

## Release Notes Version 6.1.0.003

<https://campus.barracuda.com/doc/67176472/>

Before installing any firmware version, back up your configuration and read all release notes that apply to versions more recent than the one currently running on your system.

**Do not manually reboot your system at any time during an update unless otherwise instructed by Barracuda Networks Technical Support.** Depending on your current firmware version and other system factors, updating can take up to 10 minutes. If the process takes longer, contact Barracuda Networks Technical Support for further assistance.

### Features

- Support has been added for the HTTP/2 protocol over HTTPS. [BNADC-7208]
- The Barracuda Load Balancer ADC is now available on Microsoft Azure. [BNADC-7721]
- The Barracuda Load Balancer ADC on AWS now supports clustering across two availability zones for increased resilience and high availability. [BNADC-8017]
- Support has been added for configuring auto scaling groups as back-end servers in AWS. [BNADC-8353]

### Enhancements

- High Availability now supports automatic failover in case a critical process fails on an active device. [BNADC-1485]
- Server health checks now support HTTP/1.0 and HTTP/1.1. [BNADC-5632]
- The internal platform utilities and kernel have been upgraded. [BNADC-6461]
- LDAP nested groups across different domains are now supported. [BNADC-7595]
- Support for the AWS proxy protocol in WebSocket has been added and a known issue with backend SSL over WebSocket has been addressed. [BNADC-7613]
- The FTP access log can now be exported instantly. [BNADC-8408]

### Fixes

- Global Server Load Balancing (GSLB) can now process traffic without interruption. [BNADC-7021]
- The serial number of the clustered peer Barracuda Load Balancer ADC is now displayed on the **ADVANCED > High Availability** page in the **Clustered System** section. [BNADC-7101]
- Both units in a high availability cluster are in the active state. This has been addressed. [BNADC-7134]
- You can now specify the maximum number of times a user can attempt to authenticate. [BNADC-7392]
- When starting Instant SSL with an existing HTTP service, there are duplicate database variables. This has been addressed. [BNADC-7471]
- A report is now being sent when an SMTP sever is configured with a user name and password.

[BNADC-7866]

- A character is being removed while completing a SharePoint rewrite. This has been addressed. [BNADC-7933]
- Dual Authentication is now supported with LDAP as the primary authentication service and Radius as the secondary authentication service. [BNADC-8022]
- The initial characters of a certificate name can now include numbers. [BNADC-8137]
- If you set **Enable High Availability** to **Yes**, the default value for **Failback Mode** is now set to **Manual**. [BNADC-8155]
- Changing the service type from INSTANT SSL to HTTP/HTTPS and then back to INSTANT SSL now correctly creates the Redirect service. [BNADC-8422]
- After upgrading the firmware, the system failed to reboot due to a networking issue. This has been addressed. [BNADC-8449]
- If the LDAP authentication service's default role is changed by the administrator in the **ADVANCED > Admin Access Control** page, the role of LDAP mapped users is not changed. [BNADC-8453]
- The domain name can now be sent along with the username to the Radius server for user authentication. [BNADC-8598]

© 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.