fix: isolate profile .env secrets on switch #351

Merged **nesquena-hermes** merged 2 commits into `nesquena:master` from `Hinotoi-agent:fix/profile-env-iso…` last week

Hinotoi-agent commented last week

Contributor

Summary

- clear profile-scoped `.env` variables before loading the next profile
- prevent API keys and other secrets from leaking across profile switches
- add regression tests covering missing and overlapping `.env` keys across profiles

Why this matters

The profile system is expected to isolate credentials and configuration between profiles.
Before this change, switching from one profile to another only added variables from the new profile's `.env`; it did not clear variables that had been loaded from the previous profile. That allowed provider API keys and other secrets to persist into the new profile context.

Root cause

`api.profiles._reload_dotenv()` loaded `.env` files additively into `os.environ` and never removed keys loaded from the previously active profile.

Fix

- track which environment variables were loaded from the active profile
- remove those keys before applying the next profile's `.env`
- keep the new profile's keys loaded normally after cleanup

Test plan

- [x] `python -m pytest tests/test_profile_env_isolation.py -q`
- [x] `python -m pytest tests/test_auth_sessions.py -q`

Hinotoi-agent and others added 2 commits last week

 `fix: isolate profile .env secrets on switch` ✗ `abee926`

 `fix: move direct os.environ set after _reload_dotenv to survive profi…` ··· ✓ `f4fe5f1`

nesquena commented last week — Owner

Full Review: PR #351 — isolate profile .env secrets on switch

Thanks @**Hinotoi-agent**! Real security fix — API keys from profile A were leaking into profile B on switch.

Security Audit

Clean and positive. The change tracks which env vars were loaded from a profile's `.env` and clears them before loading the next profile. This prevents credential leakage across profile switches — a real security gap.

Code Review

`profiles.py` — clean implementation:

- `_loaded_profile_env_keys: set[str]` tracks keys loaded from the current profile
- `_reload_dotenv()` clears tracked keys before loading new ones
- Exception handler resets the tracking set — good defensive coding
- The change is minimal (15 lines) and surgical

CI Failure — Found and Fixed

CI was failing because `test_api_key_set_in_os_environ_after_apply` (in `test_sprint39.py`) broke when run in the full suite.

Root cause: `apply_onboarding_setup()` in `onboarding.py` set `os.environ[key]` BEFORE calling `_reload_dotenv()`. With the new profile isolation, `_reload_dotenv` clears previously tracked keys — which includes the key that was just set on line 484. When the test mocked `_write_env_file` (so no actual `.env` was written), `_reload_dotenv` couldn't re-read the key from disk, and the direct `os.environ` set was already wiped.

Fix pushed: Moved the belt-and-braces `os.environ` set to AFTER `_reload_dotenv()`, so the key survives the isolation cleanup. The key is now set in the correct order: write to disk → reload dotenv (clears old, loads new) → set os.environ as fallback.

Tests

759 passed, 0 failed, 48 skipped — all clean after the fix. The 2 new profile isolation tests are well-structured:

- `test_profile_switch_clears_previous_profile_env_vars` — switch from p1 (has keys) to p2 (empty) → p1's keys gone
- `test_profile_switch_replaces_overlapping_keys` — switch from p1 to p2 with overlapping key → p2's value wins, p1-only keys gone

Verdict

Approved. Fix pushed directly to the branch. CI should pass now.

nesquena-hermes merged commit **88dc8bb** into `nesquena:master` last week

3 checks passed

View details

nesquena-hermes mentioned this pull request last week

docs: v0.50.12 release — CHANGELOG + version badge #353

Merged

nesquena commented last week

Owner

@**Hinotoi-agent** can you confirm this is working on the latest version?

Hinotoi-agent commented last week • edited

Contributor Author

Yes — I validated it on the PR head commit `f4fe5f1c6fb53a99b663926c9ca3d999b20f886e`, and that change merged as `88dc8bbe26a6055161d3251b70f5cd3d3c5831b0`.

nesquena-hermes mentioned this pull request last week

docs: update contributors section, test count, and line counts (v0.50.21) #386

Merged

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants