CAE Inc.

MPIC v3.0.66

Common Criteria Guide

Version 1.1

October 2022

Document prepared by

Lightship Security

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 MPIC v3.0.66 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 Target of Evaluation (TOE) includes the CAE “cae-mx6qmpic-3.0.37” software running on hardware appliances:

- MPIC
- MPIC-PCMIP
- MPIC-EMB

1.3.3 Evaluated Functions

6 The following functions have been evaluated under Common Criteria:

- **Protected Communications.** The TOE provides secure communication channels:
  i) **CLI.** Administrator access to the CLI via direct serial connection or SSH.
  ii) **Logs.** Secure transmission of log events to a Syslog server via SSH.
  iii) **NTP.** Secure time synchronization from remote NTP server.
- **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

- **Trusted Update.** The TOE ensures the authenticity and integrity of software updates via digital signature.
- **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.
- **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.
- **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 one of its core functions 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.

Assumption	Guidance
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 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 Common Criteria evaluation focused on the management plane of the device.
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.

1.4 Conventions

9 The following conventions are used in this guide:

- `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

- [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.

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

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

- [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 which are made available from the vendor.

Table 2: Related Documents

Reference	Document
[ADMIN]	Getting Started with MPIC Developer's Guide TPD 20365 Rev 7 , 20 Oct 2022

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 CAE MPIC will be delivered via commercial courier. Perform the following checks upon receipt (return the device if either of the checks fail):

- Confirm that the correct device has been delivered
- Inspect the packaging to confirm that there are no signs of tampering

13 Follow instructions at [ADMIN] Order of Installation and Setup to setup the TOE.

2.2 Verifying the TOE

14 After logging in as a system administrator use the `version` command to check current version of the software. See section 2.4 for Installation/Update instructions.

2.3 Power-on Self-Tests

15 At startup, or when initiated by a Security Administrator, the TOE undergoes the following tests:

- Integrity checks for the following packages: openssl-fips, openssl, openssh, cae-commands, cae-commands-extended.
- OpenSSL cryptographic module self-tests

16 These tests ensure the correct operation of the cryptographic functionality of the MPIC, the FIPS module and that the correct MPIC image is being used. The cryptographic functionality will not be available if the tests fail, and any operation of the MPIC supported by this functionality will not be available.

17 When a test fails it will be indicated by the name of the test that is run along with a “[FAILED]” value following it. If integrity tests fail it will also indicate which file has been affected. If the TOE fails any of the above tests, the administrator should attempt to reinstall the most current image. If the tests continue to fail post reinstall, the administrator should contact the vendor for support.

2.4 Updating and Installing the TOE

18 The TOE software packages are signed using a digital signature and are verified by the TOE when installation/upgrades are performed. Upgrade packages are delivered by the Vendor directly.

19 Perform the following to upgrade the TOE:

20 Connect to the TOE either over SSH or Serial using “admin”

21 Upload image files to the TOE using the following command:

22
```
scp [user]@<ip>/path/<image_file> /home/admin
```

23 Reboot on the rescue partition with the command: `power reboot --rescue`

24 Reconnect to the TOE using SSH or SERIAL USB. You should have a message “[RESCUE]” on the terminal.

25 Update the image with: `update-image <image_file>`

26 Once updating is finished reboot to normal mode: `power reboot --normal`

3 Configuration Guidance

3.1 Installation

27 Before beginning the instructions in the [ADMIN] documentation, first by using the root account, modify the value of `maxlogins` in `/etc/security/limits.conf` from 1 to at least 2. Next modify `PASS_MIN_DAYS` in `/etc/login.defs` from 1 to 0 to increase the frequency that passwords may be changed. Modify the `/etc/ntp.conf` and add `logconfig=all` to the end of the file.

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

29 After completing the configurations steps in [ADMIN], use the `mount -o remount,rw /` command as root, this is the final step in configuring the TOE.

3.2 Administration Interfaces

30 Only the following administration interfaces may be used:

- **CLI/Console.** Directly connected via Type B Micro USB to Type A USB Cable.
  - i) Inactivity timeout period can be configured with the following, `config set-timeout <#>, config reset-timeout`
  - ii) Authentication failure and lockout time can be configured with the following, `config set-deny-count <#>, config reset-deny-count, set-unlock-time <#>, reset-unlock-time`
  - iii) Local and remote sessions are terminated using, `exit`.
  - iv) Banner message can be configured using, `banner set <filename>`, `banner set-text <text>`.
- **CLI/SSH.** Remote access to the CLI interface via SSH.
  - i) All configurations in CLI/Console apply to SSH interactive sessions.
  - ii) Public key authentication can be configured using the `authentication add-key <type> <value> <name>` command.

3.3 Cryptography

31 FIPS mode is enabled by default. No further configuration is required to achieve the Common Criteria cryptographic configuration.

32 To generate a new Host key for the TOE: `ssh-config new-host-keys`

33 To generate SSH public keys: `ssh-config generate-auth-key -name <filename> -size [2048|3072|4096]`

34 Host keys for external IT entities can be added using: `ssh-config add-host <ip> <algorithm> <key>`

35 Host keys for remote syslog servers must be preconfigured on the TOE before a connection can occur.

36 Keys can be deleted by using the following commands:

- TOE Host keys are deleted when a new key is generated using the `ssh-config new-host-keys` command
- External host keys: `ssh-config remove-host <name>`
- TOE public key: `ssh-config remove-auth-key <filename>`
- NTP keys: `ntp remove-key <index>`

3.4 Default Passwords

37 The following passwords have default values that must be changed:

- **admin**. Default account. Follow the instructions at [ADMIN] Change Password to set a new password for this account.

38 Passwords may contain “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” special characters, uppercase letters, lowercase letters, numbers and must have a minimum length of 15 characters.

3.5 Setting Time

39 The TOE will sync it’s time via NTP. Follow the instructions at [ADMIN] *Add/Remove NTP servers* section 4.12 on page 20 to configure NTP.

40 NTP time setting is stopped when there are no configured NTP servers.

41 No additional configuration is needed to reject broadcast or multicast time updates.

3.6 Audit Logging

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

43 A syslog / other server must be configured to store the logs as follows:

- Refer to the [ADMIN] *Add SSH host to known hosts*, to configure the known hosts file for the trusted channel.
- Refer to the [ADMIN] *Configure rsyslog for remote logging*, to configure a host over SSH and enable the trusted channel. The command to configure an SSH remote logging host is: `remote-syslog enable <user>@<host> --ssh`

44 Once remote logging is configured the TOE will send logs to the remote host in real time.

45 The TOE also stores logs locally. Logs are rotated weekly with up to 4 backlogs kept, the oldest is overwritten when the backlog is full.

46 Should the connection to the trusted syslog server be unintentionally broken, the TOE will continue to attempt to connect automatically. If the disconnect persists, the administrator should use `remote-syslog disable` to stop the audit function and `remote-syslog enable <user>@<host> --ssh` to begin the connection again.

47

3.7 Administrator Authentication

48 Using the instructions at [ADMIN] *Changing parameters,* configure session lockout, lockout period and inactivity timeout settings for the administrative user. Administrator access is always available at the local CLI, no additional configuration is needed.

49 When setting the administrative user's session lockout count, the value should be set 1 value higher than the desired amount as there is an initial failure to login on every connection due to an attempt using a public key. Setting the value to 1 will result in the Security Administrator being locked out of the device immediately and setting the value to 0 will disable the lockout mechanism altogether, allowing for infinite attempts to login to the device. It is advised that this value be set to at least 2.

50 An alternative to circumvent the initial login failure, due to the public key attempt, is to explicitly configure the use of password only authentication on the Administrators client-side interface. With this configuration the TOE will not increase the tally of attempts before a password is used.

51 Refer to [ADMIN] *Change password*, to configure the administrator password and [ADMIN] *Authenticate with a key*, to configure public key authentication.

52 The instructions at [ADMIN] *Create new SSH host-keys*, can be used to generate new keys for the MPIC SSH server.

3.8 Trusted Channel

53 The audit tunnel is protected by SSH from the MPIC to the syslog server. Follow the instructions at [ADMIN] *Add SSH host to known hosts* to add a trusted syslog server to the known hosts file.

54 Follow the instructions at [ADMIN] *Configure rsyslog for remote logging*, to add the trusted server to the syslog configuration and to generate a key pair for the MPIC for public key authentication to the syslog server.

55 The TOE ssh client connection does not have configurable parameters and no additional configuration is needed.

4 Annex A: Log Reference

4.1 Format

56 Each audit record includes the following fields:

- Timestamp
- Origin of message (rsyslogd, ssh, tag_audit_log)
- Message (including user if applicable and indication of success or failure).

4.2 Events

57 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	2022-03-23 15:49:48 starting rsyslogd ... done 2022-03-23 15:49:37 EMB01 tag_audit_log:type=EXECVE msg=audit(1648075777.950:320) : argc=4 a0="/usr/bin/sudo" a1="-n" a2="/etc/init.d/syslog" a3="stop"
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	2021-09-16 21:41:13 LIGHTSHIP NTP servers were added : 10.121.1.2 2021-09-16 21:43:27 LIGHTSHIP NTP servers were removed : 10.121.1.2
FCS_SSHC_EXT.1	Failure to establish an SSH Session	2021-09-14 18:56:41 LIGHTSHIP rsyslogd: cannot connect to X.X.X.X:1468: Connection refused [v8.37.0 tr y http://www.rsyslog.com/e/2027]
FCS_SSHS_EXT.1	Failure to establish an SSH Session	2021-09-15 13:33:03 LIGHTSHIP tag_audit_log: type=USER_LOGIN msg=audit(1631712782.686:998) : pid=20382 uid=0 auid=0 ses=1 msg='op=login acct="admin" exe="/usr/sbin/sshd" hostname=? addr=10.100.1.156 terminal=sshd res=failed'
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	2021-09-15 13:42:25 LIGHTSHIP sshd[22837]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.100.1.156 user=admin
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	2021-09-15 16:02:57 LIGHTSHIP tag_audit_log: type=USER_LOGIN msg=audit(1631721774.663:1499): pid=28650 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="admin" exe="/bin/login.shadow" hostname=LIGHTSHIP addr=?

Requirement	Auditable Events	Example Event
		terminal=/dev/ttymxc1 res=success'
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	2021-09-15 13:42:25 LIGHTSHIP sshd[22837]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=X.X.X.X user=admin
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	Sep 15 14:58:06 LIGHTSHIP update-image started
FMT_SMF.1	All management activities of TSF data.	NTP: 2021-09-16 21:41:13 LIGHTSHIP NTP servers were added : 10.121.1.2 use of login 2021-09-15 15:37:47 LIGHTSHIP sshd[21761]: Accepted password for admin from X.X.X.X port 61268 ssh2 2021-09-17 17:58:24 LIGHTSHIP sshd[27126]: Close session: user admin from X.X.X.X port 54975 id 0 2021-09-15 17:49:44 LIGHTSHIP tag_audit_log: type=USER_LOGIN msg=audit(1631728174.398:1856): pid=25163 uid=0 auid=0 ses=1 msg='op=login acct="admin" exe="/usr/sbin/sshd" hostname=? addr= X.X.X.X terminal=sshd res=failed' Set timeout: 2022-07-12 14:58:10 LIGHTSHIP config[29079]: admin: parameter "timeout" changed to "300" Manage Keys: 2022-07-12 15:12:30 mx6qmpic ssh-config[27996]: admin: Host

Requirement	Auditable Events	Example Event
		X.X.X.X was added to known_hosts 2022-07-12 15:16:01 mx6qmpic ssh-config[23980]: root: Authentication key "/home/.etc/ssh/rsa" has been generated 2022-07-12 15:17:50 mx6qmpic ssh-config[27837]: admin: Host X.X.X.X was removed from known_hosts Changed Password 2022-07-12 15:20:31 LIGHTSHIP passwd[6921]: pam_unix(passwd:chauthtok): password changed for admin 2022-07-12 15:20:31 LIGHTSHIP authentication[6906]: admin: password changed Set Banner 2022-03-03 18:14:04 EMB01 tag_audit_log: type=SYSCALL msg=audit(1646349223.790:1085): arch=40000028 syscall=322 per=800000 success=no exit=-13 a0=ffffff9c a1=768eea80 a2=a00c1 a3=1a4 items=1 ppid=15502 pid=21851 auid=1200 uid=1200 gid=1200 euid=1200 suid=1200 fsuid=1200 egid=1200 sgid=1200 fsgid=1200 tty=pts0 ses=3 comm="banner" exe="/usr/bin/python3.5" key="access" 2022-03-03 18:15:14 EMB01 tag_audit_log: type=SYSCALL msg=audit(1646349223.790:1085): arch=40000028 syscall=322 per=800000 success=no exit=-13 a0=ffffff9c a1=768eea80

Requirement	Auditable Events	Example Event
		a2=a00c1 a3=1a4 items=1 ppid=15502 pid=21851 auid=1200 uid=1200 gid=1200 euid=1200 suid=1200 fsuid=1200 egid=1200 sgid=1200 fsgid=1200 tty=pts0 ses=3 comm="banner" exe="/usr/bin/python3.5" key="delete" Start and stop services: 2022-07-12 15:30:05 LIGHTSHIP tag_audit_log:type=EXECVE msg=audit(1643178161.842:21982): argc=4 a0="/usr/bin/sudo" a1="-n" a2="/etc/init.d/ntpd" a3="restart" 2022-07-12 15:33:05 LIGHTSHIP ntpd[6265]: ntpd 4.2.8p12@1.3728-o Tue Aug 14 12:30:47 UTC 2018 (2): Starting 2022-07-12 15:35:05 LIGHTSHIP ntpd[20012]: ntpd exiting on signal 15 (Terminated)
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	2021-09-15 14:58:47 LIGHTSHIP update-image failed 2022-07-12 15:21:18 LIGHTSHIP update-image[2370]: admin: update-image started 2022-07-12 15:22:50 LIGHTSHIP update-image[2370]: admin: update-image completed successfully
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)	2022-07-21 21:24:31 LIGHTSHIP ntpd[770]: 0.0.0.0 c61c 0c clock_step +4045.003394 s 2022-07-21 21:24:31LIGHTSHIP ntpd[820]: 0.0.0.0 c614 04 freq_mode

Requirement	Auditable Events	Example Event
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	2021-09-15 16:01:53 LIGHTSHIP login[28199]: pam_unix(login:session): session closed for user admin
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	2021-09-15 15:28:47 LIGHTSHIP sshd[10773]: pam_unix(sshd:session): session closed for user admin
FTA_SSL.4	The termination of an interactive session.	2021-09-15 15:28:47 LIGHTSHIP sshd[10773]: pam_unix(sshd:session): session closed for user admin
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Initiation: 2021-09-14 19:26:08 LIGHTSHIP tag_audit_log: type=EXECVE msg=audit(1631645439.582:154) : argc=4 a0="/usr/bin/sudo" a1="-n" a2="/etc/init.d/syslog" a3="start" Termination 2021-09-16 21:21:27 LIGHTSHIP sudo: admin : TTY=pts/1 ; PWD=/home/admin ; USER=root ; COMMAND=/etc/init.d/syslog stop Failure: 2021-09-16 21:24:31 LIGHTSHIP /usr/bin/ssh[19325]: error: ssh: connect to host 10.100.1.156 port 22: Connection refused
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	Initiation: 2021-09-15 15:37:47 LIGHTSHIP sshd[21761]: Accepted password for admin from X.X.X.X port 61268 ssh2 Termination: 2021-09-17 17:58:24 LIGHTSHIP sshd[29079]: Close session: user admin from X.X.X.X port 54975 id 0

Requirement	Auditable Events	Example Event
		Failure: 2021-09-15 17:49:44 LIGHTSHIP tag_audit_log: type=USER_LOGIN msg=audit(1631728174.398:1856): pid=25163 uid=0 auid=0 ses=1 msg='op=login acct="admin" exe="/usr/sbin/sshd" hostname=? addr= X.X.X.X terminal=sshd res=failed'