Release Notes

https://campus.barracuda.com/doc/16907/

What's New May 2025

- New feature now available to exempt senders from bulk email.
  - Customers can now exempt specific email senders or domains from the Bulk Email filter. This functionality is now available in the new admin user interface, located under **Email Gateway Defense > Inbound > Anti-Spam/Antivirus**. For more information, see Bulk Email Detection.

What's New April 2025

- New converged Email Protection onboarding wizard now available!
  - The rollout of our new, simplified onboarding wizard for Email Protection customers and trials is now available. This update introduces a streamlined, step-by-step experience for setting up key features, including Email Gateway Defense, Impersonation Protection, and Incident Response. This marks a significant milestone in our efforts to enhance and unify the email protection user experience. Stay tuned for upcoming enhancements, including the ability to easily configure mail flow through Inline Deployment.

What's New February 2025

- New updated Email Gateway Defense admin user interface enabled by default for new customers and available for opt-in for all customers. See Updated User Experience for Email Gateway Defense.
- Scheduled reporting is now available for Email Gateway Defense customers in the new admin user interface. This new capability allows you to automatically generate predefined reports and have them delivered straight to your inbox via email as a CSV attachment. Simply choose the report, timeframe, delivery frequency, and recipients. See Scheduled Reports.

What's New January 2025

- A new Email Gateway Defense admin user interface is now available for opt-in to 80% of customers. See Updated User Experience for Email Gateway Defense.
- Machine detection learning models updated with extortion classifier, improving false positive and false negative rates for extortion emails. See Machine Learning.

What's New December 2024

- The layout of the Email Gateway Defense Message Log has been improved to enhance usability on smaller screens.

What's New October 2024

- Email warning banners available in open beta to all customers. See Email Warning Banner Messages.
- New quarantine end user UI now available to all customers.

What's New September 2024

- Recalling encrypted messages is now available on Email Gateway Defense. See How to Use DLP and Outbound Mail Encryption.
- The Reported Email Tracker, which utilizes the Enhanced Feedback feature to report emails to Barracuda Networks, is now available in open beta for all customers. See Reported Email Tracker. Closed-loop feedback for reported emails now available in open beta to all customers.
- Email warning banners available in open beta to a select group of customers. See Email Warning Banner Messages.

What's New August 2024

- New quarantine end user UI now available to 50% of our customers.
- An updated Microsoft 365 deployment guide now available, aligned with Microsoft Enhanced Filtering capabilities. See Step 2 - Configure Microsoft 365 for Inbound and Outbound Mail.
- Simplified and streamlined login experience for administrators and end users.

What's New July 2024

- Microsoft 365 inline deployment for Email Gateway Defense currently available in beta phase. See Microsoft 365 Inline Deployment.

What's New May 2024

- Email Gateway Defense is now available in the India AWS region. See Email Gateway Defense IP Ranges Used for Configuration and Email Gateway Defense Outbound IP Ranges.
- Machine learning detection models focused on spam, phishing, and extortion now available globally for all customers. See Machine Learning.

What's New April 2024

- Machine learning detection models focused on spam, phishing, and extortion now available for US customers. See Machine Learning.

What's New March 2024

- End users on the latest new end user interface will now see an updated sidebar menu for navigation. See Email Gateway Defense New User Interface User Guide.
- Machine learning detection models focused on spam, phishing, and extortion now available for UK customers. See Machine Learning.

What's New as of December 4, 2023

- Get a deep dive into Email Gateway Defense best practices and understand how to better utilize the capabilities the solution has to offer. See Email Gateway Defense Best Practices Guide.

What's New as of November 15, 2023

- Install and configure the new Email Gateway Defense app in Azure AD. For more information, see How to Configure the New Email Gateway Defense App in Microsoft Entra ID .

What's New as of October 25, 2023

- Added feature for SPF exemptions by domain. For more information, see How to Configure Sender Policy Framework.

What's New as of October 16, 2023

- Added feature for GeoIP exemptions by email address/domain and sender IP address. For more information, see Regional Policies .

What's New as of September 19, 2023

- Latest new end user interface now available with advanced authentication. The new interface is continually being rolled out to end users. For the new user guide, see Email Gateway Defense New User Interface User Guide.
    - With the recent changes, an administrator may need to grant consent to the Email Gateway Defense app for your organization. End users may also see a consent screen based on the security consent policies set in Azure AD by the administrator. For more information, see Viewing and Changing Consent Policies in the Azure Portal.

What's New as of August 25, 2023

Public API

- The Email Gateway Defense API is now also available in the United Kingdom (UK) region. For more information, see API Overview.

Mail Flow

- Increased the size of available outbound IPs for use by servers, allowing blocked mail to be deferred and retried from a different IP to successfully deliver mail. [BNESS-23533]

What's New as of May 22, 2023

Incident Report

- Email Gateway Defense (EGD) UI outage incident report https://esstimeline.barracudanetworks.com/publications/incident-report-for-egd-ui-outage-on-may-22-2023.
    - As there was an extremely high number of affected customers and emails, Email Gateway Defense is unable to manually rescan and redeliver mail that was incorrectly blocked due to this incident. To help remediate the high number of emails, administrators can allow end users to redeliver their mail:

1. The administrator signs into Email Gateway Defense. Under the **Users** tab, select **Default Policy**.
2. For the **Allow end users to view and deliver blocked messages**, click **Yes** if the option was previously set to No.
3. Click **Save Changes**.

