



NxSAM Policy Compliance — Quick Guide

Quick reference guide for the Policy Compliance 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

Policy Compliance

- Overview
- Run a compliance audit, end to end
- Reading the Policy Compliance screens
- Policy Compliance: every screen, column and action
- Policy Compliance: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Policy Compliance

Policy Compliance

Policy Compliance checks that your systems are **configured** the way your standards require. Where vulnerability assessment asks "is anything broken here", policy compliance asks "is this built the way we said it should be".

Configuration, not vulnerabilities

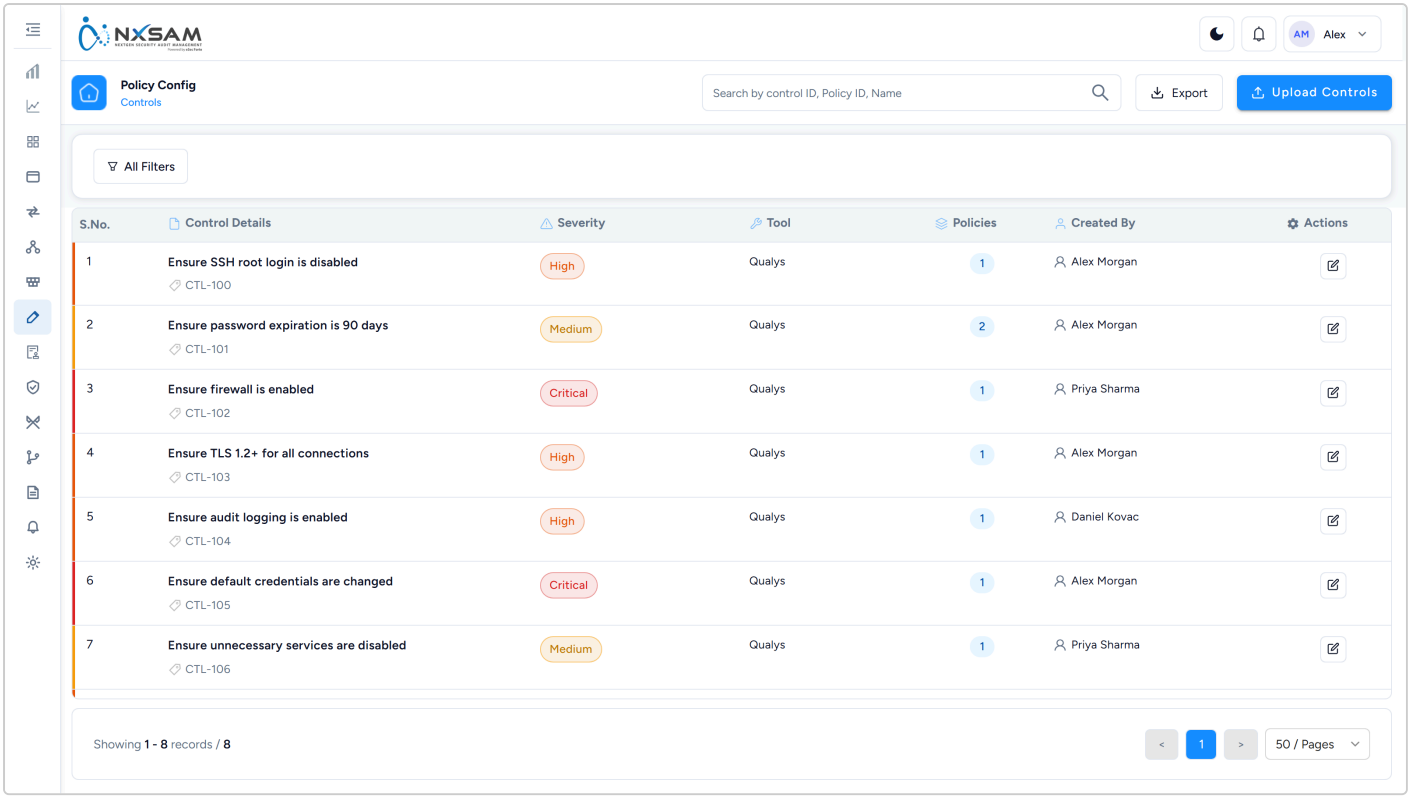
The distinction matters because the two are fixed by different people in different ways.

	Vulnerability	Policy compliance
Typical finding	A missing patch, an exploitable flaw	A setting that does not meet the standard
Typical fix	Apply an update	Change a configuration
Typical source	A vulnerability scanner	A benchmark check
Usually owned by	Application or platform teams	Infrastructure and platform teams

A server can be fully patched and still fail policy compliance — password rules too weak, logging not enabled, an unnecessary service running.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Controls and postures



The control library. Each control is a check with a defined expected state.

A control is a single requirement: "password minimum length is 14". A posture is the observed state of that control on a particular system — met, or not met.

So one control assessed across two hundred servers produces two hundred postures. This is why policy compliance volumes are so much larger than vulnerability volumes, and why the module is built around bulk assessment rather than individual findings.

How assessment works

1. Controls are defined, usually derived from a benchmark such as CIS.
2. An audit applies those controls to a set of systems.
3. Results are imported from the tool that performed the checks.
4. Each control-on-system produces a posture: compliant or not.
5. Non-compliant postures are remediated and reassessed.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reading the numbers

Compliance is usually expressed as a percentage — compliant postures over total postures. Two things to keep in mind when reading it:

- **The denominator moves.** Adding systems or controls changes the total, so the percentage can fall without anything getting worse.
- **Not all controls matter equally.** A high overall percentage can still hide failures on the controls that matter most. Read the failures, not only the ratio.

