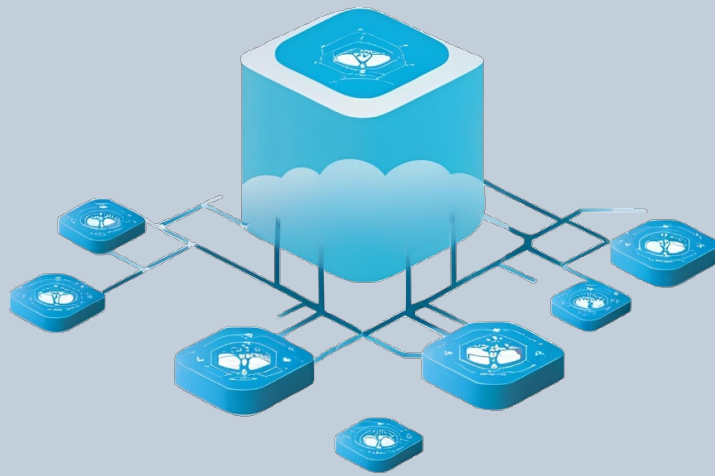

Oxygen remote monitoring and management system



Auto-configuration and dynamic service provisioning of new devices

Remote configuration of groups or specific devices

Remote diagnostics and Firmware updates

API to external applications

The Oxygen Remote Management System is a scalable, secure platform designed for remote provisioning, management, monitoring and analysis of broadband gateways. It enables automatic device registration, grouping, remote configuration, and integration with external systems through standardized interfaces and messaging protocols. The server architecture also supports IoT and SCADA environments where remote telemetry and control of distributed assets are required with operational efficiency at scale.

Device Registration and Identification

Upon connecting to the Internet, each gateway sends a secure heartbeat to the server including unique identification information. The server processes this information to create and maintain an inventory of connected devices. Registration can be automatic without manual intervention.

This mechanism is suitable for both mobile devices (e.g., vehicle-mounted gateways) and fixed installations (e.g., fixed-line gateways or industrial control systems).

Grouping and Geo-Location Management

The server supports organizational grouping of devices:

- Devices can be assigned to groups based on different criteria, like customer, project, operational role, or physical location.
- Devices may also be assigned geographic coordinates for visualization on a global map.

Grouping supports access control policies, operational management by teams, and bulk actions on related sets of devices.

The grouping structure is flexible to fit different operational models.

Device Management Functions

Remote management operations are supported at both the device and group level:

- **Configuration Management:** Update device settings remotely.
- **Firmware Management:** Initiate and monitor firmware upgrades.
- **Maintenance Operations:** Reboot, factory reset, logging or application of custom maintenance commands.

Bulk operations are available with intelligent filtering and scheduling features, allowing updates to be planned during maintenance windows to avoid service interruptions.

The server maintains operational logs for each command executed, providing traceability and auditing support.

Interfaces for Automation and Integration

REST API-Based Device Interaction.

Communication between the server and terminal routers is accomplished through REST API commands. It is possible to remotely retrieve or modify device settings, initiate device reconfiguration and firmware upgrades. All actions are transmitted securely using encrypted channels and authenticated sessions.

The API is structured, versioned, and documented to ensure consistent and stable long-term operation.

Kafka Messaging Support

The platform can also receive operational events from the managed devices using Apache Kafka:

- Heartbeats, operational status changes, and alarms can be streamed in real time.
- Kafka topics allow high-throughput integration with analytics platforms, monitoring dashboards, custom automation, and big data storage systems.

Kafka support makes the platform well-suited for broadband and IoT architectures requiring event-driven processing and for SCADA systems seeking to ingest operational telemetry into cloud services or advanced analytics engines.

Platform Architecture and Scalability

The platform is designed for operational scalability:

- Supports installations from a few dozen up to tens of thousands of devices.
- Efficient data storage and query systems maintain fast response times.
- Horizontal scaling options are available through standard database and messaging technologies.

User Interface

The management console provides an efficient, task-oriented interface:

- Device dashboards with real-time and historical views.
- Geo-maps showing live device locations and status.
- Bulk actions, filters, and search tools designed for speed and operational clarity.

The UI is responsive, usable across desktop and mobile browsers, and optimized for managing large device sets.

Security Features

Security is embedded at multiple layers:

- All device-to-server communication is secured via SSL.
- Device authentication ensures only authorized devices register.
- Admin accounts support Role-Based Access Control (RBAC).
- API and Kafka interfaces require authentication and scoped permissions.

These features align with cybersecurity best practices in broadband deployments and industrial SCADA networks.

Key System Characteristics

Automatic Registration:

Device self-registration with heartbeat mechanism

Remote Management:

Configuration, firmware, maintenance via secure server commands

Grouping and Geo-Mapping:

Logical and geographic organization of devices

REST API:

Secure and structured interaction between server and terminal devices, supporting configuration management, firmware updates, and operational control.

Kafka Event Streaming:

Real-time device events for IoT and SCADA data pipelines.

SCADA and IoT Support:

Suitable for telemetry, asset control, and large-scale deployments

Scalable Architecture:

Efficient performance across small to massive deployments

Security and Auditability:

Encrypted communication, role-based access control, operational logs

Conclusion

Through standardized APIs, real-time messaging, and robust security practices, the server enables integration into modern data-driven infrastructures, offering flexibility for evolving operational needs.

(*) Optional