Enhancement

- Users will now be able to login and deliver their incorrectly blocked mail.
  - ***Note*** that administrators must advise users to proceed with caution as this will potentially allow users to send mail that should not be delivered. If administrators are concerned about future user behavior, they can reset this setting to **No** after mail has been delivered from this incident.

What's New as of April 25, 2023

- Added a temporary passcode authentication method feature to allow users access to their shared mailbox and distribution list accounts. Enable the feature on the **Users > Quarantine Notification > Allow users to sign in with temporary passcode** page.
  - For more information, see Quarantine Notifications and Temporary Passcode Authentication. See also https://esstimeline.barracudanetworks.com/publications/temporary-passcode-authentication.
  - Note that the administrator feature under **Users > Quarantine Notification > Require login credentials to access quarantined messages** has been removed.

What's New as of March 31, 2023

- Auto-authentication has been disabled for end users from quarantine email digests. End users will now be required to authenticate before they can view their account and make updates to their quarantined emails.
- In addition, the administrator feature under **Users > Quarantine Notification > Require login credentials to access quarantined messages** has been enabled to **Yes** for all users and greyed out to ensure that all end users must log in to view their accounts.
  - For more information, see https://esstimeline.barracudanetworks.com/publications/email-gateway-defenses-update-to-end-user-authentication.

What's New as of February 8, 2023

Enhancement

- Barracuda Networks expands new end user interface to Email Gateway Defense.
  - Notes:
    - This platform launch is a 1-for-1 migration from the old framework, which means that there are no new features/capabilities at this time, just a new “skin” or “look and feel.” However, this migration will allow us to add new features or make changes to our products much more quickly in the future.
    - This launch is for the end user portion of the product only. We’ve begun work on the admin interface and will have a beta version available for users to try.
    - This new interface will be rolled out slowly to end users over the next 4-6 weeks (beginning February 8th, 2023). For the new user guide, see Email Gateway Defense New User Interface User Guide.
    - Only accounts with a “User” role will see the new UI. If you have set a user as a “domain admin” or “helpdesk” role within EGD, they will need to be set to “user” in order to see the new UI. This is NOT the same thing as setting up an administrator through Barracuda Cloud Control.

What's New as of May 23, 2022

Fixed in this Release

- Fixed an issue where 5xx inbound/outbound cache causes emails to be blocked for invalid reasons. [BNESS-19949]

What's new as of May 11, 2022

Fixed in this Release

- Fixed an issue where Link Protection parsing does not handle domains that end with a dot (.) in some circumstances, allowing links to bypass link protect action. [BNESS-22377]

What's New as of April 30, 2022

Fixed in this Release

- DKIM checking handles multiple DKIM signatures as expected. [BNESS-22325]

What's New as of January 31, 2022

Fixed in this Release

- False "Barracuda Login" events in EGD audit log are no longer present. [BNESS-21855]

What's New as of December 6, 2021

Updated new Email Gateway Defense documentation as part of the new Barracuda Email Protection.

For more information on the new Barracuda Email Protection plans, see Overview of Email Protection Plans.

What's New as of September 24, 2021

New Feature

- Enabled OneTrust cookie consent popup when loading the UI. [BNESS-20829]

Fixed in this Release

- Fixed an issue where emails are allowed but not delivered when encryption exemption is triggered and recipient is another ESS account. [BNESS-21473]
- Added group lookup by email address to existing user lookup Azure AD API to ensure all users exist in Azure AD. [BNESS-21597]

What's New as of June 4, 2021

New Feature

- Added new feature to add exemptions to outbound encryption policies. Select the **Do not encrypt** action filter to customize outbound encryption exemptions for subject, headers, body, attachments, sender, or recipient. Note that when you select **Do not encrypt** on a **Message Content Filter** and **Encrypt** on a **Predefined Filter**, the Message Content Filter exemption takes precedence over the Predefined Filter and the message will not be encrypted. See Content Analysis - Outbound Mail. [BNESS-2148]

What's New as of March 31, 2021

New Feature

- Added new feature for admins to select if user exemptions for sender policies should override admin block lists. See Understanding User Accounts. [BNESS-20406] [BNESS-20312]

What's New as of March 12, 2021

Security

- Disabled TLS 1.0/1.1 on Barracuda Email Security Service inbound mail servers. [BNESS-20269]

What's New as of February 26, 2021

Reporting

- Updated report columns in ESS reports. See Reporting. [BNESS-20544]

What's New as of February 22, 2021

New Features

- Barracuda Essentials customers who use Splunk can now download the ESS application in splunkbase. See Splunk Integration.

What's New as of January 29, 2021

Web Interface

- Added quarantine and block options from domains with no SPF records. [BNESS-20413] [BNESS-5754]
- **Report as Incorrectly Delivered** and **Report as Incorrectly Blocked** buttons in the Message Log now redirect to a feedback response form to request for additional details about the message.
- Default setting is **Off** for email categorization mailing lists to ensure all spam scanning and

policy processing is performed on the messages.

