Scale Monitor™ & CloudScale[Link]

Technical Security Architecture, Network Security & FAQ

For IT, OT, Information Security and System Integration Teams

Scale Monitor uses only two connection types:

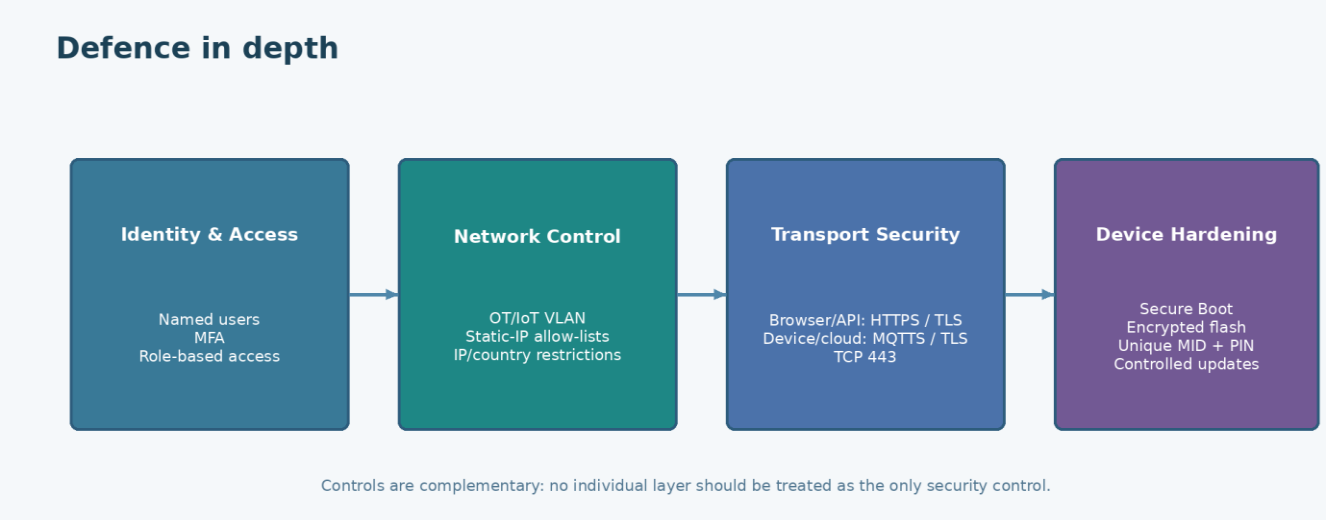
1. A user accesses Scale Monitor from their device through a web browser using an encrypted HTTPS/TLS internet connection.
2. CloudScale[Link] devices connect to Scale Monitor Cloud using outbound MQTTS over TCP 443.

Scale Monitor and CloudScale[Link] devices do not need any inbound connectivity, port forwarding, public IP address or local software installation.

Document purpose: provide a technical overview of the security controls, network communication model and deployment recommendations applicable to Scale Monitor and CloudScale[Link] devices.
The document distinguishes Scale Monitor access via browser/API via secure HTTPS/TLS connection and CloudScale[Link] devices to Scale Monitor cloud connection via encrypted MQTTS communication over TCP 443.

Document at a glance

Area	Key controls covered
Transport security	HTTPS/TLS for browser and API access; MQTTS/TLS over TCP 443 CloudScale[Link] devices connectivity.
Network architecture	Device-initiated outbound connectivity; no standard inbound remote-access requirement.
Identity and access	Named accounts, role-based access control, two-factor authentication and customer/device separation.
Access restrictions	Optional IP allow-listing, country/region-based login restrictions and static-IP deployment options for device, Cloud and API access.
Neutron hardening	Secure Boot, encrypted flash storage, unique MID/PIN per module, WPA Enterprise support and controlled firmware lifecycle with support for OTA updates.
Deployment guidance	OT/IoT segmentation, minimum firewall scope, least privilege and operational governance.



1. Security architecture overview

Scale Monitor provides cloud-based monitoring, data capture, configuration, diagnostics and authorised remote operation for connected weighing equipment and industrial processes. CloudScale[Link] devices provide the secure device-side connection between local weighing systems and the authorised cloud environment.

Core design principles

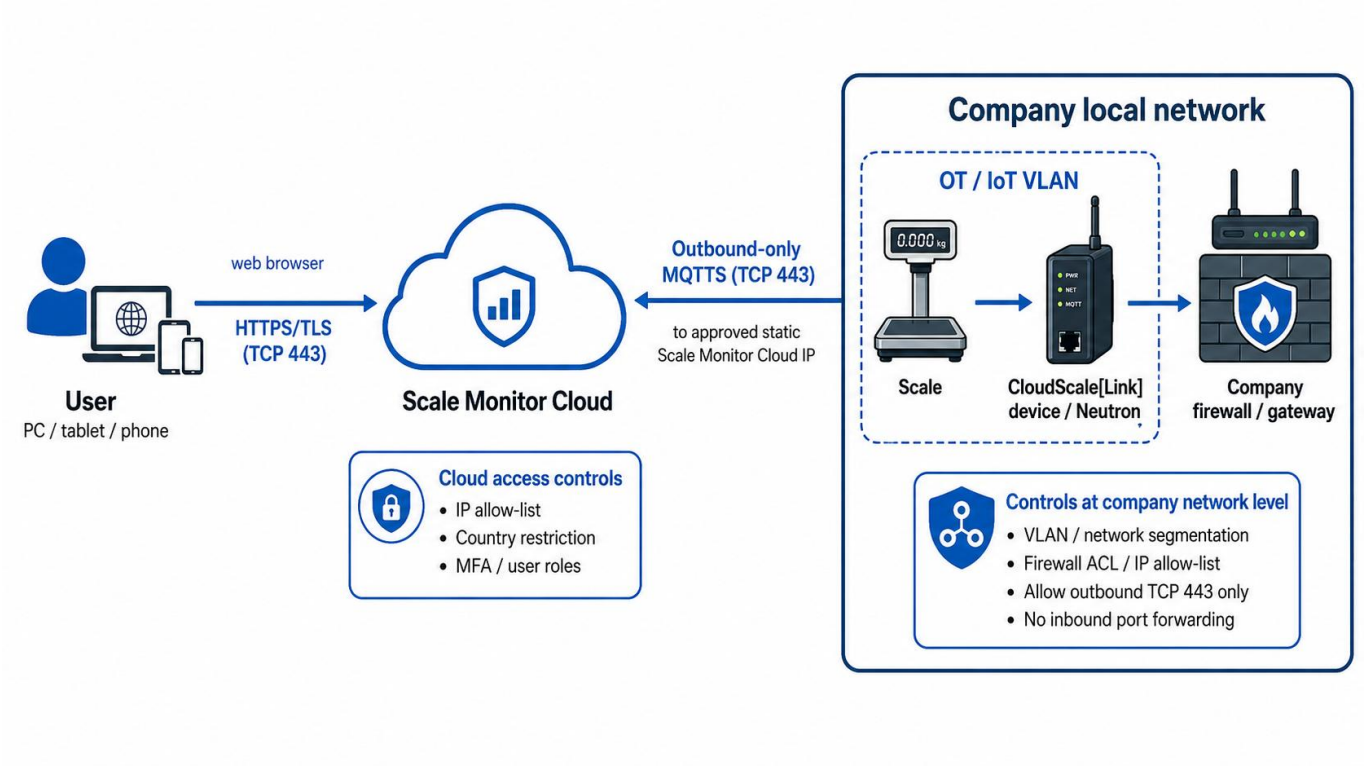
- Encrypted transport using HTTPS/TLS for browser and API access, and MQTTS/TLS over TCP 443 for device-to-cloud communication.
- Device-initiated outbound connectivity rather than public inbound exposure.
- Authenticated users, device identities and logical organisation separation.
- Role-based permissions following the least-privilege principle.
- Optional multi-factor authentication, IP allow-lists and geographic access controls.
- Defence in depth across identity, network, transport and device-security layers.

2. Network communication model

2.1 Outbound device connectivity

CloudScale[Link] devices establish an outbound MQTTS/TLS connection over TCP port 443 from the local customer network to approved Scale Monitor Cloud endpoints. The normal architecture does not require the cloud platform to create unsolicited inbound network sessions into the customer LAN, OT network or production VLAN.

This approach removes the standard need for public device IP addresses, inbound NAT rules, port forwarding, publicly exposed local web servers or direct public access to PLCs, scales and industrial controllers.



2.2 Typical secure protocols

Protocol	Typical use	Security properties
HTTPS / TLS	Scale Monitor browser access, REST APIs, configuration, reporting and update services	HTTPS over TLS on TCP 443; encrypted transport and server certificate validation. No local Scale Monitor installation is required.
MQTTS / TLS	CloudScaleLink and Neutron device telemetry, status, commands, configuration synchronisation and event messaging	MQTT transported through TLS on TCP 443; encrypted device-initiated connection to Scale Monitor Cloud.
Static IP option	Firewall and proxy allow-listing for device, browser and API access where required	A project-specific static public IP can be supplied for the Scale Monitor Cloud destination; Cloud and API access can also be assigned a static IP where required.
Secure REST API	ERP, MES, WMS, LIMS and custom application integrations	HTTPS/TLS with authenticated access and customer-defined integration controls.
DNS / NTP	Name resolution and time synchronisation where required	Customer-controlled resolver and approved time-source policy can be applied.

2.3 Firewall considerations

Scale Monitor is accessed through a standard web browser using HTTPS/TLS over TCP port 443; no local application, service, client or server installation is required. CloudScale[Link] devices communicate with Scale Monitor exclusively through MQTTS/TLS over TCP port 443. For environments using strict outbound firewall policies, a specific static destination IP can be supplied for allow-listing so that CloudScale[Link] outbound connection can be limited only to one IP.

3. Transport encryption

3.1 TLS security

Communication between users, cloud services and CloudScale[Link] devices is protected through TLS-based encrypted channels. TLS provides confidentiality of data in transit, integrity protection against unauthorised modification and server identity validation through certificates.

3.2 HTTPS/TLS browser and API access

- Scale Monitor is a browser-based cloud application. It does not require a local software installation, local server or desktop client. Browser access, authenticated user sessions, configuration actions, reports and Scale Monitor API communication use HTTPS/TLS over TCP port 443.
- Browser clients and CloudScale[Link] devices validate the server certificate before establishing a trusted encrypted session.

3.3 MQTT over TLS / MQTTS

MQTT is a lightweight publish/subscribe messaging protocol well suited to connected industrial equipment. CloudScale[Link] devices use MQTTS: MQTT transported through TLS, on TCP port 443. The device initiates the encrypted MQTTS session outbound towards the approved Scale Monitor Cloud endpoint; no inbound MQTT session from the internet to the customer device is required for normal operation.

4. Identity, authentication and authorisation

4.1 Device identity and logical separation

Each CloudScale[Link] device is associated with a unique device identity and platform configuration. The platform uses this association to determine the organisation, assigned virtual indicators or applications, authorised data streams and permitted user actions. Devices, users, data and configuration are logically separated between customer organisations.

4.2 Role-based access control

Scale Monitor supports role-based access control. Access can be assigned according to operational responsibilities and restricted for sensitive functions such as network configuration, remote calibration, OTA firmware updates, device fleet management, user management, I/O control, data export and administrative actions.

Example role	Typical access scope
Operator	View live values, use approved weighing functions, print and select operational data.
Supervisor / QA	Review records, approved production functions, reporting and quality workflows.
Service technician	Diagnostics and approved technical configuration for assigned devices.
Administrator	User management, policies, system configuration and approval of high-impact actions.
External partner	Limited access to assigned organisations, sites or devices only.

Example role	Typical access scope
Read-only auditor	View approved records and reports without process-control authority.

4.3 Two-factor authentication

Two-factor authentication can be enabled to add a second verification factor beyond the password. MFA is strongly recommended for privileged accounts, service accounts, partner accounts, users with remote configuration rights and accounts used from external networks.

4.4 IP and geographic restrictions

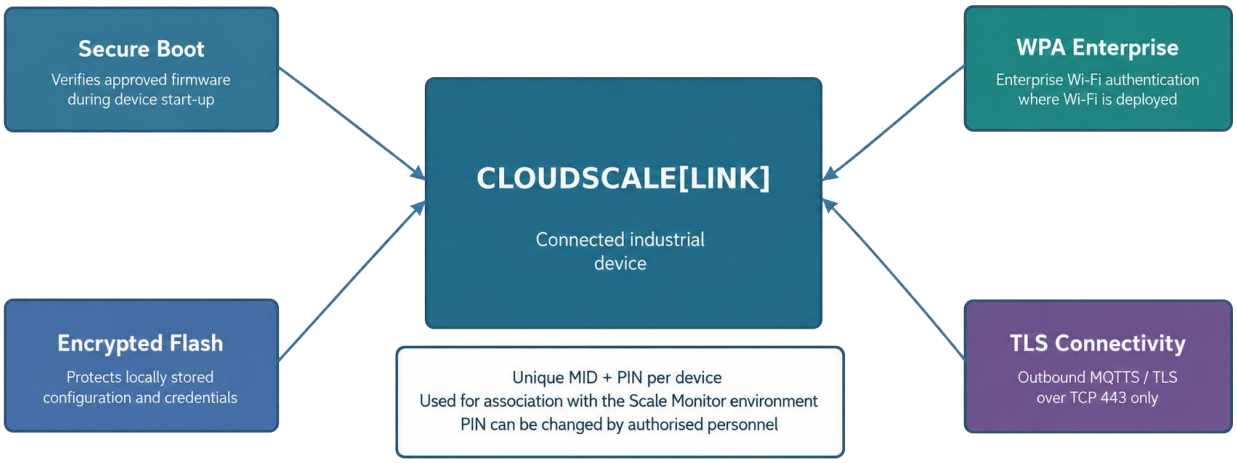
Access to Scale Monitor Cloud is by default limited to the country of the company. It can be further restricted to approved public IP addresses or IP ranges, such as corporate offices, production sites or VPN gateways. Additional country or geographic restrictions can also be applied as an additional control layer. These controls should complement, not replace, named-user accounts, MFA and role-based permissions.

4.5 Static IP deployment options

For deployments using strict IP-based firewall policies, a specific static public destination IP can be supplied for Scale Monitor Cloud. The customer can then permit outbound MQTTS/TLS traffic from CloudScale[Link] devices only to that destination IP on TCP port 443. Where required, Scale Monitor Cloud user access and the Scale Monitor API can also be assigned a static public IP, allowing the customer to restrict HTTPS/TLS access to that specific IP through its firewall, VPN gateway or proxy policy.

5. CloudScale[Link] security

CloudScale[Link] devices are designed with RED and CRA regulatory alignment in mind, where security is not optional but a requirement. Therefore, the following security functions are built into every device core.



5.1 Unique device identity: MID and PIN

Each CloudScale[Link] device is provisioned with a unique MID (module identifier) and PIN. The MID and PIN form part of the module identity used for association with the Scale Monitor environment. PIN can be changed by authorised personnel as part of the controlled device provisioning or replacement process.

5.2 Secure outbound MQTTS/TLS connectivity

CloudScale[Link] devices establishes encrypted outbound communication with Scale Monitor exclusively through MQTTS/TLS over TCP port 443. Standard cloud operation does not require a public IP address, incoming internet connections, port forwarding or direct exposure of its web interface to external networks.

5.3 Ethernet and Wi-Fi

For fixed industrial installations, Ethernet is generally recommended because it offers predictable connectivity, simpler segmentation and a reduced wireless attack surface. Where Wi-Fi is required, CloudScale[Link] can support WPA2/WPA3 Enterprise EAP-TLS & EAP-TTLS environments, enabling centrally managed authentication rather than reliance solely on shared pre-shared keys.

5.4 Secure Boot

CloudScale[Link] devices supports Secure Boot. Secure Boot verifies the authenticity and integrity of approved firmware during start-up and helps prevent the device from starting unauthorised, tampered or malicious firmware.

5.5 Encrypted flash storage

CloudScale[Link] devices uses encrypted flash storage to help protect locally stored configuration, network parameters, Wi-Fi settings, credentials, device-specific identity material, operational settings and local application data. This is an important component of device protection in the event of physical access to the hardware or storage medium.

5.6 Controlled firmware lifecycle

Firmware and software maintenance is managed through controlled update processes using authorised sources, integrity verification, access control, version tracking and change-management procedures.

Firmware updates are delivered through a secure over-the-air (OTA) update process. Before installation, the device verifies the authenticity and integrity of the firmware package, including verification of the firmware digital signature. This helps ensure that only approved and untampered firmware can be installed.

All CloudScale[Link] devices are supported with security updates for a minimum of **five years** from the product release date. Security updates are provided to address identified vulnerabilities, maintain secure operation and support the ongoing protection of connected devices.

For regulated, validated or production-critical environments, customers should incorporate update testing, approval workflows and rollback planning into their own operational procedures before deploying updates to production systems.

6. Recommended enterprise deployment model

For customers with formal IT/OT security policies, the following deployment model is recommended:

- Place CloudScale[Link] devices in a dedicated OT, IoT or VLAN.
- Do not expose devices directly to the public internet.
- Allow only approved outbound MQTTS/TLS over TCP 443 from CloudScale[Link] devices to the approved Scale Monitor Cloud static destination IP. Allow browser and API access through HTTPS/TLS over TCP 443 only.
- Where IP-based firewall rules are required, use the project-approved static destination IP for outbound device MQTTS traffic and, where assigned, the static Scale Monitor Cloud and API IPs for HTTPS/TLS access.
- Use corporate DNS and approved NTP sources where required.
- Restrict platform access to corporate VPN gateways or approved public IP ranges.
- Enable MFA for administrators, service accounts and partner accounts.
- Use named accounts instead of shared credentials.
- Apply least-privilege permissions and review access periodically.

- Use WPA Enterprise where Wi-Fi is deployed and supported by the customer network.
- Keep device firmware, network infrastructure and endpoint systems up to date.
- Protect installed devices against unauthorised physical access where required.

6.1 Example firewall matrix

Source	Destination	Protocol	Direction	Purpose
CloudScale[Link] VLAN	Approved static Scale Monitor Cloud destination IP	MQTTS / TLS - TCP 443	Outbound	CloudScaleLink and Neutron device telemetry, status, commands and configuration messaging
User browser / API client	Scale Monitor Cloud or API static IP where assigned	HTTPS / TLS - TCP 443	Outbound	Browser access and Scale Monitor API communication
CloudScaleLink VLAN	Approved DNS resolver	DNS	Outbound	Name resolution
CloudScaleLink VLAN	Approved NTP source	NTP	Outbound	Time synchronisation where required

Not required: Inbound internet connections to CloudScale[Link] devices, port forwarding to customer devices, public device web interfaces, direct public access to PLCs or unrestricted lateral movement between IT and OT networks.

7. Technical FAQ

Does the platform require port forwarding?

No. Operation is based on outbound encrypted sessions initiated by the device. Public inbound NAT or port forwarding to the CloudScale[Link] device, scale, PLC or local server is not normally required.

Which ports need to be opened?

Scale Monitor browser access and the Scale Monitor API use HTTPS/TLS over TCP 443. CloudScale[Link] devices use MQTTS/TLS over TCP 443 for the device-to-cloud connection. A project-specific static destination IP can be supplied for device firewall allow-listing; where assigned, a static IP can also be used for Scale Monitor Cloud and API access restrictions.

Does the cloud initiate unsolicited incoming connections to our OT network?

No. The standard model uses an authenticated logical session initiated outbound by the device. Cloud-to-device communication is routed through that established secure session.

Is MQTT communication secure?

Yes, when MQTT is used with TLS (MQTTS which is used by CloudScale[Link] devices), the channel is encrypted and protected against interception or modification in transit. The device initiates the connection outbound to the approved broker endpoint.

Can access be limited to our corporate VPN?

Yes. IP allow-listing can restrict platform access to approved VPN gateways, offices or managed public IP ranges.

Can country-based restrictions be applied?

Yes. Geographic restrictions can be used to allow or block login access by country or region. They are most effective when combined with MFA, named accounts and IP restrictions.

Does CloudScale[Link] devices support enterprise Wi-Fi security?

Yes. CloudScale[Link] devices supports WPA Enterprise for Wi-Fi deployments where enterprise authentication is required.

What protects CloudScale[Link] firmware and locally stored settings?

CloudScale[Link] devices use Secure Boot to verify approved firmware at startup and encrypted flash storage to protect locally stored configuration, credentials and operational data.

Can external service personnel be restricted?

Yes. External service users can be assigned named accounts with limited access to selected organisations, sites or devices, combined with roles, MFA, IP controls and country restrictions.

Can remote configuration be disabled?

Yes. Sensitive functions can be restricted or disabled for selected roles. A customer can permit normal operational use while limiting configuration, calibration, I/O control, firmware updates and administration to authorised personnel.

8. Security statement

Scale Monitor, CloudScale[Link] devices are designed for secure cloud-connected industrial weighing and process applications. The solution combines HTTPS/TLS browser and API access, MQTTS/TLS over TCP 443 for CloudScale[Link] devices connectivity, outbound-only device sessions, MID/PIN device identity, role-based access control, two-factor authentication, IP and country restrictions, secure boot, encrypted flash storage, WPA Enterprise support for applicable Wi-Fi deployments and controlled firmware lifecycle processes.

Assessment support: For projects with IEC 62443, ISO 27001, NIS2, GDPR, customer-specific OT policies, private-cloud requirements or formal cybersecurity assessments, the final architecture should be reviewed jointly with the customer's IT, OT and information-security teams.