EMC® ViPR® SRM 4.0
Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1915-000-D102
Version: 1.1
10 August 2016

EMC Corporation
176 South Street
Hopkinton, Massachusetts
01748

Prepared by:

EWA-Canada
1223 Michael Street
Ottawa, Ontario, Canada
K1J 7T2

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, Acronyms, defines the acronyms used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title: EMC® ViPR® SRM 4.0 Security Target

ST Version: 1.1

ST Date: 10 August 2016

1.3 TOE REFERENCE

TOE Identification: EMC® ViPR® SRM 4.0 – 2513 with M&R 6.7u1 - 63979

TOE Developer:	EMC Corporation
TOE Type:	Storage Resource Management Software (Other Devices and Systems)

1.4 TOE OVERVIEW

EMC ViPR SRM is storage resource management software that provides a visual representation of storage relationships, analysis of configurations and capacity growth, and optimization of storage resources. ViPR SRM receives metrics from network storage resources including applications, hosts, switches and arrays and provides analysis of that information and presents it in a variety of ways to facilitate optimization of those resources. ViPR SRM is designed to integrate with the EMC ViPR Software-defined storage platform.

ViPR SRM was designed to manage large, complex, virtualized storage environments. ViPR SRM provides detailed relationship and topology views from the application, to the virtual or physical host, to the Logical Unit (LUN) to identify service dependencies. Administrators may view performance trends and identify hosts that may be competing for storage resources. This allows administrators to understand and manage the impact that storage has on applications, and with this information, optimize storage resources to manage data growth.

1.4.1 Analysis

ViPR SRM provides functionality to analyze health, configurations and capacity growth. Custom dashboards and reports may be created to meet the needs of a wide range of users and roles. ViPR SRM also allows administrators to track block, file and object capacity consumption across data centers with built in views to indicate who is using capacity, how much they are using, and when more will be required.

1.4.2 Optimization

ViPR SRM provides functionality that allows administrators to optimize capacity and improve productivity of block, file and object storage. It shows historical workloads and response times to determine if the most appropriate storage tier has been implemented. It tracks capacity use, and analyzes relationships between primary storage and replicas to identify the total capacity used to support an application. ViPR SRM also tracks consumption of thin pools and storage groups to predict when more capacity will be required, which supports use of thin provisioning to improve utilization.

The TOE is a software only TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is made up of the ViPR SRM software. The M&R platform consists of core modules that provide monitoring and reporting functionality for a number of EMC products, including ViPR SRM. Logically, ViPR SRM consists of the M&R core platform and a set of solution packs designed to collect data from hosts, switches and storage devices. In the evaluated configuration, the TOE is installed using the four Virtual Machine (VM) vApp installation option. The VMs are:

- Collector VM – This VM hosts collectors used to discover, collect and process data from supported hosts, switches and storage devices
- Primary Backend VM – This VM hosts the primary database, back end components, load balancing components and modules which support capacity, alerting and topology
- Frontend VM – This VM hosts the web portal and centralized management applications and controls licensing
- Additional Backend VM – This VM includes additional databases and back end components used to scale back end processing

