NetSuite Passkeys 2026.2: Passwordless Login and 2FA Guide

Published August 6, 2026 36 min read

NetSuite Passkeys 2026.2: Passwordless Login and 2FA Guide

Executive Summary

NetSuite 2026.2, one of Oracle NetSuite's two scheduled major platform releases delivered each year, formally introduces **passkey** support as a passwordless alternative to the traditional NetSuite login password (Source: docs.oracle.com). According to Oracle's own 2026.2 release notes, dated **July 13, 2026**, "As of July 13, 2026, all NetSuite users can set up passwordless authentication with a passkey" (Source: meridianbusiness.com). All users in all roles can register a passkey, either a **physical** authenticator such as a USB security key or a **digital** authenticator such as a device's fingerprint or face-unlock sensor, in place of a password at login (Source: docs.oracle.com).

The 2026.2 release goes further than login replacement: by default, a **FIDO2**-compliant passkey can also satisfy NetSuite's separate two-factor authentication (2FA) challenge, collapsing what was previously a password-plus-authenticator-app flow into a single cryptographic gesture (Source: docs.oracle.com). Passkeys are scoped strictly to login; a NetSuite password is still required for actions such as self-service 2FA reset (Source: docs.oracle.com). The pattern is consistent with what platform vendors report at scale: Microsoft found that "users signing in with passkeys are three times more successful at getting into their account" than with passwords (Source: microsoft.com), and the FIDO Alliance's most recent global report states that "passkeys have reached global scale with 5 billion passkeys now in active use" as of May 2026 (Source: fidoalliance.org).

This passkey rollout sits inside a broader, mandatory NetSuite authentication framework that predates 2026.2. NetSuite requires 2FA for all Administrator and other highly privileged roles by default, an enforcement Oracle's documentation traces back through all NetSuite accounts, and extends to non-interactive web services and RESTlet access as well (Source: docs.oracle.com). The 2026.2 release notes simultaneously flag the retirement of older authentication mechanisms: Token-Based Authentication (TBA) integrations will stop being creatable starting in **NetSuite 2027.1**, with existing TBA integrations tentatively losing support in 2028.1, and legacy NLAuth login for RESTlets is likewise being phased out (Source: meridianbusiness.com) (Source: docs.oracle.com).

The shift mirrors an industry-wide move away from passwords. The FIDO Alliance's own Passkey Index reports passkey sign-ins succeed 93% of the time versus 63% for other authentication methods, and that passkey adoption cut login-related help-desk incidents by 81% among surveyed organizations (Source: fidoalliance.org) (Source: fidoalliance.org). The US Cybersecurity and Infrastructure Security Agency (CISA) states plainly that "the only widely available phishing-resistant authentication is FIDO/WebAuthn authentication" (Source: cisa.gov) and urges organizations to plan a migration to it (Source: cisa.gov). NetSuite's own peers are moving in lockstep: Microsoft will make passkeys the default authentication method in Entra ID starting **September 1, 2026** (Source: microsoft.com), Salesforce will require phishing-resistant MFA for all privileged production users beginning **July 20, 2026** (Source: duo.com), and GitHub, Google Workspace, Okta, AWS, Apple, and SAP each rolled out enterprise passkey support between 2023 and 2026.

For NetSuite administrators, the practical takeaway is threefold: plan a passkey rollout that includes recovery, device-loss, shared-device, compatibility, and SSO-policy considerations; understand that passkeys replace only the login password and not the account password itself; and inventory integrations affected by the documented 2027.1 restriction on creating new TBA integrations. The global passwordless authentication market, valued at **$21.58 billion in 2025** and projected to grow at a 14.95% compound annual growth rate (CAGR) to **$75.73 billion by 2034** according to Fortune Business Insights, underscores that NetSuite's move is part of a durable, industry-wide transition rather than an isolated product update (Source: fortunebusinessinsights.com) (Source: fortunebusinessinsights.com). At the same time, IBM's 2025 Cost of a Data Breach research found that "average global costs dropped to USD 4.44 million" per breach, a reminder of what is financially at stake when authentication and access controls fail (Source: ibm.com).

Introduction and Background

Oracle NetSuite is a cloud enterprise resource planning (ERP) platform that Oracle describes as "the #1 Cloud ERP," a unified business management suite spanning financials, customer relationship management (CRM), and ecommerce (Source: docs.oracle.com). Oracle completed its acquisition of NetSuite on **November 7, 2016**, in a deal valued at $109.00 per share, or approximately **$9.3 billion** (Source: oracle.com) (Source:

investor.oracle.com). Since that acquisition, NetSuite has operated as Oracle's flagship cloud ERP for small and midsize businesses, competing against products such as SAP Business One, Microsoft Dynamics 365 Business Central, and Acumatica, the last of which now markets itself directly at companies looking to "escape from NetSuite" (Source: sap.com) (Source: microsoft.com) (Source: acumatica.com).

Because NetSuite hosts a customer's core financial, order-management, and CRM data, the strength of its login and authentication controls has long been a first-order security question for finance and IT leaders who run their business on it. NetSuite ships **two major platform releases per year**, and customers are upgraded to each in phases over a period of a few months rather than all at once, a cadence Oracle documents consistently across its release-preparation materials (Source: docs.oracle.com). This cadence produces the familiar **YYYY.1 / YYYY.2** naming convention, of which **2026.2** is the second release of calendar year 2026.

Oracle's own 2026.2 release notes state that the document summarizes the changes to NetSuite between NetSuite 2026.2 and the previous release, and every listed feature, including passkeys, remains inert until an account is actually upgraded to that version, since features described in the notes are "not available until your account is upgraded to NetSuite 2026.2" (Source: docs.oracle.com). The release-preview draft of the 2026.2 notes carries a **July 13, 2026** revision date, and NetSuite's separately dated 2026.1 release notes carry the identical July 13, 2026 revision stamp, indicating both documents were refreshed together as part of Oracle's routine release-notes maintenance cycle. The scale of what is at stake in getting this transition right is underscored by the passwordless authentication market itself, which Fortune Business Insights values at **USD 21.58 billion in 2025** and projects will keep growing at a double-digit rate for the rest of the decade (Source: fortunebusinessinsights.com).

This report explains, in depth, what a passkey is and why it is considered more secure than a password; exactly what NetSuite 2026.2 changes about login and 2FA; how NetSuite's pre-existing MFA mandate, password policy, and integration-authentication rules interact with the new passkey option; how an administrator or end user actually enables and manages a NetSuite passkey; how passkeys compare quantitatively to passwords and traditional one-time-passcode (OTP) 2FA; and how NetSuite's move fits into the wider enterprise-software shift toward passwordless, phishing-resistant login, illustrated with named rollouts at Microsoft, Google, Okta, GitHub, Salesforce, AWS, Apple, SAP, and within Oracle's own broader Fusion Cloud product line. All figures are presented **as of August 2026**, and any subsequent change to the 2026.2 release-preview terms before general availability should be checked against Oracle's current documentation.

What Are Passkeys? Definition and Technical Taxonomy

A **passkey** is not a password stored differently; it is a fundamentally different credential type built on public-key cryptography. The FIDO Alliance, the industry standards body that co-developed the underlying specifications with the World Wide Web Consortium (W3C), defines a passkey as "a FIDO authentication credential based on FIDO standards" that allows a user to sign in "with the same process that they use to unlock their device," using standard public key cryptography techniques specifically to provide phishing-resistant authentication (Source: fidoalliance.org) (Source: fidoalliance.org). The underlying technical standard is the W3C's **Web Authentication API (WebAuthn)**, which the specification itself describes as an API "enabling the creation and use of strong, attested, scoped, public key-based credentials" for authenticating users to web applications (Source: w3.org). WebAuthn is one half of the broader **FIDO2** specification set that the FIDO Alliance and W3C jointly maintain, and it is FIDO2 compliance, specifically, that NetSuite requires for a passkey to also serve as a 2FA factor, discussed further below.

The cryptographic mechanics explain why passkeys resist phishing in a way passwords structurally cannot. When a passkey is created, the device generates a mathematically linked public and private key pair; the private key never leaves the user's device or its secure hardware enclave, while the public key is registered with the service. Passkey Central, the FIDO Alliance's implementation-guidance resource, explains that "the online service does not have the equivalent of a password hash" to steal in a server breach (Source: passkeycentral.org), and that "by design, a passkey is only presented to the site it was registered with" (Source: passkeycentral.org). Passkey Central's companion security page adds that this protection is enforced through an origin check that "requires an exact match between the domain the passkey was issued to" and the domain requesting authentication (Source: passkeycentral.org), which is precisely the mechanism a lookalike phishing domain cannot satisfy. The federal government's own guidance echoes the same logic: NIST Special Publication 800-63B frames the underlying threat model as protecting against "attempts by fraudulent verifiers and RPs [relying parties] to fool an unwary claimant" into authenticating on the wrong site, a class of attack that FIDO2's origin binding is specifically engineered to close (Source: pages.nist.gov).

NetSuite's own documentation adopts the FIDO Alliance's taxonomy directly, distinguishing two passkey form factors. A **physical** passkey is "a piece of hardware, for example portable USB tokens" such as a YubiKey, while a **digital** passkey lives on a device and is unlocked with a biometric gesture such as a fingerprint or face scan; Oracle's guidance is explicit that not all passkey-branded products meet the same bar, advising that "when creating a new passkey, always use a FIDO-certified option" (Source: docs.oracle.com) (Source: docs.oracle.com).

It is worth stating plainly what a passkey is not, because the terminology invites confusion. A passkey is not a second password, not a recovery code, and, in NetSuite's specific implementation, not a full replacement for the account's underlying password credential; Oracle's documentation notes that a NetSuite password "is still necessary for the self-service 2FA reset" process even after a passkey is registered (Source: docs.oracle.com).

Understanding that distinction, passkey as login replacement versus password as underlying account credential, is essential to correctly reading everything that follows about NetSuite 2026.2.

NetSuite Passkeys in the 2026.2 Release

The core, headline change in **NetSuite 2026.2** is that passkey-based passwordless login moves from limited availability to a capability available to "all users in all roles in your account," who "can use a passkey instead of a password during login process to NetSuite" (Source: docs.oracle.com). The July 13, 2026 date reflects release-notes revision timing; passkeys become usable only when an individual account is upgraded to NetSuite 2026.2. The release notes specify that the feature is scoped narrowly: passkeys are available only for logging in to the account, not for authorizing other in-app actions.

The second, and arguably more consequential, change bundled into 2026.2 is that passkeys can now double as the 2FA factor NetSuite already required for privileged roles. By default, "users in your account can use their passkeys for 2FA challenge during the login process," collapsing what was previously a two-step password-then-authenticator-code flow into a single passkey gesture for eligible roles (Source: docs.oracle.com). The release notes attribute this capability formally to the new version and restrict it to certified credentials: "as of NetSuite 2026.2, users who set up a passkey that complies with FIDO2" gain this option, a restriction Oracle's help documentation also confirms directly (Source: meridianbusiness.com).

Oracle built in two safeguards against over-reliance on a single passkey. First, administrators can disable the feature account-wide through a specific setting where an admin can "check the Disable Passkey as 2FA box" under Enable Features (Source: docs.oracle.com). The 2026.2 release notes describe the practical effect of that toggle: turning it off "will require the users with FIDO2 compliant passkeys to use an authenticator app" instead (Source: meridianbusiness.com). Second, even when passkey-as-2FA remains enabled, NetSuite does not let a single credential type stand in forever without a check: "NetSuite still asks for a code from an authenticator app every three months" as a periodic backup verification, ensuring users maintain a working fallback method and are not permanently locked out of it (Source: docs.oracle.com).

Table 1 below summarizes the authentication-related changes documented in the NetSuite 2026.2 release notes, alongside their effective or planned dates.

CHANGE	DESCRIPTION	EFFECTIVE VERSION / DATE
Passkey passwordless login	All users in all roles can log in with a physical or digital passkey instead of a password after their account is upgraded	Available with the account's 2026.2 upgrade
Passkey as 2FA factor	FIDO2-compliant passkeys can satisfy NetSuite's 2FA challenge, replacing an authenticator-app code by default	2026.2
Token-Based Authentication (TBA) new-integration block	New TBA integrations for SOAP web services, REST web services, and RESTlets can no longer be created; existing integrations continue working	Effective 2027.1
TBA existing-integration end of support	Support for existing TBA integrations, excluding SuiteAnalytics Connect, is tentatively scheduled to end	Tentatively 2028.1
Mandatory PKCE for new OAuth 2.0 integrations	New integrations using the OAuth 2.0 authorization code grant flow must implement Proof Key for Code Exchange (PKCE)	Effective 2027.1 (Source: meridianbusiness.com)

Read together, the table shows that passkey support affects interactive login while the TBA and PKCE changes affect integrations. Administrators managing SuiteScript integrations or RESTlets should inventory authentication methods and plan migration to OAuth 2.0 where the documented 2027.1 restriction applies. Integration rework can require more lead time than a UI-level login change.

NetSuite's Broader Authentication Framework

Passkeys do not arrive in a vacuum; they slot into an authentication framework NetSuite has enforced for years. NetSuite's help documentation states unambiguously that "NetSuite requires two-factor authentication (2FA) for all Administrator and other highly privileged roles," a requirement that is "set as 2FA required by default" and applies across all account types, including production, sandbox, development, and Release Preview (Source:

docs.oracle.com) (Source: docs.oracle.com). This is not a change introduced by 2026.2; it has been enforced in all NetSuite accounts for essentially the entire recent history of the platform.

Critically, the mandate is not limited to interactive browser logins; it extends to non-interactive web services and RESTlet access as well, pushing 2FA-required roles toward OAuth or token-based authentication rather than raw username-and-password credentials for programmatic access. There is one documented precedence rule worth noting for organizations that also use federated identity: if a role is already configured for SAML-based single sign-on (SSO), "the SAML authentication requirement takes precedence, and the 2FA requirement is ignored" for that specific role, meaning SSO-secured roles do not stack a separate NetSuite-native 2FA challenge on top of the SSO login (Source: docs.oracle.com).

For roles that use traditional 2FA rather than a passkey, NetSuite is standards-agnostic about which authenticator app is used, accepting "any authenticator app...as long it complies with the OATH TOTP standard," the open Time-based One-Time Password (TOTP) standard implemented by apps such as Oracle Mobile Authenticator, Google Authenticator, and Microsoft Authenticator (Source: docs.oracle.com). NetSuite's password policy remains a separate, still-active layer beneath all of this: "all NetSuite accounts use the Strong policy by default," which sets the minimum password length at 10 characters (Source: docs.oracle.com). Passkeys reduce reliance on that password for day-to-day login, but they do not eliminate the underlying policy, which continues to govern the credential used for 2FA resets and any fallback login path.

Finally, the integration-authentication changes flagged in 2026.2, discussed above in Table 1, extend the same directional logic to machine-to-machine access. NetSuite's documentation confirms that "starting in NetSuite 2027.1, you will no longer be able to create new integrations" using legacy Token-Based Authentication, with existing TBA integrations tentatively losing support in the 2028.1 release and SuiteAnalytics Connect carved out as an exception (Source: docs.oracle.com). Taken together, these threads distinguish stronger credentials for interactive users from a documented transition away from TBA for new integrations. Oracle's cited TBA documentation does not announce a general NLAuth retirement. This mirrors NIST's own layered logic, discussed further in the Data Analysis section below, in which the strongest authentication requirements scale with the sensitivity of the account being protected.

How to Enable and Manage Passkeys in NetSuite

For end users, NetSuite centralizes passkey management in one place. Oracle's help documentation states that a user can "manage your passkeys using the Manage Passkeys link in the Settings portlet," which is the same portlet NetSuite users already use for personal preferences (Source: docs.oracle.com). From that link, a passkey can be used instead of a password during the login process, registering either a physical security key or a device biometric as described in the taxonomy section above. Oracle's guidance repeats its certification advice at this step: administrators and end users should "consider choosing passkeys that comply with FIDO2 specification" rather than a proprietary or uncertified implementation (Source: docs.oracle.com), since only FIDO2-compliant passkeys are eligible for the 2FA-replacement behavior described in the previous section.

