NETSCOUT

nGeniusPULSE Server v3.2

Common Criteria Guide

Version 1.2

September 2020

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the nGeniusPULSE Server v3.2 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) v2.1 available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Software and Hardware

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

a) **Hardware.** nGPulse Server (Dell R740)

b) **Software.** nGeniusPULSE Server v3.2 (3.2.539-1)

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.** Administrative CLI via direct VGA/keyboard and SSH.

   ii) **GUI.** Administrative web GUI via HTTPS.

   iii) **Logs.** Logs sent to syslog via SSH (the TOE is the SSH client).

   iv) **NETSCOUT nPoint.** Secure communication with deployed nPoints via TLS.

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

   i) Administrator authentication with passwords (local users)

   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 published hash.

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

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

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

Assumption	Guidance
The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	Administrators should sanitize the device before disposal or transfer out of the organization's control.

1.4 Conventions

9 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

10 This guide supplements the below documents.

Table 2: Related Documents

Reference	Document
[INSTALL]	NETSCOUT nGeniusPULSE Hardware Installation Guide v3.2
[USER]	NETSCOUT nGeniusPULSE User Guide v3.2 https://downloads.netscout.com/nGeniusPulse/v32/Introduction.html

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

2 Secure Acceptance and Update

2.1 Obtaining the TOE

12 Your nGPulse Server 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

13 Follow instructions at [USER] *Upgrade nGeniusPULSE* to obtain the TOE software with the following alteration to the instructions:

a) If using the CLI, use the command `ngp-deploy-upgrade` rather than `sudo systemctl start ngp-upgrade`.

2.2 Verifying the TOE

14 Follow instructions at [USER] *Version Number* to check the current version of software.

15 TOE software is verified by means of a published hash (obtained from https://my.netscout.com/) as follows:

a) On CLI, an Administrator can verify the SHA256 hash via `ngp-validate-checksum nGP-3.2.539-1.tar.gz 256checksum`

16 **NOTE:** If no integrity file is provided during installation, the TOE will not perform the integrity check. The administrator must verify the hash via the above command prior to updating the TOE. If verification fails, the update file should be discarded a new update obtained.

2.3 Power-on Self-Tests

17 At start-up, the TOE will perform a series of self-test to ensure correct operation.

18 These tests ensure the correct operation of the cryptographic functionality of the TOE, the CPU and BIOS and verify firmware integrity.

19 The cryptographic functionality will not be available if the cryptographic module tests fail, and any operation of the TOE supported by this functionality will not be available. If the CPU, or BIOS tests fail, the device will not complete the boot up operation.

20 Any failure in the firmware integrity tests will be logged to */var/log/common-criteria-checks.log*. Any component that fails will show *[Fail]*. If any of the components fail the integrity test, the TOE software should be re-installed. An example of this log is included at Annex A: Log Reference.

2.4 Updating the TOE

21 Follow instructions at [USER] *Upgrade nGeniusPULSE* with the following alteration to the instructions:

a) If using the CLI, use the command `ngp-deploy-upgrade` rather than `sudo systemctl start ngp-upgrade`.

22 **NOTE:** Do not delete the script */home/nGPadmin/ngp-configure.sh* as doing so will prevent future upgrades from occurring.

23 Verify the integrity and authenticity of TOE software prior to installation per instructions above at 2.2.

3 Configuration Guidance

3.1 Installation

24 Follow the instructions of [INSTALL] and [USER] augmented by the configuration guidance in the following sections.

3.2 Administration Interfaces

25 Only the following administration interfaces may be used:

a) **CLI / Console.** Directly connected peripherals via USB and VGA ports.

   i) Session termination is supported and may be configured via `ngp-set-password-security`

   ii) Banner messages are supported and may be configured via `ngp-set-banner -t console enable` [file containing banner message]

   iii) Use `exit` command to terminate a session.

   NOTE: Account lockout for failed authentication is not enforced for the nGPadmin account at the local console.

b) **CLI / SSH.** Remote access to the CLI interface via SSH. As per above except:

   i) Account lockouts are enforced and may be configured via `ngp-set-password-security`
   NOTE: A user locked out at the SSH interface will be unlocked if the same user logs in directly at the console.

   ii) Use `exit` command to terminate a session.

c) **GUI / HTTPS.** Web based Graphical User Interface.

   i) Use command `ngp-install-ssl-certificate` to configure and manage the web server certificate and the OCSP responder service.
   NOTE: Option 4 (Import a new SSL certificate) must not be used. Option 5 (Disable/Enable unencrypted HTTP access) – HTTP encryption must be enabled. Option 7 (Import Trusted certificate(s)) is used to designate a CA certificate as a trust anchor.
   NOTE: The GUI must be used to delete trust anchors (Trusted Certificates). Refer to [USER] *Administration > System nPoint > Certificates*.

