The Security Hardening Guide for the OnCell Series

Moxa Technical Support Team

support@moxa.com

Contents

 Released on Aug 29, 2025

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 the OnCell Series cellular gateways and routers. You should consider the recommendations in this document as best practices for securing the device in most applications. It is highly recommended that you review and test the configurations thoroughly before implementing them in your production system to ensure that your applications are not negatively impacted.

2 General System Information

2.1 Basic Information About the Device

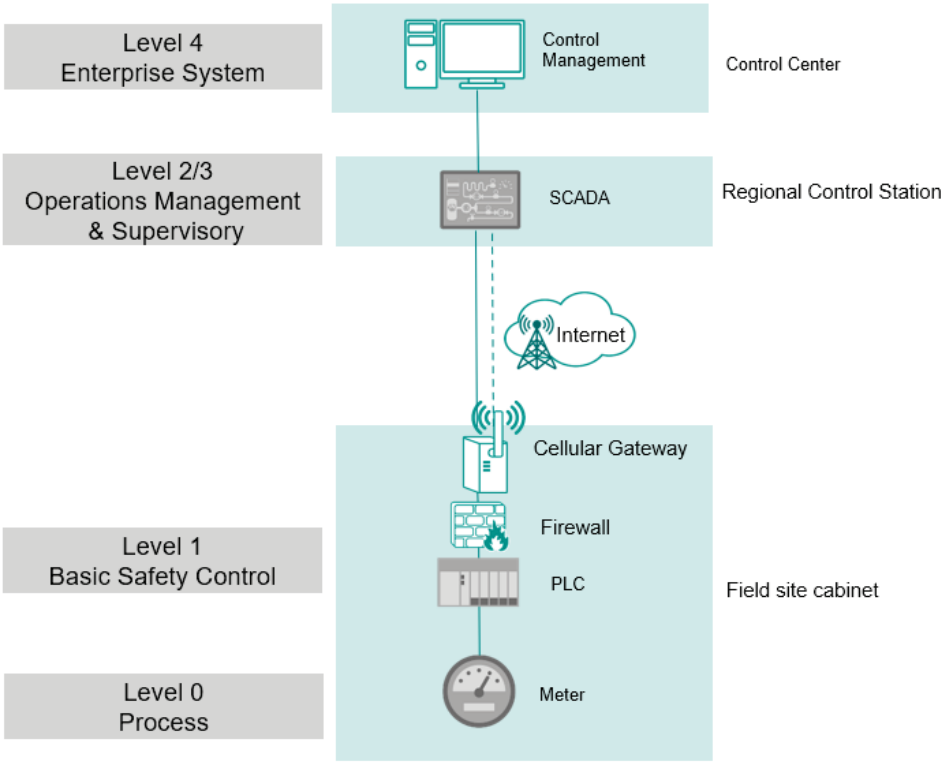
Model	Description	Stateful Firewall	Firmware
OnCell G4308-LTE4	8-port Industrial LTE Cat. 4 secure cellular routers	Yes	v3.18 and above
OnCell G4302-LTE4	2-port Industrial LTE Cat. 4 secure cellular routers	Yes	v3.18 and above
OnCell 3120-LTE-1	2-port Industrial LTE Cat. 1 cellular gateways	No	v2.4 and above

2.2 Deployment of the Device

The OnCell Series is responsible for transmitting information from connected devices at remote sites to the central control center via cellular network.

The OnCell Series and the connected devices below is typically installed in a locked cabinet or a restricted, secure area. Access to the device should be limited to authorized personnel only.

In order to enhance the security of any underlying applications, a dedicated firewall should be placed between the OnCell Series and the internal network if the OnCell device does not support built-in stateful firewall functionality.



2.3 Security Threats and Measures

There are several types of security threats that can potentially compromise the device.

