

BUILT FOR DISTRIBUTED. PROVEN FOR THE CONTROL ROOM.

Boxilla FailSafe expands Boxilla High Availability from **two nodes to as many as four Boxilla Manager units** in a single cluster. Built for distributed, mission-critical environments, it lets organizations deploy a resilient management cluster across multiple buildings, campuses, or cities, with intelligent handling of network splits and automatic recovery when connectivity is restored. The result is continuous management availability with no manual recovery procedures and no additional hardware investment for existing Boxilla customers.

HOW FAILSAFE KEEPS YOU ONLINE

Autonomous Split Management

When a network link fails, each isolated segment keeps managing its own KVM infrastructure through a self-elected master node. No management blackout, no technician callout.

Intelligent Re-join

When segments reconnect, the Cluster Monitor service orchestrates the re-join and consolidates the cluster back to a single coordinated master, freeing operators from complex manual recovery steps.

Node Priority Control

Assign a unique priority to each node so the strongest, best-connected unit always wins master election. Failover and re-join behavior become predictable and deterministic.

Why high availability matters: Mission-critical control rooms cannot tolerate a management blackout. FailSafe keeps Boxilla management available at every site, even during a network split, with no manual recovery and no new appliances for existing customers.

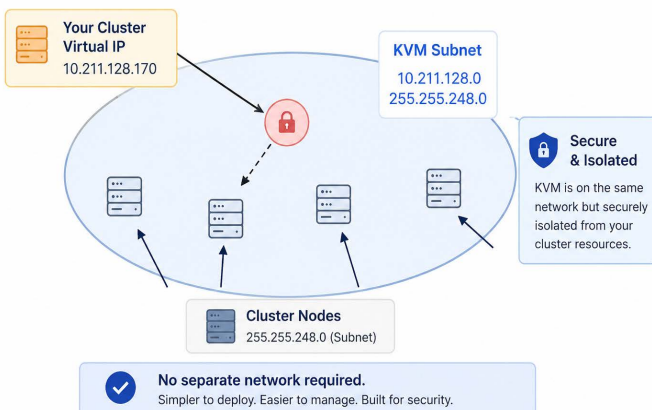
KEY PROOF POINTS

- Scales from two to four nodes on existing hardware
- Cross-subnet, multi-site deployment
- Autonomous master election per isolated segment
- Automatic re-join and cluster consolidation segment
- Deterministic node-priority failover
- Conditional Virtual IP, single or multi subnet
- TLS 1.2 encrypted management communications
- No additional appliance investment required

FailSafe allows Boxilla and KVM resources to operate on the same network segment, giving organizations a single, highly available point of access to their distributed operations. Operators can manage systems across multiple control room locations through one consistent interface, simplifying administration and reducing downtime. This approach improves operational continuity, streamlines failover, and ensures critical workflows remain accessible when every second counts.

Your Cluster Stays on the Same Network

KVM is placed on the same subnet and isolated from your cluster.



TECHNICAL SPECIFICATIONS

SPECIFICATION	DETAIL
Platform	Boxilla KVM and AV/IT Management Appliance (BXAMGR-R2)
Minimum Firmware	Boxilla FW v5.1 and above (free to upgrade)
Cluster Size	2 to 4 Boxilla Manager nodes per cluster
Node Topology	No fixed topology. Nodes deployable across locations, IP ranges, and subnets
Node Priority	Unique value (1 to 4) per node for master election and re-join arbitration
Virtual IP	Maintained on a single subnet. Master physical IP used for WebUI access on multi subnet
Cluster Monitor	Background service, configurable interval (default 20 seconds), confirms stable state before acting
Upgrade Path	Staged Detach, Upgrade, Switchover, Prepare Standby with no service interruption

CLUSTER BEHAVIOR

EVENT	CATEGORY	WHAT HAPPENS
Network Split	Availability	Each segment self-elects a master to preserve KVM management
Reconnect	Recovery	Cluster Monitor re-joins and consolidates to one master automatically
Master Election	Arbitration	Highest-priority, best-connected node wins deterministically

Re-join database behavior: if a cluster splits and configuration changes are made on more than one segment during the outage, those database timelines cannot be merged on re-join. The selected master database is carried forward and changes made on the other segment during the split are not reconciled.

TARGET ENVIRONMENTS

Multi-Site Command & Control

PSAP, ATC, EOC, and dispatch operations spanning multiple buildings or cities

Distributed Campuses

Universities, hospitals, and corporate sites running KVM across separate subnets

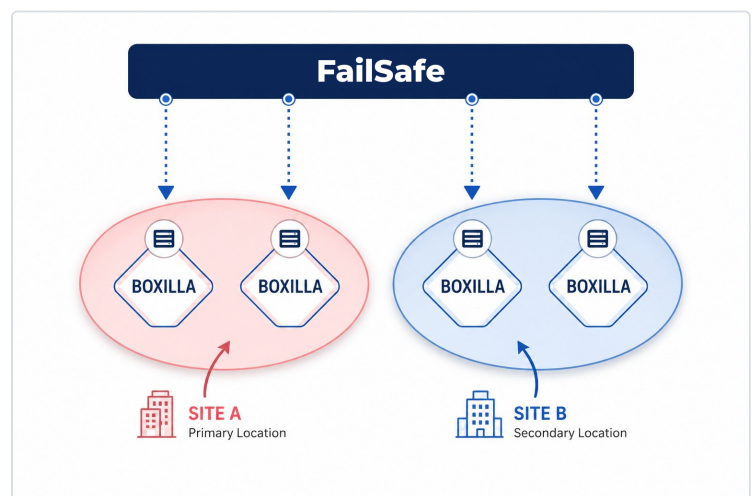
24/7 Mission-Critical Ops

Broadcast, utilities, and transportation control rooms that cannot go dark

Government & Critical Infrastructure

Defense, public sector, and industrial environments needing resilient management

FCC	CE	RoHS	UL/CB	TLS 1.2	AD / LDAP
SNMP · NTP · Syslog					



Four-Node Clustering

Scale from two to four Boxilla Managers via firmware upgrade on existing hardware

Autonomous Failover

Each isolated segment self-elects a master, with no management blackout

Intelligent Re-join

Automatic consolidation back to a single master, no manual recovery

Zero New Hardware

Runs on existing BXAMGR-R2 appliances, no additional appliance investment