What's New as of January 15, 2021

Web Interface

- Quarantine notification email updated with **BLOCK LIST** option. This adds the sender's address to their User Sender Policies list as a BLOCKED sender from their Quarantine notification. [BNESS-5072]

What's New as of December 18, 2020

Web Interface

- Added feature to prevent users from delivering quarantined mail. [BNESS-19725]

Fixed in this release

- Settings for domain level users in the Default Policy page are now working as designed. [BNESS-20242]

What's New as of November 20, 2020

Cloud Protection Layer

- After the migration process from Barracuda Email Security Service to Cloud Protection Layer, any sender policies, GeoIP policies, or linked domain policies settings set to quarantine in ESS will convert to block in CPL. See Moving from Email Gateway Defense to Barracuda Cloud Protection Layer. [BNESS-19926]

What's New as of October 23, 2020

Documentation and Web Interface

- Updated Barracuda terminology, removing whitelist/blacklist and changing to allow list/block list. [BNESS-19674] [BNESS-19737] [BNESS-19738]

Web Interface

- Enabled the download button in the Outbound Quarantine Log for messages larger than 20MB. This feature is already available for inbound and outbound mails in the Message Log. [BNESS-19873]

What's New as of September 25, 2020

Web Interface

- Enabled the download button in the Message Log for messages larger than 20MB. This feature applies to inbound and outbound mails in the Message Log, but not currently in the Outbound Quarantine Log. [BNESS-19697]
- Added Enable Read Receipts feature for encrypted emails going through the Barracuda Email Security Service. [BNESS-3728]

Cloud Protection Layer

- Added **ATP Scan Inconclusive** as a blocked message action. [BNESS-19468]

Mail Flow

- Updated time limits on the ESS caching service. See Email Cache Policies. [BNESS-19096]

What's New as of June 19, 2020

New Feature

- Barracuda Email Security Service API beta release now available. The beta release includes read-only APIs to get information on accounts, domains and inbound/outbound email statistics. The Barracuda Email Security Service API is currently only available for accounts in the US region.

Fixed in this Release

- Quarantined mail with attachments are checked by Barracuda Advanced Threat Protection. [BNESS-19051]

What's New as of June 5, 2020

Mail Processing

- Added feature to require users to enter their login credentials before they can access quarantined messages. [BNESS-2892] [BNESS-19117]

What's New as of May 22, 2020

Web Interface

- Updated to allow customers to run reports up to 30 days. [BNESS-18992]

Fixed in this release

- Only domain administrators and helpdesk can access ATD logs for domains they are managing. End users cannot access ATD logs. [BNESS-19039]

What's New as of April 24, 2020

Web Interface

- Added feature to test individual Azure AD email users. [BNESS-16869]
- Added feature to block, quarantine, or ignore password protected PDF documents. [BNESS-15548] [BNESS-16872]
- Added feature to rewrite recipients for aliased domains. [BNESS-16558] [BNESS-16814]

What's New as of April 10, 2020

Fixed in this release

- Fixed issue when domain admin users try to access the **Domain Settings** page for domains they have permission to administrate, they're no longer seeing an error. [BNESS-16822]

What's New as of March 26, 2020

Security

- Scan .eml attachments to look for threats. [BNESS-15976]

Mail Flow

- After an account is upgraded or terminated, mail flow is continued for a grace period of 30 days. [BNESS-16644]
- Added recipient cache response for mailing lists when sending to recipients with no response. [BNESS-11537]

What's New as of February 28, 2020

Cloud Protection Layer

- SPF quarantine option not available in Cloud Protection Layer. [BNESS-16538]

Web Interface

- Additional UI changes for SPF quarantine option. [BNESS-15989]

Security

- Removed insecure ciphers. See TLS with Insecure Ciphers and SSLv2/SSLv3 No Longer Supported. [BNESS-16427]

What's New as of February 14, 2020

Web Interface

- **Audit Log**: Audit Log now available. Displays all system activity. See Understanding the Audit Log. [BNESS-16390]
- **Sender Policy Framework (SPF)**: Now includes a quarantine option and changes to hard and soft fails. See How to Configure Sender Policy Framework. [BNESS-15990]
- **Outbound > Abuse Monitoring** page removed. [BNESS-16452]

What's New as of January 15, 2020

New Regions Available

The following two regions are now available for Barracuda Essentials:

- Australia [BNESS-16238]
- Canada [BNESS-16239]

What's New as of December 17, 2019

Message Log Searching

- **Beta Feature: Search for Messages Across All Domains Simultaneously** – In the Message Log, you can now search for messages across all the domains in your account simultaneously. Previously, there was a search limit of 10 domains. You can now search by single domains or by all domains. [BNESS-15948]

What's New as of August 16, 2019

Mail Flow

- Updated MX record configuration messages. [BNESS-15287]

Documentation

- Clarified MX records and aliased domains. For details, refer to Understanding the Domains Page.

What's New as of August 1, 2019

Web Interface

- Message Log has cleaner look. Displays Action and Reason for selected message. Click **Show Details** to view additional information about the message. [BNESS-14793]
- **Spam**/**Not Spam** buttons are now renamed as **Report as Incorrectly Delivered**/**Report as Incorrectly Blocked**. These options appear only when a message is blocked or allowed based on Barracuda policies, not your own configuration. Clicking one of these buttons for the selected message returns a pop-up window, confirming report has been sent. [BNESS-14796]

What's New as of July 19, 2019

Web Interface

- New Reasons added to Message Log when issue is remediated by Barracuda Sentinel or by Barracuda Forensics & Incident Response. [BNESS-15084]

Documentation

- Added instruction for moving from LDAP to Azure in How to Configure User Authentication with Microsoft Entra ID.
- Added information on Message History in Campus and online help.

What's New as of July 5, 2019

Web Interface

- Message History added to Message Log. [BNESS-12566]
- Moved Spam and Not Spam buttons in Message Log. [BNESS-14795]

Azure AD Domains

- Azure AD authorized domain no longer shows authorization date. [BNESS-12566]

Mail Flow

- Automated end-user Linked Accounts page. [BNESS-14805]
- Set up HTTP API errors. [BNESS-14883]

What's New as of June 21, 2019

Web Interface

- Message Log: Identify messages that have been remediated by either Barracuda Sentinel or Barracuda Forensics & Incident Response. [BNESS-14143]

Mail Flow

- SPF macros are now evaluated. [BNESS-8518]

Fixed in this Release

- Fixed issue where some messages were not showing up in the Advanced Threat Protection (ATP) log. [BNESS-14846]

What's New as of June 7, 2019

Mail Flow

- Automated end-user Change Password page. [BNESS-12819]

What's New as of **May 24, 2019**

Fixed in this Release

- Fixed issues with LDAP sync. [BNESS-14726]

What's New as of **May 10, 2019**

Fixed in this release

- Fixed user-aliases issue related to blank message log search. [BNESS-14646]

What's New as of **April 26, 2019**

Fixed in this Release

- A *Domain Specific Policies* flag now appears on the Domains page when a domain has its own setting for External Sender Warning. [BNESS-14424]
- *Reset to account polices* functionality now works for all policies - including the *Allow end users to view and deliver blocked messages* setting. [BNESS-14424]

What's New as of **January 8, 2019**

Web Interface

- Fixed an issue where helpdesk users were unable to block senders from the message log. [BNESS-13377]
- Changed the text on the "Advanced Search" button in message log. [BNESS-11478]

What’s New in Version 2018.16 (since December 5, 2018)

Web Interface

- Removed unneeded navigation elements for End Users, Help Desk Users and Domain Admins. [BNESS-12581]
- Added a “Login as Administrator” link on the login page. [BNESS-11511]
- Improvement to Advanced Search on Message Logs. [BNESS-11478]
- Advanced Threat Protection notification email text change. [BNESS-13009]
- Clarified CNAME record setup steps when moving a domain to a different account. [BNESS-13145]

Mail Flow

- Improved speed and consistency of DKIM validation. [BNESS-13049]
- Fixed an issue when extracting 7zip attachments. [BNESS-13099]
- Fixed an issue when looking up data from BRTS. [BNESS-13103]
- Added ATD Exemptions for customer-to-customer emails. [BNESS-9168]

What's New in Version 2018.16

Mail Flow

- Fixed an issue where policies would not be honored in certain situations [BNESS-12969]

Self-Service Domain Moves

- You can transfer a domain you own to a different account. [BNESS-11451]

Performance

- Potential LDAP sync timeout cases addressed. [BNESS-12885]

What's New in Version 2018.15

Mail Flow

- Added a new scanning layer for image-based advertisement spam. These messages will be blocked for reason *Image Analysis*. [BNESS-11216]

Message Center

- Attachments sent in replies are now scanned for viruses [BNESS-12573, BNESS-12718]

Cloud Protection Layer

- Fixed an issue with messages being *quarantined* for DMARC. They will now be blocked. [BNESS-12663]

Directory Services

- Fixed problems with LDAP manual synchronization in the UK and DE regions [BNESS-10370]

What's New in Version 2018.14

Mail Flow

- Spooling fix for empty envelope from [BNESS-12672]
- Sender whitelist always prevents the sender spoof block [BNESS-12580]
- Fixed ATP check for **allow** policies [BNESS-12190]
- Spam checking is done before bulk email check [BNESS-12422]

Web Interface

- Fixed bug affecting LDAP **Synchronize Now** feature in certain regions [BNESS-10370]

What's New in Version 2018.13

Mail Flow

- Fixed an issue with sender spoof protection blocks being overwritten by other scanning layers [BNESS-12410]

Web Interface

- Restored the **All** Message Log filter for end users [BNESS-12097]
- Added option to allow end users to view and deliver blocked emails; this does not apply to emails blocked for Advanced Threat Protection (ATP) [BNESS-12095]

What's New in Version 2018.12

Mail Flow

- Blocks for **barracuda_email_blocklist** are no longer converted to quarantine [BNESS-12005]

User Interface

- Configure Backup/Restore is now fully available in all regions

Miscellaneous

- Stability improvements

What's New in Version 2018.11

Mail Processing

- Fixed an issue with 'encrypt' predefined content filter precedence [BNESS-11692]

User Interface

- Updated wording in the dashboard's subscription panel [BNESS-11294]
- Updated help files [BNESS-11789, BNESS-11892, BNESS-11899]
- New warning displays when trying to save account settings if domain settings exist [BNESS-11364]

What's New in Version 2018.10

Mail Flow

- Fixed an issue with DKIM [BNESS-11685]
- All new Barracuda Essentials trials will have Advanced Threat Protection (ATP) enabled [BNESS-11397]
- Attachment Intent checker is now at 100% [BNESS-10512]

User Interface

- Message headers are visible to MSPs for accounts with Message Privacy enabled [BNESS-11116]
- End users can no longer view or deliver/whitelist blocked messages and the **Delete** button for quarantined messages is now separate from the other buttons [BNESS-11309, BNESS-11376, BNESS-11377, BNESS-11226]
- Added link to blocked messages at the end of the inbound quarantine notification email [BNESS-11302]
- Fixed an issue with bulk edit [BNESS-11632]
- Updated the help file for **Block on no PTR Records** [BNESS-11675]

Directory Services

- Fixed an issue where synchronized Azure AD users had the wrong linked accounts

[BNESS-11673]

