SAMSUNG

Samsung 5G AU/DU V19.A.0

Common Criteria Guide

Version 1.3

November 2020

Document prepared by

www.lightshipsec.com

Table of Contents

1 About this Guide 3

1.1 Overview 3
1.2 Audience 3
1.3 About the Common Criteria Evaluation 3
1.4 Conventions 5
1.5 Related Documents 6

2 Secure Acceptance and Update 6

2.1 Obtaining the TOE 6
2.2 Verifying the TOE 6
2.3 Power-on Self-Tests 7
2.4 Updating the TOE 7

3 Configuration Guidance 7

3.1 Installation 7
3.2 Administration Interfaces 7
3.3 Cryptography 8
3.4 Default Passwords 8
3.5 Setting Time 8
3.6 Audit Logging 9
3.7 Administrator Authentication 9
3.8 Trusted Channel 10

4 Annex A: Audit Log Reference 11

4.1 Audit Records Format 11
4.2 Audit Events 11

5 Annex B: CLI Command Reference 17

6 Annex C: NETCONF CLI Command Reference 27

7 Annex D: NETCONF API Command Reference 29

List of Tables

Table 1: Evaluation Assumptions 4
Table 2: Related Documents 6
Table 3: Audit Events 11

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the Samsung 5G AU/DU V19.A.0 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 2.

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 Samsung 5G AU/DU V19.A.0 TOE comprises the following components:

a) Cabinet DU model with Cavium CN9670 CPU and 19.A.0 software

b) AT1K01-A00(AC) with Cavium CN8370 CPU and 19.A.0 software

c) AT1K01-A10(DC) with Cavium CN8370 CPU and 19.A.0 software

1.3.3 Evaluated Functions

6 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) **Bash CLI.** Administrator access to the CLI via SSH

   iii) **NetconfD.** Administrator access to Confd CLI via SSH

   iv) **Netconf API.** Administrative API via SSH.

   v) **Logs.** Secure transmission of log events to an audit server via SSH.

   vi) **NTP.** TOE time synchronization via NTP.

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 signature.

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

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

1.3.4 Evaluation Assumptions

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

Table 1: Evaluation Assumptions

Assumption	Guidance
The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.	Ensure that the device is hosted in a physically secure environment, such as a locked server room.
The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).	Do not install other software on the device hardware.
A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit	The Common Criteria evaluation focused on the management plane of the device.

Assumption	Guidance
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).	
The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.	Ensure that administrators are trustworthy – e.g. implement background checks or similar controls.
The Network Device firmware and software is assumed to be 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.
The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.	Administrators should take care to not disclose credentials and ensure private keys are stored securely.
The Administrator must 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.	Administrators should sanitize the device before disposal or transfer out of the organization's control.

9 In addition, the TOE is expected to be preconfigured by Samsung technical support to communicate with an Operations System Support (OSS) in the environment.

1.4 Conventions

10 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 2. For example:

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

1.5 Related Documents

11 This guide supplements the below documents which are distributed with the product.

Table 2: Related Documents

Reference	Document
[AU-CMD]	Samsung 5G NR AU Command Reference for SVR 19A, v1.0
[DU-CMD]	Samsung 5G NR DU Command Reference for SVR 19A, v1.0
[CONFD-CLI]	Samsung CONFD CLI User Guide, v1.1

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

2 Secure Acceptance and Update

2.1 Obtaining the TOE

13 Your Samsung 5G AU/DU devices 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

2.2 Verifying the TOE

14 At the CLI, use command `get-pkginfo -` this command provides information about the currently installed and running software package including (in order): main version, revision, type of network element (NVGNB or DU), and build date.

15 **NOTE:** NE Type ‘NVGNB’ is the 2U rack-mounted Digital Unit (DU) and NE Type ‘DU’ is the combination DU/RU Access Unit (AU).

16 It is important to verify that the Trusted Platform Module (TPM) has the correct firmware revision to meet the certification requirements. To verify, run the following command as the ‘root’ user:

```
tpm2_getcap -c properties-fixed | grep -A1
'TPM2_PT_FIRMWARE_VERSION_1'
```

The command must return a value of:

```
TPM2_PT_FIRMWARE_VERSION_1:
```

```
value: 0x490041
```

17 If any other value is returned, then please contact your Samsung customer service/technical representative.

2.3 Power-on Self-Tests

18 The TOE includes a number of built in self-tests that are run during start-up. These tests are conducted to provide assurance of the correct operation of the cryptographic functions of the TOE, CPU, and BIOS. The tests also verify the integrity of the TOE image. A successful boot up operation indicates that all tests have passed and all cryptographic functions are operating correctly.

