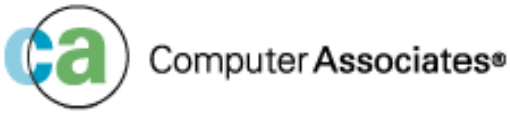

Computer Associates

eTrust™ Audit™ r8

Security Target Version 2.6

December 20, 2005

Prepared for:

Computer Associates
6150 Oak Tree Blvd, Suite 100
Park Center Plaza II
Independence, OH 44131

CYGNACOM SOLUTIONS

an Entrust Company

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

Revision History:

Date:	Version:	Author:	Description
6/26/05	2.0	Debra Baker	Update to reflect test results
9/4/2005	2.1	D. DePrez	Revised per validator's comments
10/24/2005	2.2	D. DePrez	Revised per evaluator's comments
10/25/2005	2.3	D. DePrez	Revised per editorial comments
11/25/2005	2.4	D. DePrez	Revised per validator's comments
12/1/2005	2.5	D. DePrez	Threat mappings and assurance measures updated per evaluator's comments.
12/20/2005	2.6	D. DePrez	Slight modification to Assurance Measures Tables for AGD_USR.1 and AVA_SOF.1

TABLE OF CONTENTS

SECTION
PAGE

Table of Tables

Table **Page**

Table of Figures

Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: Computer Associates *eTrust*™ Audit™ r8

ST Title: Computer Associates *eTrust*™ Audit™ r8 Security Target

ST Version: Security Target Version 2.6

ST Authors: Debra Baker, D. DePrez

ST Date: December 20, 2005

Assurance Level: EAL2

Strength of Function: Not Applicable

Vendor: Computer Associates

Vendor Address: 6150 Oak Tree Blvd, Suite 100
Park Center Plaza II
Independence, OH 44131

Keywords: intrusion detection, intrusion detection system, sensor, analyzer, Security Target, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Computer Associates *e*Trust Audit r8. *e*Trust Audit is an audit data collector (sensor) and analyzer.

*e*Trust Audit allows audit data to be selectively collected from a diverse set of systems, applications, devices and appliances that may be indicative of misuse of IT resources. In addition, *e*Trust Audit allows the user to create and manage a centralized policy regarding the retention of audit information performing, intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, and reporting of conclusions. The evaluated configuration includes the *e*Trust Audit Policy Manager and Audit Data Tools installed on MS Windows 2000 platforms with an MS Windows 2000 client from which audit data is collected.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundary of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Acronym definitions are provided in Section 9.

2 TOE DESCRIPTION

2.1 Product Type

*e*Trust Audit allows audit data to be selectively collected from a diverse set of systems, applications, devices and appliances that may be indicative of misuse of IT resources.

*e*Trust Audit (Policy Manager component) allows the user to create and manage a centralized policy regarding the retention of audit information performing, intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, and reporting of conclusions.

*e*Trust Audit (Client component) is able to collect data about all selectable events as they occur on an IT System. Events may include authentication events; data access events; configuration access events; service requests; network traffic; data introduction; and, start-up and shutdown of audit functions. Collected events can be filtered and forwarded to an Administrator for data reduction and analysis.

*e*Trust Audit (Data Tools component) is able to receive data from identified data collectors and process the specified data to make intrusion/vulnerability determinations. Responses to identified intrusions/vulnerabilities may include execution of an action program, email alerts, visual signals/alarms displayed through the Security Monitor, storage in the central audit data repository, or sending an alert to another client.

The product relies upon the IT environment to protect TSF data as well as identify and authenticate users and maintain user roles.

2.2 *e*Trust Audit Components

The TOE is described in Section 2.3. *e*Trust Audit r8 is a distributed network based product. There are four main components in the *e*Trust Audit r8 product: *e*Trust Audit Client (which collects audit events), *e*Trust Audit Policy Manager, Collector (which writes events into the central audit data repository), and Audit Data Tools. Product components can reside on the same system, or on multiple systems. In the evaluated configuration, TOE components are on separate systems.

*e*Trust Audit r8 installs an *e*Trust Audit Client on each targeted system or application host. This component works to collect, filter and redirect all audit events to other TOE components. *e*Trust Audit Client can accept event data directly from OS logs, or submitted by other applications that are not natively supported by *e*Trust Audit. Applications can send standardized SNMP trap information to the *e*Trust Audit Client for filtering and handling. All collected data are translated into a common format for viewing and reporting.

*e*Trust Audit Policy Manager supports the definition of the common audit policy that is enforced by each *e*Trust Audit Client. The common audit policy can assign patterns to events so that actions can be automatically triggered based on the matched events. This serves as a first line of defense for host intrusion detection and supports the ability to control damages that might be inflicted by unauthorized user accesses. *e*Trust Audit also ships with customizable predefined rules so that the deployment of rules specifying patterns can be performed swiftly.

Audit Data Tools supports reporting and analysis of the central audit data repository. Functions supported include report generation, real-time visual signals/alarms, email generation or execution of a program.

The Collector component serves as the point where consolidation of audit events collected by the *e*Trust Audit Client is performed: audit events collected by the *e*Trust Audit Client are written

into the central audit data repository by the Collector. Please see **Error! Reference source not found.**1 for further clarification.

2.2.1 *e*Trust Audit Client

The *e*Trust Audit Client is comprised of several subcomponents that provide services that collect and forward audit event data. *e*Trust Audit Client collects audit events in the sense that it gathers or exacts audit events from a number of sources. The subcomponents are:

- **iRecorder** - The iRecorder component taps into the event data sent to the OS Event Log. The iRecorder component enables any events sent to this standard system logging facility to be collected by *e*Trust Audit for processing. iRecorder components that read other system logs and applications are available as an interface, but are not in included the evaluated configuration.
- **iRouter -** iRouter component is middleware that bridges the HTTP protocol, XML format event used in iRecorder components to the native RPC-based SAPI event used in Audit. The iRouter component is installed on the same host as Audit Client's Router component. It receives events from iRecorder components, converts XML to SAPI and sends them to the Router component.
- **Router** - The Router component acts primarily as a filtered message forwarder. It analyzes the policies created by the administrator using the Policy Manager (deployed as .cfg files found in the *installation_path*\e*Trust Audit**cfg directory*), and then follows those policy imperatives to examine audit events that are sent to it by the iRouter and Redirector components. Based on the configuration instructions provided by the administrator, the Router component identifies those records that should be as follows:
  - Filtered out
  - Forwarded to the Action Manager
  - Forwarded to other *e*Trust Audit components for additional processing or storage
- **Action Manager** - The Action Manager component processes events sent to it by the Router component. The administrator can instruct the Action Manager to automatically perform a wide range of actions in response to receiving specific audit events. The Action Manager component gets its instructions from the policies created using the Policy Manager and executes those actions as necessary and appropriate to a specific audit event.
- **Distribution Agent** - The Distribution Agent component receives policy imperatives from the Policy Manager, and places these policies into effect.
- **Portmapper** - The Portmapper component manages the logical communications channels required to provide a standard way for a Client to access RPC services that it might require.
- **Redirector** - The Redirector component taps into local *e*Trust Audit logs and automatically redirects that audit data to a Router component on the same or on another machine.

