NordPass | Password Manager

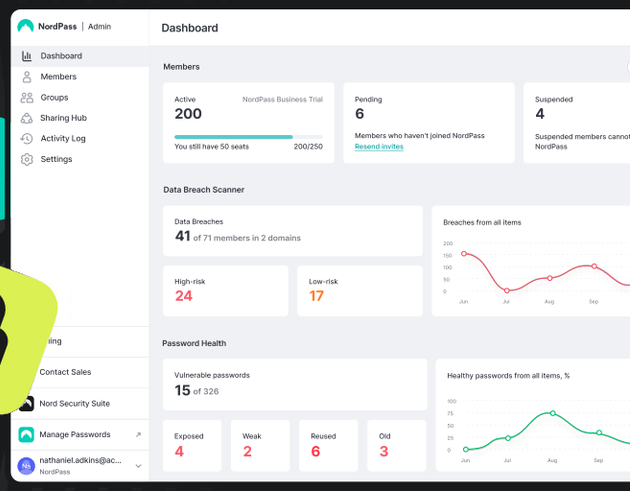
Security hardening guidelines from NordPass

Today, small businesses are the prime target of cybercriminals. Recent data reveals that 60% of small businesses identify cyber threats — including phishing, malware, and ransomware — as a top concern. Despite this, only 23% feel "very prepared" to handle a cyberattack if one occurred.

The consequences of cyberattacks on small businesses are severe. About 50% of affected businesses are forced to close due to expenses for legal fees, insurance, and technical assistance.

Implementing serious cybersecurity practices is crucial to protect your business from the growing threat. A critical component of your defense strategy should be an effective password management solution.

This document is designed to guide you through setting up and optimizing NordPass, ensuring your business's sensitive information remains secure.



User management

Multi-factor authentication (MFA)

Threat

Without MFA, accounts are highly vulnerable to breaches, exposing sensitive business data to risks like phishing, credential theft, and unauthorized access. Relying solely on passwords leaves users exposed to those threats.

Recommendation

We recommend enabling MFA for NordPass to significantly strengthen organizational account security. By design, NordPass supports only TOTP-based MFA for direct, in-app logins. Organizations using single sign-on (SSO) with Azure Entra ID, Google Workspace or Okta should offload MFA enforcement to their IdP by configuring a conditional-access rule. To ensure a seamless workflow, disable NordPass' native MFA whenever your IdP already enforces multifactor authentication. With the help of granular policy controls, you can adjust MFA settings for the whole organization, different roles or individual organization members.

See how it works in our Help Center

Single sign-on (SSO)

Threat

Recommendation

Not implementing single sign-on (SSO) increases the use of weak passwords, unauthorized access, and makes user management complex, limiting the ability to enforce multi-factor authentication (MFA) or IP restrictions, which could lead to friction and potential compliance issues.

We recommend enabling SSO options to let organization members log in to NordPass using their Google, Microsoft, or Okta credentials. When SSO is fully adopted, the Business Account password may no longer be necessary. Otherwise, keep it enabled to ensure continued access when needed.

Let us show you how it works

Business Account Session Management

Threat

Long-lived sessions that cannot be revoked or shortened increase the window of opportunity for misuse. This creates a persistent vulnerability, allowing the account to still be accessed if the device is lost and the credentials are compromised.

Recommendation

We recommend adjusting the session duration based on your organization's policy and information sensitivity.

Administrators can set a time interval of 1 hour, 4 hours, 1 day, 7 days, 30 days, or a custom time period after which members will be logged out of NordPass. To continue using NordPass, members will need to log in again, using either SSO or their Business Account credentials, and then verify their account with MFA, Master Password, or biometrics.

For optimal security, we recommend setting the interval to 7 days. After this time, members will need to log in again.

Need help? See our step-by-step guide

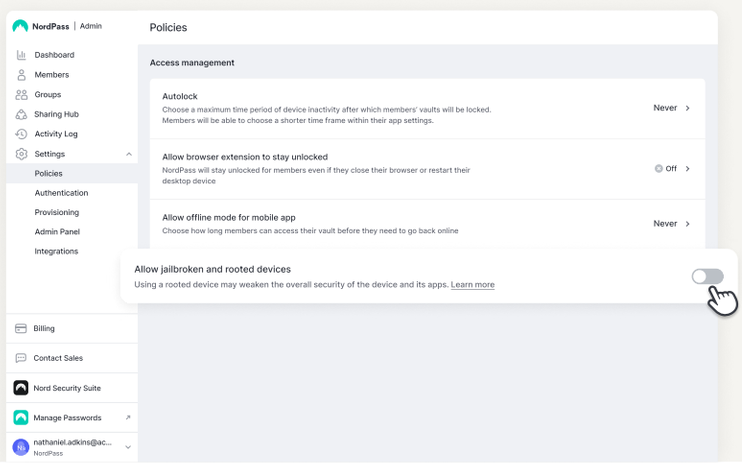
Management of access to NordPass for rooted or jailbroken devices

Threat

Rooted Android and jailbroken iOS devices pose a higher risk of data leakage, app tampering, and other security breaches.

Recommendation

We recommend that your company's admins restrict access to NordPass from such high-risk devices to safeguard user data and preserve application integrity. This feature will be defaulted, which means that any rooted or jailbroken device will be prevented from accessing NordPass.



Domain reservation

Threat

When company email domains are not reserved, employees may accidentally use their company emails to create personal NordPass accounts outside of your corporate environment. This results in unmanaged accounts that are invisible to administrators, opening significant security and compliance gaps. Manually identifying and correcting these accounts slows down onboarding, consumes administrative time, and undermines the organization's ability to enforce secure practices.

Recommendation

We recommend reserving your company's email domain(s) to ensure all employees are correctly onboarded into your NordPass organization. This feature gives administrators centralized control by preventing users from creating personal accounts with a company email. It streamlines onboarding by directing employees to the designated organization and reducing administrative overhead. It also ensures all users are governed in line with the company's security policies from day one.

Let us show you how it works

User and group provisioning

Threat

Manual management of user licenses and account access is a time-consuming process that is prone to error, potentially leaving accounts active after employees leave, increasing the risk of unauthorized access and data leaks.

Recommendation

We recommend enabling SCIM provisioning in NordPass to automate user and group management. This integration streamlines user identity and access management by automating the creation, updating, and removal of user accounts across systems. NordPass is compatible with Entra ID and Okta.

Set up user & group provisioning with Entra ID

Set up user provisioning with Entra ID

Members and ownership

Threat

If there's only one Owner in your organization and they forget or lose their Master Password, no one — not even our support team — can restore access, which poses a risk of losing access to NordPass for the entire organization. This is due to our zero-knowledge architecture and security principles.

Recommendation

We urge having at least two Owners per organization. In case one forgets their login details, the other can always recover the account. Otherwise, access to NordPass might be lost completely.

Add a second Owner to give your organization a safety net. The additional Owner can help recover access, step in in case of a lockout, or simply help manage organization.

Let us show you how it works

Threat

Improper role assignments can provide employees with unintended access to sensitive settings, credentials, or company data, introducing security risks.

Recommendation

We advise clearly defining and assigning Owner and Admin roles:

- Owners should handle critical security tasks and policy oversight, ideally held by senior leaders like the CEO, CTO, or a technically proficient manager.
- A secondary Owner should be appointed to handle day-to-day security operations, such as password resets and credential transfers. This role is best suited for an IT Manager, information security manager, or another technically proficient team member who can act quickly in case of a lockout, or simply help manage organization.
- Admins should manage routine security operations, user onboarding/offboarding, and regular security monitoring. This includes IT administrators, information security professionals, or other designated personnel managing user access and security policies.

Want a hand setting this up? Here's a quick guide

Threat

Employees on extended leave who maintain active access to business accounts pose security risks for the entire organization in terms of unauthorized access.

Recommendation

We recommend suspending NordPass access for employees on long-term leave.

