IPAManager Administration Guide

Version 1.0.0

IPAM Manager

This guide is designed for administrators who operate the platform day to day. It explains what each major module is for, why it matters operationally, and how the product supports structured address management, discovery review, configuration backup, monitoring retention, access control, and system maintenance.

The emphasis here is on platform usage and administrative value rather than on validation details or test evidence.

Using this guide

The guide is organized around administrative responsibilities instead of internal route names. This makes it easier to read the document as a product manual and to use it during onboarding, handover, or operational review.

How to read it. New administrators typically begin with the dashboard and IP address management sections, then expand into discovery, inventory, configuration backup, monitoring, access governance, and system maintenance as their responsibilities grow.

Contents

1. Prerequisites Before First Use

This chapter outlines the environment, connectivity, and access prerequisites that should be validated before the first production use of IPAM Manager.

1.1 Environment and Access Readiness

Purpose

This section helps administrators confirm that IPAM Manager can reach target devices and authenticate successfully before relying on discovery, inventory, or topology workflows.

Administrative value

Validating prerequisites up front reduces false failures, shortens troubleshooting time, and prevents avoidable first-run issues that are often caused by blocked management traffic, incorrect credentials, or missing protocol configuration.

Typical uses

- Allow management traffic from the IPAM Manager server IP to the target devices over SSH and SNMP through all relevant firewalls, ACLs, and segmentation boundaries.
- Verify that valid device credentials are available and tested for the intended management method, including username and password for SSH and the correct SNMP version, community string, or SNMPv3 parameters.
- Confirm that the IPAM Manager server can reach device management IP addresses over the expected routes and that DNS resolution is available where hostnames are used.
- Ensure the required device-side management services are enabled, such as SSH and SNMP, and confirm that topology-related protocols such as LLDP are enabled when richer neighbor visibility is expected.
- Review the initial scan scope and target subnet list before the first discovery run so the platform is pointed at the correct management ranges.
- Verify that system time is synchronized on the IPAM Manager server and on key network devices so logs, scan history, and scheduled operations remain reliable for troubleshooting and audit review.

Operational guidance. Complete these checks before the first production scan, after major network segmentation changes, or whenever a new site or device type is brought under management.

2. Getting Started

This chapter introduces the platform entry experience and the navigation model that helps administrators move efficiently between day-to-day tasks.

2.1 Dashboard

Purpose

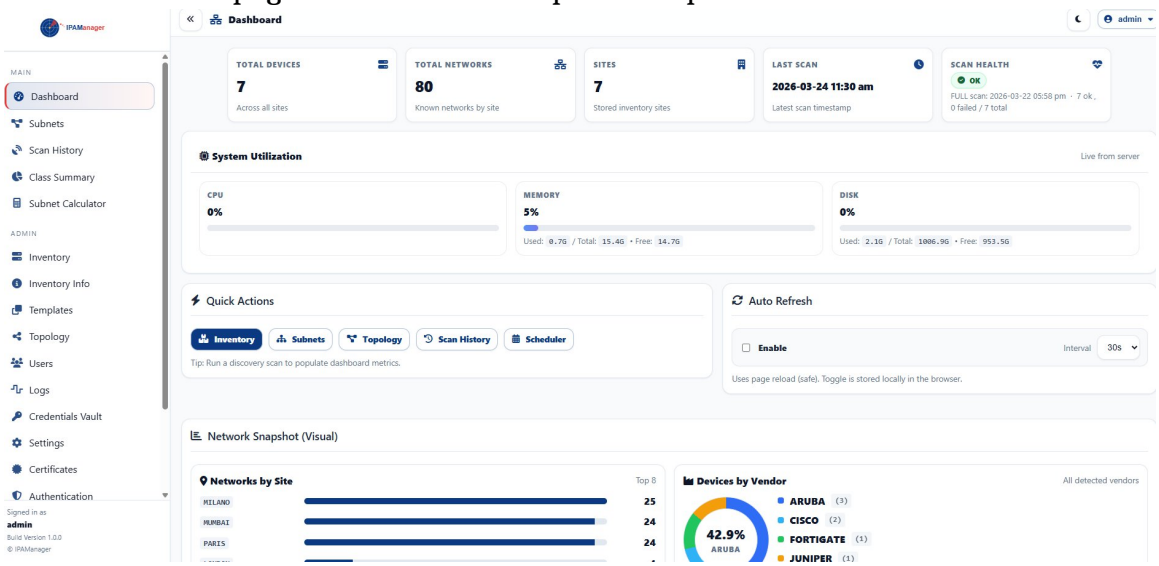
The dashboard is the operational home screen for the product. It brings the main modules together in one place and helps administrators orient themselves quickly at the start of a task or working session.

Administrative value

Use the dashboard to review the current context and move directly into the module that matches the next operational task. It is most effective as a launch point for daily work, not as a destination for prolonged data entry.

Typical uses

- Move from the landing page into addressing, discovery, inventory, and system administration with minimal navigation overhead.
- Use the dashboard to shorten the path between review and action.
- Treat the page as a central workspace for operational awareness.



Dashboard workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

3. IP Address Management

These modules support the core responsibilities of address planning, subnet oversight, and day-to-day review of managed ranges.

3.1 Subnets

Purpose

The Subnets page is the main administrative workspace for reviewing managed ranges, spotting overlap risk, and organizing subnet-related operations.

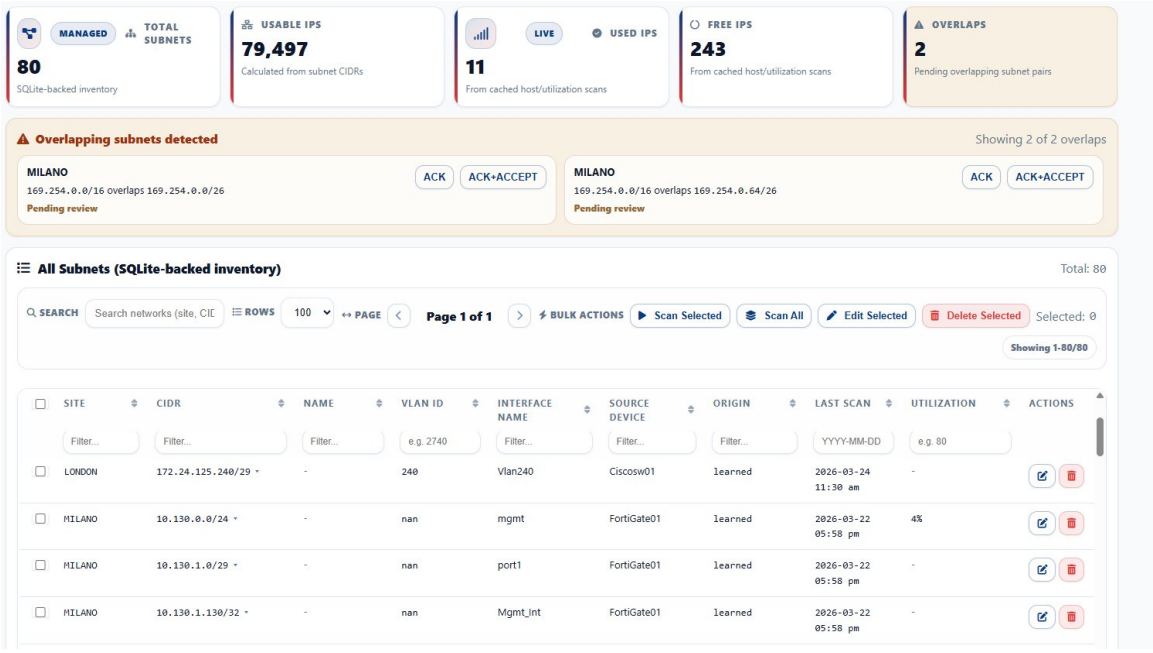
Administrative value

This page is where administrators spend much of their time. It combines visibility, structure, and operational control in a single view, making it easier to review address usage before making changes.

Typical uses

- Search and review subnet records by site, CIDR, VLAN, or naming pattern.
- Open add and bulk workflows when a controlled update is needed.
- Use the page to keep address data consistent and operationally reliable.

