PATCH RELEASE

SASVA Canvas 4.0.6

Pre-LLM user prompt policy, request-time auth public key, and thinking-card UX.

Internal product & engineering documentation • Persistent Systems

PRODUCT VERSION
4.0.6

SOFTWARE RELEASED
1 September 2026

DOCUMENT PUBLISHED
1 September 2026

SURFACES
Web · Desktop · Mobile

§ Contents

1 About this document

This document is the release note for **SASVA Canvas 4.0.6**. It describes what this release delivered — each capability in enough detail that a reader who was not in the room can brief a customer, an operator, or an auditor. It lists this release and earlier releases only.

How to read this note. Each item below is a capability or a defect closed in 4.0.6. The first sentences say what changed; the next say why it matters and what you will see after upgrade.

2 Document control

Document title	SASVA Canvas 4.0.6 Release Notes
Document version	1.0 — published with Canvas 4.0.6
Product version	4.0.6
Software released on	1 September 2026
Document published on	1 September 2026
Classification	**Internal** — Persistent Systems

Document revision history

Version	Date	Description of change
1.0	1 September 2026	Initial publication of the Canvas 4.0.6 release notes, aligned with the product release date.

3 Product release history

This table lists this release and earlier Canvas releases. The highlighted row is this document.

Version	Date	Type	Headline
4.0.6	1 Sep 2026	Current Patch	Pre-LLM user prompt policy, request-time auth public key, and thinking-card UX
4.0.5	30 Aug 2026	Patch	Content-Security-Policy, session-derived tenant isolation, and session hardening
4.0.4	26 Aug 2026	Patch	Platform FAQ catalog and trustworthy chat history
4.0.3	23 Aug 2026	Patch	Help Center, User Feedback, AI transparency, and query-time PII masking
4.0.2	6 Jul 2026	Patch	SMTP that operators can save, and a complete lifecycle email set

Version	Date	Type	Headline
4.0.1	21 Apr 2026	Patch	Release-planning persistence, owner sharing, brand PPTX, and OAuth work-account paths
4.0.0	25 Mar 2026	Major	Genesis Discovery & Planning, Lifecycle Dashboard, local-folder repos, and SSO hardening
3.1.5	25 Mar 2026	Patch	The product is named SASVA Canvas; installers and desktop runtime catch up
3.1.4	13 Mar 2026	Minor	Electron desktop app, casual-query fast-path, and session timeout settings
3.1.3	12 Mar 2026	Patch	Mobile feature parity with the web console
3.1.2	10 Mar 2026	Patch	Fact Service agent and a fix for masked API keys leaking to the backend
3.1.1	9 Mar 2026	Minor	Billing, 8-factor ROI, team collaboration, image generation, and PENTEST-001
3.1.0	8 Feb 2026	Minor	Multi-agent RAG, Business and Product workspaces, enterprise security, and mobile

Patch Web Desktop Mobile

4 In this release

4.0.6 restored production login after the 4.0.5 key-pinning work, and put an application-layer safety gate in front of every chat path. Both changes matter most where Canvas runs behind a reverse proxy or in front of an on-premise model that has no provider safety filter.

The version number is aligned to 4.0.6 across web, desktop, mobile, scripts, documentation, and product knowledge.

5 Security & trust

Auth public key served at request time

4.0.5 began verifying permissions only against a pinned Ed25519 public key from `/api/auth/public-key`. In production, Next.js could prerender that route at build time. After a key rotation or a new signing seed, the running server held one key and the browser was served another. Login failed with a signature or envelope error that looked like a client bug.

4.0.6 forces `/api/auth/public-key` and `/api/health/database` to dynamic rendering. The key the browser pins is the key this process is signing with, on this request. That is the fix for “we deployed 4.0.5 and nobody can log in.”

User prompt policy — refuse harmful generation before the LLM

A pre-LLM gate in `lib/safety/` now runs on workspace chat, knowledge chat, and multi-agent routes. Obvious malware and exploit generation, credential theft, and adult-content generation are refused at the application layer. The model is never called.

Untrusted RAG context is wrapped with delimiter instructions so a retrieved document cannot quietly override system intent. This is the control that matters on air-gapped SASVA or Bedrock deployments where the provider is not applying its own safety filter. Dual-use security topics stay allowed when they are framed as review, prevention, or requirements work.

6 Improvements

Empty assistant card hidden while agents are thinking

On web and desktop, the chat used to open an empty assistant bubble as soon as the stream started, then fill it when the first token arrived. Users saw a blank card sitting under the thinking indicator and assumed the response had failed.

4.0.6 keeps that card hidden until there is content. The thinking feed is the only thing on screen while agents work. When tokens arrive, the response card appears with text already in it.

7 What to expect after upgrade

If 4.0.5 left you with failed logins, deploy 4.0.6 and hard-refresh once so browsers drop a prerendered public key. No env-var change is required unless you already pin `ED25519_PRIVATE_KEY` across hosts — that path is unchanged.

The prompt policy is on by default. A denial is a structured refusal in the chat, not a 500. Policy tests live at `npm run test:prompt-policy`.

PREVIOUS RELEASE
4.0.5