> **Reassessment is what changes a posture**
>
> Fixing the configuration does not update NxSAM. The system must be checked again and the result imported. Between the fix and the next assessment, the posture legitimately still shows as non-compliant.

Working effectively

- Group by **control** rather than by system when one setting fails widely — that is a single configuration-management fix, not hundreds of separate ones.
- Prioritise by the sensitivity of the systems affected, not by count alone.
- Where a control genuinely cannot be met on a given system, record the exception deliberately rather than leaving it perpetually failing.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Run a compliance audit, end to end

Policy Compliance counts differently from every other module, and the differences matter from the first step. Read how the numbers work alongside this if the counting is new to you.

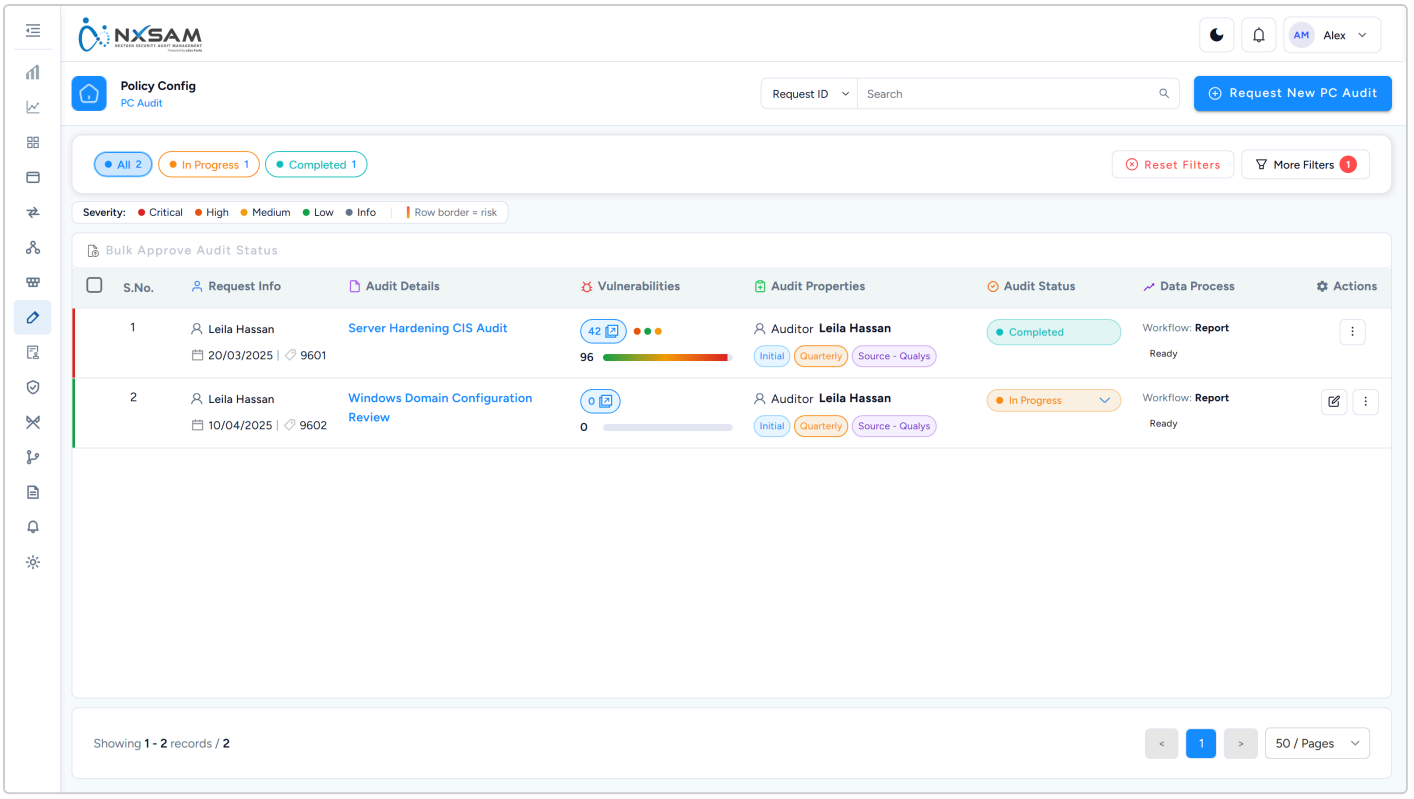
Before you start

You need	Why
The benchmark being assessed	It decides which controls apply
The host list in scope	Scope here is hosts, not applications
Working scanner credentials on those hosts	A failed check returns **error**, not **fail**

1. Create the audit

Policy Config → PC Audit → Request New Audit.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Policy Config → PC Audit

---

2. Set the scope

Add the hosts through host selection. **Export IPs** downloads the list — keep it, because compliance scope disputes are settled by comparing it against the benchmark tool's own target list.

