

Moxa Industrial Linux 3.x (Debian 11) Manual for V3000 Series Computers

Version 1.0, May 2025

www.moxa.com/products



© 2025 Moxa Inc. All rights reserved.

Moxa Industrial Linux 3.x (Debian 11) Manual for V3000 Series Computers

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2025 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction	6
Moxa Industrial Linux 3	6
MIL3 on Moxa's V3000 Series.....	6
Eligible Computing Platforms	6
2. Getting Started	7
Connecting to the V Series Computer	7
Connecting via the SSH.....	7
Managing User Accounts	10
Default User Account and Password Policy	10
Creating and Deleting User Accounts	10
Modifying User Accounts	11
Changing the Password	11
Querying the System Image Version	11
Querying Device Information.....	12
Determining Available Drive Space.....	12
Shutting Down the Device.....	12
Shutting Down the Device.....	13
3. Device Configuration	14
BIOS Setup	14
Entering the BIOS Setup	14
How to Enable and Use AMT	16
Main Page	18
Advanced Settings.....	18
Security Settings.....	29
Power Settings.....	32
Exit Settings	33
Changing the Default Hostname	34
Localizing Your V Series Computer	34
Adjusting the Time	34
NTP Time Synchronization	35
Setting the Time Zone	36
4. Using and Managing Computer Interfaces	38
Moxa Computer Interface Manager (MCIM)	38
Configuring the Log Level	38
Device Information	38
LED Indicators	39
Storage and Partitions	40
Push Button.....	42
Serial Port	43
Ethernet Interface	45
Digital Input/Output (DIO)	46
Buzzer	47
Cellular Module Interface.....	48
Wi-Fi Module Interface	49
Socket Interface.....	49
Configuring the Real COM Mode	50
Moxa MCU Manager (MMM)	51
Manage LAN Bypass.....	52
App Watchdog Modes Control Utility	53
Upgrade Moxa MCU Manager (Only available on V3000 series 8 LAN models)	53
Moxa BIOS Manager.....	54
5. V3000 Configuring and Managing Networks	55
Moxa Connection Manager (MCM)	55
Setting Up MCM With a GUI-based Configurator	57
Overview.....	57
Cellular and Wi-Fi Failover/Failback	61
Connecting via P2P Wi-Fi for Remote Access	63
Checking the Network Status	65

Checking the Interface and Connection Status	65
Cellular Signal Strength	67
Monitoring the Data Usage	68
Upgrading the Cellular Modem Firmware.....	68
Cellular Network Diagnosis.....	69
Using API to Retrieve the MCM Status	69
6. System Installation and Update.....	70
System Installation From a USB	70
Offline or Online Upgrade Using MSU.....	71
Online Update via Secure APT	73
Querying the System Image Version.....	73
Failback Update	73
Managing the APT Repository.....	73
Updating Your System	74
Customization and Programming	74
Building an Application.....	74
Creating a Customized Image	75
7. Backup, Decommission, and Recovery	77
Creating a System Snapshot	78
Creating a System Backup	79
Setting the System to the Default.....	81
Decommissioning the System.....	81
System Failback Recovery	81
Customize the Boot Up Failure Criteria	83
8. Security Capabilities	84
Communication Integrity and Authentication	84
User Account Permissions and Privileges.....	84
Switching to the Root Privilege.....	84
Controlling Permissions and Privileges.....	85
Linux Login Policy	86
Invalid Login Attempts	86
Session Termination After Inactivity	86
Login Banner Message	86
Secure Boot and Disk Encryption	87
Trusted Platform Module (TPM 2.0)	87
Host Intrusion Detection	88
Default Monitored Files.....	88
How to Perform Authenticity and Integrity Checks on All Files	90
Intrusion Prevention.....	91
Network Security Monitoring	91
Firewall	92
Pre-configured Rule	93
Common nftable Usage	94
Rate Limiting	94
Mitigating a NTP Amplification Attack	95
Service and Ports.....	96
Managing Resources	98
Audit Log	100
Linux Audit log	100
Bootloader Audit Log	102
Audit Failure Response.....	103
Security Diagnosis Tool (Moxa Guardian)	104
Diagnosing Issues in the Current Security Configuration.....	104
Restoring the Security Configuration to the Default	106
9. Security Hardening Guide	107
Defense-in-depth Strategy.....	107
Installation	109
Physical Installation	109
Environment Requirement	109
Access Control	109

Security Configuration Check 110

Operation 110

Maintenance 111

Decommissioning..... 111

A. Software Process List112

1. Introduction

Moxa Industrial Linux 3

Moxa Industrial Linux 3 (MIL3) is an industrial-grade Linux distribution developed and maintained by Moxa to address the security, reliability, and long-term support needs of industrial automation systems such as transportation, energy, oil and gas, and manufacturing.

MIL3 is based on Debian 11 with kernel 5.10 and integrated with several feature sets designed to strengthen and accelerate user application development as well as ensure system reliability and security.

MIL3 on Moxa's V3000 Series

MIL3 comes preinstalled with the default Debian 11 security configuration, Secure Boot, and additional security tools/utilities on the V3000 Series computers.

The following table lists the main features:

OS/bootloader	
TPM 2.0	✓
Security features	
Boot Guard (CPU validates Bootloader & BIOS are expected supported by root of trust)	✓
Secure Boot (Bootloader and BIOS validates OS kernel are expected supported from UEFI Secure Boot)	✓
Bootloader/BIOS Password (default value is product serial number)	✓
OS Mandatory password change upon first login	✓
Encrypted Filesystem	✓
Syslog support and log rotation rule	✓
Secure Installation (Image & Bootloader/BIOS)	✓
Ince Secure Installation (SecureAPT)	✓
Utility	
Moxa Computer Interface Manager (MCIM)	✓
Moxa Connection Manager (MCM)	✓
System Failback	✓
System Backup & Restore (snapshot & full backup)	✓
Remote Firmware Installation via SD/USB	✓
Moxa Secure Image Restore Tool	✓

Eligible Computing Platforms

This user manual is applicable to Moxa's V3000 Series computers listed below and covers the complete set of instructions applicable to all the supported models.

Series	Preinstalled OS	How to Get MIL3 Secure
V3200 Series	MIL3 Standard (Debian 11, kernel 5.10)	Order MIL3 Secure version using model name V3210 (CTO) via the CCS* program
V3400 Series	MIL3 Standard (Debian 11, kernel 5.10)	Order MIL3 Secure version using model name V3400 (CTO) via the CCS* program

*Computer Configuration System

2. Getting Started

Connecting to the V Series Computer

You will need another computer to connect to the V Series computer and log in to the command line interface. There are two ways to connect to the computer:

- Locally through serial console or ethernet cable
- Remotely via Secure Shell (SSH)

Refer to the Hardware Manual to see how to set up the physical connections.

For the default username and password, see [Default Credentials and Password Strength](#). The username and password are the same for serial console and SSH remote log in actions. The root account login is disabled until you manually create a password for the account. The user **moxa** is in the **sudo** group so you can operate system level commands with this user using the **sudo** command. For additional details, see [Sudo Mechanism](#).



ATTENTION

For security reasons, we highly recommend that you disable the default user account after the first login and create your own user accounts.

Connecting via the SSH

The V Series computer supports SSH connections remotely or over an Ethernet network. If you are connecting the computer using an Ethernet cable, refer to the following IP addresses information:

Ethernet Port	Configuration	IP Address
LAN 1*	DHCP (DHCP client)	Assigned by DHCP server. Link-local IP addresses will be assigned when DHCP server is not available
LAN 2	Static IP	192.168.4.127

*LAN 1 is by default for DHCP/link-local IP configuration and is managed by [Moxa Connection Manger \(MCM\)](#).



NOTE

Be sure to configure the IP address of your notebook/PC's Ethernet interface on the same subnet as the LAN port of V Series computer you plan to connect to. For example, 192.168.4.**126** for LAN2.

Linux Users



NOTE

These steps apply to the Linux PC you are using to connect to the V Series computer. Do NOT apply these steps to the V Series computer itself.

Use the **ssh** command from a Linux computer to access the computer's LAN2 port.

```
user@PC1:~ ssh moxa@192.168.4.127
```

Type **yes** to complete the connection.

```
The authenticity of host '192.168.4.127' can't be established.  
RSA key fingerprint is 8b:ee:ff:84:41:25:fc:cd:2a:f2:92:8f:cb:1f:6b:2f.  
Are you sure you want to continue connection (yes/no)? yes_
```

To connect using LAN1, you need to use the IP offered by DHCP server from LAN1.



ATTENTION

Regenerate SSH key regularly

In order to secure your system, we suggest doing a regular SSH-rekey, as shown in the following steps:

```
moxa@moxa-tbzk1090923:~$ cd /etc/ssh  
moxa@moxa-tbzk1090923:~$ sudo rm /etc/ssh/ssh_host_*  
moxa@moxa-tbzk1090923:~$ sudo dpkg-reconfigure openssh-server  
moxa@moxa-tbzk1090923:~$ sudo systemctl restart ssh
```

Select **"keep the local version currently installed"** following is prompt during rekey process

```
-----| Configuring openssh-server |-----  
sshd_config.moxa: A new version (/tmp/fileuorm95) of configuration file  
/etc/ssh/sshd_config.moxa is available, but the version installed  
currently has been locally modified.  
  
What do you want to do about modified configuration file  
sshd_config.moxa?  
  
install the package maintainer's version  
keep the local version currently installed  
show the differences between the versions  
show a side-by-side difference between the versions  
start a new shell to examine the situation  
  
<Ok>
```

For more information about SSH, refer to the following link.

<https://wiki.debian.org/SSH>

Windows Users

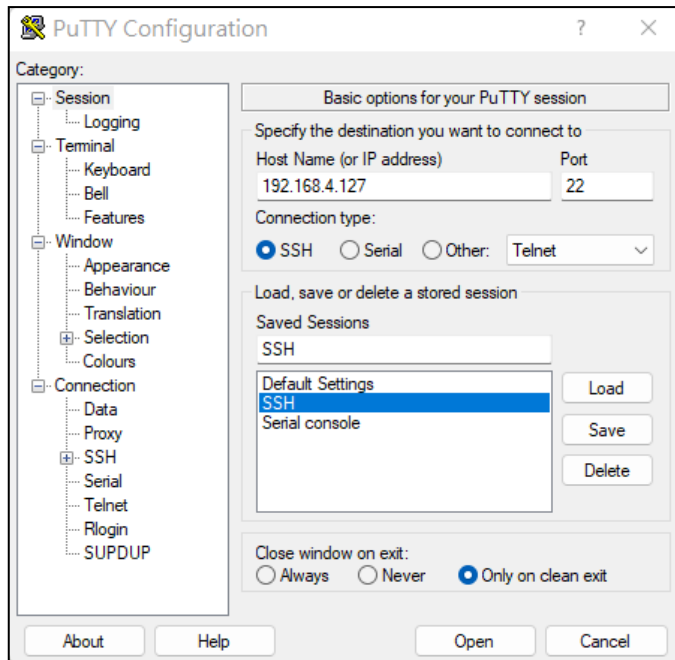


NOTE

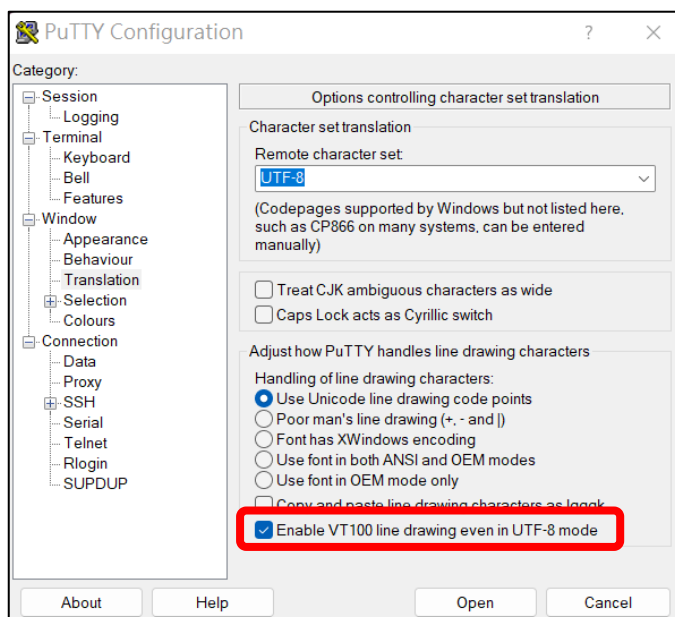
These steps apply to the Windows PC you are using to connect to the V Series computer. Do NOT apply these steps to the V Series computer itself.

Take the following steps from your Windows PC.

Click on the link <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> to download PuTTY (free software) to set up an SSH console for the V Series computer in a Windows environment. The following figure shows a simple example of the configuration that is required.



Enable **VT100 line drawing** option for the [MCM GUI configurator](#) to show correctly



Managing User Accounts

Default User Account and Password Policy

The default login username and password of Moxa Industrial Linux are both **moxa** for the first-time login. You will be prompted to set a new password before you can continue to login.

- Default Username: **moxa**
- Default Password: **moxa**

Password Strength Requirements:

- At least 8 characters in length
- Dictionary checking is enabled to prevent the use of common passwords

To modify the password strength policy, edit the `/etc/security/pwquality.conf.d/00-moxa-standard-pwquality.conf` file to configure the policy.



NOTE

For more information on the password strength configuration, see

<https://manpages.debian.org/bullseye/libpwquality-common/pwquality.conf.5.en.html>

For bootloader administrator password configuration, refer to the [bootloader configuration](#) section.

Creating and Deleting User Accounts



ATTENTION

DO NOT disable the default account before creating an alternative user account.

You can use the **useradd** and **userdel** commands to create and delete user accounts. Be sure to reference the main page of these commands to set relevant access privileges for the account. Following example shows how to create a **test1** user in the **sudo** group whose default login shell is **bash** and has home directory at **/home/test1**:

```
moxa@ moxa-tbzk1090923:~# sudo useradd -m -G sudo -s /bin/bash test1
```

To change the password for **test1**, use the **passwd** option along with the new password. Retype the password to confirm the change.

```
moxa@moxa-tbzk1090923:~# sudo passwd test1
New password:
Retype new password:
passwd: password updated successfully
```

To delete the user **test1**, use the **userdel** command.

```
moxa@ moxa-tbzk1090923:~# sudo userdel test1
```

Modifying User Accounts

You can use the **usermod** commands to create and modify the user account settings. Some examples of commonly used settings are listed here, including adding a user to a group, locking an account, activating an account and setting the password expiration date for the account.

1. Adding user test1 to the user group Moxa

```
moxa@ moxa-tbzkb1090923:# sudo usermod -a -G Moxa test1
```

2. Disabling or locking the user account test1

```
moxa@ moxa-tbzkb1090923:# sudo usermod -L test1
```

3. Activating the user account test1

```
moxa@ moxa-tbzkb1090923:# sudo usermod -U test1
```

4. Set a password expiration date of 2023-11-01 for the user account test1.

```
moxa@ moxa-tbzkb1090923:# sudo usermod -e 2023-11-01 test1
```



NOTE

Refers to below link for complete usage of **usermod**

<https://linux.die.net/man/8/usermod>

Changing the Password

You can use the **passwd** commands to change the password of a user account. Changing the password will not have any impact on other functionalities.

An example of changing the password for user account **test1**.

```
moxa@ moxa-tbzkb1090923:# sudo passwd test1
New password:
Retype new password:
passwd: password updated successfully
```

Querying the System Image Version

Use the **mx-ver** command to check the system **image version** on your V Series computer.

```
moxa@moxa-tbzkb1090923:# mx-ver
UC-8220-T-LX-US-S MIL3 version 1.0 Build 22052300
```

```
moxa@moxa-tbzkb1090923:# mx-ver -h

Usage: mx-ver [OPTION]
-a: show product information inline
-b: show the build time
-m: show the model name
-v: show the image version
-A: show all information
-M: show the MIL version
-o: show the image option code
-h: show the help menu
```

Querying Device Information

Use the # **mx-interface-mgmt deviceinfo** command to retrieve general information for your V3000 Series Computer

Command and Usage	Description
deviceinfo	Shows the following device information: <ul style="list-style-type: none">Serial number (S/N)Model nameSECUREBOOT (Enabled/Disabled)

```
moxa@moxa-tbbbb1182827:~$ mx-interface-mgmt deviceinfo
SERIALNUMBER=TBBBB1182827
MODELNAME=UC-8220-T-LX-US-S
SECUREBOOT=Enabled
```

Determining Available Drive Space

To determine the amount of available drive space, use the **df** command with the **-h** option. The system will return the amount of drive space broken down by file system. Here is an example:

```
moxa@moxa-tbzkb1090923:~$ sudo df -h

Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        485M   0    485M   0% /dev
tmpfs           497M   7.1M  490M   2% /run
/dev/mmcblk0p2  984M  150M   780M  17% /boot_device/p2
/dev/mmcblk0p3  5.9G   39M   5.5G   1% /boot_device/p3
/dev/mmcblk0p4  240M   2.8M  221M   2% /var/log
/dev/loop0      147M  147M     0 100% /boot_device/p2/lower
overlay         5.9G   39M   5.5G   1% /
/dev/mmcblk0p1   54M   15M   36M  30% /boot_device/p1
tmpfs           497M   0    497M   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           497M   0    497M   0% /sys/fs/cgroup
tmpfs           100M   0    100M   0% /run/user/1000
```

Shutting Down the Device

RTC battery powers the Real-Time Clock chip on a motherboard and retains customers' BIOS configurations. When RTC battery voltage goes low, BIOS setting will revert to Moxa default setting and miss the synchronization with the current time. Use the # **rtc-battery-level** command to check RTC battery voltage level. Here is an example:

```
moxa@moxa-tbzkb1090923:~$ rtc-battery-level
Normal voltage
```

If you want MIL to check the RTC battery level periodically, you can enable RTC battery detect daemon. Here is an example:

```
moxa@moxa-tbzkb1090923:~$ systemctl enable mx_rtc-battery_detect
Created symlink /etc/systemd/system/multi-user.target.wants/rtc-
battery_detect.service -> /etc/systemd/system/rtc-battery_detect.service
```

Shutting Down the Device

To shut down the computer, first disconnect the power source. When the computer is powered off, main components such as the CPU, RAM, and storage devices are powered off, although an internal clock may retain battery power.

You can use the Linux command **shutdown** to close all software running on the device and halt the system. However, main components such as the CPU, RAM, and storage devices will continue to be powered after you run this command.

```
moxa@moxa-tbzkbl090923: ~# sudo shutdown -h now
```

3. Device Configuration

In this chapter, we describe how to configure the basic settings on your V3000 Series computers, including using the BIOS menu, configuring the network connections and power-saving settings, and localizing the computer. The instructions in this chapter cover all functions supported on the V3000 Series computers. Before referring to the sections in this chapter, ensure that they are applicable to and are supported by the hardware specification of your V Series computer.

BIOS Setup

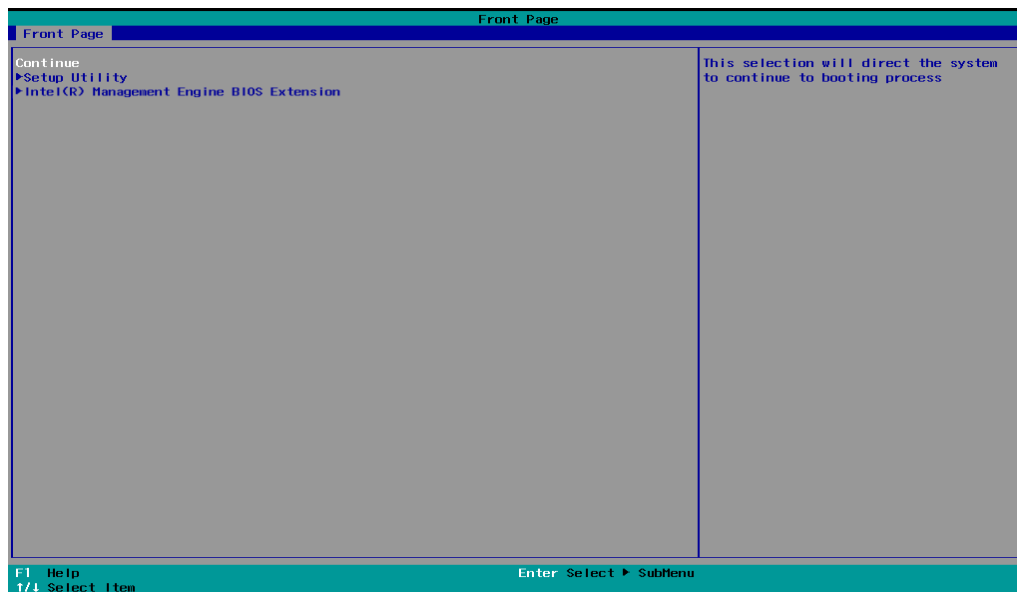
The MIL3 BIOS menus differ between the models with MIL# preinstalled and the ones that come without MIL3. On models without MIL3 preinstalled, users can install their own OS, such as Windows or Debian Linux. In such a case, the BIOS menu offers flexible options to support the different Oses. Additional details are available in the Hardware User Manual for the series. For models with MIL3 preinstalled, installation will be done before they are shipped. Preinstalled MIL3 OS allows us to enhance BIOS protection against cyberattacks as detailed in the following sections.

Entering the BIOS Setup

To enter the BIOS setup utility, press the F2 key while the system is booting up. The main BIOS Setup screen will appear. You can configure the following settings on this screen.

- Continue: Continue to boot up
- Setup Utility: Enter the BIOS configuration menu
- Intel® Management Engine BIOS Extension: Enter the AMT configuration menu

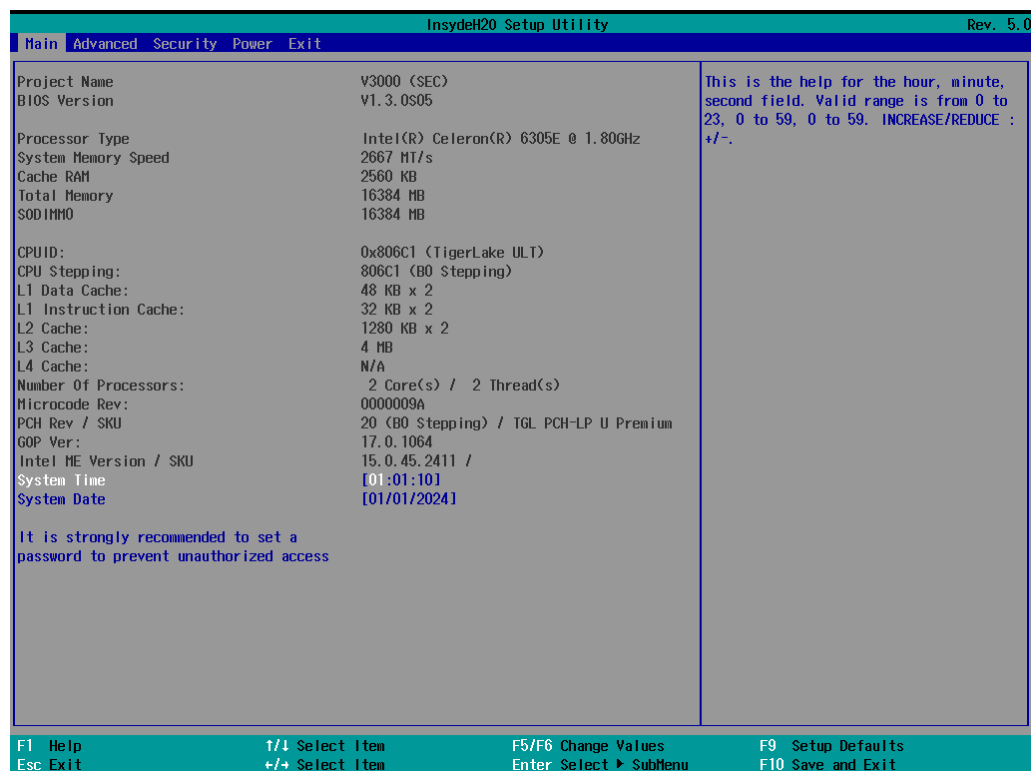
Select F2 to enter the BIOS configuration.



When you enter the Setup Utility, a basic description of each function key is listed at the bottom of the screen. Refer to these descriptions to learn how to use them.

F1	General Help	↑ ↓ .	Select Item
F5/F6	Change Values	← →	Select Menu
F9	Setup Defaults	ESC	Exit
F10	Save and Exit	ENTER	Select or go to Submenu.

The BIOS configuration screen is shown when you enter the Setup Utility option.



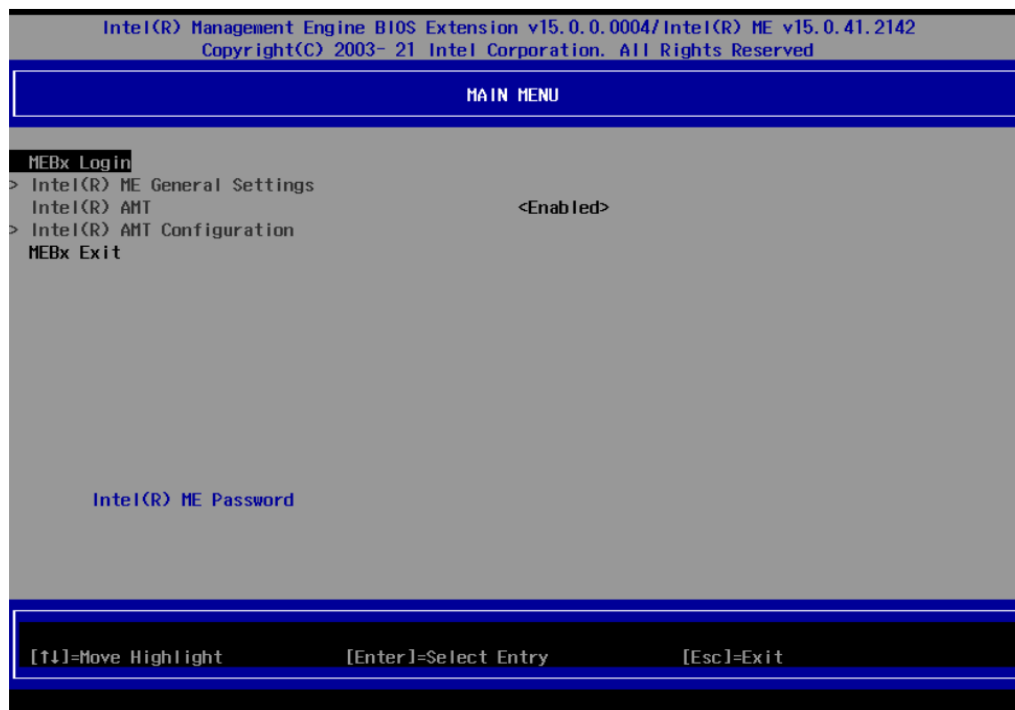
NOTE

The Processor Type information may vary depending on the model that you have purchased.

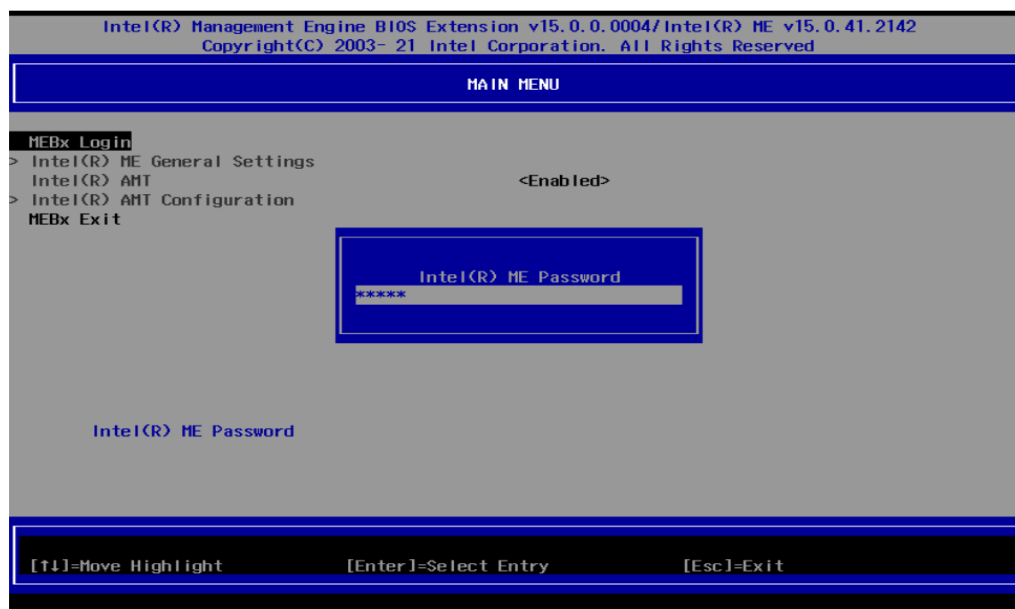
How to Enable and Use AMT

Enabling AMT

1. From the front page, select **Intel® Management Engine BIOS Extension** to enter the AMT configuration menu.
2. Press to start the login procedure.



3. Type the default password: admin.



4. Type the new password. It must include both upper-case and lower-case characters, numbers, and special symbols. E.g., Admin'12.
5. Select Intel® AMT Configuration to enable remote access without a local user present for consent, select User Consent, and then select User Opt-in and change the value to None.

- Set static IP or DHCP by request.

Intel(R) Management Engine BIOS Extension v15.0.0.0004/Intel(R) ME v15.0.41.2142
Copyright(C) 2003- 21 Intel Corporation. All Rights Reserved

WIRED LAN IPV4 CONFIGURATION

DHCP Mode	<Disabled>
IPv4 Address	192.168.1.10
Subnet Mask Address	255.255.255.0
Default Gateway Address	0.0.0.0
Preferred DNS Address	0.0.0.0
Alternate DNS Address	0.0.0.0

Enable/Disable IPV4 DHCP Mode

[↑↓]=Move Highlight [Enter]=Select Entry [Esc]=Exit

- Set Activate Network Access to enable remote access capability.

Intel(R) Management Engine BIOS Extension v15.0.0.0004/Intel(R) ME v15.0.41.2142
Copyright(C) 2003- 21 Intel Corporation. All Rights Reserved

INTEL(R) AMT CONFIGURATION

Manageability Feature Selection	<Enabled>
> SOL/Storage Redirection/KVM	
> User Consent	
Password Policy	<Anytime>
> Network Setup	
Activate Network Access	
Unconfigure Network Access	<Full Unprovision>
> Remote Setup And Configuration	
> Power Control	

[↑↓]=Move Highlight [Enter]=Select Entry [Esc]=Exit

Using AMT

You can use any AMT tool available to run the remote management function using a web browser.

- Type the IP address of your computer as configured in the AMT configuration settings with port 16992 in the browser. The AMT logon screen will appear.
- Click Log On and type the username (admin) and password.

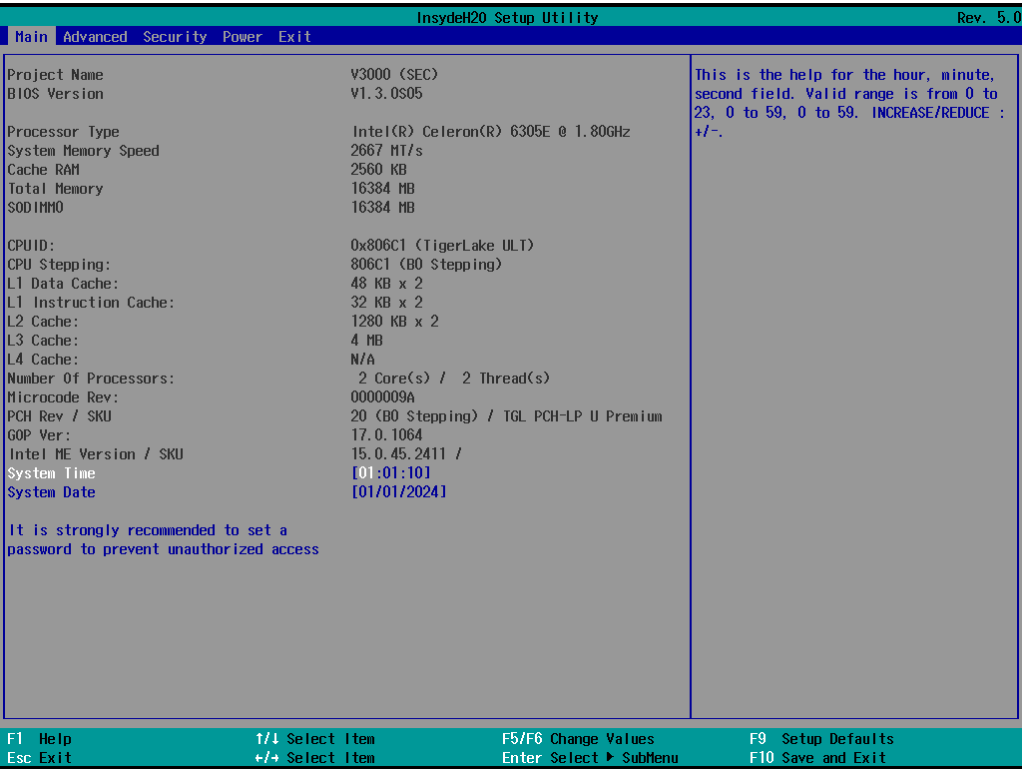


NOTE

- The AMT port is LAN1.
- For additional details, refer to the Intel® AMT Implementation and Reference Guide at:
https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm?t_url=WordDocuments%2Faccessingintelamtviathewebuiinterface.htm

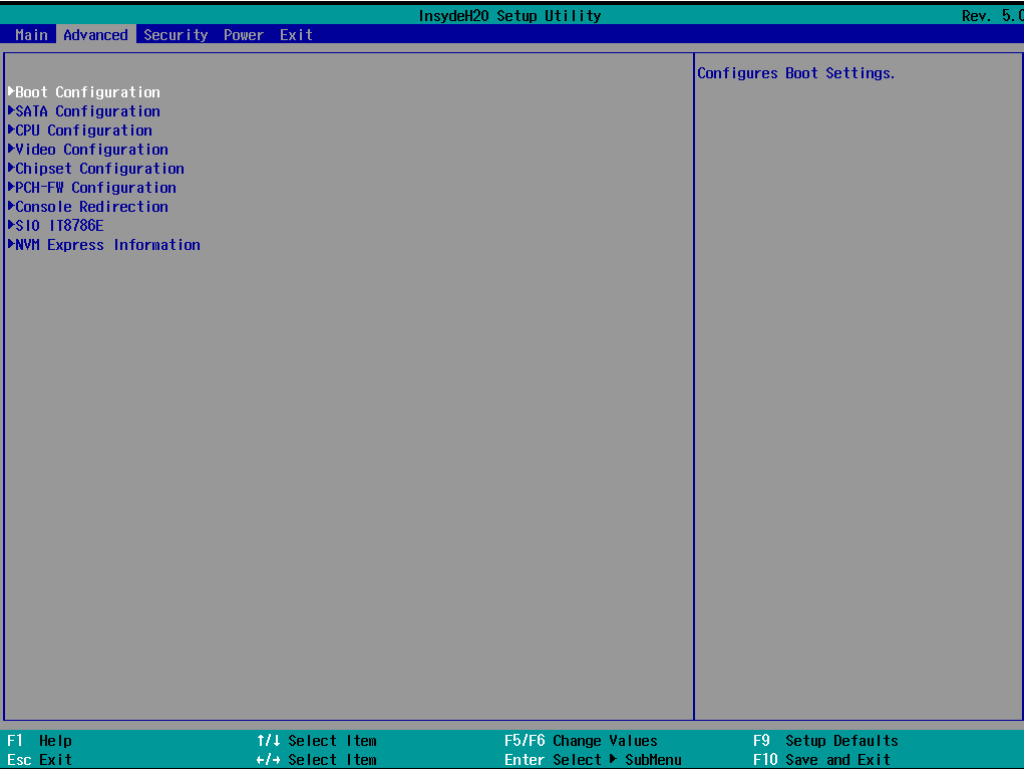
Main Page

The Main page displays basic hardware information, such as model name, BIOS version, and CPU type.



