEOSDATA table, and using table collectors as the mechanism of choice to store the relevant events
- Supporting growth through adequate hardware. For larger databases, you should also ensure that proper hard drive speed is allocated.

Using Table Collectors

Within eTrust Security Command Center, a database construct known as table collectors allows for the ability to store events from devices selectively and in a more tabular method. The use of table collectors accomplishes the following:

- Reduces the storage size of an event

  You can define each table collector to save only a portion of the original event. This can significantly reduce the storage requirements of the system.

- Allows for the quicker retrieval and select using SQL

  Each table collector defines each event field as a column. Thus, allowing for the indexing and retrieval of the data through SQL. This ability can significantly increase the speed of reporting.

Adequate segmentation of data using table collectors could remove the need of further segmentation using partitions.

Database Partitioning

A partition is a division of a logical database or its constituent elements into distinct independent parts. Typically partitioning is performed on tables within a database. Database partitioning is normally done for manageability, performance or availability reasons.

Partitioning allows a table, index, or index-organized table to be subdivided into smaller pieces. Each piece, or database object, is called a partition. Each partition has its own name, and may optionally have its own storage characteristics, such as having table compression enabled or being stored in different tablespaces (filegroups). From the perspective of a database administrator, a partitioned object has multiple pieces which can be managed either collectively or individually. This gives the administrator considerable flexibility in managing partitioned objects. However, from the perspective of the application, a partitioned table is identical to a non-partitioned table. No modifications are necessary when accessing a partitioned table using SQL commands.

Partitioning improves management, performance, and availability of data in a database and simplifies common administration tasks. Partitioning is a key tool for building multi-terabyte systems or systems with extremely high availability requirements.

We recommend that CA Technical Services assist with your volume analysis and database configuration, if you intend to use partitioning.

Performance Partitioning

By limiting the amount of data to be examined or operated on, and by enabling parallel execution, the partitioning option provides a number of performance benefits. These features include the following:

Partitioning Pruning

Partitioning pruning is the simplest and the most substantial means of improving performance using partitioning. Partition pruning can improve query performance significantly. For example, suppose that the collector database SEOSDATA table grows rapidly, and that this table has been partitioned by day. A query requesting events for a single day accesses only a single partition of the SEOSDATA table. If the SEOSDATA table had 20 days of historical data, this query would access one partition instead of 20 partitions. This query could potentially execute 20x faster as a result of partition-pruning.

Partition-wise Joins

Partitioning can also improve the performance of multi-table joins by using a technique known as partition-wise join. Partition-wise joins can be applied when two tables are being joined together, and both of these tables are partitioned on the join key. Partition-wise joins breaks a large table join into smaller joins that occur between each of the partitions, completing the overall join in less time. This offers significant performance benefits both for serial and parallel execution.

Separating Data Stores

In conjunction with partitioning, splitting storage of the data across physical disk drives improves performance. Each database management system has its own construct for implementing this technique. Within the Microsoft SQL Server DBMS, this construct is called FileGroups. For the Oracle DBMS, this construct is called TableSpaces. Although the two implementation differ slightly, the theory behind the technique is the same.

Both tablespaces and FileGroups are logical groupings of data files. Each construct is created so that you can assign a table, such as the SEOSDATA table, to a logical group. The DBMS then manages the storage of data within the operating system. A majority of the operating systems supported by both DBMS systems use files as the storage mechanism. The DBMS associates the logical constructs with the physical constructs of a file.

Additionally, you can attain a significant improvement in performance by physically separating data objects such as tables and indexes on disparate physical devices. You may realize a performance gain by separating indexes from tables and reading both objects in parallel.

Using a Pruning Strategy

One effective pruning strategy uses table collectors, and makes very little use of the SEOSDATA table. The strategy includes the following:

- Store as little data as required in the SEOSDATA table, and prune it often.
- Store as much data as required in the table collectors. Use the table collectors for reports, log viewers, and any other required visualizations.

Events stored in the SEOSDATA table typically increase the native event size by several times. If the SEOSDATA table usage is carefully controlled, the storage requirements are greatly reduced. The record size of the events within the table collectors are typically only 10% greater than the original event size and are easily gathered using standard SQL statements.

Supporting Database Growth

For data collection, hard drive types and speeds can affect performance of the overall system. The faster the hard drives spin the faster information can be retrieved. The tables that follow provide a general look at drive type, speed and throughput.

Bus Type	Speed
IDE/EIDE	15 MB/sec
SATA	150 MB/sec
SCSI-3 U160	160 MB/sec
SCSI-3 U320	320 MB/sec
FibreChannel	1 - 2 GB/sec

Hard Drive Speed	Throughput
5400 RPM	8-10 MB/sec
7200 RPM	10-16 MB/sec
10,000 RPM	20-25 MB/sec
15,000 RPM	30-35 MB/sec

Note: These speeds are based on U320 SCSI hard drives. The actual speeds you experience may vary.

If you were to use an array of 144 GB, 7200 RPM SATA drives for a 1 TB database, the speed of the hard drives and controller would limit throughput performance. Hardware striping can help improve performance, but only to a point. Even with the SCSI-3 U320 drives, you would need a total of ten 15K RPM drives in a strip to meet the theoretical maximum performance.

A recommended configuration includes SCSI-3 U320 controllers, or FibreChannel, with hard disks of 72 GB maximum size, and 10-15K RPM speed. This should ensure enough physical drives to provide good performance for larger databases, 1 TB and above.

Generally, a disk array that has a larger number of smaller and faster drives delivers higher performance.

Database Planning Worksheet

Print and complete the worksheets that follow during the installation activities detailed in the section on Installing Databases (see page 57). These worksheets help you create a record of the login information for the collector and portal databases. You will need this information later during installation of the eTrust Audit and eTrust Security Command Center components.

Collector Database	
Oracle Home Path	
Database Name	
Computer Name (or IP Address)	
Database User Name (Login ID)	
Password	
Login Account for Data Tools (write access)	
Password	
2nd Login Account for Data Tools (read-only; recommended for use by Reporter and Viewer)	
Password	

Collector Database
Notes

Note: A standard collector database name is auditdb. Do *not* use SEOSDATA or audit as database names. A standard database user name is auditdba.

Policy Manager Database
Oracle Home Path
Database Service ID (SID) or Remote Service Name
User Name
Password
Host Name
Notes

Note: A typical Policy Manager database name is policy_db.

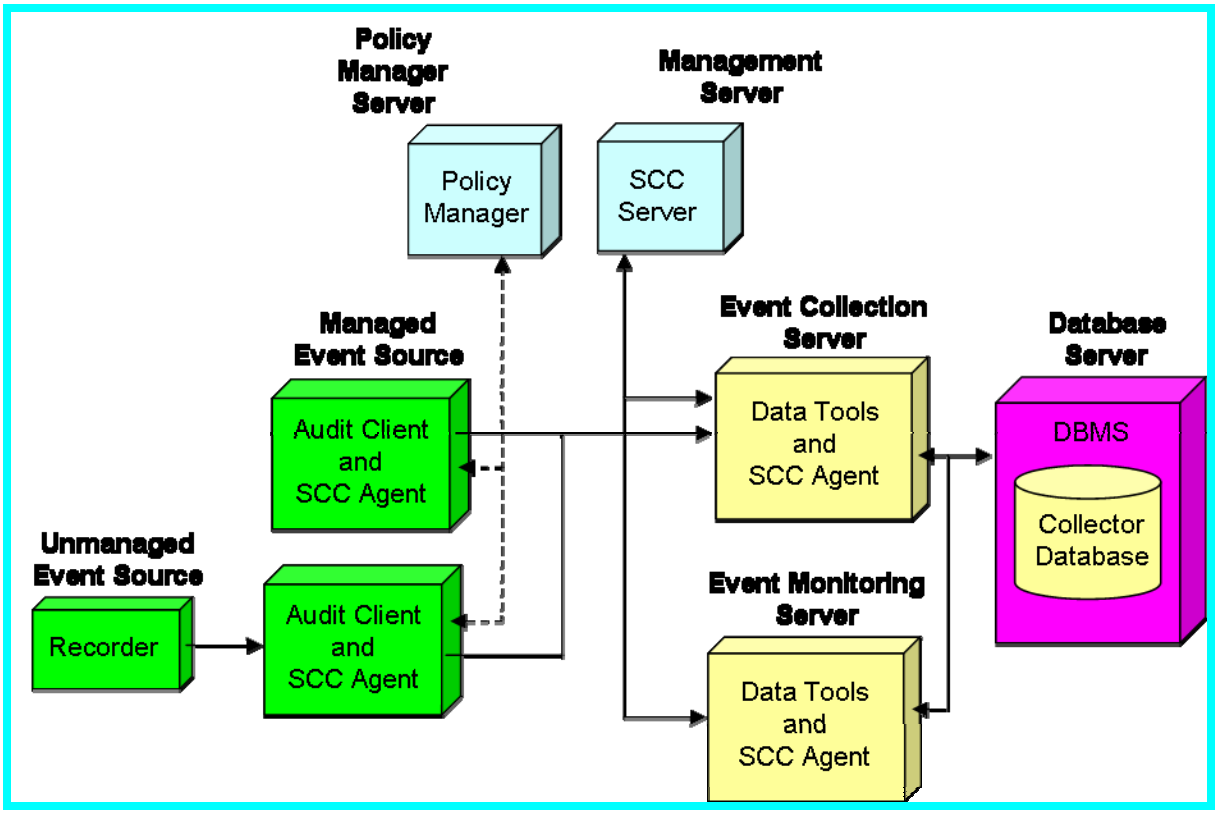
SCC Portal Database	
Computer Name (or IP Address)	
sa Password	
Portal Database Name	
Portal Database User Name (Login ID)	
Portal Database User Password	

Notes

Notes: A standard SCC portal database name is portaldb. A standard database user name and password are portaldba. The sa password is required for the CA Common Services portion of the installation, and is not used after the installation is complete.

Network Management Planning

Managing your SIM solution effectively and efficiently requires a certain number of computers to act as servers for data and routing. The following illustration shows a typical SIM solution network:



Typically there are many different event sources, both managed and unmanaged. A managed event source has client components installed and processes events using policies from the Policy Manager. If you are using eTrust Security Command Center, you can also install an SCC Agent on the managed event source to gather operational status information.

Dashed lines in the figure represent control flow between the Policy Manager and the managed event sources. This control flow includes distribution and enforcement of policies and MP files for the capture of event data.

Management Server

The SCC agent's presence allows the SCC Server to collect information about the status of the application or device through the status monitor.

If you are using the Policy Manager for Windows operating systems, both the policy manager and SCC Server can reside on the same physical server, called a management server.

If you are using the Policy Manager for UNIX operating systems, the Policy Manager can reside only on a UNIX server running the Solaris 10 operating system. In this case, the Policy Manager and the SCC Server reside on separate physical servers.

Event Collection Server

To increase the throughput of data to the database server, allocate a separate event collection server. The Collector service on the event collection server points to the database server, which then handles I/O on the storage devices. The event collection server typically hosts the Collector service from the eTrust Audit Data Tools, and the Data Tools interface itself.

An additional event server, called an event monitoring server, may also be useful in SIM solutions focused on reporting or status gathering. While the event monitoring server has the same software products on it as the event collection server, its primary function is gather information for reporting, and to provide viewer and security monitor access to event data.

In this way, the performance of the event collection server is not compromised by the additional processing related to reporting. Each of these event servers has an SCC agent installed for status monitoring, event viewing, and support of table collectors through the SCC Server.

Multiple Event Collection Servers

Systems that experience event generation greater than 500 events per second need more than one event collection server (more than one Collector service, each on a separate server). Increasing the number of processors, using faster processors and buses, and so forth, further increases the throughput.

Database Server

The database server is a dedicated computer. While it is possible to install the Collector service and SCC Audit Interface on the database server, this is not a recommended approach. Reporting and other functions could affect the performance of the database server as it communicates with the Collector database. For this reason, we recommend that you separate the database server from other functions.

Ideally, the data component of the database should be located on a storage network array (SAN or DAS). This allows for growth of the database during heavy load. Separating the Collector database from the database server improves performance, but also means that communications occur across an ODBC connection and are not encrypted.

Network Management Planning Worksheet

Complete the worksheets that follow to create a record of the login information for the various servers that provide management and control of your SIM solution. You will need this information to access the servers for both installation and operations.

Windows Management Server

The Policy Manager for Windows uses SQL Server authentication to validate access to the Policy Manager database.

You can configure the SCC Server component to use Windows logon credentials, but this is not the default.

Management Server	
Computer Name (or IP Address)	
Password	
sa Password	
EiamAdmin password	
Policy Manager Identification String for eTrust Audit Client	
SCC Server User Name	
SCC Server Password	

Management Server
Notes

Notes:

Anyone installing an eTrust Audit Client optionally requires the Policy Manager Identification String. The clients authenticate to the Policy Manager using this string value This enables the Clients to register with the Policy Manager using this value, and automatically creates entries for these hosts in the Policy Manager database.

The EiamAdmin account ID is predefined as the default account for accessing eIAM. The password for that account is set when eIAM is installed. If eIAM is already installed in your environment, contact a system administrator to get the EiamAdmin account password. If you install eIAM as part of the Policy Manager installation, you are setting the account password during that installation. You should make a note of the password you choose in this worksheet. You must use the EiamAdmin account and password to log in to the eTrust Audit Administrator the first time so that you can configure the other user accounts that have access.

Policy Manager Server

The Policy Manager for UNIX must reside on a Solaris server. Record the server's access information in the table that follows:

Policy Manager Server
Computer Name (or IP Address)
User ID

Policy Manager Server
EiamAdmin Password
Policy Manager Identification String
Java Home
WebSphere or Tomcat Web Server path
WebSphere port number
Notes

Note: Anyone installing an eTrust Audit Client optionally requires the Policy Manager Identification String. The clients authenticate to the Policy Manager using this string value. This enables the Clients to register with the Policy Manager using this value, and automatically creates entries for these hosts in the Policy Manager database.

The EiamAdmin account should be used to log in initially to the eTrust Audit Administrator to configure the user accounts that require access.

Event Collection Server

Record the event collection server's authentication credentials here for reference during implementation. Space is provided for both Oracle and Microsoft SQL Server credentials.

Event Collection Server	
Computer Name (or IP Address)	
Password	
Microsoft SQL Server User ID	sa
Password	
Database Name	

Event Collection Server	
Oracle SID	
User ID	
Password	

Notes

Note: For SIM solutions with heavy event volumes, you may want to designate both a collection server and a monitoring server. This reduces performance issues for the Collector service when other Data Tools components are active.

Event Monitoring Server

If using an event monitoring server, record the server's authentication credentials here for reference during implementation. Users access the components you install on this server through a web interface with the user access and roles (see page 153) you create for them. Record the system administrator's credentials here for ready reference.

Event Monitoring Server	
Computer Name (or IP Address)	
Password	

Event Monitoring Server
Notes

Chapter 5: Starting the Deployment

This section contains the following topics:

Getting Started

This section describes the tasks for deploying the eTrust Audit and eTrust Security Command Center components and services based on the typical implementation scenarios described earlier in this guide. Each deployment task represents a separate set of installation steps for the product components and is covered in its own chapter.

After completing the planning phase of your product implementation, you are ready to begin your SIM solution deployment based on those results.

Before you start the deployment, you should have the following planning information available, or have clearly identified the system requirements for your particular implementation:

- Database Planning Worksheet (see page 43)
- Network Management Planning Worksheet (see page 48)

To start the deployment phase, choose one of the following typical implementation scenarios that best represents the type of working environment you are implementing:

Central Data Collection

If you are implementing a SIM solution to:

- Collect event data generated from various event sources such as CA eTrust products or third-party applications
- Route, filter, and store the event data in a central database
- Control the polices by which events are collected
- Send some events to a security monitor console or event viewer
- Use email notifications through an SMTP server

Complete steps 1-7 of the eTrust Audit deployment process.

Reporting and Compliance

If you are implementing a SIM solution to:

- Collect event data generated from various event sources such as CA eTrust products or third-party applications
- Route, filter, and store the event data in a central database
- Control the polices by which events are collected
- Send some events to a security monitor console or event viewer
- Use email notifications through an SMTP server
- Create reports on the collected event data and system status

Complete steps 1-7 of the eTrust Audit deployment process.

Status Monitoring and Alerts

If you are implementing a SIM solution to:

- Collect event data generated from various event sources such as CA eTrust products or third-party applications
- Store, route, and filter the event data in a central database for viewing and reporting
- Control the polices by which events are collected
- Monitor the real-time product status and system status
- Create more advanced views of product-specific eTrust Audit events
- View SIM system status through a status monitor console

Complete steps 1-7 in the eTrust Audit deployment, and also complete the needed steps in the eTrust Security Command Center deployment.

Note: For larger and more complex implementations with additional SIM functionality, please contact CA Technical Services for additional deployment assistance.

For more information on how these implementation scenarios relate to eTrust Audit and eTrust Security Command Center, see eTrust Audit and eTrust Security Command Center in Basic Scenarios (see page 23).

How to Deploy eTrust Audit

Install the eTrust Audit and eTrust Security Command Center components, database management systems (DBMS), and the event sources you want to track in the order listed below.

Note: If earlier versions of eTrust Audit or eTrust Security Command Center are already installed, you must perform an upgrade installation. For more information, see Upgrading from a Previous Release (see page 257).

As a prerequisite, you must have some event sources already operational in your network, prior to installing the components of your SIM solution.

1. Install and configure the databases for your SIM solution. See Installing Databases (see page 57).

   Choose and install a DBMS on the database server before installing the eTrust Audit Data Tools.

   Install the Microsoft SQL Server DBMS on the management server, if you are using eTrust Security Command Center.

2. Install the eTrust Audit Data Tools. See Installing Data Tools (see page 73).
3. Install the eTrust Audit Policy Manager on the management server or on a separate Policy Manager server. See Installing Policy Manager (see page 85).
4. Install the eTrust Audit Reporter and Viewer on the desired server. See Installing Reporter and Viewer (see page 97).
5. Install eTrust Audit Clients on event sources. See Installing Clients and Event Recorders (see page 109).
6. Install the eTrust Audit event recorders on event sources. See Installing Clients and Event Recorders (see page 109).
7. Test your configuration using the steps in the section, Ensuring Your Environment is Operational (see page 149).

Note: Two utilities are provided, acstat and acreminfo, that can help you determine the status of your installation. More information about these utilities is available in the *Reference Guide*.

How to Deploy eTrust Security Command Center

Install the eTrust Security Command Center components, database management systems (DBMS), and the event sources you want to track in the order listed below.

Note: If earlier versions of eTrust Security Command Center are already installed, you must perform an upgrade installation. For more information, see Upgrading from a Previous Release (see page 257).

As a prerequisite, you must have eTrust Audit already operational in your network, prior to installing the eTrust Security Command Center components.

1. Install the eTrust Security Command Center Server components on the management server. See Installing eTrust Security Command Center (see page 197).
2. Install the eTrust Security Command Center server-side Product Integration Kits (PIKs) on the management server. See Installing eTrust Security Command Center (see page 197).
3. Install the eTrust Security Command Center Agent components on the event sources. See Install the Agent Components on Windows (see page 205) or Installing eTrust Security Command Center Agents on UNIX or Linux (see page 211).
4. Install eTrust Security Command Center agent-side PIKs on the event sources, see Install the PIK Agent Components on Windows (see page 207) or How to Install Agent Components on UNIX or Linux (eTrust Security Command Center) (see page 212).

Chapter 6: Installing Databases

This section contains the following topics:

Introduction

Installing and configuring the required databases (see page 55) is the first deployment step for your SIM solution. eTrust Audit and eTrust Security Command Center use the following databases:

- Collector database
- Policy Manager database
- SCC Server portal database
- CA Common Services Database

Collector Database

To get started installing databases for your SIM solution, choose the DBMS you want to use to manage the eTrust Audit Collector database and install it on a dedicated database server. Print the Database Planning Worksheet (see page 43) to use while you configure your databases. Make careful notes about the database names, user names, and passwords you create. You will use these names and passwords later when you install other components.

You should refer to the certification matrix on the SupportConnect website for additional details on OS and database support as the version information is dependent on which platforms are in use, and other factors. Generally, eTrust Audit supports the following databases:

OS Version	Supported DBMS
Windows 2000, XP, 2003	Microsoft SQL Server 2000 SP4
	Microsoft SQL Server 2005
	Oracle 9i
	Oracle 10g

OS Version	Supported DBMS
UNIX (Solaris, AIX, and HP)	Oracle 9i
	Oracle 10g

You must purchase your own licensed copy of the Microsoft SQL Server or Oracle DBMS. We recommend the Enterprise versions so that you can make use of advanced features. For information about installing the Microsoft SQL Server or Oracle DBMS, see your vendor's installation documentation.

eTrust Audit Policy Manager Database

The eTrust Audit Policy Manager for UNIX platforms (Solaris 10 only) uses an Oracle 10g database. You must install the Oracle DBMS and create a new database before installing the Policy Manager. If you are migrating an existing policy manager database into the new Oracle database, a script provided with the software creates the tables (tablespaces) and a separate migration tool populates them for you.

The (Aud) Policy Manager for Windows platforms uses a Microsoft SQL Server 2000 SP4 or Microsoft SQL Server 2005 database. You must install the Microsoft SQL Server DBMS. The Policy Manager installation creates a new policy database before installing the components, or migrates an existing policy manager database into the new Microsoft SQL Server database, if Policy Manager was previously installed.

eTrust Security Command Center Server Portal Database

You must also install the Microsoft SQL Server 2000 DBMS on the management server to manage the SCC Server's portal database, if you are using eTrust Security Command Center. Fill out the Database Planning Worksheet with the database name, user name, and password for later use during eTrust Security Command Center installation.

CA Common Services Database

When you install the SCC Server, the installation process creates a small MS SQL Server database to contain the status monitor messages received from SCC agents as well as the node definitions and their current status.

Prepare Microsoft SQL Server for eTrust Audit

You must perform the following tasks to configure a Microsoft SQL Server database as the Collector database:

- Verify that the database server meets at least the minimum hardware and memory requirements. For additional information, see Database Planning (see page 36).
- Ensure that the Microsoft SQL Server DBMS is installed on the database server. The Collector database resides on this computer unless you are using a storage network array. For information about installing the Microsoft SQL Server DBMS, see the applicable Microsoft documentation.
- Create a Collector database. The procedures vary by DBMS type, and are described later in this section.
- Create a user account (user name and password) to access the Collector database.

Configure Microsoft SQL Server

The steps that follow are not the only steps in the DBMS installation. The steps in this procedure contain parameters for the DBMS needed by eTrust Audit for the Collector database. For specific details about installing the Microsoft SQL Server DBMS, refer to the product specific documentation.

To configure Microsoft SQL Server for eTrust Audit

1. Log in to the database server using administrator-level credentials.
2. Install the Microsoft SQL Server DBMS using the Custom installation type.
3. Set the authentication mode to Mixed Mode.

   The eTrust Audit Data Tools component connects to the eTrust Audit Collector database using a separate login account with SQL Server authentication mode.
4. Specify a password for the sa login.

   Record the password in the Database Planning Worksheet for later use during the eTrust Audit and eTrust Security Command Center installations.
5. Specify the option, Dictionary order, case-insensitive, for use with 1252 Character Set, in the Collation Settings window.

   While the Collector database supports both case-sensitivity and case-insensitivity, you may find slightly faster performance in some areas using the case-insensitive option.

Note: Depending on your SIM implementation, you may also use the Microsoft SQL Server database to support the eTrust Security Command Center Server databases. You must specifically configure these databases during eTrust Security Command Center deployment. For information about configuring databases for eTrust Security Command Center, see Configure Microsoft SQL Server for eTrust Security Command Center (see page 70).

Create the Collector Database

To create the Collector database in Microsoft SQL Server

1. Start the Microsoft SQL Server Enterprise Manager and expand to the Databases node.
2. Create a new database. You can use any name for the database except audit or SEOSDATA. A common database name is auditdb.

   Do *not* use the default MASTER database.

   The Data Tools installation creates the main database table, named SEOSDATA, and other required tables for you.
3. Set the desired database size and growth characteristics in the Data Files tab.
4. After the database is created, create additional login accounts for the database.

Create Login Accounts

To create user accounts to access the Collector database, use the following guidelines:

- Create a Microsoft SQL Server login account for the Data Tools to access the Collector database.

  The login account must use Microsoft SQL Server authentication. The Collector database you create should be the default database for the login account.

  Note: Make a note of this user name and password for use during the eTrust Audit Data Tools installation.
- Choose the following minimum database roles for the login account, if the account is to be used by the eTrust Audit Collector and eTrust Audit Post-Collection Utility components with write access:
  - public
  - db_owner
- Choose the following database roles to create a separate login account for exclusive use by the eTrust Audit Viewer and eTrust Audit Reporter, if you plan to install them separately. Both components only read from the database and therefore need fewer privileges to access the database than the eTrust Audit Collector and Post-Collection Utility.
  - public
  - db_datareader

How to Prepare Oracle Databases for eTrust Audit

You can use an Oracle database for both the Policy Manager and Collector databases. The overall process for preparing Oracle databases for use with eTrust Audit includes the following procedures:

1. Verify that the database server meets the minimum hardware and memory requirements.

   For more information, see Database Planning (see page 36).

2. Install the Oracle Database Management System (DBMS) on the database server, and on the management or policy manager servers.

3. Review the Collector database considerations and then create the Collector database and users.

4. Review the Policy Manager database considerations and then create the Policy Manager database and a user.

   Note: If the user who installs the Policy Manager has DBA privileges, the installation creates and populates the database during installation. If required, a DBA can create the database *prior* to Policy Manager installation using one of the following approaches:

   - Review the migration prerequisites and migrate an existing database, or
   - Create a new database

   After the DBA creates the Policy Manager database and a user with appropriate rights, an admin user can install the Policy Manager components. The installation creates the Policy Manager database schema under the defined user and then inserts the default policies in the tablespaces. If the tablespaces already exist, the installation does not change them.

After you have created the databases, you can continue with the installation of eTrust Audit components.

Install the Oracle Database Management System

For information about installing the Oracle DBMS, see the applicable Oracle product documentation.

To configure Oracle for an eTrust Audit Collector database

Install the Oracle DBMS on the database server. The Collector database resides on this computer unless you are using a storage network array.

To configure Oracle for a Policy Manager database

Install the Oracle DBMS on the policy manager server.

If you are using the Policy Manager for Windows systems, you can install the Policy Manager on the management server with the SCC Server components, if desired.

Collector Database Considerations - Oracle

When creating the Collector database, consider the following guidelines:

- SID Name Length

  Ensure that you use a SID name of at least four characters in length. Valid SID names for use with eTrust Audit contain between four and eight characters.

- Character Set

  Select the AL32UTF8 for the database character set and select UTF8 for the National Character Set.

- Tablespace

  Create a new tablespace for the Collector database with a reasonable initial size. Determine the initial size of the tablespace based on the database capacity.

  When setting the initial size for the tablespace, select the AutoExtend option for the tablespace. For example, for most situations you can set the initial size as 1-10 GB and select the option to "Automatically extend datafile when full." We recommend that you select AUTOEXTEND for this option because calculation of database size is not exact.

  Note: If you do not select the "AUTOEXTEND" option, there will be a build up of queue files in the Collector component whenever the tablespace is full.

  When calculating the size of the database, take the following factors into consideration:

  - Number of Recorders/iRecorders deployed.
  - Expected number and size of events that each Recorder/iRecorder will collect. The maximum size of an event stored in the database is 2 KB for eTrust Audit 1.5 SP3 and 8 KB for eTrust Audit r8.
  - Number of events expected in a day, and the number of days the events are stored in the database.
  - Using the eTrust Security Command Center Table Collector option requires additional space to store data in the TC tables. Determine the size of all the columns defined in a TC table and multiply that value by the number of rows expected per day and the number of days needed for retention. Do this for every TC table you define.
  - Setting a proper initial size for the tablespace improves the database performance.

  Important! The database is locked during the autoextend process. This may have an impact on the insert and query rate. Take care not to set the starting value for the initial size of the tablespace too low before selecting the AUTOEXTEND option.

- Review the additional guidelines in Recommended Oracle Database Settings (see page 65).

Recommended Oracle Database Settings

The following table shows the recommended settings for an Oracle Collector database.

Parameter	Description	Recommended Setting
DB_BLOCK_SIZE	The size of single-block I/O requests. This parameter is also used in combination with multiblock parameters to determine multiblock I/O request size.	At least 8K, 32K if memory permits. Should be > and a multiple of the OS block size.
OS block size	Determines I/O size for redo log and archive log operations.	default
Maximum OS I/O size	Places an upper bound on the size of a single I/O request.	As large as possible.
DB_FILE_MULTIBLOCK_READ_COUNT	The maximum I/O size for full table scans is computed by multiplying this parameter with DB_BLOCK_SIZE. (The upper value is subject to operating system limits).	OS buffer size / DB_BLOCK_SIZE
SORT_AREA_SIZE	Determines I/O sizes and concurrency for sort operations.	20% of memory SGA + PGA should be less than or equal to 80% of system memory
HASH_AREA_SIZE	Determines the I/O size for hash operations.	default
DB_NAME	Name of the database. This should match the ORACLE_SID environment variable. Valid SID names for use with eTrust Audit contain between four and eight characters.	eaudit
DB_DOMAIN	Location of the database in Internet dot notation.	No recommendation.

Parameter	Description	Recommended Setting
OPEN_CURSORS	Limit on the maximum number of cursors (active SQL statements) for each session. The setting is application-dependent, and the default in many cases is sufficient.	Typical value is 500
CONTROL_FILES	Set to contain at least two files on different disk drives to prevent failures from control file loss.	default
DB_FILES	Set to the maximum number of files that can assigned to the database.	default
DB_CACHE_SIZE	Size of the buffer cache in the SGA. There are no defined or simple rules to set a value, as the values are application dependent. Typical values are in the range of twenty to fifty for each user session. More often, this value is set too high than too low. The DB_BLOCK_BUFFERS setting has been deprecated.	30 - 50% of memory SGA + PGA should be less than or equal 80% of system memory.
SHARED_POOL_SIZE	Sets the size of the shared pool in the SGA. The setting is application dependent, but it is typically is in the range of a few megabytes to a few tens of megabytes for each user session.	10% of memory SGA + PGA should be less than or equal to 80% of system memory.
PROCESSES	Sets the maximum number of processes that a single instance can start. This is the most important primary parameter to set, because many other parameter values are deduced from this value.	Typical value is 150
SESSIONS	This value is set by default from the value of the PROCESSES setting. However, if you are using the shared server, then the deduced value is likely to be insufficient.	default

Parameter	Description	Recommended Setting
JAVA_POOL_SIZE	If you are using Java stored procedures, then this parameter should be set depending on the actual requirements of memory for the Java environment.	default
LOG_ARCHIVE_XXX	Enables redo log archiving.	default
ROLLBACK_SEGMENTS	Allocates one or more rollback segments by name to this instance. If you set this parameter, the instance acquires all of the rollback segments named in this parameter, even if the number of rollback segments exceeds the minimum number required by the instance. This value is calculated as TRANSACTIONS / TRANSACTIONS_PER_ROLLBACK_SEGMENT.	default

Create the Collector Database - Oracle

To create the Collector database

1. Access the installation media and locate the Solaris/Shared directory.
2. Login to the Oracle DBMS as a user with DBA privileges.
3. Run the script, oracle9.sql, to create the Collector database for either Oracle 9i or Oracle 10g databases.
4. Make a note of the account credentials used to create the database on the Database Planning Worksheet (see page 43).
5. Install the eTrust Audit components as described elsewhere. The various installation procedures create the required tablespaces and populate them with default policies.

Policy Manager Database Considerations - Oracle

When creating the Policy Manager database, consider the following guidelines:

Memory and Buffer Cache

Defines the size of the memory and buffer cache. It should take less than 30% to 50% of the available physical memory. The general rule is that you should reserve enough memory for the Oracle DBMS to run efficiently, but not so much that you force the OS to swap files to disk.

Character Set

Defines the database and national character sets. Select the AL32UTF8 for the database character set and select UTF8 for the National Character Set.

Tablespaces

Defines the tablespace starting size. You create the tablespaces in the policy manager database during database creation. Use the auditdbexp.sql script for this. The tablespace initial size is based on the present size of your policy database, and add space for both new default polices and future growth. Depending on the size of your existing database, 50-100 MB is recommended as a starting value. Depending on your usage, you may need to increase the size of the tablespaces, or change settings, to allow for future growth. The set of default policies requires approximately 6 MB. Each MP file uses approximately 0.5 MB.

When setting the initial size for the tablespace, select select the option to "Automatically extend datafile when full" (AUTOEXTEND) for the tablespace. You can set this option using the Enterprise Manager Console.

Important! The database is locked during the autoextend process. This may have an impact on the insert and query rate. Take care not to set the starting value for the initial size of the tablespace too low before selecting the AUTOEXTEND option.

Create a New Policy Manager Database

The Policy Manager installation normally creates the required database objects in the policy manager database you created. However, if security in your organization requires it, a database administrator can create the required database objects prior to the Policy Manager installation.

This procedure assumes that you do not have an existing policy database to migrate, and that you want a database administrator to prepare the new Oracle database objects for the Policy Manager before the Policy Manager is installed.

To create a Policy Manager database for Oracle databases (Solaris)

1. Access the installation media and locate the Solaris/Shared directory.
2. Login to the Oracle DBMS as a user with DBA privileges.
3. Run the script, auditdbexp_ora.sql, to create the Policy Manager database objects.
4. Make a note of the account credentials used to create the database on the Database Planning Worksheet (see page 43).
5. Install the Policy Manager components as described elsewhere.

   The Policy Manager installation automatically locates the database and creates the required objects.

To create a Policy Manager database for Microsoft SQL Server databases (Windows)

1. Access the installation media and locate the Windows\Shared directory.
2. Login to the Microsoft SQL Server DBMS as a user with DBA privileges.
3. Run the script, auditdbexp_sqlsrv.sql, to create the Policy Manager database objects.
4. Make a note of the account credentials used to create the database on the Database Planning Worksheet (see page 43).
5. Install the Policy Manager components as described elsewhere.

   The Policy Manager installation automatically locates the database and creates the required objects.

Configure Microsoft SQL Server for eTrust Security Command Center

Configuring the Microsoft SQL Server DBMS for use with eTrust Security Command Center enables the creation of two databases:

- The CleverPath Portal database used by the SCC Server
- The CA Common Services database used by the Status Monitor

The steps that follow are not the only steps in the DBMS installation. Using the parameters listed below ensures that both databases operate correctly. For specific details about installing the Microsoft SQL Server DBMS, refer to the product specific documentation.

To configure Microsoft SQL Server for eTrust Security Command Center

1. Log in to the management server using administrator-level credentials.
2. Install the Microsoft SQL Server DBMS using the Custom installation type.
3. Set the authentication mode to Mixed mode.
4. Specify a password for the sa account.

   Record the password in the Database Planning Worksheet for later use during the eTrust Security Command Center installation.
5. Specify the option, Dictionary order, case-sensitive, for use with 1252 Character Set, in the Collation Settings window.

   The CA Common Services database must be set to case-sensitive for proper operation of the databases.

Configure the Portal Database

To configure the Portal Database for eTrust Security Command Center

1. Start the Microsoft SQL Server Enterprise Manager and expand to the Databases node.
2. Create a new database called portaldb.

   Do *not* use the default MASTER database.
3. Set the desired database size and growth characteristics in the Data Files tab.
4. After the database is created, create a login account for the database. Record the user name and password in the Database Planning Worksheet.

Create Portal Database User Login Account

To create a portal database user account

- Create a Microsoft SQL Server login account for the CleverPath Portal to access the SCC Portal database.

  The login account must use Microsoft SQL Server authentication. The Portal database you create should be the default database for the login account.

  Note: Do not use the greater than (>) and less than (<) symbols in database names or passwords for the eTrust Security Command Center portal database. Make a note of the user name and password you create for later use during the SCC Server installation.

- Choose the following minimum database roles for the login account:
  - public
  - db_owner

Chapter 7: Installing Data Tools

This section contains the following topics:

Introduction

Installing the eTrust Audit Data Tools (see page 55) on Windows or UNIX systems is the second deployment step for your SIM solution. Before installing the Data Tools, make sure a database management system is already installed and operational, and that you can connect to the database.

Note: It is recommended that you do not install the Data Tools on the same server as the Policy Manager.

If you are using an Oracle Collector database, an Oracle client must be present on the server prior to installing the Data Tools components.

