National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Computer Associates
*e*Trust® Admin Version 8.0

Report Number: **CCEVS-VR-06-0008**
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 Brosey
Olin Sibert
Orion Security Solutions, Inc.
McLean, VA

Catalina Gomolka
Mitretek Systems, Inc.
Falls Church, VA

Common Criteria Testing Laboratory

Peter Kukura
Nancy Gow
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® Admin Version 8.0 was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 2 February 2006. 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 Admin Version 8.0. The TOE consists of the following software components:

- *e*Trust Admin Server software
- *e*Trust Admin Web-Server Web-based Interface
- Administrator Interface

For this evaluation, the eTrust Directory component of the product, the operating system, Internet Explorer, the systems the TOE manages, the hardware platform and network are running are in the IT environment. Therefore, the *e*Trust Directory component, the operating system, Internet Explorer, the systems the TOE manages, the hardware platform and network have not been evaluated or tested. eTrust Directory is currently the target of a separate evaluation at CygnaCom Solutions.

The TOE relies on the IT environment to provide:

- Protected audit trail storage
- Specification of Management Functions
- Non-bypassability of IT environment security functions
- Domain separation of IT environment security functions
- Reliable time stamps
- Inter-TSF trusted channel

1.1 EVALUATION DETAILS

Evaluated Product: *e*Trust®Admin Version 8.0 with CAM V1.11 patch
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, Olin Sibert, and Catalina Gomolka
EAL: EAL2
Completion Date: 2 February 2006.

1.2 INTERPRETATIONS

The Evaluation Team performed an analysis of the international and national interpretations regarding the CC and the CEM and determined NIAP Interpretations are optional and are not considered for this product in order to ensure acceptance internationally.

The Evaluation Team determined that the following CCIMB interpretations were applicable to this evaluation:

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

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.ABUSE An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is not authorized to perform.

T.ACCESS An authorized user of the TOE may obtain unauthorized access to information or resources without having permission from the person who owns, or is responsible for, the information or resource.

T.MISMANAGE Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.UNDETECT Attempts by an attacker to gain access to the TOE may go undetected. If the attacker is successful, TSF data may be lost or altered.

T.MISUSE Unauthorized accesses and activity may occur on an IT System the TOE manages because user access and privileges are not applied consistently across all systems.

2 IDENTIFICATION

2.1 SECURITY TARGET AND TOE IDENTIFICATION

Security Target – *eTrust Admin V8.0 Security Target V2.3*, dated February 2, 2006.

TOE Identification – *e*Trust Admin V8.0

The Evaluated Configuration of the TOE is software only and includes the following Software Components of *e*Trust Admin V8.0 running on Windows 2000 Server SP4:

- *e*Trust Admin Server software
- Administrator Interface
- *e*Trust Admin Web-Server Web-based Interface

*e*Trust Directory is a component of the *e*Trust Admin V8.0 product, but it is not evaluated as part of the TOE.

The Report Explorer is part of the *e*Trust Admin Server component and part of the remote client, but it is not evaluated as part of the TOE.

The Workflow interface is part of the Web Server 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 - Resources, Identification, Authentication, Security Target, and Security Management

2.2 IT SECURITY ENVIRONMENT

The *e*Trust Admin ST levies requirements on the TOE as well as the IT Environment. In the case of this TOE, the IT Environment includes the of the operating system, Internet Explorer, the systems the TOE manages, the underlying hardware platforms and network, and parts of *e*Trust Admin TOE itself, including the *e*Trust Directory component, the Report Explorer, and the Workflow interface.

The TOE relies on the environment to provide:

- Protected audit trail storage
- Specification of Management Functions
- Non-bypassability of IT environment security functions

- Domain separation of IT environment security functions
- Reliable time stamps
- Inter-TSF trusted channel

2.3 OPERATING SYSTEM

The *e*Trust Admin Server and eTrust Admin Web-server portions of the TOE were evaluated with Windows 2000 Server SP4 in the IT environment. The remote client administrator interface was evaluated with Windows XP Professional SP2 in the IT environment.

2.4 HARDWARE PLATFORM

The Computer Associates eTrust Admin product was evaluated using the hardware platform as described in section 8 of this document.

3 SECURITY POLICY

The eTrust Admin TOE provides these security services:

- Security Audit
- User Login
- Security Management
- Partial Protection of the TOE Security Functions

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

3.1 SECURITY AUDIT POLICY

The *e*Trust Admin Server platform generates all TOE audit log data to support auditing of security functions. The *e*Trust Admin Server stores the audit data in two flat files, the Server Event Log and the Server Trace Log.

