

GUIDE

How to Configure and Manage Shield Matrix



Shield Matrix is a cutting-edge security solution that protects your network by automatically identifying and blocking malicious IP addresses before they can launch attacks. This intelligent threat prevention system continuously updates from a global threat database, giving powerful, hassle-free protection without impacting performance.



Shield Matrix is part of the GFI KerioControl Security Add-On, working alongside the Intrusion Prevention System (IPS) and antivirus components. It provides GFI KerioControl and its users with "zero-day" defense capability.

Key Benefits

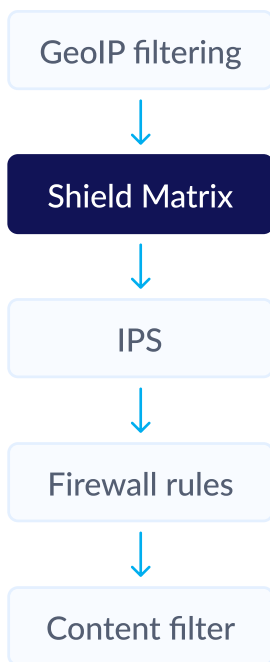
- ✓ **Zero-Day Protection:** Defends against emerging threats without waiting for traditional IPS updates
- ✓ **Intelligent Threat Detection:** Uses AI to evaluate and categorize potential threats
- ✓ **Resource Efficient:** All analysis happens on update servers, not your local appliance
- ✓ **Complementary Security:** Enhances existing IPS and antivirus protection
- ✓ **Simple Management:** Easy to enable with flexible response options
- ✓ **Enterprise-Grade Security:** Positions your infrastructure with competitive protection levels.

How Shield Matrix Works

1. Threat Detection:

- Shield Matrix gathers IP addresses through a global network of honeypots and traps.
- AI analyzes every attack attempt to assign a confidence level (Low, Medium, High).
- All analysis is performed on the update server, not your local GFI KerioControl appliance, ensuring optimal performance.

2. Real-Time Protection:



- Database updates occur every 15 minutes.
- Connections from flagged IPs are instantly dropped, preventing any data exchange.
- Shield Matrix operates immediately after GeoIP checks – the second engine to process network traffic.

Prerequisite: Shield Matrix is a new security feature in GFI KerioControl 9.5, part of the GFI KerioControl Security Add-On.

Here's how to activate and configure it:

This Knowledge Base article provides step-by-step instructions for enabling, configuring, monitoring, and troubleshooting Shield Matrix in GFI KerioControl. Shield Matrix is an advanced security feature that provides real-time, zero-day threat protection by automatically identifying and blocking malicious IP addresses.

Prerequisites:

- ✓ GFI KerioControl version 9.5 or newer
- ✓ Active GFI KerioControl Security Add-On license
- ✓ Administrator access to the GFI KerioControl administration interface.

What is Shield Matrix?

Shield Matrix is a key component of the GFI KerioControl Security Add-On, working alongside the Intrusion Prevention System (IPS) and antivirus components. It provides "zero-day" defense capability by leveraging AI to analyze and categorize potential threats, with all analysis performed on GFI's update servers rather than your local appliance.

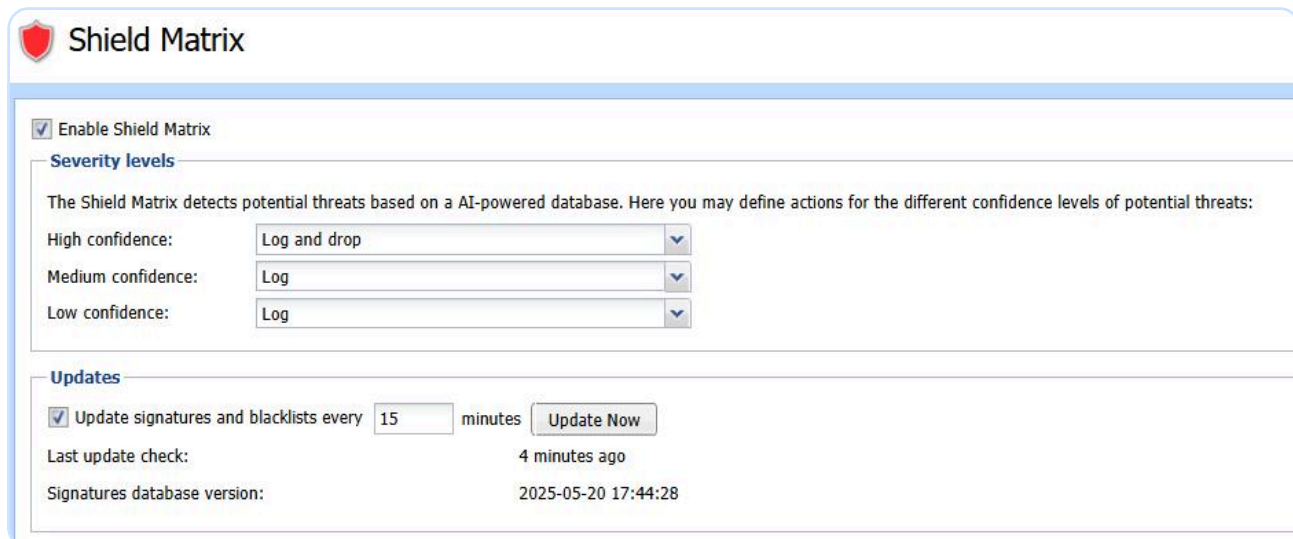
Enabling and Configuring Shield Matrix

Shield Matrix is a key component of the GFI KerioControl Security Add-On, working alongside the Intrusion Prevention System (IPS) and antivirus components. It provides "zero-day" defense capability by leveraging AI to analyze and categorize potential threats, with all analysis performed on GFI's update servers rather than your local appliance.

1 Accessing Shield Matrix

Shield Matrix can be managed through the Configuration section of your GFI KerioControl administration interface.

- Log in to your GFI KerioControl administration interface.
- Navigate to **Configuration > Shield Matrix**.



The screenshot shows the 'Shield Matrix' configuration page. At the top, there's a red shield icon and the title 'Shield Matrix'. Below this, there's a checkbox labeled 'Enable Shield Matrix' which is checked. Under the 'Severity levels' section, there's a descriptive text: 'The Shield Matrix detects potential threats based on a AI-powered database. Here you may define actions for the different confidence levels of potential threats:'. Below this text are three rows for 'High confidence:', 'Medium confidence:', and 'Low confidence:', each with a dropdown menu. The 'High confidence' dropdown is set to 'Log and drop', 'Medium confidence' is set to 'Log', and 'Low confidence' is set to 'Log'. Under the 'Updates' section, there's a checkbox labeled 'Update signatures and blacklists every' which is checked, followed by a text input field containing '15' and the word 'minutes'. To the right of this is a button labeled 'Update Now'. Below this, there's a line for 'Last update check:' with the value '4 minutes ago' to its right. At the bottom, there's a line for 'Signatures database version:' with the value '2025-05-20 17:44:28' to its right.

2 Enabling Shield Matrix

Activation is straightforward:

- In the Shield Matrix configuration screen, simply check the activation checkbox to enable the feature.
- The system will begin using the Shield Matrix protection immediately.

3 How Shield Matrix Works

Once activated, Shield Matrix will:

- Receive nearly real-time updates from the threat IP database (updates every 15 minutes)
- Analyze incoming connections using data gathered from a global network of honeypots and traps

5 How to Configure and Manage Shield Matrix

- Assign confidence levels to potential threats (Low, Medium, High) based on AI analysis and consideration of several factors, including:
 - Attacker with IP unknown to integrated 3rd party threat intelligence
 - Aggressive attack detected against trap
 - Continues attack from the same C segment IP
 - Probably human attacker detected
 - Fuzzing attack - Country-specific target attack.
- Process incoming traffic immediately after GeoIP checks (it's the second engine to process traffic).

4 Customizing Responses

You can configure how Shield Matrix responds to threats based on their confidence levels:

- Log and drop - for high threats - both records and blocks the connection
- Log only - records, but allows the connection
- No action - takes no action

5 Monitoring Shield Matrix Activity

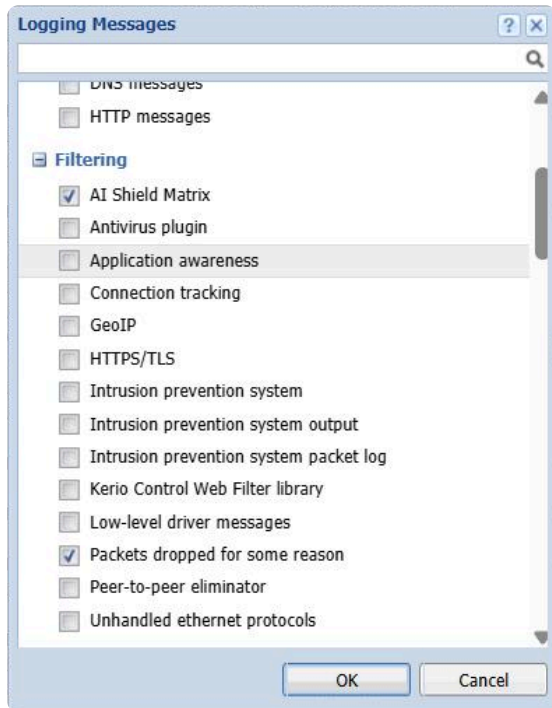
To view Shield Matrix activity:

1 item (0 selected)						
Timestamp	Source IP	Destination IP ▼	Protocol	Hit Count	Confidence Level	Shield Action
2025-05-20 17:52:27	91.223.169.83	87.197.108.82	TCP	1	High	Dropped

- Go to Status > Shield Matrix
- This screen shows connection data
 - Source IP addresses
 - Destination addresses
 - Timestamps
 - Action taken (logged/dropped)
 - Threat confidence level
- We can see whether the traffic was dropped, the severity, the source IP, and the timestamp.

Monitoring from Logs

Shield Matrix activities are also recorded in debug logs with more details.



- Go to Logs > Debug
- Enable message:
 - "AI Shield Matrix"
 - "Packets dropped for some reason."
- Look for entries labeled *"shieldMatrix, packet dropped for reason"* to track blocked threats. See sample log entries:
 - [05/May/2025 12:55:28] {pktdrop} packet dropped: ShieldMatrix determined the connection to be a threat (from WAN-TCOM, proto: TCP, len:60, 193.46.255.40:41690 -> 87.197.XXX.XXX:465, flags: [SYN], seq:142238294 ack:0, win:29200, tcplen:0)
 - [05/May/2025 12:55:53] {shieldmatrix} [ID] 569482 connection classified as a threat. Confidence=5, Action=LOG_AND_DROP

Shield Matrix is included as part of the GFI KerioControl Security Add-On bundle, alongside the IPS and antivirus features.