MARKETPLACE APP · IT-SERVICES

Password Manager

Secure team vault for passwords, 2FA codes, secure notes, and credentials.

Updated July 2026

MODEL	TIER	CAPABILITIES	INTELLIGENCE
Licensed · opt-in	**Suite**	**31+**	**AI-powered**

OVERVIEW

Password Manager shares MangoApps' own groups and directory for team access, instead of maintaining a separate team list — the same group you already use for scheduling or announcements can be granted access to a shared credential.

The Ask AI Password Agent retrieves, creates, and rotates entries by natural language in the same sidebar used for scheduling and leave requests, with semantic search that finds "WiFi" from "wireless credentials" and a confirmation prompt before anything risky.

When someone leaves, MangoApps' offboarding workflow automatically reassigns the team credentials they owned to their manager or an admin and cuts their inbound access grants, without a separate Password Manager cleanup step.

Beyond logins, it stores secure notes, credit cards, identities, API credentials, bank accounts, and software licenses, with a built-in TOTP generator, password history, and a background scan for weak, reused, and breached credentials.

WHY TEAMS CHOOSE IT

- Store logins, credit cards, identities, API credentials, bank accounts, software licenses, and secure notes in one AES-256-encrypted team vault.
- Generate the rolling 2FA one-time code for any login — paste a TOTP secret or scan an otpauth QR key and the whole team pulls the current code.
- Share team credentials with public or group/person-restricted access, auto-expiring grants, and one-click ownership transfer — with automatic reassignment when the owner is offboarded.
- Scan the vault for weak, reused, stale, and breached passwords using HaveIBeenPwned k-anonymity checks.
- Retrieve, create, and rotate passwords by natural language in Ask AI — with semantic search that finds "WiFi" from "wireless credentials".
- Audit every view, copy, reveal, and share — capturing the user, timestamp, IP, and device for compliance.

CAPABILITIES

Sharing & Team Access Control

- ✓ Personal (private) and team (shared) vaults
- ✓ Public or group/person-restricted access levels (view or edit)
- ✓ Time-limited, auto-expiring access grants
- ✓ Admin restricts who can create team passwords (by group)
- ✓ Admin access review — exactly who can read each shared entry
- ✓ Ownership transfer plus automatic offboarding (reassign owned team entries, revoke inbound grants)
- ✓ External one-time, expiring secure-share links for non-users ("secure send")

Vault, Item Types & Built-in 2FA

- ✓ Seven item types — login, secure note, credit card, identity, API credential, bank account, software license
- ✓ Built-in TOTP authenticator: rolling one-time codes from a stored secret (otpauth:// QR keys supported)
- ✓ Custom fields with concealed values revealed on demand (up to 30 per entry)
- ✓ Per-entry file attachments (license PDFs, recovery kits)
- ✓ Password history with reveal and one-click restore
- ✓ Per-user favorites and admin-managed category organization

Password Health & Breach Detection

- ✓ HaveIBeenPwned breach check (k-anonymity; team and personal scans; runs in the background)
- ✓ Weak / reused / stale / insecure-URL detection (Security Health engine)
- ✓ 0–100 strength scoring shared by the app and the AI agent
- ✓ Crypto-secure password generator with a real-time 4-level strength meter
- ✓ Per-entry expiration with expiring-soon dashboard and email + in-app reminders

AI Password Agent (Ask AI)

- ✓ Password Agent — natural-language retrieve, create, update, archive, restore, and delete
- ✓ Semantic / vector search (finds "WiFi" from "wireless credentials")
- ✓ Respects each user's access permissions in the AI context
- ✓ Confirmation prompt before risky actions; secrets scrubbed from AI logs
- ✓ Admin toggle to enable/disable the agent; honors the 2FA-to-view gate

Security, Encryption & Audit Trail

- ✓ AES-256 (non-deterministic) encryption at rest for passwords, notes, TOTP secrets, and custom fields
- ✓ Require 2FA before any password is viewed (admin toggle)
- ✓ Step-up identity verification ("sudo mode", 15-minute elevated session) before reveal, copy, or CSV export in the web and mobile app — Not yet enforced on the read API or the AI agent's retrieval
- ✓ Immutable per-entry audit log (18 action types incl. AI retrievals) with IP/device capture and configurable retention
- ✓ Fail-closed auditing in the web app — if the audit row can't be written, the secret is not returned — Mobile copy, the read API, and the AI agent don't check this yet

Import, Export & Migration

- ✓ Import from 1Password, LastPass, Bitwarden, Chrome/Edge, Dashlane, and generic CSV
- ✓ Intelligent paste with AI column mapping and a preview before anything is written (secret values never sent to the LLM)
- ✓ Round-trip CSV export of accessible entries (2FA + step-up gated in the web app) — The read API's export enforces the 2FA gate only, and isn't audited

Limits & Specs

Item types	**7 (login, secure note, credit card, identity, API credential, bank account, software license)**
Custom fields per entry	**Up to 30 (text, concealed, URL, date)**
Password history & generator	**20 versions per entry; 16-char default generator (12–64 via the AI agent)**
External share links	**1 view by default (max 25); 7-day default TTL, 30-day maximum**
Import size	**Up to 500 rows per import**

USE CASES

- **Team WiFi and shared accounts**
  Publish office WiFi and shared service logins as public team entries, and rotate the guest network monthly with an expiration date and automatic reminders.
- **Developer secrets with 2FA**
  Store API keys and tokens as API-credential entries with concealed fields, and keep each service's TOTP secret so the whole on-call team can pull the current one-time code.
- **Secure send to a vendor**
  Hand a contractor a single credential through a tokenized, expiring, one-time external link — no MangoApps login required, and the link self-exhausts after it's viewed.
- **Security and compliance review**
  Admins run a breach check and Security Health scan over team credentials, use the access review to answer "who can read this?", and rely on the immutable audit trail as evidence.

- **Migrate from another manager**
  Bulk-import from a 1Password, LastPass, Bitwarden, Chrome, or Dashlane CSV (or an intelligent paste), preview the mapped columns, then commit — up to 500 rows per import.
- **Offboarding a departing employee**
  When someone leaves, the vault reassigns the team entries they owned to their manager or an admin and deactivates their inbound access grants automatically.

PRICING & LICENSING

Access surfaces & pricing	**Web + mobile-optimized app (no browser extension); requires a license**
License	**Required (opt-in per business)**
Tier	**Suite**

Pricing is tailored to your organization — **talk to sales for pricing & a live demo**. Final commercial terms per your agreement.

FAQ

How are secrets stored and encrypted?
Passwords, notes, TOTP secrets, and custom-field values are encrypted at rest with Rails application-level AES-256 (non-deterministic) encryption, on top of per-business tenant isolation. Note this is not zero-knowledge — the server holds the keys so the AI agent, TOTP code generation, and breach checks can operate.

Can it generate 2FA codes like an authenticator app?
Yes. Store a TOTP secret on any login — as a Base32 key or a full otpauth:// QR/setup key — and the entry shows the rolling one-time code with a countdown. Custom digit counts, periods, and algorithms (SHA1/256/512) are honored.

How do I control who sees team passwords?
Shared entries can be public (all app users) or restricted to specific groups and people, each granted view or edit — and grants can auto-expire. Admins can limit who may create team passwords, and the access review shows exactly who can read each shared entry.

What extra protection happens before a secret is shown?
Admins can require 2FA to view passwords — enforced everywhere a secret can be read, including the API and the AI agent. Step-up identity verification (a 15-minute elevated session) is a second check the web and mobile app run before a reveal, copy, or CSV export, and those two surfaces are audited fail-closed — a broken audit write blocks the secret there too. The read API and the AI Password Agent don't yet enforce step-up or that fail-closed guarantee.

Can I share a password with someone outside the company?
Only if an admin enables external secure-share links. Each link is tokenized, expiring, and view-limited (one view by default), reveals a single credential on an explicit action, and self-exhausts — safe from link-preview bots.

Is it only for passwords, or can I store other things?
Beyond logins it stores seven item types: passwords, secure notes, credit cards, identities, API credentials, bank accounts, and software licenses. Typed entries keep their data in concealed custom fields (card number and CVV, license key, account and routing numbers), with up to 30 custom fields per entry and file attachments for things like license PDFs or recovery kits.

Does it warn me about weak or breached passwords?
Yes. A background Security Health scan flags weak, reused, stale (unchanged for months), and insecure http:// entries and scores each login 0–100. An opt-in breach check uses HaveIBeenPwned with k-anonymity — only the first five characters of a SHA-1 hash ever leave the server, never the password — and reports how many known breaches each password appears in.

Can I migrate from my current password manager?
Yes. Bulk-import from 1Password, LastPass, Bitwarden, Chrome/Edge, Dashlane, or a generic CSV, up to 500 rows per import. Known formats are matched by their header signature; anything unrecognized (including free-form pasted text) is mapped with AI column detection, and you preview the mapped rows before anything is written. Secret values are never sent to the LLM — only header names and type hints are.

Can I get my data back out?
Yes — there is no lock-in. You can export the entries you can access to a CSV whose columns round-trip back through the import flow. Because the file contains plaintext secrets, the web export is step-up gated (an elevated session), and the API export only returns what the requesting user is allowed to view.

Is there a browser extension or autofill?
No. Password Manager runs in the web app and a mobile-optimized web view — there is no native browser extension, page autofill, or desktop app. You open an entry and copy the password or the current one-time code (each copy is audited). If in-browser autofill is a hard requirement, this app is not the right fit.