

GAJWAF · PLAYBOOK

Onboard a site safely

Reach full blocking without ever breaking the live site

Watch first. Prove it's clean. Then enforce.

A six-stage runbook for putting a new site behind GAJWAF. Each stage ends with a clear **"move on when"** check, and the playbook closes with a sign-off checklist for your change record.

~20 min

Hands-on setup

Hours–days

Watch period in Detect

6 stages

Each with a go / no-go check

GajShield Infotech Private Limited
Mumbai, India

Version 1.0 · October 2026
For GAJWAF administrators & analysts

LEGAL NOTICE

© 2026 GajShield Infotech Private Limited All rights reserved. This document is provided for the use of GAJWAF customers and partners. No part of it may be reproduced, distributed or transmitted in any form or by any means without the prior written permission of GajShield Infotech Private Limited

The information in this document is provided "as is", without warranty of any kind, express or implied, and is subject to change without notice. Features, menu labels and default values may differ between GAJWAF releases. While every effort has been made to ensure its accuracy, GajShield Infotech Private Limited accepts no liability for any loss, damage or service disruption arising from the use of, or reliance on, this document. This playbook is general operational guidance. It does not replace your organisation's own incident-response or change-control procedures, and GAJWAF is not a substitute for network-layer (L3/L4) DDoS protection.

GAJWAF and GajShield are trademarks of GajShield Infotech Private Limited Amazon Web Services, AWS and AWS Shield are trademarks of Amazon.com, Inc. or its affiliates. Microsoft and Azure are trademarks of the Microsoft group of companies. All other product and company names mentioned in this document are trademarks of their respective owners; they are used for identification purposes only, and their mention does not imply endorsement.

AT A GLANCE

The method

GOLDEN RULE

Never switch a brand-new site straight to **Block**. Run it in **Detect** long enough to see real traffic, clear the false positives, *then* enforce.
Blocking an un-reviewed site is the number-one cause of "the WAF took down our app" calls.



Who Admin to configure the site; analyst to switch modes.	Time About 20 minutes of setup, then a watch period of hours to a few days.
---	---

✗ DON'T

- Don't go straight to **Block** on a new site.
- Don't clear false positives by lowering the whole site's sensitivity or turning off a whole category — use a **targeted exclusion**.
- Don't forget multi-node: if you added the site on one node of a cluster, roll the same config to every node (console **Export / Import**), and confirm they share `cluster.secret`.

IN THIS PLAYBOOK

Contents

1	Add the site and point traffic at the WAF	3
2	Pick a security level	3
3	Let it watch real traffic	4
4	Review what would have been blocked	4
5	Enforce	5
6	Finish the hardening.....	5
✓	Sign-off checklist	6

STAGE 1 OF 6

1 Add the site and point traffic at the WAF

SITE MODE **DETECT** TIME About 15 minutes, plus your DNS / load-balancer change

1. **Sites → Add site.** Set the **host name(s)** clients use, and the **backend** URL the WAF forwards to. (Field details: *Features & Configuration Guide*, chapters 1 and 3.)
2. Install the **TLS certificate** for the host — **Edit configuration → Backend & TLS → HTTPS certificate → Validate & install** — or confirm automatic certificate handling (Let's Encrypt).
3. **Leave the mode on Detect.** New sites are safe by default.
4. **Cut traffic over to the WAF** — change DNS, or point your load balancer at it. For a zero-downtime cutover, keep the old path ready to roll back to.
5. **Check the health chips** on the **Sites** page are green: a backend is reachable and HTTPS is serving.

IMPORTANT

A red "**No backend**" or "**No HTTPS**" chip means routing or TLS needs fixing before you go any further — see the *Troubleshooting & Support Manual*, chapter A.

✓ MOVE ON WHEN

- Health chips are **green** — backend reachable, HTTPS serving.
- Real traffic is flowing through the WAF. It is **inspecting, but not blocking**, anything.

STAGE 2 OF 6

2 Pick a security level

SITE MODE **DETECT** TIME A few minutes

1. Open **Edit configuration → General → Security level**.
2. Choose the policy template that matches the application. It sets sensible rules and the blocking threshold in one step.
3. Optionally fine-tune **Blocking sensitivity (score)**. **Lower is stricter**; one serious finding scores 5.

NOTE

The site is still in **Detect**, so this only changes what gets *scored* — nothing is blocked yet.

✓ MOVE ON WHEN

A security level is selected for the site.

STAGE 3 OF 6

3 Let it watch real traffic

SITE MODE **DETECT** TIME Hours on a busy site — days if there are weekly jobs

Leave the site in **Detect** and let genuine users — and your own smoke tests — exercise it. Make sure the watch period covers every real workflow:

☐ Logins	☐ Search
☐ File uploads	☐ Checkout / payments
☐ Admin pages	☐ Scheduled jobs
☐ API clients & integrations	

A busy site may need only hours. A quiet site, or one with weekly batch jobs, needs longer.

IMPORTANT
If the site uses **traffic learning** (positive security), let the learning period run until endpoints show **"ready"** under **Insights** before you ever turn on **Score deviations** (`learning.enforce`).

✓ MOVE ON WHEN
Every real workflow above has run at least once while the site was in Detect.

STAGE 4 OF 6

4 Review what would have been blocked

SITE MODE **DETECT** TIME Repeat until a representative period is clean

This is the core step. Open **Overview** → **"Attacks observed but not blocked"**, or **Events** filtered to this site. Every entry is something the WAF *would* block once you enforce. For each one, decide:

If the finding is...	Then	How
A real attack	Good — the WAF is doing its job.	Leave it.
A false positive (legitimate traffic flagged)	Fix it now , before you enforce.	Open the event → "Not an attack?" to propose an exclusion scoped to that rule and path. Full method: the <i>Taming false positives</i> playbook.

KNOWN GOTCHAS — CHECK THESE UP FRONT

Application	What you'll see	Fix
Matomo / analytics	<code>hidden-field-tampered</code> findings	Add <code>module</code> and <code>action</code> under Detection → "Fields your JavaScript changes" (<code>hidden_fields.exempt</code>).
APIs, webhooks, health checks, mobile endpoints	Clients being challenged by the bot check	List the paths under Bot check → "Never check these paths" (<code>challenge.exempt_paths</code>).

✓ MOVE ON WHEN

A representative period produces **no false positives** — only findings you're happy to block.

STAGE 5 OF 6

5 Enforce

SITE MODE **BLOCK** TIME Switch takes seconds — watch closely for the first hour

1. **Sites** → **switch the site to Block**. You'll be asked to confirm.
2. Watch **Events** for the first hour, filtered to **Action = block**. Every block should now be a genuine attack.

↩ IF SOMETHING BREAKS

- **Add a targeted exclusion** (preferred) — fixes the one request and keeps protection everywhere else.
- **Drop the site back to Detect** while you investigate. It is instant, and never worse than not having the WAF.

✓ MOVE ON WHEN

The first hour of **Block** events contains genuine attacks only.

STAGE 6 OF 6

6 Finish the hardening

SITE MODE **BLOCK** TIME Under an hour, once blocking is stable

Task	Why	How
Prevent WAF bypass	Clients that reach the backend directly are never inspected.	Lock the backend's firewall (AWS Security Group / Azure NSG) so it accepts traffic only from the WAF.
Pass the real client IP	Your app's logs should show visitors, not the WAF.	Configure the backend to read <code>X-Forwarded-For</code> (e.g. Apache <code>mod_remoteip</code>) — <i>Troubleshooting & Support Manual</i> , chapter A.
Turn on alerts & reports	Hear about future attack spikes.	Settings → Alerts and Reports & compliance — <i>Features & Configuration Guide</i> , chapter 13.

✓ MOVE ON WHEN

Bypass is closed, client IPs are correct, and alerts are on.

BEFORE YOU CLOSE THE CHANGE

✓ Sign-off checklist

☐	Site status	The site shows Block / "Inspecting" (green) on the Sites page.
☐	Clean enforcement	A full day of Block -mode events contains attacks only — no legitimate traffic.
☐	No bypass	The backend is reachable only through the WAF.
☐	Client IPs	Real client IPs show correctly in the application's own logs.
☐	Cluster	If you run several nodes: the site config is on every node, and all nodes share the same <code>cluster.secret</code> .

SITE

COMPLETED BY

DATE

Related documents

Document	Use it for
Taming false positives (playbook)	The full method for clearing false positives in Stage 4.
GAJWAF Features & Configuration Guide	Every option in Stages 1, 2 and 6 — chapters 1 (General), 3 (Backend & TLS) and 13 (Settings).
GAJWAF Troubleshooting & Support Manual	Red health chips, client-IP problems (chapter A) and blocked legitimate traffic (chapter C).
GAJWAF Quick Setup Guide — AWS & Azure	First-run setup, including locking the backend to the WAF.