

## Legacy Licence Isolated Mode

<https://campus.barracuda.com/doc/93192338/>

- Isolated mode deployment is *Only* applicable to users with [legacy licenses](#). You can optionally avail the isolated mode deployment with the Application Protection Premium subscription license.
- Isolated mode deployment is *not* available in the Application Protection Advanced subscription tier.

### Overview

Barracuda WAF-as-a-Service Isolated Mode ensures your traffic runs through isolated infrastructure, without traffic from any other organizations. This provides the following benefits:

- A dedicated IP address in all deployment locations, not shared with any other organizations.
- The ability to accept traffic on any domain, rather than only for the domains you specify.
- Memory isolation from any other Barracuda WAF-as-a-Service users. While Barracuda WAF-as-a-Service already ensures that no data is ever shared between customers, the memory isolation can be useful for specific compliance situations.
- The ability to configure, with assistance from Barracuda Networks Technical Support, features that are not accessible in the Barracuda WAF-as-a-Service user interface, but are supported by the Barracuda CloudGen Web Application Firewall.

### Isolated Mode Eligibility

To be eligible for Isolated Mode, you must:

- Purchase 100 Mbps bandwidth or more.
- Purchase a Barracuda Networks [Premium Support](#) subscription.
- Deploy your applications in any Microsoft Azure region other than the region titled **North America and West Europe** (Legacy). For more information, see [Understanding Deployment Locations](#).

If you have purchased less than 100 Mbps of bandwidth, or have not purchased a Premium Support subscription, contact your Barracuda Networks partner or sales representative for information on how to upgrade your account. You will only pay the difference in price for the remainder of your license term.

---

## Isolated Mode Features

---

Barracuda WAF-as-a-Service and the Barracuda CloudGen Web Application Firewall use the same underlying protection engine, so all features supported by the Barracuda CloudGen Web Application Firewall are supported in Isolated Mode within Barracuda WAF-as-a-Service. Here are a few of the most commonly used features of Barracuda CloudGen Web Application Firewall, along with links to Barracuda Campus documentation, where you can read about the full functionality of each feature:

- Importing vulnerability reports from over 30 scanners and applying virtual patches – Refer to [Mitigating Website Vulnerabilities Using Vulnerability Scanners](#)
- Customizable notifications for specific events via email or Slack – Refer to [Events and Notifications](#)
- Customizing [Smart Signatures](#) and adding [Custom Attack Patterns](#).

To configure these features, [contact Barracuda Networks Technical Support 24/7](#) via phone or email.

© 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.