If you are using a Microsoft SQL Server database, the MS SQL Server client is included in the base operating system installation for Windows 2000/2003 Server. Make sure that MS SQL Server and Client are configured to use TCP/IP for the Network library. The default setting is to use Named Pipes. This setting does not work well if the Microsoft SQL Server database is on a remote subnet.

Data Tools Components

The eTrust Audit Data Tools comprise the following components:

Data Tools Interface

Includes the following subcomponents:

Security Monitor

Allows you to monitor specific events that you designate important enough to monitor in near real-time. A variety of different recorders can send these events. You can also monitor eTrust Audit status and Self Monitor events. These events describe the status of eTrust Audit components, such as whether the Action Manager is running. The Security Monitor is only available for Windows systems.

Post-Collection Utility (PCU) - Windows Only

Provides a set of event collection utilities that let you load, view, prune, and sign events in tables outside of the SEOSDATA table.

Health Monitor

Provides operational status information based on the rate of events received from each of your event sources such as a machine with an event recorder.

Collector Service

Collects events generated from various event sources and stores the events in the Collector database. The Collector service uses the database system you configured earlier.

Installing Data Tools on Windows

This section provides instructions for installing the eTrust Audit Data Tools on a Windows system for use with a Microsoft SQL Server or Oracle database.

Data Tools Prerequisites - Windows

Before starting the eTrust Audit Data Tools for Windows installation, you will need the following information:

To configure the connection to a Oracle database:

- TNS service name
- User ID
- Password
- Oracle client installed on the computer on which you want to install the Data Tools

To configure the connection to a Microsoft SQL Server database:

- Server name
- User ID
- Password
- Database name

Install Data Tools on Windows

You can install the Data Tools to access the Security Monitor, Post-Collection Utility, and Health Monitor features. You can also install the Collector service. You can install all of the Data Tools components on a single computer, or you can install the various components on more than one computer.

Both the PCU and Health Monitor need a Collector service installed on the same computer. You only need one instance of the Health Monitor and PCU per Collector database. You can install multiple Collector services in your environment connected to the same Collector Database for load distribution and fail-over support.

The Data Tools installation log file, eAuditSetupDT.log, is located in the %temp% directory.

To begin installing the Data Tools on a Windows computer

Note: This procedure applies to both Microsoft SQL Server and Oracle. During the installation you will specify your database type and enter the necessary configuration information.

1. If the eTrust Audit installation program is not open, run setup.exe located in the eTrust Audit root folder.

   The eTrust Audit installation Main Menu page appears.

2. Select Install eTrust Audit Components.

   The Install eTrust Audit Components page appears.

3. Select Install eTrust Audit Data Tools.

4. Select Install eTrust Audit Data Tools on Windows to start the eTrust Audit installation wizard.

   The End User License Agreement page appears.

5. Review the license agreement, scrolling all the way to the bottom.

   The radio button to accept the agreement is not enabled until you have read to the bottom of the page.

6. Accept the license agreement.

   Note: If you select the radio button, I do not accept the terms in the license agreements, the installation exits.

   The Welcome page appears.

7. Click Next to continue with the installation.

   The Setup Type page appears.

8. Choose the installation type.

- Choose Typical, if you are installing all of the Data Tools components on the same computer. The Select Language for eTrust Audit page appears.
- Choose Custom, if you are installing the Data Tools components on multiple computers. The Custom installation path adds a few prompts that display before the typical installation path prompts. If you chose Custom, follow the steps under the next heading, then go on through the steps for a typical installation. The Choose Destination Location page appears.

To configure a custom Data Tools installation

1. Choose the destination folder where you want to install the Data Tools.

   The Optional Components page appears.

2. Choose the Data Tools components that you want to install.

   The Select Language for eTrust Audit page appears.

To configure a typical Data Tools installation

1. Select the language for the Data Tools installation.

   The default language, English, is selected. The Outgoing Encryption Method page appears.

2. Choose the default Encryption Method, AES 256bit.

   The Database Type page appears.

3. Choose the database management system that eTrust Audit uses as the Collector database.

   Note: The Oracle database option is enabled only if you have the Oracle client installed on the same system where you are installing the Data Tools.

   The Database Configuration page appears.

4. Enter the database information. Refer to the Database Planning Worksheet (see page 43).

   a. For Microsoft SQL Server databases, enter the following information to set up access to the database:

      - Server name
      - User name
      - Password (created during the database configuration)
      - Database name

      Note: The database name is case-sensitive.

   b. For Oracle databases, enter the following information to set up access to the database:

- TNS Service name
- User name
- Password (created during the database configuration)

Note: If a Collector database's tables already exist in the specified database, the Event Database page appears and gives you the option to create a new database or to keep the existing one. If you choose to create a new database, a dialog pops up to confirm overwrite of the existing DB. Overwriting the existing database deletes all of the events in the database.

The Specify Name of Monitor Machine page appears.

5. Enter host name or IP address of the Security Monitor computer.

   This specifies the Security Monitor computer where the eTrust Audit Data Tools sends internal or self-monitoring messages.

   Note: If you plan to install the Security Monitor on the same server as the Data Tools server, enter **localhost**. If you plan to install the Security Monitor on a different server, enter that server name.

   The Setup Services page appears.

6. Select the services for which you want to modify database user account credentials.

   This page lets you change the account under which the eTrust Audit Portmap and Collector services run. The default value is the local system account. If you change this account, the named user account must already exist on this server. If that user's password changes, you must also update the service in order for that user to start it.

   The Start Copying Files page appears, listing your specifications for the installation.

7. Review your selections and then accept them by clicking Continue.

   A Setup status page appears, showing the progress of the installation. When finished, a message appears indicating that the installation of the eTrust Audit Data Tools components is complete.

8. Start the eTrust Audit Data Tools services when prompted.

9. Click Finish after the completion message appears.

Installing Data Tools on UNIX

This section provides the steps for you to install the eTrust Audit Data Tools on a UNIX system for use with an existing Oracle database.

Data Tools Prerequisites - UNIX

Before starting the eTrust Audit Data Tools for UNIX installation, you must do the following:

- Set up the connection to the Collector database
  - For a local Oracle database, enter the following:
    - Oracle Home path - where Oracle is installed
    - Oracle database SID
    - Oracle user name
    - Oracle user password
  - For a remote Oracle database, enter the following:
    - TNS service name
- Create the SEOSDATA table in the Collector database
  - Run the Oracle SQL script for the installed version of Oracle located in the eTrust Audit installation directory

    For example, run oracle9.sql for Oracle 9i and 10g databases

Install Data Tools on UNIX

Use the following procedure to install the Data Tools on UNIX systems. The Data Tools installation log file for UNIX systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

To install the eTrust Audit Data Tools components on a UNIX computer

1. Log on to the UNIX machine as **root** (or superuser).
2. Enter the root password.
3. Insert the UNIX product installation media in the drive.

   Note: We recommend that you close any applications you have running before you insert the product installation media.
4. Change to the installation directory containing the eTrust Audit installation files and UNIX version you are running:

   cd /[*installation_path*]/r8SP2/[*platform*]/Audit

   where [*platform*] is either AIX or HP-UX.
5. Enter ls to view the contents of the installation directory:
   - A tar archive file that contains the product installation image in the form xxxxxxxxxxxxxx.tar.z for the platform and build designation
   - An installation shell script named install_eAudit
6. While still logged in as root, enter the following command from the shell prompt to start the eTrust Audit installation:

   ./install_eAudit

   The End User License Agreement appears.
7. Review the license and then enter Y to accept the license agreement.
8. Select the recommended Encryption Method, AES 128 bit.
9. Select the eTrust Audit Data Tools component for installation.

   Note: You can select additional eTrust Audit components to install at this time. For installation instructions for those components, see Install the Client Component (see page 113) or Install the Event Recorders (see page 127).
10. Enter the remote host name or IP address of eTrust Audit Security Monitor server.

    This specifies the Security Monitor server where the eTrust Audit Data Tools sends internal or self-monitoring messages.
11. Enter the Oracle Home path for the Oracle server.
12. Select local or remote for the Oracle database server.

For a local database, enter the following to set up access to the Oracle database:

- Oracle database SID
- Oracle database user ID (for example, AUDITDBA)
- Oracle user password

For a remote database, enter the following to set up access to the Oracle database:

- TNS service name

13. Press Enter to start the eTrust Audit Data Tools installation.

    When finished, a message appears indicating the installation of the eTrust Audit Data Tools components is complete.

14. Start the eTrust Audit Data Tools services.
15. When done, exit installation.

Installing Data Tools on Solaris

This section provides the steps for you to install the eTrust Audit Data Tools on a Solaris system for use with an existing Oracle database.

Note: You can run the Data Tools for Solaris systems only under the Global Zone.

Data Tools Prerequisites - Solaris

Before starting the eTrust Audit Data Tools for UNIX installation, you must do the following:

- Set up the connection to the Collector database
  - For a local Oracle database, enter the following:
    - Oracle Home path - where Oracle is installed
    - Oracle database SID
    - Oracle user name
    - Oracle user password
  - For a remote Oracle database, enter the following:
    - TNS service name
- Create the SEOSDATA table in the Collector database
  - Run the Oracle SQL script for the installed version of Oracle located in the eTrust Audit installation directory

    For example, run the oracle9.sql script for Oracle 9i and 10g installations.
- Install the eTrust Audit Shared Components

Install Shared Components on Solaris Systems

The Shared Components are a prerequisite for all of the eTrust Audit components on Solaris systems. You must install this software on any Solaris system before installing the other eTrust Audit components.

The shared components installation log file for Solaris systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

To install the common components on a Solaris UNIX system

1. Log on to the UNIX server as root (or superuser).
2. Locate the shared components installation package, AuditShared-8.0.200.xxx-all.pkg.
3. Change the current working directory to the directory containing the AuditShared-8.0.200.xxx-all.pkg file.
4. Run the following command to begin installing the shared components:

   ```
   # NONABI_SCRIPTS=TRUE pkgadd –d $PWD/AuditShared-8.0.200.103-all.pkg
   ```

   At the prompt, type the number of the installation package and press Enter. The End User License Agreement prompt appears.
5. Review the license agreement in a separate session. Make a note of the command response after reading the license agreement and return to the installation session. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   All of the subsequent Audit Administrator components use this path during their installations. You can press Enter to accept the default value, /opt/CA/eTrustAudit.

   If the directory name you enter does not yet exist, the installation prompts you for its creation.
7. Start the installation by answering the confirmation question.

   The common components installation begins.

Install Data Tools on Solaris 10 Systems

To begin installing the eTrust Audit Data Tools components on a Solaris system

1. Log on to the UNIX server as root (or superuser).
2. Locate the Data Tools installation package, AuditDT-8.0.200.xxx-all.pkg.
3. Change the current working directory to the directory containing the AuditDT-8.0.200.xxx-all.pkg file.
4. Run the following command to begin installing the Data Tools:

   ```
   # NONABI_SCRIPTS=TRUE pkgadd –d $PWD/AuditDT-8.0.200.xxx-all.pkg
   ```

   At the prompt, type the number of the installation package and press Enter. The End User License Agreement page appears.
5. Review the license agreement in a separate session. Make a note of the command response after reading the license agreement and return to the installation session. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   You can press Enter to accept the default value, shown in parentheses. The default value is the directory you entered while installing the shared components.
7. Select an encryption level from the supported levels. The AES 256 bit method is recommended.
8. Enter the name or IP address of the computer that you want to use as the Security Monitor.

To configure the connection to the Collector database

1. Provide the full path to the ORACLE_HOME directory, for example /opt/oracle/OraHome1.
2. Specify whether the database is local or remote.
3. Specify the database service ID (SID), if the database is local, or the service name, if the database is remote.
4. Provide the Collector database user account's ID and password, and then confirm the password.
5. Start the installation by answering the confirmation question.

   The Data Tools installation begins.

Chapter 8: Installing Policy Manager

This section contains the following topics:

Introduction

Installing the eTrust Audit Policy Manager (see page 55) is the third deployment step in your SIM solution. The Policy Manager is used primarily for creating, managing, and distributing Audit policies throughout your enterprise.

eTrust Audit Policy Manager is usually installed on the management server when you are using the Policy Manager for Windows. We recommend that you do not install the Policy Manager on the event collection server with the Data Tools.

You can also install the Policy Manager on a Solaris 10 server. In this case, you will need to install both the shared components and Policy Manager component on a separate policy manager server. If you also want to use the SCC Server components, you must install them on a separate Windows management server.

If you have an existing Windows policy database, you can migrate it to an Oracle database using a script supplied with the eTrust Audit installation. You must install the Policy Manager first, then migrate your database *before* you take any actions in the user interface.

Policy Manager Components

The eTrust Audit Policy Manager includes the following subcomponents:

Distribution Server

A service that communicates with the Distribution Agents and coordinates the delivery of eTrust Audit policies.

Audit Administrator

A Web-based user interface that you use to manage eTrust Audit.

Make sure Internet Explorer 6.0 SP1 is installed on the computer where you plan to run the eTrust Audit Administrator.

The Audit Administrator includes the following subcomponents:

Policy Manager

A web-based graphical user interface (GUI) that you use to manage Audit policies centrally. It lets you create, implement, and distribute policies to eTrust Audit clients.

Visualizer - Windows only

In the Audit Administrator, you can run a list of standard queries based on data collected by the Collector database. The visualizer software component helps to display the queried data in directed graphs. You can install this component on additional desktops not on the management server, if desired.

Health Monitor

Allows you to discover and access the Health Monitor, a web-based monitoring utility that lets you configure alert conditions to monitor the status of event collections from all discovered event sources. The Health Monitor provides operational status information based on the rate of events received from each of your event sources such as a machine with an event recorder.

PCU - Windows only

Allows you to discover and configure PCU installations from a central point.

iRecorder Manager

Allows you to discover and manage iRecorders in your environment.

Configuration

Allows you to configure Audit Administrator from your web browser host.

Reporter

Allows you to access the web-based graphical user interface (GUI) that you use to manage the eTrust Audit Reporter from a central point.

Viewer

Allows you to access the web-based graphical user interface (GUI) that you use to manage the eTrust Audit Viewer from a central point.

eIAM Server Access

During installation, the Policy Manager install program attempts to contact an Embedded Identity and Access Management server (eIAM server, or IAM Toolkit server) through its default administrative account, EiamAdmin. The EiamAdmin account ID is predefined as the default account for accessing the eIAM server, and as the default access for the Policy Manager, after installation is complete. The password for the EiamAdmin account is set when the eIAM server is installed. If the eIAM server is already installed in your environment, contact a system administrator to get the EiamAdmin account password.

If you install choose to install the eIAM server as part of the Policy Manager installation, you set the EiamAdmin account password during that installation. You should make a note of the password you select in the space provided in this worksheet.

Note: You must use the EiamAdmin account and password to log in to the eTrust Audit Administrator the first time so that you can configure the other user accounts that have access.

Install Policy Manager on Windows

You can install Policy Manager to create, implement, and distribute policies to eTrust Audit Clients. You should install the Policy Manager before you install the eTrust Audit Clients on the event sources.

Note: Before starting this installation, close all Windows applications.

The Policy Manager installation log file, eAuditSetupPM.log, is located in the %temp% directory.

To begin installing the Policy Manager

1. Run setup.exe located in the eTrust Audit root folder.

   The eTrust Audit installation Main Menu page appears.

2. Select Install eTrust Audit components.

   The Install eTrust Audit Components page appears.

3. Select Install eTrust Audit Policy Manager to start the eTrust Audit installation wizard.

   Note: It may take some time for the install setup to complete and the wizard to display.

   The End User License Agreement page appears.

4. Review the license agreement, scrolling all the way to the bottom.

   The radio button to accept the agreement is not enabled until you have read to the bottom of the page.

5. Accept the license agreement.

   Note: If you select the radio button, I do not accept the terms in the license agreements, the installation exits.

   The Welcome page appears.

6. Click Next to continue with the installation.

   The Setup Type page appears.

7. Choose the installation type.

   - Choose Typical, if you are installing all of the Policy Manager components on the same computer. The Select Language for eTrust Audit page appears.
   - Choose Custom, if you are installing the Policy Manager components on multiple computers. The Custom installation path adds a few prompts that display before the typical installation path prompts. If you chose Custom, follow the steps under the next heading, then go on through the steps for a typical installation. The Choose Destination Location page appears.

To configure a custom Policy Manager installation

1. Choose the destination folder where you want to install the Policy Manager.

   The Optional Components page appears.

2. Choose the Policy Manager components that you want to install.

   The Select Language for eTrust Audit page appears.

To configure a typical Policy Manager installation

1. Select the language for the Policy Manager installation.

   The default language, English, is selected.

   The Outgoing Encryption Method page appears.

2. Choose the default, AES 256bit.

   Note: If there are other eTrust Audit components installed on this computer, you may see the default value listed as, Use the existing encryption method... and the corresponding bit value.

   The Setup Internal Alert Messages page appears.

3. Enter the name of the Security Monitor computer where you want the Policy Manager components to send internal or self-monitoring events.

   If you enter a host name for a computer that does not have the Security Monitor installed, a warning appears. That computer cannot receive alerts until you install the Security Monitor.

   Note: If you are installing the Security Monitor on the same computer as the Policy Manager, enter localhost in the Host field.

   The Database Configuration page appears.

4. Enter the Policy Manager database connection parameters.

   - Server name for the SQL database server
   - User name (for example, auditdba)
   - Password for the Database Administrator (created during the database configuration)
   - Database name

   The IAM Toolkit Server page appears.

   Note: The Embedded Identity and Access Management Toolkit (IAMT) server referenced by the installation is the same product and functionality as the Embedded Identity and Access Management (eIAM) server.

5. Specify whether the IAM Toolkit server is installed locally or remotely.

   The IAM Toolkit Server page appears.

6. Enter the name of the IAM Toolkit server.

The IAM Toolkit Server Password page appears. If you plan to connect to an existing IAM server installation, you will need the password for the EiamAdmin account.

7. Enter and confirm the password for the IAMT server.

   If the installation is unable to contact the designated server, it displays an error message. Click Yes to install the IAMT server locally. Click No to re-attempt password entry. If you choose to install the IAM server locally, make a note of the password you use on the Network Management Planning worksheet (see page 48).

   The Web Server Configuration page appears.

8. Enter the Host name and port number for the Reporter and Viewer installation.

   The Policy Manager Identification String page appears.

9. Enter an identification string value that each Client installation uses to register with this Policy Manager. Record the string value you create here in the Network Management Planning Worksheet.

   Note: Use this identification value when you install the eTrust Audit Client to complete the installation of the latter. You must communicate this value directly to the person installing the Clients. If you want Clients to register with multiple Policy Managers in your network, you must use the same Policy Manager identification value for all Policy Managers and Clients. If you want to change this value after the installation, read the information in Rename the Policy Manager Identification String (see page 95).

   The Events Routing Configuration page appears.

10. Enter the name of the host computer on which you have an eTrust Audit Client installed to handle Policy Manager-related events.

    Specify localhost if you plan to install an eTrust Audit Client on the same computer as the Policy Manager (this is recommended).

    The Setup Services page appears.

11. Select the services for which you want to modify user account credentials.

    This page lets you change the account under which the services run. The default value is the local system account. If you change this account, the named user account must already exist on this server. If that user's password changes, you must also update the service in order for that user to start it.

    The Start Copying Files page appears, listing your specifications for the installation.

12. Review and then accept your selections by clicking Continue.

    A status page appears, showing the progress of the installation.

13. Click Finish after the completion message appears.

Install Policy Manager on Solaris 10

The Policy Manager installation requires the presence of the eTrust Audit Shared Components. If you have not installed the Shared Components, follow the procedure, Install Shared Components on Solaris (see page 83). The Policy Manager installation log file, etaudit.mmddyy.hhmm, is located in the /tmp directory.

Note: You can run the Policy Manager for Solaris 10 systems only under the Global Zone.

To begin installing the Policy Manager on a Solaris 10 system

1. Log on to the UNIX server as root (or superuser).
2. Locate the Policy Manager installation package, AuditPM-8.0.200.xxx-all.pkg.
3. Change the current working directory to the directory containing the AuditPM-8.0.200.xxx-all.pkg file.
4. Run the following command to begin installing the Policy Manager:

   ```
   # NONABI_SCRIPTS=TRUE pkgadd –d $PWD/AuditPM-8.0.200.xxx-all.pkg
   ```

   At the prompt, type the number of the installation package and press Enter. The End User License Agreement page appears.
5. Review the license agreement in a separate session. Make a note of the command response after reading the license agreement and return to the installation session. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   You can press Enter to accept the default value, shown in parentheses. The default value is the same directory you entered while installing the shared components.
7. Select an encryption level from the supported levels. The AES 256 bit method is recommended.
8. Enter the name or IP address of the computer that you want to use as the Security Monitor.

   You can press Enter to accept the default value, shown in parentheses.

To configure the supported database types

1. Provide the full path to the ORACLE_HOME directory, for example, /opt/oracle/OraHome1.
2. Specify whether the database is local or remote.

3. Specify the database service ID (SID), if the database is local, or the service name, if the database is remote.
4. Provide the Policy Manager database user account ID and password, and then confirm the password.

To configure IAMT server information

1. Specify a local or remote connection to the IAMT server.

   Note: The Embedded Identity and Access Management Toolkit (IAMT) server referenced by the installation is the same product and functionality as the Embedded Identity and Access Management (eIAM) server.

To configure a local connection to the IAMT server

1. Enter the IAMT admin (EiamAdmin) login password.
2. Confirm the password when prompted.

   The installation attempts to connect to the IAMT server. If an IAMT server does not exist, the Policy Manager package prompts you to install it on the local host.

To configure a remote connection to the IAMT server

1. Enter the server name on which the IAMT server is installed.
2. Enter the IAMT admin (EiamAdmin) login credentials.
3. Confirm the password when prompted.

To configure connection to the Web server

1. Specify the Web Server type.

   The value you enter is case-sensitive.
2. Enter the name of the WebSphere Server.

   If the WebSphere Server is on the local server, you can press Enter to accept the default value shown in parentheses.
3. Specify the https port to connect to the AuditAdmin application.

   You can press enter to accept the default port number, shown in parentheses.

To configure JAVA information

1. Specify the path to the Java files, JAVA HOME.

   The .../bin/java part of this path is assumed. You only need to identify the parent directory location for the Java software. For example, if you install the Java software in /usr/j2se, the installation automatically adds the assumed part of the path to create the full path entry, /usr/j2se/bin/java.

2. Specify the full path to the Java Virtual Machine (JVM) directory, for example, /usr/jdk/j2sdk1.4.2_08/jre/lib/sparc/client.

   The installation automatically uses the JAVA HOME path you supply to locate the JVM. You can press Enter to accept the default value, shown in parentheses.

To configure event routing

1. Specify whether you want the Policy Manager to forward User Monitoring events to eTrust Audit.
2. Provide the name of the Route Event Host.

   If you are using a local database, you can press Enter to accept the default value, localhost.

To configure a Policy Manager identification string value

1. Enter an identification string value that each Client installation uses to register with this Policy Manager. Record the string value you create here on the Network Management Planning Worksheet.
2. Make a note of the identification value you assign for registering the clients in the Network Management Planning Worksheet.

   Note: Use this identification value when you install the Audit Client to complete the Audit Client installation. You must communicate this value directly to the person installing the Clients. If you want Clients to register with multiple Policy Managers in your network, you must use the same Policy Manager identification value for all Policy Managers and Clients. If you want to change this password after the installation, read the information in Update the Policy Manager Identification String (see page 95).

To begin file transfer for the Policy Manager

1. Respond to the confirmation question to start or abort the installation.

   When you select Yes, the installation package transfers files for the Policy Manager.

Policy Manager Database Migration Prerequisites

To migrate an existing Policy Manager database, you need the following files and information:

- An existing Policy Manager database from eTrust Audit r1.5 or r8
- The r8 SP2 Policy Manager installed successfully, with an empty Policy Manager database
- The Data Source Name (DSN) for the new Policy Manager database
- A user name and password for the new Policy Manager database
- An Oracle client installed on the same machine as the database you want to migrate, if the new Policy Manager database is an Oracle database

Migrate an Existing Policy Manager Database

If you have an existing Policy Manager database from a previous release, you may want to migrate it for use with this release.

The migration utility automatically determines the existing Policy Manager database structure. No changes are made to the existing database, so it continues to function. The migration utility automatically stops all eTrust Audit processes and applications before performing the migration. If the processes do not shut down automatically, you can stop them manually and then proceed with the migration.

Note: To migrate an existing database successfully, you must migrate the database *before* you take any actions, such as creating, distributing, or removing policies in the r8 SP2 Policy Manager user interface.

To migrate an existing Policy Manager database

1. Copy the migration utility, PMDBMigrate.exe, onto the same computer as the old Policy Manager installation.
2. Run the utility.

   The PMDBMigrate utility uses the Windows registry to find the existing database. It makes a backup copy of the database file and performs all migration activities on the backup copy.
3. Enter the DSN name for the new Policy Manager database.
4. Enter the user name and password for the Policy Manager database and click OK.

   As the utility runs, it generates a log file located in your system temp directory. You can review this log file in case of errors.
5. Click Finish when the utility finishes processing.

Update the Policy Manager Identification String

The Policy Manager identification string value is set during the installation of the Policy Manager. The same value is used for all subsequent eTrust Audit Client installations.

At some point after initial component installation, you may have a security need to change the Policy Manager identification value used during Client installations. Use this procedure to change the value.

To update the Policy Manager identification value on Solaris 10 systems

1. Stop the acdistsrv process.
2. Navigate to the /bin directory in your eTrust Audit installation, and run the encup utility:

   ```
   # encup <user name><password>
   ```

   This generates a new encrypted value. More information on using the encup utility is available in the eTrust Audit Reference Guide.
3. Copy the new encrypted value.
4. Edit the eaudit.ini file.
5. Locate the Policy Manager section and modify the PolicyManagerID value using the encrypted value generated by the encup utility.
6. Start the acdistsrv process.

   You can now install eTrust Audit Clients using the new value.

To update the Policy Manager identification value on Windows systems

1. Stop the acdistsrv process.
2. Navigate to the \bin directory in your eTrust Audit installation, and run the encup utility:

   ```
   > encup
   ```
3. Enter and confirm the user name and password when prompted. Use the -ic parameter to have the system display what you type.

   The utility generates a new encrypted value. More information on using the encup utility is available in the eTrust Audit Reference Guide.
4. Copy the new encrypted value.
5. Edit the Windows registry key: HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Policy Manager\Distribution Server\PolicyManagerID.
6. Modify the value using the encrypted value generated by the encup utility and click OK.

7. Start the acdistsrv process.

   You can now install eTrust Audit Clients using the new value.

Update the WebSphere Port Number

The default WebSphere Web Server secure port number is 9443. You may decide to change this port number after installing the Policy Manager.

To change the WebSphere web server secure port after installing Policy Manager

1. Navigate to the AuditAdminConfig.xml file.

   The default location for this file is /opt/CA/SharedComponents/iTechnology.

2. Stop the iGateway daemon.
3. Edit the file and update the port number.
4. Save and exit the file.
5. Restart the iGateway daemon.

Chapter 9: Installing Reporter and Viewer

This section contains the following topics:

Introduction - Reporter and Viewer

Installing the eTrust Audit Viewer and Reporter is the fourth deployment step in your SIM solution. The Viewer is a web-based interface that displays, sorts, and filters audit events retrieved from the Collector database. The Viewer also lets you create and save your own customized filters for future use.

The Reporter is a web-based interface that lets you view, create, and schedule detailed, graphic reports from information extracted from the Collector database. The supported report formats include the following:

- Adobe Portable Document Format (PDF)
- Rich Text Format (RTF)
- Comma-Separated Values (CSV)
- Crystal Reports RPT, (viewable as HTML)

The Reporter and Viewer components are usually installed on the event collection server with the Data Tools.

Reporter and Viewer Prerequisites

The Reporter and Viewer are installed as a Java Server Page (JSP) servlet and require installation of a Web server. You can use either the Tomcat or WebSphere Web Servers. The installation processing deploys the auditadmin.war file among others.

At runtime, the Reporter and Viewer installation authenticates using the Embedded Identity and Access Management (EIAM) services.

The Reporter and Viewer installation requires that the following components are installed:

- eTrust Audit Shared Components
- EIAM server
- Oracle Client (for connection to the Oracle database using ODBC, if the database is remote)
- Java JDK
- A WebSphere Application Server and SunONE Web Server or Tomcat Web Server

Note: The Tomcat web server is deployed when the Reporter and Viewer are installed.

Install the Reporter and Viewer on Windows

Use the following procedure to install the Reporter and Viewer on Windows systems. The Reporter and Viewer installation log file, eAuditSetupRV.log, is located in the %temp% directory.

To begin installing the Reporter and Viewer components on a Windows system

1. Log on to the Windows server.
2. Locate the Reporter and Viewer installation package, ReporterViewer.exe.
3. Run the following command to begin installing the Reporter and Viewer:

   ```
   ReporterViewer.exe
   ```

   The End User License Agreement page appears.
4. Review the license agreement, scrolling all the way to the bottom.

   The radio button to accept the agreement is not enabled until you have read to the bottom of the page.
5. Accept the license agreement.

   Note: If you select the radio button, I do not accept the terms in the license agreements, the installation exits.

   The Welcome page appears.
6. Click Next to continue with the installation.

   The Setup Type page appears.
7. Choose the installation type.
   - Choose Typical, if you are installing all of the Reporter and Viewer components on the same computer. The Select Language for eTrust Audit page appears.
   - Choose Custom, if you are installing the Reporter and Viewer components on multiple computers. The Custom installation path adds a few prompts that display before the typical installation path prompts. If you chose Custom, follow the steps under the next heading, then go on through the steps for a typical installation. The Choose Destination Location page appears.

To configure a custom Reporter and Viewer installation

1. Choose the destination folder where you want to install the Reporter and Viewer.

   The Optional Components page appears.

2. Choose the Reporter and Viewer components that you want to install.

   The Select Language for eTrust Audit page appears.

To configure a typical Reporter and Viewer installation

1. Select the language for the Reporter and Viewer installation.

   The default language, English, is selected.

   The Outgoing Encryption Method page appears.

2. Choose the default, AES 256bit.

   Note: If there are other eTrust Audit components installed on this computer, you may see the default value listed as, Use the existing encryption method... and the corresponding bit value.

   The Event Database Type page appears.

To configure database connections

1. Choose the database management system that eTrust Audit uses as the Collector database.

   Note: The Oracle database option is enabled only if you have the Oracle client installed on the same system where you are installing the Data Tools.

   The Event Database Configuration page appears.

2. Enter the path to the Microsoft SQL Server JDBC driver, sqljdbc.jar.

   The default path after installation is <*Selected initial directory*>\Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.1\enu\sqljdbc.jar.

3. Enter the path to the JDBC driver's authentication DLL, sqljdbc_auth.dll.

   The default path after installation is <*Selected initial directory*>\Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.1\enu\auth\x86\sqljdbc_auth.dll.

4. Enter the event (Collector) database information. Refer to the Database Planning Worksheet (see page 43).

   a. For Microsoft SQL Server databases, choose the option, Use SQL Server Authentication, and then enter the following information to set up access to the database:

      - Server name
      - User name
      - Password (created during the database configuration)

- Database name

Note: This value is case-sensitive.

b. Choose the option, Use Windows NT Authentication, and enter the following information to set up access to the database:

- Server name
- Database name

Note: This value is case-sensitive.

c. For Oracle databases, enter the following information to set up access to the database:

- TNS Service name
- User name
- Password (created during the database configuration)

The Policy Manager Database page appears.

5. Choose whether you want to configure the Policy Manager database.

   If you choose Yes, the Policy Manager Database Configuration page appears.

   a. For Microsoft SQL Server databases, choose the option, Use SQL Server Authentication, and then enter the following information to set up access to the database:

      - Server name
      - User name
      - Password (created during the database configuration)
      - Database name

      Note: This value is case-sensitive.

   b. Choose the option, Use Windows NT Authentication, and enter the following information to set up access to the database:

      - Server name
      - Database name

      Note: This value is case-sensitive.

   c. For Oracle databases, enter the following information to set up access to the database:

      - TNS Service name
      - User name
      - Password (created during the database configuration)

   If you choose No, the SMTP Server page appears.

To configure a mail server

1. Enter the mail server name.

   The default value is the local server name.

2. Enter the default sender name.
3. Enter the default email subject line.

To configure the IAMT server connection

1. Enter the name of the IAM Toolkit Server.

   Note: The Embedded Identity and Access Management Toolkit (IAMT) server referenced by the installation is the same product and functionality as the Embedded Identity and Access Management (eIAM) server.

2. Enter and confirm the IAM Toolkit Server password.

   Note: If no IAMT server exists, the Reporter and Viewer installation exits.

3. Enter the JAVA Home location.

4. Enter the Web Server type.

To configure the Tomcat Web Server connection

1. Enter the Tomcat Server port number.

   The default port value is 8443.

2. Enter the self-signed digital certificate information.

To configure the Web Server self-signed certificate

1. Enter the Web Server's self signed certificate data:
   - Organizational unit
   - Organization
   - Country
   - The Setup User Privileges page appears.

To set up user privileges

1. Select the list items for which you want to modify login credentials. This is an optional step.

To configure the CA eTrust Audit Router

1. Enter the name of the Audit Router host for routing events generated by actions taken by users of eTrust Audit.
2. Enter the port number on which the Router listens for traffic.

   Set the Router port here if you have not configured fixed ports. If you did configure fixed ports, then set this Router Port value to be the same value as the Router SAPI Port value. You can do this manually after the installation.

To start the transfer of files

1. Start the installation by answering the confirmation question.

   The Reporter and Viewer installation begins.

Install the Reporter and Viewer on Solaris

The Reporter and Viewer installation requires the presence of the eTrust Audit Shared Components. If you have not installed the Shared Components, follow the procedure, Install Shared (see page 83) Components on Solaris.

Note: You can run the Reporter and Viewer for Solaris systems only under the Global Zone.

The Reporter and Viewer installation log file for UNIX systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

To begin installing the Reporter and Viewer components on a Solaris 10 system

1. Log on to the UNIX server as root (or superuser).
2. Locate the Policy Manager installation package, AuditRV-8.0.200.xxx-all.pkg.
3. Change the current working directory to the directory containing the AuditRV-8.0.200.xxx-all.pkg file.
4. Run the following command to begin installing the Reporter and Viewer:

   ```
   # NONABI_SCRIPTS=TRUE pkgadd –d $PWD/AuditRV-8.0.200.xxx-all.pkg
   ```

   Type the number of the installation package and press Enter. The End User License Agreement page appears.
5. Review the license in a separate session. Make a note of the command response after reading the license agreement and return to the installation session. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   You can press Enter to accept the default value, shown in parentheses. The default value is the same directory you entered while installing the shared components.
7. Select an encryption level from the supported levels. The AES 256 bit method is recommended.

To configure database connections

1. Provide the full path to the ORACLE_HOME directory, for example /opt/oracle/OraHome1.
2. Specify whether the Collector database is local or remote.
3. Specify the database service ID (SID), if the database is local, or the service name, if the database is remote.

4. Provide the Collector database user account's ID and password, and then confirm the password.
5. Enter the name of the owner of the Oracle Events Schema (default).
6. Enter the name of the Oracle Events Server.

   If the database is local, the installation offers the default value, localhost. If the database is remote, no default is present.
7. Confirm that you want to configure the Policy Datasource.
8. Specify a local or remote Policy Manager database.
9. Specify the Oracle database SID.
10. Specify the Policy Manager user account name and password, and confirm the password when prompted.
11. Enter the name of the owner of the Oracle Events Schema for the Policy Manager database.

    The owner of the Oracle Policy Schema is by default the ID of the user connecting to Policy Database.
12. Enter the name of the Oracle Policy server.

To configure a mail server

1. Enter the mail server name.

   The default value is the local server name.
2. Enter the default sender name.
3. Enter the default email subject line.

To configure the IAMT server connection

1. Enter the name of the IAMT Server.

   Note: The Embedded Identity and Access Management Toolkit (IAMT) server referenced by the installation is the same product and functionality as the Embedded Identity and Access Management (eIAM) server.
2. Enter and confirm the IAMT Server superuser password.

   If no IAMT server exists, the Reporter and Viewer installation exits.
3. Enter the JAVA Home location.
4. Enter the Web Server type.

   This value is case-sensitive.

To configure the WebSphere Application Server connection

1. Enter the WebSphere Application Server ID.

   The WebSphere server offers the standard default value, server 1. You can use any value.

2. Enter the WebSphere Application Server's administrative port number (SOAP).

   The default administrative port value is 8880.

3. Enter the name of the virtual host to which the Audit web application maps.

   The WebSphere server offers the standard default value, server1. You can use any value.

4. Enter the name of the Secured Web Server user.

5. Enter the Secured Web Server user's password, and confirm the password when prompted.

6. Confirm restart of the WebSphere Application Server.

   If you choose not to restart the WebSphere Server as part of the installation, you can use an installed shell script to Restart the WebSphere Application Server (see page 107).

7. Enter the full path to the WebSphere Application Server.

   The default installation path is /opt/IBM/WebSphere/AppServer/.

To configure the Tomcat Web Server connection

1. Enter the name of the Web Server host.

2. Enter the https port number to connect to the eTrust Audit Administrator application on the Web Server host.

   The default port value is 9443.

To configure the CA eTrust Audit Router

1. Enter the name of the Audit Router host for routing events generated by actions taken by users of eTrust Audit.

2. Enter the port number on which the Router listens for traffic.

   Set the Router port here if you have not configured fixed ports. If you did configure fixed ports, then set this Router Port value to be the same value as the Router SAPI Port value. You can do this manually after the installation.

To start the transfer of files

1. Start the installation by answering the confirmation question.

   The Reporter and Viewer installation begins.

Restart the WebSphere Application Server

During the Reporter and Viewer installation, you can choose to stop and restart the WebSphere Application Server as part of the installation processing. If you choose not to restart the Application Server during installation, you must do so at some point to register and start the Reporter and Viewer web applications.

To restart the WebSphere Application Server

1. Log in as the root user.
2. Navigate to the /bin directory in the eTrust Audit root directory.

   The default directory is /opt/CA/eTrustAudit/bin.
3. Run the script startWebAudit.sh, if WebSphere is installed in the default location.

   If you installed the WebSphere Application server in a custom directory, use the following command to run the start script in interactive mode:

   ```
   startWebAudit.sh
   ```
4. Provide the application server home directory, server ID, and user name and password when prompted.

   The script stops the WebSphere Application Server, initializes the deployed Reporter and Viewer applications, and restarts the Application Server.

Chapter 10: Installing Clients

This section contains the following topics:

Introduction

Installing the eTrust Audit Client (see page 55) on Windows, UNIX, or Linux is the fifth deployment step in your SIM solution.

Installing the event recorders (see page 55) for Windows or UNIX is the sixth deployment step in your SIM solution.

Install the client components on all computers on which you want to install an event recorder. This allows you to filter events at the source to reduce network traffic and distribute the processing load. If you are using network devices such as routers or firewalls as event sources, you should install the client and event recorder as close as possible to the network devices. This limits the amount of network traffic, and filters that traffic as close to the source as possible.

Install an event recorder for each event source whose events you want to collect and monitor. If you install the event recorder on an event source that is remote from the client, the event recorder sends events to the router for further processing through the iRouter. You should only use this configuration in cases where a firewall that allows only TCP traffic is located between the components. Otherwise, you should install the client and event recorder on the same event source.

Client Components Overview

The eTrust Audit Client component provides services to collect and forward audit event data and includes the following subcomponents:

Standard System Recorder

Taps into the event data sent to standard system logging facilities (Windows Event Log on Microsoft Windows platforms; syslog daemon on UNIX and Linux platforms) and enables eTrust Audit to harvest events for processing.

Portmapper

Manages the logical communications channels required to provide a standard way for a client to access Remote Procedure Call (RPC) services. The Portmapper is available only on Windows platforms.

Redirector

Taps into local audit logs created by eTrust Access Control and automatically redirects the event data to a router component on the same or on another machine. This service is disabled by default. You can start it from the Windows Control Panel (Administrative Tools) options.The Redirector is available only on Windows platforms.

Router

Analyzes the policies that you provide using the Policy Manager, and then uses that configuration information to examine events sent to it. (The configuration information resides in .cfg files found in the *[installation_path]*\eTrust Audit\cfg directory.) Based on the policies you define, the router identifies event records to filter out or to forward to the Action Manager.

iRouter

Links iRecorders with the Router. The iRecorders use eTrust Audit iTechnology communication protocol (HTTPS, Port 5250) to deliver events in XML format to the iRouter. The iRouter converts the data it receives in XML format into the SAPI protocol and sends the converted events to the Router.

The iRouter consists of the following subcomponents:

- iGateway
- iControl
- epAudit Event Plugin

Some event recorders use SAPI to communicate to the Router directly if it is installed on the same computer as the client. This bypasses the iRouter completely. It also provides higher throughput than when using remote iRouters to communicate.

Action Manager

Processes events sent to it by the router. Use the Policy Manager to write policies to instruct the action manager to perform a wide range of actions automatically when it receives specific events. The Action Manager also guarantees delivery of events by marking events for deletion only after it receives successful receipt confirmation from the target.

Distribution Agent

Receives policies and MP files from the Policy Manager on the distribution server and places these policies and MP files into effect.

Installing the Client Components on Windows

This section describes how to install the Client component on a Windows system.

Client Prerequisites - Windows

Before starting the Client installation on a Windows system, carefully consider the following:

- Only a user with administrator rights can install a Client and run its services. However, during installation you can define a user with restricted rights to run the Client services. The minimum privileges required for a user to run the Client services include the following:
  - Log on as a service. The Client setup grants this right to the user.
  - Full control over the product file system directories.
  - Full control over the product registry.

  Note: If you have defined a restricted user to run the Client services, reboot the computer after the installation and before logging in as that user, to run the Client services.

- During the Client component installation, you must specify the computer names for the following subcomponents:

  Security Monitor

  Receives status notifications from the Client components.

  Policy Manager

  Sends policies to the Client components, from the Policy Manager on the management server (or separate policy manager server).

  SMTP Mail Server

  Receives email alerts to an administrator or operator if your have identified an SMTP mail server during the client components installation.

- Obtain the Policy Manager identification value used during the Policy Manager installation.
- The Client installation for Windows systems installs the NT Event Log iRecorder by default.
- The Client installation installs the iRouter. Before installing the client, consider the following:
  - To allow iTechnology communications in a protected environment, open the iTechnology TCP port 5250 in the firewall if the iRecorders and iRouter are installed on the different sides of the firewall.
  - If you accidentally uninstall the iRouter, you must re-install it using the iRouter package. See the *eTrust Audit Reference Guide* for details about how to install and configure the iRouter.
  - Make sure that you use the iControl Pull method for network environments with outgoing traffic only.

Install the Client Components on Windows

You can install the Client component on Windows to collect and forward event data. The Client installation log file, eAuditSetupCL.log, is located in the %temp% directory.

To install the Client components on a Windows system

1. If the eTrust Audit installation program is not open, run setup.exe located in the product root folder.

   The eTrust Audit installation Main Menu page appears.

2. Select the Install Components option from the Main Menu.
3. Select the Install eTrust Audit core components option from the Install Components list.

   The Install eTrust Audit Components page appears.

4. Select Install eTrust Audit Client.

   The license agreement appears.

5. Review the license agreement, scrolling all the way to the bottom.

   The radio button to accept the agreement is not enabled until you have read to the bottom of the page.

6. Accept the license agreement.

   Note: If you select the radio button, I do not accept the terms in the license agreements, the installation exits.

   The Welcome page appears.

7. Click Next to continue with the installation.

   The Setup Type page appears.

8. Choose the installation type.

   - Choose Typical, if you are installing all of the Client components on the same computer. The Select Language for eTrust Audit page appears.
   - Choose Custom, if you are installing the Client components on multiple computers. The Optional components page appears. The Custom installation path adds a few prompts that display before the typical installation path prompts. If you chose Custom, follow the steps under the next heading, then go on through the steps for a typical installation. The Choose Destination Location page appears.

To configure a custom Client installation

9. Choose the destination folder where you want to install the Client.

   The Optional Components page appears.

10. Choose the Client components that you want to install.

The Select Language for eTrust Audit page appears.

To configure a typical Client installation

1. Select the language for the Policy Manager installation.

   The default language, English, is selected.

   The Outgoing Encryption Method page appears.

2. Choose the default, AES 256bit.

   Note: If there are other eTrust Audit components installed on this computer, you may see the default value listed as, Use the existing encryption method..., and the corresponding bit value.

   The Event Logs to Audit page appears

3. Select the event types that you want this Client to collect.

   Note: If you choose the Include all existing events option, the eTrust Audit services process all of the events that already exist in the event logs when they start, regardless of the event age. Otherwise, the services only process new events.

   The Specify Name of Monitor Machine page appears.

4. Enter the host name or IP address of the Security Monitor console that receives internal or self-monitoring messages.

   The Setting up connection to eTrust Audit Policy page appears.

5. Enter the host name or IP address of the server running the Policy Manager.

   The Client Registration page appears.

6. Indicate whether you want this Client to be registered.

   The default value is yes. Registered clients have a node and host entry in the Policy Manager database, and an audit node created automatically. You can use this node to distribute policies to the Client.

   If you choose to register this Client, the Policy Manager Identification String page appears. If you choose not to register the client, skip the next step.

7. Enter the Policy Manager identification value, if you chose to register the Client.

   The Policy Manager identification value is created during the Policy Manager installation. You must obtain this value from an administrator or the person who installed the Policy Manager.

   The SMTP Server page appears.

8. Enter the name of an SMTP server to which the Client components can route emails. Enter the default sender, and subject for the alerts.

Note: This is an optional feature that enables the Client to send alerts through a variety of mechanisms, including email. To configure the email server at a later time, see the *eTrust Audit Reference Guide*.

The Setup Services page appears.

9. Choose the Client component services for which you want to define the special user privilege, log on as service. You must provide the user name and password for each selected service.

   The default value is the local system account. If you change this account, the named user account must already exist on this server. If that user's password changes, you must also update the service in order for that user to start it.

   The Installation Verification page appears.

10. Accept the default option, Install installation verification settings.

    The option installs template policies to route failed login attempt events to the computer you identified as the Security Monitor. The Start Copying Files page appears.

11. Review your current selections and then click Continue to accept them.

    A status page showing the progress of the installation appears. It also sets up the registry and services, and installs the iRouter and the iRecorder for NT Event Log. When finished, a message appears stating that the installation of the Client components is complete.

    Note: If you are installing on a computer running Windows 2000 Server, restart the computer now.

12. Start the Client services.

Installing the Client Components on UNIX

The following section describes how to install the Client components on a UNIX system. Your installation and implementation may vary slightly from the sample installation dependent on the type of UNIX you are using. This installation enables you to capture event data on a UNIX server.

Client Prerequisites - UNIX

Before installing the Client components on UNIX, satisfy the following prerequisites:

- Obtain the name or IP address of the server that serves as the Security Monitor
- Obtain the name or IP address of the Policy Manager server
- Obtain the Policy Manager identification value used during the Policy Manager installation
- Obtain the name or IP address of the Event Management server, if you plan to use that feature

Install the Client Components on UNIX

You can install the Client component on UNIX systems to collect and forward audit event data. The Client installation log file for UNIX systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

To install the eTrust Audit Client components on a UNIX system

1. Log on to the UNIX computer as root (or superuser).
2. Enter the root password.
3. Insert the UNIX product installation media in the drive.

   Note: We recommend that you close any applications you have running before you insert the product installation media.
4. Navigate to the installation directory containing the eTrust Audit installation files for the UNIX version you are running:

   cd /[*installation_path*]/Audit80_SP2/[*platform*]/Audit

   where *[platform]* is AIX, HP-UX, UnixWare, or Tru64.
5. Enter the ls command to view the contents of the installation directory.

   The following files are in that directory:

   - A tar archive file that contains the product installation image in the form xxxxxxxxxxxxx.tar.z for the platform and build designation, such as _AIX_AC8.0.200.103.tar.z.
   - An installation shell script named install_eAudit.
6. Remain logged in as root, and enter the following command from the shell prompt to start the installation:

   ./install_AuditClient

   The End User License Agreement prompt appears.
7. Review the license agreement and accept it. If you choose not to accept the agreement, the installation exits.

To configure the Client for network operations

1. Select the recommended Encryption Method, AES 256 bit.
2. Select the eTrust Audit Client component for installation.

   Note: You can select additional components to install at this time. For installation instructions for those components, see Install the Data Tools Component (see page 80) or Install the Event Recorders (see page 127).
3. Enter the server name or the IP address of the Security Monitor.
4. Enter the server name or the IP address of the Policy Manager.
5. Indicate whether you want this Client to be registered.

The default value is yes. Registered clients have a node and host entry in the Policy Manager database, and an audit node created automatically. You can use this node to distribute policies to the Client.

If you choose to register this Client, the eTrust Audit Client registration password page appears. If you choose not to register the Client, skip the next step.

6. Enter the Policy Manager identification value, if you chose to register the Client.

   The Policy Manager identification value is created during the Policy Manager installation. You must obtain this value from an administrator or the person who installed the Policy Manager.

7. Enter the name or IP address of the server where the Router is running.

To configure event handling

1. Enter the email sender name.
2. Enter the subject for the email notification.
3. Choose Yes or No for sending event messages to the Event Management component.
4. Enter the path to the Event Management agent.
5. Choose Yes or No to activate the syslog Recorder.
6. Confirm the sulog path.
7. Confirm the syslog.conf file path.
8. Choose Yes or No to start the eTrust Audit components.
9. Start the Client services.

Installing the Client Components on Solaris

The following section describes how to install the Client components on a Solaris system. This installation enables you to capture event data on a Solaris server.

Note: You can run the Client for Solaris systems under the Global Zone or Whole Root Local Zones.

Client Prerequisites - Solaris

Before installing the Client components on Solaris, satisfy the following prerequisites:

- Install the eTrust Audit Shared components
- Obtain the name or IP address of the server that serves as the Security Monitor
- Obtain the name or IP address of the Policy Manager server
- Obtain the Policy Manager identification value used during the Policy Manager installation
- Obtain the name or IP address of the Event Management server

Install Shared Components on Solaris Systems

The Shared Components are a prerequisite for all of the eTrust Audit components on Solaris systems. You must install this software on any Solaris system before installing the other eTrust Audit components.

The shared components installation log file for Solaris systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

To install the common components on a Solaris UNIX system

1. Log on to the UNIX server as root (or superuser).
2. Locate the shared components installation package, AuditShared-8.0.200.xxx-all.pkg.
3. Change the current working directory to the directory containing the AuditShared-8.0.200.xxx-all.pkg file.
4. Run the following command to begin installing the shared components:

   ```
   # NONABI_SCRIPTS=TRUE pkgadd –d $PWD/AuditShared-8.0.200.103-all.pkg
   ```

   At the prompt, type the number of the installation package and press Enter. The End User License Agreement prompt appears.
5. Review the license agreement in a separate session. Make a note of the command response after reading the license agreement and return to the installation session. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   All of the subsequent Audit Administrator components use this path during their installations. You can press Enter to accept the default value, /opt/CA/eTrustAudit.

   If the directory name you enter does not yet exist, the installation prompts you for its creation.
7. Start the installation by answering the confirmation question.

   The common components installation begins.

Install Client Components on Solaris

Use the following procedure to install Client components on Solaris systems. The Client installation log file for Solaris systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

To begin installing the Client components on a Solaris system

1. Log on to the UNIX server as root (or superuser).
2. Locate the Client installation package, AuditCli-8.0.200.xxx-all.pkg.
3. Change the current working directory to the directory containing the AuditCli-8.0.200.xxx-all.pkg file.
4. Run the following command to begin installing the Client:

   ```
   # NONABI_SCRIPTS=TRUE pkgadd –d $PWD/AuditCli-8.0.200.xxx-all.pkg
   ```

   At the prompt, type the number of the installation package and press Enter. The End User License Agreement prompt appears.
5. Review the license agreement in a separate session. Make a note of the command response after reading the license agreement and return to the installation session. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   You can press Enter to accept the default value, shown in parentheses. The default value is the directory you entered while installing the shared components.

To configure the Client for network operations

1. Select an encryption level from the supported levels. The AES 256 bit method is recommended.
2. Enter the name or IP address of the computer that you want to use as the Security Monitor.
3. Enter the name or IP address of the computer where the Policy Manager resides.
4. Indicate whether you want this Client to be registered.

   The default value is yes. Registered clients have a node and host entry in the Policy Manager database, and an audit node created automatically. You can use this node to distribute policies to the Client.
5. Enter the Policy Manager identification value, if you chose to register the Client.

   The Policy Manager identification value is created during the Policy Manager installation. You must obtain this value from an administrator or the person who installed the Policy Manager.

6. Enter the name or IP address of the computer where the eTrust Audit Router is installed.

   Use the local server designation, localhost, if the Router is installed on same machine as the Client.

To configure event handling

1. Enter an email Sender name for alerts and event messages.
2. Enter an email Subject for alerts and event messages.
3. Choose whether to send event messages to Event Management.
4. Choose Yes or No to activate the syslog Recorder.
5. Enter the syslog.conf file path.
6. Choose Yes or No to start the Client daemons after installation.

   The Data Tools installation begins.

Installing the Client Components on Linux

The following section describes how to install the Client components on a Linux system. This installation enables you to capture event data on a Linux server.

Client Prerequisites - Linux

Before installing the Client components on Linux, satisfy the following prerequisites:

- Install the eTrust Audit Shared components
- Obtain the name or IP address of the server that serves as the Security Monitor
- Obtain the name or IP address of the Policy Manager server
- Obtain the Policy Manager identification value used during the Policy Manager installation
- Obtain the name or IP address of the Event Management server

Install Shared Components on Linux

The Shared Components are a prerequisite for all of the eTrust Audit components on Linux systems. You must install this software on any Red Hat Linux or SuSe Linux system before installing the other eTrust Audit components.

The shared components installation log file for Linux systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

To install the common components on a Linux system

1. Log on to the UNIX server as root (or superuser).
2. Locate the shared components installation package, AuditShared-r8SP2-8.0.200.xxx.i386.rpm.
3. Run the following command to begin installing the shared components:

   ```
   ./install_AuditShared
   ```

   The End User License Agreement prompt appears.
4. Review the license agreement in a separate session.

   Make a note of the command response after reading the license agreement and return to the installation session.
5. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   All of the subsequent Audit Administrator components use this path during their installations. You can press Enter to accept the default value, /opt/CA/eTrustAudit.

   If the directory name you enter does not yet exist, the installation prompts you for its creation.

   The common components installation begins automatically after the directory is created.

Install Client Components on Linux

You can install Client components on Linux systems to collect and forward event data. The Client installation log file for Linux systems, etaudit.mmddyy.hhmm, is located in the /tmp directory.

Note: Default values for the various prompts are shown in parenthesis. You can accept the default value by pressing Enter.

To begin installing the Client components on a Linux system

1. Log on to the Linux server as root (or superuser).
2. Locate the Client installation package, AuditClient-r8SP2-8.0.200.xxx.i386.rpm.
3. Run the following command to begin installing the Client:

   ```
   ./install_AuditClient
   ```

   The End User License Agreement prompt appears.
4. Review the license agreement in a separate session.

   Make a note of the command response after reading the license agreement and return to the installation session.
5. Type the command response and press Enter to accept the license agreement. If you choose not to accept the license terms, you must exit the installation.
6. Enter the full path to the shared components root directory.

   You can press Enter to accept the default value, shown in parentheses. The default value is the directory you entered while installing the shared components.

To configure the Client for network operations

1. Select an encryption level from the supported levels. The AES 256 bit method is recommended.
2. Enter the name or IP address of the computer that you want to use as the Security Monitor.
3. Enter the name or IP address of the computer where the Policy Manager resides.
4. Indicate whether you want this Client to be registered.

   The default value is yes. Registered clients have a node and host entry in the Policy Manager database, and an audit node created automatically. You can use this node to distribute policies to the Client.
5. Enter the client registration password, if you chose to register the Client.

   The client registration password is created during the Policy Manager installation. You must obtain this password from an administrator or the person who installed the Policy Manager.
6. Enter the name or IP address of the computer where the eTrust Audit Router is installed.

   Use the local server designation, localhost, if the Router is installed on same computer as the Client.

To configure event handling

1. Enter an email Sender name for alerts and event messages.
2. Enter an email Subject for alerts and event messages.
3. Choose whether to send event messages to Event Management.
4. Enter the name or IP address of the Event Management server, if you chose to send event messages.
5. Choose whether to activate the syslog Recorder.
6. Enter the syslog.conf file path.
7. Choose whether to start the Client daemons after installation.

   The Data Tools installation begins.

Chapter 11: Installing Event Recorders

This section contains the following topics:

Event Recorder Overview

This section includes information on installing event recorders for eTrust Audit on Windows and UNIX. Event recorders are iRecorders or SAPI recorders that record or capture events generated by CA or third-party products.

You can download the latest the event recorders and product documentation for the applicable iRecorder or SAPI recorder from SupportConnect on the Customer Support (http://www.ca.com/support) website.

iRecorders

An iRecorder is a dynamically loadable library, called an iSponsor, that plugs into the iGateway service. The iGateway is responsible for all iRecorder command and control functions. The iRecorders are responsible for harvesting events from various systems, applications, and devices, including third-party products. iRecorders can access event data locally or remotely.

Some of the major features and functions of iRecorders include the following:

- iRecorders extract log events from a device or from an event log repository using an API, ODBC, or file I/O.
- iRecorders parse the event fields into tokens and create "Name–Value" pairs for each parsed token.
- Where possible, an iRecorder can start accessing event data from where it last ended, from the beginning of the available log data, or it can start harvesting new event data. The relevant third-party product specifies the handling of log file rotation.
- iRecorders for all database and OPSEC can be deployed locally.
- Beginning with eTrust Audit r8, installing the Client component for Windows installs the iRecorder for NT Event Log by default.

iRecorders are available to resolve a wide variety of event tracking needs. You can find a complete list of the currently available event recorders on the CA SupportConnect website. For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support (http://www.ca.com/support).

SAPI Recorders

SAPI Recorders are software components that record events generated from CA or 3rd-party products. A separate SAPI Recorder exists for each product. A SAPI Recorder sends events to Audit in native Audit format. The communication is based on RPC/UDP SAPI protocol.

Following are examples of SAPI Recorders:

Generic Recorder

You can configure this recorder to collect clear text events from third-party products that maintain their own logs as flat files. Examples of such products include Unix syslog, iPlanet, Netscape web server, Apache web server on Unix.

Database Recorders

A separate SAPI Recorder exists for Sybase, MS SQL Server, DB2, and Oracle.

Mainframe Recorders

A separate SAPI Recorder exists for CA-Top Secret, CA-ACF2, and IBM's RACF.

Other Recorders

Other Recorders include Recorder for Check Point FW-1, SNMP. For more information about the currently available eTrust Audit Recorders, see the Computer Associates Technical Support web site at http://supportconnect.ca.com (http://supportconnect.ca.com/).

SAPI Recorder Data Flow:

- A SAPI Recorder can start accessing event data from where it left off last time, start from the beginning of log data, or start harvesting new event data. Log file rotation is handled as specified by the third-party product
- Recorders access event data either by sampling the event log with a frequency or the Recorder call back functions are invoked whenever log event data is ready.
- Events are parsed into name-value pairs and normalized according to the SAPI data model.
- Normalized events are directly submitted to the Audit Router.
- SAPI Protocol is based on RPC/UDP. By default, the Client uses the Portmapper (port 111) to get the server UDP port on which it is listening and then uses the acquired port to submit events, but can be configured to use fixed ports.

Pre-Installation Requirements

Before installing any event recorders, consider the following information:

- Check the Certification Matrix on the CA Support website: http://ca.com/support (http://ca.com/support) for the following:
  - List of the latest supported platforms for the iRecorder or SAPI Recorder you want to install
  - List of the latest supported versions of third-party software
  - List of required software for the iRecorder or SAPI Recorder you want to install
- Use the event recorder only with the supported version of third-party software.
- Install the Policy Manager and Data Tools on an accessible host on the network.
- If you are installing an event recorder on a computer without an Audit Client, then you must specify the name of the host computer where the iRouter resides during the event recorder installation..
- You can install the event recorder on the same host as the iRouter, or on a different host. We recommend always installing the Client on the same host, as this enables you to filter the data at the lowest level and thus reduce network overhead.
- To use the prepackaged template policies for a specific iRecorder, you must first convert the default policies for that iRecorder, and then import them to the Policy Manager database using the following utilities, respectively:

  [eTrust Auditinstall]\bin\acptf2xml.exe

  [eTrust Auditinstall]\bin\acxml2pmdb

  For more information, see the applicable *eTrust Audit and eTrust Security Command Center Reference Guide.*

How to Install iRecorders

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

1. Download the CAZIPXP.EXE utility, the desired iRecorder package, and the iGateway package from the CA SupportConnect website.
   - Install the latest iGateway package
   - Unzip the downloaded iRecorder package
   - Move the files to the target system manually, if necessary
2. Install the iRecorder on a specific platform or platforms as needed.

   You should decide at this point if you want to perform an attended or a silent install. A silent install allows you to record a response file from one installation and use the response file to facilitate unattended installation of the same iRecorder on other workstations. Instructions for creating response files appear with the installation instructions for each platform type.
   - Install the iRecorder on Windows
   - Install the iRecorder on UNIX
   - Install the iRecorder on Linux
3. Change the iRecorder's configuration files (optional).
4. Create or import, and then distribute, policies to capture events.
   - Import the iRecorder's default policy file to the r8 SP2 Policy Manager database
   - Update the default policy or create a new one

     Refer to the *eTrust Audit and eTrust Security Command Center Administration Guide* or the Policy Manager online help for more information.
   - Distribute the policy to audit nodes

     Refer to the *eTrust Audit and eTrust Security Command Center Administration Guide* or the Policy Manager online help for more information.
5. Test the iRecorder events from the Policy Manager.

   Refer to the *eTrust Audit and eTrust Security Command Center Administration Guide* or the Policy Manager online help for more information.

Download the cazipxp.exe Utility

If you have not already done so, navigate to and download the utility for unpacking CA zip (.caz) files, called cazipxp.exe. The utility is available for use on Windows systems only.

To download the cazipxp utility

1. Access the SupportConnect web site from the Support web site (http://www.ca.com/support).
2. Navigate to Toolbox section under the Downloads navigation section in the left pane.
3. Locate the link for CAZIPXP.EXE and download the utility.

Download and Unzip the Event Recorder Package

Most event recorder packages are contained in CA zip (.caz) files. You unzip these files using the cazipxp.exe utility, which runs on Windows systems. If you are downloading an event recorder for an operating system other than Windows, you need to download and unzip the package on a Windows system and then transfer the files manually to the desired system.

Some event recorder packages are downloaded as Qxxxxxx files, where the six-digit x designates a unique file number. These files contain program fixes available for you to download. (The file name displays in the status bar at the bottom of the browser window when you move the mouse cursor over the link.) Clicking the link to download a program fix "Q file" displays a new page that contains, in its Solutions section, the various file types that you can download. Some Solutions areas offer different download formats dependent upon operating system type. If the downloaded file is not a CA zip file, use the appropriate third-party utility to extract the files.

To download an event recorder

1. Go to the CA SupportConnect website at Customer Support (http://www.ca.com/support).
2. Choose the product home pages link from the Knowledge area in the navigation pane on the left.
3. Select the eTrust Audit product from the drop down list.
4. Select the option for eTrust Audit iRecorders from the latest downloads drop down list.
5. Download the desired specific event recorder package into a local directory.

To unzip an event recorder package

1. Copy the cazipxp.exe utility into the same directory into which you downloaded the event recorder package.
2. Unzip the download package with the cazipxp.exe utility, using the command:

   cazipxp -u *filename.caz*

3. Copy or move the event recorder files to the desired system before installing, if necessary.

Download and Install the Latest iGateway Package

Each iRecorder requires a specific version of the iGateway service. iGateway packages are available for several operating systems as either executable installation programs or shell scripts.

Downloading an event recorder may make it necessary for you to download the latest version of iGateway as well. This can happen in either of the following circumstances:

- You download an event recorder for the first time.
- You download an updated version of the event recorder that requires a new iGateway release.

Note: Event recorder requirements are listed on the same web page from which you downloaded the event recorder package. Refer to that page to find out if you need to download the latest iGateway package in addition to your event recorder.

To download and install the latest iGateway package

1. Download the iGateway installation package for the platform you want into the same directory as the unzipped event recorder installation package.

   You can find a link to the latest iGateway package from the same eTrust Audit Certification Matrix page on which the iRecorders downloads appear.

2. Access a command prompt and navigate to the directory where you downloaded the iGateway package.
3. Run the installation package with the command appropriate for your operating system.

Install an Event Recorder on Windows

You can install an event recorder on Windows to capture events generated by CA or other, third-party products. You must install the iRecorder on the computer where a DSN or DSNs are configured to the eTrust Antivirus event database.

To install the iRecorder

1. Open a command prompt.
2. Navigate to the folder that contains the unzipped iRecorder files.
3. Enter the following command to start iRecorder installation:

   eTrust_Antivirus_version_win32.exe

   The iRecorder installation starts.
4. Enter the DSN, username, and password for the iRecorder database, and click Next.
5. Follow the installation instructions to complete the installation.

   The installer deploys the following files:

   - **Configuration File**--<iRecPackageName>.conf
   - **Library File**--<iRecPackageName>.dll

Note: If the installation reports problems, it may be due to incorrect installation parameters. The problem may be corrected if you uninstall the iRecorder and install it again.

Perform a Silent Installation for Windows

Performing a silent installation requires the following steps:

- Create a custom response file
- Start the installation process

Note: You cannot use silent installation to install an event recorder which is already on your computer. If the event recorder is already present, uninstall it using the Add/Remove Programs utility in the Control Panel before setting up a silent installation.

To create a custom response file for silent installations on Windows target systems

1. Open a command prompt.
2. Navigate to the folder that contains the iRecorder package.

   Note: A sample .iss file may be provided in this directory for you to follow. For best results, we recommend that you create a *new* .iss file specific to your environment.
3. Enter the command:

   <iRecorderPackage>_version_win32.exe /r /f1"PathAndNameOfResponseFile"

   The value for *iRecorderPackage* defines the name of the package. The value for version defines the version number, and *PathAndNameOfResponseFile* defines the full path and file name of the response file. For example, a sample command line might appear as follows:

   <iRecorderPackage>_*version*_win32.exe /r /f1"C:\Temp\iRecorder_setup.iss"
4. Follow the instructions provided by the installation procedure and install the package just as you would on the target system.
5. Click Finish to create the response file to install the event recorder.

To start the installation process

1. Copy the unzipped iRecorder files, or download the iRecorder package, to the target system.

   If you download the iRecorder, you must also download the CAZIPXP.EXE utility to unzip the files.
2. Copy the response file to the target system.
3. Download or copy the appropriate iGateway package to the target system in the same directory as the unzipped iRecorder files and the response file.
4. Navigate to the directory on the target system that contains all of the files listed in the previous steps.
5. Run the iGateway installation program.

6. Enter the following command to install the event recorder silently using the response file:

   <iRecorderPackage>_*version_win32*.exe /s /f1"iRecorder_setup.iss"

   The value for *iRecorderPackage* defines the name of the package. The value for version defines the version number, and *PathAndNameOfResponseFile* defines the full path and file name of the response file.

Perform a Silent Uninstall for Windows

Enter the following command to uninstall the event recorder silently using a response file:

<iRecorderPackage>_*version_win32*.exe /s /f1"irecorder_uninstall.iss"

Install an Event Recorder on UNIX

You can install an event recorder on UNIX or Linux systems to capture events generated from CA or third-party products. The installation instructions that follow apply to supported UNIX versions, AIX, HP-UX, and Solaris.

To install an iRecorder on a UNIX system from a downloaded package

1. Open a command prompt and navigate to the folder that contains the iRecorder package.
2. Enter the following command for the type of UNIX platform on which you are installing the iRecorder:

   Solaris

   eTrust_Antivirus-version-sunos.sh

   AIX

   eTrust_Antivirus-version-aix.sh

   HPUX

   eTrust_Antivirus-version-hpux.sh

   The iRecorder installation starts.
3. Follow the installation instructions to complete the installation.

   The installer deploys the following files:

   - **Configuration File**--eTrust_Antivirus.conf
   - **Library File**--eTrust_Antivirus.so on AIX or Solaris, and eTrust_Antivirus.sl on HP-UX
   - **MP File**–syslog.mp

   After you install the iRecorder you can find the files in the default installation directory, /opt/CA/SharedComponents/iTechnology.

Note: If the installation reports problems, it may be due to incorrect installation parameters. The problem may be corrected if you uninstall the iRecorder and install it again.

To install the event recorder on UNIX from DVD media

1. Log in as the root user.
2. Insert the DVD installation media into the media drive.
   - Solaris mounts your media on a system directory such as /cdrom.
3. Verify that the installation media is available and mounted using the df -k command.

   Locate an entry that contains /cdrom under the heading Mounted on. If the entry exists, the media is mounted.

   If there is no such entry in the df output, mount the media according to instructions in the *Solaris System Administration Manual*. For example:

   ```
   mount –F hsfs –o ro /dev/dsk/c0t1d0/s1s7cc_v10n1 /cdrom
   ```
4. Navigate to the event recorder directory.

   ```
   cd /cdrom/eTrust/Audit/iRecorders/Solaris
   ```
5. Copy the iGateway package to a temporary directory on the local hard disk, for example, /tmp.

   ```
   cp iGateway_40_sunos.sh /tmp
   ```
6. Copy the event recorder package to the same directory as the iGateway package.

   ```
   cp <iRecorderPackage>-version-sunos.sh /tmp
   ```

   iRecorderPackage is the name of the install package file, *version* is the version number, and *os* is the operating system.
7. Navigate to the temporary directory and remove the media.

   ```
   cd /tmp
   umount /cdrom
   ```
8. Run the event recorder installation package.

   ```
   sh <iRecorderPackage>-version-sunos.sh /tmp
   ```
9. Execute the installation script to install the event recorder, for example:

   ```
   ./<iRecorderPackage>-version-sunos.sh
   ```

If the installation reports problems, remove the event recorder and reinstall.

SCC--Perform a Silent Installation for UNIX

Performing a silent installation requires the following steps:

- Create a custom response file
- Start the installation

Note: You cannot use silent installation to install an event recorder which is already on your computer. If the event recorder is already present, uninstall it before setting up a silent installation.

To create a custom response file for silent installations on UNIX target systems

1. Open a command prompt.
2. Navigate to the folder that contains the iRecorder package.

   Note: A sample .iss file may be provided in this directory for you to follow. For best results, we recommend that you create a *new* .iss file specific to your environment.
3. Enter the command:

   <iRecorderPackage>_version_<os>.sh -g *ResponseFileName*

   The value for *iRecorderPackage* defines the name of the package. The value for version defines the version number. The value for *<os>* defines the operating system type you are using, and *ResponseFileName* defines the full path and file name of the response file. For example, a sample command line might appear as follows:

   <iRecorderPackage>*_version*_aix.sh -g opt/CA/eTrustAudit/iRecorders/irecorder_setup.iss
4. Follow the instructions provided by the installation procedure and install the package just as you would on the target system.
5. Click Finish to create the response file to install the event recorder.

To start the installation process

1. Open a command prompt.
2. Copy the unzipped iRecorder files to the target system.
3. Copy the response file to the target system.
4. Download or copy the appropriate iGateway package to the target system in the same directory as the unzipped iRecorder files and the response file.
5. Navigate to the directory on the target system that contains the files from the previous steps.
6. Run the iGateway installation shell script.
7. Enter the following command to install the event recorder silently using the response file:

<iRecorderPackage>_version_<os>.sh -s *ResponseFileName*

The value for *iRecorderPackage* defines the name of the package. The value for version defines the version number. The value for *<os>* defines the operating system type you are using, and *ResponseFileName* defines the full path and file name of the response file.

Perform a Silent Uninstall for UNIX

To uninstall an iRecorder silently

1. Log in as the root user.
2. Open a command prompt.
3. Enter the following command:

   /opt/CA/SharedComponents/iTechnology/recorder_uninstall.sh -u <iRecPackageName>

   The iRecorder is uninstalled silently without any prompts.

Install an Event Recorder on Linux

To install an iRecorder on a Linux system from a downloaded package

1. Open a command prompt and navigate to the folder that contains the iRecorder package.
2. Enter the following command for the type of UNIX platform on which you are installing the iRecorder:

   eTrust_Antivirus-version-linux.sh

   The iRecorder installation starts.
3. Follow the installation instructions to complete the installation.

