National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Computer Associates
*e*Trust® Audit r8

Report Number:	**CCEVS-VR-05-0140**
Dated:	February 3, 2006
Version	1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

James E Brosey
Olin Sibert
Orion Security Solutions, Inc.
McLean, VA

Catalina Gomolka
Mitretek Systems, Inc.
Falls Church, VA

Common Criteria Testing Laboratory

Shari Galitzer
Nancy Gow
Peter Kukura
Kris Rogers
CygnaCom Solutions (an Entrust Company)
McLean, VA

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of the Computer Associates International, Inc. product *e*Trust® Audit r8 was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 16 December 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.2, Part 2 and Part 3, Evaluation Assurance Level (EAL 2), and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

CygnaCom Solutions is certified by the NIAP validation body for laboratory accreditation. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. The CygnaCom Security Evaluation Laboratory team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met. This Validation Report is not an endorsement of the Computer Associates International, Inc product by any agency of the U.S. Government and no warranty of the product is either expressed or implied. The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by CygnaCom Solutions.

The Target of Evaluation (TOE) is a subset of the Computer Associates product *e*Trust Audit r8. The TOE consists of the following software components:

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

For this evaluation, the Collector component of *e*Trust Audit r8, the operating system and the hardware platform are running are in the IT environment. Therefore, the collector, the operating system and the hardware platform have not been evaluated or tested. The TOE relies on the IT environment to provide:

- Audit data generation
- Protected audit trail storage
- Subset access control
- Security attribute based access control
- User authentication before any action
- User identification before any action
- Management of security attributes
- Static attribute initialization
- Security roles
- Non-bypassability of IT environment security functions
- Domain separation of IT environment security functions
- Reliable time stamps

1.1 EVALUATION DETAILS

Evaluated Product: *e*Trust Audit r8

Developer: Computer Associates International, Inc., One Computer Associates Plaza, Islandia, NY 11749

CCTL: CygnaCom Solutions, 7925 Jones Branch Dr., Suite 5200 West, McLean, VA 22102-3321.

Validation Team: James E Brosey, Orion Security Solutions, Inc., 1489 Chain Bridge Road, Suite 300, McLean, VA 22101.

EAL: EAL2

Completion Date: 20 December 2005.

1.2 INTERPRETATIONS

The evaluation team performed an analysis of the international and national (NIAP) interpretations regarding the CC and the CEM and determined that the following CCIMB interpretations were applicable to this evaluation:

- Final Interpretation for RI # 137 - Rules governing binding should be specifiable.

NIAP Interpretations are optional and are not considered for this product in order to ensure acceptance internationally.

The validation team concluded that the evaluation team correctly addressed the interpretations that it identified.

1.3 THREATS TO SECURITY

The Security Target identified the following threats that the evaluated product addresses:

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.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

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.

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.

T.BYPASS An unauthorized 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.

1.4 SECURITY POLICIES

The Security Target identified the following organizational security policies that the evaluated product addresses:

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.

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 IDENTIFICATION

2.1 SECURITY TARGET AND TOE IDENTIFICATION

Security Target – *eTrust Audit r8 Security Target V2.6*, dated December 20, 2005.

TOE Identification – *e*Trust Audit r8

The Evaluated Configuration of the TOE is software only and includes the following Software Components of *e*Trust Audit r8 running on Windows 2000 Server SP4:

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

The Post Collection Utility (PCU) is a element of the Audit Data Tools component, but it is not evaluated as part of the TOE.

CC Identification – *Common Criteria for Information Technology Security Evaluatio*n, Version 2.2, January 2004, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Securit*y, Version 2.2, Revision 256, January 2004.

Assurance Level - This ST is Common Criteria Version 2.2, Part 2 extended and Part 3 conformant, at Evaluation Assurance Level 2

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

2.2 IT SECURITY ENVIRONMENT

The *e*Trust Audit ST levies requirements on the TOE as well as the IT Environment. In the case of this TOE, the IT Environment includes the Operating System, the underlying hardware platforms, and parts of *e*Trust Audit itself, including the collector component and the PCU portion of Audit Data Tools.

The TOE relies on the environment to provide:

- Audit data generation
- Protected audit trail storage
- Subset access control
- Security attribute based access control
- User authentication before any action
- User identification before any action
- Management of security attributes
- Static attribute initialization
- Security roles
- Non-bypassability of IT environment security functions
- Domain separation of IT environment security functions
- Reliable time stamps

2.3 OPERATING SYSTEM

The TOE was evaluated with Windows 2000 Server SP4 in the IT environment.

2.4 HARDWARE PLATFORM

The Computer Associates *e*Trust Audit product was evaluated using the hardware platform as described in section 8 of this document.

3 SECURITY POLICY

The *e*Trust Audit TOE provides these security services:

- Security Audit Collection
- Security Audit Rules
- Security Audit Reporting

- Management

Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

3.1 SECURITY AUDIT COLLECTION POLICY

*e*Trust Audit is a distributed TOE with separate management, collection, and analysis components. The audit event gathering component of the TOE, the *e*Trust Audit Client, must be installed onto all targeted IT systems that the TOE monitors. *e*Trust Audit r8 supports an open design and can accept 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.

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 analyzed in the same way that audit events are collected from OS logs.

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.

3.2 SECURITY AUDIT RULES POLICY

*e*Trust Audit allows a user to create, activate, and distribute policies to clients that generate audit records. As events occur on clients, the *e*Trust iRecorder on the *e*Trust Audit client collects audit records 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 when a security relevant 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.

3.3 SECURITY AUDIT REPORTING POLICY

*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 5;
- Alerting the administrator thru the Security Monitor; and
- 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, and filter by file. Audit events can also be reported through a RPC call to a service or executable.

3.4 MANAGEMENT POLICY

The Administrator may use the administrative interfaces, consisting of a windows or web-based GUIs, to generate and maintain the configuration files. The behavior of the system data collection, analysis, and reaction functions is controlled by 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 Audit Nodes (AN)s 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.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 USAGE ASSUMPTIONS

A.INTROP	The TSF and IT environment are configured for proper interoperation.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification and access.
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.

4.2 ENVIRONMENTAL OBJECTIVES FOR THE IT ENVIRONMENT

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.
OE.AUDIT_ PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.I&A	The IT Environment shall provide functionality to require identification and authentication for all TOE users.

4.3 ENVIRONMENTAL OBJECTIVES FOR THE NON-IT ENVIRONMENT

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.
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.
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.
ON.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
ON.INTROP	The TOE is interoperable with the IT System it monitors.

4.4 CLARIFICATION OF SCOPE

The product, *e*Trust Audit r8, that a customer would purchase includes more than the evaluated TOE. The evaluated TOE does not include the Collector, which writes events into the central audit data repository. *e*Trust Audit r8 can also be bundled with other *e*Trust applications that are not part of this evaluation. The additional Computer Associates (CA) applications that may be bundled with this product are treated in this evaluation as part of the IT Environment.

Some requirements were placed upon the configuration of the IT Environment to support the analysis and conclusions reached by this evaluation. To use this product in the evaluated configuration, the IT environment requirements need to be addressed by the TOE administrator. Since the *e*Trust Audit r8 TOE supports configurations that are outside the scope of this evaluation, the TOE administrator must remember that only the functions addressed by the Security Target were evaluated.

5 ARCHITECTURAL INFORMATION

The TOE, *e*Trust Audit r8, 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 TOE is a subset of *e*Trust Audit r8, a distributed network based product. The product has four main components: *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. The collector is not a part of the TOE in its evaluated configuration.

5.1 GENERAL TOE FUNCTIONALITY

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

- Security Audit Collection
- Security Audit Rules
- Security Audit Reporting
- 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.

A functional diagram of the *e*Trust Audit r8 TOE and the environment in which it exists is provided in Figure 1. A physical diagram of the TOE is show in its evaluated configuration in Figure 4. Components of the TOE are designated by blue blocks.

