Dell EMC Networking SmartFabric OS10.5.4

Common Criteria Guide

Version 1.1

August 2023

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the Dell EMC Networking SmartFabric OS10.5.4 (Version: OS10.5.4.3P1) and related information.

1.2 Audience

2 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed in Table 3.

1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1 Protection Profile Conformance

4 The Common Criteria evaluation was performed against the requirements of the Network Device collaborative Protection Profile (NDcPP) v2.2E available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Software and Hardware

5 The Target of Evaluation (TOE) includes the following software and hardware models:

Table 1: TOE models

Type	Model	CPU	Software
Physical	S4112F-ON S4112T-ON S4128F-ON S4128T-ON S4148F-ON S4148T-ON MX5108n	Intel Atom C2338 (Silvermont)	Dell OS10.5.4
	MX9116n	Intel Atom C2538 (Silvermont)	
	S5212F-ON N3248TE-ON	Intel Atom C3338 (Goldmont)	
	S5224F-ON S5232F-ON S5248F-ON S5296F-ON Z9264F-ON	Intel Atom C3538 (Goldmont)	
	Z9432F-ON S5448F-ON	Intel Atom C3758 (Goldmont)	
	E3224F-ON	Intel Atom C3558/ C3558R (Goldmont)	
	Z9332F-ON	Intel Pentium D1508 (Broadwell)	

1.3.3 Evaluated Functions

1 The TOE interfaces within the scope of evaluation are shown in Figure 1.

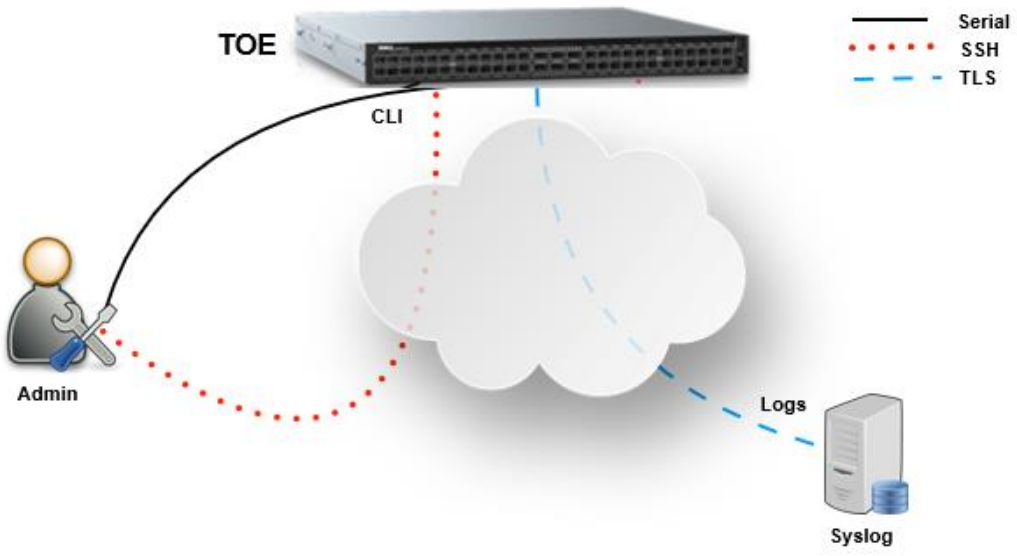

Figure 1: Example TOE deployment

2 The TOE interfaces are as follows:

a) **CLI.** Administrative CLI via direct serial connection or SSH.

b) **Logs.** Syslog via TLS.

3 The following functions have been evaluated under Common Criteria:

a) **Protected Communications.** The TOE provides secure communication channels:

i) **CLI.** Administrator access to the CLI via direct serial connection or SSH.

ii) **Logs.** Secure transmission of log events to a Syslog server via TLS.

b) **Secure Administration.** The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords

ii) Configurable password policies

iii) Role Based Access Control

iv) Access banners

v) Management of critical security functions and data

vi) Protection of cryptographic keys and passwords

c) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates via digital signatures and published hash.

d) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

e) **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

f) **Identification and Authentication.** The TOE ensures that all users must be authenticated before accessing its functions and data.

g) **Security Audit.** The TOE generates audit records of user and administrator actions.

h) **Cryptographic Operations.** The cryptographic algorithms used in the above functions have been validated for correct implementation.

4 **NOTE:** Remote authentication servers are not allowed in the evaluated configuration.

5 **NOTE:** While the user is given the option to configure IPv6, IPv6 may not be used in the evaluated configuration

6 **NOTE:** No claims are made regarding any other security functionality.

1.3.4 Evaluation Assumptions

7 The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold

Table 2: Evaluation Assumptions

Assumption	Guidance
Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Ensure that the device is hosted in a physically secure environment, such as a locked server room.
There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Do not install other software on the device hardware.
The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	The Common Criteria evaluation focused on the management plane of the device.
Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Ensure that administrators are trustworthy – e.g. implement background checks or similar controls.
The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Apply updates regularly according to your organization’s policies.