   The installer deploys the following files:

   - **Configuration File**--eTrust_Antivirus.conf
   - **Library File**--eTrust_Antivirus.so
   - **MP File**–syslog.mp and iptable.mp

   After you install the iRecorder you can find the files in the default installation directory, /opt/CA/SharedComponents/iTechnology.

Note: If the installation reports problems, it may be due to incorrect installation parameters. The problem may be corrected if you uninstall the iRecorder and install it again.

To install the event recorder on Linux from DVD media

1. Log in as root user.
2. Insert the DVD installation media into the media drive.
   - Linux should automatically mount the media on a system directory such as /mnt/cdrom.
3. Verify that the installation media is available and mounted using the df command.

   Locate an entry which starts with /dev/cdrom. If the entry exists, the media is mounted.

   If there is no such entry in the df output, mount the media according to instructions in the *Linux System Administration Manual*. For example:

   ```
   mount –t iso9660 /dev/cdrom /mnt
   ```
4. Navigate to the event recorder directory.

   ```
   cd /mnt/eTrust/Audit/iRecorders/Linux
   ```
5. Copy the iGateway package to a temporary directory on the local hard disk, for example, /tmp.

   ```
   cp iGateway_40_linux.sh /tmp
   ```
6. Copy the event recorder package to the same directory as the iGateway package.

   ```
   cp <iRecorderPackage>-version-linux.sh /tmp
   ```

   iRecorderPackage is the name of the install package file, *version* is the version number, and *os* is the operating system. For example:
7. Navigate to the temp directory and remove the media.

   ```
   cd /tmp
   umount /mnt
   ```
8. Run the event recorder installation package.

   ```
   sh <iRecorderPackage>-version-linux.sh
   ```

If the installation reports problems, remove the event recorder and reinstall.

Perform a Silent Installation on Linux

Performing a silent installation requires the following steps:

- Create a custom response file
- Start the installation

Note: You cannot use silent installation to install an event recorder which is already on your computer. If the event recorder is already present, uninstall it before setting up a silent installation.

To create a custom response file for silent installations on Linux target systems

1. Open a command prompt.
2. Navigate to the folder that contains the iRecorder package.

   Note: A sample .iss file may be provided in this directory for you to follow. For best results, we recommend that you create a *new* .iss file specific to your environment.
3. Enter the command:

   <iRecorderPackage>_version_Linux.sh -g *ResponseFileName*

   The value for *iRecorderPackage* defines the name of the package. The value for version defines the version number. The value for *ResponseFileName* defines the full path and file name of the response file. For example, a sample command line might appear as follows:

   <iRecorderPackage>_*version*_Linux.sh -g opt/CA/eTrustAudit/iRecorders/irecorder_setup.iss
4. Follow the instructions provided by the installation procedure and install the package just as you would on the target system.
5. Click Finish to create the response file to install the event recorder.

To start the installation process

1. Open a command prompt.
2. Copy the unzipped iRecorder files to the target system.
3. Copy the response file to the target system.
4. Download or copy the appropriate iGateway package to the target system in the same directory as the unzipped iRecorder files and the response file.
5. Navigate to the directory on the target system that contains the files from the previous steps.
6. Run the iGateway installation shell script.
7. Enter the following command to install the event recorder silently using the response file:

   <iRecorderPackage>_version_Linux.sh -s *ResponseFileName*

The value for *iRecorderPackage* defines the name of the package. The value for version defines the version number. The value for *ResponseFileName* defines the full path and file name of the response file.

Perform a Silent Uninstall on Linux

To uninstall an iRecorder silently

1. Log in as the root user.
2. Open a command prompt.
3. Enter the following command:

   ```
   /opt/CA/SharedComponents/iTechnology/recorder_uninstall.sh -u <iRecPackageName>
   ```

   The iRecorder is uninstalled silently without any prompts.

Start and Stop iRecorders

The iRecorder runs as a sub-component of the iTechnology iGateway service. When you start the iGateway service, it automatically starts the iRecorder.

To start the iGateway service

1. Open a command prompt.
2. Enter the command:

```
net start igateway
```

To stop the iGateway service

1. Open a command prompt.
2. Enter the command:

```
net stop igateway
```

You can also use the Windows Services Management GUI to start and stop the services on Windows systems.

To start or stop iGateway from the Windows Control Panel

1. Click the Start menu.
2. Select Control Panel.
3. Double-click the Services or Administrative Tools utility icon.
4. Select the Services tab.
5. Select the service and choose start or stop.

Change an iRecorder's Configuration Files

Each iRecorder ships with specific configuration files that control its operation. The iRecorder configuration parameters are automatically set during installation and do not require changes for normal operation. On occasion you may need to turn debugging on or off, or make adjustments to filenames or threshold values. The configuration parameters are in a configuration file, usually located in the iTechnology installation directory.

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

To change an iRecorder's configuration file

1. Stop the iGateway service or daemon before making the changes.
2. Open the eTrustAV.conf configuration file, edit the parameters as required, and save the file.

   Note: For more information about the iRecorder parameters, see the configuration parameters section of the appropriate *iRecorder Reference Guide* or *iRecorder Integration Guide*.
3. Restart the iGateway service.
4. This causes the changes to take effect, and the iRecorder begins collecting events based on the new parameters set in the configuration file.

Converting and Importing Default Policies

When you upgrade to the r8 SP2 Policy Manager, policies contained in the older policy database are automatically migrated to the new database. If you install an iRecorder after you upgrade to the r8 SP2 Policy Manager, you must import the iRecorder's default policy file if you want to use the default policies.

If you are using an iRecorder for a Windows system, you must first convert the policy file from its native .ptf file format to the newer XML file format, using the acptf2xml.exe utility provided with the r8 SP2 software.

To import the policies to the new Policy Manager database, you must use the acxml2pmdb utility.

More information on the utility parameters for importing, exporting and converting policies is available in the *eTrust Audit and eTrust Security Command Center r8 SP2 Reference Guide*.

After converting and importing the default policies, you must add actions for the captured events to the policies with the tools in the Policy Manager interface. More information on these tasks and the related workflow is available in the *r8 SP2 Administration Guide* and the Policy Manager online help.

Chapter 12: Ensuring Your Environment is Operational

This section contains the following topics:

Introduction

After you complete the eTrust Audit component installations, you can test them to ensure that they are installed and configured properly. The SIM system does not collect events until a policy is distributed to one or more audit nodes (ANs). So, to get events flowing in your system, you must first create and distribute a policy. To test the system, you complete the work flows under both the Maker and Checker user roles.

The process for ensuring that your environment is operational includes the following:

1. Start the Audit Administrator.
2. Configure Users and access (see page 153), on first time access only.
3. Basic Maker role work flows: Creating Audit Nodes and Groups (see page 163) and Creating and Submitting a Policy (see page 165)
4. Basic Checker role work flow (see page 178).
5. Review the Activation Log.
6. Create events and test the SIM system event flow.

Important! While you can define a single user with both Maker and Checker role abilities, if the Segregation of Duty option is turned on, that user cannot perform both Maker and Checker tasks on his own policy. A separate user with the Checker role must review the policy to activate it.

When you successfully complete these tasks, you have verified that your eTrust Audit environment is fully operational. If your product implementation is for eTrust Audit only, then you have successfully completed your product implementation and deployment. If your product implementation also includes eTrust Security Command Center, proceed to Installing SCC (see page 197).

Prerequisites - Ensuring the Environment

Before you can verify that your configuration is correct, you must install and configure the necessary components. Before you start the verification process, make sure you have done the following:

- Installed and configured the eTrust Audit core components.
- Installed either Oracle or Microsoft SQL Server on an eTrust Audit computer, if you are using a Collector database. For your particular implementation, you may have installed the database system on a different computer than the eTrust Audit server for remote access.
- Installed at least one eTrust Audit client on a computer in the network, and created and distributed at least one policy to it.
- Downloaded and installed an appropriate iRecorder on the same computer as the eTrust Audit Client.

  Note: It is recommended that you always install the relevant iRecorder on the same computer as the Client. Only the NT iRecorder for Windows systems is supplied with the Client. You would install a remote iRecorder if you needed to communicate through a firewall that does not allow UDP traffic. You can download iRecorders from the CA SupportConnect website, http://ca.com/support (http://ca.com/support).

The SIM system does not collect events until a policy is distributed to one or more audit nodes. So, to get events flowing in your system, you must first create and distribute a policy.

Start the Audit Administrator

You can access the web-based Audit Administrator from your browser window.

Note: On your first use of the Audit Administrator, you must log in as the eTrust Embedded Identity and Access Management (eIAM) server's administrative user so that you can configure users and roles (see page 157) to control their access to the Audit Administrator.

The role associated with your login ID determines the Audit Administrator functionality you see after you log in.

To start the Audit Administrator

1. Start a web browser.
2. Enter the URL:

   https://localhost:5250/spin/auditadmin

   Replace localhost with the server name on which you installed the Audit Administrator software.

   The Audit Administrator login page appears.
3. Log in to the Audit Administrator.

   The default EIAM administrator logon is Eiamadmin and a password configured during installation.

   The Audit Administrator window appears, and defaults to the Configuration tab.

How to Configure Users and Access

You must assign the appropriate roles to one or more users for access to Audit Administrator. The first time you access the interface, you are required to configure user roles. Thereafter, you can access user role functions as needed.

Roles allow users to create and review policies and MP files for distribution to the event sources, perform configuration activities, generate reports, and view events in the SIM system.

The user and access configuration process includes the following steps:

1. Configure access to a directory of users from CA's Management Database (CA-MDB) or from an external LDAP server using the User Source Management (see page 154) functions.

   The CA-MDB is the default user database provided with the Embedded Identity and Access Management (eIAM) server.

   Supported external directories include the Sun ONE directory, Microsoft Active Directory, Novell Directory, and others.

2. Search for users in the directory with the User Management (see page 154) options.

   When using an external directory you can define those users' Audit Administrator roles. When using the internal CA-MDB, you can create users and define their Audit Administrator roles, and set other details.

3. Set the segregation of duties between users with the Maker and Checker roles using the Access Management (see page 162) controls.

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 154)
Access Management (see page 162)

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

Search for Users (see page 155)
Assign or Change User Roles (see page 156)

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

Assign or Change User Roles (see page 156)

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 157) 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

Search for Users (see page 155)

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:

How Basic Maker Work Flows Progress (see page 163)
How Checker Work Flows Progress (see page 178)

Create Users in CA-MDB

These procedures create users who are able to access the eIAM server. If you also want these users to be able to access the Audit Administrator, create them from that interface or add roles to the user from that interface.

To create new users from Audit Administrator

1. Log in to the Audit Administrator as an Admin level user.
2. Click the User and Access Management sub-tab on the Configuration tab, and then click the User Management link.
3. Locate the Users pane below the Search pane.
4. Click the New User icon which is located to the left of the Users node in the tree.
5. Click Add Application User Details to set the Audit Administrator roles for this user.
6. Provide the Global User Details.
7. Search for Global Group Memberships, if used, and add this user to selected groups.
8. Set Authentication parameters.

   Note: If you do not specify an initial password for this user, the person named is not able to log in to the Audit Administrator.
9. Click Save.

   A confirmation message appears.

To create new users from the eIAM server

1. Log in to the Embedded Identity and Access Management server.
2. Click the Manage Identities tab or link.
3. Locate the Users pane below the Search pane.
4. Click the New User icon which is located to the left of the Users node in the tree.
5. Provide the Global User Details.

   If you want this user to access the Audit Administrator, you must set this user's roles in the Audit Administrator interface.
6. Search for Global Group Memberships, if used, and add this user to selected groups.
7. Set Authentication parameters.

   Note: If you do not specify an initial password for this user, the person named is not able to log in to the eIAM Server.
8. Click Save.

A confirmation message appears.

More information

Search for Users (see page 155)
Assign or Change User Roles (see page 156)
Set Passwords and Password Policies from Audit Administrator (see page 161)

Change User Details from Audit Administrator

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.

Change User Details from Audit Administrator

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.

To change global user details from the Embedded Identity and Access Management (eIAM) server

1. Log in to the eIAM server.
2. Click the Manage Identities tab or link.
3. Search for a global user or group in the search pane at the left.

   If the search is successful, user names appear in the Users pane as child nodes of the Users tree.
4. Click on a user name.

   The global user or group details appear to the right.
5. Scroll to the desired section to make necessary changes and then click Save.

More information

Search for Users (see page 155)
Change User Details from Audit Administrator (see page 160)
Assign or Change User Roles (see page 156)

Set Passwords and Password Policies from Audit Administrator

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.
6. Enter and confirm the new password and click Save.

Set Passwords and Password Policies in CA-MDB

Normally you set a password as part of creating a new user. If you need to change a user's password or password policies in the eIAM server, use the following procedure.

To set password policies in the eIAM server

1. Log in to the eIAM server.
2. Click the Configure tab or link.
3. Click the Password Policies link.
4. Select the options that you want to use in your password policy and then set any necessary values.
5. Click Save.

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 on, two different users 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 cannot act as a Checker for a policy or MP file for which he or she was the Maker.
- 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.

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

User Management Tasks (see page 154)
User Source Management (see page 154)

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 163)
2. Creating and Submitting a Policy (see page 165)
3. Creating and Submitting an MP File (see page 172)

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 (see page 177).

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 164) 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 164) 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 procedure.

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

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.

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.

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.

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 166)
2. Create a Policy (see page 166)
3. Create a Policy Rule (see page 167)
4. Add Actions to a Rule (see page 169)
5. Check a Policy Folder (see page 169)

   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 170)

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

1. Commit the Policy (see page 170)

   The Commit function compiles the policy, checking syntax as it goes.
2. Select the policy for activation (see page 171).

   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 171)
4. Recall the Policy Folder

   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.

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.

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.

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.

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 167).

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.

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.

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 .

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 164) 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 189), 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.

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.

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.

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 189).

   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.

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 172)
2. Add an MP File (see page 173)
3. Check an MP Folder

   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 174)

   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 175)
2. Select the MP File for activation (see page 175)
3. Submit the MP Folder (see page 176)
4. Recall the MP Folder

   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.

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.

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.

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.

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 164) 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 189), 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.

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.

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.

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 189).

   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.

How to Work with Folders

You can add or change the objects in a policy or MP folder depending on that folder's state and your user role. The flow of folder states while creating a policy is as follows:

1. When a user with the Maker role begins creating a policy, he must start with a policy folder. The folder has an Inactive status by default. The Maker then creates policies and rules in the folder.
2. The Maker also creates an audit node group and adds audit nodes (ANs) to it. When the Maker attaches a policy folder, or an MP folder, to an AN group, the folder's status becomes Attached. At this point, the Maker has not submitted the folders and their contents for review by a user with the Checker role. A user with the Maker role can create additional objects, or make changes to any of the objects in a policy or MP folder before he submits the folder to a Checker. The Maker is only changing the original, local versions.
3. After the Maker submits the folder for review by a Checker, the folder status changes to Locked. The Checker now has control of the folder and its contents. At this point, the Maker can only recall the folder, which returns the folder to the Attached status. Makers can only recall folders which are not yet approved and distributed.
4. A Checker can Approve or Reject a folder or a specific policy in the folder. If the Checker rejects the folder, its status becomes Rejected. Control of the folder reverts to the Maker. In the resulting work flow, the Maker changes one or more of the objects and then resubmits the folder for review. The folder status remains Rejected until the Maker submits it for another review.
5. After a Checker reviews a folder and approves it, the folder status changes to Activated. No changes are permitted until the folder is distributed to all nodes in the group to which it is attached. After the Policy Manager completes distribution of the folder to all nodes in the attached AN group, the folder status changes to Distributed.
6. A Maker can change a Distributed folder's contents. For example, changing a distributed policy creates a new version (see page 193) of that policy. The Maker must submit the folder containing the changed policy for approval by a Checker. After the policy is approved, its folder status changes from Distributed to Distributed-and-Changed.

   A Maker can also delete a distributed folder with the approval of the Checker. When the Maker clicks on the Delete button, the folder pending status changes to Deleting. The folder is deleted when the Checker approves the folder deletion.

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 189) 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 179)
- Reject a Policy Folder (see page 180)
- Reject a Policy

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 181)
- Reject an MP Folder (see page 182)
- Reject an MP File

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 178)

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 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 178)

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 178)

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 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 178)

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.

View the Events

The final step is to view the collected events in the eTrust Audit Viewer and eTrust Audit Security Monitor. Before you can view collected events from the event sources you are monitoring, you must generate some special occurrences that would trigger events.

You can use the following eTrust Audit components to view and monitor the events generated from our sample policies:

- Check the eTrust Audit Security Monitor for generated events. The view is real-time data that should display constantly changing event data.
- Check the eTrust Audit Viewer for recent events. This component performs an SQL query against the base component database. If events are populating this application, the Collector service is working and sending events to the database properly. You can also launch the Reporter from the Audit Administrator if you have an appropriate level of access.

How Advanced Maker Work Flows Progress

After submission and distribution of a folder, a Maker has a number of advanced tasks related to making changes to the folder or the objects it contains. Whether the folder contains policies or MP files, the Maker may add, remove, or edit the contents of the folder.

Changing a policy or MP file creates a new *version*. A Checker must approve all new policy and MP file versions, just as they did the original version. Deletion of policy or MP folders also requires Checker approval.

Makers may need to make changes to any of the following:

- Audit node groups and audit nodes
- Policy folders and MP folders
- Policies and MP files

Makers need to know how the various object properties interact to make changes to distributed objects more effectively. The sections that follow describe the types of changes and the related object properties.

Audit Node and Group Tasks

When working with audit nodes and groups, it is important to understand the relationship between the various audit node properties (see page 186) and group properties (see page 185). Properties include the states and status of both groups and nodes, which affect the tasks you can perform.

The following are advanced Maker tasks related to audit node groups:

- Delete an audit node from a group
- Add audit nodes to a group
- Remove audit nodes from a group
- Edit node group definitions (Add/Change default actions for all nodes in a group)

The following are advanced Maker tasks related to individual audit nodes:

- Deactivate a node
- Activate a node
- Disable a node
- Enable a node
- Delete a node

The following are special Maker tasks related to audit nodes:

- Create audit node types
- Edit audit node types
- Delete audit node types

Audit Node Group Properties

Audit node (AN) groups have three properties, state, status, and attach condition.

You can use the AN group *state* property to determine whether you can make changes to the group. The status values include the following types:

Unlocked

Indicates that you can make changes to the group, because it is not part of a policy or MP folder awaiting approval.

Locked

Indicates that you cannot make certain changes to the group because it is part of a policy or MP folder awaiting approval, or that distribution of policies or MP files is in progress. If the group state is Locked, you cannot do any of the following things:

- Detach the group from its folder
- Add or remove nodes
- Make changes to a group that has any *pending* status such as In Progress, Deleting, or Detaching

Use the AN group *status* property to determine the progress of enforcing policies or MP files on the nodes in that group. The status values include the following types:

In Progress

Indicates that the distribution server is currently processing the enforcement of policies or MP files. The audit node group state displays Locked while distribution is in progress.

Done

Indicates that the enforcement of policies or MP files on the nodes in the group is complete. You may make changes to the group or the nodes in the group. You need Checker approval to delete or detach a group whose status is Done.

Not Started

Indicates that the enforcement of policies or MP files is not yet in progress. You can delete a group or detach a group from its folder without Checker approval if its status is Not Started.

The *attach condition* property indicates whether the group is attached to a policy folder or MP folder. An AN Group can be either Attached or Free.

Allowed Actions	Attach Condition	State	Status	Approval Required?
Add node Delete group Detach group Remove node	Free	Unlocked	Not Started	No
Add node Delete group Detach group Remove node	Attached	Unlocked	Done	Yes
Delete group Detach group	Attached	Unlocked	Not Started	No

Audit Node Properties

Audit nodes have two properties, status and state.

An audit node's *status* tells you the node's security condition. The status values include the following:

Registered

Indicates a node that has an eTrust Audit client installed and is registered with the Policy Manager.

Enforced

Indicates a node that has policies or MP files distributed to it, and that is actively managed by the Policy Manager.

Tampered

Indicates that changes to the node have occurred since the distribution server distributed a policy or MP file to it. A distribution server option can automatically resend a policy or MP file if a node has Tampered status.

An audit node's *state* tells you if the node is actively receiving policies. The state values include the following:

Enabled

Indicates that the node is actively receiving policies and MP files from the distribution server.

Disabled

Indicates that the node is blocked from receiving policies and MP files from the distribution server. *Disabling* an audit node does not stop it from collecting event data. You might use Disable to stop policy distribution to a node while its software environment is updated or while it is down for maintenance.

Activating a node controls whether or not the node captures and handles event data. *Deactivating* a node prevents further event collection on that individual node by removing the current policy from it. When you Activate a node that you previously Deactivated, the previously used policy is pushed to that node through the distribution server. You might use Deactivate to stop the flow of events from a node that will be down for an extended period.

Pending state values tell you when an audit node's state is changing. You cannot make changes to audit nodes while they are in the following pending states:

Enabling

Displays when you enable nodes that are disabled.

Disabling

Displays when you disable nodes that are enabled.

Deleting

Displays when you delete nodes that are enabled.

Activating

Displays when you activate nodes that are deactivated.

Deactivating

Displays when you deactivate nodes that are activated.

Allowed Actions	Status	State	Approval required?
Delete a node Disable a node Enable a node	Registered	Enabled or Disabled	No

Allowed Actions	Status	State	Approval required?
Activate a node Deactivate a node Delete a node Disable a node Enable a node	Enforced	Enabled or Disabled	Yes

Policy Folder and MP Folder Tasks

When working with folders, it is important to understand the relationship between the folder status and the available tasks.

The following are the advanced Maker tasks for policy folders:

- Change the contents of a distributed policy folder
- Delete distributed policy folder

The following are the advanced Maker tasks for MP folders:

- Change the contents of a distributed MP folder
- Delete distributed MP folder

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

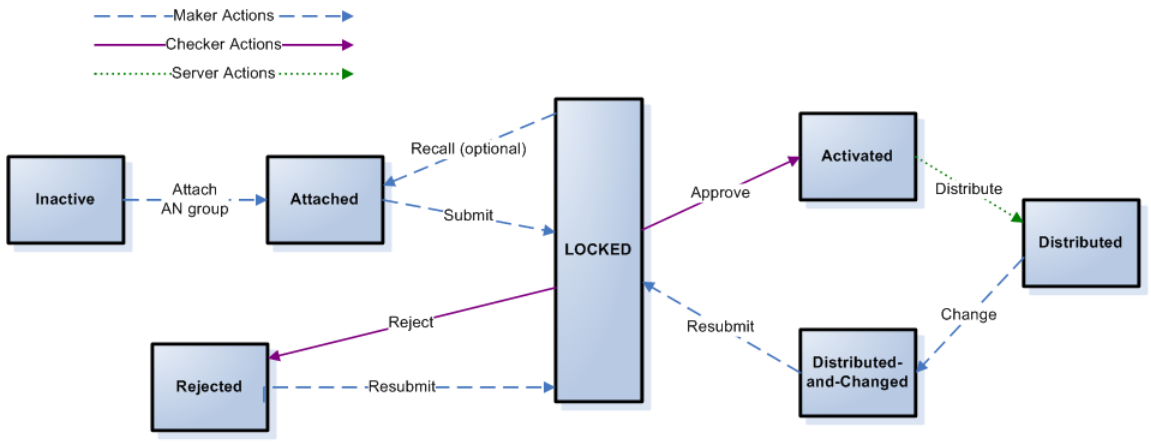
Indicates that the Checker has rejected the folder. The Maker may add, edit or delete policies, rules and MP files at this stage, as well as attach or detach AN groups. The Maker can also resubmit Rejected folders for approval by the Checker.

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.



Pending Folder Status

Deleting

Indicates that a Maker requested the deletion of a distributed folder or MP folder. The Maker sets the folder pending status to Deleting by clicking Delete. The Maker must then submit the Deleting status folder for Checker's approval.

When Checker approves the deletion of the folder, the Distribution Server removes the policies from all the audit nodes, detaches the AN groups from the folder, then deletes the folder (with all of its policies or MP files). Since distributed folders have attached audit node groups, which can contain many nodes, it may take some time to complete folder deletion. No other actions are available on a folder whose pending status is Deleting.

Policy and MP File Tasks

Advanced Maker tasks related to policies and MP files involve making changes to distributed objects. Changes to distributed objects create a new version that the Maker must submit for approval in exactly the same way as the original, using the steps in the Basic Maker Work Flow.

The following are the advanced Maker tasks for policies and policy objects:

- Add a policy
- Deactivate a policy
- Add or remove a policy rule
- Add or remove rule actions
- Delete a distributed policy from a policy folder
- Revert to a different policy version
- Delete a policy folder

The following are the advanced Maker tasks for MP files:

- Add an MP file to a distributed MP folder
- Edit a distributed MP file
- Remove a distributed MP file from a folder
- Revert to an earlier version of an MP file
- Delete an MP folder

Policy and MP File Properties

Policies and MP files have a status property.

A policy or MP file's *status* tells you the object's operational condition. The normal status values include the following:

Working

Displays while the Maker creates, edits, or deletes objects before submitting to a Checker for review.

Ready

Displays after the Maker commits the policy or MP file.

Ready-Select

Displays when an object is approved by the Checker and is distributed on the audit nodes. A Maker can submit changes to objects with this status for review by a Checker. Changing an object with Ready-Select status creates a new version of the object.

Rejected

Displays when a Checker rejects a policy, MP file, or folder. The object remains in Rejected status until a Maker submits the changed object for another review.

Note: A Maker can delete any object in Working, Ready, or Rejected status without approval from the Checker.

A policy or MP file's pending status tells you what operation is currently in progress. The pending status values include the following:

Ready

Indicates that the Maker requested removal of a distributed policy or MP file.

Ready-Select

Indicates that the Maker requested distribution of a policy.

Deleting

Indicates that the Maker requested deletion of a distributed (Ready-Select) policy.

How to Work with Versions

Makers who change distributed policies and MP files must submit their changes for review by a Checker. When the Maker commits the policy or MP file, a new version is created.

The version management actions you can take include the following:

- Revert to a Different Policy Version (see page 194)
- Compare Policy Versions (see page 194)
- Revert to a Different MP File Version (see page 195)
- Compare MP File Versions (see page 195)
- Delete a Policy Version or MP File Version

  Note: If you delete a policy or MP file version that is *not* the current, distributed version, it is removed immediately. If you delete the current, distributed version of the policy or MP file, it takes on the Deleting pending status until it can be removed from all of the nodes in the attached AN group.

Effect of Delete on Versions

The Delete button always deletes only the version of the policy that is visible in the tree. The version a user sees may vary based on that user's role and actions.

If the version that is visible in the tree is a working version, only its Maker author can see the working version. All other users see the current, committed version of the policy in the tree (if any versions are present).

If the Maker deletes that working version, he then sees the committed version in the tree, if any committed versions exist. (This may erroneously appear to be a failure to delete the policy.)

If the Maker deletes a committed (ready) version in the tree, it is removed from the tree.

If the Maker deletes a distributed (ready-select) version in the tree, it is set to *marked for deletion*. When a Checker approves the requested action, the distributed policy is deleted. The policy then has no current version, and is removed from the tree.

Revert to a Different Policy Version

You can revert to a different version of any policy in a distributed folder (see page 189). 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.

Compare Policy Versions

You can compare any two versions of a policy in a distributed folder (see page 189). 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.

Revert to a Different MP File Version

You can revert to a different version of any MP file in a distributed folder (see page 189). 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.

Compare MP File Versions

You can compare any two versions of an MP file in a distributed folder (see page 189). 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.

Chapter 13: Installing eTrust Security Command Center

This section contains the following topics:

Introduction - eTrust Security Command Center

Before you begin your eTrust Security Command Center installation, make sure your hardware and software meet the minimum requirements (see page 34).

After you verify that your event sources are sending data to the eTrust Audit Collector database, you can install the eTrust Security Command Center Server components on the management server.

We recommend that you install the eTrust Security Command Center components in the following order:

- SCC Server

  Installing the SCC Server (see page 55) is the first step in deploying eTrust Security Command Center as part of your SIM solution. This component is installed on the machine serving as the web server for eTrust Security Command Center, and includes software such as CleverPath Portal and other common service components used by both eTrust Security Command Center and eTrust Audit. You must install the SCC Server on a Windows computer.

  Notes:

  - Installation of the SCC Server using Terminal Services or Remote Desktop Connection is not supported. You must install from the media or copy the installation files to a local drive.
  - If you are deploying a Reporting and Compliance (see page 53) solution, installation of the SCC server is the final step. If you are deploying a Status Monitoring and Alerts (see page 53) solution, proceed to the following steps.

- (Optional) Server-side Product Integration Kits (PIKs)

  Installing Server-side PIKs (see page 55) is the second deployment step in implementing eTrust Security Command Center as part of your SIM solution. To integrate events and status from event sources into the menus and features of SCC, install a PIK. Each PIK requires a server component on the SCC server to enable menus and profiles for your product.

- SCC Agents

  Installing the SCC agents (see page 55) is the third eTrust Security Command Center deployment step in your SIM solution. SCC Agents are installed on each event source you want to monitor using SCC, to monitor the status and activities of products (such as firewalls, access software, antivirus servers) and send them as indicators or alarms to your SCC web views.

  Note: The server installation includes the agent components (to monitor processes on the server), so you do not need to perform a separate agent installation on the management server.

- (Optional) Agent-side Product Integration Kits (PIKs)

  Installing agent-side PIKs (see page 55) is the fourth eTrust Security Command Center deployment step in your SIM solution. The SCC Agent on an event source monitors that machine and its services. To integrate events and status from other end-point products into the menus and features of SCC, install a PIK. Each PIK requires the installation of an agent component on the event source machine you want to integrate with SCC.

Most enterprises will have to perform two installation sets on each product server: one for the eTrust Security Command Center agent components and one for the required PIK agent components. You can install all server-side components on your SCC web server machine (SCC server and PIK server components), then proceed to your end-point machines to install SCC agents followed by PIK agents. You must install the SCC server components first because they communicate with the Agent components immediately upon installation.

Note: On UNIX or Linux, PIK agents are installed as part of the SCC agent installation (see page 211).

Installing eTrust Security Command Center on Windows

This section contains instructions for installing or uninstalling eTrust Security Command Center and Product Integration Kits (PIKs) on Microsoft Windows. Check the CA Support website for information on the most recent releases and patches. See the eTrust Security Command Center Readme file for information on your release.

Note: Installing the SCC Server components using Terminal Services or Remote Desktop Connection is not supported.

Install the SCC Server Components on Windows

Install the components only on the machine that you want to use as your eTrust Security Command Center server. This allows you to use eTrust Security Command Center to view event source machines with the Agent components and PIKs installed.

To begin the eTrust Security Command Center server components installation

1. Select the setup application from your installation media.

   The eTrust Security Command Center Install Wizard appears.

2. Click Next to start the installation.

   The End User License Agreement page appears.

3. Review the license and then choose to accept the terms of the agreement. Otherwise, choose to not accept the terms and then exit the installation.

   The Customer Information page appears.

4. Validate the User Name and Company Name.

   The Setup Type page appears.

5. Select Express or Custom install.

   Note: We recommend Express install for most users.

   The Confirm Directory Locations page appears.

6. Configure the installation paths for the selected features.

   Note: If you select a directory and the Edit and Browse buttons remain disabled, you cannot alter these default locations.

   The CleverPath Portal Configuration page appears.

To configure the CleverPath portal

1. Configure CleverPath Portal as follows:

   Host Name

   Displays the local host name by default. Accept the default value.

   Note: The Host Name cannot include the underscore character (_).

   Port Number

   Accept the default value.

   Admin Password

   Accept the default value. You can change it later if you choose. You must enter this admin password when you log into eTrust Security Command Center for the first time.

   SMTP Email Host

Accept the default value or enter the host name of your SMTP mail server.

Tech Support Email

Enter the email address that you want to receive support requests for eTrust Security Command Center users.

Use SSL encryption?

Click Yes if you want to use a secure socket layer (SSL) to transfer data between client browsers and the eTrust Security Command Center server. If you select Yes here, you will be prompted to create a certificate after you click Next on this page.

Note: The Use SSL encryption? field is disabled if your host name begins with a numerical value.

2. If your environment does not use a proxy server, proceed to the next step of this procedure to continue. If it does, click Proxy Settings to configure CleverPath Portal to work with your proxy server. In this case, the CleverPath Portal Proxy Settings page appears, allowing you to enter the appropriate information. When you have entered the desired information, the wizard returns you to the CleverPath Portal Database Configuration page.
3. Click Next on the CleverPath Portal Configuration page.

   If you opted not to use SSL encryption, go to the CleverPath Portal database configuration step of this procedure to continue. If you opted to use it, the SSL Distinguished-Name Information page appears.
4. Enter the appropriate information to generate a certificate.

   Note: If you create a certificate, client browsers receive a warning message when trying to connect to the eTrust Security Command Center server.

   The CleverPath Portal Database Configuration page appears.
5. Accept the CleverPath Portal database default parameters.
6. Click Validate Logon to ensure the database user can connect to the database using that user name and password.

   If the login is not successful, review your database parameters for accuracy. If the login is validated, a message appears stating that the database connection was successful and the Global Catalog page appears.

To configure the Global Catalog and WorldView database

1. Accept the default Global Catalog selection.

   The CA Common Services WorldView Database Configuration page appears.
2. Configure the WorldView database parameters as follows:

Database Type

Accept the default selection.

Database Server

Enter the name of the current system.

Database Admin ID

Accept the default value.

Database Admin PW and Confirm Admin PW

Accept the default value or enter the password for the sa account.

3. Click Validate Logon to ensure that the sa account can connect to SQL Server using the ID and password provided.

   If successful, the Database connection successful message appears.

   The Incident Manager Node page appears.

4. Enter the name of the incident manager node. The incident manager node may be any node you are using as your audit collector.

   The SMTP Server Configuration page appears.

5. Configure the server parameters as follows:

   SMTP Server

   Accept the default value or enter another valid SMTP server name (with or without domain name) or IP address.

   SMTP Port

   Accept the default value of 25 or, if different, enter the port number on which the SMTP server listens.

   User Name

   Enter a valid SMTP server user account name.

   Password and Confirm Password

   Enter the password for the specified user name.

   Note: The password fields may be left blank if the SMTP server does not require a password to authenticate.

   The Start Copying Files page appears.

To verify installation parameters and finish the installation

1. Verify the installation parameters.

   A window appears, showing the installation progress by feature. The Express installation installs iTechnology, CleverPath Portal, CA Common Services, and the eTrust Security Command Center server components, agent components, and documentation. It also imports CleverPath content.

Note: The default installation of CA Common Services installs the WorldView Base component, but not the components for WorldView 3D or Enterprise Management with wireless messaging. To install these components, you must perform a Custom installation.

A log file (esccsetup.log) is created in your computer's TEMP folder or, if this log file already exists from a prior installation, the current data is appended to it.

When all of the files are copied, the Setup Options page appears.

2. If you already have Java 2 Runtime Environment (J2RE) V1.4.2_10 installed on your server machine, deselect the check box. If you do not yet have J2RE V1.4.2_10 installed, leave the check box selected. If you opt to install or upgrade J2RE, a Java installation wizard appears. Follow the wizard to complete the Java installation and return to the eTrust Security Command Center server installation.

   A second Setup Options page appears.

3. You are prompted to review the Readme file. Indicate whether you want to do so now by selecting or deselecting the check box.

   A dialog appears, giving you the choice to restart now or later.

4. Choose to restart your system now or later.

5. Exit the installation wizard when all selections are complete.

   The eTrust Security Command Center server components are installed.

Install the PIK Server-Side Components

There are server-side and agent-side PIK components for eTrust Security Command Center. Install the server-side PIK components on the eTrust Security Command Center server and the agent-side PIK components on every event source with products that you want eTrust Security Command Center to monitor and integrate.

Note: You must install the eTrust Security Command Center server components before you can install PIKs.

You can perform a quick default installation of the PIK components on multiple machines using Silent Installation (see page 315).

To install the PIK server components

1. Select the desired PIK setup application from your installation media.

   The PIK installation wizard opens and displays the Welcome page.

2. Click Next.

   The Select Features page appears. This page lets you choose which PIK components (server, agent, or both) you want to install on the current host.

3. Select the Server Integration Components check box for each component that you want to install.

   Note: To access the CA Common Services features (such as WorldView and Enterprise Management) in eTrust Security Command Center, you must install both the server-side and agent-side PIKs for Unicenter, available from the Unicenter Integration Kits branch.

