HOUSEBLEND

HOUSEBLEND / RESEARCH & PRACTICAL GUIDANCE

NetSuite 2FA Required for All Roles in 2027.1: What Breaks

> Make NetSuite work better for your finance and operations teams with Houseblend. We help design, implement, integrate and improve ERP systems, with practical support for the people who use them every day.

Published by Houseblend · 2026-11-12 · netsuite 2fa required for all roles · netsuite 2027.1 2fa · require 2fa for all roles · netsuite two-factor authentication · netsuite 2fa integrations · netsuite nlauth 2027.1 · netsuite sso 2fa · netsuite release preview · netsuite access controls · netsuite itgc

Original article: https://www.houseblend.io/articles/netsuite-2027-1-require-2fa-all-roles



In this article

1. Executive Summary
2. Introduction and Background
3. Key Changes
4. Who Breaks First: Login Types and Remediation Owners
5. Implementation Considerations and Process Changes
6. Data Analysis and Evidence
7. Implications and Future Directions
8. Frequently Asked Questions (FAQs)
9. Conclusion

Executive Summary

Oracle's documentation describes a **Require 2FA for All Roles** setting that administrators could switch on from **21 September 2026** (www.ebenstead.com), and states that "In NetSuite 2027.1, the Require 2FA for All Roles feature will be enabled automatically" (docs.oracle.com). The same release note says "Administrators will have the option to disable the feature, which will restore the setting to the previous state" (docs.oracle.com). Before this change, only roles with high-privileged permissions required two-factor authentication (2FA) (community.oracle.com). As of November 2026, no public 2027.1 upgrade date has been located, and 2027.1 is a release label, not a universal customer upgrade date (www.curiousrubik.com).

Scope is the first open question. Oracle's help page extends the requirement to every Employee, Vendor and Partner role (docs.oracle.com), while an Oracle customer notice lists Vendor Center, Partner Center and Advanced Partner Center roles as not included (community.oracle.com). Epiq, a NetSuite partner, repeats the broader reading (epiqinfo.com). Until a Release Preview test settles it, vendor and partner portal users should be planned as in scope. Logins that authenticate through SAML or OpenID Connect (OIDC) single sign-on (SSO) are the documented exception: the SSO requirement takes precedence and the 2FA requirement is ignored (docs.oracle.com).

The operational risk sits in logins designed when a password was enough. 2FA-required roles cannot use user credentials for API authentication (nhimg.org), and a role that gains 2FA loses the SuiteAnalytics Connect data source (estuary.dev). A draft Airbyte documentation change warns that password-authenticated connections with an Employee role fail after the upgrade unless the feature is turned off (github.com), and Epiq flags script or scheduler logins that sign in to the UI with a password alone (epiqinfo.com). These are configuration and workflow patterns that surface when a stricter default arrives, not platform defects.

Administrators keep an exit. Disabling the feature restores the per-role settings previously saved on the Two-Factor Authentication Roles page (docs.oracle.com), but Oracle warns that this "significantly reduces account security" (docs.oracle.com). This report recommends a four to six week plan: inventory every login by type, test in Release Preview, enroll users by waves, document approvals and exceptions for IT general controls (ITGC) reviewers, and hand integration fixes to the OAuth 2.0 and NLAuth workstreams. A worked, editable

example for 600 users produces about 46 helpdesk hours. Unresolved as of 12 November 2026: the Vendor and Partner scope conflict, the treatment of Web Services Only roles, and whether the disable option has an end date.

Introduction and Background

This report is a pre-upgrade impact and rollout playbook for one change: NetSuite's **Require 2FA for All Roles** feature, which Oracle says becomes automatic in NetSuite 2027.1. It is written for NetSuite administrators, IT directors, controllers and security or compliance owners at mid-market accounts who must decide whether to let the default take effect, which logins to remediate first, and who owns the rollout. A secondary reader is the executive sponsoring the access review, who needs to know whether warehouse, store, vendor-portal and partner users will be locked out on upgrade day. It does not re-explain passkeys, general login setup, or the token-based authentication (TBA) and OAuth 2.0 migrations, which belong to separate guides.

Two facts frame the decision. First, 2FA is not new to NetSuite: it has been enforced for administrative permissions in all accounts since **2018.2** (docs.oracle.com), and a Celigo FAQ written around that earlier mandate recorded that NetSuite had announced plans to eventually extend the requirement to all accounts (www.celigo.com). Second, the question is operational more than commercial, and at least one guide advises defaulting to 2FA for all roles with UI access to simplify training and reduce exceptions (www.cleverence.com). What changes in 2027.1 is the population: every Employee-type user, and possibly more, moves from "2FA only if the role is privileged" to "2FA always".

Evidence quality matters. Oracle's help center and 2026.2 release note are first-party and carry the most weight. Oracle's customer notice on its community site is Oracle-authored but differs from the help page on scope. Epiq, Airbyte's pull request, a NetSuite Professionals Slack archive and several NetSuite consultancies are third-party and are used for corroboration and for integration impact, not as a substitute for Oracle's intent. Independent standards and research (CIS, NIST, the UK National Cyber Security Centre, CISA, Microsoft Research, PCAOB, ISACA) supply the control and measurement context. Claims that could not be confirmed are labeled as such.

Key Changes

Change 1: From privileged roles to every role

The change is easiest to read as a three-stage timeline.

- **Already mandatory.** 2FA for administrative permissions has been enforced in every account since 2018.2.
- **Available since 21 September 2026.** Oracle's 2026.2 release note says administrators gained an option to enable 2FA for all Employee, Vendor and Partner roles on that date (docs.oracle.com). Consultancy summaries give the same date (www.ebenstead.com).

- **Automatic in 2027.1.** The release note states the feature "will be enabled automatically", and independent summaries repeat it (www.curiousrubik.com). Oracle's August 2026 customer notice says NetSuite is planning to update 2FA rules in the 2027.1 release, and practitioners in a Slack archive describe the feature as becoming "available and enabled by default" (archive.netsuiteprofessionals.com). A consultancy timeline adds that the plan carries "the documented account exceptions" (www.ebenstead.com), and CuriousRubik, citing Oracle, says newly provisioned accounts are treated differently: only roles already designated as 2FA-required will require it (www.curiousrubik.com). That last point does not appear in Oracle's published documentation and should be verified.

NetSuite delivers two scheduled version upgrades each year, and accounts are upgraded in waves, not on one day. The New Release portlet on the Home page shows an account's own date (docs.oracle.com), and Release Preview is available twice a year, right before each release (mokuhub.com). Sandboxes are upgraded within **seven days** after production (docs.oracle.com), so a sandbox is not a reliable place to rehearse before production flips; Release Preview is. Oracle's documentation does not state a 2027.1 date or a Release Preview opening date, and this report does not assume one.

Change 2: Scope, and the source conflict

Table 1 below sets out which login populations are in scope, with the source behind each cell. The sources do not fully agree, and the table shows the disagreement openly.

Population	Oracle help page and 2026.2 release note	Oracle customer notice (August 2026)	Third-party reading	Planning stance
Employee roles	In scope: all Employee roles become 2FA-required (docs.oracle.com)	In scope: "all users with the Employee entity" in all assigned roles (community.oracle.com)	Airbyte: 2027.1 "automatically turns on" 2FA for Employee roles (github.com)	In scope
Vendor Center roles	In scope per the help page	Not included (community.oracle.com)	NHIMG and Epiq: in scope (nhimg.org)	Treat as in scope until tested
Partner Center roles	In scope per the help page	Not included	Same conflict	Treat as in scope until tested
Advanced Partner Center	Not named in Oracle's documentation	Not included	Not named by Epiq	Unknown: test
Customer Center, web store and shopper roles	Excluded: the feature "isn't available for Customer Center roles"	Not included	Excluded (mokuhub.com)	Out of scope
SAML or OIDC SSO logins	SSO takes precedence and 2FA is ignored (docs.oracle.com)	Not addressed	OIDC also unaffected, per Slack practitioners (unofficial) (archive.netsuiteprofessionals.com)	Out of scope, but the identity provider must enforce MFA

Population	Oracle help page and 2026.2 release note	Oracle customer notice (August 2026)	Third-party reading	Planning stance
Administrator roles	Already 2FA-required and cannot be removed	Unchanged	Not applicable	Already in force

The first interpretive point is that the discrepancy is real and unresolved in public documentation. A plausible reading is that the customer notice describes the automatic 2027.1 default narrowly (Employee-entity users), while the help page describes the setting's full effect when an administrator switches it on. That reading is an inference, not an Oracle statement. The planning stance therefore errs toward the broader scope: it is cheaper to discover that vendor users were never affected than to discover on upgrade day that they were. Mokuhub's pre-upgrade checklist takes the same position and names vendor and partner portal logins among those that will meet 2FA for the first time (mokuhub.com).

The second point concerns SSO. Oracle's precedence rule means an SSO-authenticated user is not challenged by NetSuite for a second factor. An independent change tracker describes the same behavior for SAML roles (netsuitechangelog.com), and a Slack practitioner says NetSuite treats compliance as handled externally (archive.netsuiteprofessionals.com). The control implication is the analyst's own: if NetSuite stops asking for a second factor, the identity provider must require MFA, or the account has quietly moved back to single-factor access for those users. NHIMG makes the same recommendation, enforcing phishing-resistant MFA in the identity provider (nhimg.org), and the CIS Controls specification treats MFA enforced through a directory service or SSO provider as a satisfactory implementation (controls-assessment-specification.readthedocs.io).

Change 3: Per-role settings lock, and what reverts

With the feature on, per-role controls stop being the source of truth. The option to change the requirement on the Two-Factor Authentication Roles page becomes unavailable (docs.oracle.com), and the setting is switched on under Setup, Company, Enable Features, in the Access section, per Oracle's help page. Only the trusted-device duration values stay editable.

The reversal path is documented. An administrator can disable the feature at any time, and the requirements previously set on the Two-Factor Authentication Roles page then apply again. Oracle attaches a warning: "Disabling this feature significantly reduces account security". Two consequences follow. First, whatever per-role designations exist today become the fallback state, so cleaning them up before the upgrade has value even if the default is accepted. Second, Oracle's documentation does not state a deadline after which the disable option disappears, which is not proof that none exists, and the decision matrix below treats disabling as a time-boxed exception.

Change 4: What happens to API and tool logins

Two statements drive most integration impact. First, 2FA-required roles cannot use user credentials for API authentication (docs.oracle.com). Second, Oracle's Designate Two-Factor Authentication Roles page says 2FA "isn't compatible with web services or SuiteAnalytics Connect" (docs.oracle.com). Independent documentation

agrees on the consequence: Estuary says a role that gains two-factor authentication loses the NetSuite2.com data source (estuary.dev), and a Salesforce help article for a Tableau connector says the NetSuite connector does not support two-factor authentication roles (help.salesforce.com).

Web Services Only roles need care. Oracle documents them as roles whose login validation checks that access is through SOAP web services, not the UI (docs.oracle.com). Oracle's documentation does not state whether Web Services Only roles are exempt from the all-roles feature. That is the most consequential unknown for integration owners, and it should be tested in Release Preview rather than assumed. Epiq's advice is to use Web Services Only roles with scoped permissions for integrations (epiqinfo.com).

Third-party evidence points the same way. Airbyte's draft documentation pull request, opened in October 2026, says connections using a username and password with an Employee role "will fail after the account upgrades, unless the admin turns the feature off" (github.com). Two cautions apply: the request is a documentation-only change (github.com) that was marked as a draft (github.com), and Airbyte's live connector page still lists username and password among supported SuiteAnalytics Connect methods (docs.airbyte.com). The behavior described is a consequence of how those connections were configured: a human-style credential used by a machine. Connector documentation written around the token-based setup still describes a user that has 2FA enabled or disabled (fivetran.com), and one business-intelligence vendor notes that NetSuite has not supported basic user and password authentication for web services since 2020.2 (cdn.cdata.com). The same design question arose in earlier cycles; a consultancy guide warned that integrations using the affected roles would stop working at the earlier 2019 deadline (www.techfino.com), and a 2018 post had warned about integrations that cannot enter the passcode (appwrap.com).

Where a script uses the NLAuth header, the timing overlaps. Oracle's 2026.2 release note states that as of 2027.1 all integrations that use NLAuth as an authentication method will stop working (docs.oracle.com), and advises "You should switch to OAuth 2.0 as soon as possible." The NCSC lists legacy-protocol bypass as an MFA anti-pattern, because services that support strong MFA may also accept legacy and weaker authentication protocols (www.ncsc.gov.uk); retiring user-credential paths is consistent with that guidance. The fixes themselves (OAuth 2.0 client credentials, TBA inventory, NLAuth retirement) are covered in the dedicated integration guides and are not repeated here.

Change 5: Enrollment, passkeys and trusted devices

Oracle's notice says users with a working 2FA setup need take no action, while anyone else must install an authenticator app on their phone and is prompted to complete setup at the first login after the upgrade (community.oracle.com). Initial setup cannot be performed from the NetSuite mobile app (docs.oracle.com), which matters for warehouse staff who only ever touch a handheld: they need one supervised desktop session first. A practitioner in the Slack archive raised the handheld-scanner concern, and the thread shows no answer (archive.netsuiteprofessionals.com).

Passkeys add an option, not a substitute for planning. As of 2026.2 a FIDO2-compliant passkey can serve as a second authentication factor, yet NetSuite still asks for an authenticator-app code periodically; a consultancy summary says the reason is to confirm the authenticator still works for 2FA-reset scenarios (adaptivesuitesolutions.com). The passkey decision itself is covered in a separate guide. The UK National

Cyber Security Centre cautions that mandating a single MFA method for everyone often frustrates users (www.ncsc.gov.uk), which supports letting users choose between authenticator apps and passkeys where Oracle allows both.

Trusted-device duration is the main tuning control. Administrators can set hours (**4, 6, 8, 12**) or days (**1 to 30**) per role (docs.oracle.com).

Who Breaks First: Login Types and Remediation Owners

Table 2 maps each login pattern to its expected behavior on upgrade and to an owner. Behavior statements marked "analyst inference" extend published rules to common configurations and should be confirmed in Release Preview.

Login type	What happens on upgrade	Evidence	Remediation owner
Named employee, UI	Prompted to enroll at first login if no working setup exists	Oracle notice (community.oracle.com)	Helpdesk with department managers
Shared mailbox or shared finance login	One authenticator on one phone cannot serve several people (analyst inference); the shared credential becomes a bottleneck at every login	Mokuhub: a shared login never set up for 2FA finds out on upgrade day (mokuhub.com)	Controller, with IT to issue named users
Scheduler or script using the UI with a password	Hits 2FA for the first time	Epiq (epiqinfo.com)	Integration owner
Vendor portal user	In scope on the help page, out per the customer notice	Conflicting Oracle sources	Procurement or AP lead, with IT
Partner portal user	Same conflict as vendor users	Conflicting Oracle sources	Channel or partner manager, with IT
Integration user with password (SOAP, REST, RESTlet)	User credentials unavailable to 2FA-required roles	Oracle	Integration owner
BI or ETL tool using SuiteAnalytics Connect with a password	Fails unless the feature is off	Salesforce connector documentation (help.salesforce.com)	Data or BI owner
Add-in users (mail or spreadsheet add-ins)	Per CloudExtend documentation, its Outlook and Excel apps can authenticate with a 2FA-required role, so users complete 2FA as usual (analyst inference on timing)	Celigo CloudExtend documentation (intercom.help)	Application owner
SAML or OIDC SSO user	2FA ignored by NetSuite; identity provider must enforce MFA	Oracle help page	Identity team

Login type	What happens on upgrade	Evidence	Remediation owner
Warehouse handheld user	Needs desktop enrollment first	Oracle login page	Warehouse supervisor, with helpdesk

The pattern across the table is that failures concentrate where one credential serves many people or a machine. Each case is a design choice made when a stricter default did not exist: a mailbox login to save a license, a scheduler that was easier to point at a UI, a connection built with whichever credential was handy. None reflects a NetSuite defect; the platform is applying a documented rule to configurations that predate it. NIST's account-management control addresses the shared-login case directly by requiring a process for changing shared or group account authenticators (raw.githubusercontent.com), and the UK NCSC's guidance for machine access is to use modern service authentication such as certificate-based credentials, not interactive MFA (www.ncsc.gov.uk).

One legacy assumption deserves retiring. Some practitioner guides describe token-based methods as exempt from human MFA because they are non-interactive (www.cleverence.com). That remains a fair description of how tokens work, but new TBA integrations cannot be created from 2027.1 (docs.oracle.com), so "exempt" is not a durable design basis.

Implementation Considerations and Process Changes

Discovery: build the inventory

The inventory should answer four questions per user: which role center, which roles, when last logged in, and whether the login is human, shared or machine. CIS Safeguard 5.1 sets a useful standard: the inventory must include both user and administrator accounts (controls-assessment-specification.readthedocs.io), and Safeguard 5.5 adds a separate inventory of service accounts (controls-assessment-specification.readthedocs.io). The steps below use standard NetSuite pages; exact menu paths should be verified in a sandbox before they go into a runbook.

- **List users and roles.** Use the Manage Users page and the Employee lists to export users, email addresses and roles.
- **Pull login history.** The Login Audit Trail is a specialized search that tracks who logged in and when. In advanced mode the Role and Employee join fields are available (docs.oracle.com).
- **Find dormant access.** A published SuiteQL pattern lists employees who have access but have not logged in within 90 days (timdietrich.me). CIS Safeguard 5.3 uses **45 days** of inactivity as its dormant-account threshold (controls-assessment-specification.readthedocs.io). Treat the query as a starting point and test it in a sandbox.
- **Check who can see the evidence.** The Login Audit Trail is restricted by permission, so a controller or auditor may need a delegated search.
- **Flag Web Services Only roles.** Search the role list for the Web Services Only box and cross-reference integration records, since login validation treats these roles differently.

- **Tag each login.** Add a column for the login type: named, shared, scheduler, vendor, partner, integration, SSO. Shared and scheduler logins are the first remediation targets.

After the upgrade, the same search can serve as a monitor for enrollment trouble.

Decision matrix

Table 3 compares the four realistic responses.

Option	What it means	Best when	Main risk	What reverts or remains
Accept the default	Let 2027.1 switch the feature on for the whole account	Most users are named, enrolled employees and integrations already use OAuth 2.0	Unprepared shared, scheduler and password-integration logins fail on day one	Nothing to revert; per-role settings are locked
Pre-enable early in Release Preview	Turn the feature on in a Release Preview account	Integrations are numerous or the Vendor and Partner scope is uncertain	Release Preview must be requested and built ahead of the upgrade (www.kore1.com)	Production is unaffected until upgraded; Estuary advises testing there first (estuary.dev)
Roll out by wave	Designate roles as 2FA-required on the Two-Factor Authentication Roles page ahead of upgrade, in stages	Large or distributed user base; limited helpdesk capacity	Waves only work before the feature is on, because the per-role control then locks	These per-role designations are the state restored if the feature is later disabled
Disable temporarily	Turn the feature off after the upgrade as a time-boxed exception	A critical integration cannot move to OAuth 2.0 before the window	Oracle: "significantly reduces account security"; Oracle does not publish a sunset date for the option	Per-role settings apply again

The matrix shows why the options are not mutually exclusive. Pre-enabling in Release Preview informs the wave plan, and the wave plan shrinks the exception list that would justify disabling. A sensible sequence is early test, then waves, then default acceptance, with disabling held in reserve and logged as an exception with an expiry date. Practitioners recommend against flipping all roles at once because it locks out anyone who has not enrolled (www.brokenrubik.com), which is exactly what the automatic default does to unenrolled users; the wave plan exists to make enrollment finish before the flip.

A four to six week rollout plan

The plan assumes the account's upgrade date is known from the New Release portlet (www.snapshotdesign.com) and counts backward from it.

- **Weeks 1 to 2, inventory and ownership.** Build the login inventory. Name one accountable owner for the rollout, one for integrations and one for vendor or partner communications. Confirm at least two full administrators can complete 2FA on different devices (www.brokenrubik.com), and keep any break-glass access monitored, since NCSC advises that alarms should trigger when emergency accounts are used (www.ncsc.gov.uk).

- **Week 2, Release Preview test.** Opt in to Release Preview, which takes roughly **five to seven calendar days** to build (www.kore1.com). Enable the feature there and test one login of each type from Table 2. Record whether Web Services Only roles and vendor roles are affected.
- **Weeks 2 to 3, integration triage.** Hand every password-based or NLAuth integration to the OAuth 2.0 and NLAuth workstreams, starting from an inventory of every NLAuth caller and every TBA integration (epiqinfo.com). Migrate one integration at a time in a sandbox or Release Preview account (adaptivesuitesolutions.com).
- **Weeks 3 to 4, wave one.** Start with administrators and roles with financial permissions (www.brokenrubik.com). This mirrors CISA's advice to start with admin accounts and employees who handle sensitive data (www.cisa.gov) and its suggestion that help desk and IT staff form an initial phase (www.cisa.gov).
- **Weeks 4 to 5, waves two and three.** Phase by department. CISA acknowledges that it can be impractical to train, enroll and support all users at the same time (www.cisa.gov), and Microsoft's guidance suggests starting with a small group and expanding (www.microsoft.com). Place warehouse and store staff in a later wave with supervised desktop enrollment.
- **Week 5 to 6, comms and cutover.** Notify vendors and partners. Publish the helpdesk reset process, which uses the User Access Reset Tool (www.sixlakesconsulting.com).
- **Trusted-device policy.** Pick a duration from the 4, 6, 8 and 12 hour or 1 to 30 day options and apply it consistently by role.

Microsoft's guidance names concern about potential user disruption as a primary obstacle to MFA adoption (www.microsoft.com), and NIST observes that account recovery is the weak point in many authentication mechanisms, advising that subscribers keep at least two separate means of authentication (pages.nist.gov). Both support investing in the reset process before enforcement. Ebenstead likewise advises preparing enrollment, passkey or authenticator and recovery guidance before rollout (www.ebenstead.com). Choosing between an authenticator app and a passkey is a user-experience call best made per population; NCSC notes that message-based methods suit only cases where no stronger method is possible (www.ncsc.gov.uk).

Audit evidence checklist

ITGC owners need evidence that the setting was approved, that the population was complete and that exceptions were managed. ISACA's description of ITGCs treats security configuration settings as access controls (www.isaca.org) and user access recertification as a separate control (www.isaca.org). PCAOB's standard on audit evidence says that when an auditor uses company-produced information, the auditor tests the accuracy and completeness of it or the controls over it (pcaobus.org), which is why exported user and role lists should be reproducible. The checklist:

- **Approval record.** Who approved accepting, deferring or disabling the setting, and when.
- **Population.** A dated export of Employee users, roles and role centers before the upgrade, with the saved-search definition retained.
- **Enrollment completion report.** A dated list showing which users completed 2FA setup, by wave.
- **Exception register.** Every login excluded or left on single-factor SSO, with owner, reason and expiry.
- **Disable log.** If the feature is turned off, the date, approver and planned re-enable date.

- **Post-upgrade review.** Failed-verification trends from the Login Audit Trail and a recertification of access.

For teams subject to payment-card rules, the PCI Security Standards Council says multi-factor authentication is required for all access into the cardholder data environment (www.pcisecuritystandards.org), and wherever a user's access can be used to connect into it (www.pcisecuritystandards.org). BDO notes that requirement 8.4.2 became mandatory after 31 March 2025 (www.bdo.com). Readers should confirm scoping with their qualified assessor or auditor; this report does not substitute for that advice.

Data Analysis and Evidence

What the measurements say about MFA

Two quantitative claims circulate. Microsoft's 2019 blog says MFA can block over **99.9 percent** of account compromise attacks (www.microsoft.com), and the post gives no method. Microsoft Research's later preprint, using Azure Active Directory data, estimates that MFA reduces the risk of compromise by **99.22%** across the entire population (arxiv.org) and by **98.56%** in cases of leaked credentials (arxiv.org). Both figures come from the same vendor, but the preprint is more defensible because its method is published. Microsoft's 2025 Digital Defense Report summary narrows the claim to phishing-resistant MFA, which it says has proven to prevent up to 99 percent of mass password-guessing identity attacks (news.microsoft.com). CISA states that users who enable MFA are significantly less likely to get hacked (www.cisa.gov), while noting that FIDO/WebAuthn is the only widely available phishing-resistant authentication (www.cisa.gov). The NCSC takes a pragmatic view: any implementation of MFA is still superior to reliance on passwords alone (www.ncsc.gov.uk).

Australia's Cyber Security Centre goes further and says phishing-resistant MFA should be implemented for all online services (www.cyber.gov.au). Context keeps the figures honest. Verizon's 2026 data breach report summary says exploitation of vulnerabilities is now the most common initial access vector (www.verizon.com), and its landing page says vulnerabilities are "beating stolen passwords as the top way attackers get in" (www.verizon.com). MFA addresses credential abuse, not every entry path, so the setting is one control among several. On adoption, Okta's own customer data show MFA used by **66%** of workforce users and **91%** of administrators in data it reported in October 2024 (www.okta.com), a reminder that universal enforcement is still not the norm.

Helpdesk load: an editable planner

No public benchmark exists for NetSuite 2FA enrollment support effort. The only unit cost found from an identifiable originator is a Forrester Total Economic Impact study commissioned by Microsoft, which uses **$15** as the average cost to resolve a password-related help desk ticket (tei.forrester.com). It is a composite assumption for a different workflow, and the same study notes that when users do not fully enroll, requests keep reaching the help desk (tei.forrester.com).

(Hypothetical Example) Assume 600 Employee-role users in three waves of 60, 240 and 300. Assume 30% need assisted enrollment at 12 minutes each and 5% need an administrator reset at 20 minutes each. All inputs are editable assumptions, not measurements.

- **Wave 1 (60 users):** 18 assisted × 12 min + 3 resets × 20 min = 276 minutes, about 4.6 hours.
- **Wave 2 (240 users):** 72 assisted × 12 min + 12 resets × 20 min = 1,104 minutes, about 18.4 hours.
- **Wave 3 (300 users):** 90 assisted × 12 min + 15 resets × 20 min = 1,380 minutes, 23.0 hours.
- **Total:** 2,760 minutes, **46 hours**. At 210 tickets and the Forrester composite of $15 per ticket, direct handling cost would be about **$3,150**, a figure that excludes user downtime beyond what the composite includes and should be replaced with the organization's own rate.

The planner's value is sensitivity. Doubling the assisted share to 60% raises the total to about **82 hours** (360 assisted × 12 min + 30 resets × 20 min = 4,920 minutes), which is why moving shared and warehouse users into later, supervised waves matters more than the per-ticket rate.

How well the sources agree

- **Automatic enablement in 2027.1:** confirmed by Oracle's release note and consistent across the customer notice, a partner guide (www.brokenrubik.com), CuriousRubik (www.curiousrubik.com) and a Japanese practitioner's schedule, which summarizes the release as OAuth 2.0 for new integrations and 2FA for all employee users (migetsu.com).
- **Availability on 21 September 2026:** Oracle's release note and independent summaries agree.
- **Vendor and Partner scope:** unresolved, as Table 1 shows.
- **TBA final retirement:** Oracle's release note says TBA end of support is tentatively planned for **2028.2**, while a consultancy summary gives a tentative 2028.1 (www.tacsolutionsgroup.com). Use Oracle's tentative date and recheck before planning.
- **Web Services Only treatment and any sunset of the disable option:** Oracle's documentation does not address either.

Implications and Future Directions

The 2FA default arrives alongside other authentication changes, so the realistic workload is combined. Oracle states that support for SOAP web services and TBA is ending in NetSuite 2028.2, without hedging in its authentication chapter (docs.oracle.com), although its 2026.2 release note calls the TBA end of support "tentatively planned for the 2028.2 release" (docs.oracle.com). Recheck before fixing a plan. Oracle also states that new TBA integrations cannot be created from 2027.1. A password-based integration therefore faces more than one deadline, and fixing the 2FA exposure by moving to OAuth 2.0 also addresses the next. Connector vendors are adapting: Celigo's documentation expected OAuth 2.0 support in its October 2026 release (docs.celigo.com). One vendor reports that Oracle told it existing customers can create new access tokens on a pre-2027.1 integration record after 2027.1; that is not in Oracle's published documentation and should be verified (www.apideck.com). A Japanese practitioner's one-line summary captures the direction for planners: new integrations on OAuth 2.0, all employee users on 2FA (migetsu.com).

Three developments are worth watching: Oracle's 2027.1 release notes, which had not been published at the time of writing; any statement about how long the disable option remains; and clarification of whether Vendor and Partner roles are in the automatic scope. Organizations that rely on SSO should also confirm that the identity provider enforces MFA, since NetSuite will not. The How to Harden NetSuite guide gives the control-level framing: require 2FA for all NetSuite users, especially those with financial data access

(howtoharden.com). The UK NCSC adds that all accounts with access to sensitive data should have MFA enforced (www.ncsc.gov.uk), and CIS Safeguard 6.5 requires it for all administrative access accounts (controls-assessment-specification.readthedocs.io).

For teams that lack the capacity to run discovery, test and enrollment in parallel with a close or a peak season, outside assessment is a reasonable option. Houseblend, the publisher of this report, is a Montréal NetSuite consultancy that offers NetSuite administration and integration support of this kind, as do other NetSuite partners. The decision should rest on internal capacity and the size of the exception list, not on the 2FA change alone.

Frequently Asked Questions (FAQs)

Is NetSuite 2FA required for all roles?

Oracle says it will be: the feature "will be enabled automatically" in 2027.1. Customer Center roles are excluded (mokuhub.com), and SSO logins are governed by the identity provider.

What is the NetSuite 2027.1 2FA change?

It moves 2FA from privileged roles only to all Employee roles and, per Oracle's help page as summarized by NHIMG, Vendor and Partner roles (nhimg.org), with the per-role setting locked while the feature is on.

Which integrations break?

Those that rely on user credentials: 2FA-required roles cannot use them for API authentication (nhimg.org), and password-authenticated SuiteAnalytics Connect connections are reported to fail unless the feature is off. Scripts that sign in to the UI with a password alone hit 2FA for the first time.

Does 2FA work with token-based authentication?

Tokens avoid an interactive prompt, which is why some guides call them exempt (www.cleverence.com), but new TBA integrations are blocked from 2027.1 (erppeers.com). The migration path is covered in the separate TBA and OAuth 2.0 guides.

Can roles be exempted?

Not individually while the feature is on, because the option to change the requirement is unavailable. SSO roles are the documented exception. Disabling the feature account-wide restores earlier per-role settings, at a security cost Oracle describes as significant (docs.oracle.com).

What about service accounts and API users?

Treat each as an integration login: use roles and credentials designed for machine access, with scoped permissions. Oracle's documentation does not say whether Web Services Only roles are affected by the feature, so test it.

How does SSO interact with 2FA?

When a user authenticates by SAML or OIDC, NetSuite ignores the 2FA requirement (netsuitechangelog.com), and the identity provider should enforce MFA.

What belongs in the upgrade checklist and the login audit trail report?

Inventory by login type, Release Preview test, wave plan, reset process and an exception register. For evidence, a saved Login Audit Trail search with Role and Employee joins, exported to CSV (docs.oracle.com), supports the population and post-upgrade review.

What if a user loses their authenticator?

An administrator can reset 2FA through the User Access Reset Tool (www.sixlakesconsulting.com).

Conclusion

Oracle's documentation supports three firm conclusions: the feature has been available since 21 September 2026, it is stated to switch on automatically in 2027.1, and it can be disabled with a documented security warning. Three questions remain open as of 12 November 2026: whether Vendor and Partner roles are in the automatic scope, how Web Services Only roles behave, and whether the disable option has an end date.

The practical response does not depend on those answers. Inventory every login by type, test the broad scope in Release Preview, move shared and machine logins to designs that suit them, enroll people in waves with a prepared reset process, and keep the evidence an auditor will ask for. Accounts that do this convert a default change into a scheduled, owned project; accounts that do not will meet it as a set of login failures on the day their upgrade lands. Readers with SOX, PCI or similar obligations should confirm their approach with their auditors or assessors.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.ebenstead.com/intelligence/employee-access
2. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_158921905537.html
3. https://community.oracle.com/netsuite/english/discussion/4515879/upcoming-change-two-factor-authentication-2fa-for-all-employees
4. https://www.curiousrubik.com/updates/security-deprecations
5. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/article_44130215942.html
6. https://epiqinfo.com/netsuite-user-roles-permissions-access-management
7. https://nhimg.org/oracle-netsuite-security-guide
8. https://estuary.dev/blog/netsuite-to-snowflake
9. https://github.com/airbytehq/airbyte/pull/88464
10. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_1515446005.html
11. https://www.celigo.com/blog/netsuite-two-factor-authentication-2fa-faq

12. https://www.cleverence.com/amp/articles/oracle-documentation/two-factor-authentication-2fa-netsuite-5842
13. https://archive.netsuiteprofessionals.com/t/34317132/when-the-require-2fa-for-all-employees-feature-becomes-avail
14. https://www.ebenstead.com/intelligence/timeline
15. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/article_1120120832.html
16. https://mokuhub.com/blog/netsuite-release-timeline-2026-2-to-2028-2
17. https://netsuitechangelog.com/articles/saml-single-sign-setup-netsuite
18. https://controls-assessment-specification.readthedocs.io/en/latest/control-6/control-6.3.html
19. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_1532968056.html
20. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N328126.html
21. https://help.salesforce.com/s/articleView?id=001534980&language=en_US&type=1
22. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N3424894.html
23. https://docs.airbyte.com/integrations/enterprise-connectors/source-netsuite-enterprise
24. https://fivetran.com/docs/connectors/applications/netsuite-suiteanalytics/setup-guide
25. https://cdn.cdata.com/help/DNK/powerbi/pg_connectionpowerbi.htm
26. https://www.techfino.com/blog/guide-to-dealing-with-two-factor-authentication-2fa-in-netsuite
27. https://appwrap.com/blogs/2fa-making-netsuite-more-secure
28. https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/avoiding-mfa-anti-patterns
29. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_1493300400.html
30. https://adaptivesuitesolutions.com/release-notes/2026-2-passkeys-as-2fa-replacement
31. https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/why-mfa-matters
32. https://intercom.help/celigo/en/articles/2724714-working-with-2fa-admin-full-access-and-highly-privileged-roles
33. https://raw.githubusercontent.com/usnistgov/oscal-content/main/nist.gov/SP800-53/rev5/json/NIST_SP-800-53_rev5_catalog.json
34. https://controls-assessment-specification.readthedocs.io/en/latest/control-5/control-5.1.html
35. https://controls-assessment-specification.readthedocs.io/en/latest/control-5/control-5.5.html
36. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N324233.html
37. https://timdietrich.me/blog/netsuite-suiteql-employees-not-logging-in
38. https://controls-assessment-specification.readthedocs.io/en/latest/control-5/control-5.3.html
39. https://www.kore1.com/netsuite-release-testing
40. https://www.brokenrubik.com/blog/netsuite-2fa-authenticator-guide
41. https://www.snapshotdesign.com/snapshot-blog/netsuite-release-readiness
42. https://www.ncsc.gov.uk/collection/secure-system-administration/protect-your-administration-interfaces
43. https://adaptivesuitesolutions.com/release-notes/2027-1-tba-end-of-support-oauth2-migration
44. https://www.cisa.gov/require-multifactor-authentication
45. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
46. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks

47. https://www.sixlakesconsulting.com/blogs-main/how-to-reset-2fa-in-netsuite.html
48. https://pages.nist.gov/800-63-4/sp800-63b.html
49. https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/recommended-types-of-mfa
50. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/are-it-general-controls-outdated
51. https://pcaobus.org/oversight/standards/auditing-standards/details/AS1105
52. https://www.pcisecuritystandards.org/faqs/1591
53. https://www.bdo.com/insights/digital/pci-dss-version-4-0-multi-factor-authentication
54. https://arxiv.org/abs/2305.00945
55. https://news.microsoft.com/source/asia/2026/01/07/microsoft-releases-2025-digital-defense-report-highlighting-the-changing-cyber-threat-landscape-and-the-importance-of-security-in-the-ai-era
56. https://www.cisa.gov/MFA
57. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication
58. https://www.verizon.com/business/resources/executivebriefs/2026-dbir-executive-summary.pdf
59. https://www.verizon.com/business/resources/reports/dbir
60. https://www.okta.com/blog/identity-security/phishing-resistant-mfa-shows-great-momentum
61. https://tei.forrester.com/go/Microsoft/EntraSuite/docs/Forrester_TEI_The_Total_Economic_Impact%E2%84%A2_Of_Microsoft_Entra_Suite_vA.pdf
62. https://www.brokenrubik.com/blog/netsuite-sso-setup-guide
63. https://migetsu.com/entry/netsuite-2027-yosou
64. https://www.tacsolutionsgroup.com/netsuite-2026-2-release
65. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/chapter_4369651411.html
66. https://docs.celigo.com/hc/en-us/articles/54916543775643
67. https://www.apideck.com/blog/netsuite-tba-to-oauth-2-migration
68. https://howtoharden.com/guides/netsuite
69. https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/mandating-strong-mfa-for-access-sensitive-data
70. https://controls-assessment-specification.readthedocs.io/en/latest/control-6/control-6.5.html
71. https://erppeers.com/netsuite-tba-oauth-migration
72. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_1548084502.html

THE PUBLISHER

About Houseblend

Houseblend is a NetSuite consulting firm serving finance and operations teams. We help organizations implement ERP systems, connect business applications, improve existing configurations and maintain the systems that support everyday work. Our audience includes finance leaders, controllers, operations managers, NetSuite administrators and implementation teams.

Implementation and architecture

Houseblend provides NetSuite implementation, architecture and data migration services. We help teams evaluate how business processes, reporting requirements and existing data should fit together in an ERP environment. Training supports the people responsible for adopting and operating the resulting system.

Integrations, customization and AI

Our services include NetSuite integrations and customization, as well as AI integrations and AI transformation work. These engagements connect ERP data and workflows with the broader application landscape. The right design depends on the organization's systems, controls and operating needs.

Improve and support an existing system

Houseblend offers NetSuite health checks, optimization, managed support and project rescue services. We also provide expertise for analytics and specialist workflows, including NetSuite Analytics Warehouse, warehouse management and field service management. Published educational material helps teams investigate options and prepare informed questions for their implementation or support work.

Work with Houseblend

Explore NetSuite implementation, integrations, managed support and AI integrations. Contact Houseblend to discuss your current system and priorities.

Article examples explain concepts rather than promising a particular license, product capability, delivery schedule or outcome. Engagement scope is confirmed with the Houseblend team.

Website: https://www.houseblend.io

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.