Camera Onboarding at Scale — Runbook & Checklist

Discovery finds a camera; onboarding secures, configures, and manages it. Run the pipeline by template, not by hand — at 600 cameras that is roughly 5 hours versus 50. A one-page operational map.

Discovery: four ways to find cameras across a segmented network

Method	When it works	Watch out for
Multicast WS-Discovery	Cameras on the VMS's own VLAN / segment	Stops at the first router
Discovery proxy / relay	Cameras on other VLANs (managed mode)	One relay per segment to run
Unicast range scan	Across routers, when you have the ranges	Slower; schedule it, avoid storms
Direct address import	You already have an IP-address plan	Often the fastest path at scale

The onboarding pipeline: six stages, by template

Stage	Do this	Prevents
1 Authenticate	Replace the factory password first; set a strong, unique credential	Credential sprawl, breach
2 Secure identity	Issue a certificate; enrol in 802.1X where the network uses it	Untrusted devices at scale
3 Configure	Set NTP time; set recording + sub-streams by ONVIF profile	Clock skew, stream surprises
4 Assign	Name, location, and group per a naming convention	An unsearchable haystack
5 Place	Put on a recording server with measured headroom	Server overload
6 Verify	Confirm it records, both streams arrive, time + an event	Phantom (non-recording) cameras

Fleet hygiene: what keeps a large deployment healthy after day one

Topic	Keep it healthy by	Cadence
Credentials	Strong, unique, recorded per camera; bulk-rotate when needed	On staff change / policy
Firmware	Use campaign tooling; stagger pushes to spare site bandwidth	Track and patch security fixes
Certificates	Track expiry and rotate before a certificate lapses	Before expiry, automated
Discovery	Scheduled, scoped scans — never a constant broadcast	Avoid storms at scale
Verification	Re-check that a sample of cameras still records correctly	Routine audit

Rule of thumb: discover broadly, onboard by template, verify everything, and own firmware and certificates for the life of the fleet. Replace the factory password before a camera ever touches the network — default credentials are how camera fleets get breached (CISA TA16-288A). Sources: OASIS WS-Discovery 1.1; ONVIF Core Specification; IEEE 802.1X; NIST SP 1800-36; CISA TA16-288A; Milestone XProtect system scaling.