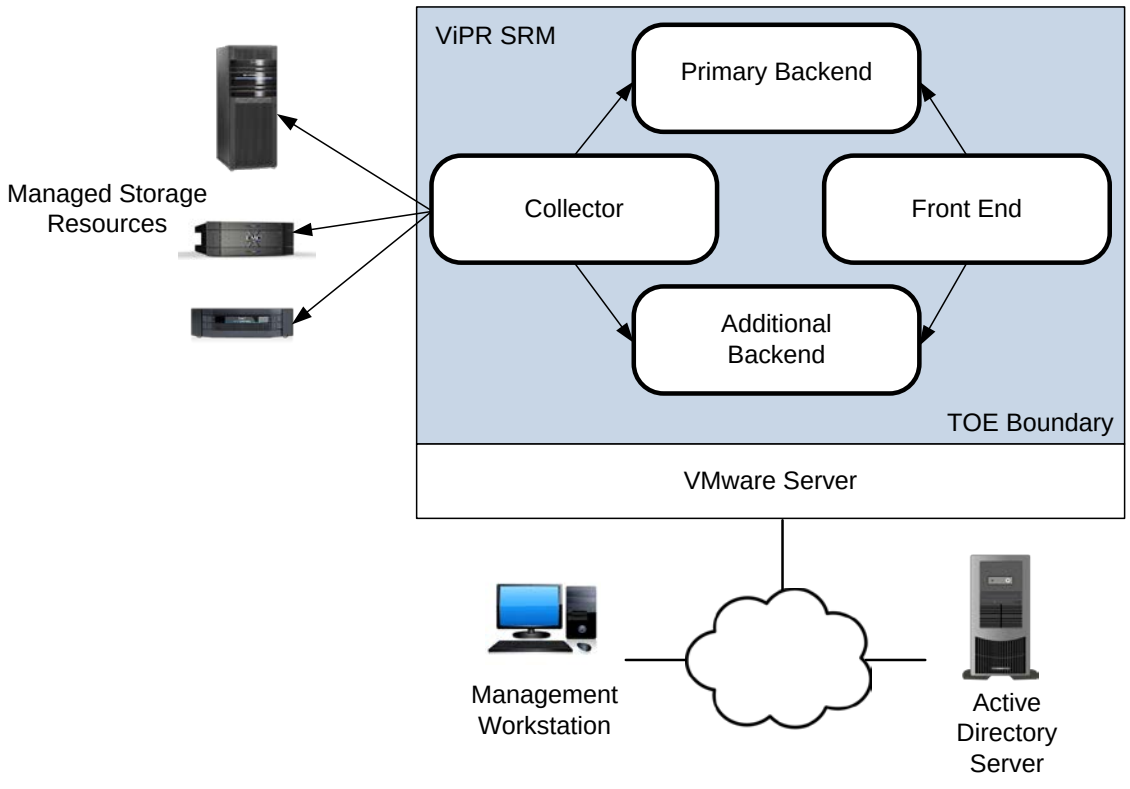

Figure 1 – EMC ViPR SRM 4.0 TOE Boundary

1.5.2 TOE Environment

The TOE is installed on a VMware Server. The following non-TOE components are also required in the evaluated configuration. The versions shown are those used in the evaluated configuration. A full list of installation requirement options may be found in the EMC ViPR SRM 3.7 Support Matrix.

Non-TOE Component	Software	Hardware
VMware Server	vCenter v5.5	General Purpose VMware Computer Hardware
Active Directory Server	Windows Server 2008 R2	General Purpose Computer Hardware
Managed Storage Resources	Unity VSA (Unisphere 4.0.0.7329527)	General Purpose Computer Hardware
Management Workstation	Windows 7	General Purpose Computer Hardware

Table 1 – Non-TOE Hardware and Software

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- EMC ViPR SRM Release number 3.7 SolutionPack Release Notes
- EMC ViPR SRM 3.7 Installation and Configuration Guide
- EMC ViPR SRM 3.7 SolutionPack Installation and Configuration Guide
- EMC M&R 6.6u1 Security Configuration Guide
- EMC ViPR SRM Version 3.7 Administrator's Guide

1.5.4 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. The following breakdown also provides the description of the security features of the TOE, and follows the security functional classes described in Section 1. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. The audit logs are stored and protected from unauthorized modification and deletion and may be reviewed by authorized administrators.

Functional Classes	Description
Cryptographic Support	Cryptographic functionality is provided to allow the communications links between TOE components and 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. The TOE supports multiple authentication mechanisms.
Security Management	The TOE provides management capabilities via user interface. Management functions allow the administrators to configure users and roles, system settings, and report parameters.
Protection of the TSF	The TOE stores and protects password information for externally monitored devices.
TOE Access	A banner is presented upon user login. The TOE supports TSF-initiated and administrator-initiated session termination.
Trusted Path/Channels	The communications links between the TOE and its remote administrators are protected using HTTPS (Transport Layer Security (TLS)).

Table 2 – Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The TOE issues SolutionPacks for discovery and monitoring of numerous external storage resources, and provides out-of-box licenses for the following:

- SolutionPack for Brocade FC Switch
- SolutionPack for Cisco MDS/Nexus
- SolutionPack for EMC VNX
- SolutionPack for EMC VMAX

Since SolutionPacks are configurations and not additional software components, they are included within the TOE boundary but are not tested as part of this evaluation. The EMC Unity Virtual Storage Appliance (VSA) is used to simulate managed storage resources in the evaluated configuration.

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 extended
- 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. 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.

