



NxSAM Getting Started — Quick Guide

Quick reference guide for the Getting Started 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

Getting Started

- Overview
- Sign in to NxSAM

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Getting Started

Getting Started

NxSAM brings security findings from many tools into one place, tracks each one until it is fixed and verified, and reports on the result. This page gets you oriented; the rest of the manual covers each area in detail.

Signing in

Sign in with the username and password issued by your administrator.

Depending on how your organisation has configured NxSAM, you may also be asked for:

- **a verification code** shown on screen, to confirm you are not an automated client, and
- **a one-time passcode**, sent to you when you sign in.

If your organisation uses corporate sign-on, your existing directory credentials are used and NxSAM does not hold a separate password for you.

Finding your way around

The **left sidebar** is the main navigation. It lists the security modules your role can reach — you will not see every module in this manual, only the ones you have access to.

The **top bar** carries notifications and your own account menu, where you change your password and sign out.

Most module screens follow the same pattern:

1. **Filters** at the top, narrowing what is listed below.
2. **A list or table** of records.
3. **Actions** on each row, and sometimes in bulk.

Once you have learned one module's list screen, the others will feel familiar.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

What you will see first

Where you land depends on your role and configuration — commonly a dashboard summarising current posture. If you would rather start somewhere else, your administrator can change the landing page.

If something is missing

The most common surprise for new users is not seeing something a colleague can see. This is almost always intentional:

- **Modules** are shown by role. If a module is absent from your sidebar, your role does not include it.
- **Assets and findings** are shown by ownership. You see the assets you are responsible for.

Neither is a fault, and neither is fixed by refreshing. Both are resolved by an administrator adjusting your role or asset ownership.

Changing your password

Use the account menu in the top bar. If your organisation uses corporate sign-on, change your password there instead — NxSAM will not hold one for you.

Notifications

The bell in the top bar collects things that need your attention — findings assigned to you, approaching SLA dates, and requests awaiting your approval. Depending on configuration you may also receive some of these by email.

Where to go next

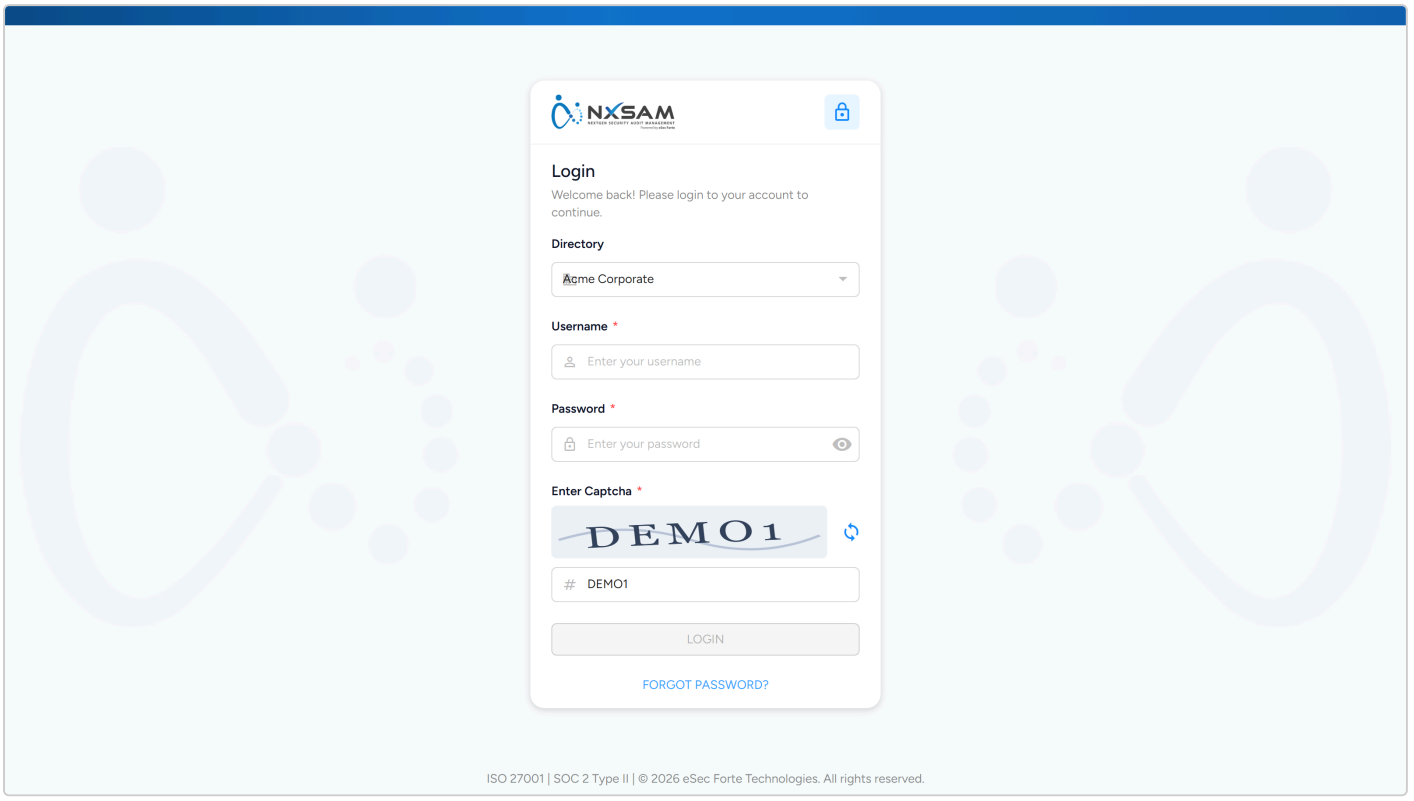
Read How NxSAM Works before diving into a specific module. It explains assets, audits, vulnerabilities and SLAs — the four ideas everything else is built from, and understanding them once saves confusion in every module.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Sign in to NxSAM

1. Open the NxSAM address your administrator gave you.
2. Enter your username and password.
3. Choose your **Directory**, if the field is shown.
4. Complete any additional verification your organisation has enabled.

The screen adapts to how your organisation authenticates, so what you see depends on your deployment.



The sign-in screen, with a directory selector and captcha enabled

The fields

Field	When it appears
Username	Always

Field	When it appears
Password	Always
Directory	Only when more than one Active Directory is configured
Captcha	When enabled for the deployment
OTP	When two-factor sign-in is enabled for your account

Choosing a directory

If your organisation authenticates against more than one Active Directory — separate domains for staff and contractors, or one per acquired entity — a **Directory** list appears above the password field. Pick the one your account belongs to.

The list is absent when only one directory is configured, because there is nothing to choose. It is also absent for accounts that sign in with an NxSAM password rather than a directory.

Signing in against the wrong directory looks like a wrong password

The credentials are checked against the directory you selected. A valid username and password fail if they belong to a different directory, and the message is the same one you get for a genuinely wrong password.

If you are certain the password is right, check the Directory selection before asking for a reset.

When sign-in fails

What you see	Usual cause
Invalid credentials, and you are sure they are right	The wrong **Directory** is selected

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

What you see	Usual cause
Account locked	Too many failed attempts — an administrator clears it with **Unlock User**
Signed in, then immediately returned to sign-in	The session was ended elsewhere, or your account was deactivated
No OTP arrives	Check the mobile or email on your account with an administrator

An administrator can see whether the platform accepted or rejected the attempt, and — for directory accounts — what the directory replied. Ask them to check the sign-in and directory logs rather than retrying repeatedly, which can lock the account.

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.