   The CleverPath Configuration page appears.

4. Enter the CleverPath Admin ID and Password.

   The Start Copying Files page appears.

5. Click Next.

   A progress window appears to show installation progress by feature. The portal service stops and the required files are copied to the machine.

6. Click Finish to complete the installation.

   The PIK is now installed on your SCC server.

Install the Agent Components on Windows

Install the eTrust Security Command Center agent components on every product server and event source that you want eTrust Security Command Center to monitor.

Note: If you attempt to install the agent components on the eTrust Security Command Center server machine, you will receive an error message that they are already installed. This is because the eTrust Security Command Center agent components are installed by default when the eTrust Security Command Center server components are installed.

You can perform a quick default installation of the agent components on multiple machines using Silent Installation (see page 315).

To install the eTrust Security Command Center agent components

1. Select the Agent setup application from your installation media.

   The eTrust Security Command Center Install Wizard appears.

2. Click Next to start the installation.

   The End User License Agreement page appears.

3. Review the license and accept the terms of the agreement. If you choose to not accept the terms, the installation exits.

   Note: You must scroll or page down to the end of the agreement to accept it and continue with the installation.

   The Customer Information page appears.

4. Validate the User Name and Company Name.

   The Setup Type page appears.

5. Accept the default selection, Express.

   The Confirm Directory Locations page appears.

6. Configure the installation paths for the selected features.

   Note: If you select a directory and the Edit and Browse buttons remain disabled, you cannot alter these default locations.

   The World Manager Node page appears.

7. Enter the name of the server on which you installed the eTrust Security Command Center Server components.

   The Start Copying Files page appears.

8. Verify the installation parameters and start the installation.

A progress window appears, showing the installation progress by feature. The Express installation installs the iTechnology, eTrust Common Services, and the eTrust Security Command Center agent components (product interface and Status Monitor).

The installation creates a log file (esccsetup.log) in your computer's TEMP folder, or appends current data to the log file if it already exists from a prior installation.

9. Select the check box to review the Readme file now, if desired.
10. Exit the installation wizard when all selections are complete.

    The eTrust Security Command Center agent components are installed.

Install the Product Integration Kit Components on Windows

There are server-side and agent-side PIK components for eTrust Security Command Center. Install the server-side PIK components on the eTrust Security Command Center server and the agent-side PIK component on every event source with products that you want eTrust Security Command Center to monitor and integrate.

Note: You must install the eTrust Security Command Center server or agent components before you can install the PIKs.

You can perform a quick default installation of the PIK components on multiple machines using Silent Installation (see page 315).

To install the PIK agent components

1. Connect to the SupportConnect website and download the desired PIK installation packages.
2. Uncompress the downloaded PIK packages into a single install directory.

   Note: Be sure to preserve the most recent setup.exe file.
3. Execute the PIK setup.exe program.

   The PIK installation wizard opens and displays the Welcome page.
4. Click Next.

   The Select Features page appears. This page lets you choose which PIK agent components you want to install on the current host.

   Note: If a software product is not installed on this machine, that product's PIK is unavailable here. However, PIKs for physical devices are always available.
5. Select the Agent Integration Components check box for each component that you want to install.

   Note: To access the CA Common Services features (such as WorldView and Enterprise Management) in eTrust Security Command Center, you must install both the server-side and agent-side PIKs for Unicenter, available from the Unicenter Integration Kits branch.

   The Start Copying Files page appears.
6. Click Next.

   A progress window appears to show installation progress by feature. The portal service stops and the required files are copied to the machine.

   If your PIK has an associated iRecorder, the wizard prompts you to install the iRecorder. When the file copy is complete, the iTechnology iRecorder Installations page appears. For more information, see the applicable *eTrust Audit iRecorder Reference Guide*.

If your PIK has no associated iRecorder, go to the final step to complete the installation.

7. Click Yes to confirm the iRecorder install.

   The iRecorder Install Wizard appears

8. Click Next to begin installing the iRecorder.

   The License Agreement page appears.

9. Review the license and then choose to accept the terms of the agreement. Otherwise, choose to not accept the terms and then exit the installation.

   Note: You must either scroll down or Page Down to the end of the agreement to continue with the installation.

   The Install is now setting up iControl page appears.

10. Enter the host name of the machine where the iRouter is installed.

    The Configuration options page appears

11. Select the desired configuration options.

    The Start Copying Files page appears.

12. Click Next.

    A progress window appears to show installation progress by feature. The installation copies the required files to the machine and the portal service automatically restarts. A page appears informing you that the eTrust Audit iRecorder installation is complete.

13. Click Finish to complete the installation.

    The agent PIK is installed.

Modify the Installation

You can modify your eTrust Security Command Center Agents by installing or removing components manually, or by using silent installation/uninstallation (see page 315).

To modify your Agent components manually

1. Access the Windows Control Panel.
2. Select the Add or Remove Programs utility.

   Highlight the Agent component you want to modify and then click Change/Remove.
3. Select Modify.

   The Select Features page appears.

   Note: This same page appears when you perform a Custom installation of the eTrust Security Command Center server components.
4. Select the check boxes for all products that you want to install and deselect the check boxes for any that you do not want to install.

   The Start Copying Files page appears.
5. Verify the installation parameters to begin the installation.

   A window appears showing installation progress by feature.

   The Agent modification is complete.

Verify the Installation

You can verify that your installation of eTrust Security Command Center is successful by logging in to the CleverPath Portal workplace.

To verify that the eTrust Security Command Center installation is successful

1. Restart your computer.
2. Open a web browser and enter the appropriate URL.
   - If you selected the SSL option, enter:

     https://*hostname*:8080

   - If you did not select the SSL option, enter:

     http://*hostname*:8080

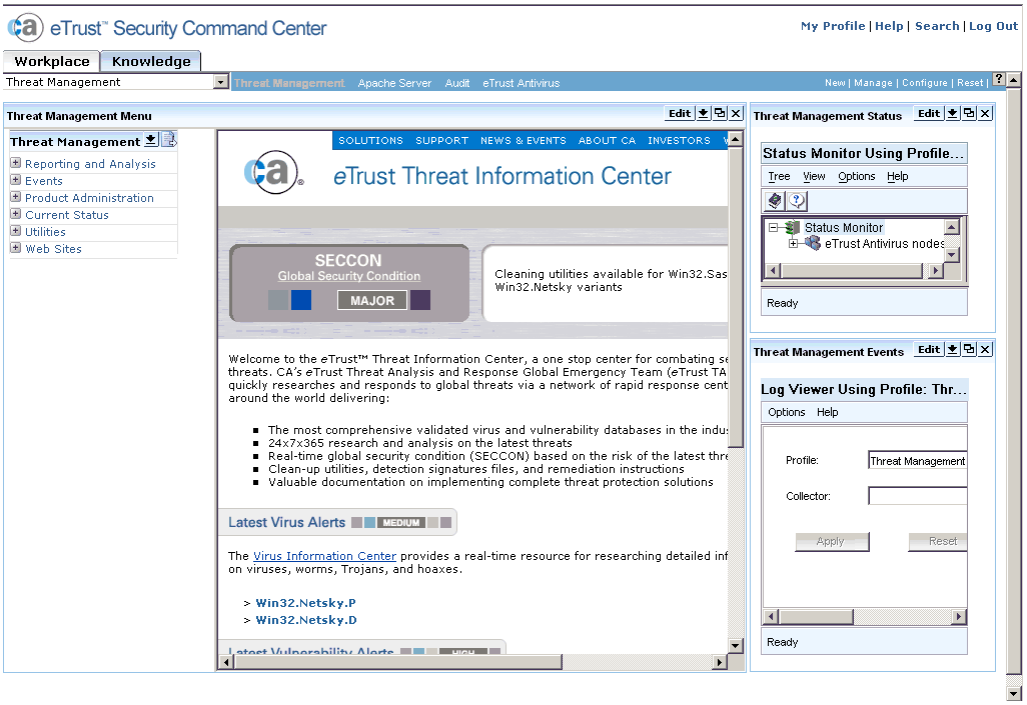
   hostname

   Identifies the system on which the eTrust Security Command Center server is running.

   Note: You must enter the host name of the system, not an IP address. You cannot enter **localhost**.

   eTrust Security Command Center opens and the login page appears.
3. Enter the user name and password that you specified during installation.

   The eTrust Security Command Center window appears.



If your window does not resemble this illustration, see Troubleshooting (see page 267) to diagnose and correct the problem. If it does, you can verify the eTrust Security Command Center workplace functions.

Installing eTrust Security Command Center on UNIX or Linux

The following topics contain instructions for installing and uninstalling eTrust Security Command Center agent components on UNIX or Linux.

Note: You can perform a quick default installation of the agent components on multiple machines using Silent Installation (see page 315).

Important! The eTrust Security Command Center server can only be installed on a Windows machine. That installation should be completed before proceeding with the agent installation described here.

On UNIX or Linux, PIK agents are installed as part of the SCC agent installation. See the CA SupportConnect website for a full list of available product PIKs.

Requirements

The basic installation requires the following:

- Name of the machine serving as the Status Monitor Manager host

The optional installation of the Audit Data Tools Integration Kit requires the following:

- Oracle User ID and password
- Oracle home directory
- Oracle Service ID

  Note: You can configure this information later by executing eAuditVwAgentConfig.

How to Install Agent Components on UNIX or Linux

The process of installing eTrust Security Command Center agent components on a UNIX or Linux system involves running the installation and some configuration. Specifically, this process includes the following steps:

1. Mount the installation media (see page 212).
2. Check the directory structure and main files (see page 212).
3. Run the installation script (see page 213).
4. Tune kernel parameters for Interprocess Communications (IPC) and eTrust Common Services (see page 215).
5. Apply patches (see page 217).

Mount the Installation Media

To install the product from your installation media, follow these steps:

1. Log in to the UNIX or Linux machine as **root** (or superuser).
2. Insert the appropriate product installation media in the drive.

   Note: We recommend that you close any applications you have running before you insert the product installation media.
3. Change the installation directory for the eTrust Security Command Center components to UNIX or Linux by entering the following command:

   cd /*[MEDIA_MOUNT_POINT]* / *[PLATFORM]* /*eSCC/Agents*

   where *[MEDIA_MOUNT_POINT]* is the path to the drive on which the installation media is mounted, and *[PLATFORM]* is AIX, HP-UX, Linux, or Solaris, as appropriate. The *eSCC/Agents* subdirectory includes the installation files for the specific platform.

Check the Directory Structure and Main Files

Before you begin the installation, list the distribution files on your product installation media to ensure you have everything necessary. To identify these files, follow these steps:

1. Enter the following list command from your *[MEDIA_MOUNT_POINT]* / [PLATFORM] /eSCC/Agents directory:

   ls
2. Verify that the required files reside in the following directories:

Directory	Description
eCS	eTrust Common Services software components

Directory	Description
eSCC	eTrust Security Command Center software components
iTechnologies	iGateway, iRecorder, and other iTechnology software
patches	OS patches from operating system vendors, present only if needed for the platform (several levels of subdirectories exist according to OS platform and version)
nls	Support files necessary for localization/internationalization

3. Verify that the following files are in the indicated location:

File	Description
setup.sh	The master installation shell script
eCS/readme_install.txt	A Readme file for installation of eTrust Common Services on UNIX

Run the Installation Script

While still logged in as the root user, enter the following command from the UNIX or Linux shell prompt to execute the setup.sh shell script.

```
./setup.sh
```

The installation script starts and guides you through the remaining tasks and creates an installation log file (/tmp/eSCC_setup.YYMMDD.HHMMSS.log) where YYMMDD.HHMMSS is the date and time of the installation.

Installation Script Functions

The installation script performs the following tasks in this order:

- Installs eTrust Common Services, if necessary
- Installs eTrust Security Command Center
- Extracts and updates tar (archive) files to target directories
- Creates symbolic links for eTrust Security Command Center shared libraries from the /opt/CA/SharedComponents/lib directory
- Creates the required registry entries
- If you are installing the eTrust Audit Data Tools Integration Kit for Solaris, AIX and HP platforms, asks for Oracle user ID and password account access information and saves this information in an encrypted format
- Detects if any security products for which eTrust Security Command Center has Product Integration Kits are present on the agent machine and, if so, prompts you to proceed with the PIK installation for those products
- Records the progress of the installation in the following log file: /tmp/eSCC_setup.YYMMDD.HHMMSS.log) where YYMMDD.HHMMSS is the date and time of the installation

Tune Kernel Parameters for Interprocess Communications (IPC) and eTrust Common Services

If the kernel parameters on the installed machine are lower than the minimum requirements, the installation script displays a message specifying the minimum recommended values.

Note: These are the minimum recommended values, so if you have other software that uses IPCs, you may need higher settings.

You may have to increase the parameter values for the installation to continue. For example, you may receive a message as follows:

```
Checking kernel parameters for required minimum values...
==================================================
* ERROR * ERROR * ERROR * ERROR * ERROR * ERROR *

The following tunable kernel parameters have values lower
than the minimum required values for this eTrust product
on this platform. Installation cannot continue.
Please examine the current and required values below.

Parameter    Current    Required
                        value     value
_____________ _______ _________
semmns                    60       184
semmsl        25        128

This installation procedure will now terminate.
Please update the kernel parameters shown above, then
run this installation again.
This information is saved in file /tmp/kernparmchk.out
for your future reference.
For more information, see the readme_install.txt file in <MEDIA_MOUNT_POINT>/eCS.
==================================================
```

To continue, press the Enter key and reconfigure your kernel parameters using the appropriate method. The following topics provide platform-specific methods for updating kernel parameters. For more information, see the vendor-supplied documentation for your platform and system.

Note: AIX does not require configuration of kernel parameters.

Configure Solaris Kernel Parameters

To configure the kernel parameters for a Solaris machine, follow these steps:

1. Edit the /etc/system file and add the required lines. Instead of these sample values, you should use the values suggested in the setup procedure:

   ```
   set msgsys:msginfo_msgmni=64
   set semsys:seminfo_semmns=256
   set semsys:seminfo_semmsl=128
   set shmsys:shminfo_shmmni=512
   ```

2. Restart the system.

Configure HP-UX Kernel Parameters

To configure kernel parameters for an HP-UX machine, follow these steps:

1. Enter the following command:

   ```
   sam
   ```

2. Select Kernel Configuration.
3. Select Configurable Parameters.
4. Select Actions.
5. Select Create A New Kernel.
6. Change settings as required.
7. After rebuilding the kernel, restart the system.

Configure Linux Kernel Parameters

To configure kernel parameters for a Red Hat Linux machine, use the sysctl command to change the kernel IPC values without restarting. For example, enter the following:

```
sysctl -w kernel.msgmni=64
```

However, the sysctl command is only available in recent releases of Linux. If it is not available in your version, follow these steps:

1. Edit the appropriate header files. For example, enter:

   ```
   /usr/src/linux-2.4/include/linux/msg.h
   ```

2. Change the appropriate #define statements. For example, enter:

   ```
   #define MSGMNI 64  /* <= IPCMNI */  /* max # of msg queue identifiers */
   ```

3. Rebuild the kernel using the instructions available from Linux Online (http://www.linux.org).
4. Restart the system.

Apply Patches

The installation procedure determines whether the C++ runtime library meets the minimum requirements. If not, then you must apply the proper operating system patches.

For Solaris (any version), the file /usr/lib/libCrun.so1 must exist. Review the contents of the patches/SunOS directory. It contains patches for different versions of Solaris. For Solaris 5.8 specifically, download the patches 108434 and 109147, or later Solaris Patch Clusters from http://sunsolve.sun.com (http:\\sunsolve.sun.com).

For AIX, the following files must exist and their versions must be 5.0.2.0 or higher:

- xlC.rte
- xlC.msg.en_US.rte
- xlC.aix43.rte or xlC.aix50.rte for AIX 5L series

Use either of the following methods to meet the minimum requirements:

- Install a Runtime PTF for VisualAge C++ for AIX, such as APAR IY17981.
- Upgrade your AIX OS level to 4.3.3.10 level or higher.

For Linux, the file /usr/lib/libstdc++-libc6.2-2.so3 must exist. If the proper libstdc++ package does not exist, you can find it at the vendor's web site (http://www.redhat.com (http://www.redhat.com)). You can then download and install the patch.

Install the Product Integration Kit Components on UNIX

There are server-side and agent-side PIK components for eTrust Security Command Center. Install the server-side PIK components on the eTrust Security Command Center server and the agent-side PIK components on every event source with products that you want eTrust Security Command Center to monitor and integrate.

Note: You must install the eTrust Security Command Center server or agent components before you can install PIKs.

You can perform a quick default installation of the PIK components on multiple machines using Silent Installation.

To install the PIK agent components

1. Connect to SupportConnect and download the PIKs you want.
2. Uncompress the downloaded PIK packages into a single install directory, for instance /tmp/SCCPIKS. Note that when doing this, be sure to preserve the most recent setupPIK.sh file.
3. Execute the script setupPIK.sh from SCC script path, for example. /opt/CA/eTrustSecurityCommandCenter/scripts, as the following syntax:

   ```
   /opt/CA/eTrustSecurityCommandCenter/scripts/setupPIK.sh /tmp/SCCPIKS
   ```

   where /tmp/SCCPIKS is the directory where the PIK package(s) reside.
4. The PIK install process will guide users through each PIK found under specified directory interactively.

Start eTrust Security Command Center

At the end of the eTrust Security Command Center agent installation, you will be prompted to start eTrust Security Command Center. If you choose to do so, eTrust Security Command Center will be launched immediately after installation. If not, you will need to use the start shell script to manually start eTrust Security Command Center.

Additionally, you will need to execute the start shell script after all UNIX/Linux agent machine restarts. The eTrust Security Command Center agent is not configured to start automatically with the system. Therefore, each time the system is restarted, you will need to run the start shell script.

To start eTrust Security Command Center on a UNIX or Linux machine, follow these steps:

1. Open a default UNIX shell. Change your directory to the path on which you installed the eTrust Security Command Center agent, as follows:

   ```
   cd /[installation_path]/scripts
   ```

   For example, you could enter:

   ```
   cd /opt/CA/eTrustSecurityCommandCenter/scripts
   ```

2. Run the start.sh shell script. To do so, enter the following command:

   ```
   ./start.sh
   ```

Chapter 14: Establishing the eTrust Security Command Center Environment

This section contains the following topics:

Getting Started with SCC

This section contains information and instructions on important eTrust Security Command Center tasks, including:

- Using table collectors for event storage and viewing
- Reporting and analysis on product content
- Monitoring events on your event source machines
- Using product administration to access native product interfaces
- Running SCC utilities

Nodes

Nodes are the servers that run the products that you want to manage and monitor. Nodes are automatically added to your menu profiles. For example, after you install the eTrust Security Command Center agent components, you might notice that a node such as systemA is running three CA products: eTrust Policy Compliance, eTrust Antivirus, and eTrust Intrusion Detection.

After you install an agent on a system running an eTrust or third-party application, it provides the appropriate information to discover the node and initiate status reporting to eTrust Security Command Center. When you install the eTrust Security Command Center agent components on the product servers, the agent notifies eTrust Security Command Center that this node is running the application and the following happens automatically:

- The agent on the node sends the status of services, processes, and daemons to the Status Monitor Manager.

  Note: eTrust Security Command Center only supports Internet Protocol version 4.0 for IP addresses of Status Monitor components.

- If the eTrust Audit client components are installed on the node, it routes events to the default audit collector according to an audit policy, which results in these events displaying in the Log Viewer (the main type of event viewer) in eTrust Security Command Center.

- The eTrust Security Command Center updates all menus that can access eTrust Antivirus to reflect the availability of eTrust Antivirus reporting services on this node.

For more information about eTrust Audit or eTrust Antivirus, see the appropriate product documentation.

Note: While an administrator must define menu profiles, application groups, and applications, the list of nodes that appears in a menu is dynamic. You can use the Administrative Controls interface in the Administration workplace to add additional nodes or to create node groups.

Using Table Collectors

eTrust Security Command Center supports custom tables for focused event storage and viewing, customized reporting, and post-collection analysis. The use of table collectors helps you to decipher cryptic event logs from various products, without altering the actual events. These tables act as "databases" that sort and filter the event data from their built-in audit logs. Whereas the default audit database is the collector that lets you view all log events in their original form, table collectors let you store events in custom tables according to your own parameters. This focuses and reduces the number of overall events that the Log Viewer has to retrieve, and adds flexibility and clarity to your view of the data.

You can use the Log Viewer to view both the default audit collector database and table collector events. However, you can do more with table collectors than with the default database, such as tracking incident priorities, owners, and pending status. Additionally, table collectors make it possible for external reporting tools such as CleverPath Reporter and Crystal Reports to access the data, enabling you to create custom reports.

The functionality of table collectors includes the following:

- Smaller row and column counts per table
- Granular control of indexes
- Configurable column names, sizes, and types
- Focused record filtering per table
- Configurable timeframes for data cleanup and reduction tasks
- Import and export facilities

Sample table collectors for particular PIKs are packaged with eTrust Security Command Center. There are also sample table collectors for various categories of events (such as lognames and taxonomy) provided in the default Audit workplace. These can be used to make additional table collectors that are more globally applicable than those relating to particular PIK products.

Note: If you want to customize a sample table collector, it is highly recommended that you first make a copy of the sample and then modify it, instead of changing the sample directly. It is also recommended that you copy the sample table collector to a non-default, non-PIK-specific menu profile in order to facilitate the eTrust Security Command Center upgrade process.

You can also create new custom table collectors from scratch. There are two ways to create a new table collector. You can create a table collector manually or automatically generate one from specified audit logs using a wizard.

Note: For performance reasons, it is highly recommended that you do not create or generate table collectors during normal business hours. Additionally, it is recommended that you do not generate new table collectors for large, existing audit collector databases. Instead, you should either use one of the supplied sample table collectors or you should create a copy of an existing table collector and customize the copy to fit your needs.

To use table collectors, you must first define and configure each table collector you want to use. Then, you must activate it by enabling the collector policy and refreshing the service. For more information, see The Process of Activating a Table Collector (see page 240).

Table Collector Criteria

Before you create a new table collector, you must decide what data you want to store in it. Careful planning is required because you cannot update the table after it is created. Therefore, you must decide in advance what fields you need to have available for later use.

Once you decide your criteria for the table collector, you can use the Generate Table Collector wizard or a manual process to create the table.

Note: You should only use the Table Collector Wizard on small databases (less than 1 million records). For larger databases, the recommended approach is to select one of the sample Table Collector definitions, copy it, and modify it to suit your needs.

Table Collector Generation

The Generate Table Collector wizard lets you gather audit lognames and the field names belonging to the lognames to prepopulate your schema definition for the new table. You can also add fields manually, which may be necessary when working with the audit fields that are not normalized between products with similar functions.

The wizard lets you do the following:

- Determine the table collector size and select the audit nodes
- Designate any field as a database index, which is useful in cases where the event viewer profiles key in on certain fields
- Eliminate specific records from inclusion in this table collector.

  Note: The use of filters is optional but highly recommended.
- Map different logname event fields to similar database columns

  For example, two products can have different named fields for status. You can map these fields to the same database column called "Status" in the table collector, which supports the normalization of different data elements.
- Define additional programmatic actions to occur on the defined eTrust Security Command Center node or node group when table collector events meet your specified filtering criteria

Generate a Table Collector from Audit Logs

To generate a table collector using the Generate Table Collector Wizard

1. Expand the Security Command Center Administration branch. Click the Table Collectors item that appears under that branch.

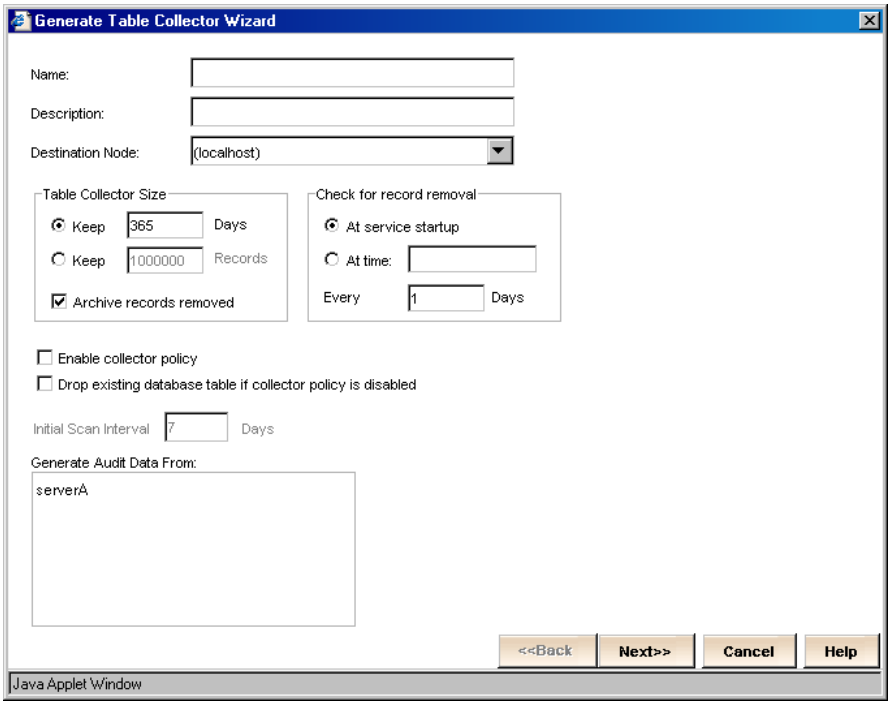
   The Table Collectors interface appears.

2. Click the Hide Menu button to make the Administration menu disappear, thus freeing up more space.

   As with the other applications, the left side of the display contains a tree menu. In this case, the items in the tree are table collectors. The right side is a work area.

3. To generate a table collector from one or more audit logs, select an existing collector and click the Generate a Table Collector from Audit Log tool bar button, or right-click Table Collectors and, from the pop-up menu, choose **Generate**.

   The Generate Table Collector Wizard appears, with the following page displayed:



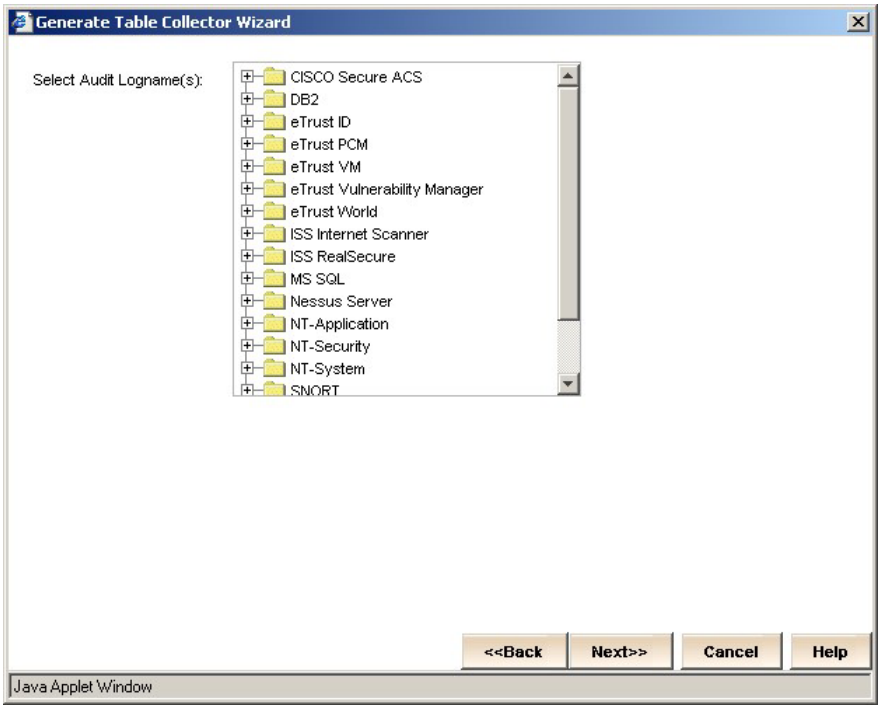
4. Enter the appropriate basic information.
   - In the Name field, enter the name of your new table collector.

     Note: The Name field stores a maximum of 30 characters.
   - In the Description field, enter a description for this collector.
   - From the Destination Node drop-down list, choose the machine to which to send the table collector events.
   - In the Table Collector Size box, select the maximum number of days or records to keep in this table collector and whether archived records should be removed.
   - In the Check for record removal box, indicate when you would like records removed if the size of the collector database gets too large or archived records are to be removed.
   - Click the Enable collector policy check box if you want to activate an audit scan, which causes the table to periodically update itself with any new records in the source audit logs.
   - Click the Drop existing database table if collector policy is disabled check box if you want the associated database table to be automatically deleted when you refresh the service (distribute option) if the table collector is not currently enabled.

     Important! It is recommended that you keep the Enable collector policy check box deselected for any table collectors you are not currently using. However, if your Drop existing database table if collector policy is disabled check box is selected, disabling your collector policy may result in an unrecoverable loss of data, so use extreme caution.
   - Indicate the amount of time (in days) to go back and obtain events to populate the table collector in the Initial Scan Interval field, which is only available if the Enable collector policy check box is selected. The value entered here only applies to the first time your table collector obtains events. After the initial scan, the global Scan Interval is used to refresh the events.
   - In the Select Audit Node box, click the machine on which your audit components are running. This setting will gather columns from this node as candidates for inclusion into a table collector schema.

When you are finished, click Next.

The following page appears:



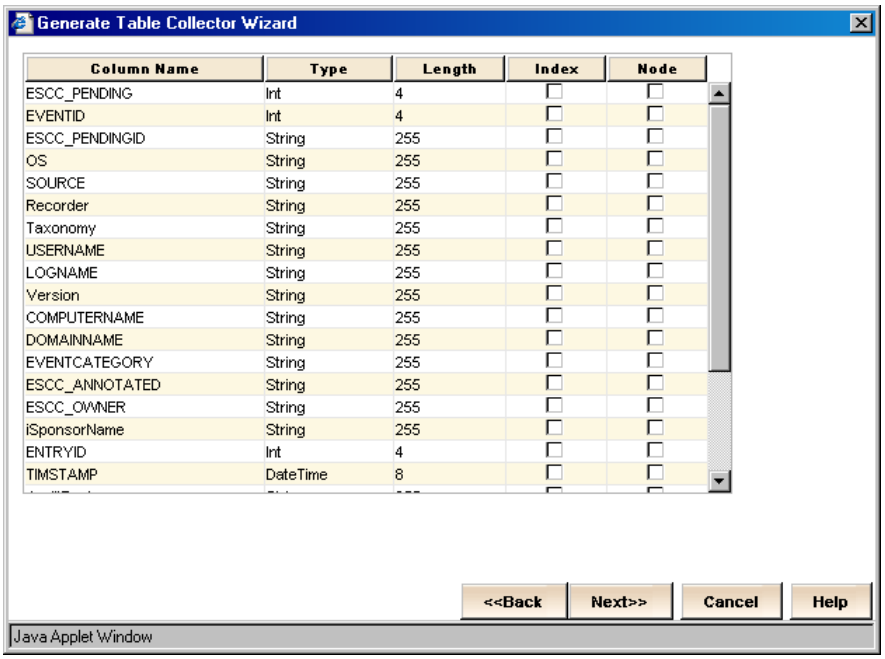
5. Expand the branches of the tree until you locate the audit logs from which you want to generate this table collector. Select them, and then click Next.

   Note: Use the **Shift** or **Ctrl** key to select multiple lognames.

   A status window appears, showing the retrieval and parsing of table data for that log, and generating the table and columns.

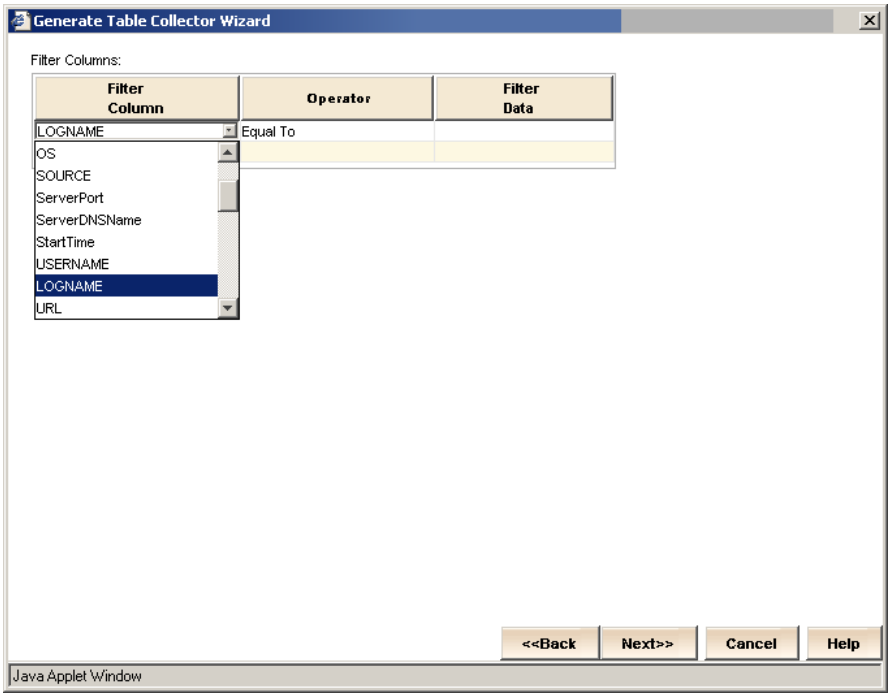
6. Click Next.

   The following page appears:



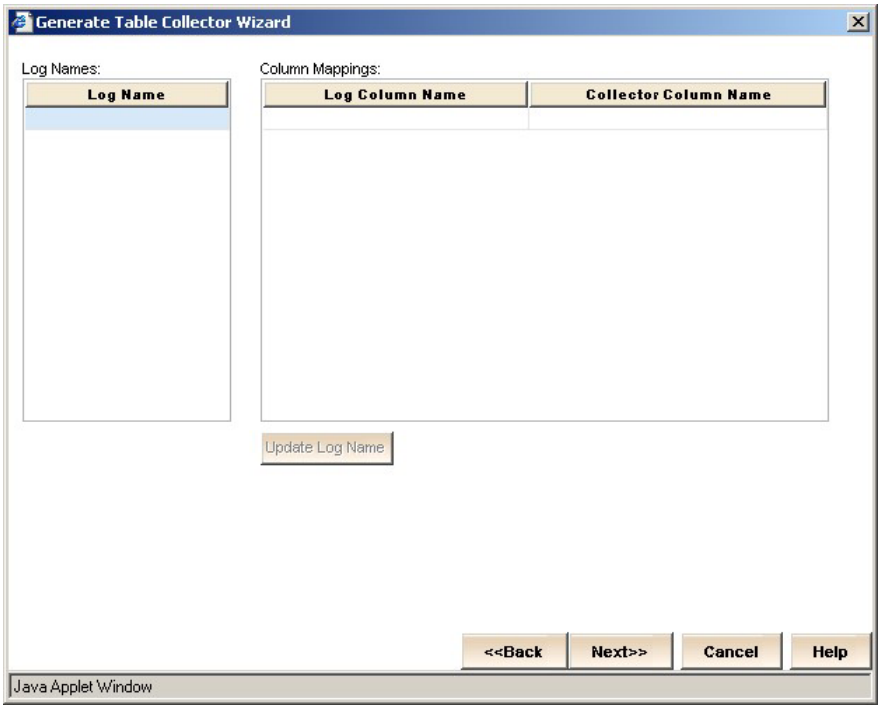
7. Click the Index check boxes next to the columns you want to use as database indices. Click the Node check boxes next to the columns for which you want any node-related information, such as machine name, IP address, or fully qualified domain name, to be normalized to the machine.domain.name form. When you are finished, click Next.