Advanced Settings

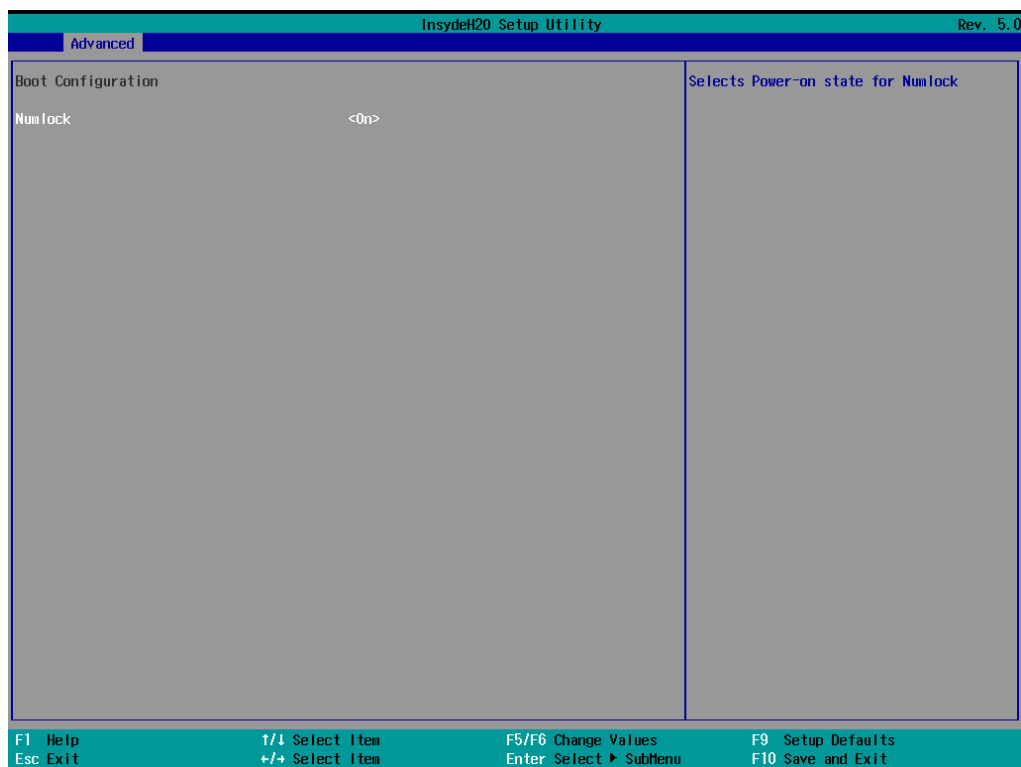
Select the Advanced tab in the main menu to open the advanced features screen



Boot Configuration

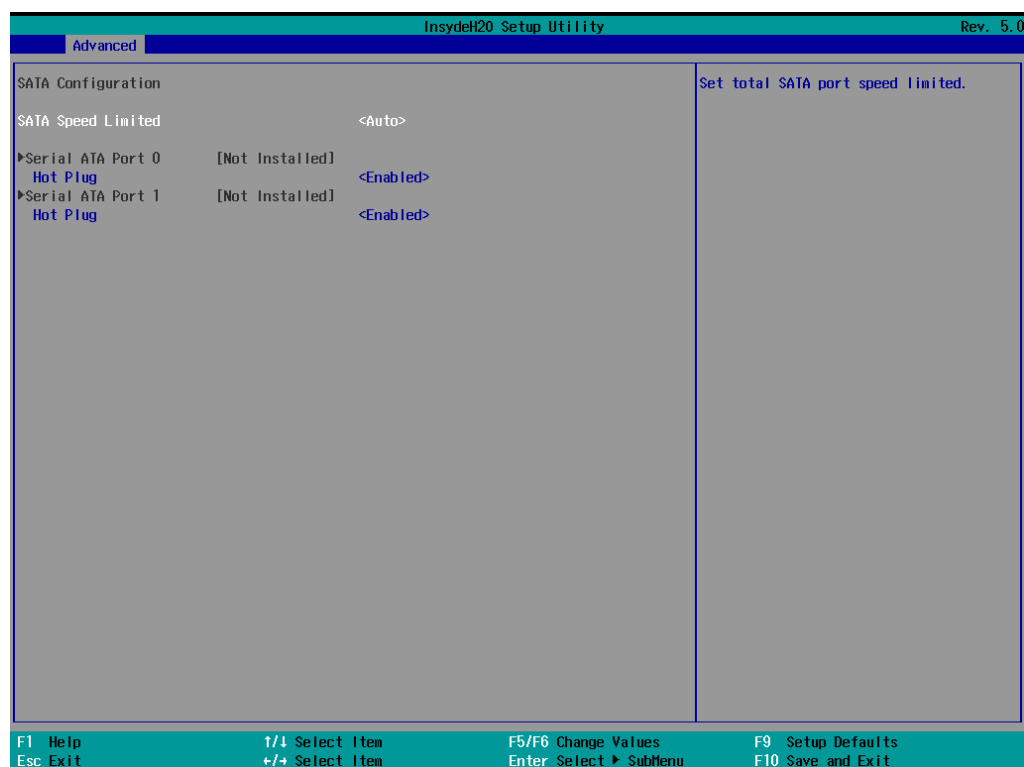
The Numlock option allows configuration of the Numlock value.

Options: On (default), Off.



SATA Configuration

These items allow you to select the SATA speed limit and enable or disable the RAID mode.



SATA Speed Limited

Options: Auto (default), Gen 1, Gen 2, Gen 3

Serial ATA Port

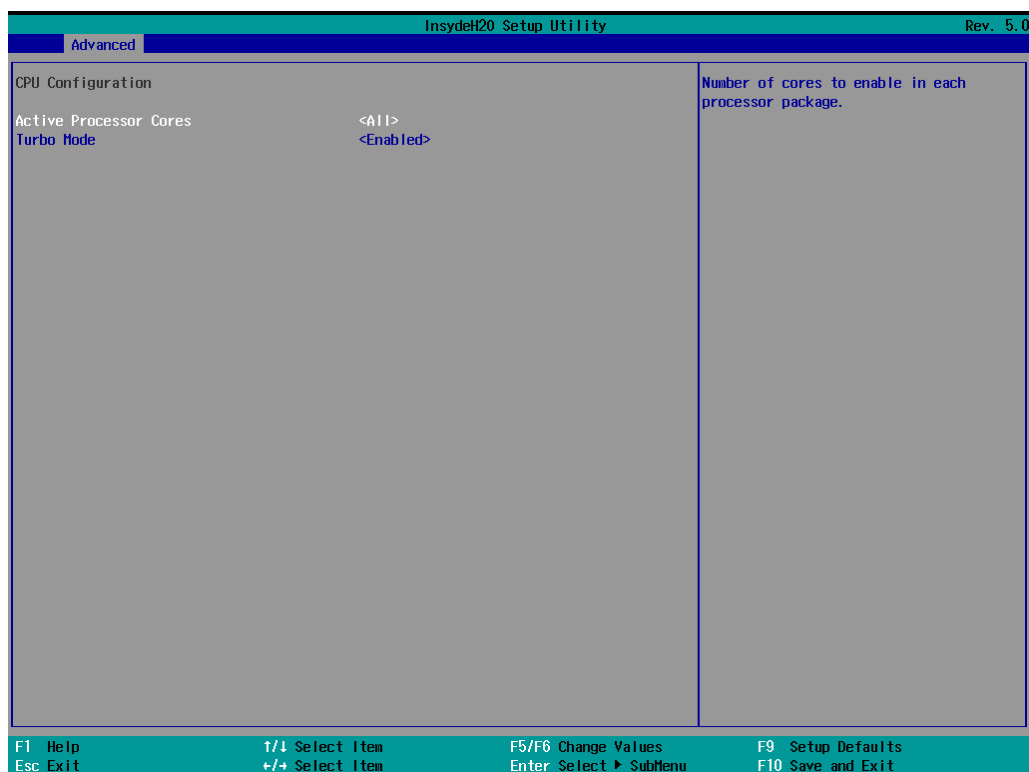
This setting displays information on the installed drives.

ATA Port Hot Plug

This setting allows you to enable/disable hot-plugging capabilities (the ability to remove the drive while the computer is running) that are configured by software for installed storage drives.

Options: Disabled (default), Enabled

CPU Configuration



Active Processor Cores

This item indicates the number of cores to enable in each processor package.

Options: All (default), 1, 2, 3

Turbo Mode

This feature allows you to enable the CPU to overclock or underclock based on system load automatically to save energy or speed up processing.

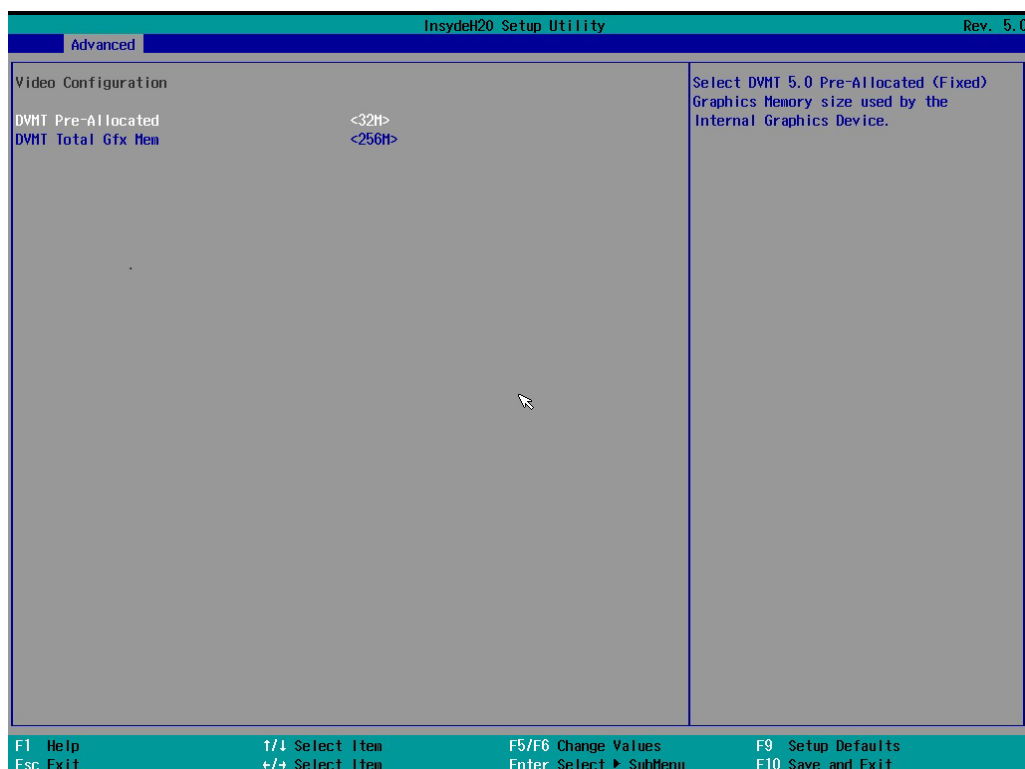
Options: Disabled, Enabled (default)



NOTE

V3210-TL1-4L-T and V3210-TL1-8L-CT-T do not support the **Turbo Mode** function because Intel® Celeron® 6305E processor does not support it.

Video Configuration



DVMT Pre-Allocated

This item allows you to configure pre-allocated memory capacity for the IGD. Pre-allocated graphics memory is invisible to the operating system.

Options: 32M (default), 64M, 96M, 128M, 160M

DVMT: The amount of video memory your computer has is dependent on the amount of pre-allocated memory set for your system plus the Dynamic Video Memory Technology (DVMT). DVMT dynamically allocates system memory for use as video memory creating the most efficient use of available resources for maximum 2D/3D graphics performance.

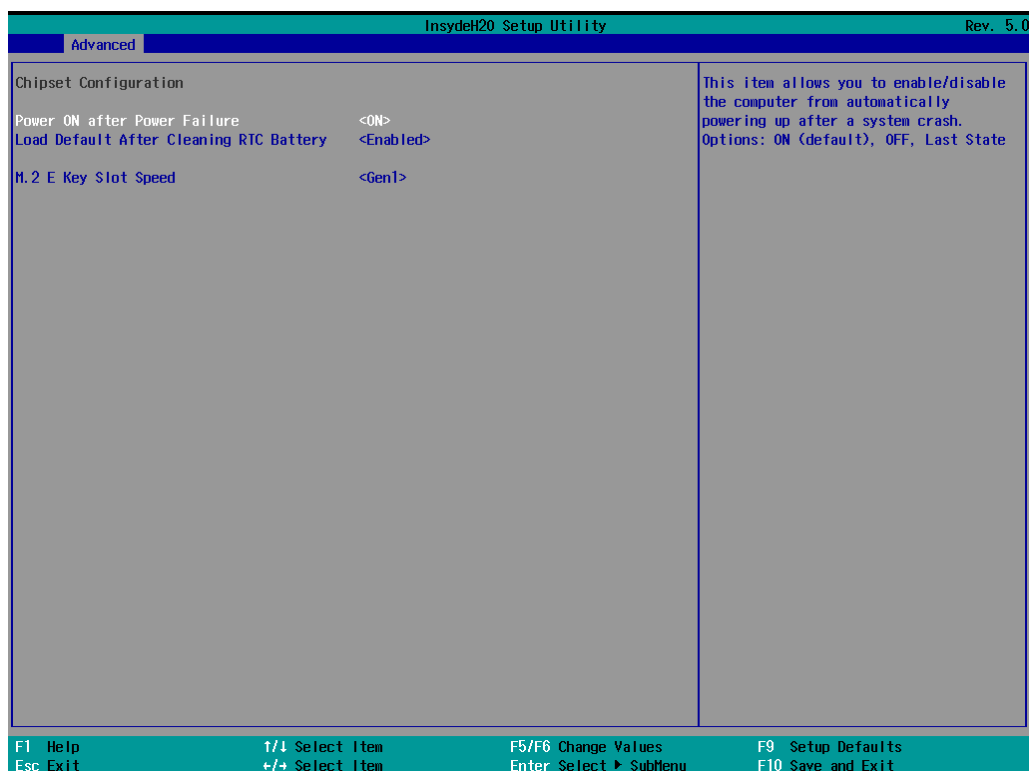
DVMT Total Gfx Mem

This item allows you to configure the maximum amount of memory DVMT will use when allocating additional memory for the internal graphics device.

Options: 256 MB (default), 128 MB, Max.

Chipset Configuration

This item allows you to configure the chipset settings.



Power ON after Power Failure

This item allows you to enable/disable the computer from automatically powering up after system power is re-enabled.

Options: ON (default), OFF, Last State

Load Default After Cleaning RTC Battery

This item allows you to enable the system to load the default setting when RTC battery loss is detected.

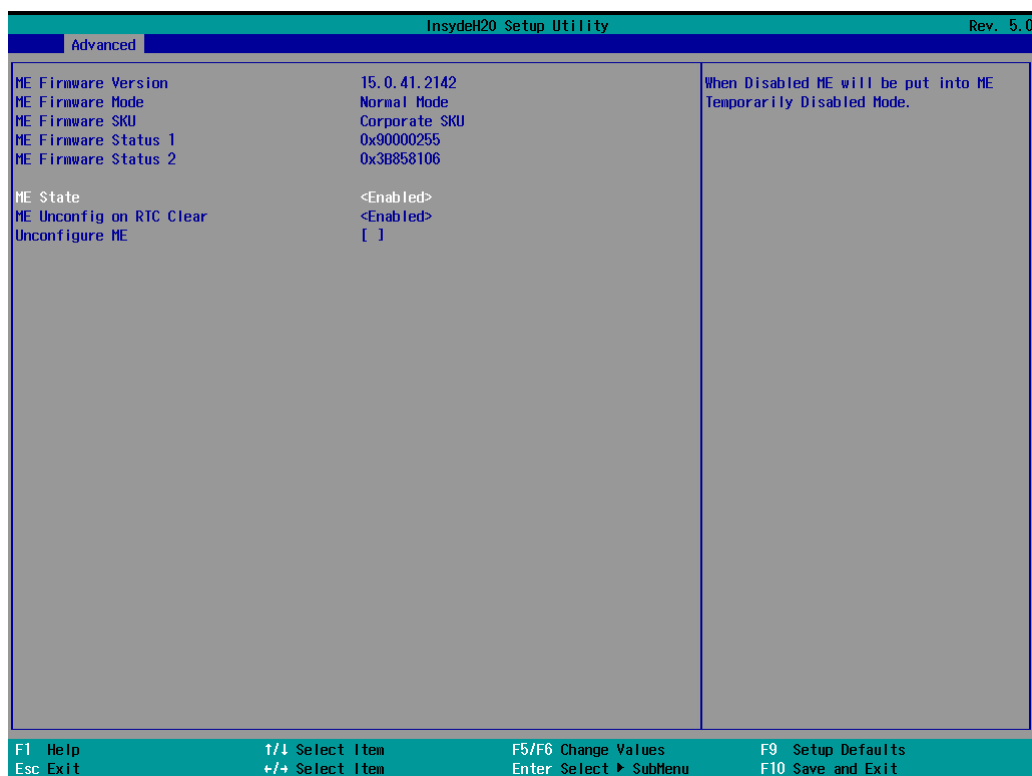
Options: Disabled, Enabled (default)

M.2 E Key Slot Speed

Options: Gen 1 (default), Gen 2, Gen 3, Auto

PCH-FW Configuration

This item allows you to configure the PCH-FW settings.



ME State

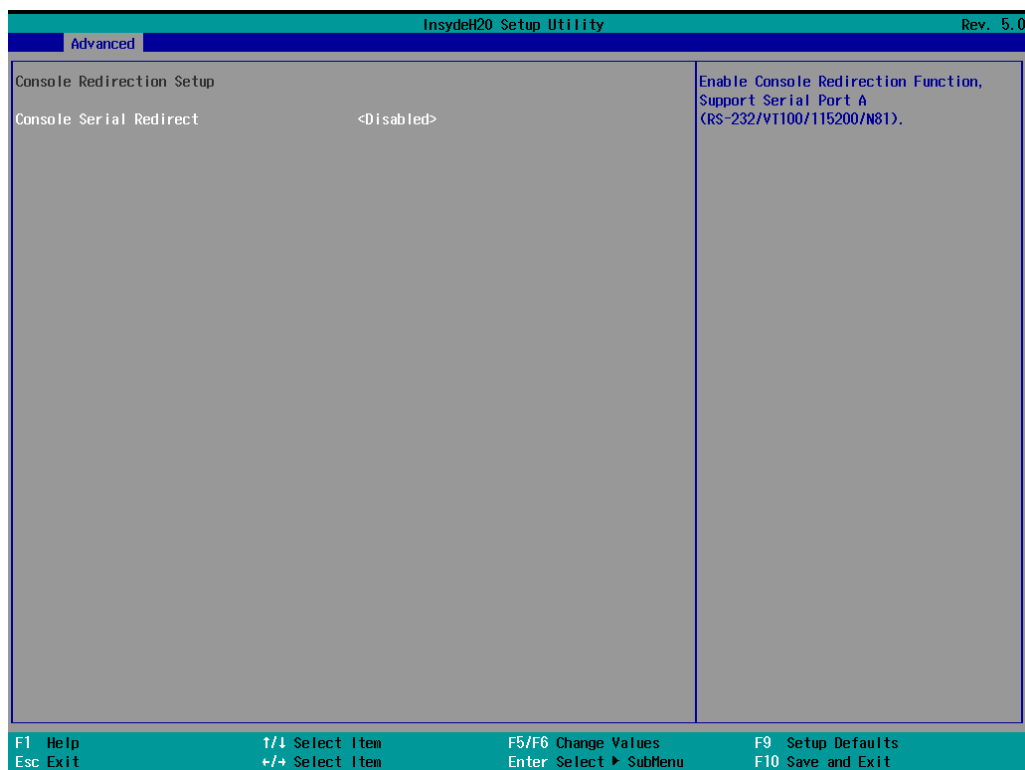
Options: Enabled (default), Disabled

ME Unconfig on RTC Clear

Options: Enabled (default), Disabled

Console Redirection

When the Console Redirection Function is enabled, the console information will be sent to both the display monitor and through the serial port.

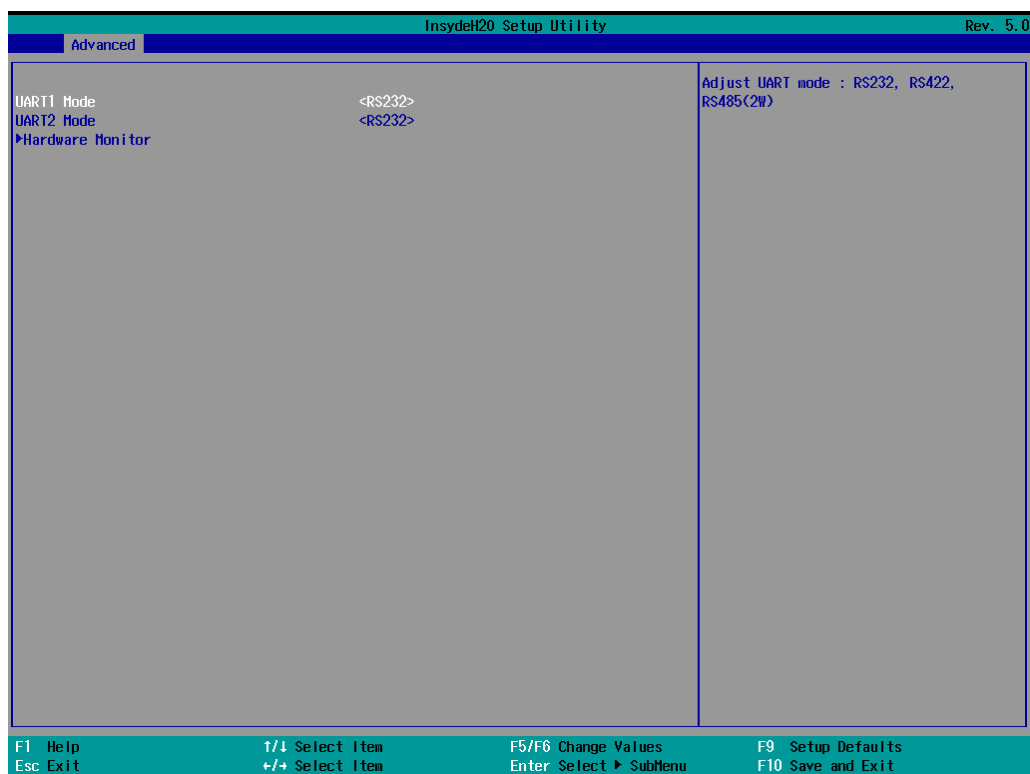


Console Serial Redirect

Options: Disabled (default), Enabled

SIO ITE8786E

This section allows users to configure SIO settings.



UART1 Mode

This function allows users to configure the UART1 mode.

Option: RS232 (default), RS422, RS485

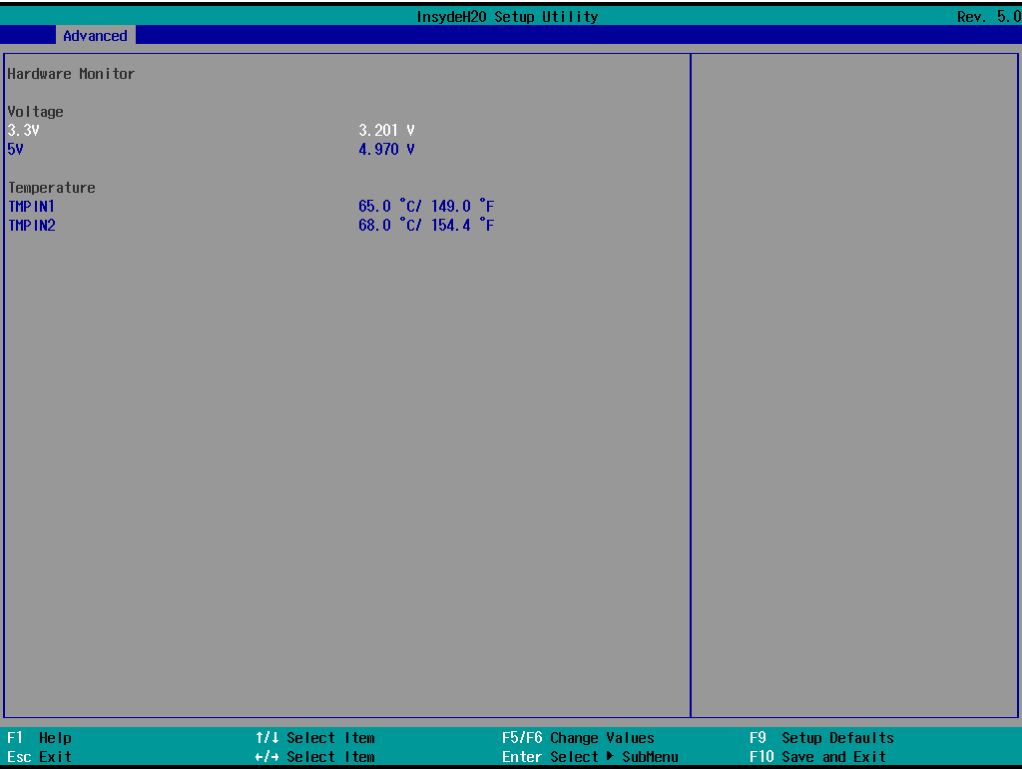
UART2 Mode

This function allows users to configure the UART2 mode.

Option: RS232 (default), RS422, RS485

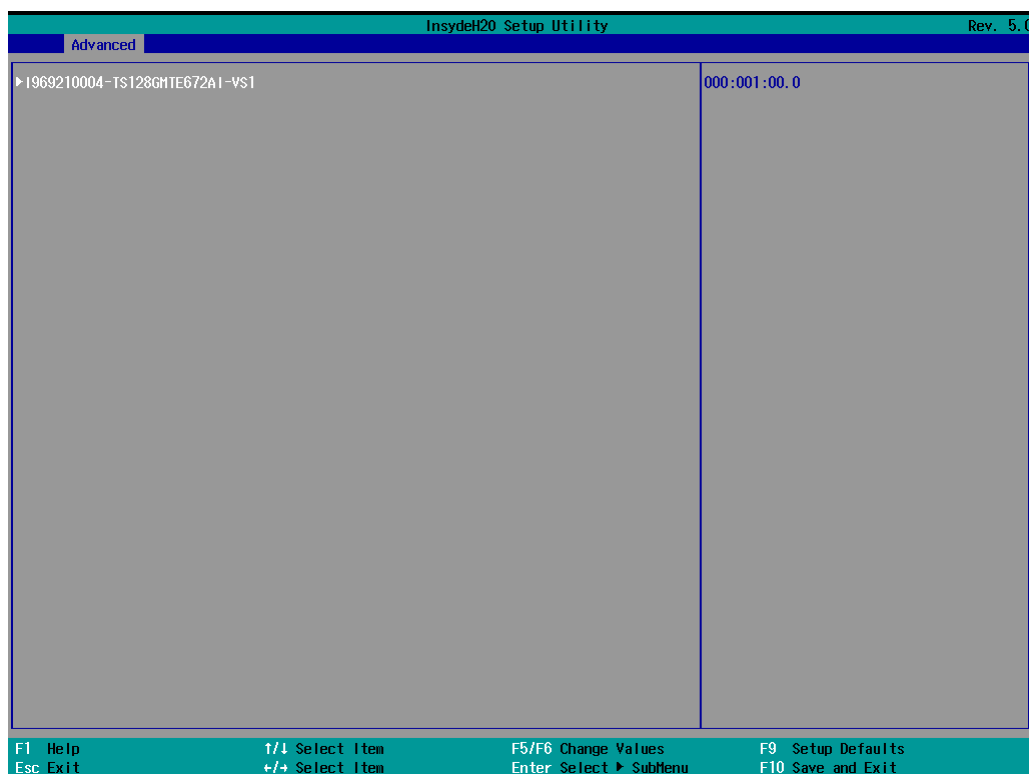
Hardware Monitor

This item allows you to view stats such as CPU and system temperature, voltage levels, and other chipset information.

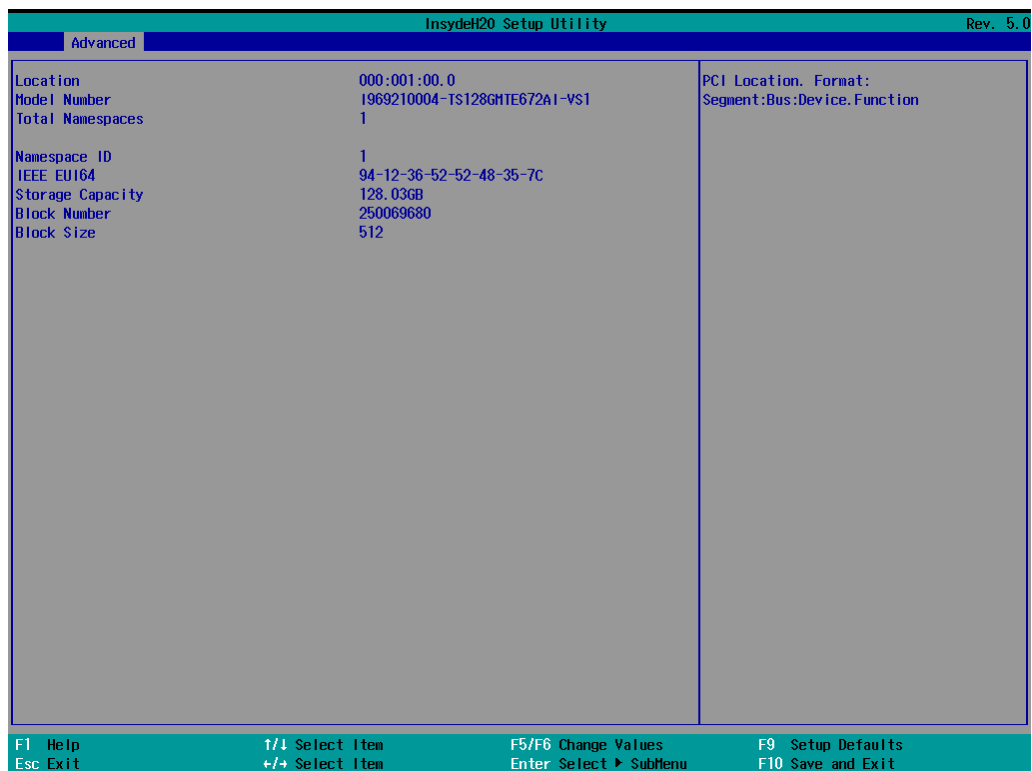


NVM Express Information

NVM Express (NVMe) is a high-performance, scalable, and non-volatile memory interface specification designed for modern SSDs. It stands for Non-Volatile Memory Express, and it's used to access storage devices over a PCI Express (PCIe) bus instead of older, slower interfaces like SATA. This section guide you how to fetch NVM express information.

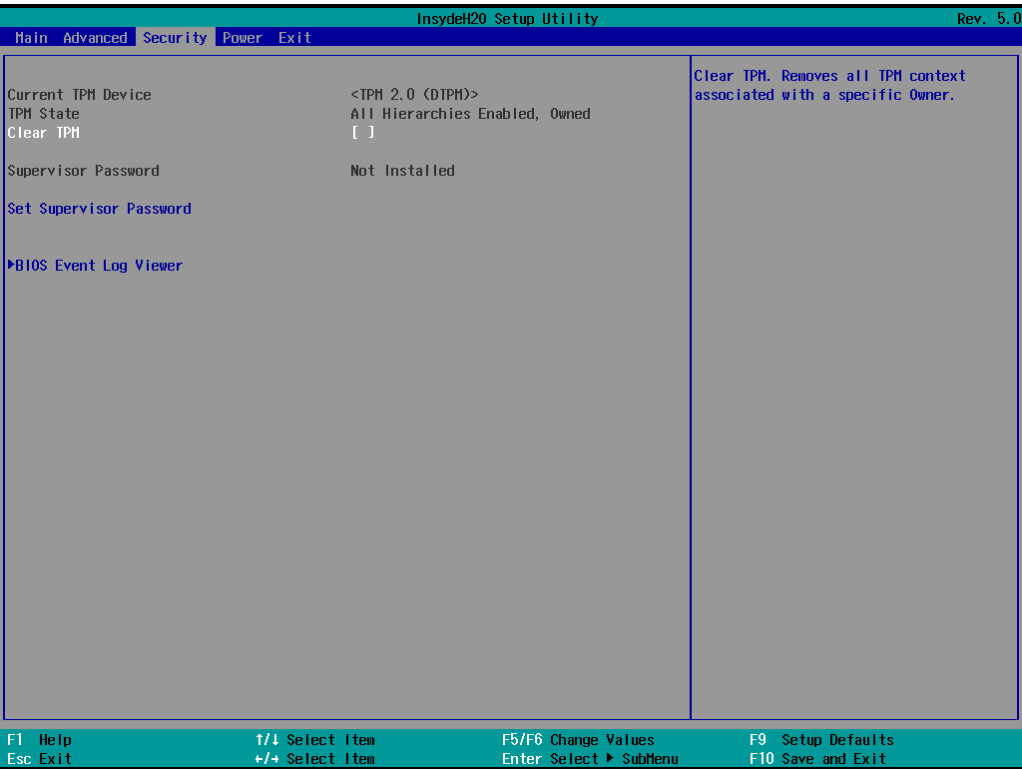


Select the NVMe SSD that you want to check, and more information will be shown for you.



Security Settings

This section allows users to configure security-related settings with a supervisor password and user password.



Current TPM Device

This item shows if the system has TPM device and its type.

TPM State


This item allows you view the status of current TPM settings.

Clear TPM

This item allows users to remove all TPM context associated with a specific owner. Select the option and press enter once to display an ✕, which indicates that the Clear TPM option is enabled. The TPM context is clear each time the system boots up.

Set Supervisor Password

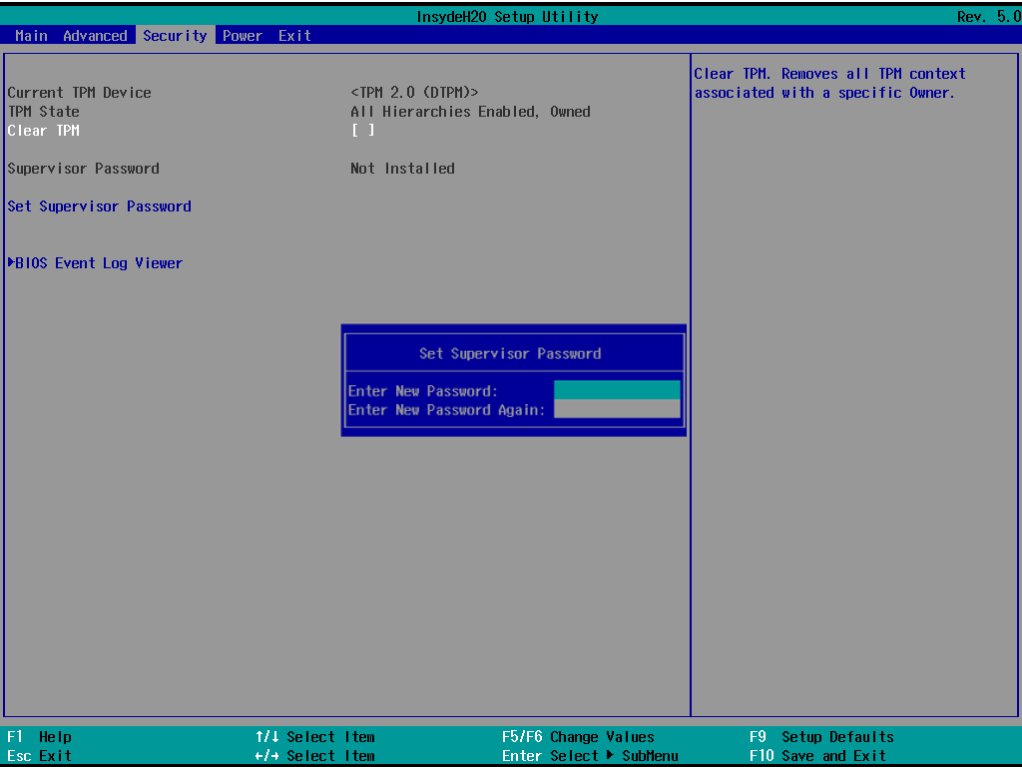
This item allows you to set the supervisor password. Select the Set Supervisor Password option and enter the password and confirm the password again.



NOTE

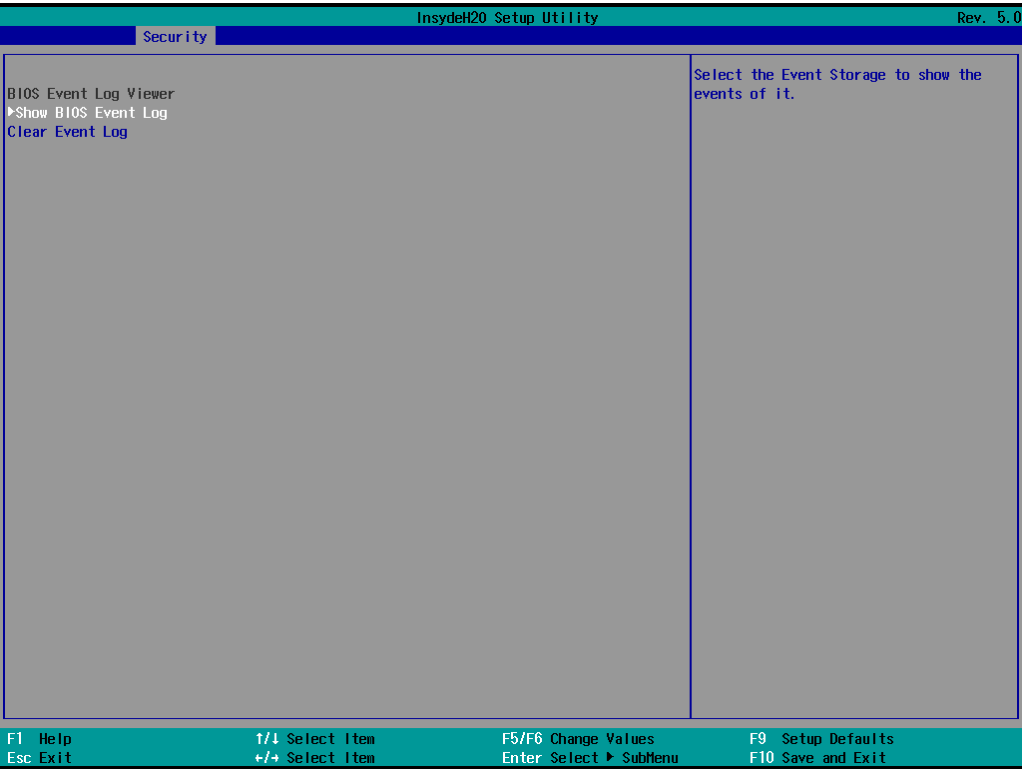
The password must be at least 8 characters.

