Release Notes

https://campus.barracuda.com/doc/11141920/

Important: Please Read Before Upgrading

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 Support. Depending on your current firmware version and other system factors, updating can take up to **30 minutes**. If the process takes longer, please contact Barracuda Technical Support for further assistance.

Before upgrading, BE SURE TO TAKE THE BARRACUDA EMAIL SECURITY GATEWAY OFFLINE. This will ensure that the inbound queue is emptied and all messages are scanned before the update process begins. See the **BASIC > Administration** page for the **Offline** button.

Updating to Version 9.x

WARNING: After clicking **Apply Now** on the **ADVANCED > Firmware Update** page, the progress bar may appear to time out and the administrator may need to manually return to the login screen after **30 minutes** if it doesn't load automatically in the browser. **PLEASE DO NOT MANUALLY REBOOT THE BARRACUDA EMAIL SECURITY GATEWAY WHILE IT IS UPGRADING.**

Firmware Version 9.1

What's New in Version 9.1

Authentication

- When a user receives a 'lockout' email after 5 failed login attempts, the email message from the Barracuda Email Security Gateway now shows the hostname from the **Quarantine Host** field on the **BASIC > Quarantine** page INSTEAD of the system IP address. If the **Quarantine Host** field is not configured, the email will instead use the **Default Domain** for the hostname. [BNSF-28981]
- New **Verify LDAP Certificate** setting on the **Domains > Manage Domains > USERS > LDAP Configuration** page to verify LDAP connections when using SSL/TLS. [BNSF-28895]

Web Interface

- New **Supported SSL Protocols** setting on the **ADVANCED > Secure Administration** page

to indicate which TLS versions to support. [BNSF-28979]
- Replaced references to Blocklist / Whitelist with Block List / Allow List. [BNSF-10230] [BNSF-35056]

Clustering

- Improved management of Quarantine inbox for clustered systems. [BNSF-35078]
- Added additional check to ensure that clustered devices cannot be upgraded/downgraded if they are not in *Standby* mode. [BNSF-28997]

Vulnerability

- Upgraded support for OpenSSL 1.1.1g. [BNSF-28929]
- Improved default TLS-over-SMTP security posture. [BNSF-34957]

Version 9.1.0.001

- Resolved an issue with the SNMP agent not starting after firmware upgrade. [BNSF-28957]
- Resolved an issue related to messages failing to delete through **ADVANCED > Queue Management**. [BNSF-28942]
- Resolved an issue related to pop-up not working for Secondary Authorization on the **BASIC > Administration** page. [BNSF-35122]
- Resolved 'Invalid username and password' error thrown when clicking on a link in the Quarantine Summary email. [BNSF-34971]

Version 9.1.0.002

- Scheduled automated reports on the **BASIC > Reports** page send successfully. [BNSF-35236]
- Synchronization between clustered systems works as expected. [BNSF-35240]
- Fixed an edge case leading to malformed email when **Inbound External Sender Warning** is enabled. [BNSF-35170]
- Quarantined emails that have wide character in subject line are delivered successfully. [BNSF-35238]

Firmware Version 9.0

What's New in Version 9.0

Web Interface

- Drop-down **Help** button control on some web interface pages, providing links to relevant Barracuda Campus articles for additional information about features configured on those

pages.
- On the **BASIC > IP Configuration** page, **Trusted Forwarder** has been renamed **Known Forwarder**.
- **Firmware Patches** option for pushing product/security patches to the Barracuda Email Security Gateway on **ADVANCED > Firmware Update** page.
- **Uptime** – Display of uptime of the Barracuda Email Security Gateway in days, hours, and minutes in the **System Management** section of the **BASIC > Administration** page.

Mail Processing

- **Block Macros** enhancement – This feature now exempts whitelisted senders. See the **BLOCK/ACCEPT > Attachment Filters** page.
- **Inbound External Sender Warning -** Ability to enable external sender warning for inbound emails on **BASIC > Administration** page. [BNSF-28378]
- Improved Spam protection.
- Added support to block RAR 5.0.
- Sender spoofing settings of child domains are now independent of the parent domain.
- Improved sender whitelisting to avoid spam though sender spoofing.

Authentication

- **SSL/TLS Mode** option – Supports LDAPS for SMTP AUTH requests. Configure on **LDAP** tab of **BASIC > Outbound** page.

Clustering

- Enhancement: The *admin* password is now synchronized across clustered systems.

Message Log

- Re-delivery log entry added to Message Log when a blocked message is manually delivered by the administrator.