   The following page appears:



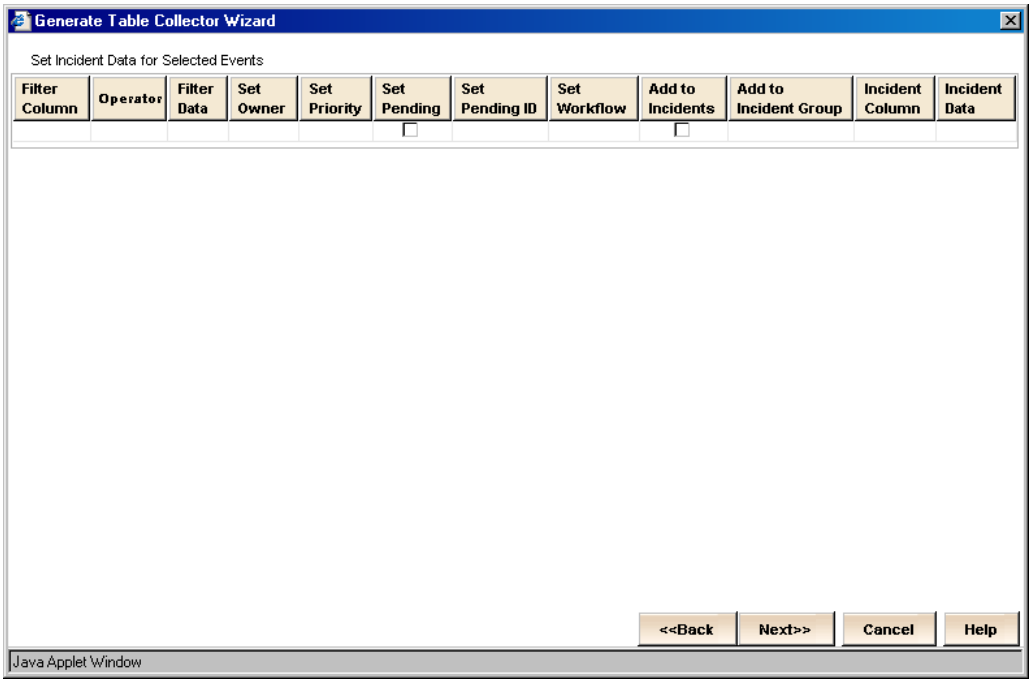
8. Set your filter criteria. Click Next.

   The following page appears:



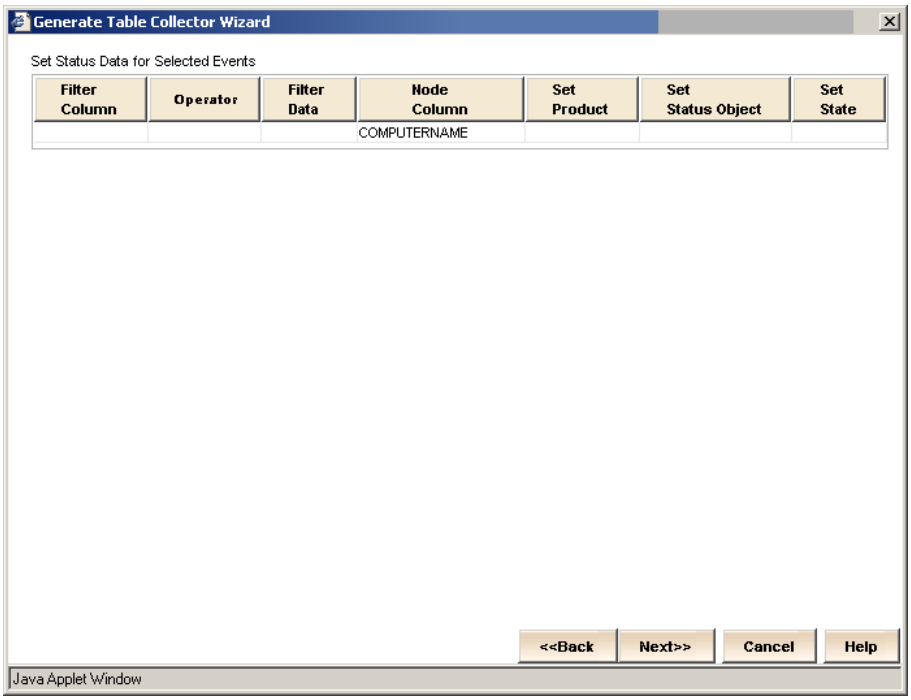
9. Map the columns from your log to the columns you want in your table collector. Click Next.

   The following page appears:



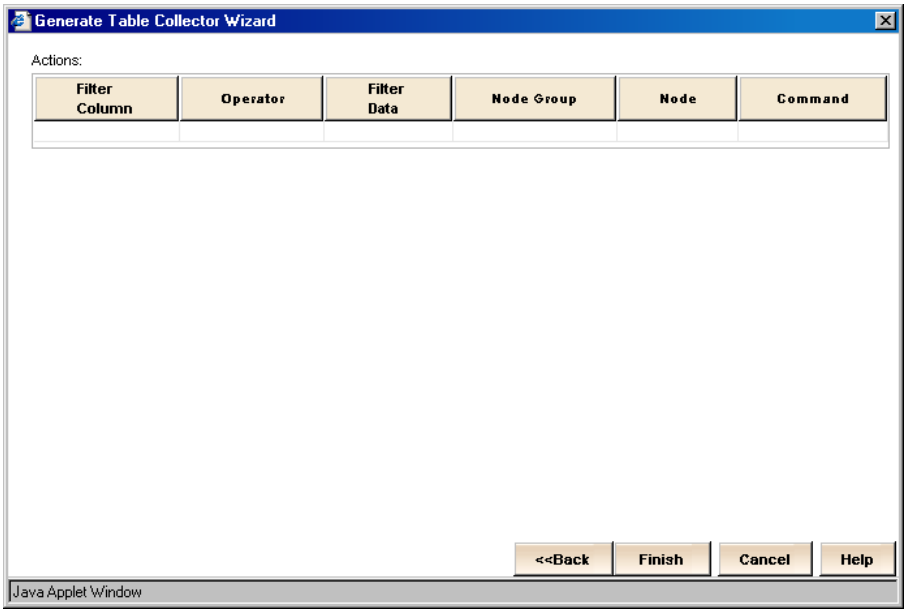
10. Create a sub-filter of events for which you want incident data populated upon retrieval by this table collector. For instance, you could set it so that events that meet this criteria are automatically added to a specified incident group. Click Next.

    The following page appears:



11. Create a sub-filter of events for which you want Status Monitor data populated upon retrieval by this table collector. For instance, you could set it so that events that meet this criteria are automatically assigned a state of Running. Click Next.

    The following page appears:



12. Define any additional programmatic actions to occur on the eTrust Security Command Center node or node group when table collector events meet your specified filtering criteria. Click Finish to complete the wizard and save your table collector settings.

The new table collector appears in alphabetical order in the tree menu on the left side of the display. If necessary, you can use the scroll bar to view the entire tree.

Create or Modify a Table Collector Manually

To create or modify a table collector manually, follow these steps:

1. Expand the Security Command Center Administration branch. Click the Table Collectors item that appears under that branch.

   The Table Collectors interface appears.

2. Click the Hide Menu button to make the Administration menu disappear, thus freeing up more space.

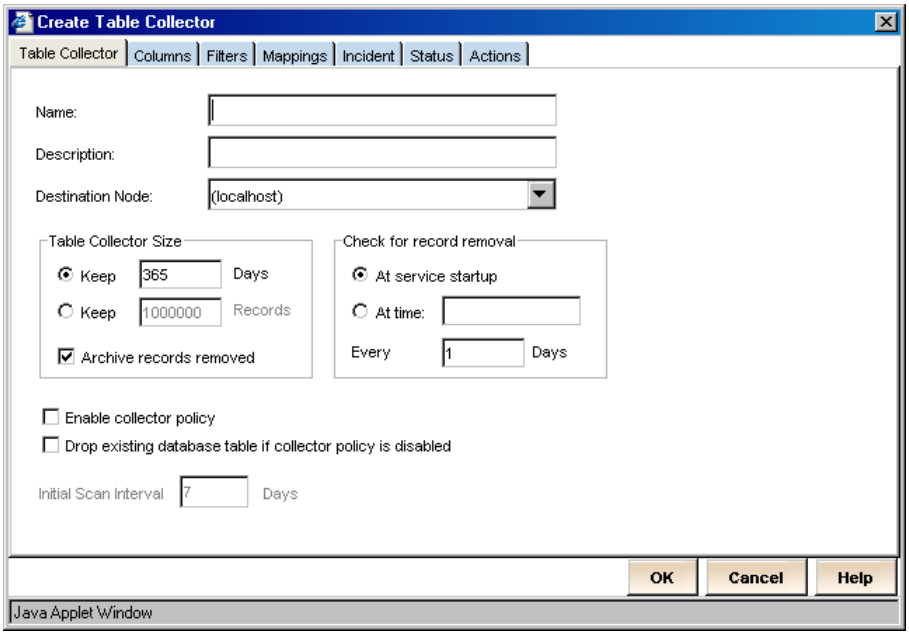
   As with the other applications, the left side of the display contains a tree menu. In this case, the items in the tree are table collectors. The right side is a work area.

3. Expand Table Collectors.

   A list of the existing table collectors appears, including the default audit collector.

4. To modify an existing table collector, double-click the collector's name. To create a new table collector, select an existing collector and click the Create a Table Collector tool bar button, or right-click Table Collectors and, from the pop-up menu, select **New**.

   The Create Table Collector dialog appears:



5. If you selected an existing collector, the fields may already contain information. Modify this information as necessary. If this is a new collector, complete all the fields on the dialog.

   - In the Name field, enter the name of your new table collector.

     Note: The Name field stores a maximum of 30 characters.

   - In the Description field, enter a description for this collector.
   - From the Destination Node drop-down list, choose the machine to which to send the table collector events.
   - In the Table Collector Size box, select the maximum number of days or records to keep in this table collector and whether archived records should be removed.
   - In the Check for record removal box, indicate when you would like records removed if the size of the collector database gets too large or archived records are to be removed.
   - Click the Enable collector policy check box if you want to activate an audit scan, which causes the table to periodically update itself with any new records in the source audit logs.
   - Click the Drop existing database table if collector policy is disabled check box if you want the associated database table to be automatically deleted when you refresh the service (distribute option) if the table collector is not currently enabled.

     Important! It is recommended that you keep the Enable collector policy check box deselected for any table collectors you are not currently using. However, if your Drop existing database table if collector policy is disabled check box is selected, disabling your collector policy may result in an unrecoverable loss of data, so use extreme caution.

   - Indicate the amount of time (in days) to go back and obtain events to populate the table collector in the Initial Scan Interval field, which is only available if the Enable collector policy check box is selected. The value entered here only applies to the first time your table collector obtains events. After the initial scan, the global Scan Interval is used to refresh the events.

6. Several columns such as owner, timestamp, priority, and so on are defaulted into each table collector's setup. If you want to select which of the default columns to include in the database indices or designate additional columns, see Select Columns to Index (see page 237).
7. If you want to specify filter values for the table collector, see Create Table Collector Filter (see page 237).
8. If you want to map columns from log names, see Map Names (see page 238).

9. If you want to assign incident data to a subset of table collector events, see Set Incident Data (see page 238).
10. If you want to assign Status Monitor data to a subset of table collector events, see Set Status Monitor Data (see page 239).
11. If you want to set additional programmatic actions to occur on the defined eTrust Security Command Center node or node group, see Set Actions (see page 239).
12. When you are finished, click OK.

If applicable, the new table collector appears in alphabetical order in the tree menu on the left side of the display.

Select Columns to Index

To set up the database indices for your table collector, follow these steps:

1. Click the Columns tab.

   The Columns window appears.
2. Click the check boxes under Index for each column that you want to use as a database index in this table collector. Click the check boxes under Node for each column for which you want any node-related information, such as machine name, IP address, or fully qualified domain name, to be normalized to the machine.domain.name form.
3. Click OK to save the information or proceed to another tab of the Create Table Collector dialog.

Create Table Collector Filter

To create a table collector filter by which to narrow the results retrieved, follow these steps:

1. Click the Filters tab.

   The Filters window appears.
2. Enter your filter criteria. The Operator drop-down list offers a variety of techniques for narrowing down the results returned by the table collector. You can enter multiple values in the Filter Data column, separated by commas. For example, in the row for LOGNAME, you could select the EQUAL TO operator and enter **eTrust AV, NT-Application**. These two values represent audit log names corresponding to events that are sent by eTrust Antivirus to the default audit collector and its self-monitoring subsystem, and events sent by applications to the NT Event Log.
3. Click OK to save the information or proceed to another tab of the Create Table Collector dialog.

Map Names

To map column names for your table collector, follow these steps:

1. Click the Mappings tab.

   The Mappings window appears.

2. Map columns from log names by selecting a log on the left and then selecting table collector columns that correspond to each of the log's columns. For example, you could select the Audit log under Log Name. For each Log Column Name that displays, select an associated Collector Column Name. The Collector Column Name drop-down list is populated by the columns that you selected to be indices on the Columns window.

3. Click OK to save the information or proceed to another tab of the Create Table Collector dialog.

Set Incident Data

To assign incident data to a selection of table collector events, follow these steps:

1. Click the Incident tab.

   The Incident window appears.

2. Using the three columns on the left, create an additional row of filter criteria for this table collector. Using the remaining columns, assign incident data to the events that this filter row retrieves. You can set the owner and/or priority (using the priority scheme you choose) for this incident, set this incident as pending (which lets you establish and use workflows), set the workflow, choose to display this incident in the Incident Viewer, and indicate the column and data of the table collector to which this incident applies.

3. Click OK to save the information or proceed to another tab of the Create Table Collector dialog.

Set Status Monitor Data

To assign Status Monitor data to a selection of table collector events, follow these steps:

1. Click the Status tab.

   The Status window appears.

2. Using the three columns on the left, create an additional row of filter criteria for this table collector. Using the remaining columns, assign Status Monitor data to the events that this filter row retrieves. You can enter the node column for which you want to change the status, choose the product for which you want to change the status, choose the status object that corresponds to that product, and indicate the state to assign to that status object.

   Note: When you select an available product, the status objects belonging to that product become available in the Set Status Object field. When you select an available status object, the states applicable to that status object become available in the Set State field.

3. Click OK to save the information or proceed to another tab of the Create Table Collector dialog.

Set Actions

To establish additional programmatic actions to occur on the defined eTrust Security Command Center node or node group when table collector events meet your specified filtering criteria, follow these steps:

1. Click the Actions tab.

   The Actions window appears.

2. Using the three columns on the left, create an additional row of filter criteria for this table collector. Using the remaining columns, assign an action to the events that this filter row retrieves. You can choose the node group and/or node on which you want the command to be executed. Enter the command to execute when the filtering criteria is met.

3. Click OK to save the information or proceed to another tab of the Create Table Collector dialog.

How to Activate a Table Collector

Only active table collectors will have events generated for them in eTrust Security Command Center. The process of activating a table collector in eTrust Security Command Center involves enabling the policy and refreshing the service. Specifically, this process includes the following steps:

1. Enable the collector policy for the table. To do this, simply click the appropriate table collector in the tree menu in the left frame, and then click the Enable collector policy check box on the Table Collector window that appears in the right frame.

   Note: The value of the Initial Scan Interval field, also available on this window, determines whether events generated prior to completing this process are added to the table collector. If the Initial Scan Interval is set to 7 days, for example, matching events from the previous seven days appear in the table collector. If you do not wish to add any previous events, set the Initial Scan Interval to 0 before distributing the table collectors. The Initial Scan Interval is effective only the first time a table collector is distributed.

2. Distribute the table to refresh the table collector service. To do this, either select **File, Distribute** from the main menu bar or click the Make all changes effective in Table Collector toolbar button.

   Note: When a table collector is distributed, database tables for the table collector are created or updated on all available collector nodes. When you select **File, Distribute** from the main menu bar or click the Make all changes effective in Table Collector toolbar button, all changes to all table collectors since the previous distribution are distributed and become effective. This means that you can distribute *all* table collectors you have created or modified simultaneously.

3. Optionally, change the table collector scan frequency. To do this, simply click the Table Collectors menu item in the left frame, and then use the up and down arrows to choose the appropriate Scan Interval (in minutes) on the Table Collector Global Setting window that appears in the right frame.

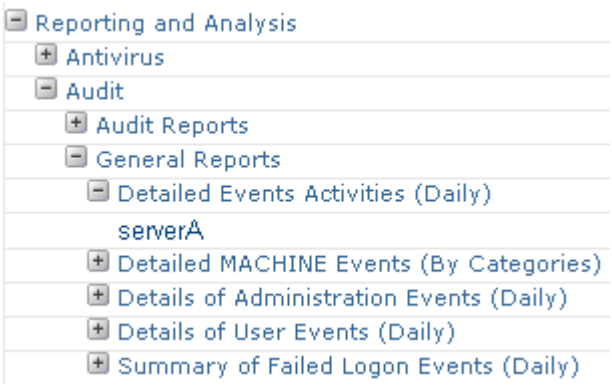
4. Generate events for the table collector to find.

Reporting and Analysis

The Reporting and Analysis menu lets you view product content, usually in HTML format. This product content is only accessible after you have installed your products and PIKs, configured your menu profiles properly, and, for eTrust Audit only, scheduled the appropriate reports. For more information, see the appropriate PIK guide.

For information about the reports available from the Audit workplace in eTrust Security Command Center, see The Audit Workplace. For information about all eTrust Audit-based reports available, see the *eTrust Audit Reference Guide*.

Expand the Reporting and Analysis branch. Your menu should look similar to the following:

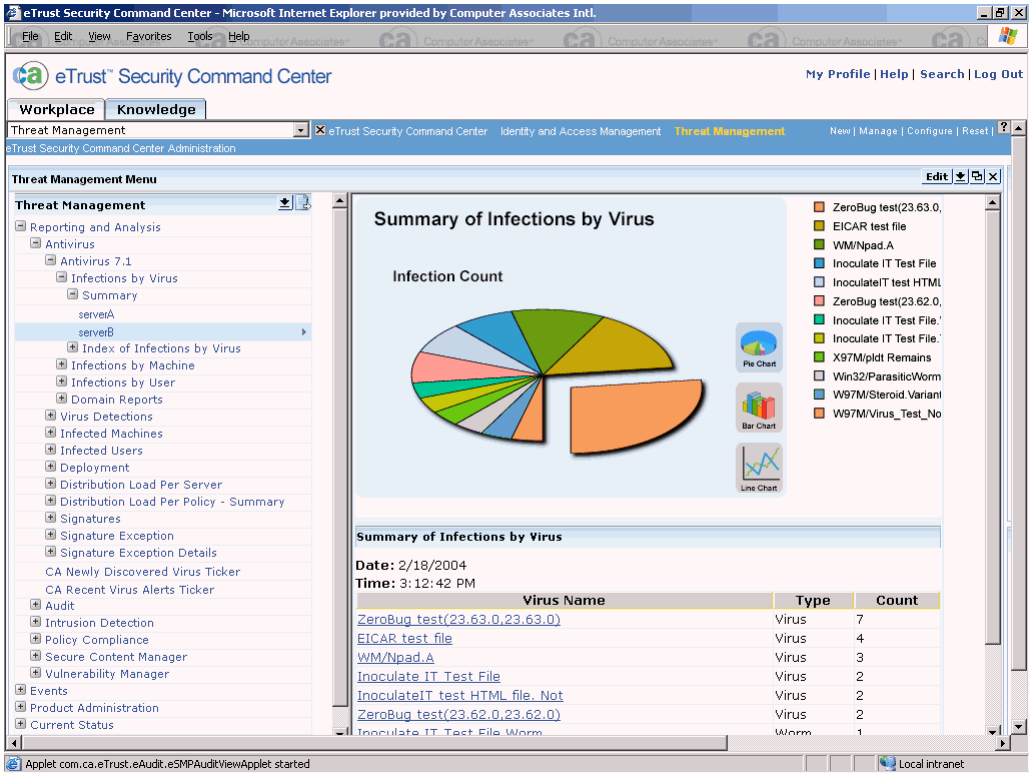


An administrator determines the menu's hierarchy while creating the corresponding menu profile.

The following list describes the parts of this menu:

- Reporting and Analysis is the name of the application group.
- Antivirus and Audit are the names of products on which you can report.
- Audit Reports and General Reports are the names of nested application groups.
- Detailed Events Activities (Daily) is the name of an application.
- serverA is a node.

An example of an available report is the Antivirus Summary of Infections by Virus report, which displays a graph of the quantity of virus infections for that node, as follows:



You can change the graph to display in pie chart, bar chart or line chart format.

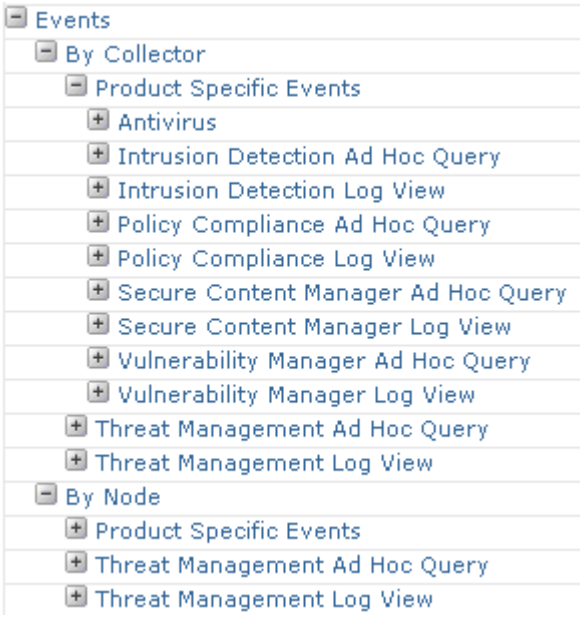
These reports help you analyze various aspects of your security setup. eTrust Security Command Center can display product content in TXT, XML, CSV, and HTML formats.

Note: Integration tools packaged with eTrust Security Command Center help you transform your product content into attractive HTML pages and can be used to manage and monitor products, even if there is no formal eTrust Security Command Center Product Integration Kit available for your product.

Events

The Events menu displays events sent by the subject product to the associated collector.

Expand the Events branch. Your menu should look similar to the following:



You can choose to view the events by collector (default audit collector), node, or table collector (when available).

Note: The sample workplace does not show events by table collector.

A *collector* is an eTrust Audit database that stores events. Depending on the size of your enterprise, you may have more than one audit collector. The *node* is the system on which the event occurred. When you select one of the nodes from the Events menu, eTrust Security Command Center automatically opens a view displaying the appropriately filtered events. A *table collector* is a specialized database table that supports sorting and filtering of specific audit event data independent of the default audit collector database. The tracking of incident priorities, owners, and pending status is not supported by the default collector database, but it is by table collectors.

You can monitor events sent to the associated collector using either the Ad Hoc Query or Log Viewer.

Monitor Events with Ad Hoc Query Viewer

The Ad Hoc Query application lets you quickly generate a query and submit it to the associated collector. It returns event data based on your selections. You can view product-specific events or those for the overall profile (workplace).

To run an ad hoc query for eTrust Antivirus events by collector

1. Expand the menu items in this order: Events, By Collector, Product Specific Events, Antivirus, Ad Hoc Queries, and All Events.
2. Click the appropriate node.

   The Ad Hoc Query Criteria dialog for that node appears in the menu content area:
3. Click a different menu item in the left panel to change the Profile or Collector, or choose **Options, Set Profile and Collector** and select the appropriate event profile and collector. To change the criteria, choose **Options, Set Criteria** and define the appropriate search criteria.
4. Click Apply.

   The Ad Hoc Query Viewer displays the results.

Monitor Events with Log Viewer

The Log Viewer appears in the content area for many of the predefined workplaces. This application lets you view event data dynamically. It continually refreshes the data according to pre-configured settings. It returns event data based on the specific product and node you select from the Events menu. You can view product-specific events or those for the overall profile (workplace).

To view the audit log for eTrust Antivirus events by collector

1. Expand the menu items in this order: Events, By Collector, Product Specific Events, Antivirus, Log Views, All Events.

   The Log Viewer window appears.

2. To change the Profile or Collector, either click a different menu item in the left pane or choose **Options, Set Profile and Collector** and select the appropriate event profile and collector. To change the criteria, choose **Options, Set Criteria** and define the appropriate search criteria.

3. Click Apply.

   The Log Viewer appears with the new settings applied.

4. Double-click any event row to view details for that event in a separate Details window.

You can track events by characteristics such as owner, priority, pending status, or workflow policy. You can also annotate them or add them to incident groups. To set these characteristics, click the Event Actions menu in the Details window, or right-click the event in the Log Viewer and select the appropriate menu item.

If you have more than one Audit Collector in your SIM environment, you may find it useful to click on the Collectors tool bar menu item so that you can view similar events (using the same Audit Viewer Profile) on a different event collection server.

Managing Profiles in the Favorites List

You can use the Options tool bar menu item to save your most frequently used Audit Viewer profiles.

To add profiles to, or remove profiles from, your Favorites list

1. Click the Options menu and then select Set Favorites.
2. Select one or more desired Audit Viewer profiles from the list on the left side of the window and click Add.

   Note: You can remove items from your Favorites list by selecting them from the list on the right side and then clicking Remove.
3. Click Apply when you are finished with your selections.
4. Click the Options menu and then select View Logs to return to viewing logs.

   You can now switch efficiently between your the configured Viewer profiles in your Favorites list.

Audit-based Reports

eTrust Audit includes a web-based Reporting capability which you can access from within eTrust Security Command Center. When you click on Audit-based reports in the eTrust Security Command Center interface, the login for web-based Reporting displays. From this point, you may use the reporting functions as if you had connected through the Audit Administrator directly.

Product Administration

The Product Administration menu invokes the "native" administration interfaces of a given product.

Expand the Product Administration branch. Your menu should look similar to the following:

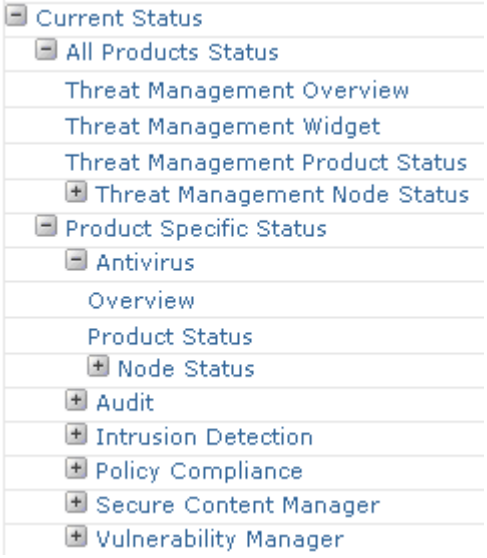
Click the plus icon to the left of these items to see the administration interfaces and nodes available. After you log into the machine represented by the selected node, the selected product interface appears in your browser. For example, you can access the fully functional Policy Manager interface for eTrust Audit.

You can also access user interfaces that are **not** web-enabled on the network using eTrust Security Command Center and a remote administration method such as Windows Terminal Services, Telnet, or secure HTTP. eTrust Security Command Center gives you access to remotely installed, non-web-enabled user interfaces in real time.

Current Status

The Current Status menu lets you monitor the current state of services, processes, and daemons on the product servers configured to work with eTrust Security Command Center. Status Monitor agents installed on the product servers automatically report the status of the objects they monitor to the Status Monitor Manager running on the eTrust Security Command Center server.

Expand the Current Status branch. Your menu should look similar to the following:



You can view status in several different ways, such as by product or by node. You can also view overall status for the selected profile (workplace). For example, the Threat Management workplace lets you view status overall, by product, by node, or by status widget (defined in a widget profile).

Additionally, you can combine status profiles (such as one for product A and another for product B) into widget or map profiles. These types of status profiles let you display overall status for a number of products in a single window.

Multiple Status Views

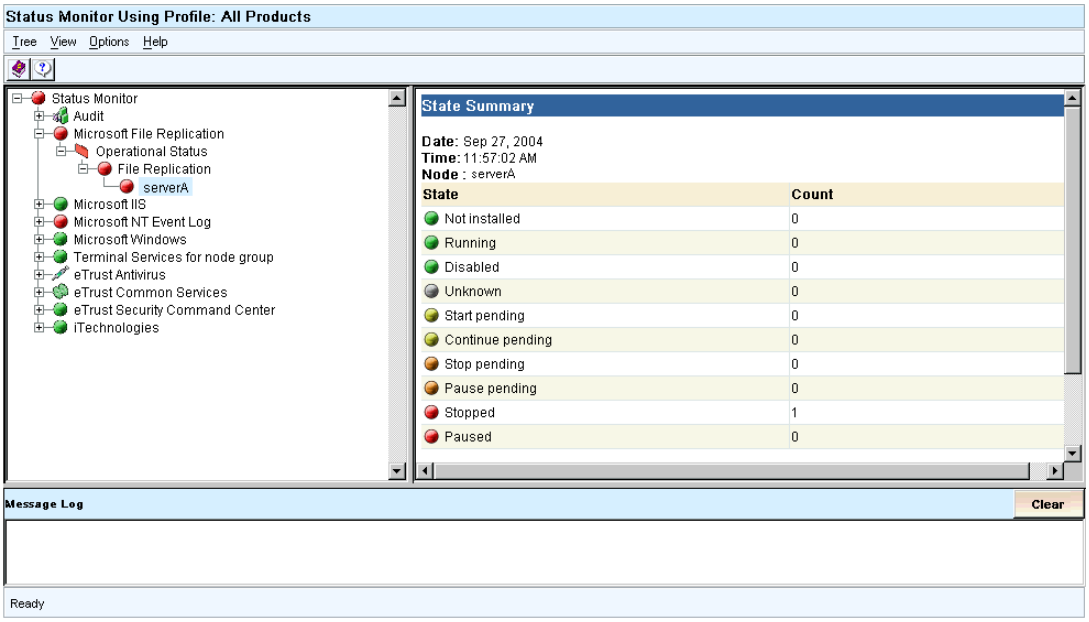
The various status views available illustrate a subtle but powerful capability of eTrust Security Command Center. It does not dictate how to organize product content, objects, and status, or from what perspective to view them. You can configure eTrust Security Command Center to reflect your own organization and viewing preferences.

The following topics describe several methods of accessing status. You can also use the View menu in the Status Monitor to switch between tree, list, severity summary, state summary, details, and log views. For more information about these views, see the *eTrust Security Command Center Administrator Guide*.

Status by Product

You can access status information by expanding the menu items under a particular product when By Node is not flagged in the View menu. Select the appropriate process, service, or daemon and then select the appropriate node. In this scenario, to determine the affected component, you navigate the hierarchy from the problem product to the problem node.

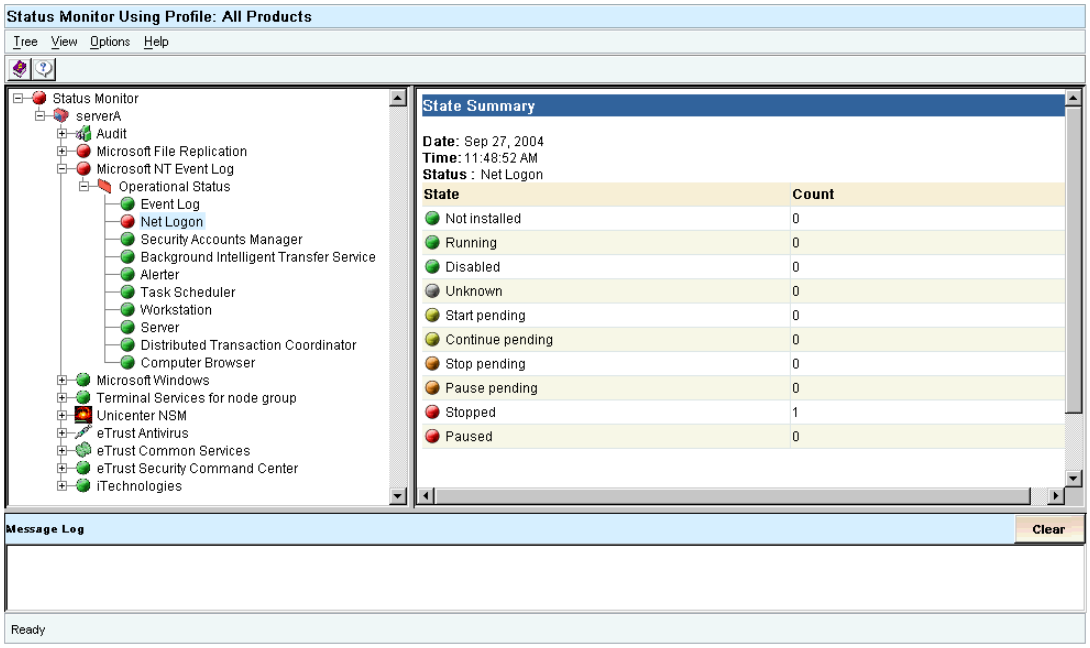
For example, the following window shows the status of a Microsoft File Replication component on the node, serverA. The File Replication component is Stopped. The example shows how to navigate the hierarchy to the State Summary when you are in the product status view.



Status by Node

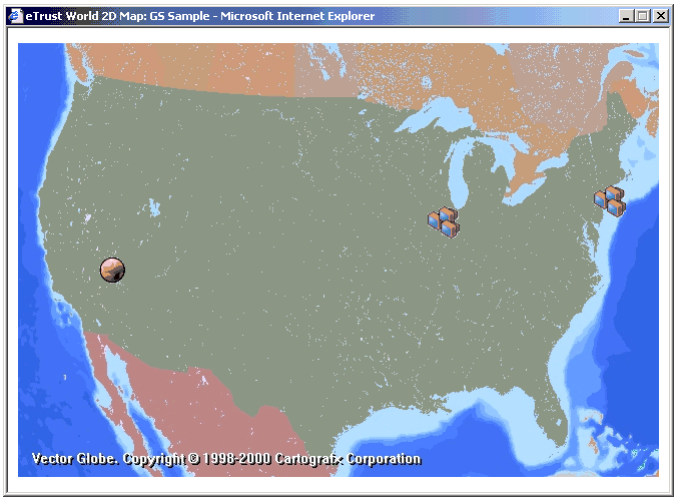
You can access status information by expanding the menu items under a particular node when By Node is flagged in the View menu. Select the appropriate node and then select the appropriate process, service, or daemon. In this scenario, to determine the affected component, you navigate the hierarchy from the problem node to the problem product.

For example, the following window shows a problem with a Microsoft NT Event Log component on the node, serverA. The Net Logon service is Stopped. The example shows how to navigate the hierarchy to the State Summary when you are in the node status view.



Map Profiles

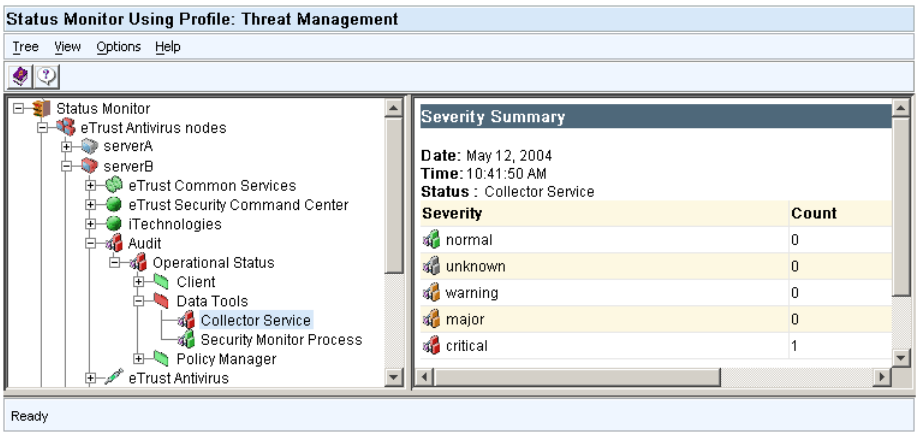
A visually intuitive way to view status applies a status widget to an image to create a map profile. For example, the following profile shows one node and two node groups in a critical state:



This gives you the same high-level status overview, but also lets you associate the status with a location. You do not have to use a specific type of image or map. You can place the status objects on any image, such as a floor plan.

Additionally, if you double-click any of the status objects on the map, you can navigate the hierarchy in the Status Monitor to locate the specific service, process, or daemon causing the problem.

The following illustration shows the Audit Collector service in a critical state at this node.

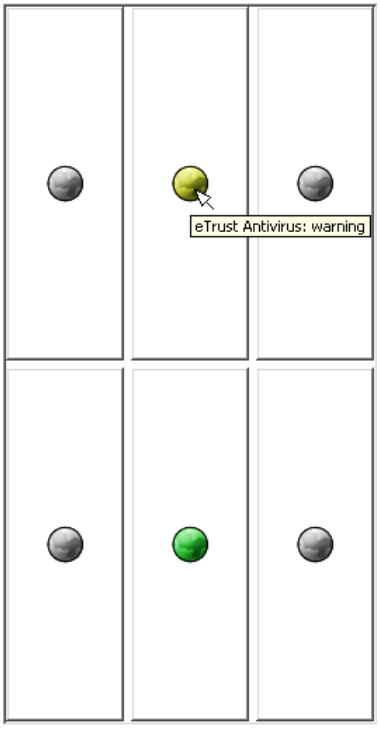


For information about creating map profiles, see the eTrust Security Command Center online help.