Based on the documented mechanics above, the practical setup sequence for an individual NetSuite user follows a consistent order: confirm the account has been upgraded to NetSuite 2026.2 or later, since the feature is not available until that upgrade completes; open the Settings portlet and select **Manage Passkeys**; register a FIDO2-certified physical or digital authenticator rather than an uncertified option; keep the existing NetSuite password accessible, since it remains the required credential for the self-service 2FA reset workflow even after a passkey is active; and be prepared to supply an OATH TOTP authenticator-app code roughly every three months when NetSuite requests it as a backup-method check.

For administrators managing the feature at the account level, rollout considerations include locating the passkey-as-2FA toggle under Enable Features, where the opt-out is the "Disable Passkey as 2FA" checkbox; deciding whether the default passkey-as-2FA posture fits the organization's recovery, device-loss, shared-device, compatibility, and SSO policies; communicating the SAML interaction to roles already on federated SSO; and planning integration remediation separately, since passkeys address human login only. For new RESTlet and web-services integrations subject to the 2027.1 restriction, Oracle directs customers to OAuth 2.0 rather than TBA. (Source: docs.oracle.com) (Source: docs.oracle.com)

Oracle's approach to passwordless sign-in at NetSuite mirrors its own implementation elsewhere in the Oracle Cloud portfolio, an alignment discussed further in the Case Studies section below. More broadly, Oracle's identity and access management product line, Oracle Access Management, advertises the same category of capability at the platform level, "enabling passwordless entry and device-level, multifactor authentication (MFA)" that includes SMS, email, TOTP, hardware keys such as YubiKey, and FIDO2.0 (Source: oracle.com) (Source: oracle.com).

Passkeys vs Passwords vs Traditional 2FA

The most common question NetSuite administrators ask when evaluating whether to promote or mandate passkeys is a direct comparison against the credentials they already use. *Table 2* below lays out the three main login-security postures available in NetSuite side by side.

DIMENSION	PASSWORD ONLY	PASSWORD + AUTHENTICATOR-APP 2FA (OTP/TOTP)	PASSKEY (FIDO2)
Phishing resistance	None; a typed password can be entered on any lookalike site	Partial; an OTP code can still be relayed to a fake site in real time by an attacker	High; FIDO Alliance states passkeys are "always strong and phishing-resistant" by cryptographic design (Source: fidoalliance.org)
Underlying mechanism	Shared secret (the password itself)	Shared secret plus a time-based one-time code compliant with the OATH TOTP standard (Source: docs.oracle.com)	Public-key cryptography per the W3C WebAuthn API (Source: w3.org)
Server-side breach exposure	High; a stolen password database is directly exploitable	High for the password component	Low; per Passkey Central, "the online service does not have the equivalent of a password hash" to steal (Source: passkeycentral.org)
NetSuite 2026.2 role	Still required as fallback for 2FA reset even after a passkey is set up	Still requested roughly every three months as a backup check even when passkey 2FA is active	Available as login replacement and, if FIDO2-certified, as the primary 2FA factor by default (Source: docs.oracle.com)
Measured success/friction (FIDO Alliance Passkey Index)	Baseline for comparison	Included in the "other methods" 63% sign-in success-rate figure (Source: fidoalliance.org)	Not separately isolated

The interpretive point of Table 2 is that passkeys are not simply "a fourth authentication factor"; they change the security model itself. A password, even a strong one meeting NetSuite's default 10-character minimum, remains a shared secret that a phishing page, keylogger, or breached database can capture and replay. Traditional OTP-based 2FA raises the bar but does not close the phishing gap entirely, since CISA's phishing-resistant MFA fact sheet warns that common MFA factors remain "vulnerable to phishing, 'push bombing' attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities" that can intercept SMS-delivered codes (Source: cisa.gov). CISA's guidance explicitly ranks phishing-resistant MFA, the category

FIDO2 passkeys occupy, as "the most secure form of MFA" available, above OTP-based approaches (Source: cisa.gov), and CISA states flatly that "the only widely available phishing-resistant authentication is FIDO/WebAuthn authentication," which is exactly the standard underlying NetSuite's passkey feature (Source: cisa.gov). The same NIST threat model discussed above, protecting against "attempts by fraudulent verifiers and RPs" impersonating a legitimate site, is precisely what separates the "High" and "Partial" phishing-resistance ratings in the second row of Table 2 (Source: pages.nist.gov).

Data Analysis and Evidence

Quantifying the case for passkeys requires separating vendor marketing claims from independently measured or industry-body-reported figures, and NetSuite administrators evaluating whether to promote passkey adoption should weigh both categories with that distinction in mind, particularly given that IBM's research puts the average cost of a breach at millions of dollars once it occurs (Source: ibm.com).

On adoption and reliability, the FIDO Alliance's Passkey Index, compiled from FIDO Alliance member companies and published **October 13, 2025**, reports that "an average of 93% of accounts are now eligible for passkeys" across the organizations surveyed, indicating passkey rollout has reached near-universal technical availability among participating services (Source: fidoalliance.org). The same report finds a stark reliability gap between credential types: "passkey sign-ins have a 93% success rate, compared to 63% for other methods," a 30-percentage-point gap that directly reflects how often users fail to correctly enter a remembered password or a manually typed OTP code (Source: fidoalliance.org). The operational consequence shows up in support costs: organizations in the index reported "an 81% reduction in login-related help desk incidents" after passkey adoption (Source: fidoalliance.org).

On the cost of the status quo, the FIDO Alliance's own consumer survey, conducted around **World Password Day 2025** across the US, UK, China, South Korea, and Japan with 1,389 respondents, found that "at least one account compromised due to weak or stolen passwords" affected more than a third of those surveyed (Source: fidoalliance.org). The same survey documented a secondary, purely commercial cost of passwords: a meaningful share of respondents reported having "abandoned an online purchase simply because they forgot their password," a friction cost with direct analogues in enterprise software when an employee cannot access a financial system during a time-sensitive close or approval workflow (Source: fidoalliance.org).

Independent breach-pattern data offers a more nuanced picture worth reporting honestly. Verizon's Data Breach Investigations Report (DBIR), the industry's most widely cited annual breach dataset, notes in its 2026 edition that attacks which "start with software vulnerabilities" have now overtaken stolen credentials as the single most common initial breach vector, a shift from prior years when credential theft dominated (Source: verizon.com). This finding should temper any claim that passkeys alone eliminate breach risk; Verizon's own summary clarifies that breaches "continue to heavily involve the human element, including social engineering, phishing, and stolen credentials" even as vulnerability exploitation has become the single largest category (Source: verizon.com).

Market-sizing data situates NetSuite's move within a large and fast-growing category. Fortune Business Insights, in a report last updated **July 6, 2026**, values the global passwordless authentication market at **USD 21.58 billion in 2025**, projecting growth to **USD 24.85 billion in 2026** and onward to **USD 75.73 billion by 2034**, "exhibiting a CAGR of 14.95% during the forecast period" (Source: fortunebusinessinsights.com) (Source: fortunebusinessinsights.com). The same research firm separately sizes the global cloud ERP market, the category NetSuite itself competes in, at **USD 65.89 billion in 2025**, projected to reach **USD 207.59 billion by 2034** at a 13.40% CAGR (Source: fortunebusinessinsights.com) (Source: fortunebusinessinsights.com).

Beyond the FIDO Alliance and Verizon data above, a wider set of measurements from national standards bodies and individual platform vendors reinforces the same pattern. Each of the following indicators is independently sourced and helps calibrate the scale of the shift already underway:

- **NIST formalizes phishing resistance by assurance level**: NIST Special Publication 800-63B-4 states that "applications assessed at AAL2 must offer a phishing-resistant authentication option" (Source: pages.nist.gov), while reserving its highest tier for hardware-bound credentials: "syncable authenticators SHALL NOT be used at AAL3" (Source: pages.nist.gov).
- **NIST extends the mandate to the federal workforce**: the same publication states that "federal agencies SHALL require their staff, contractors, and partners to use phishing-resistant authentication" (Source: pages.nist.gov).
- **Attack volume explains the urgency**: Microsoft reported observing "a staggering 7,000 password attacks per second" across its ecosystem (Source: microsoft.com).
- **Registration volume at scale**: as of May 2025 Microsoft stated "we see nearly a million passkeys registered every day" across its user base (Source: microsoft.com).
- **Success rate and speed**: Microsoft found that "users signing in with passkeys are three times more successful at getting into their account" than with passwords, and that "passkey sign-ins are eight times faster than a password and multifactor authentication" (Source: microsoft.com)

(Source: microsoft.com).

- **Passwordless is already the Windows norm**: Microsoft reports that "more than 99% of people who sign into their Windows devices with their Microsoft account" now do so without typing a password (Source: microsoft.com).
- **Consumer scale at Google**: Google reported passkeys had been used "more than 1 billion times across over 400 million Google Accounts" within roughly two years of launch (Source: blog.google).
- **Commercial conversion impact**: Google cited a partner finding that "Dashlane is seeing a 70% increase in conversion with passkeys" compared with password-based signup flows (Source: blog.google).
- **The most current cross-industry figure**: the FIDO Alliance's State of Passkeys 2026 report, published May 7, 2026, states that "passkeys have reached global scale with 5 billion passkeys now in active use" (Source: fidoalliance.org).
- **Consumer familiarity is now mainstream**: the same 2026 report finds "90% of consumers are familiar with passkeys, and 75% have enabled them" (Source: fidoalliance.org).
- **Workforce deployment has passed the halfway mark**: the FIDO Alliance found "68% of organizations deploying, piloting, or rolling out passkeys for employee authentication" (Source: fidoalliance.org), a figure NetSuite administrators can use to benchmark their own rollout against enterprise peers.
- **The financial stakes of getting it wrong**: IBM's 2025 Cost of a Data Breach research found that "average global costs dropped to USD 4.44 million" for the typical breach, even as organizations took a mean time to "identify and contain a breach within a mean time of 241 days" (Source: ibm.com).

The rough parity in growth rate between the passwordless authentication market and the cloud ERP market, roughly 15% versus roughly 13% annually, is consistent with passwordless authentication becoming a standard, expected feature of cloud ERP and other enterprise SaaS platforms rather than a niche add-on, a pattern the case studies below confirm across a wide range of vendors beyond NetSuite itself.

Case Studies and Real-World Examples

Microsoft Entra ID: Passkeys Become the Default, Not an Option

Microsoft announced in a security blog post dated **July 13, 2026**, the same day as Oracle's 2026.2 release-notes revision, that "Microsoft will begin rolling out passkeys as the default authentication experience" in Entra ID, its enterprise identity platform used across Microsoft 365 and Azure (Source: microsoft.com). The rollout begins **September 1, 2026**, and includes an aggressive downstream deprecation: Microsoft states it "will retire Microsoft-provided telecom delivery for SMS and voice" authentication entirely by **February 1, 2027**, after which any user not already enrolled in a passkey must register one (Source: microsoft.com). Microsoft's stated justification is unusually specific and time-sensitive: the company cites "AI-enabled phishing campaigns reaching click-through rates as high as 54%," a figure suggesting that generative-AI-assisted phishing has meaningfully eroded the effectiveness of OTP-based MFA in a way that made a hard deadline, rather than a purely opt-in rollout, necessary (Source: microsoft.com). The near-identical timing of Microsoft's default-passkey shift and NetSuite's 2026.2 passkey rollout illustrates that the industry's major platforms are converging on the same response to the same threat within the same calendar year.

Salesforce: A Hard Deadline for Privileged Users

Salesforce, another major enterprise SaaS platform, set its own compliance deadline: "beginning July 20, 2026, Salesforce requires phishing-resistant MFA for all privileged production users," a category that includes passkeys among the accepted methods (Source: duo.com). Unlike NetSuite's opt-in-by-default passkey model, Salesforce's requirement for its most sensitive account tier is mandatory and hard-dated, offering a comparison point for how aggressively different enterprise SaaS vendors are willing to force the issue for their highest-risk user population.

Okta: An Early, Explicit Passwordless Pitch to Enterprises

Okta, an identity-management vendor widely used to broker single sign-on into platforms such as NetSuite, announced passkey support for its Customer Identity Cloud, powered by Auth0, on **October 4, 2023**, at its Oktane conference, describing it as support "for passkeys in early access as a passwordless authentication method" (Source: okta.com), with general availability targeted for the fourth quarter of that year: the feature was "available today in early access, and will be generally available in Q4 2023" (Source: okta.com). Okta's launch messaging, echoing the FIDO

Alliance's own framing, described the status quo it was replacing bluntly: "passwords and legacy forms of 2FA are as inconvenient as they are defenseless," language that presaged, almost three years early, the same phishing-resistance argument Microsoft and NetSuite would make in 2026 (Source: okta.com).

Google Workspace and GitHub: Consumer-Grade Convenience Reaches Business Accounts

Google extended passkey support from personal Google accounts into business accounts via an open beta launched **June 5, 2023**, when Google announced it was "extending this to business users, with the open beta launch of passkeys" for Google Workspace and Google Cloud (Source: techcrunch.com). Google's own announcement, as reported by TechCrunch, framed the launch as the culmination of years of anti-phishing engineering work: "we championed the development of physical security keys and their standardization," referring to Google's earlier role in developing hardware security keys before passkeys existed as a consumer-friendly abstraction (Source: techcrunch.com).

GitHub, the software-development platform, took a similar path: after a beta period that began earlier, GitHub made passkeys generally available to all users, stating "now, all users on GitHub.com can use passkeys to protect their account" (Source: github.blog). GitHub reported that during the beta period alone, "tens of thousands of developers have adopted them," a concrete, if broad, adoption figure for a technically sophisticated user base that is often an early indicator for enterprise-wide adoption patterns (Source: github.blog).

AWS, Apple, and SAP Extend the Same Logic

The passkey shift documented above is not confined to identity-focused platforms and the largest enterprise-software vendors; it now extends into cloud infrastructure and device-management ecosystems that indirectly touch how NetSuite users and administrators authenticate elsewhere in their technology stack.

Amazon Web Services (AWS) added passkeys as a supported multi-factor authentication method for both root and standard AWS Identity and Access Management (IAM) users, stating that "you can start to use passkeys for multi-factor authentication today in all AWS Regions" (Source: aws.amazon.com). AWS separately extended the same capability to customer-built applications: "Amazon Cognito now allows you to secure user access to your applications with passwordless authentication," effective November 2024 (Source: aws.amazon.com).

Apple, whose iCloud Keychain underpins many consumer and business passkeys, documents explicit enterprise controls: "in managed environments, passkeys support Managed Apple Accounts, including syncing via iCloud Keychain," giving IT administrators policy control over how employee passkeys sync (Source: developer.apple.com). Apple's own enterprise security messaging is blunt about the threat passkeys are meant to close: a WWDC session dedicated to workplace passkey deployment describes password-based credential theft as something that is "often the initial foothold for attackers in major breaches" (Source: developer.apple.com).

SAP, one of NetSuite's direct ERP competitors referenced earlier in this report, published its own passwordless-authentication resource page in January 2026, describing passkeys in terms nearly identical to NetSuite's own documentation: "passkeys are phishing-resistant and widely supported across modern platforms," and it directs prospective customers to "explore how SAP CIAM enables passwordless, compliant customer journeys" through SAP's Customer Identity and Access Management product (Source: sap.com) (Source: sap.com). That NetSuite's closest ERP competitor is making functionally the same argument, in the same language, within months of NetSuite's own 2026.2 rollout, is further evidence that passwordless login has become a baseline competitive expectation across the ERP category rather than a differentiator any single vendor can claim exclusively, consistent with the FIDO Alliance's finding that 68% of organizations are now deploying or piloting passkeys for their workforce (Source: fidoalliance.org).

Oracle's Own Ecosystem: Passwordless Progress and Two Cautionary Reminders

Passkeys are not unique to NetSuite within Oracle's own product portfolio. Oracle Fusion Cloud Applications, a separate enterprise applications suite from NetSuite within Oracle's broader software business, implements passwordless sign-in through OCI IAM identity domains that evaluate the authentication factors "that are available to use to sign in to Oracle Fusion Cloud Applications" once a user enters a username, indicating Oracle has standardized a similar factor-negotiation pattern across more than one major product line rather than building NetSuite's passkey feature in isolation (Source: docs.oracle.com).

It is also worth including two cautionary counterexamples, because a rigorous analysis should not present authentication improvements as a complete security solution. The first involves NetSuite directly: in August 2024, security researcher Aaron Costello of AppOmni reported that "several thousand live public SuiteCommerce websites are already affected" by an access-control misconfiguration that exposed customer personally identifiable

information (PII), a finding covered by CSO Online (Source: csoonline.com). When Costello reported the exposure to Oracle, he "was told the functionality was working as intended," meaning the issue stemmed from default access-control configuration rather than a login-authentication flaw of the kind passkeys address (Source: csoonline.com).

The second involves a separate Oracle product entirely, and is a reminder that authentication strength cannot compensate for unpatched software. In October 2025, Oracle patched "a critical E-Business Suite zero-day vulnerability tracked as CVE-2025-61882 that allows attackers to perform" unauthenticated remote code execution, according to BleepingComputer's reporting (Source: bleepingcomputer.com). The extortion group Clop exploited the flaw for mass data theft; Mandiant's chief technology officer confirmed that "Clop exploited multiple vulnerabilities in Oracle EBS which enabled them to steal large amounts of data" from multiple victim organizations (Source: bleepingcomputer.com). Oracle E-Business Suite is a separate ERP product line from NetSuite, but the incident is directly relevant to any NetSuite customer: it demonstrates that even within the same vendor's portfolio, a strong authentication story on one product line offers no protection against an unpatched application-layer vulnerability on another. A comparable dynamic played out at Workday in August 2025, when attackers accessed a third-party customer relationship management (CRM) system via social engineering as part of a wider campaign against corporate Salesforce-linked tenants; Workday's own incident disclosure stated "there is no indication of access to customer tenants or the data within them" (Source: blog.workday.com), while independent reporting from SecurityWeek noted that the company "may have joined a long list of major organizations" whose Salesforce instances were targeted in that broader social-engineering wave (Source: securityweek.com). These three examples, spanning NetSuite, Oracle E-Business Suite, and Workday, are instructive precisely because none of them is a login-credential failure of the kind passkeys are designed to prevent: they are access-control misconfiguration, unpatched remote-code-execution, and third-party social engineering, respectively, reinforcing the DBIR finding above that credential-based attacks are only one component of the total breach surface an ERP customer must manage.

Table 3 below places these rollouts on a single timeline for comparison.

VENDOR / PRODUCT	MILESTONE	DATE	SCOPE
Okta Customer Identity Cloud	Passkey support announced (early access)	October 4, 2023 (Source: okta.com)	Customer-facing identity for enterprise apps
Google Workspace / Cloud	Passkey open beta for business accounts	June 5, 2023 (Source: techcrunch.com)	Business/enterprise account login
GitHub.com	Passkeys generally available to all users	Beta adopted by "tens of thousands" before GA (Source: github.blog)	Developer account login
AWS	Passkeys added as an MFA method for root and IAM users, and to Amazon Cognito	2024 (Source: aws.amazon.com)	AWS account root, IAM, and Cognito app users
Oracle NetSuite	Passkey login and passkey-as-2FA (2026.2)	Upon account upgrade to 2026.2	All users, all roles, ERP login
SAP	Official passwordless-authentication resource page and SAP CIAM positioning published	January 2026 (Source: sap.com)	SAP customer identity and access management
Salesforce	Mandatory phishing-resistant MFA for privileged production users	July 20, 2026 (Source: duo.com)	Privileged production users
Microsoft Entra ID	Passkeys become the default authentication method	September 1, 2026 (rollout begins) (Source: microsoft.com)	All Entra ID users

The pattern the table makes visible is a roughly three-year arc, from Okta's and Google's 2023 early-access launches, through AWS's 2024 rollout and GitHub's beta-to-GA transition, to a tight cluster of mandatory or default-on enterprise deadlines from NetSuite, SAP, Salesforce, and Microsoft landing within about eight months of one another across late 2025 and 2026. That clustering is unlikely to be coincidental; it corresponds to the same period in which Microsoft cites a documented spike in AI-assisted phishing effectiveness as its rationale, suggesting the entire enterprise software industry, ERP vendors included, faced a similar threat-intelligence signal at roughly the same time.

Implications and Future Directions

For a NetSuite administrator, the near-term implication of 2026.2 is that passkey adoption should be planned with recovery, device-loss, shared-device, compatibility, and SSO-policy considerations in mind. The account password remains necessary for self-service 2FA reset, and NetSuite periodically requires an authenticator-app code to confirm that a working 2FA method remains available. (Source: docs.oracle.com) (Source: docs.oracle.com) The FIDO Alliance's Passkey Index data on the 81% reduction in login-related help-desk tickets and the 93% versus 63% sign-in success-rate gap gives finance and IT leaders a concrete, quantified business case beyond pure security posture, since password-related friction has a direct productivity cost inside a system as operationally central as an ERP platform (Source: fidoalliance.org). The fact that the FIDO Alliance's 2026 workforce survey already finds "68% of organizations deploying, piloting, or rolling out passkeys for employee authentication" means an organization that has not yet started is now behind the median, not ahead of the curve (Source: fidoalliance.org). CISA's own guidance underscores why this is not merely a convenience upgrade: FIDO/WebAuthn remains "the only widely available phishing-resistant authentication," a distinction that matters directly for a system handling financial data (Source: cisa.gov).

The medium-term implication is the integration-authentication deadline embedded in the same release. New integrations can no longer be created using Token-Based Authentication starting in NetSuite 2027.1, and new OAuth 2.0 authorization code flow integrations will require PKCE from that same release forward, so organizations with custom SuiteScript integrations, third-party connectors, or RESTlet-based automation should begin an authentication-method inventory well before the 2027.1 release window opens, rather than waiting for the tentative 2028.1 hard cutoff for existing TBA integrations. Passkeys and the integration-authentication changes are, in this sense, two halves of a single Oracle strategy: eliminate weak, phishable, or replayable credentials everywhere in the platform, for humans and machines alike, an approach that echoes NIST's own tiered assurance-level model discussed above.

Longer term, the trajectory visible across Microsoft, Salesforce, Google, Okta, GitHub, AWS, Apple, and SAP suggests NetSuite's current opt-in, admin-configurable passkey posture is likely to tighten over time rather than remain static. Microsoft's move to make passkeys the Entra ID default, with SMS and voice delivery fully retired by February 1, 2027, is a template other enterprise SaaS vendors, including Oracle, may eventually follow for their own highest-privilege roles, particularly given Microsoft's own reported rate of "a staggering 7,000 password attacks per second" across its ecosystem (Source: microsoft.com) (Source: microsoft.com). Growth projections support the same conclusion from a market-structure standpoint: a passwordless authentication market growing at a 14.95% CAGR toward $75.73 billion by 2034, alongside a FIDO-reported base of 5 billion active passkeys already in use worldwide, implies passwordless login is on track to become the default expectation across enterprise software generally, not a differentiated feature any single vendor can treat as optional marketing (Source: fortunebusinessinsights.com) (Source: fidoalliance.org).

At the same time, the Verizon DBIR finding that software-vulnerability exploitation has overtaken stolen credentials as the top initial breach vector is an important caution against treating passkeys as a complete security program (Source: verizon.com), and the 2024 SuiteCommerce access-control exposure alongside the 2025 Oracle E-Business Suite and Workday incidents demonstrate that authentication strength and authorization, configuration, and patching discipline are separate disciplines that all require ongoing attention inside a NetSuite environment (Source: csoonline.com) (Source: bleepingcomputer.com). Passkeys close a specific, well-quantified gap; they are not a substitute for role-based access review, integration credential hygiene, or the underlying password policy that remains active beneath them. The financial argument for closing that gap regardless is straightforward: IBM's research puts the average global breach cost at $4.44 million, a figure that dwarfs the administrative cost of a passkey rollout many times over (Source: ibm.com).

Conclusion

After an account is upgraded to NetSuite 2026.2, NetSuite makes passkey-based passwordless login and passkey-based 2FA available to every user in every role, while preserving the account password for self-service 2FA reset and layering in a periodic authenticator-app check. The change extends, rather than replaces, an authentication framework NetSuite has enforced for years: mandatory 2FA for Administrator and other privileged roles, a Strong password policy with a 10-character minimum by default, and a SAML precedence rule for organizations already using federated single sign-on. For integrations, Oracle documents that new TBA integrations for SOAP web services, REST web services, and RESTlets cannot be created starting in 2027.1, while existing TBA integrations continue to work; Oracle recommends OAuth 2.0 for new RESTlet and REST web-services integrations. (Source: docs.oracle.com)

The broader context supports treating this as a durable shift rather than a one-off feature. Standards bodies and regulators, including the FIDO Alliance, W3C, NIST, and CISA, converge on the same conclusion: FIDO2/WebAuthn-based passkeys are materially more phishing-resistant than passwords or OTP-based 2FA, and enterprise peers including Microsoft, Salesforce, Google, Okta, GitHub, AWS, Apple, and SAP have each rolled out equivalent capabilities on a similar or even more aggressive timeline. The FIDO Alliance's own measured data, a 93% passkey sign-in success rate against 63% for other methods, an 81% drop in login-related help-desk incidents, and a global base of 5 billion active passkeys, gives NetSuite administrators a concrete efficiency argument alongside the security one (Source: fidoalliance.org). At the same time, the Verizon DBIR's finding that software-vulnerability exploitation now outpaces stolen credentials as a breach vector, and the 2024 and 2025 incidents at NetSuite's own SuiteCommerce storefronts, Oracle E-Business Suite, and Workday, are useful reminders that passkeys solve a specific, well-defined problem, credential phishing and password reuse, and are best understood as one necessary layer within a broader security program rather than a complete substitute for access-control review, integration hygiene, and ongoing patching discipline.

Tags: netsuite passkeys, netsuite passwordless login, netsuite 2fa, netsuite mfa, fido2, webauthn, oracle netsuite, netsuite 2026.2, passwordless authentication, netsuite security

DISCLAIMER

The information contained in this document is provided for educational and informational purposes only. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

Any reliance you place on such information is strictly at your own risk. In no event will Houseblend or its representatives be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of information presented in this document.

This document may contain content generated with the assistance of artificial intelligence technologies. AI-generated content may contain errors, omissions, or inaccuracies. Readers are advised to independently verify any critical information before acting upon it.

All product names, logos, brands, trademarks, and registered trademarks mentioned in this document are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, logos, trademarks, and brands does not imply endorsement by the respective trademark holders.

This document does not constitute professional or legal advice. For specific guidance related to your business needs, please consult with appropriate qualified professionals.