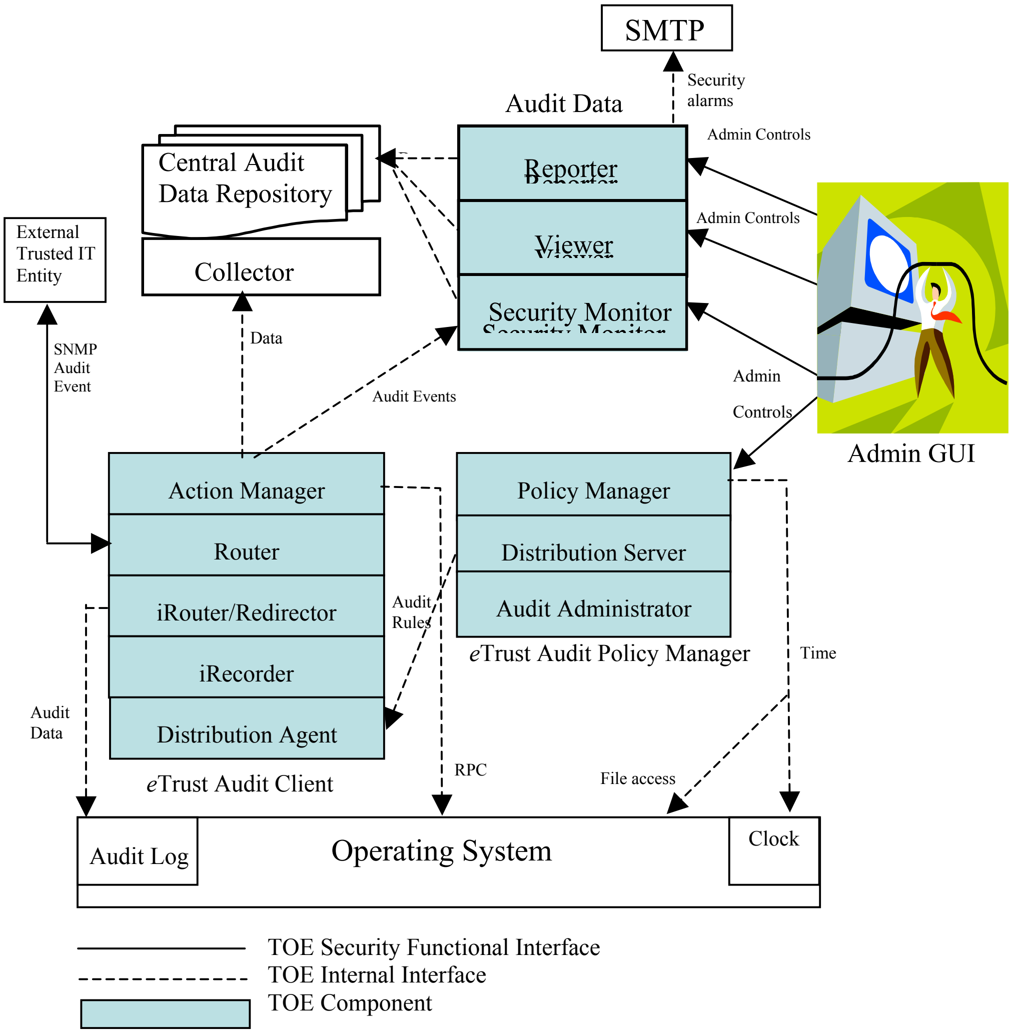

Figure 1: TOE Boundary

5.2 *TOE COMPONENTS*

*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, Audit Data Tools, and the Collector (which writes events into the central audit data repository). *e*Trust Audit Client, *e*Trust Audit Policy Manager, and Audit Data Tools are parts of the evaluated TOE. The Collector is not part of the TOE but is in the evaluated configuration in the IT environment. 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.

The Audit Data Tools component supports reporting from 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.

5.3 TOE INTERFACES

In general terms, *e*Trust Audit r8 presents two classes of external security audit user interfaces to the administrator, one through the *e*Trust Policy Manager to define the centralized audit policy, and another through the Audit Data Tools component to analyze the central audit data repository. In addition the TOE can accept standardized SNMP trap information through the *e*Trust Audit Client.

In addition to these external interfaces, the *e*Trust Audit Policy Manager distributes the audit policy to the installations of the *e*Trust Audit Client, and the *e*Trust Audit Client can pass alarms through the Action Manager subcomponent to the Security Monitor subcomponent of the Audit Data Tools component. Both of these are considered to be internal interfaces protected by measures taken in the IT environment. Also the Audit Data Tools component is capable of generating and sending alarms to administrators.

*e*Trust Audit r8 supports an interface through which it receives audit events through the *e*Trust Audit Client through which the TOE extracts events from the OS log.

In addition the interfaces already identified, the *e*Trust Audit Client has an internal interface through the Action Manager subcomponent to the Collector, and the Audit Data Tools component has an internal interface to the central audit data repository. These interfaces are controlled by the TOE, and may not be used to invoke the TOE by an external user.

The TOE may invoke an external IT entity through an RPC call. This interface is considered to be an internal interface since it can only be invoked by the TOE, and is only visible to a non-human external IT entity.

For all TOE components the interface to the OS is considered to be an internal interface since it cannot be invoked by an external user.

