The Security Hardening Guide for the Rail Wi-Fi 4 Series

Moxa Technical Support Team

support@moxa.com

Contents

 Released on Jan 8, 2026

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778

1 Introduction

This document provides guidelines on how to configure and secure Rail Wi-Fi 4 Series devices. You should consider the recommended steps in this document as best practices for security in most applications. We highly recommend that you review and test the configurations thoroughly before implementing them in your production system to ensure that your application is not negatively affected.

2 General System Information

2.1 Basic Information About the Device

The Rail Wi-Fi 4 Series acts as an access point or client in a wireless network, installed at the railway wayside or onboard to provide wireless connectivity for train-to-ground communication.

The Rail Wi-Fi 4 Family covers several product Series.

Model	Role	Operating System	Firmware
AWK-3131A-RTG	WLAN AP/Client	Moxa Operating System	v1.9 and later
TAP-213	WLAN AP/Client	Moxa Operating System	v1.9 and later
TAP-323	WLAN AP	Moxa Operating System	v1.9 and later

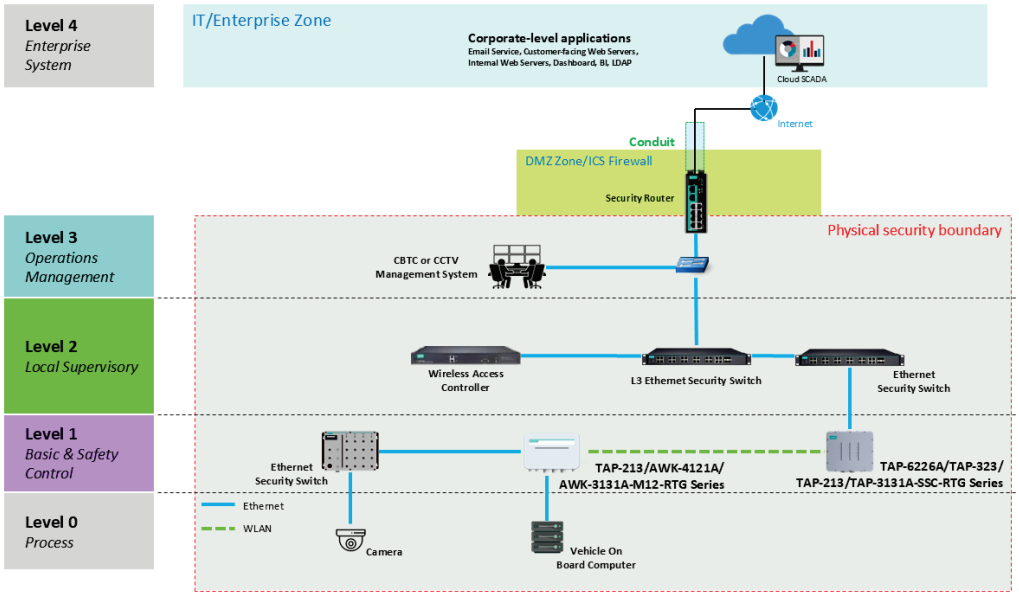
2.2 Deployment of the Device

The AWK Wi-Fi 4 Family (AWK-1137C Series, AWK-1131A Series, AWK-3131A Series, AWK-4131A Series) devices must be installed and operated within an access-controlled environment, including the wireless coverage area, where only authorized personnel have physical and logical access to the AWK Series device.

The device should never be directly connected to the Internet. Always deploy the AWK Series device within a defined security perimeter with appropriate firewall protection, such as behind a secure router or switch. Any external network communications should be protected using secure communication mechanisms such as HTTPS and TLS encryption.

In addition, application service servers such as DHCP, NTP, and RADIUS servers should be securely configured and authenticated before being allowed to access the network security perimeter.

Refer to the following diagram for an example of a secure deployment.