Type 1: Attacks over the network

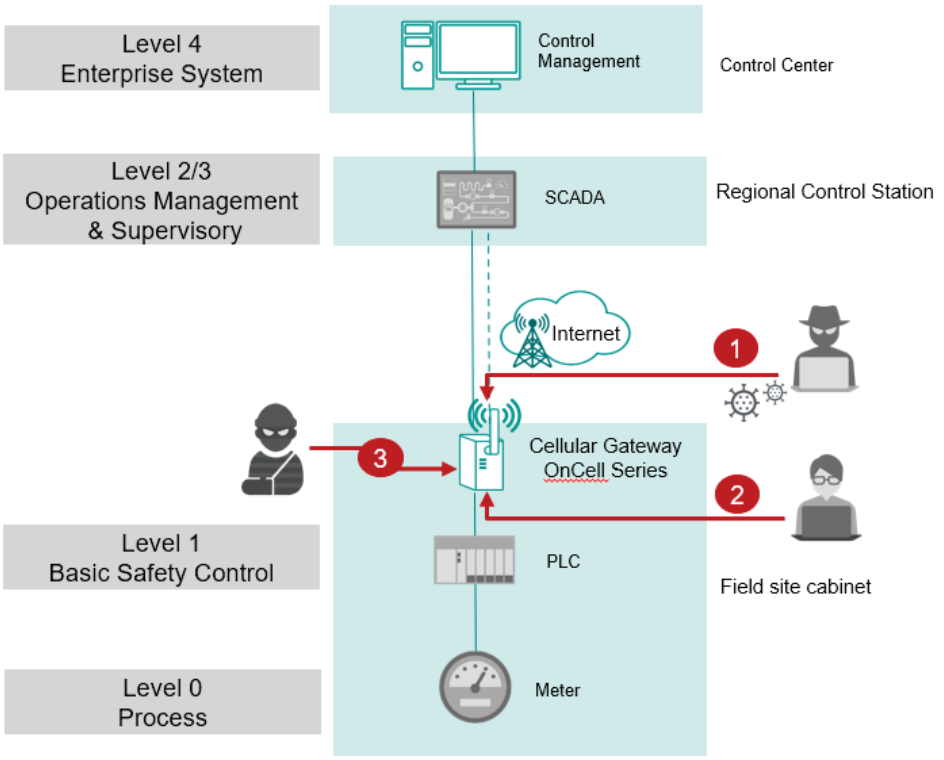
Unauthorized actors may exploit open ports or known vulnerabilities to infiltrate the device via public networks.

Type 2: Direct attacks via device access

Threats involving unauthorized individuals accessing the device to manipulate the system or steal sensitive data.

Type 3: Device or data theft

Attackers may physically access the device or extract sensitive data directly from the hardware.



To protect against security threats, we implemented a secure network environment and defined security measures for the device.

This table shows which security measures address specific threats.

Security Layer	Security Measure	Threat Mitigated				Responsibility
		Description	**Type 1**	**Type 2**	**Type 2**	
Policy and Procedure	Establish policies and procedures to guide employees on their role and responsibilities for safe use of security sensitive assets	Vulnerabilities created because of employees' lack of security policies and awareness of procedures.	Yes	Yes	Yes	Asset Owner
Physical Security	Physical access control, installing physical locks, camera surveillance	Prevents physical modification, manipulation, theft, removal, or destruction of the device.	No	Yes	Yes	Asset Owner

Device Security	Account management	Prevents unauthorized access to the device.	Yes	Yes	No	Provided by the device
	Login policy	Blocks brute-force and/or unauthorized operation of the device.	Yes	Yes	No	Provided by the device
	Console allow list	Prevents unauthorized access to the device.	Yes	Yes	No	Provided by the device
	Interface enabling/ disabling	Reduces the attack surface by disabling unused interfaces.	Yes	No	No	Provided by the device
	System logging	Helps prevent undetected unauthorized access or configuration changes by enabling audit trails and system activity tracking.	Yes	Yes	No	Provided by the device
	Firmware upgrading	Prevents exploitation of known vulnerabilities by ensuring timely patching of security flaws in outdated firmware.	Yes	No	No	Provided by the device
	Configuration backup and recovery	Prevents system misbehavior or downtime caused by accidental misconfiguration or human error by allowing quick rollback to a known safe state.	Yes	Yes	No	Provided by the device
Network Security	Network firewall deployment	Blocks unauthorized or malicious traffic.	Yes	No	No	Provided by the device

	Using VPN	Protects data in transit from interception and man-in-the-middle attacks.	Yes	No	No	Provided by the device
	DoS defense	Prevents resource exhaustion and service disruption caused by excessive or malicious traffic.	Yes	No	No	Provided by the device
Application Security	Using secure communication protocols (SSH, HTTPS, SNMPv3)	Prevents unauthorized access, credential interception, data leakage, and man-in-the-middle (MITM) attacks across management and data channels.	Yes	Yes	No	Provided by the device

3 Configuration and Hardening Information

3.1 Physical Security

3.1.1 Threat

If an attacker gains physical access to the device, they can easily compromise its operation. This may include destroying or disconnecting the device, extracting credentials from memory, tampering with its configuration, or substituting it with a malicious device under their control.

3.1.2 Security Recommendations

- **Secure installation**: Install the device in a restricted, secure area such as inside a locked cabinet to prevent unauthorized physical access to the device.
- **Restrict access**: Limit access to the device to maintenance personnel or other authorized staff with the proper security clearance.
- **Restrict access**: Ensure all cables and connectors relevant to the device are secured within the cabinet. This precaution ensures that only authorized individuals with approved access can interact with the device or its interfaces.

3.2 Device Security

3.2.1 Threat

When a device lacks proper password policies, firmware updates, interface restrictions, access control, or secure boot, it becomes vulnerable to unauthorized access, malicious configuration changes, exploitation of known vulnerabilities, and physical tampering.

3.2.2 Security Recommendations

Note Supported features and supported services depend on the product model. Refer to the relevant product's user manual for more information.

Account management

- **Limit admin access:** Only grant highest-level (admin) privileges to essential personnel who require full configuration rights.
- **Disable inactive accounts:** Temporarily disable accounts when access is not required.
- **Enforce role-based access control (RBAC):** Configure accounts the with minimum required permissions based on their respective role.
- **Create unique accounts:** Avoid shared credentials. Each user account should have unique login credentials to enable proper accountability and audit tracking.
- **Limit failed login attempts:** Automatically lock accounts after a specified number of failed login attempts to block credential-guessing attacks.

Login policy

- **Force password change on first login:** Require users to create a new password upon their first login to eliminate default or shared credentials.
- **Enforce password complexity:** Enable password strength checks to reduce the risk of brute-force attacks.
- **Set password expiration:** Force users to change passwords regularly by setting a fixed validity period.
- **Enable auto logout:** Enable automatically logging out users after a period of inactivity to prevent unauthorized access from unattended sessions.

Console allow list

- **Control service access:** Enable only essential remote services (e.g., SSH), and disable unused and non-secure services to reduce attack surfaces.
- **Define session timeout:** Set an automatic logout timer to terminate inactive console sessions and reduce the risk of unattended access.

- **Restrict interface access:** Limit access to trusted interfaces only (e.g., allow login only via Ethernet and block cellular-based console access).
- **Set up IP allowlist:** Configure the list of known, trusted IP addresses to block unauthorized sources from attempting to connect.

Service management

- **Disable unused services:** Turn off any services or features that are not in use to minimize potential attack vectors.

Service Name	Default Setting	Protocol	Listening Port	Description
HTTPS	Enabled	TCP	443	Secure web access
HTTP	Disabled	TCP	80	Non-encrypted web access
SSH	Enabled	TCP	22	Secure CLI access
SNMP	Disabled	UDP	161	Network monitoring
Telnet	Disabled	TCP	23	Non-encrypted CLI access
DHCP Server	Disabled	UDP	67	Assign IP addresses
IPsec	Disabled	UDP	500/4500	Encrypted VPN tunnel
OpenVPN Sever	Disabled	UDP	1194	Encrypted VPN tunnel
NTP/SNTP	Disabled	UDP	123	Time synchronization
Moxa Service	Enabled	UDP	40404	Moxa config/monitoring

System log

- **Enable logging:** Activate system logs to monitor and record activity for auditing.
- **Regular log review:** Periodically review logs to detect and respond to suspicious activities promptly.

Firmware upgrading

- **Regular firmware updates**: Keep the device's firmware up to date to patch known vulnerabilities.
- **Pre-update backup and integrity check**: Before updating firmware, back up the current configuration and verify update integrity of the firmware using checksums.

Configuration backup and recovery

- **Back up configurations regularly:** Regularly back up the configuration settings to allow for device recovery to a safe state in the event of a security incident.

3.3 Network Security

3.3.1 Threat

When network connections are not encrypted, boundaries are not segmented, packets are not inspected, and abnormal traffic is not monitored, the system becomes vulnerable to several types of network-side attacks. These include data interception, man-in-the-middle attacks, unauthorized access, malicious traffic infiltration, and denial-of-service threats.

3.3.2 Security Recommendations

Firewall

- **Apply layered filtering rules:** Implement IP filtering, MAC address, and port filtering rules to restrict network access to authorized devices only.
- **Log firewall events:** Enable firewall event logging to monitor traffic patterns and detect abnormal or unauthorized activities

VPN

- **Use VPNs:** Use VPN tunneling to securely transmit data over public or untrusted networks.
- **Use certificate-based or strong pre-shared key authentication:** When using pre-shared keys (PSK) , ensure the key is complex and securely stored. Certificates provide better scalability and security for enterprise deployments.
- **Monitor VPN session logs for abnormal usage:** Log tunnel establishment and failure events to look out for anomalies and help analysis.

DoS protection

- **Enable ICMP/ARP flood protection:** Enable protection measures against ICMP and ARP flooding. When enabled, excess ARP or ICMP packets are dropped once the threshold is exceeded, preserving network stability during attack attempts.

3.4 Application Security

3.4.1 Threat

If an attacker gains logical access to the network segment where the gateway operates, they can disrupt or hijack traffic in transit. Threat scenarios include network link saturation via flood attacks, traffic redirection through IP spoofing, injection of false routing updates to isolate key nodes, and forced TCP connection resets that destabilize or misdirect connected devices.

3.4.2 Security Recommendations

Telnet/SSH

- **Password-based login:** Use password-based login to prevent brute-force attacks and credential guessing.
- **Disable Telnet service when not required**: Disable the Telnet service on devices if it is not needed to minimize the attack surface.
- **Replace Telnet with SSH**: Transition to the more secure SSH wherever possible to benefit from built-in encryption, integrity checks, and stronger authentication mechanisms.
- **Console allowlist:** Restrict console login access only to a list of known, trusted IP addresses to block unauthorized sources from attempting to connect.
- **Restrict access to trusted sources:** If Telnet must be used for legacy or compatibility reasons, restrict usage to trusted LAN environments or place it behind a secure VPN tunnel.
- **Enforce strong authentication**: Use complex, non-default credentials and disable unused or factory-default accounts to reduce the risk of unauthorized access.
- **Rotate credentials regularly**: Periodically change login credentials to reduce the window of opportunity for spoofing and brute-force attacks.

HTTP/HTTPS

- **Use HTTPS for all management interfaces**: Avoid using the less secure HTTP, which transmits data—including credentials—in plaintext. Always opt for HTTPS to ensure encrypted communication.
- **Restrict access to trusted sources:** If HTTP must be enabled due to compatibility or legacy requirements, restrict usage to trusted LAN environments or place it behind a secure VPN tunnel.
- **Console allowlist:** Restrict console login access only to a list of known, trusted IP addresses to block unauthorized sources from attempting to connect.
- **Rotate TLS certificates and keys regularly**: Periodically replace TLS certificates and associated private keys to minimize the risk of long-term key exposure or compromise.
- **Monitor for certificate anomalies**: Check logs regularly for invalid certificate access attempts or possible man-in-the-middle (MITM) activity.
- **Avoid deprecated TLS versions**: Do not use TLS versions older than 1.2. If an older version must be used due to legacy constraints, ensure the deployment environment is secured well (e.g., isolated network, firewall protection, restricted access).

SNMP

- **Use SNMPv3 only**: Avoid using SNMPv1/v2c for network management, as they lack encryption and authentication.
- **Restrict access to trusted sources:** If SNMPv1/v2c must be used for legacy compatibility, restrict usage to trusted LAN environments or place it behind a secure VPN tunnel.

- **Console allowlist:** Restrict console login access only to a list of known, trusted IP addresses to block unauthorized sources from attempting to connect.
- **Use read-only access**: Configure community strings with **read-only privileges** whenever possible to minimize the risk of unauthorized configuration changes.
- **Enforce role-based access and authentication**: For SNMPv3, define user roles (e.g., read-only, read-write) with strict access controls and strong authentication mechanisms (e.g., SHA, AES).
- **Rotate SNMPv3 credentials regularly**: Use short validity periods for SNMP credentials and rotate keys or authentication data periodically. Perform regular audits of SNMP configurations to ensure ongoing compliance and security.

DHCP

- **Limit DHCP usage to trusted network zones**: Deploy DHCP services only within secure, isolated network segments to prevent exposure to untrusted or external devices.
- **Use MAC-based IP assignment**: Bind known device MAC addresses to specific IP addresses to ensure consistent addressing and to prevent unauthorized devices from obtaining network access.

DDNS

- **Use secure DDNS providers**: Choose reputable DDNS services that support secure APIs, HTTPS communication, and account protection mechanisms such as two-factor authentication.
- **Use HTTPS for DDNS**: If DDNS is enabled, ensure both dynamic DNS updates and user access to the device via its DDNS hostname are conducted over HTTPS to safeguard data integrity and prevent interception by unauthorized parties.

4 Conclusion

The OnCell Series adopts a disciplined defense-in-depth strategy that mitigates common attack vectors across every layer of the system stack.

- **Physical layer:** Install the device in a restricted, secure area such as inside a locked cabinet, preventing unauthorized physical access, damage or destruction, credential extraction, or device substitution.
- **Device layer:** Secure account management and login mechanisms help prevent errors or malicious access. Closing unnecessary interface functions can also reduce exposure and increase security.
- **Network layer:** The firewall and the always-on DoS protection safeguard OT traffic by preventing link flooding, spoofing and route poisoning. VPN tunneling ensures encrypted and secure connections.

- **Application layer:** Use secure transmission protocols with trusted sources, to enhance the security of application connections and prevent attacks such as man-in-the-middle, packet sniffing, data tampering, and unauthorized access.

Together, these multi-layer measures provide a robust security barrier that protects against device compromise, detects misuse early, and supports forensic investigation—aligning with modern industrial cybersecurity frameworks.

For mission-critical deployments where uptime and integrity are non-negotiable, the OnCell Series delivers a resilient and auditable foundation for secure private cellular infrastructure.

To help us continuously improve product security, please report any discovered vulnerabilities via the following web page:

https://www.moxa.com/en/support/product-support/security-advisory