Security

- Ability to store trusted CA. [BNSF-27319]
- Improvements for backup through FTP: Added support for FTPSSL session reuse. [BNSF-28711] .
- CVE-2016-5385 – HTTPoxy. [BNSF-25943]
- Message Log P-XSS - malicious PTR record affects N/A. [BNSF-26827]
- Upgraded Jquery library - CVE-2015-9251 [BNSF-28117]
- Vulnerability: BCrypt support [BNSF-20799]
- Vulnerability: Login susceptible to directory harvesting. [BNSF-22574]
- Vulnerability: Avoid potential leaking of ‘bcc’ email addresses. [BNSF-28723]
- Added support for TLSv1.3 over SMTP and HTTPS by default for Barracuda Email Security Gateway.

Fixed in Version 9.0

- Fixed high severity vulnerability: Upraded OpenSSL, addressed the following CVEs. (CVE-2019-1563, CVE-2019-1547, CVE-2019-1552). [BNSF-27318]
- Vulnerability: Fixed unauthenticated XSS attack via view_help.cgi [BNSF-22335]
- Vulnerability: Fixed data path based persistent XSS attack through Message Log. [BNSF-26827]
- Vulnerability: Fixed unauthenticated remote command execution on Barracuda Email Security Gateway. [BNSF-27738]
- Misspelled password in 'Dansk' language on login page. [BNSF-28012]

Version 9.0.0.005

- Fixed issue in which the Message Log did not load through Barracuda Appliance Control in some scenarios. [BNSF-29802]
- Fixed error in Syslog start-up in some cases. [BNSF-28904]

Version 9.0.0.004

- Improved help documentation for secure integration of the Barracuda Email Security Gateway with other servers. [BNSF-28817]
- Fixed issue where Barracuda Support could not access the Barracuda Email Security Gateway when the Administrator IP/Range was configured on the **BASIC > Administration** page. [BNSF-28871]

Version 9.0.0.003

- Fixed: Peer Cert verification to enable encryption for outbound email. [BNSF-28842]
- Vulnerability fix: TLS connection for outbound emails. [BNSF-28837]
- Fixed: Issue related to purging emails. [BNSF-28841]

Version 9.0.0.002

- Improvement: Improved spam scanning. [BNSF-28802]
- Improvement: When **Inbound External Sender Warning** is set to *Yes* on the **BASIC > Administration** page, the associated warning message is added to each section of emails that have both a text/plain and text/html body. [BNSF-28822]
- Fixed: Reverting from version 9.0 to earlier versions completes successfully. [BNSF-28802]
- Fixed issue with quarantine notification email for Japanese Language. [BNSF-28754]

Updating to Version 8.x

WARNING: After clicking **Apply Now** on the **ADVANCED > Firmware Update** page, the progress bar may appear to time out and the administrator may need to manually return to the login screen after 5 minutes if it doesn't load automatically in the browser

Firmware Version 8.2

What's New in Version 8.2

- Improved support for Support Tunnel 2.0.

Version 8.2.0.002

Security

- Resolved Brazil Daylight Savings Time Zone issue. [BNSF-28612]

Version 8.2.0.001

Security

- Resolved XSS vulnerability for Message Log view. [BNSF-28394]
- Resolved vulnerability related to LDAP bind password being exposed. (R7-2019-39). [BNSF-28578]
- Improved support for SMB 2.0 backups. [BNSF-28514]

Firmware Version 8.1

What's New in Version 8.1

- Microsoft Exchange 2010 is no longer supported in version v8.1.x and above.

Version 8.1.0.005

Web Interface

- Resolved compatibility issues with older kernels. [BNSF-28561]

Version 8.1.0.004

Security

- Fixed medium severity vulnerability: Updated OpenSSL to address CVE-2017-3736 with OpenSSL upgrade.

Version 8.1.0.003

- Support for SMB versions 2.0 and 3.0 for backups. [BNSF-26803]
- Improved cloud backup support.
- Added an option in the web interface to enable/disable SSO/auto login for links in Quarantine Summary emails. [BNSF-27803]
- Removed *Extended Malware* from subscription statistics on the **BASIC > Dashboard** page. [BNSF-27935]
- Updated root CA certificates. [BNSF-27930]
- New advanced LDAP setting **Disable built-in LDAP Filter** to disable default LDAP filters as needed. Configure per-domain on the **USERS > LDAP Configuration** page. [BNSF-27992]
- The Outbound Quarantine feature is now available for models 100 and 200. [BNSF-27996]
- Included support for Support Tunnel 2.0 as part of firmware. [BNSF-27807]
- Spam accuracy improvements. [BNSF-28017]

Version 8.1.0.002

Authentication

- New option on **BASIC > Quarantine** page to enable/disable SSO/auto-login for users through links in quarantine summary emails. [BNSF-27803]
- New option to disable default LDAP filters used for authenticating the user on **USERS > LDAP Configuration** page at the domain level. [BNSF-27992]

Security

- Support for support tunnel version 2.0 [BNSF-27807]
- Updated root CA certificates [BNSF-27930]
- Spam accuracy improvements [BNSF-28017]

Web Interface

- Extended Malware Subscription information is no longer displayed on the **BASIC > Dashboard**

page. [BNSF-27935]
- The Outbound Quarantine feature is now available for Barracuda Email Security Gateway models 100 and 200. [BNSF-27796]

Firmware Version 8.0

What's New in Version 8.0

Web Interface

- The Barracuda Spam Firewall has been renamed the Barracuda Email Security Gateway.

