IPAManager

RELEASE NOTES

Version 1.0.0 | Initial Release

A concise publication-ready summary of the first public release, covering product scope, included capabilities, monitoring alerts, configuration management, and security controls.

PUBLICATION DATE: [Insert release date] **AUDIENCE:** Customers, evaluators, administrators, and deployment stakeholders

IPAM Manager v1.0.0 introduces the initial production release of the platform. The release establishes a single operating workspace for IP address management, subnet oversight, discovery review, topology visibility, inventory operations, monitoring alerts, configuration management, administrative governance, maintenance, and login-access protection.

Release Summary

Product	IPAM Manager
Version	1.0.0
Release type	Initial release
Primary scope	Unified IPAM, discovery, inventory, topology, monitoring, configuration management, administration, maintenance, and security workflows
Companion document	Administration Guide (recommended for day-to-day usage and configuration reference)

Initial Release Highlights

This document is intentionally concise. It summarizes the content of the initial release rather than replacing the full Administration Guide.

- Unified dashboard-based operational entry point for daily administration.
- Core IP address management workflows through Subnets, Class Summary, and Subnet Calculator.
- Discovery traceability and network visualization through Scan History and Topology.
- Inventory review and operational standardization through Network Inventory, Inventory Info, and Templates.
- Administrative governance through Users, Credentials Vault, Logs, Settings, Certificates, License, and Scans Scheduler.
- Built-in access hardening through allowlists, brute-force protection, idle session timeout, and pre-save policy testing.
- Integrated monitoring engine for device availability, latency, CPU, memory, alert visibility, recovery awareness, and email notification workflows.
- Configuration management engine for network device configuration backup, preservation, review, and recovery-support workflows.

Included Capabilities in v1.0.0

Capability Area	Included Modules and Scope
Platform entry	Dashboard for fast navigation into addressing, discovery, inventory, and system administration.
Address management	Subnets, Class Summary, and Subnet Calculator for planning, review, CIDR validation, and subnet oversight.
Discovery and visibility	Scan History for operational traceability and Topology for device-relationship visualization.
Monitoring and alerts	Monitoring engine for availability, latency, CPU, memory, alert state, recovery awareness, and email notification rules.
Configuration management	Configuration backup and management workflows for collecting, preserving, reviewing, and supporting recovery of network device configurations.
Inventory and standardization	Network Inventory and Inventory Info for broad and targeted estate review, plus Templates for repeatable standards.
Governance and accountability	Users, Credentials Vault, and Logs for access administration, credential control, and event review.
System operations	Settings, Certificates, License, and Scans Scheduler for maintenance, trust workflows, licensing oversight, and repeatable discovery scheduling.
Security and hardening	Security workspace with global allowlist, per-user allowlists, brute-force thresholds, session idle timeout, and test-before-save validation.

Security Features Introduced in v1.0.0

The initial release includes built-in administrative controls intended to reduce unnecessary login exposure and improve access governance.

Control	Description
Global allowlist	Restricts login access to trusted addresses or address ranges at the platform level.
Per-user allowlists	Applies stricter source-IP controls to selected accounts, including privileged users.
Brute-force protection	Configurable failure window, lockout duration, and maximum failures per IP address and per username.
Session idle timeout	Automatically logs out authenticated sessions after a defined period of inactivity.
Test access before saving	Validates a proposed policy against a selected user and source IP before committing the change.

Supported OS

The current installation package is distributed in .deb format and is intended for Debian-based Linux environments.

Category	Supported Scope
Directly supported	Ubuntu deployments using the .deb installation package. Windows deployments using the .exe installation Windows 11 x64 Windows Server 2025 x64 Windows Server 2022 x64 Windows Server 2019 x64 Windows Server 2016 x64
Not covered by the .deb package	RHEL, CentOS, Rocky Linux, AlmaLinux, Fedora, openSUSE, Arch Linux, and other non-Debian package ecosystems require a different packaging approach.

Documentation and Publication Notes

- The Administration Guide should remain the primary reference for daily usage, onboarding, and configuration workflows.
- This release note provides a concise customer-facing summary of the initial release.
- Package filenames, checksums, release date, and commercial terms may be appended before publication if needed.
- Monitoring thresholds, alert notification behavior, and configuration backup retention should be validated against the Administration Guide before production rollout.

Revision History

Version	Status	Date	Notes
1.0.0	Initial release	28/03/2026	First public release notes.