

Violation Responses - Manage Locked Out Clients

<https://campus.barracuda.com/doc/100370856/>

When Barracuda Waf-as-a-Service detects any violation, the requests are blocked as per the Follow Up Action defined for the identified violation. The locked-out IP addresses/client fingerprints/suspicious clients are displayed under **VIOLATION RESPONSES > Manage Locked Out Clients**. You can view the locked-out clients and clear them individually or clear all. For information about policy settings, refer to [Violation Responses - Policy Options](#).

The **Manage Locked Out Clients** page includes the following sections:

- **LOCKED OUT CLIENT IP:** IP address(es) of the clients that were locked out when the Barracuda WAF-as-a-Service detected the violation and the **Follow-Up Action** for the violation is set to **Block Client IP** on **VIOLATION RESPONSES > Response Policies**.

The table provides the following details

- **Client IP** – IP address of the client.
 - **Applications** – Application that the client attempted to access.
 - **Lockout Time Left** – The time (in seconds) that the client will remain in the locked-out state, after which the client is unlocked.
- **LOCKED OUT FINGERPRINTS:** Client fingerprints that were locked out when the Barracuda WAF-as-a-Service detected the violation and the **Follow-Up Action** for the violation is set to **Block Client Fingerprint** on **VIOLATION RESPONSES > Response Policies**.

The table provides the following details:

- **Client Fingerprints** – Fingerprint of the client.
- **Applications** – Application that the client attempted to access.
- **Lockout Time Left** – The time (in seconds) that the client will remain in the locked-out state, after which the client is unlocked.

Client fingerprints are identified and blocked only when **Client Fingerprinting mode** is set to **ON** under **VIOLATION RESPONSES > Policy Options > Client Fingerprinting**.

- **SUSPICIOUS CLIENTS:** Clients identified as suspicious and locked out when the Follow-Up Action is set to Challenge with CAPTCHA on **VIOLATION RESPONSES > Response Policies**.

The table provides the following details:

- **Client IP** – IP address of the client.
- **SUSPICION REASONS** – The reason why the Barracuda WAF-as-a-Service identified the client as suspicious.
- **Client Type** – Type of client.

Locked Out Client IP and Locked Out Fingerprints are locked out based on specific endpoints,

but Suspicious client is global. If a client is identified and locked out as a suspicious client, the client is added /marked as suspicious for all applications deployed in that container.

To Clear the Locked-out Clients

1. On the **Manage locked out clients** page:
 1. Select the check boxes next to the locked-out clients/client fingerprints/suspicious clients and click **Clear all**.
OR
 2. Select the main check box and clear all locked-out clients.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.