



NxSAM Network Security — Quick Guide

Quick reference guide for the Network Security 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

Network Security

- Overview
- Run a network VA assessment, end to end
- Reading the Network Security screens
- Network Security: every screen, column and action
- Working a VA result
- Network Security: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Network Security

Network Security

Network Security covers weaknesses in your infrastructure — servers, network devices and the services running on them. It holds three distinct kinds of assessment.

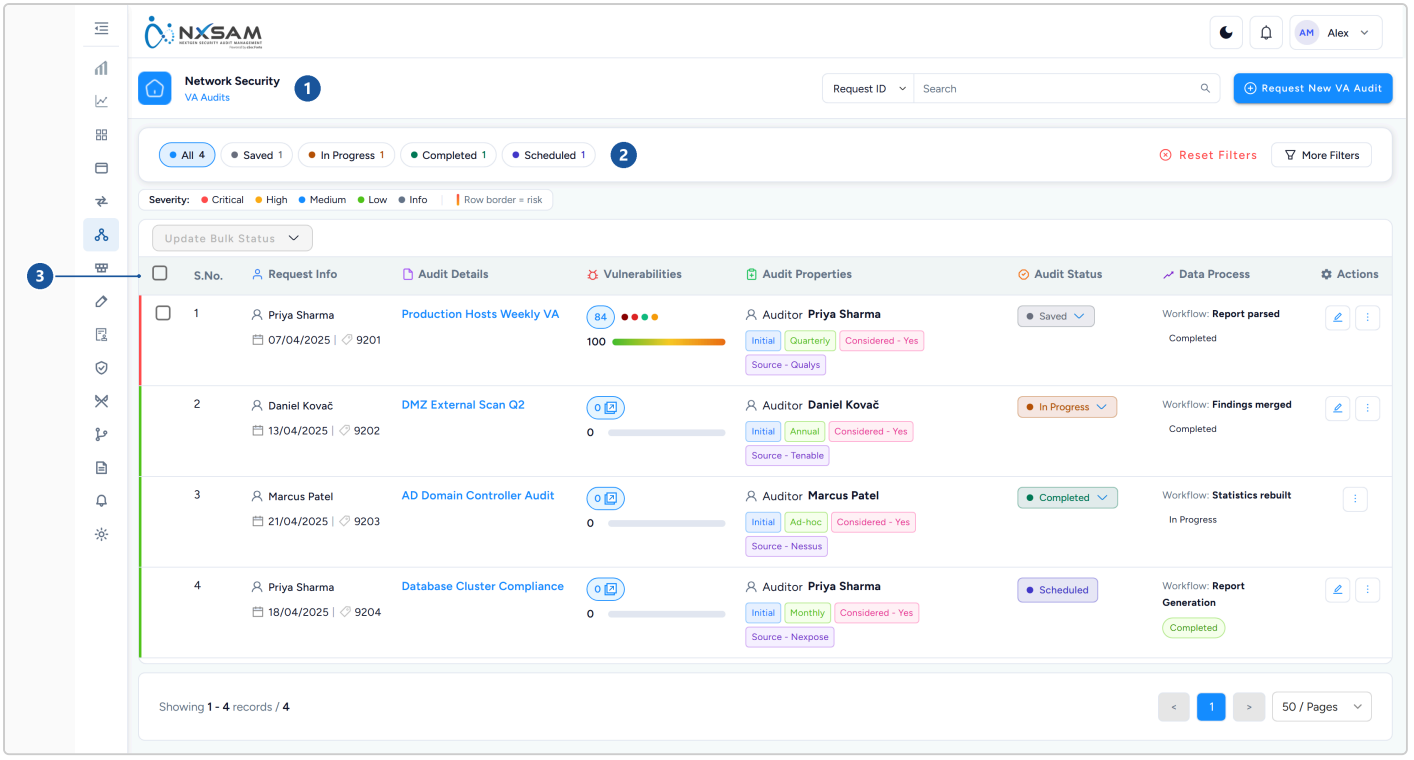
Three kinds of assessment

	What it is
VA — Vulnerability Assessment	Automated scanning, usually on a schedule, usually high volume. Findings arrive from tools such as Qualys, Tenable, Nessus or Nexpose.
PT — Penetration Testing	Human-led testing. Lower volume, higher depth, and each finding is written by the tester.
Segmentation	Verification that networks that should be separated actually are — commonly a PCI DSS requirement.

They are separated because they behave differently. A VA audit may carry thousands of machine-generated findings; a PT audit may carry a dozen carefully written ones. Reporting and workflow differ accordingly.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

VA: the shape of the work



Vulnerability assessment audits.

1 module and screen · **2** filter by status · **3** audit columns

1. A scan runs in your scanning tool.
2. Its results reach NxSAM, either by integration or by uploading the report.
3. Findings are matched against what is already known, so a weakness seen before continues as the same record rather than becoming a new one.
4. New findings are assigned SLAs by severity and become visible to asset owners.
5. Owners remediate; a later scan confirms the fix; the finding is validated and closed.

The same weakness on ten hosts is ten findings

Network findings are per host. A missing patch across ten servers produces ten findings, because each host must be fixed and verified individually.

This is why VA counts are much larger than application counts, and why they move sharply when a widely-deployed component is patched.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Repeat scans and reopening

A finding fixed and validated, then seen again by a later scan, comes back as **Reopen**. Reopening is informative rather than a failure of process — it usually means a patch was rolled back, a host was rebuilt from an old image, or a configuration drifted.

Persistent reopening on the same host is worth investigating as a build or configuration problem rather than as a series of unrelated findings.

Working with high-volume findings

VA generates far more findings than anyone can address individually, so it is normally worked in groups:

- Filter by severity and by asset criticality together — Critical findings on production assets first.
- Group by vulnerability rather than by host when a single patch resolves many findings at once.
- Use SLA state to see what is genuinely urgent rather than merely numerous.

PT: what is different

Penetration test findings are written by people, so they carry narrative detail, reproduction steps and evidence. They are usually fewer, more severe, and more likely to need discussion before remediation.

The lifecycle is the same — findings are approved, assigned SLAs, remediated and validated — but the volume means each one is normally handled on its own merits.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Run a network VA assessment, end to end

This walks one assessment from request to closure, naming what you need at each step, what changes when you act, and where it commonly goes wrong.

Every screen shown here is illustrated with demonstration data.

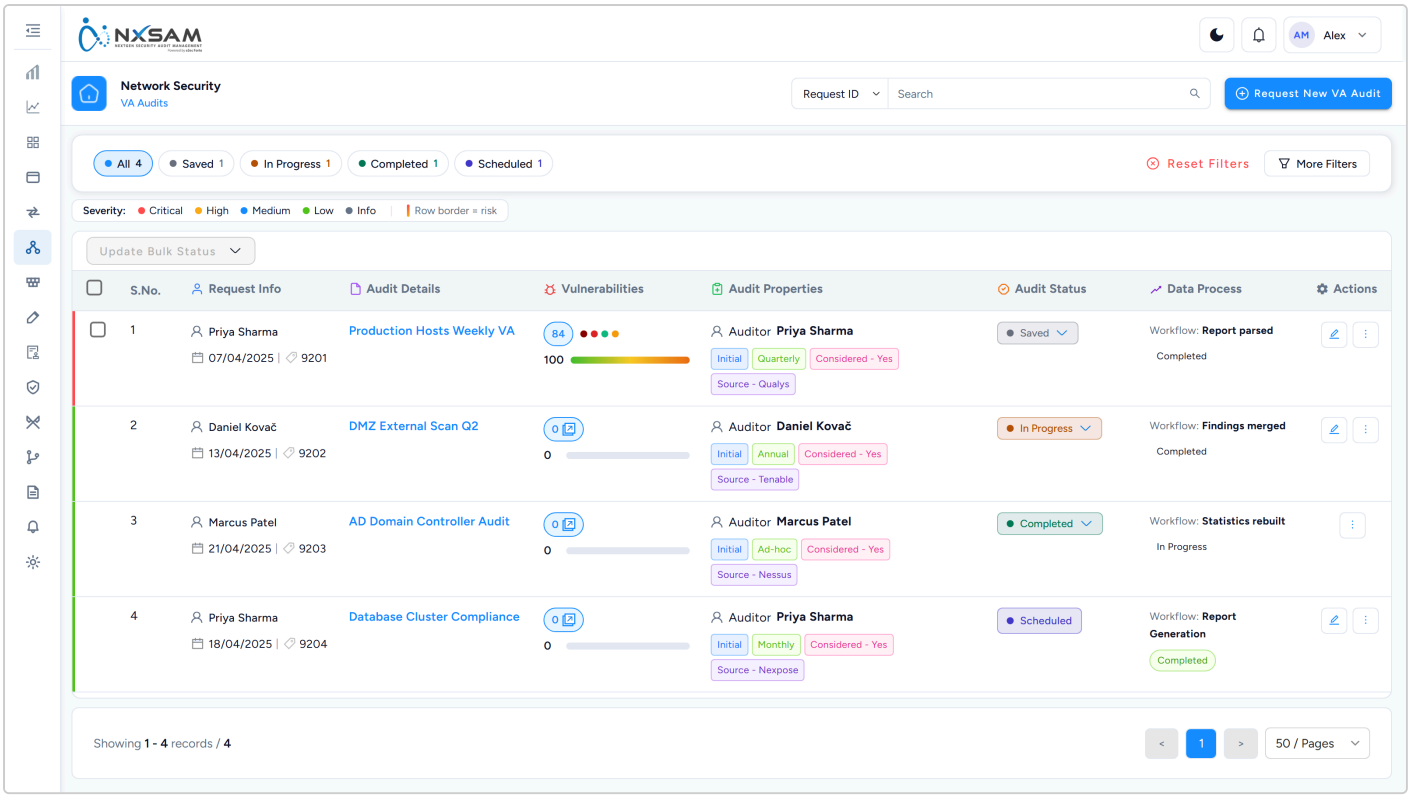
Before you start

You need	Why
The hosts in scope	Scope is a host list, and it settles later disputes
An audit type and cycle	They decide which properties are mandatory
An auditor account	An audit can be created without one and cannot be worked
Permission to request an audit	Controls you lack are hidden, not disabled

1. Create the audit

Open **Network Security** → **VA Audits** and choose **Request New Audit**.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Network Security → VA Audits

Fill the audit's name, type, category and cycle. Properties marked mandatory must be completed before the form will save — which properties are mandatory depends on the asset type and audit type together, so two audits can demand different fields.

After you save: the audit exists in its first status and appears in the list. It counts towards nothing yet.

One audit at a time per asset, where the platform is set that way

If an asset in your scope already has a VA audit in progress, the request may be refused with a message naming the rule — *only one on-going VA audit per asset*. That is a platform setting (**System → System Settings**) rather than a fault: two concurrent scans of one host would produce two sets of findings for one state. Wait for the running audit, or take the asset out of this one's scope.

Assign an auditor now

An audit can be requested and approved with no auditor assigned, and then cannot be worked. An audit sitting in an approved state with nothing happening is usually this.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

2. Define the scope

Use **Manage Audit Scope** on the audit's row menu to set the hosts covered.

Export IPs downloads that list. Keep it: when the scanning team and the platform disagree about coverage later, comparing this export against the tool's own target list settles it in minutes.

3. Bring in the findings

Either upload a scan report, or let a configured integration collect it. Both are queued.

The **Data Process** column on the audit list shows how far a tool-fed audit has got. It is the difference between "the upload finished" and "the data is ready".

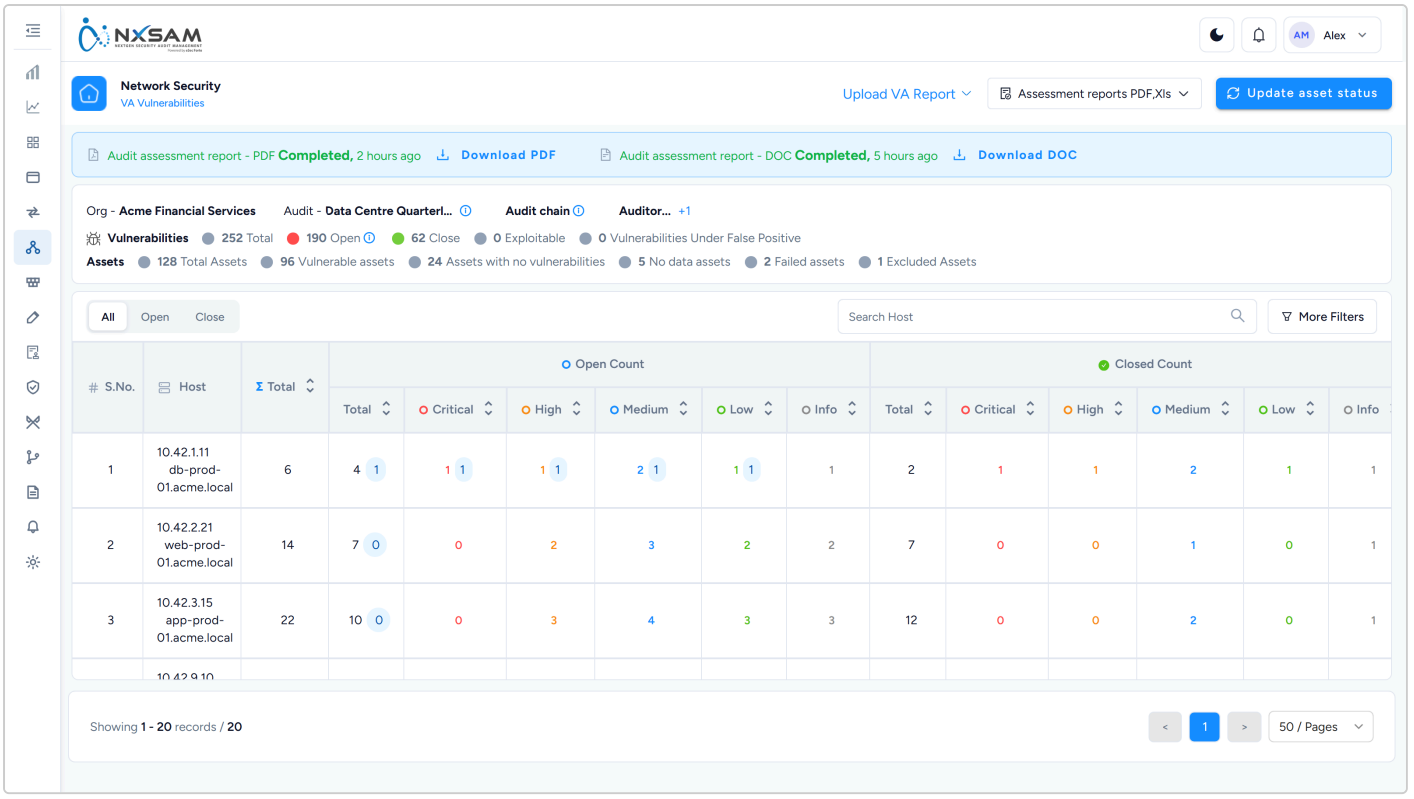
While it processes: counts move on every refresh. That is the job running, not the figures being wrong.

> **Counts that jump after an import**
>
> If totals appear to double, the identity rule changed — findings that were matched to existing records no longer match, so they arrive as new. Treat a change to the VA key configuration as a data migration, not a preference.

4. Work the findings

Open the audit to reach its findings.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Network Security → VA Audits → the audit's findings

Each row is a host with its severity split. Drill in for the individual findings on that host.

Two fields track two different things, and both are needed:

- **Validation** — has this been confirmed as a real finding?
- **Current Status** — what is being done about it?

---

5. Approve

Nothing is counted anywhere until Validation reaches **Approved**.

After approval: the finding appears in dashboards and reports, **Discovered On is populated** — it is deliberately blank before this — and its SLA clock starts from the severity and asset type.

This single step explains most "my finding isn't in the dashboard" questions.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

6. Remediate and close

As work proceeds, move **Current Status** — to be patched, patch in progress, and so on. Some transitions require a comment; the confirmation dialog says so before you commit.

> ⚠ **Only two statuses actually close a finding**
>
> **Validated** and **Exception Handled**. Everything else — including **Risk accepted** — still counts as open.
>
> That is deliberate: accepting a risk is a decision about treatment, not a statement that the weakness is gone.

---

7. Complete the audit, and make it count

Move the audit to a final state.

After completion: the audit becomes eligible to be **considered**, and the date it reached that state is the date every aggregate view files it under — not the scan date, and not the import date.

A scan run in March, imported in April and completed in May is a May audit. If a customer says findings appear in the wrong month, this is almost always why.

---

8. Re-test

Create a **Re-Audit** against the same scope. It inherits the parent's scope and is marked as a follow-up rather than as an independent assessment, so the two are not counted as two rounds of testing.

When something looks wrong

Symptom	First thing to check
Finding not in the dashboard	Is it approved? Is the audit considered?