2.2.2 *e*Trust Audit Policy Manager

*e*Trust Audit Policy Manager supports specification of rules defining an accumulation or combination of audit events based on specified criteria (a filter) that is used to determine which events are subject to the action described in the rule known to indicate a potential security violation. The *e*Trust Audit Policy Manager component includes the following subcomponents:

- **Policy Manager** – The Policy Manager component interface is a Windows GUI and Web GUI that is used to centrally manage *e*Trust Audit policies. Using the Policy Manager, the administrator can create, implement, and distribute the organization's *e*Trust Audit policies.
- **Distribution Server** – The Distribution Server component communicates with the Distribution Agent and coordinates the delivery of *e*Trust Audit policies.
- **Audit Administrator** – The Audit Administrator component is an audit management tool that performs the advanced audit management functions such as audit manager configuration and advanced queries.
- **iRecorder Manager** – (Not included in TOE) The iRecorder Manager component is available through a Web Interface. The Administrator can use the iRecorder Manager component to view status, configuration, and supported data model information for selected iRecorders. A list of all the hosts running one or more discovered iRecorders is displayed in the iRecorder Browser list. iRecorder Manager generates this list from the iRecorders that were detected on the specified network.

2.2.3 Audit Data Tools

The Audit data tools component is comprised of the following components:

- **Viewer** - The Viewer displays, sorts, and filters audit events retrieved from the central audit data repository. The viewer also allows the administrator to save customized filters for future use.
- **Reporter** - The Reporter allows the administrator to view, create, and schedule detailed, graphic reports from information extracted from the central audit data repository.
- **Security Monitor** – The Security Monitor performs the following: 1) Monitor specific events; the events can be sent from a variety of different recorders and 2) Monitor *e*Trust Audit status and "self help" events. These are events related to the status of *e*Trust Audit components (for example, whether the Action Manager is started). System administrators and security personnel can use the Security Monitor to receive heads-up notification of potentially significant events.
- **Post Collection Utility (PCU)** – The PCU application performs the following post-collection tasks on the central audit data repository:
  - Expands event data into individual entries through Load Policies;
  - Builds logical views with selectable expanded data through View Policies;
  - Detects tampering evidence by digitally signing and verifying digital signatures on collected events through Tamper Policies;
  - Manages the size and contents of the central audit data repository through Prune Policies.

Note: PCU itself is not in the TOE.

2.2.4 Collector

The Collector supports audit data collection in the sense that it brings together audit events into one place: the central audit data depository. The iRecorder and Router subcomponents of the *e*Trust Audit Client collect audit events and forward them to the Collector for storage in the central audit data repository and later viewing and analysis through the Audit Data Tools. The Collector component serves as the point where consolidation of collected audit events into the central audit data repository is performed, but does not support the TSF in collecting the audit events from the IT environment. Rather, the Collector supports a write-interface to long-term

audit data storage in the central audit data repository of audit events collected by the *e*Trust Audit Client..

2.3 TSF Physical Boundary and Scope of the Evaluation

The TOE consists of the following *e*Trust Audit software components:

- *e*Trust Audit Client
- *e*Trust Audit Policy Manager
- Audit Data Tools

The Collector component is not included in the TOE. The generalized TOE architecture is depicted within in Figure 2-1

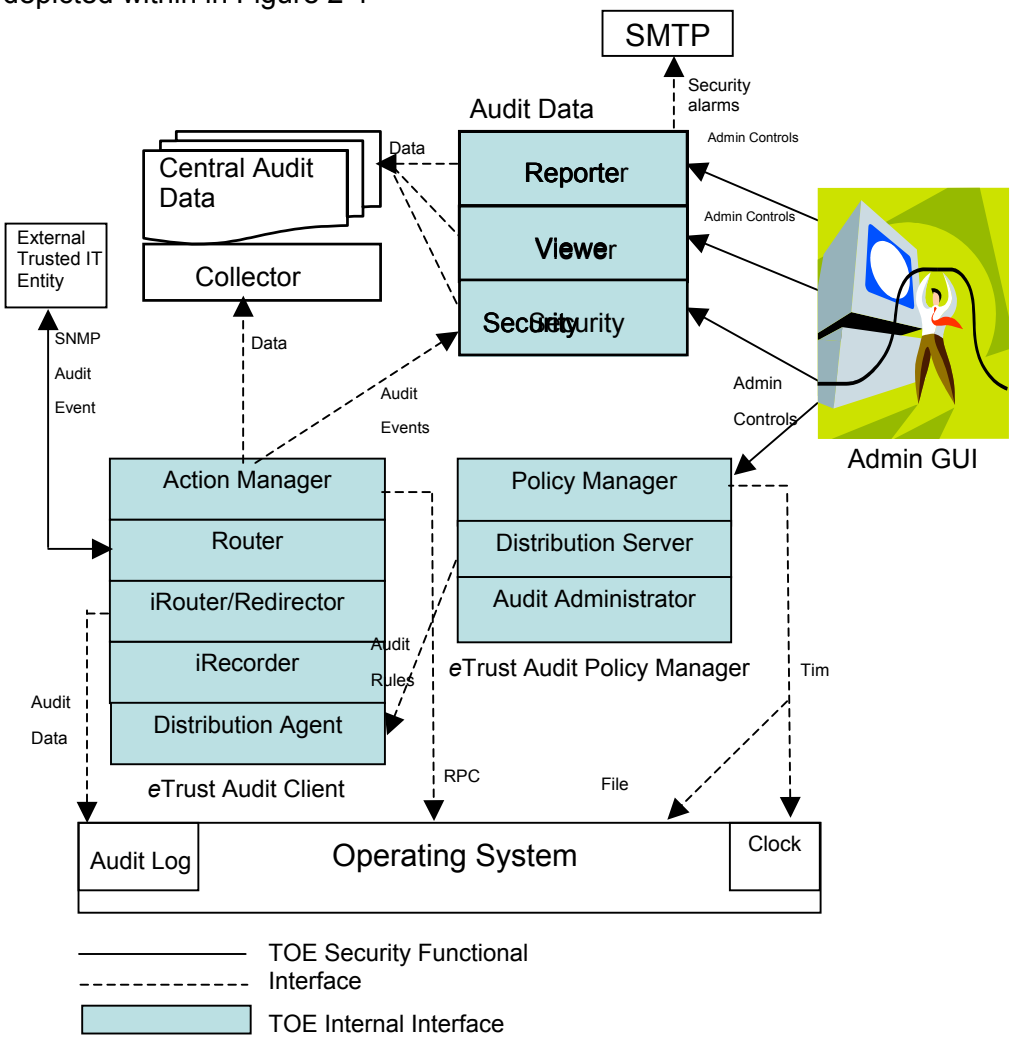

Figure 2-1 Generalized TOE Architecture

Figure 2-1 depicts the TOE components involved in policy definition and distribution. The Policy Manager GUI, in combination with the Audit Administrator supports definition of centralized security policy management functionality, including a set of predefined policies. The Distribution Server then supports remote distribution of the defined policy to each of the *e*Trust Audit Client

installations. The audit policy is then installed into the Router and Action Manager sub-components by the Distribution Agent subsystem of the Audit Client. The Portmapper subcomponent is responsible for assigning network ports to the Router, Action Manager, Monitor and Collector.

Error! Reference source not found. Figure 2-1 depicts the TOE components involved in the monitoring of enterprise-wide security events and system audit data, filtering of collected information for consolidated viewing and reporting and automatically trigger appropriate actions upon detecting unusual or malicious activities on the system. Collected events and audit data is sorted by the Router and the Action Manager as either: not needed for further processing, forwarding to the Audit Data Tools, or forwarding to the Collector for storage in the central audit data repository. The central audit data repository stores information making it available for later analysis, reporting, and correlation through the Audit Data Tools component. Neither the Collector nor the central audit data repository is part of the TOE. More critical events sent directly to the Audit Data Tools support the capability to notify systems, network, and security personnel of critical events in near real-time.

The evaluated configuration includes the following hardware, operating systems, and relational database, which are in the IT Environment:

***e*Trust Audit Policy Manager**

- Windows 2000 Server SP4
- Pentium 1 GHz Processor
- 128 MB Memory
- 300 MB Disk Space
- Microsoft Internet Explorer 6.0 SP1
- TCP/IP

***e*Trust Audit Data Tools**

- Windows 2000 Server SP4
- Pentium 1 GHz Processor
- 256 MB Memory
- 1000 MB Disk Space
- Microsoft SQL Server 2000 SP3 relational database server
- TCP/IP

***e*Trust Audit Client**

- Windows 2000 Server SP4
- Pentium 1 GHz Processor
- 256 MB Memory
- 100 MB Disk Space
- TCP/IP

The underlying operating system software (Windows 2000) and hardware, the Collector and the relational database (central audit data repository) the Collector writes into are part of the IT environment.

2.4 Logical Boundary

The security functionality provided by *e*Trust Audit includes:

- **Collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System.**
- **Perform intrusion analysis, generate conclusions, and respond accordingly in the event an intrusion is detected.** *e*Trust Audit is able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. *e*Trust Audit will take action to execute a program, send an email notification, send the event to the Security Monitor, send the event to the central audit data repository, or send an alert to another client upon detection of a potential security violation[1].
- **Provide the ability for Administrators to view, filter and manage all audit event data collected and produced.** This includes ability to perform searches, sorting, and ordering of the audit data, based on various criteria.
- **Manage TOE functions and data.**

*e*Trust Audit relies upon a third party database and the underlying operating system and hardware platform to store and protect audit data records, to provide reliable time stamps, to authenticate the TOE administrator, to maintain security roles, and to protect the *e*Trust Audit hosts from other interference or tampering.

[1] Only one client is included in the evaluated configuration. Therefore product features involving inter-client communications are not tested in the evaluated configuration.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security.

3.1 Assumptions

This section contains secure usage assumptions regarding the IT security environment.

Table 3-1 – Secure Use Assumptions

#	Assumption ID	Assumption Description
1	A.INTROP	The TSF and IT environment are configured for proper interoperation.
2	A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
3	A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification and access.
4	A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.2 Threats

The TOE must counter threats to security included in table below. The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to standard equipment and public information.

Table 3-2 – TOE Security Threats

Item	Threat ID	Threat Description
1	T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
2	T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

Table 3-3 – IT System Security Threats

Item	Threat ID	Threat Description
3	T.FALACT	Inappropriate activity on the IT system the TOE monitors by an attacker may not be identified or associated with other suspicious events allowing the IT system data to be compromised.
4	T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors allowing an attacker to violate the IT environment's access control policy or assume the identity of an authorized user, and thereby allowing the IT system data to be compromised.
5	T.BYPASS	An unauthorised user may attempt to bypass the IT Environment's information flow control policy to gain access to data stored on and protected by IT system.

3.3 Organizational Security Policies

Table 3-4 – Organizational Security Policies

Item	Policy	Policy Description
1	P.DETECT	Events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
2	P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 – Security Objectives for TOE

Item	Objective	Objective Description
1	O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the TOE.
2	O.IDANLZ	The TOE must accept event data from the IT system and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
3	O.RESPON	The TOE must respond appropriately to analytical conclusions.
4	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

The security objectives for the IT environment are as follows:

Table 4-2 – Security Objectives for IT Environment

Item	Objective	Objective Description
1E	OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control.
2E	OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
3E	OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
4E	OE.I&A	The IT Environment shall provide functionality to require identification and authentication for all TOE users.