The *e*Trust Admin product audits the complex operations supported by the TOE. For example, the management function "create account" can result from adding global users to a role, modifying global user roles, including a global user into a policy or role, synchronizing users with roles, and checking synchronization of users with roles. eTrust Admin audits the management functions that support complex operations.

Server Event log settings are set using the Logging tab of the System Task frame in the Manager. Users can optionally choose to log messages to other log file destinations.

All Server Event logs record severity level messages. The severity levels are: Fatal; Error; Warning; Info; or Success. Server event logging includes the time of the event, the identifier of the user generating the event as well as selected event parameters.

The *e*Trust Admin product will associate each auditable event with the identity of the user that caused the event. The user identity is determined at the time of authentication. Once authenticated, the TOE associates the UID and corresponding user attributes with the user session. Upon receiving a user action associated with one or more auditable events, the TOE retrieves the UID for the user session, and records that UID in the audit log along with the current time stamp.

3.2 USER LOGIN POLICY

The *e*Trust Admin product manages and maintains profile attributes for each user.

The TOE collects information for each user thru the TOE's Web and Administrator interfaces and stores this information to the Administrative Directory, which is in the IT environment. Since the TOE is software only, it must rely upon the IT environment for persistent storage. As the TOE distributes the user information to the Environments, the user data is retrieved from persistent storage (as needed) by the TOE and transmitted to the managed server in the IT Environment.

The *e*Trust Admin product requires that user passwords meet the set of rules dictated in the Security Functional Requirements. The administrator can manage the domain password profile for the eTrust Admin Server through enabling Password Quality Checks.

The eTrust Admin product may be configured to be compatible with several I&A options, however the TSF is compatible only with authentication using UID and reusable password. Once authenticated, the TOE associates the UID and corresponding user attributes with the user session. This allows the TOE to successfully authenticate a user with a UID and password before being allowed to perform any other TSF mediated actions.

Upon connecting to the *e*Trust Admin server, the user is immediately prompted for their UID and password. Users are required to successfully authenticate, thereby identifying themselves before they can access additional TOE functionality.

3.3 SECURITY MANAGEMENT POLICY

The *e*Trust Admin product restricts the ability to access data and to perform management functions to authorized administrators. Once authenticated, the TOE associates the UID and corresponding user attributes retrieved from the Administrative Directory with the user session. Based upon the user attributes, the user's privilege to perform operations on TSF data is determined.

The TSF provides the ability to manage the security functions of the TOE thru the Web GUI, Manager GUI, Batch Utility.

The Web Interface—lets administrators and users perform basic administrative tasks from a Web browser. It comprises two features: DAWI, which lets administrators perform basic tasks such as creating and managing global users and their accounts; and the SAWI, which lets global users update their account and personal information.

The Manager GUI—is an object-oriented design through which the administrator can view and manipulate objects, including their relationships, using task frames to perform administrative tasks.

The Batch Utility—provides access to the same management functions as the Manager from a command line interface.

The *e*Trust Admin product allows authorized administrators to change, default, query, modify, delete, clear and create user accounts and profiles. The changes are maintained in the Administrative Directory which is in the IT environment.

3.4 PARTIAL PROTECTION OF TSF POLICY

The TOE includes three physical interfaces, the Web Interface, the Manager GUI, and the Batch Utility command line interface, through which the TOE may be invoked that must be considered in terms of non-bypassability. In addition, The TOE may not be invoked through the Administrative Directory, or the systems controlled by the TOE.

In order for an external user to access an *e*Trust Admin Server, the client must use a protected connection between the client and the TSF. The protected connection is supported by the IT environment. The TSF authenticates the user and associates the authenticated user session with user attributes retrieved from the Administrative Directory, also in the IT environment.

Once the external user is identified and authenticated, they cannot act without invoking an interface that is protected by the TSF. Based on the user attributes the external user's access privilege is determined for the object and action. There is no communication path that passes data to the Administrative Directory or controlled systems, except though the TSF controlled interface, and hence through the TSF via the specific authenticated connection.

Hence, the TSF ensures that all information must flow through the policy enforcement mechanisms.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 USAGE ASSUMPTIONS

A.Physec	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.Noevil	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.ITAccess	The TOE has access to all the controlled IT Systems to perform its functions.

4.2 ENVIRONMENTAL OBJECTIVES FOR THE IT ENVIRONEMNT

OE.Time	The IT Environment will provide reliable timestamps to the TOE.
OE.AuditStorage	The IT Environment will provide the capability to protect audit information.
OE.Protect	The IT environment will protect itself and the TOE from external interference or tampering.