Widget Profiles

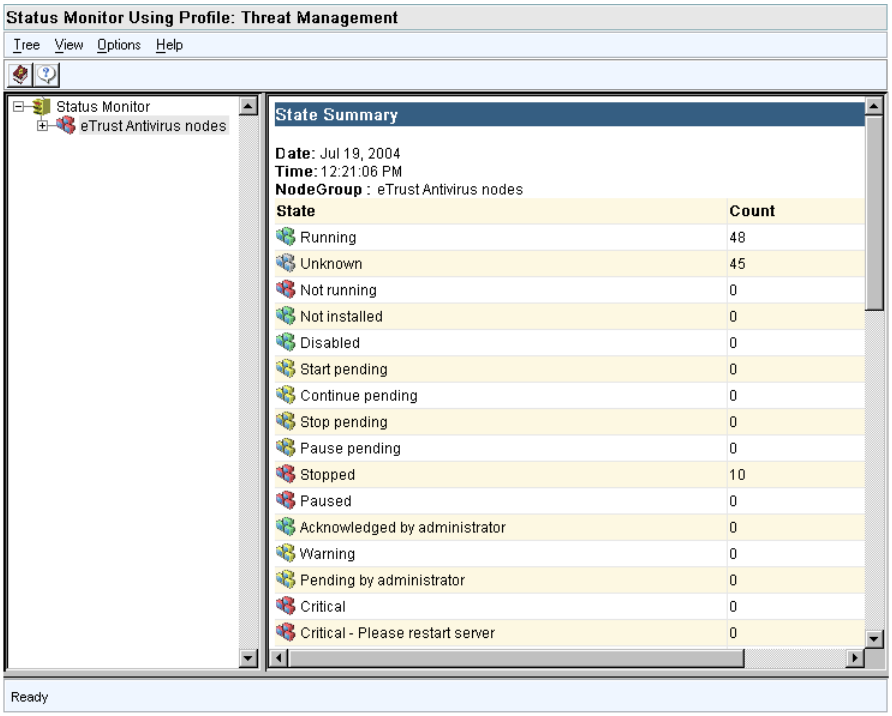
You can create a widget profile to produce a status widget. You can use these widgets to provide a high-level overview of the current state of a set of installed products in a single window.

Drag your mouse pointer over the icons in the status widget to view which product is experiencing problems. In the following example, eTrust Antivirus is in a warning state.



Note: You can launch the status widget in a separate browser window, or make it part of your active desktop.

Click the icon and a status profile for that product appears:

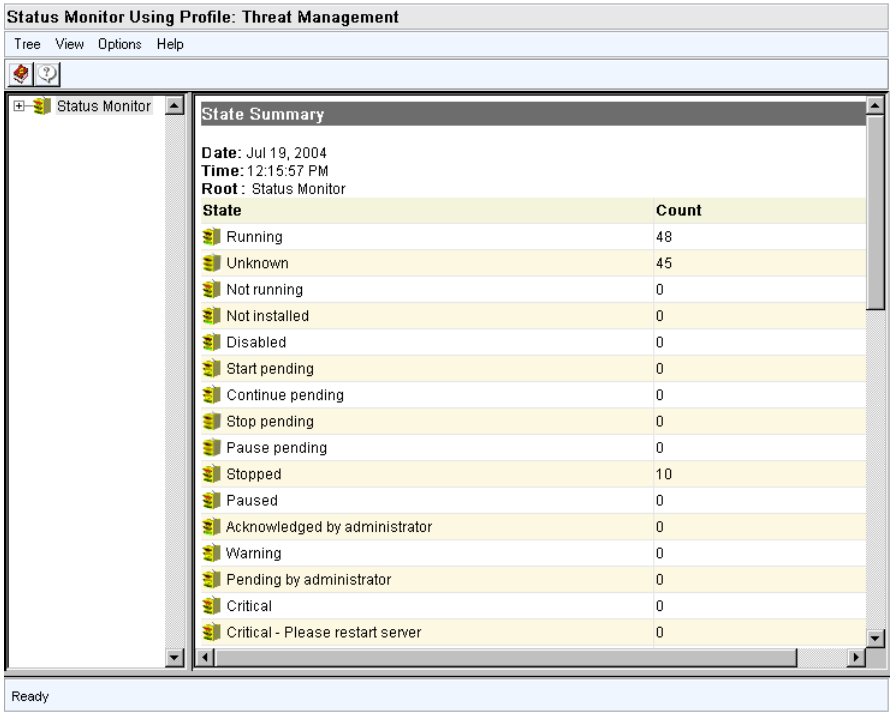


For information about creating widget profiles, see the eTrust Security Command Center online help.

Status Overviews

You can also create status overviews to provide high-level status summaries. For example, the following status overview indicates the overall status for all installed eTrust products (All eTrust Products is the node group selected):

When you click the link, the Status Monitor displays the status for all nodes and node groups as follows:



Utilities

The Utilities menu invokes the various product utilities installed on the product server that you manage and monitor with eTrust Security Command Center. For example, in the Threat Management workplace profile, there is menu item named Generate Report Data. You can select this item to initiate the utility automatically to create eTrust Antivirus Report data on the selected nodes.

Expand the Utilities branch. Your options should look similar to the following:

When you click the menu item for the node, eTrust Security Command Center sends the command to the remote system on which it runs.

Web Sites

The Web Sites menu supplies shortcuts to favorite URLs in a particular menu hierarchy. You can specify any valid URL and create a shortcut for it.

Expand the Web Sites branch. Your menu should look similar to the following:

The actual entries that appear depend on factors such as the PIKs you install.

Chapter 15: Upgrading from a Previous Release

This section contains the following topics:

Introduction

This section provides instructions for upgrading previous releases of eTrust Audit and eTrust Security Command Center.

Consult the Readme file for the latest product release information before you begin an upgrade.

During the upgrade of either eTrust Audit or eTrust Security Command Center, the previous release is completely uninstalled as part of the process before the new release is installed.

Note: When upgrading eTrust Audit or eTrust Security Command Center components on one machine, you must upgrade **all** the components to the same version on that machine. Otherwise, the system will not function properly. Also, if you upgrade eTrust Audit on a computer and you have eTrust Security Command Center components on that computer, both products need to be upgraded to the same level.

Upgrading eTrust Audit

A main feature of this release is a new web-based interface for the Policy Manager, Reporter, and Viewer. When you upgrade these applications on Windows systems, the previous versions are uninstalled and replaced with the new web-based versions. The Policy Manager no longer supports a Microsoft Access database, so you must have either a Microsoft SQL Server or an Oracle database available. (Refer to the Readme file for specific DBMS versions supported.)

Beginning with this release, you can install the Policy Manager on either Windows or Solaris 10 systems. A utility is available to convert your Microsoft Access database to the new database schema. The database conversion is done automatically during the upgrade process on Windows systems, or manually if you install the Policy Manager on a Solaris system. The Policy Manager uses an Embedded Identity and Access Management (eIAM) server, which you can install during the Policy Manager installation, if necessary.

There are also significant enhancements to the Policy Manager procedures that affect how you create, approve, and distribute policies. Before you upgrade or use the new interface, it is important to review the *eTrust Audit and eTrust Security Command Center Administration Guide*. Task-based information is also available in the online help for the Audit Administrator interface.

The separate Windows Reporter and Viewer applications have been replaced with a combined Reporter and Viewer web-based application. The Reporter and Viewer requires either the Tomcat or the WebSphere Web Application Server. The Reporter and Viewer installation can install Tomcat as an option, but it does not install the WebSphere software. If you want to use the WebSphere Application Server, you must install that product separately.

When you start the r8 SP2 installation, a prompt to perform an upgrade appears if a previous release of eTrust Audit is detected.

Note: Even if you are upgrading an existing installation, you should review the installation sections earlier in this Implementation Guide.

If you are running an earlier release of eTrust Audit, you must upgrade the Policy Manager, Data Tools, and Client components on all applicable systems. You cannot mix the release levels of these components successfully. Each of these components is available on the product installation media or downloaded install image.

You can upgrade your eTrust Audit installation in stages, but the following order is important:

1. Policy Manager
2. Data Tools

3. Reporter and Viewer
4. Client

It is important that you upgrade the Policy Manager and Data Tools first as they are both backwardly compatible with older Clients. Newly-upgraded Clients, however, are not compatible with earlier Policy Managers and Data Tools.

Note: Though previous installations are completely removed as part of an upgrade installation, the eTrust Audit Client upgrade does not remove any existing iRecorders on a system. The iRecorders will be unaffected by the upgrade and will continue to function properly after the upgrade. There is no need to re-install or upgrade any iRecorders.

Installing the r8 SP2 Policy Manager automatically migrates all of your existing policies to the new Policy Manager database. You do not need to convert, import, or export any policies manually that are *already* distributed or defined in the database.

If you add an event recorder (an iRecorder or a SAPI Recorder) to your network *after* you upgrade your eTrust Audit installation to r8 SP2, you must import that event recorder's default policies manually. This process may require conversion from .ptf file format to .xml file format. Conversion, import, and export utilities are provided with the r8 SP2 installation for this purpose.

You can find more information on importing, exporting, and converting policies in the *eTrust Audit and eTrust Security Command Center Reference Guide*.

Upgrade Considerations for Windows Systems

Review the following important considerations before upgrading eTrust Audit on Windows systems:

- When you install eTrust Audit Policy Manager over an existing installation, you must choose whether or not to import the existing policies. If you have existing policies that you wish to retain, choose the Import option. Otherwise, you will permanently lose the policies.
- We recommend that you back up the current data in the eTrust Audit Collector database before beginning your upgrade. During the upgrade, you will be prompted to do one of the following:
  - Retain your existing data
  - Create a new database
  - Overwrite your existing data
- Ensure that a supported release of eTrust Audit is currently installed.
- Ensure that the service applet window is closed.
- Verify that all eTrust Audit interface windows are closed.
- Ensure that the eTrust Audit directories are not currently selected in Windows Explorer, if that application is open.
- Verify that the computers you are using to install eTrust Audit or eTrust Security Command Center have a DVD-ROM or DVD-RW drive to read the installation media, or access to a network share where the installation media is located.

Upgrade eTrust Audit on Windows Systems

Use this general upgrade procedure to upgrade your eTrust Audit installation to use the latest features.

Each of the component installations will require specific information about other servers, databases, and user credentials in the network. You may want to use the Network Management Planning worksheet (see page 48) to help you prepare for the upgrade prior to starting the installation program.

Note: During upgrade to r8 SP2, the sulog.mp and syslog.mp files are automatically saved to *eTrust Audit default directory*/cfg/sulog.mp.bak and *eTrust Audit default directory*/cfg/syslog.mp.bak.

To upgrade from a previous release

1. Insert the installation media into the media drive, or run setup.exe from the eTrust Audit root folder.

   The eTrust Audit installation Main Menu page appears.

2. Select the Install eTrust Audit Components option from the Main Menu.

3. Select the appropriate eTrust Audit component and, if applicable, select the component platform from the eTrust Audit Components list to start the upgrade.

   Note: You should upgrade the Policy Manager first, then the Data Tools, then the Clients.

   A dialog asking for confirmation to perform an upgrade of the selected component appears.

4. Choose Yes to start the upgrade.

5. Follow the installation prompts for each component.

   The *Implementation Guide* contains chapters with additional installation information for each of the components.

6. Repeat the previous two steps for each component you wish to upgrade.

7. Complete the installation wizard and exit.

   Your eTrust Audit installation is upgraded.

Note: You can use the two utilities, acstat and acreminfo, to determine the status of your installation. More information about these utilities is available in the *Reference Guide*.

Upgrade eTrust Audit on Solaris Systems

This upgrade process upgrades eTrust Audit components from r1.5 SP2 or above to r8 SP2 components on Solaris systems. The following upgrade-related files are provided on the installation media:

upgrade_eAudit

The upgrade wrapper for the eTrust Audit components.

Note: You must run the upgrade script with the AuditShared package first.

Each installation or upgrade package for Solaris systems has a version embedded in its name, such as AuditShared-8.0.200.123-all.pkg. Use the last three digits in place of *xxx* in the following procedures.

To upgrade a Solaris system to r8 SP2

1. Log on to the Solaris server as root (or superuser).
2. Insert the installation media and navigate to the directory that contains the following files:
   - upgrade_eAudit script
   - AuditShared-r8SP2-8.0.200.xxx-all.pkg
   - AuditDT-r8SP2-8.0.200.xxx-all.pkg
   - AuditCli-r8SP2-8.0.200.xxx-all.pkg
3. Upgrade the shared components (AuditShared) using the following command:

   ```
   ./upgrade_eAudit -v 8.0.200.xxx -u AuditShared
   ```

4. Upgrade the Client components (AuditCli) using the folllowing command:

   ```
   ./upgrade_eAudit -v 8.0.200.xxx -u AuditCli
   ```

5. Upgrade the Data Tools components (AuditDT) using the following command:

   ```
   ./upgrade_eAudit -v 8.0.200.xxx -u AuditDT
   ```

Upgrade eTrust Audit on Linux Systems

This upgrade process upgrades eTrust Audit components from r1.5 SP2 or above to r8 SP2 components on Linux systems. You use the following files to upgrade your installation:

install_AuditShared

The installation and upgrade wrapper file.

install_AuditClient

The wrapper file for the Client components.

Note: You must run the install_AuditShared script first.

To upgrade the Audit components on Linux systems

1. Log on to the Linux server as root (or superuser).
2. Insert the installation media and navigate to the directory that contains the following files:
   - install_AuditShared script
   - AuditShared-r8SP2-8.0.200.xxx.i386.rpm
   - install_AuditClient script
   - AuditClient-r8SP2-8.0.200.xxx.i386.rpm
3. Run the install_AuditShared script using the following command:

   ./install_AuditShared
4. Run the install_AuditClient script using the following command:

   ./install_AuditClient

Upgrade eTrust Audit on UNIX Systems

This upgrade process upgrades eTrust Audit components from r1.5 SP2 or above to r8 SP2 components on UNIX systems. You use the following files to upgrade your installation:

install_eAudit

The installation and upgrade wrapper file for eTrust Audit components.

To upgrade eTrust Audit components

1. Log on to the UNIX computer as root (or superuser).
2. Insert the product installation media in the drive.

   Note: We recommend that you close any applications you have running before you insert the product installation media.
3. Navigate to the installation directory containing the eTrust Audit installation files for the UNIX version you are running:

   cd /[*installation_path*]/Audit80_SP2/[*platform*]/Audit

   where *[platform]* is AIX, HP-UX, UnixWare, or Tru64.
4. Enter the ls command to view the contents of the installation directory.

   The following files are in that directory:

   - A tar archive file that contains the product installation image in the form xxxxxxxxxxxxxx.tar.z for the platform and build designation, such as _AIX_AC8.0.200.123.tar.z.
   - An installation shell script named install_eAudit.
5. Remain logged in as root, and enter the following command from the shell prompt to start the installation:

   ./install_eAudit *tar_file_name*.tar.z

Upgrading eTrust Security Command Center

If you are running an earlier version of eTrust Security Command Center on your eTrust Security Command Center server, you may have to upgrade the server components. The new server components are provided on your product installation media.

When you start the installation, you will be prompted to perform an upgrade if a previous server component release is detected on your eTrust Security Command Center server. During the upgrade, the previous release is completely uninstalled as part of the process before the new release is installed.

Review the following important considerations before upgrading eTrust Security Command Center:

- No data contained in the portal database is changed or overwritten as the result of an upgrade. The new installation imports any new users, workgroups, workplaces, and content, but retains all existing information, including user modifications.
- No customization to your eTrust Security Command Center setup is overwritten by the upgrade. All profiles are automatically backed up before the previous release uninstalls. After the new installation is complete, backup files that do not exist in the new installation, that is, files created with file names other than those of the standard data files are restored, but no files created by the previous installation are overwritten.

  Important! Any manual modifications made to the standard eTrust Security Command Center data files are overwritten during the upgrade.
- We strongly recommend against any manual modifications to the SCC data files shipped with the product. However, if you have made such modifications, they can be manually retrieved from the backup files stored on the server at any time after an upgrade. Decide whether you want to overwrite all new files with their older modified versions or manually merge your changes into the new files after the upgrade.

Upgrade eTrust Security Command Center Server

Upgrades to your eTrust Security Command Center server will update the executable files for the eTrust Security Command Center server components.

To upgrade your eTrust Security Command Center server

1. Run the setup application from your eTrust Security Command Center installation media.

   A message appears informing you that setup will perform an upgrade instead of a new installation.

2. Answer Yes to the message stating that setup will perform an upgrade instead of a new installation.

   The eTrust Security Command Center server components installation wizard appears to walk you through the installation.

3. Complete the installation wizard. The wizard displays the same pages as it does during a new server installation (see page 200).

   Your eTrust Security Command Center server machine has been successfully upgraded.

Upgrade eTrust Security Command Center Agent Machines

Upgrades to your product servers (eTrust Security Command Center agents) will update the executable files for the eTrust Security Command Center agent components for each machine.

To upgrade the eTrust Security Command Center agent components

1. Run the setup application from your eTrust Security Command Center installation media.

   The eTrust Security Command Center agent components installation wizard appears.

2. Complete the installation wizard. The wizard displays the same pages as during a new agent installation (see page 205).

   Your eTrust Security Command Center agent machine has been successfully upgraded.

Appendix A: Troubleshooting

This section contains the following topics:

eTrust Audit

The topics that follow describe problems encountered during the implementation of eTrust Audit and provide solutions to these problems.

eTrust Audit Collector Service Fails to Start

Symptom:

When I attempt to install eTrust Audit, I receive the following error:
eTrust Audit Collector failed to start, error = 0x40023004

Solution:

If the portmapper is not detected during the eTrust Audit installation, the Collector service terminates. This occurs when a third-party portmapper is present on the computer and the eTrust Audit Portmap service cannot start.

Do the following:

- Set the value of the PortmapName registry key under HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\RPC to an empty string.
- Remove the dependencies that the other eTrust Audit services have on the Portmap service.

As an alternative, consider using a fixed ports configuration, which does not require a portmapper or rpcbind.

Symptom:

For Windows 2003 SP1 systems, the "eTrust Audit Collector" service fails to start during system start-up with the following error message in the Application Log:

"Description: Faulting application aclogrcd.exe, version 8.0.xxx.y, faulting module ole32.dll, version 5.2.xxxx.yyyy, fault address 0x0001f1ea."

Solution:

1. Right-click on the My Computer icon, then select Properties, Advanced tab, Performance, Settings, and then access the Data Execution Prevention tab.
2. Select the option, Turn on DEP for all programs and services except those I select.
3. Select the check boxes next to the iTechnology Application Server and Microsoft Process Kill Utility.

   The check boxes should now display a check mark to indicate that they are selected.
4. Click the Add button and use the browser list that comes up to select the aclogrcd.exe process.

   This adds aclogrcd to the list of iTechnology Application Server and Microsoft Process Kill Utility in the Data Execution Prevention screen.
5. Click Apply and then reboot the server.

This configuration causes the Collector service to start upon reboot.

Log Router Service Fails to Start

Valid on Solaris

Symptom:

I have eTrust Audit Client and eTrust Audit Recorders installed on a Solaris computer. I have defined Policy Rules to send the collected events to the eTrust Audit Collector, which is installed on a remote computer. Remote Procedure Call (RPC) service on the Solaris computer is disabled for security reasons. The eTrust Audit Log Router service on this computer fails to start, displaying the following error messages:

```
Failed SCOM_openserver() 'eaudit_SRPC_server' error=0X40023004
Failed to rmn_init(),error = 0X40023004
```

Solution:

eTrust Audit components communicate with each other using the RPC service. If the RPC service on the Solaris computer is disabled for security reasons, do one of the following:

- Enable the RPC service on the Solaris computer, but configure it so that it communicates with the remote computer where the Collector resides, blocking all other remote host RPC communications.
- Install the Collector on the same Solaris computer that hosts the eTrust Audit Client and Recorders. Start the RPC service on this computer, but allow only local RPC communications. This way the eTrust Audit components will be able to use RPC to exchange data on the local computer only.

  The following additional consideration applies to this solution:

  - You can install the eTrust Audit Security Monitor only on a Windows computer. The internal messages from the eTrust Audit components on the Solaris computer are not sent to the Security Monitor because it requires RPC communication. However, you can find the internal messages in the system log (syslog) on the Solaris computer.

Audit Portmap Service Fails to Start

Valid on Windows

Symptom:

When I have another portmap service occupying the default UDP port 111, the eTrust Audit Portmap service cannot start.

Solution:

To use a different portmap service for eTrust Audit, do the following:

1. Click Start, Settings, Control Panel, Administrative Tools, Services, and stop the eTrust Audit Portmap service.
2. Change the value for the value entry *PortmapName* to the name of the other portmap utility in the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\RPC\PortmapName

3. Delete the eTrust Audit Portmap service from the value entry *DependOnService* under the following registry keys:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eTrust Audit Collector
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eTrust Audit LogRouter

If you do not want to use a different portmap service, stop the other service to free the port.

For an eTrust Audit Client, only the Router uses the portmap service. To avoid a portmap service conflict, you can configure the Redirector service, SAPI Recorders, and iRecorders to send events to a remote Router and not use the Router on the local host.

eTrust Audit Client Installation Displays Corrupted Characters

Valid on Linux

Symptom:

When I install eTrust Audit Client on European Linux computers, corrupted characters appear on the PC monitor.

Solution:

This problem may occur only on the PC monitor. It does not occur when using VNC or X Windows on other UNIX computers, such as AIX, or on Red Hat Linux.

On some Linux PC monitors (using a Gnome terminal), the character encoding follows the locale, for example, es_ES.UTF-8. However, the screen font used by some Linux operating environments on the PC monitor may not display certain accented characters in some European languages.

If you encounter this problem, change the PC monitor encoding to ISO-8859-1.

Problem Connecting to eTrust Audit Client

Valid on Windows XP

Symptom:

When connecting to the eTrust Audit Client on Windows XP with Service Pack 2, I experience problems.

Solution:

These problems are caused by the default settings in a new Windows firewall component for Microsoft Windows XP SP2. By default, the firewall is set to block ports used by eTrust Audit.

Add the following commands to the Firewall Exceptions list:

```
netsh firewall set allowedprogram program="E:\Program Files\CA\eTrust Audit\bin\AcActmgr.exe"
netsh firewall set allowedprogram program="E:\Program Files\CA\eTrust Audit\bin\AcDistagn.exe"
netsh firewall set allowedprogram program="E:\Program Files\CA\eTrust Audit\bin\AcLogrd.exe"
netsh firewall set allowedprogram program="E:\Program Files\CA\eTrust Audit\bin\Portmap.exe"
netsh firewall set allowedprogram program="E:\Program Files\CA\eTrust Audit\bin\SeLogRd.exe"
netsh firewall set allowedprogram program="E:\Program Files\CA\SharedComponents\iTechnology\igateway.exe"
```

Error Setting Up Encryption while Installing eTrust Audit Data Tools

Valid on Windows Server 2003

Symptom:

When I attempt to install eTrust Audit Data Tools using Microsoft Access as the database, the installation sometimes fails and displays the following error message:

Setup failed while setting up encryption

Solution:

Microsoft Access is no longer supported as a Collector database. You must install either a Microsoft SQL Server or an Oracle DBMS.

Error Communicating with eTrust Audit Security Monitor

Valid on Windows 2000 Server

Symptom:

I have all the core components of eTrust Audit installed on a Windows 2000 server. When I reboot the computer, I see the following error in the NT Application Log:

Failed to communicate with target 'Monitor'

Solution:

When the eTrust Audit services starts, an internal self-monitoring message is sent to the Security Monitor designated to take internal messages. If the Security Monitor is installed on the same computer as other services, the Security Monitor may start later than other eTrust Audit services, causing the error message to appear. Because the Security Monitor is an application, not a service, someone must be logged into the server for it to be active.

The services that start before Security Monitor is started cannot successfully send self-monitoring message to the Security Monitor. You can ignore this error as eTrust Audit will work normally after all of the services start successfully.

Error Opening eTrust Audit Viewer

Symptom:

I executed a scheduled maintenance job on a Microsoft SQL Server Collector database. When I opened the eTrust Audit Viewer, I received the following error message:

Unsupported operation was attempted.

Solution:

Using Microsoft SQL Replication with the eTrust Audit Collector database is currently not supported.

When you run a scheduled maintenance job on the Collector database in Microsoft SQL Server, a new column may be added to the SEOSDATA table during replication. If this happens, the eTrust AuditViewer generates the error message and the Viewer cannot be used.

Error Refreshing eTrust Audit Viewer

Symptom:

I am using an Oracle Collector database. When I refresh the eTrust Audit Viewer data, I receive an error.

Solution:

To avoid the error while refreshing the eTrust Audit Viewer, do the following:

- Refresh again, or close and re-open the eTrust Audit Viewer.
- Increase the size of the Oracle rollback space, if the problem occurs again.

Cannot View Data in the Viewer

Symptom:

My event data exists in the Collector database, but I cannot view it in the Viewer.

Solution:

1. Check startup and pre-defined filter settings using the following:
   - Open the Viewer, click Filter by Events, and verify that the Viewer's start-up filter settings are set to display recent data, such as Last 15 min's records.
   - Click the SQL button in the Filter by Events dialog to verify the SQL statement's accuracy, such as the following:

     TIMSTAMP>(getdate()-0.01)

   - Verify that a startup filter is set in the Windows Registry key, HKLM\SOFTWARE\ComputerAssociates\eTrust Audit\Data Server\Viewer\Filter\Startup.
   - Use the tools provided by your DBMS vendor to perform an SQL query directly on the SEOSDATA table.
2. Open the Viewer, and click File, New.

   The property dialog for the data source appears.
3. Select the appropriate data source, and click OK.

   The records are retrieved from the database.

Security Monitor or Viewer Displays GUID for Object Type and Object Name

Valid on Windows Server 2003

Symptom:

I am collecting Directory Service Access events (NT-Security events, Event ID=566) using the eTrust Audit iRecorder for NT EventLog on a Windows 2003 Domain Controller. When viewing the collected events using the eTrust Audit Security Monitor or Viewer, I notice that the fields Object Type and Object Name are displayed by their GUID and not as readable text.

Solution:

The eTrust Audit iRecorder for NT EventLog supports the translation of the GUIDs to readable text for Domain Controller events from r8 SP1.

In the NTEventLog.conf file in the iTechnology folder, do the following:

- Verify that the value for the Version tag is 8.0.4.050616 or later where the last six digits of the version are in the format YYMMDD..
- Locate the DomainController tag and do the following to translate the GUIDs to readable text:
  - If the value for this tag is set to false, change it to true.
  - If you do not find this tag in the file, add the following line:

    <DomainController>true</DomainController>

Important! You must stop the iGateway service before making any changes in the NTEventLog.conf file. Restart the iGateway service so that the changes take effect.

Database Exceeds Disk Space Limits

Symptom:

I have eTrust Audit installed on a Windows Server computer with a Microsoft SQL Server Collector database. The data in the database is three months old and has exceeded 250 GB in size. The allowed space is full, and new events are not being captured.

Solution:

A database of this size should be administered by an SQL database administrator. We recommend that you discuss this with your company's SQL DBA. If you do not have a SQL DBA to administer this database, use the following procedure to remove some of your eTrust Audit events.

- To delete the records older than 30 days, use the following SQL statement:

  DELETE FROM <database owner>.seosdata where datediff(day, timstamp, getdate()) >= 30

  Note: For faster results, execute the deletion on a batch of rows; the deletion takes longer on a very large database.

- To use SQL Enterprise Manager's Job Scheduler to schedule a job, run the following statements:

  SET ROWCOUNT <number>
  DELETE FROM <database owner>.seosdata where datediff(day, timstamp, getdate()) >= 30

  Each time the job runs, it deletes the number of rows (events) that are older than 30 days. Schedule the job to run at a frequency that prevents your database from exceeding the maximum size.

  Note: For faster execution, the number of rows to delete should be as small as possible, consistent with controlling database size.

Important! We recommend that you discuss the batch number and how often to run the job with an SQL DBA to minimize impact on database performance.

Remote Action Rejected by Audit Log Router

Symptom:

I find that eTrust Audit r8 SP1 Audit Log Router rejects by default an action remote program or action remote file that comes from another Audit Log Router.

Solution:

By default, eTrust Audit r8 SP1 Audit Log Router allows remote actions for the following:

- Collector
- Monitor
- Unicenter
- Status Monitor

By default, remote actions are not allowed for the following:

- Email
- External Program
- File
- Route
- Screen
- SNMP

To allow the desired remote action on the client computer, do the following:

Windows

Edit the registry and insert a DWORD parameter *AllowRemoteAction=dword:00000001* for the remote action you want to allow.

Example: To allow the action e-mail, insert the DWORD parameter as shown:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Client\Router\Queue Manager\Actions\Mail

"AllowRemoteAction"=dword:00000001

UNIX or Linux

Edit the eaudit.ini file and insert the line *DWORD: AllowRemoteAction= 1* as a parameter for each remote action you want to allow.

Example: To allow the action e-mail, insert the DWORD line as shown:

```
Actions
{
mail
{
    LibraryName = MRA
    DWORD:LoadOnDemand = 0
    DWORD: AllowRemoteAction= 1
    Parameters
    {
            MailSubject = eTrust Audit : Notification
    }
}
}
```

Cannot Access eTrust Audit Administrator Using Internet Explorer

Valid on Windows Server 2003

Symptom:

On a computer with Windows Server 2003, the Internet Explorer (6.x) browser remains blank when I try to access eTrust Audit Administrator remotely using the URL https://computer_name:5250/spin/AuditAdmin. I am able to connect to the computer using the following command:

```
telnet computer_name 5250
```

Solution:

The enhanced security feature of Internet Explorer on Windows Server 2003 does not allow access to the eTrust Audit Administrator computer. To enable Internet Explorer to access eTrust Audit Administrator, do the following:

1. Open Internet Explorer, click Tools, Internet Options.

   The Internet Options dialog appears.

2. Select the Advanced tab, select the check box Display enhanced security configuration dialog, and click OK.

   The changes to the internet options are saved.

3. Enter the following URL in the Address bar

   ```
   https://computer_name:5250/spin/AuditAdmin
   ```

   The dialog asking whether you want to add eTrust Audit Administrator to the trusted list appears.

4. Click Add.

   eTrust Audit Administrator appears.

This behavior of Internet Explorer is further explained in Microsoft Knowledge Base Article 815141.

Error Logging In to eTrust Audit Administrator

Symptom:

When I try to log in to the eTrust Audit Administrator, I receive the following error message:

Bad Credentials

Solution:

The error message appears when the user's credentials have expired due to a long period of inactivity on eTrust Audit Administrator. Log off and log in again to renew your user credentials.

SCC--Need Administrator Privilege to Access eTrust Audit Administrator on Non-English OS

Symptoms:

Using a non-English operating system, I attempted to access the Policy Manager or Post-Collection Utilities. I receive the "Need Administrator/root Privileges" message.

Solution:

For any non-english OS where the Administrator's group name is different than the English value "Administrators" you must do the following:

1. Stop the iGateway service.
2. Add a tag to the iControl.conf file denoting the correct Admin group name in the appropriate national language. For example, for Spanish language operating systems, add the tag:

   <AdminGroupName>administradores</AdminGroupName>

3. Start the iGateway service.

Deactivating MP Folder Removes Files with No Replacement

Symptom:

Deactivating an MP folder or policy removes it, but does not replace it with a previous version or other file. After I deactivated the MP folder, the MP file was removed at the event source, which caused the following error when I restarted acrecorderd:

i9-ultra1-03 eTAudit GenericRec: [ID 854135 user.emerg] [Event Management.Agent.Diagnostic.F.W] Failed to open file '/opt/CA/eTrustAudit/cfg/sulog.mp', error = 0x400F200C.

When I tried to deactivate an MP File Folder, I received the message, "Successfully deactivated MP Folder," but in the Activation Log I see the following errors:

06-01-2006 12:00:0 <servername> Solaris MP MP File Removing Failed to receive data.
06-01-2006 12:00:16 <servername> Solaris MP MP File Removing Failed to receive data.

Solution:

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.

Policy Manager Database Not Populated during Install

Symptoms:

The Policy Manager database is not populated with data during the installation. This can happen if you install the eTrust Audit Policy Manager on a computer with only the Oracle client (with the Runtime Option) installed, and the Oracle client points to a remote Oracle Policy Manager database.

Solution:

If you have only the Oracle Runtime Option installed, you will not have the JAR file, Xsu12.jar, which contains the required OracleXML.class.

1. Download the oracle XDK package, xdk_solaris_10_1_0_3_0_production.tar.gz, from the web site: http://www.oracle.com/technology/tech/xml/xdk/software/production10g/utilsoft.html#solaris
2. Extract the XDK tarball on your computer in the $ORACLE_HOME directory, using the command:

   ```
   # gzip -dc xdk.tar | tar xvf -
   ```

3. Proceed with the Policy Manager installation.

Error Using eTrust Audit Administrator Visualizer

Symptom:

When using eTrust AuditAdministrator Visualizer, I receive the following error message.

```
Error: 405 Failed executing prompt
```

Solution:

The Visualizer cannot access the Post-Collection Utility (PCU) tables because the Visualizer and eTrust Security Command Center do not support the Microsoft Access Database.

Use the Visualizer only when you are using the Microsoft SQL Server or Oracle DBMS for PCU or Table Collectors.

Reporter Tab Does Not Display Report Templates

Symptom:

No report templates are displayed in the Reporter tab of the Reporter and Viewer in the Audit Administrator interface.

Solution:

If it is not already set, add the following Java system property to your Tomcat Web Server:

```
java.awt.headless=true
```

If you are using the WebSphere Web Server on Solaris systems, you can use the WebSphere administrator to set the parameter:

```
-Djava.awt.headless=true
```

To configure a WebSphere Web Server to use the headless property

1. Access the WebSphere Web Server's administrator interface.
2. Select Application Servers, then select your specific server instance.
3. Select Process Definition, then select Java Virtual Machine, and then select Generic JVM arguments.
4. Add the following setting:

   ```
   -Djava.awt.headless=true
   ```

5. Save your changes and restart the Web Server.

   Note: If the error is still observed, delete all temporary Internet files so that the browser is not displaying the cached page

Error Accessing Policy Manager Through Audit Administrator

Symptom:

When I log in to eTrust Audit Administrator and select the Policy Manager tab, I receive the following error:

```
Access to the Policy Manager has been denied. Unknown user error, please contact the Policy Manager Administrator for assistance
```

Solution:

To run Policy Manager using eTrust Audit Administrator, ensure that you log in to eTrust Audit Administrator as a user who has rights to run the Policy Manager.

Hostname Lookup Using Collector Does Not Stop

Symptom:

When using the Security Monitor and Collector, I cannot stop the hostname lookup feature.

Solution:

By default, the Security Monitor and Collector perform a hostname lookup if the *Location* field in the collected event contains an IP address. Thus, the Security Monitor and Viewer displays the hostname instead of the IP address. Release since eTrust Audit r8 SP1 provide functionality that allows you to use a registry key to control this behavior.

To apply to Windows systems

To stop the hostname lookup process, do the following:

1. Navigate to the following registry keys:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Monitor\Security Monitor

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Data Server\Collector

2. Right-click each key and add a new key, *HostLookup*.
3. Add a new entry with Name = Active, Type = DWORD and Value = 0x00000000(0).
4. Restart the Collector service and re-open the Security Monitor for the change to take effect.

   The hostname lookup process terminates.

To start the hostname lookup process, do the following:

5. Navigate to the following registry keys:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Monitor\Security Monitor\HostLookup

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Data Server\Collector\HostLookup

6. Edit the DWORD value Action and change to 0x00000001(1).
7. Restart the Collector service and re-open the Security Monitor for the change to take effect.

   The hostname lookup process starts.

To apply to UNIX systems

If the Collector is installed in UNIX operating environment, do the following:

To stop the hostname lookup process of the Collector:

1. In the eaudit.ini file, locate the Data Server section and add the following entry:

   ```
   …
   HostLookup
   {
       DWORD:Active = 0
   }
   …
   ```

2. Restart the Collector daemon for the change to take effect.

   The hostname lookup process is stopped.

To start the hostname lookup process:

3. In the eaudit.ini file, Data Server section, edit the following entry:

   ```
   …
   HostLookup
   {
       DWORD:Active = 1
   }
   …
   ```

4. Restart the Collector daemon for the change to take effect.

   The hostname lookup process is stopped.

Error Logging In to Policy Manager

Symptom:

When I log in to the Policy Manager, I receive the following error:

Could not use '1'; file already in use

Solution:

The error message is generated by the ODBC Jet Driver during connection. It indicates that the user does not have permission to access the directory where the Policy Manager database resides. Log in using a user account authorized to access the Policy Manager.

Error Using NT or Router for AN Group Name

Symptom:

In the Policy Manager, I am using *NT* or *router* as AN Group name. When trying to deploy the policies to which the AN Group is attached, I receive the following error.

E329: Cannot create a file when that file already exists.

Solution:

When deploying policies in the Policy Manager, you cannot use *NT* or *router* for the AN group name if the AN type is NT. Use another name for the AN group name.

Error Viewing Events in Post-Collection Utility Views

Symptom:

I attempted to use the report explorer to view eTrust Audit events in the Post-Collection Utility views. When I ran the report using Crystal Reports the report appeared, but when I used the report explorer I received the following error:

"Failed to open a rowset
Details : 4200 : [Microsoft][ODBC SQL Server Driver][SQL Server] the column prefix ?SEOSDATA? does not match with a table name or alias name used in the query"

Solution:

Ensure the following:

- When you define your reports in Crystal Reports, ensure that your view or table has an alias SEOSDATA.
- If you are joining two tables or views, ensure that one of them has an alias for SEOSDATA.

Error When Reporter Sends Email Notifications

Symptom:

I configured the eTrust Audit Reporter to send email notifications when reports are generated. I have verified that port 25 is working. When the Reporter sends out email notifications, I receive the following error message:

tkmsln05: E61524: SMTP Server didn't respond

Solution:

The eTrust Audit Reporter generates an error when the SMTP server does not respond to the SMTP HELLO request from Reporter Generator.

Verify the following:

- The mail server is processing SMTP email.
- The server is listening on port 25.
- Send mail to the mail server is responding.

eTrust Audit Cannot Run When Portmapper or rpcbind Is Disabled

Symptom:

When the Sun portmapper or Solaris rpcbind service is disabled, eTrust Audit does not run properly.

Solution:

If Sun RPC portmap or Solaris rpcbind is disabled, you can still run eTrust Audit. Ensure that the following values are defined as indicated:

- For SAPI servers (Router, Collector, Monitor), change the defined integer values as follows:

  Windows

  [HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\RPC]

  DWORD:RegisterPort = 0

  UNIX

  [/opt/CA/eTrustAudit/ini/eaudit.ini]

  RPC

  {

  DWORD:RegisterPort = 0

  }

  Also, for eTrust Audit r8 (but unnecessary for r8 SP1):

  Windows

  [HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\RPC]

  REG_SZ: PortmapName = ""

  UNIX

  [/opt/CA/eTrustAudit/ini/eaudit.ini]

  RPC

  {

  PortmapName = ""

  }

- For both SAPI servers and Clients, change the defined corresponding fixed ports (or services) as follows:

  Windows

  [HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Ports]

UNIX

[/opt/CA/eTrustAudit/ini/eaudit.ini]

Service	Port
Recorders/Router	RouterSapiPort
Communication with eAC or 1.5x Audit	RouterPort
ActionManager/Collector	CollectorSapiPort
ActionManager/Collector version 1.5x	CollectorPort
Any Module/Monitor	MonitorSapiPort
Any Module/Monitor version 1.5x	MonitorPort
Any Module/Self-Monitor Events	*Windows* [HKLM\ComputerAssociates\eTrust Audit\Messages\Targets\Monitor\Parameters] REG_SZ:MonitorPort *UNIX* Messages… Targets… Monitor… Parameters... MonitorPort

Cannot Send CISCO Events to iRouter

Symptom:

After I install the iRecorder for CISCO Devices, the iRecorder does not send events to the iRouter.

Solution:

Do the following:

1. Create a file named CiscoDevice.cfg in the iTechnology folder after installing the iRecorder for CISCO Devices, and type the following line in the CiscoDevice.cfg file:

   ```
   local7.debug c:\syslog.log
   ```

   c:\syslog.log

   Specifies the name of the syslog file that is provided during installation.

2. Stop iGateway by entering the following command:

   ```
   net stop iGateway
   ```

3. Open the CiscoDevice.conf file and search for the following string in the SYSLOGCONF tag:

   ```
   type="text">c:\syslog.log
   ```

4. Replace the preceding string with the following string:

   ```
   type="text">CiscoPIX.cfg
   ```

   c:\syslog.log

   Specifies the name of the syslog file that is provided during installation.

5. Enter the following command to start iGateway:

   ```
   net start iGateway
   ```

   The CISCO Device iRecorder starts sending the events to the iRouter.

Cannot Display syslog Events

Valid on RedHat Linux 7.3

Symptom:

I have configured eTrust Audit to collect syslog events from a RedHat Linux 7.3 host. The self-monitor events from eTrust Audit components on the RedHat Linux 7.3 computer are collected, but I cannot see the events in the Security Monitor.

Solution:

Use the eTrust Audit Generic Recorder to collect the syslog events.

eTrust Audit r8 uses the syslog iRecorder to collect syslog events. The iGateway 4.0 requires GNU C libraries GCC 3.2. The GCC package included in RedHat Linux 7.3 is GCC 2.96, which is not compatible with iGateway 4.0.

Severity Field Parsed to 0 for All Events

Symptom:

I am using eTrust Audit iRecorder for CISCO Devices to collect CISCO Device events written to a Windows computer by the Kiwi Syslog Daemon. Events are successfully collected, but the Severity field is parsed to 0 for all events, which is not correct because many events are Failure or Error. I need to use the Severity field to raise an alert.

Solution:

The Severity field problem is resolved in r8 SP1 CR1. This problem occurs if you have updated eTrust Audit components from r8 to r8 SP1 (100.12) using the updating package. This version of eTrust Audit (r8 SP1) is not supported. You should update your eTrust Audit components to r8 SP1 CR1, which is available on the CA Support web site, http://www.ca.com/support.

Post-Collection Utility and eTrust Audit Administrator Do Not Open After Installing BAB 11.1

Symptom:

When I install BrightStor ARCServer Backup (BAB) 11.1 on a computer with eTrust Audit r8 SP1, the Post-Collection Utility and eTrust Audit Administrator do not work.

Solution:

BAB 11.1 installs iGateway 3.0.40621.0, but the eTrust Audit r8 SP1 components install and work only with iGateway 4.0.

To solve the problem, you must install BAB 11.1 before installing eTrust Audit r8 SP1.

eTrust Security Command Center

The topics that follow describe problems encountered during the implementation of eTrust Security Command Center and provide solutions to these problems.

Error Testing Connection to Microsoft SQL Server Database

Symptom:

When installing eTrust Security Command Center, I tested the connection to the Microsoft SQL Server database and received the following error:

Client unable to establish connection

Solution:

Verify the following:

- Microsoft SQL Server database is currently running on the computer you specified.
- You have specified the proper computer name.

More information:

Error Microsoft SQL Server Database Not Running (see page 293)
Error in Microsoft SQL Server Computer Name (see page 293)
Error for Microsoft SQL Server Database (see page 294)

Error Microsoft SQL Server Database Not Running

Symptom:

When installing eTrust Security Command Center, I tested the connection to the Microsoft SQL Server database and received the following error:

Client unable to establish connection
The Microsoft SQL Server Database is not currently running on the machine you specified

Solution:

Do the following:

- If the remote computer is not working, contact your system administrator.
- If a firewall is blocking your access to the remote computer, disable the firewall and try again.
- If Microsoft SQL Server is not installed on the computer, install it.
- If Microsoft SQL Server is shut down, restart it.

After following any of these procedures, click Close and repeat the database connection test.

Error in Microsoft SQL Server Computer Name

Symptom:

When installing eTrust Security Command Center, I tested the connection to the Microsoft SQL Server database and received the following error:

Client unable to establish connection

You did not spell the name of the machine correctly

Solution:

Do the following:

- Verify the computer name, confirm that the computer and the Microsoft SQL Server database are running, and click Test again.
- If the computer name is not correct, click Close and correct the computer name.

Error for Microsoft SQL Server Database

Symptom:

When installing eTrust Security Command Center, I tested the connection to the Microsoft SQL Server database and received the following error:

Login failed for user 'sa'

Solution:

Verify that the user ID and password are valid credentials for a Microsoft SQL Server database administrator.

Error Installing InstallShield Scripting Runtime

Symptom:

When I try to install the eTrust Security Command Center Agent, I receive the following error:

1607: Unable to install InstallShield Scripting Runtime

Solution:

The message appears if you attempt to install an eTrust Security Command Center Agent from within a Windows Terminal Services session. You must install eTrust Security Command Center Agent from the local computer console.

Problem Performing Product Administration Tasks

Symptom:

When using Internet Explorer to access eTrust Security Command Center, I am not able perform product administration tasks.

Solution:

eTrust Security Command Center uses ActiveX controls to start a Windows Terminal Services session with a Win32 interface to perform product administration tasks. It also uses ActiveX controls to display the graphic reporting elements.

To enable Internet Explorer to display these features

1. Click Tools, Internet Options from the Internet Explorer browser.

   The Internet Options dialog appears.

2. Select the Security tab.

   The security options appear.

3. Select Local intranet, and click Custom Level.

   The Security Settings dialog appears. The ActiveX Controls and plug-ins section is at the top of the list.

4. For each of the options under ActiveX Controls and plug-ins, select one of the following:

   - Disable–The ActiveX control does not run, and you cannot launch a Windows Terminal Services session to perform policy management.
   - Enable–The ActiveX control starts without a prompt.
   - Prompt–You receive a message asking whether you want to permit the ActiveX control to run.

   Click OK.

   The Internet Options dialog appears.

5. Click OK.

   The ActiveX controls are now set to run.

6. Click OK. Close and reopen Internet Explorer.

   Your ActiveX controls should now be set to display graphics.

Error Performing Node Diagnostics

Symptom:

When performing node diagnostics, I receive the following error:

eSCC_WAG_E_005 - World Agent converse with node 'myNode' failed

Solution:

The error appears when the agent on myNode is configured to report to the eTrust Security Command Center Server using a fully qualified hostname (such as eSCCServer.mycompany.com) or its IP address (such as 127.0.0.1). When configuring the eTrust Security Command Center Server the agent will report, you must use the hostname alone (such as eSCCServer).

Error Publishing a CleverPath Report to eTrust Security Command Center

Symptom:

I am using HTTPS on the eTrust Security Command Center portal. When I publish a CleverPath r4.2 report to eTrust Security Command Center r8, I receive the following error:

Error sending HTTP request : Windows error 12031

Solution:

eTrust Security Command Center does not support report publishing using HTTPS.

Instead of publishing the report using the CleverPath Portal, use eTrust Security Command Center. To publish a report using eTrust Security Command Center, define a Product Interface Profile.

Note: Product Interface Profiles require an integration program that is able to transfer the CleverPath Reporter reports from the CleverPath Reporter directories to the eTrust Security Command Center directories. This transfer is similar to the method for publishing the eTrust Audit (Crystal) reports in the eTrust Security Command Center portal using the eADRptCp.exe program.

Appendix B: Performing Silent Upgrades

This section contains the following topics:

Silent Upgrade for Windows Systems

You can use the silent upgrade option for the eTrust Audit Client components. This silent process upgrades an eTrust Audit Client at r1.5 SP2 Client or later to an r8 SP2 Client. The following silent upgrade files are provided on the installation media:

Client.exe

Indicates the silent upgrade executable for the Client components.

response_client

Indicates the sample response file for the Client components.

upgrade_1_5.iss

upgrade_8_0.iss

upgrade_8_0_sp1.iss

upgrade_8_0_SP1_CR1.iss

Indicates the sample silent response file for the specific release level shown in the file name.

Prepare Silent Upgrade Response Files

You must create an upgrade response file for silent upgrades on Windows systems. A silent upgrade file contains different responses to prompts than a silent installation response file, so they are not interchangeable.

You should create a dedicated directory for silent upgrades on your server.

Note: If you want to customize the silent upgrade of a product, the computer must already have the product installed that you want to update. If you want to customize the silent uninstall, the computer must already have the product installed that you want to uninstall.

To record a silent upgrade response file on Windows systems

1. Access a command prompt.
2. Create a dedicated directory to contain your upgrade files, and navigate to it.
3. Locate the directory on the installation media that contains the eTrust Audit Client package.

   For example, if the G: drive is the media drive, the eTrust Audit Client package folder is:

   cd /d <media drive>:\Winnt\Audit\Client

4. Enter the following command:

   Client.exe /r /f1"*upgrade_response_filename*"

   In this example, Client.exe is the name of the install program and *upgrade_response_filename* is the fully-qualified name of the response file.

5. Follow the instructions provided in the wizard procedures, and upgrade the package as you would on the target computer.

   Note: Do not use the wizard's Back button while recording a silent response file. The resulting response file will contain too many entries and will be invalid.

6. Click Finish.

Perform Silent Upgrade for Windows Systems

You can perform a silent upgrade of the Client components 'on Windows systems.

To upgrade the Client silently on Windows systems

1. Access a command prompt.
2. Navigate to the dedicated directory you created to contain your upgrade files.
3. Enter the following command:

   Client.exe /s /f1"C:\temp*upgrade_response_filename*.iss"

Silent Upgrade for Solaris Systems

You can use the silent upgrade option for the eTrust Audit Shared and Client components. This silent process upgrades an eTrust Audit Client at r1.5 SP2 Client or later to an r8 SP2 Client. The following silent upgrade files are provided on the installation media:

installShared

Indicates the silent install wrapper for the Shared components.

response_shared

Indicates the sample response file for the Shared components.

installCli

Indicates the silent install wrapper for the Client components.

response_client

Indicates the sample response file for the Client components.

admin

Indicates the admin response file required by the native Solaris *pkg* command.

response_upgrade

Indicates the response file for the default *pkgadd* question.

The upgrade_eAudit utility uses existing response files for the Shared and Client components or for the custom-built response files.

Prepare Silent Upgrade Response Files

You can use provided scripts to prepare the silent upgrade files for the AuditShared and AuditClient packages on Solaris systems, or you can build your own response files.

To record a silent upgrade response file on Solaris systems

1. Access a command shell prompt.
2. Create a dedicated directory to contain your silent upgrade response files.
3. Locate the directory on the installation media that contains the upgrade_eAudit wrapper file and AuditShared and AuditClient packages.
4. Copy the wrapper file, upgrade_eAudit, to the dedicated directory created in step 2.
5. Record a silent response file for the AuditShared package with the command:

   ```
   ./upgrade_eAudit -v 8.0.200.xxx -u AuditShared -g upshrsilent
   ```

6. Record a response file for the AuditClient package using the following command:

   ```
   ./upgrade_eAudit -v 8.0.200.xxx -u AuditClient -g upshrcli
   ```

Perform Silent Upgrade for Solaris Systems

You can perform an upgrade of your shared and Client components silently on Solaris systems.

To perform a silent upgrade on Solaris systems

1. Access a command shell prompt.
2. Navigate to the dedicated directory you created to contain your upgrade files.
3. Put the following files in the same directory with the upgrade_eAudit script, and the AuditShared-8.0.200.xxx-all.pkg and AuditCli-8.0.200.xxx-all.pkg files:
   - admin
   - response_upgrade response file
   - upshrsilent
   - upshrcli
   - installCli
   - installShared
4. Run the upgrade script for the AuditShared package using the command:

   ```
   ./upgrade_eAudit -v 8.0.200.xxx -u AuditShared -s upshrsilent –r response_upgrade
   ```

   Replace *xxx* with the version number of the script file in your directory.
5. Run the upgrade script for the AuditCli (Client) package using the command:

   ```
   ./upgrade_eAudit -v 8.0.200.xxx -u AuditCli -s upshrsilent –r response_upgrade
   ```

   Replace *xxx* with the version number of the script file in your directory.

Silent Upgrade for Linux Systems

You can use the silent upgrade option for the eTrust Audit Shared and Client components. This silent process upgrades an eTrust Audit Client at r1.5 SP2 Client or later to an r8 SP2 Client. The following silent upgrade files are provided on the installation media:

install_AuditShared

Indicates the silent install wrapper for the AuditShared package.

response_shared

Indicates the sample response file for the AuditShared package.

install_AuditClient

Indicates the silent install wrapper for the AuditClient package.

response_client

Indicates the sample response file for the AuditClient package.

Prepare Silent Upgrade Response Files

You can use provided scripts to prepare the silent upgrade response files for the AuditShared and AuditClient packages on Linux systems, or you can build your own response files.

You should create a dedicated directory for preparing the silent upgrade response files on your server.

To record a silent upgrade response files on Linux systems

1. Access a command shell prompt.
2. Create a dedicated directory to contain the silent upgrade response files you will record.
3. Locate the directory on the installation media that contains the AuditShared and AuditClient packages.
4. Copy the two wrapper files, install_AuditShared and install_AuditClient, to the dedicated directory created in step 2.
5. Navigate to the dedicated directory.
6. Record a silent response file for the AuditShared package with the following command:

   ./install_AuditShared -g shared_response_filename

7. Follow the instructions provided by the script.
8. Record a response file for the AuditClient package using the following command:

   ./install_eAudit -g client_response_filename

9. Follow the instructions provided by the script.

Perform Silent Upgrade for Linux Systems

You can perform an upgrade of your shared and Client components silently on Linux systems. This procedure uses the silent upgrade response files created in Prepare Silent Upgrade Files (see page 303).

Note: You must run the AuditShared script first.

To perform a silent upgrade on Linux systems

1. Access a command shell prompt.
2. Navigate to the dedicated upgrade directory you created for the silent upgrade response file.
3. Put the following files in the same directory with the AuditShared-8.0.200.xxx.i386.rpm and the AuditCli-8.0.200.xxx.i386.rpm files:
   - shared_response_filename
   - client_response_filename
   - install_AuditShared
   - install_AuditClient
4. Run the upgrade script for the AuditShared package using the command:

   ./install_AuditShared -s shared_response_filename
5. Run the upgrade script for the AuditCli (Client) package using the command:

   ./install_AuditClient -s client_response_filename

Silent Upgrade for UNIX Systems

You can use the silent upgrade option for the eTrust Audit Client and Data Tools components. This silent process upgrades an eTrust Audit components at r1.5 SP2 Client or later to a r8 SP2 components. The following silent upgrade files are provided on the installation media:

install_eAudit

Indicates the install wrapper file.

installCli

Indicates the silent install wrapper for the Client components.

response_client

Indicates the sample response file for the Client components.

installDT

Indicates the silent install wrapper for the Data Tools components.

response_DT

Indicates the silent install response file for the Data Tools components.

Prepare Silent Upgrade Response Files

You must create an upgrade response file for silent upgrades on UNIX systems. A silent upgrade response file contains different responses to prompts than a silent installation response file, so they are not interchangeable.

You should create a dedicated directory for preparing the silent upgrade response files on your server.

To record a silent upgrade response file on UNIX systems

1. Access a shell prompt.
2. Create a dedicated directory to contain your upgrade files.
3. Locate the directory on the installation media that contains the Audit Client package.
4. Copy the wrapper file, install_eAudit, to the dedicated directory created in step 2.
5. Navigate to the dedicated directory.
6. Record a response file for the AuditClient package using the following command:

   ./install_eAudit -g *upgrade_response_filename*

7. Follow the instructions provided by the script.

Perform Silent Upgrade for UNIX Systems

You can perform an upgrade of the Client components silently on UNIX systems.

To perform a silent upgrade on UNIX systems

1. Access a command shell prompt.
2. Navigate to the dedicated upgrade directory you created for the silent upgrade response file.
3. Run the upgrade script for the Client component using the command:

   ./install_eAudit -s *upgrade_response_filename*

Appendix C: Performing Silent Installations

This appendix describes the process of using the silent installation feature for both eTrust Audit and eTrust Security Command Center. Silent installations enable you to quickly install components on target servers without having to run the entire installation wizard on each computer.

This section contains the following topics:

Silent Installations for eTrust Audit

The silent installation and uninstallation feature is available for eTrust Audit Client components on Windows, UNIX, Solaris, and Linux systems.

Note: No silent installation is available for the eTrust Audit server components such as Policy Manager, Data tools, and the Reporter and Viewer, because you only have to install them once on a single computer.

Sample Unicenter Software Delivery packages are available to schedule delivery of eTrust Audit components on Windows, UNIX, Solaris, and Linux systems.

Create a Response File for Windows Systems

You must create an installation response file for silent installations on Windows systems. A silent installation response file contains different responses to prompts than a silent upgrade response file, so they are not interchangeable.

You should create a dedicated directory for silent installations on your server.

To record a silent installation response file for Windows systems

1. Access a command prompt.
2. Create a dedicated directory for your silent installation files.
3. Locate the directory on the installation media that contains the eTrust Audit Client package.

   For example, if the G: drive is the media drive, the eTrust Audit Client package folder is:

   cd /d <media drive>:\Winnt\Audit\Client

4. Enter the following command:

   Client.exe /r /f1"*response_filename*.iss"

   In this example, Client.exe is the name of the install program and *response_filename* is the fully-qualified name of the response file.

5. Follow the instructions provided in the installation procedures, and install the package as you would on the target computer.

   Note: Do not use the wizard's Back button while recording a silent response file. The resulting response file will contain too many entries and will be invalid.

6. Click Finish.

   The response file is created.

Note: If you want to customize the silent installation, the computer must not contain the product you want to install. If the computer has the product installed, remove it using the Control Panel, Add/Remove Programs feature. If you want to customize the silent uninstall, the computer must already have the product installed that you want to uninstall.

Customize Response Files for Silent Installation

The response files (*.iss) provided in the directory structure contain an example of a silent installation session. You should customize the silent installation to fit your environment or create your own version by following these instructions.

Perform Silent Installation of Windows Client

This procedure uses the silent response file created in Create a Response File for Windows Systems (see page 308).

To install the Client silently on Windows systems

1. Access a command prompt.
2. Navigate to the dedicated directory you created to contain your installation and response files.
3. Locate the directory on the installation media that contains the eTrust Audit Client package.

   For example, if the G: drive is the media drive, the eTrust Audit Client package folder is:

   ```
   cd /d <media drive>:\Winnt\Audit\Client
   ```

4. Enter the following command:

   ```
   Client.exe /r /f1"response_filename.iss"
   ```

   In this example, Client.exe is the name of the install program and *response_filename* is the fully-qualified name of the response file.
5. Follow the instructions provided in the wizard procedures, and upgrade the package as you would on the target computer.

   Note: Do not use the wizard's Back button while recording a silent response file. The resulting response file will contain too many entries and will be invalid.
6. Click Finish.

Create Response Files for Solaris Systems

Silent installation of the AuditShared and AuditCli packages is supported on Solaris systems. You can use the pkgask utility to record a response file specific to an application. To install the Client components silently on Solaris systems, you must record both a shared components and a client components response file.

A silent installation response file contains different responses to prompts than a silent upgrade response file, so they are not interchangeable. You should create a dedicated directory for silent installations on your server.

To record a silent installation response file for Solaris systems

1. Log in to the Solaris server as a root user.
2. Create a dedicated directory to contain the installation response files, and navigate to it.
3. Navigate to the directory in the installation media that contains the install_eAudit script and the installation packages.
4. Execute the following command:

   pkgask -r *response_file_name* -d *package_name*.pkg

   For example, to record a response file for the AuditCli package you should run:

   pkgask -r response_client -d AuditCli-all.pkg
5. Finish the installation to complete the response file.

Perform Silent Installation of Solaris Client

You can use these procedures to perform a first-time installation of the shared and Client components silently on Solaris systems. You must install the shared components first. These procedures use the response files created in Create Response Files for Solaris Systems (see page 310).

To install the AuditShared package silently on Solaris systems

1. Access a command shell prompt.
2. Navigate to the dedicated directory you created to contain your installation files.
3. Put the following files in the same folder:
   - AuditShared-8.0.200.100.xxx-all.pkg
   - admin
   - response_shared
   - installShared
4. Run the script with the following command:

   ```
   ./installShared 8.0.200.100.xxx response_shared /opt/CA/eTrustAudit
   ```

   Note: You can use the response_shared file provided on the installation media, or you can create your own response_shared file using the pkgask command.

To install the AuditCli package silently on Solaris systems

1. Put the following files in the dedicated installation files directory:
   - AuditCli-8.0.200.100.xxx-all.pkg
   - admin
   - response_client
   - installClient
2. Run the script with the following command:

   ```
   ./installClient 8.0.200.100.xxx response_client /opt/CA/eTrustAudit
   ```

   Note: You can use the response_client file provided on the installation media, or you can create your own response_client file using the pkgask command.

Create Response Files for Linux Systems

Silent installation of the AuditShared and AuditClient packages is supported on Linux systems. To install the AuditShared package and AuditClient package silently, you must record a separate silent installation response file for both the AuditShared and AuditClient package.

A silent installation response file contains different responses to prompts than a silent upgrade response file, so they are not interchangeable. You should create a dedicated directory for silent installations on your server.

To record a silent installation response file on Linux systems

1. Access a command shell prompt.
2. Create a dedicated directory to contain the silent installation response files you will record.
3. Locate the directory on the installation media that contains the Audit Shared and Client packages.
4. Copy the wrapper files, install_AuditShared and install_AuditClient," to the dedicated directory created in step 2.
5. Record a silent response file for the AuditShared package with the following command:

   ./install_AuditShared -g *shared_response_filename*
6. Follow the instructions provided by the script.
7. Record a silent response file for the AuditClient package using the following command:

   ./install_AuditClient -g *client_response_filename*
8. Follow the instructions provided by the script.

Perform Silent Installation of Linux Client

You can use these procedures to perform a first-time installation of the shared and Client components silently on Linux systems. You must install the shared components first. These procedures use the response files created in Create a Response File for Linux Systems (see page 312).

To install the AuditShared package silently on Linux systems

1. Access a command shell prompt.
2. Navigate to the dedicated directory you created to contain your installation files.
3. Put the following files in the same folder:
   - AuditShared-r8SP2-8.0.200.*.i386.rpm
   - response_shared
   - install_AuditShared script
4. Run the installation script with the following command:

   ./install_AuditShared -s *shared_response_filename*

To install the AuditCli package silently on Linux systems

1. Put the following files in the dedicated installation files directory:
   - AuditClient-r8SP2-8.0.200.*.i386.rpm
   - response_client
   - install_AuditClient script
2. Run the installation script with the following command:

   ./install_AuditClient -s *client_response_filename*

Create a Response File for UNIX Systems

You must create an installation response file for silent installations on UNIX systems. A silent installation response file contains different responses to prompts than a silent upgrade response file, so they are not interchangeable.

You should create a dedicated directory for silent installations on your server.

Note: Do not use the wizard's Back button while recording a silent response file. The resulting response file will contain too many entries and will be invalid.

To record a silent installation response file on UNIX systems

1. Access a shell prompt.
2. Create a dedicated directory to contain your installation files, and navigate to it.
3. Locate the directory on the installation media that contains the Audit Client package.
4. Run the installation script to record a response file for the AuditClient package using the following command:

   ./install_eAudit -g *response_filename*

5. Follow the instructions provided in the wizard procedures, and install the package as you would on the target computer.
6. Click Finish to create the Client response file.

Perform Silent Installation of UNIX Client

You can perform an installation of the Client components silently on UNIX systems.

To install the Client components silently on UNIX systems

1. Access a command shell prompt.
2. Navigate to the dedicated directory you created to contain the installation files.
3. Put the following files in the same directory with the install_eAudit and AuditCli-8.0.200.xxx-all.pkg files:
   - admin
   - upshrcli
   - installCli
4. Run the installation script for the Client component using the command:

   ```
   ./install_eAudit -s response_filename
   ```

Silent Installations for eTrust Security Command Center

The Silent installation feature is available for eTrust Security Command Center agent components on Windows, UNIX, and Linux systems.

Note: No silent installation is available for the eTrust Security Command Center server components because you only have to install them once on a single computer.

Sample Unicenter Software Delivery packages are also available to schedule delivery of the eTrust Security Command Center agent components on Windows, UNIX, and Linux.

Install Agent Components on Windows Silently

To install eTrust Security Command Center agent components on Windows silently

1. Access the target server on which you want to install the eTrust Security Command Center agent component. Verify that these eTrust Security Command Center agent component is not already installed on this computer. Close any open programs.
2. Open a command prompt and change your drive to the eTrust Security Command Center media drive and the directory to Winnt\eSCC\Agents.
3. Run the eTrust Security Command Center agent installation to create a silent response file by entering the following:

   setup.exe /r /f1"*[temp]*\eSCCAgentSetup.iss"

   where *[temp]* is the temporary directory in which to store your response file.

   - The '/r' parameter instructs the installation to record the silent response file.
   - The '/f1' parameter is optional, identifying a custom path and file name for the response file. If the '/f1' parameter is not used, the setup.iss file is created in the Windows folder, or appended to setup.iss if it already exists.
4. Follow the eTrust Security Command Center agent component installation procedure in Establishing a Working eTrust Security Command Center Environment.

   Note: Do not use the wizard's Back button when recording a silent response file. The resulting response file will contain too many entries and will be invalid.
5. Copy the newly recorded response file, [temp]\eSCCAgentsetup.iss or [Windir]\setup.iss, to each computer on which you want to run the installation silently. You can place it in a temporary folder in the computer or in any network folder you use for installation in the same place as the eTrust Security Command Center Agent setup.exe.
6. On all remaining client computer, run the installation silently:

   setup.exe /s /f1"*[temp]*\eSCCAgentsetup.iss"

   - The '/s' parameter instructs the installation to run silently.
   - The '/f1' parameter gives the full path and file name to the previously recorded custom response file.

   Note: Instead of using the '/f1' parameter, you can copy the 'setup.iss' file to the directory where the setup.exe program is located.

A software delivery option (SDO) is also available to silently push the agent components out to client computers at a scheduled delivery time using the Unicenter Software Delivery program. For more information, see Software Delivery Option for Agent Components (see page 320).

Install Agent Components on UNIX or Linux Silently

To install eTrust Security Command Center agent components on UNIX or Linux silently

1. Access the target server on which you want to install the eTrust Security Command Center agent components. Verify that these eTrust Security Command Center agent component is not already installed on this computer. Close any open programs.
2. Open a default UNIX shell and change your directory to the '/*[MEDIA_MOUNT_POINT]*/XXX\eSCC\Agents' subdirectory, where *[MEDIA_MOUNT_POINT]* is the path to the drive on which the installation media is mounted and XXX is the computer platform (AIX, HPUX, Linux, or Solaris).
3. Run the eTrust Security Command Center agent installation to create a silent response file by entering the following:

   setup.sh -r "*[tmp]*/setup.iss"

   where *[tmp]* is the temporary directory in which to store your response file.

   - The '-r' parameter instructs the installation to record the silent response file.
4. Follow the installation procedure in How to Install eTrust Security Command Center Agent Components on UNIX or Linux (see page 212).
5. Copy the newly recorded response file, setup.iss, to each computer on which you want to run the installation silently. You can place it in a temporary folder on the computer or in any network folders you use for installation in the same place as setup.sh.
6. On all remaining client computers, run the installation silently:

   setup.sh -s "*[tmp]*/setup.iss"

   - The '-s' parameter instructs the installation to run silently.

Note: After running the silent installation, the necessary PIKs can be installed by running the setup.sh script again, which will detect that the agent has already been installed and prompt for PIK information.

A software delivery option (SDO) is also available to silently push the agent components out to client computers at a scheduled delivery time using the Unicenter Software Delivery program. For more information, see Software Delivery Option for Agent Components (see page 320).

Appendix D: Unicenter Software Delivery (USD)

This appendix describes the use of Unicenter Software Delivery (USD) to silently push the eTrust Audit components or Security Command Center agents out to target computers at a scheduled delivery time using the Unicenter Software Delivery program.

This section contains the following topics:

Unicenter Software Delivery (USD) for Agent Components

Unicenter Software Delivery (USD) packages are available to deliver eTrust Audit components or Security Command Center agents using the Unicenter Software Delivery program. The necessary USD packages are located in the *[MEDIA_ROOT]*\XXX\YYY\ZZZ\reginfo subdirectory where XXX is the platform, YYY is the product and ZZZ is the component. For example, if G: is your install media:

```
G:\Winnt\Audit\Client\reginfo
```

A program named SDRegister is included, which lets you register software delivery packages to your Software Delivery Manager. These packages contain pre-recorded sample response files that are available for *template purposes only*. The sample response files (*.iss) reside in a parent directory of the reginfo directory. SDRegister.exe can be run from its current location lower in the directory structure to register one package at a time, or it can be run from a root directory to see and register all available packages at one time.

Example:

If G: is your install media, and G:\ is your current directory, enter the following command to install all available packages:

```
Winnt\eSCC\Agents\SDRegister.exe
```

If G:\Winnt is your current directory, enter the following command to install all available Windows packages:

```
eSCC\Agents\SDRegister.exe
```

To use USD packages for Unicenter Software Delivery

1. Run the SDRegister program, view and acknowledge the license file, and register the necessary installation, update, or uninstall files to your Software Delivery Manager. These sealed packages are not yet ready for distributed use.
2. Unseal the packages and update the sample response files using one of the following methods:
   - Record the customized response file (.iss) using the instructions detailed in the applicable procedure: Install Agent Components on Windows Silently (see page 316), Install Agent Components on UNIX or Linux Silently (see page 318), or Creating a Response File for Windows Packages (see page 308).
   - Modify the existing sample response files to reflect your local environment.
3. Once you perform the installation to verify your settings in the custom response file, re-seal the package you unsealed.

4. Distribute the USD packages.

For more information about this method of software delivery, consult a Unicenter Software Delivery administrator.

Appendix E: Uninstalling eTrust Audit and eTrust Security Command Center

Silent Uninstallation for Windows Client

Enter the following command to uninstall the eTrust Audit Client silently using an InstallShield response file:

```
Client.exe /s /f1"c:\temp\ClientMyUnInstall.iss"
```

Remove eTrust Audit Components on Solaris 10 Systems

Remove the eTrust Audit components in the reverse order in which you installed them. You should remove the Shared Components last in any case.

To remove eTrust Audit components

1. Log in to the UNIX server as a root user.
2. Discover the installed packages with the command:

   ```
   # pkginfo | grep Audit
   ```

   A list of packages that contain the string Audit displays.
3. Use the short package name to remove the package with the command:

   ```
   # pkgrm <packagename>
   ```

Uninstalling eTrust Security Command Center on UNIX or Linux

To remove eTrust Security Command Center from a UNIX or Linux machine, simply run the deinstall.sh shell script that is located in the following path:

[installation_path]/scripts

For example, issue the following command to launch this script:

/opt/CA/eTrustSecurityCommandCenter/scripts/deinstall.sh

Note: A silent uninstallation can be executed using the following command:

deinstall.sh -s

The uninstallation script performs the following functions:

- Deletes all eTrust Security Command Center registry entries
- Deletes symbolic links for eTrust Security Command Center shared libraries from the /opt/CA/SharedComponents/lib directory
- Removes all eTrust Security Command Center files
- Uninstalls selected Product Integration Kits
- Uninstalls eTrust Common Services if no other products use it

Uninstalling eTrust Audit or eTrust Security Command Center on Windows

You can remove all eTrust Audit or eTrust Security Command Center components from your Windows environment.

To uninstall eTrust Audit or eTrust Security Command Center on Windows

1. Select Settings, Control Panel from the Start menu.
2. Select Add or Remove Programs.
3. Highlight the eTrust Audit or eTrust Security Command Center component you want to uninstall, and then click Remove.
4. Repeat the previous step for each installed eTrust Audit or eTrust Security Command Center component you want to remove.
5. When you have removed all desired components, restart your computer.

Remove eIAM Server

The Embedded Identity and Access Manager (eIAM) server is usually installed during the Policy Manager installation. As such, eIAM is uninstalled when you uninstall the Policy Manager package.

If you install eIAM manually using the shell script, then you can uninstall it using a supplied script.

To uninstall eIAM manually

1. Navigate to the eiamuninstall.sh script located in the <eIamInstallPath>.

   To locate the script, execute the following commands:

   ```
   -bash-3.00$ ls -ltr *.sh
   -r-xr--r-- 1 root root 17164 Jul 26 14:29 eiamuninstall.sh
   -bash-3.00$ pwd
   /opt/CA/SharedComponents/EmbeddedIAM
   ```

2. Run the script with the command:

   ```
   -bash-3.00$ ./eiamuninstall.sh
   ```

Index

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W