Figure 1 shows the external and internal interfaces of the TOE. The interfaces internal and external interfaces are described in Tables 3 and 4 below.

Table 1 – External TOE Interfaces

No.	External Interface	Interface Type	Characteristic	Security Function
1	Administrative Web and Windows GUIs supported by the *e*Trust Audit Policy Manager used by the administrator to define the central audit policy.	GUI	Administrator Controls	Security Audit - Rules
2	Administrative interface Reporter GUI supported by the Audit Data Tools used by the administrator to review the collected audit data.	GUI	Administrator Controls	Security Audit - Reporting
3	Administrative interface Viewer GUI supported by the Audit Data Tools used by the administrator to review the collected audit data.	GUI	Administrator Controls	Security Audit - Reporting
4	Administrative interface Security Monitor GUI supported by the Audit Data Tools used by the administrator to view alarms.	GUI	Administrator Controls	Security Audit - Reporting
5	SNMP audit event information passed to the TOE SNMP client from an *e*Trust Audit Client or external IT entity.	Network	Controlled by External IT entity	Security Audit - Collection

Table 2 – Internal TOE Interfaces

No.	Internal Interface	Characteristic	Security Function
6	SNMP audit event information passed from the TOE SNMP client (Router) to an *e*Trust Audit Client.	Between TOE components, controlled by TOE	Security Audit – Rules
7	Interface of the *e*Trust Audit Client (via the Distribution Agent) to the *e*Trust Audit Policy Manager (via the Distribution Server) of the central audit policy.	Between TOE components	Security Audit– Rules; Management
8	Interface of the *e*Trust Audit Client (via the Action Manager subcomponent) to the Audit Tools Component (via the Security Monitor subcomponent) through which audit events are passed to support generation of security alarms.	Between TOE components	Security Audit – Rules
9	*e*Trust Audit Client to the Collector	TOE controls	Security Audit– Rules
10	Audit Data Tools to Central Audit Data Repository	TOE controls	Security Audit - Reporting

No.	Internal Interface	Characteristic	Security Function
11	*e*Trust Audit Client to OS audit log	TOE controls	Security Audit - Collection
12	OS platform (time, file access, etc.)	TOE controls	IT Environment Support
13	TOE calls a Remote Procedure	TOE controls	Security Audit-Rules
14	Security alarms generated by the Audit Data Tools and passed to the administrator (i.e.: email via SMTP).	TOE controls	Security Audit-Rules

6 DOCUMENTATION

Purchasers of a product containing the *e*Trust Audit r8 receive the following TOE documentation:

- Computer Associates *eTrust Audit Release Summary r8*;
- Computer Associates *eTrust Audit Getting Started Guide r8*;
- Computer Associates *eTrust Audit, Reference Guide r8*;
- Computer Associates *eTrust Audit, Audit Management Guide r8* ; and
- Computer Associates *eTrust Audit r8 Common Criteria Supplement to the Guidance Documentation*.

The applicable guidance in these documents must be followed in order to operate *e*Trust Audit in its evaluated configuration.

7 IT PRODUCT TESTING

This section describes the testing efforts of the Vendor and the evaluation team.

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the evaluation team.

All of the testing was conducted in a test lab at the developer's site at:

Computer Associates
2291 Wood Oak Drive
Herndon, VA 20171-2823

The testing was performed in four parts over three business days. Installation Testing was performed the first day. Developer testing was performed the on all three days. Independent and penetration testing was performed on the third day of testing.

The test plan and results, as well as the evaluation team's review of the testing in the Evaluation Technical Report, were well written and complete.

7.1 INSTALLATION TESTING

The installation was performed by Computer Associates personnel while being observed and recorded by the evaluation team. The Target of Evaluation was installed following the procedures defined in the following documents:

- *e*Trust *Audit Getting Started Guide r8*

The installation was done in three stages, one for each of the installed TOE component machines.

The Minimum host system requirements for installing *e*Trust Audit are:

Component	Minimum Host System Requirements
*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
*e*Trust Audit Data Tools	Windows 2000 Server SP4 Pentium 1 GHz Processor 256 MB Memory 1000 MB Disk Space Microsoft SQL Server 200 SP3
*e*Trust Audit Client	Windows 2000 Server SP4 Pentium 1 GHz Processor 256 MB Memory 100 MB Disk Space

Figure 2: TOE Installation Requirements

The test installation resulted in a successful installation of *e*Trust Audit in the evaluated configuration. All of the *e*Trust Audit TOE components were installed correctly for the evaluated configuration by following the procedures documented in the *e*Trust Audit Getting Started Guide r8. Any discrepancies between the user guidance and what was displayed by the installation program were minor, and did not affect the ease of installation. The developer was made aware of the documentation discrepancies. After installation, the evaluated configuration of the TOE was tested without having to change any of the configuration parameters or rerun any of the installation steps.

