



NxSAM Assets — Quick Guide

Quick reference guide for the Assets 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

Assets

- Overview
- Organising the inventory
- Assets: every screen, column and action
- Assets: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Assets

Assets

An asset is anything that can carry a weakness. Everything else in NxSAM hangs off the asset inventory: audits are run against assets, findings belong to assets, and reporting is grouped by them. If the inventory is wrong, everything built on it is wrong too.

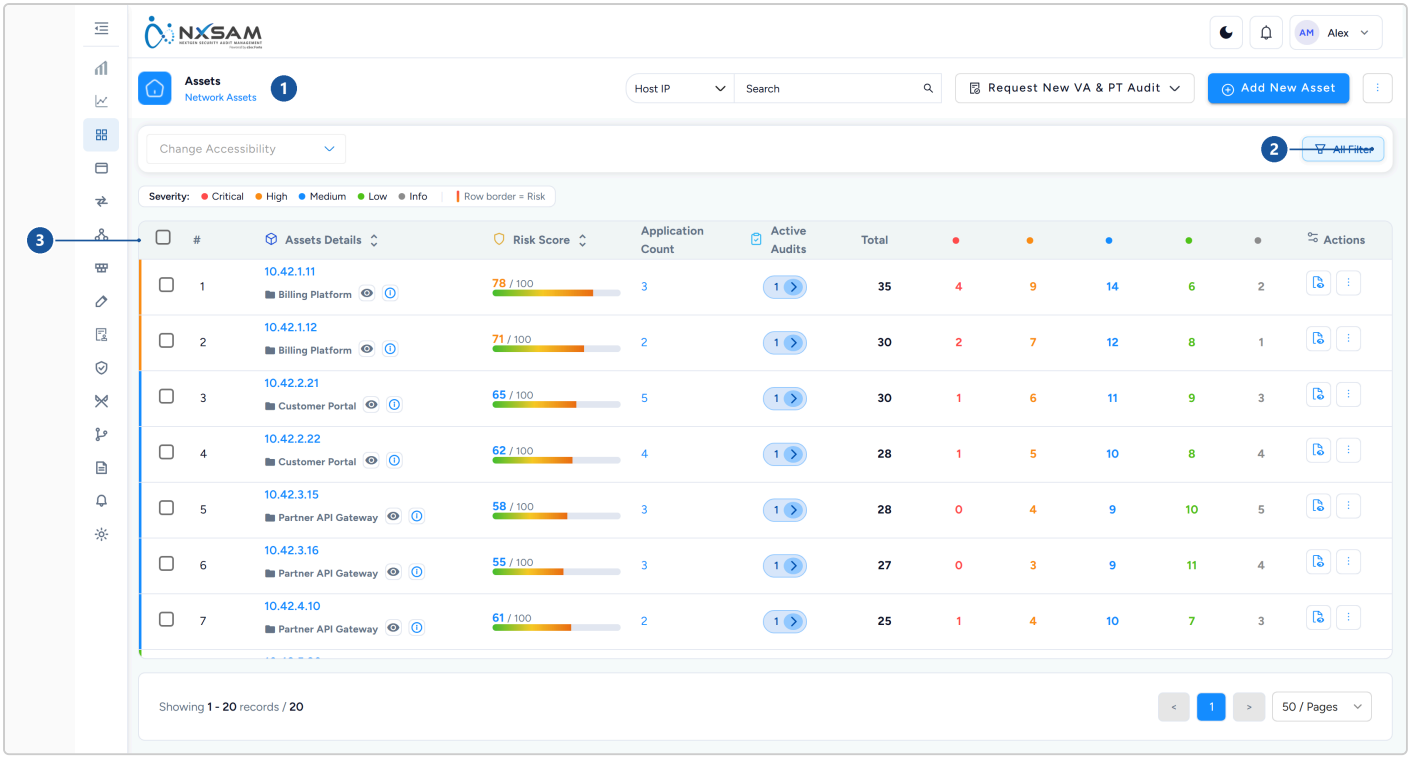
The six kinds of asset

Type	What it covers
Web Applications	Websites and web-based systems, identified by URL
Mobile Applications	iOS and Android apps, identified by package or bundle
Thick Clients	Installed desktop software
API Assets	Service endpoints assessed separately from the applications using them
Network Assets	Hosts, servers and network devices, identified by IP or hostname
Container Assets	Container images, identified by repository and tag

The type determines which security module assesses it and which scanners can contribute findings. It is set when the asset is created and is not something to change casually — existing findings are attached to the asset as it was classified.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

What an asset record carries



The network asset inventory. Each row is a host that can carry findings.

1 module and screen · 2 filters · 3 inventory columns

Beyond its name and identifier:

- **Ownership** — who is responsible for fixing things found on it. This drives who sees the asset and who is chased when findings age.
- **Business context** — organisation, business unit, project. Used for grouping and reporting rather than access.
- **Environment** — production, UAT, staging, development.
- **Criticality** — how much the business depends on it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Criticality is not severity

Criticality describes the *asset*: how much damage its compromise would cause. Severity describes a *finding*: how serious that particular weakness is.

A Low severity finding on a Critical asset and a Critical finding on a Low asset are very different situations, which is why both are recorded.

Ownership determines visibility

NxSAM shows people the assets they are responsible for. An asset owner sees their own applications and the findings on them; a security analyst sees the estate.

This has a practical consequence worth knowing before raising a ticket: if a colleague cannot see an asset you can, that is ownership and permissions working as designed. The remedy is an ownership or role change, not a data fix.

Keeping the inventory current

Assets reach NxSAM three ways:

1. **Created directly**, one at a time.
2. **Imported in bulk**, from a spreadsheet.
3. **Synchronised** from a source of truth such as a CMDB, where configured.

Where synchronisation is in place, treat the source system as authoritative and make changes there — a local edit will be overwritten on the next sync.

Decommissioning

Assets that no longer exist should be decommissioned rather than deleted. Decommissioning removes the asset from active tracking while preserving its history, so past findings and reports remain intelligible.

Deleting is a soft operation too — the record is hidden, not destroyed — which is why a deleted asset's name can still appear on historical findings and older reports.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Organising the inventory

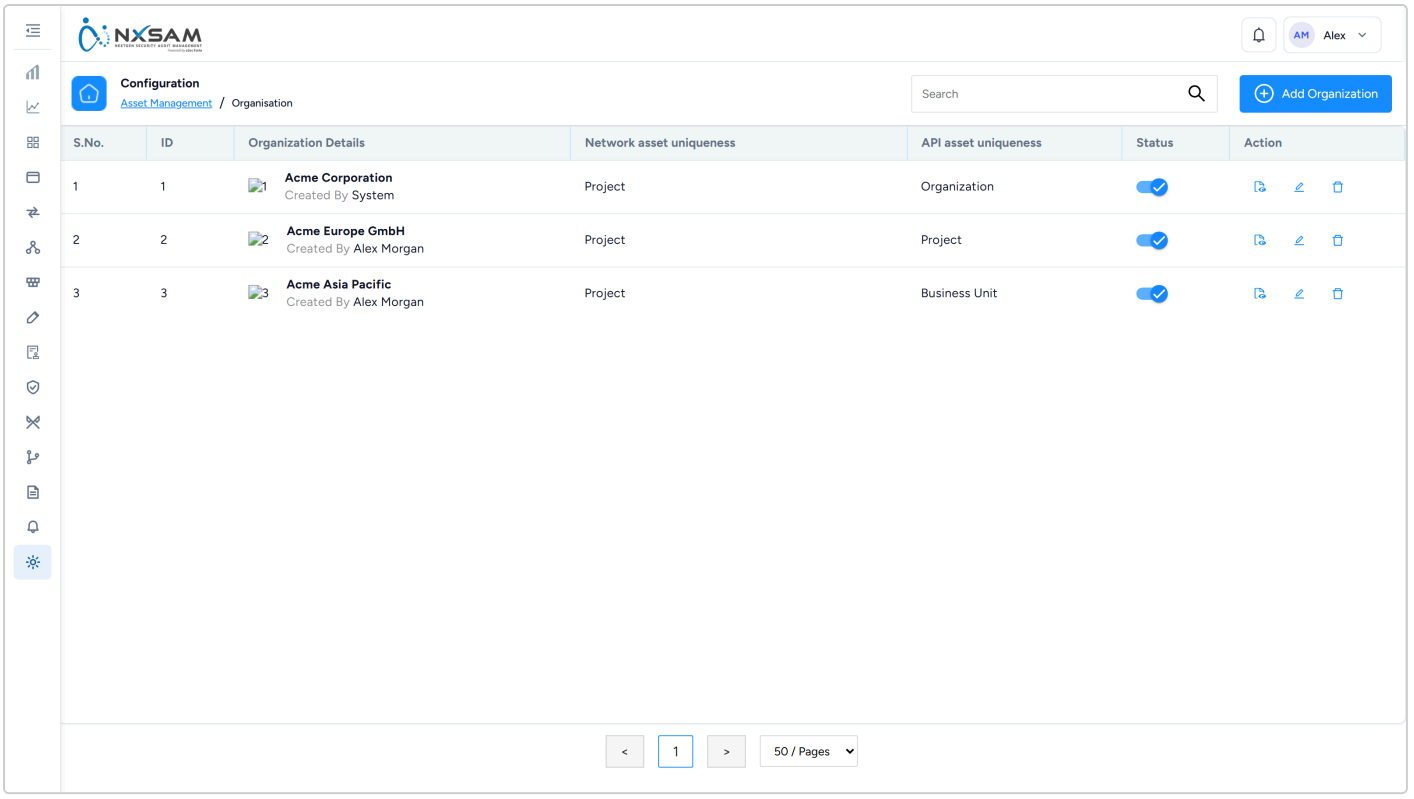
Everything in NxSAM hangs off the asset inventory, so how it is organised decides how useful every report and dashboard downstream will be. These screens are where that structure is set.

The three levels of grouping

Level	What it usually maps to
Organisation	A legal entity, or a major division
Business Unit	A department or function within it
Project	A programme of work, or a product

Every asset sits under a project, which sits under a business unit, which sits under an organisation. Reports and dashboards group by these, and access can be scoped to them.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → Asset Management → Organization — the top level, and the level at which each asset name must be unique

Set these up before importing assets in bulk

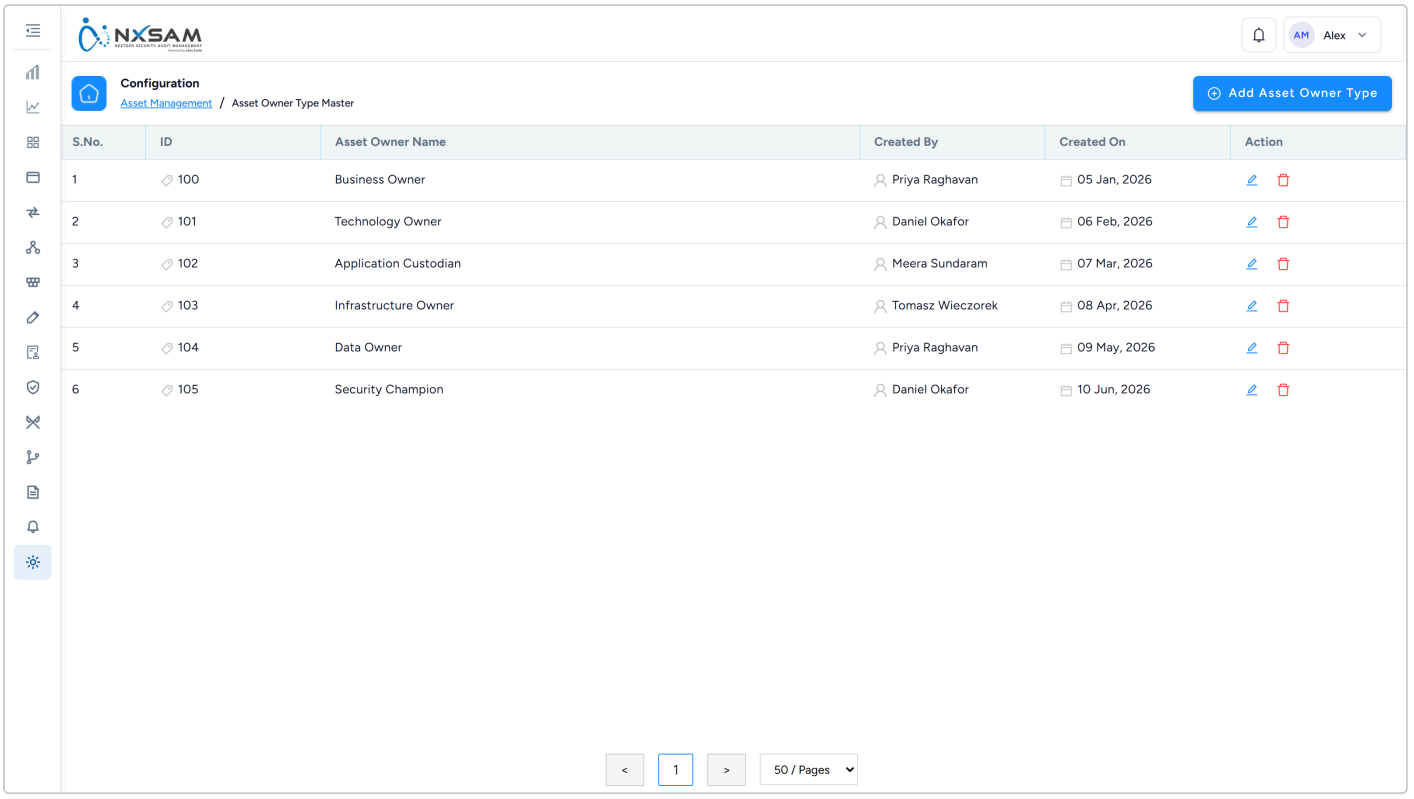
An import that references a project which does not exist yet either creates a placeholder or rejects the row. Creating the structure first avoids both, and avoids a cleanup pass later.

Asset owners

The **Asset Owner Master** holds the people who can be assigned as responsible for an asset. Ownership determines who sees an asset, and who is chased when findings on it approach their SLA.

An owner has to exist here before they can be assigned. Assigning ownership to someone who has left, and never revisiting it, is the most common cause of remediation reminders going nowhere.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → Asset Management → Asset Owner Master

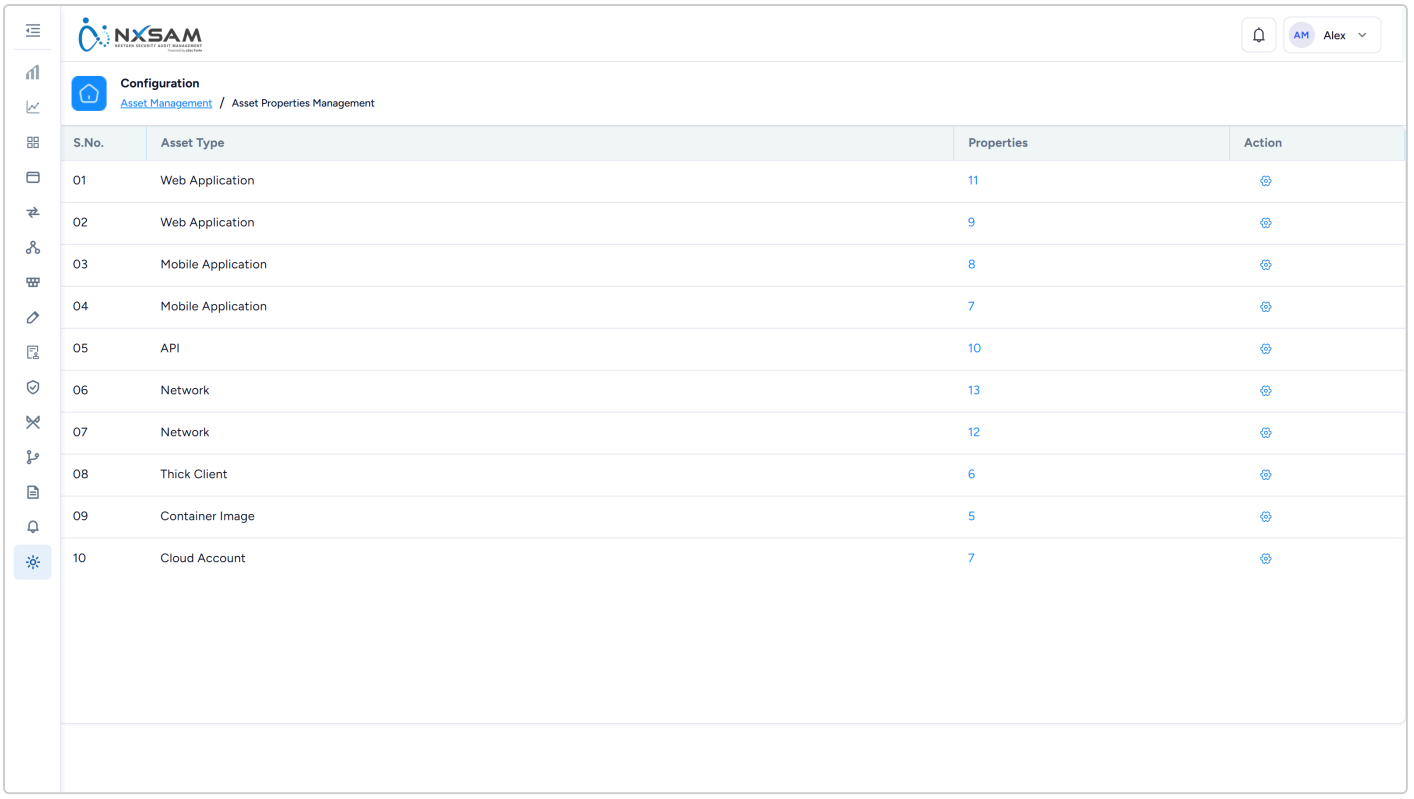
Asset properties

Beyond the built-in fields, you can define **asset properties** of your own — a data classification, a hosting region, a compliance scope. These become filterable and groupable everywhere the asset appears.

Asset Property Management maps which properties apply to which asset types, so a property that only makes sense for network hosts does not appear on mobile applications.

Properties are worth defining early for the same reason as the grouping levels: they apply going forward, and backfilling them across an existing estate is manual.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

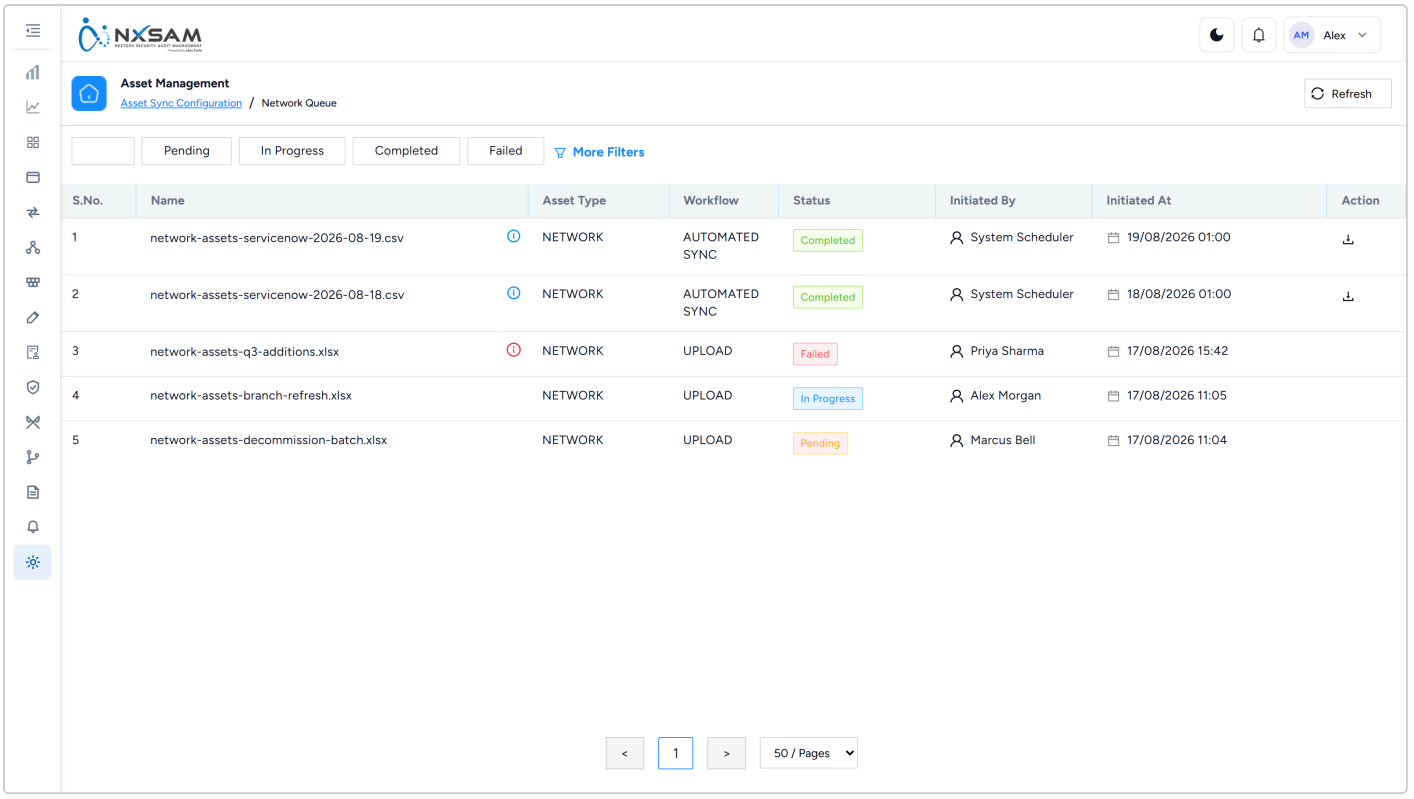


Configurations → Asset Management → Asset Property Management — which properties apply to which asset type

Bringing assets in

Screen	Use
Network asset upload	Bulk-create network assets from a file
Asset sync configuration	Connect a source of truth such as a CMDB
Network asset map	Relate network assets to the applications they host

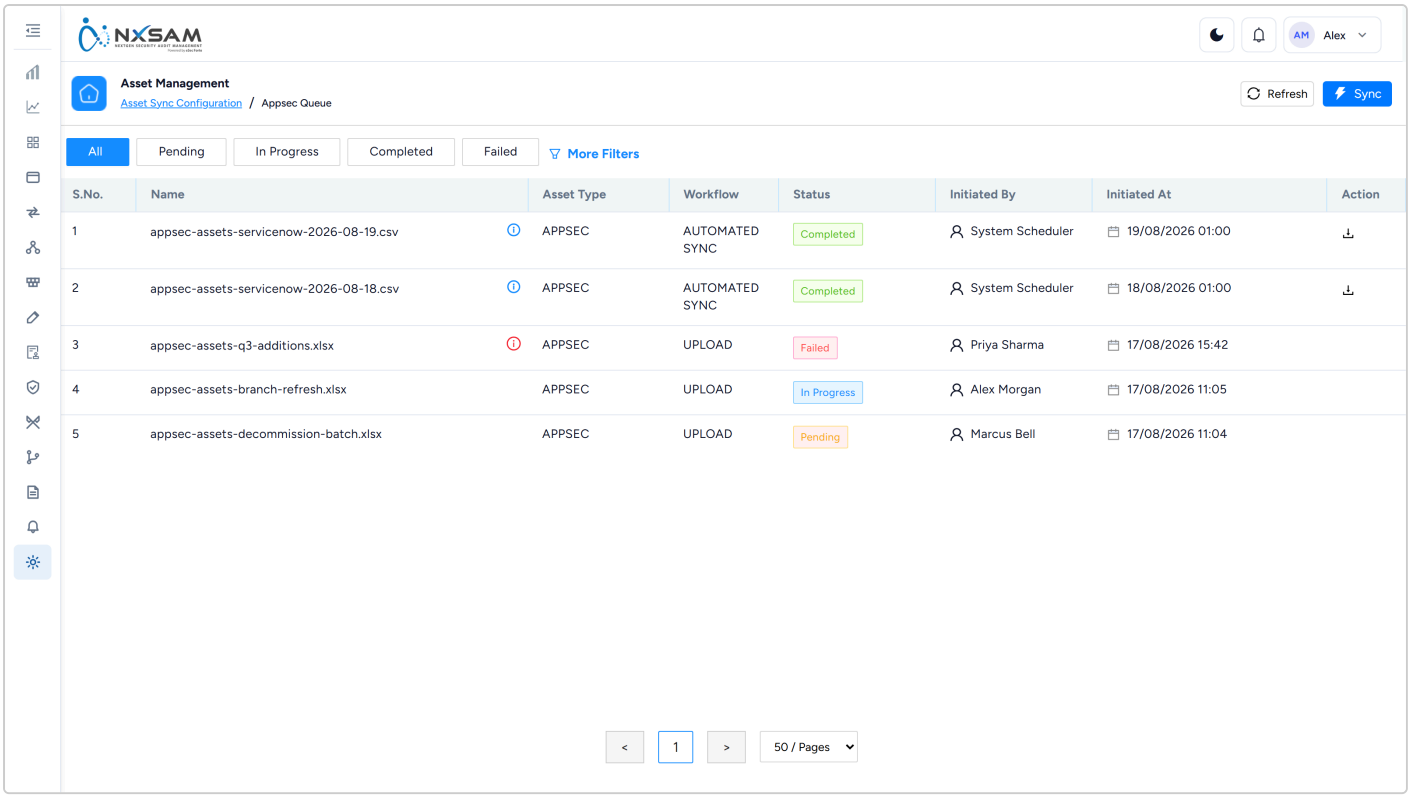
Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → Asset Management → Upload Network Assets

A bulk upload is queued rather than applied on submission, and the queue is where a rejected file explains itself.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → Asset Management → Upload Queue — what each file did, row by row

Where a sync is configured, treat the source system as authoritative. A local edit to a synchronised field is overwritten on the next run, which looks like the platform discarding work.

Decommissioning

Assets that no longer exist should be decommissioned rather than deleted. Decommissioning removes an asset from active tracking while preserving its history, so past findings and the reports that mention them remain intelligible.

Deleting is also a soft operation — the record is hidden rather than destroyed — which is why a deleted asset's name can still appear on historical findings and older reports. That is intentional, and it is not a leak of removed data.

Audit calendar planner

Plans assessments across the estate over a period, so coverage is deliberate rather than whatever was requested ad hoc. Most useful where a compliance obligation requires every asset of a given class to be assessed on a defined cycle — the planner is where you can see whether that is actually happening.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Assets: every screen, column and action

The largest module in the product — 116 columns and 52 row actions across the inventories, the management screens and the queues. Everything below is taken from the templates.

The asset inventories

Web, Mobile, Thick Client, Network, API and Container each have their own list. The four application-style inventories share a column set:

Column	What it holds
Application Details / **Assets Details**	Name, identifier and type
Risk Score	The contextual score, not raw severity
Project	Which project the asset belongs to
Audits / **Active Audits**	How many assessments exist against it
Total	Open findings
Critical / High / Medium / Low / Info	The severity split of those findings

The severity columns are labelled from the severity master, so an organisation that renames or recolours a severity sees the change here without any configuration on this screen.

App Code

Every application-style asset carries an **App Code** — your organisation's own identifier for the application, as used in your CMDB, your change process or your finance system. It is not generated by NxSAM.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

It exists so that a finding can be traced back to the system of record everyone else uses. Asset names drift (a portal gets renamed, an acquisition rebrands); the code usually does not, which is why reports, host selections and exports all carry it.

App Code can be made mandatory, and usually should be

A system setting makes App Code required when onboarding an asset. Left optional, it gets skipped during a bulk import and the gap is invisible until someone tries to reconcile findings against the CMDB months later and finds half the estate unmatched.

Turning it on later does not backfill the assets already created without one.

Network assets replace **Project** with **Application Count** — how many applications run on the host — because a host's importance follows from what it carries.

API assets replace the severity columns with **API Collections Details** and **Description**, since an API asset is a collection of endpoints rather than one deployable thing.

Container assets show **Registry / Repository**, **Org**, **Vulnerability**, **Compliance** and **Collections** — the image coordinates instead of a name.

Row actions on an application asset — ten

Action	What it does
View Web Application / **View Mobile Application** / **View Thick Client**	The asset's full record
View Overall Details	Findings and audits across the asset's whole history
Edit Web Application / **Edit Mobile Application** / **Edit Thick Client**	The asset's own fields
Edit Ownership	Who is responsible — drives visibility and chasing
Edit Tags	Labels used for grouping and reporting

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Action	What it does
Add/Download Document	Attaches or retrieves supporting files
Risk Score Overview	How the score was arrived at, factor by factor
Download Overall Report	A report covering everything known about the asset
Delete Application	Soft delete

An asset's type is fixed once it is created

The type decides which module assesses the asset and which scanners can contribute findings to it, so it is set at creation and not changed afterwards. If an asset has been classified wrongly, create it under the correct type rather than looking for a way to move it — findings already recorded stay attached to the asset as it was classified.

Use it to correct a mistake made at onboarding, not to reorganise a working estate.

Risk Score Overview is the answer to "why is this asset ranked above that one". The score combines severity with asset context — criticality, exposure, exploitability — and the overview shows the contribution of each. Without it the ranking is unexplainable to the person being asked to act on it.

Network asset actions

Edit Network Asset, **Edit Network Asset Owner**, **Edit Tags**, **Risk Score Overview**, **Download Overall Report**, **Delete Network Asset**, and **Request VA Audit** — which creates a VA audit against the host without leaving the inventory. That last one is the normal path from "this host looks wrong" to "someone is scanning it".

API asset actions

View Overall Details, **Edit Asset**, **Edit Ownership**, **Edit Tags**, **Risk Score Overview**, **Download Overall Report**, **Delete Asset**.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Page-level actions on an inventory

Action	What it does
Import Hosts	Bulk-creates network assets from a file
Update Asset Properties	Sets custom properties across selected assets at once
Update Application Tags / **Update Host Tags** / **Update Thick Client Tags**	Bulk tagging
View Queues	The status of bulk operations started from this screen
Generate Application Summary	Per-application summary report
Generate Detailed Summary	The long form
Generate Issue Dashboard Summary	Findings shaped for a dashboard view
Generate Wise Summary	Grouped summary across the inventory

Bulk updates are queued, and View Queues is where they report

Updating properties or tags across a selection does not complete when the dialog closes. It queues, and the result — including rows it could not apply to — appears under **View Queues**.

A bulk update that "did not work" has usually finished with rejections nobody read.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Asset detail views

Opening an asset shows its audits:

Latest audit details — `Audit Details`, `Start Date`, `Audit status`, `Audit testing methodology`, `Audit type`, `Type / Methodology`, `Audit Considered`.

Active audit details — `ID`, `Audit Name`, `Start Date`, `Audit status`, `Audit type`, `Audit Cycle`.

Audit Considered on the latest-audit view is the field that explains a dashboard disagreement: an asset whose most recent audit is not considered contributes its previous audit's numbers to aggregate views.

Overall details for one asset

Opened from **View Overall Details**. It gathers everything known about the asset in one place, across every audit it has ever had:

Section	What it holds
AUDITORS	Everyone who has assessed this asset, from `auditors`
Best Practice	Findings raised as recommendations rather than defects
Port / Protocol	For network assets, where each finding was observed

Best Practice findings are the ones people argue about. They are not vulnerabilities — nothing is exploitable — but a hardening recommendation the assessor considered worth recording. They carry no SLA and should not be counted as an open risk, which is why they are separated here rather than mixed into the finding list.

AUDITORS matters on a re-test dispute. When a finding closed by one assessor is re-opened by another, this is where you see that two different people assessed the same asset — which is frequently the explanation.

Ownership

User name and **Owner Type**, multi-select. An asset can have several owners of different types — a technical owner and a business owner, for instance — and each type is chased differently when findings age.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Ownership is also visibility: an asset owner sees their own assets and the findings on them. A colleague who cannot see an asset you can is an ownership question, not a permissions fault.

The organisational hierarchy

Screen	Columns
Organizations	`ID`, `Organization Details`, `Network asset uniqueness`, `API asset uniqueness`, `Status`
Business Units	`ID`, `Business Unit`, `Organisation`, `Created By`, `Status`
Projects	`ID`, `Business Unit`, `Project Details`, `Organisation`, `Status`

⚠ Asset uniqueness is set per organisation and is hard to change later

Network asset uniqueness and **API asset uniqueness** decide whether the same host or endpoint can exist twice within an organisation. Set it to unique and a second import of the same IP updates the existing asset; set it to non-unique and it creates a second one.

Changing it after assets exist does not merge or split what is already there. It only changes what the next import does, which is why two environments with the same data can end up with different asset counts.

Asset properties

Screen	Columns
Asset Properties	`Property Name`, `Property Type`, `Created By`
Asset Property Management	`Asset Type`, `Properties` — which properties apply to which type

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Screen	Columns
Manage Properties (dialog)	`Property Name`, `Property Type`, `Sequence`, `Mandatory`

Mandatory and **Sequence** are set per asset type. A property marked mandatory blocks asset creation until it is filled, which is the usual reason a bulk import starts rejecting rows after someone edits the property configuration.

Asset owner types

`ID`, `Asset Owner Name`, `Created By`, `Created On`. The catalogue of ownership roles that can be assigned — technical owner, business owner, and any others your organisation defines.

Network asset mapping

View mapped network asset — `ID`, `Host`, `Risk Master`, `Total`, `Critical`, `High`, `Medium`, `Low`, `Info`.

Update network assets — `Network Asset ID`, `Host IP/Host Name`.

Mapping relates an application to the hosts it runs on, so an application finding can be traced to infrastructure and a host's risk reflects what it carries.

The import and sync queues

Four tabs, because assets arrive four ways.

Tab	Columns
AppSec	`Name`, `Workflow`, `Asset Type`, `Status`, `Initiated By`, `Initiated At`, plus `Properties`, `Header`, `Default Value` for the column mapping
Network	The same set
CMDB	`Sync Type`, `Status`, `Initiated At`, `Completed At`

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Tab	Columns
ServiceNow	`ServiceNow Table Name`, `Asset Sync Type`, `Network Asset Type`, `Status`, then per-module `Module`, `Status`, `Initiated At`, `Completed At`, `Logs`

The ServiceNow tab filters by **All**, **Appsec Assets** or **Network Assets**, because one sync can populate both and they succeed independently.

Mapping a ServiceNow table

A ServiceNow sync is configured per table: which of its records to take, which of its fields feed which NxSAM property, and how to translate values on the way in. The mapping screen has five tools, and most "the sync imported the wrong thing" questions are one of them set wrongly.

Tool	What it does
Header Mapping	Pairs each NxSAM **Property** with a **ServiceNow Field**. Click a field cell to pick from the table's own fields; **Fetch a sample** lists them with a **Sample Value** each, and marks a **SUGGESTED** match where the names line up. A **Static property** takes a fixed **Default** instead of a field
Reference fields	A field marked **REF** points at another record. The mapping asks *which attribute of the linked record to store* — its display value, or a specific attribute — rather than the raw reference
Fallback fields	A property can read from an ordered list of fields; the first non-empty one wins. Where every field in the list is empty, the property's own default applies
Where Condition	Filters which records sync, per property: match **ALL** or **ANY** of a set of conditions, each a **Match** or **No match**. It can be tested against live data before saving
Value Mapping	Translates a field's *source values into NxSAM values* for choice-type properties, so a value ServiceNow spells one way lands as the option NxSAM recognises. The source side offers the values actually present in the column, and accepts a typed value for ones not yet seen

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Data Preview shows what the mapping would produce — the **Resolved values** for a page of records, with **VISIBLE** and **HIDDEN** columns and a search — and can export it, with the time of the **Last export** shown. Preview before the first sync, and again after any change to a where condition or value mapping: a sync that imports ten thousand rows is much harder to undo than a preview that shows ten.

A fallback chain is why a field can be populated from a column nobody mapped

When the first field in a chain is empty, the sync reads the second, then the third. An asset whose IP "came from the wrong place" usually has an empty primary field and a populated fallback — which is the chain working as designed. Check the chain before checking the data.