4.2.2 Non-IT Security Objectives

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

Table 4-3 – Security Objectives for Non-IT Environment

Item	Objective	Objective Description
1N	ON.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
2N	ON.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
3N	ON.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
4N	ON.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
5N	ON.INTROP	The TOE is interoperable with the IT System it monitors.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC, and CCIMB Final Interpretations.

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, Section 4.4.1.3.2, as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.1 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1. They are all taken from Part 2 of the Common Criteria.

Table 5-1 – Functional Components

Item	Class	Component	Component Name
1	Security audit	FAU_ARP.1	Security alarms
2	Security audit	FAU_GEN_EXP.1	Audit data collection
3	Security audit	FAU_SAA.1	Potential violation analysis
4	Security audit	FAU_SAR.1	Audit review
5	Security audit	FAU_SAR.3	Selectable audit review
6	Security management	FMT_SMF.1	Specification of management functions

5.1.1 Class FAU: Security Audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take **[*action to execute a program, send an email notification, send the event to the Security Monitor, send the event to the central audit data repository, or send an alert to another Client as specified by the audit policy*]** upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

Application Note: *The specific action taken when a potential security violation is detected is configurable. The TOE will execute a program, send an email notification, send an event to the Security Monitor, or send an event to the central audit data repository depending upon what was specified in the audit policy. Only one client is included in the evaluated configuration. Therefore product features involving inter-client communications are not tested in the evaluated configuration. All of the other configurations of audit policy will be tested. Note that when the event is sent to the central audit data repository, an administrator can use the Viewer to display events or use the Reporter to generate reports for later analysis.*

FAU_GEN_EXP.1 Audit data collection

Hierarchical to: No other components.

FAU_GEN_EXP.1.1 The TSF shall be able to collect audit information from the following resources on the targeted IT System:

a) System data.

b) Submitted audit events.

FAU_GEN_EXP.1.2 The TSF shall collect at least the following information:

a) Event time stamp, computer name, domain name, log name, event id, username, source and event category.

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: *In this SFR, collection is meant to mean gathering or exacting audit events from a number of sources. The TOE is open-ended as to the types of events that are collected from the targeted IT System resources. The TOE adds identifying information to the events captured such as computer name, domain name, log name and other fields as required.*

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of **[*audit events specified in a defined policy*]** known to indicate a potential security violation;

b) **[*no other rules*]**.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: *The TOE allows the definition of policies, which contain specific audit events, specific combinations of audit events, or specific numbers of an event that will result in the indication of a potential security violation.*

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*the TOE user*]** with the capability to read **[*all audit information stored by the TOE*]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: *Note that in this SFR "audit records" refer to the audit records collected and stored by the TOE. Audit records stored by systems outside the TOE are outside the scope of the TOE.*

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform **[*searches, sorting, and ordering*]** of audit data based on **[*event timestamp, computername, domainname, logname, event id, username, source and event category*]**.

Dependencies: FAU_SAR.1 Audit review

5.1.2 Class FMT: Security management

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[*as specified in Table 5-2*]**.

Dependencies: No dependencies

Table 5-2 – Management of TSF Data

Allowed Operations on TSF data (Security Management Functions)	TSF Data
Create, edit, and delete	audit node groups and audit nodes
Create, edit, and delete	rules, actions, and associations
Create, activate, edit, and delete	policies

5.2 Security Functional Requirements for the IT Environment

*e*Trust Audit requires that the operating system platform provide access control, identification and authentication, protection of the TSF through non-bypassability of the TSP and domain separation, and reliable time stamps. The IT environment also performs audit data generation; audit data is gathered by *e*Trust audit Redirectors or iRecorders that are installed on systems in the IT environment. In the evaluated configuration, only the OS Event Log iRecorder is tested.

Table 5-3 – Functional Components for the IT Environment

Item	Component	Component Name
1E	FAU_GEN.1	Audit data generation
2E	FAU_STG.1	Protected audit trail storage
3E	FDP_ACC.1	Subset access control
4E	FDP_ACF.1	Security attribute based access control
5E	FIA_UAU.2	User authentication before any action
6E	FIA_UID.2	User identification before any action
7E	FMT_MSA.1	Management of security attributes
8E	FMT_MSA.3	Static attribute initialisation
9E	FMT_SMR.1	Security roles
10E	FPT_RVM_EXP.1	Non-bypassability: IT
11E	FPT_SEP_EXP.1	Domain separation: IT
12E	FPT_STM.1	Reliable time stamps

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 **Refinement:** The ***IT environment*** shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[*not specified*]** level of audit; and

c) **[*All attempts to access TSF data other than thru the TOE and no other events*]**.

FAU_GEN.1.2 **Refinement:** The ***IT environment*** shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST: **[*computer that audit data originated from, domain, event ID, source, category, event description*]**.

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: *Audit records that are generated by the IT Environment are collected by eTrust audit when the system that is hosting the Redirector or iRecorder component is defined as an Audit Node (AN) to an AN group. The eTrust Audit Administrator configures which audit data is collected via the Policy Manager. This audit requirement is distinct from FAU_GEN_EXP.1 and specifies one source of event data collected by the TOE.*

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

FAU_STG.1.1 **Refinement:** The ***IT environment*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 **Refinement:** The ***IT environment*** shall be able to **[*prevent*]** unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: *This SFR specifies the protection required to protect the TOE's audit event data. This includes the TOE's audit event data (see FAU_GEN_EXP.1)*

FDP_ACC.1 - Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 **Refinement:** The ***IT environment*** shall enforce the ***[IT Environment Access Control Policy]*** on ***[subjects: TOE administrators; objects: TOE configuration data and audit data; operations: TOE configuration and audit data modification and deletion]*.**

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 **Refinement:** The ***IT environment*** shall enforce ***the [IT Environment Access Control Policy]*** to objects based on the following**: *[subjects: TOE administrators; objects: TOE configuration and data; operations: modification and deletion of TOE configuration and data is limited to TOE administrators].***

FDP_ACF.1.2 **Refinement:** The ***IT environment*** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed***; [Access is granted on requested operations based on privileges granted by the OS.]***.

FDP_ACF.1.3 **Refinement:** The ***IT environment*** shall explicitly authorize access of subjects to objects based on the following additional rules: ***[no explicit rules].***

FDP_ACF.1.4 **Refinement:** The ***IT environment*** shall explicitly deny access of subjects to objects based on the ***[no explicit rules].***

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1 **Refinement:** The ***IT environment*** shall ***prevent any TSF-mediated actions on behalf of the user from being performed before the identified user is successfully authenticated.***

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1 **Refinement:** The ***IT environment*** shall ***prevent any TSF-mediated actions*** on behalf of ***the*** user ***from being performed before that user is identified***.

Dependencies: No dependencies

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 **Refinement:** The ***IT environment*** shall enforce the ***[IT Environment Access Control Policy]*** to restrict the ability to ***[modify, delete]*** the security attributes: ***[OS attributes associated with delete, modify permissions on TOE Data]*** to ***[TOE administrator].***

Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security Roles

FMT_MSA.3 - Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 **Refinement:** The ***IT environment*** shall enforce the **[*IT Environment Access Control Policy*]** to provide **[*restrictive* [*no other properties*]]** default values for security attributes that are used to enforce the ***IT environment*** SFP.

FMT_MSA.3.2 **Refinement:** The ***IT environment*** shall allow the ***[OS administrator]*** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_SMR.1 - Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 **Refinement:** The ***IT environment*** shall maintain the roles ***[TOE administrator; OS administrator]***.

FMT_SMR.1.2 **Refinement:** The ***IT environment*** shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FPT_RVM_EXP.1 Non-bypassability: IT

Hierarchical to: No other components.

FPT_RVM_EXP.1.1: The security functions of the IT environment shall ensure that IT environment security policy enforcement functions are invoked and succeed before each

function within the scope of control of the IT environment is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1 Domain separation: IT

Hierarchical to: No other components.

FPT_SEP_EXP.1.1 The IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface.

FPT_SEP_EXP.1.2 The IT environment shall enforce separation between the security domains of subjects in the Operating System's Scope of Control.

Dependencies: No dependencies.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The TSF shall ***make use of reliable time stamps provided by the IT environment.***

Dependencies: No dependencies

5.3 Strength of Function

There are no probabilistic or permutational functions in the TOE; therefore strength of function is not applicable.

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-4.

Table 5-4 – Assurance Requirements: EAL2

No.	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance

No.	Component	Component Title
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

The following sections describe the IT Security Functions of the *e*Trust Audit Components.

Table 6-1 – Security Functional Requirements Mapped to Security Functions

Security Functions	SFRs
Security Audit – Collection	FAU_GEN_EXP.1
Security Audit – Rules	FAU_ARP.1
	FAU_SAA.1
Security Audit – Reporting	FAU_SAR.1
	FAU_SAR.3
Management	FMT_SMF.1

6.1.1 Security Audit – Collection

As discussed in Section 2, the TOE is a distributed TOE with separate management, collection, and analysis components. The audit event gathering component of the TOE (i.e.: the *e*Trust Audit Client, *see* Section 2.2.1) must be installed onto all targeted IT systems that the TOE monitors. *e*Trust Audit r8 supports an open design that accepts audit events from both the host OS, and external IT entities.

The TOE relies on the IT environment to write the collected information in the central audit data repository, via the Collector component of the product. The Collector is part of the IT environment. Please see Section 2.2.4 for further details.

In the case where the TOE is gathering audit events from the host OS, the TOE is configured thru the central audit policy to monitor an OS log and when the log is updated by the targeted IT system, the TOE collects the audit event and adds information to identify the audit event source. Standard system security events that may be collected include start-up, shutdown, changes in system IP configuration, and changes to the Allowable Use Policies.

The other category of audit events is based on SNMP messages received from external IT entities. These events are determined when the IT entity is configured external to the TSF. This category of audit events may be parsed and processed and analysed in the same way that audit events collected from OS logs are.

The following environmental and site-specific attributes can be added to collected audit events: event time stamp, computer name, domain name, log name, event id, and user name and source, and event category.

Once collected the audit events are processed as described in Section 6.1.2.

This functionality meets the requirement FAU_GEN_EXP.1.

6.1.2 Security Audit – Rules

*e*Trust Audit allows a user to create, activate, and distribute policies to clients that generate audit records (*see* Section 6.1.4). As events occur on clients, the *e*Trust iRecorder on the client collects audit records (see Section 6.1.1) and send them to the Router for filtering and processing. Based on the administrator-created policies, the Router sends records to be processed by the Action Manager. All of these events are controlled by Administrator defined policies, which are made up of Rules.

A Rule includes a filtering mechanism which evaluates traffic in real-time and determines if an action should be taken (e.g.: an event is detected). If a collected audit event does not evaluate to match an action (see below for a list of possible actions), it is dropped as not security relevant. Filters may be defined on any attribute of the collected audit event. Filters can also include an accumulation or combination of audit events based on specified criteria, as well as single events.

When *e*Trust Audit detects a particular event, it can be directed to do the following:

- Perform another action such as send an email or execute a program.
- Send the event to the Security Monitor to alert the user that the event has occurred,
- Forward the event to the central audit data repository (i.e.: to the Collector),
- Send an alert to another Client as specified by the audit policy,

*e*Trust Audit is installed with a set of predefined Rules, which can be edited and augmented by the *e*Trust Audit Administrator.

This function meets the requirements FAU_ARP.1 and FAU_SAA.1 .

6.1.3 Security Audit – Reporting

*e*Trust Audit provides three mechanisms to support the reviewing of the collected and filtered audit events. These are:

- Aggregation of audit events into a central audit database which can be analyzed with the Viewer or Reporter components of the Audit Data Tools described in Section 2.2.3,
- Alerting the administrator thru the Security Monitor,
- Performing another action such as send an email or execute a program.

Potentially valuable audit events collected at nodes throughout the enterprise are stored on a centralized, searchable, relational database, the central audit data repository. From the central audit data repository the audit events collected from all collectors are available to administrators for analysis, reporting, and correlation, supporting the need for a complete picture of system activities. In addition to the filtering that occurs at the points of audit event collection, the Administrator can specify filters on the audit events so that only relevant audit events are presented on the Viewer monitor or in a given report generated by the Reporter. The data may be filtered and sorted by audit event attribute (timestamp, event id (e.g., Windows native id), log name, source, category, user, computer, domain or event details), type of event such as logon/logoff, network, administration, and startup/shutdown, or source file. Reports can also be configured and scheduled and an alert (such as an email) can be generated to notify the Administrator.

