Dell EMC™ Secure Remote Services v3.24

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1983-000-D102
Version: 1.7
12 December 2017

Dell EMC
176 South Street
Hopkinton, MA, USA
01748

Prepared by:

EWA-Canada
1223 Michael Street, Suite 200
Ottawa, Ontario, Canada
K1J7T2

EWA CANADA | An Intertek Company

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the TOE, the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operational environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell EMC™ Secure Remote Services v3.24 Security Target
ST Version:	1.7
ST Date:	12 December 2017

1.3 TOE REFERENCE

TOE Identification:	Dell EMC™ Secure Remote Services v3.24 with Secure Remote Services Policy Manager 6.8 (ESRS VE 3.24.30.04, ESRS DE 3.24.10.04 and Policy Manager 6.8.3 Build 129692)
TOE Developer:	Dell EMC
TOE Type:	Secure communications (other devices and systems)

1.4 TOE OVERVIEW

EMC Secure Remote Services is used by EMC hardware and software at customer sites to send a variety of information including configuration data, logs, error messages, usage and performance data to EMC and to allow identified EMC support personnel remote access to those systems for troubleshooting.

ESRS is an asynchronous messaging system in which all communications are initiated from the customer site. All communications between the customer's ESRS implementation and the EMC Enterprise servers use the Hypertext Transfer Protocol Secure (HTTPS) protocol with end-to-end Transport Layer Security (TLS) tunneling with strong encryption.

ESRS securely links a customer's EMC devices to the EMC Global Services support application systems using a session-based IP port-mapping solution. This distributed system provides customers with the commands and controls to authorize and log EMC support actions such as remote access connections, file transfers, diagnostic script executions, and system updates. ESRS supports:

- Dynamic device-level customer authorization control using a Policy Manager (PM)
- Logging of EMC-requested ESRS actions at the customer site
- All access restricted to authenticated and authorized EMC and partner personnel

The customer controls all EMC remote services access to the ESRS-managed products through the ESRS Server and its associated Policy Manager software. Connections with EMC devices and EMC at the ESRS-managed site originate from, and are managed by ESRS and the Policy Manager. This ensures secure communication using strong encryption and audit logging. The customer sets the policies of the Policy Manager, which controls ESRS remote access for support and file transfer events. The Policy Manager can be set to accept, ask for approval of, or deny remote services connection requests.

At EMC, a distributed EMC Enterprise suite is the processing core of the connection from a customer's ESRS implementation. The EMC Enterprise provides the mechanism for remote access activities from EMC Global Services along with the processing of information sent from EMC hardware and software at customer sites.

Figure 1 shows a typical deployment scenario.

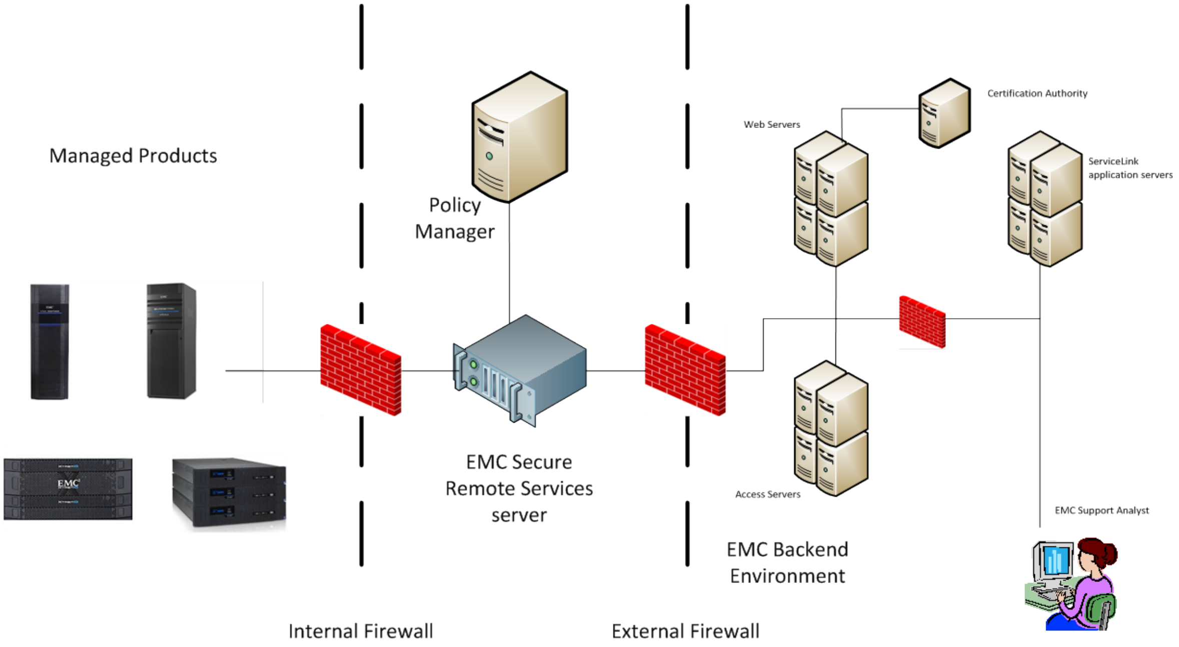

Figure 1 – ESRS Deployment

The TOE is a software only TOE.

1.4.1 ESRS System Interactions

The ESRS Server acts as a single point of entry and exit for all IP-based remote services activities and most EMC connect home notifications. Essentially, ESRS functions as a communications broker between the managed devices, the Policy Manager, and the EMC Enterprise. All communication with EMC initiates from ESRS. The ESRS servers are HTTP handlers. All messages are encoded using standard Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP) application protocols.

Once every 60 minutes, the ESRS Server determines if each managed device is available for service on the primary support applications. It does this by making a socket connection to the device on one or more of the primary support application ports and verifying that the service application(s) are responding. The information is recorded by the ESRS Server. If a change in status is detected, the ESRS Server notifies EMC over the next heartbeat.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of the ESRS Server software and the Secure Remote Services Policy Manager software.

Figure 2 shows the ESRS TOE Boundary using the ESRS Virtual Edition (VE), and

Figure 3 shows the ESRS TOE Boundary using the ESRS Docker Edition (DE).

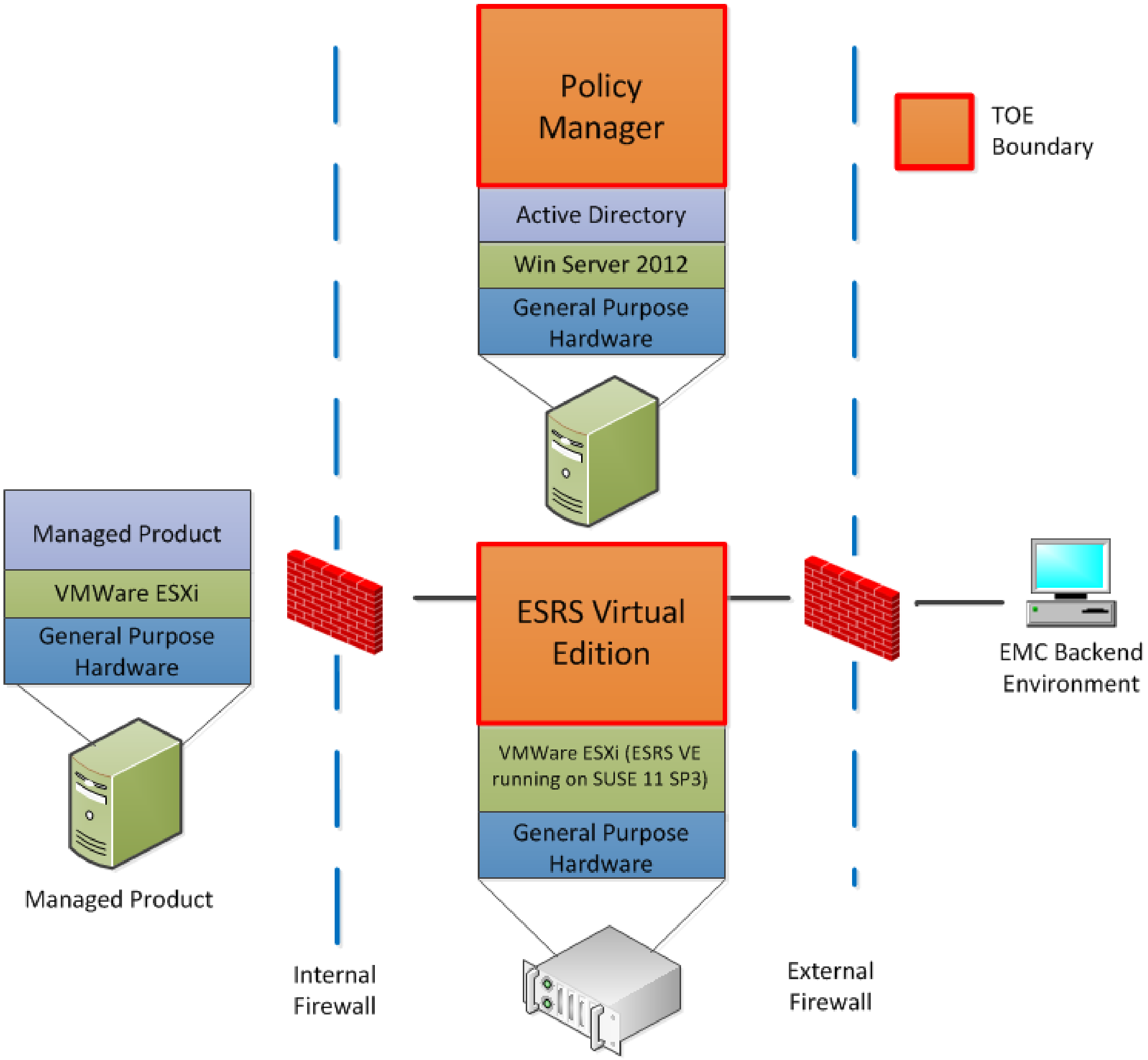

Figure 2 – ESRS TOE Boundary (ESRS VE)

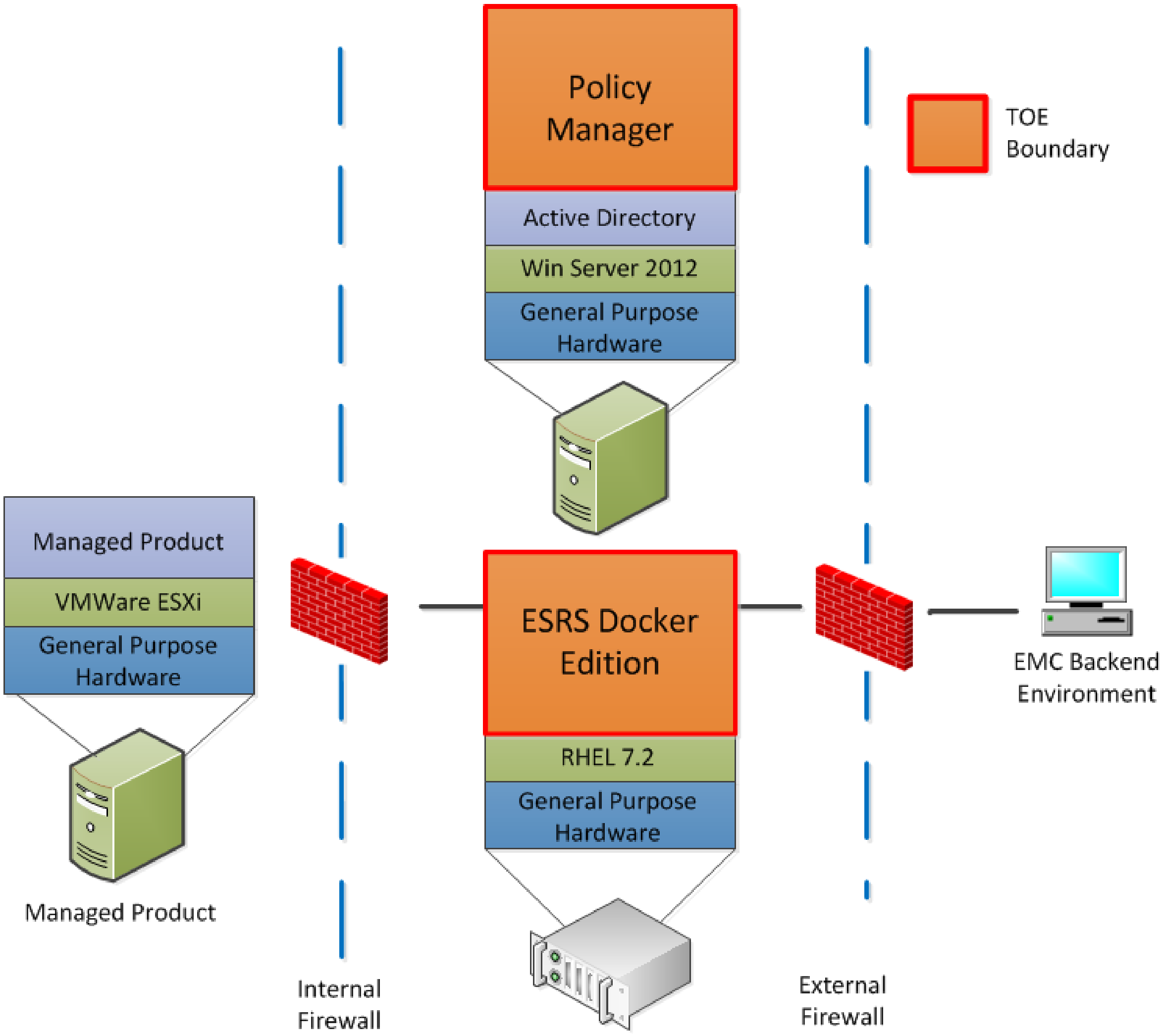

Figure 3 – ESRS TOE Boundary (ESRS DE)

1.5.2 TOE Environment

The following hypervisor, operating system, hardware and networking components are required for operation of the TOE in the evaluated configuration using ESRS Virtual Edition (VE).

Component	Supporting Operating System / Software	Hardware
ESRS Virtual Edition 3.24 (TOE component)	VMware ESXi 5.1, ESRS running on SUSE 11 SP3	General Purpose Computer Hardware

Component	Supporting Operating System / Software	Hardware
Secure Remote Services Policy Manager 6.8 (TOE component)	Windows Server 2012 R2 Active Directory	General Purpose Computer Hardware
Managed Product	Not applicable	Managed Product Hardware

Table 1 –Hardware and Software for ESRS VE

The following operating system, Docker Runtime, hardware and networking components are required for operation of the TOE in the evaluated configuration using ESRS DE.

Component	Supporting Operating System / Software	Hardware
ESRS Docker Edition 3.24 (TOE component)	Docker supported Red Hat Enterprise Linux Server 7.2 Docker EE 17.03	General Purpose Computer Hardware
Secure Remote Services Policy Manager 6.8 (TOE component)	Windows Server 2012 R2 Active Directory	General Purpose Computer Hardware
Managed Product	Not applicable	Managed Product Hardware

Table 2 –Hardware and Software for ESRS DE

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- EMC® Secure Remote Services Release 3.22 Technical Description (REV 01)
- EMC® Secure Remote Services Release 3.22 Port Requirements (REV 01)
- EMC® Secure Remote Services Release 3.22 Installation Guide (REV 01)
- EMC® Secure Remote Services Release 3.22 Operations Guide (REV 01)
- EMC® Secure Remote Services Policy Manager Version 6.8 Operations Guide (REV 001)
- Dell EMC® Secure Remote Services v3.24 Guidance Supplement, Version 1.0

1.5.4 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. Stored audit logs may be filtered and reviewed by authorized administrators.
Cryptographic Support	Cryptographic functionality is provided to allow the communications links between the TOE and trusted IT components and between the TOE and its remote administrators to be protected. Dell EMC affirms that the agent binaries for the cryptographic module are implemented as received from the module vendor. FIPS support is enabled by default through a configuration file.
User Data Protection	EMC Support personnel may be allowed access to customer owned resources to perform troubleshooting. This access is allowed or refused based on the implemented policy. The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE.
Identification and Authentication	Users must identify and authenticate prior to gaining TOE access. Passwords must meet minimum strength requirements, and are not displayed as they are entered.
Security Management	The TOE provides management capabilities via two web-based Graphical User Interfaces (GUIs), accessed via HTTPS. Management functions allow the administrators to manage users, access policies and perform audit review, based on the user's assigned role.
Protection of the TSF	Communications between the TOE and the EMC infrastructure are protected using TLS. Timestamp information is provided to support auditing.
TOE Access	Users are automatically logged out after a period of inactivity. Users may initiate log out at any time.
Trusted Path/Channel	The communications links between the TOE and its remote administrators are protected using HTTPS.

Table 3 – Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Remote user authentication verified through EMC network security
- Automatic software updates

Additionally, it should be noted that security provided by the managed product is not part of the evaluated functionality. If a connection from the EMC infrastructure to the managed product is allowed, the connection then relies on the security functionality provided by the managed product itself. If authentication is enforced by the managed product, then EMC support personnel must be provided with the appropriate credentials for logging in. Implementers must ensure that if multiple managed products are available on the same subnet, that all of these products are appropriately configured to control access. Otherwise, a support representative granted access to troubleshoot one device, may inadvertently have access to other devices on that subnet as well.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.UNAUTH	A hostile/unauthorized user may be able to gain access to troubleshooting channels to EMC storage equipment to access resources and data inappropriately.
T.TOEACCESS	An unauthorized user may be able to gain access to security management functions, resulting in unauthorized access to TOE data.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies (OSPs) applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
A.ACCESS	The TOE is connected to the network in such a way that it is able to access all of the access-controlled resources.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.

Assumptions	Description
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must control access of EMC support personnel to customer owned EMC equipment.
O.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE. The TOE must restrict security management functions from unauthorized use, in accordance with user roles.
O.AUDIT	The TOE must record audit records for use of the TOE functions, and access of the resources protected by the TOE. The TOE must provide functionality to read and filter audit records.
O.CRYPTO	ESRS must use Federal Information Processing Standards (FIPS)-validated cryptographic algorithms in support of cryptographic operations.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must ensure that the minimum password strength is enforced and that passwords are obscured as they are entered.
O.PROTECT	The TOE must protect the confidentiality of data transferred between the TOE and other IT products, and between the TOE and the administrative user.
O.TIME	The TOE must provide reliable timestamps.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.MANAGE	Those responsible for TOE deployment will provide competent administrators who are appropriately trained and follow all guidance.
OE.NETWORK	The network will be configured to allow controlled access from EMC support personnel to customer owned EMC equipment.
OE.PROTECT	Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack.

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptionsand threats identified for the TOE.

	T.UNAUTH	T.TOEACCESS	T.UNDETECT	A.ACCESS	A.LOCATE	A.MANAGE	A.NOEVIL
O.ACCESS	X						
O.ADMIN		X					
O.AUDIT			X				
O.CRYPTO		X					
O.IDENTAUTH		X					
O.PROTECT		X					
O.TIME			X				
OE.MANAGE						X	X
OE.NETWORK				X			

	T.UNAUTH	T.TOEACCESS	T.UNDETECT	A.ACCESS	A.LOCATE	A.MANAGE	A.NOEVIL
OE.PROTECT					X		

Table 8 – Mapping Between Objectives, Threats, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE back to the threats addressed by the TOE.

Threat: **T.UNAUTH**	A hostile/unauthorized user may be able to gain access to troubleshooting channels to EMC storage equipment to access resources and data inappropriately.	
Objectives:	O.ACCESS	The TOE must control access of EMC support personnel to customer owned EMC equipment.
Rationale:	O.ACCESS mitigates this threat by ensuring that access to customer owned EMC equipment is regulated by the TOE.	

Threat: **T.TOEACCESS**	An unauthorized user may be able to gain access to security management functions, resulting in unauthorized access to TOE data.	
Objectives:	O.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE. The TOE must restrict security management functions from unauthorized use, in accordance with user roles.
	O.CRYPTO	ESRS must use Federal Information Processing Standards (FIPS)-validated cryptographic algorithms in support of cryptographic operations.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must ensure that the minimum password strength is enforced and that

		passwords are obscured as they are entered. Users must be able to terminate administrative sessions, and sessions must automatically terminate after a period of inactivity.
	O.PROTECT	The TOE must protect the confidentiality of data transferred between the TOE and other IT products, and between the TOE and the administrative user.
Rationale:	O.ADMIN mitigates this threat by limiting access to security management functions to authorized administrators. O.CRYPTO mitigates this threat by ensuring that login credentials and other security management data is appropriately protected during transmission. O.IDENTAUTH mitigates this threat by ensuring that only identified and authenticated users may access security management functions and TOE data. O.PROTECT ensures that data passed to the TOE from the administrator and between the TOE and the EMC Infrastructure is appropriately protected.	

Threat: **T.UNDETECT**	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and access of the resources protected by the TOE. The TOE must provide functionality to read and filter audit records.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.AUDIT mitigates this threat by ensuring the provision of the data that may be used to discover inappropriate access. O.TIME ensures that audit data is supported with accurate time information.	

4.3.2 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption:	The TOE is connected to the network in such a way that it is able to

A.ACCESS	access all of the access-controlled resources.	
Objectives:	OE.NETWORK	The network will be configured to allow controlled access from EMC support personnel to customer owned EMC equipment.
Rationale:	OE.NETWORK supports this assumption by ensuring that access from the EMC infrastructure to the access-controlled resources is possible.	

Assumption: **A.LOCATE**	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PROTECT	Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack.
Rationale:	OE.PROTECT supports this assumption by protecting the TOE from physical attack.	

Assumption: **A.MANAGE**	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.MANAGE	Those responsible for TOE deployment will provide competent administrators who are appropriately trained and follow all guidance.
Rationale:	OE.MANAGE supports this assumption by ensuring that competent individuals are available to manage the TOE.	

Assumption: **A.NOEVIL**	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE. MANAGE	Those responsible for TOE deployment will provide competent administrators who are appropriately trained and follow all guidance.
Rationale:	OE.MANAGE supports this assumption by ensuring that the individuals managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, and an Evaluation Assurance Level that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and this is summarized in Table 9 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (Policy)
	FDP_ACC.1(2)	Subset access control (Role)

Class	Identifier	Name
	FDP_ACF.1(1)	Security attribute based access control (Policy)
	FDP_ACF.1(2)	Security attribute based access control (Role)
Identification and Authentication (FIA)	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3(1)	Static attribute initialisation (Policy)
	FMT_MSA.3(2)	Static attribute initialisation (Role)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.4	User-initiated termination
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 9 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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) [*policy changes*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

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

6.2.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*users in a role with the View privilege for the Audit Log tab*] with the capability to read [*all information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.3 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*filtering*] of audit data based on [*category, date, or group*].

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*in column 2 of Table 10*] and specified cryptographic key sizes [*in column 3 of Table 10*] that meet the following: [*standards in column 4 of Table 10*].

Usage	Key Generation Algorithm	Key Size (bits)	Standard
AES	Deterministic Random Bit Generator (DRBG)	256	SP800-90A
RSA	Keyed-hash Message Authentication Code (HMAC) DRBG	2048	SP800-90A

Table 10 – Cryptographic Operations

6.2.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*no standards*].

6.2.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in Table 11*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in Table 11*] and cryptographic key sizes [*cryptographic key sizes specified in Table 11*] that meet the following: [*list of standards specified in Table 11*].

Function	Algorithm	Key Size or Digest Length (bits)	Standard
Encryption and Decryption	AES	256	FIPS 197
Digital Signature	RSA	2048	FIPS 186-4
Keyed-Hash Message Authentication Code	HMAC-SHA-256	256	FIPS 198
Secure Hash	Secure Hash Algorithm SHA-256	256	FIPS 180-4

Table 11 - Cryptographic Operations

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1(1) Subset access control (Policy)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*Policy based access control SFP*] on [
Subjects: EMC Support Personnel
Objects: Customer-owned EMC equipment
Operations: Troubleshooting activities
].

6.2.3.2 FDP_ACC.1(2) Subset access control (Role)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*Role based access control SFP*] on [
Subjects: Policy Manager users
Objects: Access policies
Operations: view, create, *edit*
].

6.2.3.3 FDP_ACF.1(1) Security attribute based access control (Policy)

Hierarchical to: No other components.

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

FDP_ACF.1.1(1) The TSF shall enforce the [*Policy based access control SFP*] to objects based on the following: [
Subjects: EMC Personnel
Subject attributes: no attributes
Objects: Customer-owned EMC equipment
Object attributes: *Connection policy for the equipment*
].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
a. EMC support personnel will be granted access to troubleshoot a customer's equipment if the access policy for that connection is 'always allow'; and
b. EMC support personnel will be granted access to troubleshoot a customer's equipment if the access policy for that connection is 'requires approval' and the ESRS Administrator approves the access within five minutes of the request].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no other rules*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

a. *EMC support personnel will be denied access to troubleshoot a customer's equipment if the access policy for that connection is 'never allow'*; and
b. *EMC support personnel will be denied access to troubleshoot a customer's equipment if the request is issued outside of an established time window*

].

6.2.3.4 FDP_ACF.1(2) Security attribute based access control (Role)

Hierarchical to: No other components.

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

FDP_ACF.1.1(2) The TSF shall enforce the [*Role based access control SFP*] to objects based on the following: [
Subjects: Policy Manager users
Subject Attributes: Role
Objects: Access policies
Object Attributes: no attributes
].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*users of the Policy Manager application are able to view, create, edit and delete policies according to the permissions associated with the user's role*].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets ~~meet~~ **include** [

- *a minimum of 8 characters;*
- *a mix of upper and lowercase letters;*
- *a number; and*
- *a special character*

].

6.2.4.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.3 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*asterisks*] to the user while the authentication is in progress.

6.2.4.4 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Policy based access control SFP*, *Role based access control SFP*] to restrict the ability to [query, modify, delete, [*create*]] the security attributes [*connection policy*, *role*] to [*Policy Manager Administrator and Policy Manager Users*].

6.2.5.2 FMT_MSA.3 (1) Static attribute initialisation (Policy)

Hierarchical to: No other components.

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

FMT_MSA.3.1(1) The TSF shall enforce the [*Policy based access control SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*Administrator role*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 FMT_MSA.3(2) Static attribute initialisation (Role)

Hierarchical to: No other components.

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

FMT_MSA.3.1(2) The TSF shall enforce the [*Role based access control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*Administrator role*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*user management, policy management*, *audit review*].

6.2.5.5 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Policy Manager Administrator, Policy Manager User, ESRS Server Admin*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

6.2.6.2 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.1 TSF-initiated session locking

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an interactive session after [*30 minutes of user inactivity*] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [*the user must login*].

6.2.7.2 FTA_SSL.4 User-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*administration*]].

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDENAUTH	O.PROTECT	O.TIME
FAU_GEN.1			X				
FAU_SAR.1			X				
FAU_SAR.3			X				
FCS_CKM.1				X			
FCS_CKM.4				X			
FCS_COP.1				X			
FDP_ACC.1(1)	X						
FDP_ACC.1(2)		X					
FDP_ACF.1(1)	X						
FDP_ACF.1(2)		X					
FIA_SOS.1					X		
FIA_UAU.2					X		
FIA_UAU.7					X		
FIA_UID.2					X		

	O.ACCESS	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDENAUTH	O.PROTECT	O.TIME
FMT_MSA.1		X					
FMT_MSA.3(1)		X					
FMT_MSA.3(2)		X					
FMT_SMF.1		X					
FMT_SMR.1		X					
FPT_ITC.1						X	
FPT_STM.1							X
FTA_SSL.1					X		
FTA_SSL.4					X		
FTP_TRP.1						X	

Table 12 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ACCESS**	The TOE must control access of EMC support personnel to customer owned EMC equipment.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control (Policy)
	FDP_ACF.1(1)	Security attribute based access control (Policy)
Rationale:	FDP_ACC.1(1) and FDP_ACF.1(1) describe the use of policy to determine access by EMC support personnel to customer owned EMC equipment.	

Objective: **O.ADMIN**	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE. The TOE must restrict security management functions from unauthorized use, in accordance with user roles.	
Security Functional	FDP_ACC.1(2)	Subset access control (Role)
	FDP_ACF.1(2)	Security attribute based access control (Role)

Requirements:	FMT_MSA.1	Management of security attributes
	FMT_MSA.3(1)	Static attribute initialisation (Policy)
	FMT_MSA.3(2)	Static attribute initialisation (Role)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Rationale:	FDP_ACC.1(2) and FDP_ACF.1(2) describe the use of roles to determine access to Policy Manager functions. FMT_MSA.1 enforces restricted access to the security attributes that determine the behaviour of the SFPs. FMT_MSA.3(1) and FMT_MSA.3(2) describe the nature of the default values for those attributes. FMT_SMF.1 describes the security management functionality, and FMT_SMR.1 describes the security roles that are used to access that functionality.	

Objective: **O.AUDIT**	The TOE must record audit records for use of the TOE functions, and access of the resources protected by the TOE. The TOE must provide functionality to read and filter audit records. Stored audit records must be protected from unauthorized modification or deletion.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Rationale:	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FAU_SAR.1 describes the functionality to be able to read the audit records, and FAU_SAR.3 ensures that audit records may be filtered for viewing.	

Objective: **O.CRYPTO**	ESRS must use Federal Information Processing Standards (FIPS)-validated cryptographic algorithms in support of cryptographic operations.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Rationale:	FCS_CKM.1 describes the algorithms key sizes and standards used in the generation of keys.	

	FCS_CKM.4 describes the destruction of keys. FCS_COP.1 describes the algorithms, key sizes and standards applicable for the use of keys.

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must ensure that the minimum password strength is enforced and that passwords are obscured as they are entered. Users must be able to terminate administrative sessions, and sessions must automatically terminate after a period of inactivity.	
Security Functional Requirements:	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.4	User-initiated session locking
Rationale:	FIA_UID.2 and FIA_UAU.2 ensure that users are identified and authenticated before being granted access to TOE functionality. FIA_SOS.1 ensures that the ESRS passwords meet the strength requirements. FIA_UAU.7 ensures that only obfuscated feedback is provided when entering passwords. FTA_SSL.1 ensures that Policy Manager GUI sessions are terminated after a period of inactivity, and FTA_SSL.4 ensures that Policy Manager GUI users may log out at any time.	

Objective: **O.PROTECT**	The TOE must protect the confidentiality of data transferred between the TOE and other IT products, and between the TOE and the administrative user.	
Security Functional Requirements:	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FTP_TRP.1	Trusted path
Rationale:	FPT_ITC.1 ensures that data transmitted from the TOE to another trusted IT product is protected from disclosure. FTP_TRP.1 ensures that the communications path between remote administrators and the TOE is protected from modification and disclosure.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 ensures that reliable timestamps are provided in support of the audit function.	

6.4 DEPENDENCY RATIONALE

Table 13 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	This is satisfied by FCS_COP.1
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	This is satisfied by FCS_CKM.1
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	This is satisfied by FCS_CKM.1
	FCS_CKM.4	✓	
FDP_ACC.1 (1)	FDP_ACF.1	✓	This is satisfied by FDP_ACF.1(1)
FDP_ACC.1 (2)	FDP_ACF.1		This is satisfied by FDP_ACF.1(2)
FDP_ACF.1 (1)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(1)
	FMT_MSA.3		This is satisfied by FMT_MSA.3(1)
FDP_ACF.1 (2)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(2)

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_MSA.3	✓	This is satisfied by FMT_MSA.3(2)
FIA_SOS.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	This dependency is satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FIA_UAU.7	FIA_UAU.1	✓	This dependency is satisfied by FIA_UAU.2, which is hierarchical to FIA_UAU.1
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	This is satisfied by FDP_ACC.1(1) and FDP_ACC.1(2)
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3 (1)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3 (2)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	This dependency is satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FPT_ITC.1	None	N/A	
FPT_STM.1	None	N/A	
FTA_SSL.1	FIA_UAU.1	✓	This dependency is satisfied by FIA_UAU.2, which is hierarchical to FIA_UAU.1
FTA_SSL.4	None	N/A	
FTP_TRP.1	None	N/A	

Table 13 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in Table 14.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage

Assurance Class	Assurance Components	
	Identifier	Name
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 14 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

Policy Manager generates audit log entries for the following activities performed by a Policy Manager user:

- Log in to or out of the application
- Accept or deny a pending request for an action
- Modify a policy
- Create, modify, or delete a permission for a policy
- Create, modify, delete, or assign a filter to a permission
- End a remote session
- Modify the configuration of an asset group
- Modify the details of an asset
- Create, modify, or delete profiles, roles, and users

Policy Manager generates audit log entries for the following activities that are not initiated by a Policy Manager user but result from ESRS Client communication with Policy Manager:

- An action pending approval times out before it is accepted or denied.
- ESRS Client registers with Policy Manager
- ESRS Client sends a request to perform an action that has an access right of “Ask for Approval”.
- After receiving approval for an action, ESRS Client performs the action.
- ESRS Client performs an action that has an access right of “Always Allow”. The message sent to the audit log includes the name of the user who requested the action, the action that was performed, and the success or failure of executing the action.
- ESRS Client denies an action that has an access right of “Never Allow”. The message sent to the audit log includes the name of the user who attempted to perform the action, information about the action that was rejected (specific to the type of action), and the permission that caused the action to be rejected.
- ESRS Client starts or stops a remote session that was requested by a user through the Enterprise server.
- ESRS Client ends a remote session at the request of a Policy Manager user.

Logs include the following information:

- Date/Time – The date and time that the action was generated or initiated.
- Category – The category represents a type of activity, which can be User Access (logins, logouts), Asset Communication (messages from ESRS Clients or sent to ESRS Clients), Configuration (Assets tab), Remote Access (Remote Sessions tab), or Administration (Users tab -create, modify, and delete profiles, roles, and users).
- Message – A detailed description of the activity.
- Group – The name of the Policy Manager asset group related to the entry.
- User – The name of the user associated with the activity that was audited.

Audit records may be read from the Audit Log tab of the Policy Manager application. This tab is available to users in a role with the View privilege for the Audit Log tab. In the evaluated configuration, the administrator role has the required permissions to view the Audit Log tab. When viewing the audit logs, the administrator may filter the logs that appear on the Audit Log tab based on category, date or group.

The ESRS Server queues all Policy Manager-related auditing messages in its audit logs until they are sent to Policy Manager for processing. If the Policy Manager is offline, the ESRS component persists the messages until they can be communicated to the Policy Manager.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3.

7.2 CRYPTOGRAPHIC SUPPORT

ESRS employs the OpenSSL FIPS Object Module (2.0.2) (CMVP Certificate # 1747). Encryption is used in the following places:

- Using OpenSSL, all communications are encrypted between the ESRS Server and EMC. TLS 1.2 is supported in the evaluated configuration. The supported ciphersuite uses 256 bit AES, 2048 bit RSA and SHA-256.
- All communications from the ESRS to the administrator over the web GUI are encrypted using TLS 1.2. The supported ciphersuite uses 256 bit AES, 2048 bit RSA and SHA-256.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.3 USER DATA PROTECTION

7.3.1 Policy based access control SFP

ESRS allows the customer to permit EMC customer support personnel remote access to products for troubleshooting based on policies.

A heartbeat message is sent over an encrypted link from the ESRS to the EMC infrastructure every 30 seconds. If an error message, or any other information identified by the managed device for EMC, has been received from any of the managed devices, this will be sent with the next heartbeat. This information is monitored by EMC. When an EMC customer service representative recognizes a problem and requires remote access to troubleshoot, a notification is made available to the customer's ESRS implementation. When queried, the customer's ESRS gateway retrieves the request. The ESRS notifies the Policy Manager, and, if policy is set to 'Ask for Approval', the Policy Manager sends an email message to the designated contact requesting access. Access is allowed if the policy is set to 'Allow', and denied if the policy is set to 'Deny'. The request includes the identification of the product, the application to be used and the userID of the customer service representative requesting the access. ESRS checks the policy to determine if access is allowed. The options are: never allow, always allow or requires approval. If the option is never allow, the connection is denied. If the option is always allow, a session is established from EMC to the product, and the access is audited in the Policy Manager. If approval is required, an email message is sent from the Policy Manager to the designated email address. This email includes a link that will open the Policy Manager interface. The administrator must log in to Policy Manager and approve the connection. This person has five minutes to approve the connection, otherwise the connection is denied.

Additionally, a filter may be applied to the access control decision. This type of filter creates a time window (which may be called a maintenance window) in which allow or ask for approval actions are permitted. All requests received outside of the maintenance window are then denied.

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACF.1(1).

7.3.2 Role based access control SFP

Role based access control is enforced on the Policy Manager. The Policy Manager component supports two roles: Administrator and User. Administrators may perform all actions, while users may only view policies.

TOE Security Functional Requirements addressed: FDP_ACC.1(2), FDP_ACF.1(2).

7.4 IDENTIFICATION AND AUTHENTICATION

In the evaluated configuration, Active Directory authentication is used to log into the Policy Manager. Users must be identified and authenticated prior to performing any actions.

There is a single user account on the ESRS Server, with the default account name 'admin'. This name is configurable at deployment. Password rules are enforced on this account. The password must include a minimum of eight characters, upper and lowercase letters, a number and a special character. The characters of the password are obfuscated as they are entered by the admin user.

TOE Security Functional Requirements addressed: FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2.

7.5 SECURITY MANAGEMENT

There are two interfaces provided for the management of security functionality: the ESRS Server Web UI and the Policy Manager GUI. The ESRS Server Web UI may be used for configuration and status viewing related to the Managed File Transfer (MFT) communication between the customer's ESRS implementation and the EMC Infrastructure. The Policy Manager GUI is used to perform most of the security management functions related to the security claims, including user management (of Policy Manager users), policy management and audit review.

7.5.1 ESRS Server Web UI

When the ESRS Server is installed, a single administrative account is created. The ESRS Server Web UI may be used to view the system status, view remote session status, view a list of files that are to be sent to EMC, view alert messages, view the status of the various system services and control access to the MFT functionality.

7.5.2 Policy Manager GUI

Security Management functions including user management, policy management and audit review are performed using the Policy Manager GUI. Access to the various functions in Policy Manager is controlled using profiles, roles and users. Profiles are sets of permissions created to perform a particular task or set of tasks. Table 15 shows the permissions that may be assigned to a profile. Roles are a group of profiles that are assembled to allow the performance of a particular function. When a user is created, the 'Is Administrator' checkbox may be selected. This automatically gives the user all permissions. Otherwise, the user may be assigned to one or more roles. In the evaluated configuration, two roles are implemented: the default Policy Manager Administrator role with all privileges, and a Policy Manager User role with permissions to view policy and users.

Component/Privilege	Options
Policy	View
	Add/Edit
Pending Requests	View
	Add/Edit
Audit Logs	View
Assets	View
	Add/Edit
Users	View

Component/Privilege	Options
	Add/Edit
Remote Sessions	View
	End

Table 15 – Permissions

Based on the user's assigned role(s), the user will be able to query (view), modify (edit), delete (edit) or create (add) attributes that determine connection policies and user roles. The attributes used by the Policy based access control SFP are set to allow access by default, making the defaults inherently permissive. The attributes used by the Role based access control SFP do not exist until they are created by an administrator, making the default values inherently restrictive.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.6 PROTECTION OF THE TSF

Communications between the ESRS Server and the EMC Infrastructure are protected by TLS using the OpenSSL cryptographic module.

7.6.1 ESRS Server to EMC

The ESRS Server sends regular heartbeat messages to EMC. EMC monitors the values sent and may automatically trigger service requests if the ESRS Server fails to send heartbeats or if the values contained in a heartbeat exceed certain limits.

The ESRS Server serves as a conduit for EMC products to send remote notification event files to EMC. EMC hardware platforms use remote notification for several purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to EMC. When an alert condition occurs, the EMC device generates an event message file (known as a 'connect home') which is passed to the ESRS Server. When an event file is received, the ESRS Server opens the TLS tunnel to the EMC Enterprise, and posts the data file to EMC. At EMC, the file is forwarded to the Customer Relationship Management systems.

TOE Security Functional Requirements addressed: FPT_ITC.1.

7.6.2 Timestamps

ESRS ensures that reliable timestamps are included in audit logs.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.7 TOE ACCESS

Users of the Policy Manager GUI are automatically logged out after 30 minutes of inactivity. The user may also terminate the session at any time.

TOE Security Functional Requirements addressed: FTA_SSL.1, FTA_SSL.4.

7.8 TRUSTED PATH / CHANNELS

The TOE provides a TLS-protected link between the remote user and the ESRS Server. Each established link between the user and the ESRS server is logically distinct from any other communications with the ESRS. All communications are initiated by the user; therefore the user is able to identify the component by entering the correct URL. The administrative user is authenticated to the ESRS Server through username and password. The connections are used for administration. The data that is passed along this path is protected from modification and disclosure through the use of TLS.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
ESRS	The term 'ESRS' is used to refer to the system that would be procured by a customer. This includes the ESRS and Policy Manager components. 'ESRS Server' refers to the ESRS component, which may be either ESRS VE, or ESRS Docker.
Administrator	The term 'Administrator' is used to describe anyone using the Policy Manager GUI or ESRS Server Web UI. The terms 'Policy Manager Administrator', 'Policy Manager User' and 'ESRS Server Admin' are used to describe those specific roles.

Table 16 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
DE	Docker Edition
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ESRS	EMC Secure Remote Services
FIPS	Federal Information Processing Standards
FTPS	File Transfer Protocol Secure
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol

Acronym	Definition
IT	Information Technology
MFT	Managed File Transfer
OSP	Organizational Security Policy
PM	Policy Manager
PP	Protection Profile
RSA	Rivest, Shamir and Adleman
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
URL	Uniform Resource Locator
VE	Virtual Edition
XML	Extensible Markup Language

Table 17 – Acronyms