7.2 DEVELOPER TESTING

Because of the small number of security functional requirements claimed for the TOE and the small number of developer tests used to test those security functions, the evaluation team chose to perform the complete set of developer tests. The evaluation team mapped the test cases to the TOE Security Functions (TSFs) and to the TSFIs and determined that at least one test is provided for every function and for every interface.

The set of developer tests consists of 5 test procedures. The evaluation team performed all the test cases provided by the developer. All of the test cases included a test description, security functions tested, rationale, purpose for the test, explicit test steps, and an expected result. The testing was either performed by Computer Associates personnel while being observed and recorded by the evaluation team performed by the evaluation team with assistance from the Computer Associates personnel.

For all of the tests performed, the technical contact and evaluation team took screenshots, which were saved in separate files on the computers used for testing. The evaluation team also took notes during the testing, which are stored in both hard copy and electronic form at CygnaCom SEL as testing evidence for this evaluation.

No hardware test tools were used during the developer functional testing. The only software test tool used during the testing was the script “test.bat” which echoes “Intruder Alert”. This script was needed for Developer Test 1: Action Manager.

The testing did not result in any changes to the *e*Trust Audit Security Target, software or installed configuration. All developer tests were successful. Minor changes that were needed to the test steps and pre-requisites were documented and the individual test case files were updated with these changes. Only three minor features of the security functionality of *e*Trust Audit were not fully demonstrated by the developer testing observed during the on-site visit:

- Sending an e-mail notification after the occurrence of a security significant event.
- Indicating a potential security violation after combination of events.
- More extensive demonstration of the filtering and sorting of audit records.

The evaluation team developed independent tests to exercise these features.

In Section 4 of *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, Computer Associates e*Trust*™Audit™r8, ETR Version 1.6, Security Target Version 2.6, dated December 21, 2005*, the evaluation team reported that they had examined the test results and determined that the developer testing was a success. The developer’s tests run by the evaluation team completed successfully and all test results were archived in the *e*Trust *Audit Function Test Report.* The evaluation team reported that the actual test results from the developer's tests matched the developer's expected results. A list of final test cases and their actual results are shown below:

Security Function	**SFR**	**Test Case Title**	**Success/Failure**
Security Audit - Rules	FAU_ARP.1	Action Manager	**Success**
Security Audit - Rules	FAU_SAA.1	Security Monitor	**Success**
Security Audit - Rules	FAU_SAA.1	Router: Third Failed Login Event	**Success**
Security Audit - Reporting	FAU_SAR.1	Viewer & Reporter – DB access	**Success**
Security Audit - Reporting	FAU_SAR.3	Viewer	**Success**
Security Audit – Collection	FAU_GEN_EXP.1	Implicitly tested by all test cases	
Management	FMT_SMF.1	Implicitly tested by all test cases	

Figure 3: TOE Developer Test Results

All five tests cases implicitly exercised the Management and Security Audit – Collection functions.

7.3 EVALUATION TEAM INDEPENDENT TESTING

The evaluation team devised a test subset for independent testing. The test subset consisted of functions not tested by the developer. All of the test cases included a purpose, explicit test steps, and an expected result. The evaluation team produced test documentation for the test subset that was sufficiently detailed to enable the tests to be reproducible. This time the testing was performed by the evaluation team, with the Computer Associates personnel and the validator observing. The validator only observed the independent and penetration testing.

The test cases defined by the evaluation team were executed after the TOE was installed in the evaluated configuration consistent with the Security Target. The evaluation team selected independent tests to supplement and enhance the functional testing performed on Developer's Functional test suite. The team-defined functional tests were developed to cover any areas of functionality that were overlooked by the developer tests.

Each test was intended to explicitly exercise the Security Audit – Rules or Security Audit - Reporting functionality of the TOE. However, all of the tests also implicitly exercised the Security Audit – Collection and Management functions.

The environment and configuration for the Team-Defined testing was the same as that for the Developer Functional testing. No hardware test tools were used during the testing. No general test setup procedures were performed prior to the Team-Defined testing. Setup steps and pre-requisites specific to individual tests are described in the individual test case documents.

The following table identifies the security function test cases that were independently tested:

Security Function	SFR	Test Case Title	Success/Failure
Security Audit - Rules	FAU_ARP.1.1	E-Mail Security Alarms	**Success**
Security Audit - Rules	FAU_SAA.1.2	Combination of Audit Events	**Success**
Security Audit - Reporting	FAU_SAR.3.1	Combination of Filters for Audit Review	**Success**
Security Audit – Collection	FAU_GEN_EXP.1	Implicitly tested by all test cases	
Management	FMT_SMF.1	Implicitly tested by all test cases	

The validation team observed the evaluation team's independent testing effort and concluded that the testing was successful.

7.4 EVALUATION TEAM PENETRATION TESTING

For its penetration tests, the evaluation team evaluated the developer's vulnerability analysis document, the independent test plan, the guidance documentation and the TOE design to identify potential penetration test cases. Penetration tests were selected based on the evaluation team's experience with evaluating the developer's design, guidance, test, and vulnerability assessment documentation.

The evaluation team created a penetration test plan. All of the test cases included a purpose, explicit test steps, and an expected result. There were no automatic test scripts or test tools.

The testing was performed by the evaluation team, with the Computer Associates personnel and the validator observing. The validator only observed the independent and penetration testing.

The penetration tests evaluated the following scenarios:

- Whether an ill-formed rule could cause a security breach
- Attempt to cause a Denial of Service by generating vast quantities of audit information on a client machine and observe the behavior of the viewer and security monitor

- Data collection interruption through the following techniques:
    - Shut down the DataTools Server. Check that no audit data from the client was lost while the server was down. Check that alerts will be issued for events that occurred during the time the server was down.
    - Disconnect the network cable between the DataTools Server and the Client. Check that no audit data from the client was lost while the while the Network connection was disabled. Check that alerts will be issued for events that occurred during the time the Network connection was disabled
- Invalid data input through the Policy Manager and Viewer GUI.

The results of penetration testing verified that there were no exploitable vulnerabilities in the intended environment of the TOE. The results of the penetration testing are as follows:

Although it was impossible to test all possible ways of constructing an ill-formed rule, this test successfully demonstrated that the security of the TOE will not be compromised by a rule that causes a compilation error. When a rule causes a compilation error, the Policy Manager does not permit it to be activated. No adverse behavior to any component of the TOE was noticed because of the ill-formed rule. However, it is still possible for the Administrator to create or modify a rule that compiles and is distributed to Client machines but does not produce the intended results (e.g. a field is misspelled). The Administrator must be fully trained in the filter language syntax and must ensure that any new or modified policy produces the expected result after being activated.

Even when data is generated in an unending loop, the TOE did not exhibit any adverse behavior. While unending streaming data was being generated; the Policy Manager, Security Monitor and Viewer were still useable. This test was considered a success.

No audit data was lost while either the DataTools server was down or the network between the DataTools server and Client was disconnected. After the DataTools server was restarted and the network cable was reconnected, the audit events generated during the interrupted connection were visible with both the Security Monitor and the Viewer. The alert action script also executed on the client machine after the connection between the DataTools and Client was reestablished.

The validation team observed the evaluation team's penetration testing and concluded that the testing was successful.

8 EVALUATED CONFIGURATION

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.

The evaluation team verified that the test configuration was consistent with the evaluated configuration in the Security Target. The evaluation team also verified the Installation Procedures and Delivery procedures during installation of the TOE for testing. The testing activity confirmed that the installation, generation, and start-up procedures result in a secure configuration.

The TOE was tested using the following configuration:

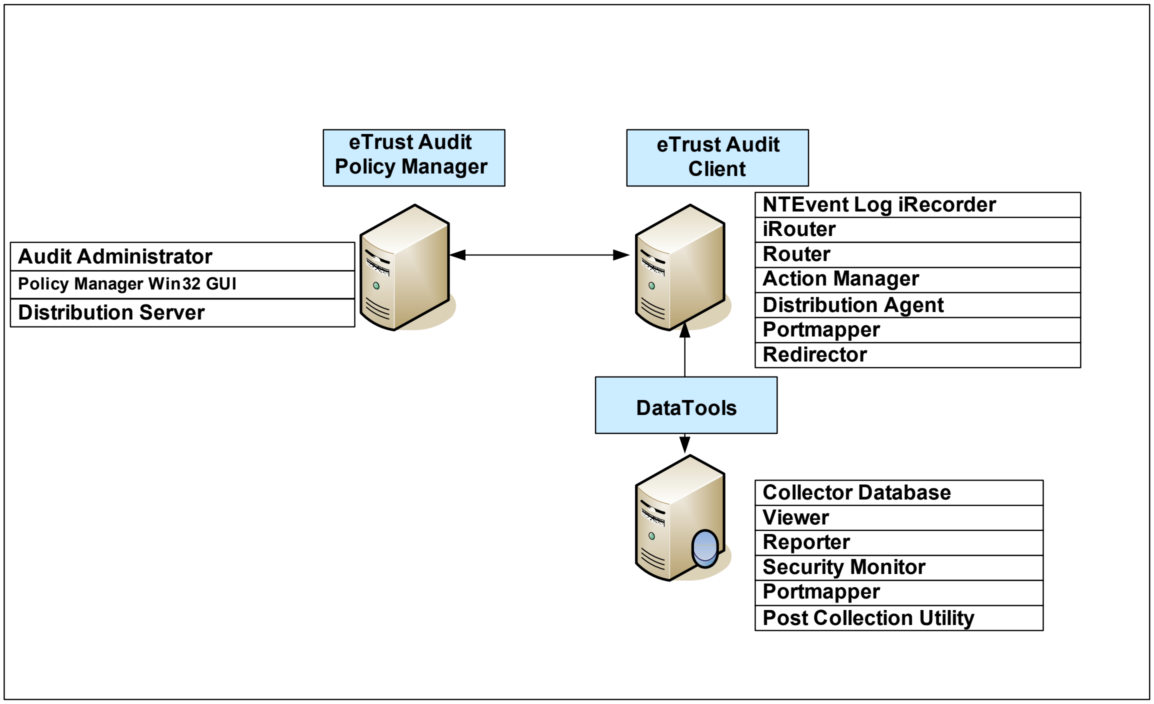

Figure 4 - Evaluated Configuration

The evaluation team chose the following evaluated configuration because it included all the components of the TOE in one of its simplest forms. The evaluation team did not test the limits of the number of *e*Trust Audit clients that might be installed, due to the limits in the lab environment. This configuration has did not demonstrate that the client software is extensible.

The *e*Trust Audit TOE was installed and tested as follows:

TOE Component (<u>computer</u>)	*e*Trust **Audit Policy Manager <u>(cclab-svr1)</u>**	*e*Trust **Audit Data Tools <u>(cclab-svr2)</u>**	*e*Trust **Audit Client <u>(cclab-pc3)</u>**
Operating System	Microsoft Windows 2000, Service Pack 4	Microsoft Windows 2000, Service Pack 4	Microsoft Windows 2000, Service Pack 4
Other Software	Microsoft Internet Explorer 6.0 SP1	Microsoft SQL Server 2000, Service Pack 3	*none*
Hardware	Pentium 1 GHz CPU 128 MB memory 300 MB disk space	Pentium 1 GHz CPU 256 MB memory 1000 MB disk space	Pentium 1 GHz CPU 256 MB memory 100 MB disk space

8.1 TEST SOFTWARE AND HARDWARE

No hardware test tools were used for the independent and penetration testing.

Two small test scripts were used in performing the developer, independent, and penetration tests.

9 RESULTS OF THE EVALUATION

The evaluation team conducted the evaluation in accordance with the CC and the CEM

The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence. In the Final ETR, all Fail or Inconclusive work unit verdicts have been resolved by the developer and the evaluation team.

In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the following documents:

- *Evaluation Technical Report for a Target of Evaluation, Volume 1: Evaluation of the ST, Computer Associates eTrust Audit r8, ETR Version 1.6, Security Target Version 2.6, dated December 21, 2005* and

- *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, Computer Associates eTrust Audit r8, ETR Version 1.6, Security Target Version 2.6, dated December 21, 2005*,

contain the verdicts of "PASS" for all the work units.

The evaluation team determined the TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements. The rationale supporting each CEM work unit verdict is recorded in the ETR.

Therefore, when configured according to the guidance documentation enumerated in section 6 of this report, the TOE *e*Trust Audit r8 is CC compliant and satisfies the *eTrust Audit r8 Security Target Version 2.6*, dated December 20, 2005.

