National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

CA
CA Access Control for Windows r8

Report Number: **CCEVS-VR-07-0041**
Dated: June 20, 2007
Version 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Olin Sibert, James Brosey

Common Criteria Testing Laboratory

Nancy Gow, Peter Kukura

CygnaCom Solutions (an Entrust Company)
McLean, VA

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of CA Access Control for Windows r8 was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 20 April 2007. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.2, Part 2 and Part 3, Evaluation Assurance Level (EAL 3), and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

CygnaCom Solutions is certified by the NIAP validation body for laboratory accreditation. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. The CygnaCom Security Evaluation Laboratory team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL3) have been met. This Validation Report is not an endorsement of the CA, Inc. product by any agency of the U.S. Government and no warranty of the product is either expressed or implied. The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by CygnaCom Solutions.

The Target of Evaluation (TOE) is the CA Access Control for Windows r8 with patch NT – 0604 CUMULATIVE RELEASE (ACW). The TOE is a security management application that regulates access to the assets, such as documents, executables and registry keys, stored on a computer by providing policy-based control of who can access specific resources, what they can do within them, and when they are allowed access. CA Access Control allows management of user privileges and supports deployment of security policies to control access to selected resources on native operating systems.

The TOE consists of the following software components:

- The CA Access Control for Windows r8 database
- The Request Management software
- The CA Access Control services: Watchdog, Agent, and Authorization Engine
- The Command Line Interface for the eTrust environment
- APIs: Language Client (LCA), Administration (seadmapi), and eAC IR

CA Access Control for Windows r8 provides:

- **Security Audit** - CA Access Control provides the ability to audit selected events. CA Access Control also provides for the ability to search and view audit records.
- **Resource Protection (User Data Protection)** – CA Access Control provides the ability to protect resources that include: Files, Executables, Server Access,

Privileged System Commands and Data, Terminals and User Accounts, through the definition of an Access Control Policy by the TOE Administrator.

- **Security Attributes (Identification & Authentication) -** There are several different types of security administration privileges in CA Access Control that allow a user the right to access a resource.

- **Security Management** - CA Access Control provides security management through the use of the Administrator Command Line Interface. Through the enforcement of the CA Access Control Policy, the ability to manage various security attributes is controlled.

- **TSF Protection** - CA Access Control provides non-bypassability of the TSP and domain separation functionality.

- **TOE Session Establishment** –CA Access Control limits access to the TOE though the ability to deny session establishment based on date and time.

2 IDENTIFICATION

Security Target – *CA Access Control r8 for Windows Security Target Version 2.0, dated 7 June 2007*.

TOE Identification – *CA Access Control for Windows r8 with patch NT – 0604 CUMULATIVE RELEASE.*

The Evaluated Configuration of the TOE is software only and includes the following Software Components *CA Access Control for Windows r8 with patch NT – 0604 CUMULATIVE RELEASE* running on Microsoft Windows 2000 Server SP4 or on Microsoft Windows XP Professional Version 2002 SP2 with a locally connected monitor/terminal.

The following components are included in the TOE:

- The CA Access Control database

- The Request Management software

- The CA Access Control services:

    - Watchdog

    - Agent

    - Authorization Engine

- The Command Line Interface for the eTrust environment

- Database classes that are stored for use of other CA applications (such as eTrust 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 CA Access Control log files.

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

The following software components are part of the CA Access Control product but are not evaluated as part of the TOE:

- The Policy Model Tool

- The GUI Administrator Interface

- 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.

- Concurrent logins (allowing the user login to the terminal from different machines)

- Resource Protection for TCP/IP services

- Domain based login enforcement

- Database classes that apply to this feature: CONNECT, DOMAIN, GHOST, HOST, HOSTNET, HOSTNP, MFTERMINAL, TCP.

- 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: DICTIONARY, PWPOLICY.
- Sensitive File Integrity Monitoring
- The Task Delegation Service
- Use of the _network, _interactive, and _abspath pre-defined groups
- 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): ADMIN, GSUDO, LOGINAPPL, PROGRAM, SECFILE, SPECIALPGM, SUDO, SURROGATE, UACC, and User Defined Classes.

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

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

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

Keywords - Access Control, Identification, Authentication, Authorization, Security Target, and Security Management

Note: During the course of the evaluation, the Vendor name was officially changed from Computer Associates, Inc. to CA, Inc. The name of the product was changed from eTrust Access Control to CA Access Control. Both Vendor and Evidence documentation that was written before these changes still have references to the old names.

2.1 APPLICABLE INTERPRETATIONS

The evaluation team performed an analysis of the international and national (NIAP) interpretations regarding the CC and the CEM and determined that one CCIMB interpretation applies to CC version 2.2:

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

Since FIA_USB, to which this interpretation applies, is not included in the TOE, this interpretation is not applicable to this evaluation, and there are therefore no international interpretations to consider.

2.2 IT SECURITY ENVIRONMENT

The CA Access Control for Windows r8 ST levies requirements on the TOE as well as the IT Environment. In the case of this TOE, the IT Environment includes the Operating System and the underlying hardware platforms.

The TOE relies on the environment to provide:

- User Identification and Authentication
- Non-bypassability of IT environment security functions
- Domain separation of IT environment security functions
- Reliable time stamps

2.3 OPERATING SYSTEM

The TOE was evaluated with Microsoft Windows XP Professional Version 2002 SP2 in the IT environment.

2.4 HARDWARE PLATFORM

The CA Access Control product was evaluated using the hardware platform as described in section 8 of this document.

3 SECURITY POLICY

The CA Access Control for Windows r8 TOE provides these security services:

- Security Audit
- User Data Protection
- Identification & Authentication (I&A)
- Security Management
- Protection of the TSF
- TOE Session Establishment

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

3.1 SECURITY AUDIT

CA Access Control provides multiple security audit features, including the ability to generate audit records, to read audit records, to protect audit records from unauthorized access, and to pre-select and post-select audit records. The TOE generates the following types of audit events:

- startup and shutdown of audit functions
- successful and failed user login attempts as determined by the CA Access Control security policy (the OS portion of the login success and failures are not audited by the TOE, so it is possible for CA Access Control to allow the login attempt and audit success, but the OS deny the login)
- successful and failed protected resource access attempts

Authorized administrators with the AUDITOR authority are allowed to read all information in the audit records. The *seaudit* utility presents the audit record content in a column format which can be interpreted by the administrator.

3.2 USER DATA PROTECTION

CA Access Control provides user data protection by managing user access to resources through enforcement of the CA Access Control Policy. The TOE provides the ability to assign security attributes for the protection of diverse resources that include: files, executables, server access, terminals, user accounts and privileged system commands and data.

3.3 IDENTIFICATION AND AUTHENTICATION

CA Access Control manages its users and their associated security attributes. The database maintains the records for the objects in the TOE. Accessors are user and group objects. Each user is represented by an accessor record in the data base. Each accessor object in the database belongs to a class. Users are defined by a record in the database defined by the USER class.

3.4 SECURITY MANAGEMENT

CA Access Control provides multiple security management functions to assist the users and administrators in using the product. These security management functions include the ability to manage the audit functions, to manage user and resource security attributes, to provide restrictive default values for security attributes, to control who can use the command line interface (CLI) functions which access TSF data, and to maintain roles.

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 of the Security Target define the capabilities of the authorized administrators.

3.5 PROTECTION OF THE TSF

CA Access Control includes self protection mechanisms to ensure that enforcement functions are not bypassed and to protect itself from interference and tampering from untrusted subjects via its own interfaces.

3.6 TOE SESSION ESTABLISHMENT

CA Access Control provides the ability to deny session establishment (login) based on the date and time of requested access. In the TOE, this is accomplished using the CLI to set the following security attributes:

- DAYTIME security attribute
- IGN_HOL authority attribute
- HOLIDAY class record

4 ASSUMPTIONS, THREATS AND OBJECTIVES

4.1 USAGE ASSUMPTIONS

The following table contains the assumptions regarding the security environment and the intended usage of the TOE.

Table 4-1 Assumptions

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

A.Time	It is assumed that the underlying operating system provides reliable time stamps.

4.2 POTENTIAL THREATS

The TOE must counter the threats to security described in the table below.

Table 4-2 Threats

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.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.
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.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.

4.3 SECURITY OBJECTIVES

The following table contains the TOE Security Objectives.

Table 4-3 TOE Security Objectives

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.Admin	The TOE must provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions.
O.Audit	The TOE must record audit records for data accesses and use of the system functions.
O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function 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.Roles	The TOE must support multiple user roles.
O.SecurityAttr	The TOE must be able to assign, store and maintain security attributes for users and selected resources.

The following table contains the Security Objectives for the IT Environment.

Table 4-4 Security Objectives for the IT Environment

OE.IDAuth	The IT environment must be able to identify and authenticate users prior to allowing access to IT environment functions and data.
OE.Time	The IT Environment must provide reliable time stamps.

The following table contains the Security Objectives for the Non-IT Environment.

Table 4-5 Security Objectives for the Non-IT Environment

ON.Install	Those responsible for the TOE must ensure that the TOE is delivered, installed, and configured in a manner that maintains IT security.
ON.Operations	There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner.
ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
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.

4.4 CLARIFICATION OF SCOPE

This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL3 in this case).

- This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.

- As with all EAL3 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM) or "vulnerabilities" to objectives not claimed in the ST.

The product, CA Access Control for Windows, that a customer would purchase includes more than the evaluated TOE. The evaluated TOE does not include the product components listed in Section 2 of this document. These components are used for functionality which was outside the scope of the evaluation:

- Interfaces that are only accessible by the administrator but not required for the configuration or operation of the TOE

- Features of the product used for a multi-server configuration

- Features of the product used to configure the native operating system of the server

- Features of the product used to integrate the TOE with other Vendor products

The product user should note that this evaluation started prior the adoption of new NIAP guidelines. Therefore the evaluation did not have an initial VOR nor did it undergo a Policy 10/13 review.

To use this product in the evaluated configuration, the IT environment requirements need to be addressed by the TOE administrator. Since the ACW TOE supports configurations that are outside the scope of this evaluation, the TOE administrator must remember that only the TOE Security Functions addressed by the Security Target were evaluated.

Since it was not practical to evaluate every possible configuration, the evaluation team chose a single server configuration on a typical hardware and software platform for evaluation purposes. Although the configuration of multiple instances of the ACW Server which communicate with each other is possible, the TOE was tested using only one server on which the product was installed. Features that allow an Access Control Policy to be defined on a single server and automatically pushed to other connected ACW servers were not tested or evaluated.

In the evaluated configuration, the Administrator would need to manually install and configure ACW on multiple servers if more the one server is to be used. A security policy defined on one ACW server could be manually installed on other ACW machines using scripts containing CLI commands. It should also be noted that ACW is not a

product that would be run on a single desktop or laptop. It is generally used only on servers.

CA Access Control may also be configured to work with other evaluated CA products, including eTrust Admin, eTrust Audit, and eTrust SSO. The integration of the TOE with these other products were not tested or evaluated. The end user should consult with the Vendor if such product integration is desired.

Some requirements were placed upon the configuration of the IT Environment to support the analysis and conclusions reached by this evaluation. CA Access Control for Windows r8 depends on the IT environment to provide the capability for user authentication and identification before action and reliable time stamps.

The ST provides additional information on the assumptions made and the threats countered.

5 ARCHITECTURAL INFORMATION

The Target of Evaluation (TOE) is the CA Access Control for Windows r8 with patch NT – 0604 CUMULATIVE RELEASE (ACW).

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.

ACW services start immediately after the operating system finishes its initialization. ACW places hooks in system services that must be protected. In this way, control is passed to ACW before the service is performed. ACW decides whether the service should be granted to the user.

For example, a user may attempt to access a resource protected by ACW. This access request generates a system call to the kernel to open the resource. ACW intercepts that system call and decides whether to grant access. If permission is granted, ACW passes control to the regular system service; if ACW denies permission, it returns the standard permission-denied error code to the program that activated the system call, and the system call ends.

The decision is based on access rules and policies that are defined in the ACW database. The TOE Administrator defines most of the records in the database. The database describes two types of objects: accessors and resources. Accessors are users and groups. Resources are objects to be protected, such as files and services. Each record in the database describes an accessor or a resource. Resources also belong to groups having the same access control attributes. Each object also belongs to a class—a collection of objects of the same type.

In general, the most important information contained in a resource record is the list of accessors authorized to access the resource. This list is called the access control list (ACL). Many resources contain another list of accessors, for which access is denied. This list is called the negative access control list (NACL). A third type of list is also used which allows access to the resource only via a specified program (PACL).

Each record that corresponds to a resource, group of resources or class of resources can also have an administrator defined default access.

CA Access Control provides the capability to apply security labels consisting of security levels and categories to users (subjects) and resources (objects). However, ACW does not enforce the DOD mandatory access control policy as specified in the Trusted Computer System Evaluation criteria. The TSF enforces the Bell and LaPadula simple security property of "no read up", but not the *-property of "no write down". For all operations in ACW, a user is granted access to a resource only if the user's security level is greater than or equal to the resource's security level and all categories specified in the resource record are included in the category list of the user security label. The access control policy is a discretionary access control policy rather than a mandatory access control policy. This capability is enforced through the standard ACW database classes and record attributes.

The access control algorithm that details the interaction between access control lists and database attributes to allow or deny a user’s access to a resource is specified in Section 5.2.2 of the Security Target.

The TOE consists of the following software components:

- The CA Access Control database
- The Request Management software
- The CA Access Control services:
    - Watchdog
    - Agent
    - Authorization Engine
- The Command Line Interface for the eTrust environment
- Database classes that are stored for use of other CA applications (such as eTrust 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 CA Access Control log files.
- The accumulated group rights option must always be set in the evaluated configuration

The following software components are part of the CA Access Control product but are not evaluated as part of the TOE:

- The Policy Model Tool
- The GUI Administrator Interface
- 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.
- Concurrent logins (allowing the user login to the terminal from different machines)
- Resource Protection for TCP/IP services
- Domain based login enforcement
- Database classes that apply to this feature: CONNECT, DOMAIN, GHOST, HOST, HOSTNET, HOSTNP, MFTERMINAL, TCP.
- 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: DICTIONARY, PWPOLICY.
- Sensitive File Integrity Monitoring
- The Task Delegation Service

- Use of the _network, _interactive, and _abspath pre-defined groups
- 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): ADMIN, GSUDO, LOGINAPPL, PROGRAM, SECFILE, SPECIALPGM, SUDO, SURROGATE, UACC, and User Defined Classes.

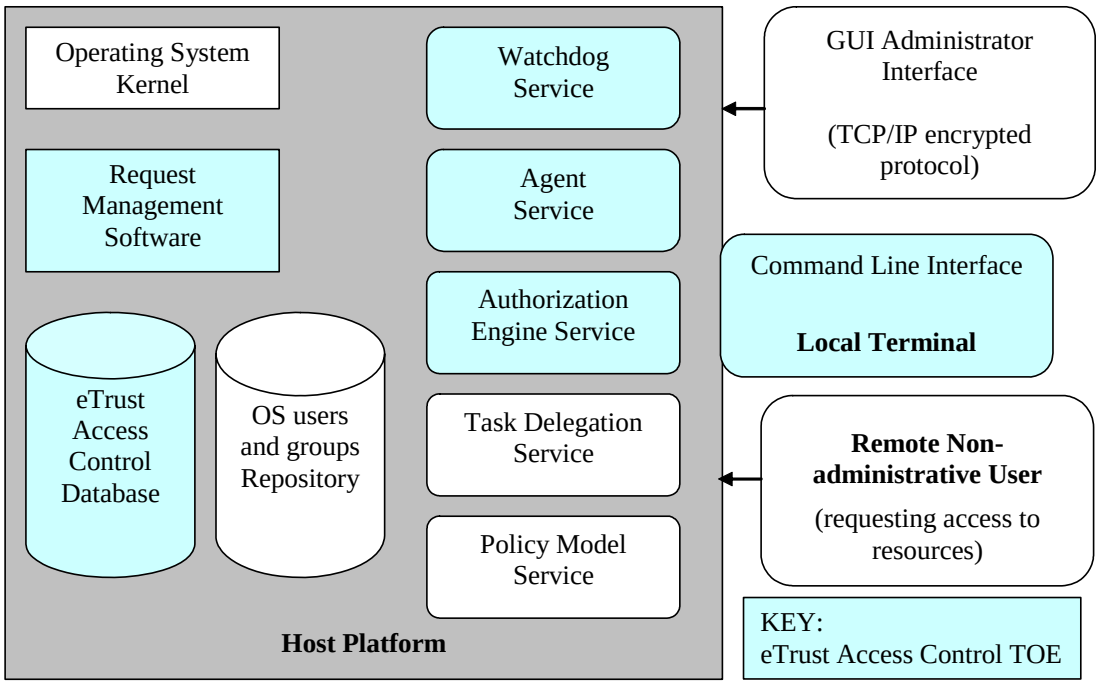

Figure 1: TOE Boundary

5.1 TOE COMPONENTS

The CA Access Control for Windows TOE (ACW) is comprised of a database, request management software, a number of services and an administrator interface.

CA Access Control Database

The ACW Database contains definitions of:

- 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

CA Access Control Request Management Software

The Request Management Software consists of two drivers:

Drveng driver

This driver intercepts requests to open/create a file, open/create a registry key, terminate a process, perform network TCP activities, perform logon events and perform impersonation activities.

Seosdrv driver

The plug-in seosdrv driver depends on the drveng driver. The seosdrv driver starts automatically when the OS starts after the drveng driver starts. The seosdrv driver passes requests received from the drveng driver to the engine service for an access control decision, receives the decision, and forwards the decision to the original operating system (OS) system call via the drveng driver. The OS system call continues processing the request based on the answer received from the drivers.

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.

CA Access Control Services

Watchdog

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.

Agent

The Agent service is responsible for:

- Communicating with ACW clients[1] through a proprietary application protocol above TCP/IP.

Authorization Engine (seosd)

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.

Command Line Interface

CA Access Control can be fully managed via a command line language called selang and a set of command line utilities.

Note: The product also includes an administration GUI which has not been evaluated. Only the administrator functions available through the CLI should be used.

5.2 SECURITY FUNCTIONAL REQUIREMENTS

Table 5-1 TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_ GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review

[1] eTrust AC 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.

FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
Class FDP: User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Class FIA: Identification & Authentication	
FIA_ATD.1	User attribute definition
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3-1	Static attribute initialization - restrictive
FMT_MSA.3-2	Static attribute initialization - permissive
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Class FPT: Protection of TSF	
FPT_RVM_EXP.1	Partial Non-bypassability of the TSP
FPT_SEP_EXP.1	Partial TSF domain separation
Class FTA: TOE session establishment	
FTA_TSE.1	TOE session establishment

Table 5-2 IT Environment Security Functional Requirements

Class FIA: Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FPT: Protection of TSF	
FPT_STM.1	Reliable time stamps
FPT_RVM_ENV.1	Environment Non-bypassability of the TSP
FPT_SEP_ENV.1	Environment TSF Domain Separation

5.3 TOE INTERFACES

This section describes and provides details for all the TOE security function interfaces (TSFIs). There are no internal interfaces for the TOE; all interfaces between the TOE subsystems are externally visible.

Callbacks

This set of interfaces includes interfaces for controlling access to files, terminals, processes, executables, and registry keys. It also includes interfaces for intercepting logon activities and driver functions.

ACW uses three different methods to intercept system calls:

File system filtering	Used to add a layer of security to the file system functions. The DrvEng driver installs itself as an upper layer filter driver to known file system drivers (FAT, NTFS, CDFS, HPFS) and receives all I/O activity for that file system. The I/O activity received includes volume mounting and file open/create/delete/read/write operations. Currently DrvEng only monitors file open/create/delete requests.
System call table modification	Used to replace system wide function pointers for functions that are being called for registry, process, and logon activities.
Targeted driver call table modification	Used to replace specific driver call table entries with ACW functions. Used to intercept TCP/IP network activity (tcp.sys). It is not included in the scope of the evaluation

When ACW determines that access is denied, it generates a denial return code that is based on the denial return code that would be produced by the system call request that was intercepted.

Callbacks are used to interface between the DrvEng driver and the Seosdrv driver which submits the callback structure to the Engine.

DrvEng Driver Interfaces

The DrvEng driver includes 2 TSF interfaces: DrvEngAttachPlugin() and DrvEngDetachPlugin(). These interfaces are used at startup by Seosdrv. However they are available for use by other processes running on the host. Both DrvEng TSFIs are available for use by any kernel mode component (driver). Therefore, privilege is required to utilize the DrvEng TSFIs.

APIs

The Agent service on the ACW server uses the Language Client API (LCA) and the Administration API to communicate with ACW clients (i.e., selang in the TOE). The eAC IR API is used by the seaudit utility to search, sort and display the ACW audit log.

Clients/Utilities

The following table identifies the ACW clients and utilities that are TSFIs. These comprise the CLI that is used as a management interface to the TOE.

TSFI	Description
seaudit	Displays the CA Access Control audit log.
secons	Provides a control console to the CA Access Control engine. Operations include control tracing of the ACW authorization engine, display run-time statistics, shutdown the CA Access Control engine and all other ACW services
selang commands in the eTrust Environment identified in ST Table 5-11.	Provides a command shell to administer CA Access Control, including providing commands for managing users, managing groups, managing resources, and other miscellaneous commands.

6 DOCUMENTATION

The following is a list of the end-user documentation that was used to support this evaluation:

- *CA eTrust™ Access Control for Windows r8 Security Target,* Version 2.0
- *eTrust™ Access Control for Windows Administrator Guide r8*, G00658-1E
- *eTrust™ Access Control for Windows Getting Started r8*, G00659-1E
- *eTrust™ Access Control for Windows Implementation Guide r8*, G00713-1E
- *eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation*
- *eTrust™ Access Control for Windows Reference Guide r8*, G00661-1E

The applicable guidance in these documents must be followed in order to operate CA Access Control for Windows r8 in its evaluated configuration.

7 IT PRODUCT TESTING

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

The purpose of the testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security

functional requirements specified in the ST. This section describes the testing efforts of the developer and the evaluation team.

Vendor testing was performed by CA Quality Assurance personnel at their sites in India and Australia.

All of the evaluation team's testing was conducted at:

CygnaCom Solutions, Inc., 7925 Jones Branch Drive, McLean VA, 22102

The evaluation team's testing was performed according to the following schedule:

11/27/06	Installation in Evaluated Configuration
11/27/06 – 12/15/06	Preliminary Execution of Developer's Functional Tests
12/06/06 – 12/08/06	Penetration (Vulnerability) Testing
12/07/06 – 12/13/06	Independent (Team-Defined) Testing
01/11/07 – 01/12/07	Preliminary Execution of Developer's Functional Tests
02/06/07 – 03/06/07	Execution of Developer's Functional Tests – Final

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

7.1 INSTALLATION TESTING

The installation was performed by the evaluation team. The Target of Evaluation was installed following the procedures defined in the following documents:

- *eTrust™ Access Control for Windows Implementation Guide r8,* G00713-1E
- *eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation*

The test installation resulted in a successful installation of the TOE in the evaluated configuration. All of the TOE components were installed correctly for the evaluated configuration by following the procedures documented. After installation, the evaluated configuration of the TOE was tested without having to change any of the configuration parameters or rerun any of the installation steps.

7.2 DEVELOPER TESTING

The developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. These test cases were mapped to SFRs, TSFIs and Sub-Systems in the test coverage document. After the test cases were defined, test procedures were written to exercise each test case. In some cases these test procedures were adapted from existing vendor quality assurance test documents. If the existing vendor test was automated, it was rewritten so that it could be run manually. If a suitable existing test document could not be found to match a test case, the vendor's quality assurance team wrote a new test procedure specifically for the CC evaluation.

All of the developer test cases were manual, i.e. all test steps including setup and cleanup steps were performed by a user entering commands at a terminal. The tests were written to use the CLI (CA Access Control command line utilities and the selang command language) to exercise the functions of the TOE. In some test cases, Windows GUI functions or DOS commands were needed, e.g. to create a text file or registry entry needed for the tests. Windows and DOS commands used in the tests were common components and no special test tools were needed.

- The developer's test procedures covered 100% of the TOE SFRs claimed in the Security Target.
- The developer's test procedures covered 100% of the external TSF interfaces.
- The developer's test procedures covered 100% of the internal subsystem interfaces.

The complete developer test procedures including test steps, expected results and the actual results obtained by the developer were provided as separate documents to the evaluation team.

The evaluation team ran a sample of the functional test procedures provided by the vendor in two phases.

Run 1

November 27, 2006 to January 12, 2007

For the first run of testing, the set of tests that were run by the evaluation team were selected to ensure that every TSFI and SFR was exercised by at least one test. In addition, all tests that exercised the access control algorithm, which is the main security feature of the product, were chosen. Tests that covered selang commands and utilities most likely to be used by an administrator in normal operation were also selected to be part of the set.

The CygnaCom evaluation team ran 35 test procedure files which corresponded to 325 of 645 test cases (approximately 50%) as documented in the test coverage document. For the first evaluator testing run, a test was considered a failure if it did not demonstrate the

security functionality of the corresponding test case or if an unrecoverable error was encountered by the evaluation team during testing.

24 of the sub-tests which had a one-to-one correspondence to the test cases were considered failures.

While the evaluation team came to the conclusion that the TOE itself exhibited the security behaviors as described in the ST, the test procedure documents did not meet the CC standards for reproducibility of results by a user with a limited knowledge of the product.

The developer was asked to correct, clean and verify the entire set of test procedure files.

Run 2

February 6, 2007 to March 6, 2007

The vendor resubmitted a corrected set of test procedure files. The evaluation team ran 17 test procedure files which corresponded to 165 of the 645 test cases (approximately 25%). The tests selected included the files which contained failures in Run1 plus a random selection of tests that had not been previously run.

For the second evaluator testing run a more stringent standard for success was applied. A test was considered a success only if the actual results obtained by the evaluator when the test was run matched the expected and actual results documented *for each test step* in that test procedure when it was run by the developer.

All of the developer functional tests run in this phase were successful. The only minor problem found was one extraneous clean-up step in one of the sub-tests. The developer test procedure documents meet the CC standards and the evaluators have confidence that the entire set of functional tests were run by the developers on the evaluated configuration of the TOE.

During testing, the parameter values used in commands were changed on an ad-hoc basis from the values documented in the developer's functional test steps. These changes did not adversely affect the behavior of the TOE.

All of the developer functional tests were run successfully. The developer test procedure documents meet the CC standards and the evaluators have confidence that the entire set of functional tests were run by the developers on the evaluated configuration of the TOE.

7.3 EVALUATION TEAM INDEPENDENT TESTING

The evaluation team devised a test subset for independent testing. The evaluation team's strategy in developing the team-defined tests of the TOE was to supplement the developer functional tests and the penetration tests. The team-defined functional tests

were devised to exercise possible areas of misuse of the TOE or vulnerabilities to the TOE that were discovered while running the developer functional and penetration tests.

All of the test cases included a purpose, explicit test steps, and an expected result. The evaluation team produced test documentation for the test subset that was sufficiently detailed to enable the tests to be reproducible. The evaluation team performed seven penetration tests:

Table 7-1 Team-Defined Tests

#	Team Defined Test	Test Description	Test Result
1	User Access when CA Access Control is Down - Utilities	The purpose of this test was to verify that only non-security related features of the CA Access Control CLI utilities (seaudit and secons) are available to a user when the CA Access Control Services are not running. The CA Access Control Services were first stopped. Then a user with ADMIN permission attempted to run the seaudit and secons utilities with a number of options.	This test proved that only non-security related features (e.g. display of the audit log) of the CA Access Control utilities are available when the services are not running.
2	User Access when CA Access Control is Down - Selang	The purpose of this test was to verify that no security related features of the CA Access Control command line interpreter (selang) are available to a user when the CA Access Control Services are not running. The CA Access Control Services were first stopped. Then a user with ADMIN permission attempted to run various selang commands with a number of options.	This test proved that no security related features (as listed in the ST) of the CA Access Control command line interpreter (selang) are available when the services are not running.
3	Holiday overrides DAYTIME restrictions	This test was written to show that the login restrictions of the HOLIDAY resource take precedence over user's login permissions using DAYTIME restrictions. It was devised as a combination of two sub-tests in the	This test successfully demonstrated that access control settings work in combination and that the restrictions of the HOLIDAY resource take precedence over a user's DAYTIME

		Developer Functional test document “Day time restrictions.doc”. The DAYTIME restrictions for a user were set to allow the user to login for the current day of the week. An instance of the HOLIDAY class was then created for the current day. The user then attempted to log in to the CA Access Control Server.	settings.
4	No Terminal Authorization	This test was designed to verify that an administrator (user with ADMIN permission) cannot successfully run selang commands without TERMINAL authorization for the CA Access Control Server. A user is created and given ADMIN authorization. The new user then logs in and tries various selang commands.	This test proved that the TERMINAL authorization step is necessary when creating a new user in an administrative role.
5	Remove Administrator	This test was designed to verify that a user with ADMIN permission can remove the system administrator from CA Access Control but not Windows. A user with ADMIN permission attempts to remove the system administrator from the CA Access Control database using selang commands.	This test proved that a user with ADMIN permission can delete the system administrator’s account from the CA Access Control database, but is unable to remove the system administrator’s Windows account using selang commands. The assumption that the administrators of the TOE are trained and trustworthy should be emphasized in the documentation.
6	Bad Input	This test was designed to verify that the selang command line interpreter will not allow bad input values to create an insecure state. An administrator attempts various selang commands, using invalid parameter values, such as: invalid date formats, unmatched quotation marks, and numeric values out of	This test showed that the selang command line interpreter will catch errors upon user input before they could cause problems for then entire TOE.

		range.	
7	Remote User File Access	The Developer Functional tests were all written to exercise the security functions of the TOE with users that login directly to the CA Access Control Server. In this test a user on a remote workstation (which has a secure connection to the server) attempts to access files that reside in a shared folder on the CA Access Control server. The user does not login to the CA Access Control server.	This test proved that the TOE applies the same access control rules to both remote and local users.

The independent test cases defined were executed by the evaluation team after the TOE was installed in the evaluated configuration consistent with the Security Target. No hardware test tools or software scripts were used during the developer functional testing.

The validation team relied on the evaluation team's report of the independent testing effort and concluded that the testing was successful.

7.4 EVALUATION TEAM PENETRATION TESTING

The penetration tests for CA Access Control for Windows r8 were developed according to the following strategy:

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

The tests for potential misuse of guidance will cover installing the TOE from guidance documentation and sampling administrator procedures.

The following public web sites were searched during the vulnerability analysis:

- Common Vulnerabilities and Exposures (CVE)
  http://www.cve.mitre.org

- National Vulnerability Database (NVD)
  http://nvd.nist.gov/

- Security Focus Vulnerability Database
  http://www.securityfocus.com/vulnerabilities

Only one vulnerability was found for the CA Access Control product and this was not applicable since it applied only to a previous version, not the evaluated version of the TOE.

CVE-2000-0762	The default installation of eTrust Access Control (formerly SeOS) uses a default encryption key, which allows remote attackers to spoof the eTrust administrator and gain privileges. This vulnerability is also described in Bugtraq ID 1583, posted on 8/11/2000.	Applies to eTrust AC 5.0 SP1, eTrust AC 5.0, eTrust AC 4.1 SP1, and eTrust AC 4.1, not eTrust AC r8.

A search of the CA Vendor documentation and customer support web sites found the following:

> *The following vulnerability was found in the eTrust™ Access Control for Windows r8 Readme G00660-1E HTML readme file found on the hard drive with the executables when the TOE is installed.*
>
> *If the host platform (eAC server) is booted in VGA mode, the system does not automatically start the eAC services when the system boots up and eAC is rendered inoperable. This is a back door used during the early stages of deployment implementation and should be disabled later.*
>
> *The vendor provides the following fix for this vulnerability:*
>
> *To disable this backdoor, define the registry value 'LockEE' of data type reg_dword under the registry key HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\eTrustAccessControl\ and set it to 1.*
>
> *The installation guidance instructs the installer to ensure that the above registry key is set.*

This potential vulnerability was the subject of the penetration test: *Close CA Access Control Services Backdoor*.

The following table lists the hypothesized vulnerabilities for CA Access Control for Windows r8. (Table created from the document: *eTrust™ Access Control r8 Vulnerability Analysis*, Section 4, Search for TOE Vulnerabilities).

Table 7-2 CA Access Control for Windows Vulnerabilities

#	Vulnerability	Description
1	Impersonation	An attacker may gain access to the administrative functions by guessing the username/password of the administrator's Windows account. This attack is mitigated by the security functionality of the IT environment as required by the FIA_UID.2 and FIA_UAU.2 requirements on the IT environment. These require each user to be successfully identified and authenticated before allowing any actions on behalf of the user.
2	TSF Data Compromise	An attacker could attempt to perform the following operations: • gain access to the audit trail and delete or modify audit records to obscure or eliminate records of resource accesses and other administrative actions • gain access to the database storing the access control rules and delete or modify the entries to allow unauthorized access to resources This vulnerability is partially mitigated by restricting access to the host platform to trusted administrators. The TOE mitigates this vulnerability by protecting the audit trail and database using its own access control features and by requiring privilege to uninstall the product.
3	Bypass Access Control Checks	An attacker could attempt to access the resources via a method that bypassed the TOE. Since the enforcement mechanisms of the TOE are integrated into the privileged mode of the kernel, only privileged users would be able to bypass the access control features provided by the TOE. The ST assumes that all administrators are trustworthy and not malicious, so this vulnerability is not exploitable in the intended environment.
4	Denial of Service	An attacker could flood the CA Access Control Server with requests for resources causing a denial of service. The ST does not claim to counter the denial of service threat, so this vulnerability is non-exploitable.

The evaluation team created a penetration test plan containing penetration tests written to determine whether hypothesized vulnerabilities are realized in the TSF. All of the test

cases included a purpose, explicit test steps, and an expected result. The evaluation team performed seven penetration tests.

Table 7-3 Penetration Tests

#	Penetration Test	Test Description	Test Result
1	Close CA Access Control Services Backdoor	CA Access Control Services start automatically upon normal boot of the Windows operating system. However, if VGA mode is selected from the boot menu, the Windows operating system boots without starting all of the CA Access Control Services, i.e. Watchdog Service, Engine Service and Service Agent. This constitutes a backdoor to the TSF. The purpose of this test is to verify that this backdoor exists, and if so, whether it can be closed by adding a modification to the eTrust Access Control Registry key in the Windows registry. The modification involves adding a value of "LockEE" to the eTrust Access Control registry key. In this test, the CA Access Control host operating system is rebooted and then the start-up state of the CA Access Control services is verified. The registry fix is applied and then the VGA boot is performed again.	This test successfully demonstrated that modifying the registry as documented above prevents a user from bypassing the access control algorithm through the Windows VGA mode at startup.
2	Disable Watchdog Service	The CA Access Control product provides a Watchdog Service (seosdw.exe) which polls the other product services to insure that they are still running. In particular, the Watchdog Service checks that the Engine Service is still running. The Engine Service (seosd.exe) performs the access control decision function within the product. In the event that Watchdog service detects that seosd.exe has stopped, it re-starts it, i.e. the Watchdog service is responsible for ensuring that the access control decision function (seosd.exe) is remains active. The purpose of this test is to determine	This test successfully demonstrated that a non-administrative user cannot disable the Watchdog Service of the CA Access Control product.

		whether the Watchdog Service can re-configured (either mistakenly or intentionally) to cease to poll status of the other services. In this scenario the user attempts to change the startup status of the service to either "manual" or disabled via the Windows Services GUI. Typically, applications installed as Windows services can be configured for the following startup modes: "automatic", "manual", "disabled." *Note: The CA Access Control system services are not intended to be configured/run in any mode other than automatic startup; and the provided secons utility is the intended administrative interface for the CA Access Control services.* In the case of "manual startup", at the next machine reboot, the Watchdog Service would not start. This would result in a situation in which the status of the CA Access Control Engine Service is not monitored. The disabled case produces the same result, except a machine reboot is not required. This test is exercised both as an ordinary user and Administrator role. A perpetrator as an ordinary user is considered to possess purposeful malicious intent. The Administrator role is considered trusted; consequently the scenarios above regarding the Administrator role involve misuse, rather than purposeful malicious intent. For this scenario, the ordinary user is a Windows user, but a user not defined within the CA Access Control system. The Administrator is the Windows Administrator.	
3	Disable CA Access Control Engine Service	The CA Access Control Engine Service (seosd.exe) performs the access control decision function within the product. The purpose of this test is to determine	This test successfully demonstrated that a non-administrative user cannot disable the Engine Service of

		whether the Engine Service can re-configured (either mistakenly or intentionally) to cease. In this scenario the user attempts to change the startup status of the service to either "manual" or disabled via the Windows Services GUI. Typically, applications installed as Windows services can be configured for the following startup modes: "automatic", "manual", "disabled." *Note: The CA Access Control system services are not intended to be configured/run in any mode other than automatic startup; and the provided secons utility is the intended administrative interface for the CA Access Control services.* In the case of "manual startup", at the next machine reboot, the CA Access Control Engine Service would not start. This would result in a situation in which the product may not properly perform the access control decision function. The disabled case produces the same result, except a machine reboot is not required. This test is exercised both as an ordinary user and Administrator role. A perpetrator as an ordinary user is considered to possess purposeful malicious intent. The Administrator role is considered trusted; consequently the scenarios above regarding the Administrator role involve misuse, rather than purposeful malicious intent. For this scenario, the ordinary user is a Windows user, but a user not defined within the CA Access Control system. The Administrator is the Windows Administrator.	the CA Access Control product.
4	Unauthorized Use of secons Shutdown	The CA Access Control product provides a utility called "secons" to perform various administrative functions, including shutdown of the	This test successfully demonstrated that an unauthorized user, even if he/she has Windows

		CA Access Control services. The purpose of this test is to determine if an unauthorized user can successfully shutdown the CA Access Control system using the product's shutdown utility, secons. In this test, an ordinary user defined within CA Access Control attempts to shutdown the CA Access Control services with the secons utility. In addition, a Windows administrative user (not defined within CA Access Control) attempts to use the secons utility to shut down CA Access Control services. *Note: As a default, in Windows administrative user can stop & start services (those whose startup type is set to non-automatic.) The CA Access Control services startup type is automatic, hence, the administrative user cannot stop CA Access Control services using Windows tools, i.e. Windows services GUI.* This test determines whether a Windows administrative user can affect a shutdown of CA Access Control services using the secons utility. It expected that the user's use of secons also prevents him/her from affecting a shutdown of the CA Access Control services. The expected outcome of this test is that the CA Access Control product prevents both the ordinary user and administrative user from executing the secons utility.	administrative privileges on the CA Access Control server, cannot shutdown the CA Access Control services using the secons utility.
5	Privilege Escalation	The purpose of this test is to determine if an authorized CA Access Control user can change his/her own security attributes to gain privileges to the system beyond those assigned by an authorized administrator.	This test successfully proved that only administrators (users with the ADMIN attribute) may increase their own security privileges. All other types of users of the TOE were unable to do so.
6	Warning Mode Set on Multiple	The purpose of this test is to determine if the WARNING mode can be set on all files of a particular type. In the event	This test proved that the access control algorithm will restrict access to an

	Files	that CA Access Control applied access controls can be bypassed by enabling the WARNING mode, can the WARNING mode be enabled on all files or all files of type *.txt.	individual file in a set of files, even if the WARNING mode was set for all files in that set.
7	Access/Modify File via DOS Commands "More", "DEL", "CACLS"	The purpose of this test is to determine if using the Windows DOS command line commands can violate the access control applied by the CA Access Control product on a Windows text file. The DOS "More" and "DEL" commands are used to attempt to gain unauthorized access to the text file, i.e. view or delete the file. User also attempts to use the DOS "CACLS" command to view and modify the Windows file ACL & grant himself/herself access.	This test proved that the access control rules cannot be bypassed through the use of DOS file manipulation commands.

The testing was performed by the evaluation team after the TOE was installed in the evaluated configuration consistent with the Security Target. No hardware test tools or software scripts were used during the penetration testing.

The validation team relied on the evaluation team's report of the penetration testing effort and concluded that the testing was successful.

8 EVALUATED CONFIGURATION

The evaluated configuration as defined in the Security Target consists of 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 ;

8.1 TEST SOFTWARE AND HARDWARE

The developer tested the TOE on three separate configurations of the TOE.

All configurations of the TOE were tested on:

- Stand-alone mode (not networked)
- Networked (CA Network)

The three OS and hardware test configurations were as follows:

- Windows 2003 Enterprise Edition SP1
    - RAM: 4GB
    - Hard Disk: 70GB
    - Processor: Dual CPU 2.40 GHz
- Windows XP Professional SP2
    - RAM: 3GB
    - Hard Disk: 110GB
    - Processor: 1 CPU 2.80 GHz
- Windows 2000 Server SP4
    - RAM: 4GB
    - Hard Disk: 70GB
    - Processor: Dual CPU 2.40 GHz

For all three configurations listed above, the software test configuration was as follows:

- CA Access Control for Windows r8 – Build 8.0.794
- Computer Associates eTrust Antivirus version 7.1.501
    - InnoculanIT Signature version 23.73.107
    - Vet Signature version 30.3.3311
- Computer Associates eTrust Pest Patrol version 5. 0. 0. 0

The CygnaCom Evaluation Laboratory's CA Access Control for Windows test configuration consisted of two machines: The CA Access Control Server and a second workstation that was used for testing remote access of the files residing on the CA Access Control Server. The two machines were configured and pre-loaded with the IT environment software before the TOE installation as follows:

CA Access Control Server (wcyg520image)

- Hardware:
    - Intel Pentium 4 Processor
    - 3.39 GHz, 2 GB of RAM

- Physical Address Extension

- Software:
  - Windows XP Professional Version 2002 SP2

Remote Access Workstation (wcygtest001)

- Hardware:
  - Intel Pentium III Processor
  - 747 MHz, 256 MB of RAM
- Software:
  - Windows XP Professional Version 2002 SP2

The two machines had a direct connection using a communications cable between the two computers.

8.2 TEST TOOLS AND SCRIPTS

No test tools were required for the Developer's functional testing or the Independent and Penetration testing. Some tests did require the use of standard Windows utilities such as regedit.

9 RESULTS OF THE EVALUATION

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

The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL3 assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence. In the Final ETR, all Fail or Inconclusive work unit verdicts have been resolved by the developer and the evaluation team.

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

- Evaluation Technical Report For a Target of Evaluation, Volume 1: Evaluation of the ST, CA eTrust™ Access Control for Windows r8

- Evaluation Technical Report For a Target of Evaluation, Volume 2: Evaluation of the TOE – EAL 3, CA eTrust™ Access Control for Windows r8

The evaluation team determined the TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL3) requirements. The rationale supporting each CEM work unit verdict is recorded in the ETR. Therefore, when configured according to the guidance documentation enumerated in section 6 of this report, the TOE is CC compliant.

The validator observations support the evaluation team's conclusion that CA Access Control for Windows r8 meet the claims stated in the Security Target.

10 VALIDATION COMMENTS/RECOMMENDATIONS

10.1 VALIDATION COMMENTS

The product, CA Access Control for Windows r8, passed all of the work units and all of the tests performed by the evaluation team. The validation team reviewed the final test report, reviewed the recommendations of the evaluation team, and was satisfied that the product performed the requirements necessary for EAL3.

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

The TOE was evaluated using a minimum configuration. Although the connection of multiple instances of the ACW Server is possible, the TOE was tested using only one server on which the product was installed. The end user should be aware that there is no guarantee of the security functions needed for a multi-server configuration.

CA Access Control may also be configured to work with other evaluated CA products, including eTrust Admin, eTrust Audit, and eTrust SSO. The integration of the TOE with these other products were not tested or evaluated. The end user should consult with the Vendor if such product integration is desired.

The product is not difficult to install. Installation of the basic product is easy following the instructions provided on the installation CD and in the *eTrust™ Access Control for Windows Implementation Guide r8.* Step-by-step instructions for downloading the patch and configuring the product to bring it into the evaluated configuration are given in *eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation*

The product is extremely flexible. Through the selang commands, the administrator can define access control rules to protect groups and classes of resources for all or groups of users. It can also provide extremely granular control of the system to protect itself and its resources by the definition of rules that protect a single resource.

Because the product is so flexible and provides various methods of protection such as access control lists, default access attributes and other security attributes, TOE administrators require training to learn the complexities of the product and the selang command language. The Vendor, CA, provides training classes for the administration of this product.

The product provides complete documentation on use and understanding the language. Once an administrator has training in the use of the product, the reference material provided in the *eTrust™ Access Control for Windows Reference Guide r8* is complete and easy to understand.

Once installed, the product is transparent to the (non-TOE) user. A user requesting access to a resource on the CA Access Control server is unaware that another layer of protection has been added to the native operating system.

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

This is a MS Windows product also includes an administration GUI which has not been evaluated. To utilize the product as a CC evaluated product, only the administrator functions available through the CLI can be used.

10.2 SIGNIFICANT FINDINGS DURING EVALUATION

As part of the evaluation, the CygnaCom Solutions, Inc SEL evaluation team discovered a vulnerability that allows the bypass of the security functionality of the TOE when booting the ACW server in VGA mode. The vulnerability is mitigated on creation of a registry key as discussed in Section 7.4 of this document. The step by step instructions for the creation of the registry key has been added to the standard instructions for the installation of the product as documented in *eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation*

Two minor bugs in the product were uncovered during testing:

- The selang check command does not work on a REGKEY resource
- The owner of the join record fails to display if the owner is a group (when joining a user to a group and viewing using the "selang showusr" command).

These two problems do not affect the security functioning of the TOE. The administrator can verify the permissions on a REGKEY resource and the owner of a join record by examining the audit record. The vendor is aware of these problems and will correct them in future versions of the product. The evaluation team recommended that the user should be made aware of the bugs and how to work around them in the *eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation.*

The following additional observations were made during testing and the evaluation team recommended that the following be added to the *eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation* to prevent any possible misuse of the TOE:

- The user password is entered in plain-text when creating or editing a user account with the selang commands. The administrator should take care that the user passwords are not observed during entry or if used in a command batch file.
- The eTrust environment selang commands do not affect the settings in the Windows environment. Likewise, the Windows environment selang commands that are used to administer the Windows environment and do not change the settings in the eTrust environment. For example, to rename a user's name in Windows, the administrator must use either selang (nt) or use the standard Windows interface directly to change the username for Windows. Exceptions are the newusr and rmusr commands. The newusr command will add a user account to Windows, if one does not already exist for that user name. The rmusr command with the parameter "native" will delete the user account both from Windows and CA Access Control.

- The selang commands are case-insensitive except for the user password. For example: FileA.txt, FILEA.txt and filea.txt are interchangeable in selang.

- Any user given the "ADMIN" attribute has complete use of all selang commands including the ability to escalate his/her own privileges (such as increase the SECLEVEL, add other attributes to his/her account, remove any DAYTIME restrictions, …) and can remove all other user accounts from CA Access Control including that of the System Administrator. The assumption that TOE administrators are trustworthy and well-trained should be emphasized.

10.3 VALIDATION RECOMMENDATIONS

The validation team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The validation team agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 3 of the ETR, volume 1, and section 4 of the ETR, volume 2. The Validation team also agrees with the Recommendation and Conclusions presented in Section 4 of the ETR, volume 1 and Section 5 of the ETR, volume 2. The validation team, therefore, concludes that the evaluation and Pass result for this TOE are complete and correct for CA Access Control for Windows r8 with patch NT – 0604 CUMULATIVE RELEASE.

11 LIST OF ACRONYMS

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

12 BIBLIOGRAPHY

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

- *Common Criteria for Information Technology Security Evaluation*, version 2.2, January 2004, Part 1.
- *Common Criteria for Information Technology Security Evaluation*, version 2.2, January 2004, Part 2.
- *Common Criteria for Information Technology Security Evaluation*, version 2.2, January 2004, Part 3.

- *Common Evaluation Methodology for Information Technology Security*, version 2.2, January 2004.

- CA *Access Control for Windows r8 Security Target*, version 2.0

- *Evaluation Technical Report For a Target of Evaluation, Volume 1: Evaluation of the ST, CA eTrust ™ Access Control for Windows r8*

- *Evaluation Technical Report For a Target of Evaluation, Volume 2: Evaluation of the TOE – EAL 3, CA eTrust ™ Access Control for Windows r8*

- *Evaluator Test Plan and Report EAL3 Evaluation CA eTrust™ Access Control for Windows r8*

- *eTrust™ Access Control for Windows Implementation Guide r8, G00713-1E*

- *eTrust™ Access Control for Windows r8 Common Criteria Supplement to the Guidance Documentation*

- *eTrust™ Access Control for Windows Reference Guide r8, G00661-1E*