19 Cryptographic functions, along with any operations of the TOE supported by these functions, will not be available should these tests fail. The boot up operation will fail if the CPU, BIOS, or boot loader image verification tests fail.

20 Should an error occur, the TOE will reboot and log any failures. If a reboot does not resolve the error and any troubleshooting steps indicated by an error message are unsuccessful, Samsung Technical Support should be engaged for troubleshooting or repair.

21 The relevant audit records are noted in Annex A: Audit Log Reference.

2.4 Updating the TOE

22 TOE software updates are hand delivered to the customer by a Samsung customer service/technical representative.

23 TOE update files are digitally signed (ECDSA using NIST P-256 / SHA-256) and the signature is verified prior using a hardcoded ECDSA public key prior to installation of the update. If verification fails, the update is aborted, and an error message is displayed.

24 `Use command upgrade-pkg <signed_firmware_file> –` this command is used to manually upgrade the TOE firmware with an image file.

25 The TOE does not support delayed activation.

3 Configuration Guidance

3.1 Installation

26 The TOE is delivered pre-installed and pre-configured. A small number of settings are configured after the first reboot using the following commands:

a) `set-cc-config 1` — used to ensure that all settings are consistent with the security requirements.

b) `passwd` —used to set the user password.

3.2 Administration Interfaces

27 Only the following administration interfaces may be used:

a) **CLI / Console.** Directly connected peripherals via serial-based RJ-45 port, or a debug port (USB). The serial cable uses a custom pinout and cables can be obtained from your Samsung customer service/technical representative).

   Terminating a session in the CLI/console interface is done using the '`exit`' command.

b) **Bash CLI / SSH.** Remote access to the CLI via SSH.

   Terminating a session in the CLI/SSH interface is done using the '`exit`' command.

c) **NetconfD CLI / SSH.** Remote access to the CLI using an SSH client.

   Terminating a session in the NetconfD/CLI interface is done using the '`exit`' command.

d) **Netconf API / SSH.** Remote access to the Netconf server.

   Terminating a session in the Netconf API uses the 'close-session' Netconf RPC command.

28 Information on specific commands can be found in Annexes B, C and D.

3.3 Cryptography

29 All cryptographic parameters in the TOE are set by default. The cryptographic parameters are not configurable.

3.4 Default Passwords

30 It is necessary to change the password for the nrcliuser and the root user upon receipt before the device is in the evaluated configuration. The root user can be accessed using the local console only. To change the passwords for these users, log in as root (using the root password provided by the Samsung customer service/technical representative):

a) `passwd` —used to set the root password.

b) `passwd nrcliuser` —used to set the nrcliuser user password while logged in as root.

31 Once in the evaluated configuration, use of the root account is not permitted except to perform maintenance. The root password should be protected.

32 After the first reboot, the lteuser password is set. Changing a password afterwards is done with the command `passwd`.

3.5 Setting Time

33 Administrator can set the time manually by using linux shell '`date`' command at the CLI / Bash CLI.

34 The TOE requires the use of an NTP server in the environment which can be configured via the Netconf CLI or Netconf API. The managed element is found under `managed-element common-management time-sync-service ntp-info`.

35 Administrators can set the specific NTP integrity key using command `set-ntp-update-key <key>`. The key ID will always be hardcoded as number 11 and needs to be synchronized with the external NTP target.

3.6 Audit Logging

36 The TOE must be configured to send logs to an audit server securely via SSH. Information can be found in section 3.8.

37 Log files are transferred via SFTP to the OSS periodically at 30 minutes after the hour, every hour. These are placed into a pre-existing folder structure on the OSS conforming to the following:

/log/system/

applog

corelog

backup

38 Two primary log file types are stored in corelog (the XXXX encompasses different components depending on the nature of the log):

a) OTXXXX – system diagnostic log files

b) CMXXXX – configuration and database backups

39 Two primary log file types are stored in applog (the XXXX encompasses different components depending on the nature of the log):

a) OTXXXX – system diagnostics and log files

b) CMXXXX – configuration and database backups

40 Finally, the configuration and database backups found in corelog and applog are also duplicated in the backup directory.

41 Of specific note, within the applog, files with a pattern such as OTXXX…uploadVarLog.periodic.tar.gz contains a copy of all log files from the /var/log directory on the TOE. It can be used to review TOE activity.

42 Logs are also stored locally in rotating log files as follows (oldest records are overwritten first):

a) **/var/log log files.** Up to 1MB of data is kept in each of the log files before they are rotated. Up to one previous log file is kept of each log file and one live log.

b) **auditd log file.** up to 8MB of log data is kept until they are rotated. A total of 5 previous logs are kept (plus the live log).

