

Credential Risk Reduction Plan

A phased, 12-week framework for organizations that have purchased Dashlane.

Compromised, weak, and reused credentials remain the leading attack vector for enterprise security breaches. This Credential Risk Reduction Plan provides a phased, 12-week framework for organizations that have purchased Dashlane. By systematically rolling out identity integrations, anti-phishing controls, user-facing Risk Alerts & Notifications, and security awareness automation, this plan minimizes the organization's credential attack surface while maintaining a positive employee experience.

AT A GLANCE

PHASE 1 · WEEKS 1-2

1 **Foundation and identity integration**

Secure the deployment, automate the user lifecycle, and establish a risk baseline.

Page 2

PHASE 2 · WEEKS 3-4

2 **Activate phishing defense and optimization**

Implement active, real-time protection against credential harvesting, and tune out noise.

Page 3

PHASE 3 · WEEKS 5-8

3 **Schedule user Risk Alerts & Notifications**

Drive user behavioral change using Dashlane's in-app risk alerts and Slack notifications in a controlled, non-disruptive sequence.

Page 4

PHASE 4 · WEEKS 9-12

4 **SIEM integration and training automation**

Integrate credential intelligence into security operations and automate remediation.

Page 5

ONGOING

5 **Operational KPIs and continuous maintenance**

Track the key performance indicators monthly and keep up the maintenance tasks.

Page 6

Foundation and identity integration

Secure the deployment, automate the user lifecycle, and establish a risk baseline.

1 Configure Confidential Single Sign-On (SSO)

ACTION

Integrate Dashlane with your Identity Provider (IdP), such as Okta, Microsoft Entra ID (Azure AD), Ping Identity, or Google Workspace using SAML 2.0.

WHY IT MATTERS

Confidential SSO allows users to access their Dashlane vaults seamlessly without needing to memorize a separate Master Password. This eliminates the risk of weak, forgotten, or exposed Master Passwords.

BEST PRACTICE

Enable Just-in-Time (JIT) provisioning or SCIM directory sync. This automates the onboarding and offboarding process directly from your source of truth.

2 Deploy Risk Detection to establish a risk baseline

ACTION

Access the Dashlane Admin Console and navigate to Risk Detection. Set up Credential Risk Detection.

WHY IT MATTERS

Before prompting users to change their habits, you must understand your current risk profile.

METRICS TO TRACK

- Number of users with compromised and weak credentials
- High-risk domains where compromised and weak credentials are being used

3 Prepare and communicate the migration plan

ACTION

Create a communication plan (announcement email) and schedule training sessions for the target group.

WHY IT MATTERS

Proactive communication ensures users understand the “why” and the expected timeline, reducing friction and increasing engagement.

BEST PRACTICE

Distribute the announcement 1-3 days prior to sending the invitation and ensure training is scheduled to coincide with the deployment.

4 Invite the first group of users

ACTION

Add first users to Dashlane, 5-10% of the user base.

WHY IT MATTERS

Validate that onboarding and login are working as expected for the general user population, and identify any questions that come in that may need to be addressed before deploying to the wider organization.

METRICS TO TRACK

- Employees who have accepted the invite and become Dashlane vault users.
- Users who have at least five passwords saved in Dashlane, as viewed on the Users page of the Dashlane Admin Console.

Activate phishing defense and optimization

Implement active, real-time protection against credential harvesting, and tune out noise.

1 Turn on AI Phishing Alerts

ACTION

Turn on AI Phishing Alerts.

WHY IT MATTERS

AI Phishing Alerts warn employees when they access a suspicious website, even if they're logged out of Dashlane or don't have a Dashlane account. Dashlane uses AI Phishing Detection to analyze websites for suspicious patterns.

2 Conduct a week-one “false positive” review

ACTION

Exactly one week after enabling AI Phishing Alerts, audit your administrative console logs.

WHY IT MATTERS

Internal staging environments, obscure subdomains, or custom legacy systems can sometimes trigger false-positive warnings.

RESOLUTION

Add verified internal or partner domains to your corporate allowlist. This mitigates alert fatigue, ensuring employees take legitimate phishing warnings seriously.

3 Prepare and communicate the migration plan

ACTION

Create a communication plan (announcement email) and schedule training sessions for the target group.

