EMC Corporation
EMC Smarts Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1

Security Target

Evaluation Assurance Level: EAL2
Document Version: 0.6

Prepared for:

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

www.emc.com

Prepared by:

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

www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2006-06-06	Adam O'Brien and Nathan Lee	Initial draft.
0.2	2006-11-03	Christie Kummers	Minor updates and changes throughout in response to lab verdicts.
0.3	2006-11-22	Christie Kummers	Updates to Table 1 - ST, TOE, and CC Identification and Conformance.
0.4	2007-04-03	Justin Dubbs	Updates to Figure 1 and product description.
0.5	2007-06-22	Justin Dubbs Nathan Lee	Minor updates and changes throughout in response to lab verdicts.
0.6	2007-06-26	Nathan Lee	Updates to address omissions from previous PETR.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), the Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the EMC Smarts Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1, and will hereafter be referred to as the TOE or EMC Smarts throughout this document. The TOE is a suite of products which monitor IT networks. The suite can map networks, monitor the availability and performance of network nodes, and show the business implications of any failures.

1.1 Purpose

This ST contains the following sections:

- 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 claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the consistency, completeness, and suitability of the security objectives, requirements, and the TOE summary specifications.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and Common Criteria (CC) Identification and Conformance

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

ST Title	EMC Corporation EMC Smarts Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1 Security Target
ST Version	Version 0.6
Author	Corsec Security, Inc. Adam O'Brien and Nathan Lee
TOE Identification	EMC Smarts Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1.157
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3 August 2005 (aligned with ISO/IEC 15408:2004); CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2006-06-29 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level (EAL)	EAL2
Keywords	Availability, IP networks

1.3 Conventions, Acronyms, and Terminology

1.3.1 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 several operations to be performed on security requirements: assignment, refinement, selection and iteration. All of these operations are used within this ST. 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 [<u>*underlined italicized text within brackets*</u>].
- Refinements are identified using **bold text**.
- Any text removed is stricken (*e.g.*: ~~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.

1.3.2 Acronyms and Terminology

The acronyms and terms used within this ST are described in Section 9 – "Acronyms."

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the capabilities and security functions 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 TOE is a suite of software products which monitor IT networks. The suite can map networks, monitor the availability and performance of network nodes, and show the business implications of any failures. The suite consolidates network events and presents them at a suitable level of abstraction to allow administrators to prioritize problems according to business impact. The TOE help administrators to distinguish the root cause of a problem from the collateral impacts.

The suite includes the following products:

- Service Assurance Manager – the core management server for the whole system
- Global Console – the primary interface to the Service Assurance Manager
- Business Impact Manager – extends the capabilities of Service Assurance Manager by calculating the business impact of events.
- Business Dashboard – extends the capabilities of Service Assurance Manager by presenting the business impacts of events.
- Report Manager – extends the capabilities of Service Assurance Manager by storing events in a database ready to compile into reports.
- Broker - manages a registry of EMC Smarts server applications.
- Discovery Manager – discovers and presents the topology of Internet Protocol (IP) networks.
- IP Availability / Performance Manager – monitors the availability and performance of IP networks.
- Server Performance Manager – monitors the performance of critical servers.

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

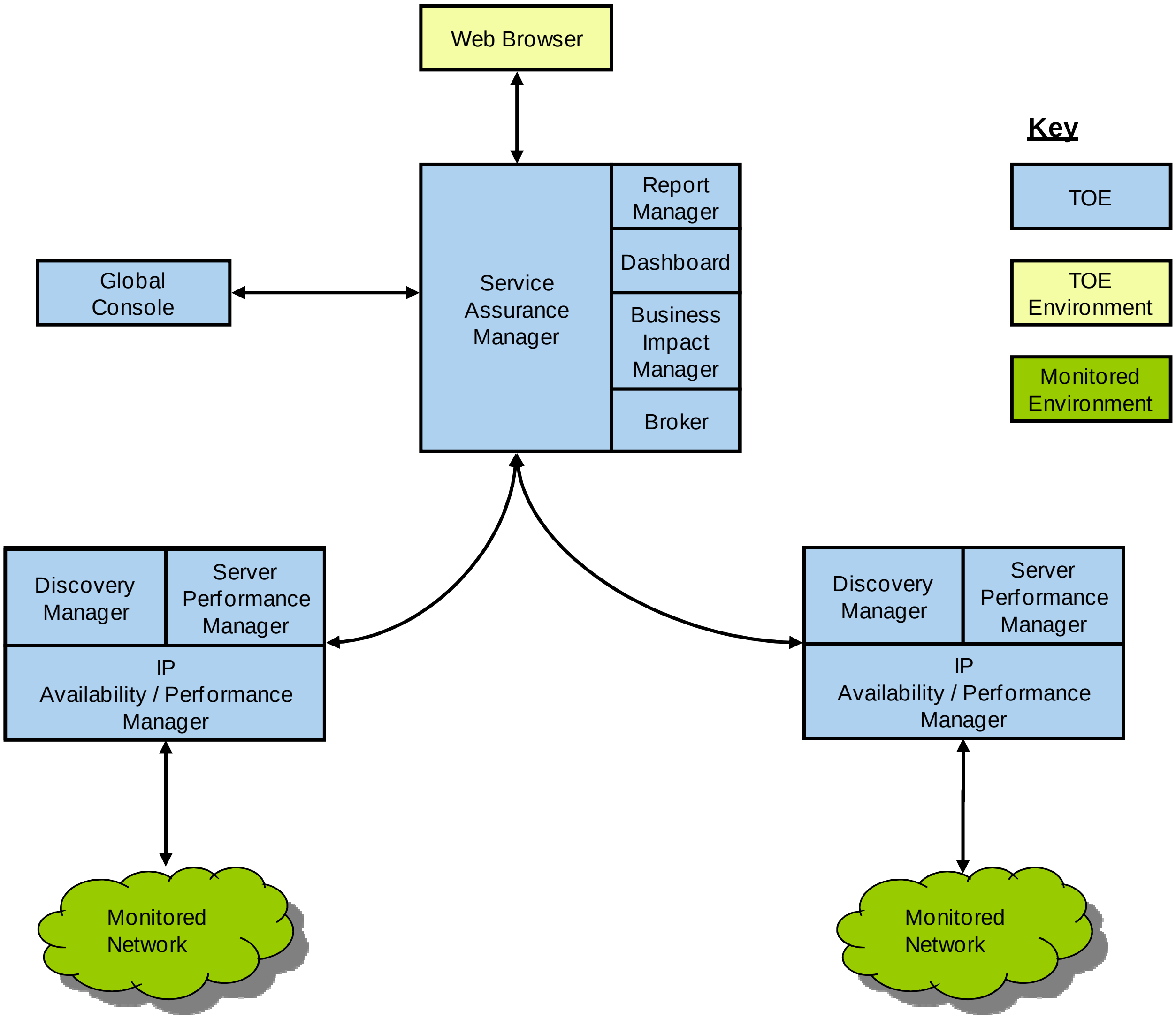

Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

The EMC Smarts consists of 3 monitoring components (IP Availability Manager, IP Performance Manager, and Server Performance Manager) and a discovery component (Discovery Manager). These components map and monitor IP networks and critical servers. They pass the information gathered to the core management server – the Service Assurance Manager. This management server aggregates this information and presents it to the user through the Global Console or the web browser. The Service Assurance Modules (Business Impact Manager, Business Dashboard, and Reports Manager) provide additional capabilities to calculate and display the business impact of infrastructure problems and to produce a wide variety of reports. The Broker manages a registry of EMC Smarts server applications, which allows each component to discover other components of the system.

The product helps system administrators cope with the flood of raw events which will be generated by a problem in the IT infrastructure. The system uses a normalized event reporting structure, the EMC Common Information Model (ECIM), which identifies and consolidates duplicated events.

The EMC Smarts can also distinguish between the root cause of problems and the collateral impacts. For example, one router failing might increase the throughput of other routers and cause them to fail. The system administrator will receive events from many routers, but only needs to address the problem on one router. The system uses patented Codebook Correlation Technology. This set of algorithms computes a correlation between the set of possible symptoms and the root cause that can best explain the symptoms, based on the nature of the symptoms and the network topology. The processing of these algorithms is distributed throughout the system for optimal performance, but the final correlation analysis, policy implementation and presentation to the user occurs in the Service Assurance Manager. The information is made available to the administrator through a web browser or the Global Console.

2.2.1 Discovery Manager

Discovery Manager is a tool which discovers and presents the topology of the IP networks. It works at layers 2 and 3 of the Open System Interconnection (OSI) model. The Discovery Manager can identify all layer 2 and 3 devices by IP and Media Access Control (MAC) address. It can determine the physical and logical relationships between these entities and the network protocols being used. This information is updated in real-time and presented in a traversable topology map.

2.2.2 IP Availability / Performance Manager

IP Availability / Performance Manager allows more detailed monitoring of IP networks. It can identify when an IP node is still operational, but is not performing optimally. IP Availability / Performance Manager identifies failures in IP networks, at layers 2 and 3 of the OSI model. It is able to distinguish between the root cause of a problem and the collateral effects.

2.2.3 Server Performance Manager

Server Performance Manager provides detailed monitoring for system servers. It can determine when servers are not performing optimally and help to identify possible future failures. It monitors utilization of server disks, file systems, processors, and memory.

2.2.4 Service Assurance Manager

The Service Assurance Manager serves as the cornerstone of network operations management. The Service Assurance Manager provides integrated, unified, and individualized views of the systems, network infrastructure, applications, and business entities that comprise the managed domain. The Service Assurance Manager communicates with the EMC Smarts monitoring components and consolidates the following information:

- Network, system, application, and business resources
- Results of domain-specific root-cause analysis
- Results of domain-specific impact analysis

The Service Assurance Manager automatically correlates topology and event data from multiple EMC Smarts managed domains to diagnose root-cause problems.

2.2.5 Business Impact Manager

The Business Impact Manager extends the capabilities of Service Assurance Manager to analyze events by calculating the business impact of events and propagating the impacts to affected business entities as discrete notifications that are linked to topology within the managed domain. The impacts are displayed in the Business Services Maps.

2.2.6 Business Dashboard

The Business Dashboard is a web console that displays a collection of EMC Smarts analysis data alongside important data from other sources.

2.2.7 Report Manager

The Report Manager uses a Structured Query Language (SQL) Data Interface adapter that enables network administrators to collect detailed notification information from the EMC Smarts Service Assurance Manager (Global Manager) and store the information in a relational database. The Report Manager enables network administrators to produce and display or print network operations and management reports through Business Objects Crystal Reports software.

2.2.8 Broker

The Broker manages a registry of EMC Smarts server applications. When an EMC Smarts server application starts it registers with the broker, providing its IP address and listening port number. When an EMC Smarts application needs to connect with another application, it gets the necessary information from the Broker. Periodically, the Broker pings the applications in its registry to determine whether they are still active.

2.2.9 Global Console

The Global Console is the primary user interface for the administration of the Service Assurance Manager. The console displays the network topology and the status of network components. Through the Global Console administrators can monitor EMC Smarts domains, acquire detailed information about topology and events, respond to problems, and take corrective action. EMC Smarts administrators with appropriate privileges can administer EMC Smarts users, user profiles and policies. The Global Console runs as a standalone Java program.

2.3 TOE Boundaries and Scope

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

2.3.1 Physical Boundary

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 the EMC Smarts Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1. The TOE consists of the following 9 software components:

- Service Assurance Manager
- Global Console
- Business Impact Manager
- Business Dashboard
- Report Manager
- Broker
- Discovery Manager
- IP Availability / Performance Manager
- Server Performance Manager

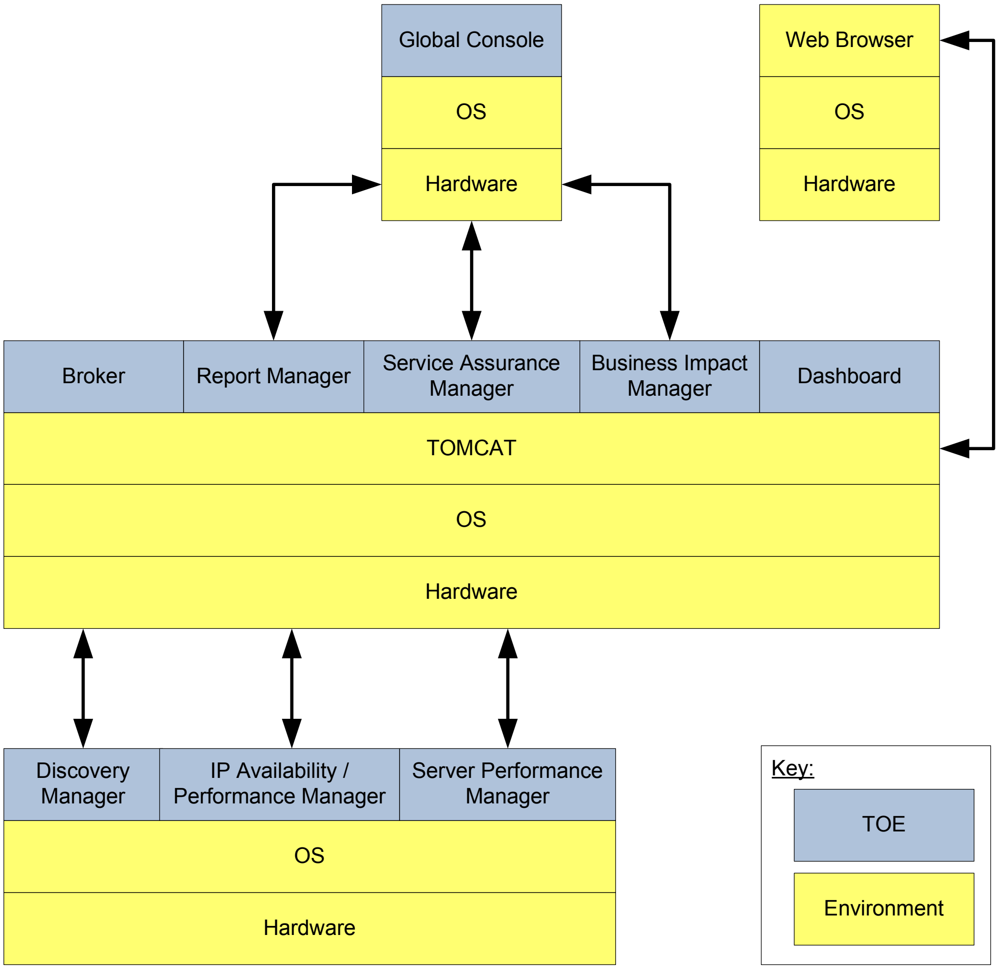

Figure 2 - Physical TOE Boundary

The operating systems (OSs) and hardware components are not part of the TOE. The Discovery Manager, IP Availability / Performance Manager, and Server Performance Manager all run on one machine, the Service Assurance Manager, Business Impact Manager**,** Business Dashboard**,** and Reports Manager on another. The machine running the Business Dashboard utilizes Tomcat v5.0.16, which is part of the environment. Both machines have the same specifications listed in Table 2. The Global Console can operate on any system which supports JRE v1.4.2. The system supports Netscape 7.0 (or higher) or Internet Explorer 6.0 SP1 (or higher) with JavaScript enabled.

Table 2 - Hardware and Operating System Platforms

Hardware	Operating System
Intel Pentium 4, 2 GHz	Red Hat Linux 3.0
	Windows 2000
	Windows 2003 SP1
HP L2000	HP-UX11.11
Solaris Sun Fire 280	Solaris 8 and Solaris 9

2.3.2 Logical Boundary

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

- Security Audit
- 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 monitored environment. The events are recorded in a standardized format and stored in the filesystem of the operating system of the machine running the Service Assurance Manager. Audit events are analyzed to determine the root cause of the event. The audit data and analytic results can be viewed by TOE users through the Global Console and the web browser.

2.3.2.2 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. When TOE users enter their username and password at the Global Console interface or the web browser interface, the information is passed to the Service Assurance Manager, where it is verified against the username and password stored in the TOE. If the provided username and password match, the TOE user is assigned the role associated with that username. Before identification and authentication, the TOE user is only able to view active TOE components.

2.3.2.3 Security Management

The TOE maintains three roles: All, Monitor and Ping. The All role has access to all elements of the TOE. The Monitor role can only view information. The Ping role can only discover which TOE components are active. Users perform all management of the TOE through the Global Console or the web browser.

2.3.2.4 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. The TOE protects information as it is transmitted between remote components of the TOE by encrypting the information using AES with a key derived from a Diffie-Hellman exchange.

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of 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 CC 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.

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.

A.CONNECT The TOE will be connected at all times to the network which it is intended to monitor.

A.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.

A.PHYSCL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.2 Threats to Security

This section identifies the threats to the IT assets against which the TOE must protect. The threat agents are individuals who are not authorized to use the TOE or the protected network. 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 IP networks and servers on the monitored networks.

The following threats are to be addressed by the TOE:

T.NETWORK An unauthorized individual might disrupt the availability or performance of IP networks or servers.

T.COMINT An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE 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

There are no Organization Security Policies.

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:

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.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.SECURE The TOE must ensure the security of all audit and System data.

O.MONITOR The TOE must gather, analyze, and present information about all events that are indicative unavailability or poor performance of IP networks or servers.

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:

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

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

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.

NOE.NOEVIL 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 SFRs and Security Assurance Requirements met by the TOE as well as SFRs met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

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

SFR ID	Description
FAU_GEN.1	Audit Data Generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1a	Management of TSF data
FMT_MTD.1b	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RVM.1	Non-bypassability of the TSP

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 1.3.1.

