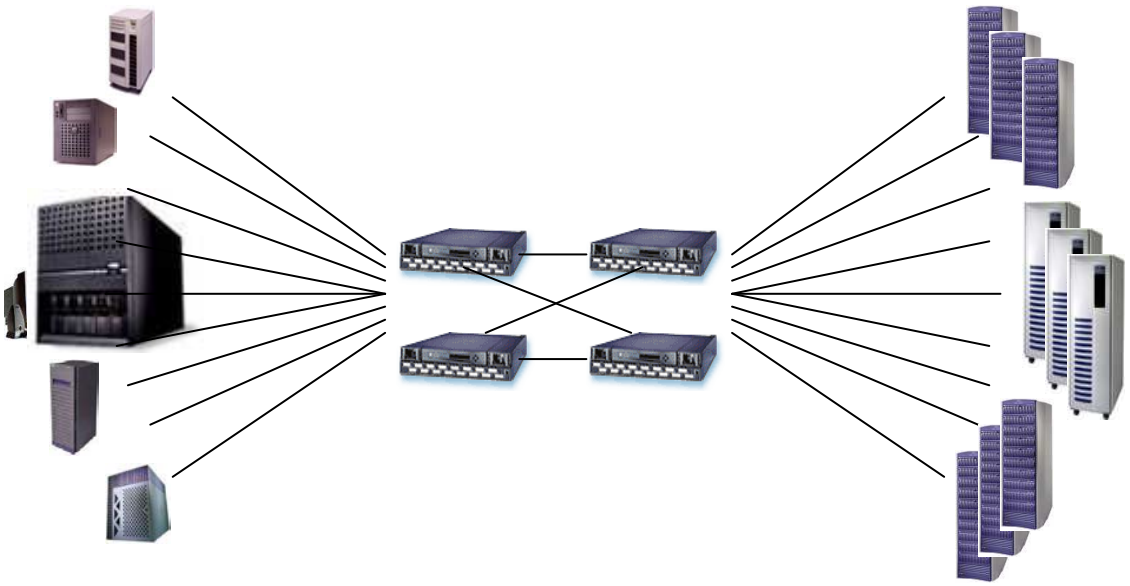
EMC Corporation
EMC ControlCenter® 5.2
Service Pack 5



Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.01

Prepared for:

EMC Corporation
176 South Street
Hopkinton, MA 01748
Phone: (508) 435-1000

http://www.emc.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	2007-10-02	Nathan Lee	Final release.
1.01	2007-10-11	Nathan Lee	Update to Evaluated Operating Systems table and Physical TOE Boundary diagram.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the EMC ControlCenter® 5.2 Service Pack 5, and will hereafter be referred to as the TOE throughout this document. The TOE is a suite of integrated software applications which allow centralized management of various SAN products.

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats 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.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile (PP) claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 – ST, TOE, and CC Identification and Conformance

ST Title	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 Security Target
ST Version	Version 1.01
Author	Corsec Security, Inc. Nathan Lee and Matthew Appler
TOE Identification	EMC ControlCenter® 5.2 Service Pack 5
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2006-06-30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+: EAL2 Augmented with ALC_FLR.1 Basic flaw remediation
Keywords	Storage Area Network (SAN), storage array, data storage

1.3 Conventions

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

The CC allows for several operations to be performed on security requirements: assignment, refinement, selection, and iteration. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis 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.

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security requirements provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The EMC ControlCenter family of products enables administrators to discover, monitor, automate, provision, and report on host storage resources, networks, and storage across their entire information environment from a single console.

EMC ControlCenter shows a consolidated view of the storage environment. This view allows administrators to monitor the health of, track the status of, report on, and control each managed object. From a single console, EMC ControlCenter can manage or monitor:

- Storage components – such as EMC Symmetrix® and other vendor's storage arrays.
- Connectivity components – such as Fibre Channel switches and hubs.
- Host components – such as host operating systems, file systems, volume managers, databases, and backup applications.