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

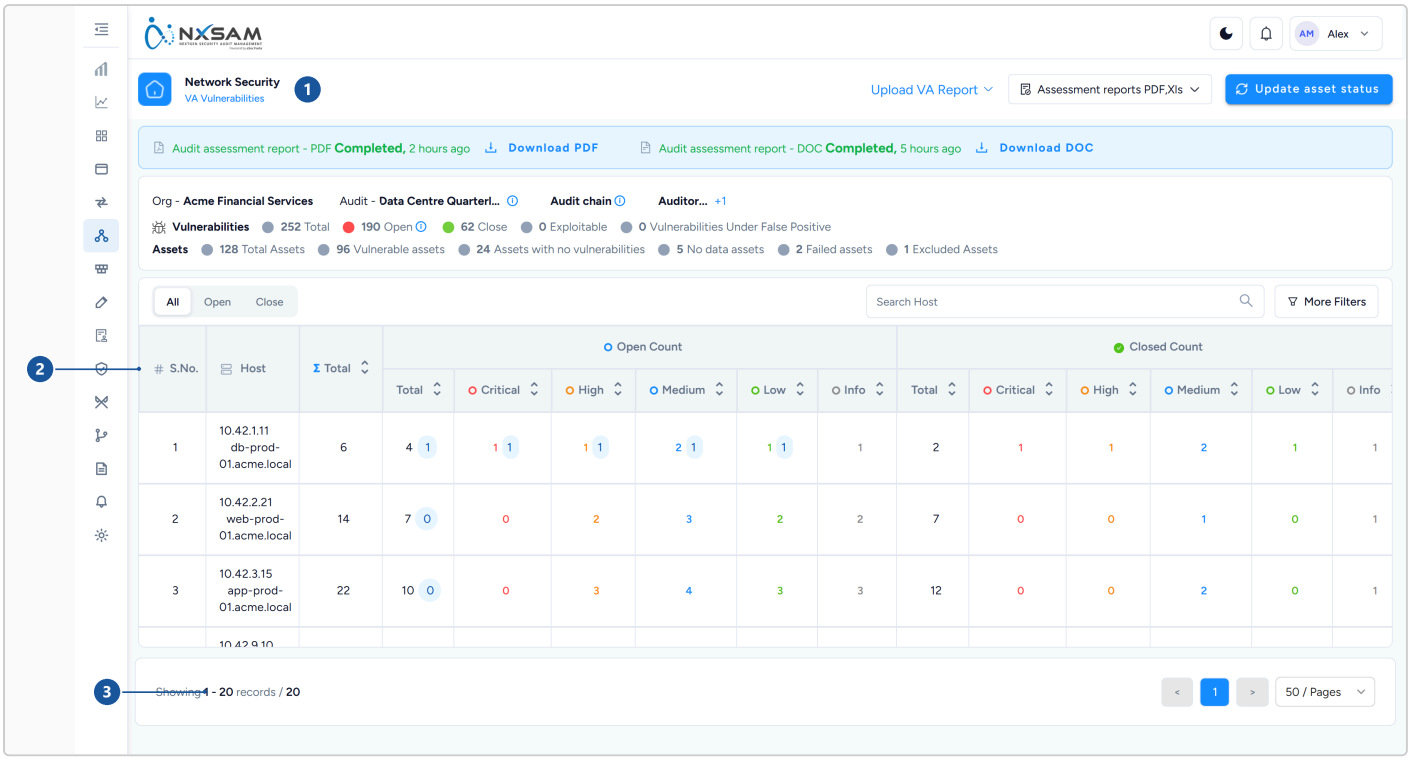
Symptom	First thing to check
Audit in the wrong month	The date it reached a final state
Numbers keep changing	Data Process — it is still running
Numbers doubled	The vulnerability key configuration changed
Action missing from a menu	Your role — hidden, not disabled
List looks empty	A filter is still applied from an earlier screen

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reading the Network Security screens

VA and PT look similar and are structured completely differently, because they answer different questions. Knowing which is which saves most of the confusion in this module.

VA: a grid of counts, not a list of findings



VA groups by host. Each row is a machine, not a finding.

1 module and screen · 2 one row per host, counts per severity · 3 paging

The first thing to understand: **one row is one host**, not one finding. A scan of 200 machines produces 200 rows regardless of how many vulnerabilities it found.

The count columns

Each severity appears up to three times across the row, and the three mean different things:

Column family	Meaning
`open_<severity>`	Currently open on this host at that severity
`closed_<severity>`	Closed on this host — fixed and confirmed by a later scan
`<severity>_exploitable`	Of the open ones, how many have a known exploit

Plus **Open**, **Closed** and **Total** counts for the row.

The closed columns are hidden entirely when nothing on the screen is closed, so a column set that changes between two audits is the table adapting, not data disappearing.

> **Exploitable is the column to sort by**
>
> Severity says how bad the weakness is in theory. Exploitable says whether someone has already written the tool to use it. A host with two exploitable Mediums is a more urgent problem than one with six theoretical Highs, and the exploitable count is the only column that surfaces this.

Host name and IP

Both are shown because both are used for matching. If findings land against a host you did not expect, compare these two against the scanner's own record — short name against fully-qualified name is the usual cause.

Status, updated on, comments

Status is the host-level working state, **Updated On** is when it last changed, and **Comments** carries whatever the analyst recorded. Updated On moves when the status moves, not when the host was last scanned — those are different dates and are frequently confused.

PT: a list of findings with evidence

The penetration testing screen is closer to AppSec than to VA. One row is one finding, because a manual test produces tens of findings rather than thousands.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	Notes
Track ID	Quote this in tickets
Issue title	What the tester found
Host and port	Where — a manual finding is usually specific to a port
Risk	The tester's rating, not a tool's score
Validation status	Whether the finding is agreed
Status	What is being done about it
Observation added	Whether the tester attached evidence
Document	The evidence itself

Why PT has evidence and VA does not

A scanner finding is reproducible by re-running the scanner. A manual finding often is not — it may depend on a sequence of steps, a particular account, or timing. The observation and the attached document *are* the proof, and a PT finding without them cannot be verified by anyone but the original tester.

If a PT finding is disputed, the first question is whether an observation was recorded.

Risk acceptance on PT findings

The acceptance's comment and date appear directly on the row. A PT finding that has been accepted shows why and until when, without leaving the screen — useful during a review, and the reason accepted findings are not simply hidden.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Segmentation: neither of the above

Segmentation audits test whether network separation holds — whether a source can reach a destination on a port it should not. Findings are about *paths*, not hosts or software, so a finding reads as a source, a destination, a port and a protocol, with `UDP Added` and `TCP Added` recording what became reachable.

The useful question here is not "how severe" but "was this path supposed to exist" — which is why the screen shows source and destination side by side rather than ranking by severity.

Which screen answers which question

Question	Screen
Which machines are worst?	VA vulnerabilities
Which single patch helps most?	Overall vulnerability status
What exactly is this finding?	Vulnerability detail
What did the tester actually do?	PT vulnerabilities, with the observation
Did segregation hold?	Segmentation findings
Has the scan finished loading?	VA import queue

The last one is worth checking before any of the others. A partly loaded scan looks identical to a complete smaller scan.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Network Security: every screen, column and action

This module has more screens, more row actions and more status values than any other, and it does not share its status model with Application Security even where the words look the same. Everything below is taken from the product's own tables and templates.

The status models — four of them, all different

> ⚠ **Network Security does not reuse the AppSec statuses**
>
> The words overlap and the sets do not. Quoting an AppSec status list to a VA caller will not match what they see.

Audit status — twelve values

`Saved` → `Requested` → `PMO Verified` → `Approved` → `Scheduled` → `IN PROGRESS` → `Completed`, with `Failed`, `Aborted`, `Review Requested`, `Changes Requested` and `Reverted` as the exceptions.

Two properties decide behaviour:

- **Comment required** — `Failed`, `Changes Requested`, `Reverted`, `PMO Verified` and `Aborted` will not save without one. The others save silently.
- **Closed type** — only `Completed` and `Aborted`. An audit sitting in `Review Requested` is still open however finished it looks.

`PMO Verified` sits between `Requested` and `Approved` and exists for organisations running a project-management gate before scanning starts. Where that gate is not used the status is simply never selected.

VA vulnerability status — eleven values

`New`, `Patched`, `False Positive`, `In Progress`, `Reopen`, `Exception Applied`, `Verified`, `Validated`, `Risk Accepted`, `Risk acceptance`, `Expired`.

Closed types are `Exception Applied`, `Verified` and `Validated` — three, where the AppSec side has two, and `Patched` is again not one of them.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

`False Positive`, `Reopen` and `Risk Accepted` require a comment.

PT vulnerability statusThe same eleven names in a separate table, so a status renamed for VA does not change for

PT. `Risk accepted` and `Risk Acceptance` additionally display a date.

PT validation status — three values

`Saved`, `Submitted`, `Approved`. **Three, not the five Application Security uses** — there is no `Closed` and no `False Positive` at validation level here, because a PT false positive is recorded through the vulnerability status instead.

VA Audits

The busiest screen in the module.