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
Unsuccessful logins
User responses to notifications
A monitored layer 2 or 3 device: • is unavailable • has high processor utilization • has a hard drive failure • has insufficient free memory
A monitored server: • is unavailable • has high processor utilization • has a hard drive failure • has insufficient free memory
A monitored network adaptor • is unavailable • has a high failure rate

FAU_GEN.1.2

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

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

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

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*all events gathered on the monitored network*] known to indicate a potential security violation;

b) [*No other rules*].

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*All and Monitor*] 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 audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 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, password, and role*].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1

The TSF shall allow [*the viewing of active TOE components*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1

The TSF shall allow [*the viewing of active TOE components*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.3 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 [*the All role*].

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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1a

The TSF shall restrict the ability to [*query*] the [*audit data and TOE configuration*] to [*the Monitor and All roles*].

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

FMT_MTD.1.1b

The TSF shall restrict the ability to [*modify, delete*] the [*audit data and TOE configuration*] to [*the All role*].

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: [*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 [*Ping, Monitor, All*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

The TSF shall protect TSF data from [*disclosure*] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

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

The TOE has the following security requirements for its IT environment. The stated Security Functional Requirement on the IT Environment of the TOE presented in this section has been drawn from Part 2 of CC Version 2.3 and hence conformant to CC Version 2.2 Part 2.

SFR ID	Description
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps

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. 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 ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	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
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of Identification
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1a	Management of TSF data
	FMT_MTD.1b	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RVM.1	Non-bypassability of the TSP

6.1.1 Security Audit

The Service Assurance Manager records an audit event whenever a user login fails or when a user responds, or fails to respond promptly, to a notification. The IP Availability / Performance Manager records events when a monitored layer 2 or 3 device or a network adaptor on a monitored layer 2 or 3 device is unavailable. The Server Performance Manager records an audit event if a monitored server: is unavailable, has high processor utilization, has a hard drive failure, or has insufficient free memory. Events which are not generated on the Service Assurance Manager are recorded in the ECIM format and sent to the Service Assurance Manager for analysis, review, and storage.

The TOE audit records contain the following information:

Table 7 – Audit Record Contents

Field	Content
Timestamp	Date and time of the event
Class	Type of event

Field	Content
Source	Subject identity
Event State	Outcome

When audit events relating to the monitored network reach the Service Assurance Manager they are analyzed to determine the root cause of the event. The system uses patented Codebook Correlation Technology. This set of algorithms computes a correlation between the set of possible symptoms and the root cause that can best explain the symptoms, based on the nature of the symptoms and the network topology. The audit data can be viewed by TOE users with the roles All and Monitor through the Global Console and the web browser. Only users with the role All can delete audit events by rolling over the audit logs. The audit logs are stored in the file system of the underlying operating system. They are protected so that only authorized users can modify or delete these files.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAA.1, FAU_SAR.1, FAU_STG.1

6.1.2 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. For each user, the TOE stores the following security attributes in the database: username, password, and role. When TOE users enter their username and password at the Global Console interface or the web browser interface, the information is passed to the Service Assurance Manager, where it is verified. If the provided username and password are valid, the TOE user is assigned the role associated with that username. Before identification and authentication, the TOE user is only able to view active TOE components. The Strength of Function (SOF)-basic claim applies to this security function.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UID.1

6.1.3 Security Management

The TOE maintains three roles: All, Monitor and Ping. The All role has full access to all elements of the TOE. The Monitor role can only view information. The Ping role can only discover which TOE components are active. Users perform all management of the TOE through the Global Console or the web browser. A user can be set a ‘role’ of None, but this is not a true role and simply denies all access.

The TOE enforces which roles have access to TSF data, such as events and notifications and configuration settings. All and monitor roles have the ability to query TSF Data. Only the All role can modify or delete configuration settings. All is the only role that can modify or delete other users’ usernames, passwords, or roles. Attempts by the user to query, modify, or delete security attributes (such as username, password, or role), TSF data (such as audit data and configuration settings), and security are mediated by the TOE. The only security attributes maintained by the TOE are cryptographic. These cryptographic attributes include the algorithms and key lengths used. They are set to secure values and cannot be changed.

TOE Security Functional Requirements Satisfied: [FMT_MOF.1, FMT_MTD.1a, FMT_MTD.1b, FMT_SMF.1, FMT_SMR.1].

