EMC ScaleIO® v1.32.3 Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1903-000-D102
Version: 0.6
8 February 2016

Prepared For:

EMC Corporation
176 South Street
Hopkinton, MA, USA
01748

Prepared by:

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

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 ScaleIO® v1.32.3 Security Target
ST Version:	0.6
ST Date:	8 February 2016

1.3 TOE REFERENCE

TOE Identification: EMC ScaleIO® v1.32.3

TOE Developer: EMC Corporation

TOE Type: Other Devices and Systems

Build numbers vary by TOE component:

- ScaleIO Virtual Machine (SDS and MDM) – 455
- SDC – 449
- vSphere Plugin – 455
- Windows CLI and GUI applications - 455

1.4 TOE OVERVIEW

EMC ScaleIO® is a software-only server-based Storage Area Network (SAN) that converges storage and compute resources to form a single-layer, enterprise-grade storage product. ScaleIO storage is elastic and delivers linearly scalable performance. Its scale-out server SAN architecture can grow from a few to thousands of servers.

ScaleIO uses existing servers' local disks and Local Area Network (LAN) to create a virtual SAN that has all the benefits of external storage—but at a fraction of cost and complexity. ScaleIO utilizes the existing local internal storage and turns it into internal shared block storage. For many workloads, ScaleIO storage is comparable to, or better than external shared block storage.

The lightweight ScaleIO software components are installed on the application servers (the ScaleIO Data Client (SDC) TOE component) and communicate via a standard LAN to handle the application I/O requests sent to ScaleIO block volumes (handled by the ScaleIO Data Server (SDS) TOE component). An extremely efficient decentralized block I/O flow, combined with a distributed, sliced volume layout, results in a massively parallel I/O system that can scale up to thousands of nodes.

Dynamic and elastic, ScaleIO enables administrators to add or remove nodes and capacity on-the-fly. The overall TOE is managed via the Meta Data Manager (MDM) TOE component. When a volume is mapped to an SDC instance (host), the MDM forwards the information to the SDC so that the volume can be made available to the host. The SDC and SDS then communicate directly to perform the block I/O operations.

Because ScaleIO is hardware agnostic, the software works efficiently with various types of disks, including: magnetic (HDD) and solid-state (SSD) disks, flash PCI Express (PCIe) cards, networks, and hosts.

ScaleIO can easily be installed in an existing infrastructure as well as in green field configurations.

Control and monitoring of ScaleIO can be performed via Command Line Interface (CLI) or Graphical User Interface (GUI) applications. The GUI application can be installed on a Windows or Linux workstation. The CLI application is installed on each MDM instance, and optionally may be installed on other systems. A VMware plug-in is also available for use in VMware environments; the plug-in provides ScaleIO management functionality via vCenter.

Only hosts whose SDC instances have been explicitly mapped to a volume may access a volume within ScaleIO. The ScaleIO management interfaces may be used to configure the volume mappings.

The TOE generates audit records for configuration actions performed via the management interfaces.

1.4.1 ScaleIO System

A ScaleIO system utilizes hardware and software components provided by the operational environment.

In general, hardware can be the existing application servers used by the datacenter, or a new set of nodes (if, for example, you want to dedicate all nodes solely for the purpose of running the ScaleIO storage system).

Nodes or servers are the basic computer unit used to install and run the ScaleIO system. They can be the same servers used for the applications (server convergence), or a dedicated cluster. ScaleIO is hardware-agnostic.

The primary software components of a ScaleIO system include the MDM, SDS, and SDC. These software components are installed on the server nodes and give rise to a virtual SAN layer exposed to the applications residing on the servers. The ScaleIO architecture is illustrated in the following diagram.

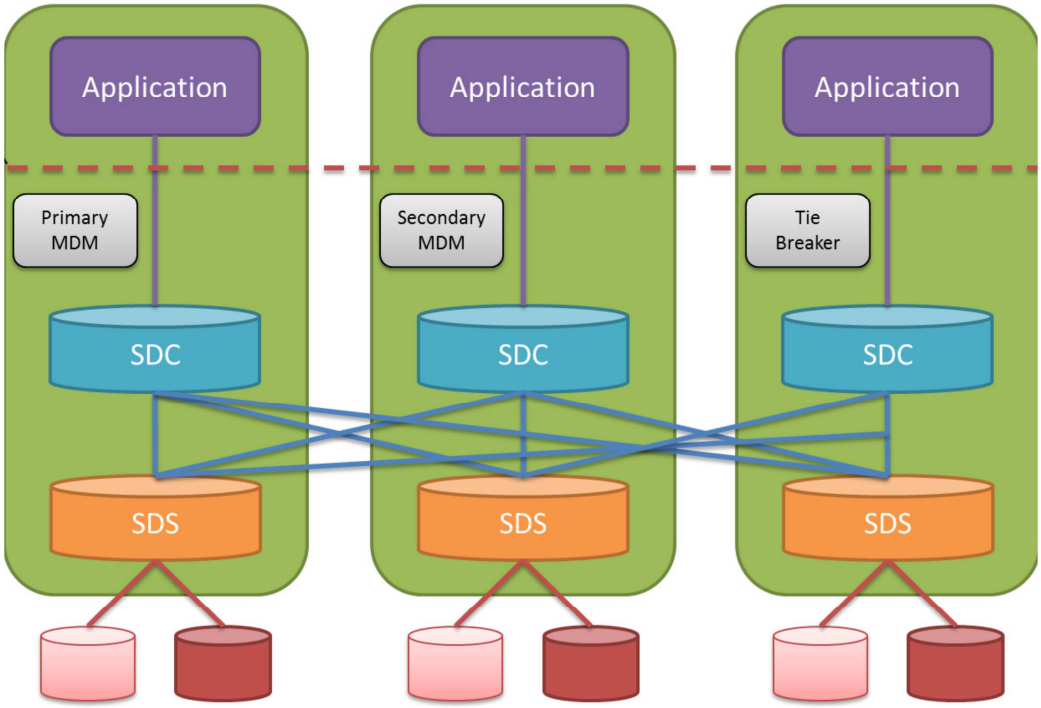

Figure 1 – ScaleIO Architecture

The MDM manages the entire system. It aggregates the entire storage exposed to it by all the SDSs to generate a virtual layer - virtual SAN storage. Volumes can now be defined over the Storage Pools and can be exposed to the applications as a local storage device using the SDCs. The MDM can be configured in redundant Cluster Mode, with three members on three servers, or in Single Mode on a single server.

The 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 the ScaleIO system. These devices are then allocated into volumes and accessed through the SDS.

The SDC is a lightweight device driver that exposes ScaleIO volumes as block devices to the application residing on the same server on which the SDC is installed. When a volume is mapped to an SDC on the MDM, the SDC is informed so that it can display that volume as being available on the server. Subsequently the SDC exchanges data directly with that SDS.

The MDM, SDS and SDC components may be distributed as desired across platforms. A given host may hold an MDM, just an SDC, just an SDS, or any combination of them.

In a VMware environment, the MDM and SDS are installed on dedicated ScaleIO Virtual Machines (SVMs) with SUSE 11 as the guest operating system. The SDC is installed inside the ESX hypervisor. The SDS adds the ESX physical devices to the SVM to be used for storage, thus enabling the creation of volumes. The volumes are then mapped to the SDC, which exposes them to the ESX hypervisor.

The TOE includes management applications as well for users to interact with the MDM. The ScaleIO GUI application may be installed on Windows 7 workstations. The ScaleIO CLI application is installed with all MDM instances and optionally may be installed on Windows 7 workstations. For VMware environments, a vCenter plug-in is available that enables access to the MDM directly from vCenter.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

A ScaleIO instance includes the following components:

- Three instances of MDM instantiated within VMware SUSE-based virtual machines (SVM)
- Three or more instances of SDS instantiated within VMware SUSE-based virtual machines (SVM)
- One or more instances of SDC instantiated within VMware ESXi 5.5 instances
- One or more instances of the CLI application on Windows 7 systems
- One or more instances of the GUI application on Windows 7 systems
- One instance of the VMware vCenter 5.5 plug-in.

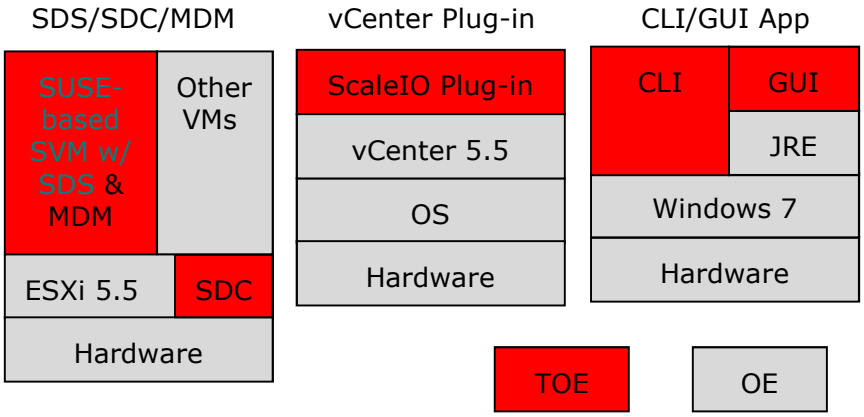

Figure 2 - EMC ScaleIO® v1.32.3 Diagram

1.5.2 TOE Environment

The following minimum requirements for systems hosting SDS/SDC/MDM components.

Component	Minimum Requirement
Processor	Intel or AMD x86 64-bit (recommended)

Component	Minimum Requirement
Physical Memory	500 MB RAM for the Meta Data Manager (MDM) 500 MB RAM for each ScaleIO Data Server (SDS) 50 MB RAM for each ScaleIO Data Client (SDC)
Disk Space	10 GB for VMware ESXi instances
Operating System/ Hypervisor	SDS/MDM SVM:SUSE 11 VMware: 5.5

Table 1 – ScaleIO SDS/SDC/MDM Minimum Requirements

The ScaleIO GUI and/or CLI applications may be installed on Windows 7 workstations. Java 1.7 or higher is requirement for the GUI application.

The ScaleIO vCenter plug-in is supported on vCenter 5.5.

Information is passed over the LAN between TOE components to perform their functions. User data is also passed over the LAN, specifically the SDS and SDC instances. It is the responsibility of the Operational Environment to protect this traffic from unauthorized disclosure or modification.

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- *EMC ScaleIO V1.32.1 User Guide (July 2015)*
- *ScaleIO V1.32 Security Configuration Guide (302-001-368 Rev 03)*
- *EMC ScaleIO V1.32.1 Installation Guide (July 2015)*
- *How to Obtain Your ScaleIO License Key (November 2013)*
- *EMC ScaleIO V1.32 Common Criteria Supplement (December 2015)*

1.5.4 Logical Scope

Functional Classes	Description
Security Audit	Audit entries are generated for security related events.
User Data Protection	The TOE mediates all block data requests from servers (SDC instances) to prevent unauthorized access to volumes accessed via SDS instances. By default access to volumes is restricted. Authorized administrators may configure allowed associations between SDC instances and volumes to allow access to the specified volumes.

Functional Classes	Description
Identification and Authentication	Users must identify and authenticate prior to TOE access.
Security Management	The TOE provides management capabilities via GUI and CLI applications; in VMware environments, a vCenter plug-in is also supported. Management functions allow the administrators to manage users, user sessions, SDC and SDS instances, and volumes.
TOE Access	User sessions may be terminated by users, or by the TOE for CLI sessions if they are inactive longer than the configured inactivity limit.

Table 2 - Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- REST API – this optional API provides an additional monitoring interface to the ScaleIO system via an extra system component, the ScaleIO REST Gateway.
- OpenStack Cinder - the optional Cinder driver provides a block storage solution interfacing between OpenStack and ScaleIO.
- Quality of Service (QoS) - limits the amount of bandwidth and storage that any given SDC can use.
- Obfuscation – data on ScaleIO volumes can be obfuscated for higher data protection.
- Failover – ScaleIO supports failover at multiple architectural levels.
- In addition to the evaluated configuration, the following deployment options are supported:
    - SDS, SDC, and MDM instances on physical servers running CentOS, Red Hat, SUSE, and Windows.
    - SDS, SDC, and MDM instances on VMware 5.1 and 6.0, Hyper-V, XenServer, and RedHat KVM hypervisors.
    - ScaleIO CLI and GUI applications on Windows and Linux workstations.

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 3 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 may attempt to access user data (volumes) that it is not authorized to access.

Table 3 - 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 4 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.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

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

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.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.
A.LANNETWORK	The TOE components will be interconnected by a segregated LAN that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

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

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

Security Objective	Description
O.ACCESS	The TOE must 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.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

Security Objective	Description
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.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.LANNETWORK	The operational environment will provide a segregated LAN that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
OE.TIME	The operational environment will maintain reliable timestamps.

Table 7 – 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.PROTECT	A.MANAGE	A.NOEVIL	A.PROTECT	A.LANNETWORK
O.ACCESS	X	X	X		X					
O.AUDITS				X						
O.EADMIN	X		X		X					
O.IDAUTH	X	X		X	X					
O.PROTCT		X			X					
OE.CREDEN					X			X		

	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.MANAGE	P.PROTECT	A.MANAGE	A.NOEVIL	A.PROTECT	A.LANNETWORK
OE.INSTAL	X				X			X		
OE.PERSON					X		X			
OE.PHYCAL						X		X	X	
OE.LANNETWORK										X
OE.TIME				X						

Table 8 - 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 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.
	OE.TIME	The operational environment 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 OE.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.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.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.	

Assumption: A.LANNETWORK	The TOE components will be interconnected by a segregated LAN that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.	
Objectives:	OE.LANNETWORK	The operational environment will provide a segregated LAN that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
Rationale:	The OE.LANNETWORK objective ensures that the intra-TOE traffic will be protected by a segregated LAN.	

5 EXTENDED COMPONENTS DEFINITION

This ST does not include extended security 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 9 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification

Class	Identifier	Name
	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
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination

Table 9 - Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*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 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 User Data Protection

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: Servers with SDC Instances,

Objects: Volumes with SDS Instances, 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: [

Servers with SDC Instances: SDC ID,

Volumes with SDS Instances: Mapped Servers].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*a Server may access a Volume if the Server's associated SDC instance is included in the list of Mapped SDCs for the Volume*].

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 the Volume is not mapped to the Server's associated SDC instance*].

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, and Role*].

6.2.3.2 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 complexity rules:*

- *Between 6 and 31 characters*
- *Include at least 3 groups out of [a-z], [A-Z], [0-9], special characters (!@#$ …)*

- *Different from the current 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 [*no TSF data or function access*] 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.

6.2.3.4 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 [*dots or no characters*] 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 [*no TSF data or function access*] 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*].

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: [*attributes do not change during a user 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 [*Mapped Servers, Server IDs*] to [*Monitor (query only), Configure, and Administrator*].

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	Administrator	Configure	Monitor
User Accounts	Query, Modify, Delete, Create	Query	None
User Session Parameters	Query, Modify	Query, Modify	Query
SDS Instances	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query
SDC Instances	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query
Volume Configuration	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query

Table 10 – 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 session management*
- *SDS management*
- *SDC management*
- *Volume 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 [*Monitor, Configure, and Administrator*].

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

6.2.5 TOE Access (FTA)

6.2.5.1 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 [*time interval of user inactivity configured by a user with the Configure or Administrator role*].

Application Note: This functionality applies to CLI sessions only.

6.2.5.2 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.

6.3 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.PROTCT
FAU_GEN.1		X			
FAU_GEN.2		X			
FDP_ACC.1					X
FDP_ACF.1					X
FIA_ATD.1				X	
FIA_SOS.1	X		X		
FIA_UAU.1	X			X	

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.PROTCT
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		
FTA_SSL.3	X				
FTA_SSL.4	X				

Table 11 – 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_SOS.1 supports this objective by requiring passwords to be effective by satisfying complexity rules. FIA_UID.1 and FIA_UAU.1 require users to complete the I&A process, which ensures only authorized users gain access and enables each user session to be bound to a role to limit. 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 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

Security Objective	Rationale
	data access can be provided to different users. FTA_SSL.3 and FTA_SSL.4 require session termination mechanisms to protect against idle sessions being used by unauthorized users.
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.
O.EADMIN	FIA_SOS.1 requires the TOE to enforce complexity rules when passwords are configured. 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. 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.PROTCT	FDP_ACC.1 and FDP_ACF.1 define the access control policy for Volume access. FMT_MSA.3 requires restrictive access to Volumes by default so that no access is granted until explicitly configured by authorized users.

Table 12 – Security Objectives for the TOE

6.4 DEPENDENCY RATIONALE

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

SFR	Dependencies	Dependency Satisfied / Rationale
FAU_GEN.1	FPT_STM.1	Satisfied by the operational environment (OE.TIME)

SFR	Dependencies	Dependency Satisfied / Rationale
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Satisfied Satisfied
FDP_ACC.1	FDP_ACF.1	Satisfied
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Satisfied Satisfied
FIA_ATD.1	None	n/a
FIA_SOS.1	None	n/a
FIA_UAU.1	FIA_UID.1	Satisfied
FIA_UAU.7	FIA_UAU.1	Satisfied
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
FTA_SSL.3	None	n/a
FTA_SSL.4	None	n/a

Table 13 - Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

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

The assurance requirements are summarized in Table 14.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	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 14 - 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. 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.

7.1.2 User Data Protection

Servers are only permitted to access (via their associated SDC instance) volumes (via their associated SDS instance) for which a mapping has been explicitly configured. When a mapping is configured, the MDM informs the SDC so that the volume can be exposed to the server.

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

7.1.3 Identification and Authentication

When users initiate sessions via the GUI or CLI applications to the MDM, they must complete the login process. Prior to successful completion of the login process, no TSF data or function access is permitted.

During collection of username and password, only dots or no characters are echoed for each character supplied for the password.

Upon successful login, the user's username and role are bound to the session. These attributes do not change during the session.

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

7.1.4 Security Management

The GUI application provides functionality for authorized users to manage user sessions, SDC instances, and SDS instances. The CLI application provides functionality for authorized users to manage users, user sessions, SDC

instances, SDS instances, and volumes. Each user session is bound to a role upon login, and that role determines access permissions as specified in FMT_MTD.1.

When volumes are created, initially no SDC instances are mapped to them, so no servers are authorized to access them. Users with the Administrator and Configure roles have the ability to configure mappings for the volumes.

When passwords are configured for users, the TOE enforces the composition rules specified with FIA_SOS.1.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_SOS.1, 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. For CLI sessions only, termination by the TOE occurs if the session remains idle for more than the configured inactivity timer value.

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

8 TERMINOLOGY AND ACRONYMS

8.1 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
API	Application Program Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HDD	Hard Disk Drive
IT	Information Technology
I/O	Input/Output
LAN	Local Area Network
MDM	Meta Data Manager
OE	Operational Environment
OSP	Organizational Security Policy
PCIe	Peripheral Component Interconnect Express
PP	Protection Profile
QoS	Quality of Service
RAM	Random Access Memory
REST	REpresentational State Transfer
RHEL	Red Hat Enterprise Linux
SAN	Storage Area Network
SDC	ScaleIO Data Client
SDS	ScaleIO Data Server
SFP	Security Function Policy
SFR	Security Functional Requirement
SSD	Solid State Drive

Acronym	Definition
ST	Security Target
SVM	ScaleIO Virtual Machine
TOE	Target of Evaluation
TSF	TOE Security Functionality

Table 15 - Acronyms