EMC ControlCenter comprises three main types of components:[1]

- ControlCenter Infrastructure: acts as the centralized management, storage, and decision-making point for the TOE
- Console software: provides administrative access to the ControlCenter Infrastructure
- Agents: provide intelligence to manage or monitor specific object domains (such as Symmetrix storage arrays; Windows, UNIX, or MVS hosts; and Fibre Channel switches)

In a typical deployment scenario, a variety of application servers and Storage Area Network (SAN) devices are connected to the ControlCenter Infrastructure via IP[2] networking or Fibre Channel, and Agents are installed throughout this infrastructure to provide management and monitoring functionality for each device. SAN administrators utilize the EMC ControlCenter product to manage and monitor these various SAN devices.

Figure 1 below shows the details of the deployment configuration of the TOE:

[1] For a more detailed general overview of these components, please refer to the document entitled *EMC ControlCenter Version 5.0 INTRODUCTION*, available at the EMC Powerlink website at: http://powerlink.emc.com.

[2] IP = Internet Protocol

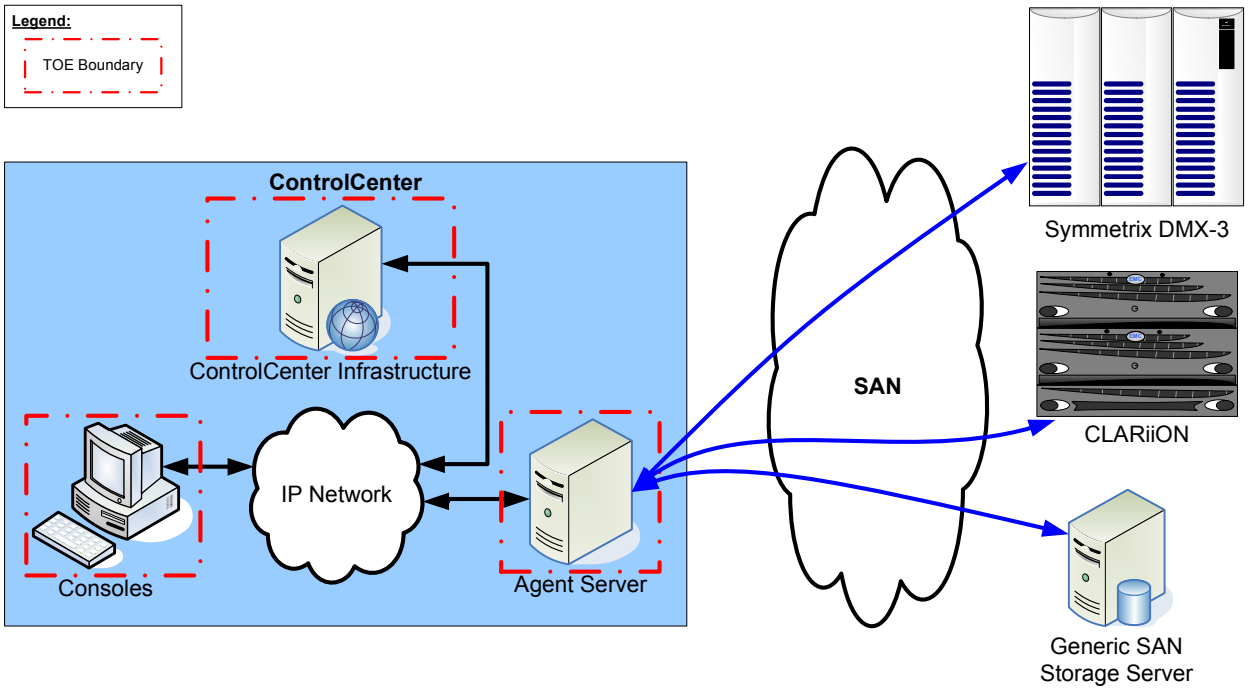


Figure 1 – Deployment Configuration of the TOE

2.2 Product Description

EMC ControlCenter is designed for use in a heterogeneous environment of multivendor storage, multivendor storage networks, and multivendor storage hosts. Information can reside on technologically disparate devices running a variety of operating systems, in geographically diverse locations. From a single console, EMC ControlCenter can monitor or manage the following types of storage arrays:

- EMC Symmetrix®
- EMC Centera®
- EMC Celerra™
- EMC CLARiiON®
- HP StorageWorks™
- HDS™ (Sun™) 7700E, 9900™
- IBM® Enterprise Storage Server™
- IBM RAMAC® Virtual Array (RVA) and StorageTek® Shared Virtual Array™ (SVA™)
- Network Appliance
- Tape Management systems, including STK, VTS, CA-1, and RMM

EMC ControlCenter can manage storage network connectivity components from a variety of vendors including:

- Brocade
- Connectrix™
- McData™
- Qlogic
- Cisco

EMC ControlCenter can manage the following hosts:

- Windows NT®, Windows® 2000, Windows® 2003

- Solaris®, HP-UX®, AIX®, Linux
- MVS™

These different host platforms typically run a varied assortment of host applications, for example, a Novell® file system; an Oracle®, Microsoft SQL Server, Sybase, Informix, or a DB2® database; or a backup system running under Tivoli® Storage Manager. EMC ControlCenter can monitor and report on these host applications also.

The ability to manage host applications and their associated storage needs across disparate platforms from a single interface not only greatly simplifies storage management tasks but also makes it possible to manage more effectively and implement cross-platform storage-wide strategies. Administrators can continue to leverage the individual strengths of each of their storage assets while EMC ControlCenter masks their complexity, bringing all the components together in one view.

2.3 TOE Boundaries and Scope

This section will primarily address what physical and logical components of the TOE are included in evaluation.

2.3.1 Physical Boundary

Figure 2 below illustrates the physical scope and 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 a software suite which runs on general purpose computing hardware running a general purpose operating system (OS).

Table 2 below shows the three main TOE Components and the evaluated operating system.

Table 2 – Evaluated Operating Systems

TOE Component	Evaluated Operating Systems
ControlCenter Infrastructure	Windows Server 2003 SP2
Console Software	Windows Server 2003 SP2
Agents	Windows Server 2003 SP2 Windows 2000 SP4 Red Hat Linux ES 4 Nahant Update 2 HP-UX B11.11 Sun Solaris 2.9 IBM AIX 5.2

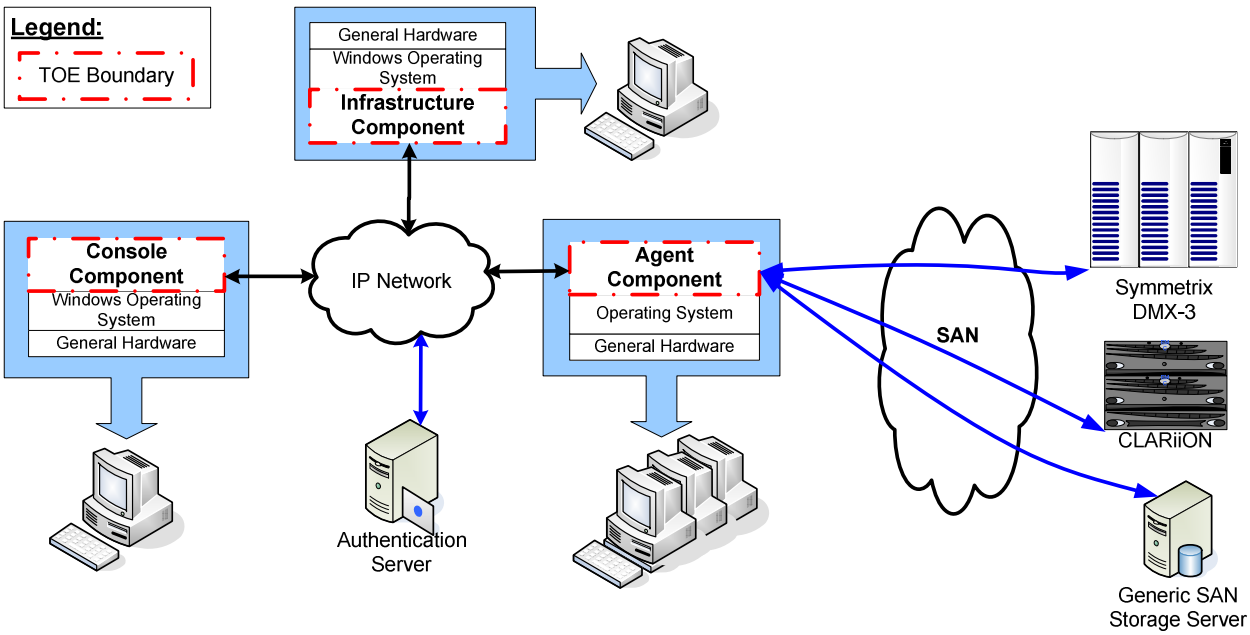


Figure 2 – Physical TOE Boundary

2.3.2 Logical Boundary

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

2.3.2.1 Security Audit

The TOE records audit events relating to the TOE and to the managed environment. The events are recorded in the TOE's "Command History" which is stored in the TOE's internal database. The audit data can be viewed by TOE users through the console application and the web console.

2.3.2.2 User Data Protection

The User Data Protection function protects data that is entrusted to the TOE. This functionality is primarily enforced by the ControlCenter Infrastructure TOE component. Once users of the TOE are identified and authenticated, either by the TOE or the TOE Environment, they are then granted access to audit data and TOE configuration data. Each user has access permissions associated with his user account that allows the user to access audit data and TOE configuration information.

2.3.2.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that is requesting a service has provided a valid username and password and is authorized to access that service. When TOE users enter their username and password at the login screen of the console application or web console, the information is passed to the ControlCenter Infrastructure. The information is then verified against the username and password stored in the TOE

environment (for example, the local Windows OS' user accounts or an Active Directory service). If the provided username and password are valid, the TOE user is assigned the privileges associated with that username within the TOE. Before identification and authentication, the TOE user is only able to identify and authenticate himself.

2.3.2.4 Security Management

The TOE assigns granular privileges directly to an unlimited number of users and user-defined user groups. Users perform all management of the TOE through the console application.

2.3.2.5 Protection of the TSF

Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. It is not possible to perform any security-relevant actions on the system without successfully authenticating. Once a user has been authenticated, he is bound to the appropriate roles and any privileges defined by the TOE access control.

2.3.3 Product Components Included In and Excluded From the TOE

The TOE has a range of command line interfaces and utilities which only need to be used during install or troubleshooting. They are excluded from the Common Criteria evaluated configuration. The TOE consists of software applications. The underlying hardware and operating systems are part of the TOE environment, as is the web server and the web browser.

Product components that are part of the evaluated configuration of the TOE are:

- SAN Manager
- StorageScope
- Symmetrix Manager

Product components that are not part of the evaluated configuration of the TOE are:

- Automated Resource Manager
- Performance Manager
- SAN Advisor
- Symmetrix Optimizer

3 Security Environment

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:

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

3.1 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.

Name	Description
A.NOEVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSCAL	Physical security will be provided for the TOE and its environment.

3.2 Threats to Security

This section identifies the threats to the Information Technology (IT) assets against which the TOE must protect. The threat agents are individuals who are not authorized to use the TOE. The threat agents are assumed to:

- have public knowledge of how the TOE operates
- possess a low skill level
- have limited resources to alter TOE configuration settings
- have no physical access to the TOE
- possess a low level of motivation
- have a low attack potential

The IT assets requiring protection are the configuration data and the servers on the managed networks.

The following threats are applicable:

Name	Description
T.COMINT	An unauthorized individual may attempt to compromise the integrity of the audit data collected and produced by the TOE or TOE configuration data by bypassing a security mechanism.
T.PRIVIL	An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section describes the organizational security policies with which the TOE must comply.

Name	Description
P.PASSWORD	An authorized TOE user must use a sound password to access the TOE. A user password must have a minimum password length of eight characters and must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of 10), and two alphabetical characters (from a set of 52, since upper- and lowercase characters are differentiated).

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

Name	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
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, can exercise such control.
O.AUDIT	The TOE must gather audit records of actions on the TOE which may be indicative of misuse.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.INTEGR	The TOE must ensure the integrity of all audit data.
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

Name	Description
OE.SEP	The IT Environment will protect the TOE from external interference or tampering.
OE.TIME	The IT Environment will 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. 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.

Name	Description
NOE.NOEVIL	TOE users are non-hostile, appropriately trained, and follow all user guidance.
NOE.PHYSCL	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 3 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 3 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓			
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1	Security roles		✓		

Name	Description	S	A	R	I
FPT_RVM.1	Non-bypassability of the TSP				

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

Section 5.1 contains the functional components from the Common Criteria (CC) Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.

5.1.1 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 auditable events specified in Table 4*].

Table 4 – Auditable Events

Auditable Event	Description
User Logon	
User Logoff	Audited when the java console exits normally via the File/Exit menu option.
Add ECC[3] User	Creating a new User
Remove ECC User	
Set User Description	Adding/updating description for a User
Add ECC User Group	Creating a new User Group
Set User Group Description	Adding/updating description for a User Group
Set User Group Name	Updating a User Group name
Add ECC User to Group	
Remove ECC User From Group	
Remove ECC User Group	
Replace Authorization Rule Set	Creating/updating/deleting an authorization rule

FAU_GEN.1.2

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

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

[3] EMC ControlCenter

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

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

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

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [*access control SFP*] on [*all security attributes*].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [*access control SFP*] to objects based on the following: [

- *Subjects: authorized users*
  - *Security Attributes:*
    - *user name*
    - *permissions*
- *Objects: audit data and TOE configuration*
  - *Security Attributes:*
    - *permissions*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an authorized user can manipulate audit data and/or the TOE configuration if the user has the appropriate permissions*].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.1.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*user name, permissions*].

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated **by the TOE Environment** before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The TSF shall require each user to identify itself **to the TOE Environment** before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [*all functions*] to [*authorized administrators*].

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*access control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*all security attributes*] to [*authorized administrators*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*access control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*authorized administrators*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, delete, clear*] the [*audit data and TOE configuration*] to [*authorized administrators*].

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [*security attribute management, TSF data management, and security function management*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*user-defined roles*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

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

Dependencies: No dependencies

5.2 Security Functional Requirements on the IT Environment

This section specifies the SFRs for the IT Environment. This section organizes the SFRs by CC class. The table below identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Name	Description	S	A	R	I
FPT_SEP.1	TSF domain separation			✓	
FPT_STM.1	Reliable time stamps			✓	

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

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The **TOE environment** shall maintain a security domain for **the TOE's** execution that protects **the TOE** from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The **TOE environment** shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The **TOE environment** shall be able to provide reliable time stamps for **the use of the TOE**.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.1. Table 5 – Assurance Requirements summarizes the requirements.

Table 5 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life Cycle	ALC_FLR.1 Basic Flaw Remediation
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

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

6.1 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 are suitable to satisfy the necessary requirements.

Table 6 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Protection of the TSF	FPT_RVM.1	Non-bypassability of the TSP
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
User Data Protection	FDP_ACC.1	Subset access control

TOE Security Function	SFR ID	Description
	FDP_ACF.1	Security attribute based access control

6.1.1 Security Audit

The Security Audit function records an audit event whenever a user attempts to login or logs off. It audits manipulation of TOE user accounts, including their addition, deletion, or modification (including user group membership). The Security Audit function audits manipulation of TOE user groups, including their addition, deletion, modification. It also audits the creation, updating, or deletion of authorization rules.

The TOE audit records contain at least the following information: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

The audit data can be viewed by TOE users through the console application and the web console. The audit logs are stored in the internal database. They are protected so that only authorized users can delete these records.

6.1.2 User Data Protection

The TOE provides the User Data Protection security function to manage access to audit data and TOE configuration data to authorized users.

Identification and authentication of authorized users is performed by the Identification and Authentication security function. After a user has been successfully authenticated, the TOE posesses the EMC ControlCenter permissions for that user. Using the Security Management security function, the user's permissions are used to mediate access and manipulation to audit data and TOE configuration data.

6.1.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that is requesting a service has provided a valid username and password and is authorized to access that service. For each user, the TOE stores the following security attributes in the database: username and permissions. When a TOE user enters his username and password at the login screen of the console software or web console, the information is passed to the ControlCenter Infrastructure, where it is in-turn passed to the TOE Environment for verification. If the provided username and password are valid then the ControlCenter Infrastructure allows the user to access the TOE with the permissions associated with that username. Before identification and authentication, the TOE user is only able to identify and authenticate himself.

6.1.4 Security Management

The TOE assigns granular privileges directly to an unlimited number of users and user-defined user groups. Users perform all management of the TOE through the console application.

The TOE enforces which users have access to TSF data, such as events, notifications, and configuration settings. Attempts by the user to query, modify, or delete security attributes (such as username or permissions), TSF data (such as audit data and configuration settings), and security are mediated by the TOE.

6.1.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to ensure that physical connections made to the TOE remain intact and unmodified.

Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. Each subject's and user's security privileges are separated. It is not possible to perform any actions on the system without successfully authenticating. Once a user has been authenticated, he is bound to the appropriate privileges defined by the TOE access control. For any user to perform a TOE operation, an Administrator must have granted that user the rights to perform that operation. These privileges are granted on a per user basis. Since all access control rights are checked by the TOE's mechanisms and the TOE uses unique attributes for each user, then the TSF maintains separation between different users. As an example, if a user without explicit permission tries to edit a policy, the user will not be able to save the changes.

6.2 TOE Security Assurance Measures

EAL2+ was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 7 – Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 - Configuration Management: Capabilities
ADO_DEL.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 - Delivery and Operation: Secure Delivery
ADO_IGS.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 Planning and Installation Guide Volume 1 P/N 300-003-716 REV A02 EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 Planning and Installation Guide Volume 2 (MVS Agents) P/N 300-003-717 REV A01
ADV_FSP.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
AGD_ADM.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 – Common Criteria Administrative Guide Supplement EMC ControlCenter® 5.2 Service Pack 5 Support Matrix P/N 300-003-704 REV A02 EMC ControlCenter® 5.2 Service Pack 5 Overview P/N 300-003-719 REV A01 EMC ControlCenter® 5.2 Service Pack 5 Administration/User Guide P/N 300-003-718 REV A01 EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 StorageScope Reference Guide P/N 300-003-712 REV A01 EMC Corporation EMC ControlCenter 5.2 Integration Packages Product Guide P/N 300-000-300 REV A05 EMC Corporation EMC ControlCenter Framework Integration Examples 5.2 P/N 300-003-519 REV A01 EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 Performance and Scalability Guidelines P/N 300-003-703 Rev A01 EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 Storage Provisioning Services Command Line Interface Reference Guide P/N 300-003-714 REV A01 EMC ControlCenter® 5.2 Service Pack 5 Integration Packages Product Guide P/N 300-003-710 REV A01 EMC ControlCenter® 5.2 Service Pack 5 Performance and Scalability Guidelines P/N 300-003-703Rev A01 SAN Manager™ Quick Start Discovery EMC ControlCenter 5.2 P/N 300-001-417 REV A01 EMC ControlCenter® 5.2 Service Pack 5 Storage Provisioning Services Allocating and Deallocating Storage P/N 300-003-720 REV A01

Assurance Component	Assurance Measure
AGD_USR.1	Note: The only “users” of the EMC ControlCenter® 5.2 Service Pack 5 are Administrators. Therefore, only AGD_ADM.1 applies.
ALC_FLR.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 – Life Cycle Support: Flaw Remediation
ATE_COV.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 – Testing: Coverage
ATE_FUN.1	Common Criteria Test Cases for ECC 5.2 SP5 EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 – Tests: Functional Tests
ATE_IND.2	Provided by laboratory evaluation
AVA_VLA.1	EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 - Vulnerability Assessment

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. The tables below demonstrate that the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, assumption, and policy.

8.1.1 Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.COMINT An unauthorized individual may attempt to compromise the integrity of the audit data collected and produced by the TOE or TOE configuration data by bypassing a security mechanism.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objectives ensure that unauthorized modifications and access to functions and data is prevented. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data.
	O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The O.IDAUTH objective requires that the TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	O.INTEGR The TOE must ensure the integrity of all audit data.	This threat is primarily diminished by the O.INTEGR objective, which requires that the TOE ensure the integrity of all audit data.
	O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.	The O.PROTECT objective requires that the TOE protect itself from unauthorized modifications and access to its functions and data.

Threats	Objectives	Rationale
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.
T.PRIVIL An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ADMIN and O.ACCESS objectives together ensure that policies won't be subverted or changed by unauthorized users. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data.
	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, can exercise such control.	The O.ADMIN and O.ACCESS objectives together ensure that policies won't be subverted or changed by unauthorized users. The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage the functions and data of the TOE.
	O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	This threat is primarily diminished by the O.IDAUTH objective, which requires that the TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.	The O.PROTECT objective requires that the TOE protect itself from unauthorized modifications and access to its functions and data.

Threats	Objectives	Rationale
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.

8.1.2 Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.PHYSCAL Physical security will be provided for the TOE and its environment.	NOE.PHYSCL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	The NOE.PHYSCL objective requires that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL TOE users are non-hostile, appropriately trained, and follow all user guidance.	The NOE.NOEVIL objective ensures that TOE users are non-hostile, appropriately trained, and follow all operator guidance.

8.1.3 Security Objectives Rationale Relating to Policies

Policies	Objectives	Rationale
P.PASSWORD	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.IDAUTH ensures that a user must identify and authenticate before access to the TOE is granted.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS ensures that only authorized users are allowed access to the TOE.

8.2 Security Functional Requirements Rationale

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

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	FAU_GEN.1 Audit data generation	Security-relevant events must be audited by the TOE.
	FAU_SAR.1 Audit review	The TOE must provide the ability to review the audit trail of the system.
O.INTEGR The TOE must ensure the integrity of all audit data.	FAU_STG.1 Protected audit trail storage	The TOE is required to protect the audit data from unauthorized deletion.
	FDP_ACF.1 Security attribute based access control	Only authorized TOE users with the appropriate permissions may access audit data.
	FMT_MSA.1 Management of security attributes	Only authorized users of the System may query and modify TOE data.
	FMT_MTD.1 Management of TSF data	Only authorized users of the System may query and modify TOE data.
	FPT_RVM.1 Non-bypassability of the TSP	The TOE must ensure that all functions to protect the data are not bypassed.
O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_ATD.1 User attribute definition	Security attributes of subjects used to enforce the authentication policy of the TOE must be defined.
	FIA_UAU.2 User authentication before any action	The TOE will not give any security sensitive access to a user until the TOE Environment has authenticated the user.
	FIA_UID.2 User identification before any action	The TOE will not give any security sensitive access to a user until the TOE Environment has identified the user.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMR.1 Security roles	The TOE must be able to recognize the different user roles that exist for the TOE.
	FPT_RVM.1 Non-bypassability of the TSP	The TOE must ensure that all functions are invoked and succeed before each function may proceed.
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FIA_UAU.2 User authentication before any action	The TOE will not give any security sensitive access to a user until the TOE Environment has authenticated the user.
	FIA_UID.2 User identification before any action	The TOE will not give any security sensitive access to a user until the TOE Environment has identified the user.
	FDP_ ACC.1 Subset access control	The TOE has an access control policy that ensures that only authorized users gain access to TOE functions and data.
	FDP_ACF.1 Security attribute based access control	The TOE is required to provide authorized users access to TOE functions and data.
	FMT_MSA.3 Static attribute initialisation	Restrictive values for TOE functions and data are provided, and the authorized administrator can change them when an object is created.
	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
	FMT_MTD.1 Management of TSF data	Only authorized users of the System may query and modify TOE data.
	FPT_RVM.1 Non-bypassability of the TSP	The TOE must ensure that all functions are invoked and succeed before each function may proceed.

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, can exercise such control.	FMT_MSA.3 Static attribute initialisation	Restrictive values for TOE functions and data are provided, and the authorized administrator can change them when a data object is created.
	FMT_MOF.1 Management of security functions behaviour	Only those roles defined in FMT_SMR.1 are given the right to control the behavior of the TSF.
	FMT_MTD.1 Management of TSF data	Only those roles defined in FMT_SMR.1 are given the right to access TSF data.
	FMT_SMF.1 Specification of management functions	Mechanisms exist to enforce the rules defined in FMT_MOF.1, FMT_MTD.1(a), and FMT_MTD.1(b).
	FMT_SMR.1 Security roles	The TOE defines a set of roles.
O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.	FDP_ ACC.1 Subset access control	The TOE has an access control policy that ensures that only authorized users can modify and access TOE functions and data.
	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to TOE functions and data.
	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
	FMT_MTD.1 Management of TSF data	Only authorized users of the System may query and modify TOE data.
	FPT_RVM.1 Non-bypassability of the TSP	The TOE must ensure that all functions are invoked and succeed before each function may proceed.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.SEP The IT Environment will protect the TOE from external interference or tampering.	FPT_SEP.1 TSF domain separation	The IT Environment must protect the TOE from interference that would prevent it from performing its functions.
OE.TIME The IT Environment will provide reliable timestamps to the TOE.	FPT_STM.1 Reliable time stamps	The IT Environment is required to provide reliable timestamps to the TOE.

8.3 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment.

8.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 8 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 8 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	✓
FAU_SAR.1	FAU_GEN.1	✓
FAU_STG.1	FAU_GEN.1	✓
FDP_ACC.1	FDP_ACF.1	✓
FDP_ACF.1	FDP_ACC.1	✓
	FMT_MSA.3	✓
FIA_ATD.1	None	✓

SFR ID	Dependencies	Dependency Met
FIA_UAU.2	FIA_UID.1	✓
FIA_UID.2	None	✓
FMT_MOF.1	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓
	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_MSA.3	FMT_MSA.1	✓
	FMT_SMR.1	✓
FMT_MTD.1	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_SMF.1	None	✓
FMT_SMR.1	FIA_UID.1	✓
FPT_RVM.1	None	✓
FPT_SEP.1	None	✓
FPT_STM.1	None	✓

8.5 TOE Summary Specification Rationale

8.5.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6.1) describes a security function of the TOE. Each description is organized by a set of requirements with rationale that indicates how these requirements are satisfied by

aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functional requirements. Furthermore, all of the security functions are necessary in order for the TSF to meet the security functional requirements. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 6 – Mapping of TOE Security Functions to Security Functional Requirements identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one SFR).

8.5.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment. The augmentation of ALC_FLR.1 was chosen to provide assurance to customers that the developer has processes in place to capture, track, and correct any future flaws that may be found in the TOE.

8.5.2.1 Configuration Management

The *EMC ControlCenter - Configuration Management: Capabilities* documentation provides a description of tools used to control the configuration items and how they are used at EMC. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.5.2.2 Delivery and Operation

The *EMC ControlCenter - Delivery and Operation: Secure Delivery* documentation provides a description of the secure delivery procedures implemented by EMC to protect against TOE modification during product delivery. The Installation Documentation provided by EMC details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

8.5.2.3 Development

The *EMC ControlCenter - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence* design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and error messages for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the

basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Representation Correspondence

8.5.2.4 Guidance Documentation

The EMC ControlCenter Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. EMC provides single versions of documents which address the Administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.5.2.5 Life Cycle Support

The *EMC ControlCenter – Life Cycle Support: Flaw Remediation* documentation describes the processes that EMC follows to capture, track, and correct flaws (or "bugs") that are found within the TOE. The documentation demonstrates that all discovered flaws are recorded and that the process ensures that flaws are tracked through their entire life cycle.

Corresponding CC Assurance Components:

- Basic Flaw Remediation

8.5.2.6 Tests

A number of components make up the *EMC ControlCenter – Functional Tests and Coverage* documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. EMC ControlCenter Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

8.5.2.7 Vulnerability Analyses

The *EMC ControlCenter - Vulnerability Assessment* documentation is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks.

Corresponding CC Assurance Components:

- Vulnerability Analysis

8.6 Strength of Function

There is no SOF claim for the TOE. There are no probabilistic or permutational functions within the TOE since I&A is performed in the TOE Environment (See Section 6.1.3).

9 Acronyms

Table 9 – Acronyms

Acronym	Definition
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ECC	EMC ControlCenter
IP	Internet Protocol
IT	Information Technology
LUN	Logical Unit
OS	Operating System
PP	Protection Profile
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy