

# Offline Capabilities Overview

This document aims to give an overview of the offline capabilities of the Avassa Edge Platform.

We're often asked how Avassa supports edge orchestration in environments with limited or no connectivity—commonly referred to as offline or air-gapped deployments. To answer that, it's useful to break down the key dimensions that define such scenarios:

## 1. Planned vs. Unplanned Connectivity

This dimension describes whether connectivity interruptions are expected and scheduled—or unpredictable and sudden.

- **Planned connectivity** refers to environments that are normally disconnected, but connect to the central component during predefined windows—for example, nightly syncs or maintenance periods.
- **Unplanned interruptions** occur in environments that are normally connected, but may lose connectivity unexpectedly due to network instability, power loss, or other failures.

Designing for both cases requires different strategies to ensure application health, state consistency, and operational continuity during and after disconnection.

## 2. Degree of Connectivity

This refers to how often and how reliably the edge environment can communicate with the central component:

- **Air-gapped environments** are fully isolated by design—no connection exists between the edge and the central system.
- **Offline environments** span a spectrum—from mostly disconnected with short windows of connectivity, to mostly online with occasional disruptions.

Understanding where a deployment falls on this scale helps determine how to handle tasks like software updates, monitoring, and orchestration logic.

### 3. Network Topology and Segmentation

Many environments, especially in industrial and OT settings, are structured as multi-layered networks. A common example is the ISA-95 architecture, which segments the network into layers with varying degrees of connectivity:

- **Inner layers** interface directly with sensors and control systems and are often completely isolated from external networks.
- **Outer layers**, closer to IT systems, may have limited or controlled access to a central component.

This segmentation means that even within the same physical location, some parts of the network may be “disconnected” while others can serve as gateways or bridges—depending on the security policies and infrastructure in place.

## Avassa Solution Principles for Offline and Air-Gapped Scenarios

### Minimal Connectivity Requirements

A key enabler of Avassa’s offline capabilities is its minimal network footprint. The only required communication is a single outgoing HTTPS (port 443) connection from each Edge Enforcer to the Avassa Control Tower. All orchestration and monitoring traffic flows over this reverse-initiated channel—meaning:

- No VPNs are needed.
- No incoming ports need to be opened on the edge side.
- Firewalls remain tight, even in sensitive environments.

This design significantly simplifies deployment in constrained or security-hardened networks.

### Offline and Air-Gapped Deployment Scenarios

Avassa is designed from the ground up to operate across the three dimensions of offline deployments: planned connectivity, varying degrees of disconnect, and segmented network topologies. Below are the core solution strategies grouped by typical deployment scenarios:

- No VPNs are needed.
- No incoming ports need to be opened on the edge side.
- Firewalls remain tight, even in sensitive environments.

This design significantly simplifies deployment in constrained or security-hardened networks.

## 1. Planned Connectivity

In many environments, edge locations are normally disconnected, but scheduled connectivity windows are available—for example, nightly syncs or weekly maintenance periods.

Avassa fully supports this model through the following capabilities:

- **Autonomous operation:** Edge Enforcers operate independently of the Control Tower. All application lifecycle actions are handled locally at the edge, without requiring central communication.
- **Edge-side caching:** All required artifacts (container images, configurations, secrets) are cached locally, so updates and restarts, migrations etc, can happen without connectivity.
- **Queued updates:** Administrators can trigger updates centrally even while the edge is offline. The Control Tower queues the changes, and Edge Enforcers will automatically reconcile and apply updates during the next connectivity window.
- **Local overrides:** Critical changes can also be applied directly at the edge, using Avassa's edge-side APIs or interfaces. Reconciliation with central intent is automatic once communication is restored.

## 2. Unplanned Interruptions and Intermittent Connectivity

Avassa is inherently resilient to unpredictable disconnections. Whether due to network instability, temporary outages, or other disruptions, the platform behaves consistently:

- **Loose coupling via pub/sub:** All interactions between Control Tower and Edge Enforcers are managed via an event-driven pub/sub bus. This architecture buffers both commands and telemetry, ensuring eventual consistency without requiring real-time connection.
- **Full edge autonomy:** As with planned disconnects, the edge continues to operate and manage applications without any dependency on the Control Tower.

## 3. Segmented Network Topologies

In OT environments, networks are often segmented across multiple layers—especially following architectures like ISA-95. Avassa supports this through:

- **Multi-hop edge hierarchies:** Edge Enforcers can be placed at various layers (e.g., OT layer, DMZ) and act as communication proxies for more deeply embedded peers.
- **Proxy chaining:** You can configure a chain of Edge Enforcers, where only the outermost node requires external connectivity. Inner layers relay orchestration traffic securely through that chain, maintaining isolation policies while enabling orchestration.

#### 4. Fully Air-Gapped Deployments

For deployments that are permanently disconnected from any external network, Avassa offers a fully self-contained mode:

- **On-prem Control Tower:** The central component can be deployed within the same isolated environment as the Edge Enforcers.
- **Internal orchestration only:** All operations—application lifecycle, configuration, monitoring—are performed entirely within the air-gapped environment.

To learn more about the Avassa platform can help your business, visit our website [avassa.io](https://avassa.io) or [get in touch](#).