Subnets workspace



Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

3.2 Class Summary

Purpose

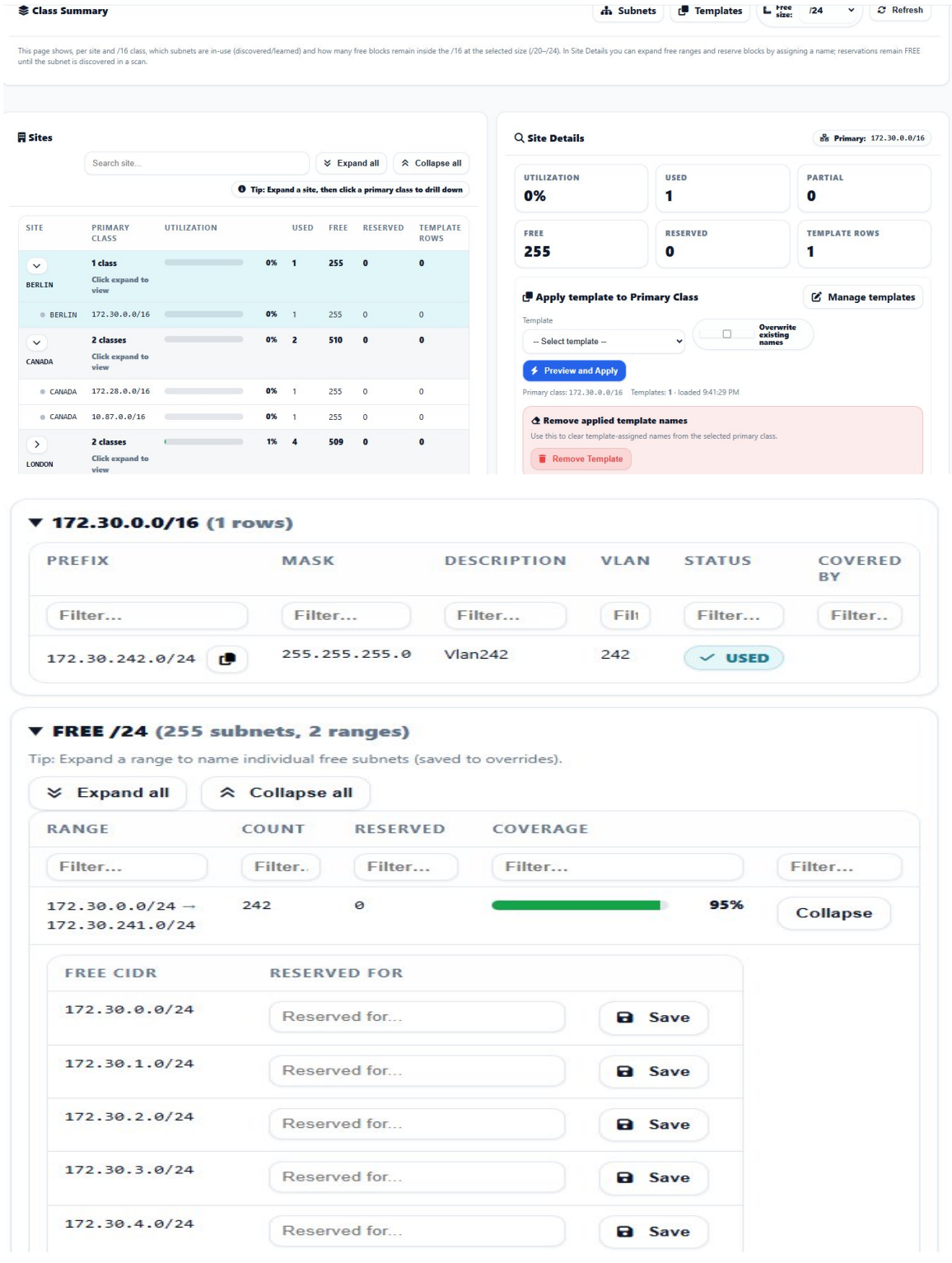
Class Summary provides a broader planning view that groups address data above the level of individual subnet records.

Administrative value

This view is valuable when administrators need to reason about structure, reservations, and planning patterns across larger blocks of address space.

Typical uses

- Expand planning groups to review organization across multiple ranges.
- Use the page when standardization matters more than record-by-record editing.
- Apply it during planning and governance reviews.



Class Summary workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

3.3 Subnet Calculator

Purpose

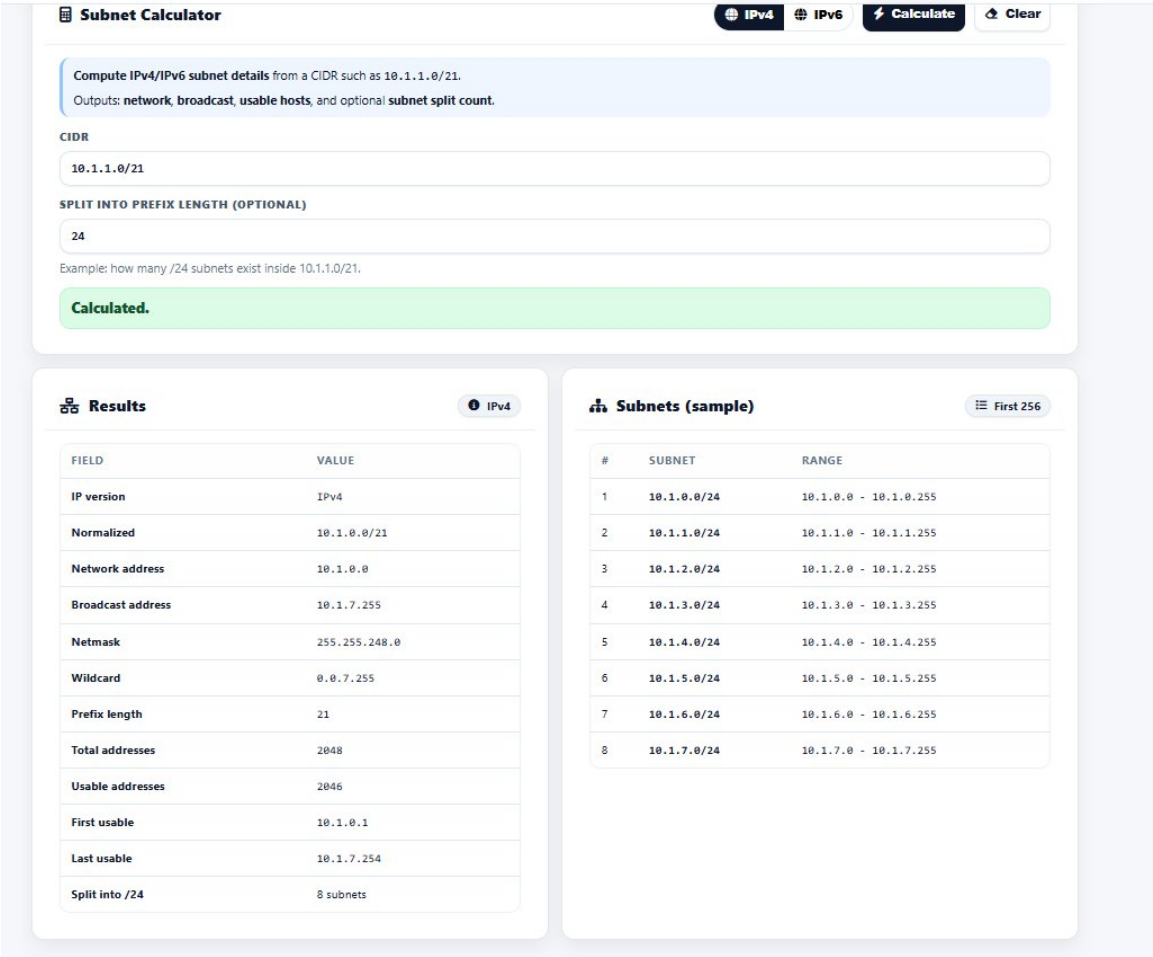
The calculator helps administrators validate CIDR input and confirm addressing outcomes before applying a real change elsewhere in the system.

Administrative value

It adds speed and confidence to planning work by keeping quick verification inside the platform rather than pushing administrators into an external calculator.

Typical uses

- Use it during design, review, and troubleshooting discussions.
- Validate expected subnet outcomes before creating or updating records.
- Keep it as a safe planning aid separate from production changes.



Subnet Calculator workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

4. Discovery, History, and Topology

These pages help administrators understand what the platform has discovered, what happened previously, and how infrastructure relationships can be reviewed visually.

4.1 Scan History

Purpose

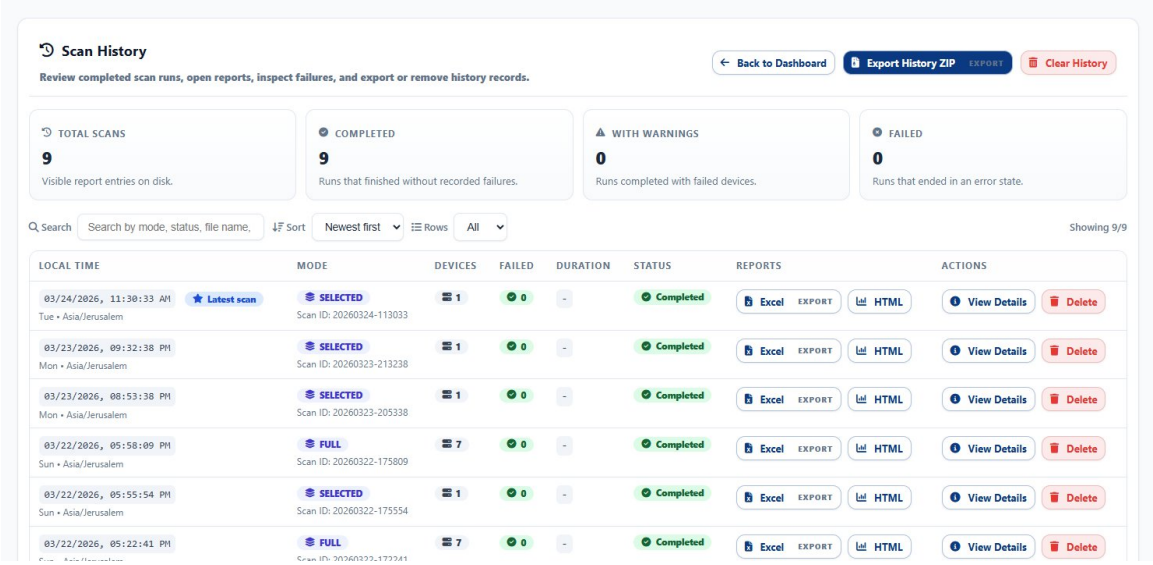
Scan History records prior discovery activity so administrators can review completed runs and inspect historical scan context.

