SALT

Salt Managed Rules for AWS WAF

Overview

Salt Managed Rules for AWS WAF – AI Agent & API Security is available in AWS Marketplace and deploys in a few clicks, with no infrastructure changes. Rules are written, managed, and updated by Salt Security experts, so there's no manual version upkeep.

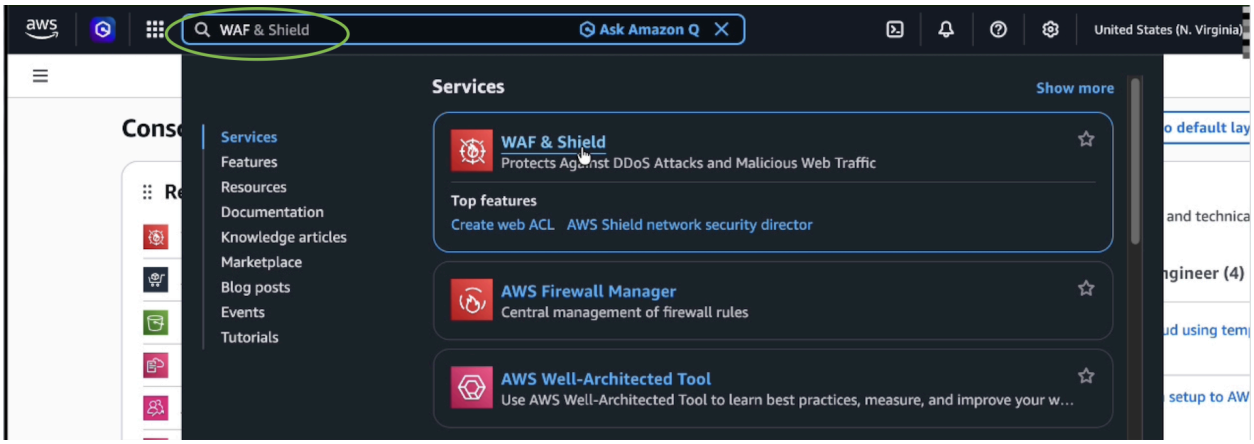
It protects against:

- **API abuse —** malformed and excessive calls, parameter tampering, known attack signatures
- **GraphQL attacks —** introspection abuse, oversized batch queries, nested-query exploitation
- **JWT anomalies —** tokens in URLs, missing signatures, and other malformed credentials
- **SSRF —** requests coercing the backend into contacting internal or metadata endpoints
- **Credential attacks —** email, user ID, and password enumeration or brute-forcing
- **AI agent & MCP activity —** discovers agent traffic and unauthenticated MCP access

