Symantec™
Control Compliance Suite v10.5.1

Security Target

Evaluation Assurance Level (EAL): EAL3+
Document Version: 0.19

Prepared for:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
United States of America

Phone: +1 (650) 527-8000

http://www.symantec.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267-6050

http://www.corsec.com

Table of Contents

1 INTRODUCTION 4
1.1 PURPOSE 4
1.2 SECURITY TARGET AND TOE REFERENCES 4
1.3 PRODUCT OVERVIEW 5
1.4 TOE OVERVIEW 9
1.4.1 Brief Description of the Components of the TOE 11
1.4.2 TOE Environment 16
1.5 TOE DESCRIPTION 16
1.5.1 Physical Scope 16
1.5.2 Logical Scope 21
1.5.3 Product Physical/Logical Features and Functionality not included in the TOE 22
2 CONFORMANCE CLAIMS 23
3 SECURITY PROBLEM 24
3.1 THREATS TO SECURITY 24
3.2 ORGANIZATIONAL SECURITY POLICIES 25
3.3 ASSUMPTIONS 25
4 SECURITY OBJECTIVES 26
4.1 SECURITY OBJECTIVES FOR THE TOE 26
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 27
4.2.1 IT Security Objectives 27
4.2.2 Non-IT Security Objectives 27
5 EXTENDED COMPONENTS 28
5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS 28
5.1.1 Class EXT_CCS: Control Compliance System 29
5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS 34
6 SECURITY REQUIREMENTS 35
6.1.1 Conventions 35
6.2 SECURITY FUNCTIONAL REQUIREMENTS 35
6.2.1 Class FAU: Security Audit 37
6.2.2 Class FCS: Cryptographic Support 38
6.2.3 Class FMT: Security Management 39
6.2.4 Class FPT: Protection of the TSF 44
6.2.5 Class FTP: Trusted path/channels 44
6.2.6 Class EXT_CCS: Control Compliance System 44
6.3 SECURITY ASSURANCE REQUIREMENTS 46
7 TOE SUMMARY SPECIFICATION 47
7.1 TOE SECURITY FUNCTIONS 47
7.1.1 Security Audit 47
7.1.2 Cryptographic Support 48
7.1.3 Security Management 49
7.1.4 Protection of the TSF 50
7.1.5 Trusted Path/Channels 50
7.1.6 Control Compliance System 51
8 RATIONALE 54
8.1 CONFORMANCE CLAIMS RATIONALE 54
8.2 SECURITY OBJECTIVES RATIONALE 54
8.2.1 Security Objectives Rationale Relating to Threats 54
8.2.2 Security Objectives Rationale Relating to Assumptions 55
8.3 RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS 56

8.4 RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS....56
8.5 SECURITY REQUIREMENTS RATIONALE....57
8.5.1 Rationale for Security Functional Requirements of the TOE Objectives....57
8.5.2 Security Assurance Requirements Rationale....59
8.5.3 Dependency Rationale....60
9 ACRONYMS AND TERMS....62
9.1 ACRONYMS....62
9.2 TERMS....64
9.3 DOCUMENT REFERENCES....64

Table of Figures

FIGURE 1 - SAMPLE DEPLOYMENT OF THE TOE....10
FIGURE 2 - PHYSICAL TOE BOUNDARY....17
FIGURE 3 - EXT_CCS: CONTROL COMPLIANCE SYSTEM CLASS DECOMPOSITION....29
FIGURE 4 - SYSTEM DATA COLLECTION FAMILY DECOMPOSITION....30
FIGURE 5 - APPLICATION AND CHANGE CONTROL ANALYSIS FAMILY DECOMPOSITION....31
FIGURE 6 - SECURITY ALARMS FAMILY DECOMPOSITION....32
FIGURE 7 – RESTRICTIVE DATA REVIEW FAMILY DECOMPOSITION....33

List of Tables

TABLE 1 - ST AND TOE REFERENCES....4
TABLE 2 - TOE IDENTIFICATION AND BOUNDARY INFORMATION....18
TABLE 3 - TOE MINIMUM REQUIREMENTS....18
TABLE 4 - CC AND PP CONFORMANCE....23
TABLE 5 - THREATS....24
TABLE 6 - ASSUMPTIONS....25
TABLE 7 - SECURITY OBJECTIVES FOR THE TOE....26
TABLE 8 - IT SECURITY OBJECTIVES....27
TABLE 9 - NON-IT SECURITY OBJECTIVES....27
TABLE 10 - EXTENDED TOE SECURITY FUNCTIONAL REQUIREMENTS....28
TABLE 11 - TOE SECURITY FUNCTIONAL REQUIREMENTS....35
TABLE 12 - AUDITABLE EVENTS....37
TABLE 13- CRYPTOGRAPHIC KEY GENERATION STANDARDS....38
TABLE 14 - CRYPTOGRAPHIC OPERATIONS....39
TABLE 15 - MANAGEMENT OF TSF DATA....39
TABLE 16 - TOE ROLES....43
TABLE 17 - ASSURANCE REQUIREMENTS....46
TABLE 18 - MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS....47
TABLE 19 - THREATS:OBJECTIVES MAPPING....54
TABLE 20 - ASSUMPTIONS:OBJECTIVES MAPPING....55
TABLE 21 - OBJECTIVES:SFRS MAPPING....57
TABLE 22 - FUNCTIONAL REQUIREMENTS DEPENDENCIES....60
TABLE 23 - ACRONYMS....62
TABLE 24 - TERMS....64
TABLE 25 - DOCUMENT REFERENCES....64

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Symantec^{TM} Control Compliance Suite v10.5.1, and will also be referred to as the TOE or "CCS" throughout this document. The TOE is a software-only automated compliance and IT[1] risk management product. It ensures and demonstrates compliance with both external regulatory mandates and internal policies. The CCS also supports automated assessment of system security configuration, permissions, patches, and vulnerabilities. These services are provided in a software solution that uses both agent-less and agent-based data collection.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) - Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) - Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) - Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) - Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) - Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) - Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) - Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) - Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	Symantec Control Compliance Suite v10.5.1 Security Target
ST Version	Version 0.19
ST Author	Corsec Security, Inc.
ST Publication Date	8/25/2011
TOE Reference	Symantec^{TM} Control Compliance Suite v10.5.1
Keywords	Compliance, IT risk management, IT governance, and risk assessment

[1] IT = Information Technology

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The CCS automates key IT risk and compliance management tasks. The CCS demonstrates compliance to external regulatory mandates, such as PCI[2], DSS[3], and internal corporate policies. The CCS allows customers to link a written policy to specific technical and procedural standards. The policies features of the CCS can be used to manage, publish, and track policies across the organization. It can also help to collect evidence of due care of policy compliance. A policy is a formal statement of the practices, procedures, and codes of conduct employees should know and abide by in any business. Policies can include behaviors to comply with government regulations or the best practices specified by the standards bodies. They can also include behaviors specific to an enterprise. An authorized administrator can use the policies features in the CCS to create and distribute policies. In the CCS, all policies are mandates. Mandates are classed as either regulations or frameworks. Generally, regulations embody government regulations, while frameworks embody best practices. CCS installation may include one or more regulations or frameworks. In addition, an authorized administrator can use the Symantec Content Studio to create their own regulations and frameworks.

The Symantec Content Studio within the CCS lets an authorized administrator manage Symantec-created content in the CCS. It also lets an authorized administrator create his own custom content that can be used in the same way that Symantec-created content is used. Policies are mapped to the control statements that in turn are mapped to regulations and frameworks. A control statement is a concise statement of a discrete portion of a regulation or framework. Because regulations and frameworks have large areas of overlap, the control statements reduce repetition by stating each portion a single time. For example, where differences exist between regulation or framework statement requirements, a single control statement can exist to which each of the entries is mapped. Since both the regulation and the framework are mapped to the single control statement, the single control statement meets the requirements of both. Mapping helps to see the existing gaps in the current policies of an organization. These gaps can exist between organization's current policies and the mandates with which it must comply. Mapping also helps to meet the requirements of the mandates with which the organization must comply.

Customers can assess those policies using agent-less or agent-based tools distributed throughout a corporate IT environment. The CCS then scores these assessment results against specified risk criteria. The CCS supports automated assessment of system security configurations, permissions, patches, and vulnerabilities.

The full CCS product offering is made up of four separate products. Each product consists of a number of software or server components that work together to provide the complete CCS functionality. The four products that make up the CCS are as follows.

Components that are part of this evaluation:

1. CCSRA (Control Compliance Suite Reporting and Analytics) product - The CCSRA product automates key IT risk and compliance management tasks. *Note: The CCS product will be referred to as "CCSRA" throughout the ST and is only one component of the Control Compliance Suite. In the context of this document, when "CCS" is used, it refers to all of the Control Compliance Suite components including CCSRA, RAM, and RMS.*

[2] PCI = Payment Card Industry

[3] DSS = Data Security Standard

2. RMS - Risk Management Server – RMS gathers information from the network via bv-Control[4] snap-ins and agent-less data collection for various platforms.

3. RAM - Response Assessment Manager – RAM provides the ability to create and distribute questionnaires regarding policies and procedures as well as analyzes the responses received.

Components that are not part of this evaluation:

4. ESM - Enterprise Security Manager – Symantec ESM manages sensitive data and enforces security policies across Windows and UNIX client or server platforms.

The CCS can work as a consolidator of information gathered by both RMS and ESM; however, ESM is sold separately whereas RMS is always sold with the CCS. ESM is not a required component in the evaluated CCS configuration and does not affect the SFR functionality of the TOE. Therefore, it is not discussed further in this ST. RAM is sold as a separate product offering but is commonly sold alongside the CCS product. RAM resides within the TOE boundary and is a required component in the evaluated CCS configuration. Therefore, users must also purchase RAM when purchasing CCS to achieve full SFR functionality.

The CCS administrators create policies and exceptions and distribute these policies to computers and users on the network. An exception is when a policy is not applied under specific circumstances as configured through the CCS Console and CCS Web Console. When administrators define a policy, the CCS creates “jobs” to collect and evaluate data from servers and other computers on the network. Jobs are defined tasks that are carried out by the CCS components on behalf of the CCS administrator. There are two different types of jobs: data collection and evaluation. A data collection job collects data from managed devices based on specific standards and criteria configured by the CCS administrator. An evaluation job is created when an authorized administrator wants to evaluate the managed devices in the target network against specific standards and criteria. The managed devices are servers and other computers, called “assets” within the CCS that are located on the targeted network. “Data collectors” process jobs and gather information from the managed devices on the network. The CCS supports the following data collectors:

- Symantec RMS
- Symantec ESM
- CSV[5] files
- ODBC[6] database

For agent-based gathering of information from specific managed devices, Symantec RMS uses one or more bv-Control snap-in modules to collect data from managed devices on the target network. There is a bv-Control snap-in for each type of OS[7] and differing clients. The following bv-Control snap-in modules are supported:

- bv-Control for Windows
- bv-Control for UNIX
- bv-Control for Oracle
- bv-Control for Microsoft SQL[8] Server
- bv-Control for Microsoft Exchange
- bv-Control for Netware/NDS[9] eDirectory

[4] bv-Control = bv-Control snap-ins are for each client and are able to collect data from the managed devices on the targeted network.
[5] CSV = Comma-Separated Values
[6] ODBC = Open DataBase Connectivity
[7] OS = Operating System
[8] SQL = Structured Query Language
[9] NDS = Novell Directory Services

- bv-Control for NetWare

In addition to the agent based data collection as described above, the RMS data collector provides the CCS with agent-less data collection from the following asset types:

- Microsoft Windows client and server computers
- UNIX client and server computers
- Microsoft SQL Server databases
- Oracle databases

In addition, RMS data collectors can perform scans of the local area network. The discovery scan results will display the following information about the discovered assets:

- Identification (IP[10] address, hostname, etc)
- Type of asset (W2K[11] server, Oracle database, etc)
- New or existing asset (based on what already exists in the RMS database)
- Other meta-data

Collected data can then be evaluated against parameters that administrators have defined within created policies and exceptions. The CCS also scores assessment results against specified security risk criteria based on external regulatory mandates as well as internal policies configured by the CCS administrator. Evaluation results are stored in the production database as well. These evaluation results can be reviewed via reports by authorized administrators and used to adjust configurations or take action to enforce policies and mitigate IT risks.

CCS includes Security Content Automation Protocol (SCAP), which is a method for using specific standards that are defined by the National Institute of Standards and Technology (NIST). SCAP uses the standards to enable automated vulnerability management, measurement, and policy compliance evaluation of the enterprise organization. SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaws and security configuration information. CCS and SCAP facilitate an organization's automation of security monitoring, vulnerability management, and security policy compliance evaluation and reporting.

CCS supports the implementation of the SCAP 1.0 specification. The SCAP 1.0 specification comprises the following six component specifications:

- eXtensible Configuration Checklist Description Format (XCCDF) v1.1.4
- Open Vulnerability and Assessment Language (OVAL) v5.3
- Common Platform Enumeration (CPE) v2.2
- Common Configuration Enumeration (CCE) v5
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS) v2

CCS facilitates import of SCAP content that an authorized administrator downloads from the Website of NIST, http://fdcc.nist.gov/download.cfm . The content that an administrator imports into CCS cannot be edited. CCS allows an administrator to leverage the in-built functionality to execute the SCAP evaluation job that collects data from assets and evaluates them against the SCAP content. The Data Processing Service (DPS) that is configured as a Windows data collector performs the task of data collection and evaluation of SCAP content.

The CCS includes three SQL Server database instances: production database, evidence database, and reporting database. The production database stores the collected data, and information about the policies that are created in the CCS Console as well as the results of the evaluation jobs.

[10] IP = Internet Protocol

[11] W2K = Windows 2000

The CCS works with other products such as Symantec Data Loss Prevention and RAM in order to import evidence data from other sources. RAM enables the CCS administrators to create, distribute, and automatically collect user response questionnaire information which is used for procedural controls to meet both regulatory and internal compliance mandates. RAM questionnaire information is also stored in the production database. Once the response information is collected, it is then analyzed by RAM.

CCS integrates with other data collection sources via connectors for evidence import. CCS provides a mechanism to extend the evidence collection capabilities through the extended evidence sources system. This system allows an authorized administrator to collect evidence from the applications which are external to CCS and contribute towards the risk and compliance assessment and reporting process. The extended evidence sources system allows an authorized administrator to add an evidence source in CCS as well as configure the evidence source to read the evidence data. Evidence data must be arranged in the format that is defined in CCS. After the evidence data of the external application is converted into the defined format, the evidence source can be configured to collect this data periodically. The extended evidence sources system leverages the evidence source to contribute to the risk and compliance scores of the CCS assets.

The extended evidence source system also provides a mechanism for extending the controls which are used to assess the CCS assets. An authorized administrator can register the extended controls of an external application with this system and also map them with the control statements. The evidence source configuration, the evidence that is imported, and the extended controls are stored in the evidence database.

A Microsoft SQL Server instance hosts the evidence database. The evidence database stores the evidence gathered from the extended evidence sources that are registered with the CCS such as incident data from Symantec Data Loss Prevention and user response information from RAM.

The reporting database stores data specific to individual dashboards or reports. The reporting database is periodically synchronized with the data that is stored in the production database and the evidence database.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a software only IT risk and compliance management solution. It provides both agent-less and agent-based capabilities to audit and scan the managed devices. It automates the compliance process. In addition, it is able to identify problems with system configurations or internal controls.

Figure 1 shows the details of a sample deployment of the TOE:

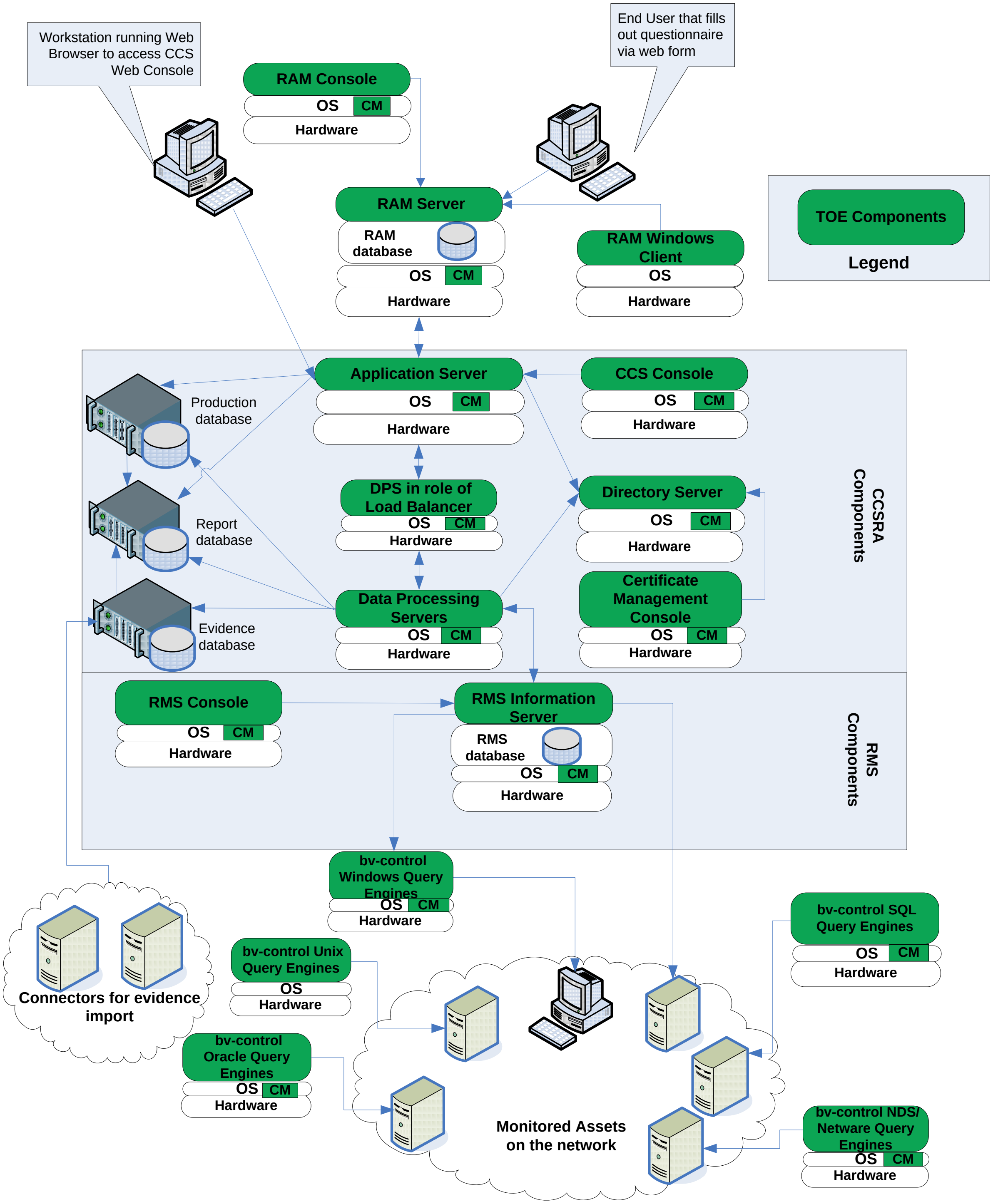

Figure 1 - Sample Deployment of the TOE[12]

[12] CM = Cryptographic Module

1.4.1 Brief Description of the Components of the TOE

The CCS consists of a number of components that work together. The components collect, store, and analyze data from a network, then transmit that data to authorized administrators in a usable form. In some instances, a single computer can serve in more than one capacity. Other functions require a dedicated server. Administrators use two primary interfaces to configure and manage the CCS: a thick client called the CCS Console and a web-based console called the CCS Web Console. In addition, the underlying Windows Operating System provides a FIPS Validated module that is considered to be part of the TOE Boundary. The Windows Operating System itself is not included in the TOE Boundary.

1.4.1.1 CCS Components

The CCS product offering is comprised of the following components:

- CCS product
  - Application Server
  - CCS Console
  - Directory Server
  - Certificate Management Console
  - Data Processing Server
- RMS
- Bv-control Windows
- Bv-control Unix
- Bv-control Oracle
- Bv-control SQL
- Bv-control NDS / Netware
- RAM

1.4.1.1.1 Application Server

The Application Server is the hub of the CCS. Authorized Administrators create both data collection and evaluation jobs in the CCS Console which are then sent to the Application Server. The Application Server manages the scheduled jobs and workflow. In addition, the Application Server manages data storage in the Directory Server which is used as a data repository for information about business objects, preferences, and other information. The Application Server includes the CCS Web Console which allows access to some CCS content without requiring the installation of the full CCS Console.

1.4.1.1.1.1 CCS Console

The CCS Console is a Windows application that runs on a client computer. The CCS Console allows access to the full range of CCS activities. Only users who have been assigned to roles that allow them to work in the CCS Console can perform activities in the CCS Console.

1.4.1.1.2 Directory Server

The Directory Server stores information about business objects, preferences, and other information. In addition, the CCS Directory Server hosts the certification authority for the CCS system which issues and validates certificates. Certificates are used to ensure secure communications between the CCS components. The Directory Server includes the Encryption Management Service, the Directory Support Service, and the Certificate Management Console.

1.4.1.1.2.1 Certificate Management Console

The Certificate Management Console runs on the same computer that hosts the Control Compliance Suite Directory. The Certificate Management Console lets an authorized administrator to create, renew, bind, unbind, or delete the certificates that the CCS uses. Certificates allow components to communicate securely in domains with no trust relationship. Certificates also enhance communications security within domains or between domains with a trust relationship. The Directory Server, Application Server, and Data Processing Server always require certificates. The Certificate Management Console must use a valid certificate to manage other certificates.

1.4.1.1.2.2 Symcert Command Line Interface

The Symcert Command Line Interface is used for installing and removing certificates on TOE server component systems. The utility is installed and automatically executed when a TOE server component is installed. Symcert adds the necessary certificate data to the component's configuration file.

1.4.1.1.2.3 Configure Service Account Utility Interface

The Configure Service Account Utility Interface is a Graphical User Interface (GUI) used for changing the service accounts of the application server service and the encryption management service. Some customers have a mandate that the install user should be different from the service accounts. A high privileged account is required for the installation of the product, but the same is not required for its functioning. Some customers change the service account to minimum privilege accounts once the installation is complete. This interface is also used for changing the encryption keys periodically as well as resetting the passphrases used to generate the encryption keys.

1.4.1.1.3 Data Processing Server

The Data Processing Server (DPS) is a single service that performs up to five different duties in the CCS. Each of these duties is called a role. Which role the DPS serves depends on how the DPS is registered. The DPS runs as a Windows Service. A single instance of the service can provide more than one role simultaneously. When a deployment contains multiple DPS installations, each DPS performs a single role.

The DPS performs the following roles: Load Balancer, Collector, Evaluator, Reporter, and Connector as described below.

1.4.1.1.3.1 DPS Load Balancer

When DPS acts as a load balancer, DPS routes data collection jobs from the Application Server to a DPS Collector. In addition, a load balancer routes the evaluation jobs to the DPS Evaluator and the reporting jobs to the DPS Reporter. If the deployment includes multiple load balancers, the Application Server automatically uses each in turn. If a load balancer fails, the Application Server automatically skips the failed load balancer and uses another load balancer. This round robin assignment gives limited fault tolerance.

1.4.1.1.3.2 DPS Collector

The DPS Collector is the interface to the programs that do the actual work of collecting data from a target network. A typical CCS deployment can include multiple data collectors, each linked with a single DPS Collector. The DPS Collector receives data collection jobs from the DPS Load Balancer and formats the job for the data collector. When the data collector processes the job and collects system data, the data collector transfers the system data to the DPS Collector. The DPS Collector then returns the collected data to the DPS Load Balancer. If necessary, the DPS Load Balancer combines the data with data from one or more other DPS Collectors. Finally, the DPS Load Balancer sends the data to the Application Server for storage in the database for use by the DPS Evaluator. The DPS Collector collects the data from the data collectors, which in turn collect the system data from the target network.

An eligible DPS Collector is any collector that has the ability to complete the data collection job. Within the evaluated configuration, CCS supports the following data collectors:

- Symantec RMS
- CSV files
- ODBC databases

1.4.1.1.3.3 DPS Evaluator

An evaluation job is comparing the system data collected against a specific standard or corporate policy. For example, does the password being used on a specific server meet the corporate policy of at least eight characters and is the password changed every three months. Evaluation jobs are sent from the Application Server to one of the DPS Load Balancers. The DPS Load Balancer then sends the evaluation job to the DPS Evaluator. The evaluator compares the data to the specifications in the standards that are configured through the CCS Console and then stores the evaluation results in the production database.

1.4.1.1.3.4 DPS Reporter

The DPS Reporter generates reports and dashboards for display by the CCS Console. In addition, a single DPS Reporter is assigned to perform database synchronization between the production database and the reporting database. The reporter executes the list of queries that are specific to the selected dashboard or the selected report. On the basis of these queries, the reporter retrieves data from the reporting database and creates the report. The DPS Reporter that is assigned to synchronize data synchronizes the contents of the reporting and the production databases. Synchronization occurs based on a schedule that is configured through the CCS Console or when an evaluation job triggers the synchronization.

1.4.1.1.3.5 DPS Connector

The DPS Connector is responsible for hosting the 3rd party integration framework which simplifies the effort required to integrate CCS with any third party data source and for importing data from these sources. The DPS Connector has out of the box support for a few products such as CCS Vulnerability Manager, Symantec Data Leakage Prevention, Symantec Response Assessment Module, and Symantec Risk Automation Suite. It also includes support for importing data from CSV and ODBC data sources. This is managed via the CCS Console. Once data is imported from these data sources via DPS Connector, it would reside in transient tables in the reporting database and would be subjected to other configurations/rules/conditions applied by the user while the time of configuration via the CCS Console. The processed data would then be synchronized and stored in the reporting database in a CCS specified format. As the data is in the CCS reporting database, it can easily be used by the authorized administrator for dashboards and policies.

1.4.1.1.4 RMS

RMS simplifies the management and administration of network operating systems, directories, and related applications. RMS gathers information from the network via bv-Control snap-ins and agent-less data collection. RMS works with the CCS to provide it information about the end user devices on the target network. RMS consists of the following components: RMS Information Server, and RMS Query Engines, and an RMS Console.

1.4.1.1.4.1 RMS Information Server

The RMS Information Server is the primary RMS component that processes data collection tasks and stores collected data. The CCS Load Balancers give the RMS Information Server a specific job to complete (i.e., what types of information to get and from which machines to get it). The RMS Information Server sends data collection jobs to one or more RMS Query Engines and then consolidates the collected data received from the RMS Query Engines. The RMS Information Server holds the ID[13]s and passwords for all the network assets it manages; this means the CCS product never has the local network asset's ID and passwords. RMS Information Server uses administrator level access to the assets to gather the needed information. This information is stored in an SQL Server database.

1.4.1.1.4.2 RMS Query Engines

The RMS Query Engines are the primary data collection engines. The RMS Query Engines primarily gather data without installing agents on the monitored assets; however, more recently one "dissolving" or self-removing agent has been created to gather specific information from assets running Windows Vista. The Query Engines process all requests for information from bv-Control for the client.

RMS retrieves system data from the target network and passes it on to the DPS Collector. When the RMS Query engine processes the job and collects the data, the RMS Information Server sends the data to the DPS Collector. The DPS Collector then forwards the collected data to the DPS Load Balancer. If necessary, the DPS Load Balancer combines the data with data from one or more other DPS Collectors. Finally, the DPS Load Balancer sends the data to the Application Server for storage in the database for use by the DPS Evaluator.

1.4.1.1.4.3 RMS Console

The RMS Console is the primary administrator interface for managing the bv-Control snap-in modules. The RMS Console installs as a snap-in to the Microsoft Management Console (MMC). The MMC is a host application that provides a common interface for the management snap-in modules such as the RMS Console.

1.4.1.2 Bv-control Windows Query Engines

The bv-control Windows Query Engines are the primary data collection engines for Windows devices. The bv-control Query Engines can gather data from Windows devices without installing agents on the monitored assets as well as via bv-control agents.

RMS retrieves system data from the target network and passes it on to the DPS Data Collector. When the bv-control Query engine processes the job and collects the data, the RMS Information Server sends the data to the DPS Data Collector.

1.4.1.3 Bv-control SQL Query Engines

The bv-control SQL Query Engines are the primary data collection engines for Windows SQL devices. Bv-control for Microsoft SQL Server version is an add-on to the RMS Console. The bv-control SQL Query Engines can gather data from SQL Server devices. Using bv-Control for Microsoft SQL Server, an authorized administrator can identify access rights, transactions, and modifications to the database, and review the SQL Server configuration. The bv-control for Microsoft SQL Server is an add-on to the RMS Console.

[13] ID = Identification

RMS retrieves system data from the target network and passes it on to the DPS Data Collector. When the bv-control Query engine processes the job and collects the data, the RMS Information Server sends the data to the DPS Data Collector.

1.4.1.4 Bv-control Unix Query Engines

The bv-control Unix Query Engines are the primary data collection engines for Unix devices. The bv-control Query Engines can gather data from Unix devices with a bv-control agent installed.

RMS retrieves system data from the target network and passes it on to the DPS Data Collector. When the bv-control Query engine processes the job and collects the data, the RMS Information Server sends the data to the DPS Data Collector.

1.4.1.5 Bv-control Oracle Query Engines

The bv-control for Oracle program provides tools to analyze and secure the Oracle devices. The bv-control for Oracle provides vulnerability management and reporting for Oracle databases by gathering system configuration settings and information. The bv-control for Oracle is an add-on to the RMS Console.

RMS retrieves system data from the target network and passes it on to the DPS Data Collector. When the bv-control Query engine processes the job and collects the data, the RMS Information Server sends the data to the DPS Data Collector.

1.4.1.6 Bv-control NDS[14] / Netware Query Engines

The bv-Control for NDS eDirectory product is a query-based addition to the RMS Console that installs into the RMS Console, extending the console's capabilities. With the bv-Control for NDS eDirectory add on, the RMS Console can access information from NDS trees on the target network.

The bv-Control for NetWare is a query-based addition to the RMS Console that installs into the RMS Console, extending the Console's capabilities. With the bv-Control for NetWare snap-in, the RMS Console can access information from NetWare servers on the target network. Using the bv-Control for NetWare product, an authorized administrator can view and manage the servers, volumes, directories, and files on a NetWare computer.

RMS retrieves system data from the target network and passes it on to the DPS Data Collector. When the bv-control Query engine processes the job and collects the data, the RMS Information Server sends the data to the DPS Data Collector.

1.4.1.7 RAM

RAM gives administrators an automated method of gathering information on procedural controls from individual employees through questionnaires. In other words, procedural controls are not programmatically assessable, and therefore require some human intervention (e.g., "Did the badge ID get taken from a terminated employee?" is not easily answered without a human response).

[14] Novell Directory Server

1.4.1.7.1 RAM Server

The RAM Server is the primary RAM component that processes the questionnaires. The RAM Server processes questionnaire inputs from end users. The RAM Server processes data collection tasks and stores the collected data in the RAM database. The questionnaires are made available on an internal web site via the RAM web client console that end users can access and use to provide response inputs to the questionnaires. In addition, a Windows based client software application can be installed on end user Windows machines on the target network. This program allows end users to provide answers to questionnaires while offline.

1.4.1.7.2 RAM Console

The RAM Console is the primary administrator interface for managing the RAM Server and for providing a GUI interface to create and manage the questionnaires. Authorized administrators can run reports based on the information received, which is stored in a SQL database.

1.4.1.8 FIPS Validated Cryptographic Modules

The Windows operating system provides a FIPS 140-2 validated cryptographic module #1337 for cryptographic functionality. Windows Server 2008 is the operating system used for the TOE Server components and it provides secure communication between TOE server components.

CCS uses another FIPS-enabled OpenSSL cryptographic module complying to the security policy of the OpenSSL FIPS module v1.2 #1111 for certificate generation as well as to secure the communication channel between the the bv-Control for UNIX snap-ins and the Information Server over SSH[15].

1.4.2 TOE Environment

The CCS relies on the underlying browser and web server to provide a secure session when a web based console is used to remotely connect to a TOE server component. For example when the CCS web console is used to access the CCS Server, the underlying browser provides the secure session with the IIS Server. Collected asset data is stored in Microsoft SQL Server databases. Stored data relies on the security that is built into the SQL Server.[16]

The CCS relies on a central Active Directory server to authenticate the administrators and users of the product. However, the CCS does verify that the administrator or user has been successfully authenticated before providing services. Microsoft Active Directory is considered to be outside the TOE Boundary.

Symantec RMS uses the Microsoft SQL Server 2005 Express database to store configuration information. The database is located on the computer that hosts the Information Server, but the database itself is considered outside the TOE Boundary. See Table 2 below for a detailed description of the environment relied upon by the TOE components.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. The TOE is software only and the TOE Components are specified in Table 2 below.

[15] SSH = Secure Shell

[16] [Plan Guide], section “How Control Compliance Suite data is secured”

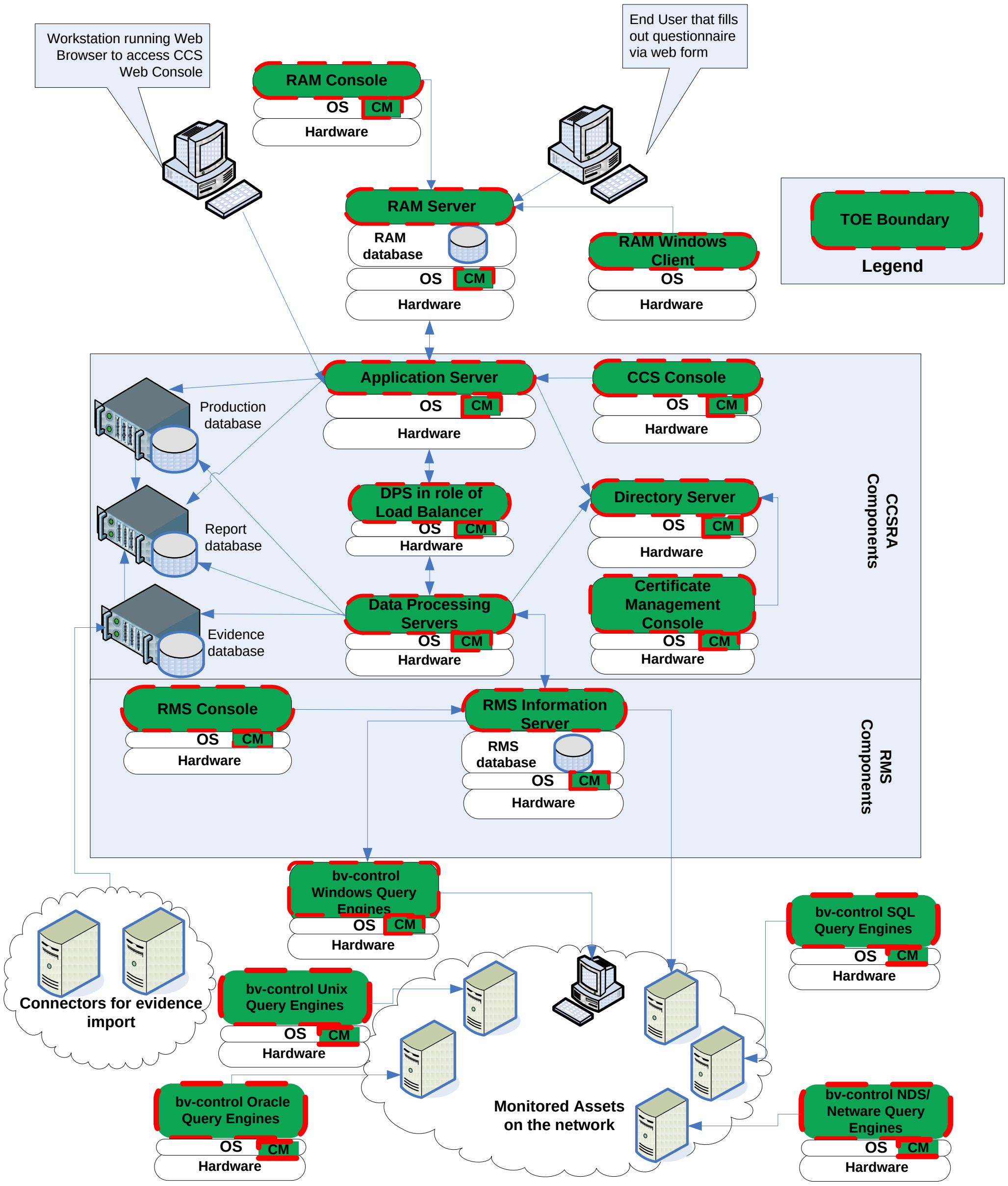
Workstation running Web Browser to access CCS Web Console
End User that fills out questionnaire via web form
RAM Console
OS
CM
Hardware
RAM Server
RAM database
RAM Windows Client
TOE Boundary
Legend
Application Server
CCS Console
Production database
Report database
Evidence database
DPS in role of Load Balancer
Directory Server
Data Processing Servers
Certificate Management Console
CCSRA Components
RMS Console
RMS Information Server
RMS database
RMS Components
bv-control Windows Query Engines
bv-control SQL Query Engines
Connectors for evidence import
bv-control Unix Query Engines
bv-control Oracle Query Engines
Monitored Assets on the network
bv-control NDS/ Netware Query Engines

Figure 2 - Physical TOE Boundary

The TOE Boundary includes all the Symantec-developed parts of the CCS product offering including the FIPS Validated cryptographic module provided by the underlying Windows Operating System for the TOE Server Components. The Windows Operating System itself is not included in the TOE Boundary. Any third-party source code or software that Symantec has modified is considered to be TOE Software. The TOE Boundary specifically does not include any of the third party software that the TOE relies upon as described in section 1.4.2 of the ST and Table 2 below. The TOE Boundary also does not include the third party SQL database that stores collected data about the managed devices. Table 2 below includes the TOE identification and boundary information.

Table 2 - TOE Identification and Boundary Information

Component	TOE	TOE Environment
CCSRA v10.5.1 10.50.530.20000	✓	
RMS v10.5.1 10.50.194.20000	✓	
RAM v10.5 10.50.166.10000	✓	
bv-control Windows v10.5.1	✓	
bv-control SQL Server v10.5.1	✓	
bv-control Oracle Subsystem v10.5.1	✓	
bv-control NDS/Netware v10.5.1	✓	
FIPS Validated cryptographic modules: (RSAENH FIPS 140-2 Certificate No. 1337) (OpenSSL FIPS module v1.2 FIPS Certificate No. 1111)	✓	
Underlying OS for all components		✓
Underlying Hardware		✓
API[17] Interfaces		✓
Microsoft SQL Server 2008 R2 Database		✓
Microsoft IIS[18] v6.0 or 7.0		✓

Table 3 below includes the TOE minimum requirements.

Table 3 - TOE Minimum Requirements

Component	Operating System	Memory	Processor	Hard Disk
Application Server	Windows Server 2003 SP2 Windows Server 2003 SP2 x64 Windows Server 2003 R2 SP2 Windows Server 2003 R2 SP2 x64 Windows Server 2008 Windows Server 2008 SP2 Windows Server 2008 x64 Windows Server 2008 SP2 x64 Windows Server 2008 R2 x64	2 GB	2.8 GHz	136 GB

[17] API – Application Programming Interface

[18] IIS = Internet Information Services

Component	Operating System	Memory	Processor	Hard Disk
Directory Server	Windows Server 2003 SP2 Windows Server 2003 SP2 x64 Windows Server 2003 R2 SP2 Windows Server 2003 R2 SP2 x64 Windows Server 2008 Windows Server 2008 SP2 Windows Server 2008 x64 Windows Server 2008 SP2 x64 Windows Server 2008 R2 x64	2 GB	2.8 GHz	136 GB
Data Processing Server	Windows Server 2003 SP2 Windows Server 2003 SP2 x64 Windows Server 2003 R2 SP2 Windows Server 2003 R2 SP2 x64 Windows Server 2008 Windows Server 2008 SP2 Windows Server 2008 x64 Windows Server 2008 SP2 x64 Windows Server 2008 R2 x64	2 GB	2.8 GHz	136 GB
CCS Console	WindowsXP Professional SP2 x64 Windows XP Professional SP3 Windows Vista Business or Enterprise Windows Vista Business or Enterprise SP1 Windows Vista Business or Enterprise SP2 Windows Vista Business or Enterprise x64 Windows Vista Business or Enterprise SP1 x64 Windows Vista Business or Enterprise SP2 x64 Windows 7 Windows 7 x64 Windows Server 2003 SP2 Windows Server 2003 SP2 x64 Windows Server 2003 R2 SP2 Windows Server 2003 R2 SP2 x64 Windows Server 2008 Windows Server 2008 x64 Windows Server 2008 R2 x64	2 GB	2.8 GHz	136 GB
RMS Information Server	Windows Server 2003 SP2 Windows Server 2003 SP2 x64 Windows Server 2003 R2 SP2 Windows Server 2003 R2 SP2 x64 Windows Server 2008 SP2 Windows Server 2008 SP2 x64 Windows Server 2008 R2	2 GB	2.8 GHz	160 GB

Component	Operating System	Memory	Processor	Hard Disk
RMS Console	Windows XP Professional SP2 Windows XP Professional SP2 x64 Windows Vista Business or Enterprise SP2 Windows Vista Business or Enterprise SP2 x64 Windows 7 Enterprise Windows 7 Enterprise x64 Windows Server 2003 SP2 Windows Server 2003 SP2 x64 Windows Server 2003 R2 SP2 Windows Server 2003 R2 SP2 x64 Windows Server 2008 SP2 Windows Server 2008 SP2 x64 Windows Server 2008 R2	1 GB	1.2 GHz	40 GB
RMS Query Engines	Windows Server 2008 R2	1 GB	Pentium IV 1.3 GHz	500 MB
bv-control Windows v10.5.1	Microsoft Windows XP Professional SP2, Microsoft Windows Server 2003 SP2 Microsoft Internet Explorer 5.0, 6.0, 7.0, or 8.0 Windows Server 2008 SP2	1 GB	Pentium IV 1.3 GHz	500 MB
bv-control SQL Server v10.5.1	Microsoft SQL Server Desktop Edition 1.0 and 2000 Microsoft SQL Server Standard Edition 7.0, 2000, and 2005 Control Compliance Suite overview 27 RMS data collector requirements Microsoft SQL Server Personal Edition 2000 Microsoft SQL Server Enterprise Edition 7.0, 2000, and 2005 Microsoft SQL Server Developer Edition 2000 and 2005 Microsoft SQL Server Workgroup Edition 2005	1 GB	Pentium IV 1.3 GHz	500 MB
bv-control Oracle Subsystem v10.5.1	Windows Server 2008 R2	1 GB	Pentium IV 1.3 GHz	500 MB
bv-control NDS/Netware v10.5.1	Novell Client 4.8 Windows Server 2008 R2	1 GB	Pentium IV 1.3 GHz	500 MB
Query Engine Component:	Windows Server 2008 R2	1 GB	Pentium IV 1.3 GHz	500 MB

Component	Operating System	Memory	Processor	Hard Disk
RAM Server	Microsoft Windows Server 2003 SP2 Microsoft Windows Server 2008 SP2 Microsoft Windows 7/XP Professional with SP2/Vista	256 MB	Pentium 4	40 MB
RAM Console	Microsoft Windows Server 2008 SP2	256 MB	Pentium 4	40 MB

1.5.1.1 Guidance Documentation

The following guides are required reading and part of the TOE:

- Symantec CCS User Guide
- Symantec CCS Installation Guide
- Symantec CCS Planning and Deployment Guide
- Symantec RMS Console and Information Server Getting Started Guide
- Symantec bv-Control for Windows Getting Started Guide
- Symantec bv-Control for Microsoft SQL Server Getting Started Guide
- Symantec CCS Guidance Documentation Supplement
- Symantec Response Assessment Module Installation Guide
- Symantec Response Assessment Module User Guide

1.5.1.1.1 The following subsections detail the TOE:

- Symantec CCS User Guide: sections "About the Control Compliance Suite Directory Server", Table 3-14
- Symantec CCS Planning and Deployment Guide: sections "About RMS Console", "About Information Server", "How the data collected by RMS is secured"
- RMS Console and Information Server Getting Started Guide: sections "About ActiveAdmin" and Table C-1

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

1.5.2.1 Security Audit

The CCS generates audit records for the actions of the CCS Components. Most security relevant Administrator actions within the CCS Console, the CCS Web Console, the RAM Console, and the RMS Consoles are audited. The CCS provides an authorized administrator access to view the audit logs created as a result of administrator actions through the CCS Console and the CCS Web Console via the reporting features.

1.5.2.2 Cryptographic Support

The Cryptographic Support of the TSF function provides cryptographic functions to issue X.509 certificates and manage those certificates. CCS manages key distribution using Public Key Infrastructure (PKI). Certificate Management is responsible for certificate generation and uses FIPS-enabled OpenSSL complying to the security policy of the OpenSSL FIPS module v1.2 (http://www.openssl.org/docs/fips/SecurityPolicy-1.2.pdf, FIPS Certificate No. 1111). Certificate generation uses RSA 2048 (and above) and SHA1 (and above) algorithms. In addition, the OpenSSL module provides the cryptographic functions for SSH between the RMS Information Server and the bv-control agents and registered Unix devices. The underlying Windows OS provides the cryptographic module, (RSAENH FIPS 140-2 Certificate No. 1337), for session encryption between TOE components as well as data encryption and decryption.

1.5.2.3 Security Management

The CCS provides a set of commands for administrators to manage the security functions, configuration, and other features of the CCS components. The Security Management function specifies user roles with defined access for the management of the CCS components.

1.5.2.4 Protection of the TSF

The CCS preserves a secure state in the event of the operational failure of a single Server Node when set up in a multi-TOE configuration.

1.5.2.5 Trusted path/channel

The TSF ensures all communications between the remote administrator user and the TOE components are via a trusted path for administration of the TOE. In addition, the communications between TOE components and another trusted IT product are secured via a trusted channel.

1.5.2.6 Control Compliance System

The agent-less clients and agents collect information from managed devices. This information includes machine hardware, software, system, network information, and questionnaire inputs. Alarms can be programmed in the CCS Console based on the collected information and settings made through the CCS Console and the CCS Web Console. In addition, the collected data is analyzed against policies and viewable only by authorized administrators.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Most features and functionality of the Control Compliance Suite v10.5.1 are part of the evaluated configuration of the TOE. The only exceptions are the following:

- all of the API interfaces will not be included in the TOE.
- Entitlements view and associated features are excluded from the TOE.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the CEM as of 2010/10/06 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL3+ augmented with ALC_FLR.2

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 5 - Threats

Name	Description
T.ACCOUNT	The security relevant actions of users may go undetected making the TSF data vulnerable to attack.
T.EXPLOIT	An attacker may attempt to gain unauthorized access to the resources of the managed devices, by exploiting vulnerabilities on a managed device.
T.SELPRO	An unauthorized user may read, modify, or corrupt security critical TOE configuration data while in transit between remote administrator users and TOE components as well as between TOE components and trusted IT products.
T.FALASC	The failure of a TOE component may result in the TOE failing to identify vulnerabilities or non compliant devices based on the association of System data received from all data sources.
T.TOEFAIL	The failure of the correct operation of a TOE component may result in the loss of collected data, its analysis, or the reporting functions of the TSF.
T.SPOOF	A hostile entity masquerading as the Server component may receive TSF data from an authorized agent that incorrectly thinks it is communicating with an authorized Server component.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 - Assumptions

Name	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.AUTHEN	The IT environment provides the TOE with identification and authentication of TOE users.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 7 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.ANALYZE	The TOE must accept data from the collectors and then apply analytical processes and information to derive conclusions about compliance (past, present, or future).
O.AUDIT	The TOE must provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of TOE security features as well as hold administrator users accountable for any actions they perform regarding the configuration of TOE Security functions.
O.CERT	The TOE must provide certificate issuance and management of certificates providing a unique identifier for TOE Components.
O.ROBUST	The TOE must secure all critical security data so that it is protected from unauthorized disclosure and modification while in transit between TOE components and between the TOE and remote trusted IT products.
O.SAFEFAIL	The TOE must protect the TSF and preserve correct operations in the event of specified failures.
O.SCAN	The TOE must be able to collect information from the managed devices and send alerts based on programmable alarms.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 8 - IT Security Objectives

Name	Description
OE.AUTHEN	The TOE environment must provide identification and authentication for the TOE.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

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

Table 9 - Non-IT Security Objectives

Name	Description
OE.MANAGE	Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PROTECT	Those responsible for the TOE must ensure that the physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE

Table 10 - Extended TOE Security Functional Requirements

Name	Description
EXT_CCS_SDC.1	System data collection
EXT_CCS_RDR.1	Restricted data review
EXT_CCS_ANL.1	Analysis
EXT_CCS_ARP.1	Security alarms

5.1.1 Class EXT_CCS: Control Compliance System

The Control Compliance System functionality involves collecting information from managed devices, analyzing the data for compliance, and sending alerts based on programmable alarms. The EXT_CCS: Control Compliance System functionality class was modeled after the CC FAU: Security audit class. The extended family and related components for EXT_CCS_SDC: System data collection was modeled after the CC family and related components for FAU_GEN: Security audit data generation. The extended family EXT_CCS_ANL: Analysis was modeled after the family FAU_SAA: Potential Violation Analysis. The extended family EXT_CCS_ARP: Security alarms was modeled after the CC family FAU_ARP: Security alarms. The extended family EXT_CCS_RDR: Restrictive Data Review was modeled after the CC family FAU_SAR: Security audit review.

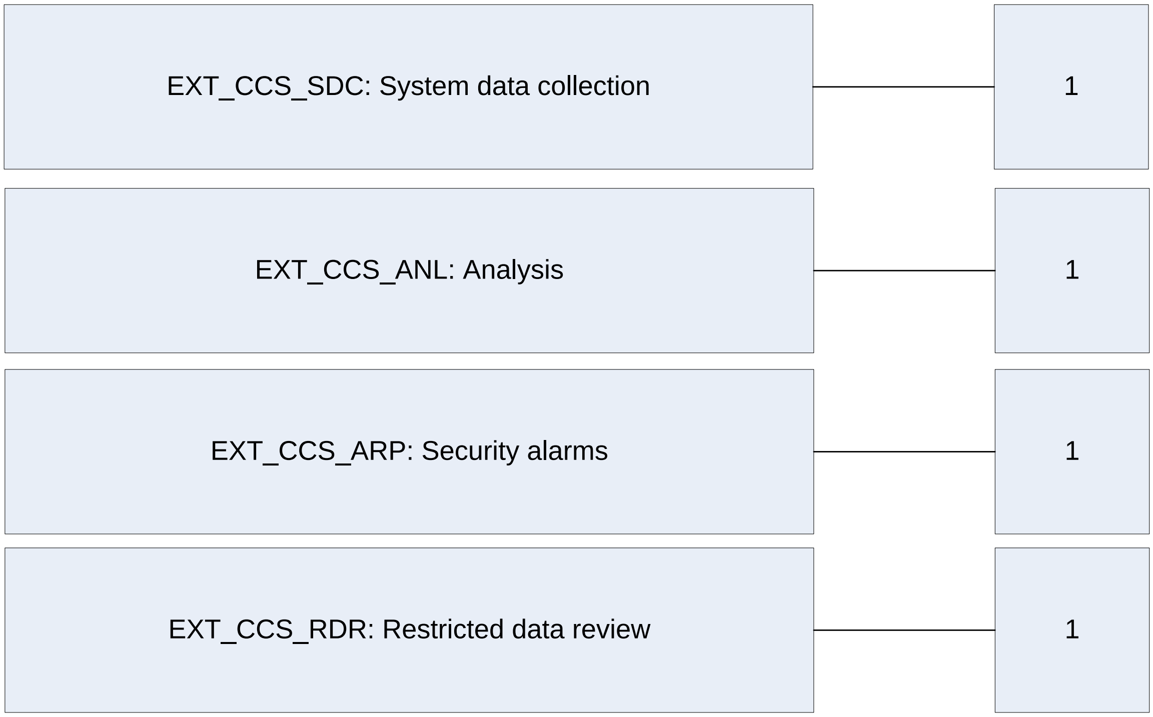
EXT_CCS_SDC: System data collection
1
EXT_CCS_ANL: Analysis
1
EXT_CCS_ARP: Security alarms
1
EXT_CCS_RDR: Restricted data review
1

Figure 3 - EXT_CCS: Control Compliance System class decomposition

5.1.1.1 System data collection (EXT_CCS_SDC)

Family Behaviour

This family defines the requirements for recording data. This family identifies the level of system data collection, enumerates the types of information that shall be collected by the TSF, and identifies the minimum set of CCS-related information that should be provided within various CCS record types.

Component Leveling

Figure 4 - System data collection family decomposition

EXT_CCS_SDC.1 System data collection, defines the level of information, and specifies the list of data that shall be recorded in each record.

Management: EXT_CCS_SDC.1

a) There are no auditable events foreseen.

Audit: EXT_CCS_SDC.1

b) There are no auditable events foreseen.

EXT_CCS_SDC.1 System data collection
Hierarchical to: No other components
EXT_CCS_SDC.1.1

The TSF shall be able to collect the following information from the managed device(s): [assignment: *specifically defined information*.]

EXT_CCS_SDC.1.2

At a minimum, the TSF shall collect and record the following information:

- Date and time of the data collection, type of data, subject identity, and the outcome (success or failure) of the collection.

Dependencies: FPT_STM.1 Reliable time stamps

5.1.1.2 Analysis (EXT_CCS_ANL)

Family Behaviour

This family defines the analysis the TOE performs on the collected application and change control data. This family enumerates the types of program code that shall be collected by the TSF, and identifies what type of control will be enforced on the executable code. This family also determines which changes are to be prevented, and which are to be monitored and reported.

Component Leveling

EXT_CCS_ANL: Analysis
1

Figure 5 - Application and Change Control Analysis family decomposition

EXT_CCS_ANL.1 Application and change control analysis, specifies the list of analyses the TOE will perform on the collected application data.

Management: EXT_CCS_ANL.1

- Maintenance of the analysis functions by (adding, modifying, deletion) of policies from the set of policies.

Audit: EXT_CCS_ANL.1

- Minimal: Enabling and disabling of any of the analysis mechanisms.

EXT_CCS_ANL.1 Application and change control analysis

Hierarchical to: No other components

EXT_CCS_ANL.1.1

The TSF shall perform the following analysis function(s) on all System data collected:

- *[assignment: analytical functions.]*

Dependencies: EXT_CCS_SDC.1

5.1.1.3 Security alarms (EXT_CCS_ARP)

Family Behaviour

This family defines the requirements for the response to be taken in case of a detected system data change or policy enforcement.

Component Leveling

Figure 6 - Security alarms family decomposition

EXT_CCS_ARP.1 Security alarms, the TSF shall take actions in case a detected system data change or policy enforcement.

Management: EXT_CCS_ARP.1

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of alarm.

Audit: EXT_CCS_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Actions taken due to a detected system data change or policy enforcement.

EXT_CCS_ARP.1 **Security alarms**
Hierarchical to: **No other components**
EXT_ CCS_ARP.1.1

The TSF shall take [*assignment: list of actions*] upon the trigger of a programmable alarm.

Dependencies: EXT_CCS_SDC.1 System data collection

5.1.1.4 Restricted data review (EXT_CCS_RDR)

Family Behaviour

This family defines the requirements for system data tools that should be available to authorized users to assist in the review of system data.

Component Leveling

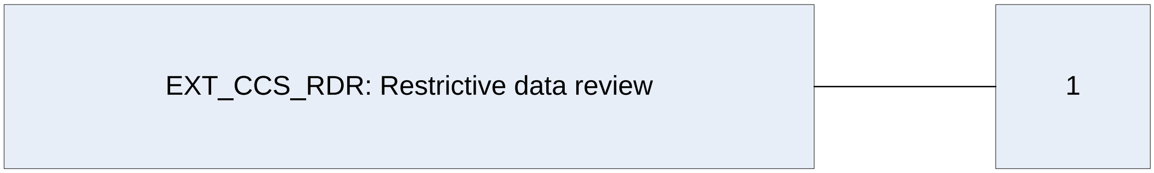

Figure 7 – Restrictive data review family decomposition

EXT_CCS_RDR.1 Restricted data review, the TSF shall take actions in case a detected system data change or policy enforcement.

Management: EXT_CCS_RDR.1

The following actions could be considered for the management functions in FMT:

There are no management activities foreseen.

Audit: EXT_CCS_RDR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Unsuccessful attempts to read information from the system data.

EXT_CCS_RDR.1 Restricted Data Review
Hierarchical to: No other components

EXT_CCS_RDR.1.1

The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

EXT_CCS_RDR.1.2

The TSF shall provide the System data in a manner suitable for the user to interpret the information.

EXT_CCS_RDR.1.3

The TSF shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.2	Cryptographic key distribution		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FTP_TRP.1	Trusted path	✓	✓		
FTP_ITC.1	Trusted channel	✓	✓		

Name	Description	S	A	R	I
EXT_CCS_ARP.1	Security alarms		✓		
EXT_CCS_SDC.1	System data collection		✓		
EXT_CCS_RDR.1	Restricted data review		✓		
EXT_CCS_ANL.1	Analysis		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

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

b) All auditable events, for the [not specified] level of audit; and

c) [*the specifically defined auditable events as listed in the 'Auditable Events' column of Table 12*].

Table 12 - Auditable Events

Server
CCS Console user login attempts (success and failure)
Administrative actions performed as operations on TSF Data as described in Table 15 except for View actions.

FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1

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

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

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*CCS Administrator*] with the capability to read [*all information*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1

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

Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*listed in the 'Key Generation Algorithm' column of Table 12*] and specified cryptographic key sizes [*listed in the 'Cryptographic Key Size' column of Table 12*] that meet the following: [*standards listed in the 'Standards' column of Table 12*].

Table 13- Cryptographic Key Generation Standards

Key Generation Algorithm	Cryptographic Key Size	Standards
RSA[19]	2048, 4096	FIPS 186-2
AES[20]	256	FIPS 197
SHA[21]		FIPS PUB 180-2

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2 Cryptographic key distribution
Hierarchical to: No other components.
FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [*certificate-based key management*] that meets the following: [*FIPS PUB 140-2, Security Level 1*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 Level 1*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

[19] RSA = Rivest, Shamir and Adleman
[20] AES = Advance Encryption Standard
[21] SHA = Secure Hash Algorithm

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1

The TSF shall perform [assignment *cryptographic operations listed in the 'Cryptographic Operations' column of Table 13*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the 'Cryptographic Algorithm' column of Table 13*] and cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 13*] that meet the following: [*the list of standards in the 'Standards' column of Table 13*].

Table 14 - Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards
Digital Signature Generation and Key Pair Generation	RSA	2048, 4096	FIPS 186-3 (cert #323)
Message Digest	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	Not applicable	FIPS 180-2 (cert #723)
Symmetric encryption and decryption	AES	256	FIPS-197 (cert # 1168)

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

6.2.3 Class FMT: Security Management

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [query, modify, delete, clear, [*and other operations as defined in column 'Operation' of Table 15*]] the [*TSF data as defined in column 'TSF Data' of Table 15*] to [*the authorized identified roles as defined in column 'Authorized Role' of Table 15*].

Table 15 - Management of TSF Data

Operation	TSF Data	Authorized Role
CCS Console		
Add, remove	User	CCS Administrator, Power User, Custom role granted permission
Add	User/group to a role	CCS Administrator, Power User, Custom role granted permission
Remove	User/group from a	CCS Administrator, Power User, Custom role granted

Operation	TSF Data	Authorized Role
	role	permission
Create, Edit, Delete	Role	CCS Administrator, Power User, Custom role granted permission
View	Roles and permissions	Standards Administrator, Policy Administrator, Reporting Administrator, Custom role granted permission
View	Roles	Policy Approver, Policy Reviewer, Custom role granted permission
Assign, Remove	Permissions to user/group	CCS Administrator, Power User, Custom role granted permission
Register	DPS	CCS Administrator, Power User, Custom role granted permission
Configure	Data collectors	CCS Administrator, Power User, Custom role granted permission
Create, edit, delete, review, approve, publish, unpublish, and track	Policies	CCS Administrator, Policy Administrator, Custom role granted permission
Accept, decline, request, view	Policies	CCS User, Policy Audience, Policy Administrator, Custom role granted permission
Approve	Policies	Policy Approver, Custom role granted permission
Review	Policies	Policy Reviewer, Custom role granted permission
Create, edit, run, schedule, and delete	Jobs	CCS Administrator, Standards Administrator, Standards Evaluator, Remediation Administrator, Policy Administrator, Reporting Administrator, Custom role granted permission
View	Jobs	Auditor, Report Result Viewer, Custom role granted permission
Create, edit, view, generate, remove	Reports	CCS Administrator, Power User, Custom role granted permission
View	Reports	Auditor, Custom role granted permission
View	Assets	CCS Administrator, Power User, Standards Administrator, Assets Viewer, Policy Administrator, Policy Approver, Policy Reviewer, Reporting Administrator, Custom role granted permission
Generate, View	Reports	Standards Administrator, Standards Evaluator, Remediation Administrator, Policy Administrator, Reporting Administrator, Report Result Viewer, Custom role granted permission
Approve	Exceptions	Exception Approver, Custom role granted permission
Request	Exceptions	Exception Requestor, Policy Administrator, Custom role granted permission

Operation	TSF Data	Authorized Role
Manage	Configuration Settings	CCS Administrator, Power User, Standards Administrator, Remediation Administrator, Policy Administrator, Reporting Administrator, Custom role granted permission
Web Console		
Accept, decline, request, view	Policies	CCS User, Policy Audience, Policy Administrator, Custom role granted permission
Respond	Response Assessment module questions	RAM Administrator, Custom role granted access rights
View	Dashboard	CCS Administrator, Power User, Standards Administrator, Assets Viewer, Policy Administrator, Policy Approver, Policy Reviewer, Reporting Administrator, Custom role granted permission
Certificate Management Console		
Create, renew, bind, unbind, or delete	certificates	CCS Administrator, Power User, Standards Administrator, Remediation Administrator, Policy Administrator, Reporting Administrator, Custom role granted permission
Symcert Command Line Interface		
Install, uninstall, view	certificates	CCS Administrator
Configure Service Account Utility Interface		
Change	service accounts, encryption keys	CCS Administrator
Reset	passwords	CCS Administrator
RMS Console		
Configure	bv-Control modules to collect data	RMS Administrator granted access rights
Query	Network and database resources for collected data	RMS Administrator granted access rights
Generate	Baseline reports of changes to queried data	RMS Administrator granted access rights
Assign	user BindView Administrator right	RMS Administrator granted access rights
Delete, edit	Resource Objects	RMS Administrator granted access rights
Delete	Historical datasets, session logs	RMS Administrator granted access rights
Create, modify	Queries	RMS Administrator with processing granted access rights
Assign	Right to create and	RMS Administrator granted access rights

Operation	TSF Data	Authorized Role
	modify queries	
Assign	right to use ActiveAdmin	RMS Administrator granted access rights
Create and run	historical dataset queries	RMS Administrator granted access rights
Assign	credential database to a user	BindView User granted access rights
Modify or delete	credential database	BindView User granted access rights
Assign	right to create and modify task lists	RMS Administrator granted access rights
Start, Stop, and restart	Agents	RMS Administrator granted access rights
RAM Console		
Create	Questionnaire	RAM Administrator, RAM Power User, granted access rights
Generate	Reports	RAM Administrator, RAM Power User, granted access rights

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*see Table 15*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*the authorised identified roles as listed in Table 16 below*].

Table 16 - TOE Roles

CCS Console, CCS Web Console, Certification Management Console
• CCS Administrator • Power User • Auditor • CCS User • Policy Audience • Asset Viewer • Standards Administrator • Standards Evaluator • Remediation Administrator • Exception Approver • Exception Requestor • Policy Administrator • Policy approver • Policy Reviewer • Reporting Administrator • Report Results Viewer • Custom
Symcert Command Line Interface
• CCS Administrator
Configure Service Account Utility Interface
• CCS Administrator
RMS Information Server, RMS Console
• RMS Administrator • BindView User
RAM
• RAM Administrator • RAM Power User

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.4 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*operational failure of a single Server Node when in a multi-TOE configuration*].

Dependencies: No dependencies.

6.2.5 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*communications between TOE components and external authorized IT entities*].

Dependencies: No dependencies

FTP_TRP.1 Trusted path
Hierarchical to: No other components.
FTP_TRP.1.1

The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2

The TSF shall permit [the TSF and remote users] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [*secure communications when users connect to a TOE management console*].

Dependencies: No dependencies

6.2.6 Class EXT_CCS: Control Compliance System

EXT_CCS_SDC.1 System data collection
Hierarchical to: No other components
EXT_ CCS_SDC.1.1

The TSF shall be able to collect the following information from the managed device(s):

- [*All hardware information*
- *All installed software*
- *System Information*
- *Current network settings*
- *Scan information from the local area network*
- *User Privileges*

- *Database Audit Trail*
- *Audit Trail*
- *Questionnaire inputs*]

EXT_ CCS_SDC.1.2

At a minimum, the TSF shall collect and record the following information:

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

Dependencies: FPT_STM.1 Reliable time stamps

EXT_CCS_ANL.1 Analysis

Hierarchical to: No other components

EXT_CCS_ANL.1.1

The TSF shall perform the following analysis function(s) on all System data collected:

[

- *comparing collected system data at some point in time with those of another point in time to detect the differences (baseline);*
- *comparing collected system data with a set of standards;*
- *comparing collected system data with a set of policies;*
- *comparing collected system data with a set of exceptions.*]

Dependencies: EXT_CCS_SDC.1

EXT_CCS_RDR.1 Restricted data review

Hierarchical to: No other components

EXT_CCS_RDR.1.1

The TSF shall provide [*authorized administrator*] with the capability to read [*all collected information*] from the System data.

EXT_CCS_RDR.1.2

The TSF shall provide the System data in a manner suitable for the user to interpret the information.

EXT_CCS_RDR.1.3

The TSF shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

Dependencies: No dependencies

EXT_CCS_ARP.1 Security alarms

Hierarchical to: No other components

EXT_ CCS _ARP.1.1

The TSF shall take [*action to send a notification via e-mail or create an alert*] upon the trigger of a programmable alarm.

Dependencies: EXT_CCS_SDC.1 System data collection

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3 augmented with ALC_FLR.2. Table 17 - Assurance Requirements summarizes the requirements.

Table 17 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw Reporting Procedures
	ALC_LCD.1 Developer defined life-cycle model
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 18 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
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
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Security Management	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
Trusted path/channels	FTP_TRP.1	Trusted path
	FTP_ITC.1	Trusted channel
Control Compliance System	EXT_CCS_ARP.1	Security alarms
	EXT_CCS_SDC.1	System data collection
	EXT_CCS_RDR.1	Restricted data review
	EXT_CCS_ANL.1	Analysis

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. As administrators manage and configure the TOE, their activities are tracked and recorded as audit records with the administrator id and are stored in the production database.

The CCS provides auditing of most administrator actions that occur within the CCS Console, the CCS Web Console, the RMS Console, Certificate Management Console, Symcert Command Line Interface, API Interface, and CSA Utility Interface. The CCS provides an authorized administrator access to view the audit logs created as a result of administrator actions through the CCS Console via the reporting features. In the CCS Console, the Evaluation Results view details each job that has been run. Only authorized administrators with the appropriate role and permissions can review the security audit logs.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2.

7.1.2 Cryptographic Support

The Cryptographic Support of the TSF function provides cryptographic functions to issue X.509 certificates and manage those certificates. This provides for certificates to be issued to TOE Server Components. A certificate helps to secure the environment by functioning as a unique identifier for communications between CCS TOE Server components including the Directory Server, Application Server, and the Data Processing Server.

CCS manages key distribution using Public Key Infrastructure (PKI). This allows the Directory Server, Application Server, and Data Processing Servers to communicate securely in domains with no trust relationship. Certificate Management is responsible for certificate generation and uses FIPS-enabled OpenSSL complying to the security policy of the OpenSSL FIPS module v1.2 (http://www.openssl.org/docs/fips/SecurityPolicy-1.2.pdf, FIPS Certificate No. 1111). Certificate generation uses RSA 2048 (and above) and SHA1 (and above) algorithms.

In addition, the Cryptographic Support of the TSF function provides cryptographic functions to secure the communication channel between the the bv-Control for UNIX snap-ins and the Information Server is secured over SSH. SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices and provides confidentiality and integrity of data sent over an unsecure network. Both the Information Server and the bv-Control for Unix uses OpenSSH which is provided by the FIPS-enabled OpenSSL complying to the security policy of the OpenSSL FIPS module v1.2 (http://www.openssl.org/docs/fips/SecurityPolicy-1.2.pdf, FIPS Certificate No. 1111).

In addition, the cryptographic functionality within the Windows operating system component is used to provide the following:

1. WCF[22] Channel Encryption is used with AES256 and SHA1for all communications to and from the Application Server (RSAENH FIPS 140-2 Certificate No. 1337).

2. The .Net framework 3.5 AesCryptoServiceProvider calls the RSAENH cryptographic module to perform symmetric encryption and decryption using the Cryptographic Application Programming Interfaces (CAPI) implementation of the Advanced Encryption Standard (AES) algorithm. This provides secure storage of sensitive information including user credentials and database connection strings (RSAENH FIPS 140-2 Certificate No. 1337).

3. WCF Channel Encryption implements SSL to secure the communications channel between TOE Components that reside on the Windows OS (RSAENH FIPS 140-2 Certificate No. 1337).

Public and private keys are provided to the Module by the calling process, and are destroyed in memory when released by the appropriate API function calls. Zeroization of sensitive data is performed automatically by API function calls for intermediate data items, and on demand by the calling process using

[22] WCF = Windows Communication Foundation

the Module provided API function calls provided for that purpose. Only the process that creates or imports keys can use or export them. The calling process can perform key zeroization of keys by calling an API function. No persistent storage of key data is performed by the Module.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1.

7.1.3 Security Management

Security management specifies how the CCS manages several aspects of the TSF including TSF data and security functions. TSF data includes configuration data of the TOE, audit data, and system data. For a detailed listing of TSF data managed by the TOE see Table 15 of this ST. The TOE provides authorized administrators with several GUI consoles as described in section 1.4.1 to easily manage the security functions and TSF data of the TOE.

The CCS supports a combination of roles and permissions-based access control. In the CCS a role is a collection of predefined tasks or functions. The administrator may perform each task that is a specific action, such as Create a policy or Run an evaluation. When the administrators log on, they see only a filtered view of the overall application that is appropriate for their role. The role defines the access privileges for the views and tasks. The permissions that the administrators and users have on the objects in the CCS Directory determine the tasks that they can perform on an object.

To have a role does not automatically grant the administrator the rights that are required to perform the task on the directory objects. In addition to the role, the administrator must have access rights on the required directory objects to successfully perform a task. For example, if the administrator is in the Evaluators role, the administrator is allowed to set up and run evaluation jobs. But when the evaluation job is run, the results are based only on the assets for which the user has been granted the Evaluate permission.

The Control Compliance Suite is delivered with a number of predefined roles that cannot be edited, but custom roles may be created. The CCS Console and the CCS Web Console use the following predefined roles as described in Table 16 under ‘CCS Console, CCS Web Console, and Certification Management Console’ of this ST.

The RMS Information Server and RMS Console enforce their own set of roles for the management of RMS functionality. RMS creates the bvConsole Admins and the bvConsole Users Windows user groups. The users in the bvConsole Admins group are RMS Administrators. The users in the bvConsole Users Windows user group are Bindview Users. The RMS components of the product use the following predefined roles as described in Table 16 under ‘RMS Information Server, RMS Console’ of this ST.

RAM enforces its own set of roles and manages the access control for RAM functionality. RAM uses the predefined roles as described in Table 16 under ‘RAM’ of this ST.

The CCS Console and the CCS Web Consoles allow an authorized administrator to manage and apply exceptions to organizational policies.

The Certificate Management Console provides a GUI[23] interface for authorized administrators to issue and manage certificates. In a distributed system, an authorized administrator creates the TOE Server certificate manually using the console. Using the console, authorized administrators can create, renew, bind, unbind, or remove certificates.

The Symcert Command Line Interface enforces the management of the CCS certificates on the Application Server host machine. In addition, the CSA Utility Interface is used for the management of encryption keys.

TOE Security Functional Requirements Satisfied: FMT_SMR.1, FMT_MTD.1, FMT_SMF.1.

[23] GUI = Graphical User Interface

7.1.4 Protection of the TSF

The Protection of the TSF function provides limited fault tolerance. When the DPS acts as a load balancer, the DPS routes data collection jobs from the Application Server to a DPS Collector. In addition, a load balancer routes the evaluation jobs to the DPS Evaluator and the reporting jobs to the DPS Reporter. When the deployment includes multiple load balancers, the Application Server automatically uses each in turn. If a load balancer fails, the Application Server automatically skips the failed load balancer and uses another load balancer. This round robin assignment gives limited fault tolerance.

The bv-Control snap-ins are responsible for collecting data from the network. The DPS Collector retrieves the data that has been collected from the bv-Control snap-ins. When the CCS has multiple DPS Collectors and associated data collectors, the load balancer assigns jobs to eligible collectors sequentially. If a query requires input from several DPS Collectors, the load balancer distributes the query appropriately. When the DPS Collectors complete the query, the load balancer combines the results and returns the results to the Application Server for storage.

The DPS Evaluator compares collected data to the standards that an authorized administrator specifies and saves the results for later use. When the CCS has multiple DPS Evaluators, the load balancer assigns jobs to evaluators sequentially.

TOE Security Functional Requirements Satisfied: FPT_FLS.1.

7.1.5 Trusted Path/Channels

The CCS provides trusted path/channels for all data from disclosure or modification while in transit between TOE components and when an authorized administrator connects to the TOE via the CCS Web Console. All communications between the CCS Web Console and the Application Server are secured via a trusted path. When an authorized administrator logs in to any CCS, RMS, and RAM Console, a secured SSL/TLS session is initiated by the TSF to secure the session.

All communications between the TOE Components are secured via a trusted channel. More specifically, collected system data is transferred to the RMS Information Server database, between the RMS Information Server and the RMS Console, and to the Data Processing Service Collector. For all data transfers, the RMS Information Server initiates a SSL session provided by the FIPS 140-2 validated cryptographic module on the Windows operating system component.

When configuration information is transmitted to the Information Server by the RMS Console, the RMS Console initiates an SSL session using the FIPS 140-2 validated cryptographic module on the Windows Server 2008 operating system component to protect it from interception or decryption. When the Information Server transmits credentials to network resources, the credentials are protected by SSL as well.

The standard communication method that is used between Master and Slave Query Engines and the Information Server is the Remote Procedure Call (RPC) over TCP/IP. When using a Windows Server 2008 Domain Controller, after bv-Control for Windows is installed, this communication is automatically encrypted for security purposes. RPC is a function on the Windows operating system component which calls a FIPS 140-2 validated cryptographic module that negotiates the highest level of encryption protocols that it can to secure the communications channel.

The standard communications channel that is used between the bv-Control for UNIX snap-ins and the Information Server is secured over SSH[24]. SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices and provides confidentiality and integrity of data sent over an unsecure network. Both the Information Server and the bv-Control for Unix uses OpenSSH which is provided by the FIPS-enabled OpenSSL complying to the security policy of the OpenSSL FIPS module v1.2 (http://www.openssl.org/docs/fips/SecurityPolicy-1.2.pdf).

All administrator web based console sessions are secured via SSL/TLS. When an administrator user or end user initiates one of these sessions with a TOE Server Component, the user designates the HTTPS session. This in turn causes the browser on the administrator or end user client machine to initiate a web session via SSL with the IIS Server on the TOE Server Component. Both the browser and the IIS Server use the FIPS 140-2 validated cryptographic module on the Windows operating system component to protect the communications channel from interception or decryption.

All administrator console sessions are secured via SSL/TLS. When an administrator initiates one of these sessions with a TOE Server Component, the TOE calls the FIPS certified cryptographic module available in the OS. This provides cryptographic functions to protect TSF data from disclosure or modification while in transit between CCS Server components and between managed devices and CCS components. The data that is collected is secured while in transit by SSL/TLS connections between computers. This encryption secures the collected asset and TSF data while in transit.

All sensitive information is stored securely including user credentials and database connection strings. CCS calls the FIPS certified cryptographic module available in the .Net framework 3.5 (AesCryptoServiceProvider) to secure sensitive information stored in secure storage.

For Windows authentication the default WCF[25] encryption algorithm AES256 encryption is used. This encryption secures the configuration data while in transit. WCF Channel Encryption provides WCF message security with AES256 and SHA1 (default setup) for all communications to and from the Application Server. The TOE calls a FIPS 140-2 validated cryptographic module available in the .Net framework.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1.

7.1.6 Control Compliance System

The CCS provides the collection of system data, analysis of the system data collected, and alerts that are sent based on the analysis. The RMS Information Server is the primary RMS component that processes data collection tasks and stores the collected data.

For gathering information from specific managed devices, Symantec RMS uses one or more bv-Control snap-in modules to collect data from the target network. The bv-Control snap-ins for each client are able to collect data from the managed devices on the target network. The data collected is specified in section 6.2.6. The bv-Control snap-ins employ a scalable, client-server architecture that provides specialized options for system data collection.

The RMS data collector provides the CCS with agent-based data collection via the bv-Control snap-ins. In addition, RMS provides for agent-less data collection from the following asset types:

- Microsoft Windows client and server computers
- UNIX client and server computers
- Oracle databases
- Microsoft SQL Server databases

[24] SSH = Secure Shell

[25] WCF = Windows Communication Foundation

The RMS data collectors can perform scans of the local area network. The discovery scan results will display the following information about the discovered assets:

- Identification (IP address, hostname, etc)
- Type of asset (W2K server, Oracle database, etc)
- New or existing asset (based on what is in the existing C1 asset database)
- Other meta-data

The Windows bv-Control provides both agent based and agentless data collection. The agent based collection is via the bv-control snap-in that is installed on targeted Windows machines. The agent-less data collection is provided by the RMS Query Engines which are installed on the Windows Domain Servers of the targeted network. The RMS Query Engines gather information from the machines with bv-Control Windows installed as well as gather information about the Windows network and agent-less machines that are registered with the Information Server. The Master Query Engine (MQE) which receives data requests in the form of queries from the RMS Console through the Information Server. The MQE then assigns data collection duties to slave engines in the form of jobs. Jobs are distributed based on the list of available slave engines that the ECS maintains. As the slave engines complete their assigned jobs, the MQE collects the slave data files and transfers the data to the Information Server.

Every MQE includes a Slave Query Engine (SQE) component that performs the actual data collection tasks. When the enterprise requires it, administrators can deploy additional SQEs to increase the performance of query processing. The SQEs use temporary data storage and store all collected data in local, unique data files. The SQEs subdivide job requests into smaller atomic jobs and do the actual data processing tasks through locally created agents. Agents are the subprocesses that the SQE spawns to process the query for a single computer. SQEs employ the following types of agents to process queries:

- Data Collection Agents (DCA) to process read requests
- ActiveAdmin Agents (AAA) to process ActiveAdmin write requests

In the agent-based architecture model of bv-Control for UNIX, an agent is installed on all UNIX target computers. The agent is used to fetch and report data of the target computer when queried. In the agent-less architecture model of bv-Control for UNIX, no agent is installed on the UNIX target computers. Remote communication is established between the Information Server and the UNIX target computers via SSH.

RAM provides the ability to create user questionnaires. The data received from the users who complete the questionnaires is gathered and linked to assets.

The Control Compliance Suite uses Symantec Information Server to retrieve data from the target network. The DPS Collector pulls the collected data from the RMS Information Server and the RAM Server. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control snap-ins to collect data from the assets. The Control Compliance Suite also uses the data collector to collect data from RMS. The DPS performs the task of data collection of the SCAP content.

Once the system data has been collected, it will be analyzed based on configured parameters. The CCS collects the system data from managed devices and evaluates it against a set of standards, policies, and exceptions. The CCS reconciles the collected system data based on certain rules. Based on the configured exceptions, temporary permission is given to violate an organizational policy or a technical standard when a valid business reason has been configured by the authorized administrator in the CCS Console or CCS Web Console. Exceptions are the temporary permissions that exempt an asset from following an organizational policy for a specific time period. Exceptions are generally made for a valid business reason. The exception management system provides a central place for handling exceptions in Control Compliance Suite. Currently, exceptions are permitted for the following:

- SCAP
- Standards

- Entitlements
- Policies

The DPS performs the task of evaluation of the SCAP content.

The assessment of the compliance and the risk posture of the system begins when an authorized administrator imports all the known managed devices into the system. The CCS proactively assesses the assets against a set of standards. The assessment is done based on the data that is collected from the data collection components of the CCS. This comparison of the computer settings to predefined Standards is called an evaluation. After an authorized administrator evaluates the collected system data against the specified standards, the CCS gives the evaluation results and the risk score. This provides an authorized administrator with the ability to identify the assets in the organization that are compliant with the set guidelines. The CCS creates baselines based on the evaluation results. The baselines make it easier to compare the managed devices. A baseline is a reference data. The baseline feature is used to compare the asset data with a previous reference data or a previous reference job. In the Control Compliance Suite, when a baseline job is executed, the records in the newer dataset are compared against the records in the older dataset. Baselines allow the user to compare the assets either with an asset that is marked as baseline or with a job-run that is marked as baseline. Control Compliance Suite supports the following types of baselines:

- Asset-based baseline: Control Compliance Suite allows an authorized administrator to mark an asset as a baseline. One can collect the data for an asset and use that data as a baseline to compare or monitor the assets in the further job runs. The asset-based baseline allows administrators to compare multiple assets of the same type with a single reference asset periodically.

- Job-based baseline: Control Compliance Suite allows the an authorized administrator to mark the entire data that is collected by the baseline job as a baseline. The job-based baseline serves the purpose of monitoring the same set of assets. When one creates a baseline job and selects a job-based baseline to compare against, the entire result data for the baseline job is compared.

An alert and/or email is sent when a programmable alarm is exceeded. An authorized administrator can configure an email notification alert for the following tasks:

- Status change of a tiered dashboard update job which can be a success or failure.
- Status change of a dashboard. A dashboard's status can change if the status of a section or an evaluation nodes changes.

The RMS Console provides the RMS Administrator with reporting capabilities to enable the administrator to view the collected system data. This information is only available to administrators who have been granted specific access to the RMS console and granted access rights to view the system data.

The CCS Console and the CCS Web Console provide reporting functions that allow reports of assets, standards, policies, and exceptions. After the DPS evaluates the SCAP data against the collected data from the assets, an authorized administrator can use the report generation feature of CCS to generate the asset details report for the SCAP evaluation results. The evaluated data are also rendered on CCS dashboards such as, Compliance Administration -SCAP profile benchmark.

TOE Security Functional Requirements Satisfied: EXT_CCS_SDC.1, EXT_CCS_RDR.1, EXT_CCS_ANL.1, EXT_CCS_ARP.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1 and 8.2.2 demonstrate the mappings between the threats and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 19 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.ACCOUNT The security relevant actions of users may go undetected making the TSF data vulnerable to attack.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE must provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of TOE security features as well as hold administrator users accountable for any actions they perform regarding the configuration of TOE Security functions.	O.AUDIT counters this threat by ensuring that all relevant TOE security actions are recorded.
T.EXPLOIT An attacker may attempt to gain unauthorized access to the resources of the managed devices, by exploiting vulnerabilities on a managed device.	O.SCAN The TOE must be able to collect information from the managed devices and send alerts based on programmable alarms.	O.SCAN counters this threat by ensuring that the TOE collects information from the managed devices and sends alerts based on programmable alarms.
T.SELPRO An unauthorized user may read, modify, or corrupt security critical TOE configuration data while in	O.ROBUST The TOE must secure all critical security data so that it is protected from unauthorized	O.ROBUST counters this threat by ensuring that the TOE must secure all critical security data so that it is protected from

Threats	Objectives	Rationale
transit between remote administrator users and TOE components as well as between TOE components and trusted IT products.	disclosure and modification while in transit between TOE components and between the TOE and remote trusted IT products.	unauthorized disclosure and modification.
T.FALASC The failure of a TOE component may result in the TOE failing to identify vulnerabilities or non compliant devices based on the association of System data received from all data sources.	O.ANALYZE The TOE must accept data from the collectors and then apply analytical processes and information to derive conclusions about compliance (past, present, or future).	O.ANALYZE counters this threat by providing the function that the TOE will recognize noncompliant activity from multiple data sources.
T.TOEFAIL The failure of the correct operation of a TOE component may result in the loss of collected data, its analysis, or the reporting functions of the TSF.	O.SAFEFAIL The TOE must protect the TSF and preserve correct operations in the event of specified failures.	O.SAFEFAIL counters this threat by protecting the TSF in the event of a failure of a single server node in a multi-TOE configuration.
T.SPOOF A hostile entity masquerading as the Server component may receive TSF data from an authorized agent that incorrectly thinks it is communicating with an authorized Server component.	O.CERT The TOE must provide certificate issuance and management of certificates providing a unique identifier for TOE Components.	O.CERT counters this threat by ensuring that the TOE issues and manages certificates providing unique identifiers for TOE Components.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 20 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE ensures that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately	OE.MANAGE Those responsible for the TOE must be competent, non-hostile	OE.MANAGE ensures that the users who manage the TOE are non-hostile, appropriately trained,

Assumptions	Objectives	Rationale
trained, and follow all guidance.	TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	and follow all guidance.
A.PROTECT The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.	OE.PROTECT Those responsible for the TOE must ensure that the physical environment must be suitable for supporting a computing device in a secure setting.	OE.PROTECT ensures that the TOE environment provides protection from external interference or tampering.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME ensures that the IT environment provides reliable timestamps to the TOE.
A.AUTHEN The IT environment provides the TOE with identification and authentication of TOE users.	OE.AUTHEN The TOE environment must provide identification and authentication for the TOE.	OE.AUTHEN ensures that the IT environment provides identification and authentication for the TOE.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A family of EXT_CCS requirements was created to specifically address the Control Compliance System functions. The CC Part 2 FAU SFRs are specifically for the auditing of TOE Security Functionality. In this case, the information being collected is from external software and machines that are outside the TOE Boundary. As a result, the FAU SFRs do not apply. The IDS SFRs are based on the CC FAU Security audit class Security Functional Requirements of the CC Part 2. Likewise the EXT_CCS SFRs are also based on the CC FAU Security audit class Security Functional Requirements of the CC Part 2. The purpose of this family of requirements is to describe the collecting of information from managed devices as well as the analysis of this system data, sending alerts based on programmable alarms, and restricted audit review of the system data. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation. The CC Part 2 FAU SFRs are specifically for the auditing of TOE Security Functionality. In this case, the information being collected is about external software and machines that are outside the TOE Boundary. As a result, the FAU SFRs do not apply.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended SARs defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 21 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
	EXT_CCS_RDR.1 Restricted data review	The requirement meets the objective by providing the authorized administrator with the capability to read the collected system data.
O.ANALYZE The TOE must accept data from the collectors and then apply analytical processes and information to derive conclusions about compliance (past, present, or future).	EXT_CCS_ANL.1 Analysis	The requirement meets the objective by ensuring the TOE analyzes the collected data.
O.AUDIT The TOE must provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of TOE security features as well as hold administrator users accountable for any actions they perform	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.

Objective	Requirements Addressing the Objective	Rationale
regarding the configuration of TOE Security functions.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that part of the TOE provides the ability to review logs.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that part of the TOE only allows authorized users to read the audit records.
O.CERT The TOE must provide certificate issuance and management of certificates providing a unique identifier for TOE Components.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can issue and manage certificates.
	FCS_CKM.2 Cryptographic key distribution	The requirement meets this objective by ensuring that the TOE can issue certificates.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE provides cryptographic operations to support certificate issuance and management.
O.ROBUST The TOE must secure all critical security data so that it is protected from unauthorized disclosure and modification while in transit between TOE components and between the TOE and remote trusted IT products.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate cryptographic keys for use during cryptographic operations.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE provides confidentiality and integrity services for TSF data being transmitted between TOE Components and trusted IT products.
	FTP_TRP.1 Trusted path	The requirement meets the objective by protecting TSF data from modification and disclosure while it is transmitted between remote administrator users and TOE components.

Objective	Requirements Addressing the Objective	Rationale
	FTP_ITC.1 Trusted channel	The requirement meets the objective by protecting TSF data from modification and disclosure while it is transmitted between separate TOE components.
O.SAFEFAIL The TOE must protect the TSF and preserve correct operations in the event of specified failures.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by protecting TSF data from modification and disclosure while it is transmitted between separate TOE components.
O.SCAN The TOE must be able to collect information from the managed devices and send alerts based on programmable alarms.	EXT_CCS_ARP.1 Security alarms	The requirement meets the objective by ensuring that the TOE sends an alert based on programmable alarm.
	EXT_CCS_SDC.1 System data collection	The requirement meets the objective by ensuring that the TOE collects information from the managed machines.

8.5.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 assurance package augmented with ALC_FLR.2. EAL3+ was selected as the assurance level because the TOE is a commercial product whose users require a moderate level of independently assured security. Control Compliance Suite v10.5.1 is targeted at an environment with good physical access security (OE.PROTECT) and competent administrators (OE.MANAGE, A.MANAGE), where EAL 3 should provide adequate assurance. Within such environments it is assumed that attackers will have basic attack potential. As such, EAL3 is appropriate to provide the assurance necessary to counter the limited potential for attack. ALC_FLR.2 was chosen to assure that the developer is able to act appropriately upon security flaw reports from TOE users.

This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 22 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 22 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
FAU_GEN.2	FIA_UID.1	✓	FIA_UID.1 is not included because user identification is provided by the environment. An environmental objective states that the IT environment will provide user identification and authentication.
	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
	FCS_CKM.2	✓	
FCS_CKM.2	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.1 is not included because user identification is provided

SFR ID	Dependencies	Dependency Met	Rationale
			by the environment. An environmental objective states that the IT environment will provide user identification and authentication.
FPT_FLS.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
EXT_CCS_ARP.1	EXT_CCS_SDC.1	✓	
EXT_CCS_SDC.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
EXT_CCS_RDR.1	No dependencies	✓	
EXT_CCS_ANL.1	EXT_CCS_SDC.1	✓	

9 Acronyms and Terms

This section describes the acronyms and terms as well as Documentation References.

9.1 Acronyms

Table 23 - Acronyms

Acronym	Definition
ADAM	Active Directory Application Mode
AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria
CCE	Common Configuration Enumeration
CCS	Control Compliance Suite
CCSRA	Control Compliance Suite Reporting and Analytics
CM	Configuration Management
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DPS	Data Processing Service
DSS	Data Security Standard
EAL	Evaluation Assurance Level
EMS	Encryption Management Service
ESM	Enterprise Security Manager
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
ID	Identification
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
MMC	Microsoft Management Console
NDS	Novell Directory Service
NIST	National Institute of Standards and Technology
OS	Operating System

Acronym	Definition
OVAL	Open Vulnerability and Assessment Language
PCI	Payment Card Industry
PP	Protection Profile
RAM	Response Assessment Manager
RMS	Risk Management Server
RSAENH	Windows Server 2008 R2 Enhanced Cryptographic Provider
SAR	Security Assurance Requirement
SCAP	Security Content Automation Protocol
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Service Pack
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
W2K	Windows 2000
WCF	Windows Communication Foundation
XCCDF	eXtensible Configuration Checklist Description Format

9.2 Terms

Table 24 - Terms

Acronym	Definition
Exception	The temporary permission that allows a user with a valid business reason to violate an organizational policy or a technical standard.
Managed device	A managed device is an asset. It is an IP host that has a CCS Agent installed on it or is on the target network and is being managed via an agentless CCS component.
Policy	A set of guidelines that are issued by a company to its employees to keep the company compliant with certain government regulations. The guidelines help to maintain the company's standards and reputation.
Standard	A collection of sections that contain checks and subsections. Assets are evaluated against a standard to provide a compliance score.
System data	The information collected by CCS.
Target network	The domain of network and managed devices to be analyzed by the TOE.

9.3 Document References

Table 25 - Document References

ID[26]	Description
[Netware Getting Started Guide]	Symantec bv-Control® for NetWare® 10.5 Getting Started Guide
[NDS Getting Started Guide]	Symantec bv-Control® for NDS® eDirectory™ 10.5 Getting Started Guide
[Oracle Getting Started Guide]	Symantec™ bv-Control for Oracle 10.5 Getting Started Guide
[SQL Getting Started Guide]	Symantec™ bv-Control® for Microsoft® SQL Server 10.5 Getting Started Guide
[User Guide]	Symantec Control Compliance Suite User Guide v. 10.5
[Plan Guide]	Symantec™ Control Compliance Suite Planning and Deployment Guide Version 10.5

[26] ID = Identification

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com