Through the Security Monitor GUI, the Administrator can view a scrolling real time list of alerts a capability that allows administrators to be notified of critical events in near real-time. The Security Monitor does not support filtering functionality but the Administrator can control the scrolling of events. By default the Security Monitor GUI will hold 500 alerts, but can be configured to hold as many as 10,000 alerts. Alerts can be saved into text files, or copied using a control sequence.

Filters are used to streamline the audit information. There are 3 types of filters: filter by field, filter by event, filter by file.

- filter by field selects events based on timestamp, event id (e.g., Windows native id), logname, source, category, user, computer, domain or event details.
- filter by event selects events based on the type: logon/logoff, network, administration, startup/shutdown, …
- filter by file selects events on access to file from open to close.

Audit events can also be reported through a RPC call to a service or executable.

This functionality meets functional requirements FAU_SAR.1 and FAU_SAR.3.

6.1.4 Management

One role exists in the TOE: Administrator. This role includes the ability to define the central audit policy, view (query) all event data and receive security alerts. This role is maintained and supported by the IT environment.

The behavior of the system data collection, analysis, and reaction functions is controlled by configuration files. The Administrator may use the administrative interfaces, consisting of a windows or web-based GUIs, to generate and maintain the configuration files. Filtering rules are specified through a proprietary filter language. Rules can be created or modified through the Administrator Interface with a wizard or text editor. Access to the Administrator interface is secured, controlled, and supported through the access control measures implemented in the IT environment.

Through the administrative interfaces the Administrator configures IT systems into ANs and AN groups monitored by the TSF, defines rules regarding the filtering of audit events collected from the configured IT systems, and associates defined rules with actions. Once a filter is associated with an action the resultant data collection, analysis, and reaction functions can be grouped to define a central audit policy. Once the Administrator defines the central audit policy the central audit policy is distributed to each of the nodes (configured IT entities) over the network. The IT environment supports the secure distribution and storage of the central audit policy.

Audit events collected can be filtered based on any of the attributes found in the collected data, as well as event frequency. The following environmental and site-specific attributes can also be specified: event time stamp, computer name, domain name, log name, event id, username, and source and event category. Specific configurable actions are: forward the event to an alternate Router, forward the event to the central audit data repository, send the event to the Security Monitor to alert the Administrator that the event has occurred, send an alert to another client, or perform another action such as send an email or execute a program. If no action is configured for a collected audit event, it is dropped.

The Administrator can monitor the distribution of the central audit policy to the targeted IT systems through the Administrator interface.

This functionality meets the requirement FMT_SMF.1.

6.2 SOF Claims

There are no specific SOF Claims, since there are no probabilistic or permutational mechanisms included in the TOE.

6.3 Assurance Measures

*e*Trust Audit satisfies the assurance requirements for Evaluation Assurance Level EAL2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-2 – Assurance Measures and How Satisfied

Item	Component	Evidence Requirements	How Satisfied
1	ACM_CAP.2	CM Documentation ▪ CM Proof ▪ Configuration Item List	Audit 1.5 SP3 file list Audit r8 file list - rev3
2	ADO_DEL.1	Delivery Procedures	Distribution Centers Procedures Manual United States And Canada SITE Visit Report for Computer Associates Product Submission Form Product Submission Form Process Flow Preservation of Product Procedure
3	ADO_IGS.1	Installation, generation, and start-up procedures	Installation of the eTrust Audit TOE eTrust Audit Getting Started r8 eTrust Audit Release Summary r8
4	ADV_FSP.1	Functional Specification	eTrust Audit r8 EAL2 Common Criteria Evaluation Proprietary Development Specification
5	ADV_HLD.1	High-Level Design	eTrust Audit r8 EAL2 Common Criteria Evaluation Proprietary Development Specification
6	ADV_RCR.1	Representation of Correspondence	eTrust Audit r8 EAL2 Common Criteria Evaluation Proprietary Development Specification
7	AGD_ADM.1	Administrator Guidance	eTrust Audit, Audit Management Guide r8 *e*Trust Audit, Getting Started Guide r8 *e*Trust Audit, Reference Guide r8 Computer Associates eTrust™ Audit™ r8 Common Criteria Supplement to the Guidance Documentation
8	AGD_USR.1	User Guidance	Not Applicable No non-administrative users of TOE
9	ATE_COV.1	Test Coverage Analysis	Test Coverage for eTrust Audit

Item	Component	Evidence Requirements	How Satisfied
10	ATE_FUN.1	Test Documentation	Evaluation Team Report for On-Site Functional Testing Common Criteria Certification Test Environment Specification QA Test Plans for eTrust Audit
11	ATE_IND.2	TOE for Testing	TOE for Testing
12	AVA_SOF.1	SOF Analysis	Not Applicable No Strength of Function Claimed
13	AVA_VLA.2	Vulnerability Analysis	Computer Associates eTrust Audit r8 Vulnerability Analysis Vulnerability Analysis Summary Spreadsheet

7 PP Claims

The *e*Trust Audit Security Target is not written to address any existing Protection Profile.

8 RATIONALE

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE.

Table 8-1 – All Threats to Security Countered

#	Threat ID	Threat Description	Objective ID	Rationale
1	T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.	1 O.IDSENS, 2 O.IDANLZ, 3 O.RESPON	The O.IDSENS and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity, either from single or multiple data sources.
2	T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.	1N ON.INSTAL, 4 O.EADMIN,	The ON.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product.

#	Threat ID	Threat Description	Objective ID	Rationale
3	T.FALACT	Inappropriate activity on the IT system the TOE monitors by an attacker may not be identified or associated with other suspicious events allowing the IT system data to be compromised.	2 O.IDANLZ 3 O.RESPON 2E OE.AUDIT_PROTECTION 3E OE.TIME	The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity, either from single or multiple data sources. OE.AUDIT_PROTECTION addresses this threat by requiring audit data be protected. OE.TIME addresses this threat by requiring accurate time stamps for the audit records
4	T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors allowing an attacker to violate the IT environment's access control policy or assume the identity of an authorized user, and thereby allowing the IT system data to be compromised.	1 O.IDSENS 2E OE.AUDIT_PROTECTION 3E OE.TIME	The O.IDSENS objective addresses this threat by requiring the TOE collect event data. OE.AUDIT_PROTECTION addresses this threat by requiring audit data be protected. OE.TIME supports this objective by requiring accurate time stamps for the audit records
5	T.BYPASS	An unauthorised user may attempt to bypass the IT Environment’s information flow control policy to gain access to data stored on and protected by IT system.	1E OE.PROTECT	OE.PROTECT objective addresses this threat by requiring system data be protected.

8.1.2 Assumptions

Table 8-2 shows that all of the secure usage assumptions are addressed by either security objectives for the IT environment or Non-IT security objectives.

Table 8-2 – All Secure Use Assumptions Addressed

No.	Assumption ID	Assumption Description	Objective ID	Rationale
1	A.INTROP	The TSF and IT environment are configured for proper interoperation.	5N ON.INTROP	The ON.INTROP objective ensures the TSF and IT environment are configured for proper interoperation.
2	A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.	4N ON.PERSON, 5N ON.INTROP	The ON.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE. The ON.INTROP objective ensures the TSF and IT environment are configured for proper interoperation.
3	A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	2N ON.PHYCAL, 3N ON.CREDEN, 1E OE.PROTECT, 2E OE.AUDIT_ PROTECTION, 4E OE.I&A, 3E OE.TIME	The ON.PHYCAL provides for the physical protection of the TOE hardware and software against unauthorized access. The ON.CREDEN objective supports this assumption by requiring protection of all authentication data. OE.PROTECT and OE.AUDIT_ PROTECTION provide that audit and system data be protected. The OE.I&A objective supports this assumption by requiring that all users must be identified and authenticated before accessing the TOE. OE.TIME supports this assumption by requiring accurate timestamps for the audit records.
4	A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	1N ON.INSTAL, 2N ON.PHYCAL, 3N ON.CREDEN 4N ON.PERSON 5N ON.INTROP,	The ON.INSTAL objective ensures that the TOE is properly installed and operated and the ON.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The ON.CREDEN objective supports this assumption by requiring protection of all authentication data. The ON.INTROP objective ensures the TOE has the proper access to the IT System. The ON.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

8.1.3 Organizational Security Policies

Table 8-3 – All Organizational Security Policies Addressed

Item	Policy	Policy Description	Objective ID	Rationale
1	P.DETECT	Events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.	1 O.IDSENS, 3E OE.TIME	The O.IDSENS objective can address this policy by requiring collection of event data. OE.TIME can address this policy because policies which require audit and system data to be generated include a timestamp.
2	P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.	2 O.IDANLZ	The O.IDANLZ objective requires analytical processes be applied to event data collected.

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-4 shows that all of the security objectives of the TOE are satisfied.

Table 8-4 – All Objectives Met by Functional Components for the TOE

Item	Objective	Objective Description	Ref	SFR and rationale
1	O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the TOE.	2	FAU_GEN_EXP.1 The TOE collects events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System.
2	O.IDANLZ	The TOE must accept event data from the IT system and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	3	FAU_SAA.1 The TOE is required to perform intrusion analysis and generate conclusions.

Item	Objective	Objective Description	Ref	SFR and rationale
3	O.RESPON	The TOE must respond appropriately to analytical conclusions.	1	FAU_ARP.1 The TOE is required to respond accordingly in the event an intrusion is detected.
4	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.	6 4,5	FMT_SMF.1, The TOE must include a set of functions that allow effective management of its functions and data. FAU_SAR.1, FAU_SAR.3 The TOE must provide the ability to review and manage the audit trail. The TOE must provide the ability for Administrators to view all audit event data collected and produced.

8.2.2 Dependencies

Table 8-5 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. (E) signifies that an environment SFR meets this dependency.

Table 8-5 – TOE Dependencies Satisfied

Item	Component	Dependencies	Reference	Rationale
1	FAU_ARP.1	FAU_SAA.1	3	
2	FAU_GEN_EXP.1	FPT_STM.1	12E	Timestamps may be included in the audit event data logged by the IT environment and collected by the TOE.
3	FAU_SAA.1	FAU_GEN.1	1E	Audit events logged by the IT environment are one source of the audit events collected and monitored by the TOE.
4	FAU_SAR.1	FAU_GEN.1	1E	Audit events logged by the IT environment are one source of the audit events collected and monitored by the TOE.
5	FAU_SAR.3	FAU_SAR.1	4	
6	FMT_SMF.1	None		

Table 8-6 – Dependencies for SFRs in the IT Environment are Satisfied

Item	Component	Dependencies	Reference
1E	FAU_GEN.1	FPT_STM.1	12E
2E	FAU_STG.1	FAU_GEN.1	1E
3E	FDP_ACC.1	FDP_ACF.1	4E
4E	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	3E, 8E
5E	FIA_UAU.2	FIA_UID.2	6E (H)

Item	Component	Dependencies	Reference
6E	FIA_UID.2	None	N/A
7E	FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	3E 9E Please see Section 8,2,3 below
8E	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	7E 9E
9E	FMT_SMR.1	FIA_UID.2	6E (H)
10E	FPT_RVM_EXP.1	None	N/A
11E	FPT_SEP_EXP.1	None	N/A
12E	FPT_STM.1	None	N/A

8.2.3 Rationale for Dependencies Not Satisfied

FMT_SMF.1 was not included in the IT environment SFR because it is not directly needed to support the TOE, and the required IT environment management functions (access controls on TOE data files) are specified in FMT_MSA.1.

8.2.4 Strength of Function Rationale

As described in Section 5.3 above, there are no probabilistic or permutational functions included in the TOE; therefore strength of function is not applicable.

8.2.5 Assurance Rationale

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data, there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

8.2.7 Explicitly Stated Requirements Rationale

FAU_GEN_EXP.1 Audit data collection is an explicitly stated requirement because of the unique TOE requirement of collecting audit data and events from the IT environment.

The explicitly stated requirements FPT_RVM_EXP.1 - Nonbypassability: IT, and FPT_SEP_EXP.1 - Domain separation: IT, were added because the TOE does not support either non-bypassability or domain separation and requires this support from the IT environment.

8.2.8 Requirements for the IT Environment

Table 8-7 shows that all of the security objectives for the IT environment are satisfied.