Columns

Column	What it holds
Request Info	Who requested the audit, when, and the request ID to quote in tickets
Audit Details	Audit name and the assets or scan target it covers
Vulnerabilities	Open counts with the severity split, and the audit's risk score
Audit Properties	The chips — cycle, type, tool, scope and whether the audit is considered
Audit Status	A dropdown offering only the legal next steps from the current status
Data Process	Whether imported scan data has finished processing for this audit

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Data Process is the one people miss. An audit can be `Completed` while its data is still being processed, and counts will keep moving until that finishes. Check this column before investigating a total that will not settle.

Row actions — twelve

Action	What it does
View Vulnerabilities	Opens the findings for this audit — the normal drill-down
Vulnerability Overview	A summary by severity and host without leaving the list
Add More Assets	Extends the audit's scope to further hosts after it was created
Export Assets	Downloads the asset list in scope, for reconciling against the scanner
Manage Audit Scope	Records what was in and out of scope, with a description and an optional image
Manage Severity Config	Overrides how this audit's severities are derived
Assign Auditors	Sets who performs the work
Edit Audit Details	Name, cycle, dates and properties
Edit Tags	Free-form labels used for grouping and reporting
Re-Audit	Creates a follow-up audit against the same scope
View Audit Chain	Shows the original and every re-audit in sequence
View Status History	Every status change, with who made it and any comment
Delete Audit	Soft delete — the record is hidden, not destroyed

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Manage Severity Config changes this audit's numbers only

It overrides the derivation for the audit it is opened from. Two audits of the same hosts can therefore report different severities for the same finding, legitimately. If two scans disagree and nothing else explains it, check this first.

View Audit Chain is the answer to "why do we have four audits for the same subnet" — they are a chain of re-audits, and the chain view shows which is current.

Launching or uploading a scan

The upload dialog is a full scan-configuration form, not a file picker. What it asks for depends on the tool:

Field	Applies to
Tool	Which scanner this data comes from or runs on
Type	Upload an existing report, or launch a scan
Credential type / Credentials	The account the scan authenticates with
Scanner	Which scanner appliance runs it
Policy / Option Profile	The scan policy — what is checked
Template / Template type	Report template for the output
Repository / Scan zone / Folder	Where the scanner stores results
Work flow	How results are processed on arrival
Schedule at	Run now or at a set time

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Field	Applies to
Upload document	The report file, when uploading rather than launching

Nessus and Tenable expose the largest set — scanner, policy, template, template type, repository, scan zone and folder — because those are the objects their APIs organise scans around. A field left empty that the tool requires is the usual cause of a launch that reports success and never produces data.

What each choice actually decides

Three of these change the *result*, not just the mechanics, and they are the ones worth deliberating over:

Type — upload or launch. Uploading parses a report the scanner already produced; launching asks the scanner to run now. An upload can be repeated and re-checked without touching the estate. A launch cannot be undone, and on a fragile production host that distinction matters.

Upload Type — how incoming rows meet existing ones. The single most consequential choice on the form:

Upload type	Effect
Merge	Adds new findings, leaves existing ones as they are
Closure	Anything absent from this report is treated as fixed and closed
Limited Closure	Closes only within the scope this report covers
Ignore	Records the upload without changing finding states

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

⚠ Closure on a partial report closes findings that were never re-tested

A report covering ten of your two hundred hosts, uploaded as **Closure**, marks findings on the other hundred and ninety as fixed — because they are absent from the file, which is exactly what closure means.

Limited Closure exists for this case: it confines the closing to the hosts actually in the report. When in doubt, that is the safer of the two, and Merge is safer still.

Work flow — how results are processed on arrival. Decides whether findings arrive already approved or require validation first. It is the difference between a scan that immediately moves your published numbers and one that waits for a person.

Policy / Option Profile decides *what was checked*, and therefore what an absence in the report means. A finding missing because the policy never tested for it is not a finding that was fixed — which is why the policy is worth recording alongside the result.

Schedule at runs the scan later. A scheduled scan that never appears to run is usually scheduled in a different timezone from the person looking for it.

Cancel Scan stops a launched scan that has not completed. It does not remove data already collected.

The upload queue

Reached from the audit, and the first place to look when imported data is questioned.

Column	What it tells you
Report Type	Which kind of report was uploaded
Upload Type	Whether this run merged with existing data or replaced it
Workflow	The processing path applied
Status	Where the job is
Initiated By / Initiated At	Who started it and when
Queue File	The file itself, for confirming what was actually uploaded

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	What it tells you
Queue Summary	What the job did — rows processed, rows rejected

Upload Type is the one to check on any "the numbers changed unexpectedly" question. A merge and a replace produce very different totals from the same file, and the difference is invisible once the job has finished.

Row actions: **Queue File**, **Queue Summary**, **Cancel Scan**. A failed job additionally offers a re-check, which re-runs the import without re-uploading the file.

Host selection, and App Code

Defining an audit's scope opens a host list carrying `Host IP`, `Host Name`, `Application Name` and **App Code**.

App Code is your organisation's own identifier for the application — from the CMDB, the change process or the finance system — not something NxSAM generates. It appears here because **VA scope is agreed per application while the scan runs per host**, and the code is what connects the two conversations.

It is also what survives a rename. Asset names drift; the code usually does not, which is why it is the field to quote when reconciling a scope disagreement with an application team.

Queue Summary — why the numbers differ from the file

This is the most useful dialog in the module, and the one most people never open. A report of 900 findings landing as 640 is not data loss; it is the sum of these counters, and the summary is the only place they are shown.

Hosts

Figure	Means
Mapped hosts on report	Hosts in the file that matched an asset in NxSAM
Unmapped hosts	Hosts in the file with no matching asset — their findings had nowhere to land
Invalid hosts	Rows whose host could not be read at all

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Figure	Means
Ignored hosts	Hosts deliberately excluded from this audit's scope
Overridden hosts	Hosts whose existing data this upload replaced

Findings

Figure	Means
Total instances added	What actually landed
Duplicate instances	The same finding on the same host more than once in the file
Invalid instances	Rows that could not be parsed into a finding
Ignored instances on merge	Existing findings the merge left untouched
Severity ignored	Findings filtered out by the severity configuration
Vulnerability type ignored	Findings filtered out by type

Unmapped hosts is the number to act on

An unmapped host means the scanner assessed something NxSAM does not know about. Those findings are not hidden or filtered — they were never created, because there was no asset to attach them to.

A steadily growing unmapped count is an inventory problem surfacing as a scanning problem, and it is invisible everywhere else in the product.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

⚠ Severity-ignored and type-ignored are configuration, not defects

Both counters reflect filters your organisation set deliberately — commonly dropping informational findings at import to keep volumes manageable. A customer asking why their scanner reports more findings than NxSAM is usually looking at these two lines.

They apply at import. Changing the filter does not retrospectively bring back findings that earlier uploads discarded.

VA Vulnerabilities

One row is a **host**, not a finding. The count columns are described in Reading the Network Security screens.

Viewing one host's findings

Opened from a host row.

Column	Notes
Vulnerability Details	The finding, its plugin and description
Port/Protocol	The same weakness on two ports is two findings
Severity/Risk	Both the scanner's severity and the derived risk
Status	One of the eleven VA statuses
Discovered On	First seen on this host
Last Observed Date	Most recent scan that still saw it — the pair is what tells you whether a fix has landed
SLA Details	Duration and expiry

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	Notes
POC	Proof of concept, where a tester attached one

Discovered On and Last Observed Date together are the most useful pair on this screen. A finding discovered in March and last observed in March is fixed but not yet re-scanned; one last observed yesterday is still present.

Row actions here are **Vulnerability History** and **View Status History** — what changed about the finding, and who changed its status.

Overall Vulnerability Status

Groups by vulnerability instead of by host, which is what makes it worth using.

Column	Notes
Vulnerability	The weakness itself, once
Port/Protocol	Where it appears
Severity	As derived
Status	Aggregate state across the hosts it affects
Audit	Which audit reported it
Open/Close Date	When it opened, and closed if it has

A scan returning four thousand findings across two hundred hosts is often sixty distinct vulnerabilities. This screen shows those sixty, and one of them patched everywhere may close a third of the total.

PT Audits

Same shape as VA with a smaller action set: **Vulnerability Overview**, **View Vulnerabilities**, **Manage Audit Scope**, **Assign Auditors**, **Edit Tags**, **View Status History**, **Delete Audit**, plus **Download Audit Status Report**, which takes a start and end date and produces a status summary for that window.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

PT Vulnerabilities — three views of one audit

By asset

Column	Notes
Asset ID / Asset	The host tested
Accessibility	`External` or `Internal` — the only two values
Port	Where the tester worked
No. of Vulnerabilities	Found on this asset
Info Gathered	Reconnaissance recorded against the asset, separate from findings

Accessibility drives prioritisation more than severity does. A Medium on an external host is usually more urgent than a High on an internal one, and this is the column that says which is which.

Info Gathered is what the tester learned that is not itself a weakness — versions, banners, enumerated accounts. It is uploaded separately, has its own type and document, and is worth reading before disputing a finding: it is often the evidence that the finding was reachable.

Grouped

Title and **No. of Vulnerabilities** — findings collapsed by name, for seeing that one issue affects nine hosts.

Flat

Column	Notes
Vulnerability	The finding
Host / Port	Where

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	Notes
Risk	The tester's rating
Validation	`Saved`, `Submitted` or `Approved` — three values only
Status	One of the eleven PT statuses
Artifacts	Screenshots and files the tester attached as proof

Row actions: **Edit Vulnerability**, **Delete Vulnerability**, **Vulnerability History**.

Artifacts are the difference between a PT finding and a scanner finding. A scanner finding is reproducible by re-running the scanner; a manual one often is not. If a PT finding is disputed and has no artifacts, there is nothing to review.

Segmentation

Tests whether network separation holds.

By source — `Host Name`, `Host`, `Info`. **By destination** — `Hosts ID`, `Destination Host`, `Source Host (Host Name)`, `Port`, `Info`.

A finding is a *path*: this source reached this destination on this port. `Info` carries what was observed. The question is not how severe it is but whether the path was supposed to exist, which is why the tables pair source and destination rather than ranking by severity.

The segmentation audit list itself carries **Audit Details**, **Business Unit**, **Status**, **Auditor**, **Source Hosts** and **Requested By**. Business Unit matters more here than elsewhere: segmentation is usually tested because two business units are meant to be separated from each other, so the column names the boundary being verified.

The Nmap report view

Where a scan was run with Nmap, its raw output is viewable per host:

Column	What it holds
Port / Protocol	The port and whether TCP or UDP

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	What it holds
State	`open`, `closed` or `filtered`
Reason	Why Nmap concluded that — which packet it saw back
Service	What Nmap believes is listening
Product / Version	The software and version it fingerprinted
Extra Info	Anything further the fingerprint returned, such as an OS hint or a module list

Version and Extra Info are the two worth reading. A finding that says "outdated service" is confirmed or refuted by what the fingerprint actually reported, and a disagreement between the two usually means the service was patched without a restart — the running binary is still the old one.

The dashboard

Its two row actions are **Download PDF** and **Download PNG**, per widget — the charts are exportable individually for putting into a report or a deck without recreating them.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Working a VA result

Network VA produces the highest finding volumes in the platform, and the screens are structured around reducing that volume to something actionable. Knowing which view answers which question saves most of the time spent in this module.

Three views of the same data

View	Groups by	Answers
Vulnerabilities	Host	Which machines are worst?
Overall vulnerability status	Vulnerability	Which single fix helps most?
View vulnerability	One finding	What exactly is this, and where?

The second is the one people miss, and it is usually the most useful. A scan reporting 4,000 findings across 200 hosts is often 60 distinct vulnerabilities — and one of them patched everywhere might close a third of the total.

Working host by host through a large VA result is the slowest available approach.

The queue view

Network VA imports are large, so they are processed in batches. The queue shows those batches and their state.

Its practical use is answering "is the scan still loading?" A partly loaded scan looks exactly like a complete scan with fewer findings — there is no marker on the module screen distinguishing the two. Before investigating why a host has fewer findings than expected, confirm the import finished.

Reading a single finding

The detail view carries the evidence: the plugin or check that fired, the affected port and protocol, the scanner's output, and remediation guidance.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Two things worth checking before assigning it:

- **Port and protocol.** The same vulnerability on two ports is two findings against one host, and they may have different fixes.
- **Whether an exploit is known.** Exploit availability, not severity alone, is what distinguishes urgent from important. A Medium with a public exploit on an internet-facing host outranks a High that requires local access.

Why a host's count changed without a new scan

Three causes, in order of likelihood:

1. **SLA states moved.** Nothing about the finding changed; a date passed. Overdue counts in particular change daily with no scan activity at all.
2. **A severity mapping was edited.** Severity is derived from the score, so changing the boundaries re-classifies existing findings in bulk.
3. **The asset's grouping changed.** Move a host between groups and it leaves one report's scope and enters another's — both are then correct and different.

Why a closed finding is open again

The host was scanned again and the vulnerability was still there. NxSAM re-opens the existing finding rather than creating a new one, so its history is preserved.

The common misreading is treating this as the platform failing to record the fix. It recorded it; the next scan disagreed. Either the fix did not take, it was reverted, or — frequently on VA — it was applied to one host in a group and not the rest.

Check whether the re-opened findings are on the same hosts as before or on different ones. Different hosts means the fix worked and the rollout was incomplete, which is a distribution problem rather than a remediation one.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

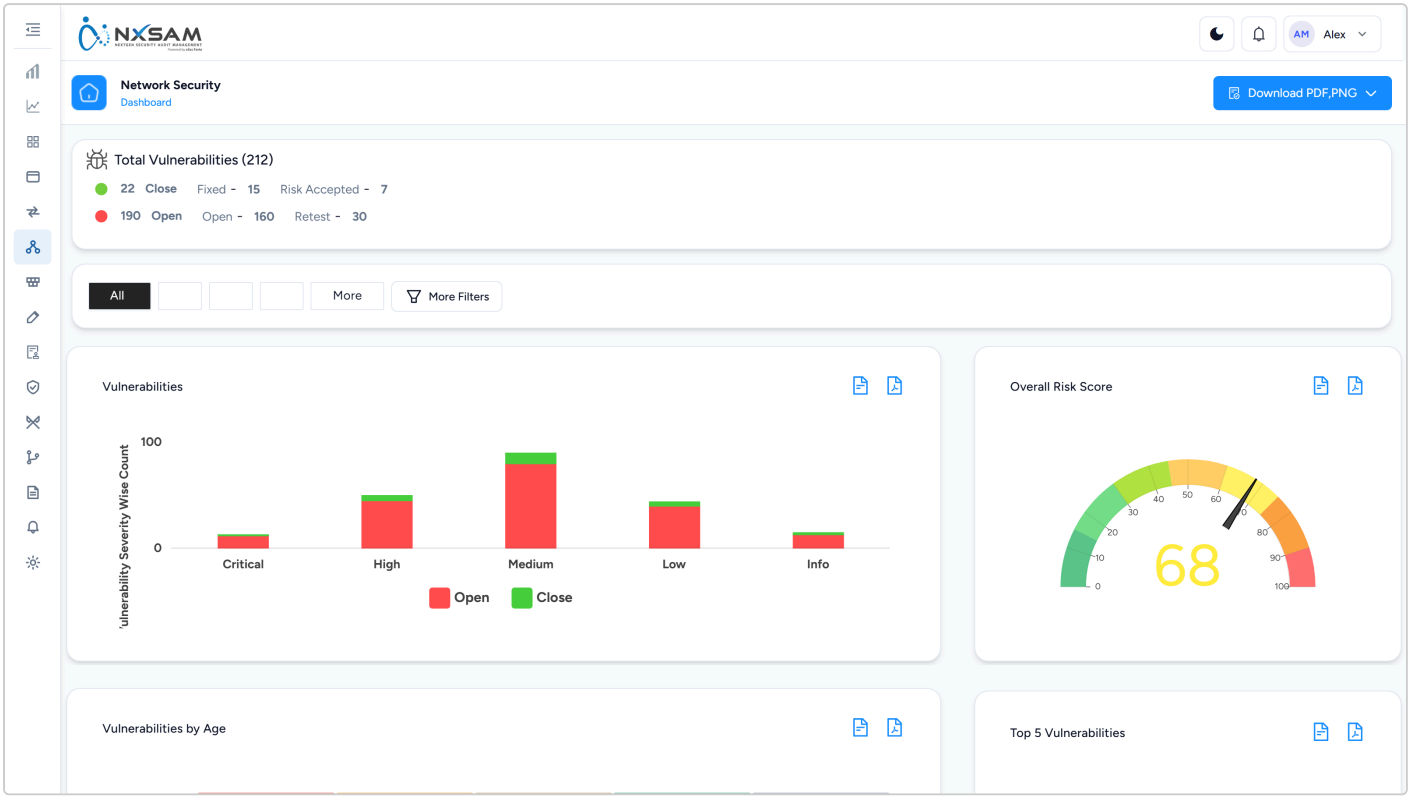
Network Security: find the right screen

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.

Network Security Dashboard

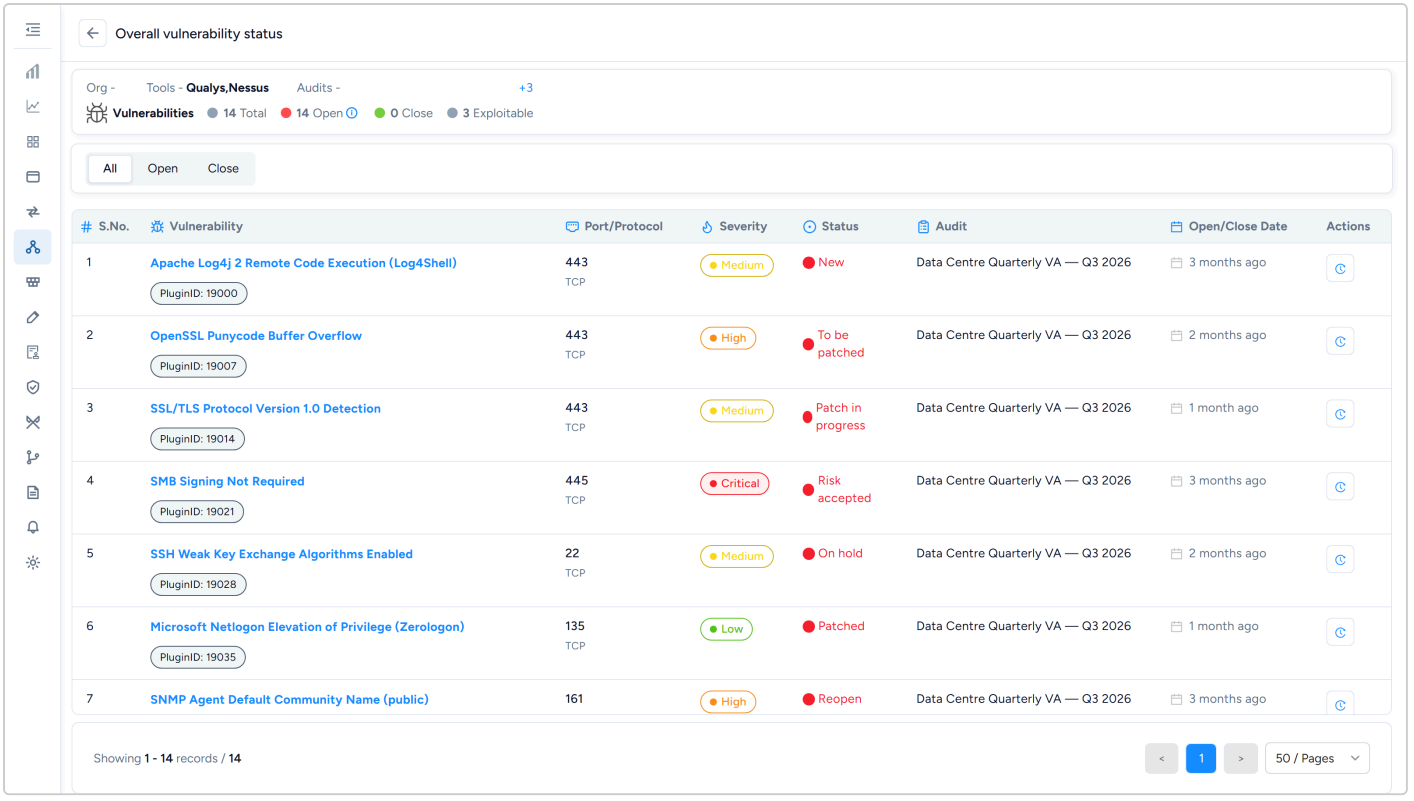
VA and PT posture together — severity mix, ageing, top hosts and the risk score trend.



Network Security → Dashboard

Overall Vulnerability Status

One host's whole history — everything ever found on it, across every audit that covered it, with what is still open.

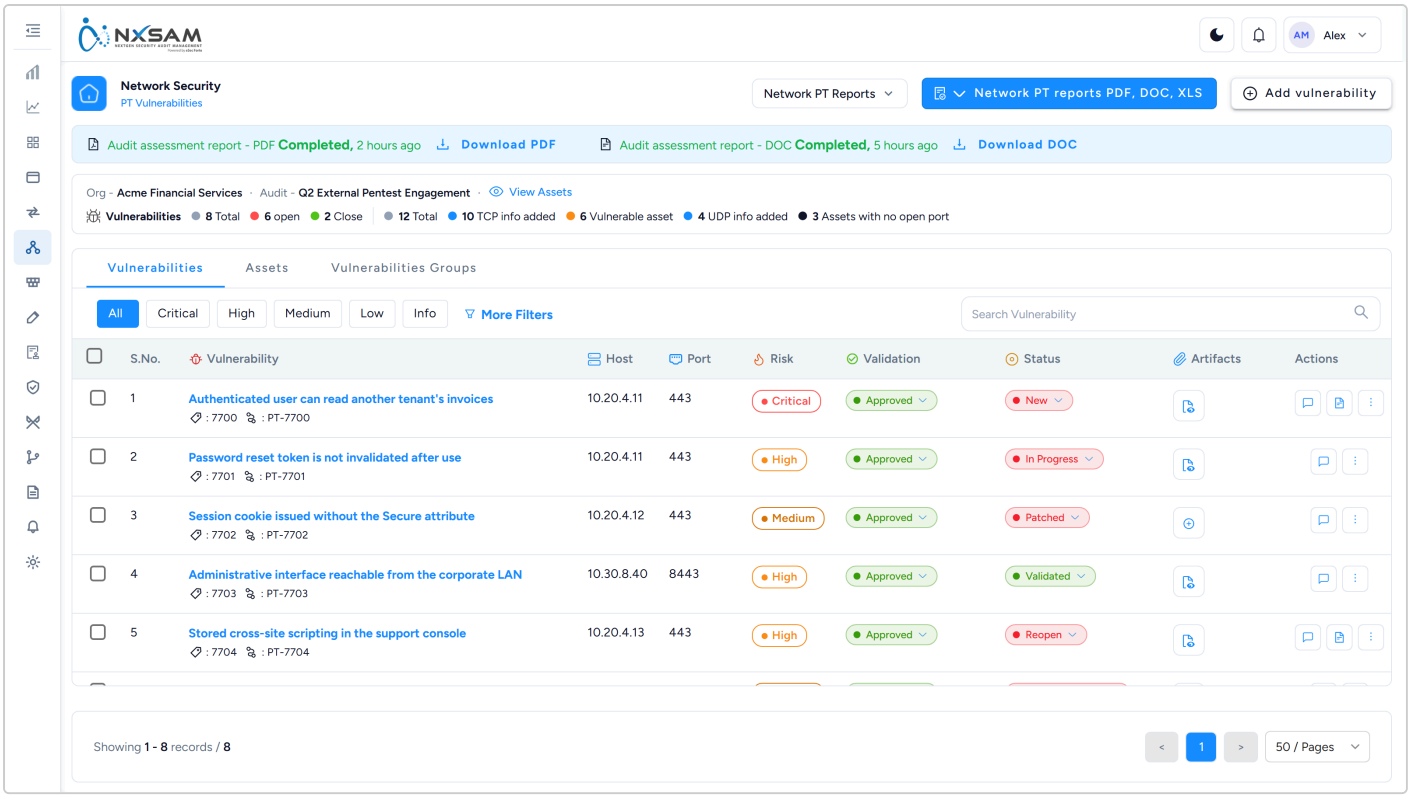


Network Security → VA Vulnerabilities → Overall Vulnerability Status

PT Findings

Findings written by a penetration tester, each with its own validation and current status. The status menu opens only once validation reaches Approved.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

