EMC VPLEX® v5.5 Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1924-000-D102
Version: 0.8
18 April 2016

Prepared For:

EMC Corporation
176 South Street
Hopkinton, MA, USA
01748

Prepared By:

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

Enabling a More Secure Future

Common Criteria Consulting LLC
15804 Laughlin Ln
Silver Spring, MD, USA
20906

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 (ST) 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 operating 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 Information Technology (IT) environment.

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	EMC VPLEX® v5.5 Security Target
ST Version:	0.8
ST Date:	18 April 2016

1.3 TOE REFERENCE

TOE Identification:	EMC VPLEX® with VS2 Hardware and v5.5 Software (5.5.1.01.00.5)
TOE Developer:	EMC Corporation
TOE Type:	Other Devices and Systems (hardware and software)

1.4 TOE OVERVIEW

EMC VPLEX federates data that is located on heterogeneous storage arrays to create dynamic, distributed and highly available data centers. VPLEX is an appliance-based solution that connects to Fibre Channel (FC) Storage Area Network (SAN) interfaces or Ethernet switches. VPLEX components are delivered as appliances.

VPLEX addresses three primary IT needs:

- Mobility: VPLEX moves applications and data between different storage installations within a geographical region.
- Availability: VPLEX creates high-availability storage infrastructure across these same varied geographies.
- Collaboration: VPLEX provides efficient real-time data collaboration over distance for Big Data applications.

VPLEX is offered in three cluster configurations based on the number of engines installed in a cluster: Single-engine, dual-engine, and quad-engine. Each configuration provides identical security functionality; the only difference between them is aggregate throughput and the number of SAN interfaces.

One management server (a dedicated appliance) is included with each cluster and provides system management capabilities via Ethernet interfaces. The management server provides the capability to configure engine interfaces in the engines and monitor the operation of the cluster.

Each engine within a cluster includes two independent directors that handle all I/O traffic, including read/write requests from hosts to back-end storage (in the TOE Environment). Each director supports 4 I/O Modules (IOMs) that provide either 8 GB/s Fibre Channel interfaces or 10 Gb/s Ethernet interfaces. The IOMs provide connections for:

- Front-end SAN connections to hosts
- Back-end SAN connections to storage
- Remote VPLEX cluster connections

VPLEX Metro consists of two VPLEX clusters connected by inter-cluster links with not more than 5ms Round Trip Time (RTT). VPLEX Metro:

- Enables seamless operation with EMC and non-EMC storage arrays. Transparent data mobility between arrays is supported for simple, fast data movement and technology refreshes.
- Standardizes LUN presentation and management using simple tools to provision and allocate virtualized storage devices.
- Improves storage utilization using pooling and capacity aggregation across multiple arrays.
- Transparently relocates data and applications over distance, protects your data center against disaster, and enables efficient collaboration between sites. All of the storage in both data centers may be managed from one management interface.
- Mirrors data to a second site, with full access at near local speeds.

VPLEX Witness may also be deployed to help automate the response to cluster failures and inter-cluster link outages. VPLEX Witness executes on a separate platform and connects to both clusters in a deployment. VPLEX Witness is part of the TOE Environment.

A representative diagram of a VPLEX Metro deployment is shown in the following diagram.

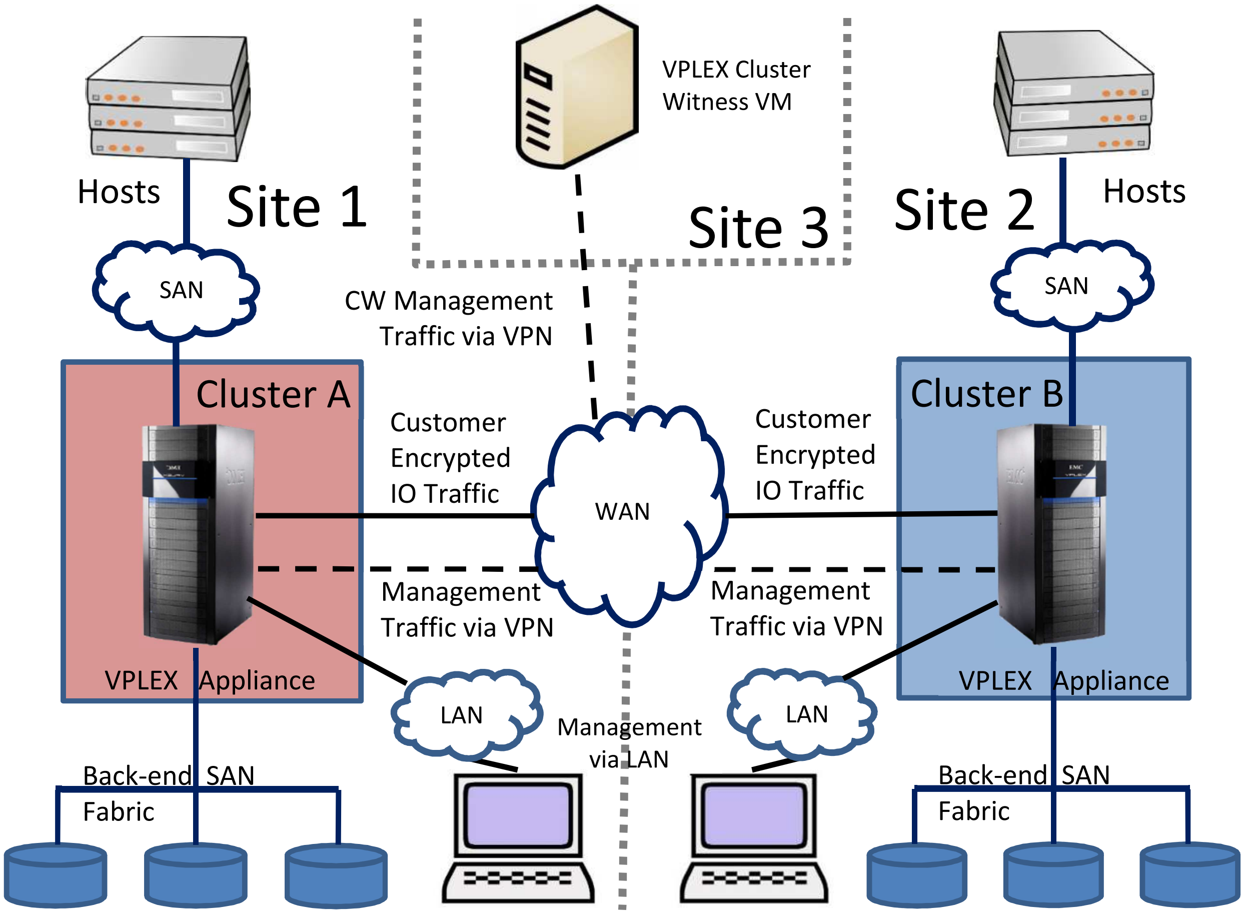

Figure 1 - VPLEX Representative Deployment

VPLEX limits access from hosts to the back-end storage based upon configured Storage Views, which define allowed connections between:

- Registered initiators – hosts with Host Bus Adapters (HBAs) installed that are connected to VPLEX through the front-end SAN.
- VPLEX IOM Ports – the front-end ports physically located on the VPLEX directors that are exposed to the hosts.
- Virtual Volumes – logical storage volumes constructed from the back-end storage arrays connected to VPLEX. Hosts are presented with Virtual Volumes when accessing the data accessed via the TOE.

Administrators interact with VPLEX via a web-based Graphical User Interface (GUI) or a Command Line Interface (CLI). Multiple simultaneous management sessions are supported. Each session requires the administrator to log in. Multiple administrator accounts and roles are supported, enabling different access permissions to be associated with different administrators. User accounts are defined within VPLEX.

SNMP access is supported for information retrieval only.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

A VPLEX system includes one or two clusters, each including the following components:

- One management server
- One, two or four engines with appropriate IOMs

VS2 hardware refers to the combination of server and engine hardware, and v5.5 software refers to the software executing on the server and engines.

The management server and engines, hardware and software, are included in the TOE boundary. The TOE is represented by the items labeled VPLEX Appliance in Figure 1. A private network is established between cluster components for intra-cluster communication.

1.5.2 TOE Environment

The hosts and storage devices that are connected to VPLEX are part of the TOE Environment. User data is passed over the SAN. It is the responsibility of the TOE Environment to protect this traffic from unauthorized disclosure or modification.

Dual-engine and quad-engine configurations use Fibre Channel switches to interconnect the cluster components.

VPN connections are required between the clusters at each location. These connections must protect the user data as well as management traffic from disclosure and modification.

VPLEX Witness may be deployed. VPN connections are required between VPLEX Witness and the clusters at each location. These connections must protect the traffic from disclosure and modification.

Administrators may access VPLEX via HTTPS (for the GUI) or SSH (for the CLI). It is the responsibility of the TOE Environment to protect this traffic from unauthorized disclosure or modification.

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- *EMC® VPLEX™ Hardware Installation Guide (Rev A01)*
- *EMC® VPLEX™ Site Preparation Guide (Rev 06)*
- *EMC® VPLEX® GeoSynchrony Configuration Guide (Rev 07)*
- *EMC VPLEX® GeoSynchrony Version 5.5 Administration Guide (Rev 01)*
- *EMC VPLEX® GeoSynchrony Version 5.5 CLI Reference Guide (Rev 01)*
- *EMC® VPLEX® Security Configuration Guide (Rev 12)*
- *EMC® VPLEX® Version 5.5 Product Guide (Rev 01)*

- *Unisphere for VPLEX Online Help (5.5.0.00.00.11)*
- *EMC VPLEX® v5.5 Common Criteria Supplement (v0.4)*

1.5.4 Logical Scope

Functional Classes	Description
Security Audit	Audit entries are generated for security related events, and can be reviewed by authorized users.
User Data Protection	The TOE mediates all data requests from Initiators to prevent unauthorized access to back-end storage. By default access to volumes is restricted. Authorized administrators may configure allowed access between Initiators and back-end storage. Authorized administrators may configure data mirroring for specified volumes.
Identification and Authentication	Administrators must identify and authenticate prior to TOE access.
Security Management	The TOE provides management capabilities via GUI and CLI interfaces. Multiple roles are supported to provide varying levels of access to data and functions.
TOE Access	User sessions may be terminated by users, or by the TOE if they are inactive longer than the configured inactivity limit. A configured banner is displayed to users during CLI login.

Table 1 - Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following product features are excluded from this evaluation:

- RecoverPoint integration
- REST API
- High Availability
- EMC Secure Remote Support (ESRS)
- Connect-Home

In addition to internal user accounts, VPLEX may be integrated with an external OpenLDAP or Active Directory server.

In addition to VPLEX Metro, single-cluster deployments known as VPLEX Local are also supported.

In addition to VS2 hardware, VS1 hardware is also supported.

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 Requirements 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 [CEM] 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

The TOE for this ST does not claim conformance with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 2 lists the threats addressed by the TOE. Mitigation to the threats is through the objectives identified in Section 4.1 Security Objectives.

Threat	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.UNAUTH_ACCESS	A server acting on a behalf of a user request may attempt to access user data (volumes) that it is not authorized to access.

Table 2 - Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed upon an organization in the operational environment. Table 3 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.MANAGE	The TOE shall only be managed by authorized users.
P.MIRROR	Administrators may configure data mirroring between clusters for data redundancy.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 3 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 4.

Assumptions	Description
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETWORK	The TOE components, front-end hosts, back-end storage and management workstations will be interconnected by a segregated network that protects the traffic from disclosure to or modification by untrusted systems or users.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

Table 4 – 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 allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for security relevant events.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.MIRROR	The TOE must perform data mirroring between clusters for administrator-specified volumes.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.TIME	The TOE will maintain reliable timestamps.

Table 5 – 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 domain or by non-technical or procedural means.

Security Objective	Description
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.NETWORK	The operational environment will provide a segregated network that protects the traffic between the TOE components and front-end hosts, back-end storage and management workstations from disclosure to or modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 6 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organisational policies identified for the TOE.

	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.MANAGE	P.MIRROR	P.PROTECT	A.MANAGE	A.NETWORK	A.NOEVIL	A.PROTECT
O.ACCESS	X	X	X		X						
O.AUDITS				X							
O.EADMIN	X		X		X						

	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.MANAGE	P.MIRROR	P.PROTECT	A.MANAGE	A.NETWORK	A.NOEVIL	A.PROTECT
O.IDAUTH	X	X		X	X						
O.MIRROR						X					
O.PROTCT		X			X						
O.TIME				X							
OE.CREDEN					X					X	
OE.INSTAL	X				X					X	
OE.NETWORK									X		
OE.PERSON					X			X			
OE.PHYCAL							X			X	X

Table 7 - Mapping Between Objectives, Threats, Organizational Security Policies, 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 and the Operational Environment back to the threats addressed by the TOE.

Threat: T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
Rationale:	The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.	

Threat: T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.	

Threat: T.UNAUTH_ACCESS	A server acting on a behalf of a user request may attempt to access user data (volumes) that it is not authorized to access.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.

	O.AUDITS	The TOE must record audit records for security relevant events.
Rationale:	The O.ACCESS objective only permits authorized access TOE data. The O.AUDITS objective supports O.ACCESS by requiring the TOE to record audit data for unauthorized access attempts.	

4.3.2 Security Objectives Rationale Related to Organizational Security Policies

The security objectives rationale related to OSPs traces the security objectives for the TOE and the Operational Environment back to the OSPs applicable to the TOE.

Policy: **P.ACCACT**	Users of the TOE shall be accountable for their actions within the TOE.	
Objectives:	O.AUDITS	The TOE must record audit records for security relevant events.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.TIME	The TOE will maintain reliable timestamps.
Rationale:	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.	

Policy: **P.MANAGE**	The TOE shall only be managed by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.

	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
Rationale:	The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.	

Policy: P.MIRROR	Administrators may configure data mirroring between clusters for data redundancy.	
Objectives:	O.MIRROR	The TOE must perform data mirroring between clusters for administrator-specified volumes.
Rationale:	The O.MIRROR objective requires the TOE to perform data mirroring as configured by administrators.	

Policy: P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.	
Objectives:	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.	

4.3.3 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: A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
Rationale:	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.	

Assumption: A.NETWORK	The TOE components, front-end hosts, back-end storage and management workstations will be interconnected by a segregated network that protects the traffic from disclosure to or modification by untrusted systems or users.	
Objectives:	OE.NETWORK	The operational environment will provide a segregated network that protects the traffic between the TOE components and front-end hosts, back-end storage and management workstations from disclosure to or modification by untrusted systems or users.
Rationale:	The OE.NETWORK objective ensures that the management traffic will be protected by a segregated LAN.	

Assumption: **A.NOEVIL**	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	
Objectives:	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.	

Assumption: **A.PROTCT**	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.	
Objectives:	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYCAL provides for the physical protection of the TOE software and the hardware on which it is installed.	

5 EXTENDED COMPONENTS DEFINITION

5.1 EXTENDED FUNCTIONAL COMPONENTS

5.1.1 FDP_MRR_EXT User Data Mirroring

Family Behaviour:

This family defines the requirements for the TOE to provide data mirroring for specified volumes in the operational environment.

Component Levelling:

FDP_MRR_EXT User Data Mirroring
1

FDP_MRR_EXT.1 User Data Backup/Restore provides for the functionality to perform data mirroring for volumes as directed by administrators.

Management:

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

a) Configuration of the mirroring operations to be performed.

Audit:

There are no auditable events foreseen.

FDP_MRR_EXT.1 User Data Mirroring

Hierarchical to: No other components.

Dependencies: None

FDP_MRR_EXT.1.1 **The TSF shall provide the capability of creating a mirror image of user data as configured by an authorized administrator.**

5.2 EXTENDED ASSURANCE COMPONENTS

This ST does not include extended security assurance requirements.

6 SECURITY REQUIREMENTS

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 underlining 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, summarized in Table 8 - Summary of Security Functional Requirements.

Class	SFR	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_MRR_EXT.1	User data mirroring
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback

Class	SFR	Name
	FIA_UID.1	Timing of identification
	FIA_USB.1	User-subject binding
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners

Table 8 - 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) [*Successful logins, Commands issued*].

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, [*user specified parameters for configuration changes*].

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 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 [*all authorized users*] with the capability to read [*all audit data*] 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.

6.2.1.4 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Volume Access Control SFP*] on [

Subjects: Initiators,

Objects: Targets, LUNs, and

Operations: Access].

6.2.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1 The TSF shall enforce the [*Volume Access Control SFP*] to objects based on the following: [

Initiators: Supplied Initiator ID, Supplied Target ID, Supplied CHAP Parameters (optional), Supplied LUN, Initiator CHAP Parameters;

Targets: Target ID, Front-end Interface;

Virtual Volumes: assigned LUN in Storage Views].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. *An Initiator may access a Target if all of the following conditions are satisfied:*
    a. *The Supplied Target ID matches a configured Target ID for the Front-end Interface on which the request is received;*
    b. *The Initiator ID matches a configured Initiator ID;*

   c. *No Initiator CHAP Parameters are configured for the Initiator ID, or the Supplied CHAP Parameters match the configured Initiator CHAP Parameters.*

2. *An Initiator may access a Virtual Volume if all of the following conditions are satisfied:*
   a. *The Initiator may access the Target being used;*
   b. *A configured Storage View permits access from the Initiator ID to the Target ID and Supplied LUN;*
   c. *The Virtual Volume accessed is the one that corresponds to the Supplied LUN in the configured Storage View].*

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*access is denied if any condition in FDP_ACF.1.2 is not satisfied*].

6.2.2.3 FDP_MRR_EXT.1 User Data Mirroring

Hierarchical to: No other components.

Dependencies: None

FDP_MRR_EXT.1.1 The TSF shall provide the capability of creating a mirror image of user data as configured by an authorized administrator.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Username, Password*].

6.2.3.3 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*viewing the configured login banner*] 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.

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 for the GUI, no output for the CLI*] to the user while the authentication is in progress.

6.2.3.5 FIA_UID.1 Timing of identification

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

FIA_UID.1.1 The TSF shall allow [*viewing the configured login banner*] 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.

6.2.3.6 FIA_USB.1 User-subject binding

Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*Username and Role*].

Application Note: The role is implicitly assigned according to the following rules:

- *For the CLI, the Admin role is implicitly bound to sessions for the Admin user; the User role is implicitly bound to all other sessions.*
- *For the GUI, all users are implicitly assigned the User role. Note that all users have the same privileges in the GUI since user account management operations can only be performed via the CLI.*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*attributes are bound to the user session upon successful login*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*the role does not change during the session*].

6.2.4 Security Management

6.2.4.1 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 [*Volume Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Initiator CHAP Parameters, Target ID, Front-end Interface, assigned LUN in Storage Views*] to [*User and Admin roles*].

6.2.4.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Volume Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*no roles*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.3 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete, [*create*]] the [*list of TSF data in the following table*] to [*the authorised identified roles in the following table*].

Role TSF Data	Admin	User
User Accounts	Query, Modify, Delete, Create	Query
User Passwords	Modify	Modify their own password
User Banner	Modify	Modify
Clusters	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Data Mirroring	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Storage Volumes	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Initiators	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Targets	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Storage Views	Query, Modify, Delete, Create	Query, Modify, Delete, Create

Table 9 – TSF Data Access Permissions

6.2.4.4 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*
- *User banner management*
- *Cluster management*
- *Storage Volume management*
- *Initiator management*
- *Target management*
- *Storage View management*].

6.2.4.5 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 [*User and Admin*].

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

Application Note: All user accounts added via the CLI, as well as the pre-defined "Service" account, are implicitly assigned the User role.

6.2.5 Protection of the TSF (FTP)

6.2.5.1 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.

6.2.6 TOE Access (FTA)

6.2.6.1 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Application Note: This SFR applies to CLI sessions.

6.2.6.2 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 [*15 minutes for CLI users and 10 minutes for GUI users*] 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.

Application Note: This SFR applies to GUI sessions.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [*providing the correct password for the session*].

6.2.6.3 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.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.MIRROR	O.PROTCT	O.TIME
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_SAR.1		X					
FAU_SAR.2		X					
FDP_ACC.1						X	
FDP_ACF.1						X	
FDP_MRR_EXT.1					X		
FIA_ATD.1				X			
FIA_UAU.1	X			X			
FIA_UAU.7	X			X			
FIA_UID.1	X			X			
FIA_USB.1	X						
FMT_MSA.1	X		X				
FMT_MSA.3						X	
FMT_MTD.1	X		X				
FMT_SMF.1			X				
FMT_SMR.1	X		X				
FPT_STM.1		X					X
FTA_SSL.1	X						
FTA_SSL.4	X						
FTA_TAB.1	X						

Table 10 – Mapping of SFRs to Security Objectives

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

Security Objective	Rationale
O.ACCESS	FIA_UID.1 and FIA_UAU.1 permit users to view the login banner prior to completing the I&A process and require users to complete the I&A process before performing other accesses, which ensures only authorized users gain further access and enables each user session to be bound to a role to limit subsequent accesses. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FIA_USB.1 defines the user attributes that are bound to each user session upon completion of the I&A process, enabling access restrictions to be properly enforced for each user session. FMT_MSA.1 and FMT_MTD.1 define the access permissions to TSF data for each role. FMT_SMR.1 ensures the TOE supports multiple roles so that appropriate data access can be provided to different users. FTA_SSL.1 and FTA_SSL.4 require session locking/termination mechanisms to protect against idle sessions being used by unauthorized users. FTA_TAB.1 provides a mechanism to warn unauthorized users against unauthorized access.
O.AUDITS	FAU_GEN.1 and FAU_GEN.2 require audit records to be generated for specific events and define the contents of the records. FAU_SAR.1 and FAU_SAR.2 require the audit records to be available to all authorized users of the TOE, and for access to be restricted for unauthorized users. FPT_STM.1 requires accurate time stamps to be available for the audit records.
O.EADMIN	FMT_MSA.1 and FMT_MTD.1 define the access permissions required for each role for TSF data. FMT_SMF.1 specifies the management functionality required for effective management of the TOE. FMT_SMR.1 defines the roles required to provide effective management capabilities for different categories of users.
O.IDAUTH	FIA_UID.1 and FIA_UAU.1 require users to complete the I&A process, which ensures only authorized users gain access and defines their access permissions prior to completing the I&A process.

Security Objective	Rationale
	FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FIA_ATD.1 specifies the security attributes that are supported for each defined user account.
O.MIRROR	FDP_MRR_EXT.1 ensures that the TOE supports data mirroring configured by administrators.
O.PROTCT	FDP_ACC.1 and FDP_ACF.1 define the access control policy for Virtual Volume access by Initiators. FMT_MSA.3 requires restrictive access to Virtual Volumes by default so that no access is granted until explicitly configured by authorized users.
O.TIME	FPT_STM.1 requires accurate time stamps to be available.

Table 11 – Security Objectives for the TOE

6.4 DEPENDENCY RATIONALE

Table 12 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	Dependencies	Dependency Satisfied / Rationale
FAU_GEN.1	FPT_STM.1	Satisfied
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	FAU_GEN.1	Satisfied
FAU_SAR.2	FAU_SAR.1	Satisfied
FDP_ACC.1	FDP_ACF.1	Satisfied
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Satisfied Satisfied
FDP_MRR_EXT.1	None	n/a
FIA_ATD.1	None	n/a
FIA_UAU.1	FIA_UID.1	Satisfied
FIA_UAU.7	FIA_UAU.1	Satisfied

SFR	Dependencies	Dependency Satisfied / Rationale
FIA_UID.1	None	n/a
FIA_USB.1	FIA_ATD.1	Satisfied
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1 FMT_SMF.1	Satisfied Satisfied Satisfied
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Satisfied Satisfied
FMT_SMF.1	None	n/a
FMT_SMR.1	FIA_UID.1	Satisfied
FPT_STM.1	None	n/a
FTA_SSL.1	FIA_UAU.1	Satisfied
FTA_SSL.4	None	n/a
FTA_TAB.1	None	n/a

Table 12 - 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 13.

Assurance Class	Assurance Components	
	Identifier	Name
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification

Assurance Class	Assurance Components	
	Identifier	**Name**
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	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_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_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 13 - EAL 2+ 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 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

Audit records are generated for the events specified with FAU_GEN.1. The audit trail is maintained on the Management Server as text files under the /var/log/VPlex/cli directory. Events associated with the system are maintained in the messages file, while separate files are maintained for each user session.

Upon successful login, files are created for each session with a naming structure session.log_*username_source_timestamp*. For CLI users, the source is "localhost". For GUI users, the source is the internet address of the browser host. The filename implies the subject identity (username).

For CLI users, all user commands issued are audited. For GUI users, all configuration changes are audited.

The following information is included in all audit records:

- Data and time of the event,
- Type of event,
- Subject identity (implicit via the filename),
- (for configuration actions) the configuration parameters specified by the user.

Any authorized user of the TOE may view the audit records via the CLI using shell commands to display the audit trail files.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FPT_STM.1.

7.1.2 User Data Protection

Initiators are only permitted to access Virtual Volumes via authorized Targets and for which a Storage View has been explicitly configured. Individual Initiators may optionally be required to provide CHAP authentication parameters. Storage Views authorize access by configured Initiators and Targets, and map LUNs specified by the Initiators to Virtual Volumes.

Data mirroring between clusters is performed as configured by administrators.

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1, FDP_MRR_EXT.1.

7.1.3 Identification and Authentication

When GUI or CLI users initiate sessions, they must complete the login process. Prior to successful completion, the only controlled data or function they can access is viewing the configured banner. CLI and GUI users always must present a valid username and password.

During collection of the password, only asterisks are echoed for each character supplied to the GUI and no characters are echoed by the CLI.

Upon successful login, the user's username is bound to the session. For CLI users, the role is implied by the user account name: Admin for the Admin user account, and User for all other users, including "Service". For GUI users, all sessions are assigned the User role. If a user account configuration command is entered via the CLI by Admin, the user must supply the password for the Admin account to revalidate their access to this functionality.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, and FIA_USB.1.

7.1.4 Security Management

The GUI and CLI interfaces provide functionality for authorized users to manage the TOE. Each user session is bound to a role upon login, and that role determines access permissions as specified in FMT_MTD.1.

When Virtual Volumes are created, they are not included in any Storage Views that grant user access. Users with the Admin and Service roles have the ability to configure Storage Views to expose the Virtual Volumes to Initiators.

Only the Admin user may perform user account management functions, and this capability is only supported via the CLI. For each user account management command issued, the user must supply the Admin password. If successful, the command is executed; otherwise the command is rejected. User account configuration commands from User sessions are always rejected.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

7.1.5 TOE Access

Once a user has logged in, the session may be terminated by the user. The TOE automatically locks GUI sessions if they remain idle for more than the allowed inactivity timer value.

The configured banner is displayed to users during CLI login.

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

8 TERMINOLOGY AND ACRONYMS

8.1 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
API	Application Program Interface
CC	Common Criteria
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
ESRS	EMC Secure Remote Support
FC	Fibre Channel
GB	GigaByte
Gb/s	Gigabit/second
GUI	Graphical User Interface
HTTPS	HyperText Transfer Protocol Secure
ID	IDentifier
IT	Information Technology
I&A	Identification & Authentication
I/O	Input/Output
IOM	I/O Module
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
OE	Operational Environment
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
REST	REpresentational State Transfer

Acronym	Definition
RTT	Round Trip Time
SAN	Storage Area Network
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure SHell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WAN	Wide Area Network

Table 14 - Acronyms