Administrative value

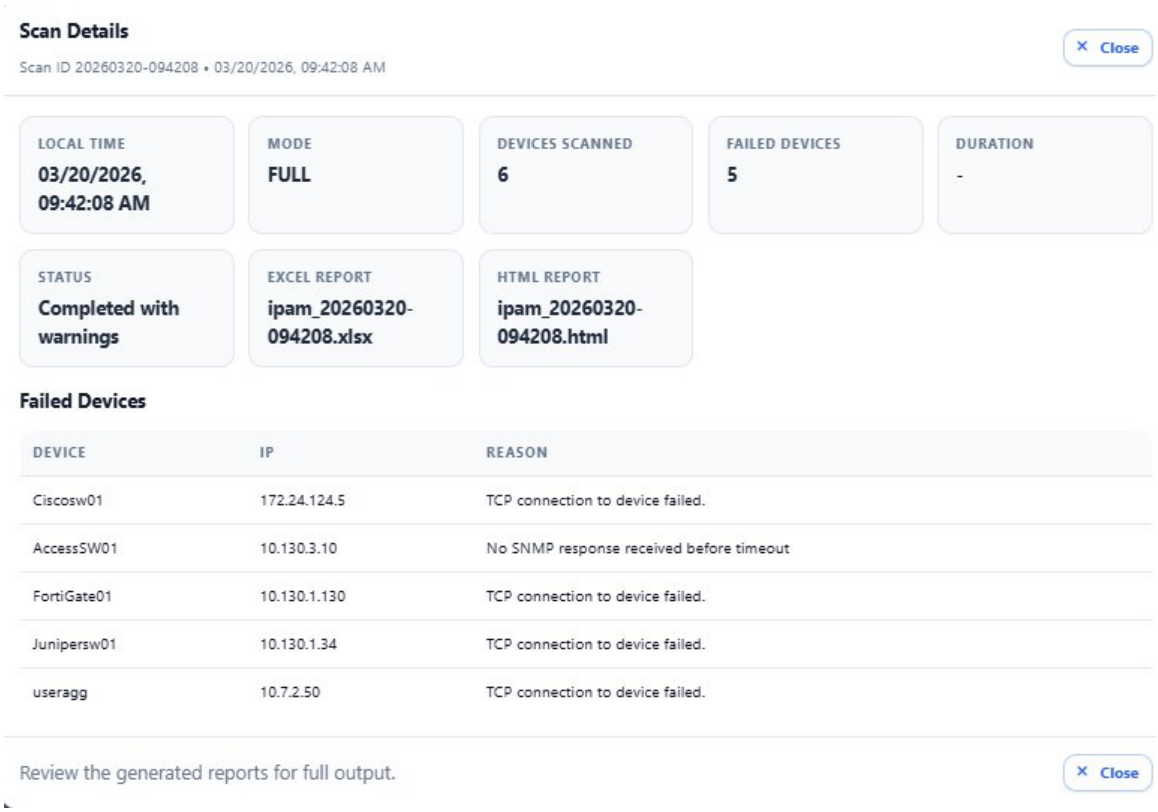
Its value is operational traceability: administrators can confirm whether discovery happened, narrow the review to a specific event, and inspect detail without leaving the platform.

Typical uses

- Search for a relevant run, period, or operational context.
- Open detail views when the summary line is not enough.
- Use the page as part of routine validation and troubleshooting.



Scan History workspace



Scan History supporting view

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

4.2 Topology

Purpose

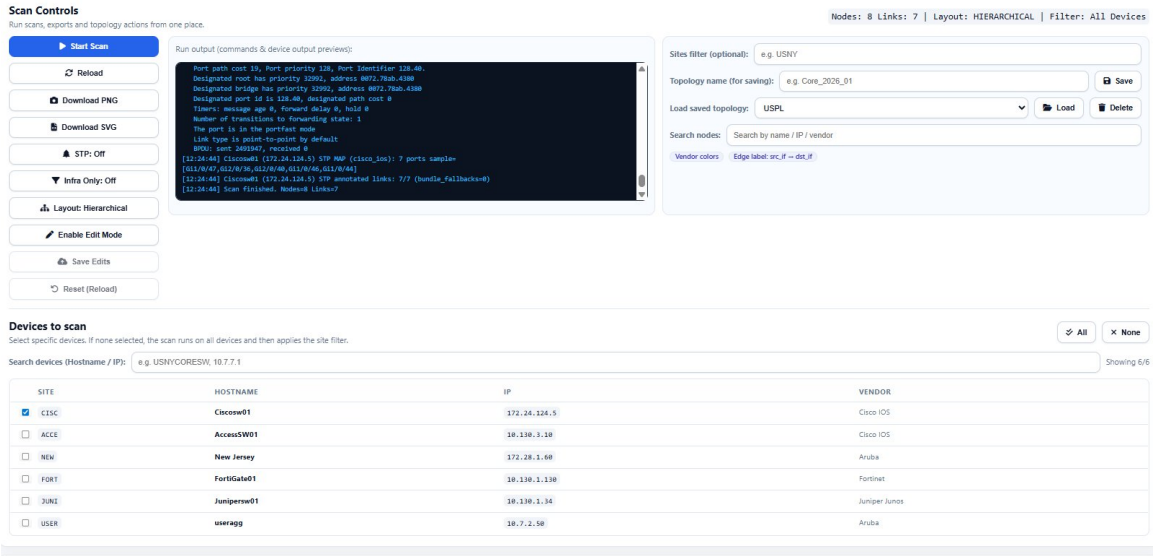
Topology presents device relationships in a visual format that complements list-based and table-based views.

Administrative value

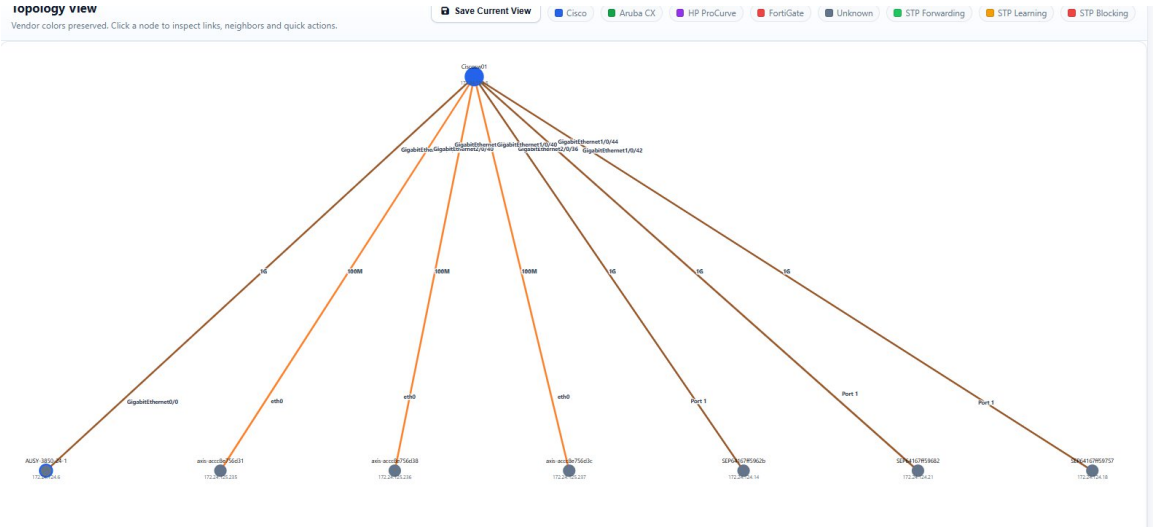
Visual context matters when administrators need to explain connectivity, review infrastructure areas quickly, or orient themselves during troubleshooting and change planning.

Typical uses

- Search for a device or area to focus the view.
- Use saved views to revisit known network segments efficiently.
- Apply the topology view when a visual explanation is more useful than raw tables.



Topology workspace



Topology output

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

5. Inventory, Templates, and Configuration Backup

These modules help administrators review the discovered estate, apply consistent structure across repeated tasks, and preserve network device configuration state for review and recovery planning.

5.1 Network Inventory

Purpose

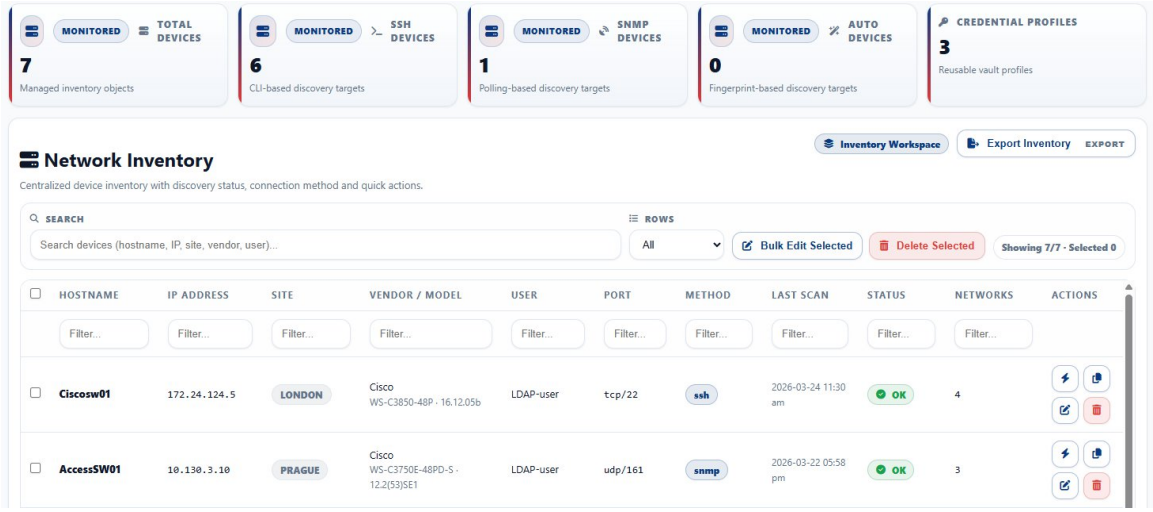
Network Inventory provides a broad, operational view of the devices and assets the platform is tracking.

Administrative value

It is most useful as a review and export surface: administrators can confirm what the platform sees and use that information to support planning, audits, or handoff activities.

Typical uses

- Use the page to review the current asset picture at a glance.
- Export information when a wider review or offline analysis is required.
- Cross-check the inventory when validating discovery coverage.



Network Inventory workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

5.2 Inventory Info

Purpose

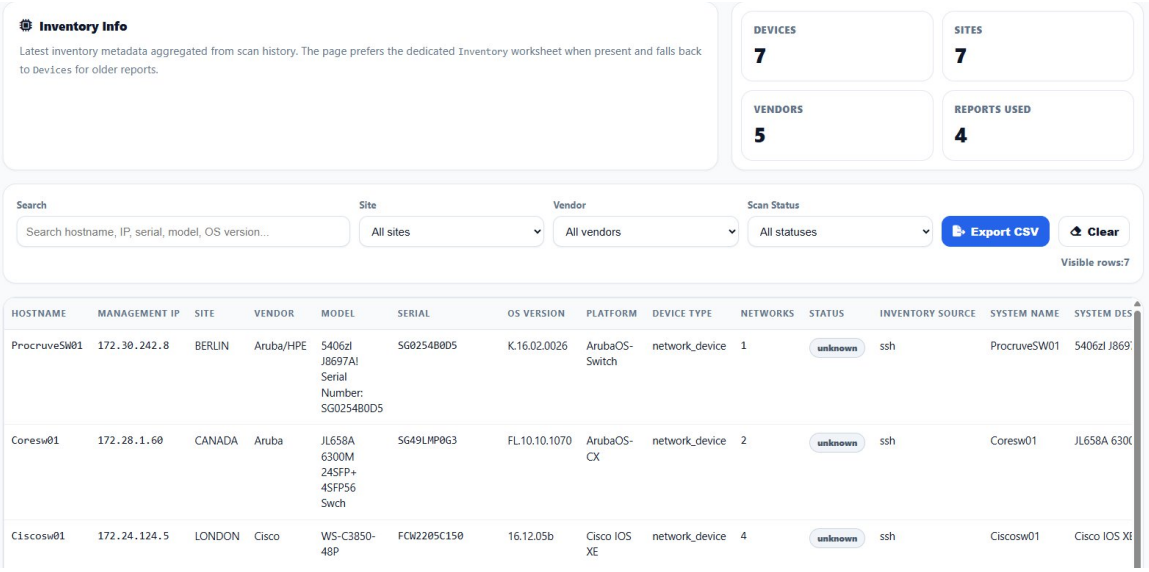
Inventory Info offers a more targeted and filter-friendly operational view of inventory data.

Administrative value

Compared with the broader inventory page, this page is better suited to focused review and support work where administrators need narrower results.

Typical uses

- Search for specific devices or operational criteria.
- Use the page when troubleshooting, documenting, or preparing a targeted export.
- Treat it as the detail-oriented companion to the broader inventory view.



Inventory Info workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

5.3 Templates

Purpose

Templates help standardize repeated patterns and reduce manual inconsistency across the environment.

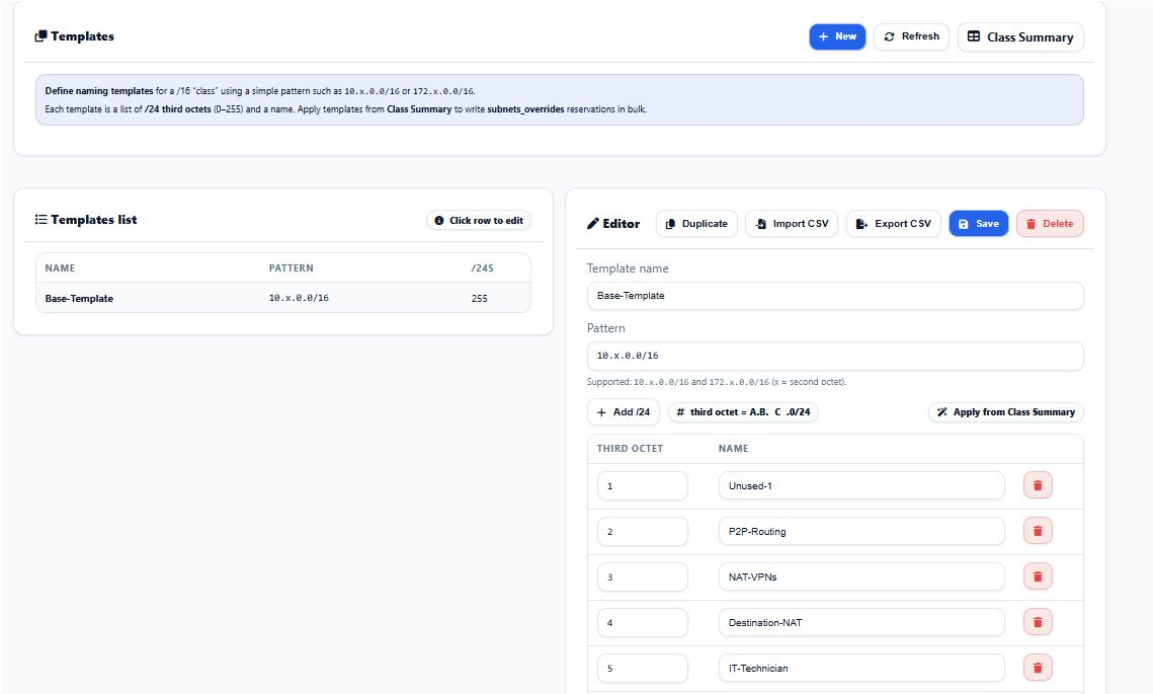
Administrative value

In mature environments, templates support better governance because they help different administrators work in a more consistent way.

Typical uses

- Create reusable patterns when the same structure appears repeatedly.
- Review template definitions as operational standards evolve.
- Use templates to reduce manual effort and improve naming discipline.

Templates workspace



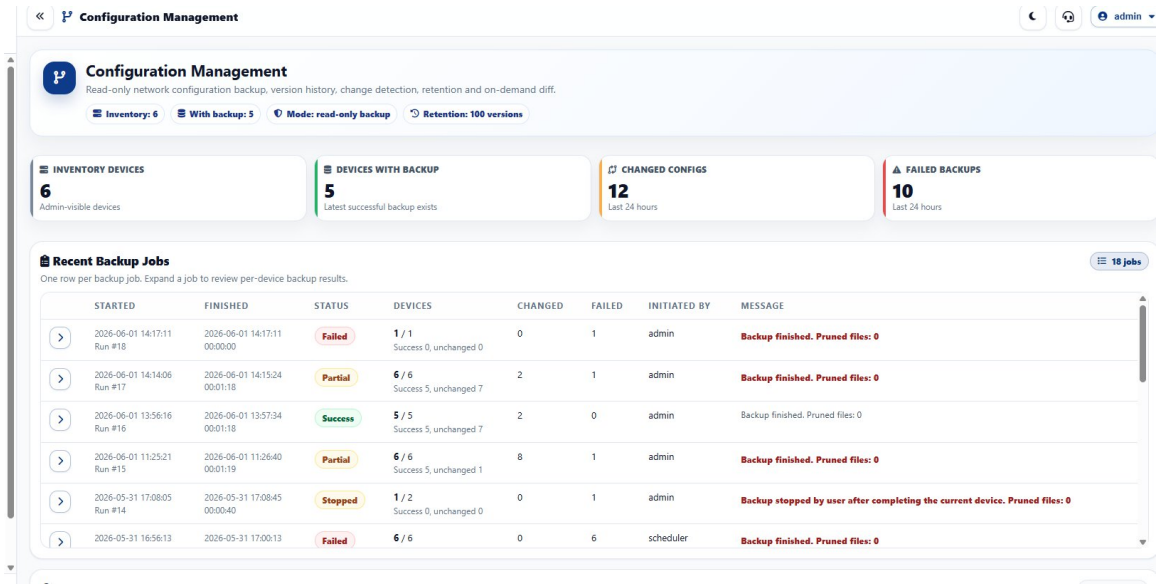
Templates supporting view

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

5.4 Configuration Backup

Purpose

The Configuration Backup page helps administrators collect, store, and review network device configurations as part of the broader IPAM Manager operating workspace.