What's New in Version 2018.9

User Interface

- Added the Help Desk Role. In this role, users can deliver messages, view message headers, view domain-level settings, and view all domain settings and users for the assigned domains. Note that the Help Desk role cannot view message body on a user's account. [BNESS-10436]
- Improved logging for messages deferred for suspicious nameserver [BNESS-10848]
- Fixed an issue with the **Delete** button in the user message log [BNESS-11113]
- Updated the Rate Control documentation to be more accurate for CPL accounts [BNESS-11262]
- Advanced Threat Protection (ATP) will be enabled by default for all Barracuda Email Security Service trials [BNESS-11397]

What's New in Version 2018.8

Mail Processing

- Spam accuracy improvements [BNESS-10837], [BNESS10806], [BNESS-10876]
- Option to block or quarantine password protected Microsoft documents is now at 100% [BNESS-7623]

User Interface

- Show error message when attempting to generate reports older than 30 days [BNESS-11074]

What's New in Version 2018.7

Active Directory Enhancements

- Added Azure AD support on a per-domain basis

Mail Processing

- Added extra headers to the message [BNESS-10844]
- CVE for the p7zip vulnerability [BNESS-10892]
- Added option to block or quarantine password protected Microsoft documents; initially available as an option to customers during slow rollout [BNESS-7623]

User Interface

- Sender Spoof feature name change in the UI to Sender Spoof Protection [BNESS-10822]
- Added more details in sender spoof protection documentation [BNESS-10987]
- Updated the help Menu for Intent Domain Policies [BNESS-9099]
- Performance improvements to the user settings page [BNESS-10165]

What's New in Version 2018.6

User Interface

- Separated the Outbound Hostname section from MX Records Configuration section [BNESS-8014]

What's New in Version 2018.5

Mail Processing

- Added Sender Spoof Protection
- Enabled Domain Based Message Authentication (DMARC) option for inbound messages; this feature was initially available as an option to customers during the slow rollout
- Improvements to content filters
- Advanced Threat Protection (ATP) supports all Microsoft Office extensions
- Limit the number of recipients per message
- Added ability to block emails based on language

User Interface

- Added Customer feedback form

What's New in Version 2018.4

Mail Processing

- Advanced Threat Protection sender exemptions now take sender headers into consideration
- Improvements to link protection
- Improvements to spam accuracy
- Select regional sender policies

What's New in Version 2018.3

Mail Processing

- Added ability to block emails by location
- Graceful failover when antivirus results are not available
- Improvements to Link Protect accuracy
- Improvements to SPF accuracy
- Free Spamhaus RBL is no longer processed

What's New in Version 2018.2

User Interface

- Performance and stability improvements

Mail Flow

- Spam accuracy improvements
- Bulk email detection for headers

What's New in Version 2018.1

Mail Processing

- Miscellaneous improvements and robustness to improve stability

User Interface

- Miscellaneous UI optimizations

What's New in Version 2017.17

Mail Processing

- Link Protect improvements:
  - Link Protect can be exempted using recipient policies
  - Improved management of space before the link
- Advanced Threat Protection improvements

What's New in Version 2017.16

Web Interface

- Admins can now restrict users from exempting or blocking messages under the **Default Policies** page

Mail Processing

- Improved spam scanning accuracy

What's New in Version 2017.14

Web Interface

- Improvements to Redelivery Queue UI to include additional detail into SMTP failures
- **Reports** include **Blocked:Policy** and **Blocked:Other** columns for Inbound and Outbound traffic
- **Message Log** displays attachment icon for messages with an attachment
- **ATP Log** displays time stamps based on the time zone selected on the account

What's New in Version 2017.12

Web Interface

- Region selection support for CPL customers using setup wizard
- Miscellaneous improvements

What's New in Version 2017.11

Web Interface

- Quarantine Notification digest text color changed to black

Mail Flow

- Advanced Threat Protection enhancements to better handle pending scan after threshold time has passed

What's New in Version 2017.10

Mail Flow

- Fix mishandling of emails in link-protected messages
- Improvements to file type detection accuracy
- Miscellaneous speed improvements

Web Interface

- Quarantine notifications are now sorted by date
- Improvements to recipient count accuracy
- Improvements on how UI redelivery handles malformed messages
- Improvements to automatic LDAP sync efficiency

What's New in Version 2017.9

Mail Processing

- SPF blocks are no longer converted to quarantine under any circumstances

What's New in Version 2017.8

Mail Flow

- Added option to quarantine Real Time System (BRTS), Reputation Block List (BRBL) and Anti-Fraud Intelligence (BAFI)
- Improved efficiency of Advanced Threat Protection (ATP)
- Improved spam accuracy

Web Interface

- Improved performance of user lists with large number of users
- Improved accuracy of dashboard stats
- Improved reliability of saved searches in Message Log

What's New in Version 2017.7

Link Protection

- Fixed issue where CID, MID, and MAILTO prefix links were being link protected
- Added ability to apply Sender or IP policy exemptions to link protect

Miscellaneous

- Fixed case sensitivity issue in Intent domain exemptions
- Fixed corner case where Admins/Users could view or download some messages blocked for virus
- Fixed issue where Saved Searches with drop-downs were not working
- Fixed issue with exporting ATP log to CSV file
- Fixed the ability to deliver the maximum 200 messages from the message log

What's New in Version 2017.6

Quarantine Notifications

- TLS support for quarantine notifications
- Quarantine notification tracking in the Message Log
- Unified inbound/outbound UI scheduling
- Updated quarantine notification UI, mobile-friendly UI
- Fixed quarantine notifications display issue for some Office 365 customers

