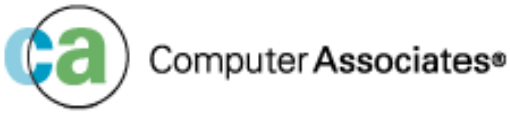

*e*Trust Admin™ V8.0

Security Target V2.3

February 2, 2006

Prepared for:

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

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

Revision History:

Date:	Version:	Author:	Description
2/10/2004	0.1	Debra Baker	First Draft
3/29/2004	0.2	Debra Baker	Second Draft
5/3/2004	1.0	Debra Baker	Update Physical and Logical Boundaries
5/6/2004	1.1	Debra Baker	Updates made throughout
5/25/2004	1.2	Debra Baker	Updates made to threats and assumptions per evaluator
8/17/2004	1.3	Debra Baker	Updates made throughout per evaluator
11/12/2004	1.4	Debra Baker	Updates made throughout
12/14/2004	1.4.1	Debra Baker	Updates made throughout
12/22/2004	1.4.2	Debra Baker	Updates made throughout
1/31/2005	1.5	Debra Baker	Updates made throughout
4/18/05	1.6	Debra Baker	Updates made throughout
5/10/05	1.7	Debra Baker	Updates made throughout
9/21/2005	1.8	D. DePrez	Updates made after testing
9/23/2005	1.9	D. DePrez	Updates made after testing
9/25/2005	2.0	D. DePrez	Formatted
10/28/2005	2.1	D. DePrez	Revised per Validator's comments
11/21/2005	2.2	D. DePrez	Revised following testing. Clarification of Web Interface functionality added in TSS. Audit events corrected. Account expiration user attribute corrected.
2/2/2006	2.3	D. DePrez	Respond to validator's comments

TABLE OF CONTENTS

SECTION PAGE

Table of Tables

Table **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: *e*Trust Admin™ V8.0 with patch CAM v1.11

ST Title: *e*Trust Admin™ V8.0 Security Target V2.3

ST Version: Security Target V2.3

ST Authors: Debra Baker, Daniel DePrez

ST Date: February 2, 2006

Assurance Level: EAL2

Strength of Function: SOF-basic

Vendor: Computer Associates

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

Registration: VID3037

Keywords: Resources, Identification, Authentication, Security Target, and Security Management.

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for *e*Trust Admin v8.0. *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.

1.3 Common Criteria Conformance

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

1.4 Document Organization

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

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

Section 0, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

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

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

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

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

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

The appendix provides acronym definitions and references.

2 TOE Description

2.1 Product Type

*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.

2.2 eTrust Admin Components

The *e*Trust Admin product consists of an *e*Trust Admin Server, Administrator Interface, Web-based Interface, and *e*Trust Directory. Briefly, the TOE includes the *e*Trust Admin Server software, the Administrator Interface, and the Web-based Interface. The *e*Trust Directory and the Windows 2000 OS, upon which the *e*Trust Admin Server runs, are included in the IT Environment. A detailed description of the TOE is found in Section 2.3.

2.2.1 eTrust Admin Server

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, described in Section 2.2.2, may be hosted on the *e*Trust Admin Server itself, and a Remote Client.

The *e*Trust Admin Server software runs on MS Windows 2000 server in the evaluated configuration; the operating system is part of the IT environment and the *e*Trust Admin Server software is part of the TOE.

2.2.2 Administrator Interface

The Administrator Interface, comprising the Manager GUI and the Batch Utility, hosted on either the Remote Client or the eTrust Admin Server, provides a graphical user interface (GUI) in the former and, in the latter, a CLI to the *e*Trust Admin Servers security functions. It is hosted on Windows 2000 in the evaluated configuration.

2.2.3 Web-based Interface

The Web-based Interface, hosted on the Web Server, allows users to access the *e*Trust Admin Server and 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:

- **DAWI** - The DAWI allows TOE administrators to perform basic tasks, such as:
  - Creating global users and accounts
  - Changing passwords
  - 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.
- **SAWI** – Global users 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.

A global user is any person or object that needs access to *e*Trust Admin or the systems that it manages.

2.2.4 *e*Trust Directory

*e*Trust Directory is bundled with *e*Trust Admin, but *e*Trust Directory is being evaluated separately at EAL3. Hence, *e*Trust Directory is not part of the TOE but rather is in the IT environment for this evaluation. eTrust Directory supports the software-only TOE by providing persistent storage of data. Although the *e*Trust Directory is bundled with *e*Trust Admin, any LDAP compliant directory may be used as the data store.

*e*Trust Directory was used in the configuration tested during the evaluation. All references to the administrative or workflow directory in this ST refer specifically to a directory hosted on the *e*Trust Directory, although the workflow directory is installed on a separate installation of *e*Trust Directory and hardware platform than the administrative directory.

*e*Trust Directory supports the software-only TOE by storing user attributes and environment specific information. *e*Trust Directory may be accessed by the TOE over a network based connection.

2.3 TSF Physical Boundary and Scope of the Evaluation

The TOE is a software-only TOE which consists of:

- *e*Trust Admin Server, which implements all evaluated security functionality
- Administrator Interface CLI/GUI (i.e.: Manager and Batch Utility) and

- Admin Web-based Interface software.

The TOE includes *e*Trust Admin Options (part of *e*Trust Admin Server) to communicate with managed systems. Only the Windows OS option was tested during the evaluation.

The IT environment of the TOE consists of:

- *e*Trust Directory, in which the TOE stores user attributes,
- Internet Explorer,
- Managed systems,
- Underlying OS software and
- Underlying host hardware and network.

The following are outside the scope of the evaluation and were neither part of the TOE nor present in its IT environment:

- Workflow Directory and the Workflow user interface since they do not support any TOE security functionality,
- The password synchronization agent, which may be installed on systems the *e*Trust Admin product manages, and
- Other *e*Trust Admin servers (e.g.: other instances of the TOE).

2.4 TOE Logical Boundary

*e*Trust Admin provides the following security features:

- **Security audit** - *e*Trust Admin provides its own auditing capabilities separate from those of the underlying OS. The audit trail is sent to flat files that are protected and reviewed through the OS interfaces. *e*Trust Admin provides the ability to select which level of audit events will be audited.
- **Identification and authentication (I&A)** - *e*Trust Admin provides user I&A through the use of user accounts and the enforcement of password policies.
- **Security management** - *e*Trust Admin provides security management through the use of the Administrator and web based Interfaces.
- **Partial protection of TSF (TOE)** - *e*Trust Admin ensures that all information that flows through it must flow through the policy enforcement mechanisms.

2.5 TOE Security Environment

*e*Trust Admin relies upon the underlying OS and hardware platform to:

- View, store, and protect audit data records,
- Provide reliable time stamps, and
- Protect *e*Trust Admin from other interference or tampering.

Also *e*Trust Admin relies on the managed systems' OS to provide an interface thru which the TOE can manage user access control and authentication. *e*Trust Admin relies on *e*Trust Directory to store and return user attributes thru an interface controlled by the TOE.

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

1. *e*Trust Admin Server, Administrator Interface and *e*Trust Directory running on a Windows 2000, SP4 server
2. *e*Trust Administrator Interface running on a separate machine with Windows XP, SP2
3. *e*Trust Admin Web-based Interface and web server running on a separate machine with Windows 2000, SP4 and Internet Explorer

The *e*Trust Admin Server is only installed on one platform, but can be accessed through all of the platforms in the evaluated configuration. Figure 2-1 shows the product components, as well as four example managed systems (namespaces) in the environment.

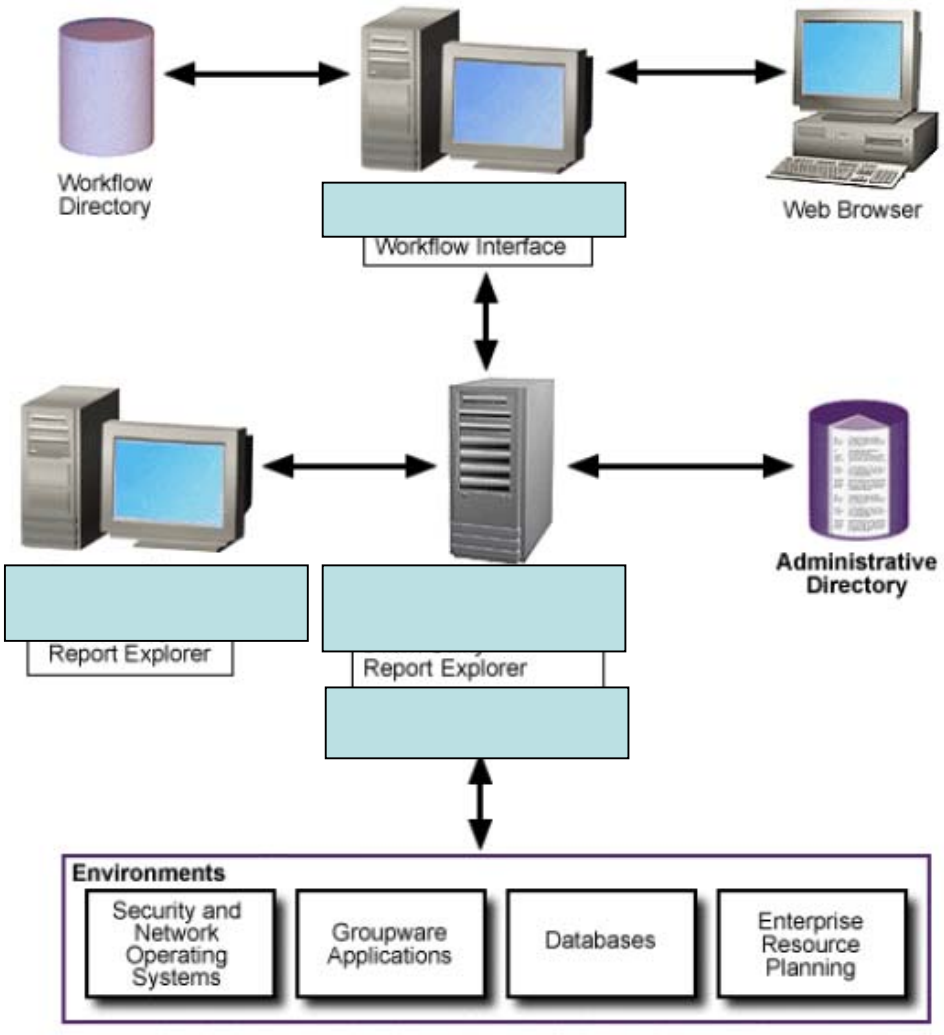

Figure 2-1: *e*Trust Admin components (software-only TOE components shaded)

Information regarding the TOE components can be found in Section 2.3 of this document. The TOE components are described in Section 2.2 of this document. In particular the Administrative Directory is described in Section 2.2.4.

In Figure 2-1 the items that are identified in Section 2.3 of this document have been shaded. The items that have not been shaded are:

Table 2-1 – Product Components not Included in the TOE

Product component not included in TOE	Product component function
Administrative Directory	Persistent storage of data.
Web Browser	A web browser on a client that is used to connect to the servers included in the TOE.
Workflow Interface	An interface that enables the definition of workflows. A workflow describes the steps in completing a task.
Workflow directory	A database where workflows are stored.
Report Explorer	generate reports for management or other administrators.
Environments	Servers in the environment to which the TOE distributes user information.

The external TOE interfaces are:

Table 2-2 – External Administrative 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.
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.

External Interface	Description
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.

The internal TOE interfaces are:

Table 2-3 – Internal 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.

The interfaces excluded from the evaluation are:

Table 2-4 – Excluded Interfaces

External Interface	Description
Programmatic Interface	The programmatic interface allows the user to customize *e*Trust Admin based on the specific requirements of his company. It varies from a simple LDAP command line interface that uses standard LDAP commands and an API to a detailed SDK.
Another Instance of the TOE	eTrust Admin servers can communicate with other eTrust Admin Servers that are managing other domains and exchange managed user information
Password Sync Option	This option is installed on managed systems (Namespace Servers) in the IT environment and transmits modifications made to user authenticators thru the IT environment's interfaces to the eTrust Admin Server.
Administrative Directory interface to the eTrust Admin Server	This interface is not included in the evaluation. Managed and administrative user data is transmitted across this interface.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 – Assumptions

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

3.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to standard equipment and public information.

The TOE must counter the following threats to security:

Table 3-2 – Threats

Item	Threat	Description
1	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.
2	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.
3	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.
4	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
5	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.

Table 3-3 – IT System Security Threats

Item	Threat	Description
6	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.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 – Security Objectives for TOE

Item	Objective	Description
1	O.Access	The TOE must allow only authorized users to access appropriate TOE functions and data.
2	O.Admin	The TSF must provide all the functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security, and restrict these functions and facilities from unauthorized use.
3	O.Attributes	The TOE must be able to maintain attributes.
4	O.Audit	The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators.
5	O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
6	O.Roles	The TOE must support multiple roles.
7	O.Prop	The TOE must be able to propagate object attribute changes to all related objects, including managed IT systems.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 – Security Objectives for the IT Environment

Item	Objective	Description
1E	OE.Time	The IT Environment will provide reliable timestamps to the TOE.
2E	OE.AuditStorage	The IT Environment will provide the capability to protect audit information.
3E	OE.Protect	The IT environment will protect itself and the TOE from external interference or tampering.
4E	OE.SecureComm	The IT environment will provide secure communication between TOE components and users, *e*Trust Directory, and managed systems.
5E	OE.Introp	The TOE is interoperable with the IT System it manages.

The following are the non-IT security objectives, which, in addition to the corresponding assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

4.2.2 Security Objectives for Non-IT Security Environment

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

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

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

5 IT Security Requirements

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

5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.1 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

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

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

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

- *Assignments* and *Selections* specified by the ST author are in ***italicized bold text.*** .
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *Comments* are provided as an aid to the ST author and evaluation team. These items will be deleted in the final version of the ST.

5.2 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1. With the exception of FPT_RVM_EXP.1-1, all SFR are taken from Part 2 of the Common Criteria.

Table 5-1 – TOE Functional Components

No.	Family	Component	Component Name
1	Security audit	FAU_GEN.1	Audit data generation
2	Security audit	FAU_GEN.2	User identity association
3	Identification and authentication	FIA_ATD.1	User attribute definition
4	Identification and authentication	FIA_SOS.1	Verification of secrets
5	Identification and authentication	FIA_UAU.2	User authentication before any action
6	Identification and authentication	FIA_UID.2	User identification before any action
7	Security management	FMT_MTD.1	Management of TSF data
8	Security management	FMT_SMF.1-1	Specification of management functions
9	Security management	FMT_SMR.1	Security roles
10	Protection of the TOE security functions	FPT_RVM_EXP.1-1	Non-bypassability of the TSP: TOE

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

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

c) the following auditable events

- ***Rejection or acceptance by the TSF of any tested secret***
- ***Identification of any changes to the defined quality metrics of any tested secret***
- ***All use of the TOE authentication mechanism***
- ***All use of the TOE user identification mechanism, including the user identity provided.***
- ***All modifications to the values of TSF data.***
- ***Use of the management functions.***
- ***modifications to the group of users that are part of a role;***
- ***every use of the rights of a role.***

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***no other information.***

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

5.2.2 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- ***User Account Name (UID);***
- ***Password;***
- ***Profile user can assume;***
- ***Roles;***
- ***Groups;***
- ***Self-Administration Privilege;***
- ***Expiration Date of when Administrator Privileges expire;***
- ***Enable/Suspend State;***

Dependencies: No dependencies.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***the rules defined in Table 5-2***

Table 5-2 – Password Rules

Requirement	Minimum Value
Minimum number of lower-case characters	1
Minimum number of upper-case characters	1
Minimum number of numeric characters.	1
Minimum number of special characters	1
Maximum number of days before a password must be changed.	30
Number of previous passwords to be checked against new passwords.	10
Minimum number of characters required in all passwords.	8
No dictionary words	

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.2.3 Class FMT: Security Management (FMT)

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to ***change_default, query, modify, delete, clear, rename, and create as specified in Table 5-3*** the ***TSF Data as specified in Table 5-3*** to ***the role as specified in Table 5-3.***

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Table 5-3 – Management of TSF data

Subjects with profiles of the following:	Allowed Operations on TSF Data (Management Functions)	Objects:
DomainAdministrator	• Create, read, modify, rename, and delete account names. • Create, read, modify, and delete groups, roles, and policies. • Enable and Suspend user accounts • Assign users to profiles, groups, and roles • Propagate object attribute changes to all related objects, including managed systems	• Accounts • Attributes • Groups • Policies • Roles
DomainAdministratorNoWeb	• Create, read, modify, rename, and delete account names. • Create, read, modify, and delete groups, roles, and policies. • Enable and Suspend user accounts • Assign users to profiles, groups, and roles • Propagate object attribute changes to all related objects, including managed systems	• Accounts • Attributes • Groups • Policies • Roles
PasswordAdministrator	• Enable and Suspend user accounts • Change passwords • Propagate object attribute changes to all related objects, including managed systems	• Accounts (Activate or Suspend) • Attributes (Password)
UserAdministrator	(Within their assigned domain) • Create, read, modify, rename, and delete account names • Create, read, modify, and delete groups • Enable and Suspend user accounts • Assign users to profiles and groups • Propagate object attribute changes to all related objects, including managed systems	• Accounts • Attributes • Groups
ReadAdministrator	(Within their assigned domain) • Read account names and groups	• Accounts • Attributes • Groups • Policies • Roles
Global User	Read-only access unless self-administration capabilities have been assigned.	▪ Accounts ▪ Attributes

FMT_SMF.1-1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1-1.1 The TSF shall be capable of performing the following security management functions:

- ***Allowed Operations on TSF Data (Management Functions) as specified in Table 5-3 .***

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles ***see profiles identified in column 1 of Table 5-3.***

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.2.4 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-1 Non-bypassability of the TSP: TOE

Hierarchical to: No other components.

FPT_RVM_EXP.1-1.1 The TSF, when invoked by the underlying IT environment, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

5.3 Strength of Function

The overall strength of function requirement is SOF-basic. The strength of function requirement applies to FIA_SOS.1. The strength of the “secrets” mechanism is consistent with the objectives of authenticating users (O.IDAuth). Strength of Function shall be demonstrated for the password based authentication mechanisms included in the TOE to be SOF-basic, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a low-level attack potential.

5.4 Security requirements for the IT Environment

*e*Trust Admin requires that the OS platform provide reliable time stamps.

Table 5-4 – Functional Components for the IT environment

No.	Component	Component Name
11	FAU_STG.1	Protected audit trail storage
12	FMT_SMF.1-2	Specification of Management Functions
13	FPT_RVM_EXP.1-2	Non-bypassability: IT
14	FPT_SEP_EXP.1	Domain separation: IT
15	FPT_STM.1	Reliable time stamps
16	FTP_ITC_EXP.1	Inter-TSF trusted channel

5.4.1 Class FAU: Security Audit

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

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

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

Dependencies: FAU_GEN.1 Audit data generation

Application Note: *This SFR specifies the protection required to protect the TOE's audit event data.*

5.4.2 Class FMT: Security Management (FMT)

FMT_SMF.1-2 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1-2.1 **Refinement:** The ***IT environment*** shall be capable of ***allowing the TOE to perform*** the following security management functions: ***administrating the list of authorised users of each controlled system by creating, deleting, and/or modifying the users along with their corresponding security attributes.***

Dependencies: No Dependencies

5.4.3 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-2 Non-bypassability: IT

Hierarchical to: No other components.

FPT_RVM_EXP.1-2.1: The security functions of the IT environment shall ensure that IT environment security policy enforcement functions are invoked and succeed before each function within the scope of control of the IT environment is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1 Domain separation: IT

Hierarchical to: No other components.

FPT_SEP_EXP.1.1 The security functions of the IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope and control of the IT environment.

FPT_SEP_EXP.1.2 The security functions of the IT environment shall enforce separation between the security domains of subjects in the scope of control of the IT environment.

Dependencies: No dependencies.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

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

Dependencies: No dependencies.

5.4.4 Class FTP: Trusted path/channels

FTP_ITC_EXP.1 Inter-TSF trusted channel

FTP_ITC_EXP.1.1 The IT environment shall provide a communication channel between the TOE and remote trusted IT products that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_EXP.1.2 The IT environment shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC_EXP.1.3 The TSF shall initiate communication via the trusted channel to support

- Bi-directional Transfer of controlled system attributes, user attributes and configuration information initiated by the TOE to and from the Administrative Directory,
- Transfer of global user attributes from the TOE to the controlled systems, and
- Communication between the hosts of distributed TSF components to support remote administration of the TOE.

Dependencies: No dependencies

5.5 TOE Security Assurance Requirements

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

Table 5-5 – EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

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

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

The following sections describe the IT Security Functions of the *e*Trust Admin Server. Together these IT Security Functions satisfy the TOE security functional requirements. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. In Section 6.1.2, the *e*Trust Admin Server Interface, Directory Server Interface, Administrator Interface, and the Web-based Interface will be mutually referred to as *e*Trust Admin.

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

No	SFRs	Security Class	Security Functions	Sub-functions
1	FAU_GEN.1	Security audit	Security Audit	AI-SA-1
2	FAU_GEN.2	Security audit	Security Audit	AI-SA-2
3	FIA_ATD.1	Identification and authentication	User Login	AI-UL-1
4	FIA_SOS.1	Identification and authentication	User Login	AI-UL-2
5	FIA_UAU.2	Identification and authentication	User Login	AI-UL-3
6	FIA_UID.2	Identification and authentication	User Login	AI-UL-4
7	FMT_MTD.1	Security management	Security Management	AI-SM-1
8	FMT_SMF.1-1	Security management	Security Management	AI-SM-2
9	FMT_SMR.1	Security management	Security Management	AI-SM-3
10	FPT_RVM_EXP.1-1	Protection of the TOE Security Functions	Partial protection of TSF	AI-PP-1

6.1.2 *e*Trust Admin Functions

Table 6-2 – Security Audit Function

Security Function: Security Audit Function		
Item	Sub-function ID	Sub-function description
1	AI-SA-1	*e*Trust Admin generates the audit events specified in FAU_GEN.1. The information recorded for all events is described in FUA_GEN.2. The *e*Trust Admin Server platform generates all audit log data. The *e*Trust Admin Server stores audit data in flat files. Two flat files are used to support auditing of security functions, the Server Event Log and the Server Trace Log. *e*Trust Admin 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. *e*Trust Admin audits the management functions that support complex operations.

Security Function: Security Audit Function		
Item	**Sub-function ID**	**Sub-function description**
		Server Event log settings are set using the Logging tab of the System Task frame in the Manager. User can optionally choose to log messages to other destinations, such as stdout and the text file eTayyyymmdd.log in the ETAHOME\Logs directory. All Server Event logs record messages of the same severity levels. These severity levels are: • Fatal • Error • Warning • Info • Success Sevrer event logging includes the time of the event, the identifier of the user generating the event as well as selected event parameters.
2	AI-SA-2	*e*Trust Admin will associate each auditable event with the identity of the user that caused the event. (FAU_GEN.2) 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.

Table 6-3 – User Login Function

Security Function: User Login Function		
Item	**Sub-function ID**	**Sub-function description**
3	AI-UL-1	*e*Trust Admin manages and maintains the following information for each user: ▪ User Account Name (UID); ▪ Password; ▪ Profile user can assume; ▪ Roles; ▪ Groups; ▪ Self-Administration Privilege; ▪ Expiration Date of when Administrator Privileges expire; ▪ Enable/Suspend State; The TOE collects information for each user thru the TOE's Web and Manager interfaces and stores this information to the Administrative Directory, which is in the IT environment, but provides persistent storage for the software-only TOE. Since the TOE is software only TOE, it must rely upon the IT environment for persistent storage. The secure transmission and storage of persistent data in the IT environment is supported by A.Physec. 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 server in the Environment. (*see* Figure 2-1). (FIA_ATD.1) This information is stored in the Administrative Directory, which is not part of the TOE, but provides persistent storage for the software-only TOE.

Security Function: User Login Function		
Item	**Sub-function ID**	**Sub-function description**
4	AI-UL-2	*e*Trust Admin requires that user passwords meet the rules found in Table 5-2. (FIA_SOS.1) When the administrator clicks the Domain button on the System Task Frame on the Management GUI, the administrator can then select the Domain Properties Button and the Password Profile tab appears. Using this tab the administrator can select the Enable Password Quality Checks checkbox and then manage the domain password profile for the eTrust Admin Server.
5	AI-UL-3	*e*Trust Admin Administrator and User Interfaces require each user to successfully authenticate with a UID and password through the TOE interfaces before being allowed any other TSF mediated actions. The 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. (FIA_UAU.2)
6	AI-UL-4	The *e*Trust Admin Administrator and User Interfaces require users to identify themselves before being allowed to perform any other actions. (FIA_UID.2). 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.

Table 6-4 – Security Management Function

Security Function: Security Management Function		
Item	**Sub-function ID**	**Sub-function description**
7	AI-SM-1	*e*Trust Admin restricts the ability to access data as specified in Table 5-3 (FMT_MTD.1). Only the authorized administrator is permitted to perform management functions. Once authenticated, the TOE associates the UID and corresponding user attributes retrieved from the Administrative Directory with the user session. User attributes have been identified in FIA_ATD.1. Based upon the user attributes, the user's privilege to perform operations on TSF data is determined.
8	AI-SM-2	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. *e*Trust Admin provides the following security management function: change, default, query, modify, delete, clear and create as specified in Table 5-3 and the TSF Data as specified in Table 5-3. (FMT_SMF.1-1). The changes are maintained in the Administrative Directory. The above identified interfaces are

Security Function: Security Management Function		
Item	**Sub-function ID**	**Sub-function description**
		described as follows: When the administrator logs on to the Web Interface, the DAWI or the SAWI appears, depending on the administrator's account privileges. The GUI is broken into four main frames. These frames are: • User name frame appears along the top of the window and identifies the user who is being administered • Command frame appears to the left of the window and displays the navigational links and functions that the administrator can perform To navigate thru the Web Interface the administrator uses the function links in the command frame. The administrator can left-click on a function link to open the working frame • Working frame appears in the middle of the window and steps the administrator through the tasks the administrator are performing • Status frame appears along the bottom of the window and displays detailed information for each main operation that was performed. The administrator can also view the detailed information for each sub-operation that was performed. The SAWI includes and Global user functions in the Command Frame so that administrators can update their own account and personal information. The Manager GUI is an object-oriented design that lets the administrator view and manipulate objects, including their relationships, using task frames. The main elements of the Manager GUI are: • Title bar Displays the name of the domain, the global user, the task window name, and a sequential number starting at zero. This number shows the administrator how many task windows of this type are open. • Menu bar Lists commands that the administrator can perform, for example, view the toolbars, access Reporting, or open the Manager help. • Task buttons Displays buttons that the administrator can click to open a task frame. • Search bar Searches for objects in an Administrative Directory. Once found, these objects appear in the list view. • List view Displays the objects from a search. The bottom of the list view is tabbed so the administrator can view the objects from previous searches in the task frame. • Property sheet view Displays the properties of the selected object in the list view. • Message log Displays the date, time, and server operations the administrator performed with the Manager. The administrator opens and uses Task Frames to complete management tasks. The frames are: the Wizards Task Frame, the Users Task frame, the Roles Task frame, and the Namespace Task frame. Wizard Task frames permit administrative tasks to be completed with accounts, roles, and users. User Task frames permit create, modify, or delete global users, global user groups, and admin profiles, make global users members of a global user groups list all the accounts that a global user

Security Function: Security Management Function		
Item	**Sub-function ID**	**Sub-function description**
		has, view the admin profiles that are available The Roles Task frame permit the administrator to create, modify, or delete roles or policies associate a policy with a role, view the global users defined to a role, view the accounts that were created from a policy. The Batch Utility lets the administrator perform the same tasks as the administrator can do with the Manager, but from a command line interface. The administrator can maintain all property sheets and inclusion pages for eTrust Admin objects. Property Sheets contain the properties of an object. Property pages consist of the descriptive and functional fields that make an object unique in its class. This includes the name, description, and many operational fields that control the behavior of the object. Inclusion Pages contain the inclusions of an object. Inclusions define the relationship between an object and other objects, such as a user in a user group. The Batch Utility is useful for performing repetitive tasks. Some tasks the administrator can perform with the Batch Utility are as follows: create a batch file to explore and correlate accounts on a directory, synchronize several accounts with the policy to which they are assigned, search and replace attribute values for a set of objects, create accounts for all global users, and duplicate a global user. CLI commands useful in performing administrative tasks through the Batch Utility are: ADD — Creates accounts for global users using roles or policies Creates accounts for global user groups Registers a directory in some namespaces COPY — Creates a new global user with the same properties as an existing global user, including the same roles. COPYALL — Performs the same function as the Copy verb and also copies the existing user's relationships (inclusions) to the new global user. DELETE — Deletes a global user and its relationships. EXPLORE — Finds existing objects in a registered directory and stores them in the Administrative Directory. Optionally, correlates or creates a global user in eTrust Admin for the person associated with each existing account in the directory. MASSCHANGE — Sets the same attribute values on a set of objects or searches and replaces attribute values on a set of objects. REPORT — Reports accounts that do not comply with their assigned policies. UPDATE — Synchronizes accounts with policies Suspends and resumes a global user Changes the attributes of a policy and propagates those changes to the associated accounts Deletes a global user, its relationships, and its accounts
9	AI-SM-3	*e*Trust Admin maintains the roles identified in column 1 of Table 5-3. (FMT_SMR.1) The TSF relies upon administrative profiles to define the administrative roles and privileges. *e*Trust Admin provides six default admin profiles that control the privileges of an administrator. These profiles give administrators access to the objects in their domain and all their subordinate domains. Like the default domain administrator objects, these profiles are created automatically when you install the

Security Function: Security Management Function		
Item	**Sub-function ID**	**Sub-function description**
		*e*Trust Admin Server: DomainAdministrator—This profile gives administrators full access to every object in the domain. Administrators that have this profile and manage objects in the root domain have full access to all *e*Trust Admin objects and security information. DomainAdministratorNoWeb—This profile gives administrators full access to every object in the domain, except the DAWI and the Workflow Interface. PasswordAdministrator—This profile lets administrators change passwords and activate or suspend global users. UserAdministrator—This profile lets administrators manage users in their domain. Administrators with this profile cannot modify roles or policies. ReadAdministrator—This profile lets administrators read every object in their domain. Global User—Global users can be granted self-administration privilege. Please also see Table 6-6.

Table 6-5 – Partial protection of TSF Function

Security Function: Security Management Function		
Item	**Sub-function ID**	**Sub-function description**
10	AI-PP-1	The TOE includes three physical interfaces, as has been described in AI-SM-2, 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 (listed in AI-UL-1) retrieved from the Administrative Directory. 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. In combination with the IT environment, the TOE environment ensures all information from an external client to an *e*Trust Admin Server goes through the TSF. The TSF ensures that all information must flow through the policy enforcement mechanisms. (FPT_RVM_EXP.1)

The Web interface supports a subset of the functionality supported by the Windows GUI. The security management functionality supported by the Web Interface is as follows:

Table 6-6 – Management of TSF data thru Web Interface

Subjects with profiles of the following:	Allowed Operations on TSF Data (Management Functions)	Objects:
DomainAdministrator	• Create, read, modify, rename, and delete account names. • Assign users to profiles, groups, and roles • Propagate object attribute changes to all related objects, including managed systems	• Accounts • Attributes • Groups • Policies • Roles
PasswordAdministrator	• Change passwords • Propagate object attribute changes to all related objects, including managed systems	• Attributes (Password)
UserAdministrator	(Within their assigned domain) • Create, read, modify, rename, and delete account names • Assign users to profiles and groups • Propagate object attribute changes to all related objects, including managed systems	• Accounts • Attributes • Groups
Global User	Read-only access unless self-administration capabilities have been assigned.	▪ Accounts ▪ Attributes

6.1.3 SOF Claims

The AI-UL-3 IT Security Function is realized by probabilistic or permutational mechanisms. Within AI-UL-3, the method used to provide difficult-to-guess passwords is probabilistic, as supported by AI-UL-2. The SOF claim for all IT security functions is SOF-basic.

6.2 Assurance Measures

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

Table 6-7 – Assurance Measures and How Satisfied

Item	Component ID	Component Name	How Satisfied
1	ACM_CAP.2	Configuration items	eTrust Admin v8 Configuration Items List
2	ADO_DEL.1	Delivery procedures	Distribution Centers Procedures Manual-North America Preservation of Product
3	ADO_IGS.1	Installation, generation, and start-up procedures	*e*Trust Admin Implementation Guide
4	ADV_FSP.1	Informal functional specification	Proprietary Development Specification for *e*Trust Admin v8
5	ADV_HLD.1	Descriptive high-level design	Proprietary Development Specification for *e*Trust Admin v8
6	ADV_RCR.1	Informal correspondence representation	Proprietary Development Specification for *e*Trust Admin v8
7	AGD_ADM.1	Administrator guidance	*e*Trust Admin Administrator's Guide
8	AGD_USR.1	User guidance	*e*Trust Admin Administrator's Guide *e*Trust Admin Getting Started Guide
9	ATE_COV.1	Evidence of coverage	Test Report *e*Trust Admin V8.0
10	ATE_FUN.1	Functional testing	Test Report *e*Trust Admin V8.0
11	ATE_IND.2	Independent testing - sample	TOE for testing
12	AVA_SOF.1	Strength of TOE security function evaluation	eTrust Admin Strength of Function Analysis
13	AVA_VLA.1	Developer vulnerability analysis	eTrust Admin V8.0 Vulnerability Analysis

7 PP Claims

The *e*Trust Admin Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8-1 below shows that all the identified threats to security are countered by Security Objectives for the TOE. Following the table is the rationale demonstrating that each threat is appropriately countered by Security Objectives.

Table 8-1 – All Threats to Security Countered

Item	Threat Name	Threat Description	Item	Security Objective
1	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.	1 3 4 5 1E 1N 4N	O.Access O.Attributes O.Audit O.IDAuth OE.Time ON.Install ON.Person
2	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	1 3 4 5 1E 4N 4E	O.Access O.Attributes O.Audit O.IDAuth OE.Time ON.Person OE.SecureComm
3	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.	2 6 2N 4N	O.Admin O.Roles ON.Phycal ON.Person
4	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	1 2 3 5 1N 2N 3N	O.Access O.Admin O.Attributes O.IDAuth ON.Instal ON.Phycal ON.Creden
5	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.	4 1E	O.Audit OE.Time
6	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.	3 7 4E 5E	O.Attributes O.Prop OE.SecureComm OE.Introp

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.Abuse is countered by:

- O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective counters this threat by providing that limit the actions an individual is authorized to perform.
- O.Attributes: The TOE must be able to store and maintain attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and administrative privileges.
- O.Audit: The TOE must record audit records for data accesses and use of the TOE functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
- O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- OE.Time: The IT Environment will provide reliable timestamps to the TOE. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.
- ON.Install: States the authorized administrators will configure the TOE properly.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

T.Access: An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource. T.Access is countered by:

- O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective counters this threat by providing access controls that limit the actions an individual is authorized to perform.
- O.Attributes: The TOE must be able to store and maintain attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and privileges.
- O.Audit: The TOE must record audit records for data accesses and use of the TOE functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
- O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- OE.Time: The IT Environment will provide reliable timestamps to the TOE. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
- OE.SecureComm: The IT environment will provide secure communication between TOE components and users, *e*Trust Directory, and managed systems. This objective provides protection for data during transmission.

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.Mismanage is countered by:

- O.Admin: The TOE must provide the functionality to enable authorized user(s) to effectively manage the TOE and its security functions. Administrative tools make it easier for administrators to correctly manage the TOE.
- O.Roles: The TOE must support multiple roles. Multiple roles can be used to enforce separation of duty, so that one administrator can catch errors made by another administrator.
- 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. This objective ensures that the TOE physically secure.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. This objective ensures that the TOE will be managed appropriately.

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.Privil is countered by:

- O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAuth objective by only permitting authorized users to access TOE functions.
- O.Admin: Ensures the TOE has all the necessary administrator functions to manage the product.
- O.Attributes: The TOE must be able to store and maintain attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and privileges.
- O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.
- ON.Instal: States the authorized administrators will configure the TOE properly.
- 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. This ensures that the TOE is physically secure.
- 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. This ensures that an attacker cannot steal access credentials.

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.Undetect is countered by:

- O.Audit: The TOE must record audit records for data accesses and use of the TOE functions. This objective records attempts to violate the security policy.
- OE.Time: The IT Environment will provide reliable timestamps to the TOE. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

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. T.Misuse is countered by:

- O.Attributes: The TOE must be able to maintain attributes. This objective provides that the user attributes will be maintained by the TOE.
- O. Prop: The TOE must be able to propagate object attribute changes to all related objects, including managed IT systems. This objective requires the TOE to be capable of propagating user access permissions and privileges to controlled systems in the IT environment.
- OE.SecureComm: The IT environment will provide secure communication between TOE components and users, *e*Trust Directory, and managed systems. This objective provides protection for data during transmission.
- OE.Introp: The TOE is interoperable with the IT System it manages.

8.1.2 Assumptions

The following table shows that single secure usage assumption is addressed by security objectives for either IT or Non-IT environment. Following the table is the rationale demonstrating that the assumption is addressed.

Table 8-2 – All Assumptions Addressed

Item	Name	Assumption	Item	Objective
1	A.Physec	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	2N 2E 3E	ON.Phycal OE.AuditStorage OE.Protect
2	A.Noevil	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	1N 4N 3N	ON.Instal, ON.Person, ON.Creden
3	A.ITAccess	The TOE has access to all the controlled IT Systems to perform its functions.	4E 5E	OE.SecureComm OE.Introp

A.Physec: The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. A.Physec is addressed by:

- 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. This ensures that the TOE is physically secure..
- OE.AuditStorage: The IT Environment will provide the capability to protect audit information. This provides that audit data be protected.
- OE.Protect: The IT environment will protect itself and the TOE from external interference or tampering. This provides that audit data and system data are protected.

A.Noevil: Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error. A.Noevil is addressed by:

- 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. This ensures that the TOE is properly installed and operated.

- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. This objective ensures all authorized administrators are qualified and trained to manage the TOE.

- 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. This objective supports this assumption by requiring protection of all authentication data.

A.ITAccess: The TOE has access to all the controlled IT Systems to perform its functions. A.ITAccess is addressed by:

- 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. The OE.Introp objective ensures the TOE has the needed access to the systems it manages.

8.1.3 Organizational Security Policies

The Security Target does not include any Organizational Security Policies.

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-3 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included following the table.

Table 8-3 – All Objectives Met by Functional Components

tem	Objective	Objective Description	Item	Security Functional Requirement
1	O.Access	The TOE must allow only authorized users to access appropriate TOE functions and data.	4 5 6 7 10	FIA_SOS.1 Verification of secrets FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action FMT_MTD.1 Management of TSF data FPT_RVM_EXP.1-1 Non-bypassability of the TSP: TOE
2	O.Admin	The TSF must provide all the functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security, and restrict these functions and facilities from unauthorized use.	7 8	FMT_MTD.1 Management of TSF data FMT_SMF.1-1 Specification of management functions
3	O.Attributes	The TOE must be able to maintain attributes.	3	FIA_ATD.1 User attribute definition

tem	Objective	Objective Description	Item	Security Functional Requirement
4	O.Audit	The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators.	1 2 15	FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association FPT_STM.1 Reliable time stamps
5	O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	5 6	FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action
6	O.Roles	The TOE must support multiple roles.	9	FMT_SMR.1 Security roles
7	O. Prop	The TOE must be able to propagate object attribute changes to all related objects, including managed IT systems.	3 8	FIA_ATD.1 User attribute definition FMT_SMF.1-1 Specification of management functions

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. O.Access is addressed by:

- FIA_SOS.1: Verification of secrets, which requires that the authentication mechanism must be sufficient to ensure unauthorized users cannot pose as authorized users with reasonable time, effort and other constraints.
- FIA_UAU.2: User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2: User identification before any action, which requires that users be successfully identified before allowing access to the TOE.
- FMT_MTD.1: Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FPT_RVM_EXP.1-1: Non-bypassability of the TSP: TOE, which requires TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

O.Admin: The TOE must provide the functionality to enable authorized user(s) to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FMT_MTD.1: Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FMT_SMF.1-1: Specification of management functions, which requires the TSF be capable of performing the specified security management functions.

O.Attributes: The TOE must be able to store and maintain attributes. O.Attributes is addressed by:

- FIA_ATD.1: User attribute definition, which requires that the TSF maintain security attributes of users.

O.Audit: The TOE must record audit records for data accesses and use of the TOE functions. O.Audit is addressed by:

- FAU_GEN.1: Audit data generation, which requires the ability to audit specified events.

- FAU_GEN.2: User identity association, which requires the ability to associate an auditable event with a specific user.
- FPT_STM.1: Reliable time stamps, which requires that a reliable time stamp be available to record in the audit record.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. O.IDAuth is addressed by:

- FIA_UAU.2: User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2: User identification before any action, which requires that users be successfully identified before allowing access to the TOE.

O.Roles: The TOE must support multiple roles. O.Roles is addressed by:

- FMT_SMR.1: Security roles, which requires that the TSF maintain multiple roles.

O. Prop: The TOE must be able to propagate object attribute changes to all related objects, including managed IT systems. O. Prop is addressed by:

- FIA_ATD.1: User attribute definition, which requires that the TSF maintain security attributes of users.
- FMT_SMF.1-1: Specification of management functions, which requires that the TSF be capable of performing the specified security management functions.

8.2.2 Dependencies

Table 8-4 demonstrates that all dependencies between the functional requirements are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 8-4 – TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	15
2	FAU_GEN.2	User identity association	FAU_GEN.1	1
			FIA_UID.1	6 (H)
3	FIA_ATD.1	User attribute definition	None	None
4	FIA_SOS.1	Verification of secrets	None	None
5	FIA_UAU.2	User authentication before any action	FIA_UID.1	6 (H)
6	FIA_UID.2	User identification before any action	None	None
7	FMT_MTD.1	Management of TSF data	FMT_SMF.1-1	8
			FMT_SMR.1	9
8	FMT_SMF.1-1	Specification of management functions	None	None
9	FMT_SMR.1	Security roles	FIA_UID.1	6 (H)
10	FPT_RVM_EXP.1-1	Non-bypassability of the TSP: TOE	None	None

Table 8-5 – IT Environment Dependencies are Satisfied

No	Component	Component Name	Dependencies	Reference
11	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
12	FMT_SMF.1-2	Specification of management functions	None	None
13	FPT_RVM_EXP.1-2	Non-bypassability: IT	None	None
14	FPT_SEP_EXP.1	Domain separation: IT	None	None
15	FPT_STM.1	Reliable time stamps	None	None
16	FTP_ITC_EXP.1	Inter-TSF trusted channel	None	None

8.2.3 Rationale why dependencies are not met

Dependencies for all TOE Security Requirements are met.

8.2.4 Strength of Function Rationale

Part 1 of the CC defines “strength of function” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this ST. SOF-basic states, “A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.”

The rationale for choosing SOF-basic was to be consistent with the assurance requirements included in this ST; namely the environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product, consistent with a Common Criteria Level of Evaluation of EAL2. Specifically, AVA_VLA.1 requires that the TOE be resistant to an attacker with a low to moderate attack potential, this is consistent with SOF-basic. Consequently, the metrics (password) chosen for inclusion in this ST for this TOE were determined to be acceptable for SOF-basic and would adequately protect information in a Basic Robustness Environment.

The one security function based on probabilistic methods is identified in Section 6.1.3 and applies to FIA_SOS.1 (*see* Section 5.2.2). The specific “strength” required of the methods used provide difficult-to-guess passwords. This maps to the Security Function: AI-UL-2.

8.2.5 Assurance Rationale

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the value of the information assets and the low level threat of malicious attack potential, including confidence that the TOE will not be tampered with during delivery. Violation of the security policy would cause minor damage to the security, safety, financial posture, or infrastructure of the organization. The most capable threat agents are presumed to be unsophisticated adversaries with only standard equipment and public information about the product who are willing to take little risk, e.g., unsophisticated hackers.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

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

FAU_GEN.1, Audit data generation, details auditable events generated by the TSF and consistent with the security functions claimed by the TOE. FAU_GEN.2, User identity association, associates each auditable event with the identity of the user that caused the event.

FIA_ATD.1, User attribute definition, specifies the security attributes belonging to individual users. FIA_SOS.1, Verification of secrets, supports strong authenticators. FIA_UAU.2, User authentication before any action, requires the user be identified before allowing any other TSF operations, and FIA_UID.2, User identification before any action, supports FAU_GEN.2.

FMT_MTD.1, Management of TSF data, specifies the management of TSF Data according to assigned roles. FMT_SMF.1-1, Specification of management functions, specifies the security management functions of the TSF, including propagation of user policy to the managed systems in the IT environment. FMT_SMR.1, Security roles, specifies the security roles needed to administer and support the TOE`s security functions, including the managed Global User.

FPT_RVM_EXP.1-1, Non-bypassability of the TSP: TOE, describes the security features of the TOE that prevent the TSP from being bypassed.

Installation functions (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions.

8.2.7 Explicitly Stated Requirements Rationale

The explicitly stated requirement FPT_RVM_EXP.1-1 was added because the TOE supports nonbypassability of the TOE through the TOE interfaces as described in AI-PP-1 with support from the IT environment.

The explicitly stated requirement FPT_RVM_EXP.1-2 was added to support FPT_RVM_EXP.1-1 so that the TOE's security functions cannot be bypassed in the IT environment.

The explicitly stated requirement FPT_SEP_EXP.1 was added to the IT environment because the presence of different classes of users present in the IT environment (i.e.: users of the TOE and non-users of the TOE) requires support for domain separation in the IT environment.

The explicitly stated requirement FTP_ITC_EXP.1 is needed to protect data flowing between the TOE components because the TOE is a distributed product that manages a large number of systems in the IT environment. The administrator can implement this security function in a number of ways, for example: using host to host encrypted channels, on a VPN protected by a firewall, and by physical mean such as dedicated NIC cards and physical protection of transmission lines.

8.2.8 Requirements for the IT Environment

Table 8-6 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included following the table.

Table 8-6 – All Objectives for the IT Environment map to Requirements in the IT environment

Item	Objective	Objective Description	No.	Requirement for the IT Environment	Component Name
2E	OE.AuditStorage	The IT Environment will provide the capability to protect audit information.	11	FAU_STG.1	Protected audit trail storage
5E	OE.Introp	The TOE is interoperable with the IT System it manages.	12	FMT_SMF.1-2	Specification of management functions
3E	OE.Protect	The IT environment will protect itself and the TOE from external interference or tampering.	13	FPT_RVM_EXP.1-2	Non-bypassability: IT
3E	OE.Protect	The IT environment will protect itself and the TOE from external interference or tampering.	14	FPT_SEP_EXP.1	Domain separation: IT
1E	OE.Time	The IT Environment will provide reliable timestamps to the TOE.	15	FPT_STM.1	Reliable time stamps
4E	OE.SecureComm	The IT environment will provide secure communication between TOE components and users, eTrust Directory, and managed systems.	16	FTP_ITC_EXP.1	Inter-TSF trusted channel

OE.AuditStorage: The IT Environment will provide the capability to protect audit information.
OE.AuditStorage is addressed by:

- FAU_STG.1: Protected audit trail storage, which provides that the IT environment will protect the audit trail and prevent unauthorized modification of the audit trail through the IT environment's interfaces.

OE.Introp: The TOE is interoperable with the IT System it manages. OE.Introp is addressed by:

- FMT_SMF.1-2: Specification of Management Functions, which provides that an interface will exist on managed systems in the IT environment through which the TOE can administer the list of authorised users of each controlled system by creating, deleting, and/or modifying the users along with their corresponding security attributes.

OE.Protect: The IT environment will protect itself and the TOE from external interference or tampering.
OE.Protect is addressed by:

- FPT_RVM_EXP.1-2: Non-bypassability: IT This SFR requires that the IT environment ensures that IT environment security policy enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

OE.Protect: The IT environment will protect itself and the TOE from external interference or tampering.

- FPT_SEP_EXP.1: Domain separation: IT requires that the IT environment maintain a security domain for TOE execution that protects it from interference and tampering by untrusted subjects.

OE.Time: The IT Environment will provide reliable timestamps to the TOE. OE.Time is addressed by:

- FPT_STM.1: Reliable time stamps, which requires that time stamps be provided to the TOE from the IT environment.

OE.SecureComm: The IT environment will provide secure communication between TOE components and users, *e*Trust Directory, and managed systems. OE.SecureComm is addressed by:

- FTP_ITC_EXP.1: Inter-TSF trusted channel, which requires that the IT environment protect inter-TSF communications whether by encrypted connections, behind a firewall that implements a VPN, or physical configuration of the HW.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-7 below shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-7 – Mapping of Functional Requirements to TOE Summary Specification

Item	SFRs	Description	Item	Security Function	Rationale
1	FAU_GEN.1	Audit data generation	1	AI-SA-1	Specifies the types of events to be audited. Specifies the information to be recorded in an audit record.
2	FAU_GEN.2	User identity association	2	AI-SA-2	Each auditable event is associated with the identity of the user that caused the event.
3	FIA_ATD.1	User attribute definition	3	AI-UL-1	Specifies the security attributes maintained for each user.
4	FIA_SOS.1	Verification of secrets	4	AI-UL-2	Specifies that user passwords meet the rules of the password policy.
5	FIA_UAU.2	User authentication before any action	5	AI-UL-3	Specifies that the *e*Trust Admin Administrator and User Interfaces require each user to successfully authenticate with a password before being allowed any other actions.
6	FIA_UID.2	User identification before any action	6	AI-UL-4	Specifies the *e*Trust Admin Administrator and User Interfaces require each user to identify himself/herself before being allowed to perform any other actions.
7	FMT_MTD.1	Management of TSF data	7	AI-SM-1	Specifies that *e*Trust Admin restricts the ability to access data.

Item	SFRs	Description	Item	Security Function	Rationale
8	FMT_SMF.1-1	Specification of management functions	8	AI-SM-2	Specifies the security management functions provided by *e*Trust Admin.
9	FMT_SMR.1	Security roles	9	AI-SM-3	Specifies the roles maintained.
10	FPT_RVM_EXP.1-1	Non-bypassability of the TSP: TOE	10	AI-PP-1	Specifies the implementation of the non-bypassability of the TOE security functions.

8.3.2 Assurance Measures

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

Table 8-8 – Assurance Measures Rationale

No	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.2	CM Documentation CM Proof Configuration Item List	Admin v8 Configuration Item List	CM Proof Shows the CM system is being used. Configuration Item List(s) is comprised of ▪ List of the source code files and version numbers ▪ List of design documents with version numbers ▪ Test documents with version numbers ▪ User and administrator documentation with version numbers
2	ADO_DEL.1	Delivery Procedures	Distribution Centers Procedures Manual-North America Preservation of Product	Provides a description of all procedures that are necessary to maintain security when distributing eTrust Admin software to the user's site. - Applicable across all phases of delivery from packaging, storage, distribution
3	ADO_IGS.1	Installation, generation, and start-up procedures	*e*Trust Admin Implementation Guide	Provides detailed instructions on how to install ETrust Admin.
4	ADV_FSP.1	Functional Specification	Proprietary Development Specification for *e*Trust Admin v8	Provides rationale that TSF is fully represented Describes the TSF interfaces and TOE functionality

No	Component	Evidence Requirements	How Satisfied	Rationale
5	ADV_HLD.1	High-Level Design	Proprietary Development Specification for *e*Trust Admin v8	Describes the TOE subsystems and their associated security functionality
6	ADV_RCR.1	Representation Correspondence	Proprietary Development Specification for *e*Trust Admin v8 includes correspondence analysis between: 1. TSS and functional specification; 2. functional specification and high-level design.	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design.
7	AGD_ADM.1	Administrator Guidance	*e*Trust Admin Administrator's Guide	Describes how to administer the TOE securely.
8	AGD_USR.1	User Guidance	*e*Trust Admin Administrator's Guide *e*Trust Admin Getting Started Guide	Describes the secure use of the TOE.
9	ATE_COV.1	Test Coverage Analysis	Test Report *e*Trust Admin V8.0	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
10	ATE_FUN.1	Test Documentation	Test Report *e*Trust Admin V8.0	Test documentation includes test plans and procedures and expected and actual results.
11	ATE_IND.2	TOE for Testing	Test Report *e*Trust Admin V8.0	The TOE will be provided for testing.
12	AVA_SOF.1	SOF Analysis	eTrust Admin Strength of Function Analysis	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
13	AVA_VLA.1	Vulnerability Analysis	eTrust Admin V8.0 Vulnerability Analysis	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

Appendix

Table A-1 – Acronyms

Acronym	Definition
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

Table A-2 – References

CCITSE	*Common Criteria for Information Technology Security Evaluation*, CCIMB-2004-01-002, Version 2.2, January 2004.
*e*Trust Admin Admin_Guidev8.0.pdf	*e*Trust Admin Administrator Guide v8.0
*e*Trust Admin_Dev_Guidev8.0.pdf	*e*Trust Admin Developers Guide v8.0
*e*Trust Admin_Imp_Guidev8.0.pdf	*e*Trust Admin Implementation Guide v8.0
*e*Trust Admin_Releasev8.0.pdf	*e*Trust Admin Release Notes v8.0