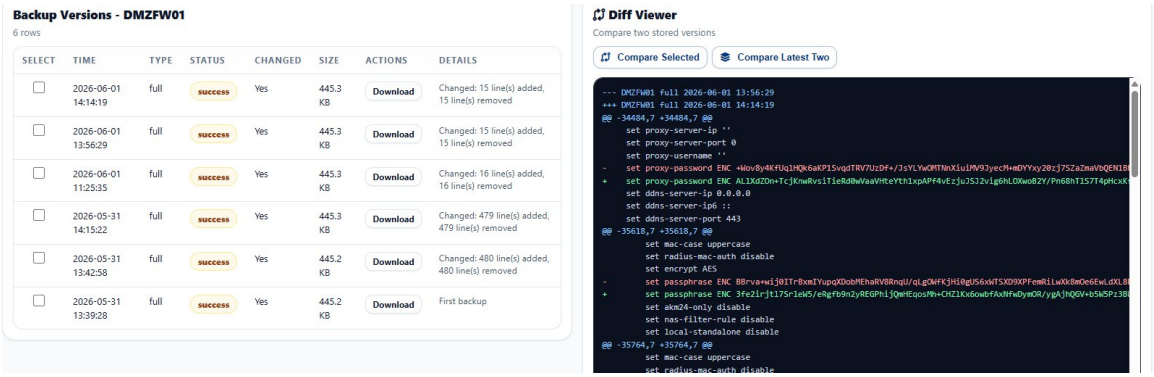
Administrative value

Configuration backup reduces dependence on manual configuration copies and gives administrators a consistent reference point for change review, recovery preparation, troubleshooting, and operational handover. It complements inventory and topology data by preserving the device state that supports real network operations.

Typical uses

- Review which managed devices are covered by configuration backup and confirm that critical infrastructure is included.
- Run or review configuration backup activity before planned changes, maintenance windows, or device replacement work.
- Confirm that recent successful backups exist for important devices and investigate failed or missing backup results.
- Use saved configuration snapshots during troubleshooting, rollback preparation, audit review, or support handoff.
- Apply retention and cleanup practices so configuration history remains useful without allowing storage usage to grow uncontrolled.

Operational guidance. Use this page before and after network changes, after onboarding new devices, and during periodic operational review. Confirm backup coverage, verify recent successful results, and keep retention aligned with the organization's recovery and audit requirements.



6. Monitoring and Retention

This chapter explains how the Monitoring page supports day-to-day operational awareness and how retention controls help administrators keep monitoring history useful, searchable, and storage-conscious.

6.1 Monitoring

Purpose

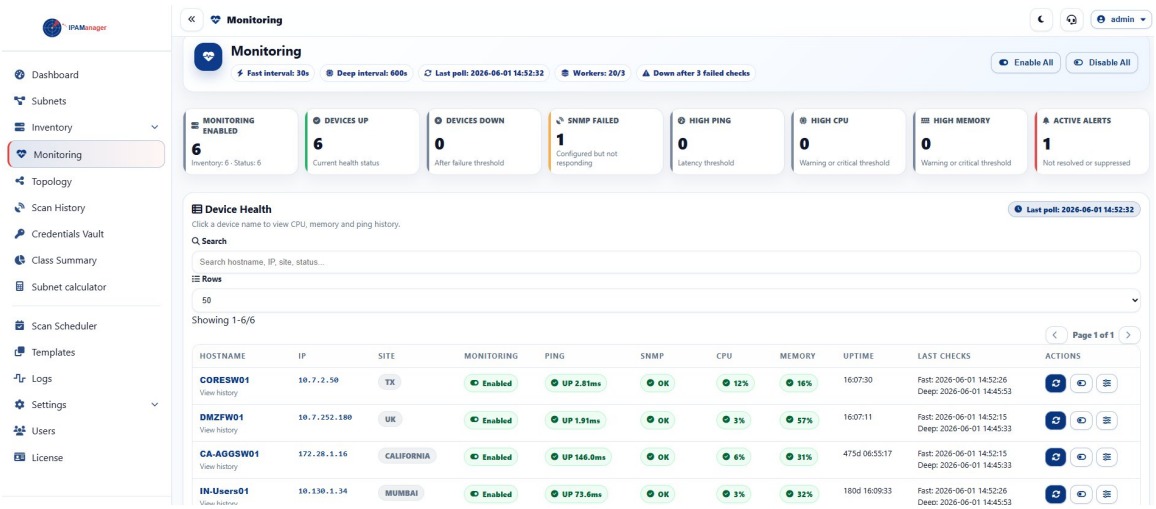
The Monitoring page provides operational visibility for monitored devices, active and resolved alerts, polling status, response health, latency, CPU usage, memory usage, and monitoring history retention.

Administrative value

Monitoring adds essential device-status awareness to the IPAM workflow. It helps administrators identify operational changes without leaving the platform, while retention settings keep historical monitoring data controlled and useful for trend review, troubleshooting, and alert analysis.

Typical uses

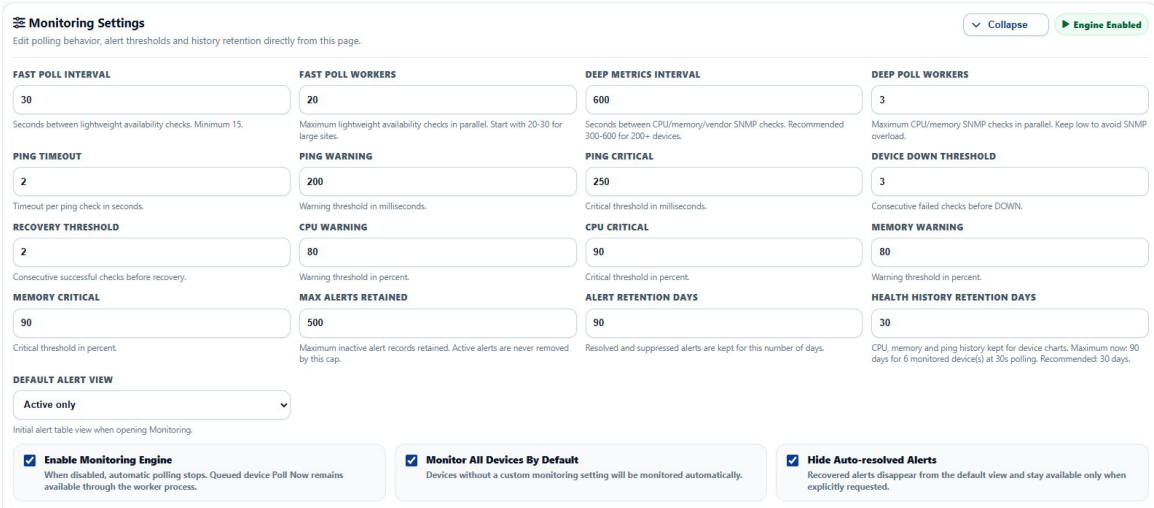
- Review monitored device status, last poll time, availability state, latency, CPU usage, and memory usage from one operational view.
- Filter active and resolved alerts to confirm current impact, recovery state, and recent operational history.
- Use device search, paging, and per-device polling actions when validating a specific device or investigating a reported issue.
- Configure thresholds and email notification rules for new alerts and recovery events so the right administrators receive timely updates.
- Review and adjust retention settings so monitoring samples, alert history, and resolved-event records remain available for the required period without unnecessary database growth.
- Reassess retention after device count, polling frequency, or operational reporting requirements change.



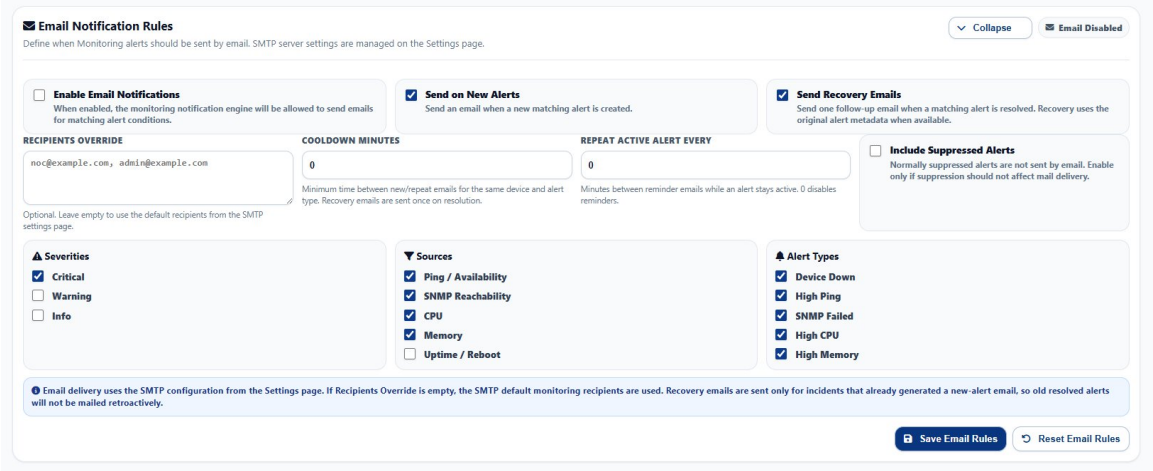
Monitoring retention guidance

Retention controls should be sized according to device count, polling frequency, alert volume, and available disk capacity. Shorter retention is suitable for compact operational review, while longer retention may be useful when teams need historical trend context, recurring incident analysis, or audit support.

Operational guidance. Review active alerts first, then confirm recent recovery events and retention settings. For larger deployments, align retention with available storage and expected polling volume before increasing polling frequency or adding many devices.



Monitoring threshold setings



Notification rules

7. Administration and Access Control

These modules support operational governance, controlled access, and administrative accountability.

7.1 Users

Purpose

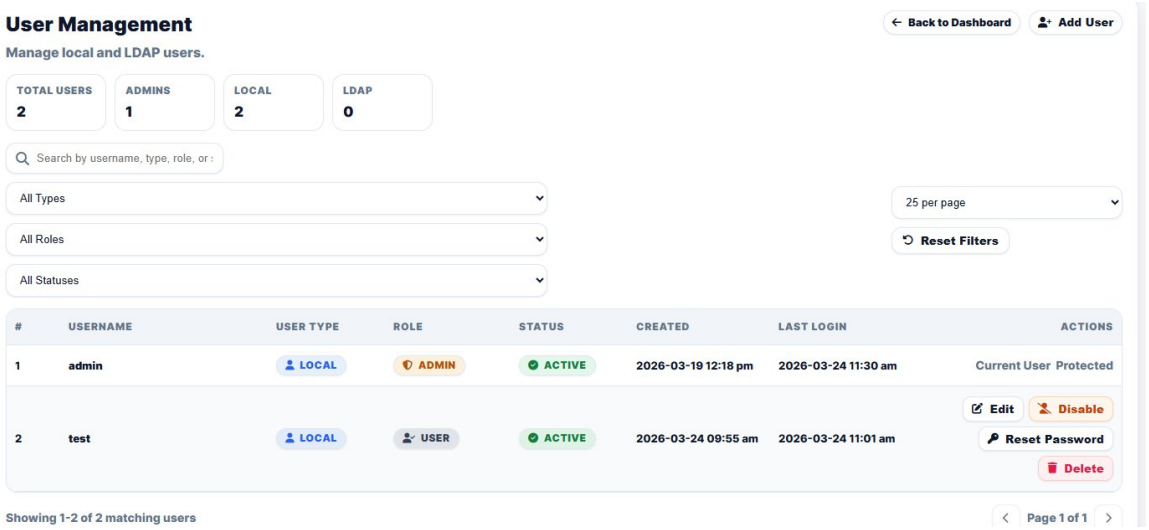
The Users page manages who can access the platform and how administrative responsibility is distributed.

Administrative value

It is a key page for onboarding, governance, and ongoing access review. Keeping it current reduces operational ambiguity and supports controlled administration.

Typical uses

- Review current user records before making access changes.
- Open the add-user flow when provisioning a new administrator or operator.
- Use the page as part of regular access governance.



Users workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

7.2 Credentials Vault

Purpose

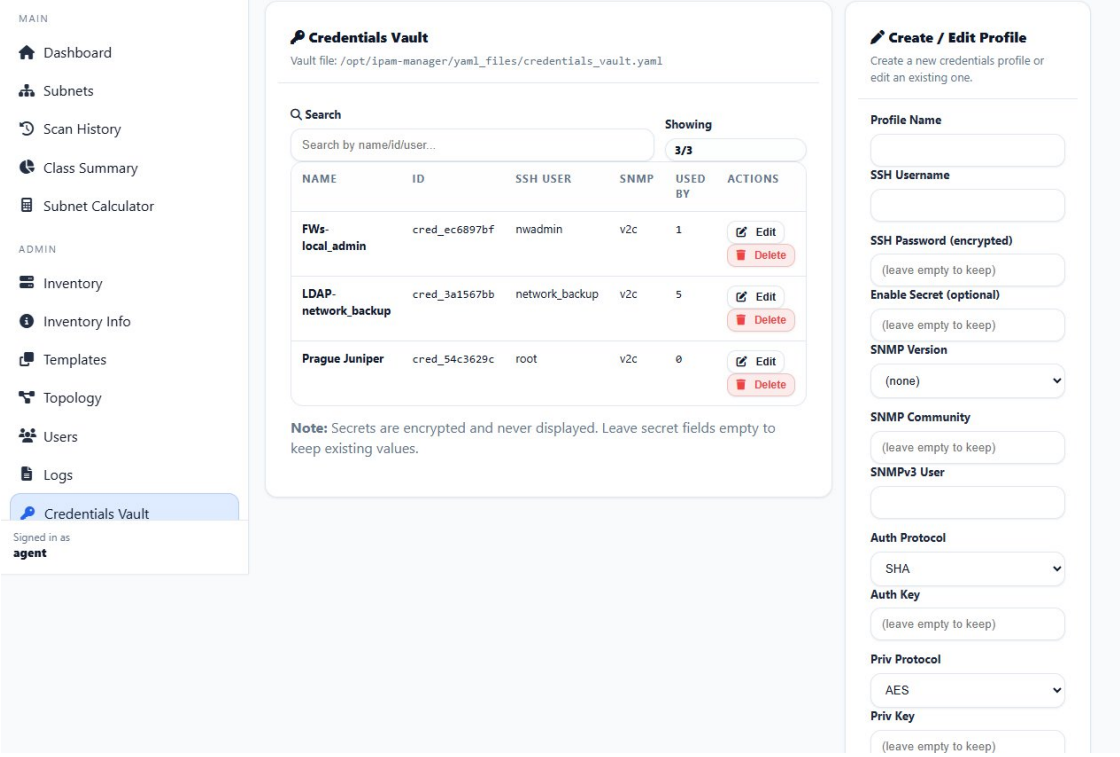
Credentials Vault centralizes the credential material the platform relies on for operational tasks.

Administrative value

Keeping credentials organized inside the platform improves consistency and reduces the risk of fragmented, informal credential handling.

Typical uses

- Use the vault as the managed home for operational credentials.
- Review entries when access-dependent workflows need validation.
- Keep records current so automation and administrative work remain reliable.



Credentials Vault workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

7.3 Logs

Purpose

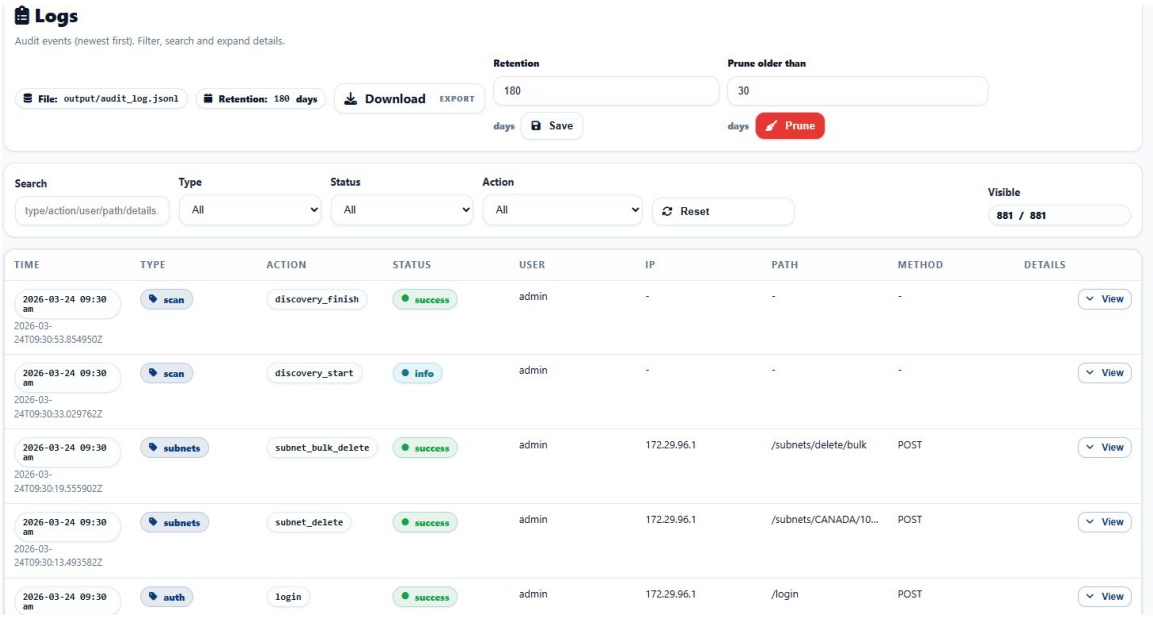
The Logs page provides direct visibility into recorded platform activity.

Administrative value

It gives administrators a practical way to review what happened, narrow the view to a relevant event, and gather context during operational review.

Typical uses

- Search logs to isolate the relevant time, event, or user.
- Open a log detail when additional context is needed.
- Use logs to support review and troubleshooting workflows.



Logs workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

8. System Configuration and Maintenance

These modules are typically used by platform owners or senior administrators responsible for maintenance, licensing, scheduling, and secure operation.

8.1 Settings

Purpose

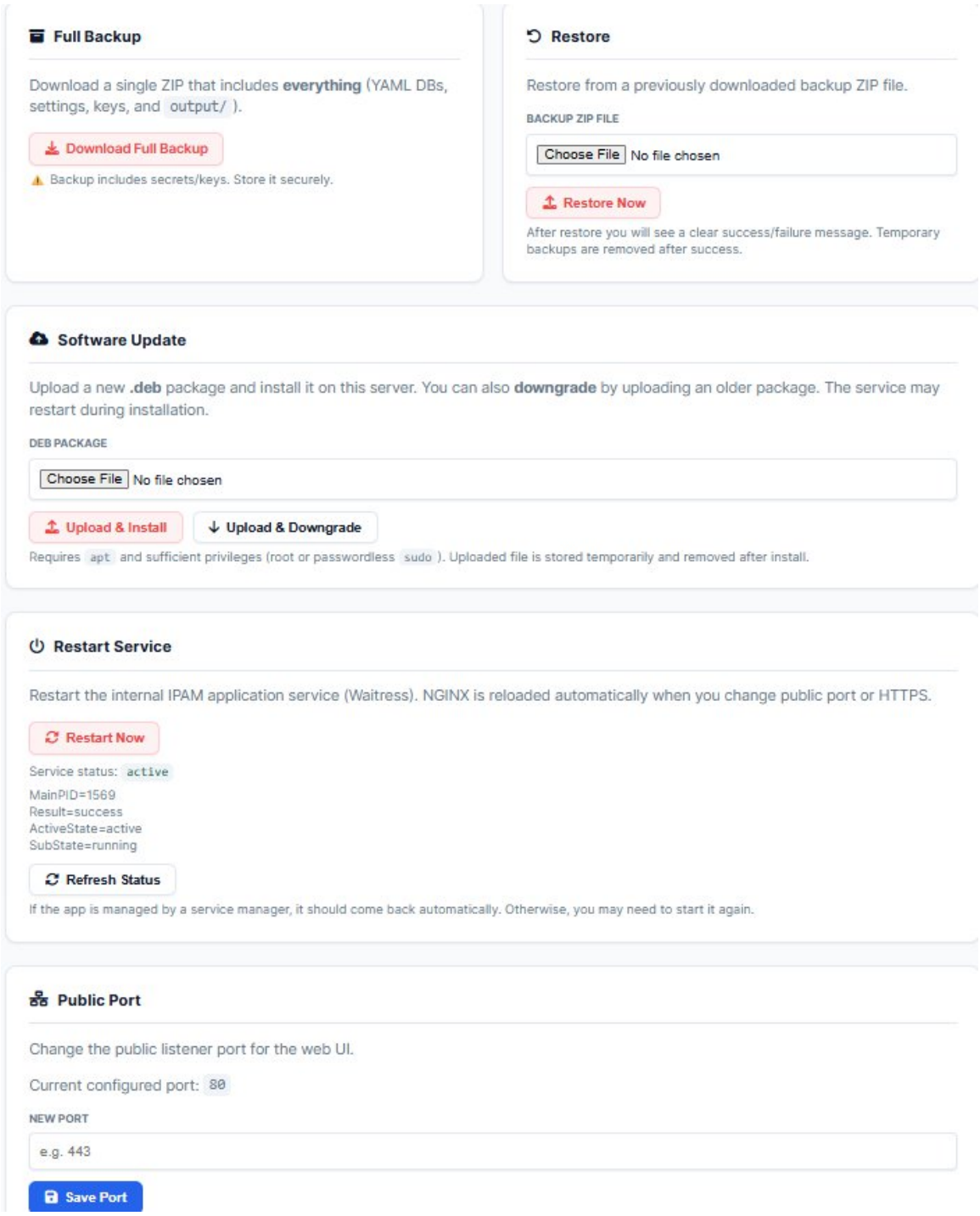
Settings is the entry point for maintenance-oriented administration and service-level review.

Administrative value

It is where administrators move when they need to assess or prepare system-level work rather than day-to-day addressing tasks.

Typical uses

- Review service state before planned maintenance.
- Use the page as the gateway into configuration and upkeep tasks.
- Reserve it for controlled administrative operations.



Settings workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

8.2 Certificates

Purpose

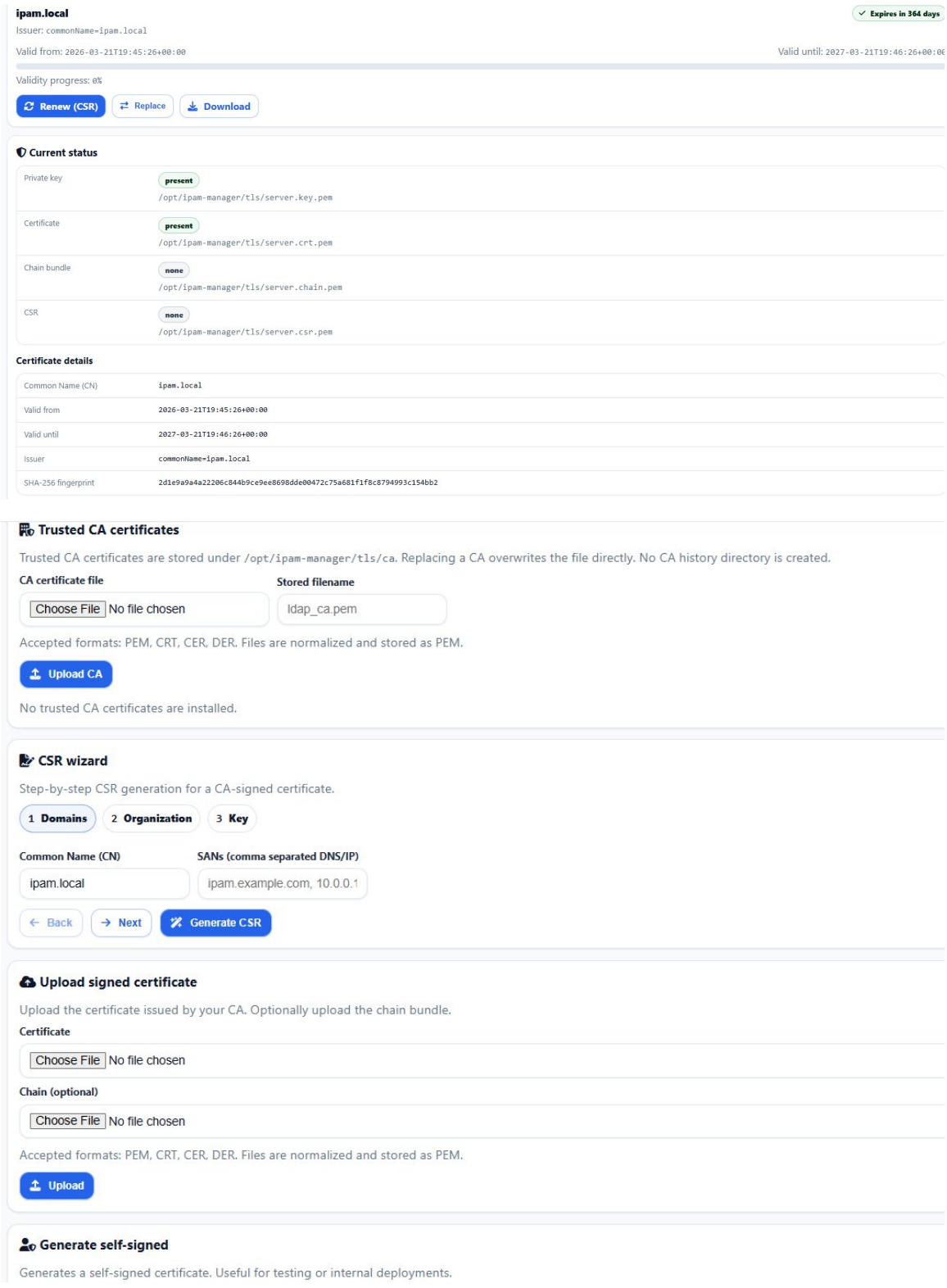
Certificates groups trust-related workflows into one dedicated operational view.

Administrative value

Certificate maintenance is easier to manage when related tasks are centralized and reviewed in a structured way rather than handled ad hoc.

Typical uses

- Use the page when reviewing certificate status or preparing maintenance.
- Work through the available certificate paths in a structured order.
- Treat certificate changes as planned administrative tasks.



Certificates workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

8.3 License

Purpose

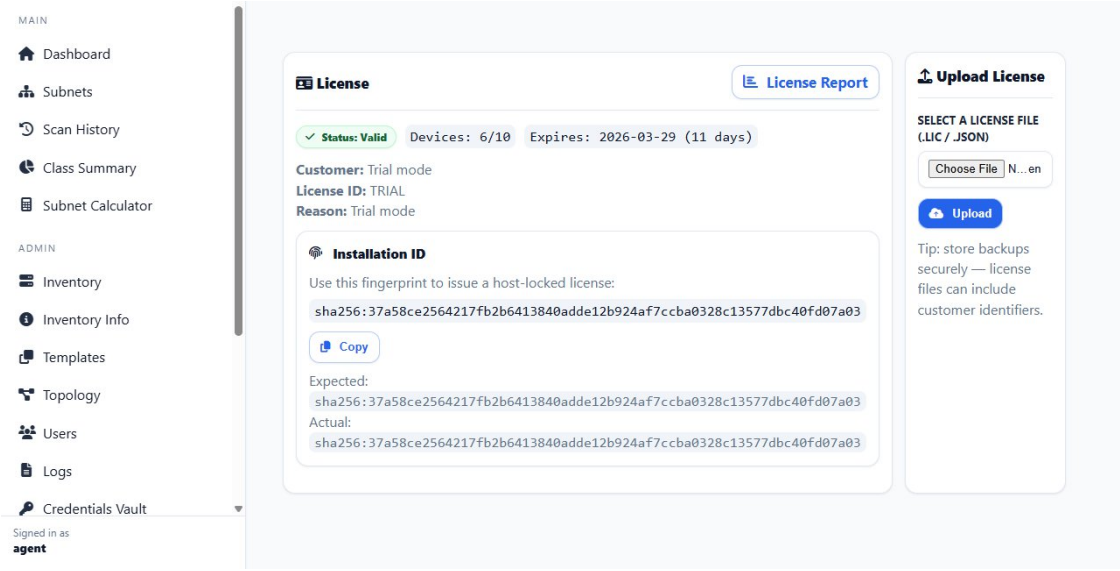
The License page exposes licensing state and support-related information needed for ongoing administration.

Administrative value

It helps keep the product supportable, auditable, and easier to manage during vendor or compliance-related interactions.

Typical uses

- Review current license state during maintenance cycles.
- Use the report and fingerprint information when support or compliance work requires it.
- Keep licensing review part of regular platform upkeep.



License workspace

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

8.4 Scans Scheduler

Purpose

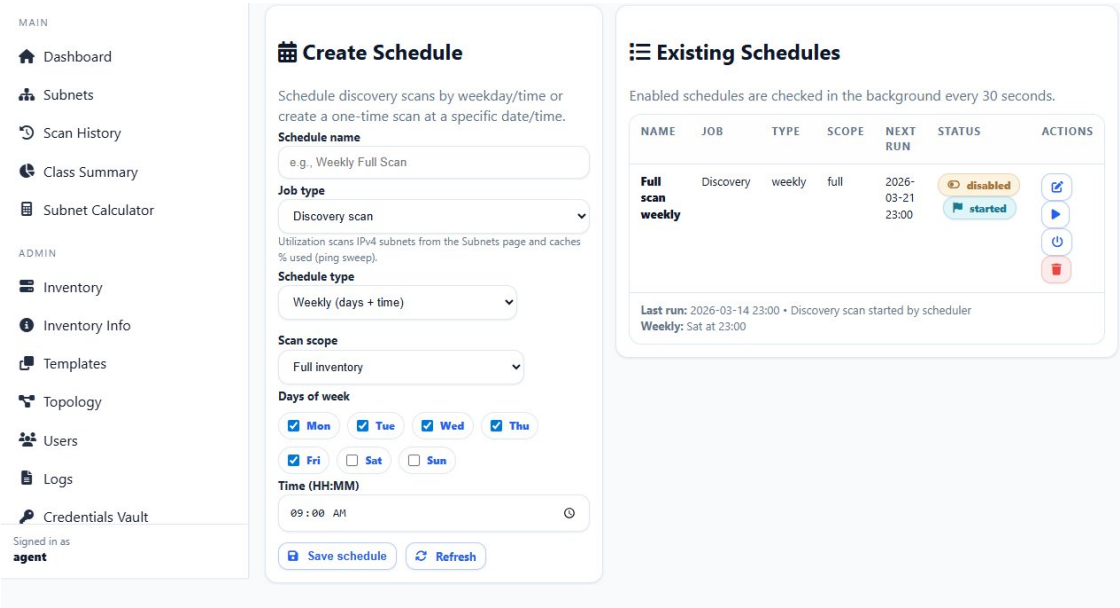
Scans Scheduler helps administrators turn discovery into a repeatable, managed process.

Administrative value

Scheduling reduces dependence on manual memory and helps maintain more consistent operational coverage across the environment.

Typical uses

- Review schedules before adding or modifying recurring discovery work.
- Open existing schedules when refinement is preferable to replacement.
- Use the scheduler to make discovery repeatable and operationally predictable.



Scans Scheduler workspace

9. Security and Access Protection

This chapter explains how the Security page helps administrators control login exposure, enforce source IP restrictions, and apply brute-force protection from one operational workspace. It is intended for administrators responsible for access governance and platform hardening.

9.1 Security

Purpose

The Security page centralizes access-related controls that influence who can reach the login flow and how repeated failed login attempts are handled. It combines preventive controls, visibility, and pre-change validation tools in one place.

Administrative value

This page helps administrators reduce unnecessary login exposure directly from the platform. Instead of relying only on external controls, administrators can define trusted source ranges, apply more restrictive rules to specific users, and tune brute-force thresholds according to operational policy.

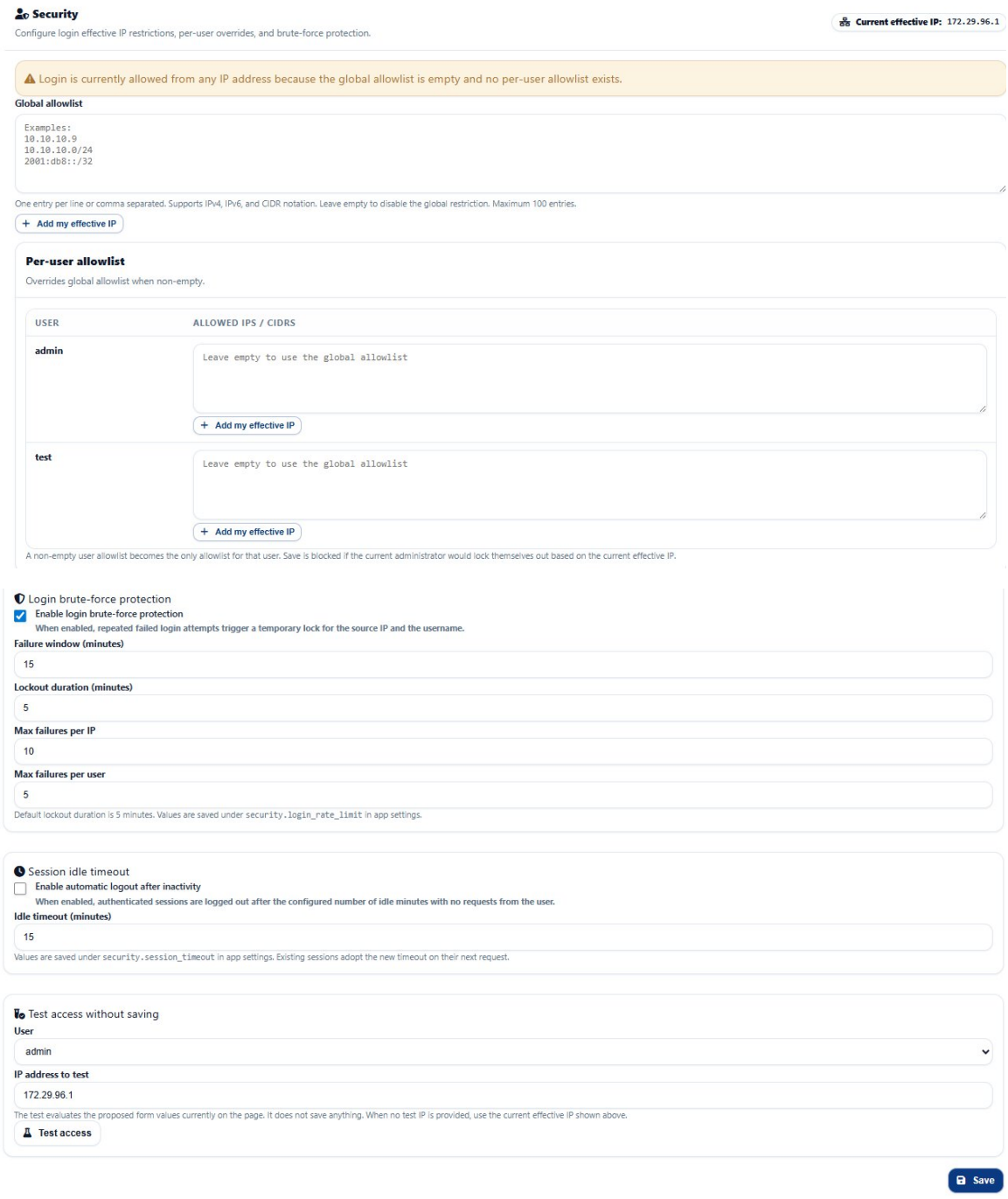
Typical uses

Restrict login to trusted addresses or network ranges by configuring a global allowlist.

Apply tighter per-user restrictions when privileged accounts should only be reachable from specific addresses.

Enable brute-force protection and tune lockout thresholds to reduce repeated failed login attempts.

Use the built-in access test to validate proposed policy changes before saving them.



Security page overview

Global and per-user allowlist controls

The upper portion of the page focuses on source IP governance. Administrators can define a global allowlist that applies platform-wide and then use per-user allowlists to apply stricter rules to selected accounts. This allows broad policy enforcement without losing flexibility for high-privilege users.

The page also displays the current effective client IP so administrators can confirm which address the platform is actually evaluating. Warning banners highlight when login remains open from any IP address because no global or per-user allowlist is currently defined.

Brute-force protection settings

The lower portion of the page controls login brute-force mitigation. Administrators can enable or disable the feature and configure the failure window, lockout duration, maximum failures per IP address, and maximum failures per username. These settings help reduce password guessing and make repeated failed login attempts less effective.

Session idle timeout

When enabled, authenticated sessions are logged out after the configured number of idle minutes with no requests from the user.

Test access without saving

A dedicated validation area allows administrators to test the proposed policy without committing the change. By selecting a user and entering an IP address to evaluate, administrators can confirm whether the current page values would allow or deny login before saving the final configuration.

Security page hardening and validation controls

Operational guidance. Use this page when access policy changes, when privileged users are onboarded, or when failed-login activity requires review. Confirm the effective client IP, review allowlist rules, test the proposed policy, and then save the final configuration.

Operational guidance. Review the current state first, then move into add, view, or configuration tasks only after confirming the target object or the exact administrative need.

Operational guidance

IPAM Manager delivers the most value when administrators use it as one operating workspace instead of a collection of disconnected screens. Address planning, discovery visibility, inventory review, configuration backup, monitoring retention, governance, and maintenance all become easier when they are handled inside one coordinated platform.

Documentation scope. This guide is intended as a customer-facing administration manual. Low-level QA evidence, validation counts, and other internal testing details should remain in separate internal materials.