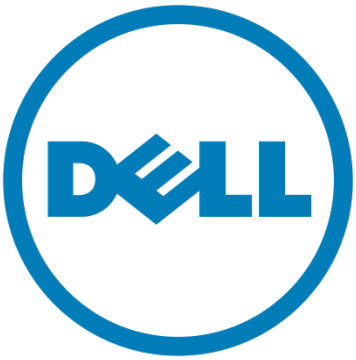
Integrated Dell™ Remote Access Controller 9

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2098-000-D102
Version: 1.3
22 October 2019



Dell Technologies
1 Dell Way
Round Rock, Texas, USA
78682

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
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 Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

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

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

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

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

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

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	Integrated Dell™ Remote Access Controller 9 Security Target
ST Version:	1.3
ST Date:	22 October 2019

1.3 TOE REFERENCE

TOE Identification: Integrated Dell™ Remote Access Controller 9 3.34.34.34

TOE Developer: Dell Technologies

TOE Type: Remote Management (Other Devices and Systems)

1.4 TOE OVERVIEW

The Integrated Dell™ Remote Access Controller 9 (iDRAC9) is a systems management solution that provides remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge systems.

The iDRAC9 uses an integrated System-on-Chip microprocessor for the remote monitor/control system. The iDRAC9 co-exists on the system board with the managed PowerEdge server. The server operating system is concerned with executing applications; the iDRAC9 is concerned with monitoring and managing the server's environment and state outside of the operating system.

The remote management functionality provided by the iDRAC9 TOE is access controlled and all administrator actions are audited. Communications to access this functionality are protected using cryptography.

The TOE is a combined firmware and hardware TOE.

In this ST, the TOE may be referred to as the TOE, the Integrated Dell Remote Access Controller 9 or iDRAC9. It should be understood that all references to the TOE are for the version of the TOE referenced in Section 1.3.

1.4.1 TOE Environment

The iDRAC9 Service Processor is implemented within a Dell server.

Figure 1 shows the evaluated configuration. Although many more servers are supported, the evaluated configuration consists of the platforms listed in Table 1. One of these systems is required to operate the TOE. The evaluated configuration also requires a Windows Server 2016 Domain Controller with Active Directory and an NTP service, and an administrator workstation.

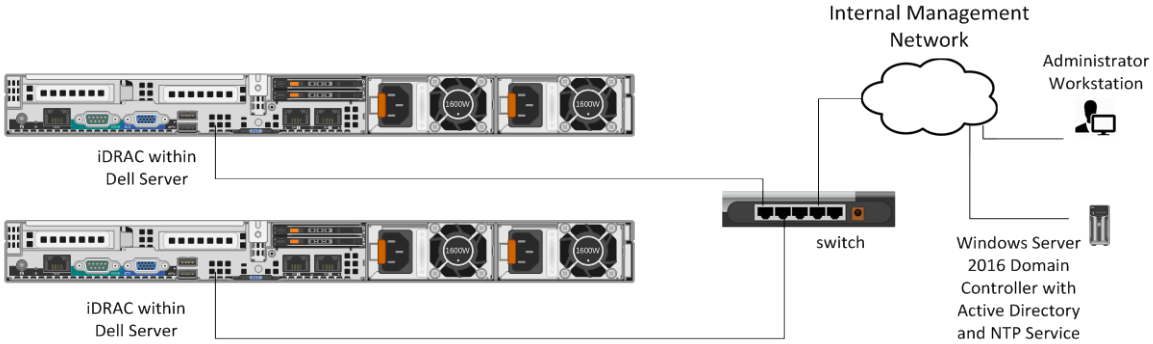


Figure 1 – Deployment Configuration

Component	Operating System	Hardware
Tower Series Server	not applicable	PowerEdge T440
		PowerEdge T640
Rack Series Server	not applicable	PowerEdge R440
		PowerEdge R540
		PowerEdge R740
		PowerEdge R740xd
		PowerEdge R640
		PowerEdge R840
		PowerEdge R940
		PowerEdge R940xa
Administrator Workstation	Windows 10	General Purpose Computer Hardware
Active Directory	Windows Server 2016	General Purpose Computer Hardware
NTP Service		

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of the iDRAC9 Advanced RISC[1] Machine (ARM) hardware and iDRAC9 firmware. The TOE includes external interfaces used for management, and interfaces internal to the managed server to communicate with the Host system.

[1] Reduced Instruction Set Computer

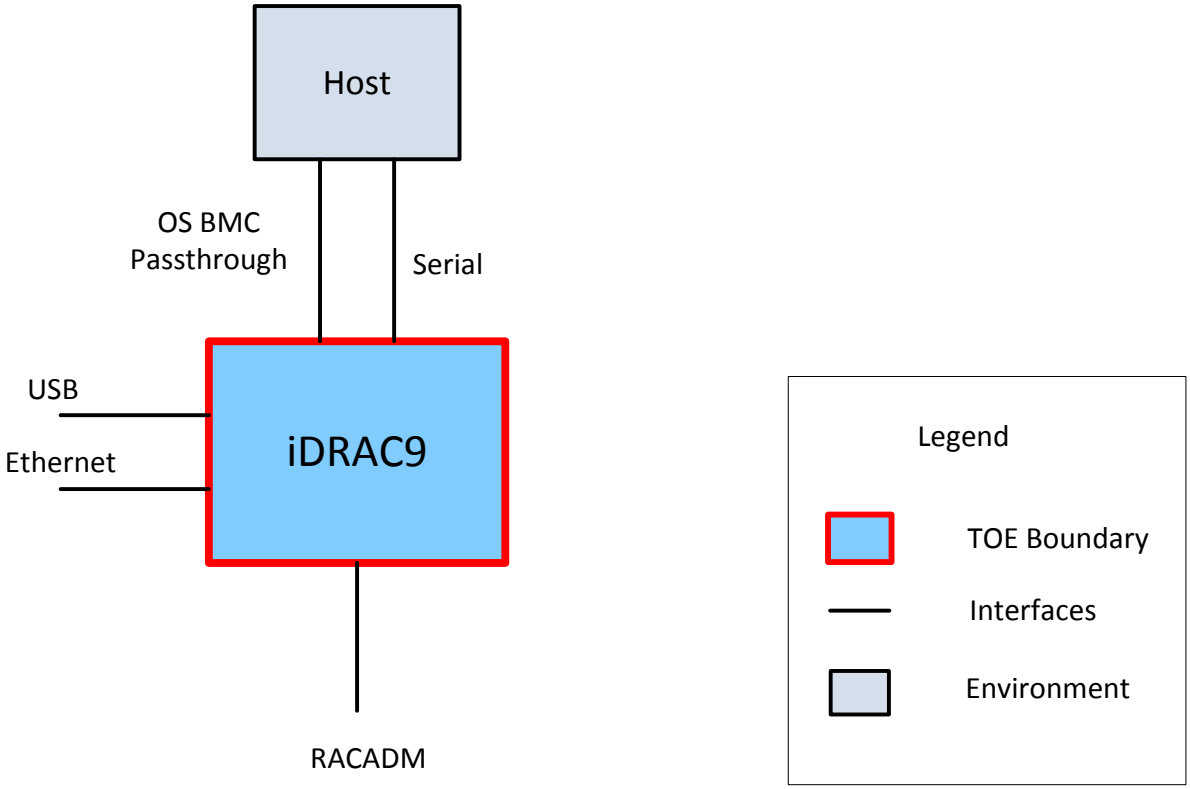


Figure 2 – TOE Boundary

The iDRAC9 hardware is implemented within one of the servers listed in Table 1.

1.5.1.1 TOE Interfaces

In the evaluated configuration, the following iDRAC9 interfaces are supported:

- **Remote Access Controller Admin (RACADM)** The RACADM interface is accessed over HTTPS.
- **Server Management USB Port** An administrator may plug a laptop directly into the micro Universal Serial Bus (USB) port and configure iDRAC9 using the Web Graphical User Interface (GUI), RACADM, WSMan or Redfish.
- **Ethernet** An administrator uses the Ethernet port to access iDRAC9 over HTTPS using the Web GUI, Remote RACADM, WSMan or Redfish.

1.5.1.2 TOE Delivery

The TOE is delivered as an integral component of the server, which is delivered by courier when ordered directly from Dell Technologies. The evaluated version of the firmware may be downloaded from the Dell support site as iDRAC_3.34.34.34_A00.exe (Windows-based Dell Update Package (DUP)) or iDRAC-with-Lifecycle-Controller_Firmware_3HT95_LN_3.34.34.34_A00.BIN (Contains both iDRAC and Lifecycle Controller firmware) update package for Red Hat Linux.

1.5.1.3 TOE Guidance

The TOE includes the following guidance documentation:

- Integrated Dell Remote Access Controller 9 (iDRAC9) Version 3.30.30.30 User's Guide, Rev. A00
  - idrac9-lifecycle-controller-v3303030_users-guide_en-us.pdf
- iDRAC9 with Lifecycle Controller Version 3.30.30.30 RACADM CLI Guide, Rev. A00
  - idrac9-lifecycle-controller-v3303030_reference-guide_en-us.pdf
- iDRAC9 with Lifecycle Controller Version 3.31.31.31 Redfish API Guide, Rev. A00
  - idrac9-lifecycle-controller-v3313131_api-guide_en-us.pdf

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. The audit logs can be reviewed by authorized administrators, and filtered to show only the desired logs.
Cryptographic Support	Cryptographic functionality is provided to allow the communications links between the TOE and its remote administrators to be protected.
User Data Protection	The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE.
Identification and Authentication	Users must identify and authenticate prior to TOE access. The password is not displayed when entered by the user.
Security Management	The TOE provides management capabilities via a Web-Based Graphical User Interface (GUI), accessed via HTTPS, or locally through the Remote Access Controller Admin (RACADM) Command Line Interface (CLI). Management functions allow the administrators to view audit records, configure users and roles, and monitor server health and configuration.
Protection of the TSF	The TOE provides reliable time stamps.

Functional Classes	Description
TOE Access	Users are automatically logged out of the management interfaces after a configurable period of inactivity. Users may log out at any time. A TOE administrator may configure the permitted services and accessible ports.
Trusted Path/Channel	The communications links between the TOE and its remote administrators are protected using Hypertext Transfer Protocol Secure (HTTPS).

Table 2 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from the evaluated configuration:

- Windows multifactor authentication
- Telnet, Secure Shell (SSH) and Simple Network Management Protocol (SNMP) are not exercised in the evaluated configuration

The following features were not evaluated as part of the evaluation:

- Hardware Root of Trust
- SELinux Policy Enforcement

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

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

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

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

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

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

2.3 PACKAGE CLAIM

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

2.4 CONFORMANCE RATIONALE

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

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 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 for the TOE.

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.UNDETECT	Authorized 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.
T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on 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.CRYPTO	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information, which is transferred between the TOE and administrators.

OSP	Description
P.MANAGE	The TOE shall provide a means of managing the health of the server in which it is implemented.

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.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NETWORK	An internal management network is provided for the sole use of management of internal resources, and is logically separate from other networks.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

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

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

Security Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
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 the availability of the server in which it is implemented, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must record audit records for use of the TOE functions. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing.
O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against the inadvertent exposure of passwords.
O.PROTECT	The TOE must protect against inadvertent access to interactive management sessions, and must provide a means of controlling and restricting access to TOE services and ports.
O.SECURE	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
O.TIME	The TOE must provide reliable timestamps.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

Security Objective	Description
OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
OE.NETWORK	The operational environment will provide an internal management network separate from the primary network for management of network resources.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

	T.ACCOUNT	T.PRIVILEGE	T.UNDETECT	P.CRYPTO	P.MANAGE	A.LOCATE	A.MANAGE	A.NETWORK	A.NOEVIL
O.ACCESS	X								
O.ADMIN	X	X			X				
O.AUDIT			X						
O.CRYPTO				X					
O.IDENTAUTH	X	X							
O.PROTECT		X							

	T.ACCOUNT	T.PRIVILEGE	T.UNDETECT	P.CRYPTO	P.MANAGE	A.LOCATE	A.MANAGE	A.NETWORK	A.NOEVIL
O.SECURE		X							
O.TIME			X						
OE.ADMIN							X		X
OE.NETWORK								X	
OE.PHYSICAL						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 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.
	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 the availability of the server in which it is implemented, 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. The TOE must protect against the inadvertent exposure of passwords.
Rationale:	O.ACCESS mitigates this threat by ensuring that users may only access the functions and data for which they are authorized. O.ADMIN provides the functions to administer the TOE, and to limit	

	access to those functions. O.IDENTAUTH provides the identifying information that determines a user's authorized access.

Threat: T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
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 the availability of the server in which it is implemented, 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. The TOE must protect against the inadvertent exposure of passwords.
	O.PROTECT	The TOE must protect against inadvertent access to interactive management sessions, and must provide a means of controlling and restricting access to TOE services and ports.
	O.SECURE	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized users. O.IDENTAUTH helps to mitigate the threat by ensuring that only credentialed users have access to the TOE. O.PROTECT mitigates this threat by ensuring that system and audit data are not accessible, except to those with explicit access permissions. O.SECURE mitigates the threat by ensuring that system management data in transit is protected.	

Threat: T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions. Audit records must be readable by authorized administrators and administrators must be able to filter records

		for ease of viewing.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against the inadvertent exposure of passwords.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.AUDIT ensures that audit records are maintained for the use of TOE functions. O.IDENTAUTH ensures that user identity is captured by the TOE for inclusion in the audit records. O.TIME provides reliable timestamps for audit records.	

4.3.2 Security Objectives Rationale Related to OSPs

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

Policy: **P.CRYPTO**	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information, which is transferred between the TOE and administrators.	
Objectives:	O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
Rationale:	O.CRYPTO supports this policy by ensuring that validated cryptographic algorithms are provided in support of cryptographic operations.	

Policy: **P.MANAGE**	The TOE shall provide a means of managing the health of the server in which it is implemented.	
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 the availability of the server in which it is implemented, and restrict these functions and facilities from unauthorized use.
Rationale:	O.ADMIN ensures that functionality is in place to manage the availability of the server in which the TOE is implemented.	

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.LOCATE	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 security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: A.MANAGE	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
Rationale:	OE.ADMIN supports this assumption by ensuring that trained individuals are in place to manage the TOE.	

Assumption: A.NETWORK	An internal management network is provided for the sole use of management of internal resources, and is logically separate from other networks.	
Objectives:	OE.NETWORK	The operational environment will provide an internal management network separate from the primary network for management of network resources.
Rationale:	OE.NETWORK supports this assumption by ensuring the availability of an internal management network.	

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.ADMIN	There are an appropriate number of trusted,

		authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
Rationale:	OE.ADMIN supports this assumption by ensuring that the individuals managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirement (SFR) used in this ST. An extended SFR has been created to address additional security features of the TOE. It is:

a. Service and port access controls (FTA_SAC_EXT.1)

This SFR belongs to the TOE Access class. A new family, Service Access, has been created to address functionality not included in CC Part 2.

5.1.1 FTA_SAC_EXT Service Access

Family Behaviour

This family defines the requirements for controlling access to TOE services and ports. The family FTA_SAC_EXT Service Access is modelled after FTA_TSE TOE Session Establishment. FTA_SAC_EXT.1 Service and port access controls is modelled after FTA_TSE.1 TOE Session Establishment.

Component Levelling

Figure 3 – FTA_SAC_EXT: Service Access Component Levelling

FTA_SAC_EXT.1 Service and port access controls, requires the TOE to provide functionality to configure port access and restrict access to TOE services.

Management

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

a. configuration of allowed services;

b. configuration of the port number used for a particular interface.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. changes to the configuration of allowed services;

b. changes to the configuration of the ports in use; and

c. changes to the configuration of the allowed Internet Protocol (IP) addresses.

FTA_SAC_EXT.1 Service and Port Access Controls

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SAC _EXT.1.1 The TSF shall restrict access to services based on system configuration.

FTA_SAC _EXT.1.2 The TSF shall allow administrators to determine the port numbers to be used to access services.

FTA_SAC _EXT.1.3 The TSF shall allow administrators to determine the IP addresses that may be used to access services.

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 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 17, summarized in Table 9.

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

Class	Identifier	Name
Identification and Authentication (FIA)	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
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_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_SAC_EXT.1	Service and port access controls
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) [*Administrator login and logout*, *configuration changes*].

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

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

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

6.2.1.3 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

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 [*cryptographic key generation algorithm in* Table 10] and specified cryptographic key sizes [*cryptographic key sizes in* Table 10] that meet the following: [*list of standards in* Table 10].

Usage	Key Generation Algorithm	Key Size (bits)	Standard
RSA[2]	RSA Key Generation	2048 bit	FIPS[3] 186-4
AES[4]	Deterministic Random Bit Generator	128, 256	SP[5] 800-90A

Table 10 – Cryptographic Key Generation

[2] Rivest, Shamir and Adleman

[3] Federal Information Processing Standards

[4] Advanced Encryption Standard

[5] Special Publication

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 [*key zeroization*] that meets the following: [*FIPS 140-2*].

6.2.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

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

Operation	Algorithm	Key or Digest Size (bits)	Standards
Signature Generation and Verification	RSA	2048 (generation) 1024, 2048 (verification)	FIPS 186-4
Symmetric Encryption/ Decryption	AES	128, 256	FIPS 197
Keyed-Hash Message Authentication Code	HMAC[6]-SHA[7]-1 HMAC-SHA2-256 HMAC-SHA2-384	160 256 384	FIPS 198
Secure Hash	SHA SHA-256	160 256	FIPS 180-4

[6] Hash Message Authentication Code

[7] Secure Hash Algorithm

Operation	Algorithm	Key or Digest Size (bits)	Standards
	SHA-384	384	

Table 11 – Cryptographic Operations

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Security Management Access Control SFP*] on [
Subjects: administrators
Objects: security management configuration
Operations: view, modify].

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 [*Security Management Access Control SFP*] to objects based on the following: [
Subjects: administrators
Subject attributes: role
Objects: security management configuration
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: [*An administrator may view and modify security management configuration if the operation is permitted for that administrator's role*].

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

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

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*viewing of the Media Access Control (MAC) Address, service tag, model and license*] 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.

6.2.4.2 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 [*obfuscated feedback*] to the user while the authentication is in progress.

6.2.4.3 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*viewing of the Media Access Control Address, service tag, model and license*] 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.

6.2.5 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 [*Security Management Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*configuration attributes*] to [*authorized administrators*].

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 [*Security Management 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 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: [

- *review audit records*

- *configure available ciphersuites*
- *manage users and roles*
- *disable services*
- *configure allowed services*].

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 [*Admin, Operator, Read-Only*].

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7.3 FTA_SAC_EXT.1 Service and port access controls

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SAC _EXT.1.1 The TSF shall restrict access to services based on system configuration.

FTA_SAC _EXT.1.2 The TSF shall allow administrators to determine the port numbers to be used to access services.

FTA_SAC _EXT.1.3 The TSF shall allow administrators to determine the IP addresses that may be used to access services.

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, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

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

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

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

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

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

Table 12 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

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

	O.ACCESS	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDENAUTH	O.PROTECT	O.SECURE	O.TIME
FAU_GEN.1			X					
FAU_SAR.1		X	X					
FAU_SAR.3		X	X					
FCS_CKM.1				X				
FCS_CKM.4				X				
FCS_COP.1				X				
FDP_ACC.1	X							
FDP_ACF.1	X							
FIA_UAU.1					X			
FIA_UAU.7					X			
FIA_UID.1					X			
FMT_MSA.1		X						
FMT_MSA.3		X						
FMT_SMF.1		X						

	O.ACCESS	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDENAUTH	O.PROTECT	O.SECURE	O.TIME
FMT_SMR.1		X						
FPT_STM.1								X
FTA_SSL.3						X		
FTA_SSL.4						X		
FTA_SAC_EXT.1						X		
FTP_TRP.1							X	

Table 13 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

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

Objective: O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Rationale:	FDP_ACC.1 and FDP_ACF.1 ensure that the security management configuration attributes are accessible only to users with the appropriate user role.	

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 the availability of the server in which it is implemented, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable 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 ensures that management functionality to review audit records is provided. FAU_SAR.3 ensures that the functionality to filter these logs is provided. FDP_ACC.1 and FDP_ACF.1 control access to the security management configuration attributes that provide the means of managing the health and availability of the server managed by the TOE. FMT_MSA.1 provides the functionality to manage the security attributes that determine TOE access. FMT_MSA.3 ensures that default values for these attributes are permissive to ensure that users are not inappropriately locked out. FMT_SMF.1 provides the security management functionality required to manage the TOE. FMT_SMR.1 provides roles that are used to restrict the authorized use of security management functionality.	

Objective: **O.AUDIT**	The TOE must record audit records for use of the TOE functions. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Rationale:	FAU_GEN.1 ensures that the TOE is able to generate audit records for security related events. FAU_SAR.1 ensures that the functionality to read audit records is provided, and FAU_SAR.3 ensures that the functionality to filter these logs is provided.	

Objective: **O.CRYPTO**	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.	
Security Functional	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction

Requirements:	FCS_COP.1	Cryptographic operation
Rationale:	FCS_CKM.1 ensures that cryptographic keys are generated in accordance with approved standards. FCS_CKM.4 ensures that cryptographic keys are destroyed in accordance with approved standards. FCS_COP.1 ensures that cryptographic operations are performed in accordance with approved standards.	

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, except data required to identify the system. The TOE must protect against the inadvertent exposure of passwords.	
Security Functional Requirements:	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Rationale:	FIA_UID.1 and FIA_UAU.1 ensure that users may access data required to identify a system prior to authentication, and that users are identified and authenticated prior to being granted access to administrative functions. FIA_UAU.7 protects against the inadvertent exposure of passwords while they are entered.	

Objective: **O.PROTECT**	The TOE must protect against inadvertent access to interactive management sessions, and must provide a means of controlling and restricting access to TOE services and ports.	
Security Functional Requirements:	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_SAC_EXT.1	Service and port access controls
Rationale:	FTA_SSL.3 and FTA_SSL.4 protect against access to interactive management sessions by logging users out after a period of inactivity, and by allowing users to log out at any time, respectively. FTA_SAC_EXT.1 ensures that the TSF provides a means of restricting access to TOE services, and a means of configuring the port numbers to be used for various services.	

Objective:	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.

O.SECURE		
Security Functional Requirements:	FTP_TRP.1	Trusted path
Rationale:	FTP_TRP.1 ensures that interactive sessions are protected against disclosure and modification.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 ensures that the TOE provides reliable time stamps.	

6.4.3 Dependency Rationale

Table 14 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	None	N/A	
FTA_SSL.3	None	N/A	
FTA_SSL.4	None	N/A	
FTA_SAC_EXT.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 14 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

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

7 TOE SUMMARY SPECIFICATION

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

7.1 SECURITY AUDIT

iDRAC9 provides two types of logs:

- **Lifecycle log** - This log contains events related to system, storage devices, network devices, firmware updates, login and logout, and configuration changes. The lifecycle log can be viewed through the iDRAC9 Web interface.
- **System Event Log (SEL)** - System events are also available as a separate log called System Event Log. For each event, the SEL page on the iDRAC9 web interface displays a system health indicator, a time stamp, and a description of the event logged.

The starting of the iDRAC9 services is audited. Stopping, which is usually the result of an unplanned event, is not audited. However, the date and time of the log previous to the restart event provides an indication of when the service was stopped. Where applicable, the logs indicate the user who was responsible for an audited event.

All of the audit information may be read by any of the users with the permission to log on to the iDRAC9 Web interface. The logs may be filtered by severity, type, date and keyword. Only a user in the Admin role can clear the logs.

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

7.2 CRYPTOGRAPHIC SUPPORT

iDRAC9 includes a Federal Information Processing Standards (FIPS)-validated cryptographic module (CMVP certificate # 2861). Cryptography is used in support of Transport Layer Security (TLS) 1.1 and 1.2 for communications with administrators, and for data at rest encryption (D@RE) of private keys used for TLS and user information. Additionally, the digital signature on the firmware is verified at boot time, and when the firmware is updated.

The operational environment for the FIPS evaluation includes iDRAC9 running on a PowerEdge R740 Rack Server. For all other hardware in Table 1, the vendor affirms that implementation of iDRAC9 with the various server models does not alter the iDRAC9 firmware or the cryptographic module within the firmware.

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

7.3 USER DATA PROTECTION

The TOE provides controlled access to the administrative functions that support the iDRAC9 remote management functionality, including:

- system monitoring, including inventory and health monitoring
- deployment and configuration activities
- update
- maintenance and troubleshooting

Access to these functions is controlled through the Security Management Access Control SFP, which allows users to perform functions based on the user's assigned role. The role to privilege mapping is shown in Table 15, and the privilege description is provided in Table 16.

Role	Privilege
Admin	Login
	Configure
	Configure Users
	Logs
	System Control
	Access Virtual Console
	Debug
Operator	Login
	Configure
	System Control
	Access Virtual Console
	Debug
Read Only	Login

Table 15 – Roles and Privileges

Privilege	Description
Login	Enables the user to log in to iDRAC9 and view configuration information and logs

Privilege	Description
Configure	Enables the user to configure iDRAC9. With this privilege, a user can also configure power management, virtual console, virtual media, licenses, system settings, storage devices, BIOS settings, and System Configuration Profile (SCP)
Configure Users	Enables the user to allow specific users to access the system
Logs	Enables the user to clear only the System Event Log (SEL)
System Control	Allows power cycling the host system
Access Virtual Console	Enables the user to run Virtual Console
Debug	Enables the user to run diagnostic commands

Table 16 –Privilege Descriptions

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

7.4 IDENTIFICATION AND AUTHENTICATION

Prior to being identified and authenticated, a user is able to see the Media Access Control (MAC) Address, service tag, model and license when using a Redfish application over the Ethernet interface. This information is provided to ensure that the user is attaching to the correct server. No other access to TOE information or functionality is provided via any other access prior to authentication. Local authentication and Active Directory authentication are used in the evaluated configuration.

Passwords are obfuscated when entered. The characters provided are browser dependent; dots are presented when using Microsoft browsers. Users cannot modify their own passwords. For local authentication, passwords are entered by the administrator and provided to the user.

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

7.5 SECURITY MANAGEMENT

The TOE provides multiple means of managing the iDRAC9 security functionality. In the evaluated configuration, administrator may manage iDRAC9 using:

- Ethernet port (over HTTPS)
    - iDRAC9 web interface
    - Remote RACADM
    - Representational State Transfer (REST) interfaces
        - Redfish applications

        - WSMan
- RACADM port (over HTTPS)
    - Remote RACADM
- Server Management USB Port
    - iDRAC9 Web GUI
    - RACADM
    - Representational State Transfer (REST) interfaces
        - Redfish applications
        - WSMan

These interfaces allow for the management of the iDRAC9 TOE. All other management interfaces are disabled in the evaluated configuration.

The default values of the security attributes used to control access are user roles. The default is considered to be restrictive in that a user has the role of 'none' until an authorized administrator assigns a role to the user.

Management interfaces allow users to perform the following security management functions:

- Review both Lifecycle and System Event Logs
- Configure the ciphersuites to be used with the TOE
- Manage users and roles
- Disable iDRAC9 services
- Configure allowed services, including port numbers

The TOE supports three default roles – Admin, Operator and Read-Only. Permissions for these roles are described in Table 15.

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

7.6 PROTECTION OF THE TSF

Network Time Protocol (NTP) is used to set the time in the embedded Linux kernel within iDRAC9. iDRAC9 then uses this time to support functions such as audit log creation.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.7 TOE ACCESS

Users may logout of the GUI or RACADM interface at any time. Users will be automatically logged out of the GUI after a configurable period of inactivity. When using a Redfish application, the password must be provided with each request.

iDRAC9 allows administrators to disable services, to ensure that only the services being used are available. For enabled services, the administrator can configure the port number on which the service is available. Additionally, iDRAC9 can filter the IP addresses over which an administrator may access the iDRAC9 security management functionality.

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

7.8 TRUSTED PATH / CHANNELS

When the iDRAC9 web interface is used, the connection between iDRAC9 and the remote administrator's browser is protected from modification and disclosure using TLS. This connection is logically distinct from other communication channels. The iDRAC9 end point is identified by the user when attempting to access the iDRAC9, and the user is authenticated prior to being granted access to security management functions.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Administrator	The term ‘administrator’ refers collectively to the users in the administrative roles ‘Admin’, ‘Operator’, and ‘Read-Only’.
Redfish	The Redfish Scalable Platforms Management API is a standard defined by the Distributed Management Task Force (DMTF). Redfish is a systems management interface standard, which enables scalable, secure, and open server management. It uses RESTful interface semantics to access data that is defined in model format to perform out-of-band systems management.
WSMan	Web Services for Management (WSMan) are a Simple Object Access Protocol (SOAP)–based protocol used for systems management. iDRAC9 uses WSMan to convey Distributed Management Task Force (DMTF) Common Information Model (CIM)–based management information. The CIM information defines the semantics and information types that can be modified in a managed system. The data available through WSMan is provided by iDRAC9 instrumentation interface mapped to the DMTF profiles and extension profiles.

Table 17 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
ARM	Advanced RISC Machine
BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
CC	Common Criteria
CIM	Common Information Model
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program

Acronym	Definition
CPU	Central Processing Unit
D@RE	Data at Rest Encryption
DMTF	Distributed Management Task Force
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
iDRAC9	Integrated Dell Remote Access Controller 9
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
NIC	Network Interface Card
NTP	Network Time Protocol
OSP	Organizational Security Policy
PP	Protection Profile
RACADM	Remote Access Controller Admin
REST	Representational State Transfer
RISC	Reduced Instruction Set Computer
RSA	Rivest, Shamir and Adleman
SEL	System Event Log
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Secure Network Mail Protocol
SOAP	Simple Object Access Protocol
SP	Special Publication
SSH	Secure Shell

Acronym	Definition
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
WSMan	Web Services for Management

Table 18 – Acronyms