Web Interface

- Ability to redeliver Inbound messages with an empty 'Envelope From' field
- Ability to redeliver Deferred emails
- The notification banner is hidden on the **Domains** page when the MX records are set correctly

Miscellaneous Stability Improvements and Fixes

- Fix to prevent Quarantine Notification settings in the UI from selecting the wrong tab on page refresh

What's New in Version 2017.5

Web Interface

- Reorganized navigation links
  - New **Overview** tab which contains the **Dashboard**, **Message Log**, **ATD Log**, and **Outbound Quarantine** sub-tabs
  - **ATP Settings** (Formerly known as ATD Settings) has been moved from **Inbound**

Settings to its own tab.

- Renamed Advanced Threat Detection (ATD) to Advanced Threat Protection (ATP)

What's New in Version 2017.4

Mail Processing

- Miscellaneous stability improvements and fixes

Web Interface

- Automatic domain verification added to the domains page
- Improved responsiveness in message actions

What's New in Version 2017.3

Web Interface

- New User will get the Domain level/Global level quarantine notification setting
- Auto enable feature for Email Continuity

Mail Processing

- When enabled, link protection is applied to blocked/quarantined messages

What's New in Version 2017.2

Web Interface

- Advanced Threat Detection
  - Log interface re-designed with support for filtering

Mail Processing

- Improvements to link protect functionality
- Miscellaneous stability improvements and fixes

What's New in Version 2017.1

Web Interface

- Domains List
  - Redesigned to improve overall user experience
  - Domains using domain level settings now have an indicator and can be reverted from the **Domains** page.
- Recipient List
  - Number of recipients are now viewable on **Dashboard** and **Domains** pages
  - List of recipients can now be viewed from **Domains** page
- Miscellaneous compatibility and performance improvements

Mail Processing

- Miscellaneous/stability improvements

What's New in Version 2016.18

UI Improvements

- Email Continuity Service
  - Added ability to choose sender address presentation from alias/linked accounts when composing, replying, or forwarding
  - Progress indicator when sending message

Mail Flow Changes

- Miscellaneous/stability improvements

What's New in Version 2016.17

Web Interface

- Email Continuity Enhancements
  - Ability to add multiple attachments
  - Ability to add attachments when forwarding email
  - When a message is sent, the sender receives a copy of the message
  - Ability to Reply All and CC through email continuity

What's New in Version 2016.16

Web Interface

- Performance and stability improvements

Mail Processing

- Performance improvements

What's New in Version 2016.15

Mail Processing

- Miscellaneous stability/performance improvements

Web Interface

- Email Continuity
  - In the case of mail server downtime, users can now receive and send mail from the web interface
- Dynamic message log/outbound quarantine log/user log loading
  - Improved the speed and response time of those pages

What's New in Version 2016.14

Mail Processing

- Miscellaneous stability improvements
- Fixed some cases of ATD exemptions not being applied

Web Interface

- Dynamic page loading
  - Certain pages will load dynamically, improving the speed and response time of those pages

What's New in Version 2016.13

Web Interface

- Performance and availability improvements

Mail Processing

- Performance improvements

What's New in Version 2016.12

Web Interface

- Message Log improvements
- ATD Log improvements
- Performance improvements

What's New in Version 2016.11

Web Interface

- View ATD Reports per attachment in the ATD Log
- Admins can now deliver messages blocked for ATD through the Message Log.
    - When delivering messages, admin needs to view the reports on blocked attachments before delivery. This provides detailed information about why an attachment was blocked and when a threat was first detected.

Mail Processing

- Managed users are now tracked independently for outbound rate limiting
- Link protect system improvements.
- Miscellaneous performance improvements.

What's New in Version 2016.10

Web Interface

- Customers can exempt trusted sender or recipient of an email from ATD scan based on email address, domain, and / or IP address.
- Fixed issue in ATD Log where certain entries remained stuck in **Scanning** status.

Mail Processing

- Improved outbound virus protection.

What's New in Version 2016.9

- Miscellaneous improvements and bug fixes.

What's New in Version 2016.8

- Stability improvements.

What's New in Version 2016.7

Web Interface

- Miscellaneous improvements and bug fixes.

Mail Processing

- Outbound message encryption improvements.
- Barracuda Reputation Block List increased efficiency.
- Advanced Threat Detection is now more robust.

What's New in Version 2016.6

- Stability improvements.

What's New in Version 2016.5

- Quarantine notifications now include a direct link to the *whitelist* action. This enables users to whitelist a sender.
- Stability improvements.

What's New in Version 2016.4

Web Interface

- Resellers can now manage multiple accounts using the pull-down selection in the Barracuda

Cloud Control web interface.
- Miscellaneous improvements and bug fixes.

Mail Processing

- Ability to scan first and then deliver messages with Advanced Threat Detection (ATD) subscription. Messages will be deferred until the scan has completed if the scan exceeds a certain timeframe.
- Improved processing efficiency.

What's New in Version 2.8.9

Web Interface and Mail Processing

- **Anti-Phishing Protection**
  - **Link Protect** – When enabled, automatically rewrites any URL in an email message to a safe Barracuda URL, and then delivers the message. If the user then clicks on that URL, the service evaluates it for validity and reputation. If the domain is determined to be valid, the user is then directed to that website. This feature protects users who click URLs in email messages from being directed to a spoofed website or otherwise revealing private information such as logins, passwords or other sensitive data. **Note:** Link Protect does not properly protect URLs in plain text messages which lack a character set identifier. See also Anti-Fraud and Anti-Phishing Protection.
  - **Typosquatting Protection** – Automatically corrects spelling of domain names that hackers miss-spell by one letter to fool the user into thinking they are visiting a valid site by clicking the URL in an email. In reality, the domain name, misspelled, would direct the user to a phishing site. For example, **bankofanerica.com** would be re-spelled correctly by the service as **bankofamerica.com** before the email is delivered to the user to protect them from being directed to a suspicious site.
- **Anti-Fraud Intelligence** and **Intent Domain Policies** settings have been moved to the **INBOUND SETTINGS > Anti-Phishing** page.
- Miscellaneous improvements and bug fixes.
- Documentation updates.

What's New in Version 2.8.8

- **Advanced Threat Detection** (**ATD**) – The Barracuda Email Security Service now provides access to the subscription-based ATD service. This service analyzes inbound email attachments in a separate, secured cloud environment to detect new threats and determine whether to block such messages. See Understanding Advanced Threat Protection for details.
- Spam accuracy improvements.

What's New in Version 2.8.7

- Stability improvements.
- Web interface improvements.

What's New in Version 2.8.6

- Web interface improvements and fixes.

What's New in Version 2.8.5

- Stability improvements.
- Web interface improvements.

Fixed in Version 2.8.5

- Adding users with an underscore "_" in the email address and other special symbols works as expected. (BNESS-4016)

What's New in Version 2.8.4

- Stability improvements.

What's New in Version 2.8.3

- Improved Dashboard performance. (BNESS-3885)
- Improved handling of message rejection in Outbound Quarantine. (BNESS-3889)

Fixed in Version 2.8.1

- Messages are now deferred if either the virus scanner or Cloudscan are unavailable. (BNESS-3660)

What's New in Version 2.8.0

Web Interface

- **New Dashboard Page Layout and Features**
  - **Threat Origins** indicates the geographical region where blocked emails originate.
  - **Top Recipient Domains** shows the volume of email received by, and average number of recipients for, each domain.
  - **Traffic Status** lets the user know when the last messages were received and delivered.
  - **Subscription** details shows when the subscription expires.
  - **Inbound Email Statistics** shows various statistics about incoming emails.
  - **Outbound Email Statistics** shows various statistics about outgoing emails.
  - **Inbound Top Recipients** shows information about the most common recipients.
  - **Outbound Top Senders** shows information about the the most common senders.

Documentation

- Updated domain LDAP documentation.

Mail Processing

- Mail sent to a child domain that is not managed by the Barracuda Email Security Service will be delivered to the parent domain if it is managed by the Barracuda Email Security Service.
  - As noted, if you send outbound mail through the Barracuda Email Security Service, mail sent to a child domain will be returned to the parent domain mail server. To deliver mail to the child domain MX record, contact Barracuda Networks Technical Support to change the default settings to allow this for your domain.

Spam Accuracy

- Added support for Microsoft Access files in attachment filters.
- Added support for archived Microsoft Office files to attachment filters.
- Added support for archived PDF files to attachment filters.
- Envelope senders with spoofed postmaster address will now be blocked.

Fixed in Version 2.8.0

- Fix for rare occurrences of “duplicate serial” when transferring serials to new accounts. (BNESS-3676)
- Account expiration warning notices now include account information. (BNESS-3449)

What's New in Version 2.7.2

Web Interface

- Scalability and performance improvements:
- Improved web server response time. (BNESS-3491)

Spam Accuracy

- Scalability and performance improvements:
- Improved spam accuracy. (BNESS-3320)

What's New in Version 2.7.1

Web Interface

- 'Empty message' text for tables with the ability to add inline will no longer be displayed. (BNESS-3440)
- Reports can now be exported to CSV format. (BNESS-2779)
- Messages delivered through the Message Log are now marked as **UI Delivered**. (BNESS-3479)
- Headers of messages contain a virus display. (BNES-2739)

Spam Accuracy

- Ability to use Domain Key Identified Mail (DKIM) for inbound spam blocking. (BNESS-3419, BNESS-3420, BNESS-3426)

Fixed in Version 2.7.1

Web Interface

- Removed **Subject** tag from **Email Categorization** setting table. (BNESS-3407)
- Minor behavioral changes to Message / Quarantine logs. (BNESS-3400, BNESS-3357, BNESS-3270)

Spam Accuracy

- Improvements on inherited policy settings. (BNESS-3405)
- General Spam Accuracy improvements. (BNESS-3346)

What's New in Version 2.7.0

Web Interface

- You can click the **Add** link to add records 'in line' from within tables throughout the web

interface. (BNESS-3392)
- Tables can now be sorted by some or all data columns throughout the web interface. (BNESS-3397)
- New **INBOUND SETTINGS > Sender Authentication** page. On this page you can configure Sender Policy Framework (previously configured on the **INBOUND SETTINGS > Anti-Spam/Antivirus** page).

Spam Accuracy

- Option to block on missing PTR Records, configured on the **INBOUND SETTINGS > Sender Authentication** page. (BNESS-3383)

Fixed in Version 2.7.0

Message Log

- The **Saved Searches** window now shows all saved searches. (BNESS-2890)

Web Interface

- Layout improvements for tables. (BNESS-3393, BNESS-3394)
- The primary tab will now remain highlighted after a refresh/reload. (BNESS-3164)
- The **USERS > Users List** page now has a **Next Page** link at the bottom of the page. (BNESS-3349)

What's New in Version 2.6.2

Web Interface

- Moved location of **Save** and **Cancel** buttons in web interface. (BNESS-3307)
- Replaced **Help** link with a 'question mark' icon **?** next to the page title to click for a help pop-up window.