6.1.4 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 assure that physical connections made to the TOE remain intact and unmodified. The TOE protects information as it is transmitted between remote components of the TOE by protecting the information using AES with a key derived from a Diffie-Hellman exchange.

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, they are bound to the appropriate roles and any 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.

TOE Security Functional Requirements Satisfied: [FPT_ITT.1, FPT_RVM.1].

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 8 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure	Description
ACM_CAP.2	EMC Smarts Suite - Configuration Management: Capabilities	The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at EMC
ADO_DEL.1	EMC Smarts Suite - Delivery and Operation: Secure Delivery	The Delivery and Operation document provides a description of the secure delivery procedures implemented by EMC to protect against TOE modification during product delivery.
ADO_IGS.1	EMC Smarts IP Management Suite Installation Guide EMC Smarts Service Assurance Management Suite Installation Guide EMC Smarts Service Assurance Manager Configuration Guide	These are the Guidance documents for Installation and configuration of the EMC Smarts Suite.
ADV_FSP.1	EMC Smarts Suite - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence	This document describes the system security functions and externally visible interfaces.
ADV_HLD.1	EMC Smarts Suite - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence	This document describes the system interfaces and subsystems.
ADV_RCR.1	EMC Smarts Suite - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence	This document establishes the correspondence between the ST, the FSP, and the HLD design data.

Assurance Component	Assurance Measure	Description
AGD_ADM.1	EMC Smarts Service Assurance Manager Introduction EMC Smarts Service Assurance Manager Operator's Guide v6.5.1 Revision A01 EMC Smarts Service Assurance Manager Dashboard Configuration Guide EMC Smarts Business Impact Manager User's Guide EMC Smarts Report Manager User's Guide EMC Smarts IP Management Suite Discovery Guide EMC Smarts IP Availability Manager User's Guide EMC Smarts IP Performance Manager User's Guide EMC Smarts Server Performance Manager User's Guide	These are Guidance documents designed to assist the management user with the EMC Smarts Suite.
AGD_USR.1	N/A	None
ATE_COV.1	EMC Smarts Suite – Functional Tests and Coverage	This document describes the completeness of test coverage preformed against the TOE.
ATE_FUN.1	EMC Smarts Suite – Functional Tests and Coverage	This document describes the functional testing for the TOE to establish that the TSF exhibits the properties necessary to satisfy the functional requirements
ATE_IND.2	Provided by laboratory evaluation	None
AVA_SOF.1	EMC Smarts Suite - Vulnerability Assessment	This document provides The Strength of TOE Security Function Analysis.
AVA_VLA.1	EMC Smarts Suite - Vulnerability Assessment	This document provides evidence of how the TOE is resistant to attacks.

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. Table 9 demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 9 - Relationship of Security Threats to Objectives

Objectives		TOE Objectives							Environmental Objectives			
									IT		NON-IT	
Threats, Assumptions		O.ADMIN	O.AUDIT	O.IDAUTH	O.PROTECT	O.ACCESS	O.SECURE	O.MONITOR	OE.TIME	OE.SEP	NOE.NOEVIL	NOE.PHYSCL
Threats	T.NETWORK							✓	✓	✓		
	T.COMINT		✓	✓	✓	✓	✓		✓	✓		
	T.PRIVIL	✓	✓	✓	✓	✓			✓	✓		
Assumptions	A.CONNECT							✓				
	A.NOEVIL										✓	
	A.PHYSCL											✓

T.NETWORK **An unauthorized individual might disrupt the availability or performance of IP networks or servers.**

This threat is mitigated by the O.MONITOR objective which makes information on the unavailability or poor performance of IP networks and servers available to administrators in a timely and clear manner. This allows the administrators to take action to limit the impact of current problems and avoid future problems. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. 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.

T.COMINT **An unauthorized user may attempt to compromise the security of the data collected and produced by the TOE by bypassing a security mechanism.**

This threat is primarily diminished by the O.SECURE objective, which requires that the TOE ensure the security of all audit and System data. The O.PROTECT objective requires that the TOE protect itself from unauthorized modifications and access to its functions and data. The O.ACCESS objectives ensure that unauthorized modifications and access to functions and data is prevented. 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. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data. 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. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. 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.

T.PRIVIL **An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security 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. 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. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data. The O.PROTECT objective requires that the TOE protect itself from unauthorized modifications and access to its functions and data. 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. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. 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.

A.CONNECT **The TOE will be connected at all times to the network which it is intended to monitor.**

The O.MONITOR objective ensures that the TOE will be able to monitor the target network.

A.NOEVIL **Operators are non-hostile, appropriately trained, and follow all operator guidance.**

The NOE.NOEVIL objective ensures that operators are non-hostile, appropriately trained, and follow all operator guidance.

A.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.

8.2 Security Functional Requirements Rationale

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

Table 10 - Relationship of Security Requirements to Objectives

	Objectives	TOE							Env	
	Requirements	O.ADMIN	O.AUDIT	O.IDAUTH	O.PROTEC	O.ACCESS	O.SECURE	O.MONITOR	OE.TIME	OE.SEP
TOE	FAU_GEN.1		✓					✓		
	FAU_SAA.1							✓		
	FAU_SAR.1		✓					✓		
	FAU_STG.1						✓			
	FIA_ATD.1			✓						
	FIA_UAU.1			✓		✓				
	FIA_UID.1			✓		✓				
	FMT_MOF.1	✓			✓	✓				
	FMT_MSA.1						✓			
	FMT_MTD.1a	✓			✓	✓	✓			
	FMT_MTD.1b	✓			✓	✓	✓			
	FMT_SMF.1	✓								
	FMT_SMR.1	✓		✓						
	FPT_ITT.1						✓			
	FPT_RVM.1			✓	✓	✓	✓			
En	FPT_STM.1								✓	
	FPT_SEP.1									✓

O.AUDIT **The TOE must gather audit records of actions on the TOE which may be indicative of misuse.**

Security-relevant events must be audited by the TOE (FAU_GEN.1). The TOE must provide the ability to review the audit trail of the system (FAU_SAR.1). FAU_GEN.1 and FAU_SAR.1 together satisfy this objective.

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 TOE defines a set of roles (FMT_SMR.1). Only those roles are given the right to control the behavior of the TSF (FMT_MOF.1) and to access TSF data (FMT_MTD.1a and FMT_MTD.1b).

Mechanisms exist to enforce these rules (FMT_SMF.1). FMT_SMR.1, FMT_MOF.1, FMT_MTD.1a, FMT_MTD1.1b and FMT_SMF.1 together satisfy this objective.

O.IDAUTH **The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.**

Security attributes of subjects used to enforce the authentication policy of the TOE must be defined (FIA_ATD.1). The TOE will not give any security sensitive access to a user until the TOE has identified (FIA_UID.1) and authenticated (FIA_UAU.1) the user. The TOE must be able to recognize the different user roles that exist for the TOE (FMT_SMR.1). The TOE must ensure that all functions are invoked and succeed before each function may proceed (FPT_RVM.1). FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FMT_SMR.1 and FPT_RVM.1 together satisfy this objective.

O.PROTECT **The TOE must protect itself from unauthorized modifications and access to its functions and data.**

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_MOF.1). Only authorized users of the System may query and modify TOE data (FMT_MTD.1a and FMT_MTD.1b). The TOE must ensure that all functions are invoked and succeed before each function may proceed (FPT_RVM.1). FMT_MOF.1, FMT_MTD.1a, FMT_MTD1.1b and FPT_RVM.1 together satisfy this objective.

O.ACCESS **The TOE must allow authorized users to access only appropriate TOE functions and data.**

The TOE will not give any security sensitive access to a user until the TOE has identified (FIA_UID.1) and authenticated (FIA_UAU.1) the user. 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_MOF.1). Only authorized users of the System may query and modify TOE data (FMT_MTD.1a and FMT_MTD.1b). The TOE must ensure that all functions are invoked and succeed before each function may proceed (FPT_RVM.1). FIA_UID.1, FIA_UAU.1, FMT_MOF.1, FMT_MTD.1a, FMT_MTD.1b and FPT_RVM.1 together satisfy this objective.

O.SECURE **The TOE must ensure the security of all audit and System data.**

The TOE is required to protect the audit data from unauthorized deletion (FAU_STG.1). Only authorized users of the System may query and modify TOE data (FMT_MTD.1a and FMT_MTD.1b). The System must protect the confidentiality of information during transmission to a remote component of the TOE (FPT_ITT.1). The TOE must ensure that all functions to protect the data are not bypassed (FPT_RVM.1). FAU_STG.1, FMT_MTD.1a, FMT_MTD1.1b, FPT_ITT.1, and FPT_RVM.1 together satisfy this objective.

O.MONITOR **The TOE must gather, analyze and present information about all events that are indicative unavailability or poor performance of IP networks or servers.**

Events relevant to the unavailability or poor performance of IP networks or servers must be audited by the TOE (FAU_GEN.1). The events will be analyzed to indicate the root cause of the security violation (FAU_SAA.1). The TOE must provide the ability to review the audit trail of events on the monitored network (FAU_SAR.1). FAU_GEN.1, FAU_SAA.1 and FAU_SAR.1, together satisfy this objective.

OE.TIME **The IT Environment will provide reliable timestamps to the TOE.**

The IT Environment is required to provide reliable timestamps to the TOE (FPT_STM.1).

OE.SEP **The IT Environment will protect the TOE from external interference or tampering.**

The IT Environment must protect the TOE from interference that would prevent it from performing its functions (FPT_SEP.1).

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. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 11 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included.

Table 11 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAA.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FIA_ATD.1	None	NA	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UID.1	None	NA	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1a and FMT_MTD.1b	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	NA	
FMT_SMR.1	FIA_UID.1	✓	
FPT_ITT.1	None	NA	
FPT_RVM.1	None	NA	
FPT_SEP.1	None	NA	
FPT_STM.1	None	NA	

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) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. These sets 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 12 identifies the relationship between SFR and security functions, showing that all SFR are addressed and all security functions are necessary (i.e., they correspond to at least one SFR)..

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function, refer to Strength of Function (SOF) Rationale section.

Table 12 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1 FAU_SAA.1 FAU_SAR.1 FAU_STG.1	Audit records are generated by the TOE for events indicative of a misuse of the TOE or a lack of availability or poor performance in the monitored network.(FAU_GEN.1) The information is analyzed to determine the root cause of the problem (FAU_SAA.1). The TSF provides the users with the capability to read the audit data through the web browser and the Global Console (FAU_SAR.1) The audit logs are stored in the file system of the underlying operating system. They are protected so that only authorized users can modify or delete these files (FAU_STG.1). Together these contribute to a coherent security audit function.
Identification and Authentication	FIA_ATD.1 FIA_UAU.1 FIA_UID.1	The toe stores a username, a hashed password and a role for each authorized user (FIA_ATD.1). Before identification and authentication, the TOE user is only able to view active TOE components. (FIA_UID.1 and FIA_UAU.1) Together these contribute to a coherent identification and authentication function.
Security Management	FMT_MOF.1 FMT_MTD.1a FMT_MTD.1b FMT_SMF.1 FMT_SMR.1	The TOE maintains three roles – All, Monitor and Ping. (FMT_SMR.1) The TOE restricts unauthorized users from enabling, disabling, or modifying the behavior of the TOE (FMT_MOF.1). The TOE prevents unauthorized users from viewing or modifying TOE data. (FMT_MTD.1a and FMT_MTD.1b). The TOE can control the management of TSF data, security attributes, and security functions (FMT_SMF.1).
Protection of the TSF	FPT_ITT.1 FPT_RVM.1	The functions that enforce the TSP must succeed first before any other function can proceed. No other administrator functions can be performed before identification and authentication of the user is completed. (FPT_RVM.1) The TSF data is protected from disclosure when it is transmitted between separate parts of the TOE, because it is transmitted protected using AES. (FPT_ITT.1) Together these contribute to a coherent TOE protection function.

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. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. The chosen assurance level was also selected for conformance with the client's needs.

8.5.2.1 Configuration Management

The *EMC Smarts Suite - 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 Smarts Suite - 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 Smarts Suite - 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 errors message 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 Guidance documentation provides administrator and user guidance on how to securely operate the TOE. 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 Tests

There are a number of components that make up the *EMC Smarts Suite – 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 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
- Independent Testing

8.5.2.6 Vulnerability and TOE Strength of Function Analyses

The *EMC Smarts Suite - 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. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function analysis
- Vulnerability Analysis

8.6 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL2 assurance requirements, this SOF is sufficient to resist the threats identified in Section 3. The evaluated TOE is intended to operate in commercial and DOD low robustness environments processing unclassified information.

The only security functional requirement which has a probabilistic or permutational function is FIA_UAU.1 with a claim of SOF-basic. The Identification and Authentication function is password-based authentication. No cryptographic claims are made for this TOE, and thus cryptographic functionality does not fall within the scope of this Strength of Function analysis.

9 Acronyms

Table 13 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
EAL	Evaluation Assurance Level
FIPS	Federal information Processing Standards
GHZ	Gigahertz
ECIM	EMC Common Information Model
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MAC	Media Access Control
OS	Operating System
OSI	Incharge Common Information Model
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOF	Strength of Function
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy