



ENDPOINT MANAGEMENT

PRODUCT GUIDE

zMAN Director

Centralized Endpoint Management for Modern IT Environments

Managing a distributed fleet of endpoints used to mean on-site visits, inconsistent configurations, and reactive support. zMAN Director eliminates all three. It is AmZetta's centralized management platform for SnapOS-powered endpoints — a single console to provision, configure, secure, update, and remotely support every device in the fleet, from a laptop on a home network to a locked-down terminal in an air-gapped facility. And for organizations already paying for a dedicated management platform, zMAN Director typically costs a fraction of what industry consolidation has driven legacy vendor pricing to.

What Is zMAN Director?

zMAN Director is a centralized endpoint management platform designed to simplify, secure, and scale the deployment and ongoing operations of SnapOS-powered endpoints. From the moment a device powers on for the first time through every firmware update, policy change, and remote support session that follows, zMAN Director gives IT teams complete visibility and control over distributed device fleets without ever leaving their desk.

The platform uses a two-component architecture. zMAN Director provides the central management interface; zDM acts as the device management relay, handling endpoint communication, provisioning, file caching, and remote access. This supports corporate offices, branch locations, remote workers, public networks, and fully air-gapped environments from a single operational view without a VPN or a direct network path to every device.

One Console

Entire fleet, every network type

Two Parts

zMAN Director + zDM relay

No VPN

Reverse-tunnel architecture

Supported Deployment Environments

zMAN Director is built for the real world, where endpoints don't all live on the same clean corporate network. It manages devices across every environment an enterprise actually runs.



Corporate Offices

LAN and WAN with DHCP or DNS auto-provisioning.



Branch Locations

Local zDM caches firmware and certificates for efficient updates without WAN dependency.



Remote Workers

Manual provisioning fallback for home and public networks. WebSSH and NoVNC for remote access.



Public Networks

Public zDM deployment enables secure management without VPN requirements.



Air-Gapped

Cloud-extension reverse tunnel allows isolated zMAN servers to manage external endpoints securely.

Core Capabilities



Zero-Touch Provisioning

Endpoints auto-discover the zDM server at first boot using DHCP scope options, DNS, or mDNS. No manual configuration required for devices on managed networks.



802.1X & SCEP Certificate Support

Operates in 802.1X-secured networks and integrates with SCEP servers for automated certificate-based authentication, distributed during provisioning or via the console.



Policy, Profile & Power Management

Deploy configuration profiles and security policies across individual devices, groups, or the entire fleet with a single operation. Control power schedules, display, and peripheral settings.



WebSSH & NoVNC Remote Access

Browser-based remote access tools let IT teams connect to any managed endpoint through public zDM deployments — without dispatching a technician or requiring user action.



Air-Gapped Cloud Extension

For fully isolated zMAN deployments, the cloud-extension model uses a cloud-hosted zDM as a secure reverse-tunnel gateway without exposing zMAN publicly.



Manages the Full SnapOS Feature Set

Including hardware-agnostic deployment on most x86 devices or VMs, live boot for contractors and BYOD users, and Dual-Boot Deployment for phased Windows migrations.



Manual Provisioning Fallback

For home, remote, and public networks where discovery services are unreachable, administrators provision endpoints manually with the zDM server IP and enrollment key.



Disk Encryption

Protect endpoint data at rest using TPM-based or passphrase-based full disk encryption. Lost, stolen, or decommissioned devices remain protected without additional tools.



Firmware & File Caching on zDM

Cache firmware images, certificates, and configuration files locally on zDM servers at each site. Reduces WAN bandwidth and improves provisioning performance at remote locations.



Remote Diagnostics with zDiag

The integrated zDiag tool gives IT teams detailed endpoint diagnostics without physical access. Identify and resolve connectivity issues, configuration mismatches, and system errors remotely.



Session & Event Management

Monitor active sessions, review event logs, and track device health across the entire fleet from the zMAN Director dashboard complete operational visibility from one interface.

Architecture Overview

zMAN Director uses a distributed architecture that separates central management from device-level communication, allowing organizations to scale across thousands of endpoints while maintaining flexibility across every network model.



zMAN Director

Central management console. Administrators monitor device status, manage profiles and policies, deploy certificates and firmware, and access remote support tools from a unified interface.



zDM Server

Device management component deployed at each site or in cloud/public configurations. Handles endpoint communication, provisioning, firmware and file caching, and WebSSH/NoVNC relay.



SnapOS Endpoint

SnapOS-powered x86 or virtual endpoint. Receives policy from zMAN via zDM, auto-provisions at first boot, and can be remotely accessed, diagnosed, and updated without IT on-site.

Four Deployment Models

zMAN Director supports four deployment models, giving organizations the flexibility to manage endpoints regardless of how their infrastructure is designed.

01. On-Premises

zMAN and zDM deployed on internal servers. Endpoints on the same LAN or WAN auto-provision via DHCP or DNS. Firmware and certificates cached locally on zDM for efficient distribution.

02. Cloud Hosted

zMAN deployed in a cloud environment. zDM servers at each site relay endpoint communication to the cloud-hosted console. Ideal for organizations reducing on-premises infrastructure.

03. Public zDM

A publicly accessible zDM instance acts as a relay for remote and home workers not on the corporate network. Endpoints connect to zDM over the internet without requiring a VPN.

04. Remote Diagnostics via zDiag

zMAN remains fully isolated on a private network. A cloud-hosted zDM acts as a secure reverse-tunnel gateway, allowing external SnapOS endpoints to reach the air-gapped zMAN server without exposing it publicly.

Built for How Enterprises Actually Run

Most endpoint management platforms assume every device is on a reliable corporate network. Real enterprise environments don't work that way. You have remote workers on home broadband, branch offices with unreliable WAN links, kiosks on public Wi-Fi, and in some industries, endpoints that can never touch the internet at all.

zMAN Director was built for those realities. The multi-model deployment architecture, local firmware caching at zDM, manual provisioning fallback, and air-gapped cloud extension are not afterthoughts. They are features designed specifically for organizations managing endpoints across environments that don't fit a clean network diagram.

THE COMPLETE ENDPOINT LIFECYCLE

Convert, provision, push, monitor, update, and support without dispatching anyone

Paired with SnapOS, zMAN Director gives IT teams the complete endpoint lifecycle: convert existing hardware or deploy virtual endpoints, provision automatically, push policy, monitor remotely, update silently, and support without ever dispatching someone on-site at a cost structure that doesn't penalize you for scaling.

The Complete AmZetta Endpoint Stack

SnapOS

Converts any x86 device or virtual machine into a secure, immutable, hardware-agnostic managed endpoint, with support for live boot sessions and dual boot for phased Windows migration.



zMAN Director

Manages every SnapOS device from a single centralized console. Together, they replace Windows endpoint complexity and the cost and lock-in of legacy management platforms with a purpose-built, centrally controlled, cost-efficient endpoint platform.

Who zMAN Director is For



IT Managers & Sysadmins

Managing distributed endpoint fleets across multiple sites and network environments without the overhead of on-site visits or reactive support workflows.



Security-Conscious Environments

Enforcing 802.1X network access, certificate-based authentication, disk encryption, and policy-driven endpoint controls across every managed device.



Healthcare, Finance & Regulated Industries

Maintaining endpoint compliance, auditability, and access controls across distributed clinical, branch, and remote environments with centralized policy enforcement.



Remote & Branch Workforces

Supporting endpoints across home networks, branch offices, public locations, and corporate headquarters from a single management plane without VPN dependency.



Air-Gapped & Zero-Trust Deployments

Managing endpoints in fully isolated environments using the cloud-extension reverse tunnel model without exposing the zMAN server to the public internet.



Teams Outgrowing Their Current Platform

Replacing a dedicated endpoint management tool that has become more expensive or restrictive after a vendor acquisition or industry consolidation without losing enterprise-grade control.

GET STARTED

See zMAN Director in Action

Connect with an AmZetta Solutions Engineer for a free 30-day evaluation of zMAN Director and SnapOS. No obligation. Expert setup guidance included.

amzetta.com/eval

Call 1-877-991-1809

Visit amzetta.com/eval or call 1-877-991-1809 to learn more or connect with an AmZetta Solutions Engineer.