For application assets, the sync can **Auto-Create Application** records for CIs with no match, **Auto-Generate App Code** where the source has none, and **Auto-Update Empty App Code** on records that already exist without one. Each is a switch on the sync setting, off by default, because each one creates or changes records rather than merely reading them.

Header and **Default Value** in the file-based tabs are the column mapping: which column of the uploaded file feeds which property, and what to use when it is empty. A default value quietly applied to thousands of rows is a common source of "why do all our assets say the same thing".

Decommissioning

Column	What it holds
Decommission Asset ID	The request
Initiator	Who raised it
Status	Where the request has got to
Pending On	Who it is waiting for

Actions: **Edit Decommission**, **Update Initiator**, **View Status History**, **Delete Decommission Request**.

Decommissioning is a request with an approval chain rather than a delete, because removing an asset from tracking changes historical reporting. **Pending On** is what you check when a request has stalled.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The selection screens list `Assets`, `Asset Type`, `Organisation`, `Business Unit`, `Project` so the right assets are chosen before the request is raised.

Audit Calendar Planner

Plans assessments across the estate so coverage is deliberate.

Column	What it holds
Planner Details / Description	The plan
Created By / Updated On	Provenance
Selected Assets & Audit Type	What is planned against what
Assets	How many are in the plan
Progress	How much of the plan has been executed
Status	Plan state

Actions include **Choose Audit type to assets**, **View All Selected Assets**, **Sync** and **Delete Audit**, with the audit type chosen from **VA**, **PT**, **Black Box**, **Grey Box** and **White Box**.

Sync is what turns the plan into real audits. Until it runs the planner is an intention; after it runs the audits exist and appear in their modules.

The supporting tables list `Assets`, `Organisations`, `BUs`, `Projects` when adding, and `Asset Details`, `Audit Type`, `Organisation`, `Project`, `Bu`, `Status` when reviewing what was selected.

Dashboard views

Manage Dashboard Views — `Name`, `Created By`, `Created On`. Each view is a saved profile deciding which sections and widgets the Assets dashboard shows, and which filter it opens with.

Creating one is three decisions:

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Decision	What it controls
Asset types	Which of Web, Mobile, Thick Client, API, Network and Container the dashboard covers. At least one is required
Sections	The panels shown — Overall, Network VA, Network PT, Policy Config and the per-asset-type sections. Each section can be expanded to pick its sub-sections individually
Filters	Organisation, business unit and project the view opens with, plus anything under More Filters

A view is **Private** unless you make it otherwise, so building one is safe: it changes nothing for anyone else until you share it.

Each row carries up to five actions, and which of them appear tells you what kind of view it is:

Action	Available on
Preview Dashboard	Every view, including the system one — the safe way to see what a view shows before adopting it
Edit Dashboard	Views you may change: your own private views, or any view if you hold the update permission. Never the system view
Make Public	A private view you may change. It publishes the view to everyone
Make Default	Any view, with the permission. Greyed out on the view that is already your default
Delete Dashboard	Any view but the system one, with the permission

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Publishing is one-way on this screen

There is a **Make Public** action and no matching action to make a view private again. If one was published prematurely, deleting it and rebuilding is the route back — so preview it and check its filters before publishing rather than after.

The **system** view is the platform's own default. It cannot be edited, published or deleted, which is deliberate: it is the arrangement everyone falls back to, and it stays recognisable.

Two things are worth knowing before you build one. The dashboard renders a heading for every enabled section, so a view with everything enabled produces a long page where most sections are empty — enabling only what a team looks at is what makes the view useful rather than complete. And the saved filter is part of the view: a view scoped to one business unit will always open scoped to it, which is the point, but it also explains a colleague's "the totals are too low" when they are using someone else's view.

Both dashboards export via **Download as PDF** / **Download as PNG**, and the asset dashboard through **PDF** / **PNG**.

Change accessibility

`Asset ID`, `Asset` — bulk-sets whether assets are externally or internally reachable. Accessibility drives prioritisation in Network PT, where an external Medium usually outranks an internal High.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

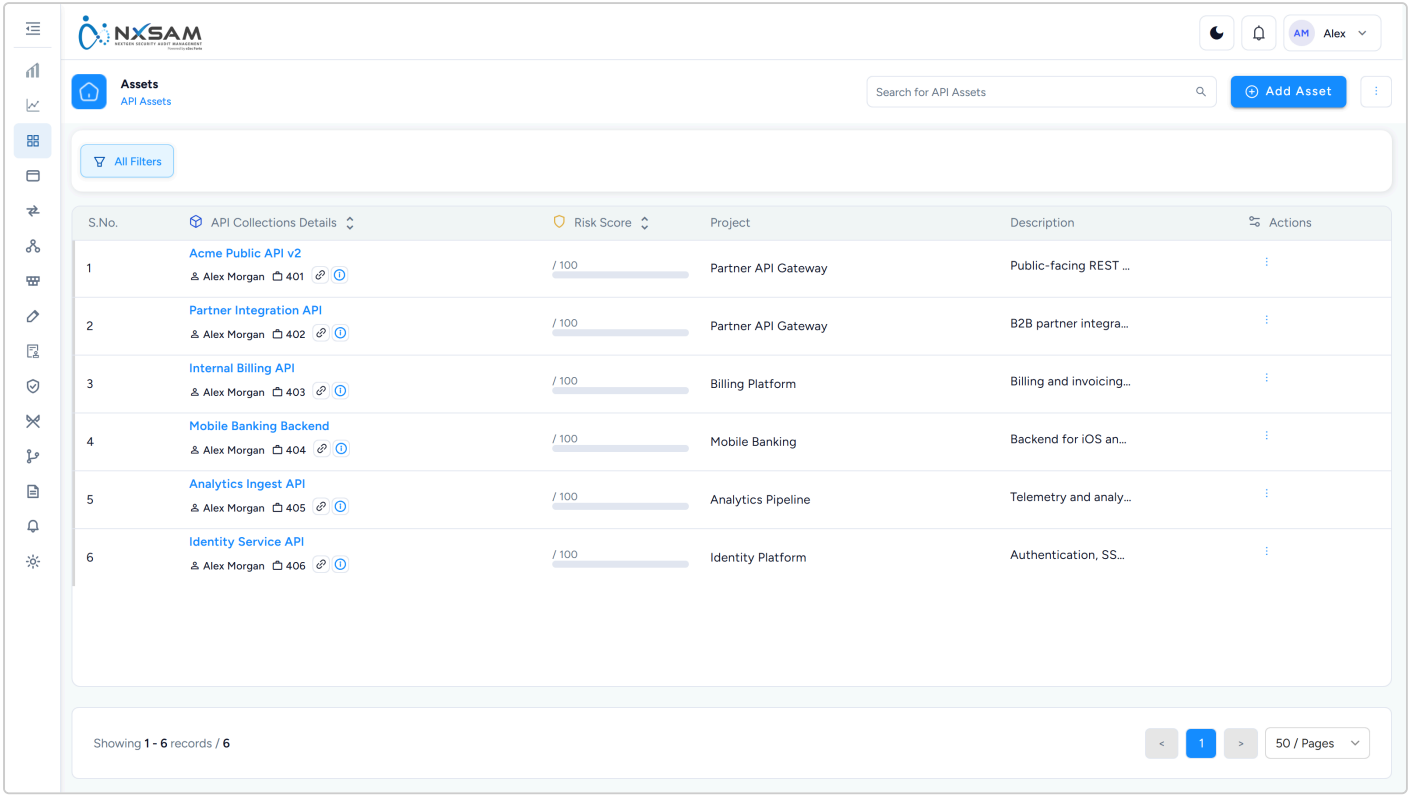
Assets: find the right screen

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.

API Assets

Service endpoints assessed separately from the applications that consume them.

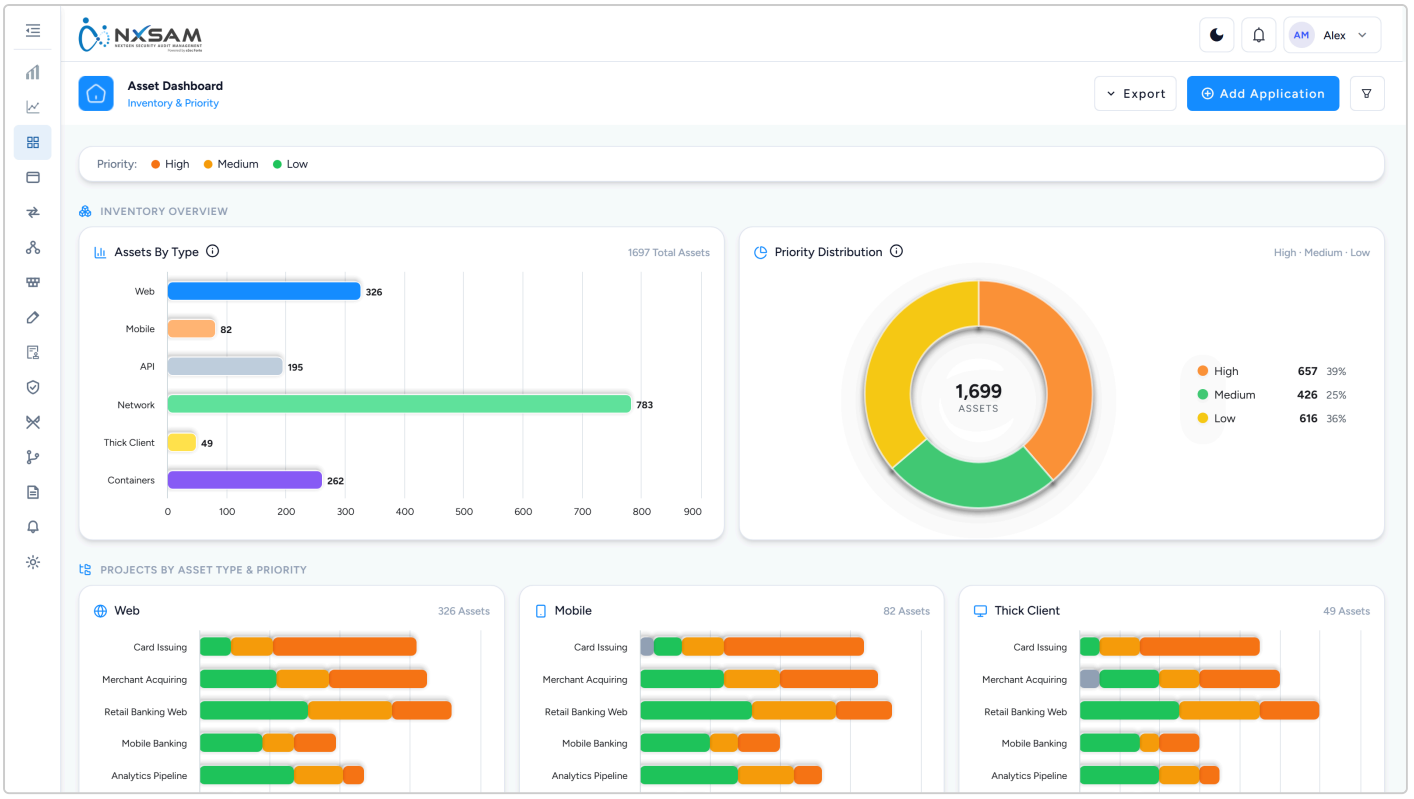


Assets → API Assets

Asset Dashboard

How many assets of each type, and how their criticality is spread across projects. The split matters more than the totals — it shows where the important assets actually sit.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

