UnityIS® Secure Gateway

Secure cloud connectivity to on-prem controllers - without port forwarding

Overview

UnityIS® Secure Gateway is an on-premises, appliance-style gateway that enables UnityIS® Cloud to communicate securely with local controllers that do not support IP Client (e.g., ELK intrusion panels, Axis A1001 panels, VertX/Edge) **without exposing those devices to the internet**. It uses an encrypted, outbound-initiated connection model and supports customer-managed security controls.

*This product is not needed for Azure, Atlas, and Mercury controllers.

Key Benefits

- **No port forwarding required** (eliminates inbound firewall exposure)
- **Encrypted connectivity** between UnityIS® Cloud and the customer site
- **OT-safe design** (no software or changes required on controllers)
- **Customer-controlled security** (IT retains ownership of hardening, patching, and monitoring)
- **Fast deployment** (plug-in, authorize, validate)

How it Works

- UnityIS® Cloud and the UnityIS® Secure Gateway join a private, encrypted overlay network.
- The gateway forwards traffic to on-prem controllers using existing **IP addresses and TCP ports**.
- Controllers remain on the customer LAN and are never directly internet reachable.

What Runs the Secure Software

- UnityIS® Cloud server (in IMRON’s cloud environment)
- UnityIS® Secure Gateway (on-prem appliance)
- **Controllers/OT devices do not run any agent** and require no configuration changes.

Network Requirements (Outbound Only)

- Outbound internet access from the gateway
- Recommended: UDP 9993
- Fallback: TCP 443
- **No inbound firewall rules** are required.

Security Model

- Outbound-initiated encrypted connectivity (no unsolicited inbound access)
- Explicit node authorization (devices must be approved to join)
- Supports least-privilege network design (restrict to specific IPs/ports)
- Gateway can be placed in a **DMZ or isolated VLAN** if desired
- Customer IT may manage:
    - OS hardening / endpoint protection
    - Firewall policy
    - Patching / maintenance windows
    - Monitoring / SIEM forwarding

Deployment Options

- **Standard:** One gateway per site / campus network
- **Optional redundancy:** Secondary gateway for failover (customer-defined)

Operational Notes

- If the gateway is offline, cloud connectivity pauses; local controller operation continues normally.
- No data is stored on the gateway (it is a transport device).
- IMRON does not require administrative access to the gateway unless explicitly authorized by the customer.

Typical Use Cases

- Secure cloud monitoring/control of legacy intrusion panels
- Secure connectivity to controllers where port forwarding is prohibited
- OT environments requiring minimal change and reduced attack surface

What's Included

- UnityIS® Secure Gateway appliance (Linux-based, hardened baseline)
- Installation guide and validation checklist
- Configuration support for approved network routes and ports

Support Model

- IMRON: UnityIS® Cloud application and integration support
- Customer IT: on-prem gateway OS security, patching, and local network controls
- Optional joint troubleshooting procedures available upon request