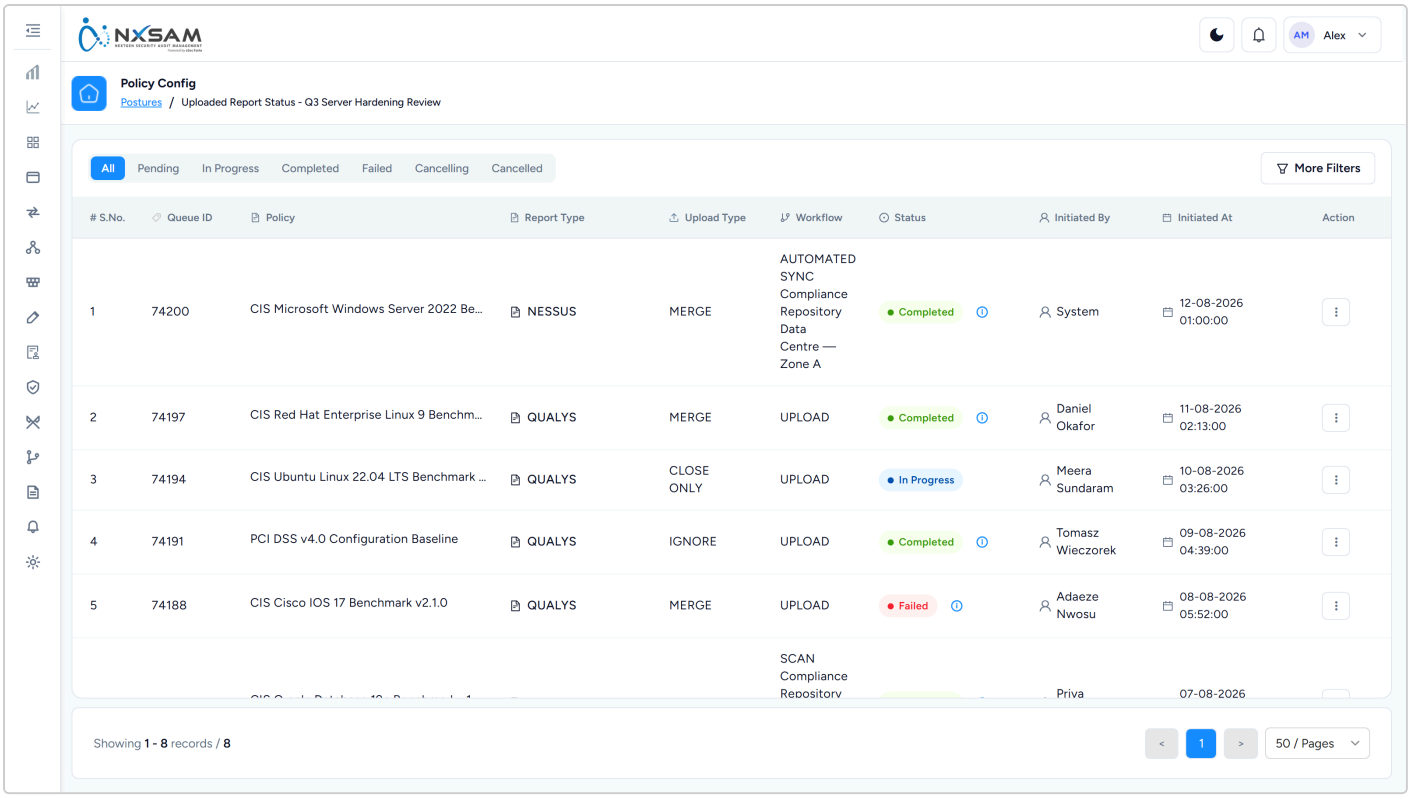
Hosts that genuinely do not apply belong in **excluded assets**, each with a **Comment** giving the justification. An exclusion without one is the first thing an external auditor questions.

---

3. Upload the results

Uploads are queued rather than applied immediately.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



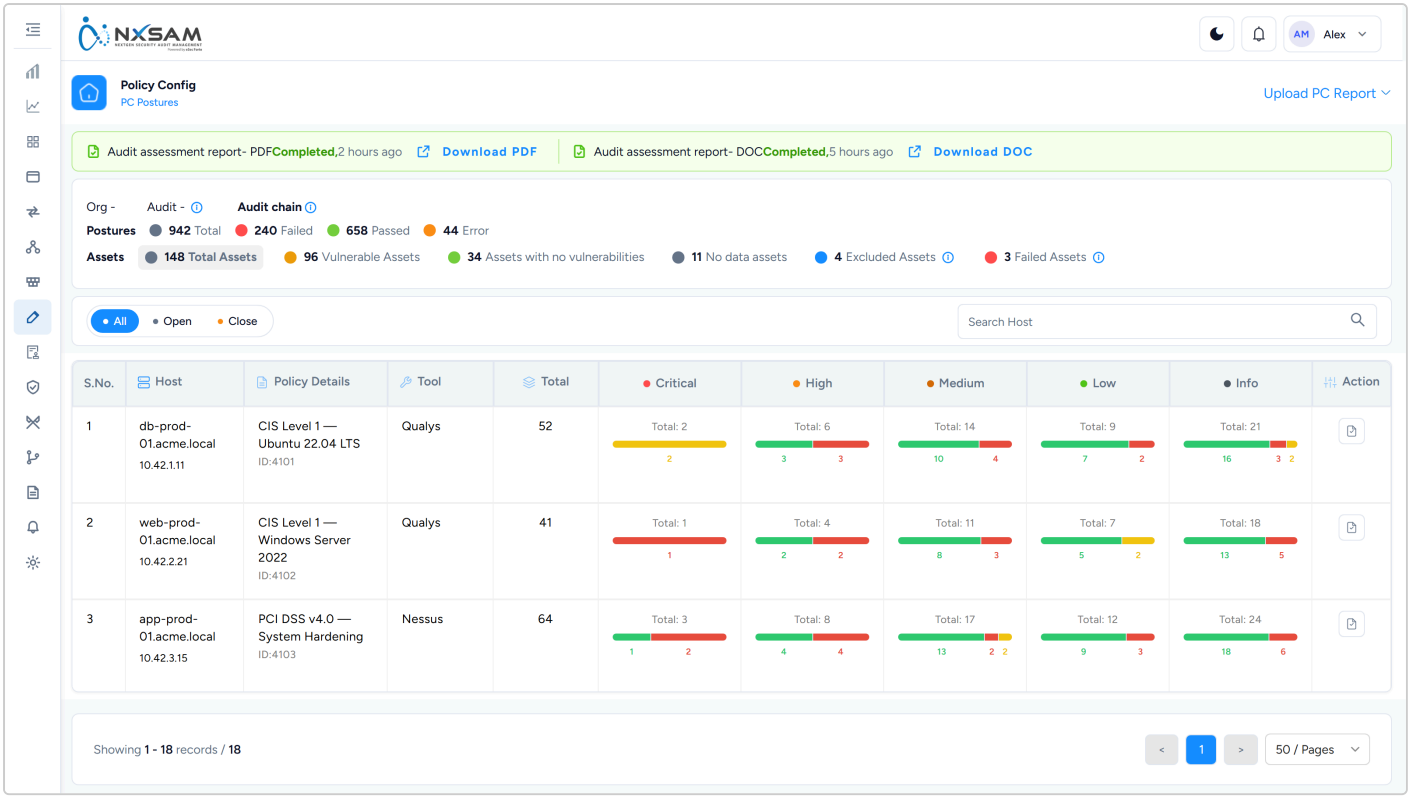
Policy Config → Postures → Uploaded Report Status

Choose the upload type carefully: it decides how incoming rows meet the existing ones — merge, closure, limited closure or ignore. The wrong choice is not a parsing error and produces no warning; it produces the wrong result quietly.

While it processes: the queue shows Pending or In Progress, and counts move. A failed job carries a per-row reason — most often a host in the file that is not in the audit's scope.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

4. Read the results



Policy Config → Config Policies → Postures

A **posture** is one control checked against one host. Every check produces a row whether it passed or not, so an audit of 400 hosts and 300 controls is 120,000 rows.

Total postures = passed + failed + error. If the three do not add up, the run is still processing.

Two columns that look alike and are not:

Column	Means
Posture Status	What the check returned — pass, fail, error
Status	What your team decided to do

A posture can be **fail** and **Risk accepted** at once. The machine is still non-compliant, and the organisation has agreed to leave it that way.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Mostly errors is a credentials problem, not a compliance result

Error means the check could not run. A benchmark returning mostly errors usually indicates the scanner could not authenticate to the targets.

---

5. Work the failures

Open a posture for **Cause** and **Evidence**. Cause is the rule's explanation; Evidence is the value actually read from the machine. When an owner says "that setting is correct", Evidence is what settles it.

Record decisions as you go:

- **Comments** — the discussion trail, with who and when.
- **Status changes** — each passes through a confirmation dialog naming the audit and the transition. Whether a comment is required depends on the target status.

Comments accept letters, numbers and `_ - . &` up to 5000 characters, so text pasted from a ticketing system is sometimes rejected for its characters rather than its length.

---

6. Approve

Bulk Approve Audit Status acts on the rows you tick, which is what the checkbox column is for — a cycle's worth of completed audits can be approved together.

---

7. Re-assess

A follow-up assessment against the same scope shows what has actually changed. The status history on each posture — including the **Evidence** recorded by whoever changed it — is what an auditor reads later.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

When something looks wrong

Symptom	First thing to check
Upload "did nothing"	The queue, not the posture list
Counts do not add up	Still processing
Everything closed, or nothing updated	The upload type used
Mostly errors	Scanner credentials on the targets
The list is empty	The filter badge — filters persist across the module
The heading says "undefined"	A known defect; the table below is still correct

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reading the Policy Compliance screens

This module counts differently from every other one, and the difference catches people out: a posture screen shows **checks**, not findings, and a single host contributes hundreds of them.

One row is a host, and the numbers are check counts

The postures screen groups by host. Each severity has four separate counts:

Column family	Meaning
`<severity>_total_posture`	Checks at that severity that ran against this host
`<severity>_total_passed`	Of those, how many passed
`<severity>_total_failed`	How many failed
`<severity>_total_error`	How many could not be evaluated

Total postures = passed + failed + error. If it does not, something did not complete.

> ⚠ **Error is not failure**
>
> A check in **error** did not run — the agent could not read the setting, the file was absent, permissions were wrong. It is neither a pass nor a fail, and treating errors as passes is how a compliance score comes out optimistic.
>
> A sudden compliance improvement with no configuration change is very often a rise in error counts. Check the error column before reporting the improvement.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Compliance percentage depends on what you divide by

Passed ÷ total is not the only defensible calculation. Passed ÷ (passed + failed) — excluding errors — gives a different and usually higher number.

When a compliance figure here disagrees with one from the scanner, this is the most likely reason, and it is worth establishing which convention each side uses before treating the gap as a data problem.

Postures versus controls

Two words used loosely in conversation and precisely in the product:

- A **control** is the rule — "SSH root login must be disabled". Defined once.
- A **posture** is the result of that rule checked against one asset. One control across 200 hosts produces 200 postures.

So "we have 40 controls" and "we have 8,000 postures" describe the same estate. Reports switch between the two, which is why a count can appear to change by two orders of magnitude between screens.

The posture upload queue

Policy Compliance data volumes are the largest in the platform — a single benchmark run across an estate produces hundreds of thousands of rows — so imports are queued and processed in batches.

The queue screen carries what you need when an import is questioned:

Column	Use
Queue status	Pending, in progress, completed or failed
Queue summary	What was processed
Queue error	Why it stopped, where it did
Upload type	Whether this run replaced or merged with existing data

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	Use
Policy title / repository / scan zone	Which benchmark, and over what
Initiator	Who started it
Automatic sync	Whether it was scheduled or hand-triggered

Upload type is the one to check first on any "the numbers are wrong after an import" question. A merge and a replace produce very different totals from the same file, and the difference is invisible once the import has finished.

Why a host disappeared from the compliance report

In order of likelihood:

1. **The scan did not cover it.** Compliance runs against a defined scope; a host outside it produces no postures and so no row — it is absent rather than passing.
2. **Every check errored.** With no passes and no failures, some views have nothing to show.
3. **The import is still running.** A partly loaded batch is missing hosts that will appear shortly.

The first is the most common and the least obvious, because an absent host looks the same as a compliant one on a summary screen.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Policy Compliance: every screen, column and action

Complements Reading the Policy Compliance screens. The module has the largest data volumes in the product, so almost everything here is queued, and the queue screens carry the answers.

The audit list

Column	What it holds
Request Info	Who requested it, when, and the request ID
Audit Details	Audit name and the benchmark being assessed
Vulnerabilities	Failed checks with their severity split
Audit Properties	Type, cycle, scope, considered
Audit Status	Current state
Data Process	Whether the uploaded data has finished processing

Data Process matters more here than anywhere else. A policy run produces hundreds of thousands of rows, so the gap between "upload finished" and "data processed" is minutes to hours — and counts move throughout. An audit reporting a number that keeps changing is still processing, not miscounting.

Row actions — eight

Action	What it does
Edit Audit Details	Name, dates, properties

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Action	What it does
Manage Audit Scope	What was in and out of scope
Assign Auditors	Who runs it
Export IPs	Downloads the hosts in scope
Re-Audit	A follow-up assessment against the same scope
View Audit Chain	The original and every re-audit — `Audit ID`, `Type`, `Audit Name`, `Status`, `Auditors`
View Status History	Every status change
Delete Audit	Soft delete

Export IPs is how a scope dispute gets settled. Compliance scope is defined by host list, and the export is what you compare against the benchmark tool's own target list when the two disagree on coverage.

Bulk Approve Audit Status acts on the audits ticked in the first column, so a cycle's worth of completed audits can be approved together rather than one at a time.

Changing an audit's status

Every status change goes through a confirmation step rather than applying on click. The dialog states, in order:

- the **audit name and ID**, so you can see you are moving the audit you meant to
- the transition itself — **from status → to status**
- a **warning**, where the transition has a consequence worth stopping for
- a **Comments** box, labelled *(optional)* or marked required depending on the target status

Then **Change Status**, or **Cancel**.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Whether a comment is required is a property of the target status

The same screen asks for a mandatory comment on one transition and offers an optional one on the next. That is configuration, not inconsistency — each status carries its own *comment required* flag on the status master.

Comments accept letters, numbers, and `_ - . &` only, up to 5000 characters. A comment pasted from a ticketing system often carries characters outside that set, and the dialog rejects it rather than truncating.

Filters

The filter drawer is reached from **More Filters** (**All Filters** on the policies screen), and the button carries a **badge with the number of filters currently applied**.

That badge is the answer to most "why can't I see my audit" questions: filters persist as you move around the module, and a non-zero badge on a screen that looks empty means the list is filtered, not empty.

Postures by host

Column	What it holds
Host	The machine
Policy Details	Which benchmark was applied
Tool	Which scanner produced the result
Total	Checks run against this host
Critical / High / Medium / Low / Info	The severity split of the failures

Remember that a row is a host and the numbers are **check counts**, not findings. One control across two hundred hosts produces two hundred postures.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Postures for one control

Opened from a host or a control.

Column	What it holds
Posture ID	The individual result
Control Name	The rule being checked
Severity	As rated
Status	The working state
Posture Status	Pass, fail or error — the technical result
Cause	Why it failed
Evidence	What was actually found on the machine
Instance	Which occurrence, where a control is checked more than once per host
Discovered On / Last Observed Date	First and most recent sighting

Row actions: **View Posture Status History**, **Vulnerability History**, and **add a comment**.

The two histories, and the comment trail

Three separate records sit behind a posture, and they answer different questions:

Screen	Columns	Answers
View Posture Status History	`By`, `On`, `Status`, **Evidence**	Who moved this posture to its current state, when, and on what basis

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Screen	Columns	Answers
Vulnerability History	`Audit Details`, `Risk`, `Status`, **Status Changed By**, with its own **More Filters**	How this finding has behaved across audits
View Posture Comments	`By/On`, `Comments`	What people said about it, in order

Both histories are headed by the **Control Name**, so a modal opened from a long list still says which control it belongs to.

> **Evidence on the status history is the audit trail, not the scan output**
>
> The **Evidence** column here is what the person changing the status recorded as their justification. It is not the machine reading — that is the Evidence column on the posture row itself.
>
> They are deliberately separate: one is what the scanner found, the other is why a human decided to accept, defer or close it.

> **Status and Posture Status are different columns**
>
> **Posture Status** is what the check returned — pass, fail, error. **Status** is what your team has decided to do about it.
>
> A posture can be `fail` and `Risk accepted` at the same time, and that combination is correct: the machine is still non-compliant, and the organisation has agreed to leave it that way.

Cause and Evidence together are what make a compliance finding arguable or not. Cause is the rule's explanation; Evidence is the actual value read from the machine. When an owner says "that setting is correct", Evidence is what settles it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Controls and policies

Screen	Columns
Controls	**Control Details** (identifier and name together), `Severity`, `Tool`, `Policies`, `Created By`
View controls	`Control ID`, `Control Name`, `Severity`, `Created By`
Policies	**Policy Title/ID**, **Tool / ID**, `organisation`, `Policy Config Category`, `Created By`
View control policies	`Policy ID`, `Title`, `Tool`, `Org`, `Category`
Categories	`ID`, `Policy Config Category`, `Created By`, `Sync`

The **Policies** column on a control counts how many policies include it — a control in six policies is checked by all six, and fixing it improves every one of their scores.

Category actions are **View Controls** and **Delete Config Category**. The **Sync** column shows whether a category is kept in step with its source tool.

Host selection

`Host IP`, `Host Name`, `Application Name`, `App Code`, `Selected` — used when defining what an audit covers. **App Code** is included because compliance scope is usually agreed per application, while the scan runs per host.

Excluded assets

`Network Asset ID`, `Host IP/Host Name`, `Comment`.

Hosts deliberately outside a compliance run — a lab machine, an appliance the benchmark does not apply to. The **Comment** is the justification, and an exclusion without one is the first thing an auditor questions.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Updating asset status

`Network Asset Id`, `Host IP/Host Name`, `Status` — bulk-sets whether hosts are active in compliance runs.

The screen accepts a **CSV** upload for bulk changes and offers a sample to download, so a list of several hundred hosts does not have to be set one at a time.

The posture upload queue

Column	What it holds
Queue ID	The job
Policy	Which benchmark
Report Type	The kind of report uploaded
Upload Type	Merge or replace
Workflow	How results were processed
Status	Where the job is
Initiated By / Initiated At	Who and when

Actions: **Queue File**, **Queue Summary**, **Log File**, and **Retry** on a failed upload. The queue can be filtered by **Host IP** as well as by status, so one host's uploads can be followed across runs.

Queue Summary is what was processed; **Log File** is the per-row detail including rejections. On any "the compliance numbers are wrong after an upload" question, check Upload Type first and the Log File second — those two answer it almost every time.

Scheduling a scan instead of uploading a report

Upload PC Report → Upload Report opens **Upload New Report**, and it is offered only on an audit that is still in progress with an auditor assigned — a completed audit's menu has **View Upload Report** alone. The form unfolds as you choose:

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Field	What it decides
Policy Config Category	Which category of the policy this run covers
Report Type	**Qualys**, **Nessus** or **Manual** — the scanner, or a hand-assessed sheet
Workflow	**Upload** takes a report file. **Scan** asks the scanner to run the benchmark and bring the result back. **Automatic Scan** — Nessus with a Tenable SC connection only — re-runs it on a schedule
Scan Option	Start a **New** scan, or reuse an **Existing** one by its **Scan Result** or **Scan ID**
Config Policy	The benchmark the scanner runs
Scan Zone, **Repository**	Where the scanner runs from and where its results are kept, as defined in Tenable SC
Track hosts which have been issued new IP address	Follow a host across an address change, for estates using dynamic addressing
Credentials	The scanner's own credential sets, one or more, for an authenticated scan
Schedule Scan / **Schedule At**	Run now, or at a chosen date and time
Upload Type	**Ignore** leaves assets that already have a posture untouched; **Override** replaces their results

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Qualys shows the same shape with an **Option Profile** in place of the Tenable fields. A scheduled scan appears in the queue like an upload and can be cancelled while it is running — the confirmation asks whether to cancel the on-going scan. A scan needs a target, so an IP is mandatory for it; a report upload has no such requirement, since the hosts are in the file.

The **Host selection** step searches by **App Code**, **Application Name**, **Host IP** or **Host Name**, so the hosts in scope can be picked from either the application side or the network side of the inventory.

Bulk upload of policies and controls

Accepts **CSV** or **XLSX**. The queue reports `Status`, `Initiated By`, `Uploaded At`, with **Download** and **Log File Download**.

Reporting

Download xlsx Report from the postures view exports the current posture set as filtered — the format compliance teams actually work in, because they annotate it and send it back to system owners.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