Threat	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.AUDACC	Authorized users may not be accountable for the actions that they perform because the audit records are not created and reviewed, thus allowing an attacker to escape detection.
T.NOAUTH	An unauthorized individual may gain access to the TOE security management functions and use this to allow unauthorized access to information protected by the TOE.
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 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.REPORT	The TOE will create storage usage reports based on system metrics.

Table 4 - Organizational Security Policy

3.3 ASSUMPTIONS

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

Assumptions	Description
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.
A.PHYSICAL	The server resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.SECCOM	The communications between the TOE and the authentication servers is secured.
A.TIME	The operational environment provides reliable timestamps.

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. Access shall be terminated after a period of inactivity, or as determined by an authorized administrator. Access must be preceded by an advisory warning regarding unauthorized use.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must generate audit records for use of the TOE functions, and provide a means to review those records.
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 the administrative functions and data of the TOE using both local and LDAP based authentication. Authentication feedback must be obscured.
O.PATH	The TOE must ensure the confidentiality of data passed between itself and remote administrators.
O.PROTECT	The TOE must ensure the confidentiality of password information used to access third party resources.
O.REPORT	The TOE must be able to gather storage system metrics and create reports on usage.

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.ADMTRA	Authorized administrators are carefully screened during the selection process. All selected administrators are trained to appropriately install, configure, and maintain the TOE in its evaluated configuration according to the TOE guidance documentation.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the enforcement of security are protected from any physical attack.
OE.SECCOM	The operational environment will protect the communications between the TOE and authentication servers.
OE.TIMESTAMP	The operational environment will provide reliable timestamps for use by the TOE.

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.ACCOUNT	T.AUDACC	T.NOAUTH	T.SENSDATA	T.UNDETECT	P.REPORT	A.NOEVIL	A.PHYSICAL	A.SECCOM	A.TIME
O.ACCESS	X									
O.ADMIN	X		X							
O.AUDIT		X			X					
O.ENCRYPT				X						
O.IDENTAUTH	X		X							
O.PATH				X						

	T.ACCOUNT	T.AUDACC	T.NOAUTH	T.SENSDATA	T.UNDETECT	P.REPORT	A.NOEVIL	A.PHYSICAL	A.SECCOM	A.TIME
O.PROTECT			X							
O.REPORT						X				
OE.ADMTRA							X			
OE.PHYSICAL								X		
OE.SECCOM									X	
OE.TIMESTAMP		X			X	X				X

Table 8 – 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.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. Access shall be terminated after a period of inactivity, or as determined by an authorized administrator. Access must be preceded by an advisory warning regarding unauthorized use.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE using both local and LDAP based authentication. Authentication feedback must be obscured.

Rationale:	O.ACCESS mitigates this threat by limiting authorized users to appropriate TOE functions and data. Prior to gaining access to the TOE, users are presented with an advisory warning regarding unauthorized use of the TOE, mitigating user error. User sessions are terminated automatically after a period of inactivity or as determined by and authorized administrator, limiting the impact of possible errors. O.ADMIN mitigates this threat by ensuring that the TOE management functions prevent authorized users from gaining unauthorized access to TOE configuration information. O.IDENTAUTH mitigates this threat by deploying multiple identification and authentication mechanisms to prevent authorized users from gaining unauthorized access to TOE configuration information. It also provides users with obscured feedback while authentication is in progress, protecting authentication information from being used by an unauthorized person.

Threat: **T.AUDACC**	Authorized users may not be accountable for the actions that they perform because the audit records are not created and reviewed, thus allowing an attacker to escape detection.	
Objectives:	O.AUDIT	The TOE must generate audit records for use of the TOE functions, and provide a means to review those records.
	OE.TIMESTAMP	The operational environment will provide reliable timestamps for use by the TOE.
Rationale:	O.AUDIT mitigates this threat by ensuring auditable events are logged, securely stored, and made viewable to authorized administrators. OE.TIMESTAMP ensures that audit data is supported with accurate time information.	

Threat: **T.NOAUTH**	An unauthorized individual may gain access to the TOE security management functions and use this to allow unauthorized access to information protected by the TOE.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE using both local and LDAP based authentication. Authentication feedback must

		be obscured.
	O.PROTECT	The TOE must ensure the confidentiality of password information used to access third party resources.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. O.IDENTAUTH restricts access to authorized users by allowing access only after proper identification and authorization has been verified through one of the available mechanisms. It also provides users with obscured feedback while authentication is in progress, protecting authentication information from being used by an unauthorized person. O.PROTECT mitigates this threat by protecting the confidentiality of password information used to access third party resources.	

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 generate audit records for use of the TOE functions, and provide a means to review those records.
	OE.TIMESTAMP	The operational environment will provide reliable timestamps for use by the TOE.
Rationale:	O.AUDIT mitigates this threat by ensuring auditable events are logged and made viewable to authorized administrators. OE.TIMESTAMP ensures that audit data is supported with accurate	

	time information.

4.3.2 Security Objectives Rationale Related to OSPs

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

Policy: **P.REPORT**	The TOE will create storage usage reports based on system metrics.	
Objectives:	O.REPORT	The TOE must be able to gather storage system metrics and create reports on usage.
	OE.TIMESTAMP	The operational environment will provide reliable timestamps for use by the TOE.
Rationale:	O.REPORT supports this policy by ensuring that the TOE is able to gather storage system metrics and create reports on usage. OE.TIMESTAMP ensures that report data is supported with accurate time information.	

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.NOEVIL**	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.ADMTRA	Authorized administrators are carefully screened during the selection process. All selected administrators are trained to appropriately install, configure, and maintain the TOE in its evaluated configuration according to the TOE guidance documentation.
Rationale:	OE.ADMTRA supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

Assumption: **A.PHYSICAL**	The server resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the

		enforcement of security are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by ensuring the physical protection of the server resources used by the TOE.	

Assumption: A.SECCOM	The communications between the TOE and the authentication servers is secured.	
Objectives:	OE.SECCOM	The operational environment will protect the communications between the TOE and authentication servers.
Rationale:	OE.SECCOM supports this assumption by requiring that information passed between the TOE and the authentication server is secured.	

Assumption: A.TIME	The operational environment provides reliable timestamps.	
Objectives:	OE.TIMESTAMP	The operational environment will provide reliable timestamps for use by the TOE.
Rationale:	OE.TIMESTAMP supports this assumption by requiring that the operational environment provide reliable timestamps for use by the TOE.	

5 EXTENDED COMPONENTS DEFINITION

This section specifies the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) used in this ST.

5.1 SECURITY FUNCTIONAL REQUIREMENTS

Two extended SFRs have been created to address additional security features of the TOE: Protection of external passwords (FTP_TPS_EXT.1) and Administrator-initiated termination (FTA_SSL_EXT.5).

5.1.1 Extended Family FPT_TPS: PROTECTION OF THIRD PARTY SECRETS

Protection of third party secrets addresses the collection of security information from monitored devices, and the actions performed on that information. The Protection of third party secrets family belongs to the Protection of the TSF class, and was modelled after the family FPT_ITT Internal TOE TSF data transfer (FPT_ITT). FPT_TPS.1 Protection of external passwords was based on FPT_ITT.1 Basic Internal TSF data transfer protection.

5.1.1.1 FPT_TPS_EXT Protection of Third Party Secrets

Family Behaviour

This family defines the requirements for the protection of third party secrets. This family may be used to specify the protection provided for third party secrets held by the TOE.

Component Levelling

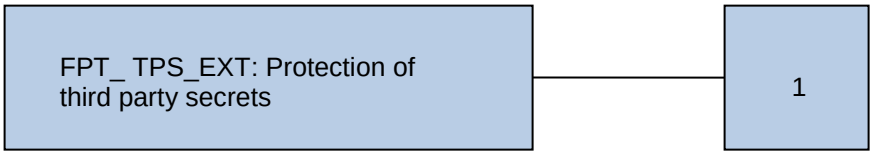

Figure 2 – FPT_TPS_EXT: Protection of third party secrets Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

FPT_TPS_EXT.1 Protection of external passwords

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TPS_EXT.1.1	The TSF shall store and protect passwords required to access external entities.

FPT_TPS_EXT.1.2 The TSF shall present the password to the external entity in accordance with the requirements of the external entity.

5.1.2 FTA_SSL_EXT.5 Administrator-initiated termination

This extended SFR is part of the Session locking and termination (FTA_SSL) family.

Component Levelling

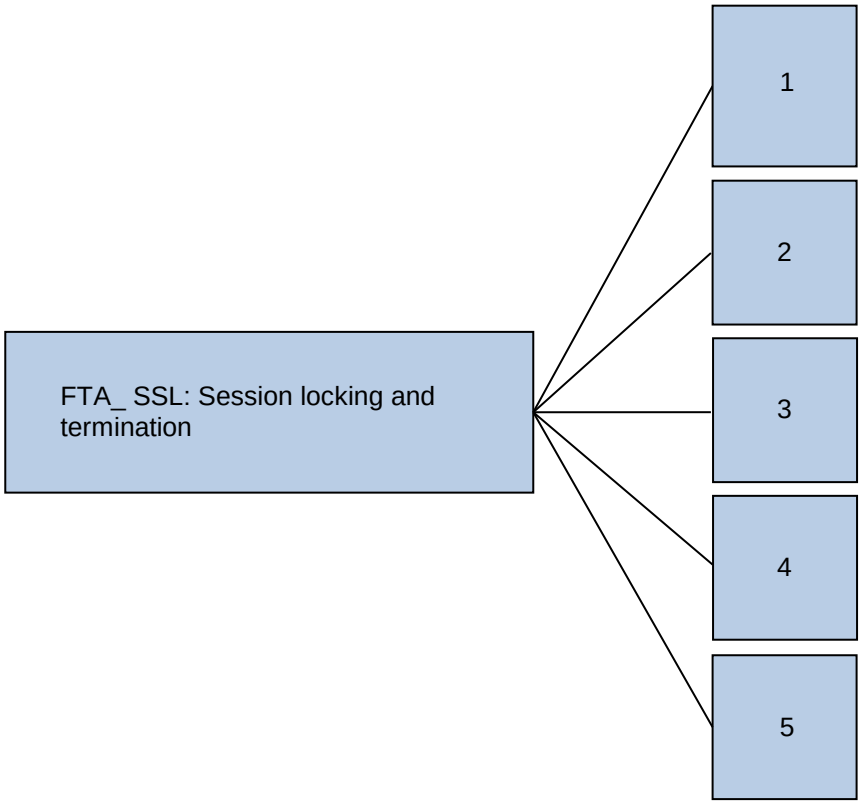

Figure 3 – FTA_SSL: Session Locking and Termination Component Levelling

Management

There are no management activities foreseen.

Audit

The TSF should create an audit entry when an administrator terminates a user's session.

FTA_SSL_EXT.5 Administrator-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL_EXT.5.1 The TSF shall allow administrator-initiated termination of a user's interactive session.

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, extended requirements, 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 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 9 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
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
	FDP_ETC.1	Export of user data without security

Class	Identifier	Name
		attributes
	FDP_ITC.1	Import of user data without security attributes
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	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)	FPT_TPS_EXT.1	Protection of external passwords
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL_EXT.5	Administrator-initiated termination
	FTA_TAB.1	Default TOE access banners
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 9 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) [*collection configuration events, reporting events, user management events, start and stop of services, user events*].

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_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorised administrators*] with the capability to read [*all audit information*] from the audit records.

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

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, 192, 256*] 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: [*no standard*].

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 10*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in Table 10*] and cryptographic key sizes [*cryptographic key sizes specified in Table 10*] that meet the following: [*standards listed in Table 10*].

Operation	Algorithm	Key Size (bits) or Digest	Standard	CAVP Certificate Number
Random Bit Generation	HMAC DRBG	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512/256	NIST Special Publication 800-90A	722
Encryption and Decryption of remote administrator sessions	AES (Advanced Encryption Standard)	128, 192, 256	FIPS PUB 197	3263
Encryption and Decryption of Third Party passwords	AES (Advanced Encryption Standard)	128, 192, 256	FIPS PUB 197	3263

Table 10 – Cryptographic Operation

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 [*Administrative Access Control SFP*] on [*Subjects: Administrative users*
Objects: TSF data
Operations: view, modify and delete TSF data to manage configuration, users and reporting functions].

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 [*Administrative 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 identified as Global administrators have full access to all TSF data*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*users with accounts identified as Disabled have no access to TSF data*].

6.2.3.3 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the [*Administrative Access Control SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

6.2.3.4 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the [*Administrative Access Control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*Authorized administrative users may configure the TSF to retrieve performance data from network storage resources*].

Application note: Administrators configure SolutionPacks to establish the connection to a storage resource and collect metrics.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 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.

6.2.4.2 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*internal authentication, LDAP authentication*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*order of authentication mechanisms indicated in the configuration file*].

6.2.4.3 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

6.2.4.4 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Administrative Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*user security attributes, report parameters, collection configuration parameters*] to [*Authorized Administrative users*].

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 [*Administrative 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 [*Authorized 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 functions, reporting functions, collection configuration functions*].

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 [*Datacenter Administrator Users, Full Control Users, NOC Operator Users, Network Administrator Users, Storage Administrator Users, Web Service Role*].

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_TPS_EXT.1 Protection of external passwords

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TPS_EXT.1.1 The TSF shall store and protect passwords required to access external entities.

FPT_TPS_EXT.1.2 The TSF shall present the password to the external entity in accordance with the requirements of the external entity.

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 [*one hour of user inactivity*].

6.2.7.2 FTA_SSL_EXT.5 Administrator-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL_EXT.5.1 The TSF shall allow administrator-initiated termination of a user's 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 [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 FUNCTIONAL REQUIREMENTS RATIONALE

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

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENAUTH	O.PATH	O.PROTECT	O.REPORT
FAU_GEN.1			X					
FAU_SAR.1		X	X					
FCS_CKM.1				X				
FCS_CKM.4				X				
FCS_COP.1				X				
FDP_ACC.1	X	X						
FDP_ACF.1	X	X						
FDP_ETC.1	X							X
FDP_ITC.1								X
FIA_UAU.2					X			
FIA_UAU.5					X			
FIA_UAU.7					X			

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENAUTH	O.PATH	O.PROTECT	O.REPORT
FIA_UID.2					X			
FMT_MSA.1		X						
FMT_MSA.3		X						
FMT_SMF.1		X						
FMT_SMR.1		X						
FPT_TPS_EXT.1							X	
FTA_SSL.3	X							
FTA_SSL_EXT.5	X							
FTA_TAB.1	X							
FTP_TRP.1						X		

Table 11 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

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

Objective: **O.ACCESS**	The TOE must allow authorized users to access only appropriate TOE functions and data. Access shall be terminated after a period of inactivity, or as determined by an authorized administrator. Access must be preceded by an advisory warning regarding unauthorized use.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FTA_SSL.3	TSF-initiated termination
	FTA_SSL_EXT.5	Administrator-initiated termination
	FTA_TAB.1	Default TOE access banners
Rationale:	FDD_ACC.1 meets this objective by enforcing an access control policy to ensure only authorized users can gain access to appropriate TOE functions and data. FDP_ACF.1 meets this objective by enforcing the rules and	

	attributes that govern the access control policy. FDP_ETC.1 meets this objective by enforcing the access control policy when exporting user data outside of the TOE. FTA_SSL.3 meets this objective by automatically terminating an interactive session after one hour of inactivity. FTA_SSL_EXT.5 meets this objective by giving authorized administrators the ability to terminate a user's interactive session. FTA_TAB.1 meets this objective by presenting users with an advisory warning message regarding unauthorized use of the TOE, before establishing a session.

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FAU_SAR.1	Audit review
	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:	FAU_SAR.1 meets this objective by providing authorized administrators the ability to access and review audit records. FDP_ACC.1 meets this objective by enforcing the access control policy limiting the management of the TOE security functions to authorized administrators. FDP_ACF.1 meets this objective by enforcing the rules and attributes that govern the access control policy. FMT_MSA.1 meets this objective by restricting the ability to manipulate the Administrative Access Control SFP security attributes to authorized administrators. FMT_MSA.3 meets this objective by restricting the ability to manipulate the Administrative Access Control SFP default security attributes to authorized administrators. FMT_SMF.1 supports this objective by identifying the management functions authorized administrators are able to perform. FMT_SMR.1 supports this objective by maintaining a list of authorized TOE roles.	

Objective: O.AUDIT	The TOE must generate audit records for use of the TOE functions, and provide a means to review those records.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Rationale:	FAU_GEN.1 meets this objective by generating audit records for auditable events. FAU_SAR.1 supports this objective by providing authorized administrators with the means to read and interpret all audit information.	

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 the administrative functions and data of the TOE using both local and LDAP based authentication. Authentication feedback must be obscured.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Rationale:	FIA_UAU.2 meets this objective by ensuring that each user is successfully authenticated before gaining access to TOE functions and data. FIA_UAU.5 meets this objective by supporting internal authentication and LDAP authentication. FIA_UAU.7 meets this objective by providing obscured feedback to users while authentication is in progress. FIA_UID.2 meets this objective by ensuring that each user is	

	successfully identified before gaining access to the TOE functions and data.

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: **O.PROTECT**	The TOE must ensure the confidentiality of password information used to access third party resources.	
Security Functional Requirements:	FPT_TPS_EXT.1	Protection of external passwords
Rationale:	FPT_TPS_EXT.1 meets this objective by storing and protecting passwords required to access external entities.	

Objective: **O.REPORT**	The TOE must be able to gather storage system metrics and create reports on usage.	
Security Functional Requirements:	FDP_ETC.1	Export of user data without security attributes
	FDP_ITC.1	Import of user data without security attributes
Rationale:	FDP_ETC.1 meets this objective by identifying the ability to export user data for the generation of network storage usage reports. FDP_ITC.1 meets this objective by specifying the ability to retrieve performance data from network storage resources.	

6.4 DEPENDENCY RATIONALE

Table 12 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	x	Timestamps are provided to the TOE by the operational environment in order to satisfy this requirement.
FAU_SAR.1	FAU_GEN.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	✓	
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	✓	
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.5	None	N/A	
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_SMR.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_TPS_EXT.1	None	N/A	
FTA_SSL.3	None	N/A	
FTA_SSL_EXT.5	None	N/A	
FTA_TAB.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 12 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

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

The assurance requirements are summarized in the Table 13.

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

Assurance Class	Assurance Components	
	Identifier	**Name**
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 13 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

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

7.1 TOE SECURITY FUNCTIONS

7.1.1 Security Audit

The TOE uses Tomcat Web-Server to produce a chronological record of system activities and security-relevant transactions in two formats. Log files are generated for each module and service and are handled using Java Logging. Audit logs are generated for specific user interactions and recovered from the connected servers. All logs are accessed through the user interface and restricted to authorized users with Global Administrator privileges. Logs can be viewed directly from the user interface or downloaded as a ZIP file on a local machine.

The TOE generates records for the following audit event types:

Event Type	Description
Collection Configuration Events	The discovery, configuration, and modification of collector devices.
Reporting Events	Records the following report transactions: • When a ReportPack, template, or schedule has been created, modified, or deleted. • Report generation stats including start, stop, and rendering time.
User Management Events	Records when users, profiles and roles are: • Created, modified, and deleted • Enabled and disabled
Start and stop of services	Start, stop, and restart times of a service, device, or module.
User Events	• Authentication success and failure • Session termination including user-initiated, idle timeout, or administrator-initiated.

Table 14 - Audit Event Types

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

7.1.2 Cryptographic Support

ViPR SRM uses the RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software Version: 6.2), Cryptographic Module Validation Program (CMVP)

certificate number 2469 to provide cryptographic support. TLS 1.2 is used to protect the link between the administrator and the TOE, and encryption is used to protect third party passwords held by the TOE.

AES keys are generated for the protection of third party passwords using the cryptographic module's Deterministic Random Bit Generator (HMAC DRBG). (Keys used in support of TLS are generated using Diffie-Hellman key exchange, in accordance with the TLS 1.2 standard (RFC 2246); however, this not part of the FCS_CKM.1 claim.) Keys are zeroized using the <object>.clearSensitiveData() function within the module.

AES encryption is used in support of both administrative sessions, and protection of third party passwords.

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

7.1.3 User Data Protection

The TOE provides role-based access to administrative functionality through the user interface. The TOE enforces the Administrative Access Control SFP to manage TOE configuration, users, and reporting functions. Only authorized users identified as Global Administrators have full access to the TSF functions and data, including import and export capabilities of all user data.

User data is imported from external hosts, switches, and storage devices by the Collector VM then stored in the Primary Backend database. Only metric data is collected, therefore associated security attributes are ignored during data import and export transactions.

For example, the TOE filters for physical and logical assets such as hosts and virtual arrays, raw and usable capacity, and data center events. Only the metric data is analyzed and exported in the form of usage reports. Usage reports can be generated in the following formats: PDF, CSV, XLS, PNG, JPEG, SVG, and XML.

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

7.1.4 Identification and Authentication

The identification and authentication functions ensure that users attempting to access the TOE have provided valid user credentials and are authorized to access the requested services.

When an authorized administrator adds a user, they're presented with the option to choose either *Internal Authentication* or *External Authentication*. External authentication requires that the administrator only provide a user login. Password validation is done through a corporate LDAP-based identity repository such as Active Directory.

Internal authentication uses Apache Tomcat's native services and requires the administrator to provide both a User Login and Password when creating users.

The TOE is configured for Single Sign On by default, but can be setup to authenticate based on Realm for individual applications.

During the authentication process, obscured feedback is provided to the user entering the password.

TOE Security Functional Requirements addressed: FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2.

7.1.5 Security Management

Security management for the TOE is implemented in a hierarchical manner. For initial installation, the TOE operator must first provide the default credentials. The default username is ***admin*** and the default password is ***changeme***. This operator account is then used to create a Global Administrator who can create additional users and assign access rights to control what they can see and do in the interface. A Global Administrator has full access to all user management, reporting, and configuration functions.

User permissions and settings are defined by a combination of User Status, Profile and User Roles.

When a user account is created, the user is first assigned a status of Normal User or Global Administrator. Note that 'Global Administrator' and 'Normal User' are not user roles. They are user status settings. 'Normal User' is the default status for all users. Various access restrictions on reports and components can be set on users assigned the 'Normal User' status. Users with 'Global Administrator' status have full rights to all components, cannot be disabled and have no restrictions on templates. At the highest level of security management, the Administrative Access Control SFP is enforced on Normal Users and Global Administrators.

Users can then be assigned to a role with access to specific TOE functions. If a user is not assigned to a role, by default, the user only sees Scheduled Reports, Stored Reports, and Favorite Reports. Table 15 identifies and defines the default user roles provided by the TOE.

User Role	Description
Datacenter Administrator Users	This role allows users to access datacenter oriented reports.
Full Control Users	This role allows users to access most modules and tools. It also gives them read-write access to all available templates.
NOC Operator Users	This role allows users to access all reports.
Network Administrator Users	This role allows users to do the following: • Access network oriented reports • Discover devices • Remove data and devices

User Role	Description
	• Modify groups and service levels • Use SNMP tools • Define alerts
Storage Administrator Users	This role allows users to do the following: • Access storage oriented reports • Discover devices • Remove data and devices • Modify groups and service levels • Define alerts
Web Service Role	This role is used for web service calls only.

Table 15 - TOE User Role Descriptions

All users of the TOE are also assigned a default profile which groups users and roles together for global reporting requirements. Profiles define global characteristics of a user, such as language and time zone. There is only one default profile however, Global Administrators can create and customize profiles at their discretion.

Global Administrators have the authority to associate all users with roles that limit or restrict access to management, reporting, and collection configuration functions. They're also given the ability modify, reset, and customize any of the default settings.

Users have permissions to configure collection operations, create reports and manage users, according to their assigned roles. In order to perform these functions, the users will be able to query, modify and delete the collection configuration parameters, the report parameters and the user security attributes accordingly. By default, when a user is first created, the user has only the 'Normal User' status and no roles until specifically added by an administrator. There are no collection parameters or report parameters until specifically added by an administrator. These are considered to be restrictive default values.

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

7.1.6 Protection of the TSF

The TOE deploys SolutionPacks to discover, connect, and collect data from physical hosts. The TOE stores and protects the passwords required to access these network storage resources by restricting management and configuration functions to authorized administrators. Only authorized administrators have the ability to configure the TOE in order to present password information in accordance with individual host requirements.

TOE Security Functional Requirement addressed: FPT_TPS_EXT.1.

7.1.7 TOE Access

The TOE can be configured to display an advisory message to users on login, warning of unauthorized use. Authenticated user sessions are terminated after one hour of user inactivity, or may be terminated by an authorized administrator.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL_EXT.5, FTA_TAB.1.

7.1.8 Trusted Path / Channels

The TOE protects information when it is transmitted between the front end web portal and the remote management workstation. The TOE achieves this by using TLS to perform the encryption and the decryption of data that is being passed. The trusted paths are established for each administrative session, making them logically distinct from other communication paths. Administrators identify the TOE by entering the known URL for the administrative interface; the TOE identifies the administrative user via username and password, thereby providing assured identification of the end points.

The TOE is preconfigured for HTTPS and enabled for SSL by default. In the evaluated configuration, it must be configured to TLS1.2 protocols to encrypt data in transit over the network.

TOE Security Functional Requirements addressed: FTC_TRP.1.

8 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advance Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generation
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
HMAC	Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OSP	Organizational Security Policy
PP	Protection Profile
RSA	Rivest, Shamir and Adleman
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security

Acronym	Definition
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
VSA	Virtual Storage Appliance

Table 16 – Acronyms