OE.SecureComm	The IT environment will provide secure communication between TOE components and users, *e*Trust Directory, and managed systems.
OE.Introp	The TOE is interoperable with the IT System it manages.

4.3 ENVIRONMENTAL OBJECTIVES FOR THE NON-IT ENVIRONEMNT

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.

4.4 CLARIFICATION OF SCOPE

The product that a customer would purchase includes more than the evaluated TOE, *e*Trust Admin V8.0. As described in TOE Identification, the *e*Trust Directory component of the product, as well as the Report Explorer, and the Workflow interface are parts of the product but not parts of the TOE. However, *e*Trust Directory is currently the target of a separate evaluation at CygnaCom Solutions.

The *e*Trust Admin product 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 Admin 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

*e*Trust Admin is a user and resource management system used for managing user access control and authentication across multiple geographically dispersed systems. The role-based administration capability of *e*Trust Admin enables authorized administrators to manage accounts, group memberships, and access control to other resources that span diverse systems and heterogeneous databases. *e*Trust Admin allows authorized administrators to define and manage security policies using a role-based approach.

5.1 GENERAL TOE FUNCTIONALITY

The security functionality provided by *eTrust Admin* includes:

- **Security Audit**
- **User Login**
- **Security Management**
- **Partial Protection of the TOE Security Functions**

The *e*Trust Admin TOE relies on functionality in the IT environment, including *e*Trust Directory, the underlying operating system, the underlying hardware platforms and network to store and protect audit data records, to allow the TOE to control manage systems, to protect data transferred between the TOE, *e*Trust Directory, and managed systems, to provide reliable time stamps, to protect the *e*Trust Admin security functions from other interference or tampering.

A diagram of the *e*Trust Admin V8.0 TOE, showing functional and physical components, and the environment in which it exists is provided in Figure 1. Components of the software TOE are designated by blue shaded blocks.

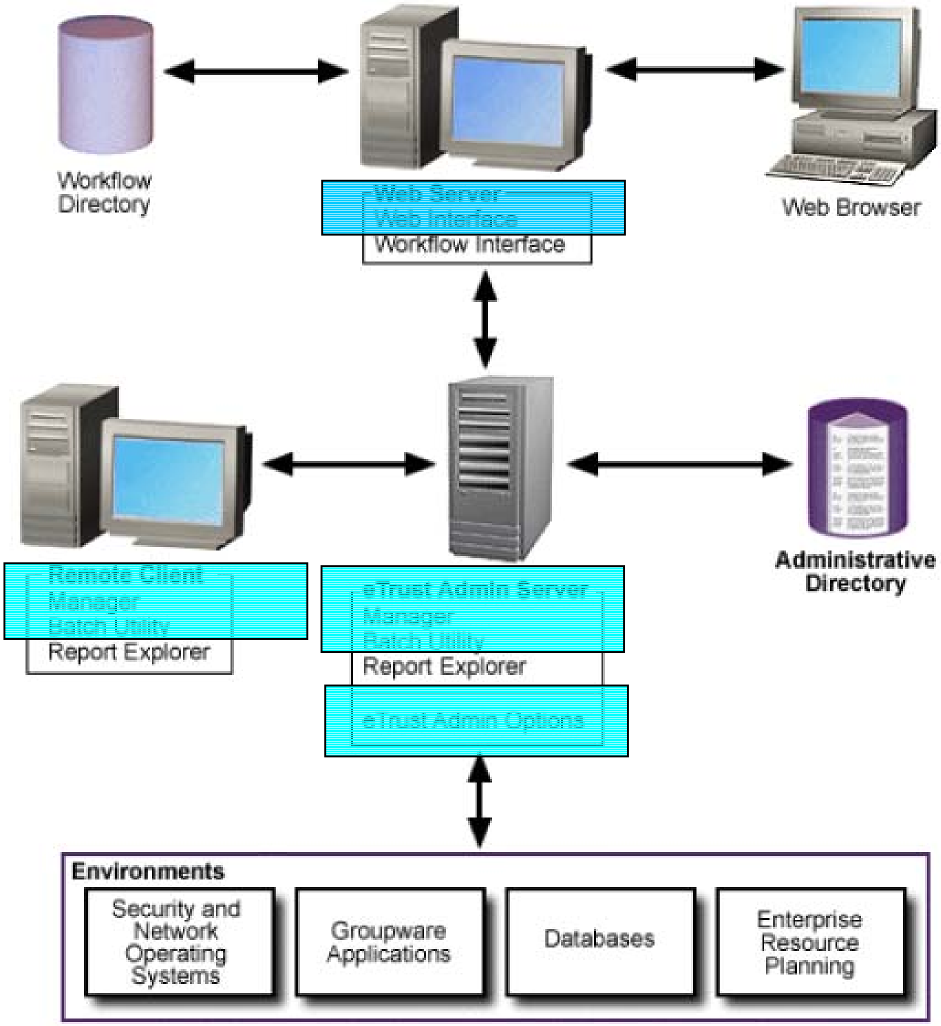

Figure 1: *e*Trust Admin TOE Boundary (software-only TOE components shaded)

5.2 TOE COMPONENTS

The *e*Trust Admin product consists of an *e*Trust Admin Server, Administrator Interface, and the *e*Trust Web-Server Web-based Interface. The *e*Trust Admin product also contains the *e*Trust Directory component which is not part of the TOE, but is included in the IT Environment

The ***e*Trust Admin Server** provides the core business logic of the application. As such, all other *e*Trust Admin components communicate with the Admin Server. In a domain, the *e*Trust Admin Server acts as the administrative command center for all communication by:

- Accepting requests from the Administrator and Web-based Interfaces,
- Storing information to and retrieving it from the Directory, and
- Issuing requests to the *e*Trust Admin Options so they can communicate with the systems that the *e*Trust Admin Server manages.

The *e*Trust Admin product provides the capability for an *e*Trust Admin Server in one domain to communicate with *e*Trust Admin Servers in other domains. However, communication between multiple *e*Trust Admin Servers is outside of the scope of this evaluation. The TOE contains a single instance of *e*Trust Admin Server.

The **Administrator Interface**, comprising the Manager GUI and the Batch Utility, provides a graphical user interface (GUI) in the former and, in the latter, a CLI to the *e*Trust Admin Servers security functions. The Administrator Interface may be hosted on both the *e*Trust Admin Server and a Remote Client.

The **Web-based Interface**, hosted on the Web Server, allows users to access the *e*Trust Admin Server and to perform certain tasks available to those users on a client platform running Internet Explorer 5.5 or 6.0 with Service Pack 2 or higher. The interface includes the Delegated Administration Web Interface (DAWI) and the Self-Administration Web Interface (SAWI). These two interfaces are described below:

> The **DAWI** allows TOE administrators to perform basic tasks, such as creating global users and accounts, changing passwords, and disabling or enabling accounts.
>
> When administrators point their web browsers at the machine running the Web Interface and log on to the Web Interface using their user identifier (UID) and password, the DAWI appears. *e*Trust Admin Server relies on its environment to provide secure communication between the DAWI user and *e*Trust Web-based Interface.
>
> The **SAWI** – Global users (any person or object that needs access to *e*Trust Admin or the systems that it manages) have access to the SAWI by pointing their web browsers at the machine running the Web Interface and logging on to the Web Interface using their UID and password. The SAWI allows users to make changes to their personal information or account passwords. *e*Trust Admin Server relies on its environment to provide secure communication between SAWI users and the *e*Trust Web-based Interface.

5.3 TOE INTERFACES

The interfaces external and internal interfaces of the TOE are described in Tables 1 and 2 below, respectively.

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.

Table 1 – TOE External Interfaces

External Interface	Description
Manager Interface	The Manager is a graphical user interface that organizes provisioning tasks into specific groups. Administrators can open the Manager Interface to the *e*Trust Admin Server from any Windows workstation or server. The most distinctive feature in the Manager is its task-oriented windows. These windows present all the managed directories, users, roles, and policies. With these windows, all tasks are performed in a consistent way, no matter how many users or directory types are managed.
Web Interface	The Web Interface lets the user perform simple administrative tasks from a web browser. When a user logs on to the Web Interface, the Delegated Administration Web Interface (DAWI) or the Self-Administration Web Interface (SAWI) appears, depending on the user account privileges.

External Interface	Description
Workflow Interface	*e*Trust Admin lets the user establish a workflow process that notifies people through email when global user or role changes are needed. When these people are notified, they can log on to the User Provisioning Workflow Interface (known as the Workflow Interface in guide documents) and approve them. Once a request is approved, *e*Trust Admin automatically creates accounts or changes them without taking valuable time away from administrators.
Report Explorer Interface	Used by administrators who generate reports for management or other administrators. The Report Explorer lets the user create, edit, and print reports using information from the Administrative Directory or managed directories. The user can access this interface through the Manager window or the *e*Trust Admin program group.
Batch Utility Interface	The Batch Utility is a command line interface that lets the user to perform repetitive and time-consuming tasks, such as auditing accounts or modifying their attributes on any directory. By using the simple etautil command with a control statement (parameters), a user can perform all the same tasks from a command line as the administrator can do in the Manager.
Server Event log	*e*Trust Admin logs all messages passed between the client interfaces and the *e*Trust Admin Server on a daily basis into flat files. To view and edit *e*Trust Admin log files, the administrator uses a text editor..
Administrator Authentication	Overall access to the eTrust Admin administrative interface is protected by authentication security. This security requires all administrators to identify themselves. If the administrator has the correct authentication information, then the administrator can log on to *e*Trust Admin.

Table 2 – Internal TOE Interfaces

Internal Interface	Description
Manager Interface to the eTrust Admin Server	The Manager GUI and the Admin Server communicate across this interface that is protected by the IT environment. The information exchanged thru this internal interface is characterized by the description of the corresponding external interface (e.g.: Manager Interface).
Batch Utility Interface to the eTrust Admin Server	The Batch Utility Interface and the Admin Server communicate across this interface that is protected by the IT environment. The information exchanged thru this internal interface is characterized by the description of the corresponding external interface (e.g.: Batch Utility Interface).
Web Interface to the eTrust Admin Server	The Web GUI and the Admin Server communicate across this interface that is protected by the IT environment. The information exchanged thru this internal interface is characterized by the description of the corresponding external interface (e.g.: Web Interface).
Managed systems in the IT environment interface to the eTrust Admin Server	The eTrust Admin Server distributes user policy to the managed systems (Namespace Servers) thru this interface that is protected by the IT environment. Managed user parameters are sent from the TOE to the managed system on this internal interface (e.g.: User Account Name (UID); Password; Profile user can assume; Roles; Groups).
Administrative Directory interface to the eTrust Admin Server	This interface is not included in the evaluation. Managed user parameters are sent from the TOE to the managed system on this internal interface (e.g.: User Account Name (UID); Password; Profile user can assume; Roles; Groups; Self-Administration Privilege; Expiration Date of when Administrator Privileges expire; Enable/Suspend State)
Host OS	Access to reliable time stamps, and support of the audit logs.

6 DOCUMENTATION

Purchasers of a product containing the eTrust Admin V8.0 receive the following TOE documentation:

- *eTrust Admin Administrator Guide*
- *eTrust Admin Getting Started Guide (GS)*
- *eTrust Admin Implementation Guide*
- *eTrust Admin Release Summary (RLS)*
- *eTrust Admin SDK Developer Guide*
- *CC Supplement to the eTrust Administrator Guidance*

7 IT PRODUCT TESTING

This section describes the testing efforts of the Vendor and the Evaluation Team.

The overall testing approach used by the developer was to create and run tests to cover the following security functions: Security Audit, Identification and Authentication, Security Management, and Protection of the TOE Security Functions. These functions were tested across the three interfaces that are present: Administrator Interface, Web-based Interface, and Command Line Interface.

7.1 TESTING PHASES

Evaluator testing occurred in three phases. The first phase of the evaluation testing consisted of the following activities:

- Observation of the installation of eTrust Admin in its evaluated configuration (ADO_IGS.1).
- Execution and observation of developer functional tests (ATE_IND.2).
- Development and execution of ad-hoc penetration tests (AVA_VLA.1).

The evaluator also verified how the TOE was delivered and TOE version number. Tests were executed using the eTrust Admin Administrator GUI interface (Admin Manager), the Web-based Interface, and Command Line Interface, as appropriate.

The second phase of testing was performed as a result of vulnerabilities that were discovered during the first phase of the eTrust Admin vulnerability analysis. These were CAN-2005-2667, CAN-2005-2668, CAN-2005-2669 from the CVE database. To alleviate these vulnerabilities, Computer Associates provided patches. While these vulnerabilities do not have a direct impact on the testing done on the evaluated configuration, the patches were installed for completeness and to ensure that installing them had no unintended side effects for the TOE. The patches were installed prior to the second phase of testing after the testing machines were confirmed to be in the evaluated configuration. These patches would normally be installed by a user after the standard installation of the TOE. The hard drives for the three test machines used during the first phase of testing had been stored untouched and were used to recover the test environment.

This second phase of testing focused on the following:

- Observation and documentation of the Installation of the software patches needed to counter the vulnerabilities discovered during the Vulnerability Analysis of eTrust Admin.
- Execution and Observation of developer functional tests (ATE_IND.2)
- Execution of independent team defined tests (ATE_IND.2)
- Execution of penetration tests (AVA_VLA.1)

The third phase of testing was performed at the Computer Associates test facility in Mason, Ohio.

This phase of testing was designed to demonstrate that changes to the TSF data objects through all three eTrust Admin user interfaces are propagated to the environments managed by eTrust Admin. The functionality demonstrated by this test demonstrates security functional requirements FMT_MTD.1, FMT_SMF.1-1, and FMT_SMR.1.

The test environment at the Computer Associates Common Criteria test laboratory in Herndon, VA was not set up with an external managed environment. This test was performed by CA's technical contact at the CA facility in Mason, Ohio to demonstrate the TOEs control of an external managed environment. After the completion of the test, documentation of the test setup, test procedures, and proof of results were sent to the evaluation team.

This third phase of testing focused on the following:

- Observation and documentation of the Installation of eTrust Admin.
- Execution and Observation of additional developer functional tests (ATE_IND.2)

7.2 INSTALLATION TESTING

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

- *eTrust Admin Getting Started Guide*

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

The Minimum hardware requirements for installing eTrust Admin are:

Component	Minimum Hardware Requirements	Software Requirements
eTrust Admin Server	Pentium 1 GHz Processor 128 MB Memory 300 MB Disk Space	Windows 2000 Server SP4 *e*Trust Directory 4.1 Build 175 Java Runtime Environnent JRE 1.3.1 Java Runtime Environnent JRE 1.4.1 Separate pre-populated LDAP directory (*e*Trust Directory 4.1 build 175) to simulate

Component	Minimum Hardware Requirements	Software Requirements
		customer data for tests *e*Trust Admin Server 8.0
eTrust Admin **Web Server**	Pentium 1 GHz Processor 256 MB Memory 1000 MB Disk Space	Windows 2000 Server SP4 Microsoft IIS Version 5.0 JRUN 4.0 *e*Trust Directory 4.1 Build 175 Java Runtime Environment JRE 1.3.1 Java Runtime Environment JRE 1.4.1 *e*Trust Admin Web Server 8.0 *e*Trust Admin Web Interface 8.0 *e*Trust Admin Workflow Web Interface 8.0
eTrust Admin Client	Pentium 1 GHz Processor 256 MB Memory 100 MB Disk Space	Windows XP Professional SP2 *e*Trust Admin Manager 8.0

Figure 2: TOE Installation Requirements

The test installation resulted in a successful installation of eTrust Admin in the evaluated configuration. All of the *e*Trust Admin TOE components were installed correctly for the evaluated configuration by following the procedures documented in the eTrust Admin Getting Started Guide. 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 vendor 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.

The Validation Team did not witness the installation testing.

7.3 DEVELOPER FUNCTIONAL TESTING

The evaluator's procedure was to select tests from the set of developer functional tests and modify the input parameters. This served the purpose of ensuring full functionality of the interface and gaining confidence in the developer's test results. The evaluator compared the results of each test with the corresponding expected results provided by the developer. All developer functional tests observed performed as expected.

In addition, a managed environment test was run by the CA technical contact to test that objects created and modified on the *e*Trust Admin Server were propagated to a managed network machine.

7.4 INDEPENDENT TEAM-DEFINED TESTING

The evaluation team's strategy for testing the TOE was to supplement the tests provided by Computer Associates. The tests provided by Computer Associates demonstrated almost all aspects of the security functional requirements for *e*Trust Admin as described in the ST. The team-defined functional tests were developed to cover any areas of functionality that were overlooked by the developer tests. Three team-defined tests were developed to test security auditing, login functionality of the command line interface and the use of the management functions through the eTrust Admin web interface.

The team-defined test cases were executed after the TOE was installed in the evaluated configuration (first test phase) and after the software patches previously described were applied (second test phase).

The testing was successful and confirmed that *e*Trust Admin limits access to the TSF and TSF data through its web interface as specified in the Security Target and that startup, shutdown and modification of the auditing functions are recorded. As a result of the testing, a change was made to the ST to reflect the discovery that there is limited functionality in the Web Interface compared to that of the Admin Interface.

The Validation Team witnessed the independent team-defined testing at the Computer Associates test facility in Herndon, VA and concluded that the testing was successful.

7.5 PENETRATION TESTING

The penetration tests for eTrust Admin were developed according to the following strategy:

- The evaluator will review the systematic vulnerability analysis of the TOE done by the developer.
- The evaluator will note possible security vulnerabilities while examining the developer's vulnerability analysis work, Functional Specification [FSP], High-level Design [HLD], and TOE security policy model [ST] while performing the work units for ADV requirements.
- The evaluator will analyze different components that make up the TOE for existing vulnerabilities.
- The evaluator will search public vulnerability databases for vulnerabilities that corresponded to these components.
- The evaluator will identify hypothesized vulnerabilities requiring low attack potential that apply to the TOE.
- The penetration tests will cover hypothesized vulnerabilities and potential misuse of guidance.
- The tests for potential misuse of guidance will cover installing the TOE from guidance documentation and sampling administrator procedures.

The penetration test cases were executed after the TOE was installed in the evaluated configuration and during the functional and independent testing. No general setup procedures were needed to perform the penetration tests other than those used for the independent testing.

The penetration testing done on-site did not expose any unknown vulnerabilities in the security functions of the TOE. However, the Command Line Interface (Batch Utility) testing in the first test phase did uncover the fact that the etautil utility requires the user to enter a password in plain text. The eTrust Admin ST was modified to remove FIA_UAU.7 (Protected authentication feedback). A warning was also added to the CC Supplement to the Administrator Guidance to caution the user. Warnings were also added to the supplement to cover impossible password policies, protection of the server configuration file, indications that the directory may be down and that program exits should not be used in a CC compliant system.

The Validation Team witnessed the penetration testing at the Computer Associates test facility in Herndon, VA and concluded that the testing was successful.

8 EVALUATED CONFIGURATION

The evaluated configuration of the TOE as tested relied on three physical platforms configured as follows:

TOE Component	***e*Trust Admin Server 8.0**	***e*Trust Admin Manager 8.0**	***e*Trust Admin Web Server 8.0** ***e*Trust Admin Web Interface 8.0** ***e*Trust Admin Workflow Web Interface 8.0**
Operating System	Microsoft Windows 2000, Service Pack 4	Microsoft Windows XP, Service Pack 2	Microsoft Windows 2000, Service Pack 4
Other Software	eTrust Directory 4.1 Build 175 Java Runtime Environment JRE 1.3.1 Java Runtime Environment JRE 1.4.1	NONE	Microsoft IIS Version 5.0 JRUN 4.0 *e*Trust Directory 4.1 Build 175 Java Runtime Environnent JRE 1.3.1 Java Runtime Environnent JRE 1.4.1
Hardware	Pentium 1 GHz Processor 128 MB Memory 300 MB Disk Space	Pentium 1 GHz Processor 256 MB Memory 100 MB Disk Space	Pentium 1 GHz Processor 256 MB Memory 1000 MB Disk Space

A domain controller server was also installed in the laboratory and used by the three test machines; however it was part of the IT environment and not touched during the installation or testing.

The evaluated configuration at the Computer Associates test facility in Mason, Ohio was similar the evaluated configuration in Herndon, VA.

The test configuration included two machines: the Admin Server and the AD Server. The Admin Server machine running Windows 2000, was installed with the same *e*Trust Admin software (Server, Windows GUI and Web Interface) that was specified in the evaluated configuration and was the same version of the software as used in the November testing in Herndon Virginia. The AD Server (an Active Directory server) machine running Windows 2003, was the managed machine and connected to the same network domain as the Admin Server.

Only the managed machine, the AD Server, was added. The rest of the evaluated configuration and interfaces were the same. The configuration of TOE was not changed since the AD Server is in the IT environment.

The evaluation team chose the evaluated configuration at the test facility in Herndon, 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 Admin remote clients that might be installed, due to the limits in the lab environment.

A Separate test setup in Mason, Ohio was required because test setup in Herndon, VA was not set up with an external managed environment. During the initial tests, password policy was pushed to domain in the evaluated configuration, but not to an active managed environment. The test in Mason, Ohio was able to demonstrate that managed users, working from a non-TOE component, were able to log into their OS with a new password policy pushed to them by the TOE.

The evaluated configuration of the TOE as tested in Mason, Ohio was configured as follows:

Admin Server (iam8vm01)

- Windows 2000 Server SP4
- *e*Trust Admin Server 8.0 (installed with CAM v1.11 patch)
- *e*Trust Admin Web Server 8.0
- *e*Trust Admin Web Interface 8.0
- *e*Trust Directory 4.1 Build 175
- Java Runtime Environment JRE 1.3.1
- Java Runtime Environment JRE 1.4.1
- JRUN 4.0

AD Server (werke01-adm81g1)

- Windows 2003 Server Standard Edition

A minimal configuration was chosen for the tests in Mason, Ohio. The evaluated configuration in Ohio did not include a separate Web Server machine or Admin Client machine. The Web Server software was installed on the same machine as the Admin Server software. The workflow option for Admin was not installed, but it is not included in the TOE. The managed machine (AD Server) did not have any Admin software installed on it. This configuration was tested without a remote client administrator interface.

The evaluation team did not test the limits of the number of managed systems that could be attached to the TOE. The only managed system test was performed by Computer Associates personnel at the test facility in Mason, Ohio. Neither the evaluation team nor validation team was present.

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 vendor 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 Admin V8.0 with CAM V1.11 patch, ETR Version 1.6, Security Target Version 2.3, dated February 9, 2006* and *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, Computer Associates eTrust Admin V8.0 with CAM V1.11 patch, ETR Version 0.7, Security Target Version 2.3, dated February 10, 2006* 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 following guidance documentation:

- *eTrust Admin Administrator Guide*
- *eTrust Admin Getting Started Guide (GS)*
- *eTrust Admin Implementation Guide*
- *eTrust Admin Release Summary (RLS)*
- *eTrust Admin SDK Developer Guide*
- *CC Supplement to the eTrust Administrator Guidance*

The TOE *e*Trust Admin V8.0 is CC compliant and satisfies the *eTrust Admin V8.0 Security Target Version 2.3*, dated February 2, 2006.

10 VALIDATION COMMENTS/RECOMMENDATIONS

10.1 VALDATION COMMENTS

The product, *e*Trust Admin V8.0, 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 configuration of one admin server, one web-server and one remote server. This configuration was simpler for the test environment. Although multiple remote servers are possible, a single remote server was used during testing since it would functionally look the same to the TOE.

Although multiple instances of the Admin remote clients are likely, The TOE was tested using only one. This was acceptable for the evaluation since the security functionality is the same for one Admin remote client as it is for many Admin remote clients. The end user should be aware that there is no guarantee of how many Admin remote clients can be used or whether multiple Admin remote clients reduce the performance of the TOE.

The *e*Trust Admin product can maintain multiple managed systems at the same time. Although multiple managed systems are possible, a single managed system was tested since it would functionally look the same to the TOE. The limit to the number of managed systems possible was not tested.

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. The customer can have no confidence, based on this evaluation, that the eTrust Admin 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 following IT environment requirement, FTP_ITC_EXP.1 Inter-TSF trusted channel (e.g., 128 bit AES option should be considered).

The user of this product should be aware that several components of the eTrust Admin product are outside of the TOE. The end user should ensure that IT environment, as described in the Security Target, is maintained securely as described it the documentation provided with the TOE.
However, *e*Trust Directory is currently the target of a separate evaluation at CygnaCom Solutions.

The CygnaCom evaluation team discovered that the communication package (CAM/CAFT) had a message queuing vulnerability. The patch, CAM V1.11, was added to the TOE to mitigate this vulnerability. Although the communication package is not part of the TOE, the evaluation team recognized that without the patch, the TOE would be vulnerable to denial of service attacks. Also buffer overflow conditions could potentially allow arbitrary code to be executed remotely with elevated privileges.

Program Exits in the TOE allow the user to reference custom code from within the eTrust Admin process flow. The Computer Associates eTrust Admin V8.0 Vulnerability Analysis states, “The associated risk is that the custom code may not work correctly or could actually be malicious code. For the purposes of this evaluation the capability is outside the scope of evaluation. End users who want to be compliant with the TOE configuration must not use this capability.”

*e*Trust Admin was not difficult to install and configure, it was easy to operate and easy to administer. Most of the interfaces were GUI interfaces. However it is possible for the administrator to access the TOE through a command line interface for batch jobs, simple commands, or 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 the TOE identified here is complete and correct: *e*Trust Admin V8.0.

11 LIST OF ACRYONYMS

CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
I&A	Identification and Authentication
ID	Identifier
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIC	Network Interface Card
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
UID	User Identifier

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.
- *eTrust Admin V8.0 Security Target Version 2.3*, dated February 2, 2006.
- *Evaluation Technical Report for a Target of Evaluation, Volume 1: Evaluation of the ST, Computer Associates eTrust Admin V8.0 with CAM V1.11 patch, ETR Version 1.6, Security Target Version 2.3, dated February 9, 2006.*
- *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, Computer Associates eTrust Admin V8.0 with CAM V1.11 patch, ETR Version 0.7, Security Target Version 2.3, dated February 10, 2006.*