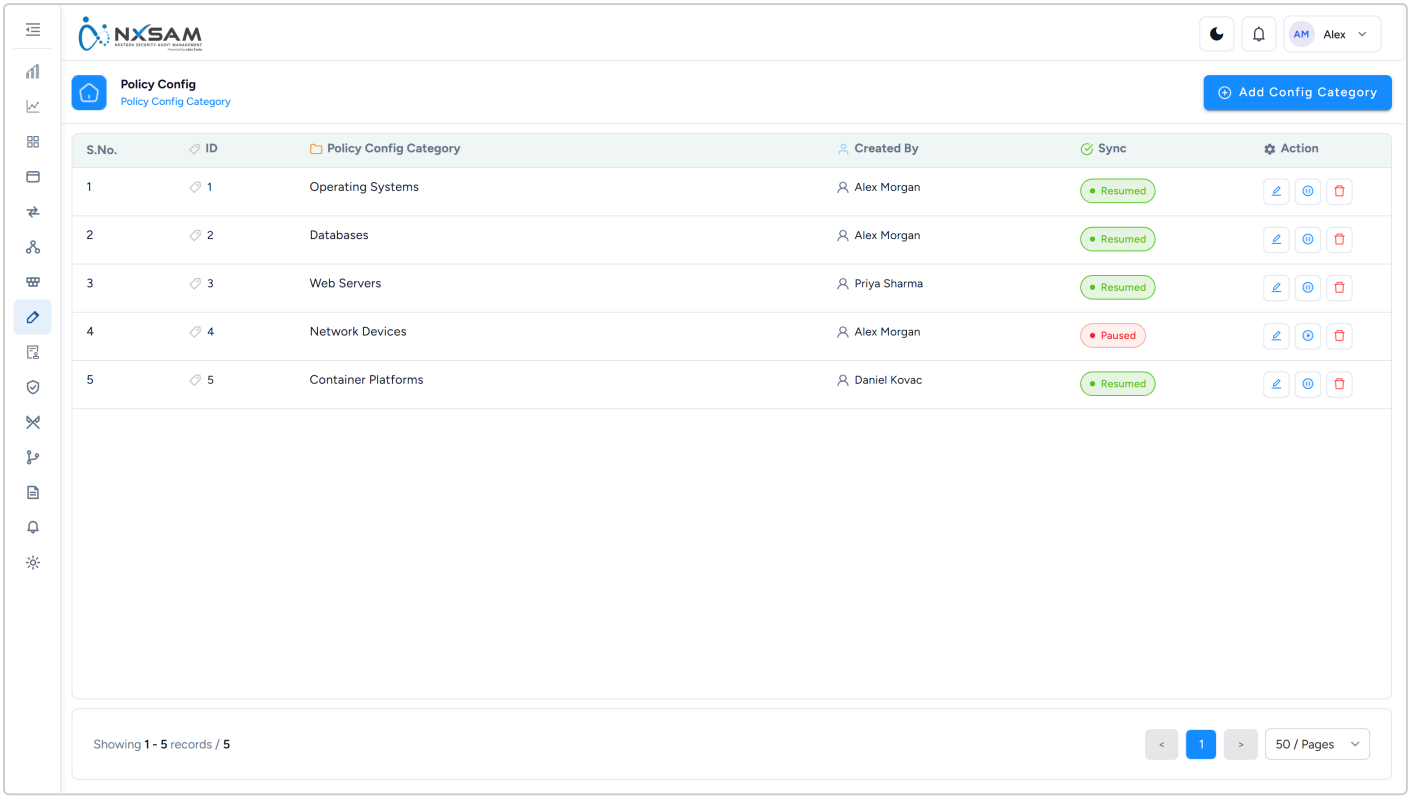
Policy Compliance: find the right screen

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.

Control Categories

How controls are grouped for reporting — by domain, benchmark section or your own scheme.

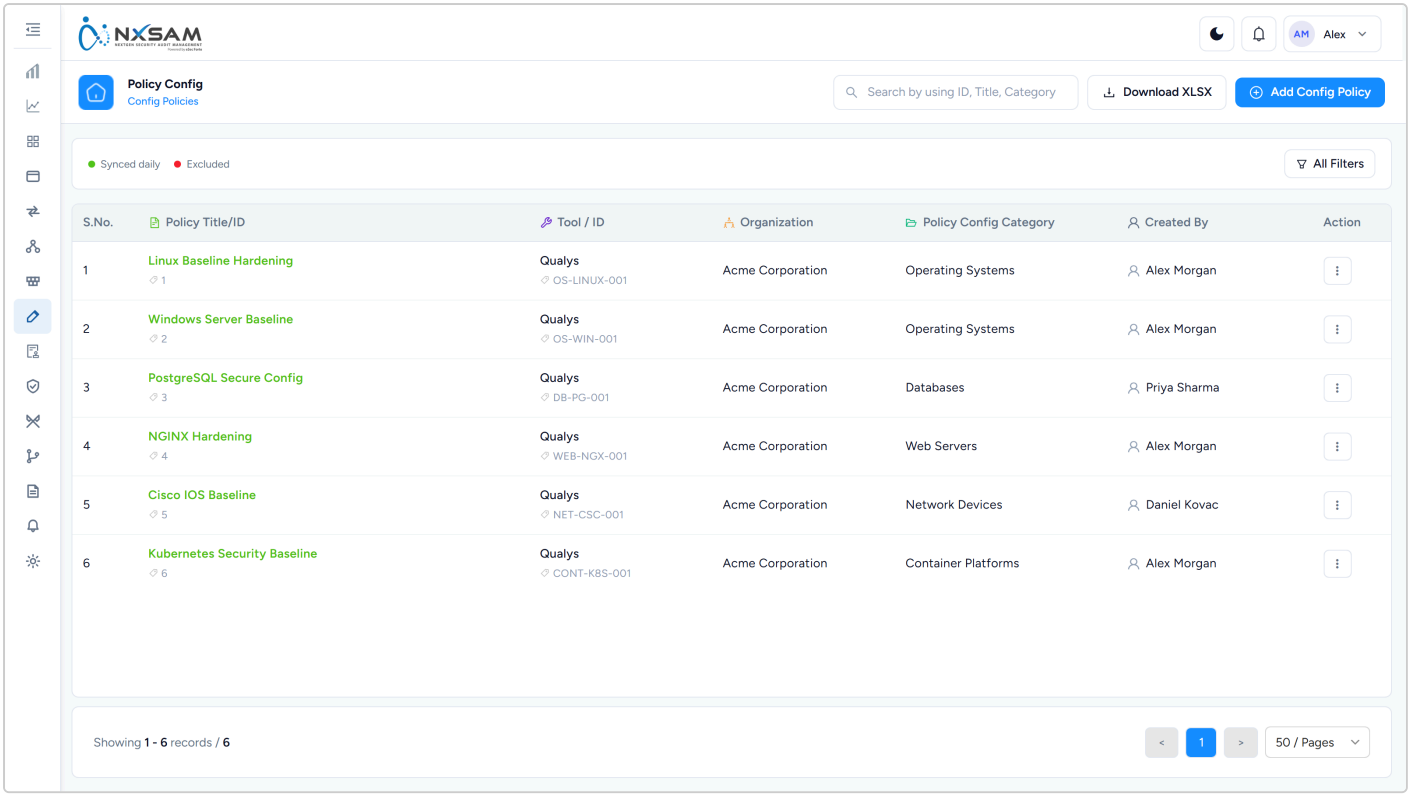


Policy Config → Policy Config Category

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Policy Configuration

Which benchmarks are in use and how their results are interpreted.

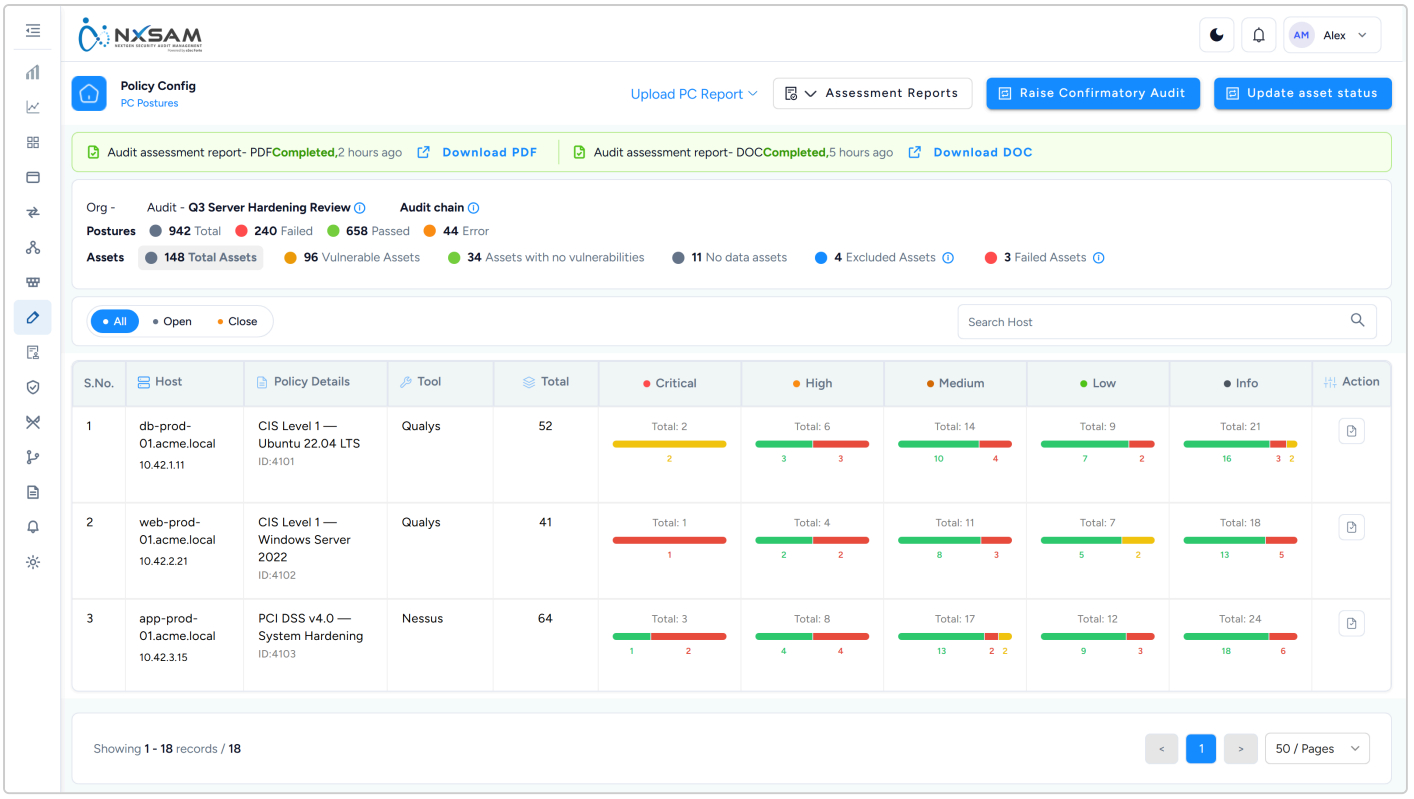


Policy Config → Config Policies

Postures

The result of one control checked against one asset — the expected value, the actual value, and whether it passed.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Policy Config → Config Policies → Postures

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.