Assumption	Guidance
The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators should take care to not disclose credentials and ensure private keys are stored securely.
The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	Administrators should sanitize the device before disposal or transfer out of the organization's control.

1.4 Conventions

8 The following conventions are used in this guide:

a) `CLI Command <replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example:

Use the `cat <filename>` command to view the contents of a file

b) [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

c) **GUI => Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File => Save** to save the file.

d) [REFERENCE] *Section* – denotes a document and section reference from Table 3. For example:

Follow [ADMIN] *Configuring Users* to add a new user.

1.5 Related Documents

9 This guide supplements the below documents.

Table 3: Related Documents

Reference	Document
[ADMIN]	Dell SmartFabric OS10 User Guide, Release 10.5.4 12 2022 Rev. A05

10 **NOTE:** The information in this guide supersedes related information in other documentation.

2 Secure Acceptance and Update

2.1 Obtaining the TOE

11 Your Dell EMC Networking switch will be delivered via commercial courier. Perform the following checks upon receipt (return the device if either of the checks fail):

a) Confirm that the correct device has been delivered

b) Inspect the packaging to confirm that there are no signs of tampering

12 The TOE software can be obtained from the secure Dell Support website by authenticating via an authorized user. The downloaded software image must be transferred to the appliance using a secure method such as Secure Copy or SFTP.

13 The TOE implements “show version” CLI command that displays information about firmware version running on the TOE. The TOE also has ‘show boot detail’ which shows versions of both active image and standby image. The “show boot detail” command will immediately recognize and display the new version after it was downloaded and verified by the administrator.

14 The TOE restricts the ability to perform software updates to Security Administrators.

2.2 Verifying the TOE

15 To validate the software image before you install the image, use the `image secure-install` command. It verifies the signature of the image files using hash-based authentication or GPG based signatures. Upgraded image files are installed after they are successfully validated. This validation procedure prevents the installation of corrupted or modified images.

16 For GPG based signature verification, follow the additional steps give below:

a) Extract or untar the update package to the current directory by running the following command:

```
tar -xvf file_name.tar
```

(Make sure to replace file_name.tar with the actual filename)

b) Import the key-id given in the README.PKGS_OS10 txt file by running the following command:

```
image gpg-key key-server keyserver.ubuntu.com key-id
<key-id>
```

(Make sure to use the long key-id and not short key-id to avoid collisions)

17 **NOTE:** Refer the *Validate and upgrade OS10 image* section of [ADMIN] Chapter 16 Security for additional information.

2.3 Self-Tests

18 On start-up, the system will run a series of self-tests:

a) **BIOS POST.** If there is an issue with any of the POST results, the system does not boot.

b) **System Software Self-tests.** If there is any major issue at startup that prevents the system from proceeding, the system automatically reboots itself,

if possible. If there are missing components that are non-critical, the system continues the boot process but report a warning message.

c) **Secure Boot.** The TOE performs kernel image digital signature verification and file integrity checking. This is not performed by default and must be enabled in accordance with section 2.12.

d) **FIPS Self-tests.** The TOE includes a suite of FIPS self-tests that validate the integrity of the Dell OpenSSL Cryptographic Library and verify the implementation of the FIPS DRBG and the cryptographic algorithms. If any of these self-tests fail, the system will be unable to operate in a FIPS-validated manner and a 'Test Failed' message will be displayed to the user along with an indication of the failed test. If this occurs, restart the TOE.

19 NOTE: Failures during boot-up may cause the machine to either attempt to boot the standby image or go into a repeated reboot cycle. The user can interrupt the boot process (during a few seconds timeframe). If the user setup a password on the boot, they would have to authenticate. Afterwards, the user can either force a reboot to the standby image or they could uninstall the OS and reinstall a new image. These actions must be done through the console, either through a connected terminal server or direct access to the console port.

2.4 Updating the TOE

20 To update the TOE, follow the instructions in [ADMIN] Validate and upgrade OS10 image section of Chapter 16 Security.

21 An authorized user must authenticate to the secure Dell Support website where the software downloads are available.
NOTE: Use the image download command to download an OS10 image to the TOE. For example:

```
image download ftp://username:password@10.11.63.122/filename
```

22 **NOTE:** The verification files (published hash) are included with the installation package. This can be seen when the download is extracted. The published hash file will be SHA256 type.

23 Use the `image secure-install` command to verify the authenticity of the update prior to installation. It verifies the signature of the image files using hash-based authentication. Upgraded image files are installed after they are successfully validated. This validation procedure prevents the installation of corrupted or modified images. For example:

```
image secure-install image-filepath {sha256 signature hash-
         string}
```

24 **NOTE:** If the image did not validate successfully, ensure you have copied the correct binary file and imported the correct key-id for upgrading your system. Repeat the procedure if there is an issue with either the selected file or the download process.

25 **NOTE:** You should verify that the configuration described in the following sections has carried over subsequent to upgrade.

26 **NOTE:** Refer the *Validate and upgrade OS10 image* section of [ADMIN] Chapter 16 Security for additional information.

27 **NOTE:** Use '`boot system standby`' command to activate the inactive image.

28 **NOTE:** To enable Secure Boot, refer to [ADMIN] Enable secure boot in OS10 section of Chapter 16 Security.

2.5 Installation

29 Follow the instructions of [ADMIN] augmented by the configuration steps in the following sections.

2.6 Administration Interfaces

30 Only the below listed administration interfaces may be used. See [ADMIN] *CLI basics* Chapter 4 for general CLI usage.

31 NOTE: Administrators need to make sure that the serial console is a local interface.

a) **Console.** Connecting a serial cable and terminal emulator to the console serial port — serial port settings are 115200, 8 data bits, and no parity.

   i) See [ADMIN] *Login banner* to configure a banner message.

   ii) Enter the following command to apply user account lockout on the console:

   ```
   password-attributes max-retry <number> lockout-
   period <minutes> console-exempt
   ```

   max-retry number — Sets the maximum number of consecutive failed login attempts for a user before the user is locked out, from 0 to 16; default 3.

   lockout-period minutes — Sets the amount of time that a user ID is prevented from accessing the system after exceeding the maximum number of failed login attempts, from 0 to 43,200; default 5.

   If you set this value to zero, no lockout period is configured. Any number of failed login attempts do not lock out a user.

   console-exempt—Applicable only if the user lockout feature is enabled. Enables the user to log in through the console, even though the user ID is blocked because of an existing lockout.

   NOTE: To prevent user lockout from the console, ensure to use the console-exempt option.

   iii) Session termination on timeout is supported – use the following commands to configure the inactivity time period and disable access to shell commands:

   Navigate to the terminal context:

   ```
   OS10#configure terminal
   OS10(configure)#exec-timeout <timeout-value>
   ```

   where value is in seconds.

   Disable shell commands:

   ```
   OS10(configure)#system-cli disable
   ```

b) **SSH.** Remote access to the CLI via SSH. See Chapter 4 [ADMIN] *CLI Basics* for opening an SSH session and Chapter 16 [ADMIN] *Configure SSH Server* section of Security for advanced settings.

   NOTE: Enable FIPS mode via the console per section 1 below prior to using SSH.

   i) Password authentication is enabled by default.

ii) See [ADMIN] *username sshkey* section of Chapter 16 Security for enabling SSH password-less login using the public key of a remote client. **NOTE**: Only RSA and ECDSA keys are allowed in the evaluated configuration.

Supported key sizes for RSA - 2048, 3072.

Supported key sizes for ECDSA - 256, 384, or 521.

iii) See [ADMIN] *Regenerate public keys* section of Chapter 16 Security for configuring and generating the server's host keys. **NOTE**: Only RSA keys are allowed in the evaluated configuration.

Supported key sizes - 2048, 3072.

iv) See [ADMIN] *Login banner* section of Chapter 8 System management to configure a banner message.

v) Session termination on timeout is supported (set as per console above).

vi) Enter the following command to configure the maximum number of authentication attempts:

```
set ip ssh server max-auth-tries 1
```

2.7 Cryptography

32 Federal information processing standard (FIPS) cryptography provides cryptographic algorithms conforming to various FIPS standards published by the National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce. FIPS mode is also validated for numerous platforms to meet the FIPS-140-2 standard for a software-based cryptographic module.

33 See [ADMIN] *crypto fips enable* section of chapter 16 Security to restrict the use of cryptographic algorithms to those supported by the NIST FIPS 140-2 standard and certification process.

34 Enable FIPS mode as follows:

35
```
OS10(configure)#crypto fips enable
```

"WARNING: Upon committing this configuration, the system will regenerate SSH keys. Please consult documentation and toggle FIPS mode only if you know what you are doing! Continue? [yes/no(default)]:"

36 **NOTE:** If the system fails to transition to FIPS mode, an error message will be displayed. E.g., the system is not in a FIPS-compliant state or no usable cipher/mac/kex found in FIPS mode.

37 To verify that FIPS mode is enabled, use the `show fips status` command.

38 The following example shows that FIPS mode is successfully enabled:

```
OS10#show fips status

FIPS Mode: Enabled
```

39 **NOTE:** No additional configuration is required on the TOE to configure the CC supported algorithms or the related characteristics (e.g., block size, key size, digest size) for data encryption, signature generation, hash, and keyed hash.

40 No additional settings are required on the TOE for configuring the RNG functionality.

41 No additional configuration is required on the TOE to configure the SSH and TLS for CC supported algorithms.

42 Within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. The TOE reacts to the first threshold reached. These thresholds are not configurable.

2.8 Default Passwords

43 The following default user accounts have default passwords that must be changed:

a) admin - refer to [ADMIN] *User accounts* section of Chapter 4 CLI Basics.

b) linuxadmin – refer to [ADMIN] *User accounts* section of Chapter 4 CLI Basics

44 **NOTE:** The linuxadmin account must be disabled, refer [ADMIN] *system-user linuxadmin disable* section of Chapter 4 CLI Basics for instructions.

45 To reset password refer [ADMIN] *Recover Linux password* section of chapter 26 Troubleshoot Dell SmartFabric OS10.

46 Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”].

47 For strong passwords, Dell recommends using multiple and easy-to-remember common words in the password instead of using complex passwords which may be difficult to remember. Combine multiple words and modify the passphrase using special characters and numbers to get a final password. For example, instead of correcthorsebatterystaple, use C0rr3c+h0r5e8atTerystapl3.

48 The minimum password length is settable by the Administrator. Minimum password length shall be configurable to between [9] and [32] characters.

49 See [ADMIN] *Configure username and password* section of Chapter 3 Getting Started with Dell SmartFabric OS10 for additional information on minimum password length.

50 See [ADMIN] *Password strength* section of Chapter 16 security on rules to set strong password.

2.9 Setting Time

51 TOE allows the Security Administrator to set the time.

52 See [ADMIN] *Configure system time and date* section of Chapter 8 System management on how to set date and time manually.

2.10 Audit Logging

53 The Common Criteria evaluation confirmed that the log events listed at Annex A: Log Reference are generated by the TOE.

54 The Security Administrator can configure the TOE to send logs to a syslog server. Logs to syslog server are sent via TLS. Log events are sent to local store and syslog server in real-time.

55 Refer to [ADMIN] *Audit log* of Chapter 16 Security and [ADMIN] *System logging of* Chapter 26 Troubleshoot Dell SmartFabric OS10 for details about enabling and viewing logs.

2.10.1 Configuring Syslog Servers

56 See [ADMIN] *System logging* of Chapter 26 Troubleshoot Dell SmartFabric OS10 for details on configuring a Syslog server.

57 To configure the Syslog server, type the following command:

```
logging server {ipv4-address | DNS} tls [port-number]
[severity severity-level] [vrf {management | vrf-name]
```

58 **NOTE:** Syslog must be used with TLS per the instructions at [ADMIN] *System logging over TLS* of Chapter 26 Troubleshoot Dell SmartFabric OS10.

59 **NOTE:** If the TLS connection between the TOE and the remote server is broken unintentionally, then the system will repeatedly try to re-establish the connection automatically.

60 **NOTE:** The reference identifier (IP, DNS) for the Audit Server is configured automatically.

61 **NOTE:** While the user is given the option to configure IPv6, IPv6 may not be used in the evaluated configuration.

62 This reference identifier will be compared to the CN or SAN in the X.509 certificate presented by the Syslog server when establishing a TLS connection.

2.10.2 Configuring X.509v3

63 Refer to [ADMIN] *X.509v3 certificates* of Chapter 16 Security for details on configuring X.509 certificates and signing requests.

64 Certificate Signing Request (CSR) supports RSA Signature Algorithm with key size of 2048-bit. Key size can be configured using the 'length' parameter. Refer to [ADMIN] Generate a certificate signing request section of Chapter 16 Security for additional details.

65 Prior to installing host certificates, checking of the certificate chain should be performed. The necessary CA and root certificates must first be installed using the '`crypto ca-cert install`' command for each one.

66 The validity of various fields for a host certificate are checked during the host certificate installation using the '`crypto cert install`' command. It is necessary to use "verify" parameter with the command, which is otherwise an optional parameter.

67 The certificate may be validated before performing the installation. The validation checks the notBefore or notAfter fields, basicConstraints CA flag, and the certificate chain (if not self-signed).

68 The server certificate is validated when the connection to the syslog server is initiated.

69 To specifically check the certificate chain of a host certificate, it is necessary to copy the candidate host certificate to the home directory of the userid, e.g. admin userid, on the system. To ensure peer-name checking and extended key checking, these options must be enabled in the security profile.

70 **NOTE:** The peer-name check parameter must be enabled for TLS configuration.

71 Refer to [ADMIN] Security profile settings used by X.509v3 authentication section of Chapter 16 Security for key-usage and validity checking of certificates.

72 **NOTE:** The key-usage check parameter must be enabled in security profile settings for TLS configuration.

73 **NOTE:** Server certificates consumed by the TOE TLS client must have a ‘serverAuthentication’ extendedKeyUsage purpose.

74 Refer to [ADMIN] Request and install host certificates section of Chapter 16 Security for additional information on installing host certificate and extendedKeyUsage fields.

75 Certificate revocation checking is performed using a CRL. TOE doesn’t support OCSP validation. OCSP signing purpose in the extendedKeyUsage is not supported. If the extended key usage field is present in the user certificate, it must include the client authentication and server authentication purpose.

76 To validates a certificate, Login as the ‘admin’ userid and enter the command as shown in a). This does not perform revocation checking.

a) `crypto cert validate {ca-cert cert-path | host-cert cert-path | file filepath}`

77 To configure certificate revocation checking using a CRL, refer the following steps:

1. Configure the URL for a certificate distribution point in EXEC mode.

`crypto cdp add cdp-name cdp-url`

Verify the CDPs accessed by the switch in EXEC mode.

`show crypto cdp [cdp-name]`

To delete an installed CDP, use the `crypto cdp delete cdp-name` command.

2. Install CRLs that have been downloaded from CDPs in EXEC mode.

`crypto crl install crl-path [crl-filename]`

Display a list of the CRLs installed on the switch in EXEC mode.

`show crypto crl [crl-filename]`

To delete a manually installed CRL that was configured with the `crypto crl install` command, use the `crypto crl delete [crl-filename]` command.

78 To enable CRL checking on the switch, refer to [ADMIN] *Security profiles* section of chapter 17 Security.

79 Refer to [ADMIN] *crypto cert validate* section of chapter 17 Security on additional details for certificate validation.

2.11 Administrator Authentication

80 Refer to [ADMIN] *Security* for configuration of administrator authentication.

81 The TOE restricts the ability to manage the TSF data to Security Administrators.

NOTE: The Common Criteria configuration mandates local authentication.

2.12 Enabling Secure Boot

82 Use the command at [ADMIN] Enable secure boot in OS10 section o Chapter 16 Security to enable secure boot.

83 **NOTE:** Once secure-boot is enabled, it cannot be disabled, and OS10 can only be updated using the `image secure-install` command documented in the *Validate and upgrade OS10 image* section of [ADMIN] *Secure Boot*.

2.13 Exiting the CLI

84 Use command `exit` to exit the CLI.

Annex A: Log Reference

2.14 Events

85 The TOE generates the following log events.

Table 4: Audit Events

Requirement	Audit Events	Examples
FAU_GEN.1	Start-up and shutdown of the audit functions	Startup audit: <165>1 2023-05-02T16:04:37.818008+00:00 OS10 dn_alm 870 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_SYSTEM_RESTART: OS10 Event and Alarm management system restarted Shutdown audit: <165>1 2023-05-02T16:04:37.818008+00:00 OS10 dn_alm 846 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %NDM_SYSTEM_RELOAD: User request to reload system Cold reload system
	Administrative login and logout	Administrative login: SSH - <38>1 2023-05-02T16:16:11.690027+00:00 dut-host sshd 6932 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Accepted password for admin from 100.64.53.224 port 60236 ssh2 <110>1 2023-05-02T16:16:20.110226+00:00 dut-host .clish 6955 - - Node.1-Unit.1:PRI [audit], CLI session started for user admin with role sysadmin on /dev/pts/0 Using public key - 2023-05-05T08:30:04.770254+00:00 OS10 sshd 25741 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Accepted publickey for admin from 10 10.121.21.2 port 33770 ssh2: RSA SHA256:oUF8beg9j1CLvGCgXcHYEgQvaJO466w3 5rEYz1wcdaY Console – <86>1 2023-05-02T16:13:29.264005+00:00 dut-host login 6517 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) pam_unix(login:session): session opened for user admin by LOGIN(uid=0) <110>1 2023-05-02T16:13:37.444834+00:00 dut-host .clish 6543 - - Node.1-Unit.1:PRI [audit], CLI

Requirement	Audit Events	Examples
		session started for user admin with role sysadmin on /dev/ttyS0 Administrative logout: SSH - 2022-12-09T18:54:03.452356+00:00 OS10 dn_alm 675 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session closed for user admin <38>1 2023-05-02T16:16:22.572908+00:00 dut-host sshd 6948 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Disconnected from user admin 100.64.53.224 port 60236 Console – <86>1 2023-05-02T16:13:23.857096+00:00 dut-host login 5985 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) pam_unix(login:session): session closed for user admin
	Changes to TSF data related to configuration changes	All configuration events in this table.
	Generating/import of, changing, or deleting of cryptographic keys	GPG key import for updates: 2023-05-05T08:09:11.139544+00:00 OS10 .clish 27625 - - Node.1-Unit.1:PRI [audit], User admin on /dev/pts/0 from 10.121.21.2 used cmd: 'image gpg-key key-server keyserver.ubuntu.com key-id D70B3F7B1079EF11EE325B841F76F5F047CB9029 ' - completed Importing SSH key: 2022-05-05T08:09:11.139544+00:00 OS10 /mgmtsys.py 1205 - - Node.1-Unit.1:PRI [audit], Userid admin role installed sshkey ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCxSub9XN3SsWr/B1EzS9kH2jcFBzmpvQRy+tScqz7amnrjnrmIUVhAfFppI4l++ePMt658LOqVeY/af27rbL/Fjp05YeJRZpL+MWTeOdV+rHEOcc17fAGa66r18aeI+BXz+cpY0oASCIfNZJ4cRq4zESeceiQvYnVt7icow1X0CaBcTUTv3aX5Bfsr2Lw95DxQoGNCxR3IukXmUgId8FSnLg9XNFrmcmRrdOm/MGE4FidsJf6JjL8Qq1HYUyhsUSGlwr/Wsah2xrF70bCm1k5QRRmxuLhXuyYZROJmjupB0+OJj6kl6XSm7k55OoNE/rtuwQYRX3zSrO3X+DcYmMQX

Requirement	Audit Events	Examples
		2022-05-05T08:09:11.139544+00:00 OS10 .clish 1205 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'username admin sshkey "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCxSub9XN3SsWr/B1EzS9kH2jcFBzmpvQRy+tScqz7amnrjnrmIUVhAfFppI4l++ePMt658LOqVeY/af27rbL/Fjp05YeJRZpL+MWTeOdV+rHEOcc17fAGa66r18aeI+BXz+cpY0oASCIfNZJ4cRq4zESeceiQvYnVt7icow1X0CaBcTUTv3aX5Bfsr2Lw95DxQoGNCxR3IukXmUgId8FSnLg9XNFrmcmRrdOm/MGE4FidsJf6JjL8Qq1HYUyhsUSGlwr/Wsah2xrF70bCm1k5QRRmxuLhXuyYZROJmjupB0+OJj6kl6XSm7k55OoNE/rtuwQYRX3zSrO3X+DcYmMQX'" – completed Failure to import SSH key: 2023-05-05T08:09:11.139544+00:00 OS10 /mgmtsys.py 1094 - - Node.1-Unit.1:PRI [audit], Userid admin role sshkey operation failed 2023-05-05T08:09:11.139544+00:00 OS10 .clish 16888 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'username admin sshkey "ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCr64U+jJSX23wYRtq4GfopJ'" – completed Generating SSH key: 2022-05-05T08:09:11.139544+00:00 OS10 mgmtsys.py 1205 - - Node.1-Unit.1:PRI [audit], Generated rsa SSH keys : Deleting SSH key: 2022-05-05T08:09:11.139544+00:00 OS10 mgmtsys.py 1205 - - Node.1-Unit.1:PRI [audit], Shredded rsa SSH keys : When generating a new private key as part of a CSR operation: 2022-05-05T08:09:11.139544+00:00 OS10 .clish 12572 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'crypto cert generate request cert-file home://test.csr key-file home://test.key country CA state BC locality Vancouver organization LS orgunit GEN2121 cname 10.121.21.10 email test@lightshipsec.com' – completed

Requirement	Audit Events	Examples
		When deleting a private key as part of a key pair operation: 2022-05-05T08:18:47.614025+00:00 OS10 /mgmtsys.py 1244 - - Node.1-Unit.1:PRI [audit], Host certificate with CN = OS10 successfully deleted 2022-05-05T08:18:49.463683+00:00 OS10 /mgmtsys.py 1244 - - Node.1-Unit.1:PRI [audit], Key for certificate with CN = OS10 successfully deleted. Key hash RTrRIokD 2022-05-05T08:18:58.846056+00:00 OS10 .clish 12572 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'crypto cert delete newclientcert.crt fips' - completed Keys cannot be changed. They can only be added or deleted.
	Resetting passwords	2022-05-05T08:30:04.764794+00:00 OS10 /mgmtsys.py 1244 - - Node.1-Unit.1:PRI [audit], User testadmin password may have changed. 2022-05-05T08:30:04.770254+00:00 OS10 .clish 12572 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'username testadmin password ***** role sysadmin priv-lvl 15' - completed
FCS_SSHS_EXT.1	Failure to establish an SSH session	Failed Password: <38>1 2023-05-02T16:40:51.294046+00:00 dut-host sshd 10754 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Failed password for admin from 100.64.53.224 port 35218 ssh2 Bad packet length: <38>1 2022-04-29T11:10:21.079406+00:00 OS10 sshd 25205 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Bad packet length 263180. <38>1 2022-04-29T11:10:21.118410+00:00 OS10 sshd 25205 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) ssh_dispatch_run_fatal: Connection from user admin 10.121.21.4 port 54468: message authentication code incorrect Failed SSH public key authentication: 2023-05-05T08:30:04.770254+00:00 OS10 sshd 17942 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Failed publickey for user.admin from 10.121.21.2 port 56638 ssh2: ECDSA

Requirement	Audit Events	Examples
		SHA256:sc1JbRavLyB+xhOMA3EphUzR7yZdt1kOhnzEIo5iDk4 2023-05-05T08:30:04.770254+00:00 OS10 sshd 17942 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) error: maximum authentication attempts exceeded for user.admin from 10.121.21.2 port 56638 ssh2 [preauth] 2023-05-05T08:30:04.770254+00:00 OS10 sshd 17942 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Disconnecting authenticating user user.admin 10.121.21.2 port 56638: Too many authentication failures [preauth]
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Bad certificate type: 2022-04-29T11:56:41.585960+00:00 OS10 syslog-ng 5876 - [meta sequenceId="10"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Alert ; vers='TLSv1.2 >>> unknown - internal error' <43>1 2022-04-29T11:56:41.585960+00:00 OS10 syslog-ng 5876 - [meta sequenceId="11"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed', location='/etc/syslog-ng/conf.d/remotehost.conf:35:16'
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	The “tally 4” indicates that this was the 4th attempt and the “deny 3” indicate that the login attempts limit has exceeded. Reason for the failure in the 3rd audit message for this event indicates the source of the attempt (IP). 2022-12-09T22:08:36.693546+00:00 OS10 dn_alm 675 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.121.21.2 user=admin 2022-12-09T22:08:47.445277+00:00 OS10 dn_alm 675 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_tally2(sshd:auth): user admin (1002) tally 4, deny 3 2022-12-09T22:11:54.939255+00:00 OS10 dn_alm 675 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session opened for user admin by (uid=0)

Requirement	Audit Events	Examples
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Serial, good password: 2022-05-05T07:37:09.328992+00:00 OS10 audit 6436 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) USER_AUTH pid=6436 uid=0 auid=4294967295 ses=4294967295 subj==unconfined msg='op=PAM:authentication grantors=? acct="admin" exe="/bin/login" hostname=OS10 addr=? terminal=/dev/ttyS0 res=success' Serial, bad password: 2022-05-05T07:37:09.328992+00:00 OS10 audit 6436 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) USER_AUTH pid=6436 uid=0 auid=4294967295 ses=4294967295 subj==unconfined msg='op=PAM:authentication grantors=? acct="admin" exe="/bin/login" hostname=OS10 addr=? terminal=/dev/ttyS0 res=failed' Serial, unknown username: 2022-05-05T07:37:09.328992+00:00 OS10 audit 6436 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) USER_AUTH pid=6436 uid=0 auid=4294967296 ses=4294967296 subj==unconfined msg='op=PAM:authentication grantors=? acct="testadmin" exe="/bin/login" hostname=OS10 addr=? terminal=/dev/ttyS0 res=failed' SSH, good password: 2022-12-21 15:11:37 10.121.21.10 1 2022-12-26T20:50:59.912337+00:00 OS10 sshd 21519 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Accepted password for admin from 172.16.200.30 port 55506 ssh2 SSH, bad password: 2022-05-05T05:50:03.505237+00:00 OS10 dn_alm 672 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.200.10 user=root Unknown user: 2022-05-05 07:16:48.756 OS10 dn_alm[notice]: Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_tally2(sshd:auth): pam_get_uid; no such user
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	

Requirement	Audit Events	Examples
		2022-05-05 07:16:48.757 OS10 dn_alm[notice]: Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:auth): check pass; user unknown 2022-05-05 07:16:52.255 OS10 dn_alm[notice]: Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.200.10
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	General purpose validation error or bad certificate (reason is augmented by examining packet Alert codes): 2022-12-21 17:47:38 10.121.21.10 1 2022-12-27T22:34:07.255929+00:00 OS10 /mgmtsys.py 1273 - - Node.1-Unit.1:PRI [audit], CA certificate failed to install. % Error: Unable to validate CA certificate file - % Error: invalid PEM certificate
	Addition of trust anchor to the trust store	<110>1 2023-08-28T20:54:50.043370+00:00 OS10 .clish 11538 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'crypto ca-cert install home://ca.cert.crt' - completed <110>1 2023-08-28T20:54:53.356274+00:00 OS10 /mgmtsys.py 1068 - - Node.1-Unit.1:PRI [audit], CA certificate with CN = Root CA successfully installed
	Deletion of trust anchor to the trust store	<110>1 2023-08-28T20:54:21.619621+00:00 OS10 .clish 11538 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'crypto ca-cert delete ca.cert' - completed <110>1 2023-08-28T20:54:26.047927+00:00 OS10 /mgmtsys.py 1068 - - Node.1-Unit.1:PRI [audit], CA certificate with CN = Root CA successfully deleted
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	See FPT_TUD_EXT.1 below.
FMT_MOF.1/ Functions	Modification of the behaviour of the transmission of audit data to an external IT entity.	The behaviour of the transmission of audit data to an external IT entity' cannot be modified. The old configuration has to be deleted and a new configuration should be added manually. 2022-05-05T03:31:11.445748+00:00 OS10 dn_etl 696 - - Node.1-Unit.1:PRI [audit], Added remote syslog server successfully

Requirement	Audit Events	Examples
		2022-05-05T03:31:11.654914+00:00 OS10 .clish 5450 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'logging server 10.121.21.2 tls' - completed
FMT_SMF.1	All management activities of TSF data.	All events in this table.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	Updating the firmware is a 4 steps process: Downloading the firmware: 2023-02-25T15:01:15.497449+00:00 OS10 dn_swupgrade 1347 - - Node.1-Unit.1:PRI [audit], Download starting for scp://admin:********@10.121.21.2/~/OS10-Enterprise-installer-x86_64.bin 2023-02-25T15:01:15.787415+00:00 OS10 .clish 4716 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'image download scp://root:*****@10.121.21.2/~/OS10-Enterprise-installer-x86_64.bin' - completed 2023-02-25T15:02:01.410298+00:00 OS10 dn_swupgrade 1347 - - Node.1-Unit.1:PRI [audit], Download complete for file scp://admin:********@10.121.21.2/~/OS10-Enterprise-installer-x86_64.bin. No error Image verification: 2023-02-25T15:05:36.962035+00:00 OS10 dn_swupgrade 1347 - - Node.1-Unit.1:PRI [audit], Verify succeeded: hash of image matches provided hash 2023-02-25T15:05:37.237810+00:00 OS10 .clish 4716 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'image secure-install image://OS10-Enterprise-installer-x86_64.bin sha256 signature 67a1790dca55b8803ad024ee28f616a284df5dd7b8ba5f68b4b252a5e925af79' - completed Installing the firmware: 2023-02-25T15:11:57.923630+00:00 OS10 .clish 4716 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'image secure-install image://OS10-Enterprise-installer-x86_64.bin sha256 signature 67a1790dca55b8803ad024ee28f616a284df5dd7b8ba5f68b4b252a5e925af79' - completed

Requirement	Audit Events	Examples
		2023-02-25T15:12:14.839774+00:00 OS10 dn_swupgrade 1347 - - Node.1-Unit.1:PRI [audit], Installation starting 2023-02-25T15:33:15.634262+00:00 OS10 dn_swupgrade 1347 - - Node.1-Unit.1:PRI [audit], Upgraded standby partition 2023-02-25T15:33:15.635274+00:00 OS10 dn_swupgrade 1347 - - Node.1-Unit.1:PRI [audit], Installation complete Making the installed firmware the boot firmware in the next boot: 2023-02-16T23:48:57.891827+00:00 OS10 dn_swupgrade 1321 - - Node.1-Unit.1:PRI [audit], Set next-boot partition to STANDBY 2023-02-16T23:48:58.201049+00:00 OS10 .clish 25702 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'boot system standby' – completed
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	<30>1 2023-05-02T17:19:21.775708+00:00 dut-host ntpd 14948 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) 0.0.0.0 c012 02 freq_set kernel -16.049 PPM 2022-04-28T17:41:00.819359+00:00 OS10 /mgmtsys.py 1244 - - Node.1-Unit.1:PRI [audit], Current system time changed from Thu May 5 08:47:28 2022 to 2022-04-28T17:41:00Z 2022-04-28T17:41:00.826014+00:00 OS10 .clish 19026 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'clock set 17:41:00 2022-04-28' - completed
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	2022-12-09T03:13:21.268552+00:00 OS10 dn_alm 210 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session closed for user admin 2022-12-09T03:13:21.268552+00:00 OS10 login 12210 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) pam_unix(login:session): session closed for user admin
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	2022-12-09T03:13:21.268552+00:00 OS10 dn_alm 820 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session closed for user admin 2022-12-09T03:13:21.268552+00:00 OS10 sshd 8591 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10)

Requirement	Audit Events	Examples
		Received disconnect from 10.121.21.2 port 14948: reason 11 - disconnected by user 2022-12-09T03:13:21.268552+00:00 OS10 sshd 8591 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Disconnected from user admin 10.121.21.2 port 14948
FTA_SSL.4	The termination of an interactive session.	For Serial: 2022-05-05T03:31:54.717749+00:00 OS10 login 8735 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) pam_unix(login:session): session closed for user admin 2022-05-05T03:31:54.717749+00:00 OS10 .clish 5450 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'exit' – completed 2022-05-05T03:31:54.717749+00:00 OS10 dn_alm 12415 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session closed for user admin For SSH: 2022-12-09T07:45:56.449202+00:00 OS10 sshd 16261 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Received disconnect from 10.121.21.4 port 34626: reason 11: disconnected by user 2022-12-09T07:45:56.449202+00:00 OS10 sshd 16261 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Disconnected from user admin 10.121.21.4 port 34626 2022-12-09T07:45:56.449202+00:00 OS10 .clish 18769 - - Node.1-Unit.1:PRI [audit], User admin on /dev/pts/0 from 10.121.21.4 used cmd: 'exit' - completed 2022-12-09T07:45:56.449202+00:00 OS10 dn_alm 816 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session closed for user admin
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Initiation of the trusted channel: 2022-05-05T03:31:26.823790+00:00 OS10 syslog-ng 5876 - [meta sequenceId="5"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Syslog connection established; fd='25', server='AF_INET(10.121.21.2:514)', local='AF_INET(0.0.0.0:0)' Termination of the trusted channel:

Requirement	Audit Events	Examples
		2022-04-15T05:03:03.232424+00:00 OS10 syslog-ng 3423 - [meta sequenceId="5"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Syslog connection failed; fd='29', server='AF_INET(10.121.21.4:6514)', error='Connection refused (111)', time_reopen='60' Failure of the trusted channel: 2022-01-13T02:30:29.864841+00:00 OS10 syslog-ng 31346 - [meta sequenceId="7"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Syslog connection broken; fd='0', server='AF_INET(10.121.21.4:6514)', time_reopen='60'
FTP_TRP.1/ Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	See FTA_SSL.4 and FCS_SSHS_EXT.1 above.

NOTE:

FTA_SSL.4 logs have the following additional audit log showing the session termination command entered by admin as compared to FTA_SSL_EXT.1 and FTA_SSL.3 logs.

"2022-05-05T03:31:54.717749+00:00 OS10 .clish 5450 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'exit' – completed"