Getting Started: Adding the Ruleset to a Web ACL

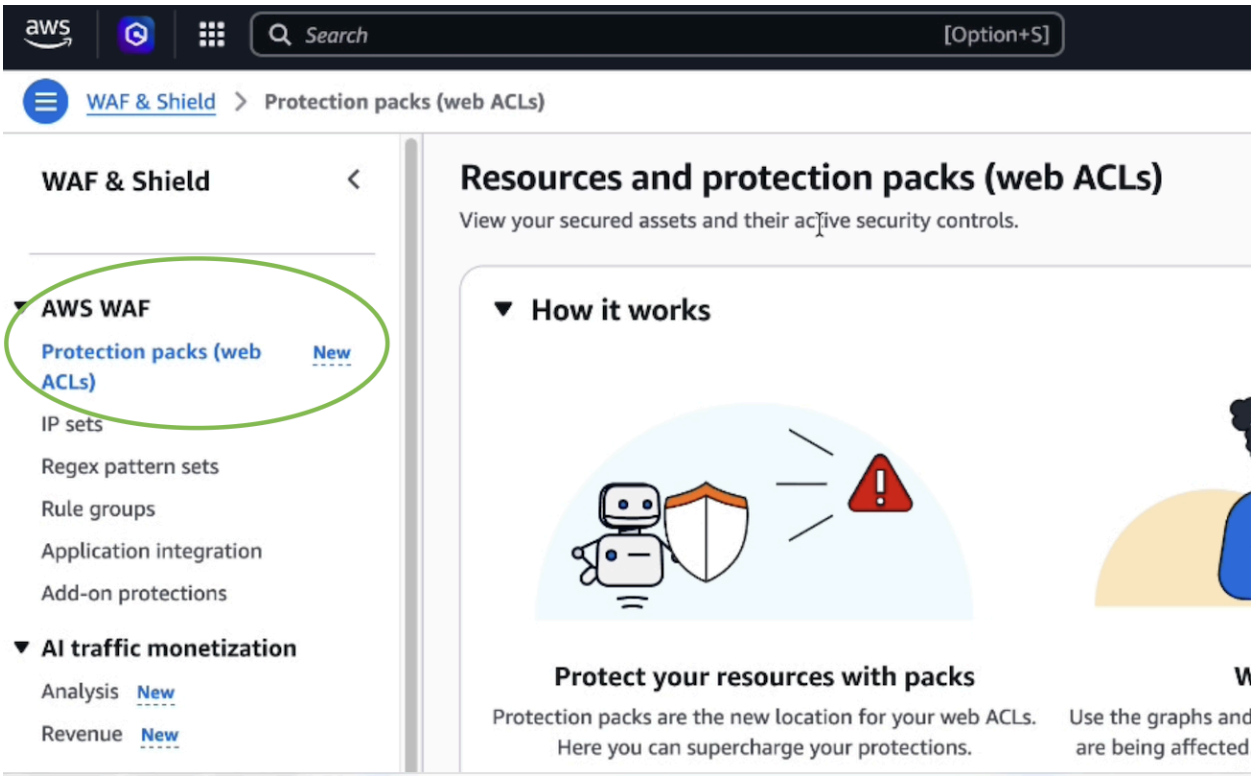
1. Open AWS WAF & Shield

In the AWS Console search bar, type “WAF” and select WAF & Shield.



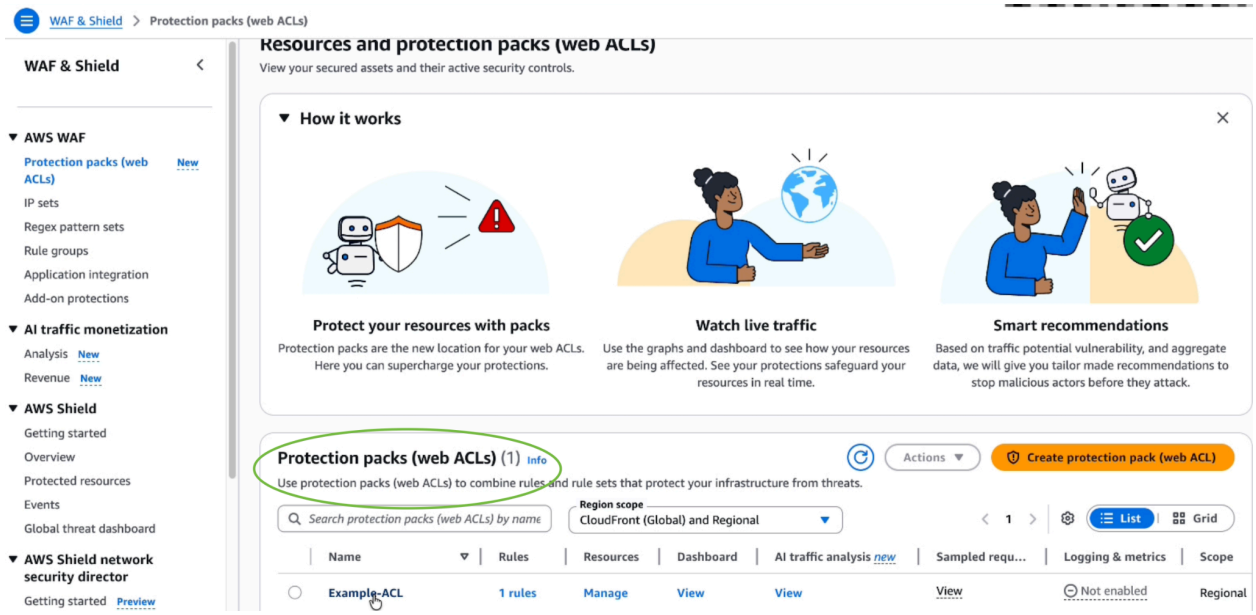
2. Choose your Web ACL

Click Web ACLs in the left nav. Confirm the Region (top right) — rule groups are Region-specific — then select your Web ACL.



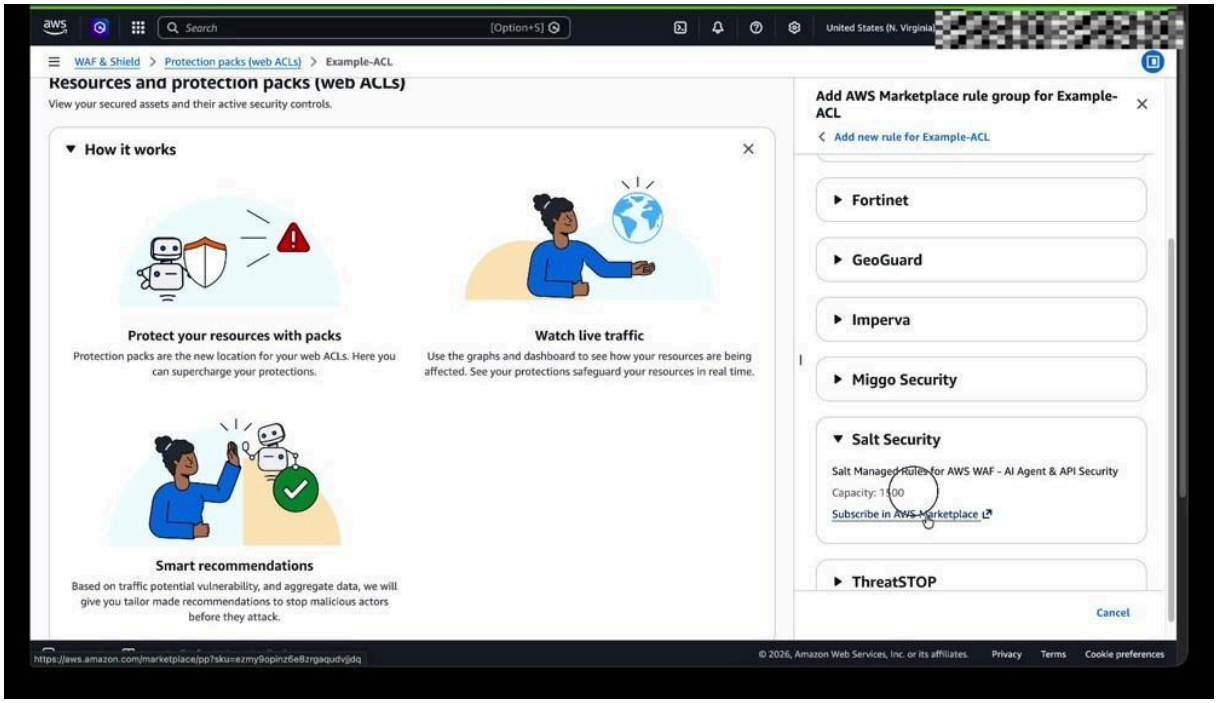
3. Add a managed rule group

Rules tab → Add Rules → Add Managed Rule Groups.



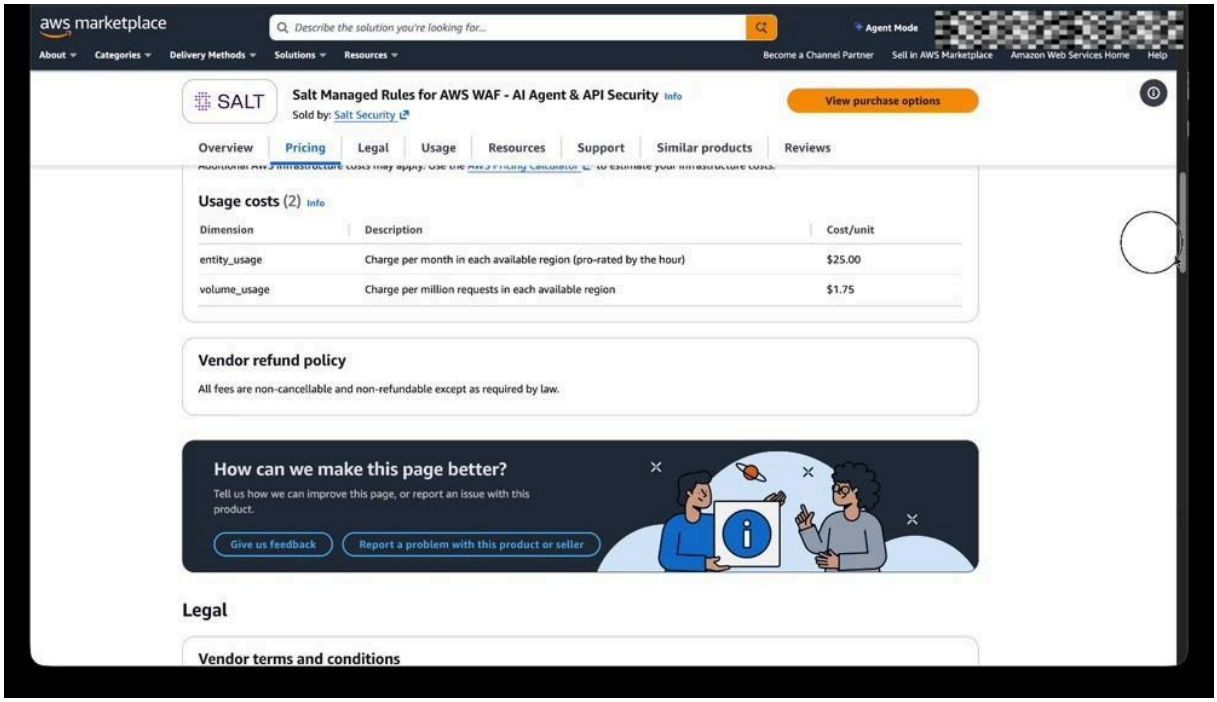
4. Find Salt Security

Scroll to Marketplace managed rule groups → click Add to Web ACL next to Salt Security.



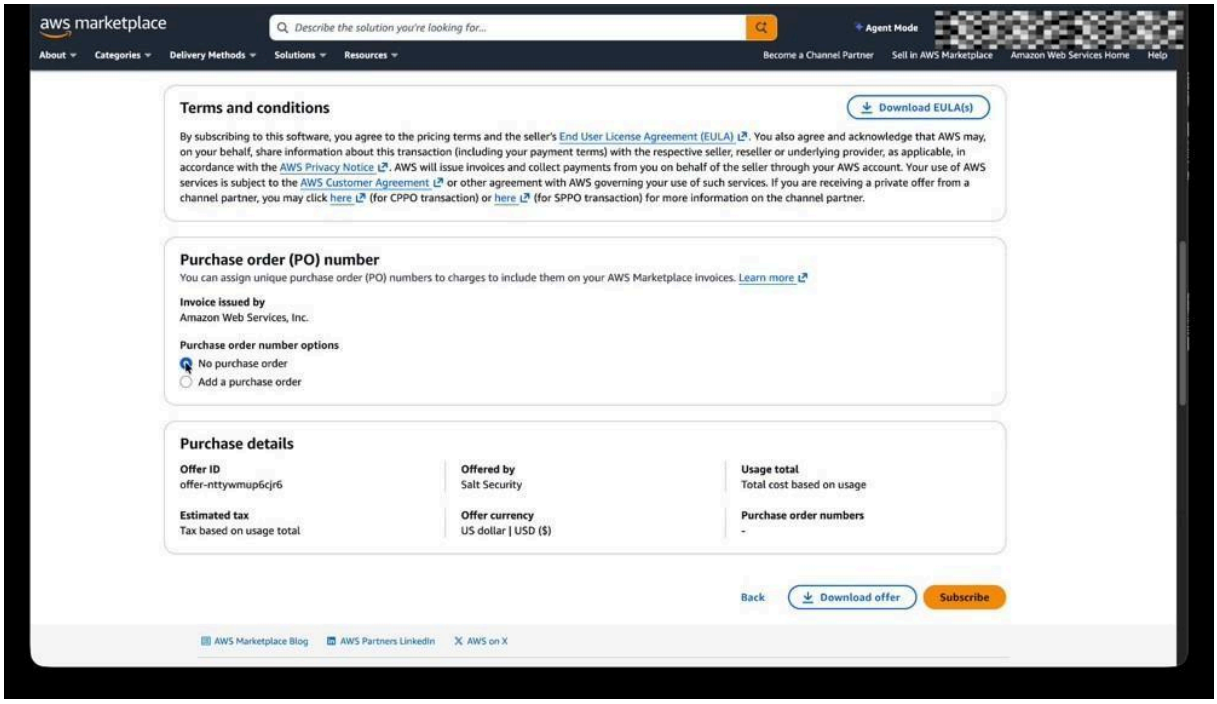
5. Subscribe on Marketplace

AWS redirects you to Marketplace. Click Subscribe on AWS Marketplace, review pricing, then Continue to Subscribe.



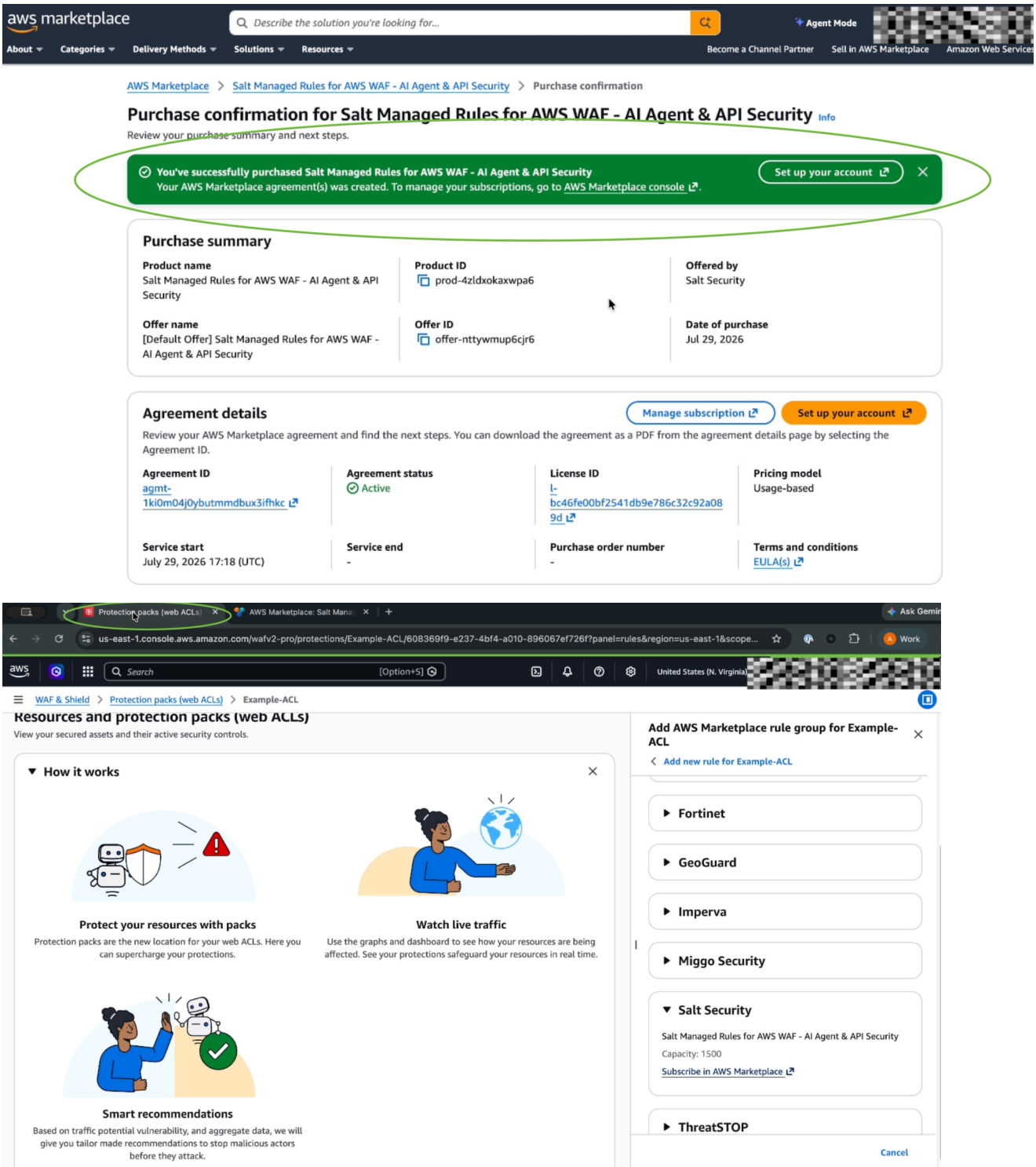
6. Accept terms

Review Terms and click Subscribe when ready. Processing takes about 30–60 seconds.



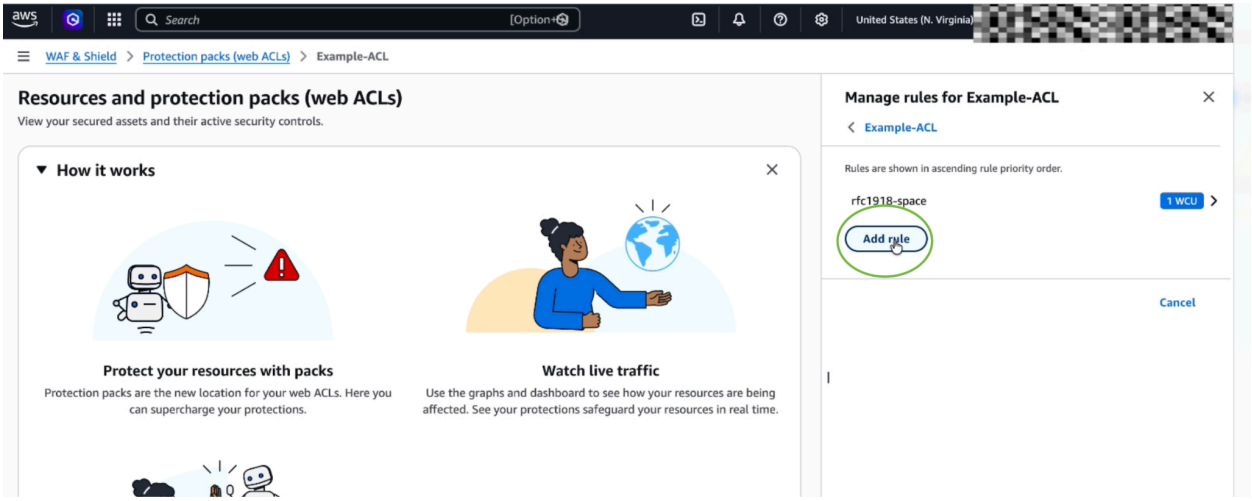
7. Return to the WAF console

Once you see the green confirmation, close the tab, return to WAF, and refresh if needed.



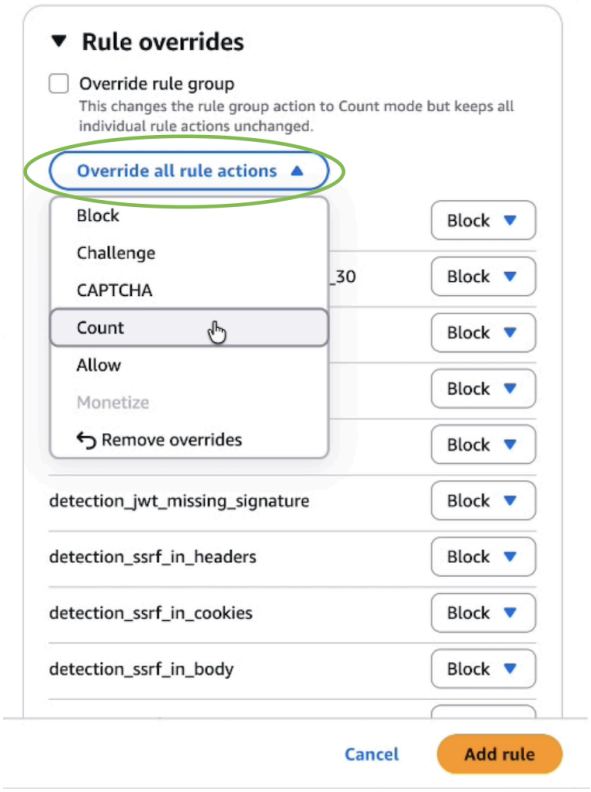
8. Add the ruleset

Click Add to Web ACL on the Salt Security ruleset. Expand it to review individual rules.



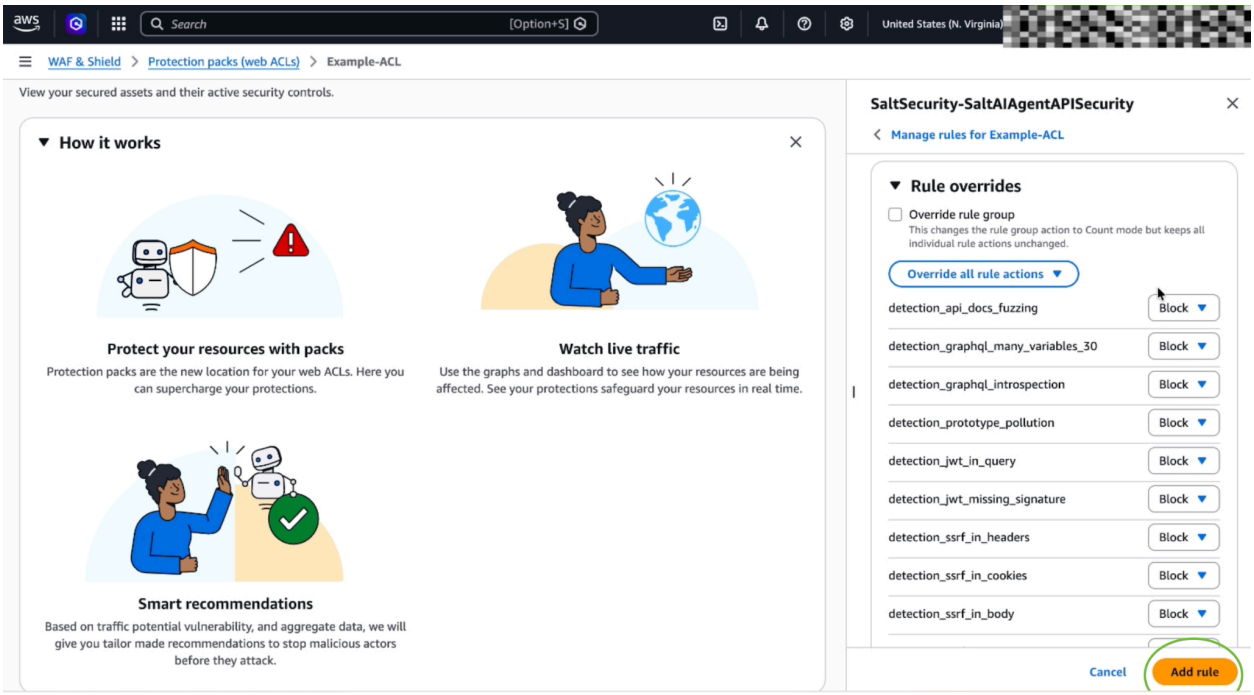
9. Trial before enforcing [OPTIONAL]

Toggle a rule's action to Count to log matches without blocking — ideal for a trial period.



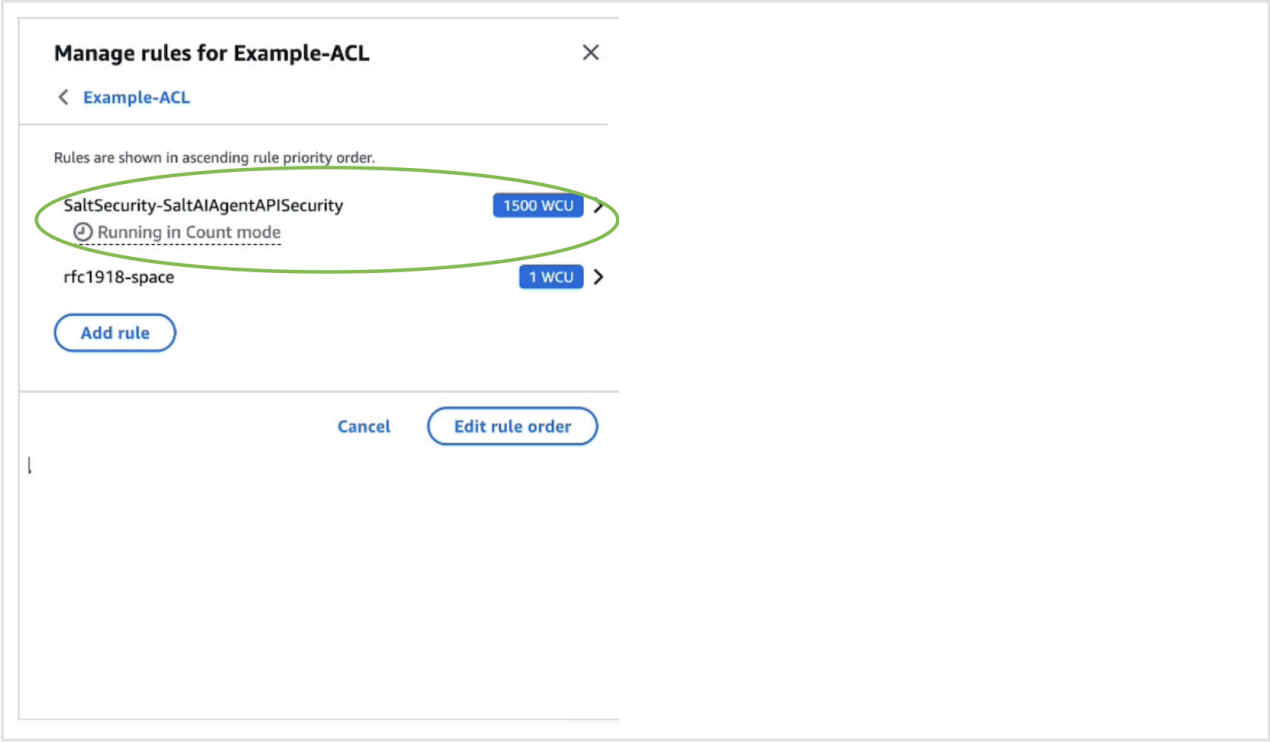
10. Set priority & save

Click Next, drag to reorder priority (specific rules before broad ones), then click Save.



11. You're live [DONE]

The ruleset appears on the Rules tab. Traffic hitting this Web ACL is evaluated immediately.



Rule Reference

The ruleset ships three kinds of rules: labels (informational tags), detections (the actual protections), and rate-based rules (throttling).

Labels — default action: Count

Rule	What it does
auth:true:header	Marks requests carrying a recognized authentication header
tech:mcp:path_method	Marks POST requests to Model Context Protocol endpoints
tech:graphql:multi	Marks GraphQL traffic
params:email	Marks requests carrying an email-shaped value
params:password	Marks requests carrying a password field
params:user_id	Marks requests carrying a user identifier
params:numeric_only	Marks requests carrying purely numeric values (likely IDs)

Detections — default action: Block

Rule	What it does	Severity
API documentation discovery	Blocks scans probing common doc paths (/swagger, /openapi, /docs)	Low
GraphQL introspection	Blocks queries asking the server to reveal its full schema	Medium
GraphQL batch abuse	Blocks queries packing 30+ variables into one operation	Medium
Prototype pollution	Blocks JSON bodies injecting into the JS prototype chain	High
JWT in URL	Blocks tokens passed in the query string (leaks credentials into logs)	High
JWT without signature	Blocks JWTs missing or stripped of their signature	Medium
SSRF (headers/cookies/body/query)	Blocks requests directing the server to internal or metadata IPs	High
Unauthenticated MCP access	Blocks POST requests to MCP routes with no auth header	High

Rate-based rules — default action: Block above threshold

Rule	What it does
Email enumeration	Throttles repeated email submissions (70 / 5 min per IP)

User ID enumeration	Throttles repeated user ID submissions (80 / 5 min per IP)
Password brute-force	Throttles repeated password submissions (30 / 5 min per IP)
Per-source volume cap	Safety-net rate limit for abnormally high traffic (150 / 5 min per IP)

Support

For questions about rule behavior, tuning, or false positives specific to this rule group, contact Salt Security support through support@salt.security.

For AWS WAF platform issues unrelated to this rule group, contact AWS Support.

Thank you.