UnityIS® Secure Gateway

The UnityIS® Secure Gateway enables encrypted, outbound-only connectivity to UnityIS® Cloud while preserving OT isolation and customer-controlled security.

Customer IT Checklist

This checklist outlines the items typically reviewed and approved by Customer IT when deploying the UnityIS® Secure Gateway.

---

1. Pre-Deployment Review

☐ Review UnityIS® Secure Gateway architecture and network diagram
☐ Confirm no inbound firewall rules or port forwarding are required
☐ Confirm controllers will remain on the internal network and unchanged
☐ Confirm UnityIS® Cloud communicates using existing IP addresses and TCP ports
☐ Confirm customer IT retains ownership of on-prem gateway security

---

2. Gateway Placement & Network Segmentation

☐ Place gateway on appropriate network segment (LAN, DMZ, or isolated VLAN)
☐ Ensure gateway has IP connectivity to controller subnet(s)
☐ Ensure gateway has outbound internet access only
☐ No inbound access to gateway from untrusted networks

Recommended:
☐ Dedicated VLAN or restricted subnet
☐ Explicit routing and ACLs

---

3. Firewall & Network Controls

☐ Allow outbound internet traffic from gateway
☐ Confirm outbound UDP 9993 is permitted (preferred)
☐ Confirm outbound TCP 443 is permitted (fallback)
☐ No inbound firewall rules required
☐ Restrict gateway forwarding to only approved controller IP addresses and TCP ports

4. ZeroTier Authorization & Access Control

☐ Approve the gateway node in ZeroTier Central (manual authorization)
☐ Verify only approved UnityIS® Cloud node(s) are authorized
☐ Confirm no unauthorized nodes appear in the ZeroTier network
☐ (Optional) Apply ZeroTier Flow Rules for additional traffic restrictions

---

5. Operating System Security (Customer-Owned)

☐ OS fully patched prior to production use
☐ Automatic security updates enabled
☐ Disk encryption enabled if required by policy
☐ SSH access restricted (key-based, limited admins)
☐ No user browsing, email, or productivity software installed

---

6. Endpoint Protection & Monitoring

☐ Endpoint protection / EDR installed (if required)
☐ Gateway logs enabled (system + firewall)
☐ Logs forwarded to SIEM (optional)
☐ Alerts configured for anomalous activity

---

7. Validation & Testing

☐ Gateway successfully joins ZeroTier network
☐ Gateway authorized and visible in controller
☐ UnityIS® Cloud can reach controllers via IP + TCP port
☐ No public exposure of controllers confirmed
☐ Local controller functionality verified unchanged

---

8. Operational Ownership & Responsibilities

Customer IT owns:
☐ Gateway OS hardening and patching
☐ Firewall and network policies

☐ Endpoint protection and monitoring
☐ Gateway availability and lifecycle

IMRON owns:
☐ UnityIS® Cloud application
☐ Integration logic and support
☐ Architecture guidance and validation

---

9. Change Management

☐ Gateway configuration changes follow customer change control
☐ IMRON cloud-side changes communicated in advance when applicable
☐ Node authorization changes reviewed and approved by IT

---

10. Business Continuity & Recovery

☐ Gateway replacement procedure documented
☐ Hardware spare or rebuild image available
☐ RTO expectations defined
☐ (Optional) Secondary gateway strategy reviewed

---

11. Security Confirmation (Sign-Off)

☐ No inbound network exposure introduced
☐ OT devices remain isolated and non-internet-reachable
☐ Access limited to least privilege
☐ Solution aligns with internal security standards

IT Approval: _____
Date: _____