3.7 Administrator Authentication

43 The TOE performs identification and authentication at its administration interfaces. It uses a password mechanism for authentication and enforces password length and password complexity requirements. It also displays a warning message at login.

44 The default minimum password length is 15. User passwords may be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “%”, “^”, “*”, “(“, “)”, ” _”, “~”, “.”, “:”, “/”, “-“

45 Two accounts exist on the TOE: ‘lteuser’ and ‘nrcliuser’. The lteuser account can access both the bash shell and the Netconf API. The nrcliuser account can only access the Netconf CLI interface. Both accounts however, share the same public key pair.

46 The TOE enforces a limit on failed authentication attempts at its user interfaces. After the limit has been reached the user account will be locked for a defined time period.

47 These are configured after the first reboot using the following commands:

a) `set-auth` used to set the minimum password length, authentication failure limit and the lockout out time period when the limit has been reached.

b) `get-auth-config` — used to query the current authentication settings.

c) `set-ssh-public-key <key-file>` – used to add a user public key to the TOE's authorized key store. *NOTE: Both 'lteuser' and 'nrcliuser' accounts share the same public/private SSH key pair.*

d) `set-banner`— used to set the login banner for local and remote interfaces.

48 The TOE enforces session locking at its interfaces, the administrator configures the session locking values with the commands:

a) `set-tmout` – this command sets the idle timeout for the bash CLI.

b) `set-netconf-tmout <number_in_minutes>` – this command is dedicated to Netconf API and sets the inactivity timeout value.

c) `set-netconf-cli-tmout` — this command is used to set the session idle timeout for the Netconf CLI.

49 **NOTE:** The local console does not enforce account locking.

3.8 Trusted Channel

50 The cryptographic parameters of the TOE are all set by default. After the first reboot, the administrator generates a key pair to be use for ssh authentication with the `set-ssh-host-key` command.

51 Logging to an external OSS entity is configured using the `set-remote-log-auth` command in the CLI. The username and (optional) password can be provided. If a password is not provided, then public/private key authentication can be configured using `set-remote-log-key` in the CLI and will be used if configured. The public key will be made available for the administrator to copy to the OSS to add to their set of authorized keys.

52 Pre-existing values can be cleared using the set-remote-log-auth-clear command. Prior SSH known host entries can be cleared, if necessary, by using the `set-ssh-known-clear` CLI command.

53 The SSH RekeyLimit specification in /etc/ssh/sshd_config and /etc/ssh/ssh_config are not configurable in the evaluated configuration. By default, the TOE is set to rekey SSH keys after 1 hour of elapsed time or 500 MB, whichever comes first.

4 Annex A: Audit Log Reference

4.1 Audit Records Format

54 Each event log includes the following fields:

a) **Date / time**. The date and time that the event occurred.

b) **Type**. The type of event.

c) **Admin ID**. The user that caused the event.

d) **Outcome**. Success/failure

4.2 Audit Events

55 The TOE generates the following log events.

Table 3: Audit Events

Requirement	Auditable Events	Example Event
FAU_GEN.1	Start-up and shutdown of the audit functions	type=DAEMON_END msg=audit(1588835753.596:991): op=terminate auid=0 pid=9070 subj=_ res=success type=DAEMON_START msg=audit(946684803.496:990): op=start ver=2.8.4 format=raw kernel=4.14.76 auid=4294967295 pid=5198 uid=0 ses=4294967295 subj=_ res=success
FCS_SSHC_EXT.1	Failure to establish an SSH Session	Jan 1 01:27:55 122_00_00_GMA1_0 varlogup[10924]: root(root console Jan 1 01:27) [UPLOADLOG_INFO] Try CNT(1): Auth type - ID/Password. Jan 1 01:27:55 122_00_00_GMA1_0 varlogup[10924]: root(root console Jan 1 01:27) [UPLOADLOG_SUCCESS] Log files(file count:12) were uploaded to 10.20.1.12:/log/system/applog.
FCS_SSHS_EXT.1	Failure to establish an SSH Session	Dec 31 19:16:31 122_00_00_GMA1_0 sshd[19371]: Unable to negotiate with 10.100.1.126 port 40236: no matching MAC found. Their offer: hmac-md5 [preauth]
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Aug 31 08:04:32 122_00_00_GMA1_0 sshd[31637]: error: maximum authentication attempts exceeded for

Requirement	Auditable Events	Example Event
		lteuser from 10.20.1.12 port 60954 ssh2 [preauth]
FIA_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Aug 31 09:28:43 122_00_00_GMA1_0 sshd[2187]: Accepted password for nrcliuser from 10.100.1.126 port 53254 ssh2 Aug 31 09:28:43 122_00_00_GMA1_0 sshd[2187]: pam_unix(sshd:session): session opened for user nrcliuser by (uid=0) Aug 31 09:26:49 122_00_00_GMA1_0 sshd[1457]: Failed password for nrcliuser from 10.100.1.126 port 53250 ssh2
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Aug 31 09:28:43 122_00_00_GMA1_0 sshd[2187]: Accepted password for nrcliuser from 10.100.1.126 port 53254 ssh2 Aug 31 09:28:43 122_00_00_GMA1_0 sshd[2187]: pam_unix(sshd:session): session opened for user nrcliuser by (uid=0) Aug 31 09:26:49 122_00_00_GMA1_0 sshd[1457]: Failed password for nrcliuser from 10.100.1.126 port 53250 ssh2
FIA_UAU.7	None.	
FMT_MOF.1/Manual Update	Any attempt to initiate a manual update	Aug 31 10:53:57 122_00_00_GMA1_0 upgrade-pkg[27308]: lteuser(lteuser pts/0 Aug 31 10:49 (10.100.1.126)) PKG(NVGNB_SVR19AR03.tar.gz.sign) is installed successfully. Aug 31 12:19:39 122_00_00_GMA1_0 upgrade-pkg[12949]: lteuser(lteuser pts/0 Aug 31 12:18 (10.100.1.126)) PKG(image-wo-sig.tar.gz.sign): Checking the PKG signature is failed(1).
FMT_SMF.1	All management activities of TSF data.	In /var/log/command/nrnm.log.1: modKeypath len 5 leafName = ntp-info

Requirement	Auditable Events	Example Event
		leaf path : /nsgnb:managed-element/common-management/time-sync-service/ntp-info[[server-type="primary-server"] leaf name : ntp-info modKeypath len 6 leafName = server-ip-address leaf path : /nsgnb:managed-element/common-management/time-sync-service/ntp-info[[server-type="primary-server"] leaf name : server-ip-address new value = 10.20.1.2 insert Operation : 1Start Epoch Time : 946768690292830 Old : 10.20.1.200, New : 10.20.1.2, path : /nsgnb:managed-element/common-management/time-sync-service/ntpp -info[server-type="primary-server"], leafName : server-ip-address Aug 31 08:53:39 122_00_00_GMA1_0 passwd[19998]: pam_unix(passwd:chauthtok): password changed for lteuser Aug 31 09:43:06 122_00_00_GMA1_0 set-banner[8180]: lteuser(lteuser pts/0 Aug 31 09:40 (10.100.1.126)) Remote(SSH) session banner has been modified. Sep 2 13:12:46 122_00_00_GMA1_0 set-ssh-host-key[16312]: lteuser(lteuser pts/0 Sep 2 13:12 (10.100.1.126)) Host key(ecdsa) has been deleted. Key ID:(b7fa2561646c529a13015be4db74681eb215f6f2) Sep 2 13:12:46 122_00_00_GMA1_0 set-ssh-host-key[16312]: lteuser(lteuser pts/0 Sep 2 13:12 (10.100.1.126)) Host key(ecdsa) has been created. Key ID:(62e02ccc771d614b2d83aa722c9aab8e0c41606f) Sep 8 14:38:59 00_00_00_G7DA-C00_0 set-ssh-host-key[29536]: lteuser(lteuser console Sep 8 14:36)

Requirement	Auditable Events	Example Event
		Host key(ecdsa) has been deleted. Key ID:(3148258fef32ec22e57b2a65905fcf64ef391654) Sep 8 14:38:59 00_00_00_G7DA-C00_0 set-ssh-host-key[29536]: lteuser(lteuser console Sep 8 14:36) Host key(ecdsa) has been created. Key ID:(34ca6cfc609afaf62b1fc3e0d4001a699e6e41dd)
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	Aug 31 10:53:57 122_00_00_GMA1_0 upgrade-pkg[27308]: lteuser(lteuser pts/0 Aug 31 10:49 (10.100.1.126)) PKG(NVGNB_SVR19AR03.tar.gz.sign) is installed successfully. Aug 31 12:19:39 122_00_00_GMA1_0 upgrade-pkg[12949]: lteuser(lteuser pts/0 Aug 31 12:18 (10.100.1.126)) PKG(image-wo-sig.tar.gz.sign): Checking the PKG signature is failed(1).
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	Aug 31 12:33:28 122_00_00_GMA1_0 date[19195]: lteuser(lteuser pts/0 Aug 31 12:18 (10.100.1.126)) User change date from "Mon Aug 31 12:33:29 EST 2020" to "Mon Aug 31 20:33:29 EST 2020" [1231|19:02:11.789|NRSWM|nrswm|0174|EVNT|72][Before ntp sync] Fri Dec 31 19:02:11 EST 1999 [0901|09:09:12.314|NRSWM|nrswm|0444|EVNT|72]ntp sync : 1 Sep 09:09:12 ntpdate2[11292]: step time server 1 [0901|09:09:12.463|NRSWM|nrswm|0174|EVNT|72][After ntp sync] Tue Sep 1 09:09:12 EST 2020
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	Sep 1 07:28:54 122_00_00_GMA1_0 bash[31749]: session idle timeout. account(lteuser) Sep 1 07:28:54 122_00_00_GMA1_0 login[31689]: pam_unix(login:session): session closed for user lteuser
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	Sep 1 07:51:07 122_00_00_GMA1_0 sshd[7287]: Close session: user nrcliuser from 10.100.1.126 port 54356 id 0 Sep 1 07:51:07 122_00_00_GMA1_0 sshd[7287]: Received disconnect from

Requirement	Auditable Events	Example Event
		10.100.1.126 port 54356:11: disconnected by user Sep 1 07:51:07 122_00_00_GMA1_0 sshd[7287]: Disconnected from user nrcliuser 10.100.1.126 port 54356 Sep 1 07:51:07 122_00_00_GMA1_0 sshd[7245]: pam_unix(sshd:session): session closed for user nrcliuser
FTA_SSL.4	The termination of an interactive session.	Aug 31 13:33:03 122_00_00_GMA1_0 sudo: lteuser : TTY=ttyAMA0 ; PWD=/mnt/CPSW/home/lteuser ; USER=root ; COMMAND=/usr/local/cptools/OUL/.securelog.sh Aug 31 13:33:03 122_00_00_GMA1_0 bash[10988]: session normal exit. account(lteuser) Aug 31 13:33:03 122_00_00_GMA1_0 bash[10988]: session normal exit. account(lteuser) Aug 31 13:33:03 122_00_00_GMA1_0 login[2045]: pam_unix(login:session): session closed for user lteuser
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Sep 8 11:51:30 00_00_00_G7DA_C00_0 sudo: root : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/sftp -vvv root@10.20.1.12 Sep 8 11:51:30 00_00_00_G7DA-C00_0 varlogup[18571]: root(root console Sep 8 11:50) [UPLOADLOG_INFO] Try CNT(1): Auth type - ID/Password. Sep 8 11:51:30 00_00_00_G7DA-C00_0 varlogup[18571]: root(root console Sep 8 11:50) [UPLOADLOG_SUCCESS] Log files(file count:3) were uploaded to 10.20.1.12:/log/system/applog.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	Aug 31 09:28:43 122_00_00_GMA1_0 sshd[18694]: Connection from 10.100.1.126 port 41912 on 10.20.1.10 port 22 rdomain "" Aug 31 09:28:43 122_00_00_GMA1_0 sshd[2187]: Accepted password for nrcliuser from 10.100.1.126 port 53254 ssh2

Requirement	Auditable Events	Example Event
		Aug 31 09:28:43 122_00_00_GMA1_0 sshd[2187]: pam_unix(sshd:session): session opened for user nrcliuser by (uid=0)

5 Annex B: CLI Command Reference

get-auth-config

This command provides the caller with the current settings for system authentication information. Specifically, the settings for four components are provided:

a) The maximum number of configured authentication attempts for a named account before the account is locked out and the amount of time that will need to pass before the account is unlocked automatically.

b) The minimum password length enforced for new passwords.

c) The amount of time before an idle session will be terminated automatically. Three separate interfaces are represented: the Unix CLI (both the local console and over SSH), the NETCONF protocol (often visualized over a NETCONF browser GUI) and a NETCONF-based CLI session available to specific user accounts.

d) The authentication credentials for the remote log offloading subsystem. This includes, at a minimum, the username and optionally a password. If public key authentication is used, the password field will indicate it is not used.

These values are reflective of the settings from the '`set-auth`', '`set-tmout`', '`set-netconf-tmout`', '`set-netconf-cli-tmout`' and '`set-remote-log-auth`' commands.

Usage: `get-auth-config`

Example:

```
get-auth-config
  - Authentication Failure Count: 5
  - Lockout Time: 90 sec
  - Minimum Password Length: 9
  - Idle Session Timeout: 180 sec
  - NETCONF GUI Idle Session Timeout: 6 min
  - NETCONF CLI Idle Session Timeout: 6 min
  - Remote Upload Log User ID: "root"
  - Remote Upload Log User Password: "****"
```

get-log

The get-log command provides access to the various log files. It will output the entire log file to the Unix standard output (i.e. stdout). The set of logs which can be viewed are limited to only those found within the /var/log directory tree.

As the `lteuser', you cannot list the contents of the /var/log directory tree. Of interest are the following logs:

- /var/log/secure*
- /var/log/secure_ssh*
- /var/log/secure_sshd*
- /var/log/One_app.log*
- /var/log/One_app_NR.log*
- /var/log/audit/audit.log*
- /var/log/confd_nr/confd.log1
- /var/log/confd_nr/netconf.log1
- /var/log/confd_nr/netconf.audit.log1*
- /var/log/confd_nr/netconf.trace.log1
- /var/log/command/nrccnm_au.log1 [AU device only]
- /var/log/command/nrnm.log1 [DU device only]

Usage: `get-log /var/log/[ log file name ]`

Example:

```
get-log /var/log/secure | grep 'lteuser'
...
```

get-log-tail

Similar to the get-log command above, the get-log-tail command will tail the given log file. Two modes are available:

a) Providing a number as the first parameter will emit the last N lines of the requested log file.

b) Providing the 'f' parameter (note: there is no hyphen!) will perform a persistent `tail' operation on the requested log file. This means that as new data is appended to the log file, this new information is immediately output to stdout.

Usage: `get-log-tail [f | <number>] [/var/log/<log file name>]`

Example:

```
get-log-tail f /var/log/secure
...
```

get-pkginfo

This command provides information about the currently installed and running software package.

Usage: `get-pkginfo`

Example:

```
get-pkginfo
19.A.0
r-02
NE Type: NVGNB
PKG Build Date: 2020-09-02_16_01_38
```

The first line is the main version number. The second line is the revision. The third line is the type of network element this software is running on. (The NVGNB is the 2U rack-mounted Digital Unit (DU). If the 'NE Type' states 'DU', this is actually the combination DU/RU Access Unit (AU).) The fourth line is the build date of the specific package and can be used in combination with the main version number and revision to identify a unique iteration of the software package.

set-auth

The `set-auth` command will permit the administrator to alter the settings for the current session limits. It can be used to set the maximum number of authentication attempts before the named account is locked. It can be used to set the amount of time until a previously locked account is automatically unlocked. Finally, this tool can be used to set the minimum password length for any new password changes.

Note that the lockout time can be as high as 2593000 seconds which is approximately 30 days.

It is not possible to disable any of these settings. They must be set to valid non-zero value.

The minimum length of password is part of an overall organizational policy regarding password strength. A longer password is generally going to be stronger than a shorter password depending on the character composition. For more information on changing passwords, please refer to 'passwd'.

Usage: `set-auth [-c <1 ~ 1000> ] [-t <1 ~ 2593000>] [-l <9 ~ 15>]`

-c : set session fail lock count

-t : set session lockout time(sec)

-l : set password limit length

Example:

Set the maximum number of login attempts to 5. On the 5th consecutive failure, the account will be locked.

```
set-auth -c 5
```

Set the amount of time before any locked accounts are automatically unlocked. This example sets the unlock time to 3600 seconds (1 hour).

```
set-auth -t 3600
```

Set the minimum password length to 10 characters.

```
set-auth -l 10
```

set-banner

This command will permit the administrator to set the legal banner which can appear prior to the administrator establishing an interactive administrative session. The banner which appears for the local console (e.g. the serial console) can differ from that appearing for the remote SSH (or NETCONF) interfaces.

The file contents are copied to a secure location and do not need persist after the command has been executed.

There is no limit on the length or character content of the banner files. They are displayed as-is.

Usage: `set-banner [-r <file name> ] [-l <file name>]`

The `-r' option is used to provide the banner contents for all remote interfaces.

The `-l' option is used to provide the banner contents for the local serial console interface.

Example:

```
echo 'My new banner' > $HOME/remote-banner.txt
set-banner -r $HOME/remote-banner.txt

# ssh 10.20.1.10 -l lteuser
My new banner
lteuser@10.20.1.10's password:
```

set-tmout

This command sets the session idle timeout for the Unix CLI shell. The idle session timeout will automatically log out the current session if no activity is detected within the configured time period.

The timeout is permitted to be between 60 seconds and 1800 seconds, inclusive (note that the online command usage summary incorrectly implies the range is 61 seconds to 1799 seconds). Idle session timeout cannot be disabled.

For this configuration setting to take effect, the current session must be terminated after setting it. The next session will use the newly set value.

Usage: `set-tmout [ 60 <= <number> second <= 1800 ]`

Example:

Set a 3 minute idle timeout.

```
set-tmout 180
```

set-netconf-cli-tmout

Similar to the `set-tmout' command, this command will set the session idle timeout for the NETCONF CLI (available to the `nrcliuser' account only). The session timeout value is in minutes. It can be disabled by setting the value of 0. Otherwise, for non-zero values, the minimum value that can be provided is 5. The number represents the number of minutes before an idle session is automatically terminated.

Usage: `set-netconf-cli-tmout [ <number> minute ]`

The timeout value should be 0, or larger than 5

Example:

Set an 11 minute idle timeout:

```
set-netconf-cli-tmout 11
```

set-netconf-tmout

The semantics and syntax for the `set-netconf-tmout' command are identical to those of the `set-netconf-cli-tmout' command. However, this command will affect the session timeout associated with the NETCONF API protocol sessions. If the NETCONF client does not send any commands to the server within the configured time period, then the NETCONF protocol session will be automatically closed. A new session will have to be established to execute additional commands.

Usage: `set-netconf-tmout [ <number> minute ]`

The timeout value should be 0, or larger than 5

Example:

Set a 30 minute NETCONF protocol session timeout.

```
set-netconf-tmout 30
```

set-ntp-update-key

This command can be used to set a custom NTP integrity key value. The key id is always fixed at #11, but the key value can be configured. For remote NTP servers, it is critical to configure a key id #11 with the same integrity key value.

The key is limited to characters in the following set [0-9,a-f] (lowercase only).

Usage: `set-ntp-update-key [ 40-lentgh key string ]`

Example:

```
set-ntp-update-key 543dc45914636d906c2e5c47bf198184bfe66bbe
```

set-remote-log-auth

Use this command to configure the username and an optional password for the user account on the remote audit log server which will receive the periodic audit logs.

The remote system must have the corresponding user. If the remote server permits the user of a password login, then the password can be configured. If the remote system uses public key cryptography to authenticate the configured user account, then the password can be omitted. See `set-remote-log-key' to configure the private key for remote log authentication.

Usage: `set-remote-log-auth [-i USER_ID ] [-p PASSWD ]`

-i : set Remote User ID

-p : set Remote User Password

Example:

Set the username and password for a user on the remote audit server

```
set-remote-log-auth -i logserv -p 'Passw0rd!'
```

set-remote-log-auth-clear

This command can be used to clear the username and password defined using the `set-remote-log-auth' command. If these values are cleared, then the remote logging mechanism will not execute.

Usage: `set-remote-log-auth-clear`

Example:

```
set-remote-log-auth-clear
```

set-remote-log-key

Use of this command permits the administrator to construct a new private and public key pair that can be used to authenticate to a remote logging server over SSH. The private key is managed by the device and the public key is provided to the administrator to copy to the remote server.

In the evaluated configuration, the administrator is to use 'ecdsa' keys only.

Usage: `set-log-private-key [ rsa | ecdsa ]`

Example:

```
set-log-private-key ecdsa
```

set-ssh-add-known-host

This command permits the administrator to assign a remote SSH server as a trusted host. This is required to be run prior to setting up when configuring a remote log server otherwise the remote log offload will fail to execute.

The IP address of the OSS must be provided. This command can be run multiple times and if any key changes have occurred, they will be added to the existing known hosts database. The database can be periodically scrubbed using the `set-ssh-known-clear' command.

This command must be run whenever the OSS logging server SSH host key has been changed, otherwise logging will fail to execute. When this happens, the /var/log/secure_ssh log file will contain a warning that the host key signature has changed.

Usage: `set-ssh-add-known-host [ IP address ]`

Example:

Recapture the OSS SSH host (10.20.1.12) key signature when it has changed.

```
set-ssh-add-known-host 10.20.1.12
```

set-ssh-host-key

Use this command to provision a new SSH host public/private key pair for the AU/DU device. This will overwrite the existing public/private key pair. This will cause any external clients to detect a change in the AU/DU host key signature which may require the administrator to reconfigure external entities accordingly.

In the evaluated configuration, the administrator is to use 'ecdsa' keys only.

Usage: `set-ssh-host-key [ rsa | ecdsa ]`

Example:

```
set-ssh-host-key ecdsa
```

set-ssh-known-clear

Use this command to clear out the known hosts database. This command will not normally be necessary unless directed to use by a support technician.

Usage: `set-ssh-known-clear`

Example:

```
set-ssh-known-clear
```

set-ssh-public-key

If an administrator would like to perform SSH public key login to the device from an external SSH client or NETCONF client, the public key can be installed to a persistent location using this CLI command.

The parameter is a file containing the public key half of a key pair. It will be copied to a secure location and therefore the user supplied file can be removed when no longer required. To clear existing public keys, use the `set-ssh-public-key-clear' utility.

The same key will be used to permit SSH public key login for either the lteuser or the nrcliuser. This command can be executed multiple times to add several simultaneously active public keys. Administrators are encouraged to ensure that the third field in the public key specification (the 'comment' field) is populated with a descriptive name of who owns the private key half.

In the evaluated configuration, the administrator is to provide ECDSA public keys only.

For information on clearing the keys, see `set-ssh-public-key-clear'.

Usage: `set-ssh-public-key [ OpenSSH public key file ]`

Example:

```
# In this example, the administrator has copied the public key
# material from their remote system.  The 'user@operator' is the
# comment and can be used to identify specific public keys.
echo 'ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNT...WRZSvfNFp5aI6Mo=
user@operator' > $HOME/mykey.pub
set-ssh-public-key $HOME/mykey.pub
```

set-ssh-public-key-clear

Use this command to clear the set of authorized public keys capable of logging in as the lteuser and the nrcliuser. For information on adding the keys, see `set-ssh-public-key'.

Usage: `set-ssh-public-key-clear`

Example:

```
set-ssh-public-key-clear
```

passwd

The `passwd' command resets the password for the current user.

The system will enforce password changes meet the minimum password length as well as other password complexity characteristics. The tool will assess the quality of the password and either accept the password or reject the password with a specific reason.

Usage: passwd

Example:

passwd

date

The `date' command can be used to set and retrieve the current date and time. The system uses NTP to manage datetime corrections.

For more information on how the date can be formatted, use the `-h' option.

Usage: date

Example:

Get the current date and time

date

Set the current date to be 1 hour later than current

date -s +"+1 hour"

upgrade-pkg

This command is used to deploy a new version of the TOE software (such as bug fixes, vulnerability patches, etc.) The digitally signed package will have been received by the administrator and copied to the device. The package is then provided to the `upgrade-pkg' command.

The CLI command will ensure that the correct software is being deployed on the correct network element.

It is important to realize that the name of the device (AU or DU) does not match the software naming convention. The Access Unit (AU) (which is a combination Digital Unit (DU) and Radio Unit (RU)) has a network element identifier of 'DU'. The 2U rack-mounted Digital Unit (DU) has a network element identifier of 'NVGNB'. These

identifiers are encoded in the package file name and can lead to confusion as to which software should be installed on the AU and the DU devices.

For clarity on the network element type, please use the `get-pkginfo' command.

Usage : `upgrade-pkg [ signed PKG file name ]`

Example:

For the AU device, we install the package that has the 'DU' in the name because that is the correct network element identifier.

```
upgrade-pkg $HOME/DU_SVR19AR0300.tar.gz.sign
```

For the DU device, we install the package that has the 'NVGNB' in the name.

```
upgrade-pkg $HOME/NVGNB_SVR19AR02.tar.gz.sign
```

6 Annex C: NETCONF CLI Command Reference

Reboot

To reboot the device, use the `initialize-system' remote procedure call in configuration mode.

```
> configure
% request initialize-system reset-mode [hard/soft]
```

By default, a soft reset is initiated. A hardware reset will cycle the power.

For more information, refer to the [AU-CMD] or [DU-CMD] depending on the device type and locate the 'initialize-system' command.

Change NTP Servers

Up to three NTP servers can be configured in addition to the use of NTP from the OSS itself.

Use the `managed-element common-management time-sync-service ntp-info' element to configure.

The current configuration can be viewed using the 'show' command in configuration mode.

```
> configure
% show managed-element common-management time-sync-service
ntp-info
ntp-info primary-server {
    server-ip-address 10.20.1.2;
}
ntp-info secondary-server {
    server-ip-address 10.20.1.200;
}
ntp-info tertiary-server {
    server-ip-address 10.20.1.201;
}
[ok][2020-09-16 20:52:52]

[edit]
```

Each of the primary, secondary and tertiary NTP service endpoints can be configured independently while in configuration mode. Changes must be committed.

For example:

```
> configure
% set managed-element common-management time-sync-service ntp-info primary-server server-ip-address 10.20.1.2
% set managed-element common-management time-sync-service ntp-info secondary-server server-ip-address 10.20.1.200
% set managed-element common-management time-sync-service ntp-info tertiary-server server-ip-address 10.20.1.201
% commit
```

For more information, refer to [DU-CMD] or [AU-CMD] depending on the device type and locate the 'ntp-info' command. The command reference only refers to a primary and secondary server: this TOE supports a tertiary server as well.

7 Annex D: NETCONF API Command Reference

The same managed element nodes described in Annex C: NETCONF CLI Command Reference can be referenced in the NETCONF API as well. Refer to [DU-CMD] and [AU-CMD] for more information.