WHY IT MATTERS

Proactive communication ensures users understand the “why” and the expected timeline, reducing friction and increasing engagement.

BEST PRACTICE

Distribute the announcement 1–3 days prior to sending the invitation and ensure training is scheduled to coincide with the deployment.

4 Invite additional users

ACTION

Invite additional users to Dashlane, targeting 100% of the purchased seats.

WHY IT MATTERS

Wider validation of the solution after the pilot phase; general rollout begins.

METRICS TO TRACK

- Employees who have accepted the invite and become Dashlane vault users.
- Users who have at least five passwords saved in Dashlane, as viewed on the Users page of the Dashlane Admin Console.

Schedule user Risk Alerts & Notifications

Drive user behavioral change using Dashlane's in-app risk alerts and Slack notifications in a controlled, non-disruptive sequence.

1 Turn on in-browser Credential Risk Alerts

ACTION

- Alert logged-out and non-vault users on compromised, weak, and/or reused credentials.
- Alert logged-in vault users on compromised, weak, and/or reused credentials.

WHY IT MATTERS

Users are prompted via in-browser pop-ups to change these passwords instantly using Dashlane's password generator. These credentials represent an active, immediate threat.

2 Turn on Risk Notifications sent through Slack

ACTION

- Integrate Dashlane with Slack first.
- Schedule notifications for logged-in vault users: compromised, weak, and/or reused.
- Risk Notifications are for logged-in vault users.

WHY IT MATTERS

Users are prompted via Slack integration to change these passwords instantly using Dashlane's password generator. Alerting users to diversify their credentials halts potential lateral movement. Now that users are comfortable with Dashlane's automated generation tools, they can clean up passwords without administrative friction.

SIEM integration and training automation

Integrate credential intelligence into security operations and automate remediation.

1 Automate coaching with KnowBe4

ACTION

Configure integration between Dashlane events and KnowBe4's User Event API.

AUTOMATED SECURITY PLAYS (EXAMPLES)

- **The Phishing Play:** If Dashlane logs an event where a user ignored an AI Phishing alert, the integration automatically enrolls that user in a 5-minute KnowBe4 training module on Spotting Spear-Phishing Attacks.
- **The Compromised Credential Play:** If a user repeatedly bypasses alerts to update a compromised password, trigger an automated email sequence prompting immediate action, backed by a brief training module on Maintaining Credential Security in your organization.

2 Centralize telemetry with SIEM

Splunk / Microsoft Sentinel / CrowdStrike / Datadog / Panther

ACTION

Export Dashlane activity logs to your Security Information and Event Management (SIEM) tool.

TECHNICAL FLOW

Integrate your desired SIEM tool.

WHY IT MATTERS

SOC teams gain central visibility into critical security events, such as when a user bypasses an AI Phishing alert or fails to rotate an actively compromised credential. Create detection rules to get alerted and take action according to your thresholds.

3 Enable Vault Enforcement to enforce adoption

ACTION

If adoption targets are missed 8 weeks post-rollout, enable Vault Enforcement to accelerate engagement. In the Vault Enforcement section of the Admin Console, add 3–5 domains that are common in the business, or review the risk detection dashboard to find domains to enforce Dashlane usage.

WHY IT MATTERS

To realize the full value of Dashlane, users should be logged into their vault and see password risk alerts to change their passwords. Vault enforcement ensures they log in to Dashlane on business-critical sites.

METRICS TO TRACK

- Employees who have become Dashlane vault users
- Users who have at least five passwords saved in their Dashlane vault

Operational KPIs and continuous maintenance

To ensure the long-term success of this risk reduction plan, track the following key performance indicators (KPIs) monthly.

1 Operational KPIs

METRIC	TARGET GOAL	FREQUENCY
Enterprise password health score	85%	Monthly
Compromised password count	0	Bi-weekly
Vault adoption rate	100% of eligible employees	Monthly
Training enrollment latency	2 hours from risk event trigger	Real-time

2 Ongoing maintenance tasks

Monthly review	Analyze SIEM reports to identify “serial offenders” who persistently ignore risk alerts, and route them to managers or targeted security training.
Quarterly audit	Audit the domain allowlist to remove decommissioned testing environments or inactive external services.
Annual review	Review Identity Provider group mapping in SCIM to ensure appropriate default vault permissions for new organizational roles.