To delete the password, select the Set Supervisor Password option and enter the old password; leave the new password fields blank, and then press enter.



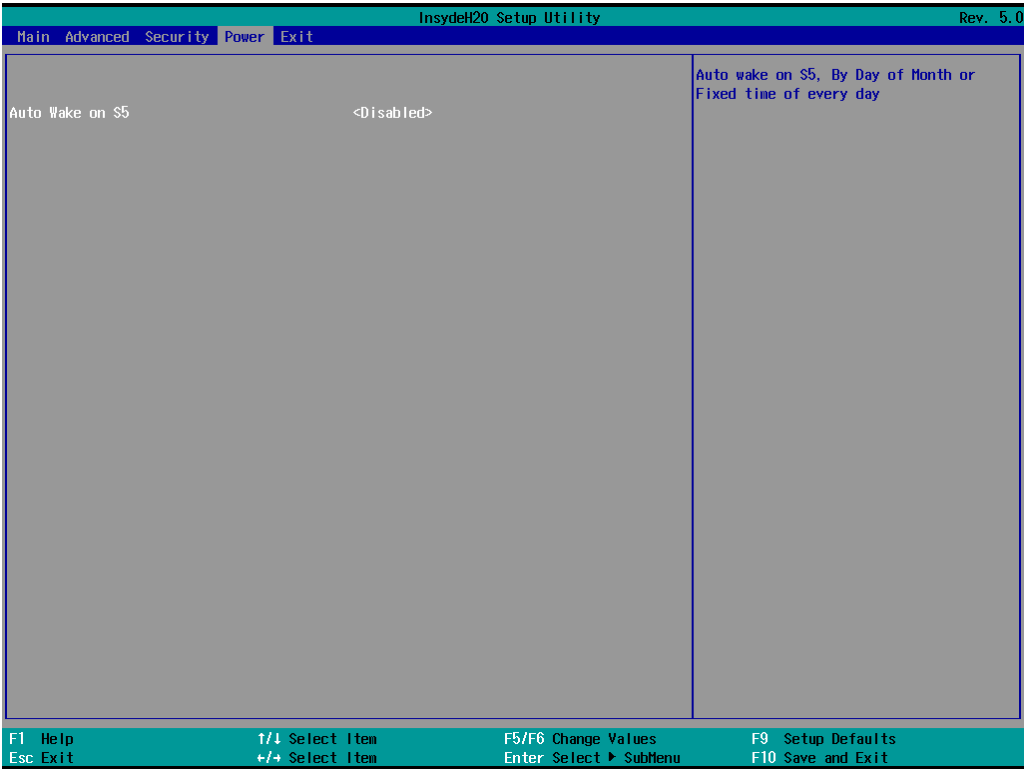
BIOS Event Log Viewer

This item allows you check and clear BIOS event Logs.



Power Settings

The section allows users to configure power settings.



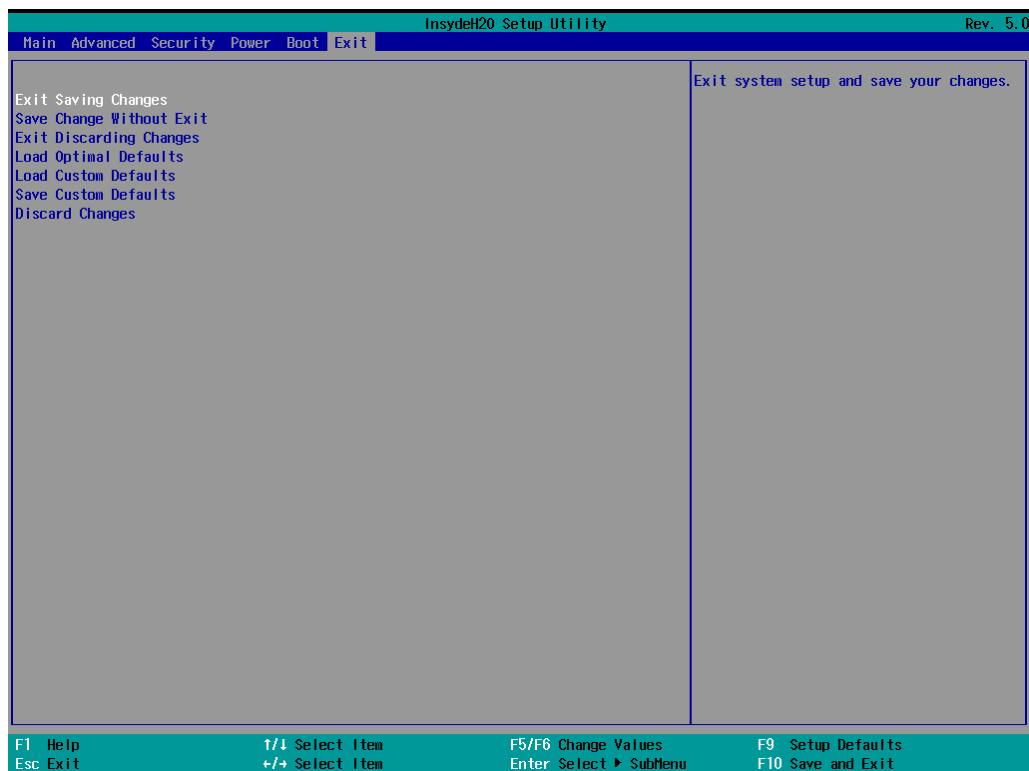
Auto Wake on S5

This item allows you to configure the computer to wake from S5 status. S5 stands for Soft Off, where the PSU remains engaged but power to all other parts of the system is cut. Auto-wake on S5 schedules a soft-reboot at certain periodic times that may be specified in the BIOS.

Options: Disabled (default); By Every Day (user specifies a regular daily time when the computer will power up); By Day of Month (user specifies a regular day each month when the computer will power up)

Exit Settings

The section allows users to exit the BIOS environment.



Exit Saving Changes

This item allows you to exit the BIOS environment and save the values you have just configured.

Options: Yes (default), No

Save Change Without Exit

This item allows you to save changes without exiting the BIOS environment.

Options: Yes (default), No

Exit Discarding Changes

This item allows you to exit without saving any changes made to the BIOS.

Options: Yes (default), No

Load Optimal Defaults

This item allows you to revert to the factory default BIOS values.

Options: Yes (default), No

Load Custom Defaults

This item allows you to load custom default values for the BIOS settings.

Options: Yes (default), No

Save Custom Defaults

This item allows you to save the current BIOS values as a “custom default” that may be reverted to at any time by the load custom defaults selection.

Options: Yes (default), No

Discard Changes

This item allows you to discard all settings you have just configured.

Options: Yes (default), No

Changing the Default Hostname

The default hostname of UC computer with Moxa Industrial Linux 3 is unique for each computer. The hostname is in a format of moxa-[serial number].

If you would like to change the default hostname, follow the below procedure:

1. Modify the hostname by editing /etc/hostname
2. Disable the moxa-hostname service with '**systemctl disable moxa-hostname**' command. moxa-hostname is a service designed to execute automatically during system startup, setting the hostname to a default unique value.
3. Reboot the computer.

Localizing Your V Series Computer

Adjusting the Time

The V Series computer has two time settings. One is the system time, and the other is the RTC (Real Time Clock) time kept by the V Series computer's hardware. Use the **date** command to query the current system time or set a new system time. Use the **hwclock** command to query the current RTC time or set a new RTC time.

Use the **date MMDDhhmmYYYY** command to set the system time:

MM = Month

DD = Date

hhmm = hour and minute

```
moxa@moxa-tbzk1090923:~# sudo date 102900282021
Fri 29 Oct 2021 12:28:00 AM GMT
```

Use the following command to set the RTC time to system time:

```
moxa@moxa-tbzk1090923:~# sudo hwclock -w
moxa@moxa-tbzk1090923:~# sudo hwclock
2021-10-28 16:25:04.077432+00:00
```



NOTE

Click the following links for more information on date and time:

<https://www.debian.org/doc/manuals/system-administrator/ch-sysadmin-time.html>

<https://wiki.debian.org/DateTime>

NTP Time Synchronization

The Moxa Industrial Linux (MIL) uses Network Time Security (NTS) to secure NTP, which provides a handshake (TLS) before using a NTP server and authentication of the NTP time synchronization packets using the results of the TLS handshake.

The default NTP client in MIL is **Chrony**. MIL disabled NTP server without NTS support by default and uses the following public NTP servers that support NTS.

- [Cloudflare](#)
- [Netnod](#)
- [System76](#)
- [PTB](#)

The default server list is configured in the `/etc/chrony/sources.d/moxa-nts.sources` file.

```
# prefer nts over ntp server
server time.cloudflare.com nts iburst prefer
server sth1.nts.netnod.se nts iburst prefer
server sth2.nts.netnod.se nts iburst prefer
server virginia.time.system76.com nts iburst prefer
server ohio.time.system76.com nts iburst prefer
server oregon.time.system76.com nts iburst prefer
server ptbtime1.ptb.de nts iburst prefer
server ptbtime2.ptb.de nts iburst prefer
server ptbtime3.ptb.de nts iburst prefer
```

The configuration file for Chrony is at `/etc/chrony/chrony.conf`.

The following example show some basic functions to monitor the current status of the Chrony's chronyc tool and make changes if necessary.

1. Check the time synchronization status between the local system and reference server using the command:

chronyc tracking

```
moxa@moxa-tbbbb1182827:~$ chronyc tracking
Reference ID    : A29FC801 (time.cloudflare.com)
Stratum        : 4
Ref time (UTC) : Sun Jul 31 18:27:42 2022
System time    : 0.000334575 seconds slow of NTP time
Last offset    : +0.000226902 seconds
RMS offset     : 0.005672113 seconds
Frequency      : 27.766 ppm fast
Residual freq  : -0.065 ppm
Skew           : 3.403 ppm
Root delay     : 0.203054637 seconds
Root dispersion: 0.006750254 seconds
Update interval: 517.4 seconds
Leap status    : Normal
```

2. Check the time source configured in the `/etc/chrony/chrony.conf` file using the `# chronyc sources` command.

```
moxa@moxa-tb11182827:~$ chronyc sources
```

MS Name/IP address	Stratum	Poll	Reach	LastRx	Last sample
=====					
^+ ohio.time.system76.com	2	9	377	147	+18ms[+18ms] +/- 141ms
^+ oregon.time.system76.com	2	9	377	203	+14ms[+14ms] +/- 137ms
^- ptbtime1.ptb.de	1	9	21	682	-2780us[-2417us] +/- 166ms
^- ptbtime2.ptb.de	1	9	21	674	-5243us[-4882us] +/- 169ms
^- ptbtime3.ptb.de	1	9	21	687	+17ms[+17ms] +/- 192ms
^+ sth1-ts.nts.netnod.se	1	9	377	220	-12ms[-12ms] +/- 162ms
^- sth2-ts.nts.netnod.se	1	8	377	91	-3843us[-3843us] +/- 171ms
^* time.cloudflare.com	3	9	377	230	+13ms[+13ms] +/- 129ms
^+ virginia.time.system76.c>	2	9	377	226	-8753us[-8753us] +/- 116ms

3. Manually synchronize the time using the `# chronyc makestep` command.



NOTE

For additional details on Chrony, check the following links:

<https://linux.die.net/man/8/chronyd>

<https://linux.die.net/man/1/chronyc>

Setting the Time Zone

There are two ways to configure the time zone on the V3000 Series computer. One is using the **TZ** variable. The other is using the `/etc/localtime` file.

Using the TZ Variable

The format of the TZ environment variable looks like this:

`TZ=<Value>HH[:MM[:SS]][daylight[HH[:MM[:SS]]][,start date[/starttime], enddate[/endtime]]]`

Here are some possible settings for the North American Eastern time zone:

1. **TZ=EST5EDT**
2. **TZ=EST0EDT**
3. **TZ=EST0**

In the first case, the reference time is GMT and the stored time values are correct worldwide. A simple change of the TZ variable can print the local time correctly in any time zone.

In the second case, the reference time is Eastern Standard Time and the only conversion performed is for Daylight Saving Time. Therefore, there is no need to adjust the hardware clock for Daylight Saving Time twice per year.

In the third case, the reference time is always the time reported. You can use this option if the hardware clock on your machine automatically adjusts for Daylight Saving Time or you would like to manually adjust the hardware time twice a year.

```
moxa@moxa-tbzkb1090923:~$ TZ=EST5EDT
moxa@moxa-tbzkb1090923:~$ export TZ
```

You must include the TZ setting in the `/etc/rc.local` file. The time zone setting will be activated when you restart the computer.

The following table lists other possible values for the TZ environment variable:

Hours From Greenwich Mean Time (GMT)	Value	Description
0	GMT	Greenwich Mean Time
+1	ECT	European Central Time
+2	EET	European Eastern Time
+2	ART	
+3	EAT	Saudi Arabia
+3.5	MET	Iran
+4	NET	
+5	PLT	West Asia
+5.5	IST	India
+6	BST	Central Asia
+7	VST	Bangkok
+8	CTT	China
+9	JST	Japan
+9.5	ACT	Central Australia
+10	AET	Eastern Australia
+11	SST	Central Pacific
+12	NST	New Zealand
-11	MIT	Samoa
-10	HST	Hawaii
-9	AST	Alaska
-8	PST	Pacific Standard Time
-7	PNT	Arizona
-7	MST	Mountain Standard Time
-6	CST	Central Standard Time
-5	EST	Eastern Standard Time
-5	IET	Indiana East
-4	PRT	Atlantic Standard Time
-3.5	CNT	Newfoundland
-3	AGT	Eastern South America
-3	BET	Eastern South America
-1	CAT	Azores

Using the localtime File

The local time zone is stored in the **/etc/localtime** and is used by GNU Library for C (glibc) if no value has been set for the TZ environment variable. This file is either a copy of the **/usr/share/zoneinfo/** file or a symbolic link to it. The V Series computer does not provide **/usr/share/zoneinfo/** files. You should find a suitable time zone information file and write over the original local time file in the V Series computer.

4. Using and Managing Computer Interfaces

In this chapter, we include more information on the V Series computer's interfaces, such as the serial interface, storage, diagnostic LEDs, and the wireless module. The instructions in this chapter cover all functions supported in Moxa's V Series computers. Before referring to the sections in this chapter, make sure that they are applicable to and are supported by the hardware specification of your V Series computer.

Moxa Computer Interface Manager (MCIM)

On many occasions, there isn't one standard method to access and configure specific interfaces on V3000 Series computers because the hardware varies. Hence, programming across different Moxa V3000 Series computer models can be difficult and time consuming. The goal of MCIM is to provide a unified software interface to access and configure non-standard computer interfaces. For example, MCIM can change the serial port interface mode (e.g., RS-232, RS-485-2W, RS-422). However, configuring the serial port baudrate is not possible in MCIM because Linux provides a standard method to set the baudrate.

MCIM is a command-line interface (CLI) utility designed by Moxa to access and manage various interfaces on the V3000 Series computers. Use the `# mx-interface-mgmt` command to display the menu page.

Configuring the Log Level

To set the log level of MCIM, edit the configuration file
`/etc/moxa/MoxaComputerInterfaceManager/MoxaComputerInterfaceManager.conf`

Key	Value	Description
LOG_LEVEL	debug/info/warn/error	The log-level settings for the logs generated by MCIM for debugging and troubleshooting. The default level is "info"

Device Information

Use the `# mx-interface-mgmt deviceinfo` command to get information on your Moxa V3000 Series computer.

Command and Usage	Description
deviceinfo	Show the following information: <ul style="list-style-type: none">Serial number (S/N)Model nameSECUREBOOT (Enabled / Disabled)

LED Indicators

For V3200 series, here are LED indicators:



For V3400 series, here are LED indicators:



Use **# mx-interface-mgmt led** command to get the list of controllable LEDs on your V Series computer. Below is an example of the available LEDs on the V3000 Series.

```
moxa@moxa-tbzk1090923:~$ mx-interface-mgmt led
```

NAME	LABEL	STATE	ALIAS
PL1_Green	PL1:green:programing	off	N/A
PL2_Green	PL1:green:programing	off	N/A
PL3_Green	PL1:green:programing	off	N/A

The MCIM commands for LED indicator controls are listed in the following table:

Command and Usage	Description
led	Shows the following information for all controllable LEDs <ul style="list-style-type: none">Name (as labeled on the device)Model Series of the deviceColor of the LEDDescription of the LEDLED state (on/off/heartbeat)
led <led_name>	Show the above information of a specified LED
led <led_name> get_state	Get the current state (on/off/heartbeat) of a specified LED
led <led_name> set_state <led_state>	Set the state of a specified LED. Value of <state> can be on , off , or heartbeat

If an LED is common across multiple Moxa computer Series, an ALIAS will be provided for that LED. You can use the alias in place of **<led_name>**.

An example of changing the current state of PL1_Green from **ON** to **OFF** is given below:

```
moxa@moxa-tbcde1020938:~$ sudo mx-interface-mgmt led PL1_Green
NAME=PL1_Green
LABEL=PL1:green:programming
STATE=on
ALIAS=N/A
moxa@moxa-tbcde1020938:~$ sudo mx-interface-mgmt led PL1_Green set_state off
moxa@moxa-tbcde1020938:~$ sudo mx-interface-mgmt led PL1_Green get_state
off
```

Storage and Partitions

Use # **mx-interface-mgmt disk** and # **mx-interface-mgmt partition** commands for managing the storage device and partitions.

Command and Usage	Description
disk	Show the following information of all embedded and external storage <ul style="list-style-type: none"> Name (e.g., eMMC, USB, SD) Device node (e.g., /dev/mmcblk0) System disk (Y/N), if 'Y', it is the disk with MIL installed. Number of partitions Automount enabled/disabled (Y/N) I/O state (enabled/disabled)
disk <disk_name>	Show the following information of a specified storage device <ul style="list-style-type: none"> Name (e.g., eMMC, USB, SD) Device node (e.g., /dev/mmcblk0) System disk (Y/N), if 'Y', it is the disk with MIL installed. Partition name and device node Automount enabled/disabled (Y/N) I/O state (enabled/disabled)
disk <disk_name> set_automount <value>	Set a specified external storage device (e.g., USB, SD) to automount when attach to device; <value> is true/false
disk <disk_name> set_io_state <io_state>	Set the I/O state for a specified USB or SD interface: <ul style="list-style-type: none"> Enabled (default) Disables the interface at the GPIO/driver level to reduce the attack surface when the interface is not in use <p><i>Note: Changing the I/O state requires a system reboot</i></p>
partition	Show the following information for partitions on all embedded and external storage devices: <ul style="list-style-type: none"> Name (e.g., eMMC_p1, eMMC_p2, USB_p1) Device node (e.g., /dev/mmcblk0p1) Partition mounted (Y/N) Partition mount point (e.g., /boot_device/p1) Filesystem (e.g., ext4, FAT32)
partition <partition_name>	Show the above information of a specified partition
partition <partition_name> mount	Mount a specified partition
partition <partition_name> unmount	Unmount a specified partition
partition <partition_name> initialize_luks	Encrypts a non-system disk partition (e.g., USB, SD) using LUKS. The encrypted disk will only be mountable on a Moxa computer with the corresponding LUKS key file. <p><i>Note: The user will be prompted to set a minimum 8-character password. This password can be used to recreate the LUKS key file if needed.</i></p> <p>Recommendation: For enhanced security, it is recommended to use this command interactively, where the user is prompted to enter the password. This prevents the password from being exposed in system logs or command history.</p>
partition <partition_name> initialize_luks -i <password>	Performs the above encryption function, but with the password provided as a parameter, bypassing the password prompt.

Command and Usage	Description
<code>partition <partition_name></code> <code>remap_luks</code>	Remaps the encrypted disk to regenerate the LUKS key file. This is useful when you need to mount the encrypted disk on another Moxa computer that does not have the corresponding LUKS key file. Recommendation: For enhanced security, it is recommended to use this command interactively, where the user is prompted to enter the password. This prevents the password from being exposed in system logs or command history.
<code>partition <partition_name></code> <code>remap_luks -i <password></code>	Performs the above remapping function, but with the password provided as a parameter, bypassing the password prompt.

Below is an example of how to query available storage devices:

```
moxa@moxa-tbcde1020938:~$ mx-interface-mgmt disk
NAME  DEVICE          SYSTEM_DISK  NUMBER_OF_PARTITIONS  AUTOMOUNT_SETTING  IO_STATE
NVMe   /dev/nvme0n1    Y            4                     false               N/A
```

To query available partitions and mount the partition 1 of the USB storage drive, use the following command:

```
moxa@moxa-tbcde1020938:~$ mx-interface-mgmt partition
NAME    DEVICE          IS_MOUNTED  FS_TYPE  MOUNTPOINT    MAPPER_DEVICE  UUID
NVMe_p1 /dev/nvme0n1p1  Y           vfat     /boot_device/p1 N/A             3572-0856
NVMe_p2 /dev/nvme0n1p2  Y           ext4     /boot_device/p2 N/A             449babd5-8df...
NVMe_p3 /dev/nvme0n1p3  Y           ext4     /boot_device/p3 N/A             debc0828-838...
NVMe_p4 /dev/nvme0n1p4  Y           ext4     /boot_device/p4 N/A             4817c801-31f...
```



WARNING

Setting external storage device to automount may expose your device to cybersecurity risks. It is strongly recommended that you not automount storage device unless your device is placed in a highly secure environment.

Creating an Encrypted External Storage (e.g., USB, SD)

Below is an example of how to create an encrypted USB storage device:

1. Insert a USB card and use **mx-interface-mgmt partition** command to check the name of the available USB partition.

```
moxa@moxa-imoxa0920070:/home/moxa# sudo mx-interface-mgmt partition

NAME    DEVICE          IS_MOUNTED  FS_TYPE  MOUNTPOINT    MAPPER_DEVI  UUID
SD_p1   /dev/mmcblk1p1  N           N/A      N/A           N/A          3e9f8825-1f7...
USB_p1  /dev/sda1       N           N/A      N/A           N/A          N/A
USB_p2  /dev/sda2       N           N/A      N/A           N/A          f4d582eb-f54...
USB_p3  /dev/sda3       N           N/A      N/A           N/A          N/A
eMMC_p1 /dev/mmcblk2p1  Y           ext4     /boot_device/p1 N/A          9ee65098-22a...
eMMC_p2 /dev/mmcblk2p2  Y           ext4     /boot_device/p2 N/A          ae9ebafe-629...
eMMC_p3 /dev/mmcblk2p3  Y           ext4     /boot_device/p3 N/A          fd7f9645-6b7...
eMMC_p4 /dev/mmcblk2p4  Y           ext4     /boot_device/p4 N/A          ab1aad4a-8a9...
```

2. Select a partition on the USB (e.g., USB_p1 for the 1st partition of the USB) to encrypt and set a password with a minimum length of 8 characters.

```
moxa@moxa-imoxa0920070:/home/moxa# sudo mx-interface-mgmt partition USB_p1
initialize_luks

[Warning]: Initializing a partition as LUKS will erase all data on the partition.
Enter password:
Re-enter password:
```

3. Now, USB_p1 is LUKS encrypted, and the corresponding LUKS key file is securely hashed using SHA-512 and stored on this computer. As a result, USB_p1 can only be mounted on this specific computer.

4. If the computer is ever restored to factory default or a new system image is installed, resulting in the loss of the LUKS key file, you can regenerate the key file using the **remap_luks** command by entering the password set in step #2. The same method can also be used when you want to mount the encrypted USB on a different Moxa computer with MIL3.

```
moxa@moxa-imoxa0920070:/home/moxa# sudo mx-interface-mgmt partition USB_p1 mount

Error: GDBus.Error:com.moxa.ComputerInterfaceManager.Error.Core.Failed: LUKS open
process failed: cannot get passphrase from config

moxa@moxa-imoxa0920070:/home/moxa# sudo mx-interface-mgmt partition USB_p1 remap_luks
Enter password:
moxa@moxa-imoxa0920070:/home/moxa# sudo mx-interface-mgmt partition USB_p1 mount
root@moxa-imoxa0920070:/home/moxa# sudo mx-interface-mgmt partition
```

NAME	DEVICE	IS_MOUNTED	FS_TYPE	MOUNTPPOINT	MAPPER_DEVICE	UUID
SD_p1	/dev/mmcblk1p1	N	N/A	N/A	N/A	3e9f8825-1f7...
USB_p1	/dev/sda1	Y	ext4	/media/USB_p1	sda1_encrypted	44efd7d6-7ea...
USB_p2	/dev/sda2	N	N/A	N/A	N/A	f4d582eb-f54...
USB_p3	/dev/sda3	N	N/A	N/A	N/A	N/A
eMMC_p1	/dev/mmcblk2p1	Y	ext4	/boot_device/p1	N/A	9ee65098-22a...
eMMC_p2	/dev/mmcblk2p2	Y	ext4	/boot_device/p2	N/A	ae9ebafe-629...
eMMC_p3	/dev/mmcblk2p3	Y	ext4	/boot_device/p3	N/A	fd7f9645-6b7...
eMMC_p4	/dev/mmcblk2p4	Y	ext4	/boot_device/p4	N/A	ab1aad4a-8a9...

Push Button

There are three actions after users push the "Push buttons". Use the # **mx-interface-mgmt button** command to switch between three actions described below:

1. Default - Moxa default action and direct link to hot swap SSD mount and unmount.
 - a. Short push (release button in 3 seconds) - scan hot swap SSD disks.
 - b. Long push (release button latter than 3 seconds) - unmount hot swap SSD disks, and users can remove SSD disks safely.
2. Disabled - no actions after users push the button
3. User-Defined - users can define preferred actions after pushing the button

Command and Usage	Description
button	Shows the current action of each button on the device. Name - DISK1 and DISK2 Action - default, disabled, user-defined
button <button_name>	Shoe detailed information of the specified button.
button <button_name> get_action	Get the action of the specified button.
button <button_name> set_action	Set the action of the specified button.

If users want to support the SSD disk auto-mount after hot swap an SSD disk, here is an example:

```
moxa@moxa-imoxa0920070:/home/moxa# mx-interface-mgmt button
NAME  ACTION
DISK1  default
DISK2  default
moxa@moxa-imoxa0920070:/home/moxa# mx-interface-mgmt disk
NAME          DEVICE          SYSTEM_DISK  NUMBER_OF_PARTITIONS  AUTOMOUNT_SETTING
NVMe          /dev/nvme0n1    Y            4                      false
SATA_DISK1    /dev/sbb        N            4                      false
SATA_DISK2    /dev/sda        N            3                      false
moxa@moxa-imoxa0920070:/home/moxa# mx-interface-mgmt disk SATA_DISK1
set_automount true
moxa@moxa-imoxa0920070:/home/moxa# mx-interface-mgmt disk
NAME          DEVICE          SYSTEM_DISK  NUMBER_OF_PARTITIONS  AUTOMOUNT_SETTING
NVMe          /dev/nvme0n1    Y            4                      false
SATA_DISK1    /dev/sbb        N            4                      true
SATA_DISK2    /dev/sda        N            3                      false
```

Serial Port

Configuring the Serial Interface via MCIM

Depending on the Moxa computer Series, the serial ports support various operation modes, including RS-232, RS-422, RS-485 2-wire, and RS-485 4-wire, with flexible baudrate settings. The default operation mode is RS-232.

Use the # `mx-interface-mgmt serialport` command to configure the operation mode, enable or disable the serial port, and adjust the resistor and terminator settings.

Command and Usage	Description
<code>serialport</code>	Shows the following information for all serial ports on the device: Name (as labeled on device) Device node (e.g., /dev/ttyM0) Current operation mode configured I/O state (enabled/disabled) Resistor <ul style="list-style-type: none">• Enabled: 1k-ohm pull-up/pull-down resistor applied• Disabled (default): 150k-ohm pull-up/pull-down resistor applied• N/A: This current operation mode (e.g., RS-232) doesn't support resistor Terminator <ul style="list-style-type: none">• Enabled: 120-ohm termination resistor applied• Disabled (default): 120-ohm termination resistor not applied• N/A: This current operation mode (e.g., RS-232) doesn't support terminator
<code>serialport <serialport_name></code>	Shows the following information for a specified serial port: - All serial port information (listed above) - Supported baudrates
<code>serialport <serialport_name> get_interface</code>	Gets the current operation mode for a specified serial port
<code>serialport <serialport_name> set_interface <serial_interface></code>	Sets the operation mode for a specified serial port.
<code>serialport <serialport_name> set_io_state <io_state></code>	Set the I/O state for a specified serial port: <ul style="list-style-type: none">• Enabled (default)• Disables the interface at the GPIO/driver level to reduce the attack surface when the interface is not in use <i>Note: Changing the I/O state requires a system reboot</i>
<code>serialport <serialport_name> set_pull_up_down <state></code>	Set the pull-up/pull-down resistor for a specified serial port: <ul style="list-style-type: none">• Enabled: 1k-ohm pull-up/pull-down resistor applied• Disabled (default): 150k-ohm pull-up/pull-down resistor applied
<code>serialport <serialport_name> set_terminator <state></code>	Set the 120-ohm termination resistor for a specified serial port: <ul style="list-style-type: none">• Enabled: 120-ohm termination resistor applied• Disabled (default): 120-ohm termination resistor not applied

Changing the Serial Port Operation Mode

For example, to change the mode of COM1 serial port from default RS-232 mode to the RS-422 mode, use the following command:

```
moxa@moxa-tbcde1020938:~$ mx-interface-mgmt serialport
NAME  DEVICE      INTERFACE  IO_STATE  PULL_UP_DOWN_RESISTOR  TERMINATOR
P1    /dev/ttyM0   RS-232     N/A       N/A                  N/A
P2    /dev/ttyM1   RS-232     N/A       N/A                  N/A
moxa@moxa-tbcde1020938:~$ mx-interface-mgmt serialport P1
NAME=P1
DEVICE=/dev/ttyM0
SUPPORTED_INTERFACES=RS-232,RS-485-2W,RS-422
SUPPORTED_BAUDRATES=50,75,110,134,150,300,600,1200,1800,2000,2400,3600,4800,7200,9600,19200,38400,57600,115200
INTERFACE=RS-232
IO_STATE=N/A
PULL_UP_DOWN_RESISTOR=N/A
TERMINATOR=N/A
moxa@moxa-tbcde1020938:~$ sudo mx-interface-mgmt serialport P1 set_interface RS-422
moxa@moxa-tbcde1020938:~$ sudo mx-interface-mgmt serialport P1 get_interface RS-422
moxa@moxa-tbcde1020938:~$
```

Changing Other Serial Interface Settings with STTY

The **stty** command is used to view and modify the serial terminal settings.

Displaying All Settings

Use the following example to display all serial terminal settings of COM1 serial port.

```
moxa@moxa-tbcde1020938:~$ mx-interface-mgmt serialport
NAME  DEVICE      INTERFACE  IO_STATE  PULL_UP_DOWN_RESISTOR  TERMINATOR
P1    /dev/ttyM0   RS-422     N/A       N/A                  N/A
P2    /dev/ttyM1   RS-232     N/A       N/A                  N/A
moxa@moxa-tbcde1020938:~$ sudo stty -a -F /dev/ttyM0
speed 9600 baud; rows 0; columns 0; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>;
swtch = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W;
lnext = ^V;
discard = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 hupcl -cstopb cread clocal -crtcts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl ixon -ixoff
-iuclc -ixany
-imaxbel -iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echopr
echoctl echoke
-flusho -extproc
moxa@moxa-tbcde1020938:~$
```

Configuring Serial Settings

The following example changes the baudrate to 115200.

```
moxa@moxa-tbzk1090923:~$ sudo stty 115200 -F /dev/ttyM0
```

Check the settings to confirm that the baudrate has changed to 115200.

```
moxa@moxa-tbzk1090923:~$ sudo stty -a -F /dev/ttyM0
speed 115200 baud; rows 0; columns 0; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>;
eol2 = <undef>; swch = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R;
werase = ^W; lnext = ^V; flush = ^O; min = 1; time = 0;
-parenb -parodd cs8 hupcl -cstopb cread clocal -crtcts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl ixon -ixoff
-iuclc -ixany -imaxbel -iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echopr
echoctl echoe
```



NOTE

Detailed information on the **stty** utility is available at the following link:

<https://manpages.debian.org/bullseye/coreutils/stty.1.en.html>

Ethernet Interface

Use # **mx-interface-mgmt ethernet** command to configure the Ethernet ports.

Command and Usage	Description
ethernet	Show the following information of all ethernet ports on the device. <ul style="list-style-type: none">Name (as labeled on device)Network interface name (eth0, eth1, etc.)I/O state (enabled/disabled)
ethernet <ethernet_name>	Show the above information of a specified ethernet port
ethernet <ethernet_name> set_io_state <io_state>	Set the I/O state for a specified ethernet port: <ul style="list-style-type: none">Enabled (default)Disables the interface at the GPIO/driver level to reduce the attack surface when the interface is not in use <i>Note: Changing the I/O state requires a system reboot</i>

```
moxa@moxa-tbcde1020938:~$ mx-interface-mgmt ethernet
NAME  DEVICE_NAME  IO_STATE
LAN1  eno1          N/A
LAN2  eno2          N/A
LAN3  eno3          N/A
LAN4  eno4          N/A
LAN5  eno5          N/A
LAN6  eno6          N/A
LAN7  eno7          N/A
LAN8  eno8          N/A
moxa@moxa-tbcde1020938:~$ mx-interface-mgmt ethernet LAN1
NAME=LAN1
DEVICE_NAME=eno1
IO_STATE=N/A
moxa@moxa-tbcde1020938:~$
```

Digital Input/Output (DIO)

Use the `# mx-interface-mgmt dio` command to query and configure the state for each digital input/output (DIO) interface, and also configure the hook script.

Command and Usage	Description
<code>dio</code>	Shows the following information of all DIO interfaces: <ul style="list-style-type: none">• Name (as labeled on device)• State (high/low)• Event• Path of falling edge script• Path of rising edge script
<code>dio <dio_name></code>	Shows the above information of a specified DI or DO interface
<code>dio <dio_name> get_state</code>	Gets the current state (high/low) of a specified DI or DO interface
<code>dio <dio_name> set_state <dio_state></code>	Sets the state (high/low) of a specified DO interface
<code>dio <di_name> get_event</code>	Gets the current event setting (none, falling, rising, or change) for the specified DI interface
<code>dio <di_name> set_event <di_event></code>	Sets the event (none, falling, rising, or change) for the specified DI interface
<code>dio <dio_name> get_direction</code>	Gets the direction (input/output) for the specified DIO interface
<code>dio <dio_name> set_direction <direction></code>	Sets the direction (input/output) for the specified DIO interface. This function is only available on computers with a DIO interface that can be configured as either DI (Digital Input) or DO (Digital Output)
<code>dio <dio_name> reload</code>	Reload the DIO configuration after using the set_event or set_direction command
<code>[Disabled] dio <dio_name> add_hook <edge> <path></code>	Execute a script from a specified path when the dio state changes. <ul style="list-style-type: none">• <edge> specifies whether the trigger should react to a "rising" or "falling" edge.• <path> is the path to the script that should be executed when the specified edge transition occurs.
<code>[Disabled] dio <dio_name> remove_hook <edge></code>	Removes the edge script (rising/falling) of an interface



NOTE

- The predetermined state of the digital output interface is high (open circuit).
- Starting from MIL 3.3, the **set_event** and **get_event** function will support only the DI interface, as it makes more sense for customers to define the desired actions in their code when controlling the DO state.
- Starting from MIL 3.1, **add_hook** and **remove_hook** have been replaced by a more flexible configuration method, as described below.

Starting with MIL 3.1, we have introduced a more flexible method for configuring the hook script for DI's edge transitions. Detailed instructions can be found in the 'README' file located in the directory `'/etc/moxa/MoxaComputerInterfaceManager/dio-scripts'`.

An example of setting up the Moxa Computer Interface Manager (MCIM) to automatically execute a script when the signal of the first digital input (DI1) changes from low to high (rising) or from high to low (falling) is outlined below:

1. Navigate to `'/etc/moxa/MoxaComputerInterfaceManager/dio-scripts/'` and create a script named 'DI1.script' :
2. Add the following content to DI1.script to log an event whenever DI1 changes:

```
#!/bin/bash
echo "The input value of Digital Input 1 (DI1) has changed" >>
/var/log/di1.log
```

3. Make the script executable

```
root@moxa-tbzgb1057611:/etc/moxa/MoxaComputerInterfaceManager/dio-scripts#
chmod +x DI1.script
```

4. Open '**peripheral-settings.conf**' located in '**/etc/moxa/MoxaComputerInterfaceManager/**' and set the event value for [DIO/DI1] to 3 to detect both rising and falling edges:

The event ID corresponds to the following actions:

- Event=0: none (default)
- Event=1: signal change from high to low (falling)
- Event=2: signal change from low to high (rising)
- Event=3: signal change from low to high (rising) or high to low (falling)

```
[DIO/DI1]
Event=3
```

5. Apply the changes by restarting the MoxaComputerInterfaceManager service:

```
root@moxa-tbzgb1057611: systemctl restart MoxaComputerInterfaceManager
```



NOTE

Steps 4 and 5 mentioned above can be replaced by the **set_event** and **reload** command in MIL version 3.2 and later.