Need help? See our step-by-step guide

Groups management

Threat

Without a clear credential management strategy, that includes role-based access control, your team may retain access to accounts even after changing roles — especially when access

Recommendation

We recommend leveraging Groups to organize your team efficiently and provide role-based access. Create Groups tailored to specific projects or departments, and ensure users are manually — or automatically, if the organization is using group provisioning — reassigned when their roles or project involvement changes to maintain appropriate access levels and limit security risks.

revocation is handled manually — leading to increased risk of human error, unauthorized access, and data exposure.

Let us show you how it works

Vault management

Password Policy

Threat

Employees often create weak or inconsistent passwords, leading to vulnerabilities that could compromise overall company security. Lack of centralized password control increases risk of breaches.

Recommendation

We strongly recommend setting a company-wide Password Policy to centralize credential usage rules, minimize the risk of vulnerabilities, and prevent password misuse.

You'll notice that Password Policy default settings are already in place.

One of these is the recommendation for a 20-character password — this isn't arbitrary. A randomly generated, non-dictionary 20-character password provides strong protection against today's brute-force attacks and even offers future-proofing against potential threats from quantum computing.

Leveraging granular policy controls, you can adjust policy settings for the whole organization, different roles, or individual organization members. For instance, you can have all members under a specific role adhere to stricter password length requirements than the others.

Nevertheless, certain compliance frameworks like SOC2 or PCI DSS require specific password standards. NordPass' Password Policy feature can support you in meeting those requirements and strengthening your overall security posture.

That said, you retain full control over the rules you enforce. You can align password complexity requirements with your internal policies to ensure consistency across systems.

Want a hand setting this up? Here's a quick guide

Guest Sharing

Threat

Sharing credentials externally over insecure channels and without strict rules can introduce major, unwanted security risks that could result in unauthorized access or even a full-blown breach.

Recommendation

We suggest disabling NordPass Guest Sharing unless absolutely necessary. This way you will ensure credentials are shared securely and only with verified and trusted external partners. You can also limit Guest Sharing to specific roles or individuals who directly work with external contractors.

Need help? See our step-by-step guide

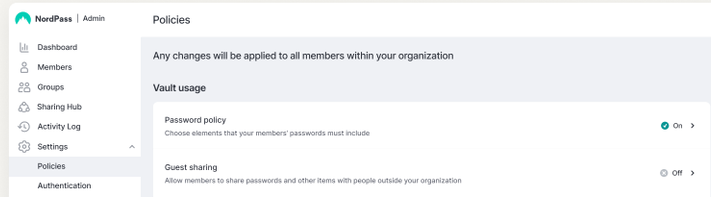
Items Exporting

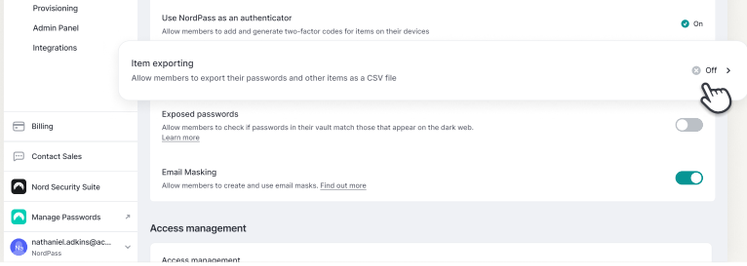
Threat

Allowing company credential exports without strict restrictions significantly increases the risk of data exposure, theft, and breaches.

Recommendation

Be sure to limit or disable credential export capabilities in NordPass to protect sensitive information. You can also adjust credential export capabilities by turning it on or off for all organization members, specific roles, or individual users.





Items Transfer

Threat

Losing track of account access when an employee leaves can result in data leaks, locked accounts, and major security threats.

Recommendation

We recommend utilizing the NordPass Items Transfer feature to maintain business continuity—specifically, to recover mission-critical credentials or clean up residual items after an employee departs. Access to deleted-user credentials in the Admin Panel should be used only in emergency situations and strictly in accordance with your organization's internal privacy policies.

Let us show you how it works

Autolock

Threat

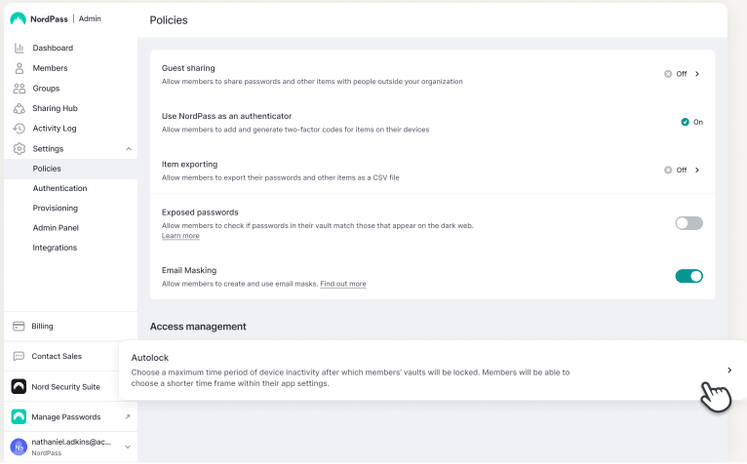
Allowing employees to set their own vault unlock durations can lead to prolonged, unattended access to their vaults that store sensitive information, which introduces major security risks.

Recommendation

We advise configuring Autolock based on the sensitivity of the data and the associated risk level of each user's role. In some low-risk, high-trust environments — such as developer workstations with persistent sessions, devices secured with full disk encryption and MFA, or workstations located in physically controlled facilities — extended autolock periods of up to a full day or even a week may be appropriate.

However, such configurations should only be considered when supported by strong compensating controls, including endpoint protection, session logging, and biometric reauthentication.

For most organizations — especially those handling sensitive data or subject to compliance requirements such as ISO 27001 or SOC 2 — we recommend a more secure default: enabling Autolock to trigger after 5 to 15 minutes of user inactivity. This helps protect vaults against walk-away risk, device theft, and unauthorized access, while maintaining a practical balance between security and usability. Using granular policy controls allows you to adjust autolock settings for the entire organization, specific roles, or individual members.



Offline Mode

Threat

With no secure access option available during a disaster or network outage, some companies have resorted to exporting their vault data and

Recommendation

You can decide which users need access to NordPass while offline. For example, Offline Mode is useful for organization members who travel frequently and often don't have internet access, but still need to log in to internal systems.

storing it in plain text. This practice poses a significant security risk and undermines the fundamental purpose of using a password manager.

As an Admin, you can customize how long users can access the NordPass vault offline: never, 1 day, 7 days, or 30 days.

To avoid prolonged access to company data, you can adjust these settings for the entire organization, specific roles, or individual members.

Once you enable Offline Mode, employees can access their credentials and other sensitive data without an internet connection. For example:

- They can seamlessly log in to internal systems or other systems that work without an internet connection by autofilling the password.
- They can also review all the documents or secure notes that the member has in their organization's vault

See how it works in our Help Center

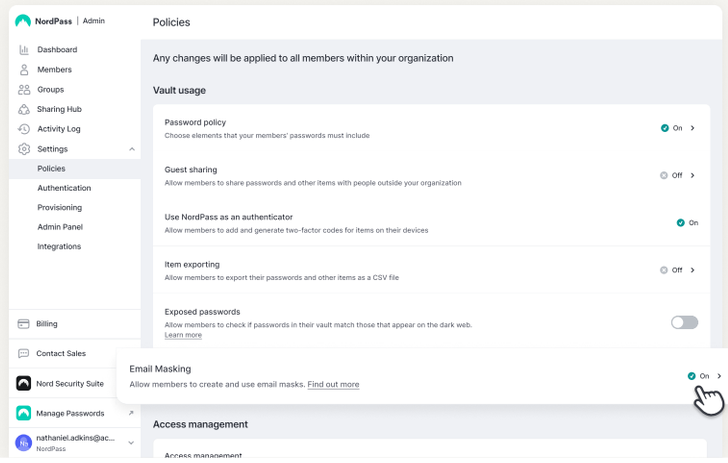
Email Masking

Threat

Using real company emails for online sign-ups, especially for testing new products/services or engaging with untrusted vendors/suppliers, can increase the risk of phishing attacks, spam, and data breaches.

Recommendation

We advise you to leverage NordPass Email Masking for online sign-ups. This feature creates unique, masked email addresses for each registration, preventing spam and phishing attempts from reaching real addresses. For example, if you want to receive correspondence from a vendor you're signing up with but don't want to expose your real email address, you can simply have the masked address forward emails to the original address you registered with NordPass. It ensures greater privacy, reduces inbox clutter, and provides an additional security layer against targeted attacks.



Authenticator

Threat

Using separate providers for credential storage and 2FA can lead to confusion, lost access, or security gaps. Shared passwords are particularly vulnerable because they are often not protected by 2FA, leaving them exposed to unauthorized use. In such situations, teams may resort to manual workarounds, further increasing the risk of breaches.

Recommendation

Our suggestion is to consolidate your organization's security tools by using the built-in NordPass Authenticator. The Authenticator feature is particularly effective for security of shared passwords because it allows you to share both the credentials and TOTP codes simultaneously. This approach reduces the need for frequent password rotation, since former employees without access to TOTP cannot log in, even if they retain the password. We especially recommend using the NordPass Authenticator for organizations that employ devices with biometric authentication capabilities.

Need help? See our step-by-step guide

Password Health

Threat

Weak or compromised passwords significantly increase the risk of unauthorized access, which can lead to breaches, revenue loss, reputation damage, and non-compliance with industry regulations. Additionally, regular audits and assessments are essential to maintain compliance.

Recommendation

We recommend using the Password Health tool to track weak, reused, and outdated passwords based on the company-wide Password Policy. Additionally, the Exposed Passwords feature checks for passwords in leaked databases, allowing for early detection and mitigation of potential breaches. To further strengthen password hygiene over time, we highly advise that Admins conduct periodic reviews every month or at least every quarter and send reminders to encourage best practices among users.

However, monitoring and demonstrating a strong cybersecurity posture can be challenging without proper tools and processes.

Want a hand setting this up? Here's a quick guide

Events and audit management

Activity Log

Threat

Without clear visibility into your team's activity, suspicious behavior may go unnoticed, increasing security vulnerabilities.

Recommendation

We suggest using the NordPass Activity Log feature, which offers a detailed record of user actions performed within the organization, including app access, authentication activities, user invitations, role changes, organization settings updates, integrations, and item management. These logs can help identify suspicious behavior and streamline investigations if something has already happened. The logs can be exported via the Activity Log API, enabling integration with various SIEM tools. On top of that, NordPass offers direct integration with Splunk® and Microsoft Sentinel, allowing organizations to synchronize Activity Log data in real time.

Let us show you how it works

Data Breach Scanner

Threat

Small businesses are often targeted by phishing, ransomware, and other cyberattacks exploiting weak or reused passwords.

Recommendation

We recommend using NordPass' Data Breach Scanner to keep watch on every asset that can be affected in a breach — your company email domains along with corporate credit-card numbers. Ask the person who manages the card (usually the finance department or the cardholder) to add the card details securely in NordPass so the scanner can alert you if it appears on the dark web. When a breach alert arrives, walk through this mini-playbook:

- Review historic breaches in NordPass and filter for the ones that still matter.
- Work with each affected user: make sure leaked passwords have been changed, 2-factor authentication has been added, or unused accounts have been deleted.
- Check for personal or financial data leaks (PII, card details). If the exposure is sensitive, escalate or offer extra support to that user.
- Close the loop: Once mitigation is complete and the breach is no longer relevant, mark it "resolved" in NordPass to keep the dashboard tidy.
- Follow up with training: Schedule a short cybersecurity refresher for everyone impacted so they understand what happened and how to avoid repeats.

See how it works in our Help Center