CA

CA Access Control r8 for Windows

Security Target

Version 2.0

Debra Baker

Dan DePrez

Michelle Ruppel

June 7, 2007

CYGNACOM
SOLUTIONS

TABLE OF CONTENTS

SECTION PAGE

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification:	CA Access Control for Windows[1] r8 with patch NT – 0604 CUMULATIVE RELEASE
ST Title:	CA Access Control r8 for Windows Security Target
ST Version:	Version 2.0
ST Authors:	Debra Baker, Dan DePrez, Michelle Ruppel
ST Date:	June 7, 2007
Assurance Level:	EAL3
Strength of Function:	Not applicable
Vendor:	CA
Vendor Address:	6150 Oak Tree Blvd, Suite 100 Park Center Plaza II Independence, OH 44131
Registration:	<To be filled in upon registration>
Keywords:	Access Control, Identification, Authentication, Authorization, Security Target, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for CA Access Control for Windows version r8 with patch NT – 0604 CUMULATIVE RELEASE[2]. CA Access Control is a security management application that regulates access to business assets by providing policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Access Control allows management of user privileges and supports deployment of security policies to control access to selected resources on native operating systems.

This document describes security aspects of the Windows version of CA Access Control only. The UNIX version of CA Access Control is the subject of a separate evaluation.

[1] Previously known as *e*Trust™ Access Control (eAC) for Windows.

[2] For brevity, this product will be called the “*e*Trust™ Access Control for Windows version r8” in the remainder of the document.

1.3 Common Criteria Conformance

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

1.4 Document Organization

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

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

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

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

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

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

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

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

Sections 9 and 10 provide the acronym definitions and references.

2 TOE Description

This section describes the Windows version of CA Access Control only. The UNIX version of CA Access Control is the subject of a separate evaluation.

2.1 Product Type

CA Access Control is a security management application that regulates access to business assets by providing policy-based control of who can access specific systems and resources, what they can do within them, and when they are allowed access. Policies can be created, managed, and distributed on an enterprise-wide basis, or customized to meet the security requirements of specific applications.

2.2 The CA Access Control approach to Security

The main security service provided by CA Access Control (ACW) is the enforcement of access controls. CA Access Control maintains information on users and the resources they can access. It provides a single interface for administrators to grant, manage, and revoke user access privileges.

Security Attributes

Records defining accessors (users of ACW controlled resources) and resources in the Access Control database can be assigned a security level, a security label and/or a security category.

Access Control List

An Access Control List (ACL) is a specific list of the accessors authorized to access a protected resource and the exact access they can have. An ACL can be used to define the access rules for a particular resource.

CA Access Control allows authorized administrators[3] to define a security policy that uses the security attributes, access control lists, and access rules to grant or deny access to selected resources for each accessor.

2.3 CA Access Control Components

CA Access Control is comprised of a database, request management software, a number of services, and an administrator interface.

2.3.1 CA *Access Control Database*

The ACW Database contains definitions of:

[3] The term “authorized administrator” in this ST includes multiple roles defined in the product. (See Table 5-12 TSF Security Roles for more detail.) Refer to Section 5.2.4 for details on roles and separation of duty.

- Users and groups of users in an organization
- System resources to be protected
- Logical resources to be protected
- Rules governing user and group access to system resources

2.3.2 CA Access Control Request Management Software

The Request Management software performs the following:

- Intercepts every request to perform a critical operating system command (such as: open/close a file, access a registry key, execute a program or terminate a process).
- Passes these requests to the ACW Authorization Engine and receives the decision of the Engine whether the request should be granted or denied.
- Forwards the decision to the original system call of the operating system, which then continues its processing based on the answer it received from the ACW kernel extension. .

2.3.3 CA Access Control Services

Watchdog

The Watchdog service performs two functions: one to keep other services running and another to perform sensitive file integrity monitoring.

The Watchdog constantly checks that the other CA Access Control services are running. If the Watchdog discovers that another service has stopped, it immediately starts it again.

The sensitive file integrity monitoring performed by Watchdog checks the signature of trusted files, which includes secured files (SECFILE class) and programs (PROGRAM class). When a difference in one of the trusted files is discovered, the Watchdog updates the ACW Authorization seos[4] Engine, marking the files as untrusted, and sends an audit record. Untrusted program files are not allowed to execute. This sensitive file integrity monitoring function is not in the evaluated configuration.

Agent

The Agent service is responsible for:

- Communicating with CA Access Control clientsT[5] through a proprietary application protocol above TCP/IP.
- Managing native security for the ACW user.

Authorization Engine (seosdT[6])

[4] seos is the previous name of the product.

[5] CA Access Control clients refer to the Policy Manager, selang, or any other 3rd party application that uses the LCA/seadmapi APIs for administration. Note that only selang is included in the TOE.

The Engine performs the following tasks:

- Manages the ACW database, including controlling all database updates.
- Decides whether to grant access requests that it has received from the Request Management software and the Agent.
- Checks that the Watchdog is running, and restarts the Watchdog if it discovers that the Watchdog has stopped running.

The Engine handles both database access requests and the decision-making function. Therefore, inter-process communication is reduced to a minimum, and maximum efficiency is achieved.

Policy Model

The Policy Model tool simplifies administration at large sites. The Policy Model allows management of many computers from one computer. The Policy Model is used with a policy model database (PMDB). Like other CA Access Control databases, the PMDB contains users, groups, protected resources, and rules governing access to the resources. In addition, the PMDB contains a list of subscriber stations. A subscriber station is one linked to the parent PMDB so that any change to the parent PMDB is automatically sent to the subscriber's database.

Using the PMDB, a baseline security policy can be created. The subscribers can include both Windows and UNIX stations, thereby ensuring uniform rules with minimal administrative efforts.

The system or security administrator updates the policy model database. The PMDB then propagates all updates from the parent policy model database to its subscribers in batch mode.

A policy model database can have two types of subscribers:

- Stations that contain a PMDB
    - The subscriber, in its role as a PMDB, also contains a list of subscribers to which it propagates database updates. This feature allows a hierarchy of PMDBs to be built.
- Stations that contain a local ACW database
    - The local ACW database can be used to protect the users, groups, and resources defined on the station on which it is located. The local database can also subscribe to a PMDB.

Note: The policy model is not in the evaluated configuration.

Task Delegation (Windows Only)

The Task Delegation service allows an administrator to grant general users the right to execute utilities and commands that require administrative privileges without being members of the

[6] seosd is the name of the on-disk executable that implements the authorization engine. seosd is a daemon which is named after the previous product name (seos).

Administrators group. The Task Delegation service is responsible for executing these privileged tasks and informing the user of the tasks outcome.

(The Task Delegation service that runs on Windows is similar to UNIX ACW utility sesudo.)

Note: The Task Delegation service is not in the evaluated configuration.

2.3.4 CA Access Control Administrator Interfaces

GUI Interface

CA Access Control has a graphical user interface through which all ACW functions are managed. This GUI is used to define users, groups, and access rules. It can also be used to monitor audit events.

Note: The GUI Interface, also known as Policy Manager, is not in the evaluated configuration.

Command Line Interface

CA Access Control can be fully managed via a command line language called selang.

2.4 Physical Boundary and Scope of the Evaluation

The evaluated configuration includes the following:

- Host Platform: CA Access Control running on Microsoft Windows 2000 Server SP4 or on Microsoft Windows XP Professional Version 2002 SP2 with a locally connected monitor/terminal ;

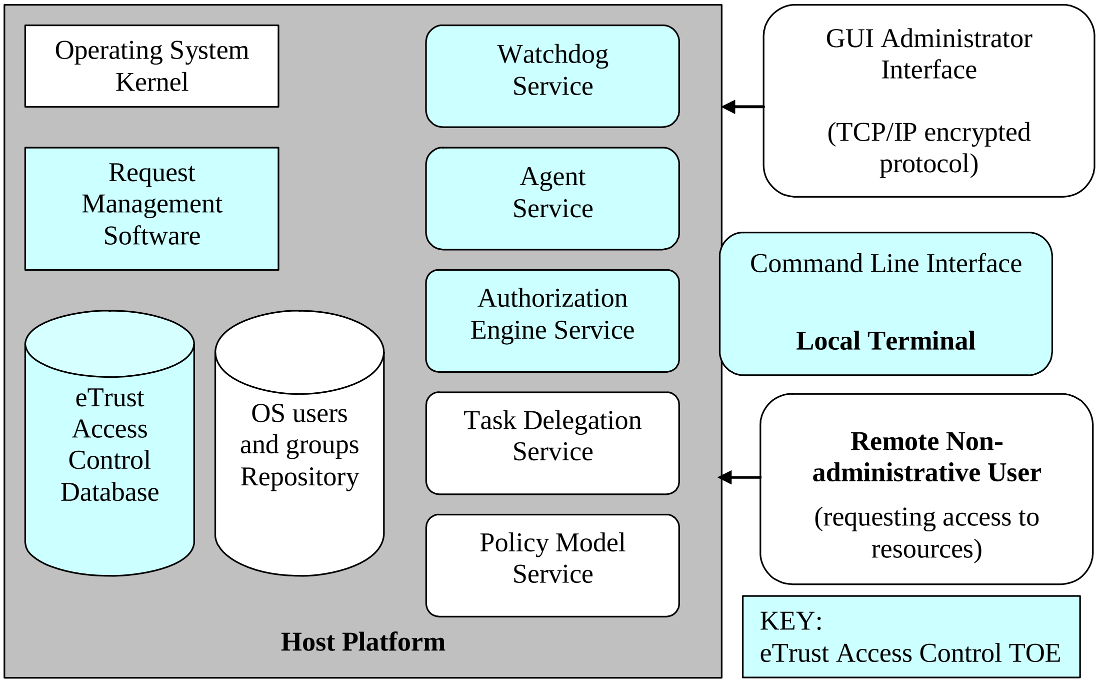
Operating System Kernel
Watchdog Service
GUI Administrator Interface
(TCP/IP encrypted protocol)
Request Management Software
Agent Service
Command Line Interface
Local Terminal
Authorization Engine Service
eTrust Access Control Database
OS users and groups Repository
Task Delegation Service
Remote Non-administrative User
(requesting access to resources)
Policy Model Service
KEY:
eTrust Access Control TOE
Host Platform

Figure 2-1 CA Access Control TOE Boundary

2.4.1 Included in TOE

The TOE encompasses the following components of the CA Access Control product:

- The ACW database (Section 2.3.1)
- The Request Management software (Section 2.3.2)
- The ACW services: (Section 2.3.3)
    - Watchdog
    - Agent
    - Authorization Engine
- The Command Line Interface for the CA environment (Section 2.3.4)
- Database classes that are stored for use of other CA applications (such as CA Single Sign-On): AGENT, AGENT_TYPE, APPL, AUTHHOST, CALENDAR, GAPPL, GAUTHHOST, RESOURCE_DESC, RESPONSE_TAB, USER_ATTR, USER_DIR, and Unicenter TNG User-Defined Classes**.** These classes, however, will not be tested in the evaluation and there are no security claims made about these classes.
- Language Client API (LCA)
- Administration API (seadmapi)
- eAC IR API. This library supplies an interface to the ACW log files.

- The accumulated group rights option must always be set in the evaluated configuration

2.4.2 Excluded from TOE

This section defines the components that are not part of the TOE. The administrator guidance informs the administrator of these exclusions. The components and features listed below require authorization to use. The administrator is trusted to not use these features in the evaluated configuration.

The following interfaces are only accessible by the administrator and the administrator is trusted to follow guidance and not use them.

- The Policy Model Tool (Section 2.3.3)
- The GUI Administrator Interface (Section 2.3.4)
- dbmgr utility (This is a maintenance utility)
- eacpg_gen utility
- Authorization and Authentication API
- Exits API
- Command Line Interface for the native Windows Environment, and Policy Model environment

Because the scope of the evaluated configuration is a standalone system, the following features are excluded.

- Concurrent logins (allowing the user login to the terminal from different machines)
- Resource Protection for TCP/IP services
- Domain based login enforcement
- Use of the _network and _interactive pre-defined groups
- Database classes that apply to this feature: CONNECT, DOMAIN, GHOST, HOST, HOSTNET, HOSTNP, MFTERMINAL, TCP.

The native operating system is not part of the CA Access Control product. CA Access Control provides methods for enhancing some of the security features of the native OS. The enforcement of these security features does not strengthen the security of the features provided by the TOE itself. Instead, it strengthens the security features implemented by the native OS. In addition, these security features require the integration of features from both CA Access Control and the native OS to provide a complete implementation

- The native Operating System of the host platform
- Native Windows Environment database classes and properties (NT environment database)
- Database classes that apply to the native operating system: ADMIN, DICTIONARY, PWPOLICY.

The following product features were not tested and are not included in the TSF:

  - Sensitive File Integrity Monitoring (Section 2.3.3)
  - The Task Delegation Service (Section 2.3.3)
  - Use of the _abspath pre-defined group
  - The ability to not set the accumulated group rights option in the evaluated configuration
  - Database classes that apply to features not included in the TOE (such as Task Delegation) or not included in the Evaluated Configuration (such as multiple hosts): GSUDO, LOGINAPPL, PROGRAM, SECFILE, SPECIALPGM, SUDO, SURROGATE, UACC, and User Defined Classes.

2.5 Logical Boundary

CA Access Control provides the following security features:

- **Resource Protection** – CA Access Control provides the ability to assign a security level for the protection of resources that include:
  - Files
  - Executables
  - Server Access
  - Privileged system commands and data
  - Terminals
  - User Accounts
- **Security Attributes** - There are several different types of security administration privileges in Access Control that allow a user the right to access a resource. Privileges are granted by:
  - Global authorization
  - User/Group authorization attributes
  - Ownership
  - Security Level
  - Access Rules
- **Security Audit** - CA Access Control (ACW) provides the ability to audit selected events. ACW also provides for the ability to search and view audit records.
- **Security Management** - CA Access Control provides security management through the use of the Administrator Interface. Through the enforcement of the CA Access Control Policy, the ability to manage various security attributes is controlled. The TOE includes three roles: Authorized Administrator, Server and User. The authorized administrator is a user with the OPERATOR, AUDITOR, or ADMIN authority. The SFRs in Section 5.2 define the capabilities of the authorized administrators.

- **TSF Protection** - ACW provides non-bypassability of the TSP and domain separation functionality.

2.6 TOE Security Environment

CA Access Control relies upon the underlying operating system platforms to provide user identification and authentication and to provide reliable time stamps.

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.Admin	The administrator is trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation and procedures developed by the organization deploying the TOE. These administrators will be trained to manage and operate the system in a secure manner.
2	A.Physical	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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 threats is unsophisticated, with access to specialized equipment and public information about the product.

The TOE must counter the threats to security described below.

Table 3-2 Threats

Item	Threat	Description
1	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.
2	T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.
3	T.Mismanage	Administrators may make errors in the management of security functions and TSF data, if administrator tools are not provided thus allowing attackers to gain unauthorized access to resources protected by the TOE.
4	T.Undetect	Attempts by an attacker to violate the CA Access Control Policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as shown below.

Table 4-1 Security Objectives for TOE

Item	Objective	Description
1	O.AccessControl	The TOE must control user access to selected resources in accordance with the set of rules defined by the CA Access Control Policy.
2	O.Admin	The TOE must provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions.
3	O.Audit	The TOE must record audit records for data accesses and use of the system functions.
4	O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
5	O.PartialDomainSep	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
6	O.Roles	The TOE must support multiple user roles.
7	O.SecurityAttr	The TOE must be able to assign, store and maintain security attributes for users and selected resources.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are shown below.

Table 4-2 Security Objectives for IT Environment

Item	Objective	Description
1E	OE.IDAuth	The IT environment must be able to identify and authenticate users prior to allowing access to the operating system of the host platform.
2E	OE.Time	The IT environment must provide reliable time stamps.
3E	OE.NonBypassSupport	The IT environment must ensure that the TOE security mechanisms cannot be bypassed in order to gain access to TOE security functions and data.
4E	OE.DomainSepSupport	The IT environment must provide an isolated domain for the execution of the TOE.

4.2.2 Non-IT Security Objectives

The Non-IT security objectives are shown below.

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

Item	Objective	Description
1N	ON.Install	Those responsible for the TOE must ensure that the TOE is delivered, installed, and configured in a manner that maintains IT security.
2N	ON.Operations	There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner.
3N	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
4N	ON.Physical	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.

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 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

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

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- 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 ***<u>italicized bold and underlined text</u>***.
- *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.*
- *NIAP Interpretations* will not be included in this ST due to Labgram 21, but *CCIMB Interpretations* will be included in the ST. CCIMB interpretations are not identified in the component name, but rather the CC text is modified to include the interpretation. The original CC text modified by the interpretation is not denoted nor explained.
- *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. All References are to the Windows Administrator Guide unless otherwise noted.

The explicitly stated requirements claimed in this ST are denoted by an additional "_XXX" extension in the unique short name for the explicit security requirement.

5.2 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1 below. The FPT_RVM_EXP.1, and FPT_SEP_EXP.1 security functional requirements are explicitly stated (based on FPT_RVM.1 and FPT_SEP.1, respectively from CC Part 2). The remaining security functional requirements are taken from Part 2 of the Common Criteria.

Table 5-1 TOE Functional Requirement

No.	Requirement	Requirement Name
1	FAU_GEN.1	Audit data generation
2	FAU_GEN.2	User identity association
3	FAU_SAR.1	Audit review
4	FAU_SAR.2	Restricted audit review
5	FAU_SAR.3	Selectable audit review
6	FAU_SEL.1	Selective audit
7	FAU_STG.1	Protected audit trail storage
8	FDP_ACC.1	Subset access control
9	FDP_ACF.1	Security attribute based access control
10	FIA_ATD.1	User attribute definition
11	FMT_MOF.1	Management of security functions behavior
12	FMT_MSA.1	Management of security attributes
13	FMT_MSA.3-1	Static attribute initialization - restrictive
14	FMT_MTD.1	Management of TSF data
15	FMT_SMF.1	Specification of Management Functions
16	FMT_SMR.1	Security roles
17	FPT_RVM_EXP.1	Partial Non-bypassability of the TSP
18	FPT_SEP_EXP.1	Partial TSF domain separation
19	FTA_TSE.1	TOE session establishment
20	FMT_MSA.3-2	Static attribute initialization - permissive

5.2.1 Class FAU: Security Audit

Table 5-2 CA Access Control Auditable Events

Database Class Type	Audit Attribute Value	Auditable Event Description
Accessor	all	All user login attempts and resource access attempts; same as including: failure, loginfail, loginsuccess, and success
	failure	Failed access attempt of ACW protected resource
	loginfail	Failed user login attempt (ACW denied the login attempt; the attempt never got to the OS)
	loginsuccess	Successful user login (ACW allowed the login attempt; the OS portion of the login is not reflected in the audit record so the OS may still deny the login attempt even though loginsuccess is audited in ACW)
	none	No user activities logged
	success	Successful access of ACW protected resource
Resource	all	All access requests for the resource; same as including: allow and deny
	allow	Authorized access request for the resource
	deny	Unauthorized access request for the resource
	none	No access requests for the resource logged

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; and

c) **[*auditable events listed in Table 5-2 CA Access Control Auditable Events*].**

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 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

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*Authorized Administrator with AUDITOR authorization*]** with the capability to read **[*all audit information*]** from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform **[*searches*]** of audit data based on **[*date, time, object identity, user identity, resource class, event type*].**

Dependencies: FAU_SAR.1 Audit review

Application Note:

- *object identity = RESOURCENAME attribute of resource record;*
- *user identity = USERNAME or GROUPNAME attribute of accessor record.*

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

[*object identity, user identity, event type*]

[*resource group membership, user group membership*].

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Application Note:

- *object identity =RESOURCENAME attribute of resource record*
- *user identity = USERNAME or GROUPNAME attribute of accessor record*
- *resource group membership = RESOURCENAME attribute of CONTAINER, GFILE, or GTERMINAL record that the resource belongs to*
- *user group membership = GROUPNAME attribute of the group record the accessor belongs to*

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **[*prevent*]** unauthorized modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the **[*CA Access Control Policy*]** on **[*Accessors and Resource Objects and Operations as listed in Table 5-3*]**.

Dependencies: FDP_ACF.1 Security attribute based access control

Table 5-3 CA Access Control Policy (Objects and Operations)

Resource Object	**Operations** **(Permitted Access Rights Values for ACL, NACL and PACL attributes)**	
FILE a specific:	all	Allows accessors to perform all operations permissible for the class.
	chdir	Allows accessors to access the directory with the equivalent of read and execute permissions.

Resource Object	**Operations** **(Permitted Access Rights Values for ACL, NACL and PACL attributes)**	
▪ file ▪ directory ▪ files that match a *file-name pattern*	chown	Allows accessors to change the owner of the file.
	control	Allows accessors all accesses except delete and rename.
	create	Allows accessors to create a file.
	delete	Allows accessors to delete a file. (ACL and PACL only)
	execute	Allows accessors to execute a program. To use this access type, the accessor must also have read access.
	none	Does not allow the accessor to perform any operations.
	read	Allows accessors to use a file or directory without changing it.
	rename	Allows an accessor to rename a file.
	sec	Allows an accessor to change the ACL of a file.
	update	Allows accessors the combination of read, write, and execute permissions.
	write	Allows an accessor to change the file or directory.
GFILE a group of: ▪ specific files ▪ specific directories ▪ files that match a *file-name pattern*	none	Does not allow the accessor to perform any operations.
	read	Allows accessors to use any file or directory in the group without changing it.
	write	Allows an accessor to change the file or directory in the group.
GTERMINAL a group of: ▪ terminals	none	Does not allow the accessor to perform any operations.
	read	Allows accessors to log in from any terminal in the group.
	write	Allows an accessor to administer CA Access Control from any terminal in the group
HOLIDAY Defines one or more periods when users need extra permission to log in	none	Does not allow the accessor to perform any operations.
	read	Allows accessors to log in during the holiday specified in the record.
PROCESS a program – executable file that runs in its own address space & needs to be protected from being killed	none	Does not allow the accessor to perform any operations
	read	Allows accessors to kill the process
REGKEY a key in the registry	all	Allows accessors to perform all operations permissible for the class.
	delete	Allows accessors to delete a Windows registry key
	none	Does not allow the accessor to perform any operations.
	read	Allows accessors to list the contents of the Windows registry key
	write	Allows an accessor to change the Windows registry key

Resource Object	**Operations** **(Permitted Access Rights Values for ACL, NACL and PACL attributes)**	
TERMINAL a terminal of the local host	none	Does not allow the accessor to perform any operations.
	read	Allows accessors to log in from the terminal .
	write	Allows an accessor to administer CA Access Control from the terminal.

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the **[*CA Access Control Policy*]** to objects based on the following: **[*Objects with attributes listed in Table 5-4 CA Access Control Policy (Security Attributes)*].**

Table 5-4 CA Access Control Policy (Security Attributes)

Object	Security Attribute	ACW Database Record Attribute
Resource Record (The File, Process, Regkey, and Terminal classes have _default object records. The use of the _default object records is included in Table 5-5. _default object records are managed the same as other resource records.)	Object Identity	RESOURCENAME
	Resource Class	CLASSNAME
	Resource Group Membership	GROUPS
	Resource Owner	OWNER
	Day and Time Restrictions	DAYTIME
	Access Control List	ACL
	Negative Access Control List	NACL
	Program Access Control List	PACL
	Default Access	UACC
	Security Category *	CATEGORY
	Security Label *	SECLABEL
	Security Level *	SECLEVEL
Accessor Record	User Identity	USERNAME
	User Group Membership	GROUPS
	Security Category	CATEGORY
	Security Label	SECLABEL
	Security Level	SECLEVEL

* The REGKEY class does not support the Security Category, Security Label or Security Level security attributes.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[rules listed in Table 5-5 CA Access Control Policy (Controlled Operation Access Rules)**) **and Table 5-6 CA Access Control Policy (Label Access Rules)].***

Table 5-5 CA Access Control Policy (Controlled Operation Access Rules)

Controlled Operation Access Rules
The following process will be followed to determine if a user is allowed to perform an operation on a resource.
Access rights will be checked in the following order:

If a record with the exact resource name is found in database:

1. Grant access if user has the OPERATOR authorization, the resource is a FILE class, and the requested access is “read”.
2. Label Access Check as described in Table 5-6
   If access is denied, stop processing. Otherwise, continue.
3. Check Resource day-time restriction
   If access is denied, stop processing. Otherwise, continue.
4. Grant access if user is owner of named resource record
5. Access Lists Check for user name in the named resource record
   If a match is found, abide by the matching permitted access rights, else continue processing.
6. Access Lists Check for user name in any of the named resource’s group records
   If a match is found, abide by the matching permitted access rights, else continue processing.
7. Access Lists Check for any of the user’s group names in the named resource record
   If a match is found, abide by the matching permitted access rights, else continue processing.
8. Access Lists Check for any of the user’s group names in any of the named resource’s group records:
   If a match is found, abide by the matching permitted access rights, else continue processing.
9. Access Lists Check for general user[7] in the named resource record:
   If a match is found, abide by the matching permitted access rights, else continue processing.
10. Access Lists Check for general user in any of the named resource’s group records
    If a match is found, abide by the matching permitted access rights, else continue processing.
11. If ACCPACL is active :
    a. Program Access Lists check for user name/program pair in the named resource.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    b. Program Access Lists check for access NONE in one of the user’s groups in the PACL.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    c. Program Access Lists check for access for the user’s groups in the PACL.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    d. Program Access Lists check for general user access in the PACL.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    e. Program Access Lists check for user name/generic program[8] pair in the named resource.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    f. Program Access Lists check for access NONE for the user’s group/generic program pair in the named resource.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    g. Program Access Lists check for access for the user’s group/generic program pair in the named resource.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    h. Program Access Lists check for access for the general user/generic program pair in the named resource.
       If a match is found, abide by the matching permitted access rights, else continue processing.
    i. Repeat a-h, checking for the Program Access List in the named resource’s group, instead of the name resource.
       If a match is found, abide by the matching permitted access rights, else continue processing.
12. Default record access check (‘defaccess’ property)

Else if generic record[9] matching the resource name is found in database: 1. Same checks as for an exact resource name, except with the generic record used in place of named resource record. Else if the resource is in the FILE or REGKEY class and a match is not found in the database and the user is in the _restricted group: Same checks as for an exact resource name, except with the _default record for FILE or REGKEY class used in place of named resource record. Else if the resource is in the TERMINAL class and if the _default object for the resource's class is found in the database: Same checks as for an exact resource name, except #1 is skipped and _default object record for the class is used in place of the named resource record. Else Grant access
The Access Lists Check will be performed in the following order: 1. Check resource record for access rights for accessor name in NACL 2. Check resource record for access rights for accessor name in ACL
If a user is a member of more than one group in an access control list: 1. If any of the access values is NONE, CA Access Control denies the user access to the resource. 2. The access control list right of a user belonging to more than one group is equal to the sum of all the access rights of the groups to which the user belongs. (NOTE: The accumulated group rights option is always set in the evaluated configuration.)

Table 5-6 CA Access Control Policy (Label Access Rules)

CA Access Label Access Rules
If CATEGORY, SECLABEL, and/or SECLEVEL classes have been activated the following rules will be applied in order:

[7] The term general user in the access rules is used to refer to an ACL entry for all users who are defined in eAC, as specified by entering an asterisk (*) for the username.

[8] The term generic program in the access rules is used to refer to program entry with wildcard patterns in the program name.

[9] The term generic record in the access rules is used to refer to a resource record with wildcard patterns in the resource name.

Security Label Check When a USER record includes a security label, the user is granted access to a resource only if both of the following are true: o The user security level specified in the security label is equal to or greater than the resource security level. o All categories specified in the resource record are included in the security category list of the user security label. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains all the security categories assigned to the resource.
Security Category Check When a user requests access to a resource that has been assigned one or more security categories ACW compares the list of security categories in the user record with the list of security categories in the resource record. If any security category in the resource record is not in the user record, ACW denies access to the resource. If the user record contains all the security categories specified in the resource record, ACW continues with other authorization checking.
Security Level Check If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[*no additional rules*].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[*no additional rules*]**.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

5.2.3 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: **[*attributes of the USER class listed in Table 5-7*].**

Dependencies: No dependencies.

Table 5-7 TSF Data (User Class Security Attributes)

User Security Attribute	Attribute Definition
AUDIT_MODE	Specifies the type of activities that Access Control records in the audit log for the user. (**event type**)
CATEGORY	One or more security categories assigned to a user.
DAYTIME	The day and time restrictions that govern when a user can access resources.
GROUPS	The list of user groups a user belongs to. This property also contains any group authorities, such as group administration authority (GROUP-ADMIN), assigned to the user for each group the user belongs to. (**user group membership**)
USERNAME	Name entered by the user when logging into the system. (**user identity**)
NOTIFY	The user notified when a resource generates an audit event.
OBJ_TYPE	Specifies the authority attributes (authorizations) of the user (ADMIN, AUDITOR, IGN_HOL, OPERATOR, SERVER).
OWNER	The user or group that is the owner of the record.
PROFILE	The profile group for the user. When the user belongs to a profile group, properties not explicitly assigned in the USER record are inherited from the profile GROUP record:
SECLABEL	The security label of a user. A security label associates a security level with security categories.
SECLEVEL	The security level of the user. The security level is a positive integer between 0 and 255.

5.2.4 Class FMT: Security Management

The CA Access Control Policy is defined by the use of the TOE security functions and the TSF data. The TSF data are the records in the CA Access Control database that define the classes and objects that enforce the TOE's purpose of providing resource protection and access control. The classes and their attributes that are included in the evaluated configuration of the TOE are listed in Table 5-7 TSF Data (User Class Security Attributes), Table 5-8 TSF Data (Group Class Security Attributes), Table 5-9 TSF Data (Resource Classes) and Table 5-10 TSF Data (Resource Class Security Attributes). The TOE security functions are those functions available to authorized users through the CA Access Control command language to act on the TSF data stored in the CA Access

Control database. The functions included in the evaluated configuration of the TOE are listed in Table 5-11 TOE Security Functions.

Table 5-8 TSF Data (Group Class Security Attributes)

Group Security Attribute	**Attribute Definition**
AUDIT_MODE	Specifies the type of activities that ACW records in the audit log for the group. (**event type**)
GROUP_MEMBER	The groups that are members of this group.
MEMBER_OF	The groups that this group is a member of. (**user group membership**)
GROUPNAME	Name of the group. (**user group identity**)
OWNER	The user or group that is the owner of the record.
SUPGROUP	The name of the parent group ("superior" group).
USERLIST	The list of users that belong to the group.

Table 5-9 TSF Data (Resource Classes)

Class		Class Attributes													
Name	**Description**	**ACL**	**CATEGORY**	**DAYTIME**	**GROUPS**	**NACL**	**NOTIFY**	**OWNER**	**PACL**	**RAUDIT**	**SECLABEL**	**SECLEVEL**	**UACC**	**WARNING**	**OTHER**
CATEGORY	Defines a security category in the database.							X							
CONTAINER	Defines a group of resource classe objects.	X		X	X	X		X	X	X				X	MEMBERS
FILE	Defines the access allowed to a specific file or directory, or to files that match a file name pattern.	X	X	X	X	X	X	X	X	X	X	X	X	X	
GFILE	Defines the access allowed to a group of specific files, specific directories, or files that match a name pattern.	X			X	X	X	X	X	X				X	MEMBERS
GTERMINAL	Defines a group of terminals.	X			X	X		X		X				X	MEMBERS
HOLIDAY	Defines one or more periods when users need extra permission to log in.	X	X		X	X	X	X		X	X	X	X	X	HOL_DATE
PROCESS	Defines a program that needs to be protected from being killed.	X	X	X	X	X	X	X	X	X	X	X	X	X	
REGKEY	Defines the tree structure of a key in the registry where Windows configuration information is saved.	X		X	X	X	X	X	X	X			X	X	
SECLABEL	Associates a security level with security categories.		X					X				X			
SEOS	The class contains only one record, called SEOS, which specifies general security and authorization options.														See Note
TERMINAL	Defines a terminal of the local host, another host on the network, or an X terminal from which a login session can be made.	X	X	X	X	X	X	X	X	X	X	X	X	X	

Application Note: The SEOS class is only used with the setoptions command to set the following SEOS modifiable attributes:

1. *CATEGORY, FILE, HOLIDAY, PROCESS, REGKEY, SECLABEL and SECLEVEL which activates or deactivates the classes of the same name.*
2. *ACCPACL which determines the order in which the attributes PACL and UACC in a resource are checked for user access.*
3. *GRACCL which determines if the accumulated group rights of users are checked. It must always be set in the evaluated configuration.*

Table 5-10 TSF Data (Resource Class Security Attributes)

Resource Security Attribute	Attribute Definition
ACL	The list of accessors (users and groups) permitted to access the resource and their access types.
CATEGORY	One or more security categories assigned to a resource.
CLASSNAME	Name of the class the resource belongs to. (**resource class**)
DAYTIME	The day and time restrictions that govern when a user can access the resource.
GROUPS	The list of GFILE, GTERMINAL or CONTAINER records a resource record belongs to. (**resource group membership**)
HOL_DATE	Specifies the period during which users cannot log in.
MEMBERS	The list of objects that are members of the group.
NACL	The list of accessors (users and groups) that are denied access to the resource and the type of access denied.
RESOURCENAME	Name of the resource. (**object identity)**
NOTIFY	The user notified when a resource generates an audit event.
OWNER	The user or group that is the owner of the record.
PACL	The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.
RAUDIT	The types of access events that CA Access Control records in the audit log.
SECLABEL	The security label of a resource. A security label associates a security level with security categories.
SECLEVEL	The security level of the user or resource. The security level is a positive integer between 0 and 255.
UACC	The default access for the resource, which indicates the access granted to accessors who are not defined to ACW or who do not appear in the ACL of the resource.
WARNING	Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Table 5-11 TOE Security Functions

Function	Function Definition	Role(s) that may use the function
selang command		
authorize	Adds or Removes accessors to a resource access control list.	o Authorized Administrator with ADMIN authorization o User with GROUP-ADMIN authorization for the group that owns the record o User specified in the OWNER attribute of the record
rmgrp	Deletes records belonging to the GROUP class from the database.	

Function	Function Definition	Role(s) that may use the function
selang command		
rmfile	Deletes resource records belonging to the FILE class from the database.	
rmres	Deletes resource records from the database.	
rmusr	Deletes records belonging to the USER class from the database.	
check	Determines if a user has access to a resource.	o Authorized Administrator with ADMIN authorization o Process with SERVER authorization
checklogin	Determines user login privileges, whether a password check is needed, and whether a terminal access check is needed.	
chfile	Modifies one or more records in the FILE class.	Modify all attributes except audit: o Authorized Administrator with ADMIN authorization o User with GROUP-ADMIN authorization for the group that owns the record o User specified in the OWNER attribute of the record Modify audit attribute only: o Authorized Administrator with AUDITOR authorization o User with GROUP-AUDITOR authorization for the group that owns the record
chgrp	Modifies one or more records in the GROUP class.	
chres	Modifies one or more records in a resource class.	

Function	Function Definition	Role(s) that may use the function
selang command		
chusr	Modifies a record in the USER class.	Modify all attributes except audit: o Authorized Administrator with ADMIN authorization Modify audit attribute only: o Authorized Administrator with AUDITOR authorization o User with GROUP-AUDITOR authorization for the group that owns the record Modify all attributes except audit and authorization: o User specified in OWNER attribute of the record o User with GROUP-ADMIN authorization for the group that owns the record • To assign a security category to the user record, the security category must appear in the owner’s user record. • To assign a security label to the user record, the security label must be assigned in the owner’s user record. • The owner of the user record can assign any security level that is less than or equal to the security level assigned in the owner’s user record.
editfile	Creates or modifies one or more records in the FILE class.	See chfile and newfile
editgrp	Creates or modifies one or more records in the GROUP class.	See chgrp and newgrp
editres	Creates or modifies one or more records in a resource class.	See chres and newres
editusr	Creates or modifies one or more records in the USER class.	See chusr and newusr
find list search	Displays classes and objects in the ACW database.	o Authorized Administrator with ADMIN, AUDITOR or OPERATOR authorization
ruler	Sets the attributes that Access Control displays for a particular class.	
join	Adds users to one or more groups, or changes their set of properties with respect to the groups.	o Authorized Administrator with ADMIN authorization
newfile	Creates a new FILE record.	
newgrp	Creates a new GROUP record.	

Function	Function Definition	Role(s) that may use the function
selang command		
newres	Defines a new resource.	
newusr	Defines a new user record.	
rename	Changes a resource name in the CA Access Control database.	o Authorized Administrator with ADMIN authorization
setoptions	Sets system-wide options related to resource protection and lists the current settings of the options.	List and Set options: o Authorized Administrator with ADMIN authorization List option only: o Authorized Administrator with AUDITOR or OPERATOR authorization
showfile	Displays the attributes of a FILE record.	o Authorized Administrator with ADMIN, AUDITOR or OPERATOR authorization o User with GROUP-ADMIN, GROUP-AUDITOR, GROUP-OPERATOR authorization for the group that owns the record or that is a parent of the group that owns the record/resource o User specified in the OWNER attribute of the record
showgrp	Displays the attributes of a GROUP record.	
showres	Displays the attributes of a resource record.	
showusr	Displays the attributes of a USER record.	
Utilities (non-selang commands)		
seaudit	Displays the CA Access Control audit log.	o Authorized Administrator with AUDITOR authority attribute
secons	Provides a control console to the CA Access Control engine. Operations include control tracing of the CA Access Control authorization engine, display run-time statistics, shutdown the CA Access Control engine and all other CA Access Control services	o –h, –m, and -refIP options are available to all users o -file, -i, -s, -t+, -t-, -tc, -ts, -tt, -tv options are available to authorized administrators with the ADMIN or OPERATOR authority attribute o –d+, -d-, -ds, -l+, -l-, -ls, –u+, -u-, -us options are not included in the scope of the evaluation.

FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to **[*determine the behavior of, disable, enable, and modify the behavior of*]** the functions **[*audit functions (see Table 5-2 CA Access Control Auditable Events)*]** to **[*Authorized Administrators with AUDITOR authorization, User with GROUP-AUDITOR authorization*]**.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the **[*CA Access Control Policy*]** to restrict the ability to **[[*function as specified in column 1 of Table 5-11*]]** the security attributes **[*attributes of the classes* as specified in Table 5-4]** to **[*roles as specified in column 3 of Table 5-11*]**.

Dependencies: [FDP_ACC.1 Subset access control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.3-1 Static attribute initialization - restrictive

Hierarchical to: No other components.

FMT_MSA.3.1-1 The TSF shall enforce the **[*discretionary access control portion of the CA Access Control Policy*[10]]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2-1 The TSF shall allow the **[*Authorized Administrator with ADMIN authorization*]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes,

FMT_SMR.1 Security roles.

FMT_MSA.3-2 Static attribute initialization - permissive

Hierarchical to: No other components.

FMT_MSA.3.1-2 The TSF shall enforce the **[daytime restrictions and label access portion of the *CA Access Control Policy*[11]]** to provide **[*permissive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2-2 The TSF shall allow the **[*Authorized Administrator with ADMIN authorization*]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes,

[10] The discretionary access control portion refers to the OWNER, GROUPS, ACL, NACL, PACL, and UACC record attributes.

[11] The daytime restrictions portion refers to the the DAYTIME record attribute. The label access portion refers to the CATEGORY, SECLABEL, and SECLEVEL record attribute.

FMT_SMR.1 Security roles.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[[*functions specified in column 1 of Table 5-11*]]** the **[*TSF Data as specified in Table 5-7, Table 5-8, Table 5-9 and Table 5-10]*** to **[*roles as specified in column 3 of Table 5-11*].**

Dependencies: FMT_SMF.1 Specification of Management Functions,

FMT_SMR.1 Security roles.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

[read and search the audit records],

[determine the behavior of, disable, enable, and modify the behavior of the audit functions], and

***[functions specified in Table 5-11]*].**

Dependencies: No Dependencies.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[*Authorized Administrator, Server, User*].**

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

Dependencies: FIA_UID.1 Timing of identification.

Table 5-12 TSF Security Roles

Security Role	**Role Definition**
Authorized Administrator	User with one or more of the following authority attribute values assigned in the OBJ_TYPE attribute of the corresponding USER record: o ADMIN o AUDITOR o OPERATOR

Security Role	Role Definition
Server	Process with the SERVER authority attribute value. A Server can: o determine if a user has access to a resource o determine user login privileges o determine whether a password check is needed o determine whether a terminal access check is needed
User	User with only the IGN_HOL authority attribute or with no authority attribute values assigned in the OBJ_TYPE attribute of the corresponding USER record. o A user may be designated in the OWNER attribute of an CA Access Control database record. The OWNER of an accessor or resource record may display or modify attributes (except for the audit attributes) of the owned record or delete the owned record. o A user may be designated as a group administrator with GROUP-ADMIN authorization. If a database record is owner by a group, the group administrator of that group has the same privileges as the owner of a record. o A user may be designated as a group auditor with GROUP-AUDITOR authorization. If a database record is owned by a group, the group auditor of that group may modify the audit attribute of that record. o A user may be designated as a group operator with GROUP-OPERATOR authorization. If a database records is owned by a group, the group operator of that group may list the attributes of that record.

5.2.5 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1 Partial Non-bypassability of the TSP

Hierarchical to: No other components.

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

Dependencies: No dependencies.

FPT_SEP_EXP.1 Partial TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2.6 Class FTA: TOE session establishment

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[*date and time*]**.

Dependencies: No dependencies.

Application Note: Users can be restricted from creating a logon session by date and time with use of the DAYTIME attribute of the USER record and further restricted by use of the HOLIDAY class.

5.3 Strength of Function

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

5.4 Security requirements for the IT Environment

The security functional requirements are listed in Table 5-13. They are all taken from Part 2 of the Common Criteria.

Table 5-13 Functional Requirement for the IT environment

No.	Component Requirement	Requirement Component Name
1E	FIA_UAU.2	User authentication before any action
2E	FIA_UID.2	User identification before any action
3E	FPT_STM.1	Reliable time stamps
4E	FPT_RVM_ENV.1	Environment Non-bypassability of the TSP
5E	FPT_SEP_ENV.1	Environment TSF Domain Separation

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 **Refinement**: The ***IT environment*** 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 **Refinement**: The ***IT environment*** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

FPT_RVM_ENV.1 Environment Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_ENV.1.1 The IT Environment shall ensure that IT Environment security policy enforcement functions are invoked and succeed before each function within the IT environment scope of control is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_ENV.1 Environment TSF Domain Separation

Hierarchical to: No other components.

FPT_SEP_ENV.1.1 The IT Environment shall maintain a security domain for the TOE's execution that protects the TOE from interference and tampering by untrusted subjects.

FPT_SEP_ENV.1.2 The IT Environment shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

5.5 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 3 (EAL3) taken from Part 3 of the Common Criteria. None of the assurance components is refined. The assurance components are listed in the table below.

Table 5-14 Assurance Requirements: EAL3

Assurance Class	Item	Assurance Requirement	
Configuration management	1	ACM_CAP.3	Authorization controls
	2	ACM_SCP.1	TOE CM coverage
Delivery and operation	3	ADO_DEL.1	Delivery procedures
	4	ADO_IGS.1	Installation, generation, and start-up procedures
Development	5	ADV_FSP.1	Informal functional specification
	6	ADV_HLD.2	Security enforcing high-level design
	7	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	8	AGD_ADM.1	Administrator guidance
	9	AGD_USR.1	User guidance
Life cycle support	10	ALC_DVS.1	Identification of security measures
Tests	11	ATE_COV.2	Analysis of coverage
	12	ATE_DPT.1	Testing: high-level design
	13	ATE_FUN.1	Functional testing
	14	ATE_IND.2	Independent testing - sample
Vulnerability assessment	15	AVA_MSU.1	Examination of guidance
	16	AVA_SOF.1	Strength of TOE security function evaluation
	17	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance requirements 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 CA Access Control TOE components. 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 this document, all CA Access Control TOE components will be mutually referred to as CA Access Control.

6.1.2 CA Access Control Security Functions

Table 6-1 Security Functional Requirements mapped to Security Functions

No.	SFR	Security Class	Security Functions	Sub-functions
1	FAU_GEN.1	Security Audit	Security Audit	AI-SA-1 AI-SA-2
2	FAU_GEN.2	Security audit	Security Audit	AI-SA-3
3	FAU_SAR.1	Security audit	Security Audit	AI-SA-4
4	FAU_SAR.2	Security audit	Security Audit	AI-SA-5
5	FAU_SAR.3	Security audit	Security Audit	AI-SA-6
6	FAU_SEL.1	Security audit	Security Audit	AI-SA-7
7	FAU_STG.1	Security audit	Security Audit	AI-SA-8
8	FDP_ACC.1	User data protection	Manage User Access	AI-MUA-1
9	FDP_ACF.1	User data protection	Manage User Access	AI-MUA-2
10	FIA_ATD.1	Identification and authentication	User Identification	AI-UI-1
11	FMT_MOF.1	Security management	Security Management	AI-SM-1
12	FMT_MSA.1	Security management	Security Management	AI-SM-2
13	FMT_MSA.3-1	Security management	Security Management	AI-SM-3
14	FMT_MTD.1	Security management	Security Management	AI-SM-4
15	FMT_SMF.1	Security management	Security Management	AI-SM-5
16	FMT_SMR.1	Security management	Security Management	AI-SM-6
17	FPT_RVM_EXP.1	Protection of the TSF	TSF Protection	AI-TP-1
18	FPT_SEP_EXP.1	Protection of the TSF	TSF Protection	AI-TP-2
19	FTA_TSE.1	TOE access	TOE Session Establishment	AI-TSE-1
20	FMT_MSA.3-2	Security management	Security Management	AI-SM-7

Table 6-2 Security Audit Function

Security Functions: Security Audit Function	
Sub-function ID	**Sub-function description**
AI-SA-1	CA Access Control will generate the following types of audit events: • Startup and shutdown of audit functions that are included with the startup and shutdown of CA Access Control • Events listed in Table 5-2 *CA* Access Control Auditable Events (FAU_GEN.1.1)
AI-SA-2	CA Access Control will record the following information for all audit events: • Date and Time of event • Event Type • User Identity • Return Code which indicates the success or failure of event • Audit Record Code that indicates the reason for the result (FAU_GEN.1.2)
AI-SA-3	CA Access Control will associate each auditable event with the identity of the user that caused the event. (FAU_GEN.2)
AI-SA-4	CA Access Control will provide the Authorized Administrator with AUDITOR authority with the capability to read all audit information in the audit records. The records will be presented in a manner suitable to interpret the information. These capabilities are provided through the use of the seaudit utility. (FAU_SAR.1)
AI-SA-5	CA Access Control will prohibit all users read access to the audit records, except those users that have been granted explicit read-access (Authorized administrators with AUDITOR authorization). (FAU_SAR.2)
AI-SA-6	CA Access Control will provide the ability to perform searches of the audit data based on: o Date and Time o User Identity (accessor record name) o Object Identity (resource record name) o Resource Class o Event Type The seaudit utility provides searching of the audit data. (FAU_SAR.3)

Security Functions: Security Audit Function	
Sub-function ID	**Sub-function description**
AI-SA-7	CA Access Control will be able to include or exclude auditable events from the set of audited events based on the attributes: o Object Identity (resource record name) o User Identity (accessor record name) o Event Type o Resource Group Membership o User Group Membership Audit events for resource class objects and groups of resource class objects can be included or excluded by setting the value of the RAUDIT attribute. Audit events for user class objects and groups of user class objects can be included or excluded by setting the values of the AUDIT_MODE attribute. (FAU_SEL.1)
AI-SA-8	CA Access Control will protect the stored audit records in the audit trail from unauthorized deletion and modification. The audit file is protected by the seos Engine. The audit log is a binary file and cannot be edited or changed. (FAU_STG.1)

Table 6-3 Manage User Access Function

Security Functions: Manage User Access Function	
Sub-function ID	**Sub-function description**
AI-MUA-1	The TSF will enforce the CA Access Control Policy on users and the resources and operations listed in Table 5-3 *CA* Access Control Policy (Objects and Operations). (FDP_ACC.1)
AI_MUA-2	The TSF will use the rules listed in Table 5-5 CA Access Control Policy (Controlled Operation Access Rules) and Table 5-6 CA Access Control Policy (Label Access Rules) to enforce the CA Access Control Policy. The _restricted group is a pre-defined group with special meaning in the access rules. This group is managed the same as the other groups. (FDP_ACF.1)

Table 6-4 User Identification Function

Security Functions: User Identification Function	
Sub-function ID	**Sub-function description**
AI-UI-1	For each user, CA Access Control will maintain the security attributes listed in Table 5-7 TSF Data (User Class Security Attributes). (FIA_ATD.1)

Table 6-5 Security Management Function

Security Functions: Security Management Function	
Sub-function ID	**Sub-function description**
AI-SM-1	CA Access Control will restrict the ability to modify and control the auditing functions to Authorized Administrators with AUDITOR authorization or users with GROUP-AUDITOR authorization. (See Table 5-2 CA Access Control Auditable Events.) (FMT_MOF.1)
AI-SM-2	CA Access Control will restrict the ability to add, display, modify and delete the security attributes of users and resources in the ACW database records. See Table 5-7 TSF Data (User Class Security Attributes), Table 5-8 TSF Data (Group Class Security Attributes), Table 5-9 TSF Data (Resource Classes), and Table 5-10 TSF Data (Resource Class Security Attributes) for a list of the ACW database classes and their security attributes. See Table 5-11 TOE Security Functions for a description of the functions and the roles that may use them. (FMT_MSA.1)
AI-SM-3	CA Access Control will provide restrictive default values for the discretionary access control security attributes listed in Table 5-4 CA Access Control Policy (Security Attributes). The default initial values of the ACL, NACL, PACL attributes are null which restricts access to resources to the owner. The default initial values of the UACC attribute are none which assigns a default access value of none. The default initial value of the GROUPS attribute is empty. The default initial value of the OWNER attribute is the user creating the resource. The Authorized Administrator with ADMIN authorization can override UACC and OWNER values when creating a new resource or user. The ACL, NACL, PACL, and GROUPS attribute initial default values cannot be changed. (FMT_MSA.3-1)
AI-SM-4	CA Access Control will restrict the ability use the command line interface functions that add, delete, modify and display the TSF Data as described in Table 5-11 TOE Security Functions. (FMT_MTD.1)
AI-SM-5	CA Access Control will provide the security management functions as defined in Table 5-11 TOE Security Functions, the ability to modify the audit functions, and the ability to read and search the audit records with the seaudit utility. (FMT_SMF.1)
AI-SM-6	CA Access Control will maintain the roles: Authorized Administrator, Server and User as defined in Table 5-12 TSF Security Roles. (FMT_SMR.1)
AI-SM-7	CA Access Control will provide permissive default values for the daytime restsrictions and label access security attributes listed in Table 5-4 CA Access Control Policy (Security Attributes). The default initial value of the daytime attribute is none which allows access to the resource at any day and time. The CATEGORY, SECLABEL, and SECLEVEL attributes are globally not activated in the TOE by default. The default initial value of the CATEGORY, SECLABEL, and SECLEVEL attributes are permissive because to restrict access they must first be connected to the resource. The Authorized Administrator with ADMIN authorization can override the values when creating a new resource or user. NOTE: Since the access control policy rules check discretionary access in addition to daytime and before label access checks, the overall resulting object access is by default restrictive. (FMT_MSA.3-2)

Table 6-6 TSF Protection Function

Security Functions: TSF Protection Function	
Sub-function ID	**Sub-function description**
AI-TP-1	CA Access Control will ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. (FPT_RVM_EXP.1)
AI-TP-2	CA Access Control will maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI. (FPT_SEP_EXP.1)

Table 6-7 TOE Session Establishment Function

Security Functions: TOE Session Establishment Function	
Sub-function ID	**Sub-function description**
AI-TSE-1	CA Access Control will be able to deny session establishment based on date and time through use of the DAYTIME attribute of a USER record and/or the HOLIDAY class. The IGN_HOL authority attribute of the USER record allows the user to login during the time defined in the HOLIDAY record. (FTA_TSE.1)

6.2 SOF Claims

There are no SOF Claims, since there are no probabilistic or permutational mechanisms included in the TOE. The AVA_SOF is vacuously satisfied when there are no applicable mechanisms and no strength is implied.

6.3 Assurance Measures

CA Access Control satisfies the assurance requirements for Evaluation Assurance Level EAL3.

The following items are provided as evaluation evidence to satisfy the EAL3 assurance requirements:

Table 6-8 Assurance Measures and How Satisfied

Item	Component	Evidence Requirements	How Satisfied
1	ACM_CAP.3	CM Plan	*e*Trust^{TM} Access Control r8 CM Plan
2	ACM_SCP.1	CM coverage	Configuration Item List
3	ADO_DEL.1	Delivery Procedures	Distribution Centers Procedures Manual United States and Canada Preservation of Product
4	ADO_IGS.1	Installation and Start-Up Procedures	*e*Trust^{TM} Access Control for Windows Administrator Guide r8 *e*Trust^{TM} Access Control for Windows Getting Started r8 CA eTrust^{TM} Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation
5	ADV_FSP.1	Informal Functional Specification	EAL3 Design Documentation CA eTrust^{TM} Access Control r8 for Windows DrvEng Engine detailed functions description
6	ADV_HLD.2	High-Level Design	EAL3 Design Documentation CA eTrust^{TM} Access Control r8 for Windows DrvEng Engine detailed functions description
7	ADV_RCR.1	Representation Correspondence	EAL3 Design Documentation CA eTrust^{TM} Access Control r8 for Windows DrvEng Engine detailed functions description
8	AGD_ADM.1	Administrator Guidance	*e*Trust^{TM} Access Control for Windows Administrator Guide r8 *e*Trust^{TM} Access Control for Windows Reference Guide r8 CA eTrust^{TM} Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation
9	AGD_USR.1	N/A	Vacuously satisifed. All users of the TOE perform an administrative function.[12]
10	ALC_DVS.1	Development Security Documentation	CA Development Security Procedures Manual
11	ATE_COV.2	Test Coverage Analysis	*e*Trust Access Control (AC) for Windows Test Cases EAL3
12	ATE_DPT.1	Depth of Testing analysis	*e*Trust Access Control (AC) for Windows Test Cases EAL3
13	ATE_FUN.1	Test Documentation	*e*Trust Access Control (AC) for Windows Test Cases EAL3 CA QA test plan documents
14	ATE_IND.2	TOE for Testing	TOE for Testing
15	AVA_MSU.1	Misuse Analysis	*e*Trust^{TM} Access Control for Windows Administrator Guide r8 *e*Trust^{TM} Access Control for Windows Reference Guide r8 CA eTrust^{TM} Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation
16	AVA_SOF.1	SOF Analysis	This ST Section 6.2
17	AVA_VLA.1	Vulnerability Analysis	*e*Trust^{TM} Access Control r8 Vulnerability Analysis

[12] Per PD0106, AGD_USR.1 is vacuously satisfied.

7 PP Claims

The CA Access Control 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 shows that all the identified threats to security are countered by Security Objectives for the TOE.

Table 8-1 All Threats to Security Countered

Item	Threat Name	Threat Description	Security Objective
1	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.	O.AccessControl O.SecurityAttr OE.IDAuth
2	T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.	O.NonBypass O.PartialDomainSep OE.NonBypassSupport OE.DomainSepSupport
3	T.Mismanage	Administrators may make errors in the management of security functions and TSF data, if administrator tools are not provided thus allowing attackers to gain unauthorized access to resources protected by the TOE.	O.Admin O.Roles
4	T.Undetect	Attempts by an attacker to violate the CA Access Control Policy may go undetected. If the attacker is successful, TSF data may be lost or altered.	O.Audit OE.Time

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.AccessControl: The TOE must control user access to selected resources in accordance with the set of rules defined by the CA Access Control Policy. This objective counters the threat by providing access controls that limit the actions an individual is authorized to perform.
- O.SecurityAttr: The TOE must be able to assign, store and maintain security attributes for users and selected resources. This objective counters the threat by providing for the attributes that associate accessors and resources with the access privileges on which the CA Access Control Policy is based.
- OE.IDAuth: The IT environment must be able to identify and authenticate users prior to allowing access to the operating system of the host platform. This objective counters the threat by providing for the identification and authentication of users prior to any user data access or TSF data access so that the CA Access Control Policy can be enforced.

T.Bypass: An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF. T.Bypass is countered by:

- O.NonBypass: The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users. The TOE will maintain separation between code executing on behalf of different users.
- OE.NonBypassSupport: The IT environment will provide an isolated domain for execution of the TOE and will ensure that the TOE security mechanisms cannot be bypassed in order to gain access to TOE security functions and data.
- OE.DomainSepSupport: The IT environment will provide an isolated domain for execution of the TOE.

T.Mismanage: Administrators may make errors in the management of security functions and TSF data, if administrator tools are not provided thus allowing 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 an authorized administrator to effectively manage the TOE and its security functions. This objective counters the threat by providing the administrative tools which make it easier for administrators to correctly manage the TOE.
- O.Roles: The TOE must support multiple user roles. This objective counters the threat by providing for multiple roles which can be used to enforce separation of duty depending on the level of training and trust of the user.

T.Undetect: Attempts by an attacker to violate the CQ Access Control Policy 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 system functions. This objective counters the threat by ensuring the recording of all security significant events, so that counter measures may be taken if there is evidence of an attack.
- OE.Time: The IT environment must provide reliable time stamps. This objective counters the threat by providing for a reliable way to correlate audit records to reconstruct a potential compromise.

8.1.2 Assumptions

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

Table 8-2 All Assumptions Addressed

Item	Name	Assumption	Objective
1	A.Admin	The administrator is trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation and procedures developed by the organization deploying the TOE. These administrators will be trained to manage and operate the system in a secure manner.	ON.Install ON.Person ON.Operations
2	A.Physical	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	ON.Physical

A.Admin: The administrator is trusted to correctly install, configure, and operate the TOE according to the instructions provided by the TOE documentation. A.Admin is covered by:

- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered, installed, and configured in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE. This objective provides for secure installation and configuration of the TOE.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective ensures that trusted personnel will be responsible for maintaining the security of the system.
- ON.Operations: There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner. The procedures will provide guidance to the administrator on how to securely operate the TOE. This objective provides for operation procedures to be in place.

A.Physical: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. A.Physical is covered by:

- ON.Physical: Those responsible for the TOE must ensure that those parts of the TOE critical to enforcing the CA Access Control Policy are protected from any physical attack. This objective provides physical security for the TOE.

Table 8-3 Mapping of Security Objectives for the Environment to Threats and Assumptions

Item	Objective Name	Threat/Policy/Assumption
1E	OE.IDAuth	T.Access
2E	OE.Time	T.Undetect
3E	OE.NonBypassSupport	T.Bypass
4E	OE.DomainSepSupport	T.Bypass

Item	Objective Name	Threat/Policy/Assumption
1N	ON.Install	A.Admin
2N	ON.Operations	A.Admin
3N	ON.Physical	A.Physical
4N	ON.Person	A.Admin

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

The table below shows that all of the security objectives of the TOE are satisfied.

Table 8-4 All Objectives Met by Functional Components

Item	Objective	Objective Description	SFR
1	O.AccessControl	The TOE must control user access to selected resources in accordance with the set of rules defined by the CA Access Control Policy.	FAU_SAR.2 FAU_STG.1 FDP_ACC.1 FDP_ACF.1 FMT_MOF.1 FTA_TSE.1
2	O.Admin	The TOE must provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions.	FAU_SAR.1 FAU_SAR.3 FMT_MTD.1 FMT_SMF.1
3	O.Audit	The TOE must record audit records for data accesses and use of the system functions.	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1
4	O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.	FPT_RVM_EXP.1
5	O.PartialDomainSep	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.	FPT_SEP_EXP.1
6	O.Roles	The TOE must support multiple user roles.	FMT_SMR.1
7	O.SecurityAttr	The TOE must be able to assign, store and maintain security attributes for users and selected resources.	FIA_ATD.1 FMT_MSA.1 FMT_MSA.3-1 FMT_MSA.3-2

O.AccessControl: The TOE must control user access to selected resources in accordance with the set of rules defined by the CA Access Control Policy. O.AccessControl is addressed by:

- FAU_SAR.2: Restricted audit review, which requires that access to the audit data be restricted to authorized users.
- FAU_STG.1: Protected audit trail storage, which requires that the audit log be protected from unauthorized deletion and modifications.
- FDP_ACC.1: Subset access control, which requires that the TSF enforce access controls on operations between subjects and objects covered by the access control SFP.
- FDP_ACF.1: Security attribute based access control, which requires the TSF enforce access controls based on specified security attributes. In addition, the TSF can explicitly authorize and deny access to specified subjects.
- FMT_MOF.1: Management of security functions behavior, which restricts the ability to disable, enable, and modify the audit functions to authorized users.
- FTA_TSE.1: TOE session establishment, which restricts the ability of users to gain access to the TOE and TOE protected resources based on date and time.

O.Admin: The TOE must provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FAU_SAR.1: Audit review, which requires that the auditor be able to read and interpret the audit records.
- FAU_SAR.3: Selectable audit review, which requires that the TSF will provide the ability to search the audit data.
- FMT_MTD.1: Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FMT_SMF.1: Specification of management functions, which requires the TSF be capable of performing the specified security management functions.

O.Audit: The TOE must record audit records for data accesses and use of the system 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.
- FAU_SEL.1: Selective audit, which requires that the TSF provide the ability to include or exclude events from the audit data depending on administrator selected attributes.

O.NonBypass: The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. O.NonBypass is addressed by:

- FPT_RVM_EXP.1: Non-bypassability of the TSP, which requires that TSP enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. O.PartialDomainSep is addressed by:

- FPT_SEP_EXP.1: TSF domain separation, which requires that the TSF protect itself from interference and tampering by attackers who gain access to the TOE through its own security interface and also requires that the TSF must protect users and processes from each other.

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

- FMT_SMR.1 Security roles, which defines the user roles that the TSF maintains.

O.SecurityAttr: The TOE must be able to assign, store and maintain security attributes for users and selected resources. O.SecurityAttr is addressed by:

- FIA_ATD.1 User attribute definition, which defines the user attributes that the TSF maintains.
- FMT_MSA.1 Management of security attributes, which defines the security attributes of users and resources in the TOE, the functions that can operate on them and the user roles that may use those functions.
- FMT_MSA.3-1 Static attribute initialization - restrictive, which requires the TSF enforce discretionary access control for specified default values of security attributes.
- FMT_MSA.3-2 Static attribute initialization - permissive, which requires the TSF enforce daytime restrictions and label access control for specified default values of security attributes.

8.2.2 Dependencies

The following tables show the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 8-5 TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	3E
2	FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1	1 2E (H)
3	FAU_SAR.1	Audit review	FAU_GEN.1	1
4	FAU_SAR.2	Restricted audit review	FAU_SAR.1	3
5	FAU_SAR.3	Selectable audit review	FAU_SAR.1	3
6	FAU_SEL.1	Selective audit	FAU_GEN.1 FMT_MTD.1	1 14
7	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
8	FDP_ACC.1	Subset access control	FDP_ACF.1	9
9	FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	8 13, 20
10	FIA_ATD.1	User attribute definition	None	None
11	FMT_MOF.1	Management of security functions behavior	FMT_SMR.1 FMT_SMF.1	16 15
12	FMT_MSA.1	Management of security attributes	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	8 16 15
13	FMT_MSA.3-1	Static attribute initialization - restrictive	FMT_MSA.1 FMT_SMR.1	12 16
14	FMT_MTD.1	Management of TSF data	FMT_SMR.1 FMT_SMF.1	16 15
15	FMT_SMF.1	Specification of management functions	None	None
16	FMT_SMR.1	Security roles	FIA_UID.1	2E (H)
17	FPT_RVM_EXP.1	Partial Non-bypassability of the TSP	None	None
18	FPT_SEP_EXP.1	Partial TSF domain separation	None	None
19	FTA_TSE.1	TOE session establishment	None	None
20	FMT_MSA.3-2	Static attribute initialization - permissive	FMT_MSA.1 FMT_SMR.1	12 16

Table 8-6 IT Environment Dependencies are Satisfied

No.	Component	Component Name	Dependencies	Reference
1E	FIA_UAU.2	User authentication before any action	FIA_UID.1	2E (H)
2E	FIA_UID.2	User identification before any action	None	None
3E	FPT_STM.1	Reliable time stamps	None	None
4E	FPT_RVM_ENV.1	Environment Non-bypassability of the TSP	None	None
5E	FPT_SEP_ENV.1	Environment TSF domain separation	None	None

8.2.3 Strength of Function Rationale

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

8.2.4 Assurance Rationale

Evaluation Assurance Level (EAL) 3 was chosen because it provides appropriate assurance measures for the expected application of the product. EAL3 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering.

8.2.5 Rationale that the 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.

For auditing, each of the SFRs build on the others. For example, FAU_SAR.1 states that the TSF shall provide authorized personnel with the capability to read all audit information from the audit records. FAU_SAR.2 builds on FAU_SAR.1 by stating the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.3 allows for easier interpretation of the audit data. FAU_STG.1 further protects the audit data from unauthorized deletion or modification. FAU_GEN.1 and FAU_GEN.2 specifies the information that will be recorded, while FAU_SEL.1 allows for the recording of only the events that are considered the most significant.

Together FDP_ACC.2 and FDP_ACF.1 provide User Data Protection by defining the CA Access Control Policy. They specify that the TSF controls user access to controlled resources based upon rules and security attributes. These requirements are supported by FIA_ATD.1 which specifies the user attributes needed to enforce the policy. User data protection is further enhanced by FTA_TSE.1 which can be used to limit when a user may log on to a TOE protected system.

The management requirements (FMT_) are related to many of the mechanisms involved with other requirements. FMT_MSA.1 enforces the CA Access Control Policy (FDP_ACC.2). These management requirements specify the security functions (FMT_SMF.1), the behavior of those functions (FMT_MOF.1), how they operate on TSF data (FMT_MTD.1, FMT_MSA.1, and FMT_MSA.2) and who may use the functions (FMT_SMR.1). In many cases, the other mechanisms will enforce the settings made through management functions. Installation mechanisms (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions.

Rationale for the protection of the TOE security functional requirements is given in Section 8.2.7.

8.2.6 Requirements for the IT Environment

The following table shows that all of the security objectives for the IT environment are satisfied.

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

Item	Objective	Objective Description	Item	IT Environment Requirement	Component Title
1E	OE.IDAuth	The IT environment must be able to identify and authenticate users prior to allowing access to the operating system of the host platform.	1E 2E	FIA_UAU.2 FIA_UID.2	User authentication before any action. User identification before any action.
2E	OE.Time	The underlying operating system must provide reliable time stamps.	3E	FPT_STM.1	Reliable time stamps
3E	OE.NonBypassSupport	The IT environment must ensure that the TOE security mechanisms cannot be bypassed in order to gain access to TOE security functions and data.	4E	FPT_RVM_ENV.1	Environment Non-bypassability of the TSP
4E	OE.DomainSepSupport	The IT environment must provide an isolated domain for the execution of the TOE.	5E	FPT_SEP_ENV.1	Environment TSF Domain Separation

OE.Time: The underlying operating system must provide reliable time stamps. OE.Time is addressed by:

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

OE.IDAuth: The IT environment must be able to identify and authenticate users prior to allowing access to the operating system of the host platform. OE.IDAuth is addressed by:

- FIA_UAU.2: User authentication before any action, which requires that the IT environment authenticate users before allowing them access to the TOE.
- FIA_UID.2: User identification before any action, which requires that the IT environment identify users before allowing them access to the TOE.

OE.DomainSepSupport: The IT environment must provide an isolated domain for the execution of the TOE. OE.DomainSepSupport is addressed by:

- FPT_SEP_ENV.1: Environment TSF Domain Separation, which requires that the IT environment provide an isolated domain for the TOE to execute within .

OE.NonBypassSupport: The IT environment must ensure that the TOE security mechanisms cannot be bypassed in order to gain access to TOE security functions and data. OE.NonBypassSupport is addressed by:

- FPT_RVM_ENV.1: Environment Non-bypassability of the TSP, which requires that the IT environment ensures that the TOE will not be bypassed.

8.2.7 Protection of the TOE Rationale

Protection of the TOE is provided by the FPT_RVM_EXP (partial non-bypassability of the TSP) and FPT_SEP_EXP (partial TSF domain separation) requirements.

CA Access Control relies upon the same functionality it uses to protect user data to protect its own program executables, files, and data structures. For example, the ACW database REGISTRY class is used to protect critical entries in the Windows Registry from unauthorized modification. Vital TSF and system services can be prevented from being killed by use of the PROCESS class. In addition, the Watchdog, Engine and Agent services provide continuous protection of the ACW services.

The CA Access Control security functions start automatically and cannot be bypassed. The security attributes of a user are checked upon session establishment. CA Access Control intercepts Windows system calls before they are processed and performs the appropriate security functionality based checks. Every request to perform a critical operating system command is intercepted and not acted upon until the CA Access Control Policy security checks have been performed and passed.

8.2.8 Explicitly Stated Security Requirements Rationale

The ST includes four explicitly stated security requirements.

FPT_SEP_EXP.1 was explicitly stated because the FPT_SEP SFR from CC Part 2 cannot be completely satisfied by an application TOE. FPT_SEP_EXP.1 defines the separation that can be performed by the TOE (applications).

FPT_RVM_EXP.1 was explicitly stated because the FPT_RVM SFR from CC Part 2 is not completely satisfied by the TOE. FPT_RVM_EXP.1 defines the non-bypassability that is performed by the TOE.

FPT_SEP_ENV.1 was explicitly stated because the FPT_SEP SFR from CC Part 2 cannot be completely satisfied by an application TOE. FPT_SEP_ENV.1 defines the separation that is performed by the IT environment.

FPT_RVM_ENV.1 was explicitly stated because the FPT_RVM SFR from CC Part 2 is not completely satisfied by the TOE. FPT_RVM_ENV.1 defines the non-bypassability that is performed by the IT environment.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

The following table shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

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

Item	Functional Component	Functional Requirement	Security Function	Rationale
1	FAU_GEN.1	Audit data generation	AI-SA-1 AI-SA-2	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	AI-SA-3	Specifies that each auditable event is associated with the identity of the user that caused the event.
3	FAU_SAR.1	Audit review	AI-SA-4	Specifies that the audit records can be read and understood.
4	FAU_SAR.2	Restricted audit review	AI-SA-5	Specifies that only specific users have read access to the audit records.
5	FAU_SAR.3	Selectable audit review	AI-SA-6	Specifies CA Access Control provides the ability to perform searches of the audit data, based on various criteria.
6	FAU_SEL.1	Selective audit	AI-SA-7	Specifies CA Access Control is able to include or exclude auditable events from the set of audited events based on designated attributes.
7	FAU_STG.1	Protected audit trail storage	AI-SA-8	Specifies that CA Access Control is able to protect the stored audit records from unauthorized deletion and prevent modifications to the audit records.
8	FDP_ACC.1	Subset access control	AI-MUA-1	Specifies the subjects, objects and operations controlled under the CA Access Control User Access Policy.
9	FDP_ACF.1	Security attribute based access control	AI-MUA-2	Specifies rules and attributes used to define the CA Access Control User Access Policy.
10	FIA_ATD.1	User attribute definition	AI-UI-1	Specifies the security attributes maintained for each user.
11	FMT_MOF.1	Management of security functions behavior	AI-SM-1	Specifies that CA Access Control restricts the ability to modify the audit functions.
12	FMT_MSA.1	Management of security attributes	AI-SM-2	Specifies that CA Access Control restricts the ability to add, delete, modify and display security attributes.
13	FMT_MSA.3-1	Static attribute initialization - restrictive	AI-SM-3	Specifies that CA Access Control provides restrictive default values for discretionary security attributes that can be overridden by authorized administrators.
14	FMT_MTD.1	Management of TSF data	AI-SM-4	Specifies that CA Access Control restricts the ability to access TSF data.
15	FMT_SMF.1	Specification of management functions	AI-SM-5	Specifies the security management functions provided by CA Access Control.

Item	Functional Component	Functional Requirement	Security Function	Rationale
16	FMT_SMR.1	Security roles	AI-SM-6	Specifies the user roles maintained by CA Access Control.
17	FPT_RVM_EXP.1	Partial Non-bypassability of the TSP	AI-TP-1	Specifies that CA Access Control ensures the CA Access Control Policy is invoked and succeeds before each function is allowed to proceed.
18	FPT_SEP_EXP.1	Partial Domain separation	AI-TP-2	Specifies CA Access Control maintains a security domain for its own execution and enforces separation between security domains of users.
19	FTA_TSE.1	TOE session establishment	AI-TSE-1	Specifies that users can be restricted from accessing the TOE by date and time.
20	FMT_MSA.3-2	Static attribute initialization – permissive	AI-SM-7	Specifies that *e*Trust^{TM} Access Control provides permissive default values for daytime restrictions and label security attributes that can be overridden by authorized administrators.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in the table below.

Table 8-9 Assurance Measures Rationale

Item	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.3	CM Plan	*e*Trust^{TM} Access Control r8 CM Plan	Describes the access controls used to control access to configuration items. Describes the roles of individuals authorized to make changes to source code configuration items.
2	ACM_SCP.1	TOE CM coverage	Configuration Item List	Lists: o source code files and version numbers o design documents with version numbers o test documents with version numbers o user and administrator documentation with version numbers
3	ADO_DEL.1	Delivery Procedures	Distribution Centers Procedures Manual United States and Canada Preservation of Product	Provides a description of all procedures that are necessary to maintain security when distributing Access Control software to the user's site. Applicable across all phases of delivery from packaging, storage, distribution.

Item	Component	Evidence Requirements	How Satisfied	Rationale
4	ADO_IGS.1	Installation, generation, and start-up procedures	*e*Trust^{TM} Access Control for Windows Administrator Guide r8 *e*Trust^{TM} Access Control for Windows Getting Started r8 CA eTrust^{TM} Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation	Provides detailed instructions on how to configure and install *e*Trust^{TM} Access Control.
5	ADV_FSP.1	Informal Functional Specification	EAL3 Design Documentation CA eTrust^{TM} Access Control r8 for Windows DrvEng Engine detailed functions description	Provides rationale that TSF is fully represented. Describes the TSF interfaces and TOE functionality.
6	ADV_HLD.2	High-Level Design	EAL3 Design Documentation CA eTrust^{TM} Access Control r8 for Windows DrvEng Engine detailed functions description	Describes the TOE subsystems and their associated security functionality.
7	ADV_RCR.1	Representation Correspondence	EAL3 Design Documentation CA eTrust^{TM} Access Control r8 for Windows v1.0 DrvEng Engine detailed functions description	Provides the following two dimensional mappings: o TSS and functional specification; o Functional specification and high-level design.
8	AGD_ADM.1	Administrator Guidance	*e*Trust^{TM} Access Control for Windows Administrator Guide r8 *e*Trust^{TM} Access Control for Windows Reference Guide r8 CA eTrust^{TM} Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation	Describes how to administer the TOE securely.
9	AGD_USR.1	User Guidance	N/A	Vacuously satisified. All users of the TOE perform an administrative function
10	ALC_DVS.1	Development Security Documentation	CA Development Security Procedures Manual	Describes the physical, procedural, personnel, and other security measures necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
11	ATE_COV.2	Test Coverage Analysis	*e*Trust Access Control (AC) for Windows Test Cases EAL3	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
12	ATE_DPT.1	Depth of Testing analysis	*e*Trust Access Control (AC) for Windows Test Cases EAL3	Demonstrates that the TSF operates in accordance with its High-Level Design.

Item	Component	Evidence Requirements	How Satisfied	Rationale
13	ATE_FUN.1	Test Documentation	*e*Trust Access Control (AC) for Windows Test Cases EAL3 CA QA test plan documents	Test documentation includes test plans and procedures and expected and actual results.
14	ATE_IND.2	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
15	AVA_MSU.1	Misuse Analysis	*e*Trust™ Access Control for Windows Administrator Guide r8 *e*Trust™ Access Control for Windows Reference Guide r8 CA eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation	The guidance documentation shall be analyzed and demonstrated to be complete.
16	AVA_SOF.1	SOF Analysis	This ST Section 6.2	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
17	AVA_VLA.1	Vulnerability Analysis	*e*Trust™ Access Control r8 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

There are no PP claims; therefore this section is not applicable.

9 Acronyms

ACL	Access Control List
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
NACL	Negative Access Control List
PACL	Program Access Control List
PMDB	Policy Model Database
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
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

10 References

CCITSE	*Common Criteria for Information Technology Security Evaluation*, CCIMB-2004-01-002, Version 2.2, January 2004.
G006581E.pdf	*e*Trust™ Access Control for Windows Administrator Guide r8
G006591E.pdf	*e*Trust™ Access Control for Windows Getting Started r8
G006611E.pdf	*e*Trust™ Access Control for Windows Reference Guide r8
G006621E.pdf	*e*Trust™ Access Control for Windows Release Summary r8