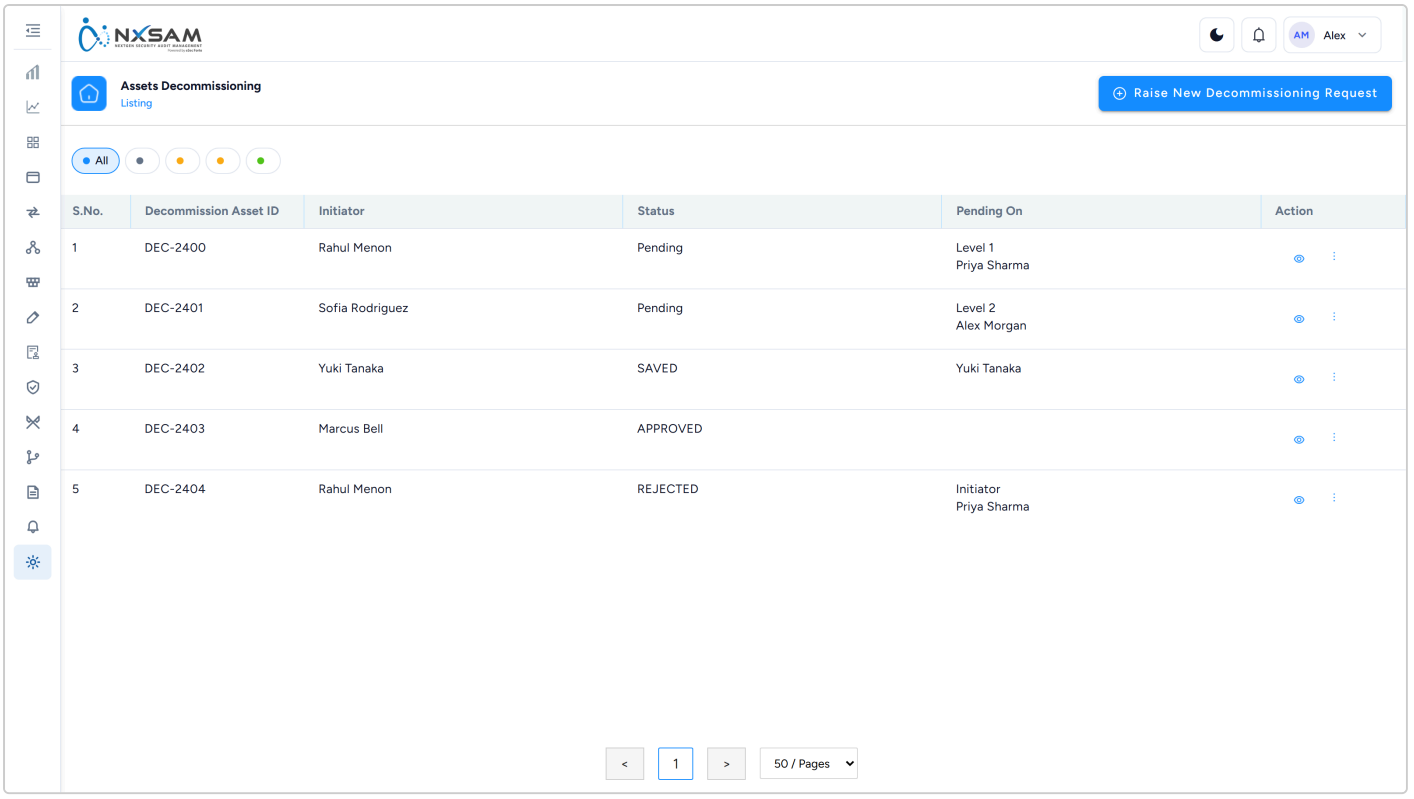


Assets → Asset Dashboard

Asset Decommissioning

Requests to retire an asset, and who each is waiting on. Decommissioning preserves history; deleting hides the record.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

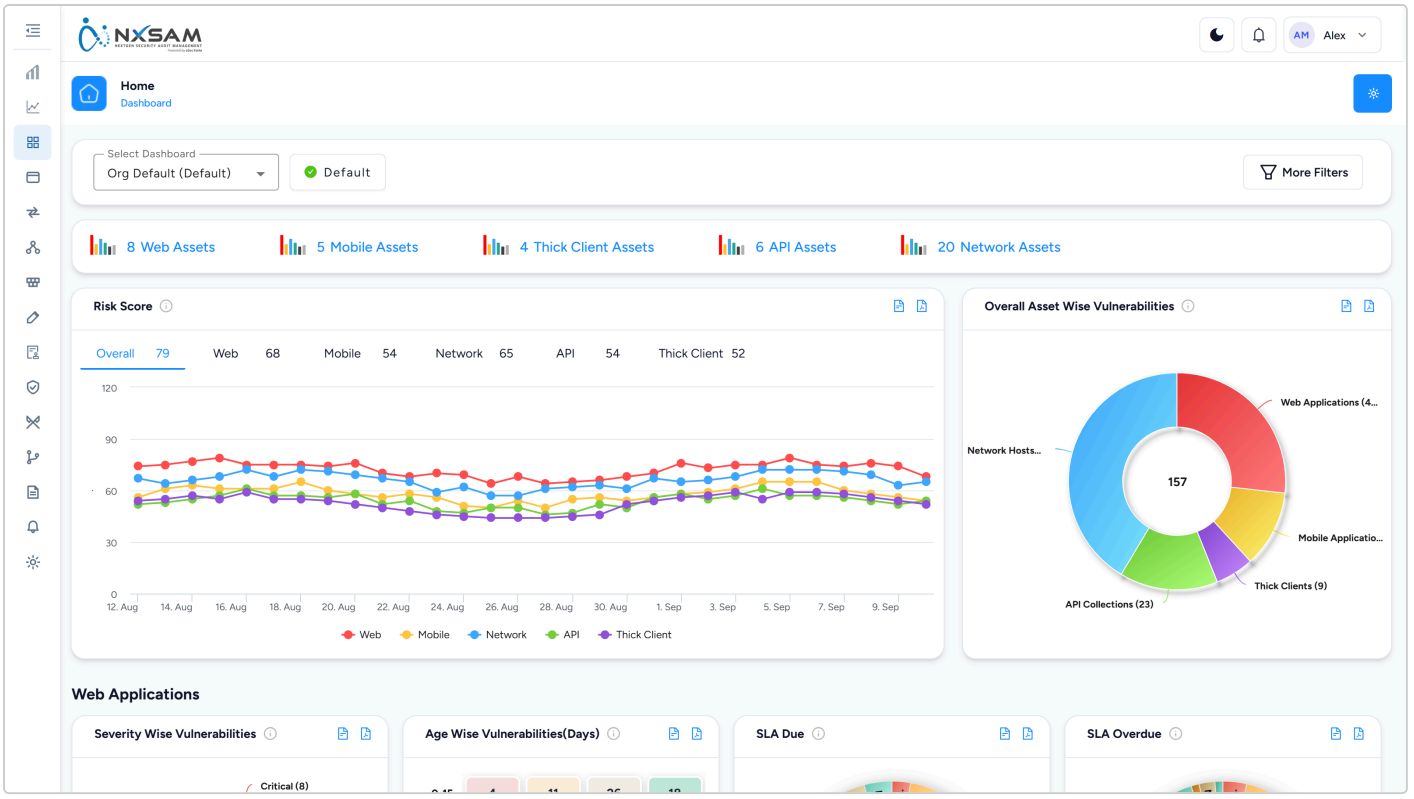


Setting → Decommission → Asset Decommissioning

Asset Main Dashboard

Posture across the whole inventory, sectioned by asset type. Which sections appear is set by the dashboard profile.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

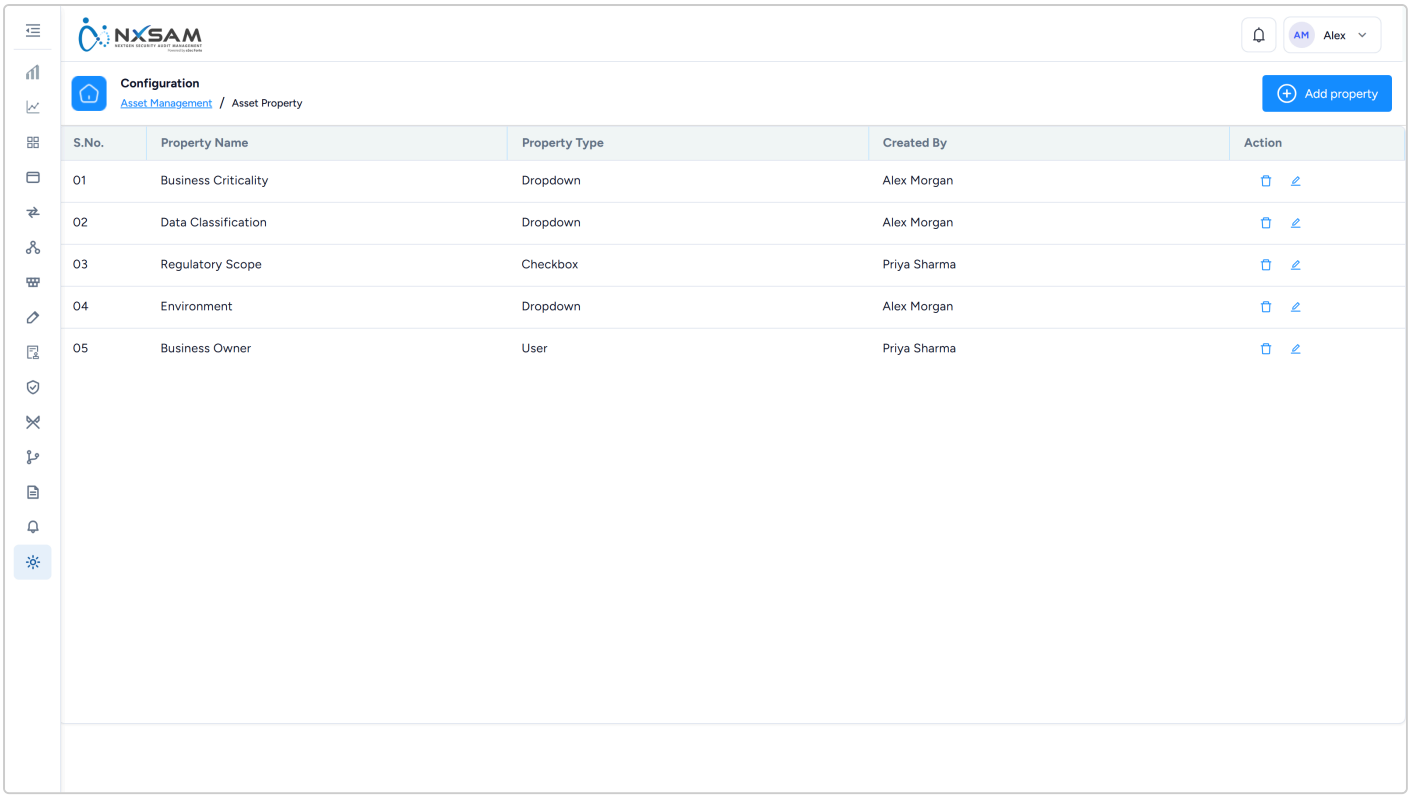


Assets → Main Dashboard

Asset Properties

Custom fields defined on assets — data classification, hosting region, compliance scope. They become filterable everywhere the asset appears.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

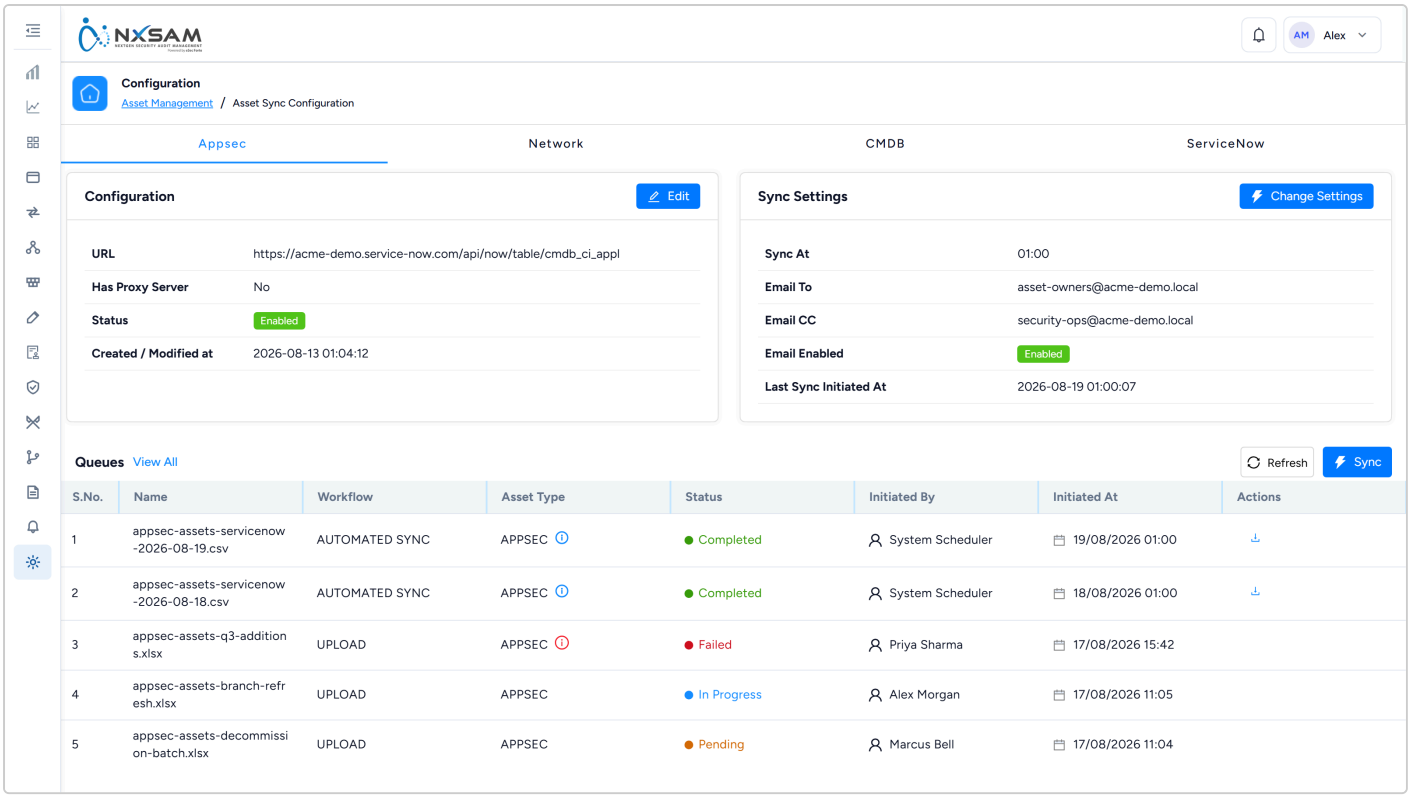


Setting → Asset Management → Asset Properties

Asset Sync Configuration

Maps a CMDB's columns onto NxSAM's asset fields, and sets the schedule. Where a sync is configured, treat the source system as authoritative.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

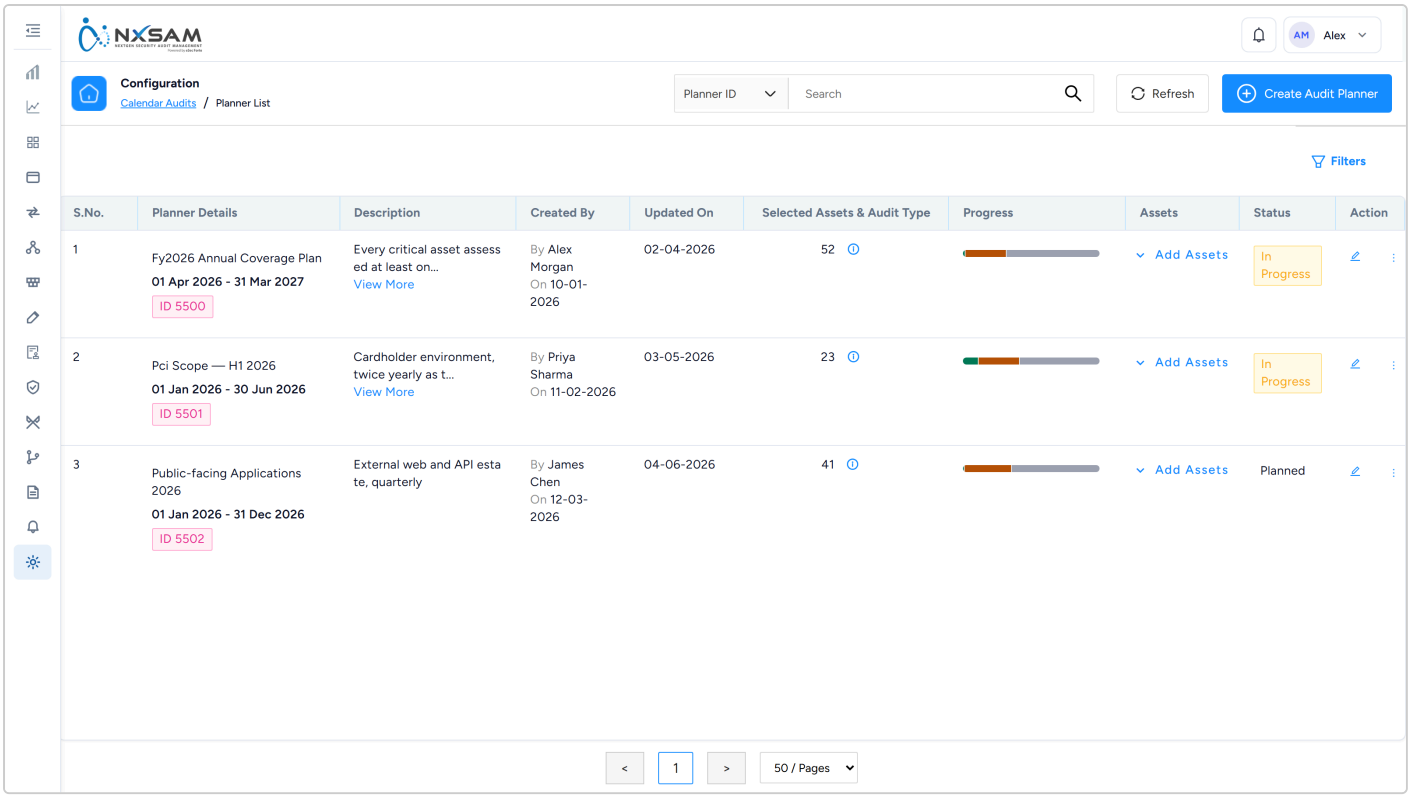


Setting → Asset Management → Asset Sync Configuration

Audit Calendar Planner

Assessment coverage planned across a period. Each plan shows how much of it has been done, so a plan nobody is executing is visible.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

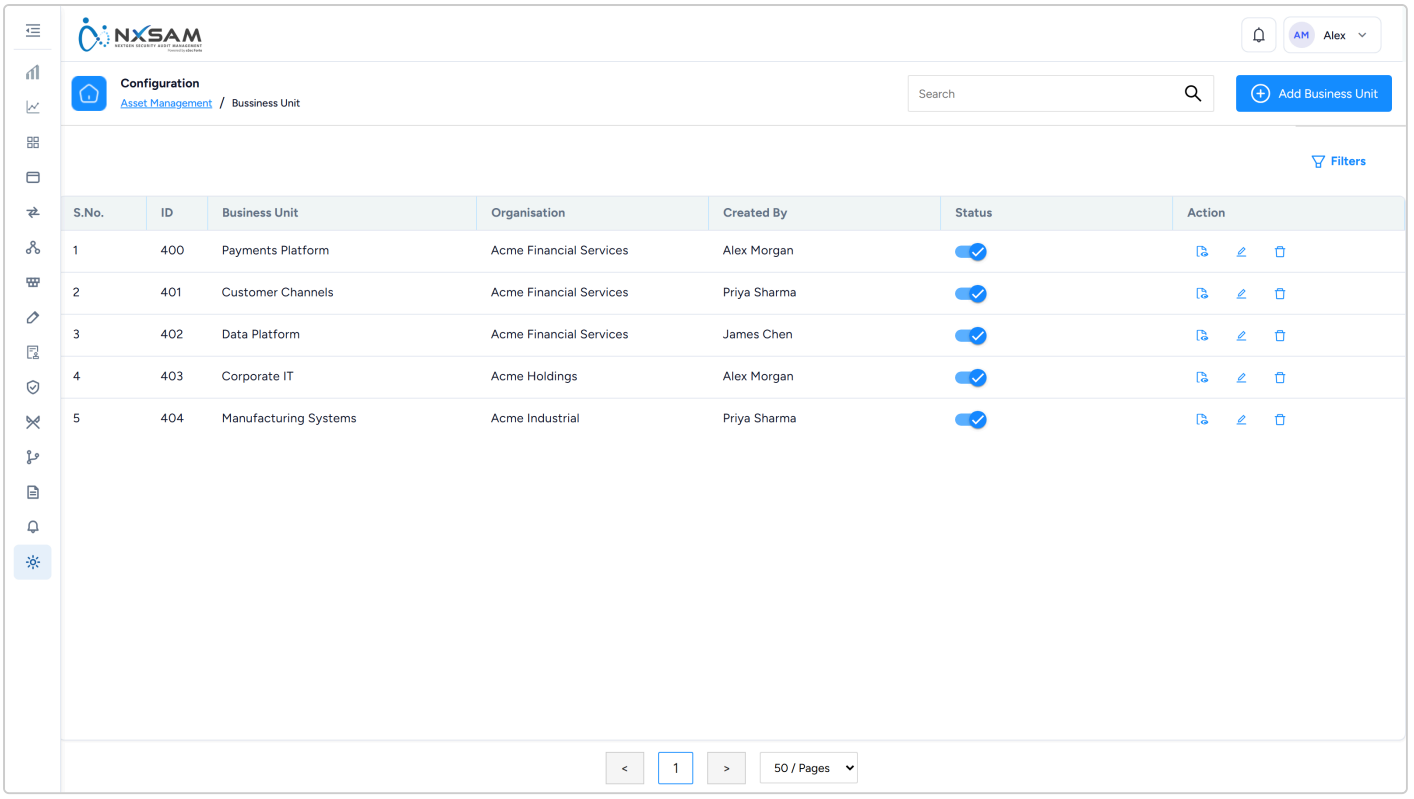


Setting → Audit Calendar Planner → Audit Calendar Planner

Business Units

The middle level of the grouping hierarchy. Every asset sits under a project, which sits under one of these.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

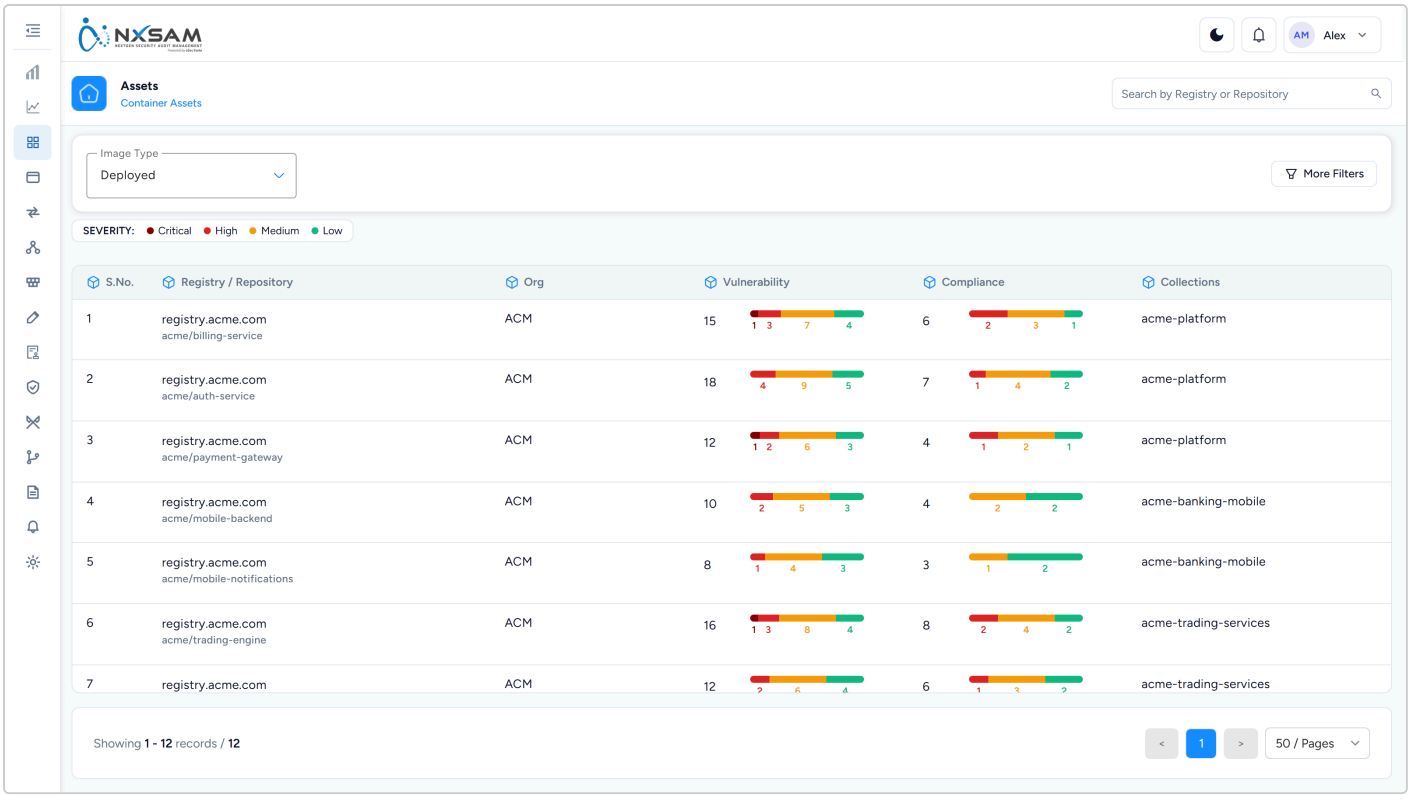


Setting → Asset Management → Business Units

Container Assets

Container images by repository and tag. A tag change is a different asset.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

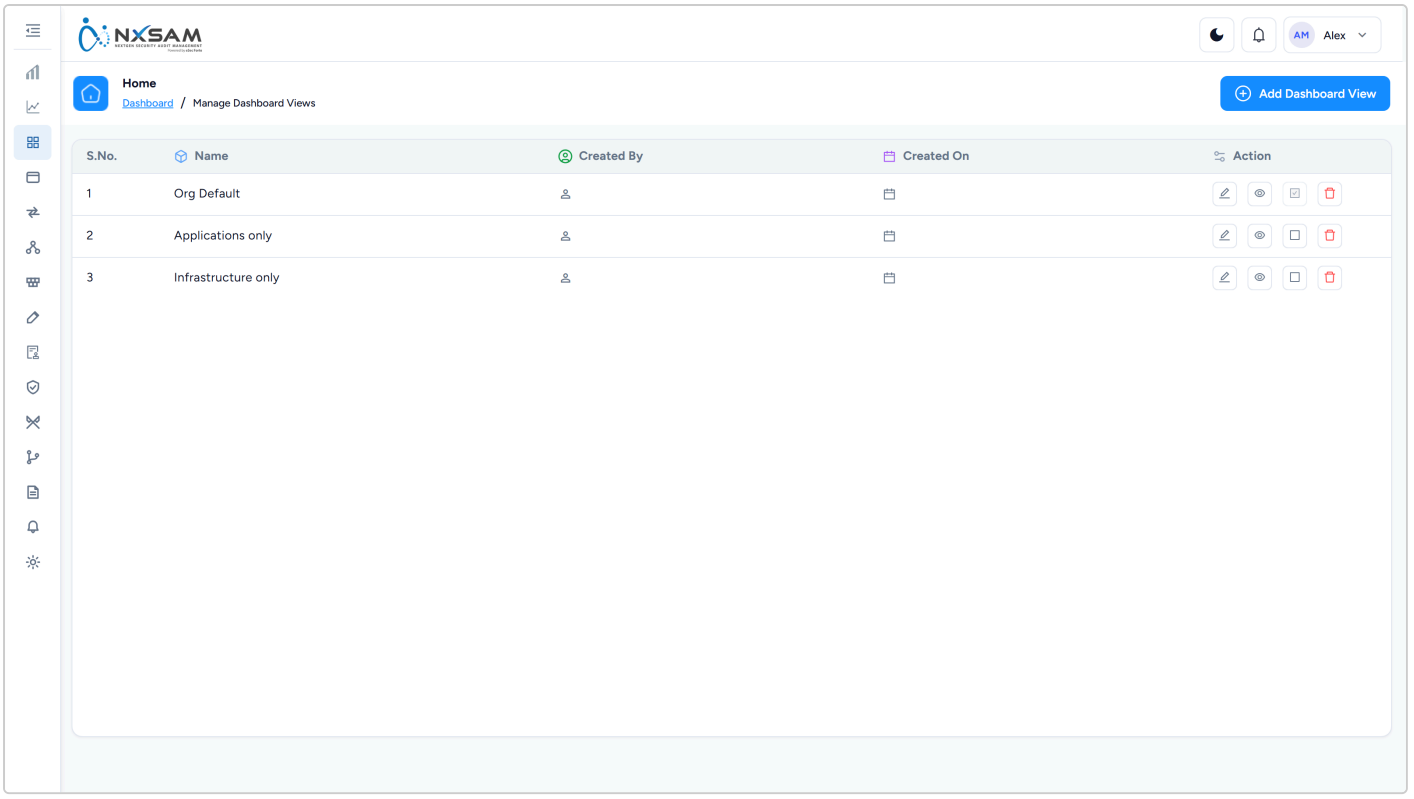


Assets → Container Assets

Manage Dashboard Views

Create and edit dashboard profiles — which sections and widgets appear, and the default filter applied.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

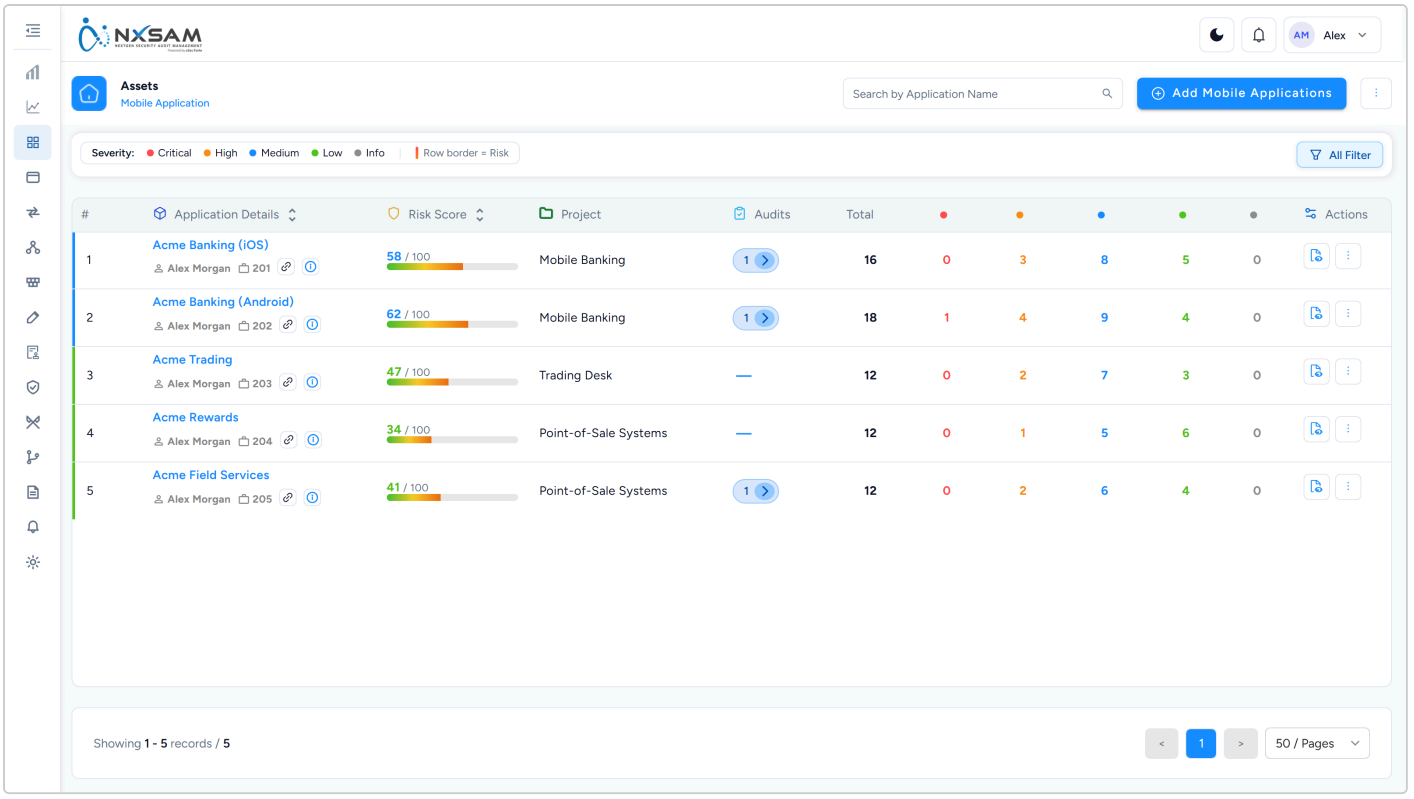


Assets → Main Dashboard → Manage Dashboard Views

Mobile Applications

iOS and Android applications, identified by package or bundle rather than URL.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

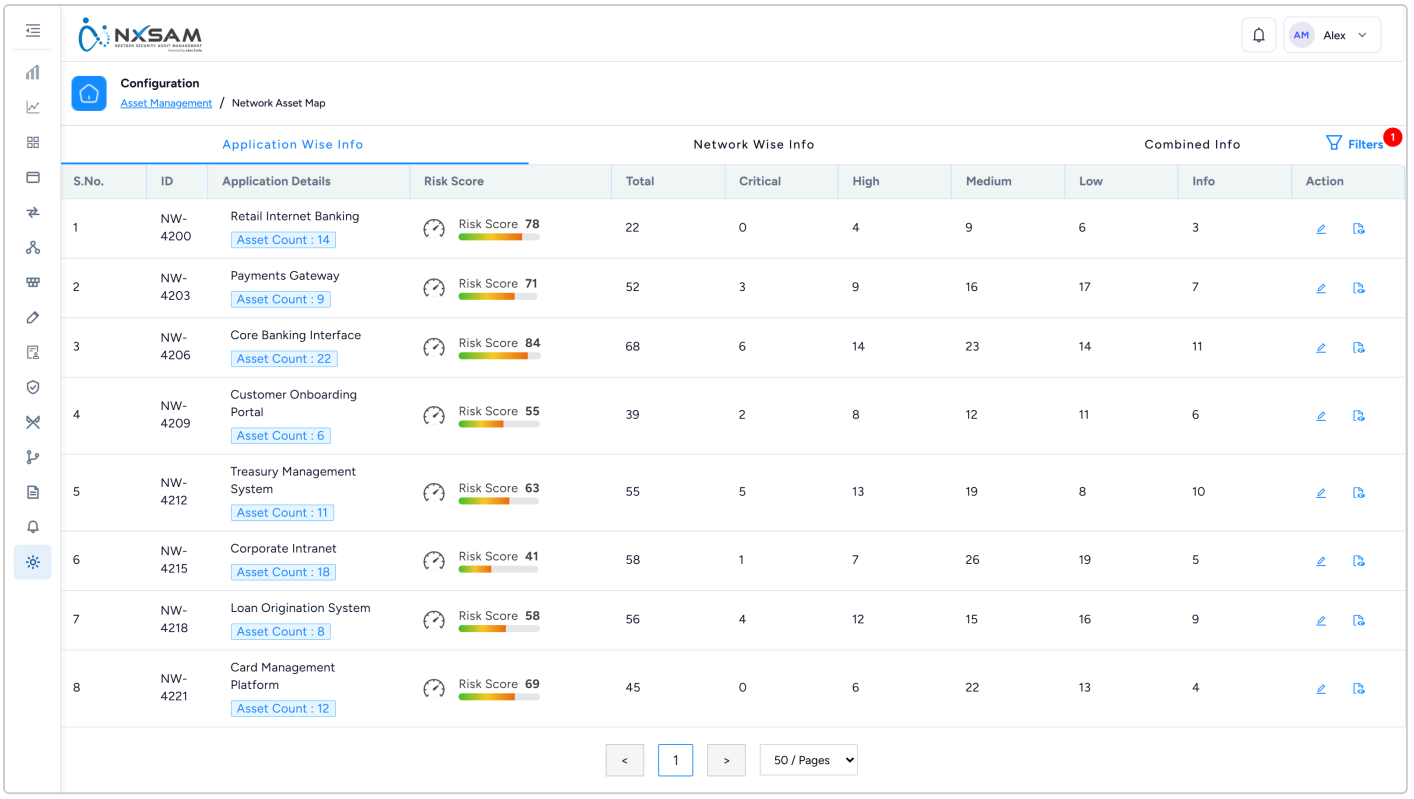


Assets → Mobile Applications

Network Asset Map

Relates network hosts to the applications running on them, so an application finding can be traced to its infrastructure.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

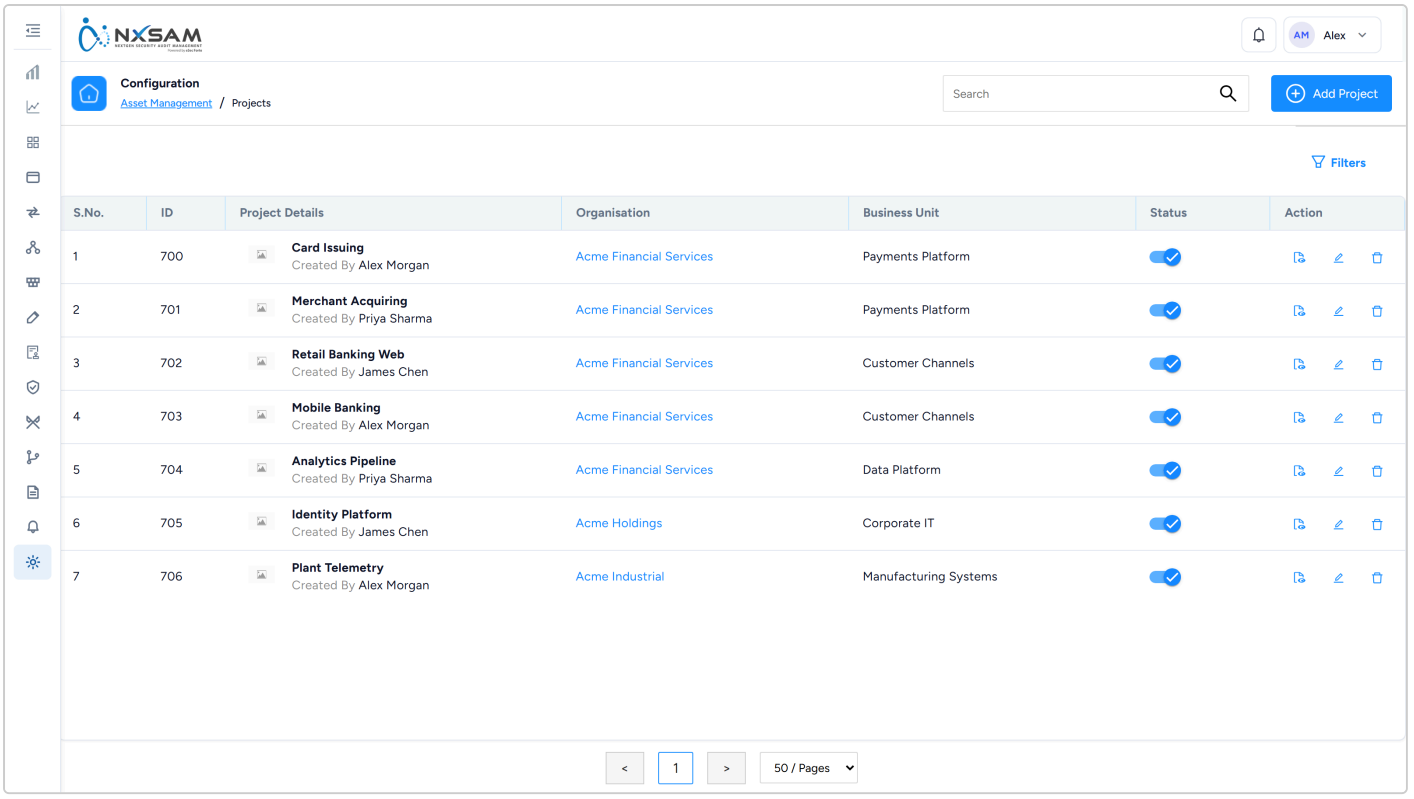


Setting → Asset Management → Network Asset Map

Projects

The narrowest grouping level, and the one most reports group by.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

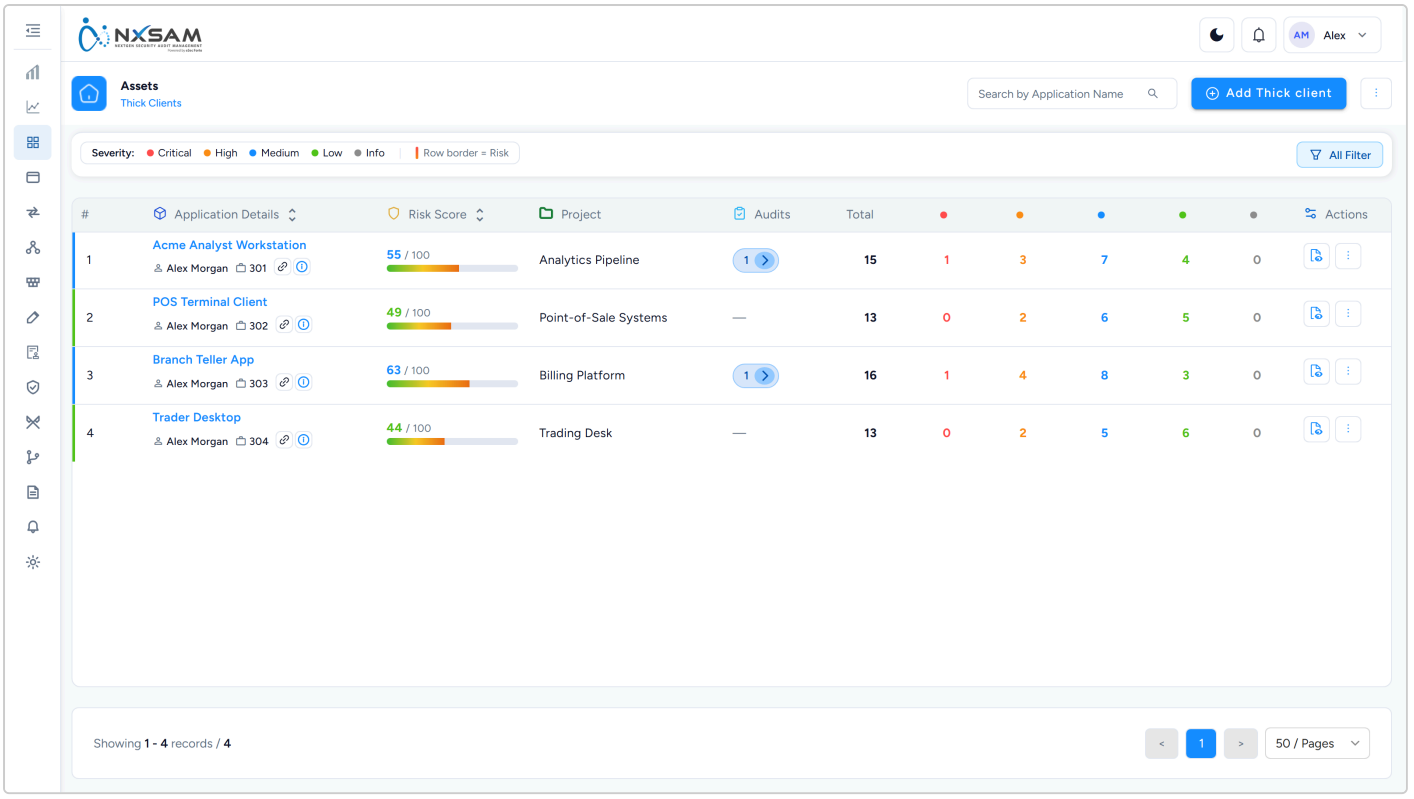


Setting → Asset Management → Projects

Thick Clients

Installed desktop software tracked as assets in their own right.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

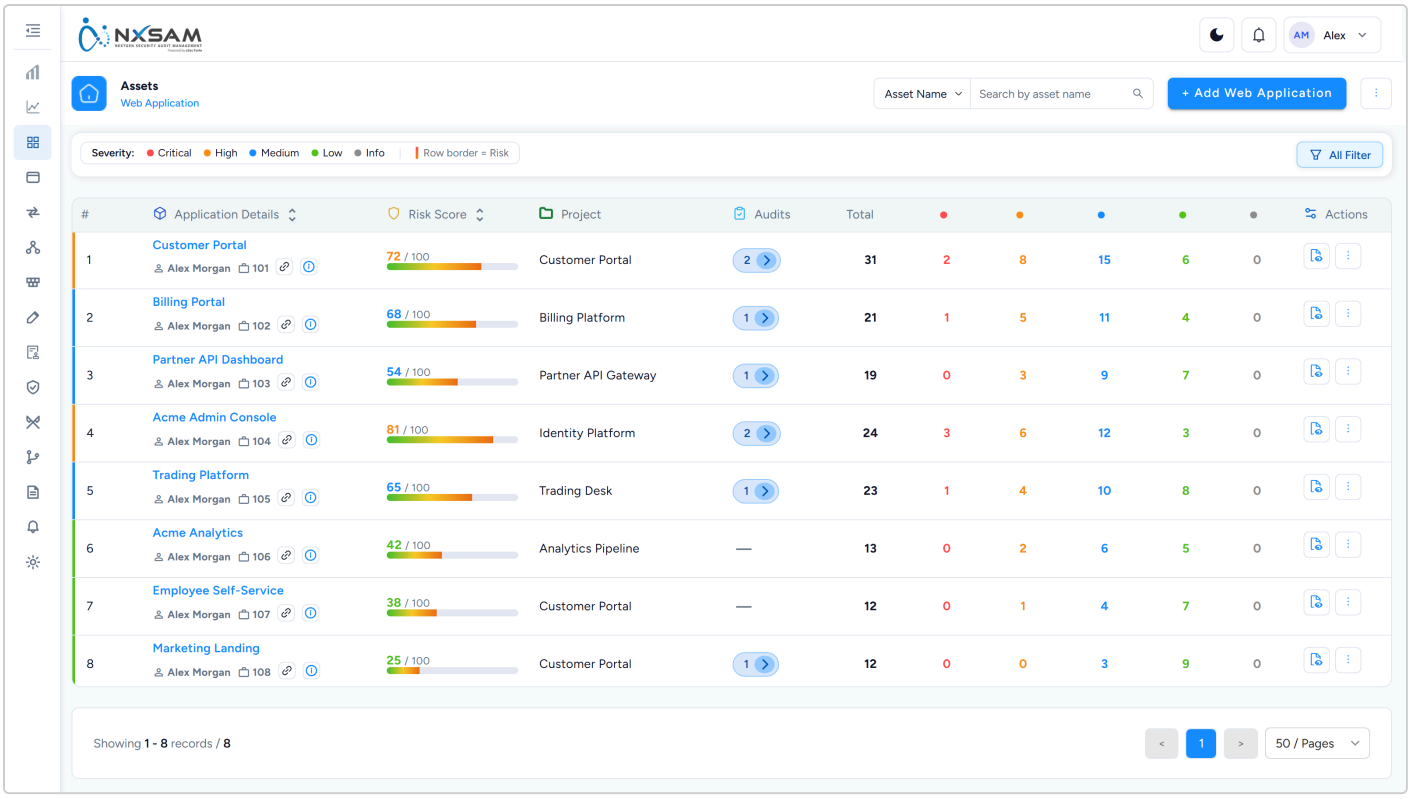


Assets → Thick Clients

Web Applications

The web application inventory. One row per site or web-based system, with its URL and open findings.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Assets → Web Applications

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.