

V1200 Series User Manual

Version 3.0, December 2025

www.moxa.com/products



© 2025 Moxa Inc. All rights reserved.

V1200 Series User Manual

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	5
Package Checklist	5
Product Features	5
Product Specifications	5
Supported Firmware Version	6
2. Hardware Introduction	7
Appearance.....	7
V1202-CT-T.....	7
V1222-CT-T.....	7
V1222-W-CT-T.....	8
Dimensions	8
Wall Mounting (default).....	8
Desk Mounting (optional)	9
DIN-rail Mounting (optional)	9
LED Indicators.....	10
Installation Options.....	10
Wall Mounting (default).....	10
Desk Mounting (optional)	11
DIN-rail Mounting (optional)	12
3. Hardware Connection Description	13
Wiring Requirements.....	13
Connecting the Power	14
Grounding the Computer	14
Connecting the Network	15
Connecting a USB Device.....	15
Connecting Serial Ports	16
Inserting the SIM Card	16
Inserting a MicroSD Card.....	17
Connecting the Console Port	17
Installing Wireless Modules	18
Installing Cables and Antennas	20
4. Getting Started	22
Disabling the Web-based Network Configuration Tool	22
Access to the Web Console	23
5. Web Console	24
Dashboard	24
System Dashboard	24
Network Dashboard	24
Tag Dashboard	26
System Settings	27
General.....	27
Serial.....	29
External Storage	30
SNMP Agent	31
Network Settings	32
Ethernet.....	32
Cellular	34
Wi-Fi Client.....	37
Network Management	38
VRRP	39
Security.....	42
Certificate Center	42
Firewall	42
HTTPS.....	45
Login Lockout	46
Session Management	46
OpenVPN Client.....	47
System Use Notification	48

Account Management	49
Accounts	49
Roles	50
Password Policy.....	51
Maintenance	52
Service	52
Reboot.....	52
Config. Import/Export.....	53
Backup & Restore.....	53
Software Upgrade	54
Reset to Default	55
Device Retirement.....	56
Diagnostics	56
System Log	56
Audit Log	57
A. Security Hardening Guide	58
Security Best Practices.....	58
Physical Installation Guidelines.....	59
Account Management Guidelines	59
Protecting Vulnerable Network Ports	60
Maintaining Communication Integrity	60
Maintaining Communication Integrity	60
Communication Integrity Features.....	60
VPN (Virtual Private Network)	60
HTTPS (Hypertext Transfer Protocol Secure)	61
SSH (Secure Shell)	61
Device Access Control Best Practices.....	61
About Device Integrity and Authenticity.....	61
Configuration Backup and Encryption.....	61
Secure Boot.....	62
Device Resource Monitoring	62
Device Resource Monitoring.....	62
Event Logs	62
Recommended Settings for Services and Features	63
Common Threats and Countermeasures	64
Recommended Operational Roles and Duties.....	64
admin	65
Recommended Patching and Backup Practices.....	65
Recommended Patching and Backup Practices	65
Firmware Upgrade.....	65
Configuration Backup.....	65
Recommendations for Vulnerability Management.....	66
Recommendations for Secure Disposal	66
B. Regulatory Approval Statements	67

1. Introduction

The V1200 computing platform is designed for railway TCMS data-acquisition and train-to-ground applications. The computer comes with dual M12 10/100/1000 Mbps Ethernet ports, built-in 5G and Wi-Fi 6 modules and dual RS-232/422/485 serial ports. The slim, compact design with multiple mounting options reduces installation space and provides flexibility for mounting in various cabinets or onboard locations. The wireless enabled models are thoroughly tested in a testing chamber, guaranteeing that the wireless-enabled computing platforms meet EN50155 OT4 requirements and are suitable for wide-temperature applications.

Each unit is equipped with Moxa Industrial Linux (MIL) for long-term Linux support and vulnerability patching. A web-based interface is provided for easy configuration of Ethernet and wireless network settings without the need for programming.

Package Checklist

Before installing a V1200 computer, verify that the package contains the following items:

- 1 x V1200 Series computer
- 1 x Wall-mounting kit
- 1 x Quick installation guide (printed)
- 1 x Warranty card (printed)



NOTE

Notify your sales representative if any of the above items are missing or damaged.

Product Features

- Arm Cortex-A53 quad-core 1.6 GHz processor
- Integrated 5G Sub-6GHz NR module and Wi-Fi 6 module with dual SIM
- Slim, compact design with multiple mounting options
- Isolated power with 24 to 110 VDC power supply range
- Moxa Industrial Linux built-in for long-term Linux support
- TPM 2.0 built-in
- Developed according to the IEC 62443-4-1 certified software development life cycle to enhance cybersecurity
- Meets EN 50155 OT4* operating temperature (-40 to 70°C with cellular and Wi-Fi modules enabled)

* The EN50155 OT4 test was performed in a sealed environment without any fans or airflow. The 5G module was kept connected at a moderate transmission power level, the Wi-Fi modules continuously sent pings, and the CPU loading was around 95%. The test lasted over four hours until the device temperature reached a steady state.

Product Specifications



NOTE

The latest specifications for Moxa's products can be found at <https://www.moxa.com>.

Supported Firmware Version

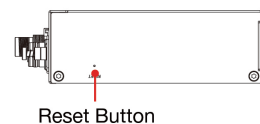
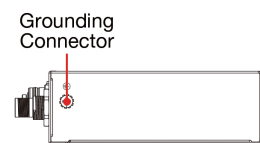
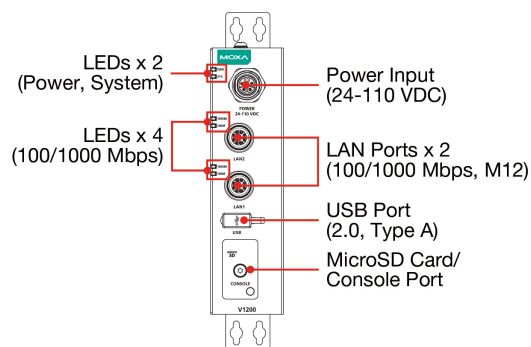
This instructions in this manual are based on firmware version v1.2. For configuration instructions, primarily focusing on the Web UI features available in this release, see the Getting Started section.

2. Hardware Introduction

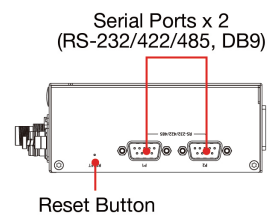
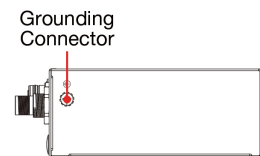
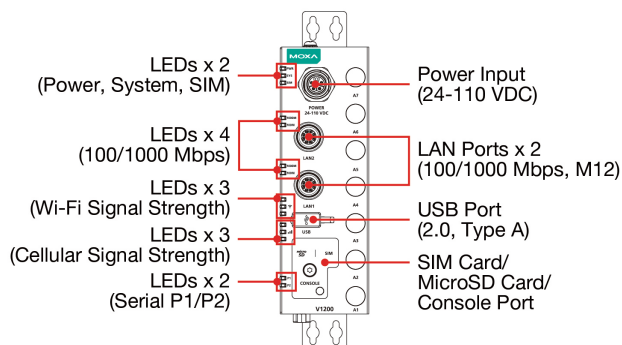
The V1200 computer is compact and designed to be rugged enough for industrial applications. This chapter provides information on the appearance and dimensions of the V1200 and describes the LED indicators that can help you monitor system performance and identify issues. The multiple installation options allow you to find the most suitable installation method for your site and ensure the correct installation of computer.

Appearance

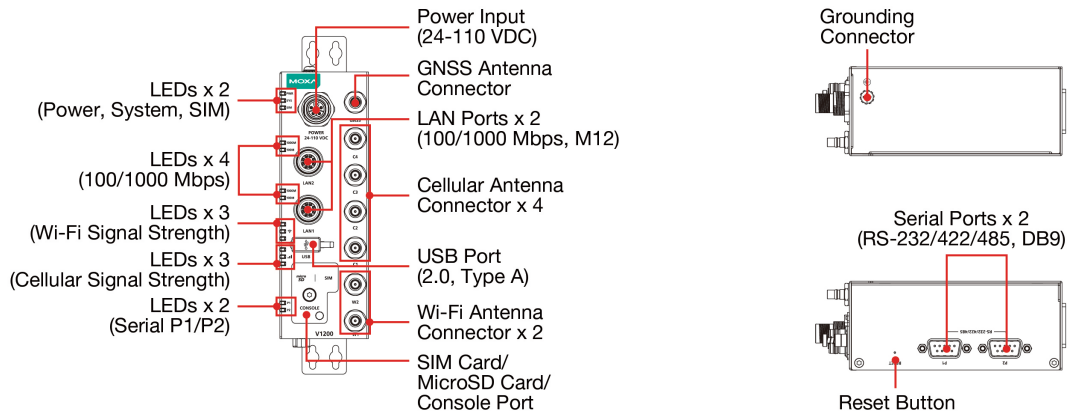
V1202-CT-T



V1222-CT-T



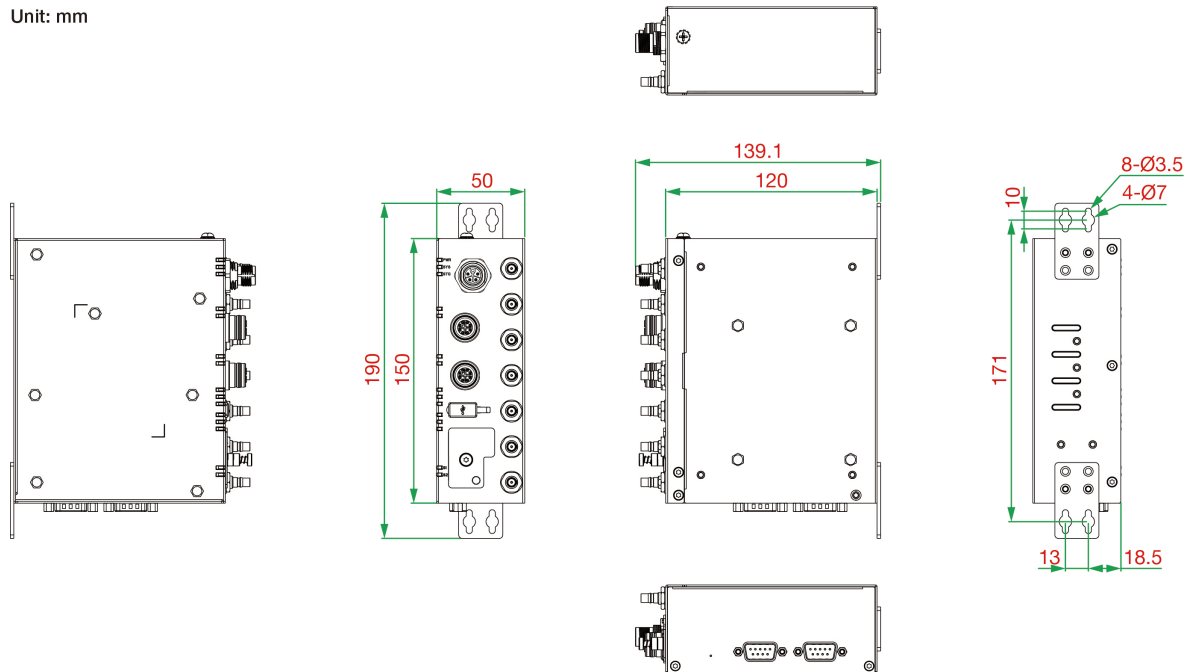
V1222-W-CT-T



Dimensions

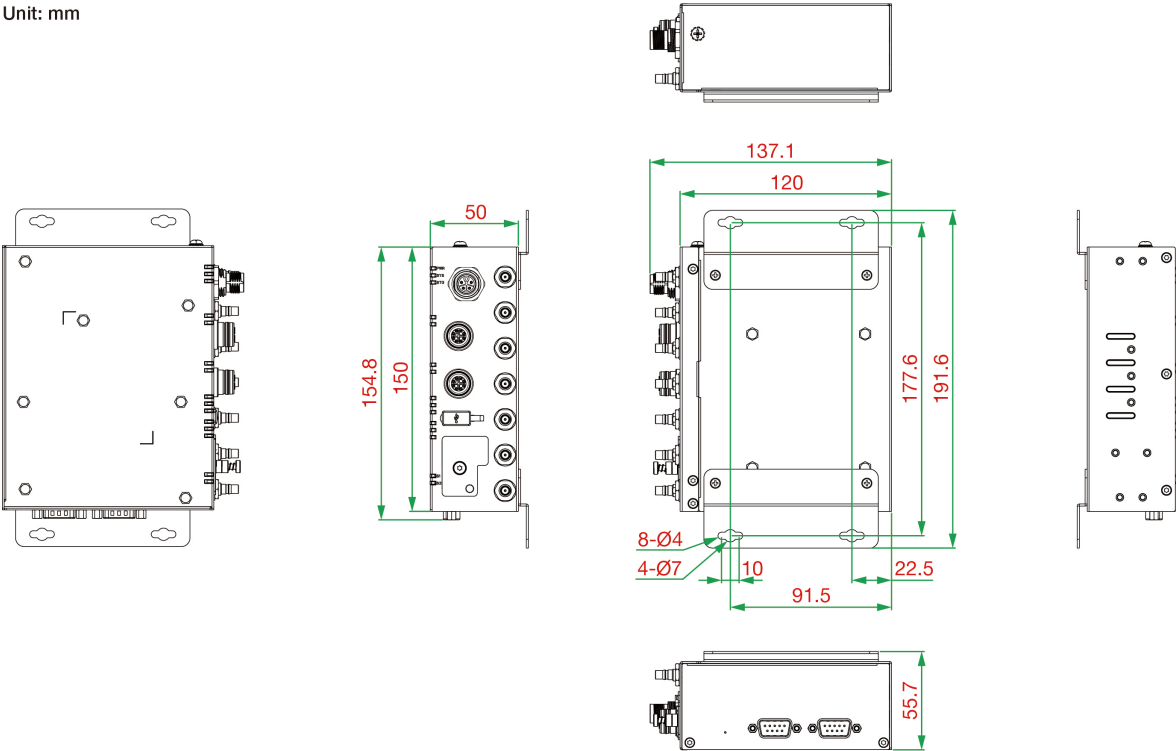
Wall Mounting (default)

Unit: mm



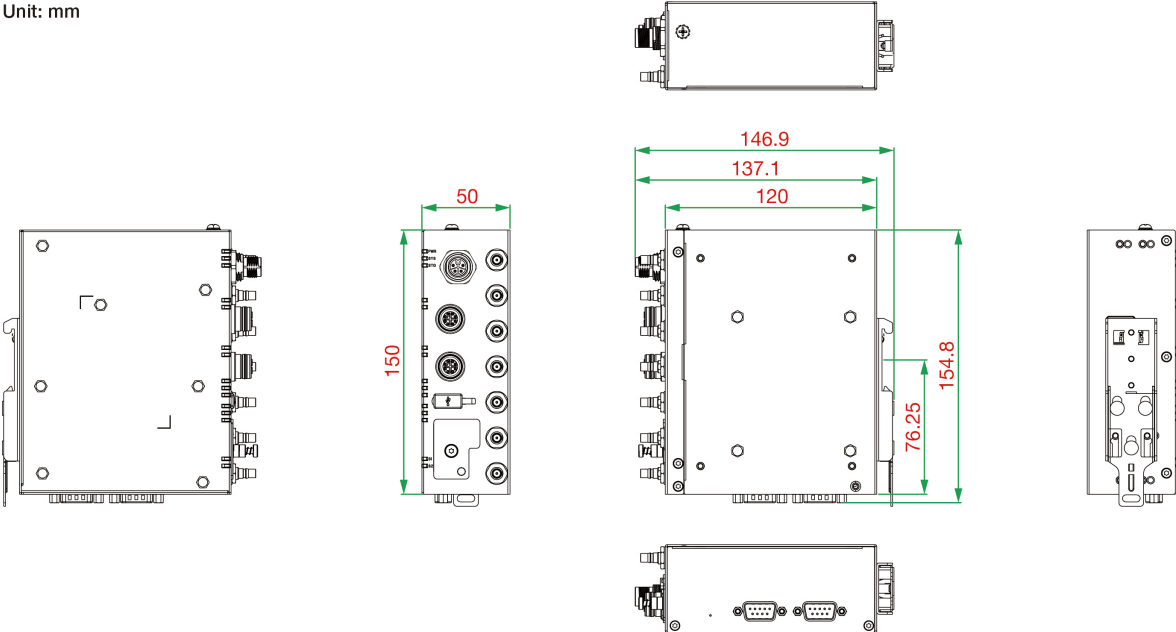
Desk Mounting (optional)

Unit: mm



DIN-rail Mounting (optional)

Unit: mm



LED Indicators

The function of each LED is described in the table below:

LED Name	Color	LED Status	Description
PWR	Green	Steady on	Power is on
	Off	Off	No power
SYS	Green	Steady on	Device has booted successfully (all system services are initialized)
	Green	Blinking	Device is in the process of booting up
	Red	Steady on	Device boot up failed (one or more system services failed to initialize)
	Off	Off	The device is still in the bootloader stage; is not booted into the kernel yet
LAN	Green	Steady on	100 Mbps Ethernet link
		Blinking	Data is being transmitted or received
	Yellow	Steady on	1000 Mbps Ethernet link
		Blinking	Data is being transmitted or received
	Off	Off	The Ethernet cable is disconnected

Installation Options



NOTE

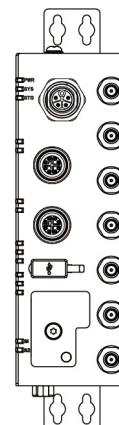
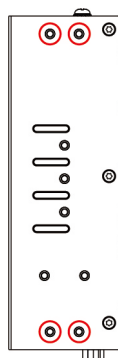
For IP40 compliance, the cover of the SD card, SIM card, and console port, should be secured properly with screws.

Ensure that the USB port is covered with the rubber cap if it is not in use.

The V1200 Series can be mounted on to a DIN rail, a wall, or installed on a desk. The wall-mounting kit is included in the product package by default. If you want to use another mounting method, you will need to order the optional DIN-rail mounting or desk-mounting kits separately. Contact a Moxa sales representative to place an order.

Wall Mounting (default)

The wall-mounting kit is included in the product package by default. To attach the wall-mounting brackets, first align them to the apertures on the back panel of the V1200 and fasten the four M3 screws (torque value of 4.5 ± 0.5 kgf-cm) included in the package to secure the mounting brackets.

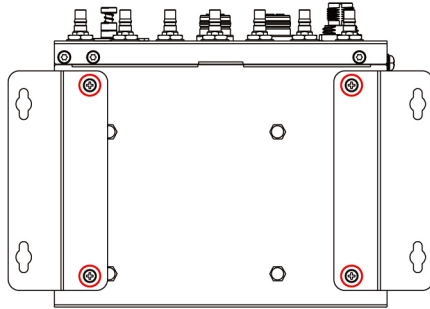


To mount the V1200 on to a wall, use four M3 x 6 mm screws and a torque value of 4.5 ± 0.5 kgf-cm. See *Additional Screws for Wall and Desk Mounting*.

Desk Mounting (optional)

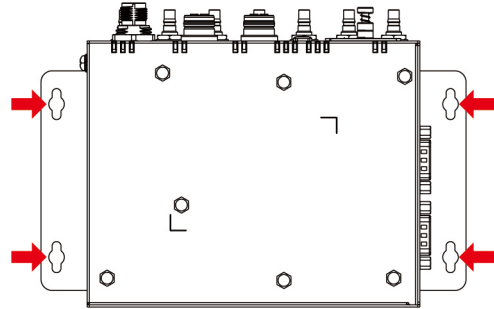
Step 1

Use the four screws (M3 x 5 mm) in the package to fasten the wall-mounting brackets to the computer.



Step 2

Use another four screws (M3 x 6 mm) to mount the computer on to a wall or in a cabinet.



To fix the V1200 on to a desk, use four M3 x 6 mm screws and a torque value of 4.5 ± 0.5 kgf-cm. See *Additional Screws for Wall and Desk Mounting*.



NOTE

- Test the screw head and shank size by inserting the screws into one of the keyhole shaped apertures of the wall-mounting plates before attaching the plate to the wall.
- Do not drive the screws in all the way—leave a space of about 2 mm to allow room for sliding the wall mount panel between the wall and the screws.

Additional Screws for Wall and Desk Mounting

You will require additional screw for mounting the V1200 with the mounting brackets on to a wall or a desk. These screws are not included in the mounting kit package and must be purchased separately. The specifications of the additional screws required are as follows:

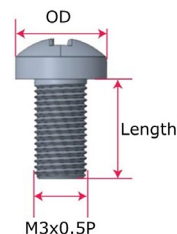
Head Type: Pan/Dome

Head Diameter $5.2 \text{ mm} < OD < 7.0 \text{ mm}$

Length $> 6 \text{ mm}$

Thread Size: M3 x 0.5P

Recommended Fastening Torque: $4.5 \pm 0.5 \text{ kgf-cm}$



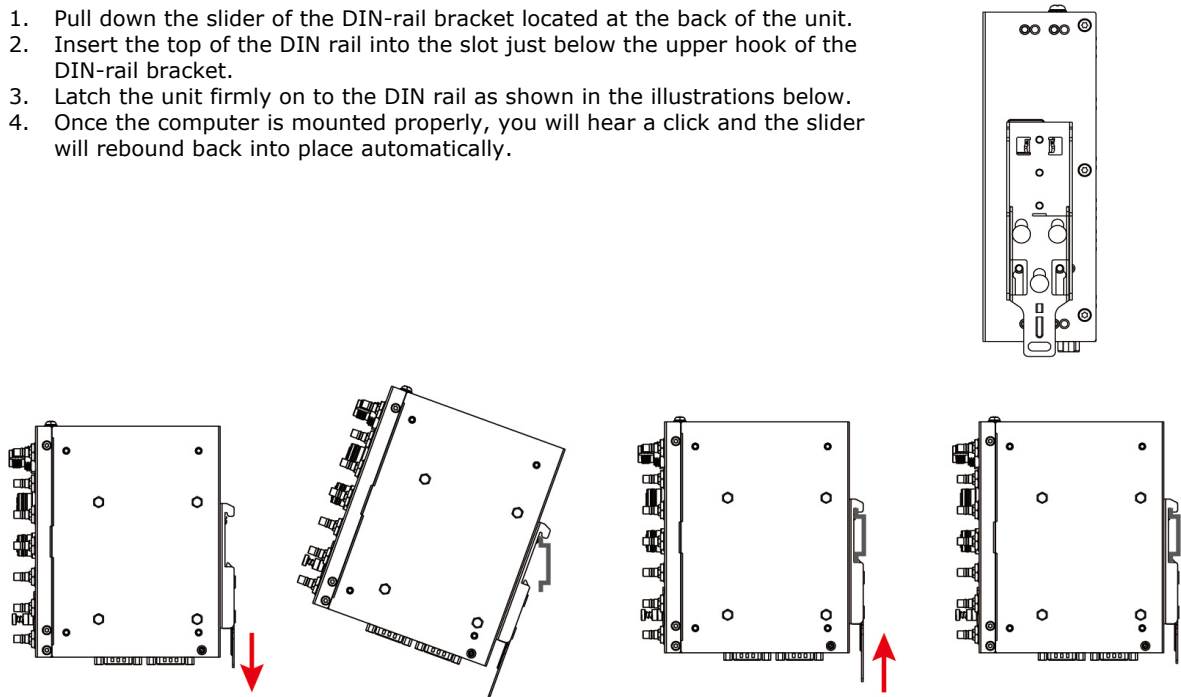
DIN-rail Mounting (optional)

The DIN-rail mounting kit is an optional accessory not included in the product package and needs to be purchased separately.

To attach the DIN-rail mounting bracket to the computer, align the mounting bracket to the mounting apertures on the back panel of the computer. Fasten the five M3 x 4 mm screws in the mounting-kit package to secure the bracket to the computer with a torque value of 4.5 ± 0.5 kgf-cm.

To mount the V1200 Series on to a DIN rail, ensure that the stiff metal spring is facing upwards and follow these steps.

1. Pull down the slider of the DIN-rail bracket located at the back of the unit.
2. Insert the top of the DIN rail into the slot just below the upper hook of the DIN-rail bracket.
3. Latch the unit firmly on to the DIN rail as shown in the illustrations below.
4. Once the computer is mounted properly, you will hear a click and the slider will rebound back into place automatically.



3. Hardware Connection Description

In this chapter, we describe how to connect the V1200 to a network and various devices.

Wiring Requirements

In this section, we describe how to connect various devices to the embedded computer. Be sure to read and follow these common safety precautions before proceeding with the installation of any electronic device:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.



NOTE

Do not run signal or communication wiring and power wiring in the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.

- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separate.
- When necessary, it is strongly advised that you label wiring to all devices in the system.



ATTENTION

Safety First!

Be sure to disconnect the power cord before doing installations and/or wiring.

Electrical Current Caution!

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.

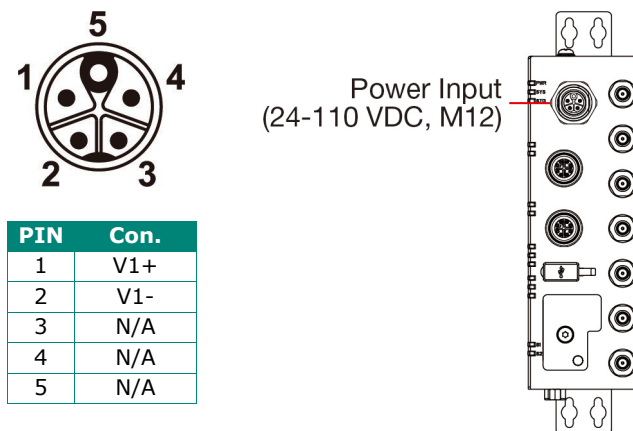
If the current goes above the maximum rating, the wiring could overheat, causing serious damage to your equipment.

Temperature Caution!

Be careful when handling the unit. When the unit is plugged in, the internal components generate heat, and consequently the outer casing may feel hot to the touch.

Connecting the Power

Connect the 24 to 110 VDC power line with M12 K-coded connector (needs to be purchased separately) to the V1200 computer. If the power is supplied properly, the "PWR" LED will glow a solid green after a 25 to 30-second delay. The power input location and pin definition are shown in the following figures:



Grounding the Computer

There is a grounding connector located on the top panel of the computer. Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Note that this product is intended to be mounted on a well-grounded mounting surface, such as a metal panel.

The power cord adapter should be connected to a socket outlet with an earthing connection.

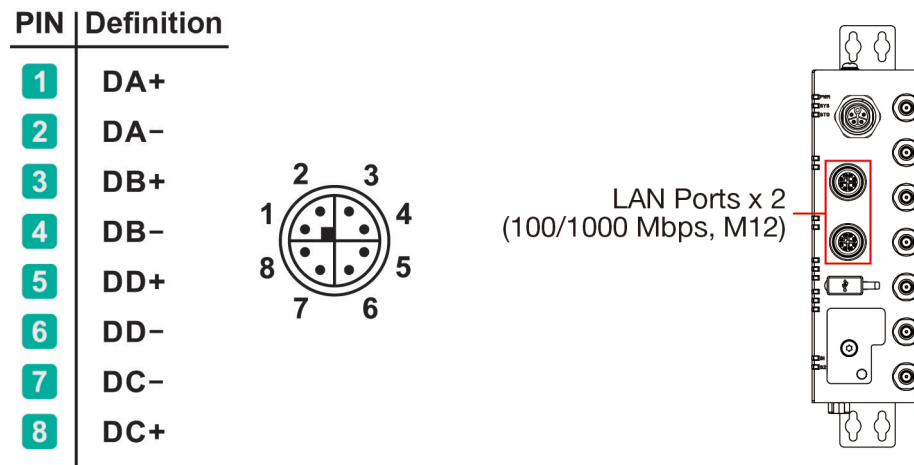


ATTENTION

This product is intended to be mounted to a well-grounded mounting surface such as a metal panel. Use the green-and-yellow cable type minimum with American Wire Gauge (AWG) 18 for grounding.

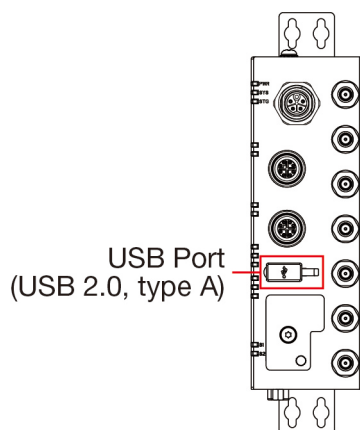
Connecting the Network

The pin assignments for the V1200 computer's Ethernet ports are shown in the following figure. If you are using your own Ethernet cable, make sure that you match the pin assignment on the connector of the Ethernet cable to the pin assignment shown below:



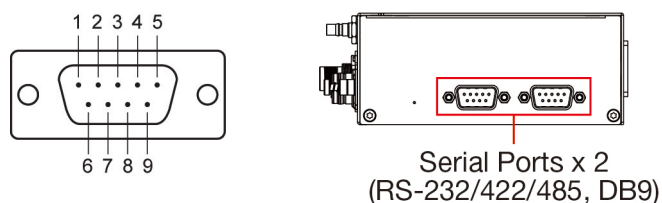
Connecting a USB Device

The USB port, located on the front panel, is a type-A USB 2.0 console port which you can use to connect a USB storage device or a type-A USB compatible device.



Connecting Serial Ports

The computer comes with two serial ports on the bottom panel. Use a serial cable to connect your serial device to the computer via a serial port. The serial ports use DB9 connector and can be configured for RS-232, RS-422, or RS-485 communication. The location and pin assignments of the serial ports are shown in the following tables:



Pin	RS-232	RS-422	RS-485 (4-wire)	RS-485 (2-wire)
1	DCD	TxDA(-)	TxDA(-)	-
2	RxD	TxDB(+)	TxDB(+)	-
3	TxD	RxDB(+)	RxDB(+)	DataB(+)
4	DTR	RxDA(-)	RxDA(-)	DataA(-)
5	GND	GND	GND	GND
6	DSR	-	-	-
7	RTS	-	-	-
8	CTS	-	-	-

Inserting the SIM Card

The V1200 models come with 1 or 2 SIM card slots on the front panel. When you install the SIM cards into the slots, ensure that they are inserted in the correct direction, as indicated on the label.

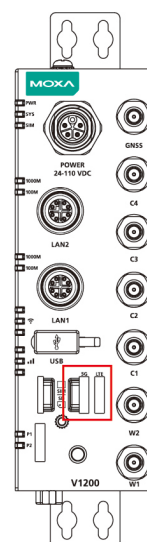
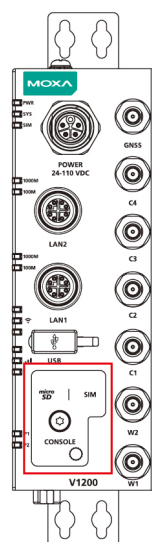
To install a SIM card, do the following:

Step 1

Remove the screw securing the SIM card holder cover on the front panel of the computer.

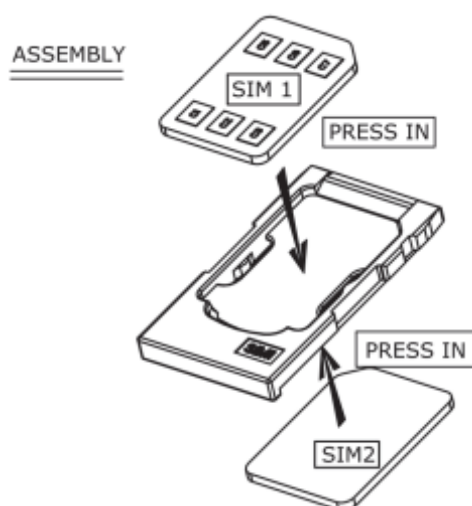
Step 2

Remove the SIM card tray by pressing the tray inwards and releasing it to eject the tray, then pulling out the tray.



Step 3

The SIM card tray can hold two SIM cards, one on each side. Install the first SIM card in the SIM1 slot and the second SIM card on the other side of the tray.



NOTE

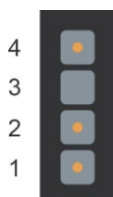
When the V1222-CT-T model is used with a 5G module, LTE communication is supported through backward compatibility. Therefore, if you are using an LTE-only SIM card, ensure that the SIM card is inserted into the 5G SIM slot for proper operations..

Inserting a MicroSD Card

The V1200 comes with a microSD socket for storage expansion. The microSD socket is located on the lower part of the front panel. To install the card, remove the screw and the protection cover to access the socket, and then insert the microSD card into the socket. You will hear a click when the card is in place. To remove the card, push the card in before releasing it.

Connecting the Console Port

The console port is an RS-232 port located on the lower part of the front panel. To install the card, remove the screw and the protection cover to access the console port. Connect a 4-pin pin header cable and use the port for debugging issues or system image upgrades.



Pin	Signal
1	TxD
2	RxD
3	NC
4	GND

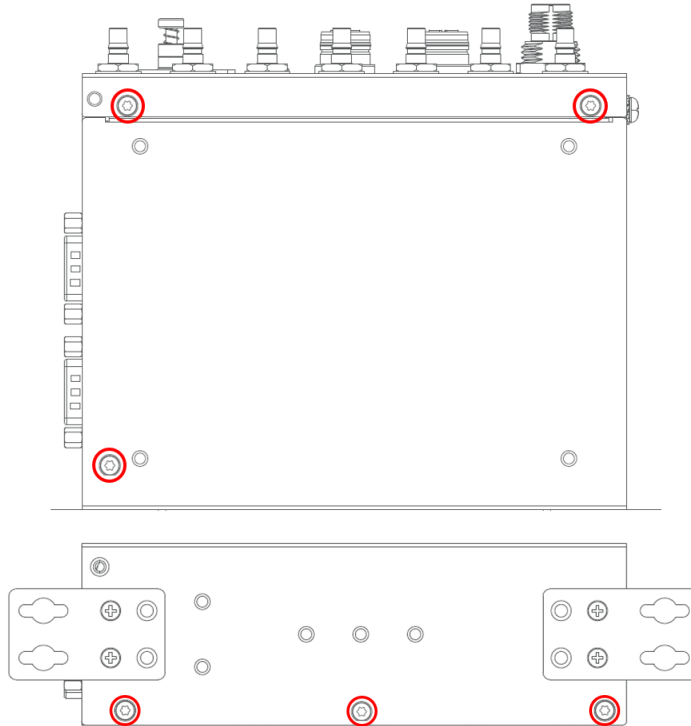
Installing Wireless Modules

Before you install the V1200 Series wireless module, ensure that the wireless module package from Moxa contains the following items:

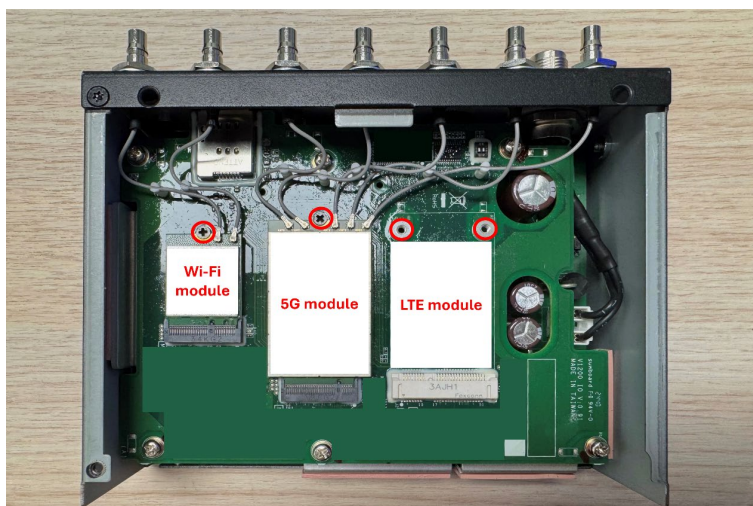
- * Wireless module
- * Heat sink, and thermal pads (quantity may vary depending on the wireless module model)
- * Coaxial cables, lock washers, and nuts (quantity may vary depending on the wireless module model)

To install wireless modules, do the following:

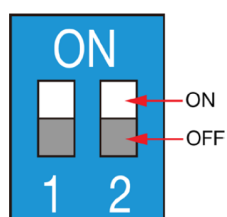
1. Remove the cover by unfastening the six screws on the panel of the computer as indicated in the following diagrams:



2. Install the modules in their corresponding slots.
Use the indicators in the picture and the instructions as a guide to install the modules

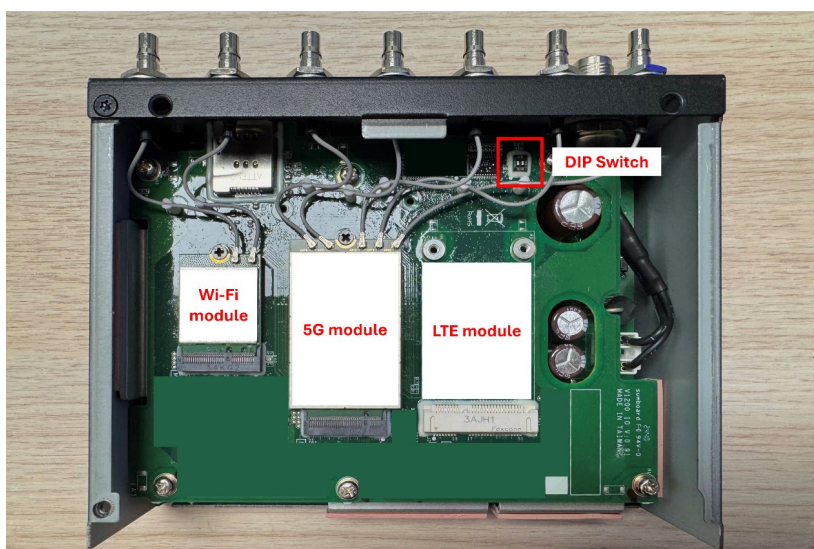


- Step 1: Paste the heat sink on the area marked in the picture.
 - Step 2: Paste the first thermal pad on top of the heat sink.
 - Step 3: Insert the module into the socket.
 - Step 4: Fasten the screws to secure the module in place.
 - Step 5: Paste the second thermal pad on top of the module.
3. If using a 5G or LTE module, ensure the DIP switch is set to the correct position.



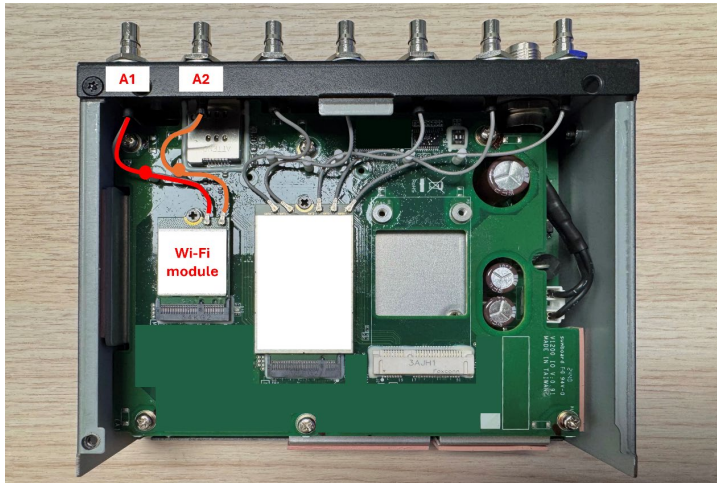
ON	LTE Module
OFF	5G Module

The location of the DIP switch on the board is shown here:

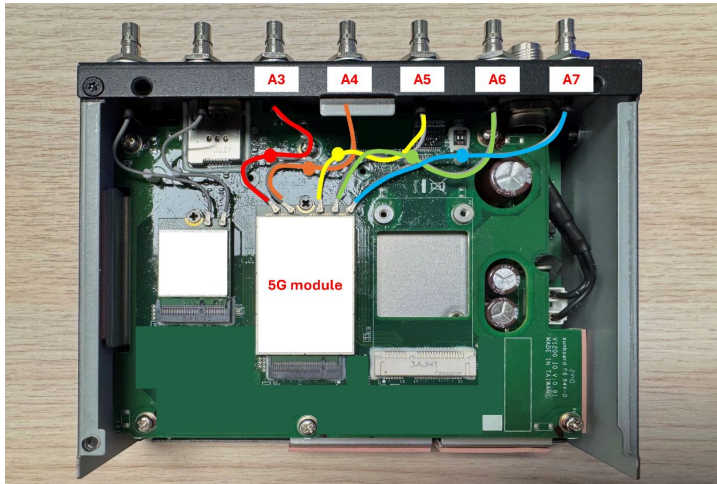


Installing Cables and Antennas

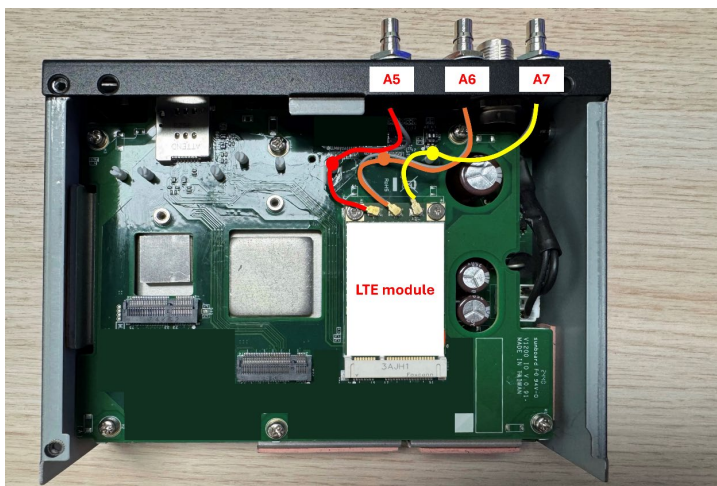
1. Insert the QMA connector of the coaxial cable through the antenna aperture on the front panel. Based on the length of the cable and the location of the module, we recommend:
 - A1 and A2 for Wi-Fi 6 module.



- A3, A4, A5, A6, A7 for 5G modules.



- A5, A6, A7 for LTE module.



2. Insert the lock washer through the connector from outside and hold it against the panel.
3. Finally, secure the antenna connector with the nut by tightening it on the on the threaded protection ring towards the lock washer.



4. Getting Started

The V1200 Series offers a flexible computing platform. Users can develop their own applications based on the Moxa Industrial Linux (MIL). In addition, we provide a Web-based Network Configuration Tool that allows users to easily configure network settings without using command-line instructions.

Disabling the Web-based Network Configuration Tool

If you prefer not to use the web-based network configuration tool, you can disable it and manage the settings via the command line using the following commands:

- `sudo systemctl stop tpe`
- `sudo systemctl disable tpe`
- `sudo nft flush ruleset`
- `sudo systemctl enable ssh`
- `sudo systemctl start ssh`

For instructions on getting started with cmd, see [Moxa Industrial Linux Arm-based Computers Manual](#).



NOTE

If you configure the network via a console or terminal (e.g., SSH) using Linux commands and notice that the settings revert back to the default, we recommend one of the following:

- Use the web-based network configuration tool to configure the network settings, or
- Disable the web-based network configuration tool before configuring network settings via cmd.



NOTE

The ping function is not supported when the web-based network configuration tool is running. To use the ping command, first disable the web-based network configuration tool.

Access to the Web Console

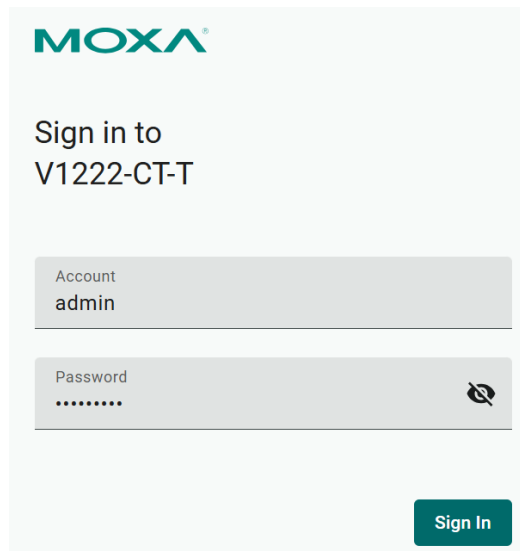
The default LAN2 IP address to access the web console of the V1200 is 192.168.4.127.

When you use the default IP address to access the V1200, do the following:

1. Ensure your host and the V1200 are in the same subnet (V1200's default subnet mask is 255.255.255.0). Connect to LAN2 and enter **https://192.168.4.127** in your web browser.
2. Read the system notification and click **Agree and Continue**.
3. Enter the account and password information.

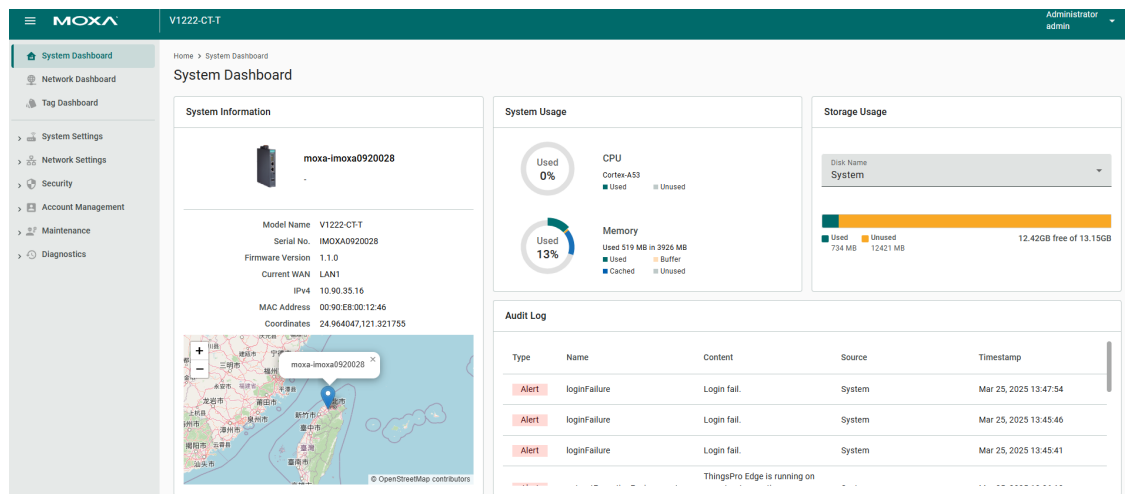
Default account: **admin**

Password: **admin@123**



The login page for the Moxa V1222-CT-T device. It features the Moxa logo at the top, followed by the text "Sign in to V1222-CT-T". Below this are two input fields: "Account" with the value "admin" and "Password" with masked characters ".....". A "Sign In" button is located at the bottom right of the form.

You will see the following homepage after logging in successfully.



The System Dashboard for the Moxa V1222-CT-T device. The dashboard includes a sidebar with navigation options: System Dashboard, Network Dashboard, Tag Dashboard, System Settings, Network Settings, Security, Account Management, Maintenance, and Diagnostics. The main content area displays several widgets: System Information (Model Name: V1222-CT-T, Serial No. IMOXAD920028, Firmware Version 1.1.0, Current WAN LAN1, IPv4 10.90.35.16, MAC Address 00:90:E8:00:12:46, Coordinates 24.964047,121.321755), System Usage (CPU Cortex-A53, Memory Used 519 MB in 3926 MB), Storage Usage (Disk Name System, Used 734 MB, Unused 12421 MB, 12.42GB free of 13.15GB), and an Audit Log table.

Type	Name	Content	Source	Timestamp
Alert	loginFailure	Login fail.	System	Mar 25, 2025 13:47:54
Alert	loginFailure	Login fail.	System	Mar 25, 2025 13:45:46
Alert	loginFailure	Login fail.	System	Mar 25, 2025 13:45:41



NOTE

After the first login, we force a password change to comply with general security policies and practices and to increase the security of your device.

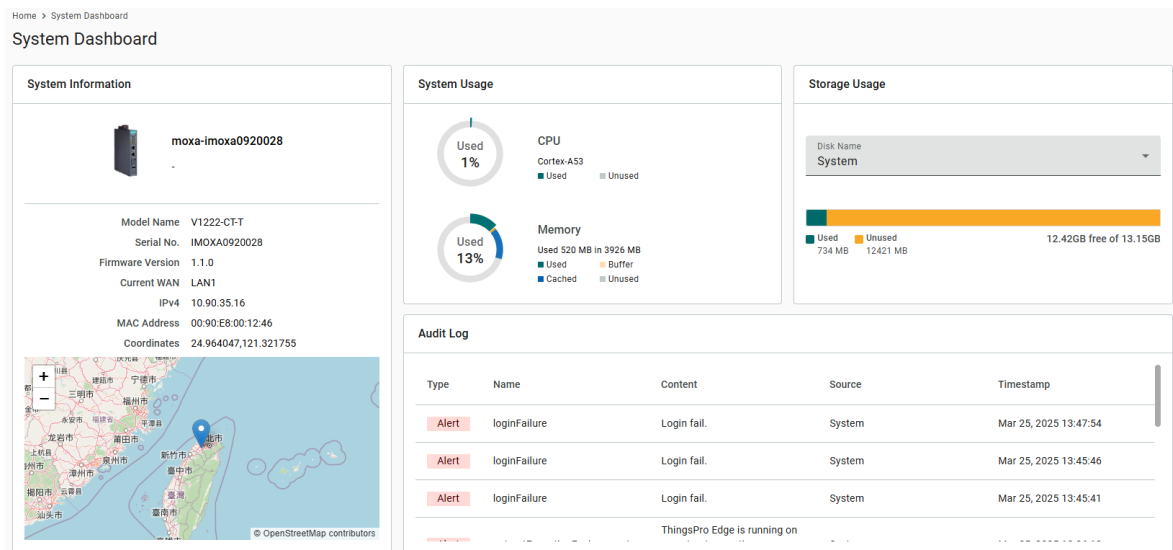
5. Web Console

Dashboard

System Dashboard

To view the device's system status, go to System Dashboard.

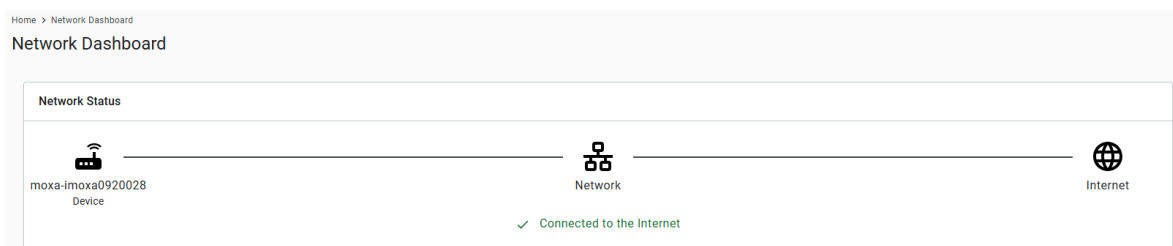
This page displays basic system information such as model name, serial number, firmware version, system usage, storage usage, and audit logs.



Network Dashboard

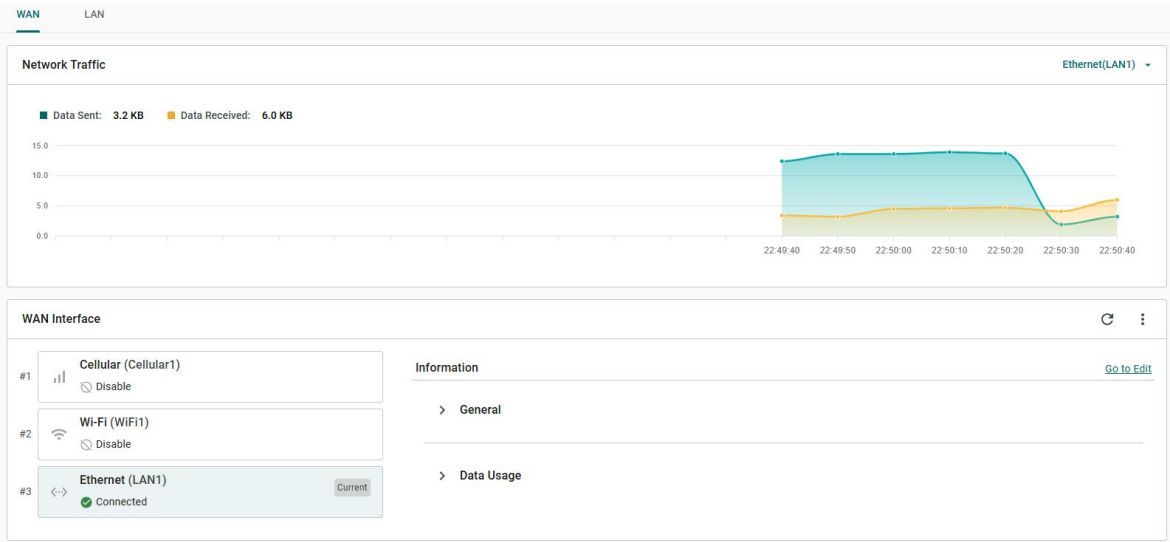
To view information about WAN/LAN interfaces and traffic statistics, go to Network Dashboard.

The dashboard shows interface usage details and network status, including Internet connectivity.



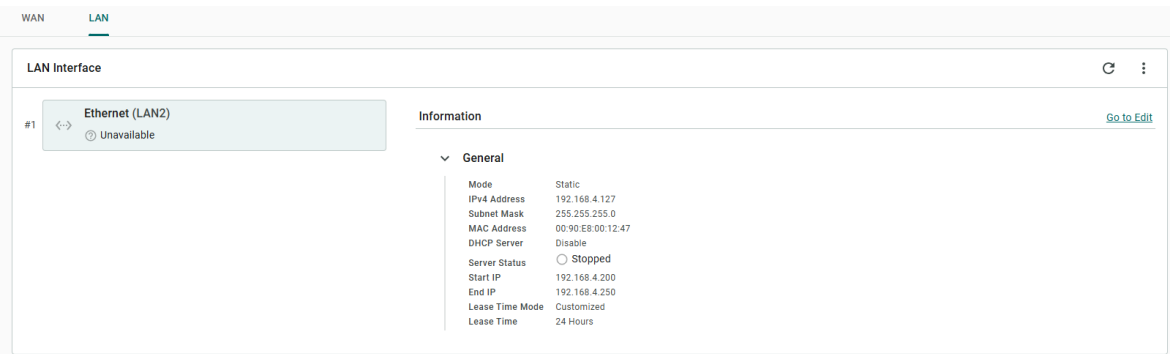
WAN

The WAN tab displays information about data sent and received through the WAN interfaces. You can select a specific interface to monitor. Additional usage details are also provided. The information is refreshed every 10 seconds.



LAN

The LAN tab displays usage details and traffic statistics for the LAN interfaces. You can view real-time data for each interface under this section.



Tag Dashboard

To create and monitor real-time tag values for troubleshooting, go to Tag Dashboard. You can add tags for monitoring and view their current values in real time.

Home > Tag Dashboard

Tag Dashboard

Add tags and monitor them here. You can also set values for writable tags by clicking "i". The values take effect within a few seconds.

Search

Edit Tags

Provider	Source	Name	Type	Value	Access	Last Update
No tags are being monitored. Click + Edit Tags to add the first tag to monitor.						

Items per page:

10

0 of 0

<<<>>>

To create and monitor the real-time tag value, click + **Edit Tags** first, select the tags to monitor in the list then click Save.

Edit Tags

Select the tags you want to display in the list.

1 item(s) selected

Clear

Search

<div></div>	Provider	Source	Name	Type	Access
<input type="checkbox"/>	system	storage	systemDiskFree	uint64	Read
<input checked="" type="checkbox"/>	system	status	memoryUsed	uint64	Read
<input type="checkbox"/>	system	status	memoryFree	uint64	Read
<input type="checkbox"/>	system	network	wifi1NetworkRx	uint64	Read
<input type="checkbox"/>	system	status	gpsLong	double	Read

Items per page:


5

1 - 5 of 30

<<<>>>

Cancel

Save

(Optional) Click the icon  to deactivate the monitoring tags.

Home > Tag Dashboard

Tag Dashboard

Add tags and monitor them here. You can also set values for writable tags by clicking "i". The values take effect within a few seconds.

Monitoring tags...

Search

Edit Tags

Provider	Source	Name	Type	Value	Access	Last Update
system	status	memoryUsed	uint64	548794368	Read	Mar 25, 2025, 23:03:27

Items per page:

10

1 - 1 of 1

Write value

Deactivate monitoring

System Settings

General

Go to **System Settings > General > System** to specify a new server/host name and enter a description for the device.

Home > System Settings > General

General

System Time GPS

Server/Host Name

moxa-imoxa0920028

Description - optional

Factory A1

Parameter	Value	Description	Default Value
Server/Host Name	Alphanumeric string	You can enter a name to identify the unit, such as the function, etc.	Moxa-imoxaxxxxxxx
Description - optional	Alphanumeric string	You can enter a description to help identify the unit location such as "Factory A1".	Factory A1

Go to **System Settings > General > Time** to select a time zone. Choose between the Manual or Auto option to update the system time.

Home > System Settings > General

General

System **Time** GPS

Current date and time: Mar 25, 2025 23:11:11

Time Zone

(GMT +08:00) Asia/Taipei

Sync Mode

☒ Manual ☐ Auto

Sync with browser

Date

Mar 25, 2025

Hour

23

Minute

9

Second

27

Save

Home > System Settings > General

General

System **Time** GPS

Current date and time: Mar 25, 2025 23:11:54

Time Zone

(GMT +08:00) Asia/Taipei

Sync Mode

☐ Manual ☒ Auto

Interval (sec)

7200

Source

NTPsec Server

Time Server

time.cloudflare.com

Save

Parameter	Value	Description	Default Value
Time Zone	User's selectable time zone	The field allows you to select a different time zone.	Current Time Zone
Sync Mode	Manual, Auto	Manual: input the time parameters by yourself Auto: it will automatically sync with time source. NTP and GPS can be selected. NOTE: When the Auto mode is selected, in general, it takes 2 to 4 minutes. If the satellite search is slower, it could take up to 12 minutes (worst-case scenario)	Manual
Interval (sec)	3600 to 86400	The time interval to sync the time source	7200
Source	NTPsec Server, NTP Server, GPS	The way to sync the time clock	N/A
Time Server	IP or Domain address	This field is required to specify your time server's IP or domain name if you choose the NTP server as the source	N/A



NOTE

When using GPS as a time-synchronization source, set the GPS mode to **Auto** before entering the configuration page.

Go to **System Settings > General > GPS** to view the GPS location of the device on a map. There are two options:

- Input latitude and longitude in **manual**.
- Check the **Automatically adjust coordinates for GPS changes** option if you want the system to automatically update the device coordinates.

Home > System Settings > General

General

System Time **GPS**

☒ Manually enter coordinates
☐ Automatically adjust coordinates for GPS changes

Coordinates

Latitude
24.964047

Longitude
121.321755


,

Save

Serial

Go to **System Settings > Serial** to view and configure serial parameters.



To configure serial settings, do the following:

1. Click the icon  on the chosen port and select Edit.

Home > System Settings > Serial

Serial

Search Refresh

Port	Interface	Baud Rate	Parity, Data Bits, Stop Bits	Flow Control	
#1 P1	rs232	9600	none, 8, 1	none	
#2 P2	rs232	9600	none, 8, 1	none	

Items per page: 10 1 - 2 of 2

Edit Clone

2. Set and click **Save** for the settings to take effect.

Home > System Settings > Serial > Port #1

< Port#1

Serial Settings

Interface
rs232

Baud Rate
9600

Parity
none

Data Bits
☐ 7 ☒ 8

Stop Bits
☒ 1 ☐ 2

Flow Control
none

Save Clone

Parameter	Value	Description	Default Value
Interface	rs232, rs485-2w, rs422, rs485-4w	The serial interface type to use for the serial device.	rs232
Baud Rate	300 to 115200	The data transmission rate to and from the serial device.	9600
Parity	none, odd, even, space, mark	The parity mode of the serial device.	none
Data Bits	7, 8	The size for data characters.	8
Stop Bits	1, 2	The size for stop characters.	1
Flow Control	none, hardware, software	The flow control method determines how the system will suspend and resume data transmissions to prevent data loss. If hardware is selected as flow control method, it will be controlled by RTS/CTS signal.	none



NOTE

Incorrect settings will cause communication failures.

3. (Optional) Click the icon : on the chosen port and select Clone to clone the setting to the chosen port.

Clone Port Settings

Clone serial port #1 settings to other ports.

☒ All Ports

☒ Port #2

[Cancel](#) [Submit](#)

External Storage

To manage external storage devices, go to System Settings > External Storage. You can attach external storage to the V1200 to save logs, provide buffer space for Store and Forward, and create system backups. Once connected, the storage device will appear in the **Device List**.

External Storage

You can reduce the space occupied on the main system disk by using external storage devices.

Device List

USB_p1

[Refresh](#)



NOTE

LIMITATION

- V1200 does not allow the connection of multiple USB devices through a USB hub.
- The external USB format supported for V1200 is FAT.

SNMP Agent

Go to **System Settings > SNMP Agent** to view and configure SNMP agent service.

Select Enable SNMP agent service to enable SNMP agent service.

Home > System Settings > SNMP Agent

SNMP Agent

This page allows you to configure SNMP agent settings for efficient network management. Set up SNMP with support for multiple versions (V1, V2c, V3) to ensure compatibility and enhance security.

☐

Enable SNMP agent service

SNMP Version

V3

Account(s)

+ Create

admin

Authentication Type : None

Account Privacy : None

Parameter	Value	Description	Default Value
SNMP Version	V3 V1, V2c, V3 V1, V2c	The SNMP protocol version used to manage your device. It's strongly recommend choosing the 'V3' option for enhanced security.	V3

V1200 Series User Manual

31

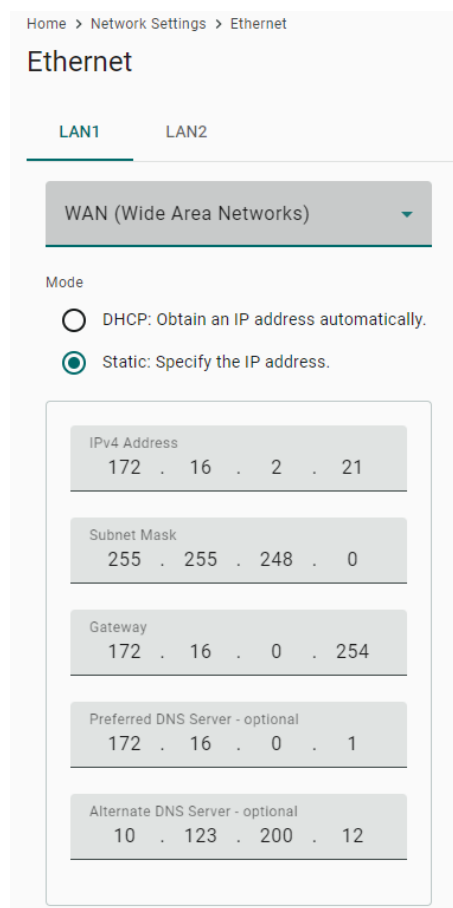
Network Settings

Ethernet

Go to **Network Settings > Ethernet** to view and configure LAN1 and LAN2 network settings.

To configure the network, do the following:

1. Choose **LAN1** or **LAN2** for configuration.
2. Select the **WAN (Wide Area Networks)** or **LAN (Local Area Networks)**.
3. Select **DHCP** or **Static** mode.
4. Configure **IP address**, **Subnet mask**, **Gateway**, and **DNS**.



Home > Network Settings > Ethernet

Ethernet

LAN1 LAN2

WAN (Wide Area Networks) ▼

Mode

☐ DHCP: Obtain an IP address automatically.

☒ Static: Specify the IP address.

IPv4 Address
172 . 16 . 2 . 21

Subnet Mask
255 . 255 . 248 . 0

Gateway
172 . 16 . 0 . 254

Preferred DNS Server - optional
172 . 16 . 0 . 1

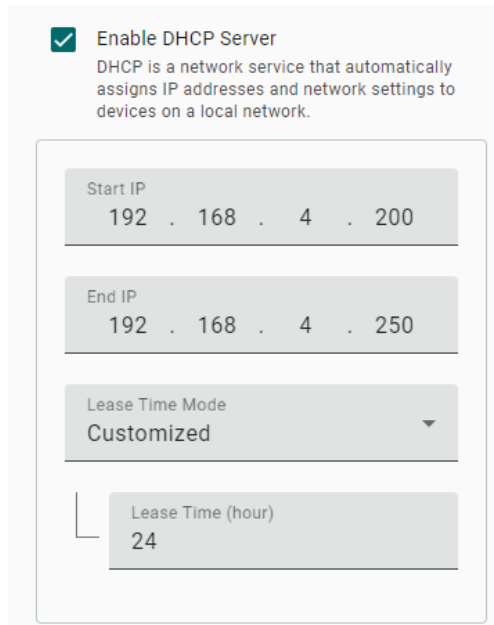
Alternate DNS Server - optional
10 . 123 . 200 . 12

Parameter	Value	Description
Types of connectivity	WAN, LAN (NOTE: LAN2 does not support WAN.)	WAN: Wide Area Networks LAN: Local Area Networks
Mode	DHCP, Static	DHCP: Obtain the IP address automatically. Static: Specify the IP address
IPv4 Address	LAN1 default: DHCP LAN2 default: 192.168.4.127	The IP (Internet Protocol) address identifies the server on the TCP/IP network
Subnet Mask	Default: 255.255.255.0	Identifies the server as belonging to a Class A, B, or C network.
Gateway—optional	0.0.0.0	The IP address of the router that provides network access outside the server's LAN.
Preferred DNS Server—optional	0.0.0.0	The IP address of the primary domain name server.
Alternate DNS Server—optional	0.0.0.0	The IP address of the secondary domain name server.

If the LAN is selected as type of connectivity, the V1200 can be configured to operate as a DHCP server, offering the additional benefit of dynamically assigning IP addresses to devices on the network.

To configure DHCP server settings, do the following:

1. Check Enable DHCP Server.
2. Input IP Address Range parameters.
3. Specify Lease Time.
4. Click **Save**.



☒ **Enable DHCP Server**
DHCP is a network service that automatically assigns IP addresses and network settings to devices on a local network.

Start IP
192 . 168 . 4 . 200

End IP
192 . 168 . 4 . 250

Lease Time Mode
Customized ▼

Lease Time (hour)
24



NOTE

Limitation: When V1200 acts as the DHCP server, it will not allocate the DNS IP to the DHCP client.

Cellular

Go to **Network Settings > Cellular** to view the current cellular settings. You can enable or disable cellular connectivity on your device, create profiles, manage **Profile Settings**, and enable or disable the connection **Check-alive** function to optimize the cellular connection.

Home > Network Settings > Cellular

Cellular

CELLULAR1


☒ Enable cellular data communication

Profile Settings

Create and manage profiles for a SIM card and its data plan.

Connection Retry Timeout (sec)
120

Profile List + Create

#1 Profile-1
SIM1 

Check-alive

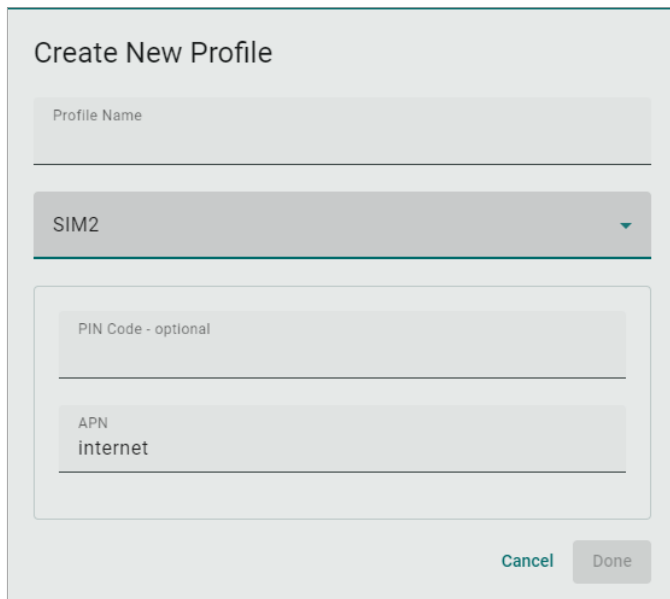
☒ Enable check-alive

Target Host
8.8.8.8

Ping Interval (sec)
60

Save

You can create customized cellular profiles in the **Profile Settings** section. A list of all the profiles in the system is displayed. **Create**, **Edit**, or **Delete** cellular profiles here.

A screenshot of a 'Create New Profile' dialog box. It has a title bar at the top. Below the title, there is a text input field labeled 'Profile Name'. Underneath that is a dropdown menu currently showing 'SIM2'. Below the dropdown is a section containing two more text input fields: 'PIN Code - optional' and 'APN' (with 'internet' entered below it). At the bottom right of the dialog are two buttons: 'Cancel' and 'Done'.

To create a new cellular connection profile, do the following:

1. Click **+ Create**.
2. Specify a unique **Profile Name**.
3. Specify the target **SIM** card.
4. Enter the **PIN Code** if your SIM card requires it.
5. Input **APN**.
6. Click **Done**.
7. On the **Cellular** setting page, click **Save**.

When you click **Save** in the Cellular section, the module restarts to apply the changes. The settings will take effect after the cellular module is successfully initialized.



NOTE

To prevent the SIM from being locked due to three incorrect attempts, a mechanism in the V1200 stops attempting to unlock the SIM when the PIN Retry count reaches 2 (only one attempt is remaining). At this point, insert the SIM into another device (e.g., cellphone) and attempt to unlock it. This way, when you reinsert the SIM card into the V1200 and restart, the PIN Retry count is reset to 3.



NOTE

LIMITATION

V1200 does not support hot-plugging of the SIM card; device restart is required after inserting or removing the SIM card.

The **Check-alive** function will help you maintain the connection between your device and the carrier service by pinging a specific host on the Internet at periodic intervals.

Check-alive

☒ Enable check-alive

Target Host
8.8.8.8

Ping Interval (sec)
60



NOTE

After configuring the Cellular network, you can check the cellular network's connection status by going to **Network Dashboard > WAN**

Wi-Fi Client

Go to **Network Settings > Wi-Fi** to view the Wi-Fi settings. You can enable or disable Wi-Fi connectivity on your device, create profiles, manage Profile Settings, and enable or disable the connection Check-alive function to optimize the cellular connection.

Home > Network Settings > Wi-Fi Client

Wi-Fi Client

WIFI1

☐ Enable Wi-Fi

AP List + Create

1

moxa
 ⓘ --

⋮

IP Settings

Mode

☒ DHCP: Obtain an IP address automatically

☐ Static: Assign IP address by manual configuration

Check-alive

☒ Enable check-alive

Target Host
8.8.8.8

Ping Interval (sec)
60

Save

To configure Wi-Fi settings, check **Enable Wi-Fi** and do the following:

1. Click **+create** to manually **Create by SSID** or be **Created by Scan Results**.

Add by SSID

SSID

Security Mode

WPA/WPA2 Personal

Password

CANCELADD

Add by Scan Results

1 Select AP2 View Details

Info: Please choose the Wi-Fi network that you want to add from the list. Note that only WPA and WPA2 Personal are supported.

SQA3_WiFi6		
sqa-iiot-lan-50G		
SQA2-TestBed-AWK3131A		
SQA-LAB-TV		
.M-Guest		

CANCELNEXT >

2. Select **DHCP** or **Static mode**.
3. Check **Check-alive** function which can be used to ensure Internet connectivity.
4. Click **Save**.



NOTE

After configuring the Wi-Fi network, you can check the Wi-Fi network's connection status by going to **Network Dashboard > WAN**

Network Management

DNS

By manually configuring specific DNS server addresses, users can ensure stable and predictable internet connectivity without relying on potentially fluctuating or unreliable DNS settings provided by dynamic configurations (such as those obtained from a DHCP server). This helps to improve DNS resolution speed, enhance overall network performance, and strengthen control over network traffic and security by specifying trusted DNS servers.

Network Management

DNSRouting

☒ Enable static DNS

Primary DNS

Secondary DNS - optional

Save

Routing

The Routing priority feature allows the V1200 to prioritize different network interfaces (such as cellular, LAN, and Wi-Fi) as needed to optimize network performance.

Network Management

DNS Routing

# 1	Cellular
# 2	WiFi
# 3	LAN1

Save

VRRP

Go to **Network Settings > VRRP** to view and configure the VRRP settings.

Home > Network Settings > VRRP

VRRP

This page allows you to configure VRRP instances to enhance network reliability. Create up to 2 VRRP instances to manage different network segments and automatically failover to a backup router in the event of a failure.

VRRP Instance(s) [Refresh](#) [+ Create](#)

Instance 1 ⋮

☐ Initial

Interface : LAN1
Virtual IP Address : 10.0.0.1
Virtual Router ID : 1
Object Ping Tracking : Disable
[> More Information](#)

Create VRRP Instance

1 Basic Instance Step 2 Select Authentication 3 Configure Tracking

Interface ▼

Virtual IP Address

Virtual Router ID

Priority ⊙
100

Preemption ⊙
Enable ▼

Preempt Delay(sec) ⊙
120

Advertisement Interval(sec)
1

Cancel Next

Parameter	Value	Description	Default Value
Interface	Drop-down list of interfaces	Specify which network interface to use for the VRRP interface.	N/A
Virtual IP Address	Valid IP address	Specify the virtual router IP address for the VRRP interface.	N/A
Virtual Router ID	1-255	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group.	N/A
Priority	1-254	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.	100
Preemption	Enabled / Disabled	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled
Preempt Delay (sec)	0-300	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	120
Advertisement Interval	1-30	Specify the advertisement interval in seconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	1

Create VRRP Instance

✓ Basic Instance Step
2 Select Authentication
3 Configure Tracking

Authentication

< Back

Cancel

Next

Parameter	Value	Description	Default Value
Authentication	None/ Simple/ AH		None
Authentication Password		Specify the password when Simple or AH is chosen for authentication method.	N/A

Create VRRP Instance

✓ Basic Instance Step
✓ Select Authentication
3 Configure Tracking

Object Ping Tracking

Enable

Target IP

Interval(sec)

1

Timeout

3

Priority Decrement Value

20

Success Count

3

Failure Count

3

< Back

Cancel

Create

Parameter	Value	Description	Default Value
Object Ping Tracking	Disabled/ Enable	Disable or specify which interface to use for Object Ping Tracking for the VRRP interface. When enabled, if all interfaces on the device are disconnected, it will be considered to be a disconnection.	Disabled
Target IP	Valid IP address	Specify the target IP to ping to verify if the connection to the destination is working.	N/A
Interval (sec)	1-100	Specify the interval in seconds the device will use for pinging the target IP.	1
Timeout	1-100	Specify the timeout duration in seconds the device will wait for a response before timing out.	3
Priority Decrement Value	1-254	Specify the amount by which the priority of a backup router is decreased when a ping test fails.	20
Success Count	1-100	Specify the success count, which indicates how many responses the device must receive to consider the connection as working.	3
Failure Count	1-100	Specify the failure count, which indicates how many times the target IP fails to respond before the device considers the connection as not working.	3

Click (:) to Edit or Delete the existing VRRP instances.

Home > Network Settings > VRRP

VRRP

This page allows you to configure VRRP instances to enhance network reliability. Create up to 2 VRRP instances to manage different network segments and automatically failover to a backup router in the event of a failure.

VRRP Instance(s)
Refresh
+ Create

Instance 1
☐ Initial

Interface : LAN1
Virtual IP Address : 10.0.0.1
Virtual Router ID : 1
Object Ping Tracking : Disable
[More Information](#)

⋮

Edit

Delete

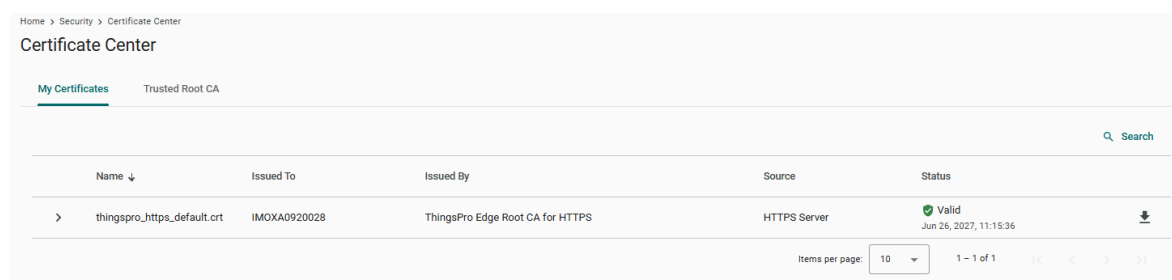
Security

Certificate Center

To check what certificates have been used on the devices, go to **Security > Certificate Center** to view all of them. On this page, you can search, view the status, and download the certificate for backup purposes.

The **ThingsPro Edge Root CA for HTTPS** certificate is used to sign the HTTP SSL X.509 certificate, default.crt. You can download this root CA and import it to your client devices to trust the HTTPS connection between clients and V1200. To import to Google Chrome, you can refer to the below link:

https://docs.moxa.online/tpe/users-manual/security/certificate_center/#import-rootcacer-to-google-chrome



The screenshot shows the 'Certificate Center' page with a breadcrumb 'Home > Security > Certificate Center'. Below the title, there are tabs for 'My Certificates' (active) and 'Trusted Root CA'. A search bar is on the right. The main table has columns: Name, Issued To, Issued By, Source, and Status. One certificate is listed: 'thingspro_https_default.crt' issued to 'IMOXAO920028' by 'ThingsPro Edge Root CA for HTTPS' from an 'HTTPS Server'. The status is 'Valid' with a green checkmark and the date 'Jun 26, 2027, 11:15:36'. A download icon is on the right. At the bottom, it shows 'Items per page: 10' and '1 - 1 of 1'.

Name ↓	Issued To	Issued By	Source	Status
> thingspro_https_default.crt	IMOXAO920028	ThingsPro Edge Root CA for HTTPS	HTTPS Server	Valid Jun 26, 2027, 11:15:36

Firewall

V1200 provides a firewall that allows you to create inbound rules for inbound Internet network traffic and enable NAT service to protect your gateway of train-to-ground communication.



The screenshot shows the 'Firewall' page with a breadcrumb 'Home > Security > Firewall'. Below the title, there are tabs for 'Inbound Rules' (active) and 'NAT Service'. The main area shows a list of rules: 'System Default', 'Allowed List', and 'Port Forwarding', each with a dropdown arrow on the right.

System Default	▼
Allowed List	▼
Port Forwarding	▼

Inbound Rules

System Default

V1200 reserves ports for certain services and purposes as indicated in the table below.

No.	Service/purpose	Port
1	HTTP service	80
2	HTTPS service	443
3	SSH server	22
4	Discovery service	5353



NOTE

The V1200 disables all ports by default excluding the reserved ports mentioned above. To enhance the security of your device, we recommend configuring a rule that includes the source IP and source port, thereby granting access only to specific individuals.

Home > Security > Firewall

Firewall

Inbound Rules

NAT Service

System Default

Q Search

Rule Name	Gateway Port ↑	Protocol	Source IP	Source Port	
ssh server	22	TCP	Any	Any	
http service	80	TCP	Any	Any	
https service	443	TCP	Any	Any	
discovery service	5353	UDP	Any	Any	

Items per page: 10

1 - 4 of 4

<<

<

>

>>

Allowed List

V1200 provides an allowed list for creating firewall rules. You can create, edit, and delete firewall rules here.

To create firewall rules, do the following:

1. Click **+ Create Rule**.
2. Specify the protocol, gateway port, and rule name.
3. Specify a source IP or a subnet.
4. Specify a source port or a range of ports.
5. Click **Save**.

Home > Security > Firewall

Firewall

Inbound Rules

NAT Service

System Default

Allowed List

Port Forwarding

Rule Name

No data to display. Click [Create rule](#) button to

Q Search

Create rule

Source Port

Items per page: 10

0 of 0

<<

<

>

>>

Create Rule

Protocol

☒ TCP
 ☐ UDP

Gateway Port

Rule Name

Port_ 5 / 32

Source IP

Customized

IP Range

Source Port

Customized

Port Range

Cancel

Save

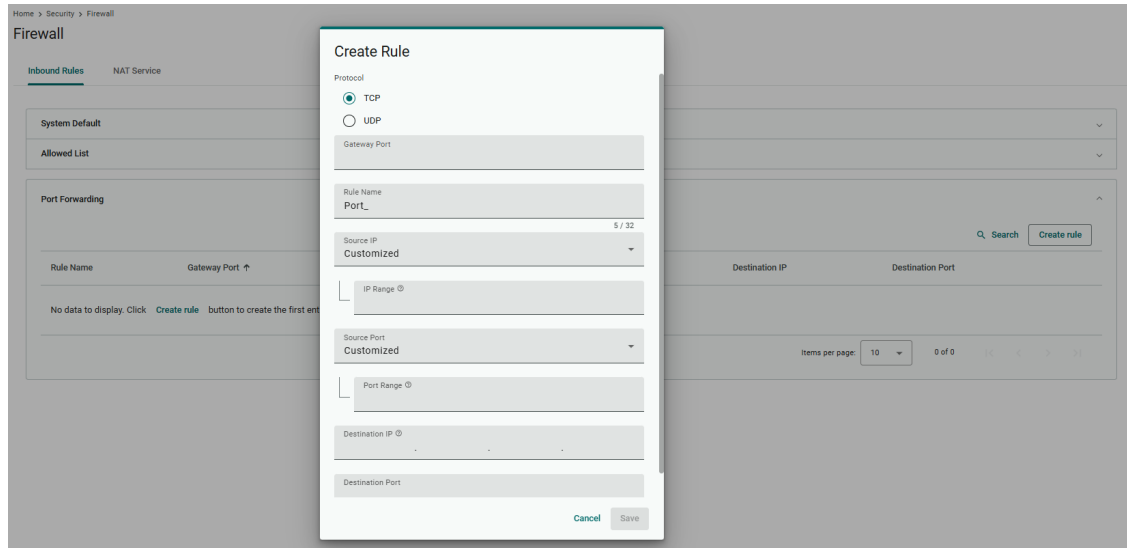
V1200 Series User Manual

43

Port Forward

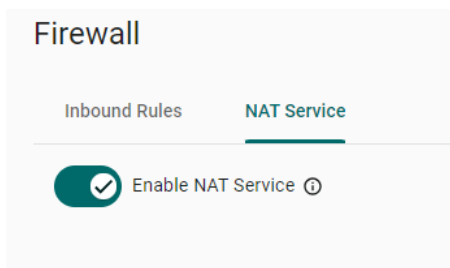
V1200 provides port forwarding function. You can create, edit, and delete firewall rules here. To create firewall rules, do the following:

1. Click **+ Create Rule**.
2. Specify the protocol, gateway port, and rule name.
3. Specify a source IP.
4. Specify the destination IP and port.
5. Click **Save**.



NAT Service

Enable the NAT service to allow child devices to connect to external networks.



HTTPS

To ensure the securely access web console of the device, HTTPS has been enabled by default.

To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority. If there are no imported certificates, the V1200 Series can generate the "ThingsPro Edge Root CA for HTTPS" certificate instead.

Home > Security > HTTPS

HTTPS

HTTP Service

☒ Redirect HTTP to HTTPS


HTTPS Service

Port Number

443


Import TLS/SSL Certificate

Certificate

 Browse

thingspro_https_default.crt

Private Key

 Browse

thingspro_https_default.key

Save

Login Lockout

To avoid hackers repeatedly logging into the account to crack the passwords, you may choose to enable the login failure lockout and configure related settings. Login Lockout has been disabled by default.

Login Lockout

To avoid hackers from repeatedly logging in into the account to crack passwords, you can enable the Login Failure Lockout setting and configure related settings.

☒ Enable login failure lockout

Max Failed Retries (times)

10

Failure Counter Reset Period (min) ⓘ

15

Lockout Period (min)

10

Save

Parameter	Value	Description	Default Value
Max Failed Retries (times)	3 to 32	You can specify the maximum number of failures retries, if exceed the retry times, V1200 will lock out for that account login	10
Failure Counter Reset Period (min)	1 to 60	The login failure counter will be recalculated after the reset period that you have set.	15
Lockout Period (min)	5 to 1440	When the number of login failures exceeds the Max Failed Retries, the V1200 will lock out for a period.	10

Session Management

You can review session statuses for all accounts and manage sessions for individual accounts.

Home > Security > Session Management

Session Management

Check the session statuses for your accounts and perform session-management tasks.

Last Updated Apr 01, 2025, 00:18:09

SearchRefresh

<input type="checkbox"/>	No.	Account	Source IP	Created On	Last Activity ↓	
<input type="checkbox"/>	1	admin	10.160.123.111 (your web)	Apr 01, 2025, 00:12:28	Apr 01, 2025, 00:20:34	

Items per page: 10

1 - 1 of 1

In the event of detecting unusual connections, you can enhance the security of your device by deleting the respective session.

The screenshot shows the 'Session Management' page with a breadcrumb trail: Home > Security > Session Management. Below the title, there is a description: 'Check the session statuses for your accounts and perform session-management tasks.' A status bar indicates '1 item selected.' and includes a 'Search' button and a 'Delete' button. A table lists session details:

<input checked="" type="checkbox"/>	No.	Account	Source IP	Created On	Last Activity ↓	
<input checked="" type="checkbox"/>	1	admin	10.160.123.111 (your web)	Apr 01, 2025, 00:12:28	Apr 01, 2025, 00:20:34	

Below the table, there is a 'Delete Session' dialog box with the following text:

Delete Session

ATTENTION: This could be a session linked for your account.

This session will be permanently deleted. Invoking this session after deletion will result in an "unauthorized" response. Are you sure you want to proceed?

Buttons: Cancel, Delete

OpenVPN Client

OpenVPN allows you to create secure connections over the internet. It provides encryption and authentication to ensure confidentiality and integrity of your data. OpenVPN uses a client-server architecture where the server acts as the VPN endpoint and the client connects to the server to establish a secure connection.

To enable the function, go to **Security > OpenVPN Client** and do the following:

1. Download the OpenVPN sample profile template.
2. Revise the profile by inputting the necessary information provided by your VPN service provider.
This information includes:
 - a. Remote server IP: This is the address of the VPN server you want to connect to.
 - b. Port number: The port through which the VPN connection will be established. The default is usually 1194.
 - c. Protocol: The protocol to be used for the VPN connection, such as UDP or TCP.
 - d. Authentication method: The method used to authenticate your connection.
 - e. Encryption settings: The encryption algorithm to be used for securing the VPN connection.
3. Import the OpenVPN profile.
You should see it listed in the OpenVPN client.
4. Click the button to enable OpenVPN client to connect.

If the connection is successful, you will be connected to the VPN network, and your internet traffic will be encrypted and routed through the VPN server.

The screenshot shows the 'OpenVPN Client' page with a breadcrumb trail: Home > Security > OpenVPN Client. Below the title, there is a description: 'Upload profile to make connection.' Below this, there is a text box: 'Upload the profile to enable the OpenVPN Client. Or download the sample profile to edit if you are not sure how to configure it.' Below the text box, there are two buttons: 'Upload Profile' and 'Download Sample'. On the right side, there is a 'No Profile' icon.

Home > Security > OpenVPN Client

OpenVPN Client

OpenVPN Client (V)

Current Profile

sample-2024-01-24-15-01.ovpn

Manage

Download the Sample File

Connection Information

Refresh

Connection Status	Local IP	Remote IP	Netmask	Gateway	
Disconnected	--	--	--	--	

System Use Notification

The System Use Notification feature is designed to provide users with essential information prior to accessing the main functionalities of the system. These notifications are displayed on the login screen to ensure users are aware of important details before logging in. The system usage notification has been enabled by default.

Home > Security > System Usage Notification

System Usage Notification

The following information will be displayed prior to the login page. You can choose not to display it.

Enable system usage notification

Mode

Default

Message to Display

This gateway system is for the use of authorized users only.

Individuals using this gateway system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Save

Account Management

You can maintain user accounts and assign a role with specific permissions to each account. These functions allow you to track and control who accesses this device.

Accounts

You can **View**, **Create**, **Edit**, **Deactivate**, and **Delete** user accounts. In the main menu, go to **Account Management > Accounts** to manage user accounts.

Home > Account Management > Accounts

Accounts

Search Create

Account Name	Role	Status	Creation Date	
admin (you)	Administrator	✓ Active	26 Aug, 2024	⋮
Op_1	Operator	✓ Active	01 Apr, 2025	⋮

Items per page: 10 1 – 2 of 2 < >

Creating a New User Account

Click on **+ Create** to create a new user account. In the dialogue box that is displayed, fill up the fields and click **SAVE**.

Home > Account Management > Accounts

Accounts

Search Create

Create New Account

Account Name

0/64

Role

Administrator

Password

Contains at least 8 characters.

Confirm Password

Email - optional

Cancel Save



NOTE

To comply with security policy and best practices, specify a strong password that is at least eight characters long, consisting of at least one number and at least one special character.

All roles, with the exception of the Administrator role, must be created prior to creating a new account associated with them. Go to Account Management > Role

Managing Existing User Accounts

To manage an account, click on the pop-up menu icon for the account.

Home > Account Management > Accounts

Accounts

Search Create

Account Name	Role	Status	Creation Date	
admin (you)	Administrator	Active	26 Aug, 2024	
Op_1	Operator	Active	01 Apr, 2025	

Items per page: 10 1 - 2 of 2

Edit

Change password

Deactivate

Delete

Function	Description
Edit	Change the role, email, or password of an existing account.
Deactivate	Does not allow the user to log in to this device.
Delete	Delete the user account. (NOTE: This operation is irreversible.)



NOTE

You cannot **Deactivate** or **Delete** the last remaining account with an Administrator role. This is to prevent an unauthorized account from fully managing this system. When the system detects only one active account when the Administrator role is selected, all items in the pop-up menu will be grayed out.

Roles

You can **View**, **Create**, **Edit**, and **Delete** user roles on your V1200 device.

Home > Account Management > Role

Roles

Search Create

Role Name	Number of Accounts	
Administrator (built-in) Users of this role have full permissions. This is a built-in role and can't be modify or delete.	1 account(s)	
Operator --	1 account(s)	

Items per page: 10 1 - 2 of 2

Click **+ Create** to set up a new user role. Specify a unique name for the role and assign the appropriate permissions. When you are done, click **Save** to create the role in the system.

The screenshot shows the 'Roles' management interface. At the top, there's a breadcrumb trail: 'Home > Account Management > Role'. Below this is the 'Roles' title and a search bar with a 'Create' button. A table lists existing roles: 'Administrator (built-in)' with 'Users of this role have full pe...' and 'Operator'. A modal titled 'Create New Role' is open in the center. It has a 'Role Name' field with 'User' entered, a 'Description - optional' field, and a 'Permission' section with checkboxes for 'Account Management', 'Maintenance', 'System Settings & Network Settings' (which is checked), 'Security Management', and 'Data Management'. At the bottom of the modal are 'Cancel' and 'Save' buttons. The background table also shows 'Number of Accounts' for each role, with '1 account(s)' for both listed roles.

You can **edit** the settings or **delete** an existing role by clicking on the pop-up menu icon next to the role. When the Role has been set up, it is available for selection under the Account.

Password Policy

You can define password policy for the V1200.

The screenshot shows the 'Password Policy' configuration page. It has a breadcrumb trail: 'Home > Account Management > Password Policy'. The title 'Password Policy' is at the top. Below it is an 'Info' box stating: 'This setting will be applied to the password of new accounts or to future password changes. Existing passwords will not be affected.' A paragraph explains: 'To enhance security, set a password with minimum password length and apply the password-strength policy.' There's a 'Min Password Length' field set to '8'. Below that is the 'Password Strength Policy' section with three checkboxes: 'Requires at least one digit (0-9)', 'Mix upper-case and lower-case letters (A-Z, a-z)', and 'Include at least one special character (~`!@#\$%^&*()_+=0[]|\\"';<>?,./)'. A paragraph states: 'Upon logging in, the system will send password-change reminders when an account has reached the Reminder Threshold set.' There's a checked checkbox for 'Enable password change reminders' and a 'Reminder Threshold (days)' field set to '180'. At the bottom is a 'Save' button.

Parameter	Value	Description	Default Value
Min. Password Length	8 to 256	The minimum password length.	8
Password Strength Policy	N/A	To define how the V1200 checks the password's strength.	Disabled
Password Change Reminders	N/A	Notify user to change the password.	Enabled
Reminder Threshold (days)	10 to 360 days	Period to remind the change of password.	180

Maintenance

Service



NOTE

To be able to use SSH, you must first enable the Debug Mode.

To enhance system security, make sure to disable any services that are not in use. Enable or disable system services by toggling the switches in Maintenance > Service.

Home > Maintenance > Services

Service

Users can enable/disable system services by toggling the buttons.

Service List

BIOS Menu

Discovered Service

Debug Mode

Local Console

Internet Check Alive Service ⓘ

Reboot

If you want to reboot the device, go to **Maintenance > Reboot** and click **Reboot Now**.

Home > Maintenance > Reboot

Reboot

History of the Last Reboot: Mar 25, 2025 13:35:18

Reboot Now

Config. Import/Export

Go to **Maintenance > Config. Import/Export**, where you can import or export the configuration file. The exported configuration file will be compressed into the **tar.gz** format and downloaded on your computer.

Home > Maintenance > Config. Import/Export

Config. Import/Export

Export


Click Export to save the current system log file and export it.

Export

Import

Click Browse to select and upload a previously exported configuration file.

Configuration File

 **Browse**

Upload



Backup & Restore

The backup function backs up the data on V1200 device to a file (only one back up file can be created at a time). Backup files are encrypted and stored in a designated location on the device. You can restore the data from the backups when needed.

Home > Maintenance > Backup & Restore

Backup & Restore

The backup function backs up the data (excluding Audit Log and System Log, which can be manually exported from the relevant page) on V1200 devices to a file. Backup files are encrypted and stored in a designated location on the device. You can restore the data from the backups when needed.

	V1200 Backup File	Manage ▾
	None	Backup
Last Backup: --		Restore
File Size: --		Delete

Software Upgrade

Before performing a software upgrade, take the following precautions:

- Back up your configuration before upgrading the software
- Ensure that the device has power during the entire process
- Ensure that the connection to the software source is not interrupted during the upgrade process

Upload Package

A pack that integrates all patches between two versions (e.g., from version 1.0 to version 1.1.) This scenario is applicable when the V1200 cannot access the Internet.


Home > Maintenance > Software Upgrade

Software Upgrade

[Upload package](#) [Upgrade Settings](#) [Upgrade History](#)

You can upload a product package file or patch file from your local drive.

Local File

 [Browse](#)

[Upload](#)

Upgrade Settings

Home > Maintenance > Software Upgrade

Software Upgrade

[Upload package](#) [Upgrade Settings](#) [Upgrade History](#)

☒ Save disk snapshot before upgrading

[Save](#)

Upgrade History

This page shows the latest upgrade records.

Home > Maintenance > Software Upgrade

Software Upgrade

Upload package Upgrade Settings **Upgrade History**

This page shows the latest upgrade records.

Latest History

Type	Name	Version	Status	Last Update
No upgrade history available.				

Items per page: 10 0 of 0 <

Reset to Default

There are two ways to reset to the default.

1. If you only want to reset the configuration settings, use the **Reset** under **Configuration Reset**.
2. If you want to reset both the configuration settings and revert to the factory default firmware settings, use the **Reset** under **Factory Reset**.

Home > Maintenance > Reset to Default

Reset to Default

Configuration Reset

If you wish to revert all configurations to their default settings, please utilize the "configuration default" option. It's important to note that the DLM connection will remain active (excludes **EULA agreement**).

> Show details on storage location of log files

☐ Reserve network settings

Reset

Factory Reset

If you want to reset the device back to the factory default use the **Factory Reset** function. It's important to note that the DLM connection will remain active.

Reset



NOTE

When **Reserve network settings** under **Configuration Reset** is selected, the VRRP settings will not be reserved; it will be reset to the default.

Device Retirement

Utilize this function when the device is being retired, and you wish to securely delete all files and logs for security purposes to ensure the data cannot be recovered. Due to the low-level formatting of memory that is required to erase data, it may take approximately 1.5 hours.

Device Retirement

You can initiate a process to securely erase a device, including all software, settings, and data on its internal disk. With this, the device will be restored to the factory default settings and all log files cleared, thereby preventing any potential data recovery from the device.

Retire

Diagnostics

System Log

The main purpose of system log is to help Moxa engineers with troubleshooting. When you encounter an issue that you are not able to solve by yourself, export the log file and send it to Moxa TS for analysis.

Go to **Diagnostic > System Log** to export the system log file and specify the location to save the system logs.

Click **Storage Settings** to specify the location to store the event logs. To optimize the use of storage space on your V1200, you can check the Enable **Time to Live** option and specify the maximum storage space for the system logs. Click **Save** to confirm your settings.

Home > Diagnostics > System Log

System Log

You can utilize the system log for error diagnosis and adjust the storage location and related settings of the system log through [Storage Settings](#).

Export

Click Export to save the current system log file and export it.

Export

Audit Log

When you face issues, you can go to **Diagnostic > Audit Log** to check historical events that help you to narrow down the problems. When there are a large number of event logs, exporting them allows for easier review. The audit logs can be exported and downloaded onto your computer.

Home > Diagnostic > Audit Log

Audit Log

Log ViewLog Settings

Q SearchExport

Type	Name	Content	Source	Timestamp ↓
> Notice	loginSuccess	Account admin login success.	System	Feb 01, 2024, 14:51:02
> Notice	loginSuccess	Account admin login success.	System	Feb 01, 2024, 14:41:42
> Notice	loginSuccess	Account admin login success.	System	Feb 01, 2024, 14:05:48
> Notice	configurationExport	Configuration export success.	admin	Feb 01, 2024, 13:49:14
> Notice	configurationExport	Configuration export success.	admin	Feb 01, 2024, 13:48:49
> Notice	loginSuccess	Account admin login success.	System	Feb 01, 2024, 13:44:07
> Notice	loginSuccess	Account admin login success.	System	Feb 01, 2024, 13:40:18
> Alert	loginFailure	Login fail.	System	Feb 01, 2024, 13:39:13
> Notice	loginSuccess	Account admin login success.	System	Feb 01, 2024, 13:36:45
> Notice	loginSuccess	Account admin login success.	System	Feb 01, 2024, 13:26:53

Items per page: 101 - 10 of 4531<<>>|

In the **Log Settings**, you can specify the storage size to store the logs and notification threshold. Also, you also can enable time to live for maximum stored days.

Home > Diagnostics > Audit Log

Audit Log

Log ViewLog Settings

Storage Reserved (MB) ⓘ
100

Notification Threshold (%) ⓘ
80

☐ Enable time to live

Save

A. Security Hardening Guide

This chapter provides an overview of security strategy, standards, and recommended best practices to improve the security landscape.

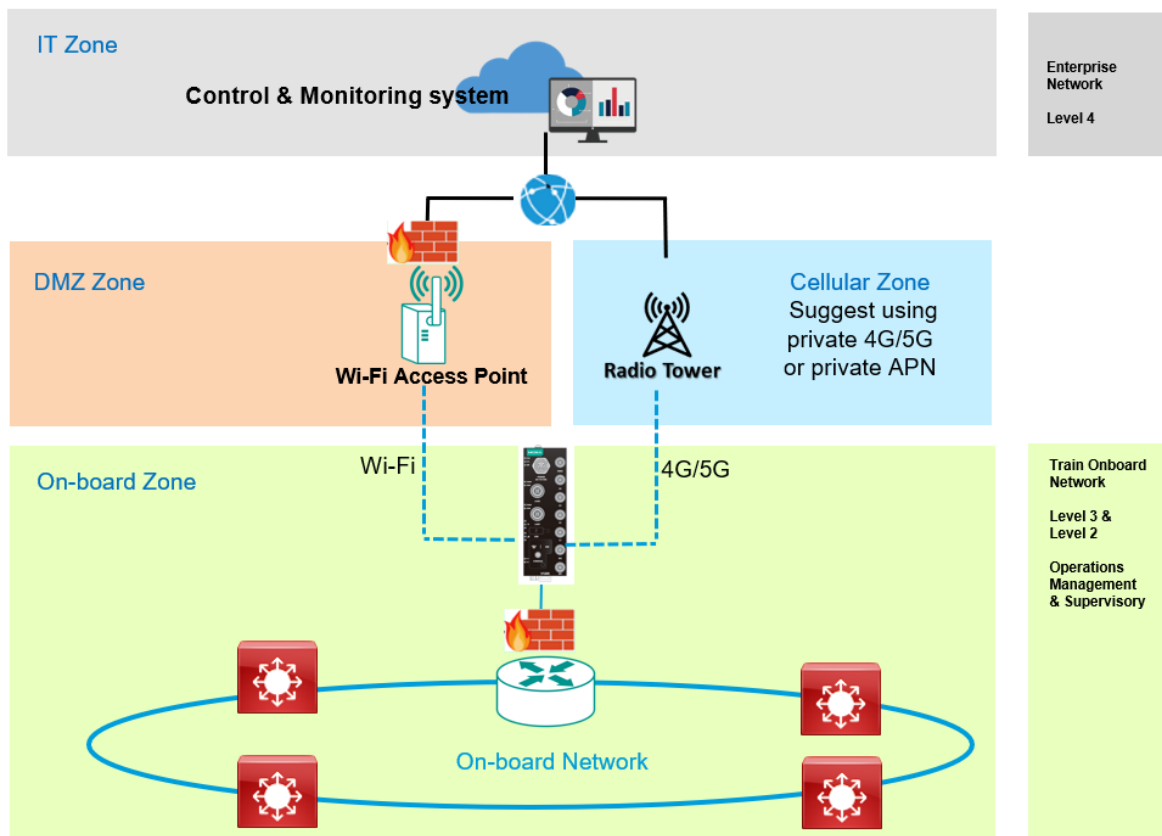
The threat landscape is constantly evolving, and no security guide can ever provide 100% protection. This chapter is constantly being expanded, and is not exhaustive.

Security Best Practices

Product Security

This section provides essential information on the installation of your product.

The diagram below illustrates common network architectures used to maintain network security.



Physical Installation Guidelines

Physical protection of devices is vital to network security. With physical access to devices, prospective attackers can physically bypass security mechanisms, alter network conditions, or plant additional malicious devices in networks.

Follow these tips to help reduce the risk of tampering with networking devices by unauthorized personnel.

- The device **MUST** be installed in an access-controlled area. Where only the necessary personnel have physical access to the device. To further protect your device from potential physical attacks, it is important to implement appropriate physical security measures. This may include CCTV surveillance, security guards, locks, and access control systems, among other measures. The specific measures you choose should be based on your environment and the level of risk you face.
- Security screws are used on the enclosures as a physical tamper-resistance measure, enhancing the difficulty of accessing the internal components in the event of a physical security breach.

Account Management Guidelines

V1200 supports local account authentication. You can manage user accounts, set passwords, and restrict access to allow only authorized personnel.

- Assign the appropriate account privileges.
Limit the number of users with full read and write privileges to only those who need to perform device configuration or modifications. For other users, read-only access is sufficient. For details, refer to Account Management.
- Implement good password practices. Good password practices include:
 - a. Enabling and configuring a Password Policy to ensure your password meets specified requirements.
 - b. Setting the minimum password length to at least eight characters.
 - c. Require passwords to have at least one uppercase and lowercase letter, a digit, and a special character.
 - d. Updating passwords regularly.
 - e. Never sharing passwords.Refer to [Password Policy](#) for details.
- Assign a Web Welcome message:
 - The welcome web message can reference local regulatory requirements or proprietary property declarations to deter malicious attackers.
 - The system also allows the definition of a **Web Login Fail Message** to notify users within the web interface when authentication fails.
 - The system holds all the attempts of login within the device. These traces could be found in **Diagnostic > Audit Log**.
 - These logs do not provide any indication of the reason for the login failure, thereby preventing attackers from gaining insights into current usernames or passwords.

Protecting Vulnerable Network Ports

Understand security risks and mitigate them by configuring network ports correctly. Properly securing network ports is critical to maintaining the integrity of the network

- Disable any service or functionality that is not in use, as they could pose an unacceptable security risk.
- Regularly monitor port activity through logging and alerting mechanisms to detect unauthorized connection attempts or unusual traffic patterns.
- Configure appropriate firewall rules and IP Sets to restrict traffic flow between network segments based on the principle of least privilege.
- Use encrypted communication protocols wherever available. Device only allows you to use HTTPS, and SSH for management purposes, use SNMPv3 instead of SNMPv1/v2c.
- Generate new certificates and keys for the devices prior to using HTTPS or SSH applications.
- Generate new certificates and keys for backup configuration files prior to dealing with backup settings.
- For security-critical applications, it is highly recommended to use a private APN for cellular networks.

Refer to the following sections for additional details:

- [Certificate Center](#)
- [Firewall](#)

Maintaining Communication Integrity

Maintaining Communication Integrity

Ensure that information sent is accurate, complete, and secure.

Maintaining communication integrity reduces risks risk of data corruption or interception, and associated security breaches, data loss, and other negative effects on networks and their users.

- Use encryption.
Encryption uses mathematical algorithms to convert data into a secret code, making it extremely difficult for people without the correct codes to read or change the data. By using encryption, you can ensure that the data being transmitted is secure and cannot be intercepted by unauthorized users.
- Use digital signatures.
Digital signatures verify the authenticity and integrity of digital documents or messages. Using a digital signature, you can ensure that the message or document came from the expected sender and has not been altered.
- Use access control.
Access control restricts access to only authorized users to the network and its resources. By implementing access control measures, such as specifying the source IP address and source port via firewall rules, you can prevent unauthorized access and reduce the risk of data breaches.

Communication Integrity Features

Moxa devices provide support for VPNs and secure versions of protocols to help maintain communication integrity.

VPN (Virtual Private Network)

VPN is a secure network connection allowing users to access a private network. VPNs use encryption and authentication to protect the data in transit, which makes it difficult for anyone to intercept or tamper with the data. VPNs also provide access control features to ensure only authorized users can access the network. VPNs are commonly used to securely connect Ground control centers to a rail network securely or to allow secure access to restricted resources.

Refer to [VPN: OpenVPN](#) for more information.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is a secure version of the regular HTTP protocol for transmitting data over the internet. HTTPS uses TLS (Transport Layer Security) encryption and digital certificates to protect the data in transit from interception, tampering, or eavesdropping.

Refer to [Certificate Center](#) for more information.

SSH (Secure Shell)

SSH is a secure protocol for remote terminal login and secure file transfers. SSH uses encryption to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SSH also provides authentication and access control features to ensure only authorized users can access the network.

Refer to [Certificate Center](#) for more information.

Device Access Control Best Practices

Device access control is an essential aspect of network security that helps protect against unauthorized access to network resources. Unauthorized access can occur through various means, including physical access to network devices, hacking, or social engineering. Without proper access control measures in place, networks are vulnerable to security breaches, data theft, and other malicious activities. The following are some ways to ensure device access control:

- Use strong passwords. Passwords should be complex and unique for each device.
Refer to [Password Policy](#) for further information.
- Use a firewall. Firewall is a network security device operating at the OSI model's network layer. Firewalls can monitor and filter traffic based on IP addresses, ports, protocols, and other network-level attributes. Using firewalls, network administrators can prevent unauthorized access to the network and block potential security threats.

Refer to [Firewall](#) for further information.

About Device Integrity and Authenticity

Integrity and authenticity are vital elements of trust within a network.

Device integrity refers to the state of a device being complete, unaltered, and free from any unauthorized changes or modifications.

Authenticity refers to the assurance that the device is genuine and comes from a trusted source.

Both integrity and authenticity are critical aspects of device security. Methods to sustain these aspects include:

- Configuration Backup & Encryption
- Secure Boot

Configuration Backup and Encryption

Configuration backup and encryption protects a device's sensitive data and configuration by creating an encrypted copy storing it securely. In the event of unauthorized device changes, correct configuration information can be quickly and securely restored.

The process involves creating a backup of the device's configuration and then encrypting it using a strong encryption algorithm. The encrypted backup is then stored securely to prevent unauthorized access. This process is particularly important for devices that store sensitive information, such as network equipment, servers, and other critical infrastructure. Encrypting the configuration backup ensures that the data remains protected even if the backup location is compromised.

Secure Boot

Secure Boot is a security mechanism designed to ensure that devices boot using only software that is verified as trusted. The primary function of Secure Boot is to prevent unauthorized software from running during the boot process. It achieves this by verifying the integrity and authenticity of the bootloader and firmware.

A bootloader refers to the initial software that runs when a device is powered on. Its primary role is to load the device's operating system. Firmware is software embedded within the device that manages and controls the device's hardware functions.

Moxa hardware makes use of cryptographic modules embedded in devices to support verification processes. The device's BIOS contains approved bootloaders and associated digital certificates, which are used to verify the integrity of the firmware.

When the device boots, the first thing to run is the bootloader. Secure boot checks the digital signature against the certificate stored in BIOS. If the signatures match, the boot process continues. If they do not match, or there is evidence of tampering, the boot process halts to prevent potential security breaches.

Device Resource Monitoring

Device Resource Monitoring

Network device resource management is essential for network reliability and security. By monitoring use of network resources, administrators can verify that network guidelines are being followed and devices are operating efficiently and effectively.

Proactive monitoring and management of device resources such as CPU utilization, memory utilization, and network traffic allows administrators to identify potential security breaches early, and help avoid network downtime and disruption. For example, abnormal spikes in network traffic or CPU utilization could be indicative of a malware infection or a denial-of-service attack.

Examples of activities to monitor include:

- CPU usage
- Memory usage
- Interface status
- Wireless signal and bitrate
- Cellular and SIM status

Refer to [Dashboard](#) for more information.

Event Logs

In addition to real-time monitoring and management, Moxa devices provide advanced logging options to help identify security events. Those events can feed into larger security monitoring systems.

Moxa devices offer two kinds of logs:

- System Logs: It holds details of all system-related event logs.
- Audit Event Log: It holds information about file access, system calls, user authentication, network connections, and other security-related events. It's suitable for forensic investigation.

Refer to the following sections for additional information:

- [System Log](#)
- [Audit Log](#)

Recommended Settings for Services and Features

When prioritizing device security, the first point of assessment is often the network interfaces and services. By deactivating unneeded interfaces and services, one can reduce potential vulnerabilities and associated security threats. Additionally, activating the appropriate security features enhances early anomaly detection and bolsters the device's defense against cyber-attacks.

Common Protocols and Ports

Service Name	Default Port	Default Setting	Security Suggestions
HTTPS	TCP 443	Enabled	
SSH	TCP 22	Disabled	Disable the service if it is not in use.
NTP	UDP 123	Disabled	Disable the service if it is not in use. Enable NTP authentication if possible.
SNMP server	UDP 161 UDP 162	Disabled	Disable the service if it is not in use. SNMP v3 is recommended option for enhanced security. For V1 & V2c, change default community string names, i.e. public & private, to other unique names. For V3, enable SNMP admin account authentication.
DHCP server	UDP 67	Disabled	Disable the service if it is not in use.

Security-Related Functions

Function	Default Setting	Security Suggestions
Password Policy	Enabled	Strong password policy to comply enterprise security policies is enabled by default.
Login lockout	Disabled	It is highly recommended that administrators enable the login failure lockout and configure the related settings after the initial device setup to prevent repeated login attempts and password-cracking attacks.
Session Management	Enabled	Session Management allows administrators to control user accounts, connection sources, and the number of concurrent sessions. It is recommended to set a limit on the maximum number of sessions that a single account can establish simultaneously to prevent unauthorized connections. Delete any connections that are unfamiliar, especially when an account has more than one active session.
OpenVPN Client	Disabled	It is recommended to enable OpenVPN when communicating over public networks to provide secure, encrypted tunnels for remote access and maintenance. Adopt certificate-based authentication and configure strong encryption algorithms, such as AES-256, while avoiding legacy ciphers. Limit OpenVPN access to specific source IP ranges or networks through firewall rules, and assign unique certificates to each client connection instead of using shared certificates to enable granular access control.
Firewall	Enabled	By default, the V1200 disables all ports except the reserved ports: HTTP (port 80), HTTPS (port 443), SSH (port 22), and the discovery service (port 5353). It is highly recommended to configure firewall rules that specify the source IP address and source port to drop or reject unsolicited incoming traffic on the interfaces, allowing access only for authorized users.
NAT	Disabled	Only enable NAT when child devices need to connect to external networks to prevent unnecessary exposure of internal devices.

Common Threats and Countermeasures

These are examples of common known threats, and suggestions for mitigation.

Incident Category	Detailed Description	Mitigation Suggestions
Tampering & Information Disclosure	An attacker can read or modify data transmitted over HTTP data flow.	Use HTTPS instead of HTTP. (Device redirects all incoming HTTP to HTTPS)
Tampering & Information Disclosure	An attacker can read or modify data transmitted over Telnet data flow.	Use SSH instead of Telnet. (Device does not allow to use Telnet)
Denial of Service	Web Server crashes, halts, stops, or runs slowly by excessive quires.	ICMP is currently not supported. Rate limiting is enabled by default for the web service APIs to mitigate potential Denial-of-Service (DoS) attacks. Users can further enhance security by configuring per-account session limits and regularly removing connections from unfamiliar IP addresses to prevent unauthorized access.
Denial of Service	Device halts, stops, or runs slowly by an icmp flood attack.	ICMP is currently not supported. Rate limiting is enabled by default for the web service APIs to mitigate potential Denial-of-Service (DoS) attacks. Users can further enhance security by configuring per-account session limits and regularly removing connections from unfamiliar IP addresses to prevent unauthorized access.

Refer to [Security](#) setting for more information.

Recommended Operational Roles and Duties

Adhering to the principle of least privilege reduces risks by ensuring users operate at the minimum privilege required to complete their tasks.

Device allows for individual allocation user permission for each specific web functions.

For optimized device security, we recommend assign privileges levels according the needs of each user that could be added.

Refer to [Account Management: Roles](#) for further information about role-based settings.

admin

This is the sole default user available from the outset.

This user has an access level of read and write for all settings and views. The device will force the first time to set up a proper password according to the password policies. With the admin role it could create additional user accounts with specified permission. The permission includes:

Account Management	<ul style="list-style-type: none">• Account Management Permission
Maintenance	<ul style="list-style-type: none">• Reboot Device, Backup & Restore, Configuration Import/Export, Software Update, Reset to Default, Device Retirement, System Log, ...• SSH Server, Discovered Service, BIOS Menu, ...
System settings & Network Settings	<ul style="list-style-type: none">• Networking: Ethernet, Cellular, Wi-Fi Client, Network Management, VRRP, ...• Peripheral Interface: Serial Ports, ...• System Settings: General, Time, GPS, SNMP, ...
Security Management	<ul style="list-style-type: none">• Audit Log Permission• HTTP Server Permission• Firewall Management Permission• Session Management Permission• Certificate Management Permission
Data Management	<ul style="list-style-type: none">• System Dashboard Permission• Network Dashboard Permission• Tag Dashboard Permission

Recommended Patching and Backup Practices

Recommended Patching and Backup Practices

Moxa's guidance on ensuring device security through regular firmware upgrades and configuration backups.

Firmware Upgrade

Moxa continuously releases firmware throughout the product lifecycle to improve features and rectify identified issues. Upon discovering a vulnerability, our approach aligns with the Moxa Product Security Incident Response Team (PSIRT) guidelines, ensuring swift and appropriate action.

Maintaining current firmware on your network devices is vital to maintain security. Using outdated firmware can expose the device to potential threats. We strongly advise periodic firmware updates. We consistently release the latest firmware and software on our official website, along with respective release notes. Check for these updates regularly.

Configuration Backup

For network operators and system administrators, it is essential to regularly back up device configurations. This precaution allows for quick recovery in unforeseen scenarios, such as cyber-attacks.

Refer to:

- Firmware Upgrade
- Configuration Backup and Restore

Recommendations for Vulnerability Management

As the adoption of the Industrial IoT (IIoT) continues to grow rapidly, security becomes an increasingly high priority.

The Moxa Product Security Incidence Response Team (PSIRT) takes a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

To report vulnerabilities for Moxa products, please submit your findings on the following email:
psirt@moxa.com.

Recommendations for Secure Disposal

Prior to disposing of this device, the following steps must be completed to ensure secure data removal and compliance with applicable regulations:

- **Backup Critical Data:** Securely save configuration files, system logs, or other relevant data to an approved storage location before initiating the disposal process
- **Remove All Sensitive Configurations and Data (Decommissioning Phase):** Remove all user-specific configurations, including network settings, user accounts, digital certificates, and cryptographic keys. To avoid the disclosure of sensitive information such as account passwords or network configurations, this shall be performed via the device's web interface Device Retirement button to ensure the complete deletion of all imported certificates and full restoration to factory default settings.
- **Physical Preparation:** Extract and separately destroy any removable storage media (e.g., SD cards) that may contain sensitive information, following approved data destruction protocols.
- **Documentation:** Record the device's serial number, disposal date, and the method of disposal. This documentation is essential for compliance tracking and audit purposes.
- **Authorized Disposal:** Engage a certified electronic waste disposal provider that issues a formal certificate of destruction, verifying proper handling and disposal of the device.
- **Verification and Record Retention:** Ensure that disposal certification documents are obtained and securely stored for future reference and regulatory compliance.

Important Notice

This device must not be discarded through regular waste channels. Industrial-grade device may contain hazardous components and must be processed by certified e-waste facilities in accordance with local environmental regulations.

Refer to [Backup & Restore](#) and [Device Retirement](#) for further information about restore and decommission functionalities.

B. Regulatory Approval Statements

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated at a minimum distance of 20 cm between the radiator and your body.

This device and its antenna must not be co-located or operating with any other antenna or transmitter.