Barracuda Exchange Antivirus Agent

- The Barracuda Exchange Antivirus Agent no longer supports Microsoft Exchange Server 2007. See How to Get and Configure Barracuda Exchange Antivirus Agent 8.x for details.

Fixed in Version 8.0

Version 8.0.4.002

Security

- Upgraded SAVAPI version to continue support for 'Extended Malware Protection'. [BNSF-27814]

Version 8.0.4.001

Authentication

- Feature: All users can now set and use a local password to access their quarantine account. [BNSF-27556]

Mail Processing

- Option to disable TLS 1.0 over SMTP through Barracuda Email Security Gateway web interface to conform to PCI standards of TLS 1.1+. [BNSF-27561]

Message Log

- Improvement: Added a popup to indicate that only 10k messages lines from the Message Log can be exported when the Barracuda Email Security Gateway is clustered. [BNSF-27650]

Security

- Resolved vulnerability with 7zip file compression (CVE-201810115). [BNSF-27684]

Version 8.0.3.004

- Fix: When a user logs in (as *user* role) and marks an email in quarantine as *NOT* spam, the email auto-delivers as expected. [BNSF-27442]

Version 8.0.3.003

- Feature: Active session tokens are now transmitted via cookies, rather than in a URL. This means that end-users will no longer be able to click on a link in the quarantine summary email to log directly into a quarantine inbox without the use of a password. [BNSF-26659]

Version 8.0.3.002

- Fixed bug affecting mail processing after upgrading the firmware. [BNSF-26691]

Version 8.0.3

Barracuda Outlook Add-in

- Enhancement: Added support for TLS 1.1 and TLS 1.2. [BNSF-25586]

Notifications

- Enhancement: The system administrator and email recipient can receive notifications when a message is blocked due to a virus. Configure on the **ADVANCED > Bounce/NDR Settings** page. [BNSF-25486]

Mail Processing

- Improved spam scanning. [BNSF-26591]

Version 8.0.2

Barracuda Exchange Antivirus Agent

- Feature: Added support for Microsoft Exchange 2016.

Web Interface

- Fix: A Welcome email is not sent when a new user account is created due to a quarantined email. [BNSF-25904]

Security

- High severity vulnerability: authenticated, remote code injection [BNSEC-6613 / BNSF-25407]
- High severity vulnerability: unauthenticated, remotely exploitable, code injection [BNSEC-6223 / BNSF-24618]
- High severity vulnerability: remotely exploitable, buffer overflow [BNSEC-2012 / BNSF-24897]
- Medium - High severity vulnerability: unauthenticated, remotely exploitable, denial of service (DoS), ssl weakness [BNSEC-7107 / BNSF-25937]
- Medium - High severity vulnerability: unauthenticated, remotely exploitable, limited HTML content control, XSS delivered outside of the web based interface [BNSEC-6227 / BNSF-24635]
- Medium - High severity vulnerability: unauthenticated, remotely exploitable [BNSEC-6225 / BNSF-24621]
- Medium severity vulnerability: non-persistent XSS [BNSEC-2678 / BNSF-23507]

Version 8.0.1.001

Mail Processing

- Enhancement: Mail with Microsoft Office attachments that contain macros can be blocked. [BNSF-23786]

Web Interface

- Resolved issue which prevented the Dashboard from displaying during update server outages. [BNSF-25934]
- Resolved issue preventing access to **ADVANCED > Energize Updates** and **ADVANCED >Firmware Update** pages when the Barracuda Email Security Gateway was offline. [BNSF-25929]

Barracuda Exchange Antivirus Agent

- Enhancement: The Barracuda Exchange Antivirus Agent supports Microsoft Exchange Server 2016. [BNSF-25828]

Version 8.0.0.007

Mail Processing

- Enhancement: Improved Sender Spoof Protection efficiency. [BNSF-25835]
- Resolved issue which could cause excessive system load. [BNSF-25831, BNSF-25884]
- Resolved issues with malformed headers causing incorrect parsing. [BNSF-25836, BNSF-25838]
- Resolved issue with Multi-Level Intent Analysis. [BNSF-25907]

Clustering

- Improved handling of Standby mode in a clustered system. [BNSF-25797]

Version 8.0.0.005

Mail Processing

- Outbound messages from whitelisted IP addresses are now properly checked for encryption if encryption is enabled. [BNSF-25732]
- Links in the **BASIC > Message Log** message view page now work properly. [BNSF-22345]