Table 8-7 – All Objectives for the IT Environment Met by Requirements in the IT Environment

Item	Objective	Objective Description		SFR
1E	OE.PROTECT[2]	The IT environment will protect itself and the TOE from external interference or tampering.	11E	FPT_SEP_EXP.1 Requires that the IT environment maintain a security domain for TOE execution that protects it from interference and tampering by untrusted subjects.
			10E	FPT_RVM_EXP.1 Requires that the IT environment ensures that IT environment security policy enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
2E	OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.	1E	FAU_GEN.1 requires that the IT environment audit attempts to access TSF data other than thru the Toe's interfaces.
			2E	FAU_STG.1 requires that the audit data be protected from unauthorized deletion and modification.
			3E	FDP_ACC.1 requires that the IT environment enforces the IT environment access control policy.
			4E	FDP_ACF.1 requires that the IT environment enforces the attribute based IT environment access control policy.
			7E	FMT_MSA.1 requires that the IT environment restrict the ability to modify or delete the security attributes to the TOE administrator.
			8E	FMT_MSA.3 requires that the IT environment enforce the default values for security attributes used to enforce the IT environment SFP.
3E	OE.TIME	The IT Environment will provide reliable timestamps to the TOE.	12E	FPT_STM.1 Requires that the IT environment provides reliable time stamps for use by the TOE.

[2] The end user can protect communication between the TOE components and/or the components of the IT environment as they choose, i.e., through network configuration, physical protection of a dedicated LAN, or thru cytological means.

Item	Objective	Objective Description		SFR
4E	OE.I&A	The IT Environment shall provide functionality to require identification and authentication for all TOE users.	5E,	FIA_UAU.2 requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
			6E,	FIA_UID.2 requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
			9E	FMT_SMR.1 requires that the IT environment be capable of maintaining roles of TOE administrator; OS administrator.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-8 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-8 – Mapping of Functional Requirements to TOE Summary Specification

Item	Component	Component Name	TSF	Rationale
1	FAU_ARP.1	Security alarms	Security Audit - Rules	Specifies that *e*Trust Audit will take action to execute a program, send an email notification, send an event to another Client, send the event to the Security Monitor, or send the event to the central audit data repository upon detection of a potential security violation.
2	FAU_GEN_EXP.1	Audit data collection	Security Audit - Collection	Specifies *e*Trust Audit provides the ability to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System.
3	FAU_SAA.1	Potential violation analysis	Security Audit - Rules	Specifies that *e*Trust Audit is able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. *e*Trust Audit will enforce the following rules for monitoring audited events: Accumulation or combination of audit events based on specified criteria (a filter) that *e*Trust Audit uses to determine which events are subject to the action described in the rule known to indicate a potential security violation.

Item	Component	Component Name	TSF	Rationale
4	FAU_SAR.1	Audit review	Security Audit - Reporting	Specifies *e*Trust Audit to provide a set of data tools including the Viewer, the Reporter and the Security Monitor. The Viewer allows the user to view, filter, and print all collected audit records.
5	FAU_SAR.3	Selectable audit review	Security Audit - Reporting	Specifies *e*Trust Audit provides the ability to perform searches, sorting, and ordering of the audit data, based on various criteria.
6	FMT_SMF.1	Specification of management functions	Management	Specifies *e*Trust Audit provides a set of functions that allow effective management of its functions and data.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-9.

Table 8-9 – Assurance Measures Rationale

Item	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	Audit 1.5 SP3 file list Audit r8 file list - rev3	• CM Proof - Shows the CM system being used. • Configuration Item List(s) - is comprised of a list of the source code files and version numbers - is comprised of a list of design documents with version numbers - is comprised of test documents with version numbers - user and administrator documentation with version numbers
2	ADO_DEL.1	Delivery Procedures	Distribution Centers Procedures Manual United States And Canada SITE Visit Report for Computer Associates Product Submission Form Product Submission Form Process Flow Preservation of Product Procedure	Provides a description of all procedures that are necessary to maintain security when distributing *e*Trust Audit software to the user's site. Applicable across all phases of delivery from packaging, storage, and distribution.

Item	Component	Evidence Requirements	How Satisfied	Rationale
3	ADO_IGS.1	Installation, generation, and start-up procedures	Installation of the eTrust Audit TOE eTrust Audit Getting Started r8 eTrust Audit Release Summary r8	Vendor Guides - Provides detailed instructions on how to install and configure *e*Trust Audit. Installation Report – Describes on-site installation of the evaluated configuration.
4	ADV_FSP.1	Functional Specification	eTrust Audit r8 EAL2 Common Criteria Evaluation Proprietary Development Specification	Describes the TSF interfaces and TOE functionality.
5	ADV_HLD.1	High-Level Design	eTrust Audit r8 EAL2 Common Criteria Evaluation Proprietary Development Specification	Describes the TOE subsystems and their associated security functionality.
6	ADV_RCR.1	Representation Correspondence	eTrust Audit r8 EAL2 Common Criteria Evaluation Proprietary Development Specification	Provides the following two dimensional mappings: ▪ HLD to FSP ▪ External interfaces to the SFRs
7	AGD_ADM.1	Administrator Guidance	*e*Trust Audit, Getting Started Guide r8 *e*Trust Audit, Reference Guide r8 eTrust Audit, Audit Management Guide r8 Computer Associates eTrust™ Audit™ r8 Common Criteria Supplement to the Guidance Documentation	Vendor Guides - Describes how to administer the TOE. CC Supplement – Describes how to administer the TOE securely in the evaluated configuration.
8	AGD_USR.1	User Guidance	Not applicable	No non-administrative users of the TOE. This requirement is effectively the same as AGD_ADM and therefore does not require additional evidence.
9	ATE_COV.1	Test Coverage Analysis	Test Coverage for eTrust Audit	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Item	Component	Evidence Requirements	How Satisfied	Rationale
10	ATE_FUN.1	Test Documentation	Evaluation Team Report for On-Site Functional Testing Common Criteria Certification Test Environment Specification QA Test Plans for eTrust Audit	Test documentation includes test plans and procedures and expected and actual results.
11	ATE_IND.2	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
12	AVA_SOF.1	SOF Analysis	Not applicable	No probabilistic or permutational functions are included in the TOE; therefore SOF Analysis is not required.
13	AVA_VLA.2	Vulnerability Analysis	Computer Associates eTrust Audit r8 Vulnerability Analysis Vulnerability Analysis Summary Spreadsheet	Provides an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 ACRONYMS

Acronym	Description
AN	Audit Node
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
OS	Operating System
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy