National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

CA

*e*Trust™ Security Command Center™ Version 8 SP 1 with CR2 Patch

Report Number: **CCEVS-VR-07-0004**

Dated: January 26, 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

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

Common Criteria Testing Laboratory

Mossadeq Zia

CygnaCom Solutions (an Entrust Company)
McLean, VA

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of the CA, Inc. product ***e*****Trust™ Security Command Center™ Version 8 SP 1 with CR2 Patch** was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 25 January 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 2), and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

CygnaCom Solutions is certified by the NIAP validation body for laboratory accreditation. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. The CygnaCom Security Evaluation Laboratory team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met. This Validation Report is not an endorsement of the 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 a subset of the CA product ***e*****Trust™ Security Command Center™ Version 8 SP 1 with CR2 Patch (SCC)**. The TOE consists of the following software components:

- *e*Trust SCC Server
- *e*Trust Audit Policy Manager
- Audit Data Tools

The *e*Trust SCC product components not in the TOE are:

- *e*Trust Audit Client
- *e*Trust SCC Agent
- Product Integration Kits (PIKs)

Even though many of the components of *e*Trust SCC are similar to *e*Trust Audit, the previous evaluation of *e*Trust Audit is irrelevant to this TOE because the *e*Trust Audit components used in this evaluation are different versions. Since the versions are different, the previous NIAP certification does not apply. *e*Trust SCC contains all of the required components for this TOE. Purchasing a separate *e*Trust Audit Product order is not required. A trained administrator will install the TOE using *e*Trust SCC installation guide found in the SCC delivered product. Should there be additional Audit Clients installed in the environment from the previous versions, the TOE will not automatically discover them and integrate them as nodes managed by the TOE. The trained administrator will only integrate the correct version of the *e*Trust Audit Client into the TOE.

eTrust SCC provides the capabilities to:

- Collect security event and audit data from a wide range of sources throughout an enterprise and allows the data to be analyzed and managed at a centralized location
- Create and manage a centralized policy regarding the retention of audit information
- Manage remote product servers (eTrust SCC Clients)
- Monitor the status of network resources
- Correlate events with resources
- Provide alerts and event notifications

For this evaluation, the Collector component of ***e*Trust™ Security Command Center™ Version 8 SP 1 with CR2 Patch**, the operating system and the hardware platform are running are in the IT environment. Therefore, the collector, the operating system and the hardware platform have not been evaluated or tested. The TOE relies on the IT environment to provide:

- Audit data generation
- Protected audit trail storage
- Basic internal TSF data transfer protection
- Partial non-bypassability
- Partial domain separation
- Reliable time stamps

1.1 EVALUATION DETAILS

Evaluated Product: *e*Trust™ Security Command Center™ Version 8 SP 1 with CR2 Patch

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

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

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

EAL: EAL2

Completion Date: 25 January 2007.

1.2 INTERPRETATIONS

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

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

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

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

1.3 THREATS TO SECURITY

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

T.Attack Unauthorized accesses and activity indicative of misuse on IT system resources the TOE monitors may not be identified or associated with other suspicious events thereby allowing the resource to be compromised by an attacker.

T.Bypass An attacker may attempt to bypass TSF security functions to gain unauthorized access to TOE security functions and data.

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

2 IDENTIFICATION

2.1 SECURITY TARGET AND TOE IDENTIFICATION

Security Target – *CA eTrust ™ Security Command Center ™ r8 SP1 with CR2 Patch Security Target Version 1.5.3, dated 25 January 2007.*

TOE Identification – *eTrust ™ Security Command Center ™ r8 SP1 with CR2 Patch*

The Evaluated Configuration of the TOE is software only and includes the following Software Components of *eTrust ™ Security Command Center ™ r8 SP1 with CR2 Patch* running on Windows 2000 Server SP4:

- *e*Trust SCC Server
- *e*Trust Audit Policy Manager
- Audit Data Tools

The *e*Trust Audit Client, *e*Trust SCC Agent, and Product Integration Kits (PIKs) are part of the *e*Trust SCC product but are not evaluated as part of the TOE.

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

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

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

Keywords - Security Monitor, Audit Analyzer, Event Analyzer, Security Target, Security Management

2.2 IT SECURITY ENVIRONMENT

The *e*Trust SCC ST levies requirements on the TOE as well as the IT Environment. In the case of this TOE, the IT Environment includes the Operating System, the underlying hardware platforms, and parts of *e*Trust SCC itself, including the *e*Trust Audit Client, *e*Trust SCC Agent components, and Product Integration Kits (PIKs). The Collector Database and Common Object Repository Databases (TNG Core Database and Portal Database) are also in the IT Environment.

The TOE relies on the environment to provide:

- Audit data generation
- Protected audit trail storage
- Basic internal TSF data transfer protection
- Non-bypassability of IT environment security functions
- Domain separation of IT environment security functions
- Reliable time stamps

2.3 OPERATING SYSTEM

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

2.4 HARDWARE PLATFORM

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

3 SECURITY POLICY

The *e*Trust Security Command Center TOE provides these security services:

- Security Audit
- Security Management
- Identification & Authentication (I&A)
- Protection of the TSF

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

3.1 SECURITY AUDIT

*e*Trust SCC has the following security auditing functions

- **Audit Collection Policy**: Collects audit information generated by itself and from its managed resources.
- **Audit Reporting Policy**: Provides users with audit record viewing capabilities.
- **Audit Rules Policy**: Provides the administrators with rule and filter based specification of security significant events.

3.1.1 Audit Collection Policy

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

The TOE relies on the IT environment to send the collected information in the central audit data repository, via the Collector sub-component of the product. The Collector is part of the *e*Trust Audit Data Tools component of the TOE.

In the case where the TOE is gathering audit events from the host OS, the TOE is configured through the central audit policy to monitor an OS log and when the log is updated by the targeted IT system, the TOE collects the audit event and adds information to identify the audit event source. Standard system security events that may be collected include start-up, shutdown, changes in system IP configuration, and changes to the Allowable Use Policies.

Polices must be defined for events to be collected on operations done on TSF data objects such as a user accessing the TOE, or administrator activities such as managing workplaces, workflow policies, managing profiles, etc.

The following baseline environmental and site-specific attributes make up collected audit event records: event time stamp, computer name, domain name, log name, event id, and user name and source, and event category.

If the audit events are operations on TSF data objects, then the audit records also include the fields: SCC Object Class (e.g.: Audit, iTicker Profile,etc.), SCC Object Name (e.g.: a user defined name), Operation on SCC Object (e.g.: Create/Modify/Delete).

3.1.2 Audit Rules Policy

*e*Trust SCC allows a user to create, activate, and distribute policies to clients that generate audit records. As events occur on clients, the *e*Trust iRecorder on the *e*Trust Audit client collects audit records and send them to the Router for filtering and processing. Based on the administrator-created policies, the Router sends records to be processed by the Action Manager. All of these events are controlled by Administrator defined policies, which are made up of Rules.

An Audit Rule includes a filtering mechanism which evaluates traffic in real-time and determines if an action should be taken when a security relevant event is detected. If a collected audit event does not evaluate to match an action (see below for a list of possible actions), it is dropped as not security relevant. Filters may be defined on any attribute of the collected audit event. Filters can also include an accumulation or combination of audit events based on specified criteria, as well as single events.

When the TOE detects a potential security violation as indicated by an event that meets a defined audit policy, it can:

- Execute a program
- Send an email notification to responsible personnel
- Send the event to the central audit data repository (the collector database)

The action taken depends on the audit policy defined by the administrator. *e*Trust SCC is installed with a set of predefined Audit Rules, which can be edited and augmented by the *e*Trust SCC Administrator.

The TOE also enforces policies to detect a potential security violation as indicated by an event that meets a defined incident. Incident definitions are based on events recorded in the audit data that are tagged by the administrator during the creation of an incident filter. Incident data is incident filter's attributes: owner of the incident, priority of execution of a workflow, identification number for the incident workflow, associated workflow policy, and status of the workflow. Incident Groups organize associated incidents, or events that need special attention.

When an incident filter is triggered the TOE can execute a workflow that is associated with the incident. Workflows are time-based programs that can perform activities such as override incident data (such as assign an incident not acted upon to another administrator), set status on nodes, notify personnel of the incident, and perform other commands specified by the administrator. Each incident workflow can precede or follow another in sequence based on the time the event occurred, so that the sum of these time-based workflows makes up a workflow policy.

3.1.3 Audit Reporting Policy

*e*Trust SCC with the support of the *e*Trust Audit Data Tools provides three mechanisms to support the reviewing of the collected and filtered audit events. These are:

- Aggregation of audit events into a central audit database which can be analyzed with the Viewer or Reporter components of the Audit Data Tools;
- Alerting the administrator through the SCC Alarms and Incident Filters; and
- Performing another action such as send an email or execute a program.

Potentially valuable audit events collected at nodes throughout the enterprise are stored on a centralized, searchable, relational database, the central audit data repository. From the central audit data repository the audit events collected from all collectors are available to administrators for analysis, reporting, and correlation, supporting the need for a complete picture of system activities. In addition to the filtering that occurs at the points of audit event collection, the Administrator can specify filters on the audit events so that only relevant audit events are presented on the Viewer monitor or in a given report generated by the Reporter. The data may be filtered and sorted by audit event attribute (timestamp, event id (e.g., Windows native id), log name, source, category, user, computer, domain or event details), type of event such as logon/logoff, network, administration, and startup/shutdown, or source file. Reports can also be configured and scheduled and an alert (such as node status GUI indicator or an email) can be generated to notify the Administrator.

3.2 SECURITY MANAGEMENT

*e*Trust SCC has the following security management policies

- Security Management of Roles
- Audit Management Policy
- SCC Portal Management Policy

3.2.1 Security Management of Roles

The TOE has three roles:

- SCC User
- SCC Administrator
- Portal Administrator

All roles have administration capabilities. A user may have more than one role.

SCC User

A SCC User will have access to workplaces assigned to them by a Portal Administrator. The SCC User role is normally that of an administrator (security operator) of one or more of the security products that are integrated into the eTrust SCC. Users having the SCC User role are only allowed to monitor and manage the products in their assigned workplace. For example a user with SCC User privilege may have access only to a workplace which contains administrative functions limited to viewing audit and event data, viewing status information and executing product administration interfaces for products not associated with *e*Trust Security Command Center such as a database management system on a remote server.

SCC Administrator

An *e*Trust SCC Administrator will have access to the *e*Trust Security Command Center, *e*Trust Security Command Center Administration, *e*Trust Security Command Center Menus workplaces. This resource type allows a user to manage audit polices, display status profile of enterprise nodes, the workflow incident policies, and the incident groups.

Portal Administrator

This role has the most privilege. The Portal Administrator can be thought of as the *e*Trust SCC system administrator since that role has access to all TOE functions and data, including user administration. After installing the TOE, the 'admin' user has rights based on this role and is allowed access to the TOE first. The default user name and password is stated in the administrator's guide.

3.2.2 Audit Management Policy

Through the SCC Client GUI the Portal Administrator configures IT systems into SCC/Audit Nodes (AN)s and SCC/AN groups monitored by the TSF, defines rules regarding the filtering of audit events collected from the configured IT systems, and associates defined rules with actions. Once a filter is associated with an action the resultant data collection, analysis, and reaction functions can be grouped to define a central audit policy. Once the Administrator defines the central audit policy the central audit policy is distributed to each of the nodes (configured IT entities) over the network. The IT environment supports the secure distribution and storage of the central audit policy.

Audit events collected can be filtered based on any of the attributes found in the collected data, as well as event frequency. The following environmental and site-specific attributes can also be specified: event time stamp, computer name, domain name, log name, event id, username, and source and event category. Specific configurable actions are: forward the event to an alternate Router, forward the event to the central audit data repository, send the event to the Security Monitor to alert the Administrator that the event has occurred, send an alert to another client, or perform another action such as send an email or execute a program. If no action is configured for a collected audit event, it is dropped.

The Administrator can monitor the distribution of the central audit policy to the targeted IT systems through the Administrator interface.

3.2.3 SCC Portal Management Policy

General configuration and modification of the TSF data is constrained to the SCC Administrator and Portal Administrator roles. Only the Portal Administrator has access to the Portal Database which is used to store viewing characteristics, URL information, user accounts, workgroups, workplaces and other management objects (all TSF data). Therefore only the Portal Administrator can use the management functions that act on this data, such as the functions to define a new user or create a new workplace or workgroup. The SCC Administrator has access to the administration workplace which allows use of the functions that act on the TSF data such as audit policies.

3.3 IDENTIFICATION AND AUTHENTICATION POLICY

*e*Trust SCC provides user identification through user accounts and password-based authentication. The Administrator uses the SCC Client GUI, a web-based GUI, to gain access to the TOE. The user must invoke this interface by launching Microsoft's Internet Explorer 6 and typing in the appropriate URL which points to the SCC Server IP and TCP port (e.g., https://hostname:port). The user fills in a form with text fields for user name and password and submits the I&A request. The password field is obfuscated with asterisks. The TOE compares the entered user name and password with the attributes of the user account objects stored in the object repository database for its I&A of users. Upon successful I&A the appropriate information is presented to the user based on the user role. The evaluated configuration of the TOE allowed the user to connect to over SSL. A policy to ensure a hard-to-guess password is specified in the administrator guidance.

3.4 PROTECTION OF THE TSF POLICY

3.4.1 Partial Non-bypassability of the TSP

The TSF ensures that TOE security functions are non-bypassable. Since this is a distributed, software-only TOE, it also relies on the underlying operating system to provide non-bypassability. The TSF ensures that security protection enforcement functions are invoked and succeed before each function within the TOE's scope of control is allowed to proceed. All management user operations are conducted in the context of an associated management session. This management session is allocated only after successful authentication into the TOE. User operations are checked for conformance to the granted level of access (implemented by user role and workplace assignment), and rejected if not conformant. The management session is destroyed when the corresponding user logs out of that session.

3.4.2 Partial TSF Domain Separation

The TSF has well defined external interfaces with its users and its interface to the IT environment on which it depends. Supplementing this, *e*Trust SCC relies on Microsoft SQL Server to manage the Collector database and the databases used as its common object repositories.

Since the TOE is software only, it relies partially on the operating system of the TOE server(s) to provide file protections and process separation. In addition, the underlying assumption regarding the operation of TOE is that the server components are maintained in a physically secure environment.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 USAGE ASSUMPTIONS

A.NoEvil	It is assumed that the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation to install and manage the TOE securely
A.NoUntrusted	It is assumed that there will be no untrusted software on the TOE servers.
A.Password	It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data
A.Physical	It is assumed that the TOE server hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.2 ENVIRONMENTAL OBJECTIVES FOR THE IT ENVIRONMENT

OE.AuditProtection	The IT Environment shall provide the capability to protect the collected audit information.
OE.AuditResource	The IT Environment shall provide the capability to generate records of events that are indicative of potential security violations of critical resources.
OE.PartialProtect	The IT Environment shall provide protection for the TOE and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
OE.Time	The underlying operating systems shall provide reliable time stamps.

4.3 ENVIRONMENTAL OBJECTIVES FOR THE NON-IT ENVIRONMENT

ON.NoUntrusted	There shall be no untrusted software on the eTrust SCC Server and eTrust Audit hosts.

ON.Personnel	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE and they shall ensure that the TOE is installed, managed and operated in a manner which is consistent with the TOE guidance documentation.
ON.Physical	Those responsible for the TOE shall ensure that the TOE servers are protected from any physical attack.
ON.PwdProtect	Users of the TOE shall ensure that they choose strong passwords and that they protect their authentication data as instructed by the administrator guidance.

4.4 CLARIFICATION OF SCOPE

The product, *e*Trust SCC, that a customer would purchase includes more than the evaluated TOE. The evaluated TOE does not include the *e*Trust Audit client, the *e*Trust SCC Agent, or the Product Integration Kits (PIKs). These components reside in the IT Environment because *e*Trust Audit client, SCC Agent, and PIKs can be targeted for variety of platforms. Since it was not practical to evaluate every possible configuration, the evaluation team chose a single managed node configuration on a typical hardware and software platform for evaluation purposes. This was acceptable for the evaluation since the security functionality is the same for one Audit Client as for many Audit Clients. The end user should be aware that there is no guarantee of how many Audit Clients can be used or whether multiple Audit Clients reduce the performance of the TOE. These client components should be evaluated by the TOE user as necessary to gain confidence.

Even though many of the components of *e*Trust SCC are similar to *e*Trust Audit, the previous evaluation of *e*Trust Audit is irrelevant to this TOE because the *e*Trust Audit components used in this evaluation are different versions. Since the versions are different, the previous NIAP certification does not apply. *e*Trust SCC contains all of the required components for this TOE. Purchasing a separate *e*Trust Audit Product order is not required. As provided by the TOE's assumptions, a trained administrator will install the TOE using *e*Trust SCC installation guide found in the SCC delivered product. Should there be additional Audit Clients installed in the environment from the previous versions, the TOE will not automatically discover them and integrate them as nodes managed by the TOE. The trained administrator will only integrate the correct version of the *e*Trust Audit Client into the TOE.

The *e*Trust Audit Client components gather and process event information from the network resources that are managed by *e*Trust SCC. A number of product specific *e*Trust Audit client components are provided with on the *e*Trust SCC installation media and users may also develop custom components to collect audit data from other applications. Multiple versions of the *e*Trust Audit client components may reside on a single host machine. The *e*Trust Audit client must also be installed on the *e*Trust SCC server for generation of audit records for the events produced by *e*Trust SCC itself. (Therefore the *e*Trust SCC Server machine may be considered a client of the *e*Trust Audit Servers.)

The *e*Trust Audit Clients are part of the evaluated configuration, but not part of the evaluate TOE itself. The TOE relies entirely on the environment to gather and store the data that is analyzed and reviewed. *e*Trust SCC also relies on the environment for secure transfer of data between TOE components.

The *e*Trust SCC Agent components also reside on the product servers (*e*Trust SCC Clients) managed by *e*Trust SCC. The *e*Trust SCC Agents consist of system-specific sub-components that monitor services, process and daemons operating on the product servers (*e*Trust SCC Clients) and provide status information to the *e*Trust SCC server.

Product Integration Kits (PIKs) are product specific software developed to provide access to the content, monitoring and management interfaces of the resources managed by *e*Trust SCC. A PIK consists of a server-side sub-component that resides on the *e*Trust SCC Server host and an agent-side sub-component that is installed on a network product server (*e*Trust SCC Client) . PIKs developed by CA, Inc. for a number of products are provided with *e*Trust SCC. A user also has the option to create custom PIKs to integrate additional products and applications. As with the *e*Trust Audit client, multiple PIKs may reside on a single product server (*e*Trust SCC Client).

The TOE is installed with AES encryption enabled. Audit Data Tool Server and Audit Client provides encryption in the form of AES (128 bit key) and DES (56 bit key) for backward compatibility, however the default setting is AES. This environmental component encrypts information transferred by *e*Trust Audit Client to the Audit Data Tools server across the network. This supports the functional components for the IT environment FPT_ITT.1 Basic internal TSF data transfer protection. This functionality is part of the evaluated configuration, but since this functionality is in the environment, it was not evaluated.

Any additional CA applications that may be bundled with this product are treated in this evaluation as part of the IT Environment.

Some requirements were placed upon the configuration of the IT Environment to support the analysis and conclusions reached by this evaluation. To use this product in the evaluated configuration, the IT environment requirements need to be addressed by the TOE administrator. Since the *e*Trust SCC 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.

5 ARCHITECTURAL INFORMATION

The TOE, *e*Trust SCC, allows audit data to be selectively collected from a diverse set of systems, applications, devices and appliances that may be indicative of misuse of IT resources. In addition, *e*Trust SCC allows the user to create and manage a centralized policy regarding the retention of audit information performing, intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, and reporting of conclusions. The TOE is a subset of *e*Trust SCC, a distributed network based product. The product has six main components of which only three are part of the evaluated TOE: The *eTrust SCC Server, the eTrust Audit Policy Manager*, and *the Audit Data Tools.*

Product components can reside on the same system, or on multiple systems. The eTrust Audit Policy Manager and the eTrust Audit Data Tools are separated for the evaluated configuration.

5.1 GENERAL TOE FUNCTIONALITY

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

- Security Audit
- Security Management
- Identification & Authentication (I&A)
- Protection of the TSF

*e*Trust SCC relies upon a third party database and the underlying operating system and hardware platform to generate, store and protect audit data records, to provide reliable time stamps, to protect internal TSF data transfer, to provide domain separation of IT environment security functions, and to protect the *e*Trust SCC functions from other interference or tampering.

A functional diagram of the *e*Trust SCC TOE and the environment in which it exists is provided in Figure 1. Components of the TOE are designated by dark blue blocks. A physical diagram of the TOE is shown in its evaluated configuration in Figure 3.

Table 5-1 provides a list of the interfaces shown in Figure 1. The internal and external interfaces are described in Tables 5-2 and 5-3.

Table 5-1 – External TOE Interfaces

Interface Number	**Interface Title**
1	SCC Client Interface
2	SCC Server – SCC Agent Interface
3	SCC Server – Audit Data Tools Interface
4	SCC Server – Audit Policy Manager Interface
5	SCC Server – TNG Core Database
6	SCC Server – Portal Database
7	Audit Policy Manager – Audit Client
8	Audit Data Tools – Collector Database
9	Audit Data Tools – Audit Client Interface
10	Audit Data Tools and the OS Interface
11	SCC Server – Administrated Product

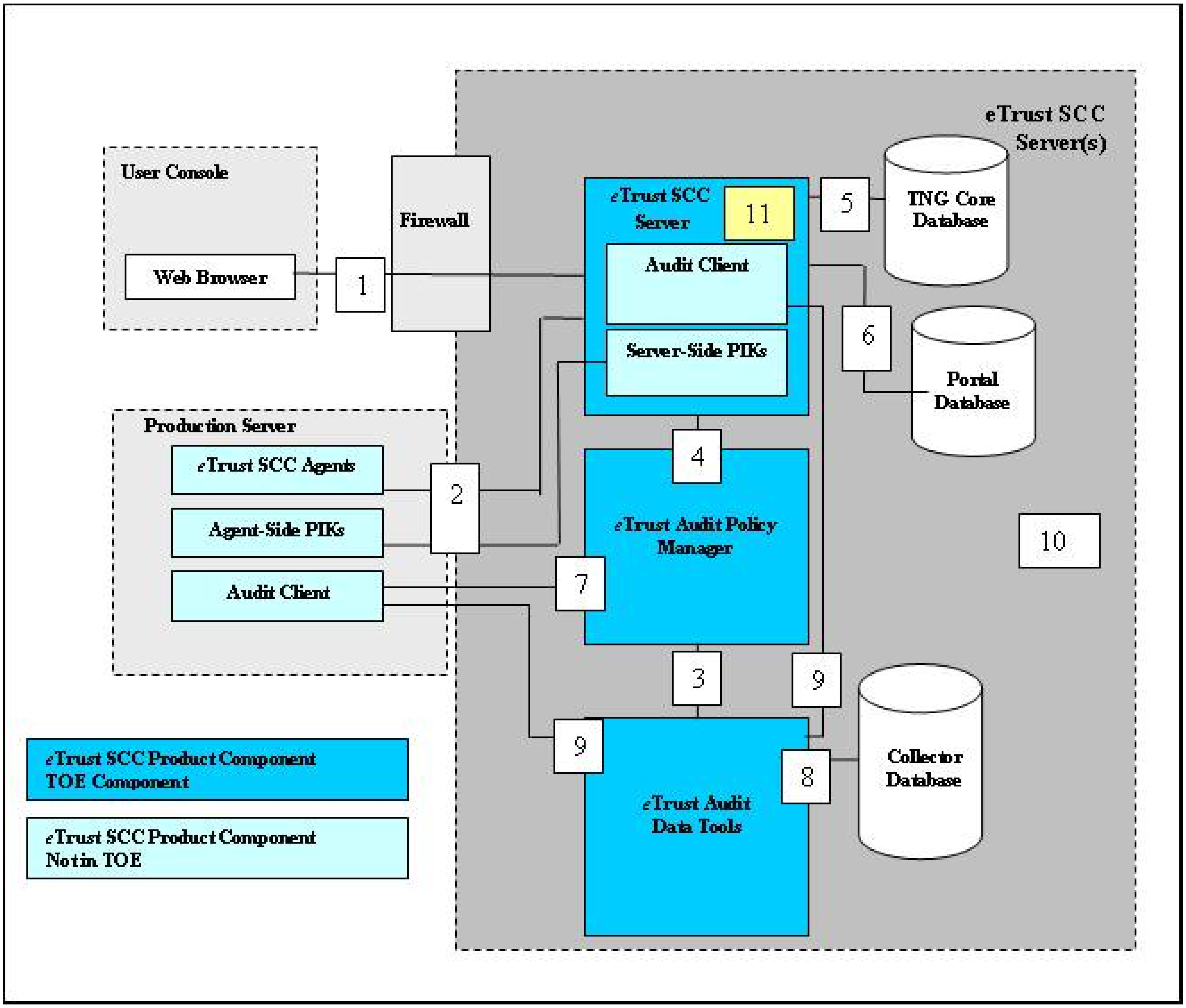

Figure 1: TOE Boundary

5.2 PRODUCT COMPONENTS

The *e*Trust SCC is a software-only product. The components of the *e*Trust SCC Product, as delivered to the customer, are described below:

*e*Trust SCC Server

The *e*Trust SCC Server component provides the core functionality of the product. Security functions provided by the *e*Trust SCC Server are:

User Identification and Authentication

The *e*Trust SCC Server performs user identification and password based authentication before allowing access to management and monitoring functions.

User Interface

eTrust SCC provides a graphical user interface (GUI) through a comprehensive set of configuration, management, and monitoring web applications. A user accesses the *e*Trust SCC GUI through a standard web browser over SSL from any workstation on the local area network that connects the SCC, Audit and product servers (*e*Trust SCC Clients). A user's access to security data and functions can be restricted. The appearance of the user interface can be customized by both the administrator and the user.

Event Monitoring

Several methods of monitoring security relevant events are provided. Audit data is collected from network resources and stored in a database in the IT Environment that is used as a central data repository. User defined audit policies and incident filters determine which data is collected and designated as significant. Various event viewers allow a user to display, sort, and filter the collected data. The *e*Trust SCC Server component also provides several methods of alerting responsible personnel when a security relevant event occurs.

Status Monitoring

*e*Trust SCC monitors and discovers services, processes, and daemons running on the managed product servers (*e*Trust SCC Client machines) on the network. The status monitoring functions of the *e*Trust SCC Server lets the users create customized views of the status of security in an enterprise. These views can be organized by application or by area of responsibility.

Product Administration

Products residing on the network servers may be managed through the *e*Trust SCC user interface. This functionality is provided both by running product utilities and by access to a product's native administrative and management interfaces through the web based *e*Trust SCC GUI described previously.

The eTrust SCC Server component is supported by two third-party relational databases which are used as common object repositories: The TNG Core database used to store status information and the Portal Database used to store viewing characteristics, URL information, user accounts, workgroups, workplaces and other management objects.

*e*Trust Audit Policy Manager

The *e*Trust Audit Policy Manager provides the functionality that allows the creation, implementation and distribution of an organization's audit policies. Audit polices specify the event data to be collected from resources residing across the network. Audit policies also assign patterns to events so that a security relevant event can be designated through policy rules. This component also provides for the analysis of the collected audit data so that actions and alerts can be automatically triggered when a significant event occurs.

***e*Trust Audit Data Tools**

The eTrust Audit Data Tools component supplies the functionality that manages the collector database. The collector database is a third-party relational database in the IT Environment that acts as the central repository for audit data collected from the network resources. The *e*Trust Data Tools component also provides support for the event viewing functions of the *e*Trust SCC GUI.

***e*Trust Audit Client**

The *e*Trust Audit client components gather and process event information from the network resources that are managed by *e*Trust SCC. A number of product specific *e*Trust Audit client components are provided with on the *e*Trust SCC installation media and users may also develop custom components to collect audit data from other applications. Multiple versions of the *e*Trust Audit client components may reside on a single host machine. The *e*Trust Audit client must also be installed on the *e*Trust SCC server for generation of audit records for the events produced by *e*Trust SCC itself. (Therefore the *e*Trust SCC Server machine may be considered a client of the *e*Trust Audit Servers.)

eTrust SCC Agent

eTrust SCC Agent components also reside on the product servers (eTrust SCC Clients) managed by eTrust SCC. The eTrust SCC Agents consist of system-specific sub-components that monitor services, process and daemons operating on the product servers (eTrust SCC Clients) and provide status information to the eTrust SCC server.

Product Integration Kits (PIKs)

Product Integration Kits (PIKs) are product specific software developed to provide access to the content, monitoring and management interfaces of the resources managed by eTrust SCC. A PIK consists of a server-side sub-component that resides on the eTrust SCC Server host and an agent-side sub-component that is installed on a network product server (eTrust SCC Client) . PIKs developed by CA, Inc. for a number of products are provided with eTrust SCC. A user also has the option to create custom PIKs to integrate additional products and applications. As with the eTrust Audit client, multiple PIKs may reside on a single product server (eTrust SCC Client)

5.3 TOE INTERFACES

There is essentially only one external interface in the evaluated configuration of the *e*Trust SCC TOE.

The SCC Client Interface is the only interface through which administrative functions are performed.   All of the *e*Trust Security Command Center functionality is visible through this web portal interface.

Other locally accessible GUI interfaces exist to administer to the TOE functionality, however the administrators of the TOE are told not to use these interfaces in the administrator guidance.

The A.NoEvil assumption assumes that the administrators are trained, not careless, not willfully negligent, not hostile, and will follow and abide by the instructions provided by the TOE documentation to install and manage the TOE securely.

The *e*Trust SCC TOE also depends on multiple internal interfaces. The interfaces that exist between physically separate TOE components are internal interfaces.

The TOE has an internal interface to the Collector, TNG Core, and Portal Databases. These interfaces are controlled by the TOE, and may not be used to invoke the TOE by an external user.

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

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

The TOE has interfaces to each instance of eTrust Audit Clients, eTrust SCC Agents, or Product Integration Kits (PIKs). These interfaces are also controlled by the TOE, and after proper installation may not be used to invoke the TOE by an external user.

The SCC Server to Administrated Product interface is an interface entirely within the SCC Server component.

Figure 1 pictorially shows the external and internal interfaces of the TOE. The interfaces internal and external interfaces are described in Tables 5-2 and 5-3 below.

Table 5-2 – External TOE Interfaces

	Subsystem	**Interface Type**
1	SCC Client Interface	The only interface through which administrative functions are carried out is using the User Console GUI (SCC Client Interface). The eTrust Security Command Center interface is a web portal that runs in a web browser. The web browser uses is http or https which are well known application layer protocol.

Table 5-3 – Internal TOE Interfaces

	Subsystem	Interface Type	Connection
2	SCC Server – SCC Agent Interface	This interface is used to convey status and report information to the SCC Server. The reports and the status are eventually viewed from the eTrust SCC Client interface. For Reporting: Product Integration Kit – SCC Agent Product Interface servlet – SCC Server Interface type is web based for status	TOE to Environment
3	SCC Server – Audit Data Tools Interface	This interface is used to retrieve the event data stored in the SQL server. In this case, the user selects a menu item from the Events branch of the tree menu of the eTrust SCC Client GUI. That user can choose to view events using the Log Viewer or the Ad Hoc Query Viewer. Interface type is a CA proprietary interface.	TOE to TOE
4	SCC Server – Audit Policy Manager Interface	The eTrust SCC Client user with appropriate privileges can view, create, modify, delete and manage audit policies using the interface between the SCC Server and the Audit Policy manager. Interface type: SCC web client invokes an ActiveX control	TOE to TOE
5	SCC Server – TNG Core Database	This is a standard JDBC interface between the SCC server and embedded TNG Core Database. This interface is used to store and retrieve status information from the database.	TOE to Environment
6	SCC Server – Portal Database	This is a standard JDBC interface between the SCC server (Portal Component) and embedded Portal Database. The Portal Database used to store viewing characteristics, URL information, user accounts, workgroups, workplaces and other management objects.	TOE to Environment
7	Audit Policy Manager – Audit Client	This interface is used to provide services to collect and forward audit event data, this can result in the generation of actions and alerts. This interface is also used to collect policy information from the Audit Policy Manager. Interface type is a CA proprietary interface.	TOE to Environment
8	Audit Data Tools – Collector Database	This is a standard JDBC interface between the Audit Data Tools and SQL Server. This is used to retrieve status, events and reports information from the collector database.	TOE to Environment
9	Audit Data Tools – Audit Client Interface	This interface helps in receiving the data sent by the Audit Clients residing on the Production severs and storing the data in the collector database. Interface type is a CA proprietary interface	TOE to Environment
10	Audit Data Tools and the OS Interface	The Audit Data Tools reside and execute on the host operating system such as the file system, time stamps, etc. OS interfaces	TOE to Environment

	Subsystem	Interface Type	Connection
11	SCC Server – Administrated Product	This interface represents the flow of data among eTrust SCC components in a typical configuration during Administration of the SCC product. Product administration lets you invoke native product interfaces so that you can manage other eTrust products from within eTrust Security Command Center. These interfaces are made available by using Windows Terminal Services, web-based interfaces, or Telnet web sessions, depending on the product. In this instance it was tested with the Policy Manager GUI on localhost and web server installed by the TOE. Internal Interface.	TOE to TOE

6 DOCUMENTATION

Purchasers of a product containing the *e*Trust Security Command Center r8 receive the following TOE documentation:

- *eTrust Command Center Administrator Guide r8 - G00160-1E;*
- *eTrust Security Command Center User Guide r8 - G00159-1E;*
- *eTrust Command Center Getting Started Guide r8 - G00200-1E;*
- *eTrust Command Center Integration Guide r8 - G00161-1E;* and
- *Security Command Center Release Summary r8 - G00199-1E.*

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

7 IT PRODUCT TESTING

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

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

All of the testing was conducted in at:

CygnaCom Solutions, Inc.
7925 Jones Branch Drive, Suite 5200
McLean, VA 22102-3321

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

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

7.1 INSTALLATION TESTING

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

- CA *eTrust Security Command Center Getting Started Guide r8 - G00200-1E*

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

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

Component	Minimum Host System Requirements
*e*Trust SCC Server	Windows 2000 Server with SP4. Pentium-III, 1.4 GHz processor 1 GB RAM minimum 6 GB Disk Space Microsoft SQL Server 2000 with Service Pack 3 (with Dictionary order, case-sensitive, for use with 1252 Character Set) TCP/IP installed Microsoft Internet Explorer 6.0
*e*Trust Audit Data Tools Server	Windows 2000 Server SP4 Pentium-III, 1.4 GHz processor 1 GB RAM minimum 6 GB Disk Space Microsoft SQL Server 2000 with Service Pack 3 (with Dictionary order, case-sensitive, for use with 1252 Character Set) TCP/IP installed
*e*Trust Product Server (SCC Client)	Windows 2000 Server SP4 Pentium II 400 MHz 128 MB Memory 100 MB Disk Space TCP/IP installed Microsoft Internet Explorer 6.0

Figure 2: Minimum TOE Installation Requirements

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

7.2 DEVELOPER TESTING

The set of developer tests consists of 64 test procedures. The evaluation team performed 20% of the tests provided by the developer.   All of the test cases included a test description, security functions tested, rationale, purpose for the test, explicit test steps, and an expected result. The testing was either performed by evaluator while being observed and recorded by the evaluation team performed by the evaluation team with assistance from the CA personnel.

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

No hardware test tools were used during the developer functional testing. The only software test tool used during the testing was the script “test.bat” which executed and program called LOGEVENT.EXE that generated OS level events: application and system process launch. This script was needed for Developer test AU-1-01 Security Alarms.

The testing did result in minor updates to the *e*Trust SCC Security Target, but did not affect the software or installed configuration. Most of the sample developer tests were successful, except for one set of audit function tests. These tests were removed from the developer’s test suite sample, modified, and run as independent tests. Minor changes were needed to the test steps and prerequisites to adequately exercise the security function. The evaluation team developed independent tests to exercise these audit features. The tests run as independent test cases were successful.

In Section 4 of *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, CA e*Trust *™ Security Command Center r8, ETR Version 0.3, Security Target Version 1.5.3, dated January 25, 2007*, the evaluation team reported that they had examined the test results and determined that the developer testing was a success. The developer’s tests run by the evaluation team completed successfully and all test results were archived in the *CA eTrust ™ Security Command Center ™ Version 8 SP 1 with CR2 Patch, Test Report V0.1, dated December 20, 2006.*. The evaluation team reported that the actual test results from the developer’s tests matched the developer’s expected results. A list of final test cases and their actual results are shown in Table 7-1 below:

SFR	TSS Security Function		Success/Failure
	Security Audit		
FAU_ARP.1	AU-1	Security Alarms	**Success**
FAU_GEN.1-1	AU-2	Audit Data Generation: TOE	**Success**
FAU_GEN_EXP.1	AU-3	Audit Data Collection	**Success**
FAU_SAA.3	AU-4	Simple Attack Heuristics	**Success**
FAU_SAR.1-1	AU-5	Audit Review: TOE Audit Data	**Success**
FAU_SAR.1-2	AU-6	Audit Review: Collected Audit Data	**Success**
FAU_SAR.3	AU-7	Selectable Audit Review	**Success**
	Identification and Authentication		
FIA_UID.2	IA-3	User Identification before any Action	**Success**
FIA_UAU.2	IA-1	User Authentication before any Action	**Success**
FIA_UAU.7	IA-2	Protected Authentication Feedback	**Success**
	Security Management		
FMT_MTD.1	SM-1	Management of TSF Data	**Success**
FMT_SMF.1	SM-2	Specification of Management Functions	**Success**
FMT_SMR.1	SM-3	Security Roles	**Success**
	Protection of TSF		
FPT_RVM_EXP_TOE.1	PT-1	Partial Non-bypassability of the TSP: TOE	Implicitly tested by all test cases and pen tests
FPT_SEP_EXP_TOE.1	PT-2	Partial TSF Domain Separation: TOE	Implicitly tested by all test cases and pen tests

Table 7-1 –TOE Developer Test Results

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

7.3 *EVALUATION TEAM INDEPENDENT TESTING*

The evaluation team devised a test subset for independent testing. The test subset consisted of functions not tested by the developer. All of the test cases included a purpose, explicit test steps, and an expected result. The evaluation team produced test documentation for the test subset that was sufficiently detailed to enable the tests to be reproducible. This time the testing was performed by the evaluation team, with the CA personnel present. The Validator relied on the independent and penetration test report in *CA eTrust™ Security Command Center™ Version 8 SP 1 with CR2 Patch, Test Report V0.1, dated December 20, 2006.*

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

Each test was intended to explicitly exercise the Security Audit, Security Management, Identification & Authentication (I&A) and implicitly tested Protection of the TSF by all test cases and the team defined penetration tests.

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

A list of final security function test cases that were independently tested and their actual results are shown in Table 7-2: Independent Evaluator Test Results below:

SFR	**TSS Security Function**		**Success/Failure**
	Security Audit		
FAU_ARP.1	AU-1	Security Alarms	**Success**
FAU_GEN.1-1	AU-2	Audit Data Generation: TOE	**Success**
FAU_GEN_EXP.1	AU-3	Audit Data Collection	**Success**
FAU_SAA.3	AU-4	Simple Attack Heuristics	**Success**
FAU_SAR.1-1	AU-5	Audit Review: TOE Audit Data	**Success**
FAU_SAR.1-2	AU-6	Audit Review: Collected Audit Data	**Success**

SFR	TSS Security Function		Success/Failure
FAU_SAR.3	AU-7	Selectable Audit Review	**Success**
	Identification and Authentication		
FIA_UID.2	IA-3	User Identification before any Action	**Success**
FIA_UAU.2	IA-1	User Authentication before any Action	**Success**
FIA_UAU.7	IA-2	Protected Authentication Feedback	**Success**
	Security Management		
FMT_MTD.1	SM-1	Management of TSF Data	**Success**
FMT_SMF.1	SM-2	Specification of Management Functions	**Success**
FMT_SMR.1	SM-3	Security Roles	**Success**
	Protection of TSF		
FPT_RVM_EXP_TOE.1	PT-1	Partial Non-bypassability of the TSP: TOE	Implicitly tested by all test cases and pen tests
FPT_SEP_EXP_TOE.1	PT-2	Partial TSF Domain Separation: TOE	Implicitly tested by all test cases and pen tests

Table 7-2 – Independent Evaluator Test Results

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

7.4 EVALUATION TEAM PENETRATION TESTING

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

The evaluation team created a penetration test plan. All of the test cases included a purpose, explicit test steps, and an expected result. In addition to this there were test scripts and test tools:

- Nessus Vulnerability Scanner and nmap port scanner.

- Test Script EventGen.bat was used to generate large volumes of data that was collected by the Audit Data Tools. This assisted to test the resilience of TOE against DoS attacks during audit collection.

The testing was performed by the evaluation team. The Validator relied on the independent and penetration test report

The penetration tests evaluated the following scenarios:

- Attempt to cause a Denial of Service by generating vast quantities of audit information on a client machine and observe the behavior of the viewer and security monitor

- Data collection interruption through the following techniques:

    - Shut down the DataTools Server. Check that no audit data from the client was lost while the server was down. Check that alerts will be issued for events that occurred during the time the server was down.

    - Disconnect the network cable between the DataTools Server and the Client. Check that no audit data from the client was lost while the while the Network connection was disabled. Check that alerts will be issued for events that occurred during the time the Network connection was disabled.

The results of initial penetration testing exposed vulnerabilities in the intended environment of the TOE by the Nessus Scanner. Two vulnerabilities were exposed:

The first vulnerability affects the TOE itself. The iTechnology iGateway Content-Length Buffer Overflow Vulnerability causes the remote web server to be affected by a buffer overflow vulnerability.

The second vulnerability affects the environment in the evaluated configuration. The Computer Associates Message Queuing Denial Of Service Vulnerability makes it possible to crash the remote messaging service.

These vulnerabilities were countered by the CR2 patch. Rerunning the set of penetration tests showed that the vulnerabilities were no longer exploitable.

A description of the penetration test results are in section 10.2.

8 EVALUATED CONFIGURATION

8.1 TEST SOFTWARE AND HARDWARE

The evaluated configuration consists of three servers running the Windows 2003 SP1 operating system: two are SCC Servers and will be installed with the TOE component software, the third is the product server (eTrust SCC Client) that will be managed and monitored by the TOE. The evaluated configuration is shown below in 4.

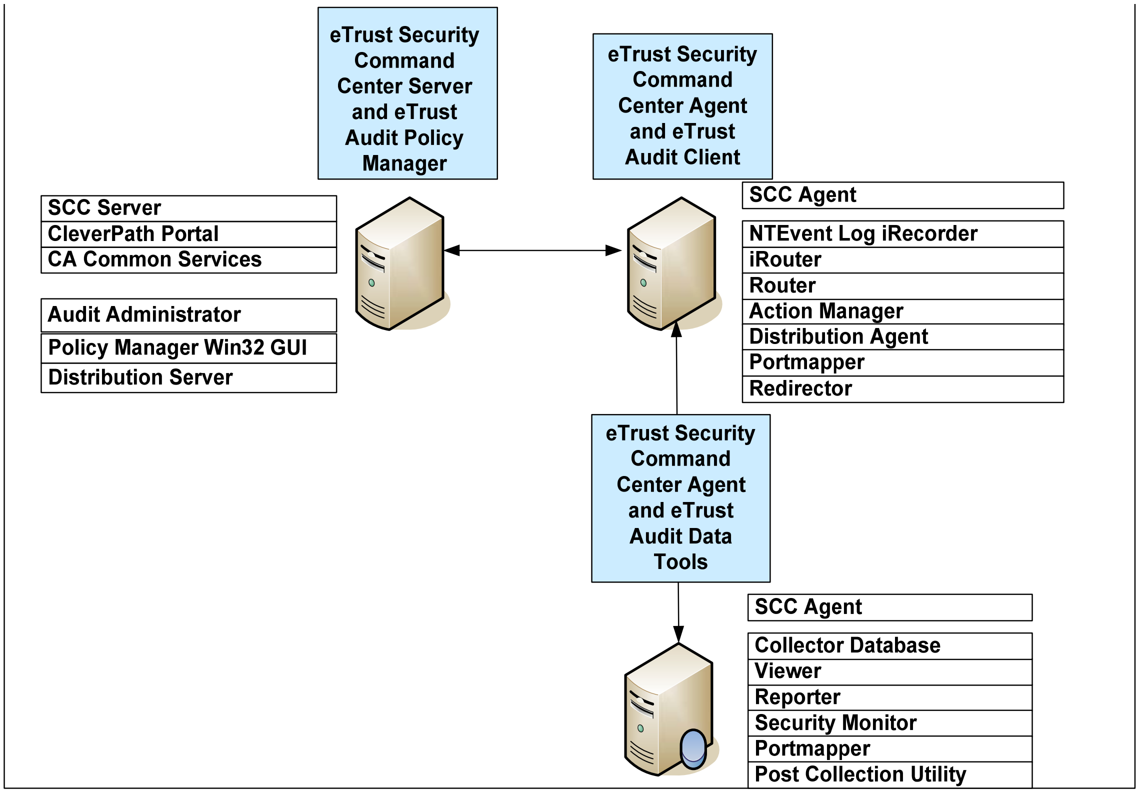

Figure 3: Evaluated Configuration

The following tables specify the hardware, operating systems, and software which are in the IT Environment of the evaluated configuration. The second column lists the minimum requirements and versions of the software and hardware on which the TOE is compliant, the third column specifies the tested configuration that was used for the evaluation.

Table 8-1 – eTrust SCC Server Configuration

	Requirements	Tested Configuration
SCC Product Components:	eTrust SCC Server eTrust Audit Policy Manager eTrust Audit Client Server-Side PIKs	eTrust SCC Server eTrust Audit Policy Manager eTrust Audit Client Server-Side PIKs
Windows System Requirements:	Windows 2000 Server with SP4. Windows 2003 Server EE with SP1	Windows 2000 Server with SP4

	Requirements	Tested Configuration
Minimum Hardware Requirements:		
Processor:	Pentium-III or higher, 1.4 GHz processor or higher	Intel® Xeon™ 3.00 GHz processor
Memory:	1 GB RAM minimum	2 GB
Disk Space:	Greater than 6 GB	33.8 GB
Other Hardware:	None required	DVD Drive
Database Requirements:	Microsoft SQL Server 2000 with Service Pack 3 (with Dictionary order, case-sensitive, for use with 1252 Character Set)	Microsoft SQL Server 2000 Enterprise Edition
Software:	TCP/IP installed Microsoft Internet Explorer 6.0 or higher	TCP/IP installed Microsoft Internet Explorer 6.0 SP1

Table 8-2 – eTrust Data Tools Server Configuration

	Requirements	Tested Configuration
SCC Product Components:	eTrust Audit Data Tools eTrust SCC Agent	eTrust Audit Data Tools eTrust SCC Agent
Windows System Requirements:	Windows 2000 Server with SP4. Windows 2003 Server EE with SP1	Windows 2000 Server with SP4.
Minimum Hardware Requirements:		
Processor:	Pentium 1 GHz	Intel® Xeon™ 3.00 GHz processor
Memory:	256 MB	2 GB
Disk Space:	1000 MB	33.8 GB
Other Hardware:	None required	DVD Drive
Database Requirements:	Microsoft SQL Server 2000 with Service Pack 3 (with Dictionary order, case-sensitive, for use with 1252 Character Set)	Microsoft SQL Server 2000 Enterprise Edition (with Dictionary order, case-sensitive, for use with 1252 Character Set)
Software:	TCP/IP installed	TCP/IP

Table 8-3 – Product Server (eTrust SCC Client) Configuration

	Requirements	Tested Configuration
SCC Product Components:	eTrust SCC Agent eTrust Audit Client Agent-Side PIKs	eTrust SCC Agent eTrust Audit Client Agent-Side PIKs
Windows System Requirements:	Windows 2000 Windows 2003 Windows XP	Windows XP 2002 Professional with SP2
Minimum Hardware Requirements:		
Processor:	Pentium 1 GHz	Pentium III 498MHz
Memory:	128 MB	640 MB
Disk Space:	100 MB	18 GB
Other Hardware:	None	DVD +/-R Drive
Database Requirements:	None	None
Software:	TCP/IP installed Microsoft Internet Explorer 6.0 or higher	TCP/IP installed Microsoft Internet Explorer 6.0

8.2 TEST TOOLS AND SCRIPTS

The following hardware test tools were used for the independent and penetration testing.

- Nessus Vulnerability Scanner and nmap port scanner.
- Test Script EventGen.bat

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

9 RESULTS OF THE EVALUATION

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

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

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

- *Evaluation Technical Report for a Target of Evaluation, Volume 1: Evaluation of the ST, CA eTrust ™ Security Command Center ™ Version 8 SP 1 with CR2 Patch, ETR Version 0.7.2, Security Target Version 1.5.3, dated January 25, 2007.*

- *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the ST, CA eTrust ™ Security Command Center ™ Version 8 SP 1 with CR2 Patch, ETR Version 0.4, Security Target Version 1.5.3, dated January 25, 2005.*

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

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

Therefore, when configured according to the guidance documentation enumerated in section 6 of this report, the TOE *e*Trust SCC is CC compliant and satisfies the *CA eTrust ™ Security Command Center ™ r8 SP1 with CR2 Patch Security Target Version 1.5.3, dated 25 January 2007.*

10 VALIDATION COMMENTS/RECOMMENDATIONS

10.1 VALDATION COMMENTS

The product, *e*Trust SCC, 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 EAL2.

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

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

The TOE is distributed, but there is no TOE security functional requirement to protect TOE data between machines. Since there are no requirements to protect the TOE data between distributed components of the TOE, the evaluation team did not check whether the network traffic between TOE machines could be intercepted, modified, manipulated, or otherwise interfered with. The customer can have no confidence, based on this evaluation, that the *e*Trust Audit product is capable of protecting itself from any type of threat that could have access to the communication paths between components. To ensure that data transmission between TOE components is secure, the TOE should be installed with adequate encryption strength in the environment to protect the TSF data from disclosure and modification when it is transmitted between separate parts of the TOE as required by FPT_ITT.1.1. The default installation of *e*Trust SCC installs AES (128 bit key) in the IT Environment. This functionality is part of the evaluated configuration, but since this functionality is in the environment, it was not evaluated. This encryption may be adequate since there are no known exploits for AES (128 bit key).

There is essentially only one external interface in the evaluated configuration of the *e*Trust SCC TOE. The SCC Client Interface is the only interface through which administrative functions are performed. All of the *e*Trust Security Command Center functionality is visible through this web portal interface. Other locally accessible GUI interfaces exist to administer to the TOE functionality, however the administrators of the TOE are told not to use these interfaces in the administrator guidance.

The *e*Trust SCC TOE also depends on multiple internal interfaces. The interfaces that exist between physically separate TOE components and entirely within one TOE component are internal interfaces. These interfaces are controlled by the TOE, and may not be used to invoke the TOE by an external user.

The TOE also relegates audit data generation, protected audit trail storage, basic internal TSF data transfer protection, partial non-bypassability, partial domain separation, and reliable time stamps to the IT environment. The TOE depends on the functionality of the IT environment for much of its traditional security functionality.

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

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

*e*Trust SCC was not difficult to install and configure, it was easy to operate and easy to administer. The external internal interface is a GUI interface.

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

10.2 SIGNIFICANT FINDINGS DURING EVALUATION

As part of the evaluation, the CygnaCom Solutions, Inc SEL evaluation team discovered vulnerabilities during a full Nessus scan. These vulnerabilities are mitigated upon installation of the CR2 patch. The evaluation team determined that these vulnerabilities were mitigated by rerunning the full Nessus Scan. Details of the vulnerabilities can be found in table 10-1 below.

Table 10-1 Vulnerabilities Discovered and Mitigated

CA Vulnerability Description	Comments
iTechnology iGateway Content-Length Buffer Overflow Vulnerability (TOE) *Synopsis:* *The remote web server is affected by a buffer overflow vulnerability.* *Description:* *The remote host is using Computer Associates iTechnology iGateway service, a software component used in various products from Computer Associates.* *The version of the iGateway service installed on the remote host reportedly fails to sanitize Content-Length HTTP header values before using them to allocate heap memory. An attacker can supply a negative value, which causes the software to allocate a small buffer, and then overflow that with a long URI. Successful exploitation of this issue can lead to a server crash or possibly the execution of arbitrary code. Note that, under Windows, the server runs with local SYSTEM privileges.* *See also:* *http://www.idefense.com/intelligence/vulnerabilities/display.php?id=376* *http://supportconnectw.ca.com/public/ca_common_docs/igatewaysecurity_notice.asp* *Solution:* *Contact the vendor to upgrade to iGateway 4.0.051230 or later.* *Risk factor :* ***Critical** / CVSS Base Score : 10* *(AV:R/AC:L/Au:NR/C:C/A:C/I:C/B:N)* *CVE : CVE-2005-3653* *BID : 16354*	This vulnerability affects the TOE. The Evaluator installed a patch provided by the Vendor support web site which removed this risk. The patch upgraded the TOE from eTrust SCC r8 SP1 to eTrust SCC r8 SP1 CR2. The component fix was verified by checking its version number and rerunning the Nessus scanner tool.

Other references : OSVDB:22688 *Nessus ID: 20805*	
Computer Associates Message Queuing Denial Of Service Vulnerabilities (Environment) *Synopsis:* *It is possible to crash the remote messaging service.* *Description:* *The remote version of Computer Associates Message Queuing Service is vulnerable to tow flaws which may lead to a denial of service :* *- Improper handling of specially crafted TCP packets on port 4105* *- Failure to handle spoofed UDP CAM requests* *See also:* *http://supportconnectw.ca.com/public/ca_common_docs/camsecurity_notice.asp* *Solution:* *Computer Associates has released a set of patches for CAM 1.05, 1.07 and 1.11.* *Risk factor:* *Medium / CVSS Base Score : 5* *(AV:R/AC:L/Au:NR/C:N/A:C/I:N/B:A)* *CVE : CVE-2006-0529, CVE-2006-0530* *BID : 16475* *Other references : OSVDB:21146* *Nessus ID: 20840*	This vulnerability affects the TOE. The Evaluator installed a patch provided by the Vendor support web site which removed this risk. The patch upgraded the TOE from eTrust SCC r8 SP1 to eTrust SCC r8 SP1 CR2. The component fix was verified by checking its version number and rerunning the Nessus scanner tool.

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 *e*Trust™ Security Command Center™ Version 8 SP 1 with CR2 Patch.

11 LIST OF ACRONYMS

Acronym	Description
CC	Common Criteria [for IT Security Evaluation]
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 Evaluatio*n, version 2.2, January 2004, Part 1.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 2.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 3.
- *Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3*, Version 1.0, February 2002.
- *Common Evaluation Methodology for Information Technology Security, version 2.2, Revision 256,* January 2004.

- *CA eTrust ™ Security Command Center ™ r8 SP1 with CR2 Patch Security Target Version 1.5.3, dated 25 January 2007.*

- *Evaluation Technical Report for a Target of Evaluation, Volume 1: Evaluation of the ST, CA eTrust ™ Security Command Center ™ Version 8 SP 1 with CR2 Patch, ETR Version 0.7.3, Security Target Version 1.5.3, dated January 25, 2007.*

- *Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the ST, CA eTrust ™ Security Command Center ™ Version 8 SP 1 with CR2 Patch, ETR Version 0.4.1, Security Target Version 1.5.3, dated January 25, 2005.*

- *CA eTrust ™ Security Command Center ™ Version 8 SP 1 with CR2 Patch, Test Report V0.1, dated December 20, 2006.*