10 VALIDATION COMMENTS/RECOMMENDATIONS

10.1 VALDATION COMMENTS

The product, *e*Trust Audit r8, passed all of the work units and all of the tests performed by the evaluation team. The validation team witnessed the independent and penetration testing, reviewed the recommendations of the evaluation team, and was satisfied that the product performed the requirements necessary for EAL2.

The items included in this section are to make the user aware of the limits of the evaluation.

The TOE was evaluated using a minimum configuration. Although multiple instances of the Audit Client are likely, The TOE was tested using only one. This was acceptable for the evaluation since the security functionality is the same for one Audit Client as for many Audit Clients. The end user should be aware that there is no guarantee of how many Audit Clients can be used or whether multiple Audit Clients reduce the performance of the TOE.

The TOE is distributed, but there is no functional requirement to protect TOE data between machines. Since there are no requirements to protect the TOE data between distributed components of the TOE, the evaluation team did not check whether the network traffic between TOE machines could be intercepted, modified, manipulated, or otherwise interfered with. The customer can have no confidence, based on this evaluation, that the *e*Trust Audit product is capable of protecting itself from any type of threat that could have access to the communication paths between components. To ensure that data transmission between TOE components is secure, the system should be installed with adequate encryption strength (e.g., 128 bit AES option should be considered).

The TOE relegates user identification and authentication, audit data generation, security role management, and other functionality to the Operating System in the IT environment. The TOE depends on the functionality of the IT environment for much of its traditional security functionality.

One possible problem for the TOE was encountered during the data collection interrupt penetration test. Occasionally the operating system does not start the SQL Server before trying to start the Collector Service when the DataTools machine comes back up. If this occurs, the Collector Service will not start automatically and must be restarted manually by the Administrator. This is a Windows timing issue and happened only once during testing. *e*Trust Audit will send an audit event to the Security Monitor when this happens. The *Computer Associates e*Trust*™Audit*™ *r8 Common Criteria Supplement to the Guidance Documentation V0.1, dated October 28, 2005* instructs the administrator on this possible problem and its remedy.

If an *e*Trust Audit filtering rule is modified with the text editor option, it is possible for an administrator to make a syntax error. The error will be noted when the policy is activated (not before). The compiler errors will be specified and an error message will also appear noting that the policy was not activated. If this happens, existing policies will not be replaced, but will remain in effect. It is also possible for the administrator to make a typographical error that changes the meaning of the rule, but does not contain incorrect syntax. The end user will need to remember to test all hand-edited policies to ensure that they act as intended after they are activated in production.

The centralized servers (that host *e*Trust Audit components such as the Policy Manager or the Data Tools components) are susceptible to being targeted for DoS type attacks. Therefore, the end user should be aware that the server is only as secure as it has configured to be. The primary line of defense is to operate this TOE and related IT Environment in a secured network environment (as dictated by the TOE's assumptions), such as a VPN solution or to configure the TOE to use strong encryption. This helps in the prevention of IP spoofing and network scanning for TSF data. The next line of defense would be to install and operate the OS and the relational database (MS SQL Server 2000 in this case) in a secure manner. This includes remembering to check vulnerability (www.cve.mitre.org) and vendor websites (www.microsoft.com) for updates and security notices.

*e*Trust Audit was not difficult to install and configure, it was easy to operate and easy to administer. All of the interfaces were GUI interfaces, however it is possible for the administrator to write a script for use with the TOE.

The evaluation team worked well with the validation team. The evaluation team provided all the necessary information to perform a complete and effective review of the product to the validation team.

10.2 VALIDATION RECOMMENDATIONS

The validation team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The validation team agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 4 of the ETR, volume 1, and the Conclusions presented in Section 5 of the ETR, volume 1. The validation team, therefore, concludes that the evaluation and Pass result for this TOE are complete and correct for *e*Trust Audit r8.

11 LIST OF 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

12 BIBLIOGRAPHY

The validation team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 1.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 2.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 3.
- *Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3*, Version 1.0, February 2002.
- *Common Evaluation Methodology for Information Technology Security, version 2.2, Revision 256,* January 2004.
- *e*Trust® *Audit® r8 Security Target Version 2.6*, dated December 20, 2005.
- *Evaluation Technical Report for a Target of Evaluation, Volume 1: Evaluation of the ST, Computer Associates e*Trust® *Audit® r8, ETR Version 1.6, Security Target Version 2.6, dated December 21, 2005.*
- *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, Computer Associates e*Trust® *Audit® r8, ETR Version 1.6, Security Target Version 2.6, dated December 21, 2005.*