



OFFICIALLY VALIDATED

This certificate attests that the WAF++ PASS run identified below was cryptographically signed by the organization and, for official validations, counter-signed by the WAF++ central validation authority. The certificate can be re-verified at any time using the public verification URL or the wafpass verify command.

Validation ID	waf-ex-12345678-1234-1234-1234-123456789abc
Run hash	7184231525be8173ccb7eb0b5fc804630e37c49c2ec3c511b3c47b8d875a54a6
Project	acme-platform/prod
Branch	main
Git SHA	a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0
Score	87%
Status	OFFICIAL
Signed by	organization
Signed at	2026-08-17T19:46:04.813508Z
Validated at	2026-08-17T19:46:04.813718+00:00
Expires at	2026-11-15T19:46:04.813718+00:00
Verification URL	https://wafpass.example.com/api/v1/validations/waf-ex-12345678-1234-1234-1234-123456789abc/verify

Certificate Chain

Server Intermediate	–	(could not parse certificate)
WAF++ Root CA	–	(could not parse certificate)

Independent Verification

Anyone can verify this validation by running:
wafpass verify <envelope.json>
For official validations, the server status can also be checked online at the Verification URL shown above. The local attestation proves the run result has not been altered since it was signed; the server countersignature proves the WAF++ authority reviewed and recorded the validation.
Generated 2026-08-17 19:46 UTC · WAF++ PASS v1.1.2 waf2p.dev