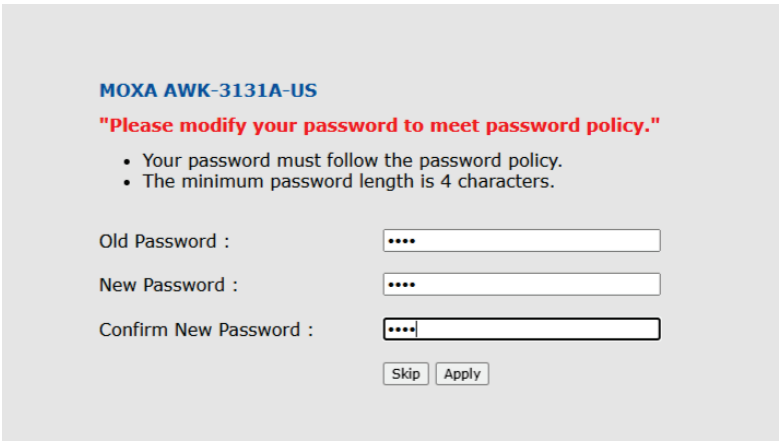
3 Configuration and Hardening Information

3.1 Initial Setup

For security reasons, account and password protection is enabled by default. You must provide the correct username and password to unlock the device before entering the web console or CLI interface.

The default login credentials are:
Username: **moxa**
Password: **admin**

Once you are successfully logged in, you will be prompted to update the default password. You must update the default password to continue accessing the device and configure settings.



3.2 TCP/UDP Port Status and Suggested Settings

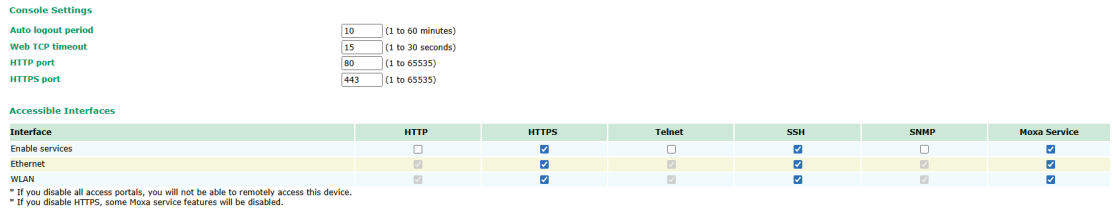
For security reasons, it is recommended to disable any unused services. After completing the initial setup, use services that support more secure protocols such as HTTPS, SSH, or SNMPv3, to reduce security risks.

Rail Wi-Fi 4 Series devices can be securely integrated with user applications and network management systems, helping to ensure stable operations while enhancing security and manageability. To integrate Rail Wi-Fi 4 Series devices into your network topology and secure applications, consider managing the following services with the appropriate settings to enhance the security architecture of the network.

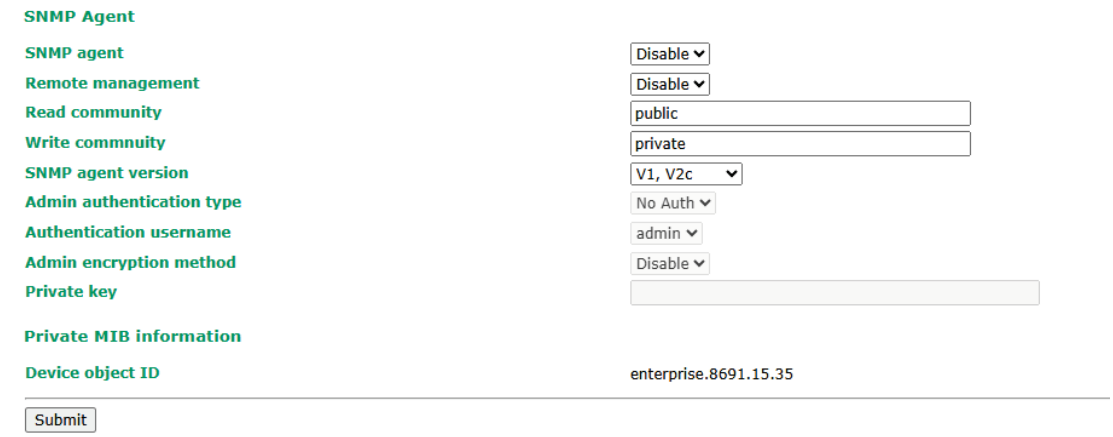
Refer to the following table for an overview of all the services, protocols, and ports used for communication by Rail Wi-Fi 4 Series devices.

Process Name	Suggested Setting	Type	Port Number	Description	Security Remark
HTTP Server	Disable	TCP	80	Web console	Disable HTTP services for transmissions involving plain text.
HTTPS Server	Enable	TCP	443	Secured web console	Encrypted data channel with trusted certificate for AWK configurations.
SSH	Enable	TCP	22	SSH console	Enable SSH if you prefer to configure the device via the console. If you prefer the web GUI, disable SSH.
Telnet Server	Disable	TCP	23	Telnet console	Disable this service when it is not in use.
SNMP	Disable	UDP	161	SNMP handling routine	We suggest enabling this service using SNMPv3 instead of SNMPv1/v2c.
SNTP/NTP Client	Enable	UDP	123	For assigning an IPv4 IP address to DHCP clients	Only authorized personnel is allowed to enable this service. The service is stored in a trusted, isolated zone.
DHCP Server	Disable	UDP	67	For assigning an IPv4 IP address to DHCP clients	Use DHCP only within trusted, isolated network zones.

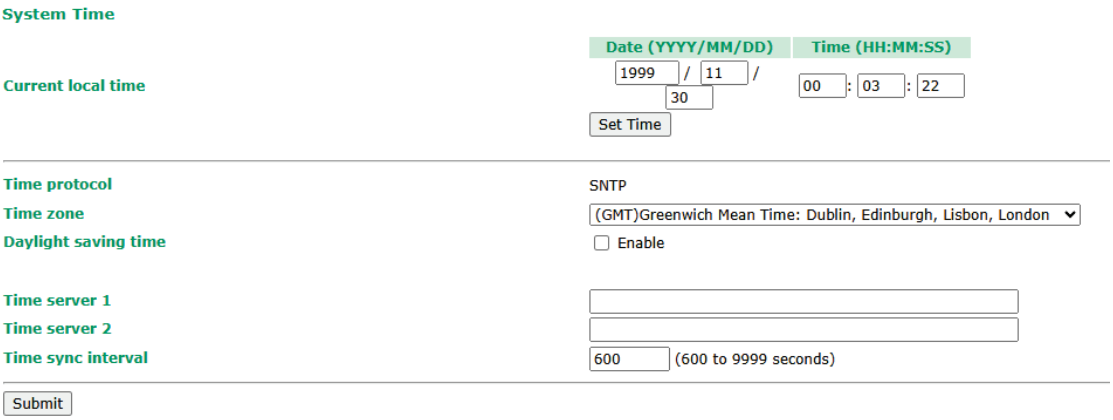
For optimal security, we recommend only allowing access to the device via the secure HTTPS and SSH interfaces. To configure access interfaces, go to **Maintenance > Console Settings**.



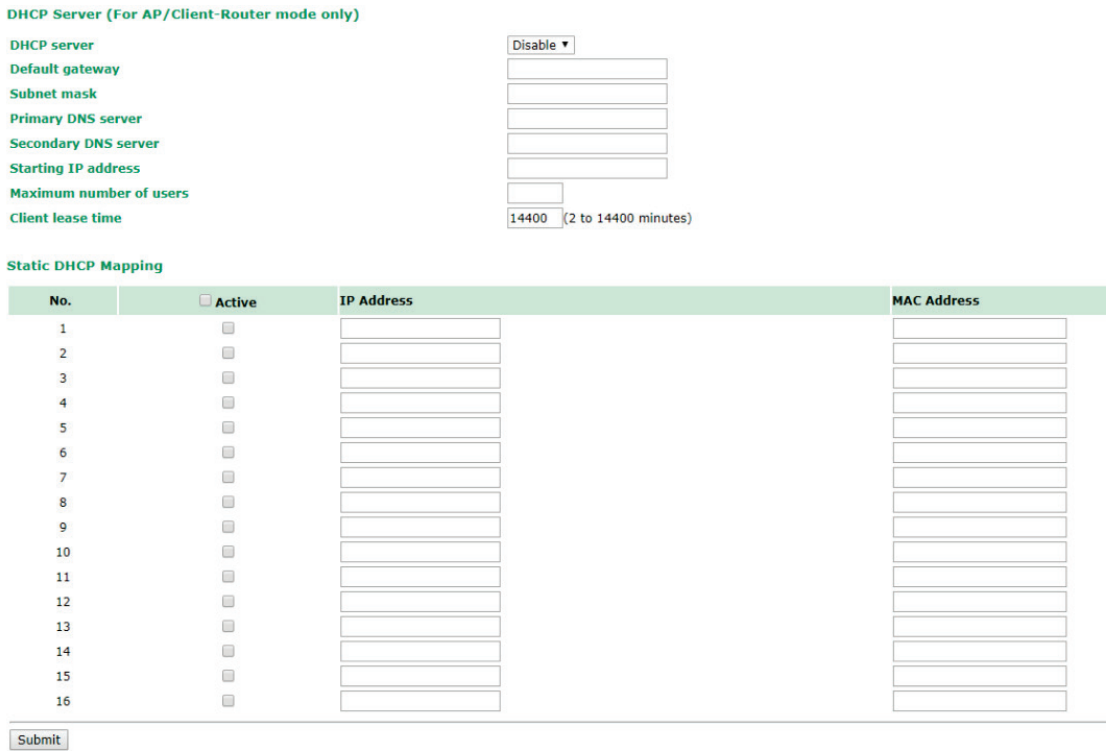
To disable the SNMP agent service, go to **Advanced Setup > SNMP Agent**. Set the **SNMP Agent** setting to **Disable**. This service is disabled by default.



To disable the SNTP server, go to **General Setup > System Time**. Leave the **Time Server 1/2** fields blank.



To disable the DHCP server (for AP/ Client-router mode only), go to **Status > DHCP Client List**. Set the **DHCP Server** setting to **Disabled**. This service is disabled by default.



Note When modifying any of the above service settings, click the **Submit** button to save your changes and restart the device for the new settings to take effect.

3.3 HTTPS and SSL Certificates

For security reasons, Rail Wi-Fi 4 Series devices only support the TLS v1.2 cryptographic algorithm to protect your HTTPS/SSH applications. Make sure to use a web browser that supports TLS v1.2 to access the device's web interface. Refer to the following table for an overview of all compatible browsers with TLS v1.2 support.

Browser	Version
Microsoft Edge	All versions
Mozilla Firefox	v27 and above
Chrome	v38 and above
Apple Safari	v7 and above for OS X 10.9 (Mavericks) and above

Reference: https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility#Browsers.

We recommend that administrators use HTTPS with an internally generated certificate or an imported certificate issued by a Certificate Authority (CA) to configure the device.

To manage HTTPS certificates, go to **Maintenance > Console Setting**.

Importing a third-party SSL certificate from a trusted authority helps enhance security.

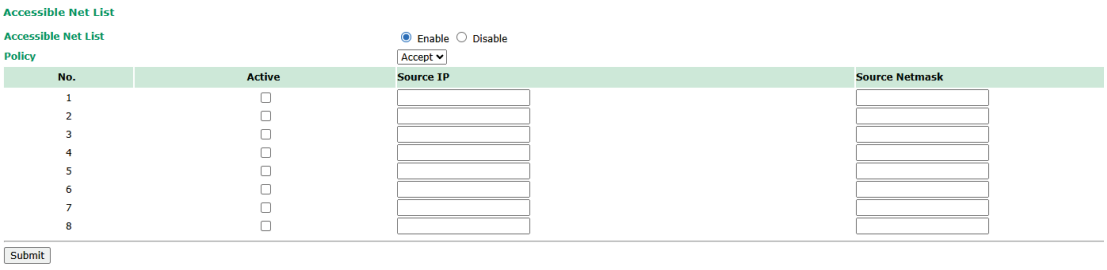
To import a third-party trusted SSL certificate, use the following instructions:

1. Create a certification authority (Root CA)), such as Microsoft AD Certificate Service (https://mizitechinfo.wordpress.com/2014/07/19/step-by-step-installing-certificate-authority-on-windows-server-2012-r2/).
2. Find a tool to issue a certificate signing request (CSR) file. Get one from a third-party CA company such as DigiCert (https://www.digicert.com/easy-csr/openssl.htm).
3. Submit the CSR file to a public certification authority to get a signed certificate.
4. Import the signed SSL certificate into the device. Note that Rail Wi-Fi 4 Series devices only support certificate files in **.pfx** or **.p12** format.

3.4 Accessible Net List

Rail Wi-Fi 4 Series devices support the **Accessible Net List** function, which allows you to add or block remote host IP addresses to prevent unauthorized access. If enabled, the host IP addresses in the list will either be allowed to access the device or blocked, depending on the selected **Policy**.

To configure the access list, go **Maintenance > Console Settings**. Set the **Accessible Net List** to **Enable** to activate this function.



Select a **Policy** and add the host IP addresses to the list. Depending on the selected **Policy**, the following behavior will take effect:

- **Accept**: Only the host IP addresses in the list are allowed to access the Rail Wi-Fi 4 Series device. All other hosts will be blocked.
- **Block**: The host IP addresses in the list will be blocked from accessing the Rail Wi-Fi 4 Series device. All other hosts will be allowed.

You can add a specific address or range of addresses by using a combination of an IP address and a netmask as follows:

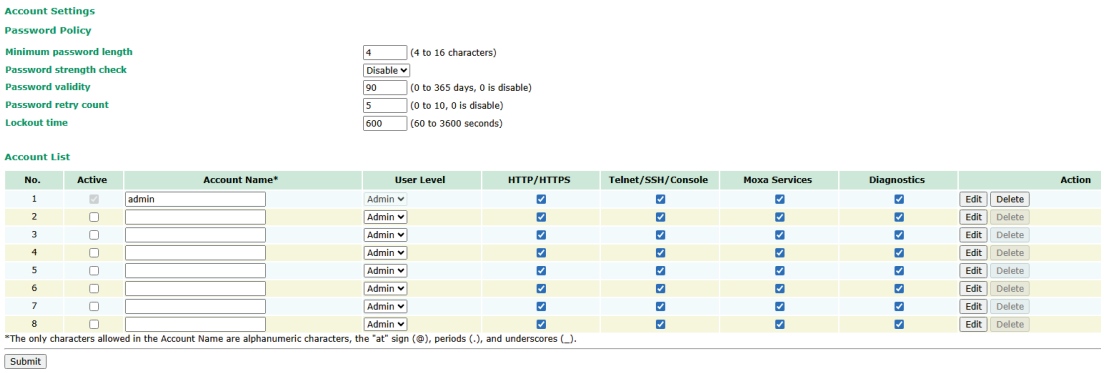
- To add a specific IP address: Enter the IP address in the **Source IP** field and enter 255.255.255.255 as the netmask.
- To add hosts on a specific subnet: For both the IP address and netmask, Use 0 as the last digit for both the IP and netmask (e.g.: IP address: 192.168.1.0, Netmask: 255.255.255.0).
- To allow all IP addresses: Set **Accessible Net List** to **Disable**.

WARNING

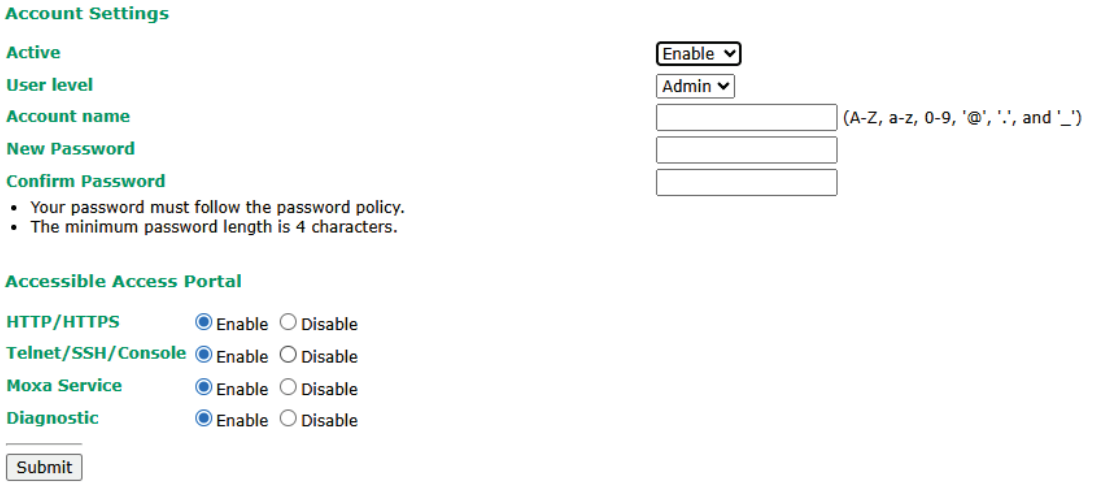
Depending on the selected **Policy** (Accept or Block), ensure that the IP address of the PC you are using to access the web console is added to or omitted from the **Accessible Net List**.

3.5 Account Management

You can configure multiple user accounts on Rail Wi-Fi 4 Series devices, each with a specific role. To manage accounts, go to **Maintenance > Account Settings**.



Click **Edit** in the **Action** column to modify the corresponding user account.



For optimal security, follow these best practices when setting up user accounts for the Rail Wi-Fi 4 Series devices.

3.5.1 User Levels

Assign the correct privileges to each account. Only allow the minimum number of people to have admin privileges to perform device configurations. All other users should only be assigned the minimum required access privileges to fulfill their respective roles.

Rail Wi-Fi 4 Series devices support the following roles:

- **Administrator**: Allows the user to access the web UI, change the device's configuration, and use the device's import/export capability.
- **User**: Allows the user to access the web UI, but is not allowed to change the device's configuration or use the device's import/export capability.

3.5.2 Password Policy

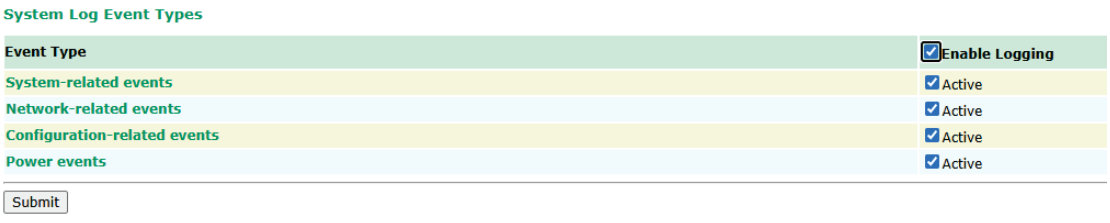
Applying both password lifetime and password complexity requirements helps enforce stronger password protection. Password lifetime sets a fixed password expiration date and will force users to update their passwords frequently. Password complexity applies a set of requirements that must be met for valid passwords, which helps enforce stronger passwords. To configure password policy settings, go to **Maintenance > Account Settings**.

- Review and adjust the password lifetime according to your organization's policies.
- Review and adjust the password complexity options to meet the requirements of your organization's security guidelines.

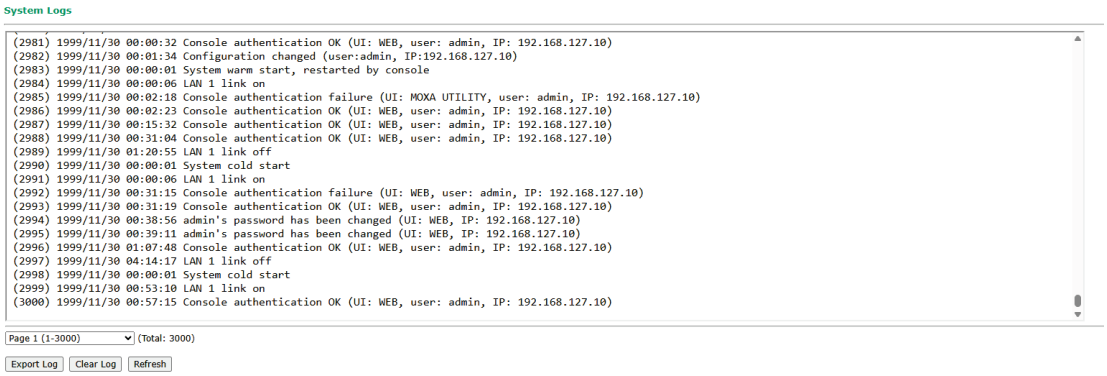
3.6 Logging and Monitoring

Rail Wi-Fi 4 Series devices can record logs for specific events for troubleshooting and diagnostics purposes. Events are grouped under different categories. All event log categories are enabled by default.

To enable logging, go to **Logs and Notifications > System Logs** and check the **Enable Logging** box. To enable or disable logging certain event categories, check or uncheck the corresponding box.



To view recorded events in the system log, go to **Status > System Logs**.



4 Defense-in-depth Strategy

The defense-in-depth strategy is a security approach to protect systems from various types of attacks by using multiple independent defense mechanisms. This strategy involves incorporating multiple layers of security to protect the product against potential attacks and vulnerabilities at various stages of its design, development, and use.

It is important to understand that no single protection measure can guarantee complete security. That's why the defense-in-depth approach makes it difficult for attackers to exploit one weakness to attack the product or the network as a whole. By implementing a defense-in-depth approach, attackers must overcome multiple security layers undetected, making breaches increasingly difficult.

Refer to the following table for measures you can leverage to create a defense-in-depth security environment on Rail Wi-Fi 4 Series devices.

Security Function	Description	Type	Implementation
Account Management	Reduces human error by enforcing access privileges	Administrative Control	Admin/User role settings
Syslog Logging	Logs operations and anomalies	Administrative Control	Supports remote syslog server
Web/CLI Login Authentication	Prevents unauthorized user access to the device	Administrative Control	Use RADIUS for remote authentication, use HTTPS for secure access to the device
Device Certificate & Authentication	Prevent man-in-the-middle (MITM) attacks	Logical/Technical Control	Supports TLS v1.2, SNMPv3
Signed Firmware Validation	Prevents unauthorized firmware uploads	Logical/Technical Control	Signature verification ensures firmware integrity

Security Function	Description	Type	Implementation
Critical Service Access Control	Restricts internal services such as DHCP/NTP	Logical/Technical Control	Configuration is restricted to authorized internal users, external access is blocked
Wireless Security Mechanisms	Controls AP/Client behavior and access	Logical/Technical Control	WPA2/WPA3, 802.1X, MAC filter
Accessible Net List	Limits access by IP/Port/Protocol	Logical/Technical Control	Layer 2/3 ACL to manage device access
Physical Security	Prevents unauthorized physical access	Physical Control	Install the device in cabinets with strict access control and surveillance

5 Firmware Upgrading and Configuration Backup

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

5.1 Firmware Upgrades

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

Running the latest firmware on your network devices is vital to maintaining 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 release notes. Visit the relevant Rail Wi-Fi 4 Series product page on https://www.moxa.com regularly to check for firmware updates.

5.2 Configuration Backup

It is highly recommended to regularly back up the device configuration. This precaution allows administrators to quickly recover the device configuration in case of unforeseen events such as cyberattacks. Always store configuration backup files in a secure location.

6 Recommendations for Decommission

- Power off the device to be decommissioned and dismount it from its physical installation location.

- Identify the serial number or device name and locate (if applicable) any configuration backup files or certificates generated by the device to be decommissioned and ensure these files are deleted.
- To avoid any sensitive information such as the organization's information, account passwords, or certificates from being leaked, always reset the device to the factory default settings before decommissioning the device.

7 Security Information and Vulnerability Feedback

The Moxa Product Security Incident 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 email your findings to PSIRT@moxa.com.

For the most up-to-date Moxa security information, please visit our security advisory page: https://www.moxa.com/en/support/product-support/security-advisory.