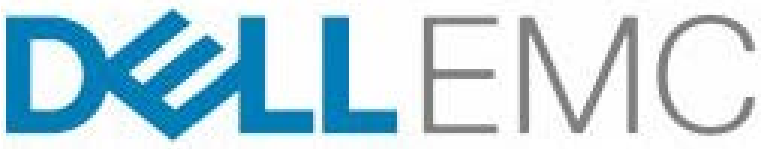
Dell EMC™ VxFlex 3.0.1

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2115-000-D102
Version: 1.1
8 August 2020



Dell EMC
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

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 Target of Evaluation (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 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 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™ VxFlex 3.0.1 Security Target
ST Version:	1.1
ST Date:	8 August 2020

1.3 TOE REFERENCE

TOE Identification: Dell EMC™ VxFlex 3.0.1.208 with VxFlex Ready Node 14G Hardware

TOE Developer: Dell EMC

TOE Type: Storage Area Network component (Other Devices and Systems)

1.4 TOE OVERVIEW

The VxFlex operating system (OS) is the VxFlex software component and provides the ability to use existing servers' local disks and Local Area Network (LAN) resources to create a virtual Storage Area Network (SAN). VxFlex OS utilizes the existing local storage devices and turns them into shared block storage.

The lightweight VxFlex OS software components are installed on the application servers and communicate via a standard LAN to handle the application input/output (I/O) requests sent to VxFlex OS block volumes. This decentralized block I/O flow, combined with a distributed, sliced volume layout, provides a parallel I/O system that can scale up to thousands of nodes.

VxFlex OS enables administrators to securely manage servers and capacity. The software immediately responds to the changes, rebalancing the storage distribution and achieving a layout that optimally suits the new configuration.

Access to security management is controlled such that system administrators must be authenticated before being granted access. Restrictions on user sessions prevent unauthorized access to administrative functions. Additionally, VxFlex maintains audit logs that record access events and changes to the system configuration. Communications between the TOE and remote administrators are protected using TLS.

VxFlex Ready Node is the combination of VxFlex OS software-defined block storage and Dell PowerEdge servers, optimized to run VxFlex OS. The solution is managed by the VxFlex OS Graphical User Interface (GUI) and VxFlex OS Command Line Interface (CLI) which enable a simple or customized deployment process from bare metal, no IP state, to a fully-configured system with IP address assignment, VxFlex OS deployment and configuration, and vCenter configuration.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following networking components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Network Switch	N/A	10/25/100 GbE network switch
Management Workstation	Windows 10 running the Java Client application and JRE 8.0.2210.11	General Purpose Computing Hardware

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The VxFlex System is made up of hardware and software.

The VxFlex Ready Node system includes dedicated server nodes. The system refers to the following hardware components:

- **Nodes -** Nodes are the basic computer unit used to install and run the operating system and VxFlex OS. They can be the same servers used for the applications (server convergence), or in a 2-layer architecture.
- **Storage Media** - The storage media is supplied as part of the hardware.

The VxFlex OS virtual SAN consists of the following software components:

- **Meta Data Manager (MDM)** - MDM configures and monitors VxFlex OS. In the evaluated configuration, the MDM is configured in redundant cluster mode, with three members on three servers.
- **Storage Data Server (SDS)** - SDS manages the capacity of a single server and acts as a back-end for data access. The SDS is installed on all servers contributing storage devices to VxFlex OS. These devices are accessed through the SDS.
- **Storage Data Client (SDC)** - SDC is a lightweight device driver that exposes VxFlex OS volumes as block devices to the application that resides on the same server on which the SDC is installed.
- **VxFlex OS GUI** – The VxFlex OS GUI is a management solution that runs on the MDM. It's accessed from a Java-based client application on the remote workstation.
- **VxFlex OS CLI**- The VxFlex OS CLI is a command line application that runs on the MDM. Administrators connect to the VxFlex OS CLI from the remote management workstation via terminal application (PuTTY for example).

In the evaluated configuration, the TOE consists of three Ready Node Appliances running VMware. Table 2 identifies the TOE components and Figure 1 illustrates the TOE in its evaluated configuration.

TOE Component	Description
Ready Node Servers (R640, R740xd, or R840)	Three Ready Node Servers each running ESXi 6.7.0-20190802001, vCenter Server Appliance (vCSA) v6.7u3b and VxFlex OS, including: • MDM • SDS • SDC • VxFlex OS GUI • VxFlex OS CLI

Table 2 – TOE Components

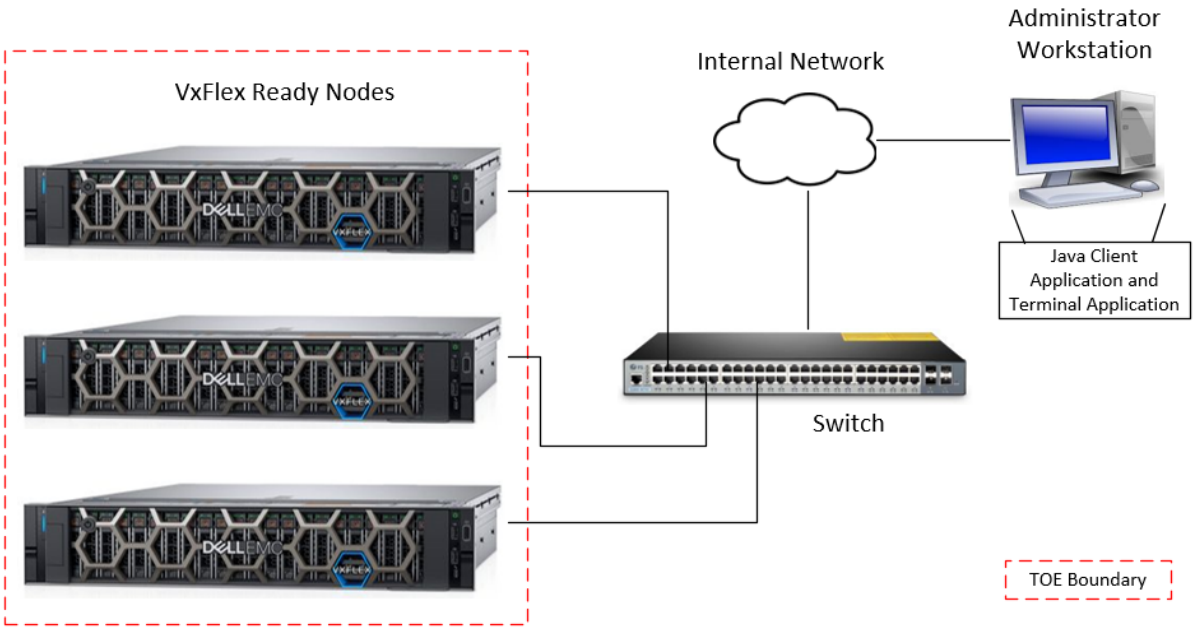


Figure 1 – VxFlex Deployment Diagram

1.5.1.1 TOE Delivery

The VxFlex Ready Nodes are shipped directly to the customer. The customer then installs the VxFlex OS GUI and discovers the node. Once the node is discovered, the management software facilitates the installation and configuration of the VxFlex OS. All software components, including the VxFlex OS GUI, are available for download to registered customers at https://support.emc.com/downloads/.

The complete VxFlex software package is presented to customers as a zip file:

- *VxFlex_OS_3.0.1_208_Complete_Software.zip*

1.5.1.2 TOE Guidance

All guidance documentation is provided in Portable Document Format (PDF) and is available for download to registered users at: https://support.emc.com/products.

The TOE includes the following guidance documentation:

- Dell EMC VxFlex OS, Version 3.x, CLI Reference Guide, March 2019
  - *CLI Reference Guide.pdf*
- Dell EMC VxFlex OS, Version 3.x, Monitor, March 2019
  - *Monitor VxFlex OS.pdf*
- Dell EMC VxFlex OS, Version 3.x, Deploy Dell EMC VxFlex OS, April 2019
  - *Deploy VxFlex OS v3.x.pdf*
- Dell EMC VxFlex OS, Version 3.x, Security Configuration Guide, March 2019
  - *Security Configuration Guide.pdf*
- Dell EMC VxFlex Ready Node 14th generation servers, Server Installation Guide, April 2019
  - *VxFlex Ready Node Server Installation Guide.pdf*
- Dell EMC VxFlex Ready Node R640/R740xd, Operating System Installation and Configuration Guide – ESXI Servers, June 2019
  - *VxFlex Ready Node v3.x Operating System Installation & Configuration Guide – R640 R740xd – ESXi.pdf*
- Dell EMC VxFlex Ready Node R840, Operating System Installation and Configuration Guide, April 2019
  - *VxFlex Ready Node v3.x Operating System Installation and Configuration Guide – R840.pdf*

The following Common Criteria Guidance Supplement is also available to customers, in PDF format, upon request:

- Dell EMC™ VxFlex 3.0.1 Common Criteria Guidance Supplement, Version 1.0
  - *VxFlex_EAL2_AGD_1.0.pdf*

1.5.2 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.
Cryptographic Support	Cryptographic functionality is provided to allow the communications links between the TOE and its remote administrators to be protected.
User Data Protection	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 TOE access.
Security Management	The TOE provides management capabilities via GUI and CLI applications. Management functions allow the administrators to configure users and roles, user sessions, and storage volumes.
Protection of the TSF	The TOE provides reliable timestamps used for the generation of audit events.
TOE Access	A banner is presented on user login.
Trusted Path/Channel	The communications links between the TOE and its remote administrators are protected using TLSv1.1 and TLSv1.2.

Table 3 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- The TOE supports REST clients; however no REST clients are implemented in the evaluated configuration.
- The TOE supports a vCenter Plugin GUI required for installation and setup. Once setup is complete, this interface is not used in the evaluated configuration. Access to this interface requires vCenter admin credentials.
- The following deployment options are supported but not implemented in the evaluated configuration:

- SDS, SDC, and MDM instances on physical servers running CentOS, Red Hat, SUSE, and Windows.
- SDS, SDC, and MDM instances on Hyper-V, XenServer, and Redhat KVM hypervisors.
- Automated Management Service (AMS)

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-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

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

2.3 PACKAGE CLAIM

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

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

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.PRIVILEGE	An unauthorized user may gain access to the TOE and change the configuration or exploit system privileges to gain access to TOE security functions and data.
T.SENSDATA	An unauthorized user may be able to view sensitive data passed between the TOE and its administrators, and exploit this data to gain unauthorized privileges on the TOE.
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

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 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.PROTECT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

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.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.PROTECT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

Table 6 – 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.ADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.AUDIT	The TOE must record audit records for security relevant events.
O.ENCRYPT	The TOE must make use of FIPS-validated cryptographic functions for the protection of sensitive data.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PATH	The TOE must ensure the confidentiality of data passed between itself and remote administrators.
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.TIME	The TOE must provide reliable timestamps.

Table 7 – 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.CREDENTIALS	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.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

	T.PRIVILEGE	T.SENSDATA	T.UNDETECT	P.PROTECT	A.MANAGE	A.NOEVIL	A.PROTECT
O.ACCESS	X						
O.ADMIN	X						
O.AUDIT			X				
O.ENCRYPT		X					
O.IDENTAUTH	X						
O.PATH		X					
O.PROTECT	X						
O.TIME			X				
OE.CREDENTIALS	X					X	

	T.PRIVILEGE	T.SENSDATA	T.UNDETECT	P.PROTECT	A.MANAGE	A.NOEVIL	A.PROTECT
OE.INSTAL	X					X	
OE.PERSON	X				X		
OE.PHYSICAL				X		X	X

Table 9 – Mapping Between Objectives, Threats, OSPs, 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.PRIVILEGE	An unauthorized user may gain access to the TOE and change the configuration or 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.ADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
	OE.CREDENTIALS	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:	O.IDENTAUTH provides for authentication of users prior to any TOE function accesses. O.ACCESS builds upon O.IDENTAUTH by only permitting authorized users to access TOE functions. O.ADMIN ensures the TOE has all the necessary administrator functions to manage the product. O.PROTECT addresses this threat by providing TOE self-protection against unauthorized modifications and access. OE.CREDENTIALS requires administrators to protect all authentication data. OE.PERSON ensures competent administrators will manage the TOE. OE.INSTAL builds upon OE.PERSON by ensuring that authorized administrators will configure the TOE properly.	

Threat: **T.SENSDATA**	An unauthorized user may be able to view sensitive data passed between the TOE and its administrators, and exploit this data to gain unauthorized privileges on the TOE.	
Objectives:	O.ENCRYPT	The TOE must make use of FIPS-validated cryptographic functions for the protection of sensitive data.
	O.PATH	The TOE must ensure the confidentiality of data passed between itself and remote administrators.
Rationale:	O.ENCRYPT mitigates this threat by using FIPS-validated cryptographic functions for the protection of sensitive data. O.PATH mitigates this threat by using a trusted path for remote administration of the TOE.	

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 security relevant events.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.AUDIT mitigates this threat by ensuring that auditable events are	

	recorded for user activity. O.TIME mitigates this threat by ensuring that accurate time information is included for all audit records.

4.3.2 Security Objectives Rationale Related to OSPs

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.PROTECT**	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this policy by ensuring the TOE is protected 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:	OE.PERSON ensures all authorized administrators are qualified and trained to manage the TOE.	

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.CREDENTIALS	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.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.CREDENTIALS supports this assumption by requiring protection of all authentication data. OE.INSTAL ensures that the TOE is properly installed and operated. OE.PHYSICAL provides for physical protection of the TOE by authorized administrators.	

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

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 (EAL) 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 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 10.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
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	Subset access control
	FDP_ACF.1	Security attribute based access control

Class	Identifier	Name
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	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	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 10 – 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) [*changes to TSF data, login attempt results, logouts*].

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_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.

6.2.2 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 [*Deterministic Random Bit Generation*] and specified cryptographic key sizes [*128, 256 bits*] that meet the following: [*NIST Special Publication 800-90A*].

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: [*FIPS 140-2*].

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 [*the cryptographic key sizes specified in Table 11*] that meet the following: [*standards listed in Table 11*].

Operation	Algorithm	Key Size (bits)	Standard
Encryption and Decryption of remote administrator sessions	AES (Advanced Encryption Standard)	128, 256	FIPS PUB 197

Table 11 – Cryptographic Operations

6.2.3 User Data Protection (FDP)

6.2.3.1 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 [*Role-Based Access Control SFP*] on [

- *Subjects: administrative users*
- *Objects: TSF data*
- *Operations: configure and manage users, frontend operations, and backend operations*].

6.2.3.2 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 [*Role-Based Access Control SFP*] to objects based on the following: [

- *Subjects: Administrative users*
- *Subject Attributes: role*
- *Objects: TSF data*
- *Object attributes: none*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the Administrative user is able to access the TSF data and perform the operations associated with an administrative function if the role allows access to the administrative function*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

- *users assigned the Administrator role have full access to all TSF data*
- *users assigned the Configure role can configure frontend and backend operations*
- *users assigned the Monitor role have query access only*].

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

6.2.4 Identification and Authentication (FIA)

6.2.4.1 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, Role*].

6.2.4.2 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 [*the following password complexity rules:*

- *be between 6 and 31 characters in length*
- *must include at least 3 groups out of [a-z], [A-Z], [0-9], special characters (!, @, #, $)*].

6.2.4.3 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.

6.2.4.4 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 [*obscured feedback for the GUI and no characters for the CLI*] to the user while the authentication is in progress.

6.2.4.5 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 [*Role-Based Access Control SFP*] to restrict the ability to [query, modify, delete, [*create*]] the security attributes [*user roles, storage pool attributes, storage volume attributes*] to [*users assigned the authorized role*].

6.2.5.2 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 [*Role-Based 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 [*authorised administrative users*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 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*
- *Backend operations (SDS and storage pool management)*
- *Frontend operations (SDC and volume management)*
- *Login banner configuration*].

6.2.5.4 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 [*Monitor, Configure, Administrator*].

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_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.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a**n** [*administrator configured time interval of user inactivity*].

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.

6.2.7.3 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.

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 [[*remote administration*]].

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

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
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample

Assurance Class	Assurance Components	
	Identifier	**Name**
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 12 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

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

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENTAUTH	O.PATH	O.PROTECT	O.TIME
FAU_GEN.1			X					
FAU_GEN.2			X					
FCS_CKM.1				X				
FCS_CKM.4				X				
FCS_COP.1				X				
FDP_ACC.1							X	
FDP_ACF.1							X	
FIA_ATD.1					X			
FIA_SOS.1	X							
FIA_UAU.2	X				X			
FIA_UAU.7	X				X			
FIA_UID.2	X				X			
FMT_MSA.1	X	X					X	
FMT_MSA.3							X	

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENTAUTH	O.PATH	O.PROTECT	O.TIME
FMT_SMF.1		X					X	
FMT_SMR.1	X	X					X	
FPT_STM.1			X					X
FTA_SSL.3	X							
FTA_SSL.4	X							
FTA_TAB.1	X							
FTP_TRP.1						X		

Table 13 – Mapping of SFRs to Security Objectives

6.4.2 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 allow authorized users to access only appropriate TOE functions and data.	
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
	FMT_MSA.1	Management of security attributes
	FMT_SMR.1	Security roles
	FMT_SSL.3	TSF-initiated termination
	FMT_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
Rationale:	FIA_SOS.1 supports this objective by requiring passwords to be satisfied by complexity rules.	

	FIA_UID.2 and FIA_UAU.2 require users to complete the I&A process, which ensures only authorized users gain access to the TOE and TSF. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FMT_MSA.1 defines 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.3 and FTA_SSL.4 ensure that interactive sessions can be terminated by the user or by the TOE to protect against idle sessions being used by unauthorized users. FTA_TAB.1 provides a mechanism to warn unauthorized users against unauthorized access.

Objective: **O.ADMIN**	The TOE must include a set of functions that allow effective management of its functions and data.	
Security Functional Requirements:	FMT_MSA.1	Management of security attributes
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale:	FMT_MSA.1 defines the permissions required to access 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.	

Objective: **O.AUDIT**	The TOE must record audit records for security relevant events.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 and FAU_GEN.2 require audit records to be generated for specific events and define the contents of the records. FPT_STM.1 ensures that reliable timestamps are used for all audit records.	

Objective: **O.ENCRYPT**	The TOE must make use of FIPS-validated cryptographic functions for the protection of sensitive data.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Rationale:	FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 meet this objective by providing FIPS-validated cryptographic functionality required to protect sensitive data.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Rationale:	FIA_ATD.1 specifies the security attributes that are supported for each defined user account. FIA_UID.2 and FIA_UAU.2 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. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE.	

Objective: **O.PATH**	The TOE must ensure the confidentiality of data passed between itself and remote administrators.	
Security Functional Requirements:	FTP_TRP.1	Trusted Path
Rationale:	FTP_TRP.1 meets this objective by specifying the use of cryptography for data passed between the TOE and remote administrators.	

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

O.PROTECT		
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale:	FDP_ACC.1 and FDP_ACF.1 define the access control policy for users. FMT_MSA.1 ensures that access to TOE administrative functions is based on role. FMT_MSA.3 requires restrictive default values for the attributes that provide administrators with privileges. FMT_SMF.1 defines the management functions accessible by authorized administrators. FMT_SMR.1 defines the roles that are used to restrict access to the administrative functions.	

O.TIME	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 meets this objective by ensuring that the TOE provides reliable timestamps.	

6.4.3 Dependency Rationale

Table 14 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_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_ATD.1	None	N/A	
FIA_SOS.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	None	N/A	
FTA_SSL.3	None	N/A	
FTA_SSL.4	None	N/A	
FTA_TAB.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 14 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

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.

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

Audit records are generated for the events specified with FAU_GEN.1. Startup and shutdown of the audit function is equivalent to startup and shutdown of the MDM. The following information is included in all audit records:

- Data and time of the event,
- Type of event,
- Subject identity (if applicable),
- Outcome (success or failure) of the event (if it is not apparent from the Event type), and
- Associated TOE server component.

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

7.2 CRYPTOGRAPHIC SUPPORT

Federal Information Processing Standard (FIPS) mode must be enabled in the evaluated configuration. When in this mode, VxFlex uses the OpenSSL FIPS Object Module version 2.0.8 Cryptographic Module Validation Program (CMVP) certificate # 1747 to provide cryptographic support. Cryptography is used in support of Transport Layer Security (TLS) v1.2 for communications with remote administrators. TLS v1.2 using TLS_RSA_WITH_AES_256_CBC_SHA are enabled by default in the evaluated configuration.

The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.

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

7.3 USER DATA PROTECTION

The TOE enforces the Role-Based Access Control SFP which dictates a user's ability to manage the TSF based on their assigned role. Users assigned the Administrator role have full access all TOE functions and data. Users assigned the Configure role only have access to frontend and backend configuration parameters. Users assigned the Monitor role have query access only.

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

7.4 IDENTIFICATION AND AUTHENTICATION

When users initiate sessions via the GUI or CLI, they must complete the login process and authenticate with the TOE. Prior to successful authentication, no TSF data or function access is permitted. Upon successful login, the user's

username and role are bound to the session. These attributes do not change during the session.

During collection of the password for the login process, obscured feedback is echoed for the GUI and no characters are echoed for the CLI. Passwords but must adhere to the complexity rules as outlined in the FIA_SOS.1.

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

7.5 SECURITY MANAGEMENT

The GUI application provides functionality for authorized users to manage frontend and backend operations. Frontend operations include management of the SDCs and storage volumes. Backend operations include management of the SDSs and storage pools. The CLI application provides functionality for authorized administrators to manage users, as well as all frontend and backend operations. The login banner can only be configured using the CLI and is restricted to users assigned the Administrator role.

Each user session is bound to a role upon login, and that role determines access permissions. In the evaluated configuration, the TOE supports the Administrator, Configure, and Monitor roles. Users with the Administrator role have full access to all management functions. Users with the Configure role can manage SDCs, SDSs, and storage volumes. Users assigned the Monitor role have view access only. Access to the TOE management functions is considered restrictive in that users must be assigned a role. Only authorized administrators assigned the Administrator role have the ability to create and modify users.

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

7.6 PROTECTION OF THE TSF

Timestamp information used for the generation of audit records is provided by the VxFlex Ready Node hardware.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.7 TOE ACCESS

Users are able to terminate their own session with the TOE at any time. For CLI sessions only, a user's session may be terminated by the TOE after an administrator configured amount of inactivity time.

When the login banner is set up, it appears during the system login process before the login credential prompts. The login banner displays differently in the VxFlex OS GUI and in the CLI interfaces:

- GUI – When logging in, the login banner is displayed, and must be approved.
- CLI – When logging in, the user is prompted to press any key, after which the banner is displayed. To continue, the banner must be approved.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1.

7.8 TRUSTED PATH / CHANNELS

When the VxFlex OS GUI is used, the connection between the TOE and the remote administrator is protected from modification and disclosure using TLS. This connection is logically distinct from other communication channels. The VxFlex end point is identified by the user specifying the IP address of the primary MDM on the Ready node Server. User authentication is required prior to being granted access to the security management functions.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terms are used in this ST:

Term	Description
Authenticated	The term 'authenticated' refers to a user that has provided valid credentials (username and password) when logging into the TOE.
Authorized	The term 'authorized' refers to an authenticated user who has been assigned permissions.
Backend	The term 'backend' refers to objects in the system which includes SDSs and storage pools.
Frontend	The term 'frontend' refers to objects in the system which includes volumes, SDCs, and snapshots.

Table 15 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
AMS	Automated Management Service
CC	Common Criteria
CLI	Command Line Interface
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GbE	Gigabyte Ethernet
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	Hashed Message Authentication Code

Acronym	Definition
IT	Information Technology
I/O	Input/Output
LAN	Local Area Network
MDM	Meta Data Manager
NIST	National Institute of Standards and Technology
OS	Operating System
OSP	Organizational Security Policy
PCIe	Peripheral Component Interconnect Express
PDF	Portable Document Format
PP	Protection Profile
PUB	Publication
REST	Representational State Transfer
SAN	Storage Area Network
SDC	ScaleIO Data Client
SDS	ScaleIO Data Server
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSD	Solid State Drive
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
vCSA	vCenter Server Appliance

Table 16 – Acronyms