   ii) Banner messages are supported and may be configured via `ngp-set-banner -t console enable <file containing banner message>`

   iii) Session termination is supported and may be configured via **Administration > System > General > Web Session Management**

   iv) Account lockouts are enforced and may be configured via **Administration > System > General > Web Session Management**

   v) Use **Sign Out** to terminate a session

3.3 Cryptography

26 FIPS mode is enabled by default. No additional configuration is necessary.

3.4 Default Passwords

27 The following accounts have default credentials:

a) **nGPadmin.** Default CLI account - user will be prompted to change the password on first use.

b) **sysadmin@netscout.com.** Default GUI account - user will be prompted to change the password on first use.

3.5 Setting Time

28 The use of NTP has not been evaluated. NTP should therefore be disabled via `ngp-configure`

29 Administrator can set the time manually via `ngp-date -s '<timestamp>'` command.

3.6 Audit Logging

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

31 The Common Criteria configuration requires communication with a syslog collector to be performed over SSH. The openssh version on the syslog collector must be version 7.4 (2017) or later and rsyslogd must be installed. The instructions below are for the syslog collector on CentOS 7.

32 A syslog collector must be configured to store the logs as follows:

a) Copy the `/opt/ngp/log-audit/remote` directory to the syslog collector (you can place it in the `home` directory). This directory contains the necessary files and instructions to configure syslog server / collector.

b) Log into the syslog collector and run `rpm -q lsof || sudo yum install -y lsof`

c) On the syslog collector, in the `remote` directory, run `sudo ngp-remote-setup <USER>` where <USER> is the user account present in the syslog collector designated for use by remote logging. The output of this command includes a host key fingerprint that will be used in `ngp-log-audit` command

d) Log into the nGP server

e) Run `ngp-log-audit <REMOTE_USER> <REMOTE_HOST> <REMOTE_HOST_FINGERPRINT>` to start the tunnel. Where:

   i) <REMOTE_USER> is the same user configured in the syslog collector via ngp-remote-setup

   ii) <REMOTE_HOST> is the hostname of the syslog collector

   iii) <REMOTE_HOST_FINGERPINT> is the remote host key fingerprint provided as an output by ngp-remote-setup

f) Verify the status of the logging channel by using `ngp-log-audit -s`

g) The logs are found on the syslog collector in `/var/log/nGenius_audit.log`

33 The TOE stores logs locally and sends then to syslog in real-time. When the local logs space is full, the TOE will overwrite the oldest logs.

34 **NOTE:** The SSH tunnel does not automatically reconnect in the event of a failure. Use Step e) above to manually re-establish the SSH tunnel in this case.

3.7 Administrator Authentication

35 Follow instructions at [USER] *General* to configure the number of successive unsuccessful authentication attempts and period of inactivity.

36 A user account that has been blocked due to multiple unsuccessful authentication attempts can be unblocked as follows:

a) The lockout time specified in minutes expires;

b) A password reset is performed at the Web UI; or

c) Use command `ngp-reset-lockout` at the CLI.

37 Refer [USER] *General* for details about Password complexity and various password length. The minimum administrator passwords length may be set to between 8 and 20 characters. Passwords may include special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”

NOTE: The session timeout value enforced at the Web UI is the next multiple of 3 (i.e. modulo 3). For example, if the timeout value is set to 10 minutes, the session will be terminated after 12 minutes.

NOTE: To enable public key authentication for the ngpuser account, the following permissions change is required: `chmod 750 /home/ngpuser`

Annex A: Log Reference

3.8 Format

38 Each audit record includes the following fields:

a) Timestamp

b) Severity Level (info, warn)

c) Message (including user if applicable and indication of success or failure)

3.9 Events

39 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	Start-up of audit function: 2020-04-20T23:10:47-04:00 ngp tag_sys_msg: Apr 20 23:10:37 ngp systemd: Stopping System Logging Service... 2020-04-20T23:10:47-04:00 ngp tag_sys_msg: Apr 20 23:10:37 ngp rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-38.el7" x-pid="250997" x-info="http://www.rsyslog.com"] exiting on signal 15. 2020-04-20T23:10:47-04:00 ngp tag_sys_msg: Apr 20 23:10:37 ngp systemd: Stopped System Logging Service. Shutdown of audit function: 2020-04-20T23:10:47-04:00 ngp tag_sys_msg: Apr 20 23:10:37 ngp systemd: Stopped System Logging Service. 2020-04-20T23:10:47-04:00 ngp tag_sys_msg: Apr 20 23:10:37 ngp rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-38.el7" x-pid="144056" x-info="http://www.rsyslog.com"] start 2020-04-20T23:10:47-04:00 ngp tag_sys_msg: Apr 20 23:10:37 ngp

Requirement	Auditable Events	Example Event
		systemd: Started System Logging Service.
	Administrative login and logout	Login as the administrator user: 2020-04-06T12:26:21-04:00 ngp tag_api_log: 2020-04-06T16:26:12.341Z - #033[32minfo#033[39m: [authentication.audit] User administrator attempting to login from 172.16.100.26. User status ENABLED 2020-04-06T12:26:21-04:00 ngp tag_api_log: 2020-04-06T16:26:12.512Z - #033[32minfo#033[39m: [authentication.audit] User administrator successfully logged in Logout 2020-04-06T12:30:02-04:00 ngp tag_api_log: 2020-04-06T16:29:56.338Z - #033[32minfo#033[39m: [authentication.audit] User administrator logout from 172.16.100.26
	Generating/import of, changing, or deleting of cryptographic keys	Generating/ Import of cryptographic keys generating a new CSR operation (unique reference name is highlighted in yellow): 2020-04-17T18:02:01-04:00 ngp tag_sys_msg: Apr 17 18:01:57 ngp nGP.Admin: Generating CSR with private key ID (public key hash): d1c23f0bf970c141968fa3e4d99c525f41edd037be9d4c78f28832378d68f295, by user nGPadmin from (10.100.0.137). 2020-04-17T18:02:31-04:00 ngp tag_sys_msg: Apr 17 18:02:23 ngp nGP.Admin: CSR generated, by user nGPadmin from (10.100.0.137). Changing cryptographic keys:

Requirement	Auditable Events	Example Event
		Keys cannot be changed. They can only be added or deleted Deleting of cryptographic Keys: 2020-04-24T12:45:25-04:00 ngp tag_sys_msg: Apr 24 12:45:20 ngp nGP.Admin: Current SSL certificate and key are being removed by user nGPadmin from (10.100.0.137). 2020-04-24T12:45:25-04:00 ngp tag_sys_msg: Apr 24 12:45:20 ngp nGP.Admin: File: [privateKey.key] shredded by user nGPadmin from (10.100.0.137). 2020-04-24T12:45:25-04:00 ngp tag_sys_msg: Apr 24 12:45:20 ngp nGP.Admin: File: [server.crt] shredded by user nGPadmin from (10.100.0.137). 2020-04-24T12:45:25-04:00 ngp tag_sys_msg: Apr 24 12:45:20 ngp nGP.Admin: File: [dhparams.pem] shredded by user nGPadmin from (10.100.0.137).
	Resetting passwords	2020-04-06T13:59:00-04:00 ngp tag_sys_msg: Apr 6 13:58:55 ngp passwd: pam_unix(passwd:chauthtok): password changed for nGPadmin
	Web session lockout settings	2020-04-06T12:29:22-04:00 ngp tag_api_log: 2020-04-06T16:29:15.519Z - #033[32minfo#033[39m: [authentication.audit] User administrator managed web user account settings, lockout time after multiple login failures rule changed from 15minutes to 3minutes 2020-04-06T12:29:22-04:00 ngp tag_api_log: 2020-04-06T16:29:15.519Z - #033[32minfo#033[39m: [authentication.audit] User administrator managed web user account settings, number of login failures to lockout rule changed from 6 to 3

Requirement	Auditable Events	Example Event
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	2020-04-17T14:53:43-04:00 ngp tag_nginx_err: 2020/04/17 14:53:35 [info] 21253#21253: *51332 SSL_do_handshake() failed (SSL: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher) while SSL handshaking, client: 10.100.0.137, server: 0.0.0.0:443
FCS_SSHC_EXT.1	Failure to establish a SSH Session	Apr 21 11:18:30 ngp ngp-audit-tunnel.sh: Audit log forwarding tunnel to 10.100.0.33 failed to start Apr 21 11:18:30 ngp ngp-audit-tunnel.sh: Ssh exit code 255, Unable to negotiate with 10.100.0.33 port 22: no matching cipher found. Their offer: none
FCS_TLSS_EXT.1	Failure to establish a TLS Session	2020-04-17T14:53:43-04:00 ngp tag_nginx_err: 2020/04/17 14:53:35 [info] 21253#21253: *51332 SSL_do_handshake() failed (SSL: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher) while SSL handshaking, client: 10.100.0.137, server: 0.0.0.0:443
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	2020-04-06T12:33:32-04:00 ngp tag_api_log: 2020-04-06T16:33:27.262Z - #033[32minfo#033[39m: [authentication.audit] User administrator at 172.16.100.26 has been locked out 2020-04-06T11:36:59-04:00 ngp tag_sys_msg: Apr 6 11:36:55 ngp login: pam_faillock(login:auth): Consecutive login failures for user nGPadmin account temporarily locked
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	2020-04-08T03:18:14-04:00 ngp tag_sys_msg: Apr 8 03:18:05 ngp login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost= user=ngpuser
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	

Requirement	Auditable Events	Example Event
		2020-04-08T03:18:14-04:00 ngp tag_sys_msg: Apr 8 03:18:07 ngp login: FAILED LOGIN SESSION FROM tty1 FOR ngpuser, Permission denied 2020-04-08T02:29:42-04:00 ngp tag_sys_msg: Apr 8 02:29:34 ngp sshd[208135]: Accepted password for ngpuser from 10.100.0.137 port 34950 ssh2 2020-04-08T02:29:42-04:00 ngp tag_sys_msg: Apr 8 02:29:34 ngp systemd-logind: New session 1303 of user ngpuser. 2020-04-08T02:29:42-04:00 ngp tag_sys_msg: Apr 8 02:29:34 ngp systemd: Started Session 1303 of user ngpuser. 2020-04-08T02:29:42-04:00 ngp tag_sys_msg: Apr 8 02:29:34 ngp sshd[208135]: pam_unix(sshd:session): session opened for user ngpuser by (uid=0) 2020-04-08T02:29:52-04:00 ngp tag_sys_msg: Apr 8 02:29:44 ngp ngpuser: [authentication.audit] User ngpuser has logged out 2020-04-08T02:29:52-04:00 ngp tag_sys_msg: Apr 8 02:29:44 ngp ngpuser: [authentication.audit] User ngpuser has logged out 2020-04-08T02:29:52-04:00 ngp tag_sys_msg: Apr 8 02:29:44 ngp sshd[208169]: Received disconnect from 10.100.0.137 port 34950:11: disconnected by user 2020-04-08T02:29:52-04:00 ngp tag_sys_msg: Apr 8 02:29:44 ngp sshd[208169]: Disconnected from user ngpuser 10.100.0.137 port 34950 2020-04-08T02:29:52-04:00 ngp tag_sys_msg: Apr 8 02:29:44 ngp sshd[208135]:

Requirement	Auditable Events	Example Event
		pam_unix(sshd:session): session closed for user ngpuser 2020-04-08T02:29:52-04:00 ngp tag_sys_msg: Apr 8 02:29:44 ngp systemd-logind: Removed session 1303.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Import of CAs failure 2020-04-21T00:14:30-04:00 ngp tag_sys_msg: Apr 21 00:14:22 ngp nGP.Admin: A new Trusted CA imported failed, certificate sha256 hash = defdea80160cfdbb364b7867d26ee4ff0739bc9337155b6564bec1bc40f7e64d , by user nGPadmin from (10.100.0.137). Importing a new trusted CA 2020-04-17T17:14:29-04:00 ngp tag_sys_msg: Apr 17 17:14:21 ngp nGP.Admin: Successfully imported certificate, with certificate ID (public key hash): d0c33b9e14ffb67dc52bfb82a8b13b3d53a57a0935544f09c2a94e32ac2c824f, by user nGPadmin from (10.100.0.137). 2020-04-17T17:14:29-04:00 ngp tag_sys_msg: Apr 17 17:14:21 ngp nGP.Admin: A new Trusted CA imported, by user nGPadmin from (10.100.0.137). Attempt install the leaf certificate fails due to the chain verification failure 2020-04-17T18:03:51-04:00 ngp tag_sys_msg: Apr 17 18:03:51 ngp nGP.Admin: Certificate Chain verification failed, try importing valid trust certificates via option number 7 in this program.. Error message: ngp_server.cert.pem: C = CA, ST = ON, L = Ottawa, O = Lightship Security, OU = CC1901, CN = 10.19.1.10error 20 at 0 depth lookup:unable to get local issuer

Requirement	Auditable Events	Example Event
		certificate , by user nGPadmin from (10.100.0.137). Delete the intermediate CA: 2020-04-17T18:16:12-04:00 ngp tag_api_log: 2020-04-17T22:16:10.426Z - #033[32minfo#033[39m: [nGP.Admin] User administrator successfully deleted trust certificate with hash = ab0a8bf12d7da5f5af1f1b860e1e2d9948fac41274bbe6a02f478ba8b89eb5b3 using GUI
FIA_X509_EXT.2	TOE is unable to verify the validity of the certificate due to network connection problem	
FIA_X509_EXT.3	Create CSR	2020-04-17T18:02:01-04:00 ngp tag_sys_msg: Apr 17 18:01:52 ngp nGP.Admin: ngp-install-ssl-certificate is being run. user=root, pid=45301, shell=/bin/bash, shell_info=nGPadmin pts/0 2020-04-17 17:58 (10.100.0.137) 2020-04-17T18:02:01-04:00 ngp tag_sys_msg: Apr 17 18:01:57 ngp nGP.Admin: Generating CSR with private key ID (public key hash): d1c23f0bf970c141968fa3e4d99c525f41edd037be9d4c78f28832378d68f295, by user nGPadmin from (10.100.0.137). 2020-04-17T18:02:31-04:00 ngp tag_sys_msg: Apr 17 18:02:23 ngp nGP.Admin: CSR generated, by user nGPadmin from (10.100.0.137).
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	No manual update option available to non- privileged user Audit event for administrator 2020-04-09T03:01:03-04:00 ngp tag_api_log: 2020-04-09T07:01:02.329Z - #033[32minfo#033[39m: [upgrade.audit] Firmware upgrade

Requirement	Auditable Events	Example Event
		started by administrator from 172.16.100.26 10:17 2020-04-09T03:05:54-04:00 ngp tag_appliance_log: Upgrade to version 3.2.525-1 complete. 10:18 2020-04-09T03:05:54-04:00 ngp tag_appliance_log: ***Finished: appliance/package/upgrade/install.sh***
FMT_MOF.1/Functions	Modification of the behaviour of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full.	
FMT_SMF.1	All management activities of TSF data.	2020-04-14T15:23:18-04:00 ngp tag_sys_msg: Apr 14 15:23:12 ngp nGP.Admin: Enabled the Console banner 2020-04-14T15:23:18-04:00 ngp tag_sys_msg: Apr 14 15:23:12 ngp nGP.Admin: Console banner text changed to: ##012 TEST BANNER!!#012 CLI#012CC1901 - NDcPP - FTA_TAB.1 TESTING#012##
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	2020-04-09T03:01:23-04:00 ngp tag_sys_msg: Apr 9 03:01:16 ngp ngp-upgrade.sh: The checksum matches the file, "ngp-upgrade.tar.gz" 2020-04-09T03:01:23-04:00 ngp tag_sys_msg: Apr 9 03:01:16 ngp nGP.Admin: The checksum matches the file, "ngp-upgrade.tar.gz" 2020-04-09T03:01:23-04:00 ngp tag_sys_msg: Apr 9 03:01:16 ngp nGP.Admin: The checksum

Requirement	Auditable Events	Example Event
		matches the file, "ngp-upgrade.tar.gz" 2020-04-09T03:01:03-04:00 ngp tag_api_log: 2020-04-09T07:01:02.329Z - #033[32minfo#033[39m: [upgrade.audit] Firmware upgrade started by administrator from 172.16.100.26 2020-04-09T03:05:54-04:00 ngp tag_appliance_log: System is healthy. 2020-04-09T03:05:54-04:00 ngp tag_appliance_log: Upgrade to version 3.2.525-1 complete. 2020-04-09T03:05:54-04:00 ngp tag_appliance_log: Thu Apr 9 03:05:50 EDT 2020 2020-04-09T03:05:54-04:00 ngp tag_appliance_log: ***Finished: appliance/package/upgrade/install.sh***
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)	2020-04-10T18:00:05-04:00 ngp tag_sys_msg: Apr 9 04:08:29 ngp sudo: nGPadmin : TTY=pts/0 ; PWD=/home/nGPadmin ; USER=root ; COMMAND=/opt/ngp/configure/ngp-date.sh 041018002020.00 2020-04-10T18:00:05-04:00 ngp tag_sys_msg: Apr 9 04:08:29 ngp sudo: pam_unix(sudo:session): session opened for user root by nGPadmin(uid=0) 2020-04-10T18:00:05-04:00 ngp tag_sys_msg: Apr 09 04:08:29 root ngp-date: entry_time=Thu Apr 9 04:08:29 EDT 2020, user=root, pid=24124, shell=/bin/bash 2020-04-10T18:00:05-04:00 ngp tag_sys_msg: Apr 09 04:08:29 root ngp-date: shell_info=nGPadmin pts/0 2020-04-09 03:59 (10.100.0.137)

Requirement	Auditable Events	Example Event
		2020-04-10T18:00:05-04:00 ngp tag_sys_msg: Apr 10 18:00:00 ngp systemd: Time has been changed
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	2020-04-10T18:10:45-04:00 ngp tag_sys_msg: Apr 10 18:10:44 ngp nGPadmin: [authentication.audit] User nGPadmin has exceeded inactivity time of 60 seconds and has been logged out
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	2020-04-10T18:51:57-04:00 ngp tag_sys_msg: Apr 10 18:51:51 ngp ngpuser: [authentication.audit] User ngpuser has exceeded inactivity time of 60 seconds and has been logged out 2020-04-10T18:51:57-04:00 ngp tag_sys_msg: Apr 10 18:51:51 ngp sshd[50258]: Received disconnect from 10.100.0.137 port 35092:11: disconnected by user 2020-04-10T18:51:57-04:00 ngp tag_sys_msg: Apr 10 18:51:51 ngp sshd[50258]: Disconnected from user ngpuser 10.100.0.137 port 35092 2020-04-10T18:51:57-04:00 ngp tag_sys_msg: Apr 10 18:51:51 ngp sshd[50200]: pam_unix(sshd:session): session closed for user ngpuser 2020-04-10T18:51:57-04:00 ngp tag_sys_msg: Apr 10 18:51:51 ngp systemd-logind: Removed session 21. 2020-04-10T18:51:57-04:00 ngp tag_sys_msg: Apr 10 18:51:51 ngp systemd: Removed slice User Slice of ngpuser. 2020-04-10T18:52:57-04:00 ngp tag_sys_msg: Apr 10 18:52:49 ngp nGPadmin: [authentication.audit] User nGPadmin has exceeded inactivity time of 60 seconds and has been logged out

Requirement	Auditable Events	Example Event
FTA_SSL.4	The termination of an interactive session.	2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp nGPadmin: [authentication.audit] User nGPadmin has logged out 2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp login: pam_unix(login:session): session closed for user nGPadmin 2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp systemd: getty@tty1.service has no holdoff time, scheduling restart. 2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp systemd: Stopped Getty on tty1. 2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp systemd: Started Getty on tty1. 2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp systemd-logind: Removed session 669. 2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp systemd: Removed slice User Slice of nGPadmin. 2020-04-14T13:46:03-04:00 ngp tag_sys_msg: Apr 14 13:45:55 ngp nGPadmin: [authentication.audit] User nGPadmin has logged out
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Apr 14 17:19:28 ngp sudo: nGPadmin : TTY=pts/1 ; PWD=/home/nGPadmin ; USER=root ; COMMAND=/opt/ngp/log-audit/local/ngp-log-audit.sh root 10.100.0.33 YJ5X3MLsGAwn1jAPJvQDMzkBXutSbhwDRnF9jFPQh8Y Apr 14 17:19:29 ngp systemd: Starting SSH tunnel for remote audit daemon... Apr 14 17:19:29 ngp ngp-audit-tunnel.sh: Audit log forwarding tunnel starting ... Apr 14 17:19:29 ngp ngp-audit-tunnel.sh: Audit log forwarding

Requirement	Auditable Events	Example Event
		tunnel to 10.100.0.33 started. PID 239967 Apr 14 17:19:29 ngp systemd: Started SSH tunnel for remote audit daemon. Apr 14 17:18:27 ngp sudo: nGPadmin : TTY=pts/1 ; PWD=/home/nGPadmin ; USER=root ; COMMAND=/opt/ngp/log-audit/local/ngp-log-audit.sh root 10.100.0.33 YJ5X3MLsGAwn1jAPJvQDMzkBXutSbhwDRnF9jFPQh8X Apr 14 17:18:28 ngp systemd: Stopping SSH tunnel for remote audit daemon... Apr 14 17:18:28 ngp ngp-audit-tunnel.sh: Audit log forwarding tunnel starting ... Apr 14 17:18:28 ngp ngp-audit-tunnel.sh: /opt/ngp/log-audit/local/ngp-audit-tunnel.sh: line 16: kill: SIGHUP: arguments must be process or job IDs Apr 14 17:18:28 ngp rsyslogd: action 'action 0' suspended, next retry is Tue Apr 14 17:18:58 2020 [v8.24.0-38.el7 try http://www.rsyslog.com/e/2007] Apr 14 17:18:28 ngp ngp-audit-tunnel.sh: Audit log forwarding tunnel is stopped
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	Initiation of the trusted path: 2020-04-08T02:48:03-04:00 ngp tag_sys_msg: Apr 8 02:47:57 ngp sshd[217710]: Accepted publickey for nGPadmin from 10.100.0.137 port 34960 ssh2: RSA SHA256:oUF8beg9j1CLvGCgXcHYEgQvaJO466w35rEYz1wcdaY 2020-04-08T02:48:03-04:00 ngp tag_sys_msg: Apr 8 02:47:57 ngp systemd: Created slice User Slice of nGPadmin.

Requirement	Auditable Events	Example Event
		2020-04-08T02:48:03-04:00 ngp tag_sys_msg: Apr 8 02:47:57 ngp systemd-logind: New session 1310 of user nGPadmin. 2020-04-08T02:48:03-04:00 ngp tag_sys_msg: Apr 8 02:47:57 ngp systemd: Started Session 1310 of user nGPadmin. 2020-04-08T02:48:03-04:00 ngp tag_sys_msg: Apr 8 02:47:57 ngp sshd[217710]: pam_unix(sshd:session): session opened for user nGPadmin by (uid=0) Termination of the trusted path: 2020-04-14T14:05:44-04:00 ngp tag_sys_msg: Apr 14 14:05:37 ngp ngpuser: [authentication.audit] User ngpuser has logged out 2020-04-14T14:05:44-04:00 ngp tag_sys_msg: Apr 14 14:05:37 ngp sshd[141166]: Received disconnect from 10.100.0.137 port 35444:11: disconnected by user 2020-04-14T14:05:44-04:00 ngp tag_sys_msg: Apr 14 14:05:37 ngp sshd[141166]: Disconnected from user ngpuser 10.100.0.137 port 35444 2020-04-14T14:05:44-04:00 ngp tag_sys_msg: Apr 14 14:05:37 ngp sshd[141100]: pam_unix(sshd:session): session closed for user ngpuser 2020-04-14T14:05:44-04:00 ngp tag_sys_msg: Apr 14 14:05:37 ngp systemd-logind: Removed session 673. 2020-04-14T14:05:44-04:00 ngp tag_sys_msg: Apr 14 14:05:37 ngp systemd: Removed slice User Slice of ngpuser. Failure of the trusted path functions:

Requirement	Auditable Events	Example Event
		2020-04-16T14:45:36-04:00 ngp tag_sys_msg: Apr 16 14:45:26 ngp sshd[16440]: Bad packet length 263180. 2020-04-16T14:45:36-04:00 ngp tag_sys_msg: Apr 16 14:45:26 ngp sshd[16440]: ssh_dispatch_run_fatal: Connection from user ngpuser 10.100.0.137 port 35692: message authentication code incorrect 2020-04-16T14:45:36-04:00 ngp tag_sys_msg: Apr 16 14:45:26 ngp sshd[16438]: pam_unix(sshd:session): session closed for user ngpuser 2020-04-16T14:45:36-04:00 ngp tag_sys_msg: Apr 16 14:45:26 ngp systemd-logind: Removed session 1032. 2020-04-16T14:45:36-04:00 ngp tag_sys_msg: Apr 16 14:45:26 ngp systemd: Removed slice User Slice of ngpuser.

Firmware Integrity Tests

```
Wed Jul  1 22:03:36 UTC 2020 ------------------------------------------------
Wed Jul  1 22:03:36 UTC 2020 Starting Common Criteria Checks
Wed Jul  1 22:03:36 UTC 2020 Certificate Check: Start
Wed Jul  1 22:04:06 UTC 2020 Validating current SSL certificate in nGPULSE: OK
Wed Jul  1 22:04:06 UTC 2020 Certificate Check: End 30 seconds
Wed Jul  1 22:04:06 UTC 2020 Application Integrity check: Start
Wed Jul  1 22:04:24 UTC 2020 Verifying:    mongodb-org-mongos-3.6.3-1.el7.x86_64  [Ok]
Wed Jul  1 22:04:24 UTC 2020 Verifying:                ngp-fips-3.2.47-1.x86_64  [Ok]
Wed Jul  1 22:04:24 UTC 2020 Verifying:                   redis-3.2.10-1.x86_64  [Ok]
Wed Jul  1 22:04:25 UTC 2020 Verifying:                ipm-smon-3.2.14-1.x86_64  [Ok]
Wed Jul  1 22:04:25 UTC 2020 Verifying:               log-audit-3.2.92-1.x86_64  [Ok]
Wed Jul  1 22:04:25 UTC 2020 Verifying:       systemd-sysv-219-67.el7_7.1.x86_64  [Ok]
Wed Jul  1 22:04:26 UTC 2020 Verifying:                ipm-plmc-3.2.18-1.x86_64  [Ok]
Wed Jul  1 22:04:27 UTC 2020 Verifying:                ipm-nmon-3.2.17-1.x86_64  [Ok]
Wed Jul  1 22:04:27 UTC 2020 Verifying:    mongodb-org-server-3.6.3-1.el7.x86_64  [Ok]
Wed Jul  1 22:04:29 UTC 2020 Verifying:                ngp-kafka-3.2.4-1.x86_64  [Ok]
Wed Jul  1 22:04:29 UTC 2020 Verifying:                ngp-rngd-3.2.92-1.x86_64  [Ok]
Wed Jul  1 22:04:29 UTC 2020 Verifying:            audit-libs-2.8.5-4.el7.x86_64  [Ok]
Wed Jul  1 22:04:29 UTC 2020 Verifying:             rsyslog-8.24.0-38.el7.x86_64  [Ok]
Wed Jul  1 22:04:49 UTC 2020 Verifying:                ipm-assets-3.2.1-1.x86_64  [Ok]
Wed Jul  1 22:04:49 UTC 2020 Verifying:                ipm-query-3.2.36-1.x86_64  [Ok]
Wed Jul  1 22:04:50 UTC 2020 Verifying:                ngp-wmon-3.2.14-1.x86_64  [Ok]
Wed Jul  1 22:04:50 UTC 2020 Verifying:               ipm-proxy-3.2.92-1.x86_64  [Ok]
Wed Jul  1 22:04:50 UTC 2020 Verifying:     mongodb-org-shell-3.6.3-1.el7.x86_64  [Ok]
Wed Jul  1 22:04:51 UTC 2020 Verifying:       systemd-libs-219-67.el7_7.1.x86_64  [Ok]
Wed Jul  1 22:04:51 UTC 2020 Verifying:        ngp-entity-access-3.2.14-1.x86_64  [Ok]
Wed Jul  1 22:04:51 UTC 2020 Verifying:               ipm-winrm-3.2.14-1.x86_64  [Ok]
Wed Jul  1 22:04:52 UTC 2020 Verifying:                ipm-ping-3.2.15-1.x86_64  [Ok]
Wed Jul  1 22:04:53 UTC 2020 Verifying:           ipm-analytics-3.2.25-1.x86_64  [Ok]
Wed Jul  1 22:04:53 UTC 2020 Verifying:                  ngp-cli-3.2.1-1.x86_64  [Ok]
Wed Jul  1 22:04:53 UTC 2020 Verifying:         ipm-portal-fonts-3.2.92-1.x86_64  [Ok]
Wed Jul  1 22:04:53 UTC 2020 Verifying:              ipm-manager-3.2.92-1.x86_64  [Ok]
Wed Jul  1 22:04:54 UTC 2020 Verifying:         ngp-openssh-fips-3.2.47-1.x86_64  [Ok]
Wed Jul  1 22:05:16 UTC 2020 Verifying:               ipm-portal-3.2.77-1.x86_64  [Ok]
Wed Jul  1 22:05:16 UTC 2020 Verifying:                 audit-2.8.5-4.el7.x86_64  [Ok]
Wed Jul  1 22:05:16 UTC 2020 Verifying:          cassandra-tools-3.11.4-1.noarch  [Ok]
```

Requirement	Auditable Events	Example Event

```
Wed Jul  1 22:05:17 UTC 2020 Verifying:                ngp-server-3.2.43-1.x86_64  [Ok]
Wed Jul  1 22:05:18 UTC 2020 Verifying:                ipm-syslog-3.2.14-1.x86_64  [Ok]
Wed Jul  1 22:05:25 UTC 2020 Verifying:          ipm-bind-service-3.2.3-1.x86_64  [Ok]
Wed Jul  1 22:05:25 UTC 2020 Verifying:     mongodb-org-tools-3.6.3-1.el7.x86_64  [Ok]
Wed Jul  1 22:05:30 UTC 2020 Verifying:                 ipm-xms-3.2.64-1.x86_64  [Ok]
Wed Jul  1 22:05:30 UTC 2020 Verifying:               ngp-ocsp-3.2.92-1.x86_64  [Ok]
Wed Jul  1 22:05:31 UTC 2020 Verifying:           ngp-nginx-fips-3.2.47-1.x86_64  [Ok]
Wed Jul  1 22:05:32 UTC 2020 Verifying:            systemd-219-67.el7_7.1.x86_64  [Ok]
Wed Jul  1 22:05:33 UTC 2020 Verifying:            ipm-ng1import-3.2.16-1.x86_64  [Ok]
Wed Jul  1 22:05:33 UTC 2020 Verifying:                 ipm-vmon-3.2.17-1.x86_64  [Ok]
Wed Jul  1 22:05:33 UTC 2020 Verifying:           mongodb-org-3.6.3-1.el7.x86_64  [Ok]
Wed Jul  1 22:05:34 UTC 2020 Verifying:                 ipm-dds-3.2.92-1.x86_64  [Ok]
Wed Jul  1 22:05:34 UTC 2020 Verifying:              cassandra-3.11.4-1.noarch  [Ok]
Wed Jul  1 22:05:35 UTC 2020 Verifying:            elasticsearch-5.5.0-1.noarch  [Ok]
Wed Jul  1 22:05:35 UTC 2020 Verifying:               ngp-backup-3.2.8-1.x86_64  [Ok]
Wed Jul  1 22:05:35 UTC 2020 Verifying:                ipm-plcc-3.2.21-1.x86_64  [Ok]
Wed Jul  1 22:05:37 UTC 2020 Verifying:           ngp-configure-3.2.117-1.x86_64  [Ok]
Wed Jul  1 22:05:38 UTC 2020 Verifying:         ngp-openssl-fips-3.2.47-1.x86_64  [Ok]
Wed Jul  1 22:05:38 UTC 2020 Application Integrity check: End 92 seconds
```