



NxSAM Administration — Quick Guide

Quick reference guide for the Administration module

Product release	**NxSAM 2026.09**
Verified against code on	**2026-09-10**
Document revision	**b441b08-dirty**
Audience	**End users**
Document owner	**eSec Forte Technologies — Product Documentation**

Screenshots are taken from a demonstration data set. Figures are illustrative.

eSec Forte Technologies

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Table of Contents

Administration

- Overview
- Design a scheduled email report
- Tuning how findings are classified
- Administration: every screen, column and action
- Administration: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Administration

Administration

Administration covers who can use NxSAM, what they can see, and how the platform behaves. Most of it is set up once and revisited rarely — but the settings here shape what everyone else experiences, so changes deserve care.

Users, roles and groups

Three separate ideas that are easy to conflate:

	Controls
Role	What a person can *do* — which modules and actions are available
Ownership	What a person can *see* — which assets and findings
User group	A convenient way to assign the above to several people at once

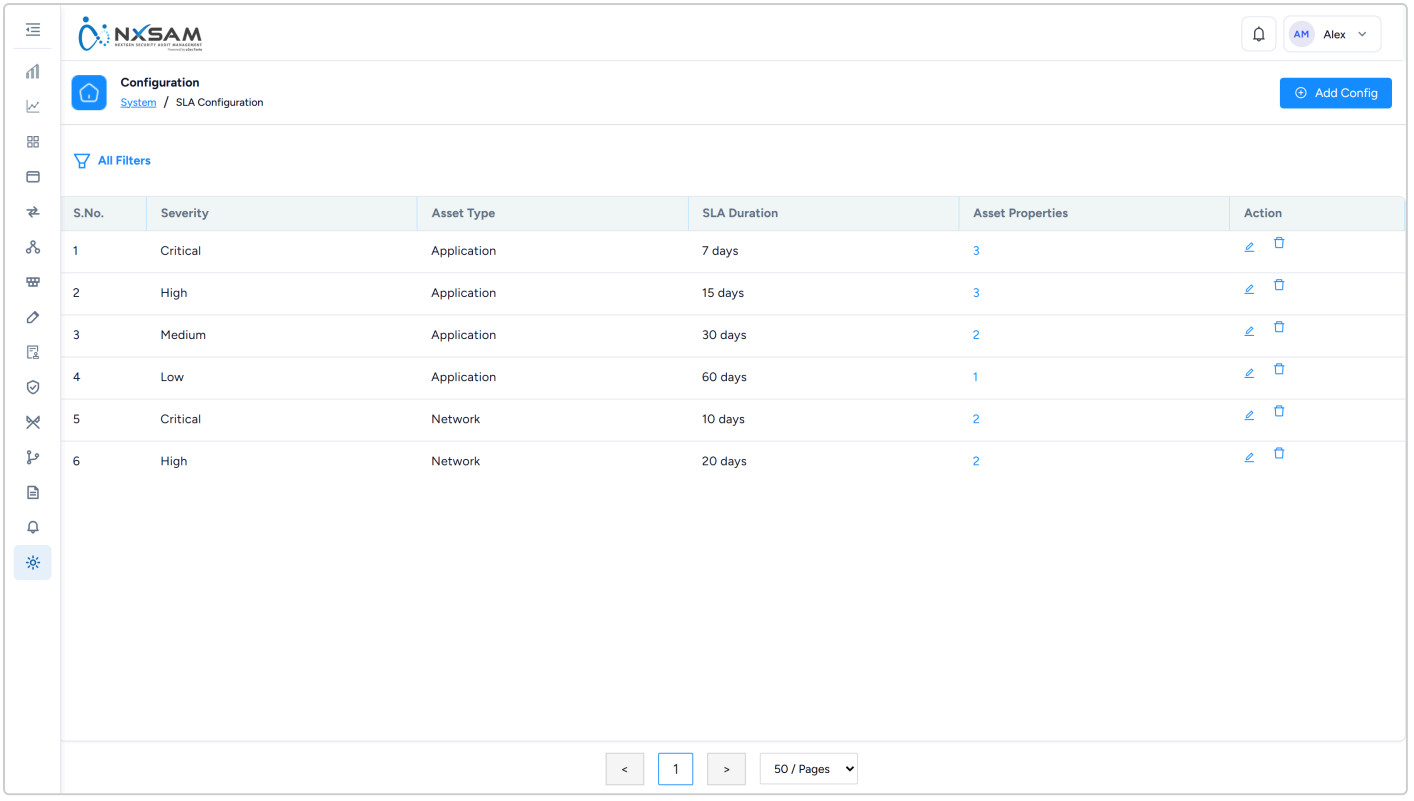
Role and visibility are different mechanisms

Giving someone the Security Analyst role does not automatically show them every asset, and granting asset ownership does not give them new abilities.

"I can't see the module" is a role problem. "I can see the module but it's empty" is an ownership problem. They have different fixes.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

SLA configuration



SLA configuration. Each row sets how long a severity has on a given asset type before it is overdue.

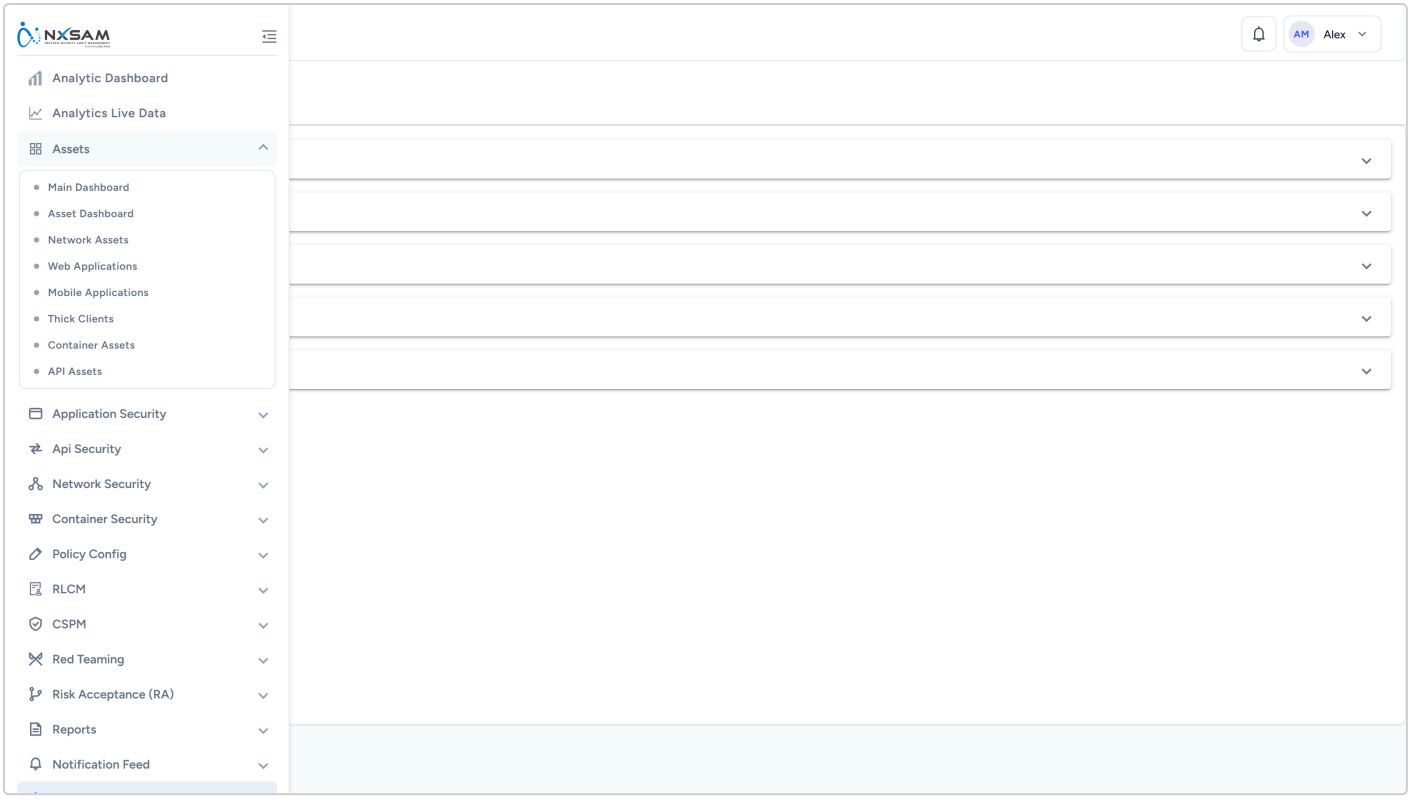
SLA settings define how long each severity has before it is overdue. This is the single most consequential setting in the platform: it determines what counts as late for every finding.

Two things to know before changing it:

- **It applies going forward.** Findings already carrying an SLA date keep it.
- **Shortening an SLA can make many findings overdue at once**, because the comparison is against today's date. Expect the overdue count to move immediately.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Severity colours



Severity colours apply across every screen, report and email.

Severity colours are configurable and are used consistently across screens, reports and emails. Changing them changes every visual output, including reports already familiar to recipients — worth a note to users if you do.

Email configuration and templates

Email configuration is the connection to your mail server. Templates control what notifications actually say.

The email log is the first place to look when someone reports not receiving a notification: it distinguishes "never sent" from "sent but not delivered", which are very different problems.

Directory integration

Where corporate sign-on is configured, users authenticate against your directory and NxSAM does not hold their passwords. Roles and ownership are still managed in NxSAM — the directory answers *who they are*, not *what they may do*.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Audit management

Audit types and properties define the kinds of assessment your organisation runs and what metadata each captures. Adding a property makes it available on future audits; existing audits will not have a value for it.

A note on changing settings

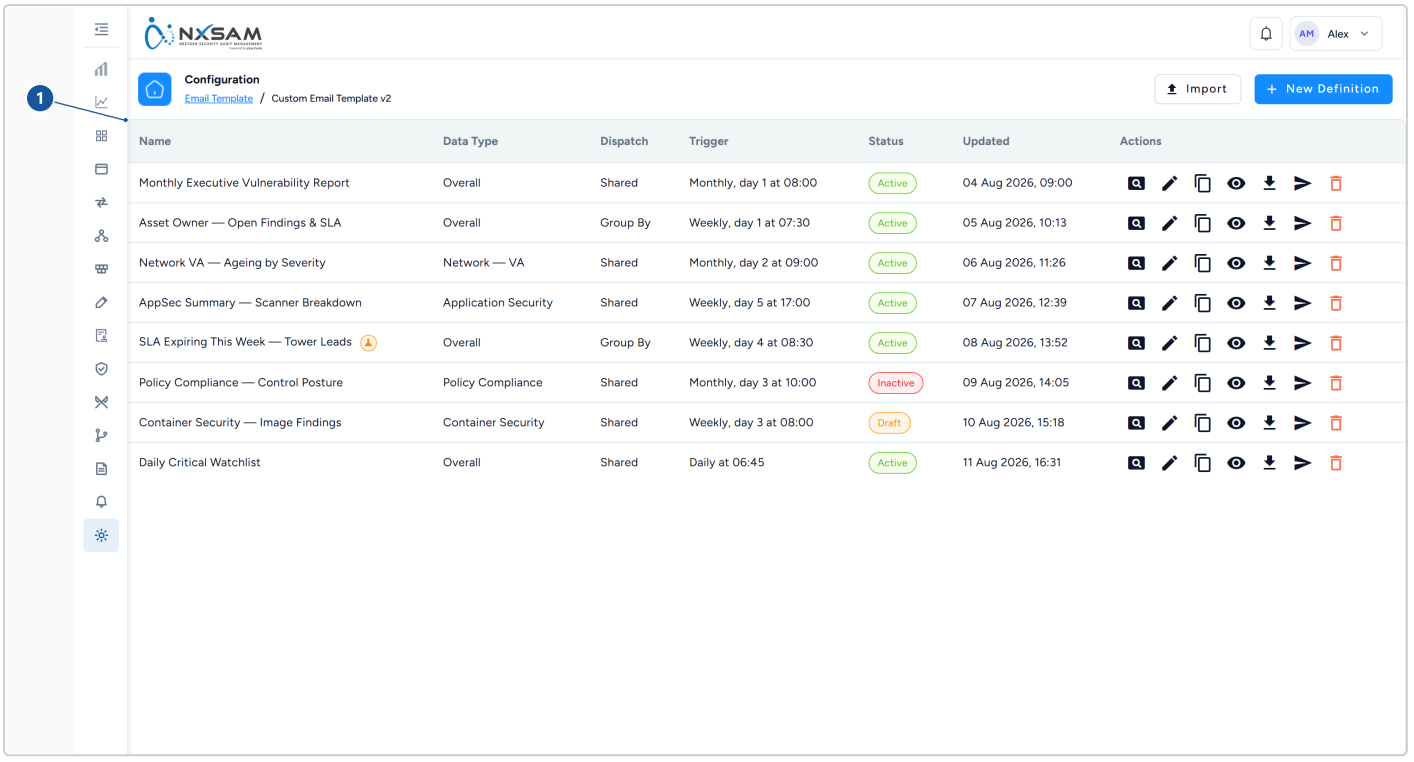
Most settings here apply to what happens next, not to what has already happened. Changing an SLA does not re-date existing findings; changing an approval matrix does not re-route requests already raised. When a change appears not to have taken effect, check whether the records in question predate it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Design a scheduled email report

Configuration → Email Template → Custom Email Template v2 lets you assemble a recurring security email — its figures, its tables, its charts, its spreadsheet attachment, its recipients and its schedule — without anyone writing a template for you. One definition can also fan out into many emails, one per owner, each carrying only that owner's findings.

This is the deepest configuration surface in the platform, so it is worth reading before you build rather than after.



Configuration → Email Template → Custom Email Template v2

1. Dispatch mode, send cadence and status

The list, and what you can do from it

Each definition shows its **Name**, **Data Type**, **Dispatch**, **Trigger**, **Status** and when it was last **Updated**. A template running in test mode is flagged on its name.

New Definition starts an empty one; **Import** loads a definition exported elsewhere.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Action	What it does
View	Opens every tab read-only. A banner says so, and Preview still works
Edit	Opens the same screen for changes
Clone	Copies the whole definition. The usual way to start — begin from something that already works
Preview email	Renders the email against live data, without sending
Export	Downloads the definition as a file
Import	Loads a definition exported from another instance
Send Now	Sends immediately, off-schedule
Delete	Removes it

Each is separately permissioned, so a colleague can be allowed to preview and send without being allowed to edit or delete.

Status is `Draft`, `Active` or `Inactive`. Only Active definitions are picked up by the schedule — a finished template left on Draft is the usual reason a report never arrives.

Import and Export are how a report travels between environments

Build and prove a definition on a test instance, export it, import it into production. The file carries the whole definition, including any advanced settings the screen does not display.

Before you start: two decisions that shape everything else

One email, or one per owner?

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Dispatch mode is the first choice and the one hardest to change later.

- **Shared** — a single email to a fixed audience. An executive summary, a weekly digest.
- **Group by** — one email per distinct value of a chosen field, each containing only that group's findings. Choose the field in **Group By Field**: any standard dimension, or any asset property you have defined. Pick the property that carries ownership, and each owner receives their own report with nobody else's findings in it.

Group-by is what turns one definition into a hundred personalised emails. It also changes what the recipient options mean, which is covered under Recipients.

Which findings are in scope?

Data Type groups the template in the list; **Client scope** restricts every data source to the chosen clients. Both are set on the first tab.

Tab 1 — Scope & Data

The name, subject and scope, and then the data sources — the figures everything else draws from.

The subject line

Type it freely and use **Insert variable** for values resolved at send time:

Variable	Resolves to
Group value	The group this email is for — the owner's name, on a group-by template
Client name	The client the report belongs to
Today's date	The date the email is generated
Month & year	For example *June 2026* — the natural choice for a monthly report title
Month	The month name alone

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

A subject of *Monthly Vulnerability Report — Group value — Month & year* produces *Monthly Vulnerability Report — Payments Platform — June 2026* for one recipient and the same line with their own group for the next.

Data sources

A data source is one query. Every table, chart and card in the email names a source, so build these first. Give each a short **Key** — you will pick it by that name later.

Each source has three parts: where it reads from, how it shapes the result, and what it excludes.

Source is the population: **Open Issues**, **VA Closed** or **PC Closed**.

Mode decides the shape, and which fields appear below it:

Mode	Shape	Feeds
Aggregate	One metric, grouped by one dimension	Summary tables, summary cards, bar charts, chart images
Metrics	Several metrics as columns, grouped by one dimension	Metrics tables
Matrix	One metric across two dimensions, optionally grouped by a third	Matrix tables, grouped matrix tables, charts
Nested	Parent group → member rows → value columns	Nested tables
List	Raw finding rows with the columns you choose	Data tables, and the attachment
Trend	A metric over months	Line charts

Metrics available to aggregate, metrics and matrix modes:

Metric	Notes
Issue Count	The default

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Metric	Notes
Affected Assets	Distinct assets rather than findings
Avg Vuln Score, **Total Vuln Score**	Weighted views
Overdue Count, **Overdue %**	Past the SLA date
No-SLA Count	Findings with no SLA date at all
Within-SLA Count	Still inside the SLA
Exception Count, **No-Exception Count**	Risk-accepted and not
SLA Breached (exclusive), **Within SLA (exclusive)**, **Exception (exclusive)**, **Exception Under Approval (exclusive)**	Mutually exclusive states — see the note below
MTTR (Days)	Mean time to remediate. Closed sources only

The 'exclusive' metrics exist so a table can total correctly

The plain metrics overlap: a risk-accepted finding can also be past its SLA date, so it appears under both Exception Count and Overdue Count, and a table built from them sums to more than the real total. The exclusive family assigns each finding to exactly one state, so the columns add up. Use the exclusive set whenever a table shows a total; use the plain set when you want each question answered on its own.

Dimensions are the fields to group by: Severity, Module, Asset Type, Vuln Status, Age Band, Age (Days), Age Since Overdue (Days), SLA Status, SLA Status (exclusive), SLA, Tool, Audit Category, Application, Application Name (Linked), App Sub Type (Linked), Assessment Group and Module Bucket — plus every asset property you have defined.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Every source carries its own filters, and they are the difference between a report that answers a question and one that dumps everything:

- **Severities** and **Modules** — restrict the population
- **Tool** — restrict to particular scanners
- **Dimension Filters** — any dimension or asset property, **Include** or **Exclude**, with real values offered from your data rather than typed from memory. This is how a source becomes "servers only" or "everything except the sandbox environment"
- **Sort** — high to low, or low to high
- **Row limit** — list mode only

SLA window appears on Open sources and restricts by SLA date: *already overdue*, *expiring today*, or *expiring soon*, where you set how many days ahead counts as soon. Those three windows are exactly the classic SLA-warning emails, now built rather than coded.

Age buckets appear whenever the source groups by age. Enter ascending day counts — `30, 90, 180, 365` produces 0–30, 31–90, 91–180, 181–365 and 365+. Leave it blank for the standard bands. Matrix sources can also render those labels compactly, which matters when a table has five age columns and a narrow email body.

Tab 2 — Body

The email body is an ordered list of blocks. **Add Block**, choose a type, set its width, and move it with the arrows in its header. Widths run from full to two-thirds, half, a third and a quarter, so two half-width blocks sit side by side.

A block reads from a data source, and **the source list only offers sources it can actually render** — a matrix table will not offer you a list source. If a block's source dropdown is empty, the data source it needs has not been built yet.

Block	Reads from	What it produces
Text	—	Free rich text, with the same variables as the subject plus a running total per data source
Summary cards	Aggregate	The headline figures as cards

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Block	Reads from	What it produces
Summary table	Aggregate	The simple one-dimension table
Metrics table	Metrics	A dimension down the side, several metrics across
Matrix table	Matrix	Two dimensions crossed, with totals
Grouped matrix table	Matrix with a group dimension	Three dimensions: an outer status grouping, ageing rows and severity columns
Nested table	Nested	Parent rows with member sub-rows
Data table	List	Actual findings, with the columns and headings you choose
Bar chart	Aggregate or matrix	Bars drawn in the email itself — crisp at any zoom, and visible even where images are blocked
Chart image	Aggregate, matrix or trend	A rendered chart: column, grouped, line, pie or donut
Section repeat	Aggregate or metrics	Repeats a set of blocks once per value of a field
Link	—	A labelled link

Controls worth knowing

Every table lets you rename its headings. First column label, total label, and on data and metrics tables a custom heading per column. An email that says *Application* where your organisation says *Service* is one field away from matching how people speak.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Row and column order are yours: type the values in the order you want them, comma separated. Severity columns in *Critical, High, Medium, Low, Info* rather than alphabetical is a comma-separated list, not a support request.

Zero handling — show zero values or leave the cell blank, and hide rows that are all-zero. A monthly report whose table is nine-tenths empty usually needs one toggle.

Conditional formatting on metrics and nested tables colours a cell when it crosses a threshold — *Overdue % at or above 50 → red*. Choose the metric, the comparison (including *between*), the value and the colour. This is what makes a table scannable rather than merely accurate.

Box height appears on charts and data tables. Set the same value on two side-by-side blocks and their boxes align, which is the difference between a tidy email and a ragged one.

Chart options vary by type: value labels and legend on all of them; curve and point markers and a zero-based axis on lines; stacking on grouped columns; count, percentage or one-decimal formatting on pie and donut; sort order and a top-N cut on bars; and a series order you can type when the default order is not the one you mean.

> **Data tables are a preview, not the full list**
>
> A data table's **Max Rows** caps it at the most severe findings — up to a hundred. The complete list belongs in the attachment. An email carrying thousands of rows inline is one many mail clients will truncate or refuse.

Tab 3 — Attachment

Turn the attachment on and choose **XLSX** or **CSV**. Then choose a mode:

- **Flat** — one row per finding. Pick the columns and give each its own heading.
- **Grouped** — grouped by a dimension or column, with a severity count per group. Choose which severities become columns.
- **Grouped multi** — a parent and a member dimension, with severity columns, split across **sheets** you define. Each sheet bundles a set of tools onto its own tab — one for SAST, one for DAST, one for dependency findings.

The attachment reads a **list** source, and the columns available include the full finding detail — title, asset, host, port, protocol, CVE, scanner and its identifier, status, first reported, SLA expiry, risk acceptance and its comment, audit, project, client, app code, public-facing flag, duration, plus description, synopsis, diagnosis, impact and solution, and every asset property you have defined.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

⚠ The builder warns when the attachment cannot reconcile with the email

If the attachment's source is filtered differently from the sources feeding the body — a different tool or module set — a warning appears on this tab. Ignore it and you will ship an email whose table says one number and whose spreadsheet says another, which costs more trust than the report earns. Align the filters.

Tab 4 — Recipients & Dispatch

Recipients are **resolved at send time** rather than listed, which is what keeps a group-by report correct as ownership changes.

Resolver	Resolves to
Asset owner	The owner named on the asset. Choose which property carries ownership
Group owner	The group's owner — a tower lead, for instance
Asset access	Everyone with access to this group's assets. Super-admins are excluded unless you switch them in
Static emails	Addresses you type, comma or newline separated

Build **To** and **CC** independently, and mix resolvers freely — the owner in To, a static distribution list in CC.

Test mode

Test mode redirects every email to addresses you name. Each message is still generated with its **real per-group data** and its **real resolved recipients**, shown in a banner at the top, but delivery goes only to the test addresses.

This is how you validate a group-by report that would otherwise reach a hundred people: turn it on, send, read what each owner would have received, then turn it off.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Test mode with no recipients sends nothing

That is deliberate. A blank list fails safe rather than falling back to the real audience.

Tab 5 — Schedule and branding

Frequency is daily, weekly or monthly. Weekly and monthly ask for a day; all three ask for a time. A monthly report set for day 31 will not fire in a short month — pick 28 or earlier for a report that must arrive every month.

Branding & style applies to the whole email:

- **Brand name** in the header
- **Theme preset** — eSec Maroon, Corporate Navy, Slate Professional, Teal & Amber, Indigo & Rose, or Graphite for printing and colourblind readers. A preset fills every colour below in one click and you can then adjust any of them
- **Frame colours** — primary, primary dark, panel header and border
- **Chart series colours** — the first three series
- **Shell width** in pixels, between 480 and 1200

Severity colours stay fixed. Red for the most severe is a convention people read without thinking, and re-colouring it costs more comprehension than any palette gains.

Preview before you save, and again before you activate

Preview renders the email against live data at any point, including on a draft you have not saved. On a group-by template it renders one group, so you see a real recipient's email rather than an abstraction.

The sequence that avoids embarrassment:

1. Build it and **Preview** until the figures look right.
2. Turn on **Test mode**, set it Active, and **Send Now**. Read the real thing.
3. Check the attachment reconciles with the body.
4. Turn test mode off and leave it Active on its schedule.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

A template can carry settings this screen does not show

If a definition was authored elsewhere and uses options beyond the builder, a banner lists them by name. Those settings are **preserved** when you save — the screen will not quietly drop them — but changing them means exporting the definition, editing the file and importing it back.

When a report does not arrive

In order of likelihood:

1. **Status is Draft or Inactive.** Only Active definitions are scheduled.
2. **Test mode is still on**, so it went to the test addresses. The list flags this on the template's name.
3. **The schedule has not come round yet** — a daily template sends at its time, not when you finish editing. Use **Send Now** to confirm the template works.
4. **No recipient resolved.** A group with no owner set produces no address. Preview shows the resolved recipients per group.
5. **The email was sent but not delivered** — check the email log, which records what was queued, to whom, and whether it failed.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Tuning how findings are classified

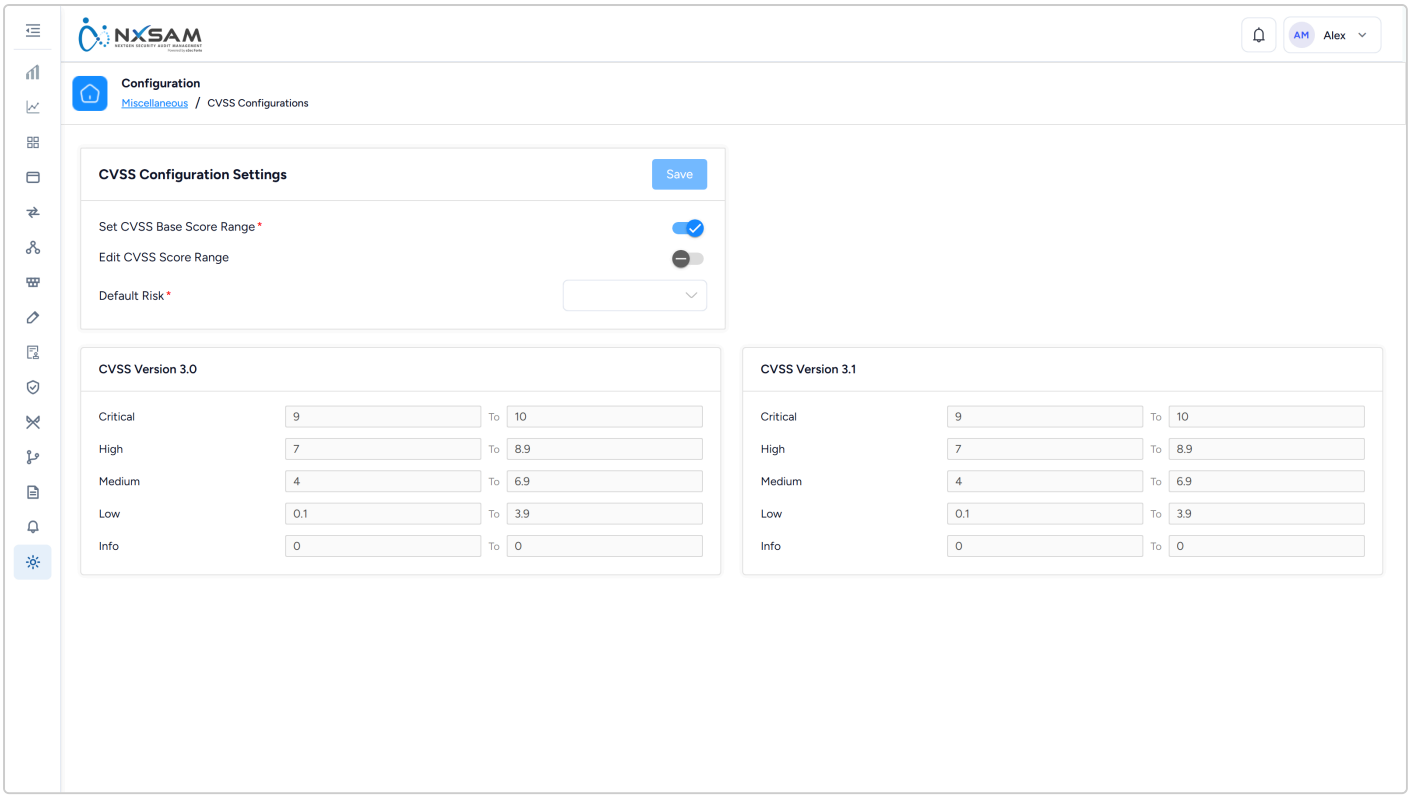
These screens decide how a raw scanner finding becomes a prioritised item of work. They are set up rarely and have wide effects, so each one is worth understanding before it is changed.

CVSS configuration

Sets how CVSS scores map onto NxSAM's severity levels — the boundary between High and Critical, and so on.

> ⚠ **Changing the mapping re-classifies existing findings**
>
> Severity is derived, not stored per finding. Move a boundary and findings on either side of it change severity — which changes their SLA, which can make a batch of findings overdue that were not overdue yesterday.
>
> This is the single change most likely to produce a sudden, unexplained jump in overdue counts. If one appears, ask what was changed here before investigating the data.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → Miscellaneous → CVSS Configuration — the score bands behind every severity

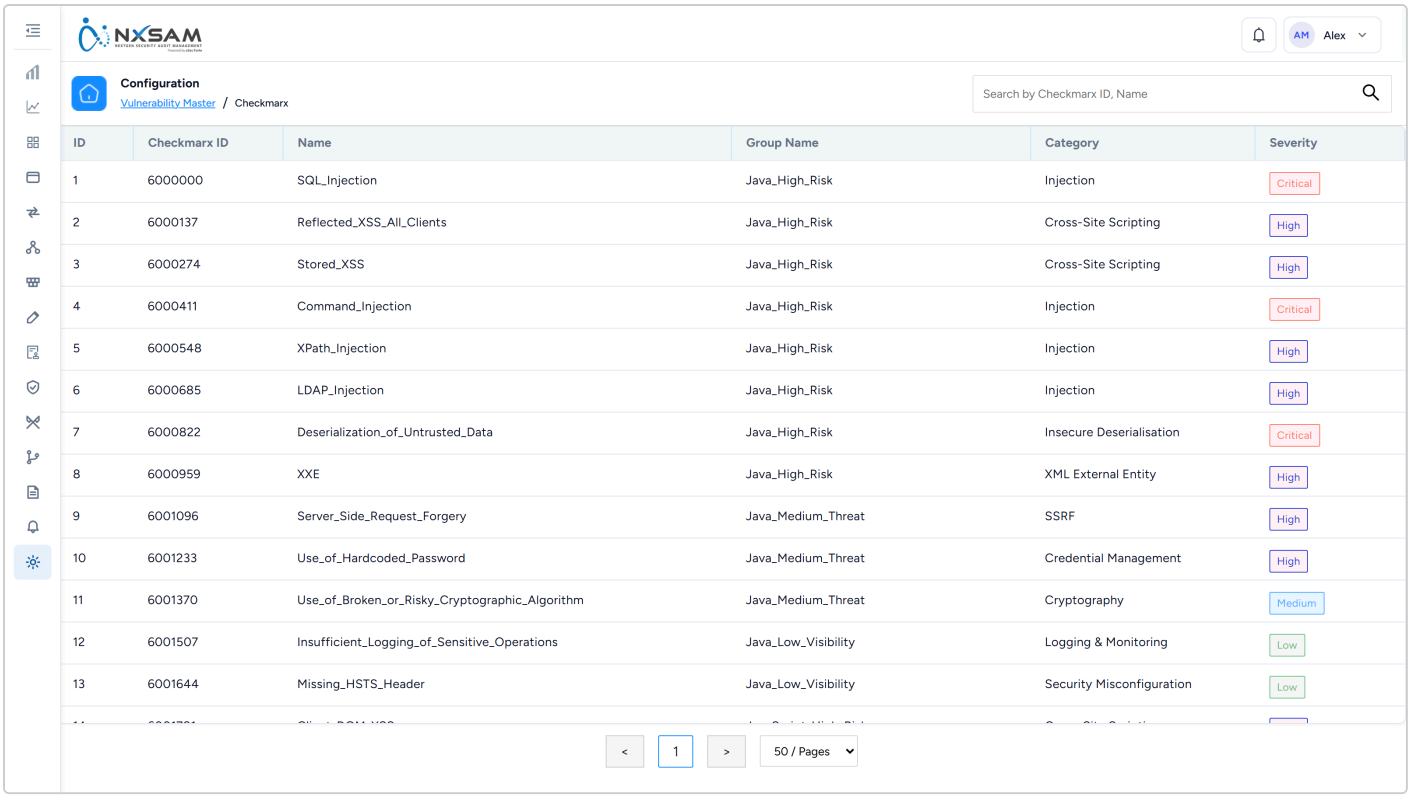
Vulnerability master and tool mapping

Two related things, easily confused:

- **Vulnerability master** is the catalogue of known vulnerabilities NxSAM holds for a given tool — the descriptions, remediation guidance and default severities.
- **Vulnerability master mapping** decides how that tool's identifiers line up with the catalogue, so the same weakness reported by two tools is recognised as one thing.

There is one of each per tool, and they are near-identical screens. Getting the mapping right is what stops the same vulnerability being counted twice under two names.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → Vulnerability Master → Checkmarx — one tool's catalogue; every tool has the same pair of screens

Risk scoring rules

Risk score combines severity with context — asset criticality, exposure, exploitability — into a single number used for ranking. Every weight in that combination is configurable, including which likelihood signals participate at all.

Ranking is only as good as the context feeding it. If asset criticality is unset across the estate, risk score degrades to severity with extra steps, and the "top risky assets" list stops being informative.

The rules live at **Setting → System → Analytics Risk Scoring**, and are covered in full under System, in *Tune the risk scoring rules* — the two axes, remediation health, the thresholds the charts draw from, and which scanners are scored under which rule set.

Network VA groups and sub-groups

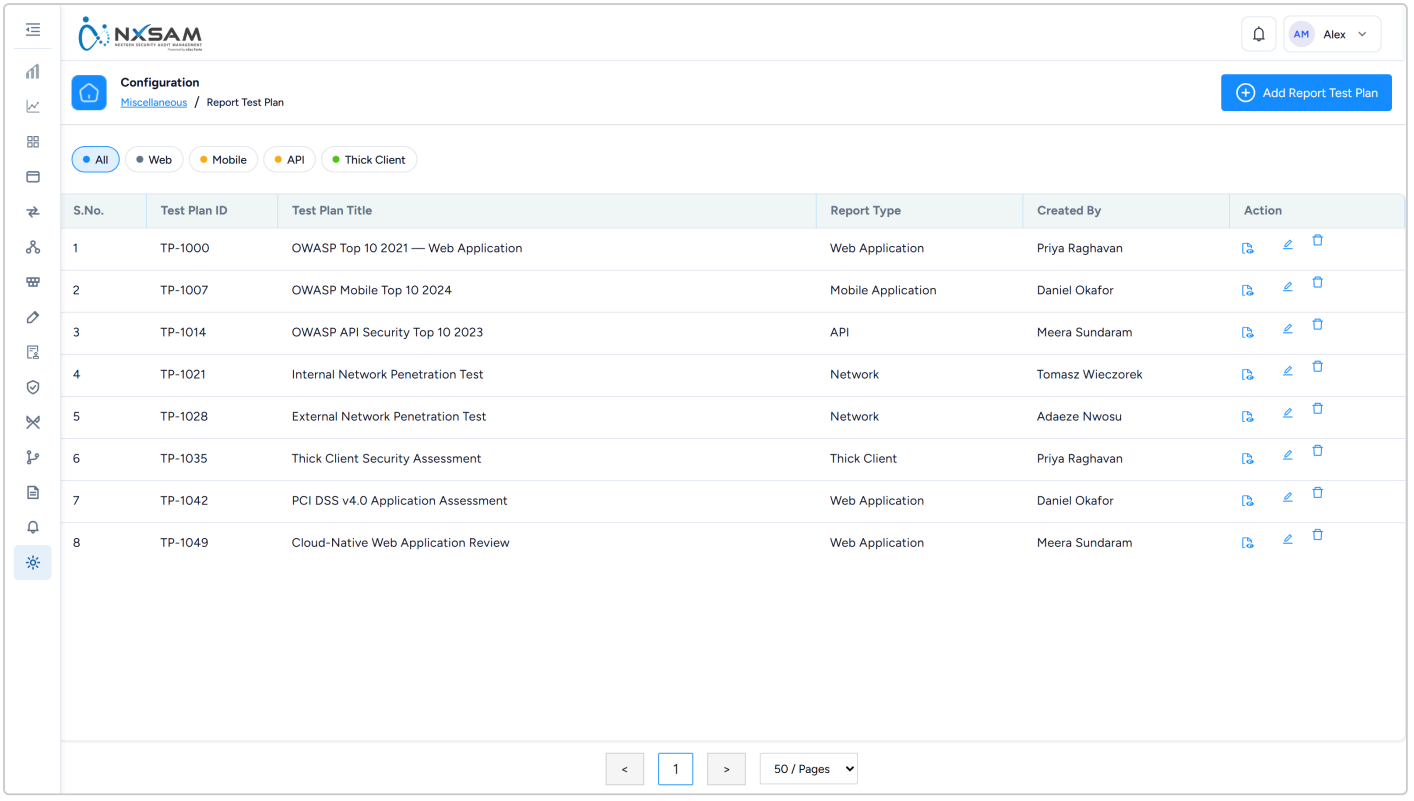
Group network assets for assessment and reporting — usually by location, environment or network segment. A finding inherits the grouping of its host, so this is what makes "which site is worst" answerable.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Test cases, categories and plans

For manual assessment work. A **test plan** is a set of **test cases**, organised into **categories**, that a tester works through during an audit.

This is what makes manual testing repeatable and reviewable: two testers running the same plan cover the same ground, and an auditor can see what was checked rather than taking it on trust. Without it, a manual audit's scope exists only in the tester's head.

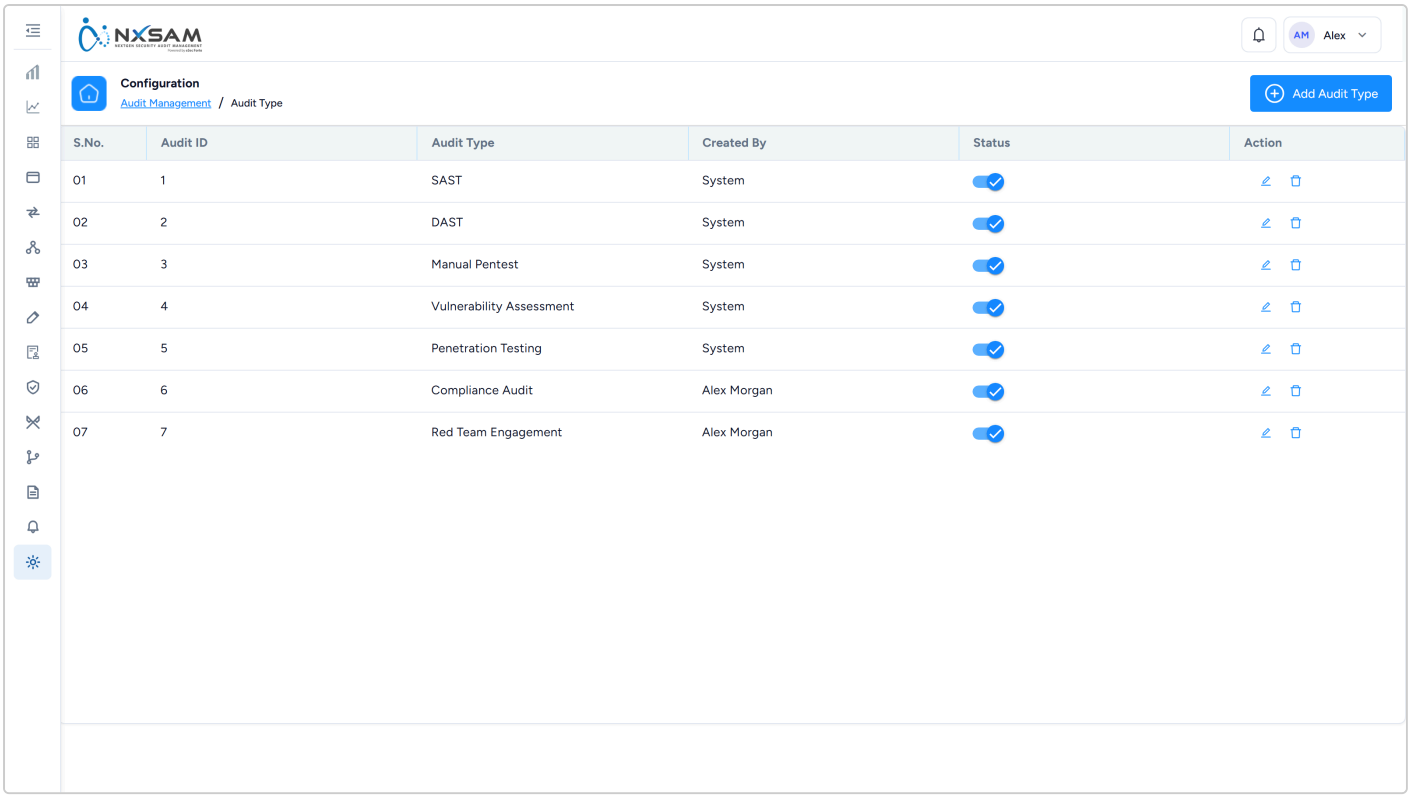


Configurations → Miscellaneous → Report Test Plans — the plans a manual tester works through

Audit status master

The set of states an audit can be in, and which transitions are permitted. Changing this affects every module that runs audits, and existing audits sitting in a state you remove have to go somewhere — so treat it as a schema change rather than a preference.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

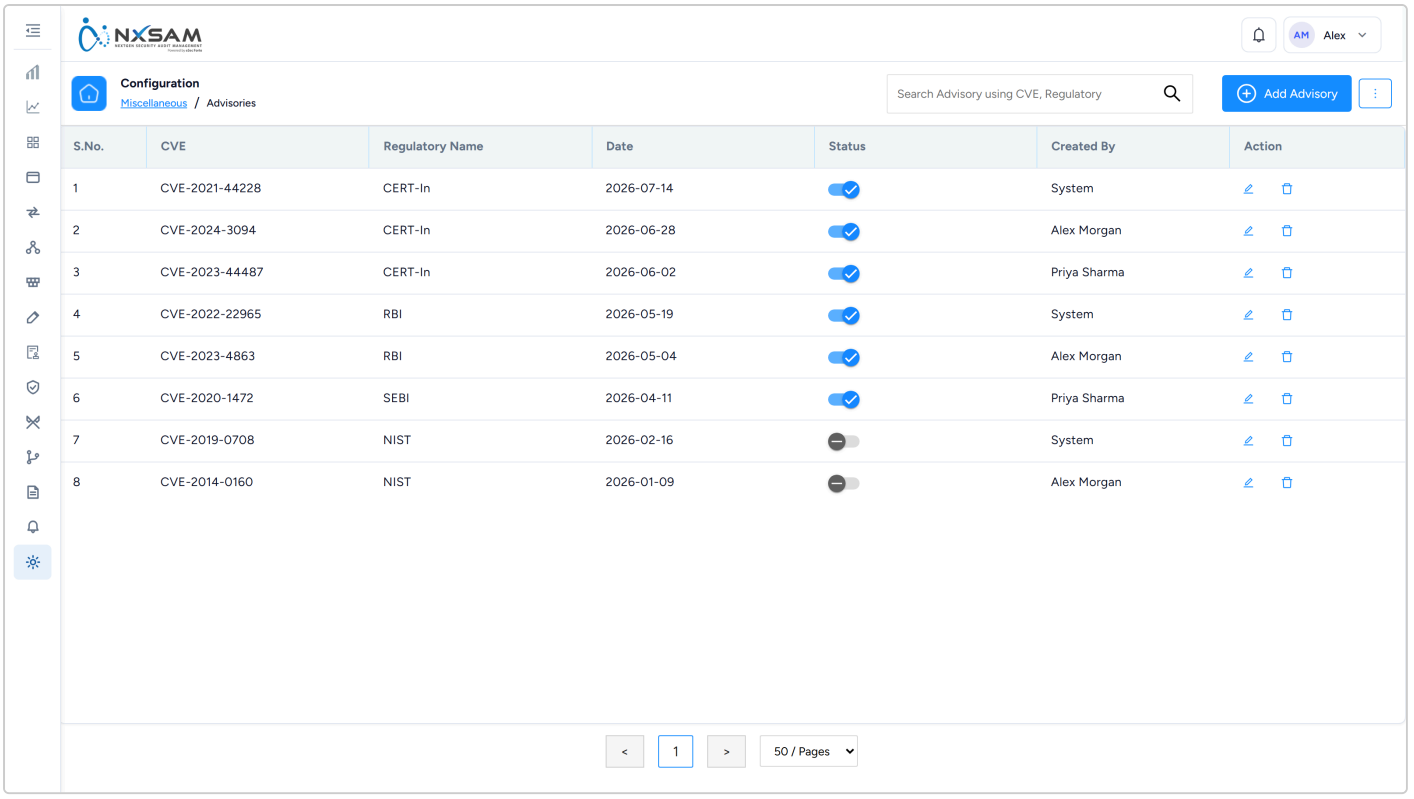


Configurations → Audit Management → Audit Type — audit types and the states they may pass through

Advisories

Security advisories published to users inside the platform. Useful for a coordinated response: when a widely-exploited vulnerability is disclosed, an advisory tells everyone what is expected of them without depending on email.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → Miscellaneous → Advisories — notices published to every user in the platform

Beats configuration

Scheduled background jobs — the periodic work that keeps derived data current, such as recalculating SLA states as dates pass and refreshing pre-computed statistics.

If a screen shows figures that are stale by a fixed interval rather than randomly wrong, this is the first place to look: a beat that stopped running produces exactly that symptom, and nothing else in the product will report an error.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Administration: every screen, column and action

User access, audit configuration and the master data other modules read.

Users

Column	What it holds
User Details	Name and contact
Roles	Which roles the account holds
Username	The sign-in name
User/Auditor	Whether the account performs assessments as well as using the platform
IP Group	Which address range they may sign in from
Created By	Who provisioned them
Last Sign-In	When they were last active
Status	Active, inactive or locked

Row actions — six

Action	What it does
Edit User	Account details and roles

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Action	What it does
Edit User Level	The seniority tier used in approval chains
Edit Asset Ownership	Which assets this person owns
Export Application	The applications they can see
Unlock User	Clears a lockout
Delete User	Removes the account

Edit Asset Ownership from here, not from each asset

When someone joins or leaves, their ownership has to move. Doing it asset by asset is the slow path and the one that leaves orphans; this action reassigns everything they own in one place.

Ownership is also visibility — an owner sees their assets and the findings on them — so leaving a departed user as owner means nobody is receiving those notifications.

Directory-backed accounts

When an account is created as an Active Directory user, the form requires a **Directory** — which of the configured directories the account authenticates against. It is mandatory because the same username can exist in more than one directory, and the pairing of the two is what identifies the person.

Choosing the wrong directory produces an account that looks correct in the list and fails at sign-in with an invalid-credentials message. Correcting it is an edit, not a re-create.

User/Auditor matters because auditors appear in assignment lists across every assessment module. An account not flagged as an auditor cannot be assigned to an audit, which is a common "why can't I select this person" question.

Last Sign-In is the column for an access review. Accounts with no sign-in for months are the ones to question first.

Page-level actions

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Export Users, **Download all users with assets**, **Upload CSV**, **View Bulk Update Logs**.

Download all users with assets is the access-review export: every user with everything they can reach, which is what an auditor asks for and what nothing else in the product produces.

The bulk update queue reports `Status`, `Summary`, `Initiated By`, `Initiated At` and a **Download Log File** — the per-row outcome of a CSV upload.

Roles, groups and levels

Screen	Columns
Roles	`Roles`, `Created By`, and the members — `User Id`, `User Name`
User Groups	`User Group Name`, `Organisation`, `No of Users`, `Created By`
User Levels	`User ID`, `Level 1`, `Level 2`, `Level 3`, `Created By`
Super Admins	`User ID`, `User Name`, `Created By`

User Levels are three independent tiers, not one ladder. They are used by approval chains to decide who can approve what, and a user can hold a different level in each — which is how an organisation models someone senior in one domain and junior in another.

Super Admins deserve a periodic review of their own. The list is short by design, and anything on it has unrestricted access.

IP restriction

Screen	Columns
IP Groups	`IP Group #`, `IP Group Name`, `Additional Info`, `Created By`
Assigned IPs	`IP Address ID`, `IP Address`, `Remarks`, `Created By`

Actions: **Assign IP**, **View Assigned IPs**.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Sign-in can be restricted to an address range per user. **Remarks** is where the justification goes — "site VPN egress", "vendor jump host" — and an entry without one is impossible to review later, because an IP address alone tells you nothing about why it was permitted.

Audit configuration

Screen	Columns
Audit Types	`Audit ID`, `Audit Type`, `Created By`, `Status`
Audit Properties	`Property Name`, `Property Type`, `Created By`
Property management	`Asset Type`, `Audit Type`, `Properties`
Manage properties (dialog)	`Property Name`, `Property Type`, `Sequence`, `Mandatory`

Properties are mapped per **asset type and audit type together**, so a property meaningful for a web DAST audit need not appear on a network VA. **Mandatory** blocks audit creation until filled — the usual reason an audit that used to save now will not.

Master status tables

The RLCM masters are administered here rather than in the module:

Screen	Columns
Audit status	`Audit Status`, `Colour`, `Audit Status Order`, `Comment Required`, `Auditor Required`, `Closed Type`
Risk status	`Audit Finding`, `Colour`, `Audit Status Order`, `Comment Required`, `Evidence Required`, `Closed Type`, `Is Exception`
Priority status	`Priority Levels`, `Colour`, `Priority Order`

Four flags decide behaviour, and all four are enforced at save time rather than announced in advance:

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

- **Comment Required** — will not save without one
- **Auditor Required** — needs an auditor assigned before the status can be set
- **Evidence Required** — needs an attachment
- **Closed Type** — whether the status stops something counting as open

Is Exception marks a status representing an agreed exception rather than a resolution. It is what separates "we fixed it" from "we agreed not to", and reporting that conflates the two overstates remediation.

Advisories

`CVE`, `Regulatory Name`, `Date`, `Status`, `Created By`.

Actions: **Upload Advisories**, **Export Advisories**, **Manage Regulatory Master**.

Advisories publish a coordinated response inside the platform. **Regulatory Name** links one to the regulator that issued it, which is what makes an advisory a compliance obligation rather than an internal notice — and the reason the regulatory master is maintained separately.

Network VA grouping

Groups — `Group Name`, `Sub Groups`. **Sub-groups** — `Sub Groups Name`, `Group Name`.

Two levels of grouping for network assets, usually site then environment. Findings inherit the grouping of their host, so this is what makes "which site is worst" answerable.

Test cases and plans

Screen	Columns
Categories	`Category No.`, `Category Name`, `Report Type`, `Created By`
Test cases	The cases within a category

Actions: **Manage Test Cases**, **Edit Test Case**, **Delete**.

A test plan is a set of cases grouped into categories, worked through during a manual assessment. **Report Type** ties a category to the report it appears in, so what the tester records and what the customer receives stay aligned.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Without a plan, a manual audit's scope exists only in the tester's memory — which is the difference between an assessment an auditor accepts and one they do not.

Test plans carry `Test Plan ID`, **Test Plan Title**, `Report Type`, `Created By`, with **View Status History** showing how a plan has changed — which matters when two assessments run against the same plan produce different coverage.

Email templates

There are two screens here, and they do different jobs.

Scheduled email reports are the recurring security reports you build yourself. Each definition carries `Name`, `Data Type`, `Dispatch`, `Trigger`, `Status`, `Updated`.

- **Dispatch** is how many emails go out — *Shared* is one to a fixed audience, *Group By* is one per owner, each carrying only that owner's findings.
- **Trigger** is the send cadence, not an event: *Daily at 06:45*, *Weekly, day 4 at 08:30*, *Monthly, day 1 at 08:00*.
- **Status** must be `Active` to be scheduled at all. A finished definition left on `Draft` is the usual explanation for a report nobody receives — followed by test mode still being on, which the list flags beside the name.

Building one is covered in full in Design a scheduled email report — data sources, body blocks, attachment, recipient resolvers, branding and the safe way to go live.

Notification templates are the platform's own transactional mail — the wording sent when an audit completes or a password reset is requested. That list shows `Scenario`, **Triggered On**, **Triggered At**, **Frequency**, **Send** and `Status`:

- **Scenario** — the situation the mail covers, such as an SLA approaching expiry
- **Triggered On** — the event that fires it
- **Triggered At** — the time of day it goes, for scheduled mail
- **Frequency** — how often, for anything recurring
- **Send** — sends a scheduled template now, off-schedule, to the recipients it would resolve to at the next scheduled send. It does not move the schedule: the next scheduled send still happens when it was due

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Frequency is why a notification arrives late rather than not at all

A template with a daily frequency and a fixed time sends once a day, not when the event occurs. A user reporting that an SLA warning "came a day late" has usually met exactly this — the event happened after that day's send.

Email logs

`Email Type and ID`, **Subject**, `To`, `CC`, **Added On**, **Triggered By**, `Status`.

Triggered By distinguishes a mail the schedule sent from one a person sent with **Send** — which is the first thing to check when a recipient reports receiving a report twice on one day.

The record of what was actually sent. **Status** distinguishes queued from sent from failed, and `To` / `CC` show who received it — which settles "I was never told" without involving the mail administrator.

Added On is when the mail was queued, not when it was delivered. A large gap between Added On and an absent delivery points at the mail server rather than at NxSAM.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

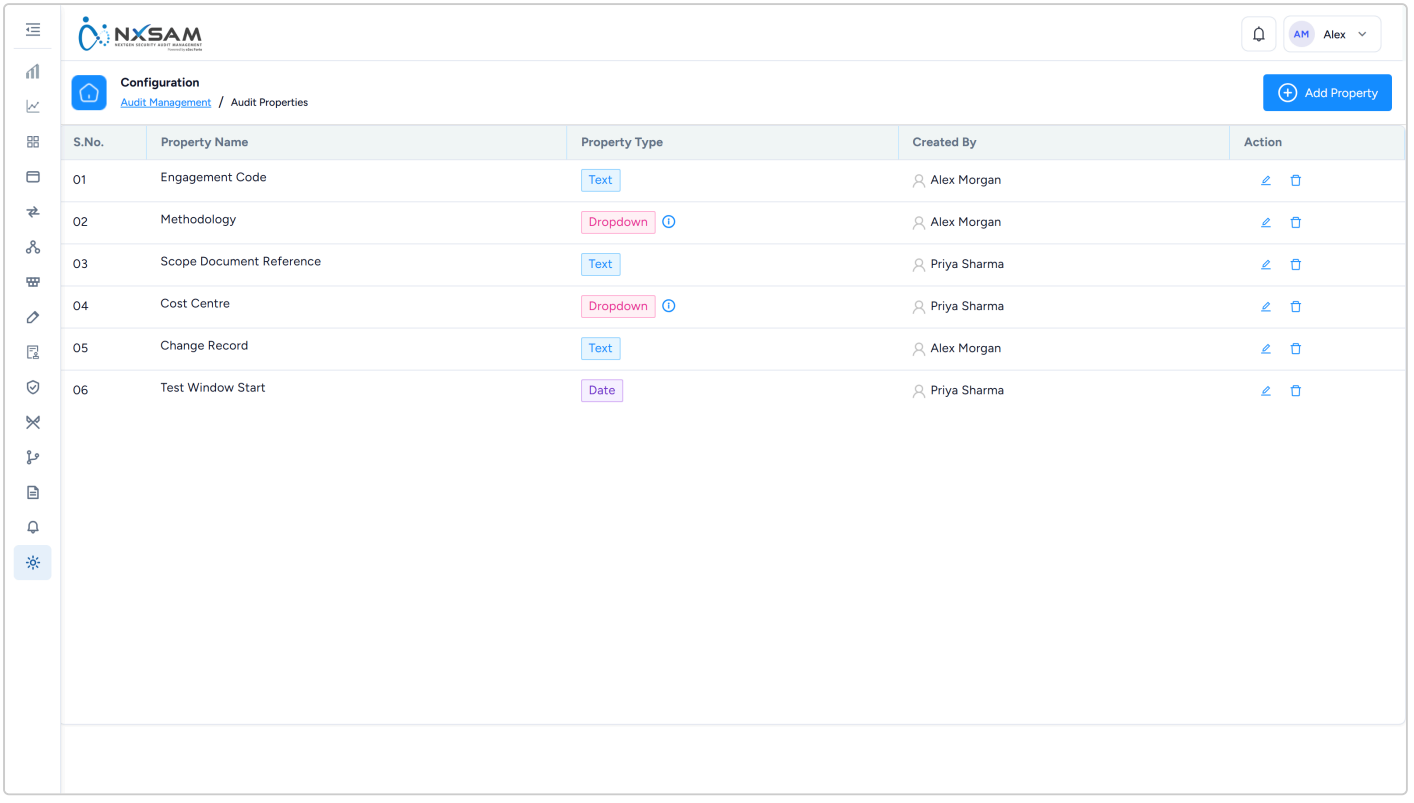
Administration: find the right screen

Every screen in this module, what each one is for, and where it lives. Use it to find the right screen quickly, and to confirm you are on the one a colleague means — several screens in this product have similar names and different jobs.

Screenshots come from a demonstration data set, so the figures are illustrative. Click any screenshot to open it at full resolution.

Audit Properties

Additional fields recorded against an audit.

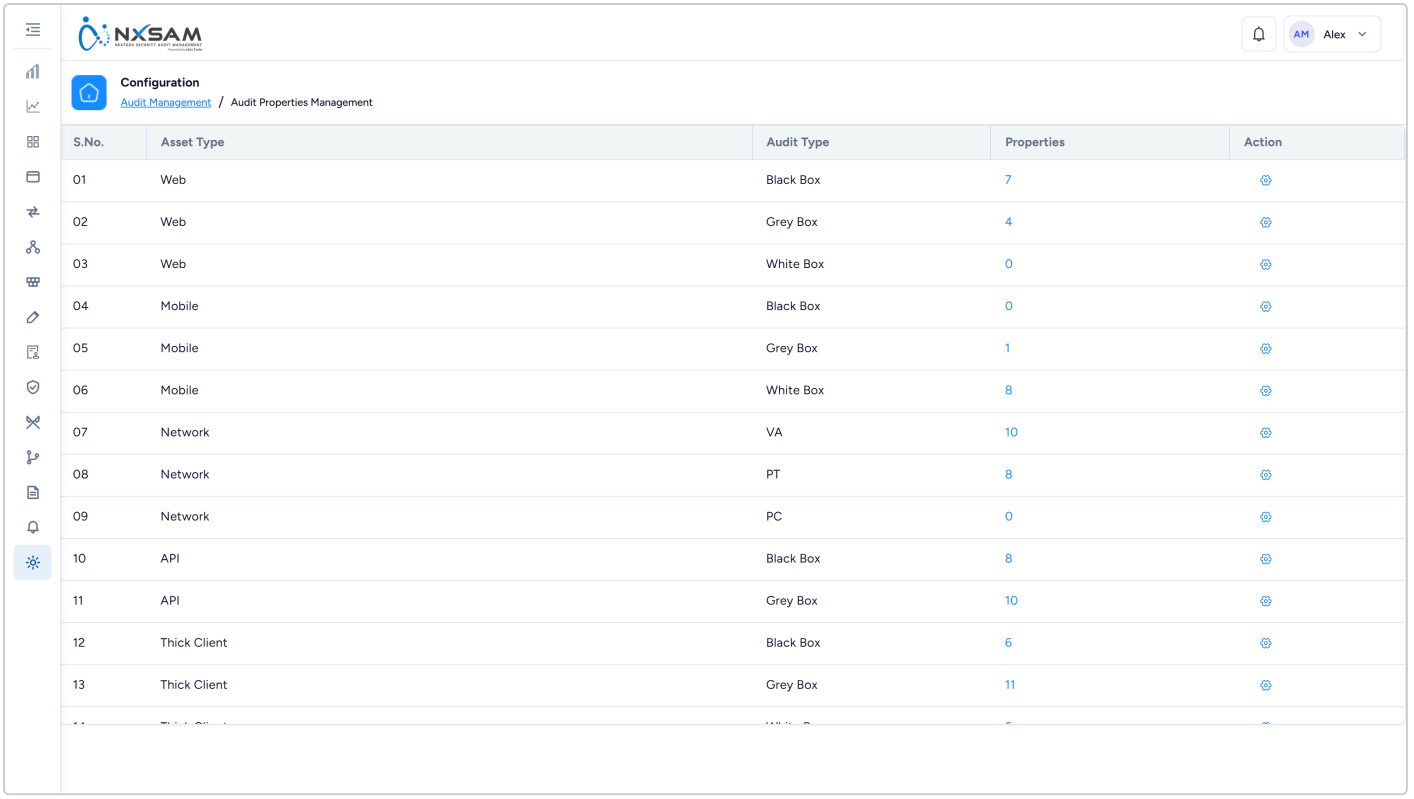


Setting → Audit Management → Audit → Audit Properties

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Audit Property Management

Which audit properties apply to which combination of asset type and audit type — the reason two audits can demand different fields.

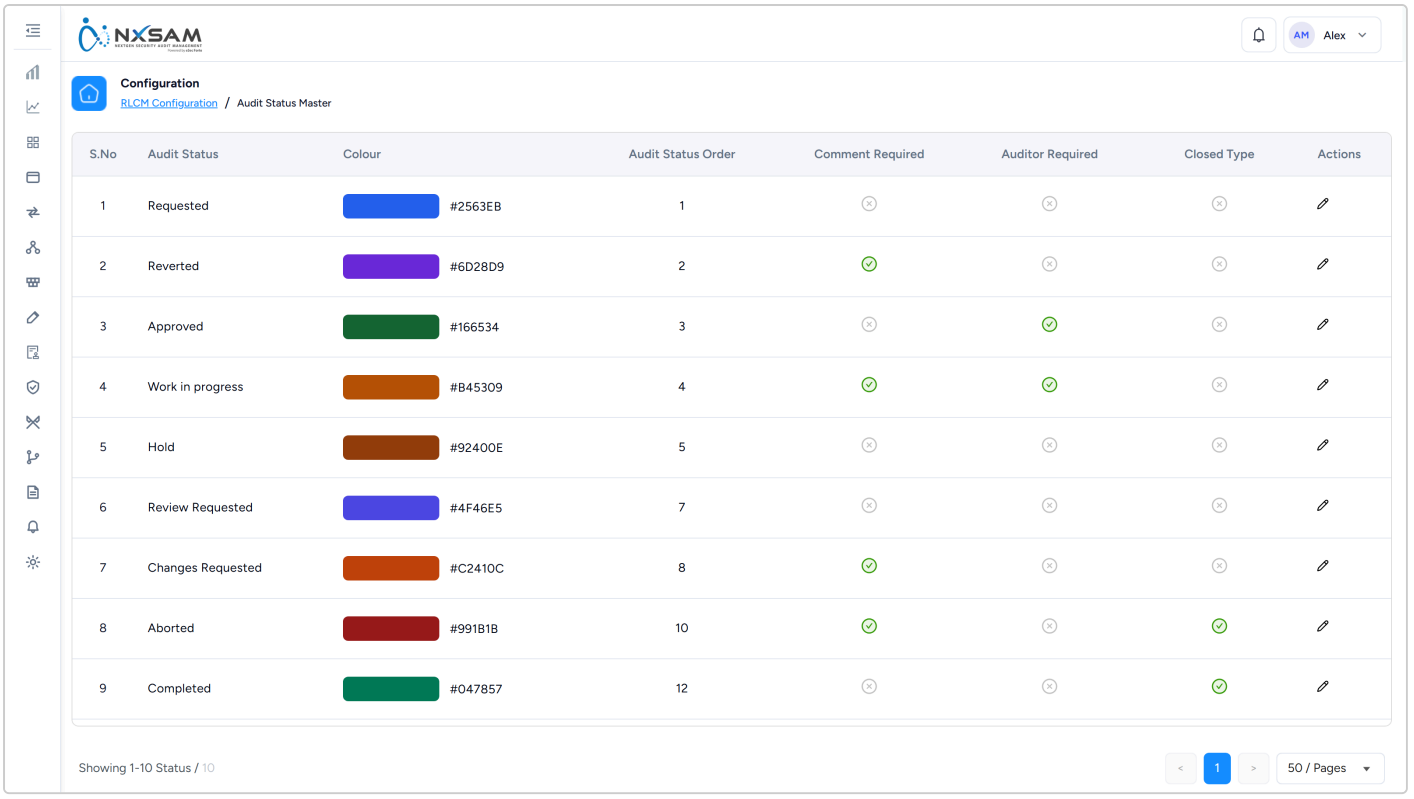


Setting → Audit Management → Audit → Property → Audit Property Management

Audit Status Master

The states an audit can hold, their order, and which of them demand a comment or an auditor.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

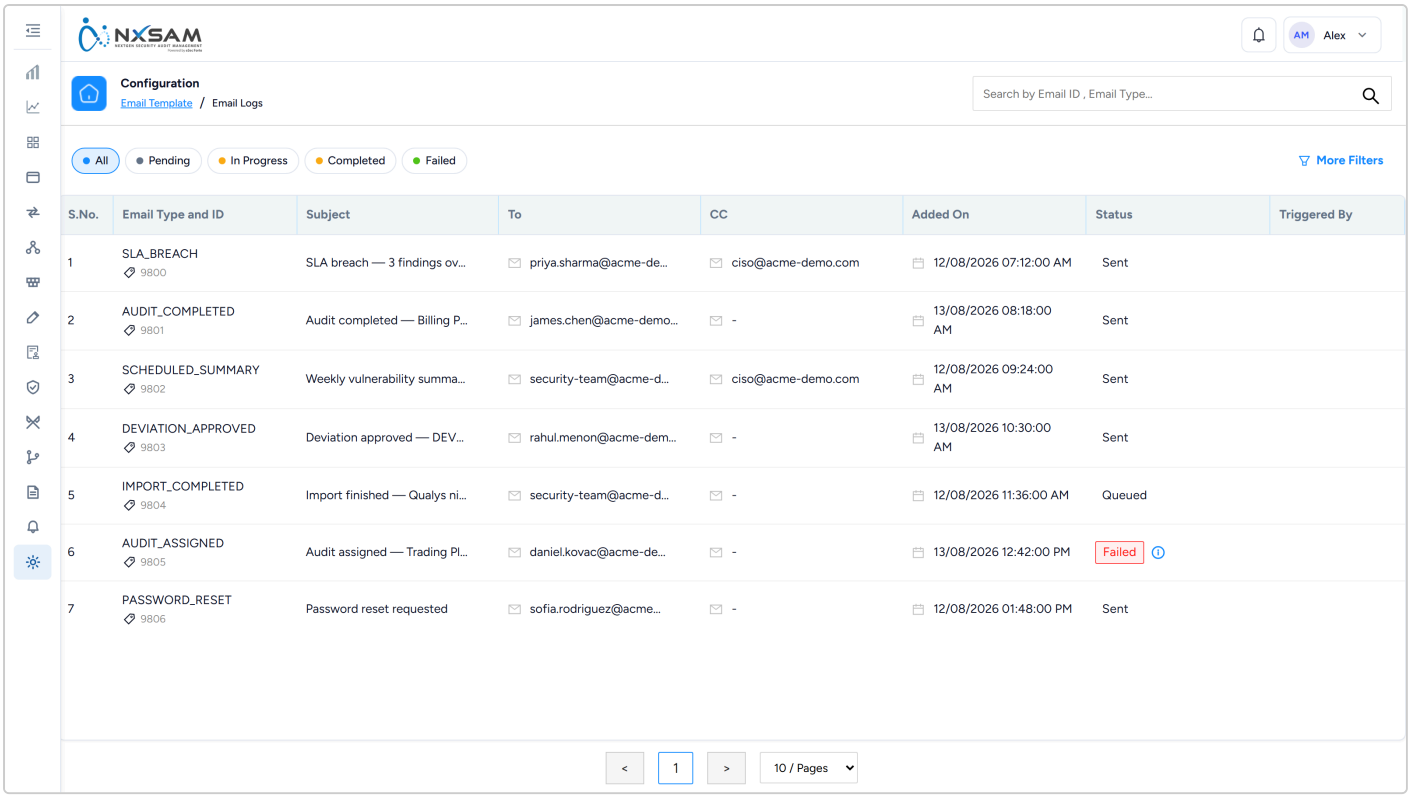


Master → Audit Status Master

Email Log

Every message the platform tried to send and what became of it. The first place to look when someone says a notification never arrived.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

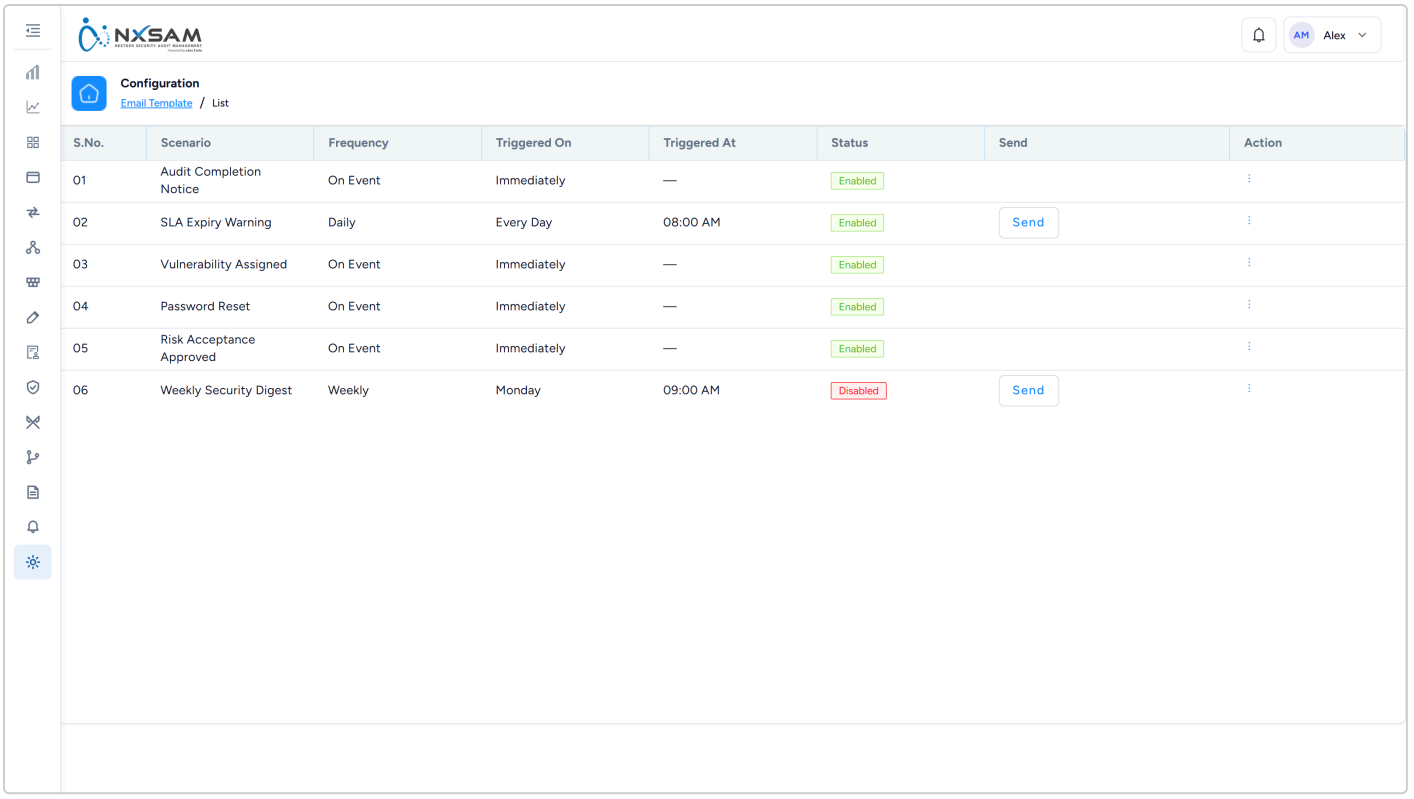


Setting → Email Template → Email Log

Email Templates

The wording of every notification the platform sends.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

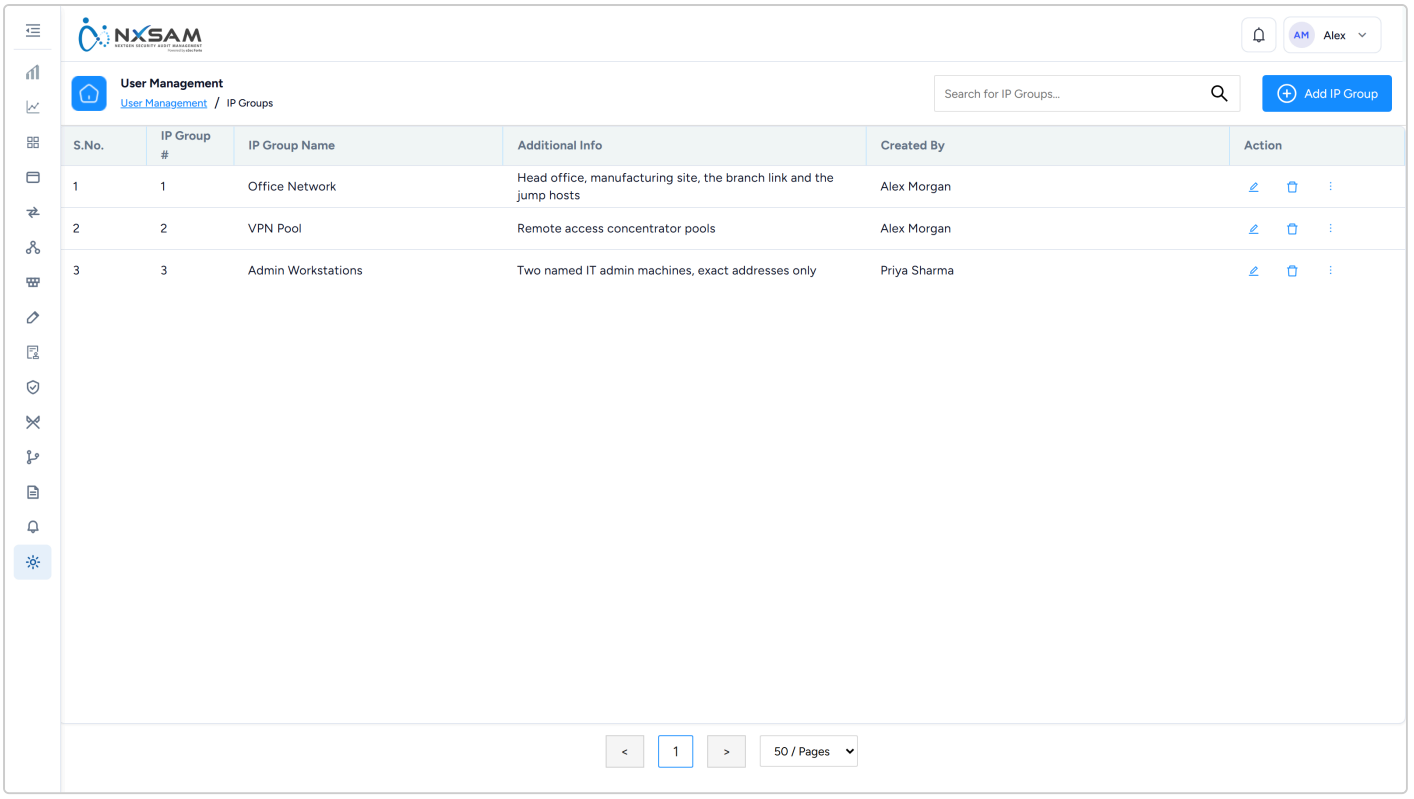


Setting → Email Template → Email Templates

IP Groups

Address ranges sign-in can be restricted to.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

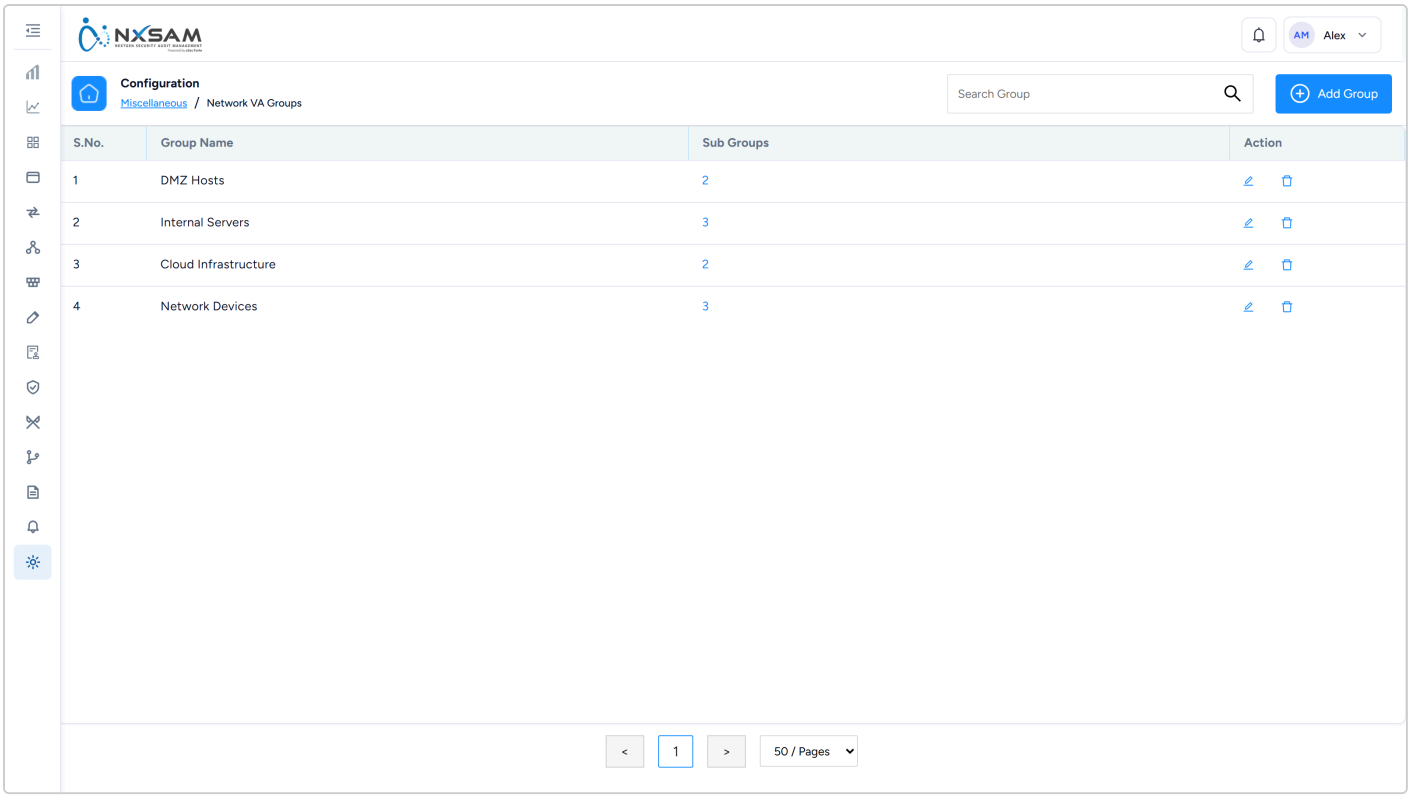


Setting → User Management → IP Groups

Network VA Groups

Groupings of network assets for assessment and reporting, usually by site or environment.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

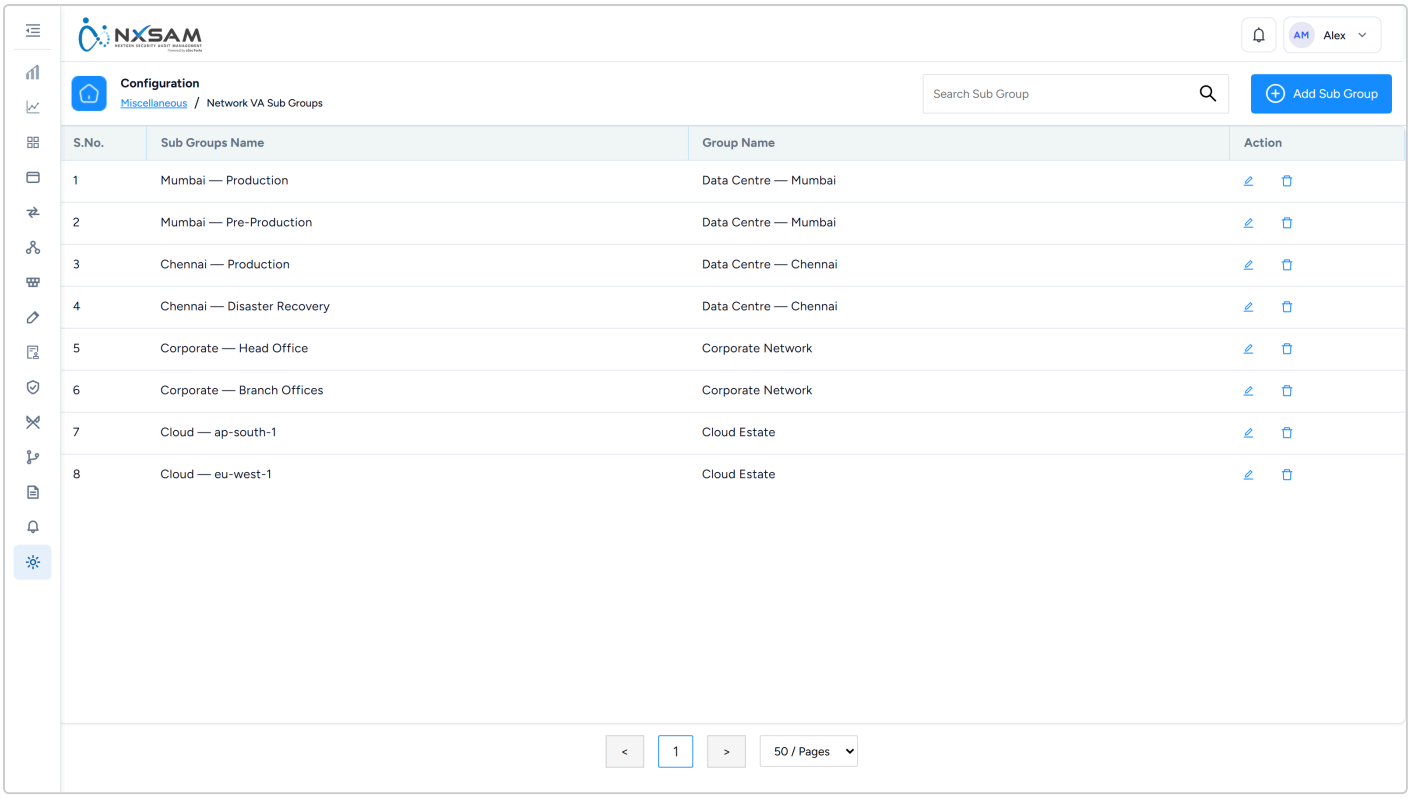


Setting → Miscellaneous → Network VA Groups

Network VA Sub-Groups

A second level of grouping within a VA group.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

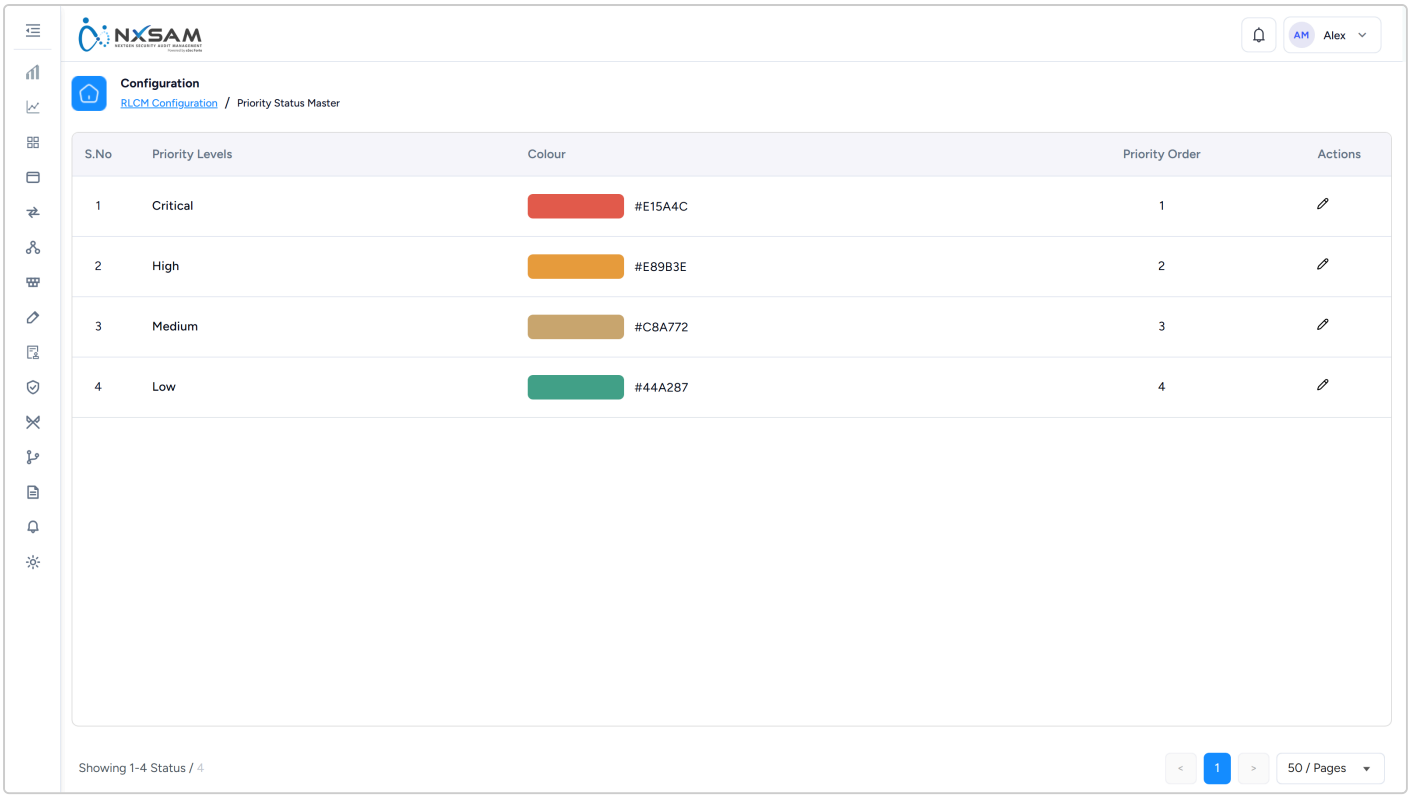


Setting → Miscellaneous → Network VA Sub-Groups

Priority Statuses

The priority values available on findings.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

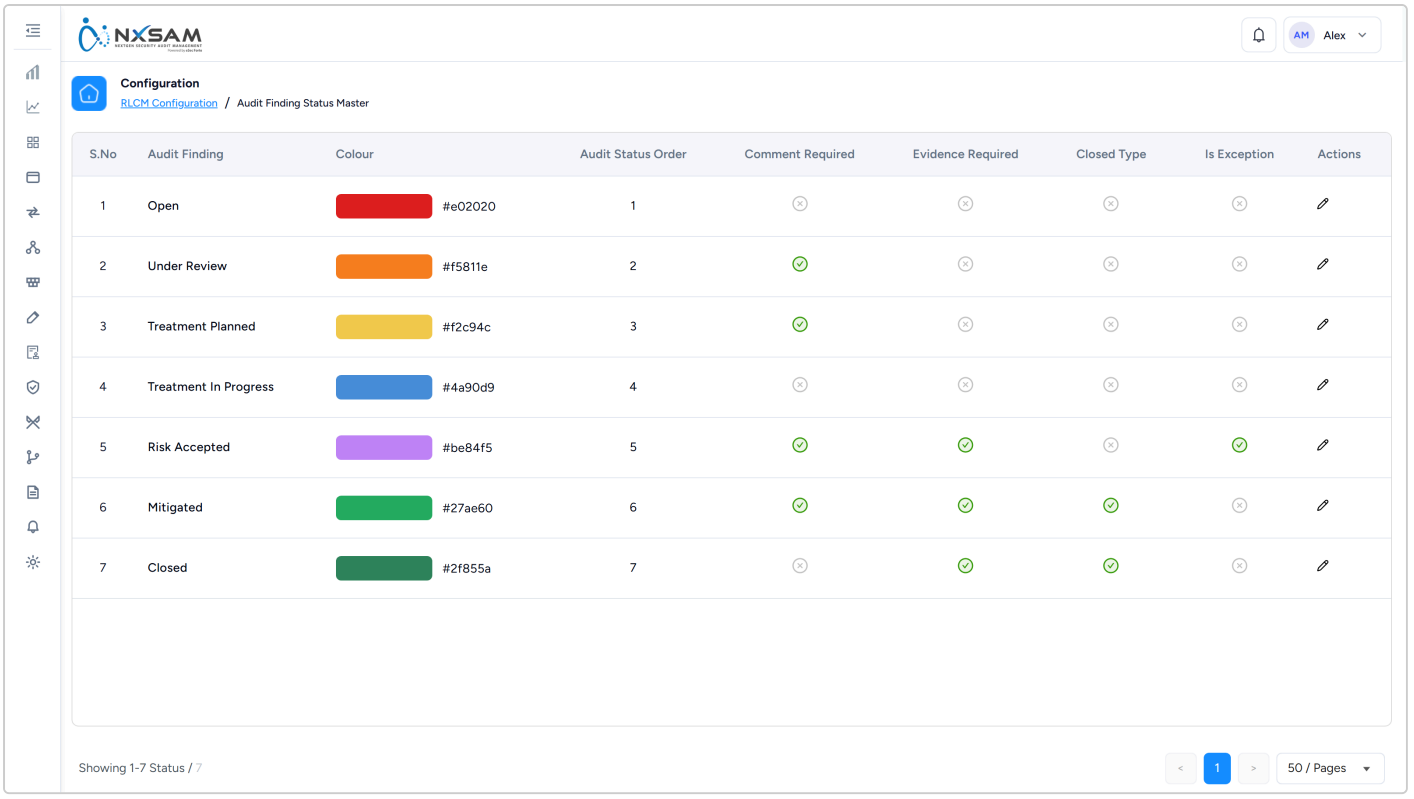


Master → Priority Statuses

Risk Statuses

The risk states available across modules.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

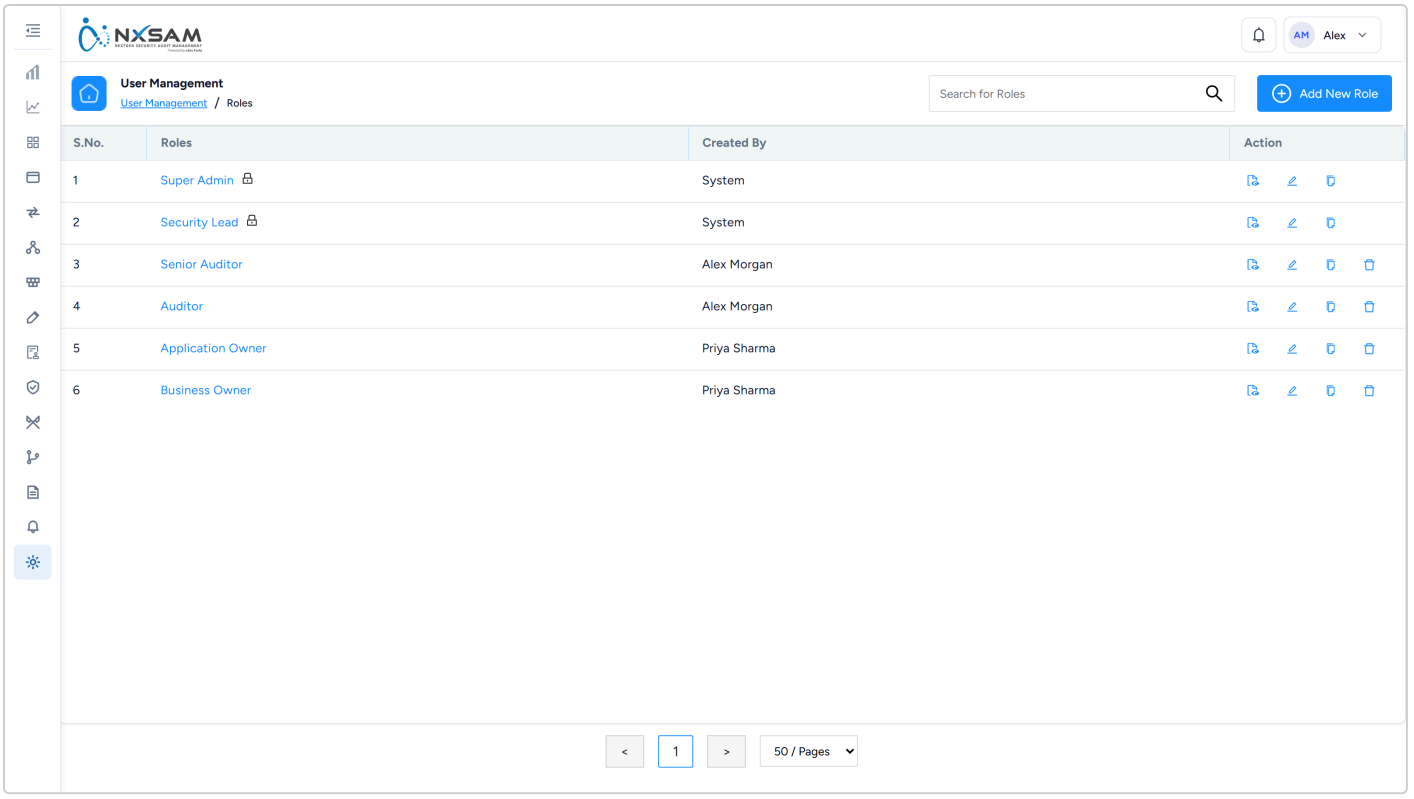


Master → Risk Statuses

Roles

What each role can see and do. Permissions are granted to roles, never to people directly.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

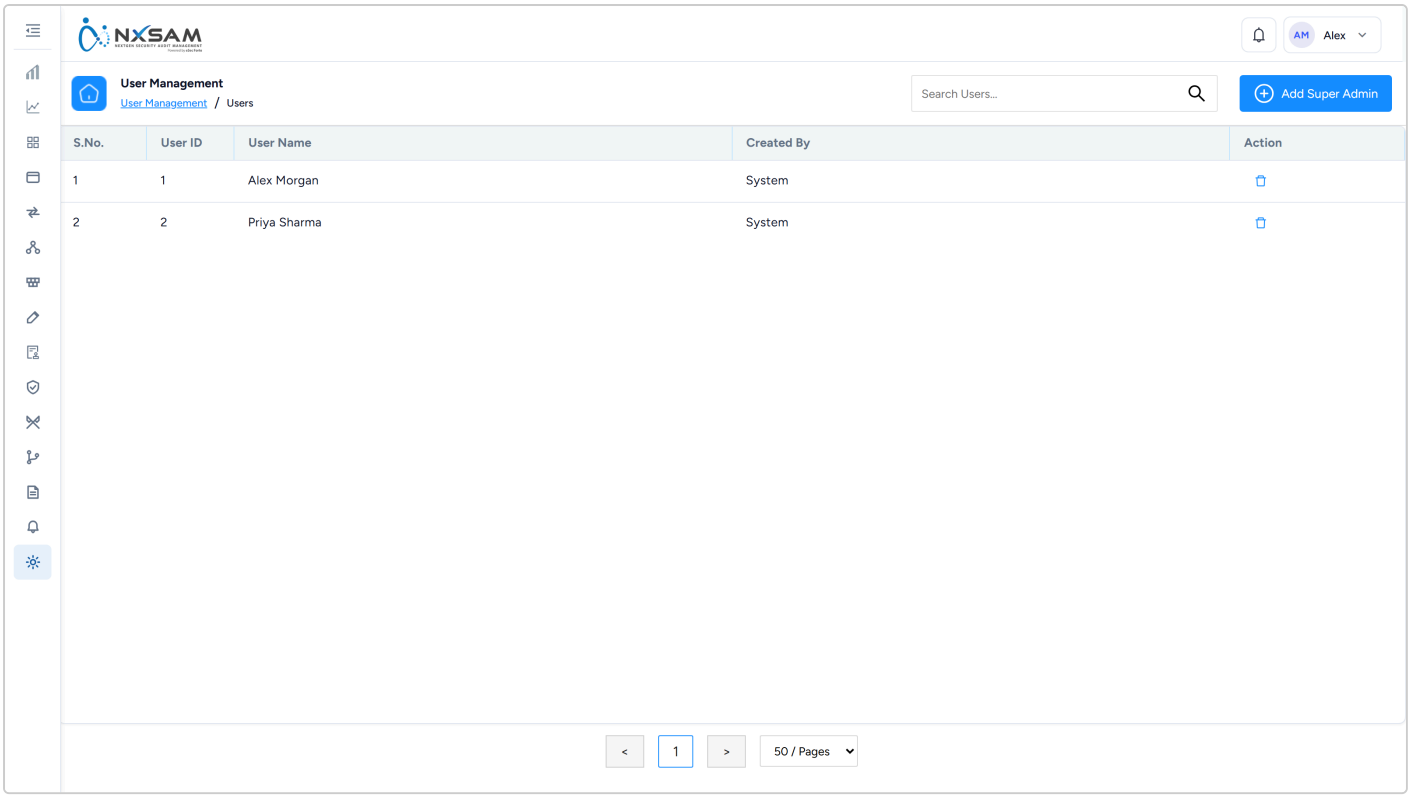


Setting → User Management → Roles

Super Administrators

Accounts with unrestricted access. Worth reviewing on a schedule.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

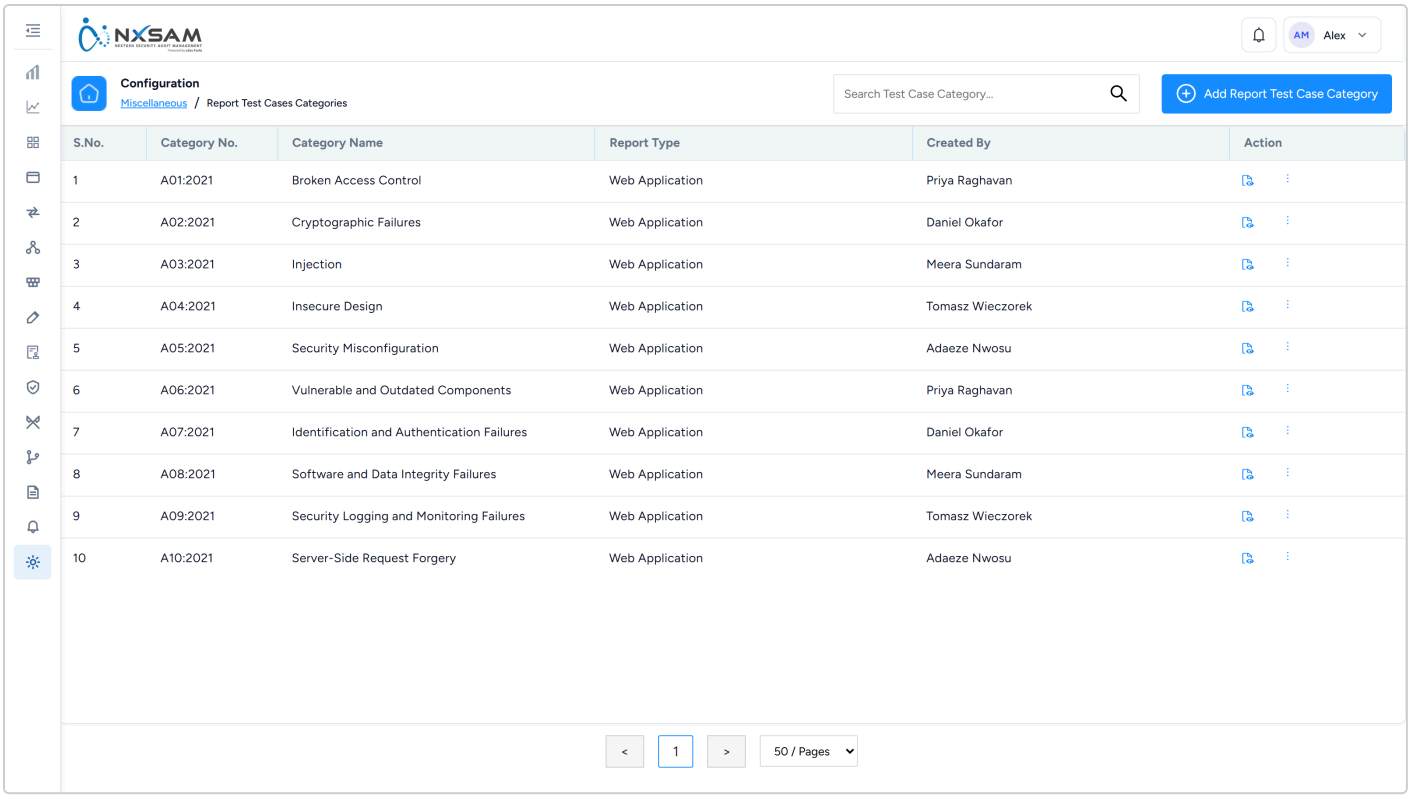


Setting → User Management → Super Administrators

Test Case Categories

How test cases are grouped for reporting, and which report type each group belongs to.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

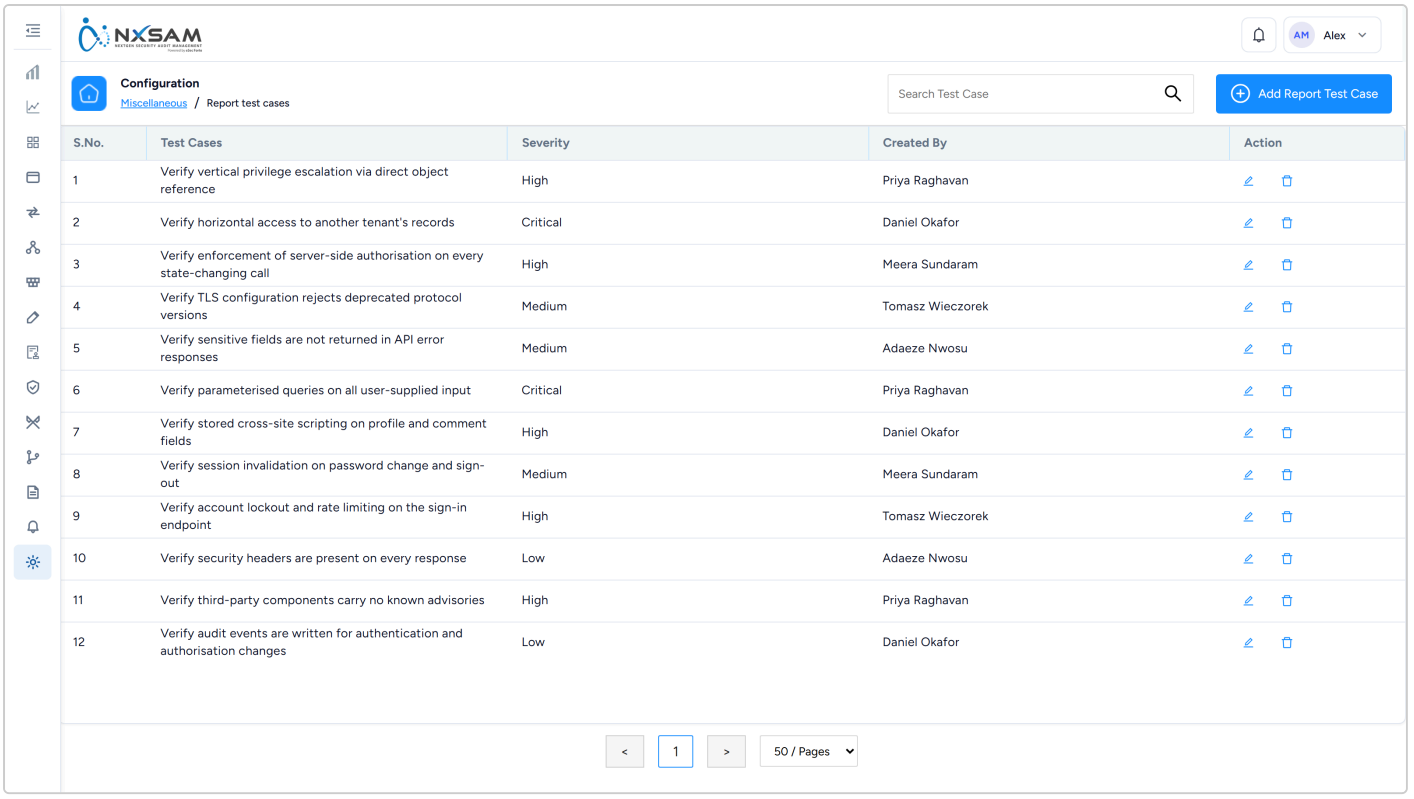


Setting → Miscellaneous → Test Case Categories

Test Cases

Individual checks a tester works through during a manual assessment.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

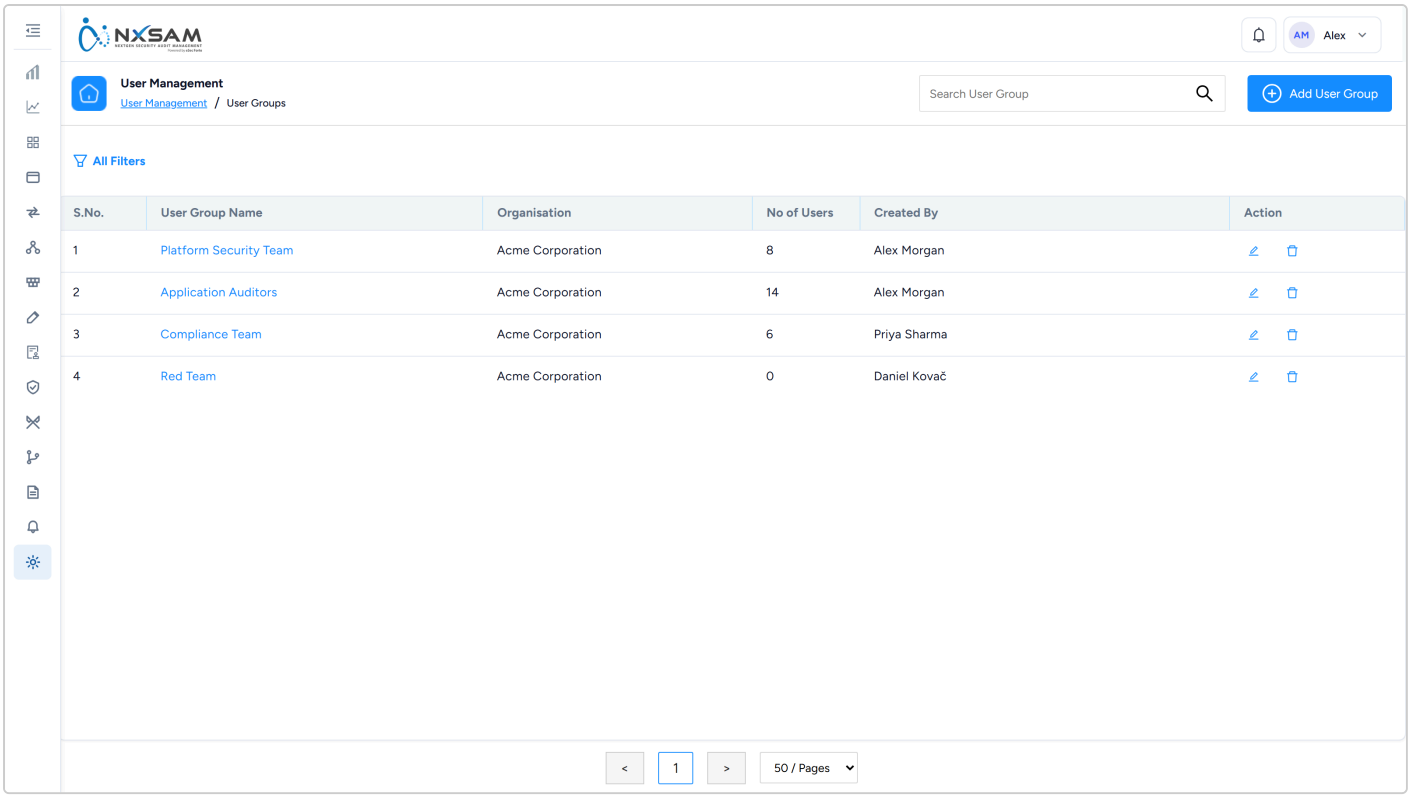


Setting → Miscellaneous → Test Cases

User Groups

Groups used to assign access to several people at once.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

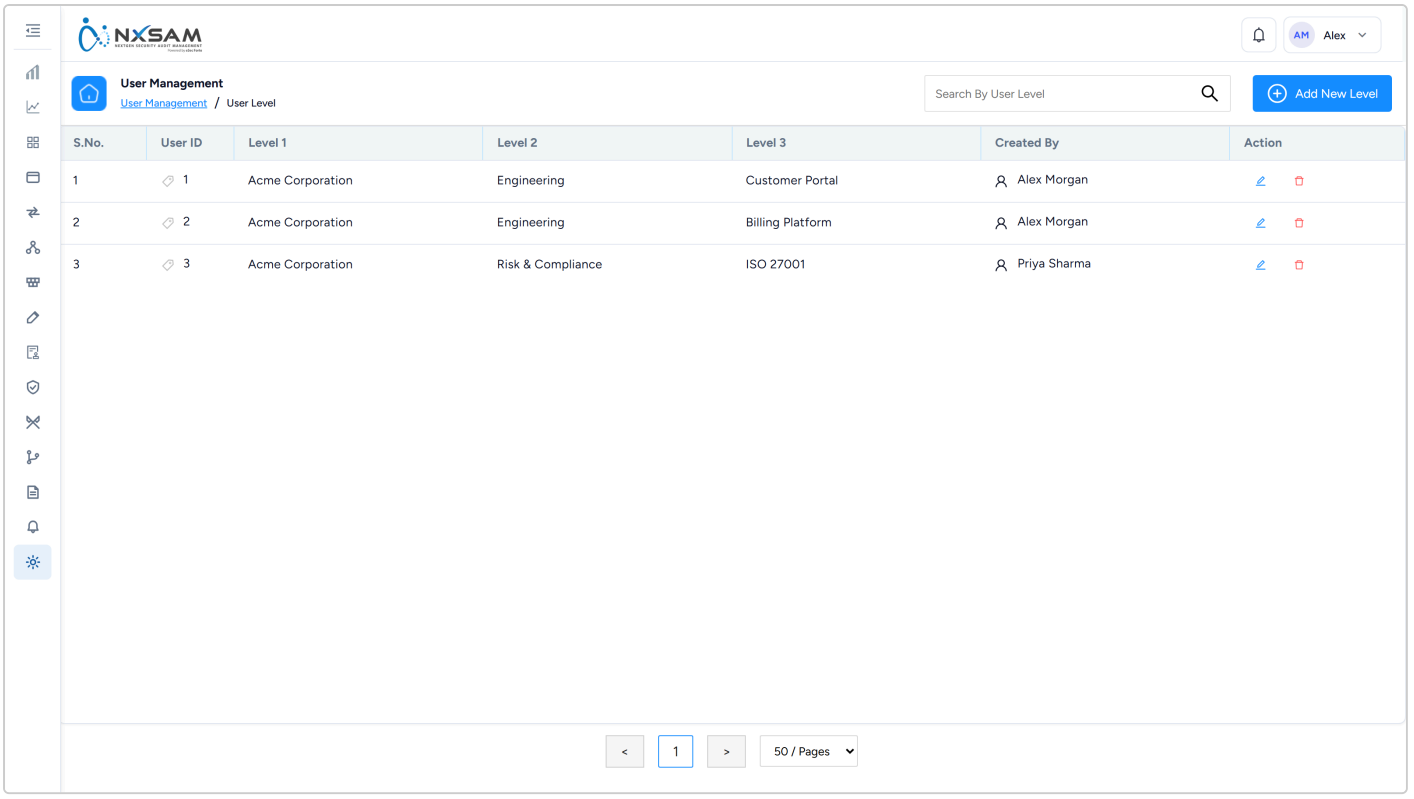


Setting → User Management → User Groups

User Levels

Seniority tiers used in approval chains and escalation.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

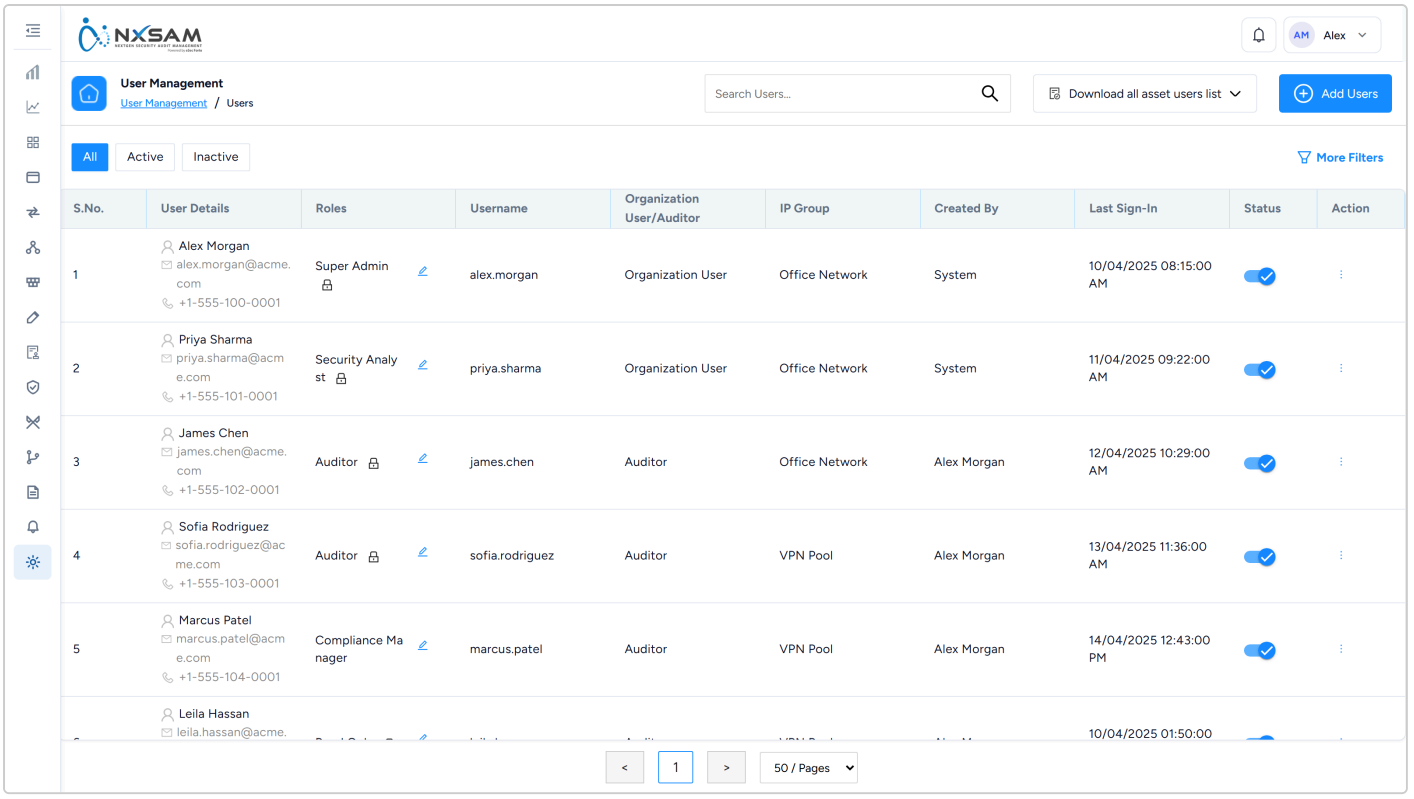


Setting → User Management → User Levels

Users

User accounts, their roles and when they last signed in.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Setting → User Management → Users

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reference

Glossary

Terms as NxSAM uses them. Several are ordinary security words with a narrower meaning here, and those are the ones worth reading even if the term is familiar.

Assets and scope

Asset — anything that can hold a vulnerability: a web or mobile application, an API, a network host, a thick client, or a container image. Each type is a separate inventory with its own columns and its own licensed limit.

Asset property — an attribute recorded against an asset, such as criticality or whether it is internet-facing. Properties are more than description: they narrow SLA durations and feed the contextual risk score.

Bifurcation — splitting one application into separately assessed parts, so a large system can be tested module by module rather than as one unit.

Collection — a grouping of container images that comes from the scanning platform rather than from NxSAM, and is not editable here.

Scope — what an assessment covers. For applications this is the application; for compliance it is a host list, which is why compliance scope disputes are settled with an exported list of addresses.

Assessments

Audit — one assessment of one asset. It has a type, a category, a cycle, a scope, and a status of its own, separate from any finding's status.

Audit cycle — which round of a recurring programme an audit belongs to.

Confirmatory audit — a re-test created against a parent audit to verify that fixes hold. It is evidence about the original rather than an independent assessment, so the two should not be counted as two rounds of testing.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Considered — the marker deciding whether an audit contributes to aggregate figures. Normally the latest audit per asset that reached a final state. An audit that is *not* considered still shows its findings on the module screen while contributing to no dashboard or report.

Initial audit — a first assessment, as opposed to a confirmatory one.

Findings

Vulnerability (also *finding*, *issue*) — one weakness on one asset, found by one assessment.

Vulnerability master — the catalogue entry (title, description, remediation) inherited by every occurrence of that vulnerability everywhere. Editing the master changes all of them.

Posture — Policy Compliance's unit: one control checked against one host. Every check produces a posture whether it passed or failed, which is why this module's volumes dwarf the others.

Artifact — the evidence attached to a finding: the steps, description and images that let someone else reproduce it.

Instance — which occurrence, where the same control or finding applies more than once to the same asset.

Status

Validation status — whether a finding has been confirmed. Nothing is counted anywhere until this reaches *Approved*, which is also when **Discovered On** is populated.

Client status (also *current status*) — what is being done about the finding. Of its values, only two close it.

Closed type — the flag deciding whether a status stops something counting as open. It is configuration rather than a fixed rule, so a deployment can change what "closed" means.

Posture status — what a compliance check returned: pass, fail or **error**. Error means the check could not run — a scanner or credentials problem rather than a compliance result.

Sub status — the qualifier beneath a main status: which kind of acceptance, or which stage of an approval.

Time and SLA

SLA duration — how long a finding of a given severity on a given asset type may remain open. Configurable, and narrowable by asset property.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

SLA expiry — the resulting deadline. Changing an SLA duration re-derives expiry dates, which can make a batch of findings overdue with no data change at all.

Discovered On — when a finding was first observed. Blank until the finding is approved.

Last observed — the most recent sighting, which is how a finding is known still to exist.

Overdue — past SLA expiry and not closed.

Decisions

Deviation (also *risk acceptance*, *RA*) — a recorded decision not to fix something, with an approval chain and an expiry. It does **not** close the finding: the exposure is still live and still counts as open.

Exception — a status marking an agreed exception rather than a resolution. Reporting that conflates the two overstates remediation.

Auto reject end date — when a temporary acceptance lapses on its own.

Integrations and processing

Integration — a connection to a scanning tool, either pulling from its API or parsing an uploaded report.

Vulnerability key — the columns deciding whether an incoming finding is one already seen. Changing it redefines "the same finding" and splits history.

Queue — asynchronous work: imports, syncs, report generation. A screen that seems not to have updated usually has a queue entry that explains it.

Data process — how far a tool-fed audit has got through the import pipeline; the difference between "the upload finished" and "the data is ready".

Beat — a scheduled job maintaining derived data, such as recalculating SLA states as dates pass. A stopped beat produces figures wrong by a fixed interval and raises no error.

Governance

RLCM — Red Line Compliance Management: assessment of controls against frameworks, rather than of systems for weaknesses.

TPRM — Third-Party Risk Management: the same control assessment applied to suppliers. It shares screens with RLCM and differs by the audit's type.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

UCF — Unified Control Framework: the mapping that lets one control satisfy several frameworks at once, so answering it once covers each of them.

Control — a requirement being assessed, as opposed to a weakness being found.

Standard — the framework a control belongs to, such as ISO/IEC 27001 or PCI DSS.

Reporting

Considered audit filter — the switch on Report Search that reproduces either the dashboard's numbers or the module screens'. Comparing the two settles most disagreements about counts.

Design template — the layout a report renders through, separate from the template that decides its content.

Share view against share copy — sharing a template as a view keeps one definition that your edits reach; sharing a copy creates an independent template that will drift.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.