



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

IPAM Manager	1
Using this guide.....	1
Contents.....	3
1. Prerequisites Before First Use.....	4
1.1 Environment and Access Readiness	4
2. Getting Started.....	5
2.1 Dashboard.....	5
3. IP Address Management.....	6
3.1 Subnets.....	6
3.2 Class Summary.....	7
3.3 Subnet Calculator.....	9
4. Discovery, History, and Topology.....	10
4.1 Scan History.....	10
4.2 Topology.....	11
5. Inventory, Templates, and Configuration Backup.....	12
5.1 Network Inventory.....	13
5.2 Inventory Info.....	13
5.3 Templates.....	14
5.4 Configuration Backup.....	15
6. Monitoring and Retention.....	16
6.1 Monitoring.....	16
7. Administration and Access Control.....	17
7.1 Users.....	17
7.2 Credentials Vault.....	18
7.3 Logs.....	19
8. System Configuration and Maintenance.....	20
8.1 Settings.....	20
8.2 Certificates.....	22
8.3 License.....	24
8.4 Scans Scheduler.....	25
9. Security and Access Protection.....	26
9.1 Security.....	26
Operational guidance.....	29

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

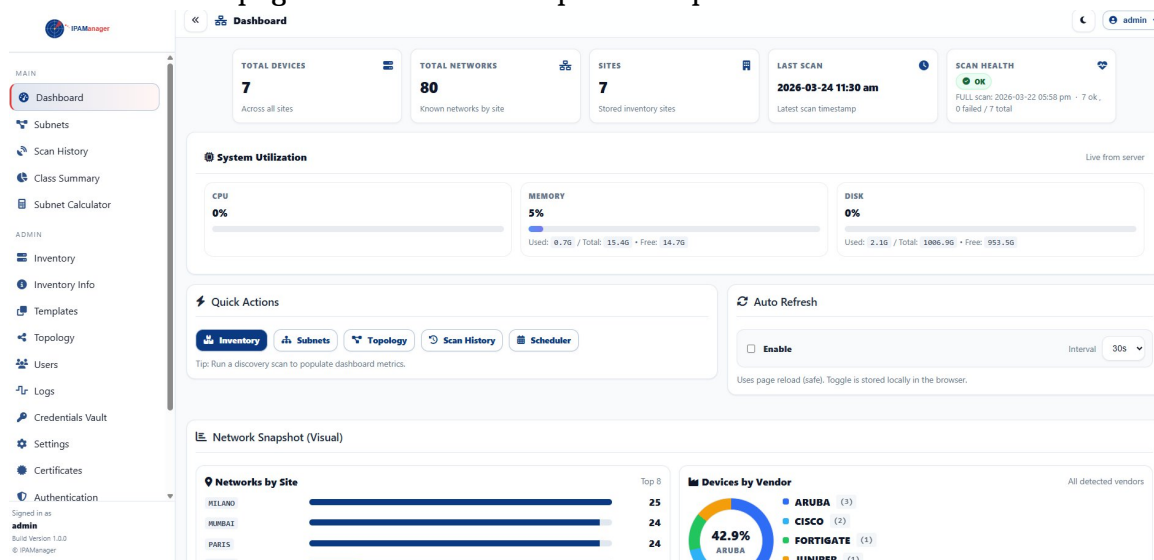
The dashboard is the operational home screen for the product. It brings the main modules together in one place and helps administrators orient themselves quickly at the start of a task or working session.

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

MANAGED

80

SQLite-backed inventory

TOTAL SUBNETS

79,497

Calculated from subnet CIDRs

LIVE

11

From cached host/utilization scans

USED IPS

243

From cached host/utilization scans

OVERLAPS

2

Pending overlapping subnet pairs

Overlapping subnets detected

MILANO
169.254.0.0/16 overlaps 169.254.0.64/26
Pending review

ACK

ACK+ACCEPT

MILANO
169.254.0.0/16 overlaps 169.254.0.64/26
Pending review

ACK

ACK+ACCEPT

Showing 2 of 2 overlaps

All Subnets (SQLite-backed inventory)

Total: 80

SEARCH Search networks (site, CIDR)

ROWS 100

PAGE Page 1 of 1

BULK ACTIONS

Scan Selected

Scan All

Edit Selected

Delete Selected

Selected: 0

Showing 1-80/80

☐	SITE	CIDR	NAME	VLAN ID	INTERFACE NAME	SOURCE DEVICE	ORIGIN	LAST SCAN	UTILIZATION	ACTIONS
☐	LONDON	172.24.125.240/29	-	240	Vlan240	Ciscosw01	learned	2026-03-24 11:30 am	-	
☐	MILANO	10.130.0.0/24	-	nan	mgmt	FortiGate01	learned	2026-03-22 05:58 pm	4%	
☐	MILANO	10.130.1.0/29	-	nan	port1	FortiGate01	learned	2026-03-22 05:58 pm	-	
☐	MILANO	10.130.1.130/32	-	nan	Mgmt_int	FortiGate01	learned	2026-03-22 05:58 pm	-	

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.

▼ **172.30.0.0/16 (1 rows)**

PREFIX	MASK	DESCRIPTION	VLAN	STATUS	COVERED BY
Filter...	Filter...	Filter...	Filter...	Filter...	Filter...
172.30.242.0/24	255.255.255.0	Vlan242	242	✓ USED	

▼ **FREE /24 (255 subnets, 2 ranges)**

Tip: Expand a range to name individual free subnets (saved to overrides).

⌵ Expand all
⌴ Collapse all

RANGE	COUNT	RESERVED	COVERAGE	
Filter...	Filter...	Filter...	Filter...	Filter...
172.30.0.0/24 → 172.30.241.0/24	242	0		95% Collapse

FREE CIDR	RESERVED FOR
172.30.0.0/24	Reserved for... Save
172.30.1.0/24	Reserved for... Save
172.30.2.0/24	Reserved for... Save
172.30.3.0/24	Reserved for... Save
172.30.4.0/24	Reserved for... Save

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

IPv4IPv6CalculateClear

Compute IPv4/IPv6 subnet details from a CIDR such as 10.1.1.0/21.
Outputs: network, broadcast, usable hosts, and optional subnet split count.

CIDR
10.1.1.0/21

SPLIT INTO PREFIX LENGTH (OPTIONAL)
24

Example: how many /24 subnets exist inside 10.1.1.0/21.

Calculated.

ResultsIPv4

FIELD	VALUE
IP version	IPv4
Normalized	10.1.0.0/21
Network address	10.1.0.0
Broadcast address	10.1.7.255
Netmask	255.255.248.0
Wildcard	0.0.7.255
Prefix length	21
Total addresses	2048
Usable addresses	2046
First usable	10.1.0.1
Last usable	10.1.7.254
Split into /24	8 subnets

Subnets (sample)First 256

#	SUBNET	RANGE
1	10.1.0.0/24	10.1.0.0 - 10.1.0.255
2	10.1.1.0/24	10.1.1.0 - 10.1.1.255
3	10.1.2.0/24	10.1.2.0 - 10.1.2.255
4	10.1.3.0/24	10.1.3.0 - 10.1.3.255
5	10.1.4.0/24	10.1.4.0 - 10.1.4.255
6	10.1.5.0/24	10.1.5.0 - 10.1.5.255
7	10.1.6.0/24	10.1.6.0 - 10.1.6.255
8	10.1.7.0/24	10.1.7.0 - 10.1.7.255

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

Review completed scan runs, open reports, inspect failures, and export or remove history records.

← Back to Dashboard

Export History ZIPEXPORT

Clear History

TOTAL SCANS

9

Visible report entries on disk.

COMPLETED

9

Runs that finished without recorded failures.

WITH WARNINGS

0

Runs completed with failed devices.

FAILED

0

Runs that ended in an error state.

Q Search

Search by mode, status, file name.

4F Sort

Newest first

Rows

All

Showing 9/9

LOCAL TIME	MODE	DEVICES	FAILED	DURATION	STATUS	REPORTS	ACTIONS
03/24/2026, 11:30:33 AM Tue • Asia/Jerusalem	★ Latest scan SELECTED Scan ID: 20260324-113033	1	0	-	Completed	ExcelEXPORTHTML	View DetailsDelete
03/23/2026, 09:32:38 PM Mon • Asia/Jerusalem	SELECTED Scan ID: 20260323-213238	1	0	-	Completed	ExcelEXPORTHTML	View DetailsDelete
03/23/2026, 08:53:38 PM Mon • Asia/Jerusalem	SELECTED Scan ID: 20260323-205338	1	0	-	Completed	ExcelEXPORTHTML	View DetailsDelete
03/22/2026, 05:58:09 PM Sun • Asia/Jerusalem	FULL Scan ID: 20260322-175809	7	0	-	Completed	ExcelEXPORTHTML	View DetailsDelete
03/22/2026, 05:55:54 PM Sun • Asia/Jerusalem	SELECTED Scan ID: 20260322-175554	1	0	-	Completed	ExcelEXPORTHTML	View DetailsDelete
03/22/2026, 05:22:41 PM Sun • Asia/Jerusalem	FULL Scan ID: 20260322-172241	7	0	-	Completed	ExcelEXPORTHTML	View DetailsDelete

Scan History workspace

Scan Details

×

Close

Scan ID 20260320-094208 • 03/20/2026, 09:42:08 AM

LOCAL TIME

03/20/2026, 09:42:08 AM

MODE

FULL

DEVICES SCANNED

6

FAILED DEVICES

5

DURATION

-

STATUS

Completed with warnings

EXCEL REPORT

ipam_20260320-094208.xlsx

HTML REPORT

ipam_20260320-094208.html

Failed Devices

DEVICE	IP	REASON
Ciscosw01	172.24.124.5	TCP connection to device failed.
AccessSW01	10.130.3.10	No SNMP response received before timeout
FortiGate01	10.130.1.130	TCP connection to device failed.
Junipersw01	10.130.1.34	TCP connection to device failed.
useragg	10.7.2.50	TCP connection to device failed.

Review the generated reports for full output.

×

Close

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.

Scan Controls

Run scans, exports and topology actions from one place.

Start Scan

Reload

Download PNG

Download SVG

STP: Off

Infra Only: Off

Layout: Hierarchical

Enable Edit Mode

Save Edits

Reset (Reload)

Run output (commands & device output preview):

```

Port path cost 10, Port priority 128, Port Identifier 128.48.
Designated root has priority 32768, address 0012.70ab.4308
Designated bridge has priority 32768, address 0012.70ab.4308
Designated port id is 128.48, designated path cost 0
Hello: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
This port is in the portfast mode
Link type is point-to-point by default
BPDU: sent 2693467, received 0
[12:28:44] CiscoSW01 (172.24.124.5) STP RMP (cisco_sw): 7 ports sample
[01/0/47,012/0/36,012/0/08,011/0/46,011/0/44]
[12:28:44] CiscoSW02 (172.24.124.5) STP annotated links: 7/7 (handle_fallbacks=0)
[12:28:44] Scan Finished. Network links?

```

Nodes: 8 Links: 7 | Layout: HIERARCHICAL | Filter: All Devices

Sites filter (optional):

Topology name (for saving): Save

Load saved topology: USPL Load Delete

Search nodes:

Vendor colors: Edge label: src if == dst if

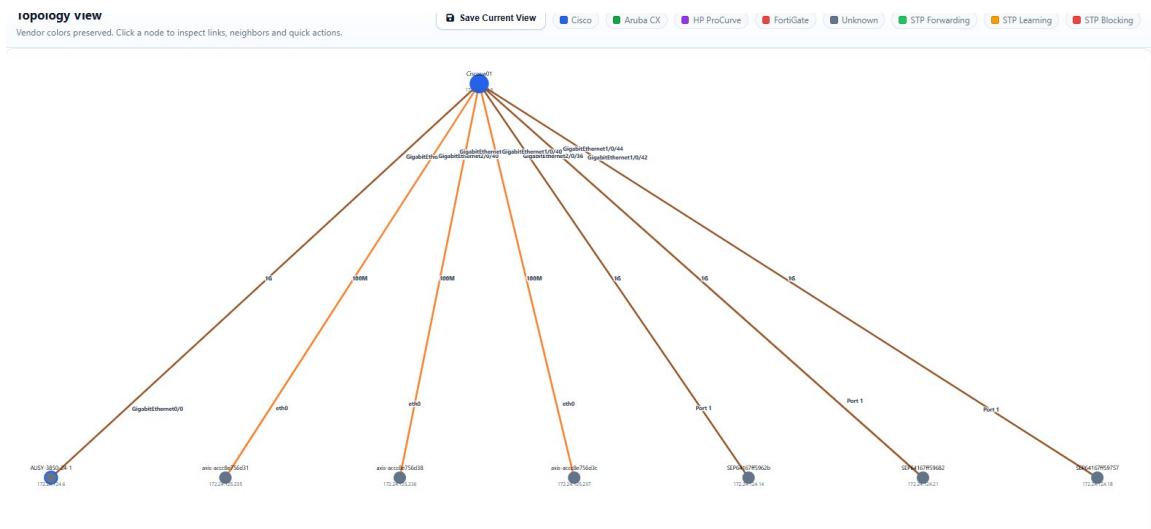
Devices to scan

Select specific devices. If none selected, the scan runs on all devices and then applies the site filter.

Search devices (Hostname / IP): Showing 6/6

SITE	HOSTNAME	IP	VENDOR
☒ CISC	CiscoSW01	172.24.124.5	Cisco IOS
☐ ACCE	AccessSW01	10.130.3.10	Cisco IOS
☐ NEW	New Jersey	172.28.1.68	Aruba
☐ FORT	FortiGate01	10.130.1.138	Fortinet
☐ JUNI	JuniperSW01	10.130.1.34	Juniper Junos
☐ USER	useragg	10.7.2.58	Aruba

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.

The screenshot displays the 'Network Inventory' workspace. At the top, there are five summary cards: 'Managed inventory objects' (7), 'CU-based discovery targets' (6), 'Polling-based discovery targets' (1), 'Fingerprint-based discovery targets' (0), and 'Credential Profiles' (3). Below these is the main 'Network Inventory' section with a search bar, filters, and a table of devices. The table has columns for Hostname, IP Address, Site, Vendor / Model, User, Port, Method, Last Scan, Status, Networks, and Actions. Two devices are listed: 'CiscoSW01' and 'AccessSW01'.

HOSTNAME	IP ADDRESS	SITE	VENDOR / MODEL	USER	PORT	METHOD	LAST SCAN	STATUS	NETWORKS	ACTIONS
CiscoSW01	172.24.124.5	LONDON	Cisco WS-C3850-48P - 16.12.05b	LDAP-user	tcp/22	ssh	2026-03-24 11:30 am	OK	4	[Edit] [Delete]
AccessSW01	10.130.3.10	PRAGUE	Cisco WS-C3750E-48PD-S - 12.2(53)SE1	LDAP-user	udp/161	snmp	2026-03-22 05:58 pm	OK	3	[Edit] [Delete]

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.

Templates workspace

Templates

New

Refresh

Class Summary

Define naming templates for a /16 "class" using a simple pattern such as 10.x.0.0/16 or 172.x.0.0/16.

Each template is a list of /24 third octets (0-255) and a name. Apply templates from Class Summary to write subnets_overrides reservations in bulk.

Templates list

Click row to edit

NAME	PATTERN	/24S
Base-Template	10.x.0.0/16	255

Editor

Duplicate

Import CSV

Export CSV

Save

Delete

Template name

Base-Template

Pattern

10.x.0.0/16

Supported: 10.x.0.0/16 and 172.x.0.0/16 (x = second octet).

+ Add /24

third octet = A.B. C .0/24

Apply from Class Summary

THIRD OCTET	NAME	
1	Unused-1	
2	P2P-Routing	
3	NAT-VPNs	
4	Destination-NAT	
5	IT-Technician	

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.

« Configuration Management admin

Configuration Management
Read-only network configuration backup, version history, change detection, retention and on-demand diff.

Inventory: 6 With backup: 5 Mode: read-only backup Retention: 100 versions

INVENTORY DEVICES
6
Admin-visible devices

DEVICES WITH BACKUP
5
Latest successful backup exists

CHANGED CONFIGS
12
Last 24 hours

FAILED BACKUPS
10
Last 24 hours

Recent Backup Jobs 18 jobs

One row per backup job. Expand a job to review per-device backup results.

	STARTED	FINISHED	STATUS	DEVICES	CHANGED	FAILED	INITIATED BY	MESSAGE
>	2026-06-01 14:17:11 Run #18	2026-06-01 14:17:11 00:00:00	Failed	1 / 1 Success 0, unchanged 0	0	1	admin	Backup finished. Pruned files: 0
>	2026-06-01 14:14:06 Run #17	2026-06-01 14:15:24 00:01:18	Partial	6 / 6 Success 5, unchanged 7	2	1	admin	Backup finished. Pruned files: 0
>	2026-06-01 13:56:16 Run #16	2026-06-01 13:57:34 00:01:18	Success	5 / 5 Success 5, unchanged 7	2	0	admin	Backup finished. Pruned files: 0
>	2026-06-01 11:25:21 Run #15	2026-06-01 11:26:40 00:01:19	Partial	6 / 6 Success 5, unchanged 1	8	1	admin	Backup finished. Pruned files: 0
>	2026-05-31 17:08:05 Run #14	2026-05-31 17:08:45 00:00:40	Stopped	1 / 2 Success 0, unchanged 0	0	1	admin	Backup stopped by user after completing the current device. Pruned files: 0
>	2026-05-31 16:56:13	2026-05-31 17:00:13	Failed	6 / 6	0	6	scheduler	Backup finished. Pruned files: 0

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.

Backup Versions - DMZFW01

6 rows

SELECT	TIME	TYPE	STATUS	CHANGED	SIZE	ACTIONS	DETAILS
☐	2026-06-01 14:14:19	full	success	Yes	445.3 KB	Download	Changed: 15 line(s) added, 15 line(s) removed
☐	2026-06-01 13:56:29	full	success	Yes	445.3 KB	Download	Changed: 15 line(s) added, 15 line(s) removed
☐	2026-06-01 11:25:35	full	success	Yes	445.3 KB	Download	Changed: 16 line(s) added, 16 line(s) removed
☐	2026-05-31 14:15:22	full	success	Yes	445.3 KB	Download	Changed: 479 line(s) added, 479 line(s) removed
☐	2026-05-31 13:42:58	full	success	Yes	445.2 KB	Download	Changed: 480 line(s) added, 480 line(s) removed
☐	2026-05-31 13:39:28	full	success	Yes	445.2 KB	Download	First backup

Diff Viewer

Compare two stored versions

Compare Selected Compare Latest Two

```

--- DMZFW01 full 2026-06-01 13:56:29
+++ DMZFW01 full 2026-06-01 14:14:19
@@ -34484,7 +34484,7 @@
 set proxy-server-ip ''
 set proxy-server-port 0
 set proxy-username ''
- set proxy-password ENC +MouBy4KfUq1HQ6AKP15vqdtRV7UzDF+/3sYLWQHTMxUuIMV9JecHwDYYxy28zj752aZnaVQEN18
+ set proxy-password ENC AL1XZDn+TcJknRvsl7IeRdWaaVMEyth1xpAPF4Ezju352vg6HL0xw082Y/Ph68NT15774gHckx
+ set dns-server-ip 8.8.8.8
 set dns-server-id6 1
 set dns-server-port 443
@@ -35618,7 +35618,7 @@
 set mac-case uppercase
 set radlin-mac-auth disable
 set encrypt AES
- set passphrase ENC 8Brya+wiJ8ITrBxmTYupQDobMEhaVB8nqU/qLgOWFKJH18gJS6xMTSXD9XPFeeR1lw0x8mDe6EwLdX18
+ set passphrase ENC 3fe2irj1t175+1ek5/eRgt9n2yREGPH1JQwEqsNn+GH21Kx6owbFAHfWdymOR/ygA3HQGV+b5MSPz3B
 set akm04-only disable
 set nro-filter-role disable
 set local-standalone disable
@@ -35764,7 +35764,7 @@
 set mac-case uppercase
 set radlin-mac-auth disable

```

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

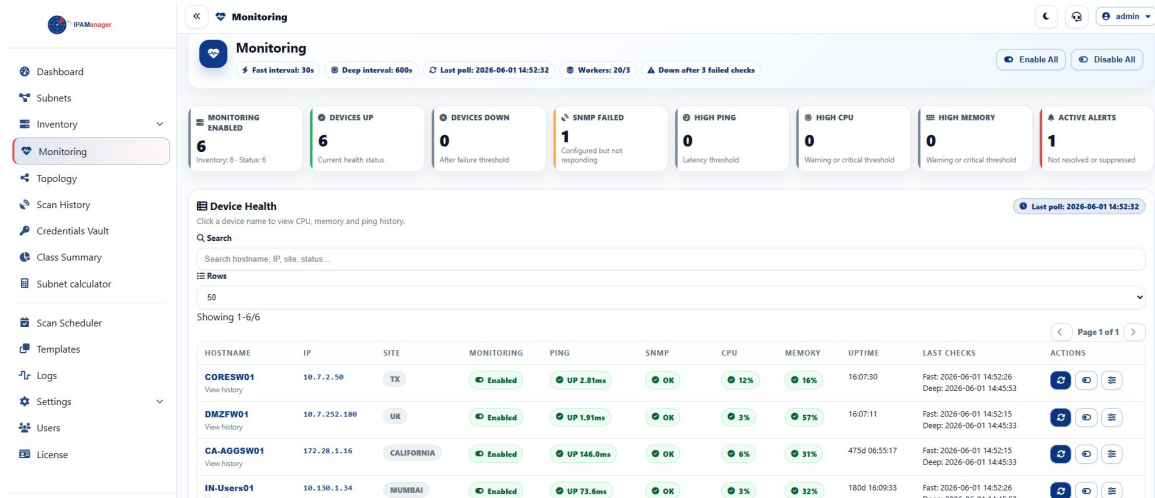
The Monitoring page provides operational visibility for monitored devices, active and resolved alerts, polling status, response health, latency, CPU usage, memory usage, and monitoring history retention.

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

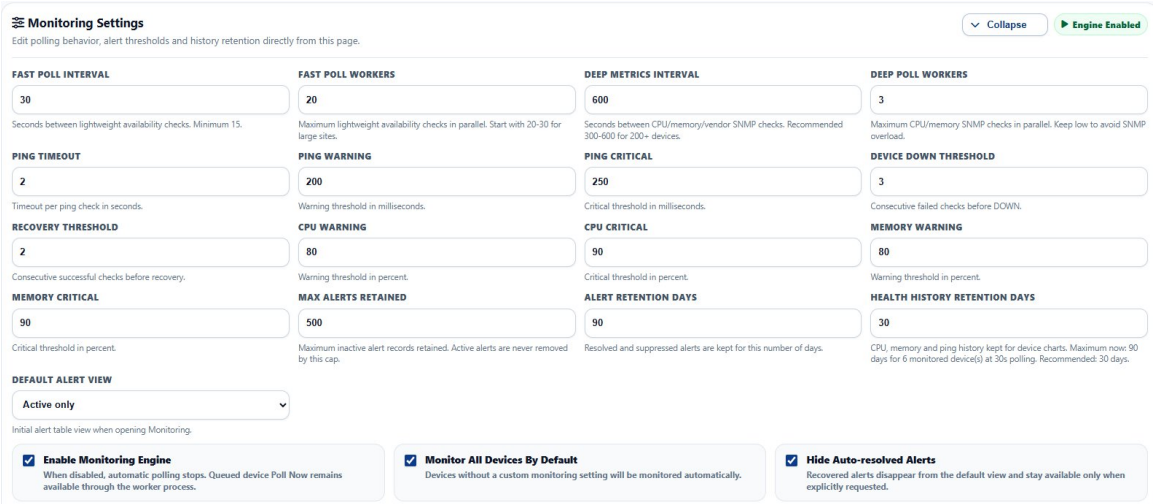
- Review monitored device status, last poll time, availability state, latency, CPU usage, and memory usage from one operational view.
- Filter active and resolved alerts to confirm current impact, recovery state, and recent operational history.
- Use device search, paging, and per-device polling actions 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 settings

Email Notification Rules

Define when Monitoring alerts should be sent by email. SMTP server settings are managed on the Settings page.

Collapse

Email Disabled

☐ **Enable Email Notifications**
 When enabled, the monitoring notification engine will be allowed to send emails for matching alert conditions.

☒ **Send on New Alerts**
 Send an email when a new matching alert is created.

☒ **Send Recovery Emails**
 Send one follow-up email when a matching alert is resolved. Recovery uses the original alert metadata when available.

RECIPIENTS OVERRIDE

COOLDOWN MINUTES

Minimum time between new/repeat emails for the same device and alert type. Recovery emails are sent once on resolution.

REPEAT ACTIVE ALERT EVERY

Minutes between reminder emails while an alert stays active. 0 disables reminders.

☐ **Include Suppressed Alerts**
Normally suppressed alerts are not sent by email. Enable only if suppression should not affect mail delivery.

Severities
☒ Critical
☐ Warning
☐ Info

Sources
☒ Ping / Availability
☒ SNMP Reachability
☒ CPU
☒ Memory
☐ Uptime / Reboot

Alert Types
☒ Device Down
☒ High Ping
☒ SNMP Failed
☒ High CPU
☒ High Memory

Email delivery uses the SMTP configuration from the Settings page. If Recipients Override is empty, the SMTP default monitoring recipients are used. Recovery emails are sent only for incidents that already generated a new alert email, so old resolved alerts will not be mailed retroactively.

Save Email Rules

Reset Email Rules

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.

User Management

Manage local and LDAP users.

TOTAL USERS

2

ADMINS

1

LOCAL

2

LDAP

0

Q

Search by username, type, role, or :

All Types

▼

All Roles

▼

All Statuses

▼

25 per page

▼

Reset Filters

#	USERNAME	USER TYPE	ROLE	STATUS	CREATED	LAST LOGIN	ACTIONS
1	admin	LOCAL	ADMIN	ACTIVE	2026-03-19 12:18 pm	2026-03-24 11:30 am	Current User Protected
2	test	LOCAL	USER	ACTIVE	2026-03-24 09:55 am	2026-03-24 11:01 am	Edit Disable Reset Password Delete

Showing 1-2 of 2 matching users

<

Page 1 of 1

>

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

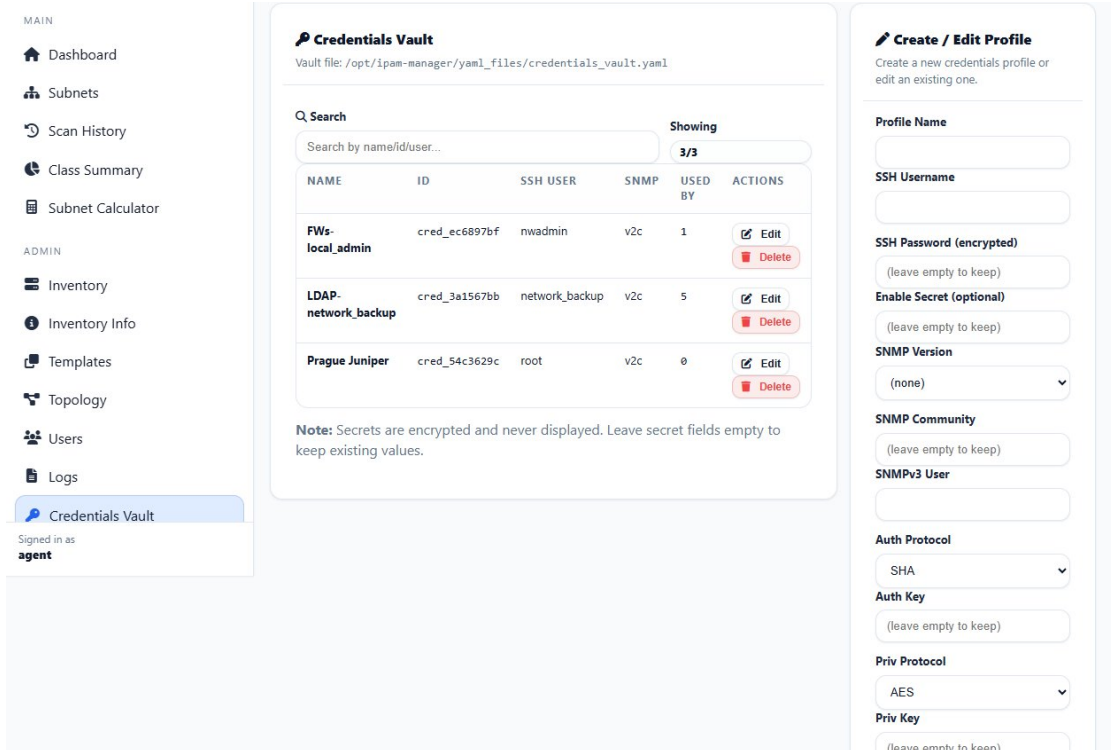
Credentials Vault centralizes the credential material the platform relies on for operational tasks.

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.

Audits

Audit events (newest first). Filter, search and expand details.

File: output/audit_log.json

Retention: 180 days

Download EXPORT

Retention

180

days

Save

Prune older than

30

days

Prune

Search

type/action/user/path/details

Type

All

Status

All

Action

All

Reset

Visible

881 / 881

TIME	TYPE	ACTION	STATUS	USER	IP	PATH	METHOD	DETAILS
2026-03-24 09:30 am 2026-03-24T09:30:53.854950Z	scan	discovery_finish	success	admin	-	-	-	View
2026-03-24 09:30 am 2026-03-24T09:30:33.029762Z	scan	discovery_start	info	admin	-	-	-	View
2026-03-24 09:30 am 2026-03-24T09:30:19.555902Z	subnets	subnet_bulk_delete	success	admin	172.29.96.1	/subnets/delete/bulk	POST	View
2026-03-24 09:30 am 2026-03-24T09:30:13.493582Z	subnets	subnet_delete	success	admin	172.29.96.1	/subnets/CANADA/10...	POST	View
2026-03-24 09:30 am 2026-03-24T09:30:13.493582Z	auth	login	success	admin	172.29.96.1	/login	POST	View

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.

Full Backup

Download a single ZIP that includes **everything** (YAML DBs, settings, keys, and `output/`).

[Download Full Backup](#)

⚠ Backup includes secrets/keys. Store it securely.

Restore

Restore from a previously downloaded backup ZIP file.

BACKUP ZIP FILE

[Choose File](#) No file chosen

[Restore Now](#)

After restore you will see a clear success/failure message. Temporary backups are removed after success.

Software Update

Upload a new `.deb` package and install it on this server. You can also **downgrade** by uploading an older package. The service may restart during installation.

DEB PACKAGE

[Choose File](#) No file chosen

[Upload & Install](#) [Upload & Downgrade](#)

Requires `apt` and sufficient privileges (root or passwordless `sudo`). Uploaded file is stored temporarily and removed after install.

Restart Service

Restart the internal IPAM application service (Waitress). NGINX is reloaded automatically when you change public port or HTTPS.

[Restart Now](#)

Service status: `active`
MainPID=1569
Result=success
ActiveState=active
SubState=running

[Refresh Status](#)

If the app is managed by a service manager, it should come back automatically. Otherwise, you may need to start it again.

Public Port

Change the public listener port for the web UI.

Current configured port: `80`

NEW PORT

e.g. 443

[Save Port](#)

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.

ipam.local

Issuer: commonName=ipam.local

Valid from: 2026-03-21T19:45:26+00:00

Validity progress: 0%

Renew (CSR)

Replace

Download

Expires in 364 days

Valid until: 2027-03-21T19:46:26+00:00

Current status	
Private key	present /opt/ipam-manager/tls/server.key.pem
Certificate	present /opt/ipam-manager/tls/server.crt.pem
Chain bundle	none /opt/ipam-manager/tls/server.chain.pem
CSR	none /opt/ipam-manager/tls/server.csr.pem

Certificate details	
Common Name (CN)	ipam.local
Valid from	2026-03-21T19:45:26+00:00
Valid until	2027-03-21T19:46:26+00:00
Issuer	commonName=ipam.local
SHA-256 fingerprint	2d1e9a9a4a22206c844b9ce9ee8698dde00472c75a681f1f8c8794993c154bb2

Trusted CA certificates

Trusted CA certificates are stored under /opt/ipam-manager/tls/ca. Replacing a CA overwrites the file directly. No CA history directory is created.

CA certificate file

Stored filename

Choose File

No file chosen

ldap_ca.pem

Accepted formats: PEM, CRT, CER, DER. Files are normalized and stored as PEM.

Upload CA

No trusted CA certificates are installed.

CSR wizard

Step-by-step CSR generation for a CA-signed certificate.

1 Domains

2 Organization

3 Key

Common Name (CN)

SANs (comma separated DNS/IP)

ipam.local

ipam.example.com, 10.0.0.1

Back

Next

Generate CSR

Upload signed certificate

Upload the certificate issued by your CA. Optionally upload the chain bundle.

Certificate

Chain (optional)

Choose File

No file chosen

Choose File

No file chosen

Accepted formats: PEM, CRT, CER, DER. Files are normalized and stored as PEM.

Upload

Generate self-signed

Generates a self-signed certificate. Useful for testing or internal deployments.

Certificates workspace

Page 24 of 30

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

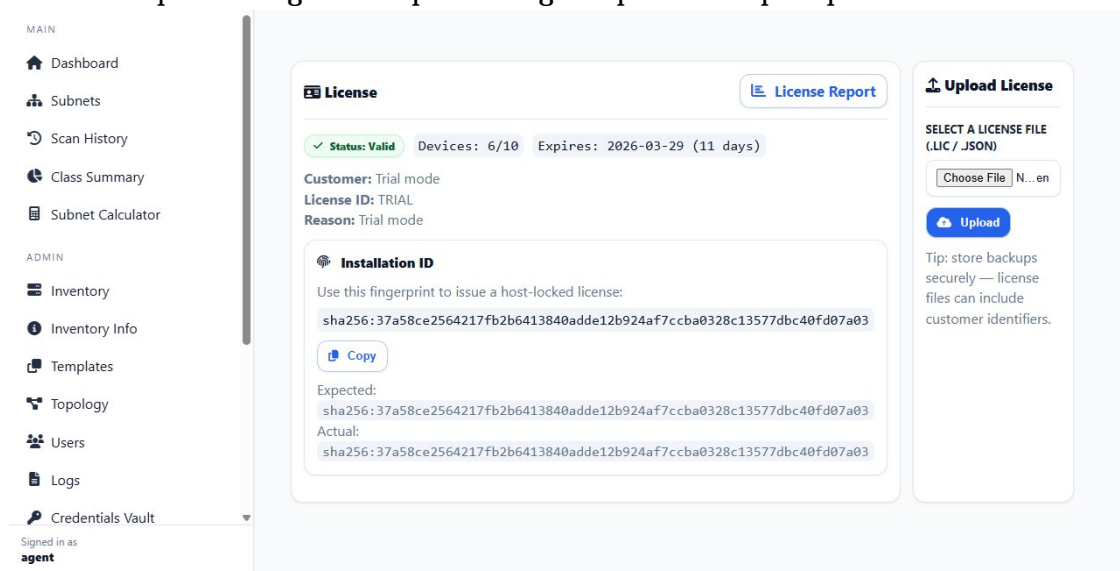
The License page exposes licensing state and support-related information needed for ongoing administration.

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.

MAIN

Dashboard

Subnets

Scan History

Class Summary

Subnet Calculator

ADMIN

Inventory

Inventory Info

Templates

Topology

Users

Logs

Credentials Vault

Signed in as
agent

Create Schedule

Schedule discovery scans by weekday/time or create a one-time scan at a specific date/time.

Schedule name

e.g., Weekly Full Scan

Job type

Discovery scan

Utilization scans IPv4 subnets from the Subnets page and caches % used (ping sweep).

Schedule type

Weekly (days + time)

Scan scope

Full inventory

Days of week

☒ Mon

☒ Tue

☒ Wed

☒ Thu

☒ Fri

☐ Sat

☐ Sun

Time (HH:MM)

09:00 AM

Save schedule

Refresh

Existing Schedules

Enabled schedules are checked in the background every 30 seconds.

NAME	JOB	TYPE	SCOPE	NEXT RUN	STATUS	ACTIONS
Full scan weekly	Discovery	weekly	full	2026-03-21 23:00	disabled started	

Last run: 2026-03-14 23:00 • Discovery scan started by scheduler
Weekly: Sat at 23:00

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

Configure login effective IP restrictions, per-user overrides, and brute-force protection.

Current effective IP: 172.29.96.1

⚠ Login is currently allowed from any IP address because the global allowlist is empty and no per-user allowlist exists.

Global allowlist

Examples:
10.10.10.9
10.10.10.0/24
2001:db8::/32

One entry per line or comma separated. Supports IPv4, IPv6, and CIDR notation. Leave empty to disable the global restriction. Maximum 100 entries.

+ Add my effective IP

Per-user allowlist

Overrides global allowlist when non-empty.

USER	ALLOWED IPS / CIDRS
admin	Leave empty to use the global allowlist + Add my effective IP
test	Leave empty to use the global allowlist + Add my effective IP

A non-empty user allowlist becomes the only allowlist for that user. Save is blocked if the current administrator would lock themselves out based on the current effective IP.

Login brute-force protection

☒ Enable login brute-force protection

When enabled, repeated failed login attempts trigger a temporary lock for the source IP and the username.

Failure window (minutes)

15

Lockout duration (minutes)

5

Max failures per IP

10

Max failures per user

5

Default lockout duration is 5 minutes. Values are saved under security.login_rate_limit in app settings.

Session idle timeout

☐ Enable automatic logout after inactivity

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

Idle timeout (minutes)

15

Values are saved under security.session_timeout in app settings. Existing sessions adopt the new timeout on their next request.

Test access without saving

User

admin

IP address to test

172.29.96.1

The test evaluates the proposed form values currently on the page. It does not save anything. When no test IP is provided, use the current effective IP shown above.

Test access

Save

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.

The screenshot displays a web interface for configuring security settings. It is divided into two main sections. The top section, titled 'Login brute-force protection', contains a checkbox for 'Enable login brute-force protection'. Below this, a note states: 'When enabled, repeated failed login attempts trigger a temporary lock for the source IP and the username.' There are four input fields: 'Failure window (minutes)' with a value of 15, 'Lockout duration (minutes)' with a value of 5, 'Max failures per IP' with a value of 10, and 'Max failures per user' with a value of 5. A small note at the bottom of this section reads: 'Default lockout duration is 5 minutes. Values are saved under security.login_rate_limit in app settings.' The bottom section, titled 'Test access without saving', features a 'User' dropdown menu currently set to 'admin', and an 'IP address to test' input field containing '172.29.96.1'. A note below these fields states: 'The test evaluates the proposed form values currently on the page. It does not save anything. When no test IP is provided, use the current effective IP shown above.' There is a 'Test access' button with a warning icon. At the bottom right of the entire form area is a blue 'Save' button with a save icon.

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.