

Device Provisioning Policy

The Grand Marina Hotel — Water Monitoring System

Document Version	1.0
Created By	Maya Al Hourani
Date	18th September, 2026
Approved By	Maya Chen, Senior Security Engineer

1. Scope and Purpose

This policy governs the provisioning, management, and decommissioning of HYDROLOGIC devices connected to The Grand Marina Hotel's water monitoring system.

Devices Covered

All devices follow the pattern HYDROLOGIC-[UNIT]-[NUMBER], where HYDROLOGIC= Hydroficient sensor, UNIT = building (Main Building, Pool & Spa, Kitchen & Laundry, etc.), and NUMBER = sequential three-digit number within that unit.

Device ID	Location	Certificate	Status
HYDROLOGIC-MainBuilding-001	Mechanical Room A	device-001.pem	Active
HYDROLOGIC-PoolSpa-002	Pool Pump House	device-002.pem	Active
HYDROLOGIC-Kitchen-003	Kitchen Mechanical	device-003.pem	Active
[Future devices as deployed]			

Total active devices: 3

2. New Device Onboarding Process

Step 1: Device Registration

To register a new device, say a sensor for a newly constructed building or wing, Hydroficient will provision this device by generating a certificate for it and signing it by the same CA the other sensors use.

It will register the device's serial number in two systems: (a) Hydroficient Device Registry, our internal tracking system that maps device IDs to certificates and locations; (b) Grand Marina IT Asset Database — the resort's inventory system, required for compliance audits. Assign a device ID following the HYDROLOGIC-[UNIT]-[NUMBER] naming convention. Confirm the device ID does not already exist in either system before proceeding.

Step 2: Certificate Generation

Generate a digital security credential (TLS client certificate) that proves this specific device is authorized to connect to the resort's network. Use Hydroficient's internal Certificate Authority (our secure system for issuing these credentials). Run the provisioning script: `python generate_client_certs.py`. The script generates a certificate with the device ID embedded as the certificate's identity label (Common Name field). It requires access to the CA's master signing key, which is stored in a tamper-proof hardware vault (Hardware Security Module) in the IT office. Only authorized Hydroficient security engineers have access credentials. Each device receives a unique certificate — like a unique ID badge. Certificates are never shared between devices.

Step 3: Certificate Installation

Flash the certificate to the device via the secure USB provisioning station in the IT office. The device must be physically present — remote provisioning is not permitted.

Two-person verification required: Technician A installs the certificate on the device. Technician B independently confirms the certificate's unique digital fingerprint (thumbprint) on the device matches the fingerprint recorded in the Hydroficient Device Registry. If the fingerprints do not match, stop immediately. Revoke the certificate and restart from Step 2.

Step 4: Connection Verification

Connect the device to the hospital network. Verify the following within 10 minutes:

Device establishes an encrypted data channel (MQTT connection on port 8883).

Unencrypted connections (port 1883) must be rejected.

Device sends vitals through its assigned data route (MQTT topic):
hydroficient/grandmarina/sensors/[unit]/readings.

Readings appear on the clinical dashboard within 60 seconds.

Run connectivity test: send 10 test messages from the device. Verify all 10 are received by the message server (broker) and displayed on the dashboard.

If any check fails, disconnect the device and troubleshoot before placing it in a water service line.

Step 5: Documentation

Update the Hydroficient Device Registry with: Device ID, physical location (unit + bed/room number), certificate fingerprint (thumbprint), certificate expiration date, provisioning date, and technician names (both A and B). Notify the system supervisor/operators for the assigned unit that a new monitoring device is active at the specified location.

Estimated time for full onboarding: 45 minutes per device

3. Certificate Rotation Schedule

Current certificate validity period: 1 year

Rotation Schedule:

- Manual rotation triggered 30 days before expiry
- Automated email alerts at 30, 14, and 7 days before expiration sent to Hydroficient Security Engineering Team and Grand Marina IT Director

Rotation Procedure:

1. Generate a new security credential for the same device ID using `generate_client_certs.py` (same process as Section 2, Step 2).
2. Schedule a maintenance window during low-activity hours (2:00 AM - 4:00 AM) to minimize impact on patient monitoring. Coordinate with the on-duty security supervisor 24 hours in advance.
3. Install the new credential on the device at the water service line using a portable provisioning kit. Two-person verification required (same as Section 2, Step 3).
4. Verify the device reconnects to the message server (MQTT broker) within 60 seconds and readings resume on the security dashboard.
5. Revoke the old credential in the Certificate Authority. Add to the revocation list (a registry of credentials that are no longer valid).
6. Update the Hydroficient Device Registry with the new certificate fingerprint and expiration date.

Who is responsible: Hydroficient Security Engineering team (primary). Grand Marina IT Director (backup, for emergency rotation if Hydroficient team is unavailable).

Important: A device must never operate with an expired certificate. If rotation cannot be completed before expiration, the device must be taken offline and patient monitoring must switch to manual checks until a valid certificate is installed.

4. Compromised Device Procedure

If a device is suspected to be compromised:

IMMEDIATE ACTIONS (within 15 minutes):

1. Revoke the device's security credential immediately. This blocks all future connections from that device — even if the attacker still has physical access to it.
2. Disconnect the device from the resort network. Unplug the ethernet cable or disable the device's WiFi radio. Do not simply power it off — a compromised device could re-establish connection on reboot.
3. Notify Grand Marina IT Director and the on-duty security supervisor. Sensor monitoring for the affected building must switch to manual reading sign checks immediately. A security engineer must be assigned to check readings every 15 minutes until monitoring is restored.

INVESTIGATION (within 24 hours):

1. Review the message server logs for the affected device. Look for: unauthorized connections, unexpected data patterns, connections from unusual network addresses, or messages sent outside normal intervals.
2. Assess whether reading data was exposed. If any readings may have been accessed by an unauthorized party, determine if any "Emergency Shutoff" commands were executed during the compromise window. initiate the Compromised Device Procedure. Notify Hydrocient Security Lead (Maya Chen) within 24 hours of discovery.

RECOVERY:

1. Factory reset the device to remove any compromised firmware or stored credentials.
2. Generate a completely new security credential with fresh encryption keys (do NOT reuse the old keys — they may be compromised).
3. Re-provision the device following the standard onboarding process (Section 2, Steps 2-5).
4. After reinstatement, monitor the device's network activity for 48 hours. Flag any anomalies for immediate review.

Emergency contact:

- Hydroficient Security Operations Center (24/7): +1-800-555-HYDRO
- Grand Marina IT Director (on-call): Extension 1234

5. Decommissioning Process

When a device is removed from service:

Step 1: Revoke Certificate

Revoke the device's certificate immediately — even if the device is being retired, not compromised. Add it to the revocation list so no system will accept it again. A revoked credential must never be reused, even if the same device ID is assigned to a replacement unit later.

Step 2: Remove from Monitoring

Remove the device from the message server's authorized device list. Remove the device from the security dashboard. Update alert routing rules so security staff are not alerted about a device that no longer exists. Verify the dashboard no longer shows a "device offline" warning for the retired device.

Step 3: Physical Removal

Factory reset the device to wipe all stored certificates, encryption keys, and configuration data. If the device is being returned to Hydroficient inventory for refurbishment, document the return in both the Hydroficient Device Registry and Grand Marina's IT asset database. If the device has reached end-of-life, document its secure destruction (certificate of destruction required).

Step 4: Documentation

Update the Hydroficient Device Registry: mark the device as "Decommissioned" with the decommission date, reason, and technician name. Update Grand Marina's IT asset database to match. Archive 90 days of the device's network activity logs for compliance and audit purposes.

6. Policy Review

This policy will be reviewed:

- Annually
- After any security incident
- When new devices are added

Next review date: September 18, 2027

Signatures

Role	Signature	Date
Prepared by: Maya Al Hourani	Maya al Hourani	Sep 18, 2026
Reviewed by: Maya Chen, Senior Security Engineer	Maya Chen	Sep 18, 2026
Approved by: Marcus Webb, General Manager, The Grand Marina Hotel		