Adtran's FSP 3000R7 Network Element r22.2.2 Supplemental Administrative Guidance for Common Criteria

Version: 1.0
January 12, 2024

Adtran Networks North America, Inc.
(formerly known as Optical Networking North America, Inc)
5755 Peachtree Industrial Boulevard
Norcross, Georgia 30092

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Table of Contents

List of Tables

1 Introduction

The TOE is the Adtran's FSP 3000R7 Network Element operating with software release 22.2.2. In its evaluated configuration, the FSP 3000R7 Network Element is a standalone network device consisting of the Network Control Unit 3 (NCU-3) hardware platform and optional modules for operational network connectivity. The TOE was evaluated against the requirements defined in the FSP 3000R7 Network Element Security Target. The TOE, also referred to as the FSP 3000R7, is an optical network management tool. The product is a scalable optical transport solution that is meant to adapt to the bandwidth demands of the network it is deployed in and ensure secure transfer of data across the network. The TOE does not require additional components in order to fulfill its intended purpose and is a standalone appliance. The TOE consists of both hardware and software. When deployed within a network, the FSP 3000R7 Network Element is utilized as a traffic maintenance tool within the network infrastructure and aligns with the requirements of a network device. Therefore, the FSP 3000R7 Network Element claims conformance to all NDcPP requirements.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating FSP 3000R7 Network Element. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is expected to be familiar with the Security Target for FSP 3000R7 Network Element and the general CC terminology that is referenced in it.

This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions on how to perform only the security functions that are defined by these SFRs. Additionally, this document includes references to FSP 3000R7's standard documentation set for the product which contains functionality that is outside the scope of the evaluation. The FSP 3000R7 product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described in this supplemental document or in the FSP 3000R7 Network Element Security Target was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the FSP 3000R7 Network Element Security Target.

Administrator: A user assigned the 'Administrator' role on the TOE.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Provision: A user assigned the 'Provision' role on the TOE.

Security Administrator: Represents a person that has authorized access to the TOE to perform configuration and management tasks. Assigned either the 'Administrator' or 'Provision' role on the TOE.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of the FSP 3000R7 Network Element that contain the security functions that were tested as part of the CC evaluation process.

4 References

The following documents are part of the FSP 3000R7 Network Element. This is the standard documentation set that is provided with the product.

[1] Adtran's FSP 3000R7 Network Element r22.2.2 Security Target, v1.0 [ST]
[2] Secure System Configuration Guide, Fiber Service Platform 3000R7, Product Release 22.2
[3] Network Element Director, Fiber Service Platform 3000R7, Product Release 22.2
[4] Installation and Commissioning Manual Fiber Service Platform 3000R7

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims:

5.1 TOE Components

The FSP 3000R7 Network Element is a rack-mounted hardware device. The model specific hardware and their configurations are as follows:

		FSP 3000R7 Series			
	PROPERTY	SH1HU	SH7HU	SH9HU	Acronym Definitions
Management Plane	Power	AC/DC/Mix	AC/DC/Mix	AC/DC/Mix	NCU-Network Control Unit PSU/HU-Power Supply Unit/Housing Unit CEM-Common Equipment Module
	Processor	NCU-3 (NXP QorIQ T-Series T1042E)	NCU-3 (NXP QorIQ T-Series T1042E)	NCU-3 (NXP QorIQ T-Series T1042E)	
	Local Console Connection	RJ45 Jack Serial Connector 1 USB Port	RJ45 Jack Serial Connector 1 USB Port	RJ45 Jack Serial Connector 1 USB Port	
	Management Network Connection	3 RJ45 Ethernet	3 RJ45 Ethernet	3 RJ45 Ethernet	
	Size	1 rack unit	7 rack units	9 rack units	
	Module Slots	2	16	16	
	Commons	FAN/1HU, PSU/1HU-AC, PSU/1HU-DC	FAN/Plug-in, PSU/7HU-AC, PSU/7HU-DC	CEM/9HU, FAN/9HU, PSU/9HU-AC, PSU/9HU-DC	

Table 1: TOE Model Specifications Management Plane

		FSP 3000R7 Series			
	PROPERTY	SH1HU	SH7HU	SH9HU	Acronym Definitions
Operational Data Plane	Passive Shelf Accessory	SH1HU/PASSIV E/FT 1 rack unit 4 module slots	SH1HU/PASSIV E/FT 1 rack unit 4 module slots	SH1HU/PASSIV E/FT 1 rack unit 4 module slots	
	Management and Switch Modules	SCU-II, UTM, PSCU, OSCM-PN, HDSCM-PN, OPPM	SCU-II, UTM, PSCU, OSCM-PN, HDSCM-PN, OPPM	SCU-II, OSCM-PN, HDSCM-PN, OPPM	SCU-Shelf Control Unit UTM-Utility Module PSCU-Passive Shelf Control Unit OSCM-Optical Supervisory Channel Module HDSCM-High Density Subshelf Module OPPM-Optical Path Protection Module
	Reconfigurable Optical Modules	4ROADM, MROADM, PSM40, PSM80, 4-OPCM	9ROADM, 4ROADM, MROADM, PSM40, PSM80, 4-OPCM	9ROADM, 4ROADM, MROADM, PSM40, PSM80, 4-OPCM	ROADM-Reconfigurable Optical Add/Drop Module PSM-Power Splitter Module OPCM-Optical Power Control Module
	Optical Amplifiers	GCB, V(L)GC(B), RAMAN, AMP, EDFA, 2EDFA, MA(L)P(B), MTP(B)	GCB, V(L)GC(B), RAMAN, AMP, EDFA, 2EDFA, MA(L)P(B), MTP(B)	GCB, V(L)GC(B), RAMAN, AMP, EDFA, 2EDFA, MA(L)P(B), MTP(B)	EDFA-Erbium Dobed Fiber Amplifier GCB-Gain Controled Balanced V(L)GC(B)-Variable (Low) Gain Controled AMP-EDFA and BWD RAMAN Amplifer Pair MTP(B)-MicroTerminal Pre (Booster) Amplifier MA(L)P(B)-Micro Amplifer (Low) Pre (Booster) Amplifiers
	Access Modules	2WCA, 5WCA, 6WCA	2WCA, 5WCA, 6WCA	2WCA, 5WCA, 6WCA	WCA-Wavelength Converter Module Access
	Core 100G Modules	WCC, 4TCC, 10TCC		WCC, 4TCC, 10TCC	WCC-Wavelength Channel Module Core TCC-TDM Channel Module Core
	Core <100G Modules	2(16)TCC, 2(4)WCC	2(16)TCC, 2(4)WCC	2(16)TCC, 2(4)WCC	
	Enterprise 100G Modules	10TCE		10TCE	TCE-TDM Channel Module Enterprise
	Enterprise <100G Modules	9TCE	9TCE	9TCE	
	Encryption Modules	9TCE+AES, 10TCE+AES, WCC+AES	9TCE+AES	9TCE+AES, 10TCE+AES, WCC+AES	+AES-FIPS 140-2 Encryption
	Dispersion Compensation Modules	DCF, DCG	DCF, DCG	DCF, DCG	DCF-Dispersion Compensation Fiber Modules DGG-Dispersion Compensation Fiber-Bragg_Gratings
	Passive Filter Modules	OSFM(A),(x)PSM, (x)PM, (x)PSM(x), ILM, (x)CSM	OSFM(A),(x)PSM, (x)PM, (x)PSM(x), ILM, (x)CSM	OSFM(A),(x)PSM, (x)PM, (x)PSM(x), ILM, (x)CSM	OSFM(A)-Optical Supervisory Filter Module (integrated ALM/OTC Coupler) PSM-Port Splitter Module PM-Protection Splitter Module ILM-Interleaver Module for

					even/odd channels CSM-Channel Splitter Modules

Table 2: TOE Model Specifications Operational Plane

5.2 Supporting Environment Components

The following table lists components and applications in the TOE's operational environment that must be present for the TOE to be operating in its evaluated configuration:

Component	Definition
Remote Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. For the TOE to be managed remotely the management workstation is required to have: • Supported browser to access the TOE's Web GUI • SSHv2 client installed to access the TOE's CLI The TOE acts as a server for all protocols. TCP communications from the Remote Management Workstation to the TOE is secured using: • SSH for remote access to the CLI • HTTPS for remote access to the Web GUI
Audit Server	The TOE connects to an Audit Server to send the audit records for remote storage via TLS. For this connection the TOE is the TLS client. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
Certificate Authority (CA) Server	A server that acts as a trusted issuer of digital certificates and distributes a CRL that identifies revoked certificates.
NTP Server	The TOE can connect to a NTP Server to maintain accurate timestamps for the TOE and the audit records generated.
OTH or WDM Network	The OTH or WDM Network represents the optical transport hierarchy and wavelength division multiplexing components. There are no SFR's to address the TOE's management of the OTH or WDM Network. Therefore, these components and interfaces to them are out of scope for the NDcPP and the CC evaluation.

Table 3: Supported Components in the Operational Environment

5.3 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Physical security:** The FSP 3000R7 product does not claim any sort of physical tamper-evident or tamper-resistant security mechanisms. Therefore, it is necessary to deploy the product in a locked or otherwise physically secured environment so that it is not subject to untrusted physical modification.
- **Limited functionality:** The FSP 3000R7 product must only be used for its intended networking purpose. General purpose computing applications, especially those with network-visible interfaces, may compromise the security of the product if introduced.
- **No through traffic protection:** The security boundary of the Common Criteria evaluation is limited to traffic flowing to or from the TOE. The intent is for FSP 3000R7 to protect data that originates on or is destined to the device itself, to include administrative data and audit data.

Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).

- **Trusted administration:** The FSP 3000R7 product does not provide a mechanism to protect against the threat of a rogue or otherwise malicious administrator. Therefore, it is the responsibility of the organization to perform appropriate vetting and training for security administrators prior to granting them the ability to manage the product.
- **Regular updates:** Adtran Networks North America, Inc. provides regular product updates for the FSP 3000R7 product that include bug fixes as well as functionality and security enhancements. It is expected that administrators are reasonably diligent in ensuring that software patches are applied regularly as they are made available.
- **Secure admin credentials:** FSP 3000R7 protects the administrator's credentials stored on FSP 3000R7 that are used to access it.
- **Residual information:** It is the responsibility of the administrator to ensure 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.

6 Secure Installation and Configuration

The ability to order and acquire the TOE starts with using the 'Contact Us' section of Adtran's website: www.adtran.com. When receiving delivery of a TOE model, refer to "Unpacking and Inspecting the Equipment" section of document [4]. The 'Deliverable Verification Procedure' section of document [2] can be referenced for secure delivery of the TOE's software. Additionally, this documentation should be checked as part of the acceptance procedures so that the correctness of the hardware can be verified.

6.1 Initial Out-of-the-Box Setup

An administrator can use any general-purpose computer to manage the TOE. Initially the TOE must be administered locally using the local CLI. The local CLI requires the management workstation (local console) to be physically connected to the TOE using the serial port and have a terminal emulator that is compatible with serial communications. Once the initial setup is performed, the TOE can also be managed remotely, in which case the management workstation requires an SSH client to access the remote CLI or a web browser to access the Web GUI.

For more information on the initial out-of-the-box setup procedures refer to document [2].

1. Authenticate to the local CLI using the default credentials:

   Username: ADMIN
   Password: CHGME.1A

   NOTE: During this initial configuration, the TOE forces the user to change the default password to a non-default password. The default password (CHGME.1A) will never be accepted as a valid password in any future attempts to change the password.

2. Enable Enhanced Security Mode:

a. Navigate to “System Security Management” → “Security Settings” → “General”.
b. In the “Security Mode” field, select “Enhanced”.
c. Select “Apply”.

3. Disable disclosure of TOE version information prior to authentication:
   a. Navigate to “System Security Management” → “Security Settings” → “Login”.
   b. Select “Prompt” for the “Login Presentation”.
   c. Select “Apply”

   NOTE: This is the only configuration needed to limit services provided before login.
4. Configure the TOE to prevent local Administrator lockout:
   a. Navigate to “System Security Management” → “Security Settings” → “Login”.
   b. Specify “Account Lockout” to “Allow Lock of All Users”.
   c. Specify “Serial Access Lockout” to “Do Not Lock Admins”.
   d. Select “Apply”.

   NOTE: This configuration will ensure that administrator access will always be maintained and there will not be any temporary lockouts of all administrators.
5. Specify the TOE IP address:
   a. Navigate to “System Management” → “System IP Settings” → “System IP”.
   b. Specify the IP Address.
   c. Select “Apply”.
6. Disable insecure protocols:
   a. Navigate to “System Security Management” → “Security Settings” → “Protocols”.
   b. Verify or set the “Telnet Interface”, “FTP Client”, and “FTP Server” fields to “Disable”.
   c. Select “Apply”.
   d. Navigate to “System Management” → “System General Settings” → “Controls”.
   e. Verify or set the “HTTP Redirect to HTTPS”, “SNMPv1 and v2c”, “SNMPv3”, “TL1 Interface”, and “GNMI Interface” fields to “Disable”.
   f. Select “Apply”.
7. Configure TLS:
   a. Navigate to “System Security Management” → “TLS Configuration” → “General”.
   b. Make sure the “TLS Versions” is set to only “V1_2”.
   c. Make sure the “TLS Ciphers Profile” is set to “CSfC”.
   d. Make sure that the “ECDHE curves Profile” is set to “CSfC”.
   e. Select “Apply”.
8. Configure SSH:
   a. Navigate to “System Security Management” → “SSH Configuration” → “Ciphers” → “General”.
   b. Make sure the “SSH Ciphers Profile” is set to “CSfC”.
   c. Select “Apply”.
9. Enable HTTPS:
   a. Navigate to “System Management” → “System General Settings” → “Controls”.
   b. Verify that the “Web Interface” field is set to “Enable”.
   c. Select “Apply”.
10. Specify the X.509v3 certificate to use for the HTTPS web server:
    a. Navigate to “System Security Management” → “Public Key Infrastructure (PKI)” → “Keys” → “Create private key”.

b. Select one of the available PKI_KEY-# slots.
c. Specify the “Key Algorithm” as “ECDSA”.
d. Select “Next”.
e. Specify the “Key Curve Name” as “secp384r1”.
f. Select “Next”.
g. Specify the “Key Profile” as “Web Services”.
h. Select “Next”, then select “Next”, and then select “Next”.
i. Select “Apply”.
j. Navigate to “System Security Management” → “Public Key Infrastructure (PKI)” → “Certificates”.
k. Select any existing certificates, other than the one that was just created in the previous steps, and then select “Delete”.
l. Confirm the certificate deletion.
m. Select the certificate that was created in the previous steps, then select the “Activate” tab.
n. In the “Activate” field and choose “Activate”.
o. Select “Apply”.

11. Configure audit behavior:
    a. Navigate to “System Security Management” → “Security Settings” → “General”.
    b. Select “Enable” for “Audit Logs”.
    c. Select “Apply”.
12. Configure the failure threshold counter for the ADMIN account:
    a. Navigate to “System Security Management” → “User Management”.
    b. Select the “ADMIN” user and select “Edit”.
    c. Specify the “Login Fail Count” to a value between “1” and “10”.
    d. Select “Apply”.

    NOTE: It is also recommended that one or more additional administrative accounts are made using the directions in Section 7.3.
13. Reboot the TOE:
    a. Navigate to “Reboot NCU”.
    b. Select “OK” to confirm.
14. Using a supported web browser, enter the TOE IP address and authenticate to the Web GUI with the ADMIN user’s credentials.
15. Configure the Ethernet port:
    a. Navigate to “Configure” → “Shelf 1” → “Slot A” → “Ethernet Ports”.
    b. Edit the existing port (e.g., C1).
    c. Specify the “IP Configuration” value to “Unnumbered”.
    d. Select “Apply”.
    e. If the option is unavailable, delete the port.
    f. Re-create the port and then repeat steps d and e.
    g. Reboot the TOE.
16. Using a supported web browser, enter the TOE IP address and authenticate to the Web GUI with the ADMIN credentials.
17. Disable protocols:
    a. Navigate to “Node” → “Controls” → “Interfaces”.
    b. Select “Disable” for the “CP REST Interface” and “NETCONF Interface”.

c. Click “Apply”.

18. Configure the presented certificate validation requirements (syslog):
    a. Navigate to “Node” → “Security” → “Certificate Authorities”.
    b. Add a new Certificate Authority.
    c. Select an available identifier from the drop-down list.
    d. Specify the user label.
    e. Specify the “CRL Method” as “Strict Base CRL (all)”.
    f. Specify the “CRL Update Interval” to preferred value (e.g., “30 Minutes”).
    g. Specify the “Extended Key Usage” as “Required”.
    h. Specify the “Basic Constraints” as “Required”.
    i. Specify the “Subject Name” as “Required”.
    j. Click “Add”.
    k. Navigate to “Node” → “Security Applications” → “Syslog” → “Syslog Secure Connection”.
    l. Specify the Server Authority to the Certificate Authority that was defined in Steps b through j.
    m. Click “Apply”.
19. Generate a certificate for the TOE’s use:
    a. Navigate to “Node” → “Security” → “Certificates & Keys”.
    b. Under “Keys” choose “Add”.
    c. Select an available identifier.
    d. Specify the Key Algorithm as “ECDSA”.
    e. Specify the Key Curve Name as “secp384r1”.
    f. Specify Common Name as the TOE’s IP address.
    g. Choose “Add”.
    h. Specify Renewal Mode as “Manual (CSR only)”.
    i. Select the newly created key corresponding to the identifier from Step c. from the list of keys.
    j. Under the “Key And Certificate Renewal” section, choose “Request”.
    k. Manually have the generated key signed by the CA.
    l. In the “Certificates” area, select the signed key corresponding to the identifier from Step k. from the list of keys.
    m. In the “Configure Details” window, in the “Certificate Activation” area, click “Activate”.
    n. Click “Apply” and “Exit”.
20. Import required CA certificate(s) into the TOE’s CA trust store:
    a. Navigate to “Node” → “Security” → “Certificates & Keys” → “Certificates”.
    b. Add a new certificate.
    c. Select an available identifier from the drop-down list.
    d. Specify the user label.
    e. Paste the Certificate Data (PEM) into the text field.
    f. Choose “Trusted (Root Authority)” for the “Trust Setting”.
    g. Associate the certificate with the corresponding Certificate Authority: PKI_CA-#
    h. Click “Add”.
21. Require TLS Mutual Authentication for Remote Web Administration (TLS/HTTPS):
    a. Navigate to “Node” → “Security” → “Certificate Authorities”.
    b. Choose “Add”.
    c. Specify the “PKI_CA-#” identifier.
    d. Specify the “CRL Distribution Point” for node certificates.

e. Specify the “CRL Method” to “Strict Base CRL (all)”.
f. Specify the “CRL Update Interval” to “30 Minutes”.
g. Choose “Add”.
h. Perform the steps in “Import required CA certificate(s) into the TOE’s CA trust store”.
i. Navigate to “Node” → “Security Applications” → “HTTPS” → “Client Authentication”.
j. Specify the Client Authority to the PKI CA that was created for mutual TLS.
k. Choose “Apply”.
l. Choose “Enable” for “Client Authentication”.
m. Choose “Apply”.

22. Ensure Session Resumption is disabled:
    a. Navigate to “Node” → “Security Applications” → “HTTPS” → “TLS Options”.
    b. Specify “None (Disabled)” for “Session Resumption.

NOTE: The administrator installing the TOE is expected to perform all of the operations in Sections 6.1 of this document. This will result in the TOE’s cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE’s cryptographic engine as these steps will limit the configuration (e.g., ciphersuites and algorithms) to those defined in the Security Target [1] as well as ensure automatic zeroization key destruction functionality. The TOE is not subject to any situations that would prevent or delay key destruction and strictly conforms to the key destruction requirements.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

6.2 Verify Software Version

Once the TOE is initially configured, the administrator needs to verify the TOE is operating the evaluated version (i.e., r22.2.2) of software or a later software release. The currently executing version of the TOE’s software is displayed immediately following successful authentication to each of the administrative interfaces. If the software version needs to be updated, utilize the following steps to upgrade the software:

1. Obtain, verify, and sign software update:
    a. Download the TOE software from the Adtran’s Customer Portal:
    b. Ensure that the software download was successful by verifying that the SHA-256 checksum of the download matches the published checksum.
        i. If the checksums do not match, this could be an indication of software modification or communication errors, and the software needs to be downloaded again.
    c. Extract the contents of the update.
    d. Sign the “F#######RC##.CON” update file by executing the following command:

```
openssl cms -md sha384 -sign -binary -in F#######RC##.CON -
outform DER -out F#######RC##.SIG -signer foo.pem -inkey
foo.pem -nosmimecap
```

NOTE: In the above command, foo.pem needs to be replaced with the name of the CA certificate (PEM format) used to sign the software update.

NOTE: The CA certificate used to sign the software update needs to be uploaded to the TOE following the procedures under Section 6.1, Step 20.

2. Using a supported web browser, enter the TOE IP address and authenticate to the Web GUI with the ADMIN user's credentials.
3. Configure the TOE to perform software update validation:
    a. Navigate to "Node" → "Security" → "Certificate Authorities".
    b. Define a new Certificate Authority.
    c. Specify "Strict Base CRL (all)" for "CRL Method".
    d. Specify "30 Minutes" for "CRL Update Interval".
    e. Under "Certificate Validation Requirements" specify "ECDSA" for "Public Key Algorithm", specify "Required" for "Basic Constraints", "Extended Key Usage".
    f. Click "Add".
    g. Navigate to "Node" → "Security" → "Certificates & Keys".
    h. Import the required certificates to validate the software update.
    i. Mark the imported certificates as Trusted and specify the assigned Certificate Authority to the one defined in Step b.
    j. Navigate to "Node" → "Security Applications" → "SW Install".
    k. Under "Secure Sw Installation", choose "Enable" for "Signature Validation", choose the Certificate Authority defined in Step b for "Software Sign Authority", and ensure "Default (Secure Only)" is selected for SW Install Digest.
4. Ensure the capability to transfer the update to the TOE via the Web GUI upload form is enabled:
    a. Navigate to "Node" → "General" → "Controls" → "Functionality".
    b. Ensure "Upload & Download" is selected for "Local Computer Transfer".
    c. Click "Apply".
5. Perform the following steps to fetch and initiate the TOE software update:
    a. Navigate to "Node" → "Software" → "NCU" → "Transfer Software to Standby Area".
    b. Specify "Local Computer" for "Source Location".
    c. Click the "Import" button and select the following files from the update package:

        E#######RC##.PGM
        F#######RC##.CON
        S#######RC##.PGM
        F#######RC##.SIG

    d. After these files are imported, click "Transfer to Standby".
    e. On the "NCU" page, in the "Activate Software in Standby Area" section, choose "Activate".
6. After the TOE fully reboots, authenticate to the Web GUI and verify that the version number increased to the updated software version by navigating to "Node" → "Software" → "NCU".

6.3 Certificate Validity Checking

The TOE performs certificate validity checking for TLS connections to a remote audit server (audit log transmission) and HTTPS client (remote Web GUI administration) with mutual authentication enabled. In addition to the validity checking that is performed by the TOE, the TOE will validate certificate revocation status using a certificate revocation list (CRL) that the TOE will download automatically from

a Certification Authority in the Operational Environment, based upon the administratively configurable frequency defined in Section 6.1. The TOE determines the validity of certificates by ensuring that the certificate and the certificate path are valid. The TOE also ensures that the extendedKeyUsage field includes the correct purpose for its intended use, which includes Server Authentication for TLS server certificates, Client Authentication for TLS client certificates, and Code Signing for trusted updates. The TOE does not handle certificates associated with OCSP responses.

If a presented certificate is deemed valid, then the TSF will perform certificate revocation checking according to the following rules:

- accept the certificate if the cached CRL is not yet expired and none of the certificates in the certificate chain (including the leaf certificate) are revoked.
- reject the certificate if the cached CRL is not yet expired and if the CRL identifies that any of the certificates in the certificate chain (including the leaf) are revoked. In this case, the TSF produces an audit record that reports an error message identifying the revoked certificate.
- reject the certificate if the cached CRL is expired regardless of the TOE's ability to successfully download a newer CRL from the CRL distribution point (CDP). In this case, the TSF produces an audit record that reports an error message identifying the certificate as invalid due to an expired CRL.

The CRL is cached until the TOE successfully downloads a newer CRL from the CRL distribution point (CDP) or it is manually updated by the administrator, replacing the currently cached value with the one it successfully retrieved. The TSF follows the above rules for determining the revocation status of a certificate chain regardless of the TOE’s ability to connect to the CDP. The TSF does not provide a mechanism to override the validation decision.

NOTE: The TOE does not claim handling certificate validation any differently whether a full certificate chain or only a leaf certificate is being presented.

6.4 TOE Self-Tests

The TOE performs the following self-check procedures before starting the operating system to assure integrity of the filesystem, TOE software, and cryptographic functions.

Standard Linux Filesystem Check:

The TOE performs the following checks of the file system:

- mounts (creates) basic virtual RAM file systems
- verifies and mounts the non-volatile file system
- verifies and mounts the active or standby software partition file system

Failures for any of these checks may result in entering a non-operational state. The TOE is designed to automatically attempt to fix and continue if errors are found.

Software Integrity Check:

The TOE validates software integrity on the filesystem by verifying the current state of the constant files on the root partition against the manifest file that was generated and included in the software as part of the build process. The manifest contains the following information:

- executable binary files
- executable text files (scripts);
- shared libraries
- all constant files on root partition
- SHA-384 hashes for comparison
- Ownership for comparison
- file permissions for comparison

This check will result in errors that indicate an integrity issue with one or more of the TOE's software files. A failure of this check results in the non-operational state.

Cryptographic Check:

The TOE executes Known Answer Tests for the following cryptographic functionalities:

- CTR_DRBG
- AES256-GCM
- Diffie-Hellman Safe Primes Key Generation
- Diffie-Hellman Safe Primes Key Verification
- Diffie-Hellman Safe Primes Shared Secret Computation
- ECDSA Key Generation
- ECDSA Key Verification
- ECDSA Signature Verification
- HMAC-SHA-384
- SHA-384
- SHA-512

Based on FIPS 140-2 methodology, failure of the cryptographic checks will result in the TOE NOT performing any cryptographic services. This check results in errors identifying the failed cryptographic operations. A failure of this check results in the non-operational state.

6.4.1 POST Execution Report

The TOE generates a POST Execution Report which is available to administrators in a dedicated file accessible from a shell, from CLI, or Web GUI. This report will also be sent to the syslog server when the TOE completes its startup. The report contains the following information for each test executed:

- test name or identifier
- test result (success or failure)
- date and time

6.4.2 Non-Operational State

In the non-operational state, the front NCU panel blinks with alternating yellow-red. The system does not provide access via any remote administration interface. However, access to the system can be achieved through a serial RJ45 interface. Upon access, the TOE:

- Provides a POST Execution Report
- Allows access to the system shell

- Allows you to reboot the system
- Allows you to try to reach the operational state

Whenever the TOE enters the non-operational state, the administrator should save the information from the POST Execution Report. The administrator should then attempt to reboot the TOE to determine if rebooting resolves the issue. If rebooting the TOE does not resolve the issue, the administrator should contact Adtran Technical Assistance and provide them details regarding the failed self-tests from the Post Execution Reports.

7 Secure Management of FSP 3000R7

The following sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. Note that this information is largely derived from [3] but summarized here to discuss only the actions that are required as part of the 'evaluated configuration'. The Security Administrator is encouraged to reference this document in full in order to have in-depth awareness of the security functionality of the FSP 3000R7, including functions that may be beyond the scope of this evaluation.

7.1 Authenticating to FSP 3000R7

Users must authenticate to FSP 3000R7 in order to perform any management functions. Section 8.3 of [1] discusses the process in which FSP 3000R7 authenticates users access the TOE via the Local CLI, Remote CLI, or Web GUI. Section 8.7.2 of [1] also discusses the trusted channels that are invoked in order to send the data securely over the remote administrative connections.

When connecting remotely to the TOE's Web GUI via HTTPS, users must authenticate by providing their username/password credentials to the TOE. The TSF then verifies the credentials using a native authentication mechanism. The user must acknowledge the warning banner displayed before the authentication can proceed. The successful verification of the credentials presented to the TOE via HTTPS will provide the user access to all role-based functionality that is assigned to them for the Web GUI.

NOTE: To be able to connect to the TOE, the web browser must support the following:

- Protocol Versions: HTTPS (TLS 1.2)
- Ciphersuites: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Key Establishment Methods: secp384r1

NOTE: The TOE only supports IPv4 addresses in the Common Name (CN) or the Subject Alternative Name (SAN) extension. Thus, the X.509v3 certificate MUST contain an IPv4 address in the CN or SAN extension utilizing the octet format. The TOE does not support the use of wildcards in the CN or SAN.

When connecting to the TOE remotely via an SSH connection to the Remote CLI, users can authenticate by providing their username/password credentials to the TOE. The TOE then verifies the credentials using a native authentication mechanism. Alternatively, the user can authenticate by providing a public-key for validation. The TSF will validate the public-key against the administratively imported and internally stored public-key assigned to that user requesting access. A successful verification of the credentials or public-key presented to the TOE via SSH will provide the user access to all role-based functionality that is assigned to them for the CLI.

NOTE: To be able to connect to the TOE, the SSH2 client must support diffie-hellman-group15-sha512 or ecdh-sha2-nistp384 as the key exchange method, and one or more of the following encryption and data integrity algorithms.

- Encryption Algorithms: aes256-gcm@openssh.com
- Data Integrity Algorithms: keyed-hash message authentication is done implicitly with aes256-gcm@openssh.com

NOTE: The MAC algorithms defined in the ST are the only ones included in the evaluated configuration. If deviating from this configuration, the "none" MAC algorithm is never allowed for SSH.

NOTE: The SSH rekey time and size threshold parameters are not administratively configurable. The TSF enforces the connection to be rekeyed after no longer than one hour, and no more than one gigabyte of transmitted data, whichever threshold is reached first.

When connecting to the TOE locally via a direct connection to the TOE platform, users must authenticate by providing their username/password credentials to the TOE. The TOE then verifies the credentials using a native authentication mechanism. The successful verification of the credentials presented to the TOE via a local connection will provide the user access to all role-based functionality that is assigned to them for the CLI.

7.1.1 Public-Key Based Authentication Configuration

A public/private key pair using ecdsa-sha2-nistp384 must be generated and loaded on the TOE, so that SSH authentication using a public-key is possible. Perform the following steps to add an authorized public-key to a user on the TOE:

1. Authenticate to the TOE via the CLI as an Administrator user.
2. Navigate to "System Security Management" → "SSH Configuration" → "Settings" → "Authorized Keys" → "Add".
3. Specify the applicable SSH Public Key into the "SSH Public Key" field.
4. Select "Apply".
5. Ensure the specified authorized SSH Public Key is associated with the intended user.

NOTE: The SSH Private Key will need to be loaded on the Remote Management Workstation used by the intended user and needs to be accessible to the SSHv2 client.

Perform the following steps to delete an authorized public-key:

1. Authenticate to the TOE via the CLI as an Administrator user.
2. Navigate to "System Security Management" → "SSH Configuration" → "Settings" → "Authorized Keys".
3. Select the applicable SSH Public Key.
4. Select "Delete".

7.2 Failed Authentication Lockout

The TOE provides an administratively configurable counter threshold for consecutive failed password authentication attempts that will lock a user account for a defined period of time when the failure counter threshold is reached. A single failure counter is used, per user, across all interfaces (local, SSH, HTTPS).

The failure counter increases with every failed login attempt, regardless of which interface is used, until the counter reaches its administratively defined threshold. A successful password-based authentication occurring, through any interface, prior to the failure counter reaching its threshold will reset the failure counter to 0.

The failure threshold counter is configured on a per account basis and must be configured to lock a user after 1-10 failed authentication attempts. The default setting of 0 must be changed upon initial configuration of the TOE for the default account of ADMIN and not be used when subsequent user accounts are created. The steps below will allow for the modifying of a user's failure threshold counter:

1. Authenticate to the TOE via the CLI.
2. Navigate to "System Security Management" → "User Management".
3. Select the user and select "Edit".
4. Specify the "Login Fail Count" to a value between "1" and "10".
5. Select "Apply".

Refer to "Adding User Accounts" or "Editing User Accounts" in [3] for directions to setting the failure threshold counter in the Web GUI.

Once a user account has been locked, the user account will automatically unlock after the configured time interval has passed. The Security Administrator can configure the lockout period between 0-99999 seconds. The default lockout time period is globally configured for all administrative interfaces to 86400 seconds (24 hours). The steps below will allow for the modifying the global lockout period:

1. Authenticate to the TOE via the CLI as the Security Administrator.
2. Navigate to "System Security Management" → "Security Settings" → "Login".
3. Specify "Account Lockout Period" to a value between "0" and "99999"
4. Select "Apply".

Refer to "Provisioning Node Security" in [3] for directions to setting the global lockout period in the Web GUI.

Additionally, an administrative account from any interface has the ability to unlock another administrative account in the event of an administrative account reaching the failed authentication attempts threshold. The steps below will allow for the unlocking of an administrative account:

1. Authenticate to the TOE via the CLI.
2. Navigate to "System Security Management" → "User Management".
3. Select the user and select "Edit".
4. Select "Unlock User".
5. Select "OK".

Refer to "Editing User Accounts" in [3] for directions to unlock an administrative account in the Web GUI.

7.3 Managing Users

The TOE support numerous types of user roles. The TOE is designed to use permissions which allow, limit or prevent user access to specific administrative tools based on the aligned user role. Upon successful authentication, the TSF associates the administratively defined set of permissions (role) for that

user to the subject acting on behalf of that user. The TSF then enforces role-based access control (RBAC) to limit access to TSF functions and data based on the set of permissions bound to the subject.

The TOE has two administrative roles for the NDcPP defined management functions:

- Administrator – has the ability to perform all PP defined management functions
- Provision – administrative abilities are limited to updating TOE software

Each user has the following security attributes associated with them:

- Username
- Password
- SSH public key (optional - used for remote CLI login only)
- Role (privilege)
- Login Fail Count – setting which initiates user lockout due to matching successive number of failed authentication attempts

The username and password or SSH public key are for authenticating to the TOE. These credentials are verified using the TOE's local authentication mechanism. Once the username has been validated, the username is used to query the role which has been associated with that username. The TOE then uses the role assigned to the authenticated user to determine if an action is authorized per FSP 3000R7's s role-based access control system.

7.3.1 Create a New Administrative User Account

1. Authenticate to the TOE via the CLI as an Administrator.
2. Navigate to "System Security Management" → "User Management".
3. Select "Add".
4. Specify the username and privilege (role).
5. Select "Next" and then "Next".
6. Specify a password and retype the password.
7. Specify the "Login Fail Count" to a value between "1" and "10".
8. Select "Apply".

Refer to "Adding User Accounts" in [3] for directions to create a new administrative user in the Web GUI.

7.3.2 Modify User Password

The steps below will allow for the changing of a user's own password via the CLI:

1. Authenticate to the TOE via the CLI.
2. Navigate to "System Security Management" → "User Management".
3. Select a user and then select "Edit".
4. Navigate to the "Password" tab.
5. Specify the current password.
6. Specify a new password that conforms to the TOE's password requirements.
7. Confirm new password.
8. Select "Apply".

The steps below will allow for the changing of a user's own password via the Web GUI:

1. Authenticate to the TOE via the Web GUI.
2. Click the account button in the upper right corner.
3. Select "Change Password".
4. Specify the current password.
5. Specify a new password that conforms to the TOE's password requirements.
6. Confirm new password.
7. Select "Apply".

7.4 Password Management

In Enhanced Security Mode, passwords can be composed using any combination of upper case and lower-case letters, numbers and special characters. The special characters that are supported include the following: "!", "@", "#", "$", "%", "^", "(", ")", "_" , "+" , "|" , "~" , "{", " }" , "[" , "]" , "-", and ".".

The password policy includes a configurable minimum length, which can be configured by an Admin user to any value between 15 and 128 in the evaluated configuration.

In order to minimize the risk of account compromise, it is recommended to use a password that includes a mixture of uppercase, lowercase, numeric, and special characters and is not a common word or phrase, but is not so complex that it must be written down in order to be remembered. Password information is never revealed during the authentication process including during login failures.

7.4.1 Configure the Password Length

Perform the following steps to configure the minimum length for passwords:

1. Authenticate to the TOE via the CLI as the Security Administrator.
2. Navigate to "System Security Management" → "Security Settings" → "Login".
3. Specify "Min Password Length" to a value between "15" and "128".
4. Select "Apply".

Refer to "Provisioning Node Security" in [3] for directions to setting the minimum password length in the Web GUI.

7.5 Session Termination

7.5.1 Admin Logout

Any user accessing the TOE is capable of terminating their own session. A Web GUI user may terminate their own sessions by pressing "Logout" under the account button in the top right corner of the screen. A Local and Remote CLI user may terminate their own session by navigating the menu and selecting "Quit".

For all administrative interfaces, a manual user session termination can be verified through the appearance of a login prompt. Once a session has automatically terminated, the user will be required to reauthenticate to the TOE and open a new user session.

7.5.2 Termination from Inactivity

The TOE will automatically terminate a session on the Local CLI and Remote CLI due to inactivity according to an inactivity timer configuration set by the TOE's Security Administrator. The CLI timeout is configured via the following steps:

1. Authenticate to the TOE via the CLI as the Security Administrator.
2. Navigate to "System Security Management" → "Security Settings" → "Timeouts".
3. Specify the "Craft Session Timeout" to a value between "30" and "3600".
4. Select "Apply".

The TOE will automatically terminate a session on the Web GUI due to inactivity according to an inactivity timer configuration set by the TOE's Security Administrator. The Web GUI timeout is configured via the following steps:

1. Authenticate to the TOE via the CLI as the Security Administrator.
2. Navigate to "System Security Management" → "Security Settings" → "Timeouts".
3. Specify the "Web Session Timeout" to a value between "30" and "3600".
4. Select "Apply".

7.6 Login Banner

There are three possible ways to authenticate to the TOE: Local CLI, Remote CLI, and Web GUI. These interfaces have a configurable login banner that is displayed prior to the user authenticating to the TOE. The security banner is created by an Admin user authenticated to the CLI with the following steps:

1. Navigate to "System Security Management" → "Security Settings" → "Login" → "Access Warning".
2. In the "Access Warning" field, select "Enable".
3. In the "Access Warning Message" field, specify a message.
4. Click Apply.

Refer to "Enable Security Banner" in [3] for directions to configure the Login Banner in the Web GUI.

7.7 System Time Configuration

7.7.1 Manual Time Configuration

In the evaluated configuration of the TOE, the system time can be set manually. Only an Administrator can perform this operation by performing the steps below.

1. Authenticate to the TOE via the Web GUI as the Security Administrator.
2. Navigate to "Node" → "General" → "Date & Time".
3. Specify "Disable" for "NTP Operation".
4. Specify the Date (yyyy-mm-dd) and Time (hh:mm:ss on a 24 clock) values.
5. Select "Apply".
6. Select "Cancel".
7. Verify that the date/time value in the lower right corner reflects the expected value.

7.7.2 NTP Server Configuration

In the evaluated configuration of the TOE, the system time can be provided through the use of a NTP Server. Only an Administrator can perform this operation by performing the steps below.

1. Authenticate to the TOE via the Web GUI as the Security Administrator.
2. Navigate to "Node" → "General" → "Date & Time".
3. In the "Date & Time" area, set the time zone for this node.
4. Set the "NTP Operation" field to "Client", and then click "Apply".
5. To add an NTP server, in the "Network Time Protocol (NTP) Servers" area:
    a. Click the add icon
    b. Complete to relevant fields with the NTP Server's information.
    c. Click "Add"
6. Repeat Step 5 for multiple NTP servers. (maximum 3)

NOTE: The TOE only utilizes NTP v4 which does not require configuration.

NOTE: The TOE does not accept broadcast and multicast NTP packets.

The following steps are performed to configure NTP Server Authentication:

1. Authenticate to the TOE via the Web GUI as the Security Administrator.
2. Navigate to "Node" → "General" → "Date & Time".
3. Set the "NTP Operation" field to "Client", and then click "Apply".
4. In the "Network Time Protocol (NTP) Keys" area, click the add icon.
5. In the "Add NTP Key" window:
    a. Complete the relevant fields. The "NTP Digest Algorithm" field must be configured to "SHA-384".
    b. Click Add.
6. In the "Network Time Protocol (NTP) Servers" area:
    a. If applicable, add the NTP server. Refer to the steps above to add an NTP Server.
    b. Left-click on the relevant NTP server.
7. In the "Edit NTP Server" window:
    a. In the "Admin State" field, select "Enabled".
    b. In the "NTP Authentication" field, select "Private Key".
    c. In the "NTP Key Id", select the applicable key id number.
    d. Click "Apply".

Refer to "Synchronizing the Date and Time Using NTP" in [3] for more information on the TOE's NTP configuration settings.

7.8 Secure Updates

To maintain security throughout the lifecycle of the FSP 3000R7 product, the TOE provides a mechanism to apply software upgrades. The following sections describe the steps which must be taken in order to install a new software image.

7.8.1 Display the Current Version

The Web GUI displays the currently executing version of the TOE's software in the header of the Web GUI page in the top left corner of the screen. A Security Administrator can also view the currently executing version of the TOE's software by navigating to the Node's page. Once in the Node's page, a Security Administrator must navigate to the "Software" page in the options tree on the left hand side of the page and click "NCU". The "Active Software Release" tab in the NCU page will display the current executing version of the TOE's software.

For both the Remote CLI (SSH) and the Local CLI, the currently executing version of the TOE's software is displayed in a banner along the top of the options menu screen. This options menu is shown following a Security Administrator's successful authentication to the TOE. A Security Administrator can also view the currently executing version of the TOE's software by navigating through the "System Management" page followed by the "Software & Database Control" page. The software version is available under the "NCU Updates" tab. Additionally, the standby image of the TOE can be viewed on this page under the heading "STBY".

7.8.2 Installing a New Software Image

The TOE does not automatically check for software and firmware updates for the system. The Security Administrator (Administrator or Provision) must download the TOE's update image from the Adtran Customer Portal page to the application server or local workstation. The administrator must use a computer separate from the TOE to recompute the hash of the downloaded image and verify it matches the published hash obtained from the Customer Portal page. Once this validation is complete, the administrator must sign the validated software, using the end user's approved code signing X.509v3 certificate. This creates the trusted update package. The trusted updated package is then placed on the customer's file server. The administrator must import the certificate authority (CA) certificates for the code signing certificate and mark the certificate as trusted.

The administrator must fetch the trusted update package from the application server or local workstation using the Web GUI. Upon downloading, the TSF will validate the package. The TSF validates the package by validating the code signing certificate inside the package, including the CRL revocation checking, and then verifying the digital signature that was applied to software package. The determination to place the code into the standby area is based on the following:

- If the certificate is deemed invalid (e.g., expired or revoked), the image is not installed and is removed from the system.
- If the certificate is deemed valid, the TSF will then validate the digital signature applied to the code:
    - If the digital signature is not valid, the image is not installed and is removed from the system.
    - If the digital signature check succeeds, the software image is placed in the Standby Area.

If the validation fails, the package is deleted from the TOE. If the validation succeeds, at this point the trusted update has been loaded into the standby area where it will reside dormant until the administrator activates that image (delayed activation); which will result in the reboot of the machine. There is no administrative override capabilities to install a package that fails the validation checks.

The following steps provide guidance on performing the software update process using the Web GUI with the software package located on the user's local workstation. Refer to "Managing NCU Software" in [3] for more information and options (e.g., transfer from an application server) with the software update process.

1. Obtain, verify, and sign software update:
    a. Download the TOE software from the Adtran's Customer Portal:
    b. Ensure that the software download was successful by verifying that the SHA-256 checksum of the download matches the published checksum.
        i. If the checksums do not match, this could be an indication of software modification or communication errors, and the software needs to be downloaded again.
    c. Extract the contents of the update.
    d. Sign the "F#######RC##.CON" update file by executing the following command:

```
openssl cms -md sha384 -sign -binary -in F#######RC##.CON -
outform DER -out F#######RC##.SIG -signer foo.pem -inkey
foo.pem -nosmimecap
```

    NOTE: In the above command, foo.pem needs to be replaced with the name of the CA certificate (PEM format) used to sign the software update.
    NOTE: The CA certificate used to sign the software update needs to be uploaded to the TOE following the procedures under Section 6.1, Step 20.
2. Authenticate to the Web GUI as a Security Administrator.
3. Ensure the capability to transfer the update to the TOE via the Web GUI upload form is enabled:
    a. Navigate to "Node" → "General" → "Controls" → "Functionality".
    b. Ensure "Upload & Download" is selected for "Local Computer Transfer".
    c. Click "Apply".
4. Perform the following steps to fetch and initiate the TOE software update:
    a. Navigate to "Node" → "Software" → "NCU" → "Transfer Software to Standby Area".
    b. Specify "Local Computer" for "Source Location".
    c. Click the "Import" button and select the following files from the update package:

        E#######RC##.PGM
        F#######RC##.CON
        S#######RC##.PGM
        F#######RC##.SIG

    d. After these files have been selected for import, click "Transfer to Standby".
        i. At this time, certificate validation occurs. If certificate validation fails, verify the CA certificate has been loaded on the TOE using steps from Section 6.2. Then repeat all procedures in Section 7.8.2

    On the "NCU" page, in the "Activate Software in Standby Area" section, choose "Activate". This will cause an automatic reboot of the TOE.

5. After the TOE fully reboots, authenticate to the Web GUI as a Security Administrator and verify that the version number increased to the updated software version by navigating to "Node" → "Software" → "NCU".

8 Auditing

In order to be compliant with Common Criteria, FSP 3000R7 must audit the events in Table 4. The audit records that FSP 3000R7 creates include the date and time, outcome of the event, event type, subject identity and the source of the event.

Local auditing is configured on via the steps outlined in Section 6.1. The Logs page displays audit information. The Logs page provides a search function that allows a user to filter the events by entering all or part of the information of interest. Events can be additionally filtered by a date range.

The right most column in Table 4 provides examples for each audit event for which the TOE needs to produce a record. The following is an example of an audit record to describe the contents of the records:

> **192.168.1.75 WDM[5552] 893 2023-05-08T20:55:25.20Z LOGIN: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SERIAL, SESSION_ID=ttyS0**

The following are the fields for this audit record:

- **192.168.1.75** = This is the IP address of the TOE (i.e., source) that recorded the event.
- **WDM[5552]** = This is the session thread for the event.
- **893** = This is an identifier for that unique event.
- **2023-05-08T20:55:25.20Z** = This is the date and time the event occurred.
- **LOGIN: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SERIAL, SESSION_ID=ttyS0 =** This is the event message that will provide different details depending on the type of event. This event's details indicate the type of event (LOGIN), outcome (success), and subject identity (ADMIN). Additionally, this event's message includes session information regarding the connection to the TOE.

Note that in the case of start-up and shut-down of the audit functions, the audit records have the same contents, but the information is provided in a different format:

> **2023-09-25.log:Sep 25 15:30:15 192.168.1.75 WDM[6502] 2729 DEST-SYSLOG-192.168.1.76 NA ADMIN LCT Edit {"SYSLOG":"ENABLE"}**

The following are the fields for this audit record:

- **2023-09-25.log:Sep 25 15:30:15**
- **192.168.1.75** = This is the IP address of the TOE (i.e., source) that recorded the event.
- **WDM[6502]** = This is the session thread for the event.
- **2729** = This is an identifier for that unique event.
- **DEST-SYSLOG-192.168.1.76 NA ADMIN LCT Edit {"SYSLOG":"ENABLE"} =** This event's details indicate the type of event (start-up of audit functions), outcome (success), and subject identity (ADMIN).

Auditable Event	Sample Data
Start-up and shut-down of the audit functions	**Start-up of audit functions** 2023-09-25.log:Sep 25 15:30:15 192.168.1.75 WDM[6502] 2729 DEST-SYSLOG-192.168.1.76 NA ADMIN LCT Edit {"SYSLOG":"ENABLE"} **Shut-down of audit functions** 2023-09-25.log:Sep 25 16:13:13 192.168.1.75 WDM[6502] 0 DEST-SYSLOG-192.168.1.76 NA ADMIN LCT Edit {"SYSLOG":"DISABLE"}
Administrative login and logout	**Local Console Successful Login using Password** 192.168.1.75 WDM[5552] 893 2023-05-08T20:55:25.20Z LOGIN: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SERIAL, SESSION_ID=ttyS0 **Local Console Failed Login using Password** 192.168.1.75 WDM[5841] 19324 2023-08-30T18:05:24.90Z LOGIN (fail): STATUS=AUTH-ERR, USER=ADMIN, PROTOCOL=SERIAL **Local Console Logout** 192.168.1.75 WDM[5552] 894 2023-05-08T20:55:26.35Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SERIAL, SESSION_ID=ttyS0 **Remote SSH Successful Login using Password** 192.168.1.75 WDM[5845] 27142 2023-09-08T15:09:13.34Z AUDIT: USER=ADMIN, ACCESS=LOCAL, OPERATION=SSH-AUTH-PASSWORD, SRC_IP=192.168.1.98, PORT=23012, PROCESS=sshd, PID=16962 192.168.1.75 WDM[5845] 27143 2023-09-08T15:09:13.36Z AUDIT: OPERATION=SSH-CHANNEL-ESTABLISH, SRC_IP=192.168.1.98, PORT=23012, PROCESS=sshd, PID=16970 **Remote SSH Failed Login using Password** 192.168.1.75 WDM[5845] 27186 2023-09-08T15:32:39.65Z AUDIT (fail): STATUS=FAIL, USER=ADMIN, ACCESS=LOCAL, OPERATION=SSH-AUTH-PASSWORD, SRC_IP=192.168.1.98, PORT=23020, PROCESS=sshd, PID=18468 192.168.1.75 WDM[5845] 27187 2023-09-08T15:32:39.65Z LOGIN (fail): STATUS=AUTH-ERR, USER=ADMIN, PROTOCOL=SSH, SRC_IP=192.168.1.98 **Remote SSH Successful Login using Public Key** 192.168.1.75 WDM[5841] 19354 2023-08-30T18:10:23.80Z AUDIT: USER=ADMIN, ACCESS=LOCAL, OPERATION=SSH-AUTH-PUBKEY, SRC_IP=192.168.1.98, PORT=12090, PROCESS=sshd, PID=18965, INFO=ECDSA SHA256:RPZzbFJBbvvMPqqqgyfZTNCSGF35EuiHjMcBxC8qaas 192.168.1.75 WDM[5841] 19355 2023-08-30T18:10:23.81Z AUDIT: OPERATION=SSH-CHANNEL-ESTABLISH, SRC_IP=192.168.1.98, PORT=12090, PROCESS=sshd, PID=18971 **Remote SSH Failed Login using Public Key** 192.168.1.75 WDM[5718] 4741 2023-06-20T20:52:26.76Z AUDIT (fail): STATUS=FAIL, USER=ADMIN, ACCESS=LOCAL, OPERATION=SSH-AUTH-PUBKEY, SRC_IP=192.168.1.102, PORT=2461, PROCESS=sshd, PID=18205, INFO=ECDSA SHA256:MneCLdX58ER7zIAaQVcGD?b1nbZguJraM3vCxe/GQHw **Remote SSH Logout** 192.168.1.75 WDM[5845] 27571 2023-09-08T18:53:49.35Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SSH, SRC_IP=192.168.1.98, SESSION_ID=pts/0

	Remote Web GUI Successful Login using Password 192.168.1.75 WDM[5841] 19450 2023-08-30T18:25:10.41Z LOGIN: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=HTTPS, SRC_IP=192.168.1.98, SESSION_ID=web/0 **Remote Web GUI Failed Login using Password** 192.168.1.75 WDM[5841] 19461 2023-08-30T18:26:02.04Z LOGIN (fail): STATUS=AUTH-ERR, USER=ADMIN, PROTOCOL=HTTPS, SRC_IP=192.168.1.98 **Remote Web GUI Logout** 192.168.1.75 WDM[5843] 32602 2023-09-18T13:13:28.17Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=HTTPS, SESSION_ID=web/1
Security related configuration changes	**Administrator configured login banner** 192.168.1.75 WDM[6500] 2858 2023-10-18T17:20:14.22Z NE NA ADMIN LCT Edit {"ACCESS_WARNINGMSG":"FTA_TAB.1 - WARNING", "ACCESS_WARNING":"ENABLE"} **Manual setting of system time** 192.168.1.75 WDM[6514] 2203 2023-09-08T18:17:13.22Z TIME-NTP NA ADMIN LCT Edit {"NTPMODE":"NTP-OFF"} 192.168.1.75 WDM[5845] 27527 2023-09-08T15:10:15.00Z NOTIFY: Time Change, USER=ADMIN, ACCESS=LOCAL 192.168.1.75 WDM[6514] 108844 2023-09-08T18:17:40.43Z TIME-NTP TIMECHG NA NSA n/a {"TIME":"11-10-13", "TIMECHG-REASON":"MANUAL-CHANGE", "DATE":"23-09-08", "TIME-ZONE":"USEastern", "TZOFFSET":"-18000", "DST":"Y"} **Failure Authentication Threshold** 192.168.1.75 WDM[5845] 27723 2023-09-08T19:30:46.31Z EDIT_USER: USER=ADMIN, ACCESS=LOCAL, TARGET_USER=admin2, LOGIN_FAIL_COUNT=4 **Automatic unlock time** 192.168.1.75 WDM[6514] 2223 2023-09-08T19:33:07.73Z NE NA ADMIN LCT Edit {"UNLOCK-TIME":"60"} **Manual unlock of account** 192.168.1.75 WDM[5845] 27746 2023-09-08T19:32:00.74Z EDIT_USER: USER=ADMIN, ACCESS=LOCAL, TARGET_USER=admin2, ACCOUNT_STATE=UNLOCK **Idle Session Timeout Threshold SSH** 192.168.1.75 WDM[6500] 2870 2023-10-25T14:20:51.15Z NE NA ADMIN LCT Edit {"SSH_LOG-TMOUT":"180"} **Idle Session Timeout Threshold Web GUI** 192.168.1.75 WDM[6500] 2859 2023-10-18T18:08:36.68Z NE NA ADMIN LCT Edit {"WEBGUI_SESS-TMOUT":"60"} **Idle Session Timeout Threshold Local Console** 192.168.1.75 WDM[6501] 2668 2023-09-25T13:38:17.26Z NE NA ADMIN LCT Edit {"CRAFT_SESS-TMOUT":"60"}

Generating/import of, changing, or deleting of cryptographic keys	**Generation of a key** 192.168.1.75 WDM[6514] 2225 2023-09-12T13:40:58.82Z PKI_KEY-3 NA ADMIN LCT Enter {"ALIAS":"", "KEY-ALGORITHM":"ECDSA", "KEY-LENGTH":"NONE", "KEY-CURVE-NAME":"SECP384R1", "KEY-STORAGE":"NCU", "KEY-EXPORTABLE":"NO", "KEY-PROFILE":"WEB", "CERT-RENEW-MODE":"AUTOMATIC", "CERT-RENEW-INTERVAL":"30-DAY", "CERT-EXP-WARN-PERIOD":"NONE", "AUTO-CLEANUP":"ENABLE", "CERT-RENEW-RETRY-COND":"ANY", "CERT-RENEW-RETRY-INTERVAL":"1-HOUR", "CERT-RENEW-RETRY-LIMIT":"USER", "CERT-RENEW-RETRY-LIMIT-USER":"3", "CERT-COMMON-NAME":"FSP 3000R7", "CERT-EQPT-SERNO":"", "CERT-ALT-NAME-IP":"0.0.0.0", "CERT-ALT-NAME-DNS":"nemi", "CERT-KEY-USAGE-LIST":"NONE", "CERT-EXT-KEY-USAGE-LIST":"SERVER-AUTH", "CERT-VALID-PERIOD":"825-DAY", "CERT-REQ-CHALLENGE":"", "CERT-TEMPLATE-NAME":"", "CA-AID":"NONE", "CERT-AID-LIST":"NONE", "BACKUP-KEY-AID":"NONE"} 192.168.1.75 WDM[6514] 111354 2023-09-12T13:40:58.98Z PKI_KEY-3 KEY-GEN-PENDING NA NSA Set {} 192.168.1.75 WDM[6514] 111355 2023-09-12T13:40:58.98Z PKI_KEY-3 KEY-GEN-START NA NSA n/a {} 192.168.1.75 WDM[6514] 111356 2023-09-12T13:40:59.38Z PKI_KEY-3 KEY-GEN-COMPL NA NSA n/a {"FINGERPRINT-SHA256":"a9:c8:45:7a:a4:04:67:9b:0c:71:a9:26:a8:6e:36:ef:10:4b:28:0f:d3:b0:69:be:1a:7b:53:51:71:a0:6a:da", "KEY-GEN-STATUS":"OK", "PRIVKEY-STORAGE-PATH":"", "PRIVKEY-STORAGE-ID":""} 192.168.1.75 WDM[6514] 111357 2023-09-12T13:40:59.44Z PKI_KEY-3 KEY-GEN-PENDING NA NSA Clear {} 192.168.1.75 WDM[6514] 111358 2023-09-12T13:40:59.95Z PKI_KEY-3 CERT-REQ-PENDING NA NSA Set {} 192.168.1.75 WDM[6514] 111359 2023-09-12T13:41:00.12Z PKI_KEY-3 CERT-REQ-START NA NSA n/a {} **Storage of Certificate** 192.168.1.75 WDM[6514] 2226 2023-09-12T13:41:00.68Z PKI_CERT-1 NA system SYSTEM Enter {"ALIAS":"", "CERT-TYPE-LIST":"SELF-SIGNED&END-ENTITY", "FINGERPRINT-SHA256":"a1:6d:b3:d7:09:a4:5d:e8:bc:b8:64:3c:bc:00:9c:6b:69:e2:39:54:6f:2b:c9:31:18:21:fc:be:68:b1:e0:0e", "AUTO-CLEANUP":"DISABLE", "CERT-PURPOSE":"WEB", "CERT-TRUST":"END-ENTITY", "CERT-UCID-FORMAT-LIST":"NONE", "CERT-ISSUER":"/CN=FSP 3000R7", "CERT-SERNO":"29F9E28CC947D069FB424E26E6B9841F41E61C82", "CERT-SUBJECT":"/CN=FSP 3000R7", "CERT-COMMON-NAME":"FSP 3000R7", "CERT-EQPT-SERNO":"", "CERT-VALID-FROM":"23-09-12,13:41:00", "CERT-VALID-FROM-LOCAL":"23-09-12,09:41:00", "CERT-VALID-TO":"25-12-15,13:41:00", "CERT-VALID-TO-LOCAL":"25-12-15,08:41:00", "CERT-SIGNATURE-ALGORITHM":"SHA256", "CERT-ALT-NAME-DNS-LIST":"nemi", "CERT-EXT-KEY-USAGE-LIST":"SERVER-AUTH", "CERT-BASIC-CONSTRAINTS":"CA:FALSE", "KEY-ALGORITHM":"ECDSA", "KEY-LENGTH":"NONE", "KEY-CURVE-NAME":"SECP384R1", "CA-AID":"NONE", "KEY-AID-LIST":"PKI_KEY-3"} 192.168.1.75 WDM[6514] 111360 2023-09-12T13:41:01.86Z PKI_KEY-3 CERT-REQ-COMPL NA NSA n/a {"CERT-RENEW-RETRY-LIMIT":"USER", "CERT-RENEW-RETRY-LIMIT-USER":"3", "CERT-RENEW-RETRY-COUNT":"0", "CERT-REQ-STATUS":"OK", "CERT-AID-LIST":"PKI_CERT-1", "LATEST-CERT-AID":"PKI_CERT-1"}

	192.168.1.75 WDM[6514] 111361 2023-09-12T13:41:02.36Z PKI_KEY-3 CERT-REQ-PENDING NA NSA Clear {} **Import X.509 Certificate** 192.168.1.75 WDM[6530] 1983 2023-09-01T17:15:13.14Z PKI_CERT-11 NA ADMIN LCT Enter {"ALIAS":"int01CA_exp", "CERT-TYPE-LIST":"CA", "FINGERPRINT-SHA256":"e3:b0:e5:31:ff:a2:cf:7e:ee:82:fa:93:97:1b:4d:c7:58:d5:84:d6:20:8a:c0:cd:b9:0a:b8:23:bd:5d:57:f0", "AUTO-CLEANUP":"DISABLE", "CERT-PURPOSE":"CA", "CERT-TRUST":"TRUSTED-CA", "CERT-UCID-FORMAT-LIST":"NONE", "CERT-ISSUER":"/C=US/ST=Maryland/L=Laurel/O=Booz Allen/OU=CATL/CN=rootCA_384_exp", "CERT-SERNO":"01", "CERT-SUBJECT":"/C=US/ST=Maryland/O=Booz Allen/OU=CATL/CN=int01CA_384_explicit", "CERT-COMMON-NAME":"int01CA_384_explicit", "CERT-EQPT-SERNO":"", "CERT-VALID-FROM":"23-09-01, 13:05:00", "CERT-VALID-FROM-LOCAL":"23-09-01, 17:05:00", "CERT-VALID-TO":"33-08-29,17:05:00", "CERT-VALID-TO-LOCAL":"33-08-29,13:05:00", "CERT-SIGNATURE-ALGORITHM":"SHA384", "CERT-KEY-USAGE-LIST":"SIGN&CERT-SIGN&CRL-SIGN&CRITICAL", "CERT-BASIC-CONSTRAINTS":"CA:TRUE, pathlen:1, Critical", "KEY-ALGORITHM":"ECDSA", "KEY-LENGTH":"NONE", "KEY-CURVE-NAME":"secp384r1", "CA-AID":"PKI_CA-3", "KEY-AID-LIST":"NONE"} **Import SSH public key for a user** 192.168.1.75 WDM[5841] 19342 2023-08-30T18:09:27.44Z ADD_KEY: USER=ADMIN, ACCESS=LOCAL, KEY-ALGORITHM=ECDSA, KEY-LENGTH=384, FINGERPRINT-STR=SHA256:RPZzbFJBbvvMPqqqgyfZTNCSGF35EuiHjMcBxC8qaas, ALIAS=catl@DESKTOP-7P0THJ7 **Delete X.509 Certificate** 192.168.1.75 WDM[5845] 27406 2023-09-08T17:09:27.32Z DELETE_KEY: USER=ADMIN, ACCESS=LOCAL, KEY-ALGORITHM=ECDSA, KEY-LENGTH=384, FINGERPRINT-STR=SHA256:RPZzbFJBbvvMPqqqgyfZTNCSGF35EuiHjMcBxC8qaas, ALIAS=catl@DESKTOP-7P0THJ7
Resetting passwords	**Successful password change** 192.168.1.75 WDM[5845] 28676 2023-09-12T13:10:36.29Z EDIT_USER: USER=admin2, ACCESS=LOCAL, TARGET_USER=admin2, PASSWORD=???????? **Unsuccessful password change** 192.168.1.75 WDM[5845] 28764 2023-09-12T13:33:12.66Z EDIT_USER (fail): STATUS=FAIL, USER=admin2, ACCESS=LOCAL, TARGET_USER=admin2, PASSWORD=????????
Configuration of a new time server	192.168.1.75 WDM[6446] 1587 2023-08-07T22:23:48.15Z NTPKEY-NTP-1 NA ADMIN LCT Enter {"NTPKEY":"", "NTPKEY-ID":"1", "NTPDIGEST-ALGORITHM":"SHA384"} 192.168.1.75 WDM[6446] 1590 2023-08-07T22:24:11.02Z NTPSRV-NTP-192.168.1.77 NA ADMIN LCT Enter {"ADMIN":"IS", "SRCIP":"SYS-IP", "NTPSYNC":"NO_DATA", "NTPAUTH-TYPE":"PRIVATE-KEY", "NTPKEY-ID":"1"}
Removal of configured time server	192.168.1.75 WDM[6446] 1600 2023-08-07T22:39:39.24Z TIME-NTP NA ADMIN LCT Edit {"NTPMODE":"NTP-OFF"} 192.168.1.75 WDM[6446] 77987 2023-08-07T22:39:40.03Z NTPSRV-NTP-192.168.1.78 NTPAUTH-FAIL MJ NSA Clear {}
Failure to establish a HTTPS Session (HTTPS Server)	See ‘Failure to establish a TLS session (TLS Server)’

Failure to establish an SSH session (SSH Server)	192.168.1.75 WDM[5845] 27176 2023-09-08T15:25:03.70Z AUDIT: OPERATION=TCP-OPEN, SRC_IP=192.168.1.98, PORT=23018, PROCESS=sshd, PID=6245 192.168.1.75 WDM[5845] 27177 2023-09-08T15:25:03.93Z AUDIT (fail): STATUS=FAIL, OPERATION=SSH-CHANNEL-REKEY, SRC_IP=192.168.1.98, PORT=23018, PROCESS=sshd, PID=17992, INFO=Unable to negotiate with 192.168.1.98 port 23018: no matching host key type found. Their offer: ssh-rsa 192.168.1.75 WDM[5845] 27178 2023-09-08T15:25:03.94Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=23018, PROCESS=sshd, PID=17991
Failure to establish a TLS session (TLS Client)	192.168.1.75 WDM[5843] 41110 2023-07-26T16:44:33.57Z AUDIT (fail): STATUS=FAIL, OPERATION=TLS-CHANNEL-ESTABLISH, SRC_IP=192.168.1.76, PORT=6514, PROCESS=rsyslogd, PID=10498, INFO=wrong certificate type
Failure to establish a TLS session (TLS Server)	192.168.1.75 WDM[5841] 19527 2023-08-30T18:46:10.12Z AUDIT (fail): STATUS=FAIL, OPERATION=WEB-TLS-OPEN, SRC_IP=192.168.1.98, PORT=12199, PROCESS=nginx, PID=27750, INFO=certificate not provided
Unsuccessful login attempts limit is met or exceeded.	192.168.1.75 WDM[5845] 27735 2023-09-08T19:31:24.72Z EDIT_USER: USER=admin2, ACCESS=LOCAL, ACCOUNT_STATE=LOGIN_RETRIES_LOCK
All use of the identification and authentication mechanism	See ‘Administrative login and logout’
Unsuccessful attempt to validate a certificate	**Issuer Certificate Failed** 192.168.1.75 WDM[5761] 9870 2023-07-26T17:32:40.00Z AUDIT (fail): STATUS=FAIL, OPERATION=CERT-VERIFY, SRC_IP=192.168.1.98, PORT=7166, PROCESS=nginx, PID=21698, INFO=SUBJECT: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:192.168.1.98, ISSUER: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:int02CA, FINGERPRINT-SHA256: e5:42:6d:91:28:26:4c:21:f7:d5:62:3a:67:a4:70:fe:4f:f5:60:c9:b8:65:84:f3:08:89:fa:e6:dd:1e:cc:78,SIGNATURE-ALGORITHM: ecdsa-with-SHA384, SERIAL-NUMBER: 07, REASON: certificate signature failure **Certificate Expired** 192.168.1.75 WDM[5761] 10030 2023-07-26T20:24:09.31Z AUDIT (fail): STATUS=FAIL, OPERATION=CERT-VERIFY, SRC_IP=192.168.1.98, PORT=7206, PROCESS=nginx, PID=21892, INFO=SUBJECT: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:192.168.1.98, ISSUER: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:int02CA, FINGERPRINT-SHA256: ff:1c:83:b4:37:bf:05:cc:46:75:e6:9d:34:f3:37:9b:71:b6:8e:e5:47:f8:3a:06:40:af:66:e8:6e:7e:b5:ab,SIGNATURE-ALGORITHM: ecdsa-with-SHA384, SERIAL-NUMBER: 17, REASON: certificate has expired **Certificate Revoked** 192.168.1.75 WDM[5780] 11232 2023-07-27T15:36:20.96Z AUDIT (fail): STATUS=FAIL, OPERATION=CERT-VERIFY, SRC_IP=192.168.1.98, PORT=7576, PROCESS=nginx, PID=28104, INFO=SUBJECT: /C:US/ST:Maryland/O:Booz Allen/OU:CATL/CN:int01CA, ISSUER: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:rootCA, FINGERPRINT-SHA256: 72:31:65:a1:d7:a0:56:6b:c4:87:2a:e6:fe:63:02:47:02:cb:1a:4e:ea:b9:31:a6:b1:63:0f:ff:56:d1:95:22,SIGNATURE-ALGORITHM: ecdsa-with-SHA512, SERIAL-NUMBER: 01, REASON: certificate revoked **Missing CRL signing** 192.168.1.75 WDM[5861] 19895 2023-08-30T22:18:26.71Z AUDIT (fail): STATUS=FAIL, OPERATION=CERT-VERIFY, SRC_IP=192.168.1.98, PORT=12739, PROCESS=nginx, PID=15364, INFO=SUBJECT: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:192.168.1.98, ISSUER: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:int02CA_384_noCRLSign, FINGERPRINT-SHA256: f0:4d:ea:4b:d0:36:2e:6f:69:c8:41:e5:ce:31:96:97:20:69:92:8d:e3:56:83:27:76:c7:19:60:70:3

	6:38:41,SIGNATURE-ALGORITHM: ecdsa-with-SHA384, SERIAL-NUMBER: 09, REASON: key usage does not include CRL signing **Invalid CA** 192.168.1.75 WDM[5763] 12337 2023-07-27T19:53:57.87Z AUDIT (fail): STATUS=FAIL, OPERATION=CERT-VERIFY, SRC_IP=192.168.1.98, PORT=7874, PROCESS=nginx, PID=27557, INFO=SUBJECT: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:int02_nobasic, ISSUER: /C:US/ST:Maryland/O:Booz Allen/OU:CATL/CN:int01CA, FINGERPRINT-SHA256: 6b:b7:ec:17:59:73:0e:1e:be:4d:93:b0:00:4c:b8:31:12:82:fd:d7:ed:07:22:de:ee:35:80:a6:e6:7b:46:06,SIGNATURE-ALGORITHM: ecdsa-with-SHA384, SERIAL-NUMBER: 05, REASON: invalid CA certificate
Any addition, replacement or removal of trust anchors in the TOE's trust store	See 'Generating/import of, changing, or deleting of cryptographic keys'
Any attempt to initiate a manual update	See 'Initiation of update; result of the update attempt'
All management activities of TOE's Security Functionality data	See 'Security related configuration changes'
Discontinuous changes to time – either Administrator actuated or changed via an automated process	192.168.1.75 WDM[6514] 107523 2023-09-06T19:10:28.97Z TIME-NTP NTPNSYNC MJ NSA Set {"TIME":"15-10-28", "DATE":"23-09-06", "TIME-ZONE":"USEastern", "TZOFFSET":"-18000", "DST":"Y"} 192.168.1.75 WDM[6514] 2178 TIME-NTP NA ADMIN LCT Edit {"NTPMODE":"CLIENT-ONLY"} 192.168.1.75 WDM[6514] 107524 2023-09-06T19:10:35.00Z TIME-NTP TIMECHG NA NSA n/a {"TIME":"15-21-47", "DATE":"23-09-06", "TIMECHG-REASON":"STEP-CORRECTION", "TIME-ZONE":"USEastern", "TZOFFSET":"-18000", "DST":"Y"}
Initiation of update; result of the update attempt (success or failure)	**Initiation of update** 192.168.1.75 WDM[5763] 16634 2023-08-23T13:18:55.87Z NOTIFY: Software Install, USER=ADMIN, ACCESS=LOCAL **Result of the update attempt (Success)** 192.168.1.75 WDM[6420] 86910 2023-08-23T13:18:56.27Z SRV-UBR CPY-MEM-PRTL NA NSA n/a {"FILE":"F7022022RC03.CON"} 192.168.1.75 WDM[6420] 1635 2023-08-23T13:18:56.31Z PKI_CERT-15 NA SYSTEM Enter {"ALIAS":"", "CERT-TYPE-LIST":"END-ENTITY", "FINGERPRINT-SHA256":"88:c1:7a:f4:29:93:1d:d6:cb:67:1e:48:92:ad:ca:5b:3d:0d:39:9e:cb:92:c8:b2:3e:16:13:a9:c9:4d:97:32", "AUTO-CLEANUP":"DISABLE", "CERT-PURPOSE":"SW-SIGN", "CERT-TRUST":"END-ENTITY", "CERT-UCID-FORMAT-LIST":"NONE", "CERT-ISSUER":"/C=US/ST=Maryland/L=Laurel/O=Booz Allen/OU=CATL/CN=int02CA", "CERT-SERNO":"03", "CERT-SUBJECT":"/C=US/ST=Maryland/L=Laurel/O=Booz Allen/OU=CATL/CN=ADVA-codesign", "CERT-COMMON-NAME":"ADVA-codesign", "CERT-EQPT-SERNO":"", "CERT-VALID-FROM":"23-08-23,13:14:34", "CERT-VALID-FROM-LOCAL":"23-08-23,09:14:34", "CERT-VALID-TO":"33-08-20,13:14:34", "CERT-VALID-TO-LOCAL":"33-08-20,09:14:34", "CERT-SIGNATURE-ALGORITHM":"SHA384", "CERT-KEY-USAGE-LIST":"SIGN&KEY-ENC&CRITICAL", "CERT-EXT-KEY-USAGE-LIST":"CODE-SIGN", "CERT-BASIC-CONSTRAINTS":"CA:FALSE", "CERT-CDP-URL-LIST":"http://192.168.1.74/_crl/intermediate2.crl", "KEY-ALGORITHM":"ECDSA", "KEY-LENGTH":"NONE", "KEY-CURVE-NAME":"SECP384R1", "CA-AID":"NONE", "KEY-AID-LIST":"NONE"}

	192.168.1.75 WDM[6420] 1636 2023-08-23T13:18:57.55Z PKI_CERT-15 NA SYSTEM Edit {"CA-AID":"PKI_CA-3"} 192.168.1.75 WDM[6420] 1637 2023-08-23T13:18:58.63Z PKI_CERT-15 NA SYSTEM ForcedDelete {} 192.168.1.75 WDM[6420] 86911 2023-08-23T13:18:58.76Z SRV-UBR CPY-MEM-VALIDATION-COMPL NA NSA n/a {"FILE":"F7022022RC03.CON"} 192.168.1.75 WDM[6420] 86912 2023-08-23T13:19:00.93Z SRV-UBR CPY-MEM-COMPL NA NSA n/a {"FILE":"F7022022RC03.CON"} 192.168.1.75 WDM[6420] 86913 2023-08-23T13:19:01.16Z SRV-UBR CPY-MEM-PRTL NA NSA n/a {"FILE":"E7022022RC03.PGM"} 192.168.1.75 WDM[6420] 86914 2023-08-23T13:19:32.12Z SRV-UBR CPY-MEM-COMPL NA NSA n/a {"FILE":"E7022022RC03.PGM"} 192.168.1.75 WDM[6420] 86915 2023-08-23T13:19:32.34Z SRV-UBR CPY-MEM-PRTL NA NSA n/a {"FILE":"S7022022RC03.PGM"} 192.168.1.75 WDM[6420] 86916 2023-08-23T13:19:45.93Z SRV-UBR CPY-MEM-COMPL NA NSA n/a {"FILE":"S7022022RC03.PGM"} 192.168.1.75 WDM[5763] 16643 2023-08-23T13:23:15.51Z NOTIFY: Software Activate, USER=ADMIN, ACCESS=LOCAL 192.168.1.75 WDM[6420] 86917 2023-08-23T13:23:15.52Z SRV-UBR SWACT NA NSA n/a {"DBSRST":"N"} **Result of the update attempt (Failed)** 192.168.1.75 WDM[5763] 16526 2023-08-21T15:55:08.21Z NOTIFY: Software Install, USER=ADMIN, ACCESS=LOCAL 192.168.1.75 WDM[6420] 85835 2023-08-21T15:55:08.61Z SRV-UBR CPY-MEM-PRTL NA NSA n/a {"FILE":"F7022022RC03.CON"} 192.168.1.75 WDM[5763] 16527 2023-08-21T15:55:09.03Z AUDIT (fail): STATUS=FAIL, OPERATION=CERT-VERIFY, PROCESS=verify_install_cert, CERT-STATUS-LIST=FAIL 192.168.1.75 WDM[6420] 85836 2023-08-21T15:55:09.04Z SRV-UBR CPY-MEM-FAIL__SIGNATURE NA NSA n/a {"FILE":"F7022022RC03.CON"}
The termination of a local session by the session locking mechanism.	192.168.1.75 WDM[5845] 39202 2023-09-25T13:40:30.86Z NOTIFY: Session Timeout, USER=ADMIN, ACCESS=LOCAL, SESSION_ID=ttyS0 192.168.1.75 WDM[5845] 39203 2023-09-25T13:40:30.87Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SERIAL, SESSION_ID=ttyS0
The termination of a remote session by the session locking mechanism	**SSH** 192.168.1.75 WDM[5845] 39346 2023-09-25T14:24:54.75Z NOTIFY: Session Timeout, USER=ADMIN, ACCESS=LOCAL, SESSION_ID=pts/0 192.168.1.75 WDM[5845] 39347 2023-09-25T14:24:54.76Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SSH, SRC_IP=192.168.1.98, SESSION_ID=pts/0 192.168.1.75 WDM[5845] 39348 2023-09-25T14:24:54.76Z AUDIT: OPERATION=SSH-SESSION-CLOSE, SRC_IP=192.168.1.98, PORT=44988, PROCESS=sshd, PID=15574 192.168.1.75 WDM[5845] 39349 2023-09-25T14:24:54.79Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=44988, PROCESS=sshd, PID=15566 **Web GUI** 192.168.1.75 WDM[5844] 44533 2023-10-18T18:11:26.86Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=HTTPS, SESSION_ID=web/0 192.168.1.75 WDM[5844] 44534 2023-10-18T18:11:26.86Z NOTIFY: Session Timeout, USER=ADMIN, ACCESS=LOCAL, PROTOCOL=HTTPS, SESSION_ID=web/0 192.168.1.75 WDM[5844] 44535 2023-10-18T18:11:31.64Z AUDIT: OPERATION=WEB-TLS-CLOSE, SRC_IP=192.168.1.98, PORT=46238, PROCESS=nginx, PID=29504

	192.168.1.75 WDM[5844] 44536 2023-10-18T18:11:31.64Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=46238, PROCESS=nginx, PID=29504
The termination of an interactive session	**Local CLI** 192.168.1.75 WDM[5552] 894 2023-05-08T20:55:26.35Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SERIAL, SESSION_ID=ttyS0 **SSH CLI** 192.168.1.75 WDM[5845] 27562 2023-09-08T18:50:25.86Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SSH, SRC_IP=192.168.1.98, SESSION_ID=pts/0 192.168.1.75 WDM[5845] 27563 2023-09-08T18:50:25.86Z AUDIT: OPERATION=SSH-SESSION-CLOSE, SRC_IP=192.168.1.98, PORT=23113, PROCESS=sshd, PID=3901 192.168.1.75 WDM[5845] 27564 2023-09-08T18:50:25.88Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=23113, PROCESS=sshd, PID=3891 **Web GUI** 192.168.1.75 WDM[5552] 917 2023-05-08T21:09:42.89Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=HTTPS, SESSION_ID=web/0 192.168.1.75 WDM[5552] 918 2023-05-08T21:09:42.95Z AUDIT: OPERATION=WEB-TLS-CLOSE, SRC_IP=192.168.1.98, PORT=55086, PROCESS=nginx, PID=6525 192.168.1.75 WDM[5552] 919 2023-05-08T21:09:42.95Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=55086, PROCESS=nginx, PID=6525
Initiation of the trusted channel	192.168.1.75 WDM[5843] 41110 2023-09-25T20:13:22.83Z AUDIT: OPERATION=TCP-CONNECT, SRC_IP=192.168.1.76, PORT=6514, PROCESS=rsyslogd, PID=16179 192.168.1.75 WDM[5843] 41111 2023-09-25T20:13:23.39Z AUDIT: OPERATION=CERT-VERIFY, SRC_IP=192.168.1.76, PORT=6514, PROCESS=rsyslogd, PID=16179, AID=PKI_CERT-5 192.168.1.75 WDM[5843] 41112 2023-09-25T20:13:23.39Z AUDIT: OPERATION=TLS-CHANNEL-ESTABLISH, SRC_IP=192.168.1.76, PORT=6514, PROCESS=rsyslogd, PID=16179
Termination of the trusted channel	192.168.1.75 WDM[5843] 41113 2023-09-25T20:13:29.63Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.76, PORT=6514, PROCESS=rsyslogd, PID=16179
Failure of the trusted channel functions	See 'Failure to establish a TLS session (TLS Client)'
Initiation of the trusted path	**Initiation of the trusted path (SSH)** 192.168.1.75 WDM[5845] 28804 2023-09-12T13:46:47.25Z AUDIT: OPERATION=TCP-OPEN, SRC_IP=192.168.1.98, PORT=23188, PROCESS=sshd, PID=6245 192.168.1.75 WDM[5845] 28805 2023-09-12T13:46:47.56Z AUDIT: OPERATION=SSH-CHANNEL-REKEY, SRC_IP=192.168.1.98, PORT=23188, PROCESS=sshd, PID=30492, KEX-ALGORITHM=ecdh-sha2-nistp384, HOSTKEY-ALGORITHM=ecdsa-sha2-nistp384 192.168.1.75 WDM[5845] 28806 2023-09-12T13:46:50.68Z AUDIT: USER=ADMIN, ACCESS=LOCAL, OPERATION=SSH-AUTH-PASSWORD, SRC_IP=192.168.1.98, PORT=23188, PROCESS=sshd, PID=30491 192.168.1.75 WDM[5845] 28807 2023-09-12T13:46:50.69Z AUDIT: OPERATION=SSH-CHANNEL-ESTABLISH, SRC_IP=192.168.1.98, PORT=23188, PROCESS=sshd, PID=30499 192.168.1.75 WDM[5845] 28808 2023-09-12T13:46:50.69Z AUDIT: OPERATION=SSH-SESSION-OPEN, SRC_IP=192.168.1.98, PORT=23188, PROCESS=sshd, PID=30499 192.168.1.75 WDM[5845] 28809 2023-09-12T13:46:50.74Z LOGIN: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SSH, SRC_IP=192.168.1.98, SESSION_ID=pts/0 **Initiation of the trusted path (HTTPS)** 192.168.1.75 WDM[5843] 32592 2023-09-18T13:13:17.85Z AUDIT: OPERATION=TCP-

	OPEN, SRC_IP=192.168.1.98, PORT=24105, PROCESS=nginx, PID=9769 192.168.1.75 WDM[5843] 32593 2023-09-18T13:13:17.95Z AUDIT: OPERATION=CERT-VERIFY, SRC_IP=192.168.1.98, PORT=24105, PROCESS=nginx, PID=9769, INFO=SUBJECT: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:192.168.1.98, ISSUER: /C:US/ST:Maryland/L:Laurel/O:Booz Allen/OU:CATL/CN:int02CA_384, FINGERPRINT-SHA256: 10:29:bb:5c:9c:59:e6:59:0f:38:57:c6:df:71:58:b7:88:29:bd:ac:51:e7:9f:54:2f:6a:1a:2b:30:0d:da:67,SIGNATURE-ALGORITHM: ecdsa-with-SHA384, SERIAL-NUMBER: 06 192.168.1.75 WDM[5843] 32594 2023-09-18T13:13:17.98Z AUDIT: OPERATION=WEB-TLS-OPEN, SRC_IP=192.168.1.98, PORT=24105, PROCESS=nginx, PID=9769 192.168.1.75 WDM[5843] 32595 2023-09-18T13:13:24.68Z LOGIN: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=HTTPS, SRC_IP=192.168.1.98, SESSION_ID=web/1
Termination of the trusted path	**Termination of the trusted path (SSH)** 192.168.1.75 WDM[5845] 28810 2023-09-12T13:46:52.84Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=SSH, SRC_IP=192.168.1.98, SESSION_ID=pts/0 192.168.1.75 WDM[5845] 28811 2023-09-12T13:46:52.84Z AUDIT: OPERATION=SSH-SESSION-CLOSE, SRC_IP=192.168.1.98, PORT=23188, PROCESS=sshd, PID=30499 192.168.1.75 WDM[5845] 28812 2023-09-12T13:46:52.87Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=23188, PROCESS=sshd, PID=30491 **Termination of the trusted path (HTTPS)** 192.168.1.75 WDM[5843] 32601 2023-09-18T13:13:25.19Z AUDIT: OPERATION=WEB-TLS-OPEN, SRC_IP=192.168.1.98, PORT=24107, PROCESS=nginx, PID=9769 192.168.1.75 WDM[5843] 32602 2023-09-18T13:13:28.17Z LOGOUT: USER=ADMIN, ACCESS=LOCAL, PROTOCOL=HTTPS, SESSION_ID=web/1 192.168.1.75 WDM[5843] 32603 2023-09-18T13:13:28.23Z AUDIT: OPERATION=WEB-TLS-CLOSE, SRC_IP=192.168.1.98, PORT=24107, PROCESS=nginx, PID=9769 192.168.1.75 WDM[5843] 32604 2023-09-18T13:13:28.23Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=24107, PROCESS=nginx, PID=9769 192.168.1.75 WDM[5843] 32605 2023-09-18T13:13:30.15Z AUDIT: OPERATION=WEB-TLS-CLOSE, SRC_IP=192.168.1.98, PORT=24105, PROCESS=nginx, PID=9769 192.168.1.75 WDM[5843] 32606 2023-09-18T13:13:30.15Z AUDIT: OPERATION=TCP-CLOSE, SRC_IP=192.168.1.98, PORT=24105, PROCESS=nginx, PID=9769
Failure of the trusted path functions	**Failure of the trusted path functions (SSH)** See ‘Failure to establish an SSH session (SSH Server)’ **Failure of the trusted path functions (HTTPS)** See ‘Failure to establish a TLS session (TLS Server)’

Table 4: Sample Audit Records

8.1 Audit Storage

The TOE compresses audit log files in order to reduce the storage footprint of the audit records within each log’s respective storage location. When the current audit log file reaches its maximum file size or number of entries, the TOE will rotate audit log files in the following manner:

- If the maximum number of archived audit log files exists: delete oldest archived audit log file in order to maintain the maximum number of archived audit log files (FIFO methodology)
- Archive current audit log file (close, compress, and rename file)
- Open a new audit log file for receiving current audit records

Audit log files are archived according to the type of audit log following the below archiving rules:

Audit Log File Type	Min Audit Log File Size to Trigger Archiving	Max Number of Audit Record Entries per Log File (M)	Max Number of Archived Audit Log Files (N)	Max Audit Log File Storage Space (Current + Archived)
Condition Log (Event)	-	100	19	2 MB (*)
Database Change Log	-	50	19	2 MB (*)
Security Log (System)	≥80 KB	-	9	800KB

Table 5: Audit Log Archiving Rules

(*) the Condition and Database Change logs are kept in **one shared** SRAM 2MB-sized partition.

The audit records may be viewed using any of the Security Administrator interfaces. The viewing of the audit records via the Web GUI can be accomplished through the following steps:

1. Authenticate to the Web GUI
2. Select “Node”
3. Select “Logs” to display the log types.
4. Select the wanted log file to view its recorded events.

There is no access to delete or modify audit records through the Web GUI. However, the audit log files can be accessed at the OS level by a Security Administrator that has the ability to escalate to root privileges, using the sudo command, to make authorized file deletions or modifications.

8.1.1 Configuring the Audit Server

The TSF allows a Security Administrator to configure the near real-time forwarding of the audit trail to an external Audit Server in the Operational Environment. The TOE is a standalone appliance responsible for storing and sending its own generated audit records to the external Audit Server. Once configured, generated audit data is first saved locally on the TOE. The TOE then securely transmits audit data via a TLS channel to the external Audit Server in the Operational Environment without administrator intervention. During a connection outage to the Audit Server, the TOE continues to save audit data locally. Once the connection to the Audit Server is re-established, the TOE automatically starts forwarding new audit records. The TOE does not forward the records created during the outage.

1. Authenticate to the TOE via the CLI.
2. Navigate to “System Management” → “System General Settings” → “Syslog”.
3. Select “Add”.
4. Specify the IP address of the syslog server in the appropriate field.
5. Ensure that “Send Alarms”, “Send Database Changes”, and “Send Security Events” are set to Enable.
6. Select “Apply”.

7. Navigate to “System Security Management” → “Security Settings” → “General”.
8. Select “Enable” for “Audit Logs”.
9. Select “Apply”.

NOTE: To be able to connect to the TOE, the Audit Server must support the following:

- Protocol Versions: HTTPS (TLS 1.2)
- Ciphersuites: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Key Establishment Methods: secp384r1
- Software: Syslog Server that supports RFC 5424

NOTE: The TOE only supports IPv4 addresses in the Common Name (CN) or the Subject Alternative Name (SAN) extension. Thus, the X.509v3 certificate MUST contain an IPv4 address in the CN or SAN extension utilizing the octet format. The TOE does not support the use of wildcards in the CN or SAN.

NOTE: If the connection to the Audit Server is unintentionally broken, no action is required by the administrator to re-establish the connection through the TOE.

9 Obtaining Technical Assistance

Adtran offers technical assistance through their website: https://www.adtran.com/en under the heading “Support”. There is a specific customer support portal with website: https://advaoptical.my.site.com/customerportal/CustomLoginPage where customers can login with a username and password.

Support in North American can be contacted using the telephone number: +1 888-423-8726 (Toll Free). In addition, the support team can be contacted by opening a ticket through the support center at: https://www.adtran.com/en/about-us/support. Other support contact information can be found at the same location.