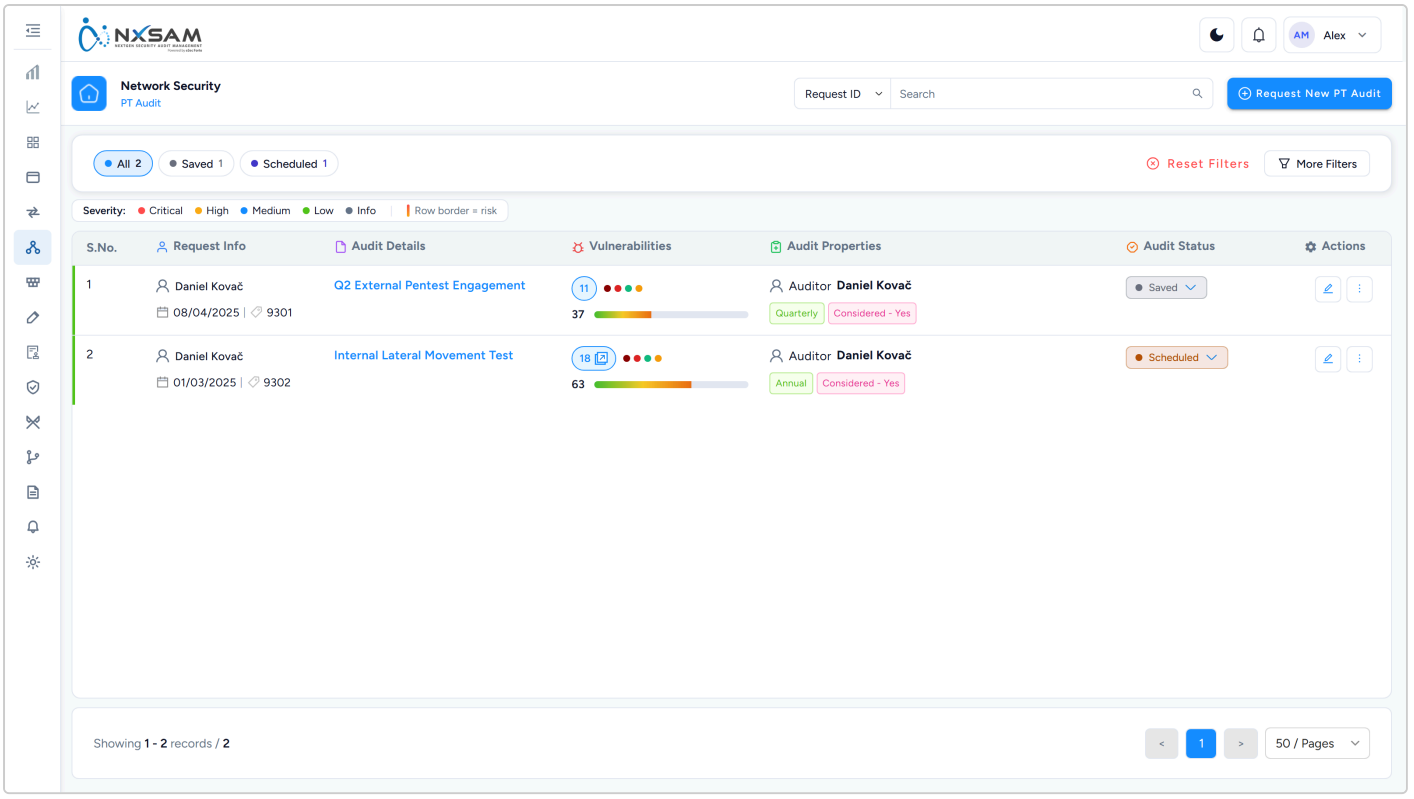


Network Security → PT Findings

Penetration Test Audits

Manual penetration tests, tracked as audits with their own findings and evidence.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

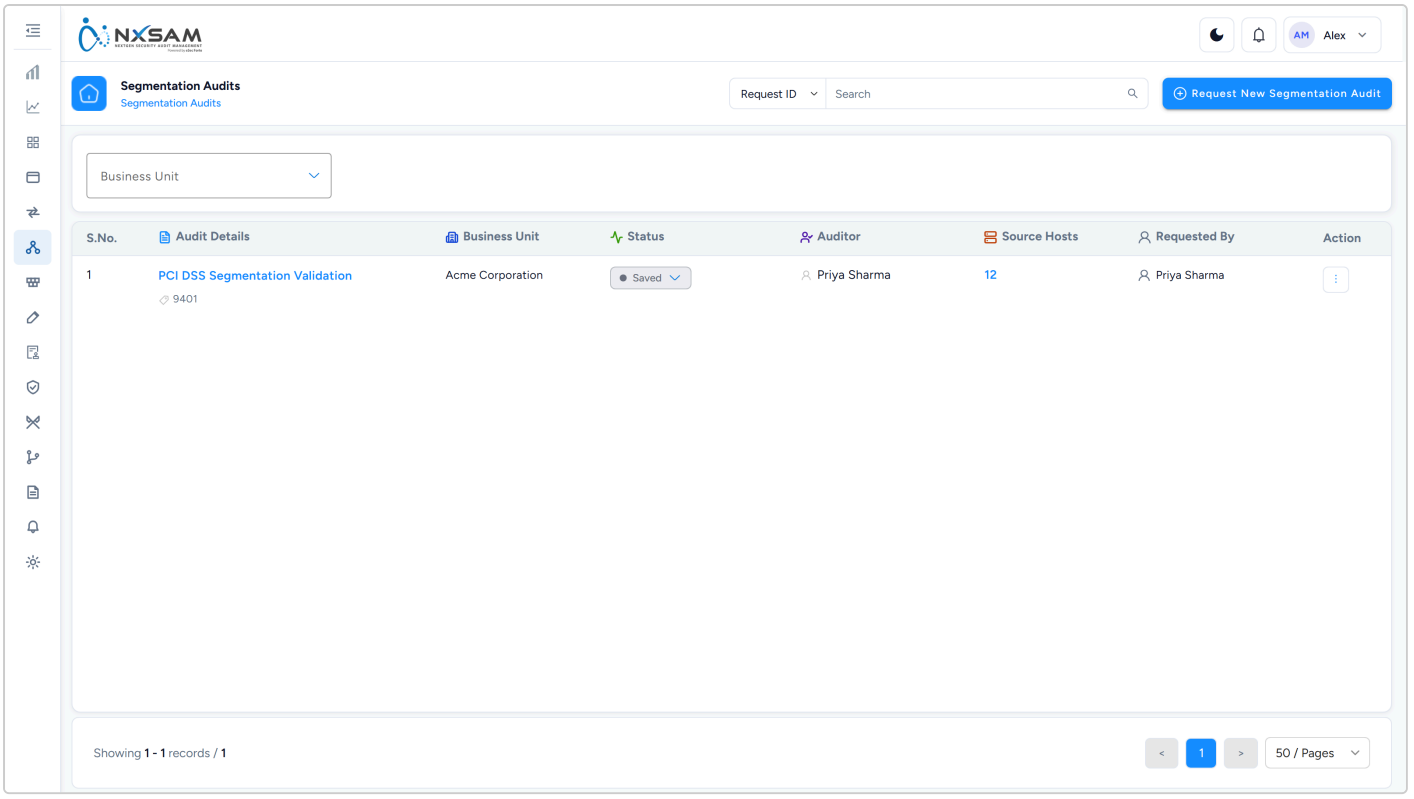


Network Security → PT Audits

Segmentation Audits

Tests that network segregation holds — which source can reach which destination on which port.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

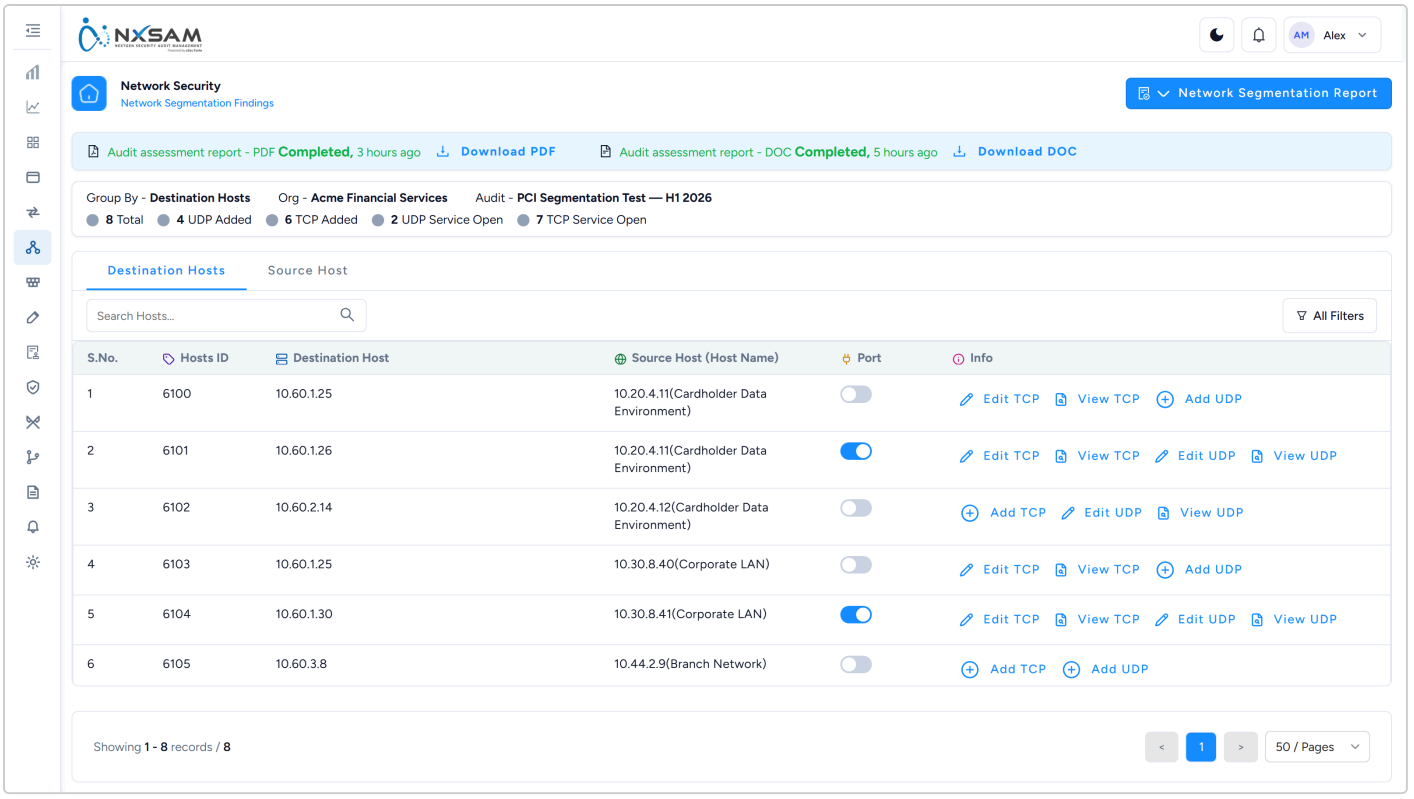


Network Security → Segmentation Audits

Segmentation Findings

Which source host reached which destination, and on which ports. A row where a service answered across a boundary is a segmentation failure.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

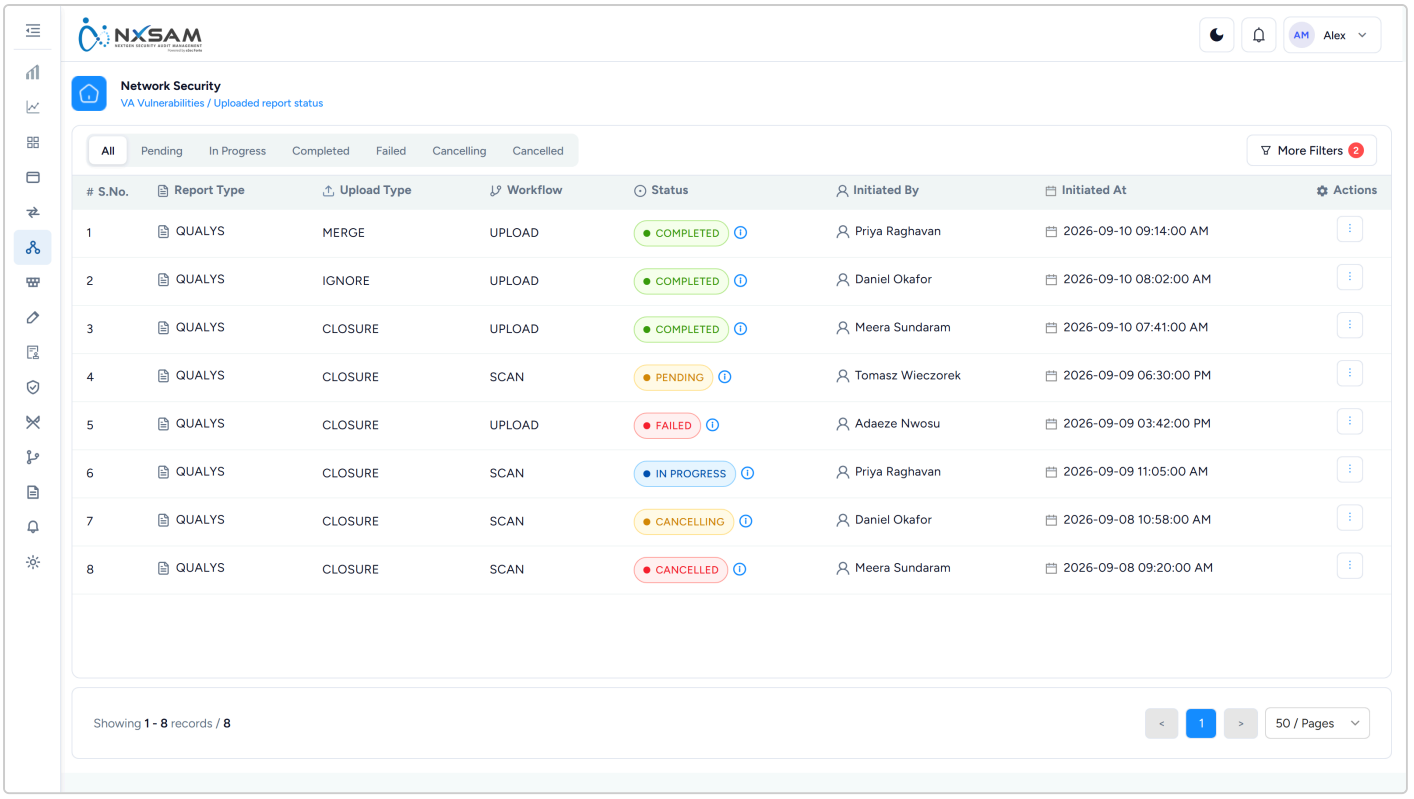


Network Security → Segmentation Findings

VA Import Queue

Batches of a VA import and their state. A partly loaded scan looks like a complete smaller scan on the module screen.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

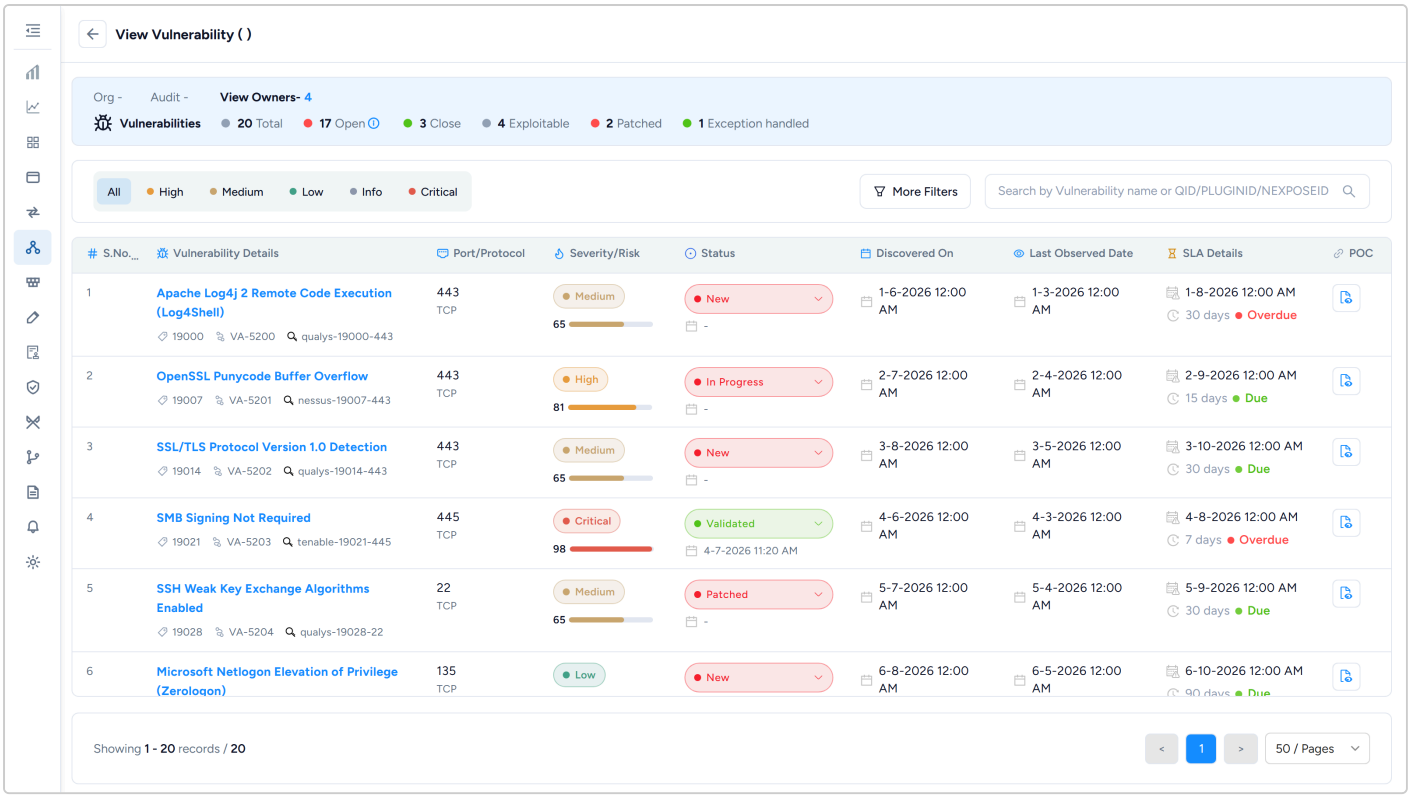


Network Security → VA → Vulnerabilities → VA Import Queue

Vulnerability Detail

One finding in full — the check that fired, affected port and protocol, scanner output and remediation guidance.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Network Security → VA Vulnerabilities → Vulnerability Detail

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.