6. Ensure the script is correctly configured and active by checking the settings. The '**EVENT**' should be set to '**change**' and '**ACTIVE**' should show '**yes**':

```
root@moxa-tbcib1020938:~$ mx-interface-mgmt dio
NAME  STATE  EVENT  ACTIVE  GPIO_PIN  DIRECTION
DI1   high   change  yes     456       input
DI2   high   none    no      457       input
DO1   high   none    no      453       output
DO2   high   none    no      454       output
```

Buzzer

Use the # **mx-interface-mgmt buzzer** command to query and set the state for buzzer alarm on the V3000 Series computer that has a buzzer.

Command and Usage	Description
buzzer	Show the following information of all buzzers <ul style="list-style-type: none"> • Name • State (on/off) • Device Type • GPIO pin
buzzer <buzzer_name>	Show the following information of a specified buzzer <ul style="list-style-type: none"> • Name • State (on/off) • Device Type • GPIO pin
buzzer <buzzer_name> get_state	Get the current state (on/off) of a specified buzzer
buzzer <buzzer_name> set_state	Set the state (on/off) of a specified buzzer

Cellular Module Interface

Use # `mx-interface-mgmt cellular` command to query and manage cellular module(s)

Command and Usage	Description
<code>cellular</code>	Show the following information for all cellular modules. <ul style="list-style-type: none">Name (e.g., Cellular1)Network interface name (wwan0, wwan1, etc.)Cellular module detected (true/false)
<code>cellular <name></code>	Show the detail information of a specified cellular module <ul style="list-style-type: none">Name (e.g., Cellular1)Network interface name (wwan0, wwan1)Cellular module detected (true/false)QMI Port (e.g., /dev/cdc-wdm0)AT Port (e.g., /dev/ttyUSB4)GPS Port (e.g., /dev/ttyUSB3) if GPS is supportedCellular module power status (on/off)Number of available SIM slots on the deviceThe SIM slot # that is currently used by the cellular module <i>Note: SIM slot # correspond to the labeled slot # on the device</i>
<code>cellular <name> get_power</code>	Get the cellular module power status (on/off).
<code>cellular <name> set_power <power_state></code>	Set the cellular module power status (on/off). <i>Note: Module will power-on when device reboot</i>
<code>cellular <name> get_sim_slot</code>	Get the SIM slot # that is currently used by the cellular module
<code>cellular <name> set_sim_slot <sim_slot></code>	Set the SIM slot # used by cellular module. Module power off/on is required for SIM slot changed to take effect. <i>Note: SIM slot # will be set to default (slot 1) when the device reboot</i>



NOTE

1. Some cellular modules may not support power on/off or SIM slot control.
2. If you are using Moxa Connection Manager (MCM) to manage the cellular connection, do not use `set_power` or `sim_slot` commands as they might interrupt MCM's network failover/failback operations.

An example of using MCIM to query the cellular module information and changing the SIM slot # use by the module from slot 1 to 2 is given below:

```
moxa@moxa-tbzk1090923:~$ mx-interface-mgmt cellular
NAME          DEVICE_NAME  DEVICE_DETECTED
Cellular1     wwan0        true
moxa@moxa-tbzk1090923:~$ mx-interface-mgmt cellular Cellular1
NAME=Cellular1
DEVICE_NAME=wwan0
QMI_PORT=/dev/cdc-wdm0
AT_PORT=/dev/ttyUSB4
GPS_PORT=/dev/ttyUSB3
DEVICE_DETECTED=true
POWER=on
SIM_SLOT_NUMBER=2
SIM_SLOT=1
moxa@moxa-tbzk1090923:~$ mx-interface-mgmt cellular Cellular1 set_sim_slot 2
moxa@moxa-tbzk1090923:~$ mx-interface-mgmt cellular Cellular1 get_sim_slot 2
```


Wi-Fi Module Interface

Use the # `mx-interface-mgmt wifi` command to query and manage Wi-Fi modules.

Command and Usage	Description
<code>wifi</code>	Shows the following information of all Wi-Fi modules. <ul style="list-style-type: none">Name (e.g., WiFi1)Network interface name (wlan0, wlan1)Wi-Fi module detected (true/false)
<code>wifi <name></code>	Shows the above information for a specified Wi-Fi module
<code>wifi <name> get_power</code>	Gets the Wi-Fi module power status (on/off).
<code>wifi <name> set_power <power_state></code>	Set the Wi-Fi module power status (on/off). <i>Note: The module will power-on when the device reboots.</i>



NOTE

Some Wi-Fi modules may not support power on/off control.

Socket Interface

Use the # `mx-interface-mgmt socket` command manage the Mini PCI-E sockets on the Moxa V Series Computer

Command and Usage	Description
<code>socket</code>	List all the available sockets' name (e.g., Socket1, Socket2)
<code>socket <socket_name></code>	Shows the following information for a specified Mini PCI-E socket <ul style="list-style-type: none">Name (e.g., Socket1, Socket2)Power status (on/off)Number of available SIM slots if a cellular module is insert to this Mini PCI-E socketGet the SIM slot # that is currently used by the cellular module on this Mini PCI-E socket <i>Note: SIM slot # correspond to the labeled slot # on the device.</i>
<code>socket < socket_name> get_power</code>	Gets the power status (on/off) for a specified Mini PCI-E socket
<code>socket <name> set_power <power_state></code>	Set the power status (on/off) for a specified Mini PCI-E socket. <i>Note: The socket will power-on when the device reboots.</i>

Configuring the Real COM Mode

You can use Moxa's NPort Series serial device drivers to extend the number of serial interfaces (ports) on your UC computer. The NPort comes equipped with COM drivers that work with Windows systems and TTY drivers for Linux systems. The driver establishes a transparent connection between the host and serial device by mapping the IP Port of the NPort's serial port to a local COM/TTY port on the host computer.

Real COM Mode also supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device at the same time.

One of the major conveniences of using Real COM Mode is that Real COM Mode allows users to continue using RS-232/422/485 serial communications software that was written for pure serial communications applications. The driver intercepts data sent to the host's COM port, packs it into a TCP/IP packet, and then redirects it through the host's Ethernet card. At the other end of the connection, the NPort accepts the Ethernet frame, unpacks the TCP/IP packet, and then sends it transparently to the appropriate serial device attached to one of the NPort's serial ports.

To install Real COM driver, download the driver using apt from Moxa software repository with internet access. You will be able to view the driver related files in the `/usr/lib/npreal2/driver` folder after successful installation.

```
root@moxa-tbzkbl090923:~# apt install moxa-nport-real-tty-utils

> mxaddsvr (Add Server, mapping tty port)
> mxdelsvr (Delete Server, unmapping tty port)
> mxloadsvr (Reload Server)
> mxmknod (Create device node/tty port)
> mxrmnod (Remove device node/tty port)
> mxuninst (Remove tty port and driver files)
```

At this point, you will be ready to map the NPort serial port to the system **tty** port. For a list of supported NPort devices and their revision history, click <https://www.moxa.com/en/support/search?psid=50278>.

Mapping TTY Ports

Make sure that you set the operation mode of the desired NPort serial port to Real COM mode. After logging in as a super user, enter the directory `/usr/lib/npreal2/driver` and then execute `mxaddsvr` to map the target NPort serial port to the host tty ports. The syntax of `mxaddsvr` command is as follows:

```
mxaddsvr [NPort IP Address] [Total Ports] ([Data port] [Cmd port])
```

The `mxaddsvr` command performs the following actions:

1. Modifies the `npreal2d.cf`.
2. Creates tty ports in the `/dev` directory with major & minor number configured in `npreal2d.cf`.
3. Restarts the driver.

Mapping TTY Ports (automatic)

To map tty ports automatically, execute the `mxaddsvr` command with just the IP address and the number of ports, as shown in the following example:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16
```

In this example, 16 tty ports will be added, all with IP 192.168.3.4 consisting of data ports from 950 to 965 and command ports from 966 to 981.



ATTENTION

You must reboot the system after mapping tty ports with `mxaddsvr`.

Mapping TTY Ports (manual)

To map tty ports manually, execute the **mxaddsvr** command and specify the data and command ports as shown in the following example:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16 4001 966
```

In this example, 16 tty ports will be added, all with IP 192.168.3.4, with data ports from 4001 to 4016 and command ports from 966 to 981.



ATTENTION

You must reboot the system after mapping tty ports with **mxaddsvr**.

Removing Mapped TTY Ports

After logging in as root, enter the directory `/usr/lib/npreal2/driver` and then execute the **mxdelsvr** command to delete a server. The syntax of **mxdelsvr** is:

mxdelsvr [IP Address]

Example:

```
# cd /usr/lib/npreal2/driver
# ./mxdelsvr 192.168.3.4
```

The following actions are performed when the **mxdelsvr** command is executed:

1. Modify `npreal2d.cf`.
2. Remove the relevant tty ports from the `/dev` directory.
3. Restart the driver.

If the IP address is not provided in the command line, the program will list the installed servers and total ports on the screen. You will need to choose a server from the list for deletion.

Moxa MCU Manager (MMM)

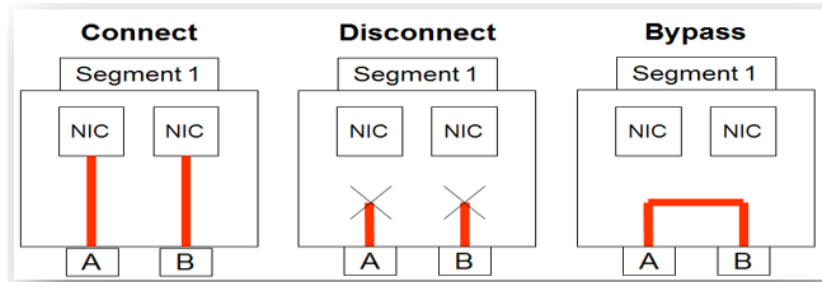
Moxa MCU Manager (MMM) is a tool that manages microcontroller (MCU) features on Moxa x86 computer products, including LAN bypass, panel display, panel programmable LEDs, and MCU ROM firmware updates. MMM is a command-line interface (CLI) utility, and you can use the **# mx-mcu-mgmt** command to manage microcontrollers.

Command and Usage	Description
mcu_version	Get MCU firmware version
relay	Manage relay status
Wdt_relay	Manage watchdog relay status
poweroff_relay	Manage power off (S5) relay status
app_wdt_relay	Manage app watchdog relay status
app_wdt_timeout	Configure app watchdog timeout
mcu_upgrade	Upgrade MCU firmware

Manage LAN Bypass

The LAN Bypass feature support the following three modes:

1. Connect - LAN A and LAN B ports are connected to the NICs and is data transmitted through system normally.
2. Disconnect - LAN A and LAN B ports are neither connected to the NICs nor to each other, which means that data packets are blocked.
3. Bypass - LAN A and LAN B ports are connected to each other to keep transmitting data without interruption even when a system device crashes or encounters cyberattacks.



Use the **# mx-mcu-mgmt relay** command to manage the LAN bypass mode.

Command and Usage	Description
get_mode	Get current LAN bypass mode
Set_mode connect	Set LAN bypass mode to the connect mode
Set_mode disconnect	Set LAN bypass mode to the disconnect mode
Set_mode bypass	Set LAN bypass mode to the bypass mode

Manage Watchdog Relay

Use the Watchdog Relay to change MCU RTC watchdog status.

use the **# mx-mcu-mgmt wdt_relay** command to manage the watch relay mode.

Command and Usage	Description
get_mode	Get current watch relay mode
Set_mode connect	Set watch relay mode to the connect mode
Set_mode disconnect	Set watch relay mode to the disconnect mode
Set_mode bypass	Set watch relay mode to the bypass mode

Manage Power Off Relay

Use the Power Off Relay to change powered off (S5 state) status.

use the **# mx-mcu-mgmt poweroff_relay** command to manage the power off relay mode.

Command and Usage	Description
get_mode	Get current power off relay mode
Set_mode disconnect	Set power off relay mode to the disconnect mode
Set_mode bypass	Set power off relay mode to the bypass mode

App Watchdog Modes Control Utility

App watchdog modes utility is used to configure microcontroller parameters such as timeout value, timeout-reset function, timeout-relay mode, and kicking service and daemon.

App WDT

Use App WDT to enable or disable the MCU watchdog application. Activating the watchdog function is key to creating a trigger to activate LAN bypass when your application encounters issues or is unresponsive.

use the **# mx-mcu-mgmt app_wdt_timeout** command to configure the MCU watchdog application.

Command and Usage	Description
get_timeout	Get the time out of MCU watchdog application
Set_timeout X	Enable MCU watchdog application and set timeout to X sec
Set_timeout 0	Enable MCU watchdog application

App WDT Relay

Use App WDT relay to change the MCU watchdog application relay status.

use the **# mx-mcu-mgmt app_wdt_relay** command to manage the MCU watchdog application status.

Command and Usage	Description
get_mode	Get the current MCU watchdog application mode
Set_mode connect	Set MCU watchdog application to the connect mode
Set_mode disconnect	Set MCU watchdog application to the disconnect mode
Set_mode bypass	Set MCU watchdog application to the bypass mode

Upgrade Moxa MCU Manager (Only available on V3000 series 8 LAN models)

use the **# mx-mcu-mgmt mcu_upgrade** command to upgrade firmware running in the microcontroller. Before using this command, ensure that all Moxa MCU related services are stopped. Here is an example:

```
root@moxa-tbzk1090923:~# mx-mcu-mgmt mcu_upgrade FB_MCU_V3000_V1.bin
MCU firmware file path: FB_MCU_V3000_V1.bin
Do you want to upgrade the firmware? (y/n): y
Upgrade in progress, please DO NOT power off the system!
[#####] 100%
Upgrade completed! Please reboot the system.
root@moxa-tbzk1090923:~#
```

After rebooting your system, you can use the **# mx-mcu-mgmt mcu_version** to check the current running MCU firmware version. Here is an example:

```
root@moxa-tbzk1090923:~# mx-mcu-mgmt mcu_version
1.0.0[S08]
```

Moxa BIOS Manager

Moxa BIOS Manager is a command-line interface (CLI) utility to help you update V3000 series BIOS, and you can use the # **mx-bios-mgmt** command to manage BIOS itself.

Command and Usage	Description
update	Update BIOS
info	Get BIOS version

Here is an example to upgrade V3000 series BIOS.

```
root@moxa-tbzk1090923:~# mx-bios-mgmt update -f V3400_BIOS_V1.5.0S00.bin
ROM file BIOS version: V1.5.0S00
Current BIOS version: V1.4.0S03
BIOS update failure could result in device malfunction.
Please make sure that there will be no interruption during the update process.
Do you want to continue? (y/n) y
Start to update BIOS from ROM file: V3400_BIOS_V1.5.0S00.bin

      Insyde H2OFFT (Flash Firmware Tool) cersion (SEG) 200.02.00.13
      Copyright(c) 2012 - 2024, Insyde Software Corp. All Rights Reserved.

      Initializing
      Current BIOS Model name: V3000
      New      BIOS Model Name: V3000

      Current BIOS version: V1.4.0S03
      New      BIOS version: V1.5.0S00

      Warning
      Please do not remove the power
```

5. V3000 Configuring and Managing Networks

Moxa Connection Manager (MCM)

MCM is a network management utility developed by Moxa to manage the LAN and WAN network on your Moxa V3000 Series computer, including Wi-Fi, cellular, and ethernet interfaces. With MCM, you can easily fill in the connection profile and priority in the configuration file; then MCM will automatically connect and keep the connection alive. Following are the major features of MCM:

- Cellular, Ethernet and Wi-fi connection
- Connection auto keep-alive, failover, and failback
- DHCP server
- Data usage monitoring
- Cellular connection diagnosis tool
- Cellular modem and network information
- Cellular modem firmware upgrade with failback



NOTE

You can find the detailed online user manual for the Moxa Connection Manager (MCM) at the following link: [Moxa Connection Manager Reference Manual](#)

The default configurations for the Moxa Connection Manager (MCM) are listed in the following table:

Interface	Default Managed by MCM	Network Configuration
LAN1	Yes	<ul style="list-style-type: none">• Set as DHCP WAN by default.• After boot up, if LAN1 cannot obtain IP from DHCP server for 20 seconds, then link-local IP addresses is automatically assigned. <i>Note: This process is achieved by setting profile-1 of LAN1 to WAN type with IPv4 DHCP, and profile-2 to IPv4 link-local. If profile-1 fails to obtain an IPv4 address from the DHCP server, it will automatically switch to profile-2.</i>
LAN2	No	Static IPv4, 192.168.4.127 retrieve from /etc/network/interfaces
Cellular/ Wi-Fi	No	Not configured

To run **MCM**, you must use root permission to run **# mx-connect-mgmt**

```
MOXA Connection Management Command-line Utility

USAGE:
  mx-connect-mgmt [SUBCOMMAND]

FLAGS:
  -h, --help      Prints help information
  -V, --version    Prints version information

SUBCOMMANDS:
  GPS              Control GPS interface
  configure        MOXA Connection Management via GUI dialog
  datausage        Show interface data usage information and related functions
  default          Reset to default configuration
  debug            and diagnose cellular connection
  help             Show the help menu
  ls               List available network interfaces
  modem            Upgrade cellular modem firmware
  nwk_status       Show network and modem's information and connection status
  reload           configuration files and restart interfaces
  start            to control interfaces
  stop             to control interfaces
  unlock_pin       Unlock SIM PIN for the specified interface
  unlock_puk       Unlock PUK and reset SIM PIN for the specified interface
  wifi            Search Wi-Fi AP
```



NOTE

By default, only LAN1 port is managed by MCM.

There are 2 types of configuration files for MCM. One is main configuration file to manage the interrelationship between each interface, and one configuration files per each network interfaces available on Moxa V3000 Series computer

Config Type	Description	File Location
Main Config.	Main configuration file which is to configure which network interface you would like MCM to manage and set the priority during failover/failback	/etc/moxa/MoxaConnectionManager/ MoxaConnectionManager.conf
Interface Config.	Per interface configuration file which is to configure properties of individual interfaces. Such as APN, PIN code of cellular connection or SSID and password of Wi-Fi.	/etc/moxa/MoxaConnectionManager/ /interfaces/[interface name].conf



NOTE

- When modification is made to configuration file, you must use **# mx-connect-mgmt reload** to make the change effective.
- You can find the detailed configuration file structure in the "Configuration File" chapter of the [Moxa Connection Manager Reference Manual](#).
- We highly recommend using the GUI Configurator, described in the next section, instead of editing the configuration file directly, as it automatically checks for conflicts.

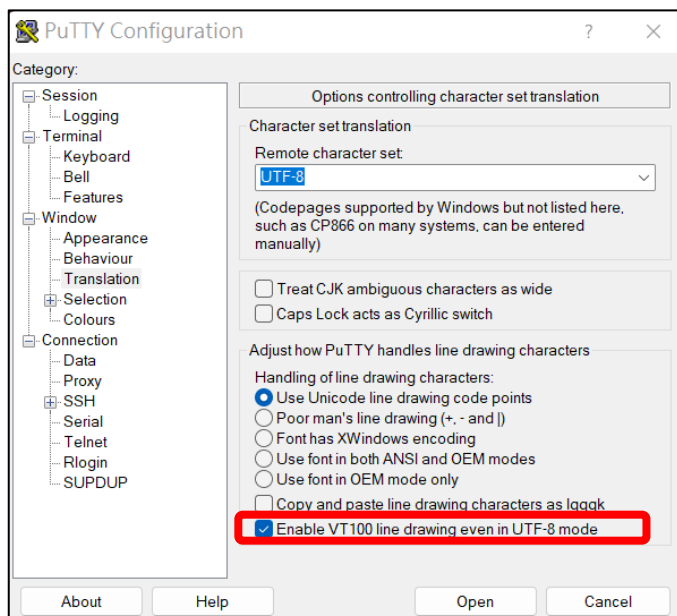
Instead of modifying the configuration file directly, we highly recommend you use the **GUI Configurator** described in next section to configure MCM.

Setting Up MCM With a GUI-based Configurator

Overview

To configure the WAN network through Ethernet, Wi-Fi, or cellular interface on the V3000 computer, you can use the simple GUI dialog provided by running the `# mx-connect-mgmt configure` command.

If you are using PuTTY, enable **VT100 line drawing** option under **Windows > Translation** for the GUI to show correctly.



To configure the network settings, do the following:

1. Go to the main page.

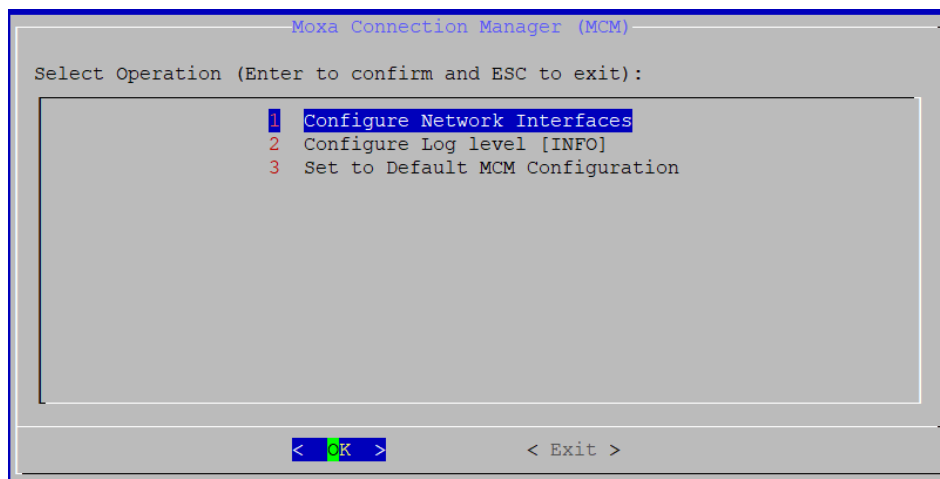


Figure 5.1 – Main page

Option Name	Description
Configure Network Interface	Configure network setting for each network interface
Configure Log Level	<ul style="list-style-type: none">• Available syslog levels are ERR, WARN, INFO, DEBUG, TRACE• MCM log is save in /var/log/syslog
Set to Default MCM Configuration	Set all configuration to default

2. Configure network type for each interface and set the WAN connection priority for failover/failback.

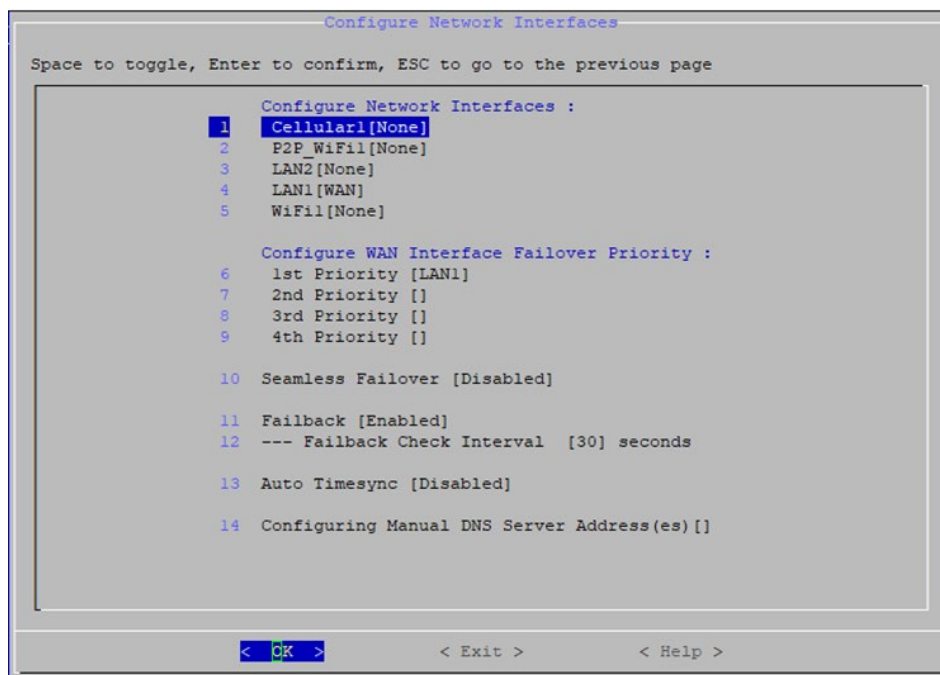


Figure 5.2 –Configure network interface

Option Name	Description
Configure Network Interfaces	<p>A list of available network interfaces will show, where you can set the network type for each interface. The options are:</p> <ul style="list-style-type: none"> WAN - When set to WAN, this interface will be added to the default gateway list and allow MCM to apply automatic keep-alive and failover/failback control over it LAN - When set to LAN, MCM will connect this interface using the network attributes defined in Profile-1 and DHCP server can be enabled for this interface LAN Bridge - Bridge two or more LAN interfaces to construct a larger LAN Manual - When set to Manual, it allows the user to have total control over this interface. MCM will connect this interface one-time only network attributes defined in Profile-1. MCM will not set these interfaces as the default gateway nor apply connection keep-alive and failover/failback control over it. None - MCM will not manage this interface
Seamless Failover	<ul style="list-style-type: none"> Disabled (default) - If the primary connection fails, MCM tries all pre-configured profiles before switching to the backup interface, causing some downtime during failback. Enabled - If the primary connection fails, MCM will not attempt to try all the profiles configured for the primary connection. MCM will immediately switches to the connected backup interface, avoiding downtime. <p><i>Note: Using ping for the backup's keep-alive may incur data costs.</i></p>
Configure WAN Interface Priority	<p>MCM will use the WAN interface set as 1st Priority as the default gateway. When the 1st priority interface becomes unavailable, MCM will automatically failover to the next priority interface.</p>
Enable/Disable Failback	<ul style="list-style-type: none"> When enabled, the backup connection will automatically failback to the higher priority connection when it became available again Failback Check Interval - This value specifies how long (in seconds) the higher priority connection must remain stable before MCM triggers a failback, preventing frequent failover and failback due to instability
Auto Timesync	<ul style="list-style-type: none"> Disabled (default) - Disables the auto time-sync function. GPS - Syncs the system clock using GPS time. Requires a GPS antenna and the GPS function to be enabled. Chrony - Uses the Chrony service to sync the system clock via an NTP server. Cellular - Syncs the system clock using the cellular base station's time. A cellular connection is required.

Option Name	Description
Configure Manual DNS server Address(es)	This function allows you to manually specify DNS server addresses for the MCM to use for domain name resolution. If the DHCP server does not provide a DNS server, setting manual DNS addresses ensures that your system can still resolve domain names.

3. Configure individual network interface.

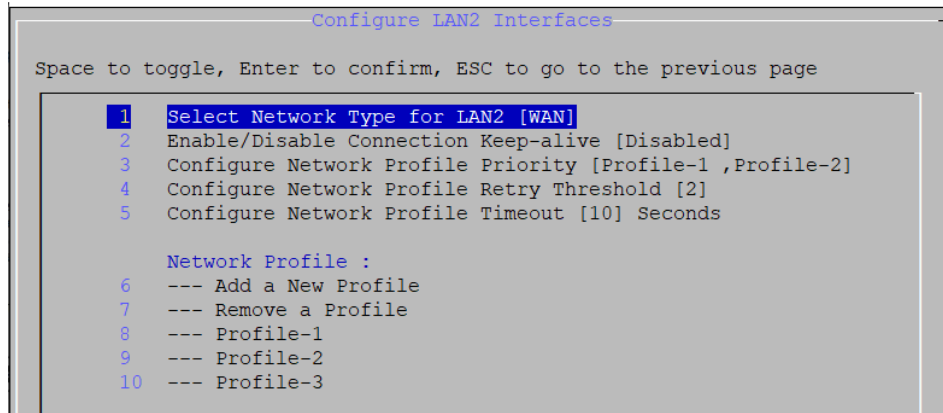


Figure 5.3 –Configurable options for WAN interface

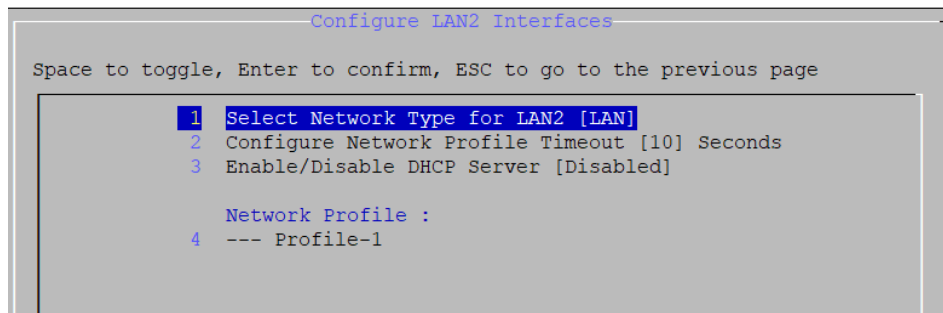


Figure 5.4 –Configurable options for LAN interface

Option Name	Network Type	Description
Select Network Type	All	Available options are WAN/LAN/LAN Bridge/Manual/None
Configure Network Profile Priority	WAN	When the 1st priority WAN network's profile cannot connect or becomes unavailable, MCM will automatically failover to the next profile in this priority list <i>Note: network profile failback is currently not supported</i>
Configure Network Profile Retry Threshold	WAN	This value determines the maximum attempts MCM will try to connect using the current WAN network profile before failover to the next profile in the priority list.
Configure Network Profile Timeout	All	This value (in seconds) determines the maximum time MCM will try to connect using the current network profile before determining the connection is unavailable
Bridge IPv4 Address	LAN-bridge	Assign a static IPv4 address for the bridged LAN interfaces
Bridge IPv4 Subnet Mask	LAN-bridge	Assign a static IPv4 subnet mask for the bridged LAN interfaces
Enable/Disable DHCP Server	LAN, LAN-bridge	Configure a specific LAN or bridged LAN interfaces as DHCP server
Network Profile	WAN, LAN, Manual	<ul style="list-style-type: none"> This section displays all network profile in a list with option to add, modify or remove a profile. If network type is set to LAN or Manual, only profile-1 will be used because network profile failover is only available for WAN

4. Configure network profile of an interface.

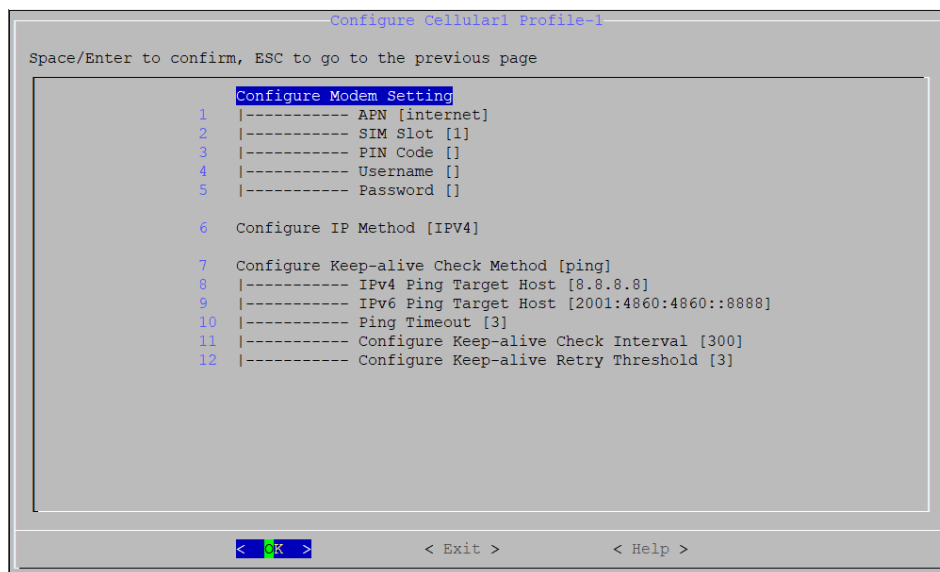


Figure 5.5 –Network profile setting (cellular interface as an example)

Option Name	Interface	Description
Configure Modem Setting	Cellular (WAN)	Configure cellular connection parameters including APN , SIM slot (which SIM slot number to use), PIN Code , Username , Password
	Wi-Fi (WAN)	Configure Wi-Fi connection parameters including Mode (only Wi-Fi client mode is supported), SSID , and Password <i>Note: make sure to leave the password field empty if you are connecting to a public Wi-Fi without password</i>
Configure IP Method	All interfaces	Configure IP related parameters including protocol version (IPv4, IPv6 or IPv4v6) and IP assignment method (DHCP, auto*, static IP or Link-local)
Configure Keep-alive Check Method	All interfaces	Select the method to check connection is alive <ul style="list-style-type: none"> Ping: Connection is only considered alive if pinging the target server specified is successful <ul style="list-style-type: none"> ➢ Optionally, select "ping-signalmonitor" to also include signal strength as a criterion for a healthy connection. Check-ip-exist: As long as an IP is assigned to the interface (e.g., the base station assigns IP to the cellular modem or DHCP server assigns IP to LAN port), are considered connection is alive <ul style="list-style-type: none"> ➢ Optionally, select "check-ip-exist-signalmonitor" to also include signal strength as a criterion for a healthy connection.

* IP assignment method "auto" is for IPv6 only, which support Stateless Address Auto-Configuration (SLACC) and Stateless for DHCPv6.

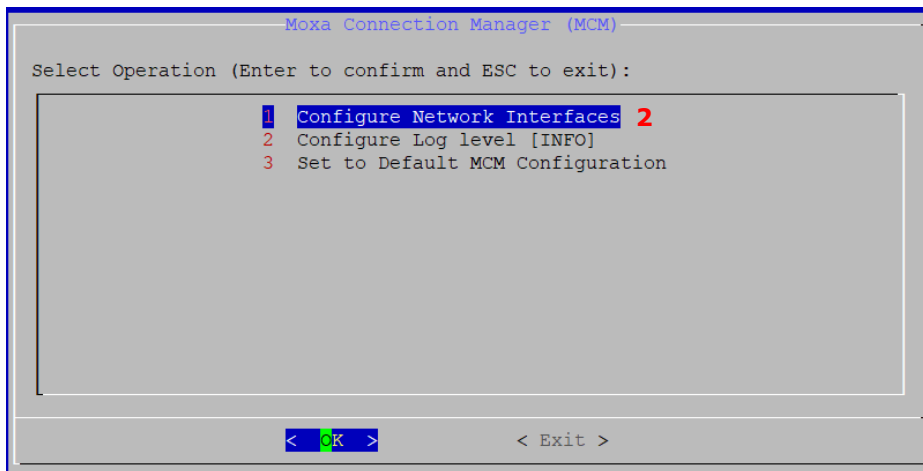
Cellular and Wi-Fi Failover/Failback

One of the key features in MCM is WAN connection auto-failover, where you can configure multiple backup WAN networks. When the primary connection becomes unavailable, MCM will automatically fail over to the backup network depending on the priority you set. You can even configure the connection to fall back to the primary one when it is back online.

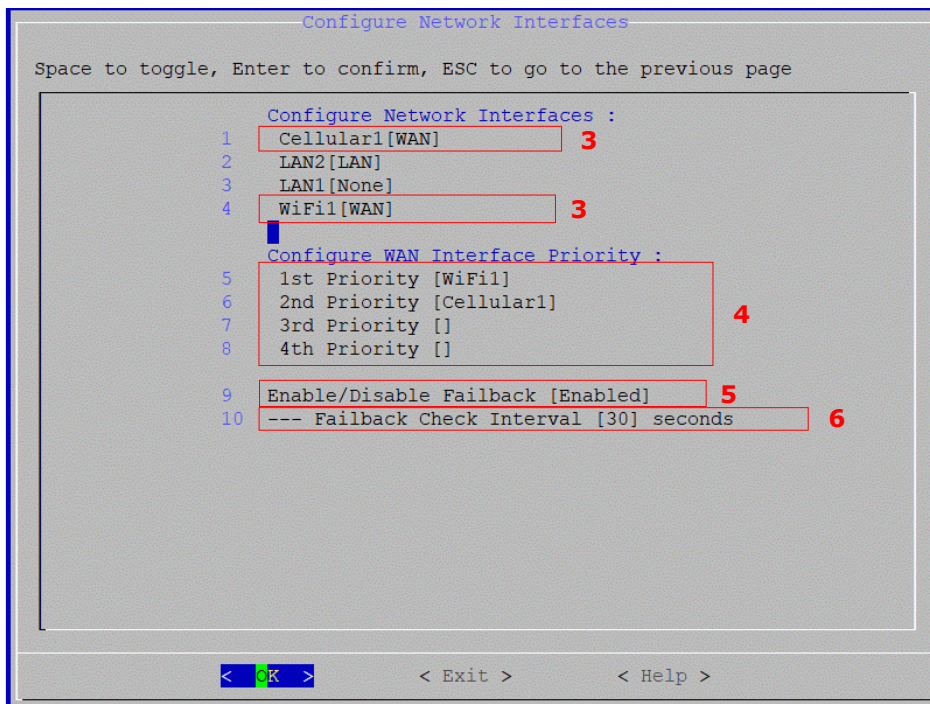
In below example, we will set Wi-Fi interface as the primary WAN network and Cellular(4G/LTE) as the backup. MCM will automatically switch to using Cellular(4G/LTE) when Wi-Fi is down and back to Wi-Fi when it is back online.

1. Run # **mx-connect-mgmt configure** to launch a simple GUI dialog configurator.

```
root@moxa-tbbbbb1182827:/# mx-connect-mgmt configure
```



2. Select "Configure Network Interfaces".
3. Set interface Cellular1 and Wi-Fi both to WAN, and
4. Set Wi-Fi as the 1st priority and Cellular1 as 2nd priority.
5. Make sure Failback is enabled if you would like MCM to automatically switch back to Wi-Fi from cellular when it is back online.
6. Failback Check Interval [30] seconds mean MCM will make sure Wi-Fi connection is alive and stable for 30 seconds before failback to use Wi-Fi as the primary connection (default gateway). The purpose is to avoid unstable connections causing frequent failover and failback.



7. Go to the interface configuration page of WiFi1 and Cellular1 (Figure 5.5 is an example of Cellular).
8. The option "**Enable/Disable Connection Keep-alive**" is disabled by default. It means there will be a short period without network during Wi-Fi to cellular failover process since MCM will only initiate the cellular connection when failover is triggered.

You can enable this setting if a seamless failover experience is desired. When enabled, it allows MCM to failover to a ready-to-use backup connection without the initialization downtime.



NOTE

Enable/Disable Connection Keep-alive setting in this page has been replaced by "Seamless Failover" configuration in the main page since MCM v1.3.x, see [Figure 5.2 –Configure network interface](#)

9. MCM also supports network profile failover. For example, on a Moxa V3000 Series computer with dual SIM slots, you can set up two profiles for cellular interface; each uses a different SIM slot and SIM card.
 - **Network Profile Priority:** in this example, MCM will use profile-1 by default and failover to use profile-2 when it cannot establish a connection with profile-1.
 - **Network Profile Timeout and Retry Threshold:** in this example, MCM will try to connect with profile-1 two times, each with a maximum of 90 seconds timeout before switching to profile-2.
10. You can modify the default profile-1 and profile-2 or add/remove a profile.

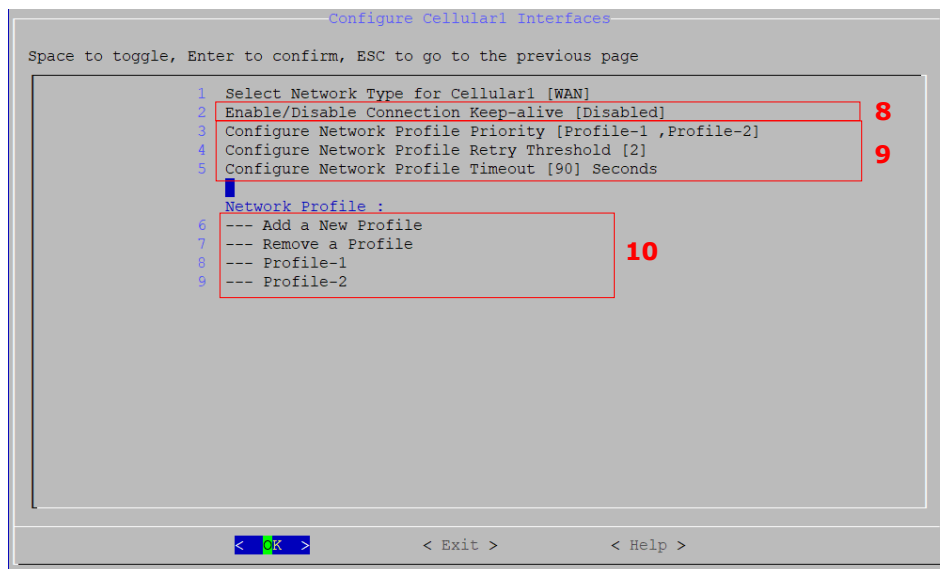


Figure 5.6 –Interface configuration page of Cellular1

11. Go to profile configuration page.
12. Configure the cellular modem related attribute. In this example, a SIM card in SIM slot 1 with PIN code "0000" and APN "internet" is used for Profile-1.
13. Select the IP protocol generation. IPv4, IPv6, and IPv4v6 are the available options.
14. Select how MCM determine the connection is alive. Currently, only "ping" method is supported for WAN network. In this example, following configuration are set for Profile-1 of Cellular1 interface.
 - MCM will ping the Google DNS once every 700 seconds.
 - MCM will try to ping the target host maximum 3 times (Retry Threshold) before concluding profile-1 cannot connect. For each ping attempt, MCM will consider ping fails if server doesn't response in 3 seconds (Ping timeout).

15. Once completed the configuration, exit MCM and select save and reload configuration file for the configuration to take effect.

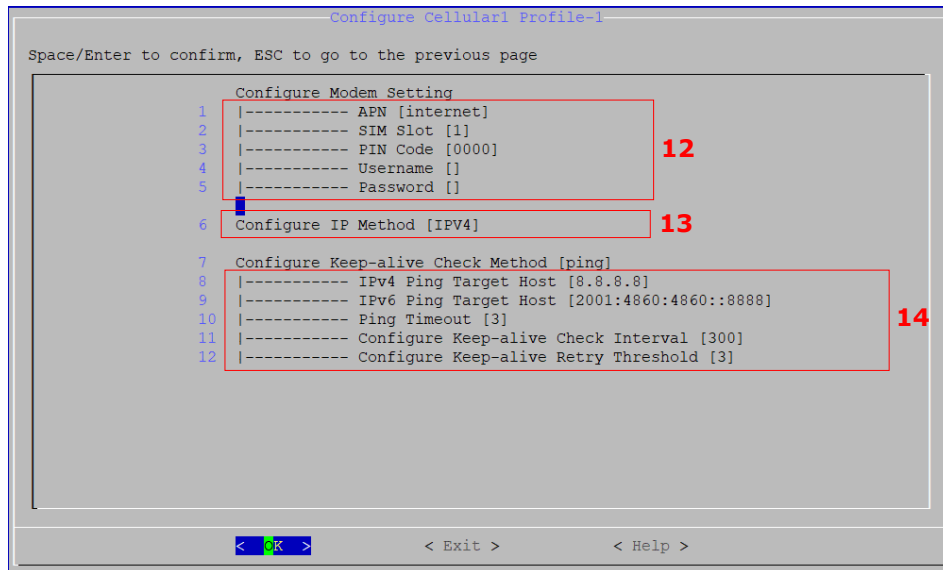
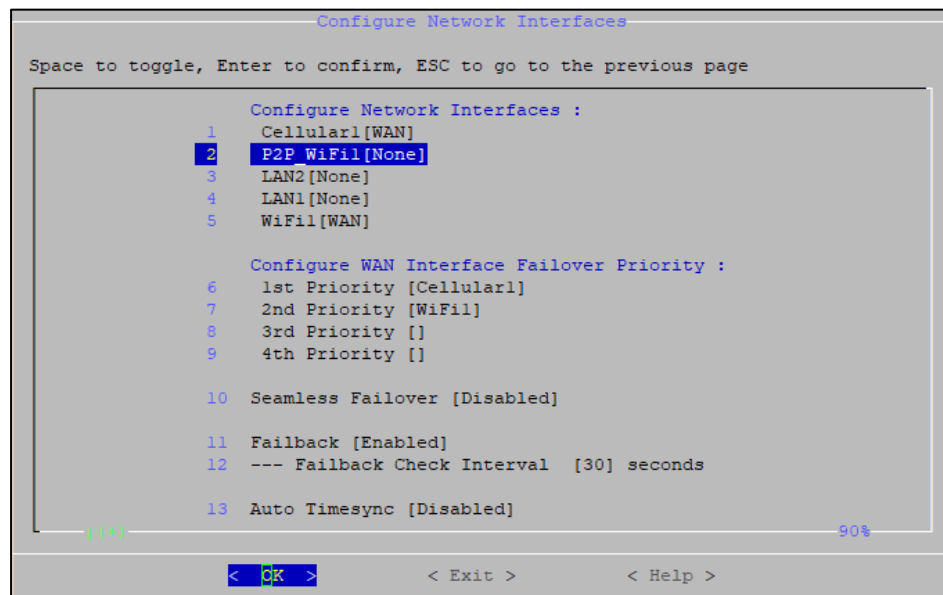


Figure 5.7–network profile configuration page of Cellular1 interface

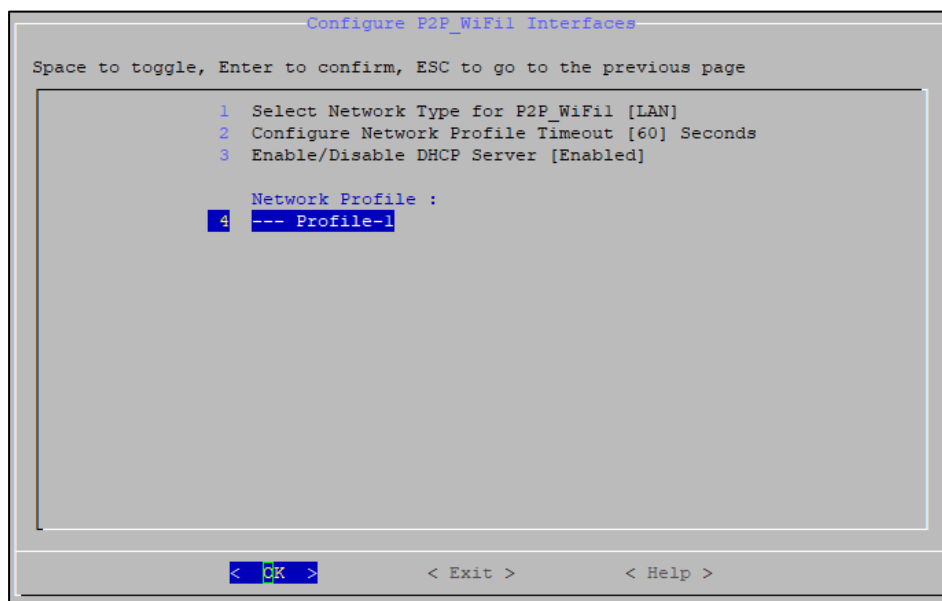
Connecting via P2P Wi-Fi for Remote Access

Starting from MIL 3.2, MCM includes a feature that allows remote access to Moxa computers via P2P Wi-Fi. This is useful for remote debugging when a cellular connection is unavailable, and the device is in a difficult-to-access location without wired connections. P2P Wi-Fi can be enabled alongside Wi-Fi client mode, allowing simultaneous peer-to-peer communication and internet access through a Wi-Fi network, providing flexibility in maintaining connectivity while troubleshooting.

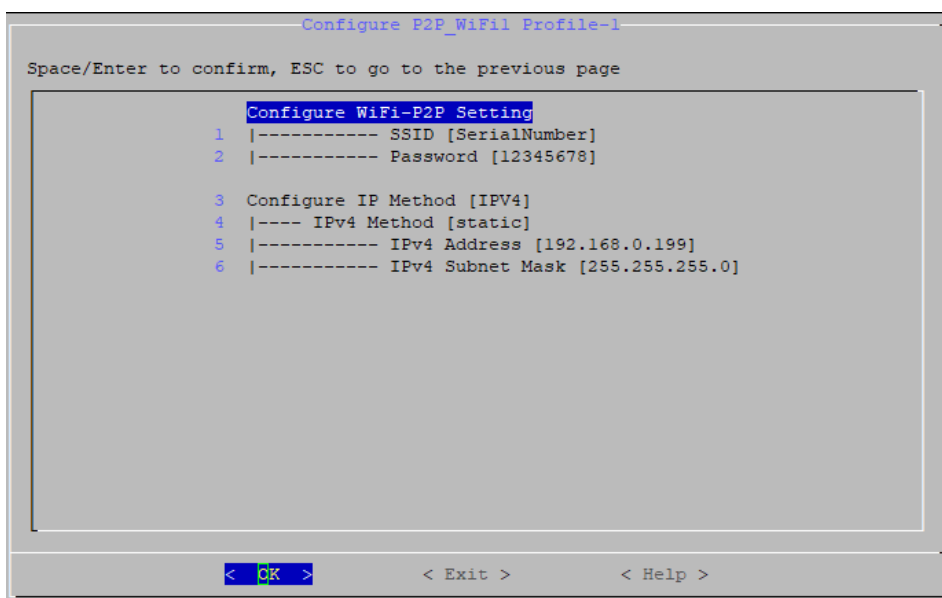
1. If your Moxa computer has a supported Wi-Fi module installed, P2P Wi-Fi will show up as an interface.



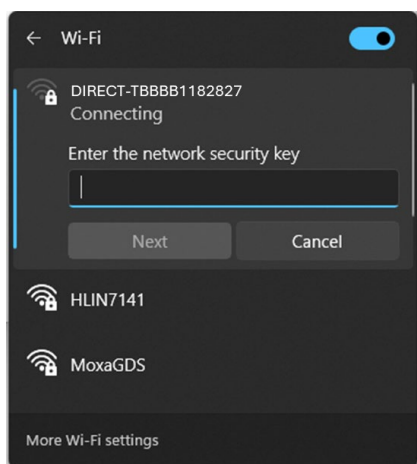
2. Enable P2P Wi-Fi interface and configure the profile.



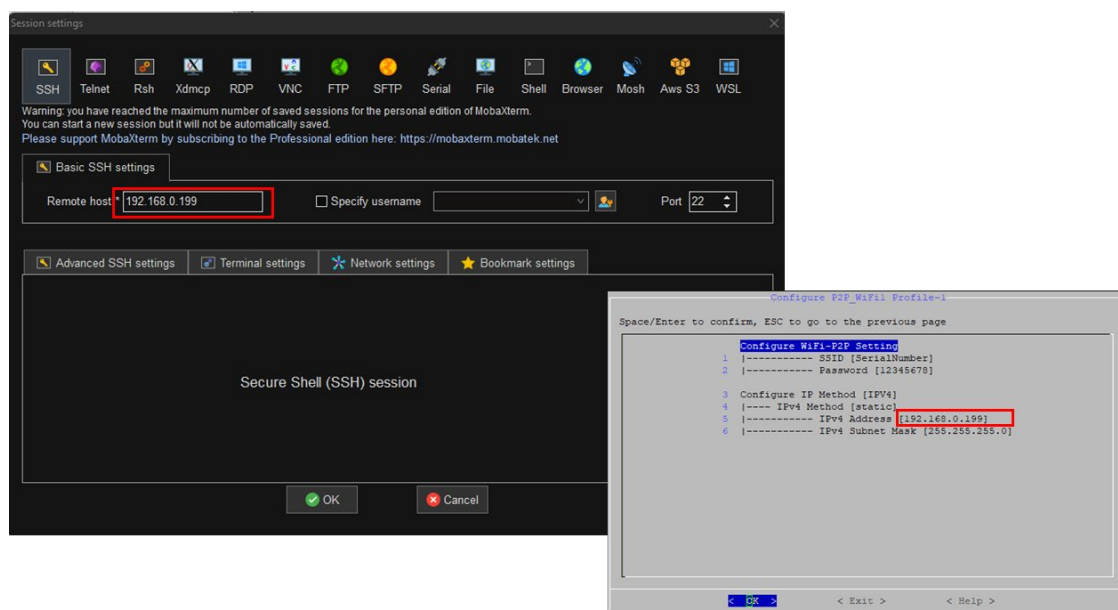
3. Configure the SSID and Password. The default SSID is DIRECT-[Moxa computer's serial number].



4. Configure the SSID and Password. The default SSID is DIRECT-[Moxa computer's serial number].
5. On another device with Wi-Fi, search for the configured Wi-Fi SSID and enter the password.



- You can now remotely access the Moxa computer via SSH using the static IPv4 address set in the P2P Wi-Fi profile.



Checking the Network Status

Checking the Interface and Connection Status

- Use `# mx-connect-mgmt nwk_info [Interface name]` to check the interface and connection status.
- Use `# mx-connect-mgmt nwk_info -a [Interface name]`

```
-----
Interface Name      : Cellular1
Enabled             : true
WAN Priority        : 1
Device Name        : cdc-wdm0
Device Type        : Modem
Network Ifname     : wwan0
Network Type       : WAN
Mac Address        :
IPv4 Method        : dhcp
IPv6 Method        :
-----
Modem State         : Connected
-----
Radio Access Tech   : LTE
Signal Strength     : Poor
Operator Name      : Chunghwa Telecom
Unlock Retries     : SIM PIN(3)
SIM Slot           : 2
IMSI               : 466924253357038
APN                : internet(Auto)
ICCID              : 89886920042533570383
Cell ID/TAC        : 01C10722/2EE0
LTE RSRP           : -94 dBm
LTE RSSNR          : 0 dB
Modem Version       : 25.30.626 1 [Jun 07 2021 06:00:00]
Modem Name         : Telit LE910C4-WWxD 1.00
IMEI               : 353338974279918
-----
Connection Status   : Connected
Default Route       : true
```

```

-----
IPv4 | Address      : 25.8.139.168
    | Netmask    : 255.255.255.240
    | Gateway    : 25.8.139.169
    | Primary DNS : 168.95.1.1
    | Secondary DNS : 168.95.192.1
-----

IPv6 | Address      :
    | Netmask    :
    | Gateway    :
    | Primary DNS :
    | Secondary DNS :

```

Figure 5.8 –an example of `nwk_info` result of interface `Cellular1`

Most of the data fields and values are self-explanatory. Below are additional details to some of the data fields:

Fields	Description	Available Interface
Enabled	<ul style="list-style-type: none"> True: This interface is managed by MCM False: This interface is not managed by MCM 	Wi-Fi, Ethernet, Cellular
WAN priority	The WAN priority set in Figure 5.2	Wi-Fi, Ethernet, Cellular
Network Type	WAN/LAN/Manual/None according to the set value in Figure 5.2	Wi-Fi, Ethernet, Cellular
Modem State	<ul style="list-style-type: none"> Not Ready: The cellular modem can't be detected, or some configuration is not set correctly in MCM configuration files. Initializing: The cellular is initializing SIM PIN Locked: SIM PIN is locked; you can unlock with <code>unlock_pin</code> command SIM PUK Locked: SIM PUK is locked; you can unlock with <code>unlock_puk</code> command Radio Power Off: The cellular modem is entering flight mode Radio Power On: The cellular modem is exiting flight mode Searching Base Station: The cellular modem has exited flight mode and searching for base-station Attached to Base Station: The cellular modem is registered with a network provider but without data connections. Connecting: The cellular modem is connecting Connected: The cellular modem is connected No SIM: SIM card is missing or malfunctioning 	Cellular only
Radio Access Tech	GSM/GSM COMPACT/UMTS/LTE/5G SA/5G NSA, etc.	Cellular only
Signal Strength	<ul style="list-style-type: none"> None/Very Poor Poor Fair Good Excellent <p><i>Note: see cellular signal strength for defined criteria</i></p>	Cellular only
SIM Slot	The SIM slot number being used	Cellular only
Connection Status	<ul style="list-style-type: none"> Initializing: Initializing network connection Device Ready: Detected the network interface is ready Connecting: Connecting according to setting in profile Configuration Error: Profile configuration error Disabling: Stopping the connection Disabled: When an interface is not managed by MCM, or MCM service is stopped Connected: Connection is "working". The criteria for "working" are determine by the Keep-alive Check Method in Figure 5.5. For example, if method is set to ping, the connection is consider working if ping is successful Unable to connect: The network profile is set correctly but the connection is not working determined by the Keep-alive Check Method in Figure 5.5 Reconnecting: Connection is being reconnecting 	Wi-Fi, Ethernet, Cellular
Default Route	<ul style="list-style-type: none"> True: This interface is currently being used as default route False: This interface is not the default route 	Wi-Fi, Ethernet, Cellular

Cellular Signal Strength

Signal Indicator

- 3G Signal Indicators:
 - **RSSI** (Received Signal Strength Indicator): Measures the received signal strength in dBm.
 - **EC/IO** (Energy per Chip over Interference): Indicates the signal quality by measuring the ratio of the received energy per chip to the interference level, in dB.
- 4G Signal Indicators:
 - **RSRP** (Reference Signal Received Power): Represents the power of the reference signal in dBm, used to assess the signal strength in LTE networks.
 - **RSSNR** (Reference Signal Signal-to-Noise Ratio): Measures the quality of the reference signal by evaluating the signal-to-noise ratio in dB.
- 5G Signal Indicators:
 - **RSRP** (Reference Signal Received Power): Measures the power of the 5G reference signal when connected to a 5G cell, similar to SA.
 - **SINR** (Signal-to-Interference-plus-Noise Ratio): Reflects the quality of the 5G signal, considering the presence of 4G signals in the same environment.

Signal Level Criteria

Below are the criteria that MCM uses to determine the signal strength for 3G(UMTS), 4G(LTE), 5G SA and 5G NSA:

Using 4G(LTE) signal level as an example:

- For the signal level "Excellent", both RSRP and RSSNR need to meet the defined criteria in below table
- If the criteria for RSRP and RSSNR differ, the MCM will display the lower of the two signal levels. For example, if the RSRP value meets the "Excellent" criteria but EC/IO RSSNR meets only the "Good" criteria, then the MCM will show "Good" signal level

5G NSA Signal Level	LTE RSRP (dBm)	LTE RSSNR (db)	5G RSRP (dBm)	5G SINR (dBm)
Good	≥ -90	≥ 10	≥ -80	≥ 15
Fair	$-105 \leq x < -90$	$5 \leq x < 10$	$-90 \leq x < -80$	$5 \leq x < 15$
Poor	$-125 \leq x < -105$	$-20 \leq x < 5$	$-110 \leq x < -90$	$-20 \leq x < 5$
No Signal	< -125	< -20	< -110	< -20

5G SA Signal Level	RSRP (dBm)	SINR (db)
Good	≥ -80	≥ 15
Fair	$-90 \leq x < -80$	$5 \leq x < 15$
Poor	$-110 \leq x < -90$	$-20 \leq x < 5$
No Signal	< -110	< -20

4G(LTE) Signal Level	RSRP (dBm)	RSSNR (db)
Excellent	≥ -85	≥ 13
Good	≥ -95	≥ 5
Fair	≥ -105	≥ 1
Poor	≥ -115	≥ -3
None/Very Poor	< -115	< -3

3G(UMTS) Signal Level	RSSI (dBm)	EC/IO (db)
Excellent	≥ -77	≥ -6
Good	≥ -87	≥ -10
Fair	≥ -97	≥ -14
Poor	≥ -107	≥ -20
None/Very Poor	< -107	< -20

Monitoring the Data Usage

Use # **mx-connect-mgmt datausage** to check the data usage of a specified interface between a specified start and end date

```
moxa@moxa-tbbbbb1182827:~# sudo mx-connect-mgmt datausage -h

mx-connect-mgmt-datausage
Show interface data usage information and related functions

USAGE:
  mx-connect-mgmt datausage [FLAGS] [OPTIONS] [interface]
FLAGS:
  -h, --help      Prints help information
  -r, --reset      data usage database
OPTIONS:
  -s, --since <date>    Sets the begin date of data usage cumulative period,
                        expected date format YYYY-MM-DD HH:MM or YYYY-MM-DD
  -t, --to <date>       Sets the end date of data usage cumulative period,
                        expected date format YYYY-MM-DD HH:MM or YYYY-MM-DD
ARGS:
  <interface>
```

Below is an example of how to check the data usage of Wi-Fi interface between 2022/7/3 and 2022/7/4

```
moxa@moxa-tbbbbb1182827:~# sudo mx-connect-mgmt datausage --since 2022-07-03 --to
2022-07-04 Wi-Fi1
moxa@moxa-tbbbbb1182827:~#
rx: 21884544 bytes
tx: 116086 bytes
```

Upgrading the Cellular Modem Firmware

Use # **mx-connect-mgmt modem upgrade [Interface name]** will check and install the latest cellular modem firmware tested by Moxa from Moxa APT server.

- Your cellular network will be down temporary during the upgrade and the connection will be reconnected by MCM after the upgrade is complete
- You can also upgrade the firmware locally by specifying a file path following **-F** or **--filepath** option
- By default, firmware downgrade is not allowed and not recommended. If you insist to downgrade the firmware, you can add **-f** flag to force the downgrade.
- You can use **mx-connect-mgmt nwk_info [interface name] -a** command to check the current cellular modem firmware version
- MCM will perform auto-reinstallation if upgrade fails.

```
moxa@moxa-tbbbbb1182827:~# sudo mx-connect-mgmt modem upgrade -h
mx-connect-mgmt-modem-upgrade
Upgrade modem FWR

USAGE:
  mx-connect-mgmt modem upgrade [FLAGS] [OPTIONS] [interface]
FLAGS:
  -f          force upgrade FWR
  -h, --help  Prints help information
OPTIONS:
  -F, --filepath <filename>    Sets the FWR file path
ARGS:
  <interface>
```

An example of automatically updating the cellular modem firmware from Moxa APT server is given below:

```
moxa@moxa-tbbbbb1182827:~# sudo mx-connect-mgmt modem upgrade Cellular1
```

An example of manually updating the cellular modem firmware by specifying a firmware file is given below:

```
moxa@moxa-tbbbbb1182827:/# sudo mx-connect-mgmt modem upgrade Cellular1 -F /etc/firmware/Telit-LE910C4-EU-Info-1.1.0
```

An example given below indicates how to manually force the cellular modem firmware update even if the current firmware is newer than the provided firmware:

```
moxa@moxa-tbbbbb1182827:/# sudo mx-connect-mgmt modem upgrade Cellular1 -f -F /etc/firmware/Telit-LE910C4-EU-Info-1.0.0
```

Cellular Network Diagnosis

Use # **mx-connect-mgmt debug** to perform diagnosis on the cellular network if you have trouble getting it to connect. The diagnosis tool can identify common issues such as missing antenna, weak signal strength, SIM card pin code error, SIM locked, etc.

```
moxa@moxa-tbbbbb1182827:/# sudo mx-connect-mgmt debug -h
mx-connect-mgmt-debug
Debug and diagnose cellular connection

USAGE:
    mx-connect-mgmt debug [SUBCOMMAND]

FLAGS:
    -h, --help    Prints help information

SUBCOMMANDS:
    diag          Perform diagnosis on the cellular interface
    help          Prints this message or the help of the given subcommand(s)
    listen        Listen to properties changed
```



NOTE

Cellular network diagnosis is not available for 5G yet.

Using API to Retrieve the MCM Status

MCM provides C application programming interfaces (APIs) for developers to retrieve various network and interface statuses. For details, refer to the C API document:

<https://moxa.gitlab.io/open-source/linux/gitbook/moxa-connection-manager-reference-manual/MCM/Libmcm>

To integrating your applications securely with the MC C API, you should follow the below guideline:

1. Confirm that the return value of the API is 0 and the returned struct pointer is not NULL to avoid using the wrong memory address.
2. Always free the structure pointer returned by the API to avoid memory leak.

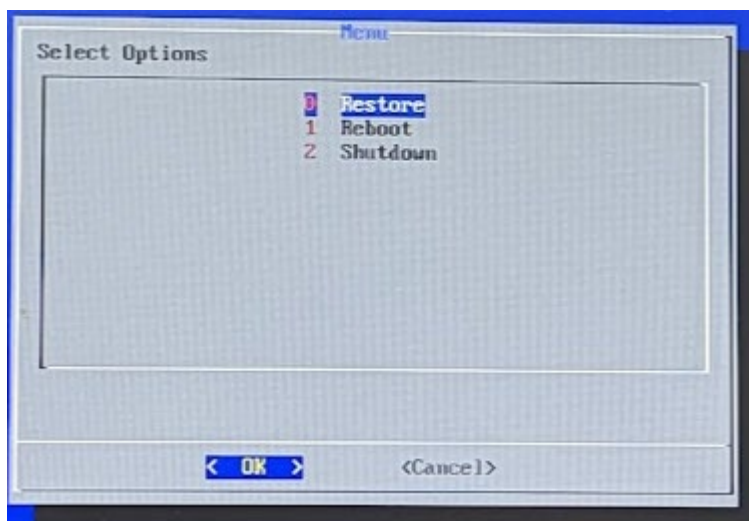
6. System Installation and Update

In this chapter, we will introduce how to install and update Moxa Industrial Linux and the bootloader.

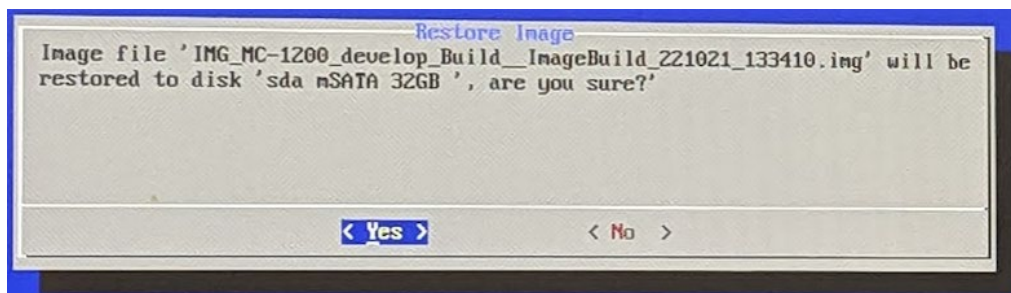
System Installation From a USB

To install MIL3 on the V3000 using a USB, do the following:

- Step 1:** Prepare a USB storage and create a fat32 partition.
- Step 2:** Create two folders on the USB storage - \EFI\boot and \images
- Step 3:** Contact Moxa GTS or FAE to obtain a signed Live USB EFI file (bootx64.EFI) and copy it to the \EFI\boot folder.
- Step 4:** Contact Moxa GTS or FAE to obtain a signed image file and copy it to the \images folder.
- Step 5:** Insert the USB storage to the target V3000 and reboot it via the USB storage.
- Step 6:** In the Menu that pops up, select "Restore".



- Step 7:** Select the image and destination disk and confirm the information before selecting Yes to start the installation of MIL3.



Offline or Online Upgrade Using MSU

Moxa Software Updater (MSU) is a Moxa utility for performing both offline and online software upgrades to update the MIL version on Moxa computers. For offline upgrades, two types of upgrade packages are available: the **Upgrade Pack** and the **Refresh Upgrade Pack**.

- The **Upgrade Pack upgrades** the system while preserving user data and configurations. It contains only the differences between the current and target versions, making it significantly smaller in size.
- The **Refresh Upgrade Pack** performs a full system upgrade by wiping all user data and restoring the system to its factory default environment. This pack contains all the files from the target version and is, therefore, larger in size.

MSU is available starting from MIL 3.2. For all MIL versions after MIL 3.2 (e.g., MIL 3.3), Moxa will release software update packs on the [Moxa Software Release Service \(SRS\)](#) for you to download.

To use Moxa Software Updater (MSU), run the command # **mx-sw-updater** [command]

Command and Usage	Description
configure [flags]	<p>The mx-sw-updater configure command sets up an offline upgrade pack (root required). It prepares the upgrade or refresh pack and verifies it with a signature file. This step ensures that the package and metadata are copied and configured to the device's local cache before upgrading.</p> <p>Key Flags</p> <ul style="list-style-type: none">• -p, --path: Specifies the path to the upgrade pack or refresh upgrade pack.• -s, --signature: Provides the path to the signature file for verification. If not specified, it will attempt to find a matching signature file in the same directory.
update	<p>The mx-sw-updater update command fetches the latest metadata from the MOXA Apt Repository to the device's local cache. This command ensures that the system's package information is up-to-date and ready for installing or upgrading packages.</p>
upgrade [flags]	<p>The mx-sw-updater upgrade command updates the system to a target official version while preserving user data and configurations, with options to perform the upgrade using a local package or remote APT server with automatic recovery. This command requires root privileges.</p> <p>Key Flags</p> <ul style="list-style-type: none">• -l, --latest: Upgrade to the newest version in the local cache• --remote: Upgrade remotely via the APT server (default option).• --local: Upgrade using the local upgrade pack• --system-failback: Performs the upgrade with system failback enabled to ensure auto system recovery if the upgrade fails.• -r, --release <string>: Upgrades to a specified target version (e.g., -r V1.1).
Refresh-upgrade [flags]	<p>The mx-sw-updater refresh-upgrade command upgrades the system by wiping all user data and restoring it to the factory default environment. Unlike the mx-sw-updater upgrade command, which preserves user data, the refresh-upgrade command resets the system to its original state. This command supports only local upgrades and requires root privileges.</p> <p>Key Flags</p> <ul style="list-style-type: none">• -l, --latest: Upgrade to the newest version in the local cache.• --system-failback: Performs the upgrade with failback enabled, ensuring automatic system recovery if the upgrade fails.• -r, --release <string>: Upgrade to a specified target version (e.g., -r V1.1).

Command and Usage	Description
show [flags]	<p>The mx-sw-updater show command displays details about the upgrades that have been added to the device's local cache via the mx-sw-updater configure and mx-sw-updater update commands. The details include the version number, supported Moxa computer models, and the changelog.</p> <p>Key Flags</p> <ul style="list-style-type: none"> • -a, --all: Shows information of all available upgrades. • -l, --latest: Displays information of the newest upgradable version. • -r, --release <string>: Shows details of a specified upgradable version (e.g., -r V1.1). • --from <string>: Specifies the starting version for a range. • --to <string>: Specifies the ending version for a range. <p><i>Note: The --from and --to flags can be used together to display information for a range of versions</i></p>
status [flags]	<p>The mx-sw-updater status command provides information about the current status of upgrade packages that have been added to the device's local cache via the mx-sw-updater configure and mx-sw-updater update commands, allowing users to check the availability and progress of various software updates.</p> <p>Key Flags</p> <ul style="list-style-type: none"> • -a, --all: Shows the status of all available upgrades. • -l, --latest: Displays the status of the newest upgradable version. • -r, --release <string>: Shows the status of a specified upgradable version (e.g., -r V1.1). • --from <string>: Specifies the starting version for a range. • --to <string>: Specifies the ending version for a range. <p><i>Note: The --from and --to flags can be used together to display the status for a range of versions</i></p>
list [flags]	<p>The mx-sw-updater list command is used to display information about software packages, including installed packages, upgradable packages in the local cache, and differences between versions.</p> <p>Key Flags</p> <ul style="list-style-type: none"> • -l, --latest: Lists all packages from the newest upgradable version in the local cache • -s, --system: Lists all packages currently installed on the system. • -r, --release <string>: Lists all packages from a specified upgradable version (e.g., -r V1.1). • -c, --compare <stringArray>: Show the changed packages between two specified versions (e.g., -c V1.0 -c V1.1). If the second version is not specified, it compares the specified version with the installed system packages. • --detailed: Shows both changed and unchanged packages. This flag is to be used with -c, --compare. • --no-fixed: Display output without fixed-length formatting.
Verify [flags]	<p>The mx-sw-updater verify command is used to verify the integrity and authenticity of an upgrade pack or refresh-upgrade pack by checking its digital signature. This ensures that the upgrade package has not been tampered with and is valid before performing any system upgrades.</p> <p>Key Flags</p> <ul style="list-style-type: none"> • -p, --path <string>: Specifies the path to the upgrade pack or the refresh upgrade pack. • -s, --signature <string>: Specifies the path to the signature file for verification. If not specified, the command will try to find the .sha512.bin.signed file in the same directory as the upgrade pack.

Online Update via Secure APT

Moxa V3000 Series computers support Secure APT, which uses a GPG public key system to ensure the integrity and authenticity of patches are validated before download, and x.509 certification authentication for secure transmission via HTTPS. The private key pair of the GPG key for the Moxa APT repository is stored in an on-premises Sign Server, accessible only by authorized Moxa personnel.



NOTE

Click the following link for more information on how SecureAPT works: <https://wiki.debian.org/SecureApt>

Querying the System Image Version

Use the `mx-ver` command to check the system image version on your Moxa V3000 Series computers.

```
moxa@moxa-tbzkb1090923:# mx-ver
UC-8220-T-LX-US-S MIL3 version 1.0 Build 22052300
```

Failback Update

We strongly recommend enabling the failback function before performing an update. Refer to failback feature in the Moxa System Manager (MSM) for details.

Managing the APT Repository

The APT Repository is the network server from which APT downloads packages that are installed on your Moxa V3000 Series computer. By default, Moxa V3000 Series computers include the following repositories that contain stable and well-tested packages best suited for ensuring the stability of your project.

Source list	Repository URL	Description
/etc/apt/sources.list	https://deb.debian.org/debian/bullseye	Debian official repository containing the latest stable Debian 11 release (released about every 2 months).
	https://deb.debian.org/debian/bullseye-updates	Debian official repository containing bug fixes that will be included in the upcoming Debian 11 release.
	https://deb.debian.org/debian-security/bullseye-security	Debian official repository containing security hotfixes that will be included in the upcoming Debian 11 release.
/etc/apt/sources.list.d/moxa.list	https://debian.moxa.com/mil3/bullseye	Moxa repository containing Moxa's proprietary library, tools, utilities, and kernel. Moxa will maintain security and bug fixes even after Debian 11 has reached its end of life (EOL).

To add a new repository, you must add the repository URL and official GPG key to the source list and keyring in your Moxa V3000 Series computer.

Here is an example for adding the Docker repository <https://docs.docker.com/engine/install/debian/>.

1. Add the repository URL to the source list on your V Series computer.

```
moxa@moxa-tbzkb1090923:# echo "deb https://download.docker.com/linux/debian
bullseye stable" > /etc/apt/sources.list.d/docker.list
```

2. Add the official GPG public key of the Docker repository to the keyring in your computer for SecureAPT.

```
moxa@moxa-tbzkb1090923:# curl -fsSL
https://download.docker.com/linux/debian/gpg | gpg --dearmor -o
/etc/apt/trusted.gpg.d/docker.gpg
```

3. Verify the newly added Docker repository by running an update.

```
moxa@moxa-tbzkb1090923:~# apt update
Get:1 https://download.docker.com/linux/debian bullseye InRelease [43.3 kB]
Hit:2 http://deb.debian.org/debian bullseye InRelease Get:3
http://deb.debian.org/debian-security bullseye-security InRelease [48.4 kB]
Get:4 https://download.docker.com/linux/debian bullseye/stable amd64
Packages [13.8 kB] Get:5 http://deb.debian.org/debian bullseye-updates
InRelease [44.1 kB] Get:6 http://deb.debian.org/debian-security bullseye-
security/main amd64 Packages [191 kB] Fetched 341 kB in 1s (356 kB/s)
Reading package lists... Done Building dependency tree... Done Reading state
information... Done 30 packages can be upgraded. Run 'apt list --upgradable'
to see them.
```

Updating Your System

Preparing a Staging Environment

Since Moxa V3000 Series computers are open platforms, you are free to install any software that you would like to use. However, we highly recommend that you test all new software on a staging platform before installing them on your production gateways.

Synchronizing the Repository Information

The first and most important step is to synchronize the package index files in your V Series computer with the source repositories specified in the file `/etc/apt/sources.list`. When you perform the synchronization, information related to the packages, including versions and dependencies, will also be downloaded from the repositories.

To perform the synchronization, make sure that your network environment can connect to the APT repositories, and then run the `apt update` command with root permission to synchronize the package index.

```
moxa@moxa-tbbbb1182827:~# sudo apt update
```

Updating the Entire System

Use the `apt full-upgrade` command to upgrade all packages used by your Moxa V3000 Series computer to latest versions.

```
moxa@moxa-tbbbb1182827:~# sudo apt full-upgrade
```

Customization and Programming

Building an Application

Introduction

Moxa's V Series computers support native compiling of code. Native compilation is more straightforward since all the coding and compiling can be done directly on the device.

Native Compilation

Follow these steps to update the package menu and compile the code on your device:

1. Make sure a network connection is available.
2. Use **aptupdate** to update the Debian package list.

```
moxa@moxa-tbzkb1090923:~$ sudo apt update
```

3. Install the native compiler and necessary packages.

```
moxa@moxa-tbzkb1090923:~$ sudo apt install gcc build-essential flex bison automake
```

4. Compile the hello.c code.

```
moxa@moxa-tbzkb1090923:~$ gcc -o hello hello.c
moxa@moxa-tbzkb1090923:~$ strip -s hello
```

or

use the Makefile as follows:

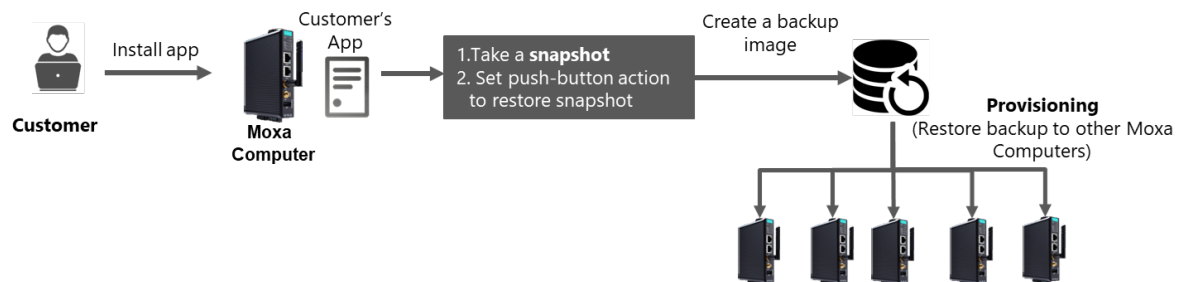
```
moxa@moxa-tbzkb1090923:~$ make
```

5. Run the program.

```
moxa@moxa-tbzkb1090923:~$ ./hello
Hello World
```

Creating a Customized Image

You can create a customized image (snapshot) and set the push-button on Moxa Computer as the trigger to reset to the customized environment from Moxa factory default settings. This customized image can also be used for provisioning other Moxa Computers.



Using System Snapshots and Backups

1. Configure your Moxa V3000 Series computer and install applications.
2. Create a **Snapshot**.
3. **Customize the Button Action** section to configure the action of push-button on Moxa V3000 Series computer to restore from a snapshot.
 - Copy content of default script to custom.script, change to reset-to-default.
 - Change the set-to-factory-default function (mx-system-mgmt default restore -y) of button to restore snapshot (**mx-system-mgmt snapshot restore -y**).

```
#!/bin/sh
ACTION="${1}"
SECONDS="${2}"
if [ "${ACTION}" = "press" ]; then
    /usr/bin/mx-interface-mgmt led SYS set_state heartbeat
elif [ "${ACTION}" = "hold" ]; then
    if [ ${SECONDS} -eq 7 ]; then
        /usr/bin/mx-interface-mgmt led SYS set_state on
    elif [ ${SECONDS} -eq 9 ]; then
        /usr/bin/mx-interface-mgmt led SYS set_state off
    fi
elif [ "${ACTION}" = "release" ]; then
    if [ ${SECONDS} -lt 1 ]; then
        /usr/sbin/reboot
    elif [ ${SECONDS} -ge 7 ] && [ ${SECONDS} -lt 9 ]; then
        /usr/sbin/mx-system-mgmt snapshot restore -y
        /usr/sbin/reboot
    fi
    /usr/bin/mx-interface-mgmt led SYS set_state on
fi
```

4. Create a [Backup Image](#).
The backup will include the snapshot taken in step #2
5. (optional) Use the backup image to provision other Moxa computers of the same model using the [backup restore](#) command.

7. Backup, Decommission, and Recovery

In this chapter, we will introduce how to use Moxa System Management (MSM) utility to perform snapshot, backup, decommission, and recovery of your system. MSM provides an automatic failback mechanism to ensure that the device can recover to the last known working and secure state when the device fails after a critical event such as a system update.

Function	Description
Snapshot	<ul style="list-style-type: none">The snapshot has a smaller footprint as it saves just the differences (partition 3 in Figure 7.1) compared to the out-of-factory rootfs (partition 2 in Figure 7.1).The snapshot is saved in the Moxa V3000 Series computer and cannot be exported. Hence, a snapshot can only be used to restore the computer that the snapshot was taken from.
Backup	<ul style="list-style-type: none">The backup has a larger footprint as it saves the entire system including the out-of-factory rootfs.The backup can be exported to an external storage.The backup can be used to restore the Moxa V3000 Series computer that the backup is taken from or another computer of the same model.
Automatic Failback Recovery	<ul style="list-style-type: none">When failback recovery is enabled, a replica of the system including the snapshot and bootloader is created.If a boot failure event occurs after failback recovery is enabled, the system will automatically use the replica to recover the systemFailback recovery should be enabled before performing any critical actions that may potentially result in a device failure (e.g., power loss during a bootloader update could brick a computer).

Below diagram illustrate an overview of MIL3 system layout:

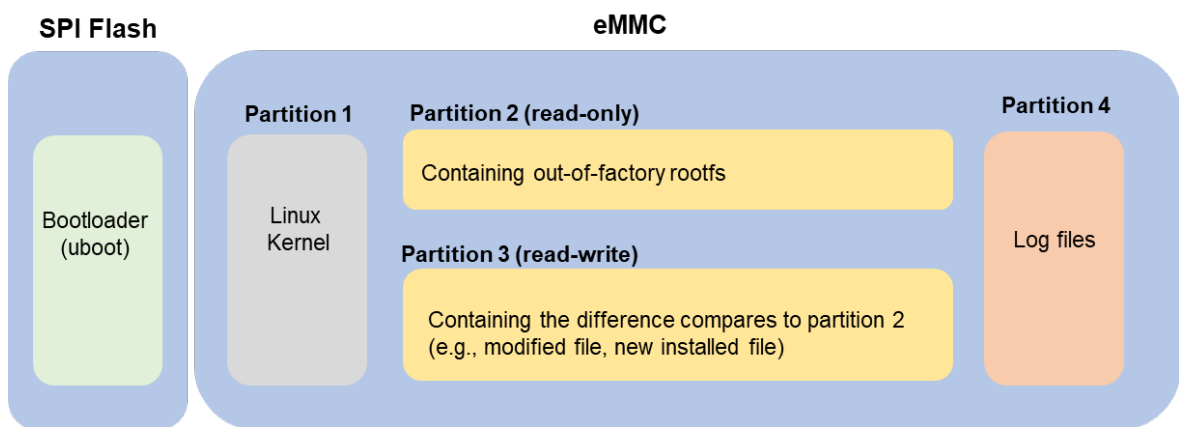


Figure 7.1 - Layout Overview of V Series Computer with MIL3

Creating a System Snapshot

A snapshot preserves the state and data of the Moxa V3000 Series computer as a restoration point at a specific point in time so that you can restore it to that point if something goes wrong. Snapshots only save the Linux kernel and new and modified files to the out-of-factory rootfs (partition 2). Therefore, the size of a snapshot is much smaller than a backup.

Use the # `mx-system-mgmt snapshot <sub-command> <options> <flag>` to create restore a system. You must use `sudo` or run the command with root permission.

Sub-commands	Description
create	Creates a snapshot of system <ul style="list-style-type: none">A snapshot includes kernel (partition 1) and rootfs (partition 3)Only one snapshot is saved. A new snapshot will overwrite the previous snapshotSnapshot is stored in rootfs (partition 3)
restore	Restores the system with the snapshot. System fallback will be disabled after a system is restored from the snapshot.
delete	Deletes the existing snapshot
Info	Displays the create time and size of the existing snapshot

Options	Description
--cold	Creates a snapshot after restarting the system in a minimal environment, such as initrd. This ensures data consistency but requires system downtime during the snapshot creation process.
--hot	<ul style="list-style-type: none">This is the default mode if neither the <code>--cold</code> nor <code>--hot</code> options are specified.Using <code>--hot</code> creates a snapshot of the system while it remains fully operational, without requiring system downtime. <p>Caution: While the hot snapshot method minimizes disruption, there is a potential risk of data inconsistencies due to changes that may occur during the snapshot process.</p>
--size	Estimates the additional disk space required to create the snapshot.

Flag	Description
-y or --yes	Automatically consent to the prompts during create, restore, and delete processes



WARNING

Before initiating the backup or snapshot process with `--hot` option, it is crucial to ensure that all active services involving customer-developed software, are temporarily disabled. Services that are running during the backup may lock certain files, preventing them from being copied and resulting in an incomplete backup. This can compromise the integrity of your backup and the ability to fully restore your system later.

Creating a System Backup

Compares to snapshot, a backup saves Linux kernel and the rootfs on your Moxa V3000 Series Computer. Therefore, a backup can be exported and use to restore a Moxa V3000 Series computer of the same model with MIL 3.0. For example, if you create a backup on UC-8200 Secure model with MIL3, you can use the backup to restore another UC-8200 Secure model with MIL3

Use # **mx-system-mgmt backup <sub-command> ,options> <flag>** command to create, delete, and restore a backup. You must use **sudo** or run the command with the root permission.

Sub-commands	Description
create	<p>Creates a backup of the system</p> <ul style="list-style-type: none">The backup includes kernel (partition 1), rootfs (partition 2), and rootfs (partition 3)By default, the backup is created in the /boot_device/p3/backup/ directory with the name backup.tar, together with an info file that contains the backup information and cryptographic hash of the backup.The backup includes system snapshot. If you would like to reduce the size of backup, you can delete the snapshot in the system before performing the backup if the snapshot is not needed.
delete	Deletes the backup from the default directory
restore	<p>Restores the system using the backup from default directory.</p> <ul style="list-style-type: none">System fallback will be disabled after restoration.Existing snapshot on system will be deleted after restoring the system from a backup.The cryptographic hash in the info file will be used to validate the integrity of the backup file before the restore process begins.A system reboot is required after restoration.
info	Displays the create time and size of the backup in the default directory

Options	Description
--cold	<p>Creates a backup after restarting the system in a minimal environment, such as initrd. This ensures data consistency but requires system downtime during the backup creation process.</p> <p><i>Note: This feature is available in MIL v3.2 and later versions.</i></p>
--hot	<ul style="list-style-type: none">This is the default mode if neither the --cold nor --hot options are specified.Using --hot creates a snapshot of the system while it remains fully operational, without requiring system downtime. <p>Caution: While the hot backup method minimizes disruption, there is a potential risk of data inconsistencies due to changes that may occur during the backup process. Ensure that all active services involving customer-developed software, are temporarily disabled.</p>
--compress	<p>Create a backup with compression. Please note that this might result in a significantly longer backup time</p> <p><i>Note: This feature is available in MIL v3.3 and later versions.</i></p>
-D or --directory	Specifies the directory (e.g., /media/USB_p1) where the backup will be created
--size	Estimates the additional disk space required to create the backup.

Flag	Description
-y or --yes	Automatically consent to the prompt during create, delete and restore



ATTENTION

When restoring a backup from one Moxa computer to multiple other Moxa computers, the SSH host key will be identical across all devices. If you need each computer to have a unique SSH host key, ensure you regenerate the host key after restoring the backup.

The following example demonstrates how to perform a system backup using the hot method to a USB storage drive mounted at **/media/USB_p1**:

```
moxa@moxa-tbzkbl090923:# sudo mx-system-mgmt backup create --hot -D
/media/USB_p1
Set /media/USB_p1 as backup directory.
Check the backup information...
There is no backup information
Start evaluating space, please wait...
Estimation of Required Space: 628MB
Available Space: 32756MB
Would you like to continue? (y/N)y
Synchronize boot files...
      0   0%   0.00kB/s      0:00:00 (xfr#0, to-chk=0/2)
Start creating backup file...
 628MiB 0:00:57 [11.0MiB/s] [ <=> ]
Type: backup
Create Time: 2021.11.06-17:32:29
Size: 628MB
The backup has been created successfully under: /media/USB_p1
```

The following example shows how to restore a backup from the USB storage drive with the mounting point **/media/USB_p1**:

```
moxa@moxa-tbzkbl090923:# sudo mx-system-mgmt backup restore -D /media/USB_p1
Set /media/USB_p1 as backup directory.
Check the backup information...
Type: backup
Create Time: 2021.11.06-17:44:43
Size: 628MB
Start verifying backup file, please wait...
Verified OK!
Start evaluating space, please wait...
Estimation of Required Space: 628MB
Available Space: 5125MB
Would you like to continue? (y/N)y
Check the snapshot information...
Type: snapshot
Create Time: 2021.11.06-15:42:47
Size: 235MB
This will delete the existing snapshot.
Do you want to continue? (y/N)y
Check the snapshot information...
Type: snapshot
Create Time: 2021.11.06-15:42:47
Size: 235MB
The snapshot has been deleted successfully.
To restore the backup file will overwrite current system and factory default
system.
Do you want to continue? (y/N)y
Start using the backup file to restore the system...
 628MiB 0:01:00 [10.4MiB/s] [=====>]
100%
Synchronize boot files...
      0   0%   0.00kB/s      0:00:00 (xfr#0, to-chk=0/2)
System has been restored successfully. Reboot is required to take effect.
moxa@moxa-tbzkbl090923:# sudo reboot
```



WARNING

Before initiating the backup or snapshot process with **--hot** option, it is crucial to ensure that all active services involving customer-developed software, are temporarily disabled. Services that are running during the backup may lock certain files, preventing them from being copied and resulting in an incomplete backup. This can compromise the integrity of your backup and the ability to fully restore your system later.

Setting the System to the Default

Press and hold the **FN** button for 7 to 9 seconds to reset the computer to the factory default settings. When the reset button is held down, the LED will blink once every second. The LED will become steady when you hold the button continuously for 7 to 9 seconds. Release the button immediately when the LED become steady to load the factory default settings. For additional details on the LEDs, refer to the quick installation guide or the user's manual for your V Series computer



ATTENTION

Reset-to-default will erase all data stored on the boot-up storage

Back up your files before resetting the system to factory defaults. All the data stored in the V Series computer's boot-up storage will be destroyed after resetting to factory defaults.

You can also use the `mx-system-mgmt default restore` command to restore the computer to factory default settings. You must use sudo or run the command with the root permission.

```
moxa@moxa-tbzk1090923:/# sudo mx-system-mgmt default restore
```

If you would like to configure the **FN** button for a different action (e.g., restore to a snapshot), refer to [Customize the Button Action](#) section.

Decommissioning the System

Compared with the set-to-default function, decommissioning will further erase all data stored in the log partition to help erase security-sensitive information.



ATTENTION

Decommission will erase all the data including event and audit logs

Please back up your files before resetting the system to factory defaults. All user data including logs in your V Series computer will be destroyed after performing decommissioning. Bootloader configuration, including administrator password, will also be set to factory default.

You can also use the `mx-system-mgmt default decommission` command to restore the computer to factory default. You must use sudo or run the command with the root permission.

```
moxa@moxa-tbzk1090923:/# sudo mx-system-mgmt default decommission
```

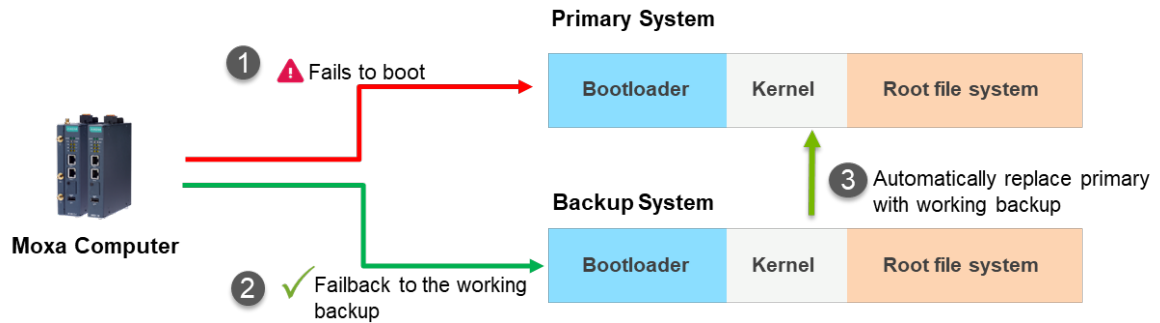
The decommissioning process will do the following:

1. Overwrite the system partition 4 times with shred so that all user files will be deleted and cannot be recovered.
2. Overwrite the log partition 4 times with shred so that all log files will be deleted and cannot be recovered.
3. Trigger the bootloader decommissioning function, so all configurations and log messages in the bootloader are also deleted and cannot be recovered.

System Failback Recovery

A system bootup failure may occur when critical files are lost or corrupted. A typical and common cause of boot up failure is power lost during system update. Moxa System Management (MSM) provides system failback capability which can automatically recovers your system to the last known working state if boot up failure is detected after critical change(s) are made to the primary system. The boot failure criteria are customizable by user.

Before applying critical update or changes to the device, it is recommended to enable system failback first.



Use # `mx-system-mgmt system-failback <sub-command> <flag>` to enable or disable system failback. You must use sudo or run the command with the root permission.

Sub-commands	Description
enable	Enables system failback and create a replica of the system <ul style="list-style-type: none"> The replica includes Bootloader, kernel (partition 1) and rootfs (partition 3) The replica is stored in rootfs (partition 3) When the Moxa V3000 Series computer fails to boot up, the device will automatically reboot and replace the broken system with the working replica. The replica includes a system snapshot. If you would like to reduce the size of the replica, you can delete the snapshot if you no longer need it.
disable	Disables the system failback and delete the existing system replica
info	Displays the create time and size of replica
state	Displays the status of system failback (enabled/disabled)

Options	Description
--cold	Creates a replica after restarting the system in a minimal environment, such as initrd. This ensures data consistency but requires system downtime during the replica creation process.
--hot	<ul style="list-style-type: none"> This is the default mode if neither the --cold nor --hot options are specified. Using --hot creates a replica of the system while it remains fully operational, without requiring system downtime. <p>Caution: While the hot replica method minimizes disruption, there is a potential risk of data inconsistencies due to changes that may occur during the replica creation process.</p>
--size	Estimates the additional disk space required to create the replica.
-V or --value	Displays only the binary value of the system failback state: <ul style="list-style-type: none"> Enabled : 1 Disabled: 0 <p>Example: mx-system-mgmt system-failback state -V</p>

Flag	Description
-y or --yes	Automatically consent to the prompts during the enable and disable processes



WARNING

Before initiating the replica creation process with **--hot** option, it is crucial to ensure that all active services involving customer-developed software, are temporarily disabled. Services that are running during the creation process may lock certain files, preventing them from being copied and resulting in an incomplete replica. This can compromise the integrity of your replica and the ability to fully recover your system later.

Below is an example of how to enable system failback using the cold method and display the information of the system replica:

```
moxa@moxa-tbzkbl090923:/# sudo mx-system-mgmt system-failback enable
Start evaluating space, please wait...
Estimation of Required Space: 233MB
Available Space: 5333MB
Would you like to continue? (y/N) y
Start processing...
Synchronize boot files...
      0   0%   0.00kB/s   0:00:00 (xfr#0, to-chk=0/2)
      0   0%   0.00kB/s   0:00:00 (xfr#0, to-chk=0/2)
Start creating replica...
  244,670,045  99%  11.94MB/s   0:00:19 (xfr#170, to-chk=0/294)
Type: replica
Create Time: 2021.11.06-14:35:14
Size: 235MB
The system failback has been enabled and the replica has been created
successfully.
moxa@moxa-tbzkbl090923:/# sudo mx-system-mgmt system-failback info
Check the replica information...
Type: replica
Create Time: 2021.11.06-14:35:14
Size: 235MB
```

Customize the Boot Up Failure Criteria

If you would like to customize the boot failure criteria, you can edit below script to add criteria you like Moxa System Manager to check.

/etc/moxa-system-manager/check-hooks.d/99-example.sh

In the following example **99-example.sh**, Moxa System Manager will consider the boot up is successful if "moxa-connection-manager.service" start successfully by returning a zero value. If the program returns a non-zero value, the moxa-system-manager service will not mark this startup as successful, and it will enter the system-failback process to restore the system.

```
#systemctl is-active moxa-connection-manager.service && exit 0 || exit 1
```

8. Security Capabilities

In this chapter, we will introduce the key security functions on the V3000 computers and provide a security hardening guide to guide in deploying and operating the computer in a secure manner

Communication Integrity and Authentication

Below is a list of network communication services and protocols available with the Moxa V3000 Series computer and their mechanisms for data integrity, authentication, and protection.

Service	Protocol	Data Integrity	Data Authentication
SSH server and client	SSH	HMAC algorithm is used to guarantee data integrity	Uses key signature algorithms such as ED25519, ECDSA, or RSA to verify authenticity.
SFTP server	SSH		
SCP server	SSH		
APT client	HTTPS	SecureAPT uses checksum to guarantee data integrity	SecureAPT uses GPG public key system to validate data authenticity
NTP client (NTS support)	TLS/SSL, NTP	NTS guarantees data integrity via NTS Authenticator and Encrypted EF	NTS provides TLS layer to guarantee authenticity



ATTENTION

For additional communication services and protocols that you install, ensure that data integrity and authentication mechanisms are implemented for system protection. If integrity and authentication are not available, you must use additional compensating countermeasures in system to compensate the risk. For example, physical cable protection for serial Modbus RTU.

User Account Permissions and Privileges

Switching to the Root Privilege

In the V3000 Series computers, the root account is disabled in favor of better security. The default user account **moxa** belongs to the sudo group. Sudo is a program designed to let system administrators allow permitted users to execute some commands as the root user or another user. The basic philosophy is to give as few privileges as possible but still allow people to get their work done. Using sudo is better (safer) than opening a session as root for a number of reasons, including:

- Nobody needs to know the root password (sudo prompts for the current user's password). Extra privileges can be granted to individual users temporarily, and then taken away without the need for a password change.
- It is easy to run only the commands that require special privileges via sudo; the rest of the time, you work as an unprivileged user, which reduces the damage caused by mistakes.
- Some system-level commands are not available to the user moxa directly, as shown in the sample output below:

```
moxa@moxa-tbzk1090923:~$ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:90:e8:00:00:07
          inet addr:192.168.3.127  Bcast:192.168.3.255  Mask:255.255.255.0
          UP BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

```

RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth1      Link encap:Ethernet  HWaddr 00:90:e8:00:00:08
          inet addr:192.168.4.127  Bcast:192.168.4.255  Mask:255.255.255.0
          UP BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2592 (2.5 KiB)  TX bytes:2592 (2.5 KiB)

```

You can switch to the root account using the **sudo -i** (or **sudo su**) command. For security reasons, do not operate the **all** commands from the root account.



NOTE

Click the following link for more information on the **sudo** command.

<https://wiki.debian.org/sudo>



ATTENTION

You might get the permission denied message when using pipe or redirect behavior with a non-root account.

You must use **'sudo su -c'** to run the command instead of using **>**, **<**, **>>**, **<<**, etc.

Note: The single quotes enclosing the full command are required.

Controlling Permissions and Privileges

Moxa Industrial Linux uses Discretionary Access Control (DAC) based on Access Control Lists (ACLs) to manage permissions and privileges, which an object has an owner that controls the permissions to access the object. Subjects can transfer their access to other subjects. In other words, the owner of the resource has full access and can determine the access type (rwx: read, write, execute) of other users.

You can use **chmod** command to configure who (user, group, other) can do what (read, write, execute) to a file or directory. The access permission is extended by Access Control Lists (ACLs) authorization. ACL provides a more flexible mechanism that allows multiple users and groups to own an object. You can check and configure access control lists of a specific file or directory using **getfacl** and **setfacl** commands.



NOTE

Click the following link for more information on usages of **chmod** and Access Control Lists (ACLs)

<https://wiki.debian.org/Permissions>

The V3000 Series computers only provide one account in the **sudo** group by default because it is intended for the system integrator to customize and build their applications on top.

The system integrator shall be responsible for setting the appropriate permissions to roles and user accounts to enforce the concept of least privilege.

Linux Login Policy

Invalid Login Attempts

Moxa Industrial Linux provides the capability to configure allowed invalid login attempts to mitigate against Denial-of-Service (DoS) and Brute-force attack.

Security Model	Default Rule
Secure model	[5] consecutive invalid login within [60] seconds will deny access for [300] seconds.
Standard model	Not set

Following is the configuration file and variable to configure the setting for **Secure model**:

Configuration Option	Configuration file	Variable to Set
Consecutive invalid login	/etc/security/faillock.conf	deny
Within how many seconds	/etc/security/faillock.conf	fail_interval
Deny access for how long (in seconds)	/etc/security/faillock.conf	unlock_time

More configurable options can be found in following reference:

- [login.defs\(5\) > login > Debian bullseye > Debian Manpages](#)
- [faillock.conf\(5\) > libpam-modules > Debian bullseye > Debian Manpages](#)

Session Termination After Inactivity

This setting automatically terminates the login sessions after a standard period of inactivity. Below is the default configuration set in Moxa V3000 Series computer.

Security Model	Default Value
Secure model	<ul style="list-style-type: none">• Automatically logout standard user after 900 second of inactivity• Automatically terminate root privilege of sudo user after 900 second of inactivity
Standard model	Not set

Follow below instructions to configure the inactivity time:

Login Method	Configuration
Serial Console and SSH (Secure Shell)	<ul style="list-style-type: none">• Set the value (in seconds) of variable TMOUT in /etc/profile.d/99-moxa-profile.conf• Apply the same value to variable ClientAliveInterval in /etc/ssh/sshd_config.d/00-moxa-sshd.conf• To apply the rule to sudo user, make sure variable env_keep+= "TMOUT" exists in /etc/sudoers.d/00-moxa-sudoers.conf.

Login Banner Message

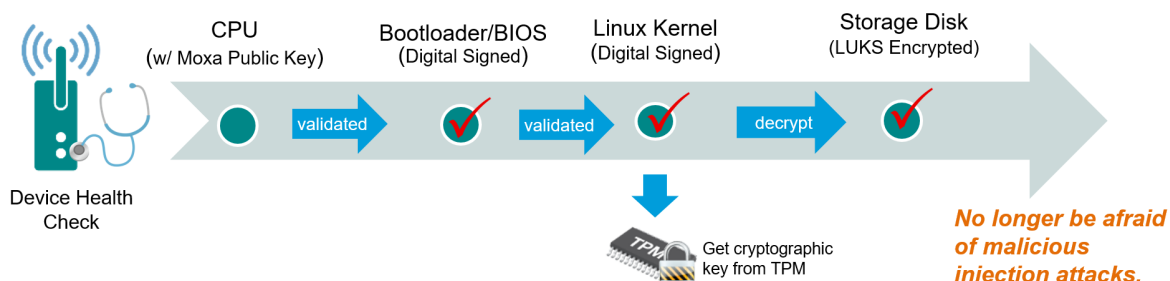
You can set a message banner message to displaying welcome or informational messages or warning message to un-authorized users. Follow below instructions to add a banner Moxa Industrial Linux 3.0 UM for V Series Computers Moxa Industrial Linux 3.0 UM for V Series Computers.

Login Method	Banner Content	Additional Configuration Required
Serial Console	/etc/issue	n/a
SSH (Secure Shell)	/etc/issue.net	Add variable Banner /etc/issue.net is added in /etc/ssh/sshd_config.d/00-moxa-sshd.conf

Secure Boot and Disk Encryption

Secure Boot and disk encryption are available in Secure model, designed to make platform integration more secure. Moxa's secure boot process begins from CPU as hardware root-of-trust to ensure integrity and authenticity of bootloaders and Linux kernels are validated with Moxa digital signature before execution, preventing malicious or un-authenticated bootloader and kernels to run on Moxa V3000 Series computer.

Next, only after bootloader and kernel have been validated, the LUKS (Linux Unified Key Setup) encrypted root file system (rtfs) will be decrypted by a key provisioned in TPM during factory production. The disk encryption prevent confidential data could be read without authorization when the device is stolen or lost.



Public key infrastructure (PKI)

Moxa secure boot use X.509 public key infrastructure (PKI) to validate authenticity and integrity of bootloader and Linux kernel.

How are private keys protected?

Private keys used to digital sign Moxa software are stored in on-premises tamper and intrusion-resistant hardware security module (HSM), where strict access authorization and 24-hour video surveillance are applied.

Key lifecycle and revocation

In an unlikely scenario where the private key stored in HSM is compromised, Moxa will announce the news on [Moxa Security Advisory](#), including instructions to revoke the compromised public key burned in the CPU via a utility downloadable from Moxa APT repository. Then update the bootloader and system image signed by a new private key.



ATTENTION

DO NOT arbitrarily replace the kernel or bootloader on Secure models, or the computer will not be able to boot up.

Trusted Platform Module (TPM 2.0)

The Moxa V3000 Series computer includes a TPM 2.0 hardware module. TPM provides a hardware-based approach to manage user authentication, network access, data protection and more that takes security to higher level than software-based security. It is strongly recommended to manage keys with TPM and also store digital credentials such as passwords

The TPM can be managed via the tpm2_tools pre-installed in Moxa Industrial Linux (<https://github.com/tpm2-software/tpm2-tools>).

TPM software stack & tool is maintained by tpm2-software community <https://tpm2-software.github.io/>

A good reference of TPM 2.0 introduction https://link.springer.com/chapter/10.1007/978-1-4302-6584-9_3

Host Intrusion Detection

Secure model of Moxa V3000 Series computer comes with **AIDE** (Advanced Intrusion Detection Environment) preconfigured. AIDE is a lightweight but powerful host intrusion detection utility for checking the integrity of files.

The out-of-factory Moxa V3000 Series computer comes with a database created by AIDE at the first time bootup containing all security configurations set by Moxa. You can compare the system's status against this database to find out if there is any integrity breach. You can also update the database after making changes to the configuration or adding additional software.

Default Monitored Files

Below are the security configuration files and directories included in the default database created by Moxa.

- The database is **aide-moxa.db** and put under **/var/lib/aide/aide-moxa.db**
- The configuration file of AIDE is **/etc/aide/aide-moxa.conf**; you can add additional files and directories to the database

Configuration Type	Path
File	/etc/adduser.conf
	/etc/login.defs
	/etc/logrotate.conf
	/etc/nftables.conf
	/etc/profile
	/etc/rsyslog.conf
	/etc/sudoers
	/etc/security/pwquality.conf
	/etc/sysctl.conf
	/etc/moxa/moxa-guardian/
Directory	/etc/aide/
	/etc/audit/
	/etc/logrotate.d/
	/etc/moxa/MoxaComputerInterfaceManager/
	/etc/moxa/MoxaConnectionManager/
	/etc/moxa/moxa-guardian/
	/etc/pam.d
	/etc/security/
	/etc/profile.d/
	/etc/rsyslog.d/
	/etc/ssh/
	/etc/sudoers.d
	/var/lib/moxa-guardian/
	/etc/chrony/
	/etc/fail2ban/
	/etc/fstab
	/etc/security/pwquality.conf.d/
	/etc/sysctl.d/

To run a comparison between current system against the Moxa AIDE database, run **aide --check -c /etc/aide/aide-moxa.conf**

```
moxa@moxa-tbbbbb1182827:/# sudo aide --check -c /etc/aide/aide-moxa.conf
Start timestamp: 2022-06-12 13:47:38 +0000 (AIDE 0.17.3)
AIDE found NO differences between database and filesystem. Looks okay!!

Number of entries:      254
-----
The attributes of the (uncompressed) database(s):
-----
/var/lib/aide/aide-moxa.db
MD5      : A8wKxphrNVlWz31AVf3esA==
SHA256   : trGvVioXdZf/RISmj3v60mQsmcrqK4kV
          sUFm068cLOs=

End timestamp: 2022-06-12 13:47:39 +0000 (run time: 0m 1s)
```

To update the database after you have make configuration changes, run **aide --init -c /etc/aide/aide-moxa.conf**

You should see following output which created a new AIDE database **aide-moxa.db.new** under **/var/lib/aide**

```
moxa@moxa-tbbbbb1182827:/# sudo aide --init -c /etc/aide/aide-moxa.conf

Start timestamp: 2022-06-12 14:39:30 +0000 (AIDE 0.17.3)
AIDE initialized database at /var/lib/aide/aide-moxa.db.new

Number of entries:      254
-----
The attributes of the (uncompressed) database(s):
-----

/var/lib/aide/aide-moxa.db.new
MD5      : Mb74vEG93jjVfJMGSZa+DA==
SHA256   : ENl5QGVgYXKuKEwE3FSXRfzx13vJg0TxU
          WsQnHN16E74=

End timestamp: 2022-06-12 14:39:30 +0000 (run time: 0m 0s)
```

For AIDE to use the new database, you need to rename it to **aide-moxa.db**

```
moxa@moxa-tbbbbb1182827:/# sudo mv /var/lib/aide/aide-moxa.db.new
/var/lib/aide/aide-moxa.db
```

At this point, you can run **aide --check -c /etc/aide/aide-moxa.conf** to compare current system against the updated AIDE database

How to Perform Authenticity and Integrity Checks on All Files

If you would like to ensure authenticity and integrity of all files in the Moxa V3000 Series computer, you can create an OpenSSL signed database containing every single file under the filesystems, then validate the authenticity of the database before using AIDE to check the integrity of all files in the filesystem. Following below steps to create such AIDE database.

1. Create a database using `/etc/aide/aide-fs.conf`; this configuration file monitors every single file in the filesystem.

```
moxa@moxa-tbbbb1182827:/# sudo aide --init -c /etc/aide/aide-fs.conf
```

2. Rename the created database to `/var/lib/aide/aide-fs-moxa.db`
3. Generate a 4096-bit RSA private key.

```
moxa@moxa-tbbbb1182827:/# sudo openssl genrsa -out aide-key.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for aide-key.pem:
```



ATTENTION

You MUST keep the private key and pass phrase in a secure location.

4. Generate a public key from the private key:

```
moxa@moxa-tbbbb1182827:~$ sudo openssl rsa -in aide-key.pem -pubout -out
aide-
key.pub
Enter pass phrase for aide-key.pem:
writing RSA key
moxa@moxa-tbbbb1182827:~$
```

5. Generate a digital signature of `aide-filesystem-moxa.db` by the private key.

```
moxa@moxa-tbbbb1182827:~$ sudo openssl dgst -sha256 -sign aide-key.pem -out
aide-filesystem-moxa.db.sha256 /var/lib/aide/aide-fs-moxa.db
Enter pass phrase for aide-key.pem:
```

6. Now, you can distribute the database, public key and signed signature to other locations, such as a centralized remote system.
7. Verify if the database has been tampered or not.

```
moxa@moxa-tbbbb1182827:~$ sudo openssl dgst -sha256 -verify aide-key.pub -
signature aide-filesystem-moxa.db.sha256 /var/lib/aide/aide-fs-moxa.db
Verified OK
```

8. After the AIDE database' authenticity has been validated, you can run a comparison check between current system against the AIDE database using `aide --check -c /etc/aide/aide-fs.conf`



NOTE

Click the following link for more information on usages of AIDE
<https://manpages.debian.org/bullseye/aide-dynamic/aide.1.en.html>

Intrusion Prevention

Fail2ban is pre-installed in Moxa Industrial Linux as an intrusion prevention software framework designed to prevent against brute-force attacks



NOTE

Click the following link for detail instructions of Fail2ban usage

https://www.fail2ban.org/wiki/index.php/Main_Page

Network Security Monitoring

Zeek is pre-installed in Moxa Industrial Linux for network security monitoring. Zeek is a passive network traffic analyzer. Many operators use Zeek as a network security monitor (NSM) to support investigations of suspicious or malicious activity. Zeek also supports a wide range of traffic analysis tasks beyond the security domain, including performance measurement and troubleshooting. Zeek provides an extensive set of logs describing network activity. These logs include not only a comprehensive record of every connection seen on the wire, but also application-layer transcripts

If you have configured **cellular (4G/LTE)** and **ethernet** networks in [Moxa Connection Manager \(MCM\)](#). You can also enable Zeek to monitor the network traffic of these interfaces. Following the simple instruction below:

1. Export the Zeek environment.

```
export PATH=$PATH:/opt/zeek/bin
export ZEEK_PREFIX=/opt/zeek
```

2. [Required] Configure the interface to monitor by running # **vim \$ZEEK_PREFIX/etc/node.cfg**.
3. [Required] Modify the interface list according to the interface you like to monitor. For example, add LAN1, LAN2, and cellular (4G/LTE) in the list.

```
# This example has a standalone node ready to go except for possibly
# changing
# the sniffing interface.

# This is a complete standalone configuration. Most likely you will
# only need to change the interface.
[zeek]
type=standalone
host=localhost
interface=eth0,eth1,wwan0
```

4. [Optional] change the **MailTo** email address to a desired recipient and the **LogRotationInterval** to a desired log archival frequency

```
vim $ZEEK_PREFIX/etc/zeekctl.cfg
```

```
# Recipient address for all emails sent out by Zeek and ZeekControl.
MailTo = root@localhost

# Rotation interval in seconds for log files on manager (or standalone)
# node.
# A value of 0 disables log rotation.
LogRotationInterval = 3600
```

5. [Required] Run **\$ZEEK_PREFIX/bin/zeekctl** to start Zeek

```
root@moxa-tbbbbb1182827:/home/moxa# $ZEEK_PREFIX/bin/zeekctl

Hint: Run the zeekctl "deploy" command to get started.
Welcome to ZeekControl 2.4.0

Type "help" for help.
[ZeekControl] >
```

6. [Required] For the first-time use of the shell, use **install** command to perform initial installation of the ZeekControl configuration.

```
[ZeekControl] > install

creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
[ZeekControl] >
```

7. [Required] Start Zeek instance by **start** command (Use CTRL+D to exit if initializing successfully).

```
[ZeekControl] > start

starting zeek ...
(zeek still initializing)
```

8. View the Zeek logs under **\$ZEEK_PREFIX/logs**.

```
root@moxa-tbbbbb1182816:/# ls -alh /opt/zeek/logs/current/
total 96K
drwxr-sr-x 2 root zeek 4.0K Jun 19 04:18 .
drwxrws--- 1 root zeek 4.0K Jun 19 04:17 ..
-rw-r--r-- 1 root zeek 250 Jun 19 04:18 capture_loss.log
-rw-r--r-- 1 root zeek 128 Jun 19 04:17 .cmdline
-rw-r--r-- 1 root zeek 583 Jun 19 04:18 conn.log
-rw-r--r-- 1 root zeek 352 Jun 19 04:17 .env_vars
-rw-r--r-- 1 root zeek 30K Jun 19 04:17 loaded_scripts.log
-rw-r--r-- 1 root zeek 753 Jun 19 04:18 notice.log
-rw-r--r-- 1 root zeek 227 Jun 19 04:17 packet_filter.log
-rw-r--r-- 1 root zeek 5 Jun 19 04:17 .pid
-rw-r--r-- 1 root zeek 61 Jun 19 04:17 .startup
-rw-r--r-- 1 root zeek 686 Jun 19 04:17 stats.log
-rwxr-xr-x 1 root zeek 19 Jun 19 04:17 .status
-rw-r--r-- 1 root zeek 19 Jun 19 04:17 stderr.log
-rw-r--r-- 1 root zeek 204 Jun 19 04:17 stdout.log
-rw-r--r-- 1 root zeek 367 Jun 19 04:18 weird.log
```



NOTE

Click the following link for Zeek's detail instruction and also the explanation on log types
<https://docs.zeek.org/en/master/quickstart.html>

If you prefer not to use ZeekControl (e.g., you don't need its automation and management features), you can refer to <https://docs.zeek.org/en/master/quickstart.html#zeek-as-a-command-line-utility> on how to directly control Zeek for your analysis activities from the command line for both live traffic and offline working from traces.

Firewall

nftable is the built-in firewall in Moxa Industrial Linux. Secure model of Moxa V3000 Series computer has pre-configured rules to further protect your device from network attacks.



NOTE

Click the following link for detail instructions of nftable usages

https://wiki.nftables.org/wiki-nftables/index.php/Main_Page

https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes

Pre-configured Rule

Below is a summary of nftable rules in `/etc/nftables.conf` set by Moxa in Secure model of Moxa V3000 Series computer. For Standard model, nftable is not enabled by default.

Rules Set	Location/Parameters
Allowed only ports following port <ul style="list-style-type: none">TCP: SSH (22), HTTPS (443), SNMP TRAP (162)UDP: NTP (123), DNS (53), SNMP (161), SNMP TRAP (162)	define tcp_port_allow = { ssh, https, 161, 162}; define udp_port_allow = { 53, ntp, 161, 162};
Allow all traffic from loopback interface	iifname "lo" accept
Drop all input traffic except for traffic from allowed ports and icmp (ping)	chain input {}
Allow related and established traffic by using conntrack	ct state invalid drop ct state established,related accept
Drop all forward traffic	chain forward {}
Accept all output traffic	chain output {}

```
flush ruleset

define tcp_port_allow = { 22, 443 };
define udp_port_allow = { 53, 123 };

table inet filter {
    # input: drop all traffic
    chain input {
        type filter hook input priority 0; policy drop;
        ct state invalid drop
        ct state established,related accept
        # allow icmp
        icmp type {
            echo-request,
            echo-reply,
            time-exceeded,
            parameter-problem,
            destination-unreachable
        } accept

        # allow icmp6
        icmpv6 type {
            echo-request,
            echo-reply,
            time-exceeded,
            parameter-problem,
            destination-unreachable,
            nd-neighbor-solicit,
            nd-router-advert,
            nd-neighbor-advert
        } accept

        # accept lo
        iifname "lo" accept
        tcp dport $tcp_port_allow accept
        udp dport $udp_port_allow accept
    }

    # forward: drop all traffic
    chain forward {
        type filter hook forward priority 0; policy drop;
    }

    # output: accept all traffic
    chain output {
        type filter hook output priority 0; policy accept;
    }
}
```

Common nftable Usage

1. List the currently loaded nftable rules # **nft list ruleset**
2. Debug and tracing if traffic are drop or accept as expected # **nft monitor trace**
 - a. Add trace_chain before the existing input chain

```
nft add chain inet filter trace_chain { type filter hook prerouting
priority -1\; }
```

- b. Add nfttrace flag

```
nft add rule inet filter trace_chain meta nfttrace set 1
```

- c. Monitor trace (you can use another device with ncat tool to test it)dd nfttrace flag

```
moxa@moxa-tbbbbb1182816:/# sudo nft monitor trace
```

```
trace id d51bda11 inet filter trace_chain packet: iif "eth0" ether saddr
d8:5e:d3:a5:7b:29 ether daddr 00:90:e8:a6:37:cb ip saddr 192.168.1.102 ip
daddr 192.168.1.107 ip dscp cs0 ip ecn not-ect ip ttl 128 ip id 36481 ip
protocol tcp ip length 52 tcp sport 1142 tcp dport 53 tcp flags == syn
tcp window 64240 trace id d51bda11 inet filter trace_chain rule meta
nfttrace set 1 (verdict continue) trace id d51bda11 inet filter
trace_chain verdict continue trace id d51bda11 inet filter trace_chain
policy accept trace id d51bda11 inet filter input packet: iif "eth0"
ether saddr d8:5e:d3:a5:7b:29 ether daddr 00:90:e8:a6:37:cb ip saddr
192.168.1.102 ip daddr 192.168.1.107 ip dscp cs0 ip ecn not-ect ip ttl
128 ip id 36481 ip protocol tcp ip length 52 tcp sport 1142 tcp dport 53
tcp flags == syn tcp window 64240 trace id d51bda11 inet filter input
verdict continue trace id d51bda11 inet filter input policy drop
```

- d. Once debugging is completed, make sure to remove the debug flag by either method below:
 - ☐ Restart nftable # **systemctl restart nftables** or
 - ☐ Reload the configuration again # **nft -f /etc/nftables.conf**

Rate Limiting

Rate limiting is a common strategy to prevent network attacks such as DOS, DDOS, and brute force by limiting the network traffic within a specified time. As the suitable rate limit configuration depends heavily on the asset owner's applications, rate limiting is not configured by default in Moxa Industrial Linux.

nftable Rate Limit Usage	Example of Rate Limit Configuration
rate [over] <value> <unit> [burst <value> <unit>]	limit rate 400/minute limit rate 400/hour limit rate over 40/day limit rate over 400/week limit rate over 1023/second burst 10 packets limit rate 1025 kbytes/second limit rate 1023000 mbytes/second limit rate 1025 bytes/second burst 512 bytes limit rate 1025 kbytes/second burst 1023 kbytes limit rate 1025 mbytes/second burst 1025 kbytes limit rate 1025000 mbytes/second burst 1023 mbytes

You can directly add rate limit to existing rule in **/etc/nftables.conf**:

Below is an example of limiting TCP and UDP network traffic to 4 packets per second

```
#!/usr/sbin/nft -f

flush ruleset

define tcp_port_allow = { ssh, https };
define udp_port_allow = { 53, ntp };

table inet filter {
    # input: drop all traffic
    chain input {
        type filter hook input priority 0; policy drop;

        ct state invalid drop
        ct state established,related accept

        # allow icmp
        ip protocol icmp icmp type {
            echo-request,
            echo-reply,
            time-exceeded,
            parameter-problem,
            destination-unreachable
        } accept

        # allow icmp6
        ip6 nexthdr icmpv6 icmpv6 type {
            echo-request,
            echo-reply,
            time-exceeded,
            parameter-problem,
            destination-unreachable
        } accept

        # accept lo
    }
    iifname "lo" accept

    tcp dport $tcp_port_allow limit rate 4/second accept
    udp dport $udp_port_allow limit rate 4/second accept
}
```

Mitigating a NTP Amplification Attack

The default configured NTP servers in Moxa Industrial Linux(MIL) are with NTS support. If you use public NTP servers without NTS support, it is vulnerable to the **NTP amplification attack**, in which the attacker could exploit the public NTP servers to overwhelm Moxa V3000 Series computer with UDP traffic. Under such an incident, you can follow the steps to stop the attack:

1. Stop NTP service temporarily with the # systemctl stop systemd-timesyncd command.
2. Block the tainted NTP server by nftables command

- a. Create new firewall table

```
nft add table inet firewall-filter
```

- b. Create new chain input in firewall table

```
nft add chain inet firewall-filter input
```

- c. Create new chain input in firewall table

```
nft add rule inet firewall-filter input tcp dport { ntp } ip saddr <your ip> reject
```

- d. Block NTP server IP

```
nft add rule inet firewall-filter input tcp dport { ntp } ip saddr <your ip> reject
```

- e. Check the rule set

```
nft list ruleset

...
table inet firewall-filter {
    chain input {
        tcp dport { 123 } ip saddr 10.213.123.55 reject
    }
}
```

3. You can choose to specify another NTP server (modify `/etc/systemd/timesyncd.conf`) or wait for this server to finish troubleshooting
4. Remember to flush the rule after recovery

```
nft delete chain inet firewall-filter input # delete chain
# or
nft delete table inet firewall-filter # delete table
```

Service and Ports

Only activate protocols that you require to use the system. Below is the list for the protocol and port numbers used for all external interfaces. Please refer to [Firewall](#) section to modify the list of allowed port if additional port is required.

Protocol	Protocol Type	Port Number
SSH	TCP	22
HTTPS	TCP	443
NTS	UDP	123/4460
DNS	UDP	53

Disable Unused Interface

To enhance cybersecurity by reducing the attack surface, disable any unused interfaces using the [Moxa Computer Interface Manager \(MCIM\)](#)

- Serial console port
- Serial port
- CAN port
- Ethernet port
- External storage (e.g., USB, SD)

Disable Unnecessary Protocols, Services, and Ports

You can use `#ss` to list all the current running processes using with the associated service, protocol, and network port.

```
moxa@moxa-tbbbb1182827:~$ sudo ss -tulpn
Netid State  Recv-Q Send-Q Local Address:Port Peer Address:Port Process
tcp    LISTEN  0      128   0.0.0.0:22      0.0.0.0:*      users:("sshd",pid=974,fd=3))
tcp    LISTEN  0      128   [::]:22       [::]:*        users:("sshd",pid=974,fd=4))
```

You can disable a daemon or service by killing process ID (PID) directly. For example:

```
moxa@moxa-tbbbb1182827:~$ sudo kill 974
```

Or you can just stop and disable the service using `#systemctl`. For example:

```
moxa@moxa-tbbbb1182827:~$ sudo systemctl stop sshd
moxa@moxa-tbbbb1182827:~$ sudo systemctl disable sshd
```


Restrict Unnecessary Protocols, Services, and Ports

1. Protocols:

Use **nftables** meta to match kind of TCP traffic Matching packet metainformation. Refers to [nftables wiki](#).

2. Services:

Use **# systemctl list-unit-files** to find unused services and disable them by **systemctl disable <service>**.

3. Ports:

Use nftables to add accepted ports in whitelist. Refers to the [Firewall](#) section for detail instructions.

Services Enabled by Default

Below is the list of services enabled by default in the "secure" model of V3000 Series computers.

Service Name	Description
auditd.service	Security Audit log service
dbus.service	System Message Bus
fail2ban.service	Fail2ban IPS (intrusion prevention software)
getty@tty1.service	Getty on tty1
ifupdown-pre.service	Helper to synchronize boot up for ifupdown
kmod-static-nodes.service	Create list of static device nodes for the current kernel
ModemManager.service	DBus-activated daemon which controls mobile broadband (2G/3G/4G) devices and connections
moxa-connection-manager.service	Moxa Connection Manager (MCM)
moxa-guardian.service	Initializing security configuration for Moxa Industrial Linux
moxa-sys-rdy.service	A service the light up the "READY" or "RDY" when the computer successfully boots up
moxa-system-manager-init.service	Moxa System Manager initialization service
moxa-system-manager.service	Moxa System Manager
MoxaComputerInterfaceManager.service	Moxa Computer Interface Manager
moxa-hostname.service	This service is designed to execute automatically during system startup, setting the hostname to a default unique value in the format moxa-[serial number]. If you prefer to define a custom hostname, you can disable this service by utilizing the 'systemctl disable moxa-hostname.service' command."
networking.service	Raises or downs the network interfaces
NetworkManager.service	Network Manager
nftables.service	nftable
polkit.service	For controlling system-wide privileges is Moxa Industrial Linux
rsyslog.service	System Logging Service
serial-getty@tty0.service	Serial Getty on tty0
serial-getty@tty1.service	Serial Getty on tty1
snmpd.service	Linux service for the Simple Network Management Protocol (SNMP)
ssh.service	SSH Server
sysstat.service	A collection of performance monitoring tools for Linux.
systemd-journal-flush.service	Flush journal to persistent storage
systemd-journald.service	Journal service
systemd-logind.service	User login management
systemd-modules-load.service	Early boot service that loads kernel modules
systemd-random-seed.service	Service that loads an on-disk random seed into the kernel entropy pool during boot and saves it at shutdown
systemd-remount-fs.service	early boot service that applies mount options listed in fstab(5)
systemd-sysctl.service	An early boot service that configures sysctl(8) kernel parameters
systemd-sysusers.service	Creates system users and groups, based on the file format and location specified in sysusers.d(5)
systemd-timesyncd.service	System service that synchronizes the local system clock with a remote Network Time Protocol (NTP) server
systemd-tmpfiles-setup-dev.service	Create Static Device Nodes in /dev
systemd-tmpfiles-setup.service	Create Volatile Files and Directories

Service Name	Description
systemd-udev-trigger.service	Coldplug all udev devicesd-udev-trigger.service
systemd-udevd.service	Listens to kernel uevents
systemd-update-utmp.service	Service that writes SysV runlevel changes to utmp and wtmp, as well as the audit logs
systemd-user-sessions.service	a service that controls user logins through pam_nologin(8)
user-runtime-dir@1000.service	Default user
user@1000.service	Default user
vnstat.service	network traffic monitor
watchdog.service	Watchdog service
wpa_supplicant.service	WPA supplicant

Managing Resources

Setting The Process Priority

A process can be manually adjusted to increase or decrease its priority. Use the **top** or **ps** commands to find out the process priority.

```
moxa@moxa-tbbbb1182827:/# sudo top
top - 22:08:43 up 6 min, 1 user, load average: 0.01, 0.04, 0.01
Tasks: 105 total, 1 running, 104 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.8 sy, 0.0 ni, 98.8 id, 0.1 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 2068192 total, 1874520 free, 57416 used, 136256 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 1799712 avail Mem

  PID USER      PR  NI   VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    1 root        20   0   9492    6220   5236 S   0.0   0.3   0:00.98 systemd
    2 root        20   0        0        0        0 S   0.0   0.0   0:00.00 kthreadd
    3 root        20   0        0        0        0 S   0.0   0.0   0:00.01 ksoftirqd/0
    4 root        20   0        0        0        0 S   0.0   0.0   0:00.02 kworker/0:0
    5 root         0 -20        0        0        0 S   0.0   0.0   0:00.00 kworker/0:0H
    6 root        20   0        0        0        0 S   0.0   0.0   0:00.01 kworker/u2:0
    7 root        20   0        0        0        0 S   0.0   0.0   0:00.02 rcu_sched
  ...
```

You can also use the **ps** command with the **-l**, long list option to find out the priority of the process.

```
moxa@moxa-tbbbb1182827:/# sudo ps -efl
F S UID  PID PPID C  PRI  NI ADDR  SZ WCHAN  STIME TTY     TIME CMD
4 S root  1    0    0  80   0 -    2373 ep_pol 22:02 ?    00:00:01 /sbin/init
1 S root  2    0    0  80   0 -        0 kthrea 22:02 ?    00:00:00 [kthreadd]
1 S root  3    2    0  80   0 -        0 smpboo 22:02 ?    00:00:00 [ksoftirqd/0]
1 S root  5    2    0  60 -20 -        0 worker 22:02 ?    00:00:00 [kworker/0:0H]
1 S root  6    2    0  80   0 -        0 worker 22:02 ?    00:00:00 [kworker/u2:0]
1 S root  7    2    0  80   0 -        0 rcu_gp 22:02 ?    00:00:00 [rcu_sched]
1 S root  8    2    0  80   0 -        0 rcu_gp 22:02 ?    00:00:00 [rcu_bh]
...
```

The PRI (Priority) or NI (Nice) is the priority of the process. The PRI is adjusted by kernel automatically. The NI can have a value in the range -20 to 19. A smaller value means that the program could use more CPU resources.

The nice utility can be given a specific nice value while running a program. This example shows how to launch the **tar** utility with the nice value 5.

```
moxa@moxa-tbbbb1182827:/# sudo nice -n 20 tar -czvf TheCompressFile.tar /src1 /src2 ...
OR
moxa@moxa-tbbbb1182827:/# sudo nice -adjustment 20 tar -czvf
TheCompressFile.tar /src1 /src2 ...
```

You can use the **renice** utility to dynamically adjust the nice value of a program. This example uses renice to adjust the auditd, PID 639, with highest priority as -20.

```
moxa@moxa-tbbbb1182827:/# sudo renice -n 20 -p 639
moxa@moxa-tbbbb1182827:/# sudo ps -efl|grep auditd
1 S root          639      1  0  75  -20 -   1519 poll_s 22:02 ?           00:00:00
/sbin/auditd -n
...
```



NOTE

Click the following link for more information on usages of nice and renice

<https://manpages.debian.org/bullseye/coreutils/nice.1.en.html>

<https://manpages.debian.org/bullseye/bsdutils/renice.1.en.html>

Setting the Process I/O Scheduling Class and Priority

The **ionice** command can adjust the priority of the program using I/O. The class and priority are adjustable for a process.

-c class	0: none 1: realtime 2: best-effort 3: idle
-n classdata	The realtime and best-effort can set from 0 to 7. A smaller value means the program has a higher priority.
-p PID	Process ID

```
moxa@moxa-tbbbb1182827:/# sudo ps -l
F S    UID     PID  PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
4 S      0      895    886  0  80   0 -   1794 wait  pts/0        00:00:00 bash
4 S      0     1099    895  0  80   0 -   1659 poll_s pts/0        00:00:00 sudo
4 R      0     1100   1099  0  80   0 -   1850 -      pts/0        00:00:00 ps
moxa@moxa-tbbbb1182827:/# sudo ionice -c 2 -n 0 -p 895
moxa@moxa-tbbbb1182827:/# sudo ionice -p 895
best-effort: prio 0
```



NOTE

Click the following link for more information on usages of ionice

<https://manpages.debian.org/bullseye/util-linux/ionice.1.en.html>

Limiting the CPU Usage of a Process

The **cpulimit** program is a simple way to limit the CPU usage of a process (expressed in percentage, not CPU time). The program is useful to control batch jobs, to regulate the use of the CPU so that they do not take too much CPU resources. The program can also run in the background.

The following example uses **cpulimit**, running in the background, to limit the usage of CPU by the **sshd** process to 25%. The **-p** is the process ID. **-e** is the executable program file name, and **-l** is the CPU limit percentage. The option **-b** is for running the **cpulimit** program in the background to free up the terminal.

```
moxa@moxa-tbbbb1182827:/# sudo cpulimit -p 895 -l 25 -b
```



NOTE

Click the following link for more information on usages of cpulimit

<https://manpages.debian.org/bullseye/cpulimit/cpulimit.1.en.html>

Limiting the Rate

Refer to the [Chapter 8 Security Firewall Rate Limiting](#) to customize the network limitation of the firewall configuration.

Audit Log

In this section, we will introduce the audit event log design in Moxa Industrial Linux and the bootloader, including security event monitoring and recommended response and approach for auditing process failures.

Linux Audit log

Moxa Industrial Linux enables system administrators to monitor detailed information about system operation using **auditd** log. The log provides a way to track and record security-relevant information on the system with the following features:

- Log partition size:

Computer Series	Log partition size
V3000 Series	1024 MB

- Log partition applies Linux Unified Key Setup (LUKS) encryption and restrict non root user from access
- Logs are stored under **/var/log/audit/** and the log format follows **auditd** standard.

- Below is a reference of where to find the commonly used log data fields in audit log

Common Log Data Fields	Data Fields in auditd log
timestamp	msg=audit(TIMESTAMP)
source	proctitle, comm, exec, uid, gid, etc.
category	key
type	type
eventID	pid, ppid

- Audit log records are automatically rotated daily and up to 14 achieved logs are kept at a time. When log rotates, the oldest archive will be deleted if 14 achieved logs exist.
 - Audit log rotation rule can be modified in **/etc/logrotate.d/auditd**
- The log timestamp is the local system time which synchronize with a remote Network Time Protocol (NTP) server.
 - For time synchronization status and configuration, see [timedatectl\(1\)](#).



NOTE

Click the following link for more information on usages of auditd and log search:

<https://manpages.debian.org/bullseye/auditd/auditd.8.en.html>

<https://manpages.debian.org/bullseye/auditd/ausearch.8.en.html>

The following table lists the security events that Moxa Industrial Linux is pre-configured to monitor in the Secure mode of the Moxa V Series computer.

Event Category	Event Logged	File or Directory to Monitor	key used for ausearch
Access control	Users logins, logouts, system events, etc.	/var/run/utmp /var/run/btmp /var/run/wtmp	session
Backup and restore	Use of Moxa System Manager tool	/sbin/mx-system-mgmt	system_mgmt
Control System	Shutdown system	/bin/systemctl	control_system
	Power off system		
	Reboot system		
	Halt system		
	Use of APT package management system	/usr/bin/apt	system_package
	Use of aptitude tool	/usr/bin/aptitude	system_package
	Use of add-apt-repository tool	/usr/bin/apt-add-repository	system_package
	Use of apt-get tool	/usr/bin/apt-get	system_package
Security configurations	Use of dpkg package manager tool	/usr/bin/dpkg	system_package
	Add user configuration change	/etc/adduser.conf	adduser
	AIDE configuration and database change	/etc/aide	aide
	Audit configuration and log change	/etc/audit /var/log/audit	auditconfig auditlog
	Chrony configuration change	/etc/chrony	chrony
	Fail2ban configuration change and log change	/etc/fail2ban /var/log/fail2ban.log	fail2ban fail2ban-log
	Fail lock configuration change	/etc/security/faillock.conf	faillock
	Login policy change	/etc/login.defs	login
	Log rotate configuration change	/etc/logrotate.conf /etc/logrotate.d	logrotate
	nftable configuration change	/etc/nftables.conf	nftables
	Moxa Computer Interface Management configuration change	/etc/moxa/ MoxaComputerInterfaceManager	mcim
	Moxa Connection Manager configuration change	/etc/moxa/MoxaConnectionManager	mcm
	Moxa Guardian configuration and log change	/etc/moxa/moxa-guardian /var/lib/moxa-guardian	moxa-guardian moxa-guardian-registry
	Password policy change	/etc/pam.d	pam
	Linux system wide environment configuration change	/etc/profile /etc/profile.d	profile
	Password rule change	pwquality.conf pwquality.conf.d	pwquality
	Rsyslog configuration change	/etc/rsyslog.conf /etc/rsyslog.d	rsyslog
	SSH (Secure Shell) configuration change	/etc/ssh/sshd_config /etc/ssh/sshd_config.d	sshd
	Sudo configuration change	/etc/sudoers	sudo
	Kernel parameters change	/etc/sysctl.conf /etc/sysctl.conf.d	sysctl

Bootloader Audit Log

1. Log is stored in SPI flash with a storage size of **1 MB**.
2. Log can be viewed via **(2) Advance Setting > (4) View Bootloader Log** options in the Bootloader menu.
3. The maximum number of logs is 4,000 records, wherein the oldest log will be overwritten when the maximum capacity is reached.
4. The timestamp of the log read from the local real-time clock (RTC) is synchronize with Network Time Protocol (NTP) server.
5. The log format and log events are described in the following tables:

Audit Log Structure

Header	Explanation	Possible Values
Time	Time stamp of the device	Format: [YYYY-MM-DDThh:mm:ss] For example: [2022-06-03T15:54:38]
User	Identifies the authenticated user	Admin
Category	Event category	<ul style="list-style-type: none">• System• Bootcfg (see Boot Configuration)• Install• Security
Event ID	ID of a logged event	1 ~ 15
Event Message	Description of the logged event	See below table for the list of events

Audit Events

Category	Event ID	Event Type	Event Message
System	1	Info	All bootloader configuration set to default
System	2	Info	Exit bootloader and reboot system
System	3	Info	Exit bootloader and boot to Linux
bootcfg	4	Info	Set boot configuration to default ok
bootcfg		Warning	Set boot configuration to default fail
bootcfg	5	Info	Set boot from SD/USB/eMMC ok
bootcfg		Warning	Set boot from SD/USB/eMMC fail
bootcfg	6	Warning	USB is not available on this device
bootcfg	7	Info	Bootarg and bootcmd changed
Install	8	Info	Install system image from TFTP ok
Install		Warning	Destination net unreachable
Install		Warning	Hash/Signature file not find
Install		Warning	System image file error
Install		Warning	File size is too large
Install		Warning	Upgrade system image fail
Install		Alert	System image authenticity check fail
Install		Info	Install system image from SD ok
Install	9	Warning	SD/USB/eMMC device not find
Install		Warning	Hash/Signature file not find
Install		Warning	System image file error
Install		Warning	File size is too large
Install		Warning	Upgrade system image fail
Install		Alert	System image authenticity check fail
Secure	10	Info	Install system image from USB ok
Secure		Warning	SD/USB/eMMC device not find
Secure		Warning	Hash/Signature file not find
Secure		Warning	System image file error
Secure		Warning	File size is too large
Secure		Warning	Upgrade system image fail
Secure		Alert	System image authenticity check fail
Secure	11	Info	TFTP setting changed
Secure	12	Info	Login success
Secure		Warning	login fail

Category	Event ID	Event Type	Event Message
Secure	13	Alert	Boot failure due to system image integrity or authenticity check fail
Secure	14	Info	Admin password disabled
Secure		Info	Admin password enabled
Secure	15	Info	Admin password set to default
Secure	16	Info	Admin password changed
Secure	17	Info	Admin password policy changed
Secure	18	Info	Advance settings set to default
Secure	19	Info	Auto reboot threshold changed
Secure	20	Info	Login message changed
Secure	21	Info	Invalid Login Attempts changed
Secure	22	Info	Clear TPM ok
Secure		Warning	Clear TPM fail
audit	23	Info	View bootloader log ok

Audit Failure Response

Without appropriate response to audit processing failure, an attacker's activities can go unnoticed, and evidence of whether the attack led to a breach can be inconclusive. Here we set out guidelines for protection of critical system functions in case of audit processing failure. Some of the common approaches are as follows:

1. Log rotation

Log rotation is enabled by default in Moxa V3000 Series computer to prevent exceeding the audit storage capacity. Refer to **Linux Audit Log** and **Bootloader Audit log** sections for details.

In Linux, configure logrotate to limit the disk space usage and prevent running out of space. The logrotate configuration file is at `/etc/logrotate.conf` and `/etc/logrotate.d/*` has all the log files created by log rotation.

This example we configure `/etc/logrotate.d/rsyslog` to rotate `/var/log/syslog` while it overs the size 2M with only three rotation.

```
/var/log/syslog
{
    {
        rotate 3
        maxsize 2M
        ...
    }
}
```

2. Saving the logs in external storage

- For auditd, change the file path of parameter **log_file** in `/etc/audit/auditd.conf`
- For rsyslog, change the default file path `/var/log/` in `/etc/rsyslog.conf` to external storage

3. Use a centralized log server

Use a centralized log managements system to collect and store the logs from Log from multiple devices. Refers to [How to Set Up Centralized Logging on Linux with Rsyslog](#)

4. Assign appropriate action when audit storage space is full, or an error occurs

You can configure **space_left** and **space_left_action** parameters in `/etc/audit/auditd.conf` to specify the remaining space (in megabytes or %) for low disk alert and what action to take. The actions are ignore, syslog, rotate, exec, suspend, single, and halt.

In example below, warning email will be sent to email account specified in **action_mail_acct** parameter when the free space in the filesystem containing log files drop below 75 megabytes.

```
space_left = 75
space_left_action = email
```

Configure **disk_full_action** and **disk_error_action** in `/etc/audit/auditd.conf` to specify what actions to take when audit storage disk got error or full. The actions are ignore, syslog, rotate (for disk full only), exec, suspend, single, and halt.

Refers to [auditd\(8\)](#) for detail explanation of each action and parameters.

Security Diagnosis Tool (Moxa Guardian)

The secure models of Moxa's V3000 Series computer are secure-by-default and certified to IEC 62443-4-2 SL2. However, on many occasions, the default security settings are unintentionally changed and they no longer adhere to the standard, especially when conducting customization development on the computer.

Moxa Guardian is a security diagnosis tool that gives you an overview of the gap between the current security configurations based on the IEC 62443-4-2 Security Level 2 standards and the Moxa recommended security configurations. You can also use the tool to restore the security configurations to the default out-of-box secured configurations.

Use the # **mx-guardian** command to display the menu page.

```
Moxa Guardian is a cli tool allows users to operate security configs

Moxa Guardian is a CLI security diagnosis tool that gives you an overview of
the gap between the current security configurations against the IEC 62443-4-2
Security Level 2 host device requirement and the Moxa recommended security
configurations.

Usage:
  mx-guardian [command]

Available Commands:
  diagnose  Diagnose security settings and output report
  help      Help about any command
  set       Apply a pre-defined security profile
  version   Show Moxa Guardian version and build info

Flags:
  -f, --force      force mode
  -h, --help       help for mx-guardian
  --no-color       disable color
  -q, --quiet      quiet mode (imply force)
  -v, --verbose    verbose mode
  --version        get version

Use "mx-guardian [command] --help" for more information about a command.
```



ATTENTION

As the Moxa computer is an open platform that allows users to install any software they desire, Moxa Guardian's diagnosis tool only compares the current configurations against the default out-of-box IEC 62443-4-2 compliance configurations. For example, if additional protocols are installed, Moxa Guardian will not diagnose such protocols' communication integrity and authenticity capabilities. It is the responsibility of the user to follow the hardening guidelines and the IEC 62443 standard to meet the security requirements.

Diagnosing Issues in the Current Security Configuration

Use # **mx-guardian diagnose <flags>** to initiate a diagnosis of the current security configurations against the default out-of-box secured configuration, which include all IEC 62443-4-2 security level 2 compliance configurations and also additional Moxa recommended security setting not covered in IEC 62443 standard. The diagnosed result are shown in the sequential orders of IEC 62443-4-2 requirement (CR 1.1 to CR 7.8), followed by Moxa's recommended security settings.

Flags	Description
-d or -detail	Show details including the reason and guideline for the failed requirements
-h or -help	Print the help menu for diagnose command
-o or -output <target filepath>	Output the diagnose result to a file

The diagnosis result could be one of the following:

- **PASS:** The device's security configuration meets the IEC 62443-4-2 security level 2 standard or Moxa recommended setting.
- **FAIL:** The device's security configuration fails to meet the IEC 62443-4-2 security level 2 standard or Moxa recommended setting.
- **INFO:** The device's security configuration meet the IEC 62443-4-2 security level 2 standard but additional configuration can be applied if suitable.

An example of Moxa Guardian's diagnosis output is given below:

```
root@moxa-tbbbb1182816:/home/moxa# mx-guardian diagnose -d
INFO[2022-11-14T12:19:33Z] start diagnosing requirement
INFO[2022-11-14T12:19:33Z] diagnose requirement all detail=true

#####
As the Moxa computer is an open platform that allows users to install any software
they desire, Moxa Guardian's diagnosis tool only compares the current configurations
against the default out-of-box IEC-62443-4-2 compliance configurations
#####

CR 1.1: Human user identification and authentication
-----
[+] Precondition
  > Package
    - openssh-server [PASS]
    - openssh-client [PASS]
    - libpam-modules [PASS]
[+] Check
  > Option: SSHD:UsePAM [PASS]
    - info: Check UsePAM is set to yes in sshd
    - guide: Modify or add "UsePAM yes" in /etc/ssh/sshd_config or /etc/ssh/sshd_config.d/*.conf

CR 1.2: Software process and device identification and authentication
-----
[+] Precondition
  > Package
    - openssh-server [PASS]
    - libpam-modules [PASS]
[+] Check
  > Option: SSHD:UsePAM [PASS]
    - info: Check UsePAM is set to yes in sshd
    - guide: Modify or add "UsePAM yes" in /etc/ssh/sshd_config or /etc/ssh/sshd_config.d/*.conf
  > Option: SSHD:PubKeyAuthentication [PASS]
    - info: Check PubkeyAuthentication is set to yes in sshd
    - guide: Modify or add "PubkeyAuthentication yes" in /etc/ssh/sshd_config or
             /etc/ssh/sshd_config.d/*.conf

CR 1.3: Account management
-----
[+] Precondition
  > Package
    - passwd [PASS]

CR 1.4: Identifier management
-----
[+] Precondition
  > Package
    - base-passwd [PASS]
    - passwd [PASS]

CR 1.5: Authenticator management
```

Restoring the Security Configuration to the Default

Use # `mx-guardian set <command> <flags>` to restore the Moxa V3000 Series security configuration to the to the default out-of-box IEC 62443-4-2 compliance secured configurations.

Command	Description
secure	Restore the Moxa V3000 Series configuration to a pre-defined security profile

Flags	Description
-d or -detail	Show details including the reason and guideline for the failed requirements
-h or -help	Print the help menu
-m or --mode <string>	The <string> parameter support 2 values (m1 or m2) Description of each mode is given below : M1: Apply only the IEC 62443-4-2 security level 2 required settings M2: Apply both M1 and Moxa recommended settings <i>Note : M2 is the default out-of-box security setting</i>

An example of restoring the computer's security profile to M2 (IEC 62443-4-2 security level 2 and Moxa recommended settings) is give below:

```
moxa@moxa-tbzkbl090923:~$ sudo mx-guardian set secure -m m2
INFO[2022-11-10T05:53:51Z] start setting secure command
INFO[2022-11-10T05:53:51Z] apply all changes with
force=false mode="IEC62443-4-2 and MOXA suggested settings" quiet=false
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/adduser.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/audit/auditd.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/profile.d/99-moxa-profile.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/security/faillock.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/security/pwquality.conf.d/99-moxa-pwquality.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/login.defs
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/logrotate.d/00-moxa-logrotate.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/ssh/ssh_config.d/00-moxa-ssh.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/sysctl.d/99-moxa-sysctl.conf
INFO[2022-11-10T05:53:51Z] no changes
file=/etc/rsyslog.d/99-moxa-rsyslog.conf
Attention : you must reboot your computer for the changes to take effect
```



ATTENTION

You must reboot your computer for the changes to take effect.

9. Security Hardening Guide

In this chapter, we will provide guidance on how to deploy and operate [Secure model](#) of Moxa V3000 Series computer in a secure manner

Defense-in-depth Strategy

Security Layer	Security Measures	Threat mitigated/handled	Responsibility
Policy and procedure	Establish policies and procedures to guide employee on their role and responsibilities to for safe use of security sensitive assets. Refers to Operation and Maintenance section for some recommendations	Vulnerabilities created due to employee lack of security policies and procedures awareness Malicious code attack that could create or exploit system vulnerabilities (Threat ID #6)	Asset owner (Essential)
Perimeter Security	Use LTE service provide with Carrier Grade NAT (CGNAT) and firewall	Unauthorized and malicious communications from untrusted network	Asset owner (Essential)
	Perimeter firewall	Unauthorized and malicious communications from untrusted network	Asset owner (Essential)
	Physical security (Refers to section Physical Installation)	Physical modification, manipulation, theft, removal, or destruction of asset	Asset owner (Essential)
Network Security	Network IDS/IPS	Network attacks from various sources such as port scanning, DDOS, etc.	Asset owner (Recommended)
	VPN	Man-in-the-middle attacks that allow hackers to intercept and manipulate network traffic (Threat ID #4)	
Endpoint Security	End point Firewall (nftable)	Unauthorized and malicious communications from untrusted network (Threat ID #2 , Threat ID #5)	Provided by Moxa V3000 Series Computer
	Brute-force attacks IPS (fail2ban)	Trial and error attack attempting to crack login credentials (Threat ID #3)	
	Automatic network Connection failover (Refers to MCM failover configuration)	Radio jamming attack (Threat ID #1)	
	Patch management	Vulnerabilities from outdated software could expose to security breach.	
	Secure transmission protocol	Man-in-the-middle attacks that allow hackers to intercept and manipulate network traffic (Threat ID #4)	Asset owner/Moxa V3000 Series Computer (Essential)
	Audit processing failure response	Audit processing failure without appropriate response results in the attacker's activities can go unnoticed, and evidence of whether the attack led to a breach can be inconclusive (Threat ID #7)	
Application Security	IEC 62443-4-1 certified secure design, implementation, validation, and defect management process	Potential vulnerabilities generated from development and testing process that doesn't follow the security best practices.	Provided by Moxa V3000 Series Compute

Security Layer	Security Measures	Threat mitigated/handled	Responsibility
Data Security	Host Intrusion Detection System (AIDE)	Unexpected changes to important files that could potentially lead to security breach.	Provided by Moxa V3000 Series Computer
	Access control and login policy including limit invalid login attempts, automatic session termination and login banner	Unauthorized operation to Moxa V3000 Series computer that could lead to system confidentiality and integrity breach or availability attack.	
	Disk encryption	Access to confidential data in storage without authorization.	
	Secure Boot	Tampering of bootloader, OS kernel and rootFS.	

Table 9.1 – Defense-in-Depth Strategy

*Essential: Security measure that must be taken by asset owner to ensure secure use of Moxa V3000 Series computer
 *Recommended: Security measures that need to be taken by the asset owner if the threats apply.

Potential Threats and Corresponding Security Measures

Below is a list of potential security threats that can harm Moxa's V3000 Series computers and the corresponding security measures that need to be taken by the **asset owner** if the threats apply.

Threat ID	Threat mitigated/handled	Security Measures
1	Radio jamming attack resulting in Wi-Fi and cellular connection DOS	<ul style="list-style-type: none"> For Moxa V3000 Series computer with both Wi-Fi and cellular interface, configure connection failover to use backup connection when primary connection is attack by radio jamming Extend the perimeter of physical security to reduce the impact from radio jamming attack
2	Network data flow through ethernet, Wi-Fi, cellular interface could be potentially interrupted, crashed or stopped by DOS attack	<ul style="list-style-type: none"> Setup network monitoring tool to detect abnormal traffic Configure rate limiting to limit the network traffic
3	SSH server could be potentially interrupted, crashed or stopped by DOS attack	<ol style="list-style-type: none"> Following parameters are set in SSH server configuration file by Moxa as countermeasure. <ul style="list-style-type: none"> ➤ MaxSessions: set to 6 to protect a system from denial of service due to a large number of concurrent sessions ➤ MaxStartups: set to 6:30:60 to protect a system from denial of service due to a large number of pending authentication connection attempts Fail2ban is pre-installed and running in Moxa V3000 Series computer to automatically ban malicious IP
4	Data flowing across ethernet may be sniffed by an attacker	<ol style="list-style-type: none"> Make sure secure protocol with encryption and authentication are used for data transmission (e.g., SSHv2, HTTPS) Install and use VPN for secure data transmission
5	DOS attack from untrusted NTP server when Moxa V Series computer attempt to synchronize time	If public NTP servers without NTS support are used, it is vulnerable to an NTP amplification attack. Attackers could exploit public NTP servers to overwhelm the Moxa V3000 Series computer with UDP traffic. To way to mitigate this, see Mitigate NTP Amplification Attack .
6	Data read from USB or SD card could be spoofed	<ol style="list-style-type: none"> Use sha256 or other checksums tools to check the integrity of the file before installing or transferring it to devices. If the file is a Debian package (.deb), see "How to manually check for package's integrity" to validate the package. Scan the file with Clamav before installing or transferring it to the device Use OpenSSL to verify the signature of the file before installing or transferring to the device.
7	Insufficient auditing storage causing logs to rotate frequently	Store log in external storage or use a centralized log managements system to collect and store the logs from multiple devices. Refers to How to Set Up Centralized Logging on Linux with Rsyslog

Installation

Physical Installation

1. Moxa V3000 Series computer MUST be used to ensure safe use.
2. Moxa V3000 Series computer MUST be protected by physical security that can include CCTV surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, etc. The proper form of physical security should apply depending on the environment and the physical attack risk level.
3. Moxa V3000 Series computer has anti-tamper labels on the enclosures. This allows the administrator to tell whether the device has been tampered with.
4. Moxa V3000 Series computer uses security screw on the enclosures as physical tamper resistance measure to increase the difficulty of probing the product internals in case of physical security breach.
5. Moxa V3000 Series computer MUST not be used to **control** the operation of mission-critical IACS component which failure to maintain control of such device could result in threat to human, safety, environment or massive financial lost.

Environment Requirement

1. If Moxa V3000 Series computer connects to untrust network (e.g., Internet) via ethernet or Wi-Fi, it MUST NOT directly connected to the untrust network, which means a firewall must be setup between ethernet and Wi-Fi connection from Moxa V3000 Series computer and the untrust network.
2. For security-critical applications, we strongly recommend using a private APN for cellular networks.

Access Control

1. The default user account **Moxa** of Linux belongs to the sudo group. Before deploying Moxa V3000 Series computer after development, you must disable this default account and create new account(s) following the least privilege principle, granting only the necessary access right and permission for the intended operation.
2. Each account should be assigned the correct privileges. Moxa Industrial Linux uses Discretionary Access Control (DAC) based on Access Control Lists (ACLs) to manage permissions and privileges. Refers to [Permissions and Privileges Control](#) for details.
3. The default password policy requires the password to be at least 8 characters in length. We strongly recommend keeping the default setting, or you can reduce the password length by adding additional complexity rules to the password, such as special character or numeric character enforcement. Refers to instructions to configure the policy for [Linux](#) and [Bootloader](#), respectively.
4. Update user passwords on a timely manner. For administrator, we recommend refreshing password at least every 3 months.
5. [Bootloader configuration menu](#) comes with a single administrator account shared by all users. Asset owner MUST have access and identity records of the personnel who accessed the bootloader to ensure non-repudiation in case of security breach incidents.
6. Below is a list of all services in Moxa V3000 Series computer uses to connect with external processes and components.

Service	Protocol	Interfaces	Owner (uid/gid)	Authorization Enforcement
SSH server	SSH	Ethernet, cellular, Wi-Fi	root/root	Yes
SFTP server	SSH	Ethernet, cellular, Wi-Fi	root/root	Yes
SCP server	SSH	Ethernet, cellular, Wi-Fi	root/root	Yes
Serial Getty service	RS-232	Serial console port	root/root	Yes
APT client	HTTPS	Ethernet, cellular, Wi-Fi	root/root	Yes
NTP client (NTS support)	TLS/SSL, NTP	Ethernet, cellular, Wi-Fi	root/root	Yes

Security Configuration Check

The secure models of Moxa's V3000 Series computer are secure-by-default and certified to IEC 62443-4-2 SL2. However, on many occasions, the default security settings are unintentionally changed and they no longer adhere to the standard, especially when conducting customization development on the computer.

Moxa Guardian is a security diagnosis tool that gives you an overview of the gap between the current security configurations based on the IEC 62443-4-2 Security Level 2 standards and the Moxa recommended security configurations. Make sure you run the security diagnosis before deploying the product. Refer to [Security Diagnosis Tool](#) section for details usage of Moxa Guardian

Operation

Administrator

1. Disable default account

Use the `passwd` command to lock the default user account so that the **moxa** user cannot log in. Make sure to create a new account before disable the default account

```
moxa@moxa-tbzkb1090923:~# sudo passwd -l moxa
```

2. Disabled interfaces that are not in use

The interfaces that are not in use should be deactivated. Please refer to [Disabled Unused Interface](#) for detailed instructions.

3. Periodically regenerate the SSH server key

Periodically regenerate the SSH server key in order to secure your system in case the key is compromised. Please refer to [Rekey SSH](#)

4. Trusted administrator

Make sure only trusted and reliable persons are registered in the sudo groups for root privilege.

5. Audit failure response

Refer to [Audit Failure Response Guideline](#) to protection of critical system functions in case of audit processing failure

6. System integrity validation

- Frequently run system integrity check to protect your system against malware, viruses and detect unauthorized activities. Refers to [Intrusion Detection System](#) for the utility that come with Moxa V3000 Series computer
- We recommend you reset Moxa V3000 Series computer to [factory default](#) upon receiving it to avoid the risk of potential software tampering before the computer reaches your hand.

7. Only use secure cryptographic

- Moxa Industrial Linux on Moxa V3000 Series computer only uses secure cryptographic that are commonly accepted industry best practices and recommendations as defined in NIST SP 800-57.
- Moxa Industrial Linux installed OpenSSL by default but doesn't disable weak algorithms such as TLS 1.0/1.1 and SSLv3. It is recommended that your application deployed on Moxa Industrial Linux only uses secure algorithms defined in NIST SP 800-57. You can disable the weaker cryptographic algorithm in OpenSSL by setting CipherString = DEFAULT@SECLEVEL=[desired level] in `/etc/ssl/openssl.cnf` to a higher level. For details, see https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_security_level.html

8. Malicious code protection

- Downloading file from untrusted sources is not recommended. If you still want to do it, make sure to verify the file using following recommendation:
 - ❑ Use sha256 or stronger algorithms checksums tools to check the integrity of the file before installing or transferring to device
 - ❑ If the file is Debian package (.deb), follow "[How to manually check for package's integrity](#)" for the instruction.
 - ❑ Use [OpenSSL](#) to verify the signature of the file before installing or transferring to the device.

Administrator and User

1. Periodically refresh password

Update user passwords on a timely manner. For administrator, we recommend refreshing password at least every 3 months

2. Encrypt confidential file

Use GPG to encrypt confidential file or directory with a password in Linux. You can reference [How To Encrypt And Decrypt Files With A Password](#) for quick instructions.

Maintenance

1. Perform Update Frequently

- Perform [software upgrades](#) frequently to enhance features, deploy security patches, or fix bugs.
- We recommend you enable [System Failback Recovery](#) before performing critical update.

2. Perform Backup Frequently

Frequently backup of system on timely manner

3. Examine Audit Logs Frequently

Examine audit logs frequently to detect any anomalies.

4. Report Vulnerability to Moxa

To report vulnerabilities of Moxa products, submit your findings on this web page:
<https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability>.

Decommissioning

1. To avoid any sensitive information such as your account password or certificate from being disclosed, always use the **mx-system-mgmt default decommision** command to reset the computer to factory default and further wipe out all user data, including logs, in an unrecoverable manner before removing the Moxa V3000 Series computer from .

You must use sudo or run the command with the root permission.

```
moxa@moxa-tbzkb1090923:/# sudo mx-system-mgmt default decommision
```

The decommissioning process will do the following actions :

- a. Overwrite the system partition 4 times with [shred](#) so that all user files will be deleted and cannot be recovered.
 - b. Overwrite the log partition 4 times with [shred](#) so that all log files will be deleted and cannot be recovered.
 - c. Trigger the bootloader decommissioning function, so all configurations and log messages in the bootloader are also deleted and cannot be recovered.
2. If asset owner key or sensitive data is stored in the TPM, switch to bootloader [Developer Mode](#) and then perform [Clear TPM](#) action will clear all data stored in TPM

A. Software Process List

Here is a list of Moxa Industrial Linux software processes that can run on the Moxa V3000 Series computer.

Software Process for Administrator	UID	GID
addgnupghome	root	root
addgroup	root	root
add-shell	root	root
adduser	root	root
agetty	root	root
applygnupgdefaults	root	root
arp	root	root
arpd	root	root
audisp-syslog	root	root
auditctl	root	root
auditd	root	root
augenrules	root	root
aureport	root	root
ausearch	root	root
autrace	root	root
badblocks	root	root
blkdeactivate	root	root
blkdiscard	root	root
blkid	root	root
blkzone	root	root
blockdev	root	root
bridge	root	root
capsh	root	root
cfdisk	root	root
chcpu	root	root
chpasswd	root	root
chmem	root	root
chpasswd	root	root
chronyd	root	root
chroot	root	root
cpgr	root	root
cppw	root	root
cracklib-check	root	root
cracklib-format	root	root
cracklib-packer	root	root
cracklib-unpacker	root	root
create-cracklib-dict	root	root
ctrlaltdel	root	root
debugfs	root	root
delgroup	root	root
deluser	root	root
depmod	root	root
devlink	root	root
dhclient	root	root
dhclient-script	root	root
dmsetup	root	root
dmstats	root	root
dnsmasq	root	root
docfdisk	root	root
doc_loadbios	root	root

Software Process for Administrator	UID	GID
dpkg-fsys-usrunmess	root	root
dpkg-preconfigure	root	root
dpkg-reconfigure	root	root
dumpe2fs	root	root
e2freefrag	root	root
e2fsck	root	root
e2image	root	root
e2label	root	root
e2mmpstatus	root	root
e2scrub	root	root
e2scrub_all	root	root
e2undo	root	root
e4crypt	root	root
e4defrag	root	root
faillock	root	root
fdformat	root	root
fdisk	root	root
filefrag	root	root
findfs	root	root
flashcp	root	root
flash_erase	root	root
flash_eraseall	root	root
flash_lock	root	root
flash_otp_dump	root	root
flash_otp_info	root	root
flash_otp_lock	root	root
flash_otp_write	root	root
flash_unlock	root	root
fsck	root	root
fsck.cramfs	root	root
fsck.ext2	root	root
fsck.ext3	root	root
fsck.ext4	root	root
fsck.minix	root	root
fsfreeze	root	root
fstab-decode	root	root
fstrim	root	root
ftl_check	root	root
ftl_format	root	root
genl	root	root
getcap	root	root
getpcaps	root	root
getty	root	root
groupadd	root	root
groupdel	root	root
groupmems	root	root
groupmod	root	root
grpck	root	root
grpconv	root	root
grpunconv	root	root
halt	root	root
hwclock	root	root
iconvconfig	root	root
ifconfig	root	root
ifdown	root	root
ifquery	root	root
ifup	root	root
init	root	root

Software Process for Adminstrator	UID	GID
insmod	root	root
installkernel	root	root
invoke-rc.d	root	root
ip	root	root
ipmaddr	root	root
iptunnel	root	root
isosize	root	root
iw	root	root
jffs2dump	root	root
jffs2reader	root	root
killall5	root	root
ldattach	root	root
ldconfig	root	root
locale-gen	root	root
logrotate	root	root
logsave	root	root
losetup	root	root
lsmod	root	root
lsmttd	root	root
lxftp	root	root
mcmd	root	root
mii-tool	root	root
mke2fs	root	root
mkfs	root	root
mkfs.bfs	root	root
mkfs.cramfs	root	root
mkfs.ext2	root	root
mkfs.ext3	root	root
mkfs.ext4	root	root
mkfs.jffs2	root	root
mkfs.minix	root	root
mkfs.ubifs	root	root
mkhomedir_helper	root	root
mklost+found	root	root
mkswap	root	root
ModemManager	root	root
modinfo	root	root
modprobe	root	root
MoxaComputerInterfaceManager	root	root
moxa-telit-firmware-upgrade-tool	root	root
mtdd_debug	root	root
mtddinfo	root	root
mtddpart	root	root
mx-bootloader-mgmt	root	root
mx-connect-mgmt	root	root
mx-guardian	root	root
mx-guardian-init	root	root
mx-system-mgmt	root	root
nameif	root	root
nanddump	root	root
nandtest	root	root
nandwrite	root	root
NetworkManager	root	root
newusers	root	root
nft	root	root
nftldump	root	root
nftl_format	root	root
nologin	root	root

Software Process for Administrator	UID	GID
pam-auth-update	root	root
pam_getenv	root	root
pam_timestamp_check	root	root
parted	root	root
partprobe	root	root
pivot_root	root	root
plipconfig	root	root
poweroff	root	root
pwck	root	root
pwconv	root	root
pwunconv	root	root
rarp	root	root
raw	root	root
readprofile	root	root
reboot	root	root
recv_image	root	root
regdbdump	root	root
remove-shell	root	root
resize2fs	root	root
rfdump	root	root
rfdformat	root	root
rmmod	root	root
rmt	root	root
rmt-tar	root	root
route	root	root
rsyslogd	root	root
rtacct	root	root
rtcwake	root	root
rtmon	root	root
runlevel	root	root
runuser	root	root
serve_image	root	root
service	root	root
setcap	root	root
sfdisk	root	root
shadowconfig	root	root
shutdown	root	root
slattach	root	root
sshd	root	root
start-stop-daemon	root	root
sudo_logsrvd	root	root
sudo_sendlog	root	root
sulogin	root	root
sumtool	root	root
swaplabel	root	root
swapoff	root	root
swapon	root	root
switch_root	root	root
sysctl	root	root
tarcat	root	root
tc	root	root
telinit	root	root
tipc	root	root
tune2fs	root	root
tzconfig	root	root
ubiattach	root	root
ubiblock	root	root
ubicrc32	root	root

Software Process for Adminstrator	UID	GID
ubidetach	root	root
ubiformat	root	root
ubihealthd	root	root
ubimkvol	root	root
ubinfo	root	root
ubinize	root	root
ubirename	root	root
ubirmvol	root	root
ubirsvol	root	root
ubiupdatevol	root	root
unix_chkpwd	root	shadow
unix_update	root	root
update-ca-certificates	root	root
update-cracklib	root	root
update-locale	root	root
update-passwd	root	root
update-rc.d	root	root
useradd	root	root
userdel	root	root
usermod	root	root
validlocale	root	root
vigr	root	root
vipw	root	root
visudo	root	root
vnstatd	root	root
watchdog	root	root
wd_identify	root	root
wd_keepalive	root	root
wipefs	root	root
wpa_action	root	root
wpa_cli	root	root
wpa_supplicant	root	root
zic	root	root
zramctl	root	root

Software Process for Non-Adminstrator	UID	GID
addpart	root	root
addr2line	root	root
aide	root	root
apt	root	root
apt-cache	root	root
apt-cdrom	root	root
apt-config	root	root
apt-extracttemplates	root	root
apt-ftpparchive	root	root
apt-get	root	root
apt-key	root	root
apt-mark	root	root
apt-sortpkgs	root	root
ar	root	root
arch	root	root
arm-linux-gnueabi-hf-addr2line	root	root
arm-linux-gnueabi-hf-ar	root	root
arm-linux-gnueabi-hf-as	root	root
arm-linux-gnueabi-hf-c++filt	root	root
arm-linux-gnueabi-hf-dwp	root	root
arm-linux-gnueabi-hf-elfedit	root	root

Software Process for Non-Administrator	UID	GID
arm-linux-gnueabi-hf-gold	root	root
arm-linux-gnueabi-hf-gprof	root	root
arm-linux-gnueabi-hf-ld	root	root
arm-linux-gnueabi-hf-ld.bfd	root	root
arm-linux-gnueabi-hf-ld.gold	root	root
arm-linux-gnueabi-hf-nm	root	root
arm-linux-gnueabi-hf-objcopy	root	root
arm-linux-gnueabi-hf-objdump	root	root
arm-linux-gnueabi-hf-ranlib	root	root
arm-linux-gnueabi-hf-readelf	root	root
arm-linux-gnueabi-hf-size	root	root
arm-linux-gnueabi-hf-strings	root	root
arm-linux-gnueabi-hf-strip	root	root
as	root	root
asc2log	root	root
aulast	root	root
aulastlog	root	root
ausyscall	root	root
auvirt	root	root
awk	root	root
b2sum	root	root
base32	root	root
base64	root	root
basename	root	root
basenc	root	root
bash	root	root
bashbug	root	root
bcmserver	root	root
bootctl	root	root
busctl	root	root
cal	root	root
canbusload	root	root
can-calc-bit-timing	root	root
candump	root	root
canfdtest	root	root
cangen	root	root
cangw	root	root
canlogserver	root	root
canplayer	root	root
cansend	root	root
cansequence	root	root
cansniffer	root	root
captoinfo	root	root
cat	root	root
catchsegv	root	root
c++filt	root	root
chacl	root	root
chage	root	shadow
chatr	root	root
chcon	root	root
chfn	root	root
chgrp	root	root
chmod	root	root
choom	root	root
chown	root	root
chronyc	root	root
chrt	root	root

Software Process for Non-Administrator	UID	GID
chsh	root	root
cksum	root	root
clear	root	root
clear_console	root	root
cmp	root	root
col	root	root
colcrt	root	root
colrm	root	root
column	root	root
comm	root	root
corelist	root	root
cp	root	root
cpan	root	root
cpan5.32-arm-linux-gnueabi	root	root
cpulimit	root	root
c_rehash	root	root
csplit	root	root
ctstat	root	root
curl	root	root
cut	root	root
cvtsudoers	root	root
dash	root	root
date	root	root
dbus-cleanup-sockets	root	root
dbus-daemon	root	root
dbus-monitor	root	root
dbus-run-session	root	root
dbus-send	root	root
dbus-update-activation-environment	root	root
dbus-uuidgen	root	root
dd	root	root
debconf	root	root
debconf-apt-progress	root	root
debconf-communicate	root	root
debconf-copydb	root	root
debconf-escape	root	root
debconf-set-selections	root	root
debconf-show	root	root
debsums	root	root
deb-systemd-helper	root	root
deb-systemd-invoke	root	root
delpart	root	root
df	root	root
dh_bash-completion	root	root
dialog	root	root
diff	root	root
diff3	root	root
dir	root	root
dircolors	root	root
dirmngr	root	root
dirmngr-client	root	root
dirname	root	root
dmesg	root	root
dnsdomainname	root	root
domainname	root	root
dpkg	root	root
dpkg-deb	root	root

Software Process for Non-Administrator	UID	GID
dpkg-divert	root	root
dpkg-maintscript-helper	root	root
dpkg-query	root	root
dpkg-realpath	root	root
dpkg-split	root	root
dpkg-statoverride	root	root
dpkg-trigger	root	root
du	root	root
dumpimage	root	root
dwp	root	root
echo	root	root
editor	root	root
egrep	root	root
elfedit	root	root
enc2xs	root	root
encguess	root	root
env	root	root
ex	root	root
expand	root	root
expiry	root	shadow
expr	root	root
factor	root	root
fail2ban-client	root	root
fail2ban-python	root	root
fail2ban-regex	root	root
fail2ban-server	root	root
fail2ban-testcases	root	root
faillog	root	root
fallocate	root	root
FALSE	root	root
fgrep	root	root
file	root	root
fincore	root	root
find	root	root
findmnt	root	root
flock	root	root
fmt	root	root
fold	root	root
free	root	root
fw_printenv	root	root
fw_setenv	root	root
getconf	root	root
getent	root	root
getfacl	root	root
getopt	root	root
gold	root	root
gpasswd	root	root
gpg	root	root
gpg-agent	root	root
gpgcompose	root	root
gpgconf	root	root
gpg-connect-agent	root	root
gpgparsemail	root	root
gpgsm	root	root
gpgsplit	root	root
gpgtar	root	root
gpgv	root	root

Software Process for Non-Administrator	UID	GID
gpg-wks-server	root	root
gpg-zip	root	root
gprof	root	root
grep	root	root
groups	root	root
gunzip	root	root
gzexe	root	root
gzip	root	root
h2ph	root	root
h2xs	root	root
hd	root	root
head	root	root
helpztags	root	root
hexdump	root	root
hostid	root	root
hostname	root	root
hostnamectl	root	root
iconv	root	root
id	root	root
infocmp	root	root
infotocap	root	root
install	root	root
instmodsh	root	root
ionice	root	root
ip	root	root
ipcmk	root	root
ipcrm	root	root
ipcs	root	root
ischroot	root	root
isotpdump	root	root
isotpperf	root	root
isotprecv	root	root
isotpsend	root	root
isotpserver	root	root
isotpsniffer	root	root
isotptun	root	root
j1939acd	root	root
j1939cat	root	root
j1939spy	root	root
j1939sr	root	root
join	root	root
journalctl	root	root
jq	root	root
json_pp	root	root
kbxutil	root	root
kernel-install	root	root
kill	root	root
kmod	root	root
kwboot	root	root
last	root	root
lastb	root	root
lastlog	root	root
lcf	root	root
ld	root	root
ld.bfd	root	root
ldd	root	root
ld.gold	root	root

Software Process for Non-Administrator	UID	GID
libnetcfg	root	root
link	root	root
linux32	root	root
linux64	root	root
ln	root	root
Instat	root	root
locale	root	root
localectl	root	root
localedef	root	root
log2asc	root	root
log2long	root	root
logger	root	root
login	root	root
loginctl	root	root
logname	root	root
look	root	root
ls	root	root
lsattr	root	root
lsblk	root	root
lscpu	root	root
lsipc	root	root
lslocks	root	root
lslogins	root	root
lsmem	root	root
lsmod	root	root
lsns	root	root
lspgpot	root	root
mawk	root	root
mcookie	root	root
md5sum	root	root
md5sum.textutils	root	root
mesg	root	root
migrate-pubring-from-classic-gpg	root	root
mkdir	root	root
mkenvimage	root	root
mkfifo	root	root
mkimage	root	root
mknod	root	root
mksunxiboot	root	root
mktemp	root	root
mmcli	root	root
more	root	root
mount	root	root
mountpoint	root	root
mv	root	root
mx-interface-mgmt	root	root
mx-ver	root	root
namei	root	root
nawk	root	root
ncal	root	root
netstat	root	root
networkctl	root	root
newgrp	root	root
nice	root	root
nisdomainname	root	root
nl	root	root
nm	root	root

Software Process for Non-Administrator	UID	GID
nmcli	root	root
nm-online	root	root
nmtui	root	root
nmtui-connect	root	root
nmtui-edit	root	root
nmtui-hostname	root	root
nohup	root	root
nproc	root	root
nsenter	root	root
nstat	root	root
numfmt	root	root
objcopy	root	root
objdump	root	root
od	root	root
openssl	root	root
pager	root	root
partx	root	root
passwd	root	root
paste	root	root
pathchk	root	root
pdb3	root	root
pdb3.9	root	root
perl	root	root
perl5.32.1	root	root
perl5.32-arm-linux-gnueabi	root	root
perlbug	root	root
perldoc	root	root
perlvp	root	root
perlthanks	root	root
pgrep	root	root
piconv	root	root
pidof	root	root
pidwait	root	root
pinentry	root	root
pinentry-curses	root	root
ping	root	root
ping4	root	root
ping6	root	root
pinky	root	root
pkaction	root	root
pkcheck	root	root
pkexec	root	root
pkill	root	root
pktyagent	root	root
pl2pm	root	root
pldd	root	root
pmap	root	root
pod2html	root	root
pod2man	root	root
pod2text	root	root
pod2usage	root	root
podchecker	root	root
pr	root	root
printenv	root	root
printf	root	root
prlimit	root	root
prove	root	root

Software Process for Non-Administrator	UID	GID
ps	root	root
ptar	root	root
ptardiff	root	root
ptargrep	root	root
ptx	root	root
pv	root	root
pwd	root	root
pwdx	root	root
py3clean	root	root
py3compile	root	root
py3versions	root	root
pydoc3	root	root
pydoc3.9	root	root
pygettext3	root	root
pygettext3.9	root	root
python3	root	root
python3.9	root	root
ranlib	root	root
rbash	root	root
rcp	root	root
rdebsums	root	root
rdma	root	root
readelf	root	root
readlink	root	root
realpath	root	root
renice	root	root
reset	root	root
resizepart	root	root
resolvectl	root	root
rev	root	root
rgrep	root	root
rlogin	root	root
rm	root	root
rmdir	root	root
route	root	root
route	root	root
routel	root	root
rrsync	root	root
rsh	root	root
rsync	root	root
rsync-ssl	root	root
rtstat	root	root
runcon	root	root
run-parts	root	root
rview	root	root
rvim	root	root
savelog	root	root
scp	root	root
script	root	root
scriptlive	root	root
scriptreplay	root	root
sdiff	root	root
sed	root	root
select-editor	root	root
sensible-browser	root	root
sensible-editor	root	root
sensible-pager	root	root
seq	root	root

Software Process for Non-Administrator	UID	GID
setarch	root	root
setfacl	root	root
setpriv	root	root
setsid	root	root
setterm	root	root
sftp	root	root
sg	root	root
sh	root	root
sha1sum	root	root
sha224sum	root	root
sha256sum	root	root
sha384sum	root	root
sha512sum	root	root
shasum	root	root
shred	root	root
shuf	root	root
size	root	root
skill	root	root
slabtop	root	root
slcan_attach	root	root
slcand	root	root
slcanpty	root	root
sleep	root	root
slogin	root	root
snice	root	root
sort	root	root
splain	root	root
split	root	root
ss	root	root
ssh	root	root
ssh-add	root	root
ssh-agent	root	ssh
ssh-argv0	root	root
ssh-copy-id	root	root
ssh-keygen	root	root
ssh-keyscan	root	root
stat	root	root
stdbuf	root	root
streamzip	root	root
strings	root	root
strip	root	root
stty	root	root
su	root	root
sudo	root	root
sudocedit	root	root
sudoreplay	root	root
sum	root	root
sync	root	root
systemctl	root	root
systemd	root	root
systemd-analyze	root	root
systemd-ask-password	root	root
systemd-cat	root	root
systemd-cgls	root	root
systemd-cgtop	root	root
systemd-delta	root	root
systemd-detect-virt	root	root

Software Process for Non-Administrator	UID	GID
systemd-escape	root	root
systemd-hwdb	root	root
systemd-id128	root	root
systemd-inhibit	root	root
systemd-machine-id-setup	root	root
systemd-mount	root	root
systemd-notify	root	root
systemd-path	root	root
systemd-resolve	root	root
systemd-run	root	root
systemd-socket-activate	root	root
systemd-stdio-bridge	root	root
systemd-sysusers	root	root
systemd-tmpfiles	root	root
systemd-tty-ask-password-agent	root	root
systemd-umount	root	root
tabs	root	root
tac	root	root
tail	root	root
tar	root	root
taskset	root	root
tee	root	root
tempfile	root	root
test	root	root
testj1939	root	root
tic	root	root
timedatectl	root	root
timeout	root	root
tload	root	root
toe	root	root
top	root	root
touch	root	root
tpm2	root	root
tpm2_activatecredential	root	root
tpm2_certify	root	root
tpm2_certifycreation	root	root
tpm2_certifyX509certutil	root	root
tpm2_changeauth	root	root
tpm2_changeeps	root	root
tpm2_changepps	root	root
tpm2_checkquote	root	root
tpm2_clear	root	root
tpm2_clearcontrol	root	root
tpm2_clockrateadjust	root	root
tpm2_commit	root	root
tpm2_create	root	root
tpm2_createak	root	root
tpm2_createek	root	root
tpm2_createpolicy	root	root
tpm2_createprimary	root	root
tpm2_dictionarylockout	root	root
tpm2_duplicate	root	root
tpm2_ecdhkeygen	root	root
tpm2_ecdhzgen	root	root
tpm2_ecephemeral	root	root
tpm2_encryptdecrypt	root	root
tpm2_eventlog	root	root

Software Process for Non-Administrator	UID	GID
tpm2_evictcontrol	root	root
tpm2_flushcontext	root	root
tpm2_getcap	root	root
tpm2_getcommandauditdigest	root	root
tpm2_geteccparameters	root	root
tpm2_getekcertificate	root	root
tpm2_getrandom	root	root
tpm2_getsessionauditdigest	root	root
tpm2_gettestresult	root	root
tpm2_gettime	root	root
tpm2_hash	root	root
tpm2_hierarchycontrol	root	root
tpm2_hmac	root	root
tpm2_import	root	root
tpm2_incrementalselftest	root	root
tpm2_load	root	root
tpm2_loadexternal	root	root
tpm2_makecredential	root	root
tpm2_nvcertify	root	root
tpm2_nvdefine	root	root
tpm2_nvextend	root	root
tpm2_nvincrement	root	root
tpm2_nvread	root	root
tpm2_nvreadlock	root	root
tpm2_nvreadpublic	root	root
tpm2_nvsetbits	root	root
tpm2_nvundefine	root	root
tpm2_nvwrite	root	root
tpm2_nvwritelock	root	root
tpm2_pcrallocate	root	root
tpm2_pcrevent	root	root
tpm2_pcrextend	root	root
tpm2_pcrread	root	root
tpm2_pcrreset	root	root
tpm2_policyauthorize	root	root
tpm2_policyauthorizenv	root	root
tpm2_policyauthvalue	root	root
tpm2_policycommandcode	root	root
tpm2_policycountertimer	root	root
tpm2_policycphash	root	root
tpm2_policyduplicationselect	root	root
tpm2_policylocality	root	root
tpm2_policynamehash	root	root
tpm2_policynv	root	root
tpm2_policynvwritten	root	root
tpm2_policyor	root	root
tpm2_policypassword	root	root
tpm2_policypcr	root	root
tpm2_policyrestart	root	root
tpm2_policysecret	root	root
tpm2_policysigned	root	root
tpm2_policytemplate	root	root
tpm2_policyticket	root	root
tpm2_print	root	root
tpm2_quote	root	root
tpm2_rc_decode	root	root
tpm2_readclock	root	root

Software Process for Non-Administrator	UID	GID
tpm2_readpublic	root	root
tpm2_rsadecrypt	root	root
tpm2_rsaencrypt	root	root
tpm2_selftest	root	root
tpm2_send	root	root
tpm2_setclock	root	root
tpm2_setcommandauditstatus	root	root
tpm2_setprimarypolicy	root	root
tpm2_shutdown	root	root
tpm2_sign	root	root
tpm2_startauthsession	root	root
tpm2_startup	root	root
tpm2_stirrandom	root	root
tpm2_testparms	root	root
tpm2_unseal	root	root
tpm2_verifysignature	root	root
tpm2_zgen2phase	root	root
tput	root	root
tr	root	root
TRUE	root	root
truncate	root	root
tset	root	root
tsort	root	root
tty	root	root
tzselect	root	root
ucf	root	root
ucfq	root	root
ucfr	root	root
udevadm	root	root
ul	root	root
umount	root	root
uname	root	root
uncompress	root	root
unexpand	root	root
uniq	root	root
unlink	root	root
unshare	root	root
update-alternatives	root	root
uptime	root	root
users	root	root
utmpdump	root	root
vdir	root	root
vi	root	root
view	root	root
vim	root	root
vim.basic	root	root
vimdiff	root	root
vimtutor	root	root
vmstat	root	root
vnstat	root	root
w	root	root
wall	root	tty
watch	root	root
watchgnupg	root	root
wc	root	root
wdctl	root	root
wget	root	root

Software Process for Non-Administrator	UID	GID
whereis	root	root
which	root	root
whiptail	root	root
who	root	root
whoami	root	root
wpa_passphrase	root	root
write	root	root
write.ul	root	tty
xargs	root	root
xsubpp	root	root
xxd	root	root
yes	root	root
ypdomainname	root	root
zcat	root	root
zcmp	root	root
zdiff	root	root
zdump	root	root
zegrep	root	root
zfgrep	root	root
zforce	root	root
zgrep	root	root
zipdetails	root	root
zless	root	root
zmore	root	root
znew	root	root