Message Log

- Added support for "size_lt:" (message size less than <size in bytes>) search. (BNESS-1261)

Fixed in Version 2.6.2

- Improved accuracy of "size_gt:" (message size greater than) search. (BNESS-3277)
- Searching users in linked accounts in Users list works as expected. (BNESS-3329)
- Browser-specific improvements in rendering web interface. (BNESS-3278, BNESS-3279)
- Improved Spam Accuracy. (BNESS-3167)

What's New in Version 2.6.1

Message Processing

- Improved efficiency of Multilevel-Intent. (BNESS-3081)

Web Interface

- Updated the web interface styling for improved look and feel, consistency.
- Improved Self-Service setup wizard. (BNESS-3150)
- Improved LDAP efficiency for authentication. (BNESS-3149)

Fixed in Version 2.6.1

- Improved handling of users' policies (See **USERS > Default Policy**). (BNESS-2386)

What's New in Version 2.6.0

Message Processing

- Rate Control for inbound mail. This feature protects your mail server from spammers or spam-programs (also known as "spam-bots") that send large amounts of email to the server in a small amount of time. See the **INBOUND SETTINGS > Rate Control** page to configure.

Web Interface

- Updated the web interface styling for improved look and feel. There are no navigation changes.
- Added support for domain verification via CNAME records or via the technical contact from the WHOIS database. See the **DOMAINS** page or How to Validate Your Domain.
- Added support for domain verification via the technical contact from the WHOIS database in the Barracuda Email Security Service Setup wizard.

Fixed in Version 2.6.0

- On the **OUTBOUND SETTINGS > Notifications** page, the **Quarantine Sender Notification** default setting is **No**. (BNESS-3043)
- If the admin tries to reject a message in the **OUTBOUND QUARANTINE**, but has not already filled in the **Reject Notification Address** field on the **OUTBOUND SETTINGS > Notifications** page, the error message now provides a link for the admin to click to enter that email address (BNESS-3043)

What's New in Version 2.5.4

Quarantine

- Outbound quarantine support enables administrators to quarantine outbound messages based on policy - see the **OUTBOUND SETTINGS > Content Policies** page to configure.
- Quarantined messages are moved to an inbox, on the **OUTBOUND QUARANTINE** page, where the administrator can export, deliver, reject and delete messages in the list. Notification summary emails for quarantined messages can be sent to the administrator immediately, or on a daily or weekly basis. See the **OUTBOUND SETTINGS > Notifications** page to configure.
- Quarantine notifications to senders of outbound quarantined messages can be enabled by the administrator to indicate that the message has not been delivered, and awaits evaluation by the administrator.
- An NDR (non-delivery report) will be sent to senders of quarantined outbound messages that are rejected by the administrator. See the **OUTBOUND SETTINGS > Notifications** page to configure.

Web Interface

- With the Barracuda Express Setup, new Barracuda Email Security Service accounts have an updated setup wizard that includes Office 365 configuration.

Fixed in Version in 2.5.4

- Improved message processing. (BNESS-2785)

What's New in Version 2.5.3

Mail Processing

- Added support for Perfect Forward Secrecy. (BNESS-2871)
- "Domain Not Found" response now includes IP address. (BNESS-2817)
- Improved recipient verification. (BNESS-2785)

Spam Accuracy

- Improved outbound multi-level policy processing. (BNESS-2851)
- Apply email chain exemptions to bulk email. (BNESS-2869)

Documentation

- Enhanced documentation regarding encryption for domain settings and for CloudScan settings.

Fixed in Version 2.5.3

Mail Processing

- Ability to 'pass through' known cloud archivers for outbound traffic. (BNESS-2865)
- Improved check for adding outbound IP addresses. (BNESS-2765)

Message Log

- The **Whitelist ALL** function works as expected on the Quarantined Delivered page. (BNESS-2807)

Web Interface

- The Domain pull-down menu now only displays when necessary. (BNESS-2766)
- Improved domain-level access control. (BNESS-2810, BNESS-2527)
- Increased limits on access to messages that were sent to the Barracuda Message Center (Encryption Service). (BNESS-2792)
- General web interface improvements. (BNESS-2435)
- Fixed rare cases in which some messages were not always listed in the user Quarantine. (BNESS-2864)

What's New in Version 2.5.2

Spam Accuracy

- New cloud-based spam scanning engine, CloudScan, which leverages many of the spam scanning and detection techniques currently available on the Barracuda Spam Firewall appliance, including spam scoring.
- Improved ability to handle long email discussions. (BNESS-2754)
- Improved response times to TLS setting changes. (BNESS-2683)
- Improved handling of URL redirects. (BNESS-2381)
- Improved handling of MX record lookups. (BNESS-2388)
- Additional SPF information added to message headers. (BNESS-2711)

Message Log

- System-wide sender block policies as put into place by Barracuda are now identified as "System Sender Policies", to distinguish them from sender block policies as configured by administrators. (BNESS-2773)
- Ability to submit categorization requests for previously uncategorized messages. (BNESS-2737)
- Multiple improvements to the Message Log, including to its display and filtering capabilities. (BNESS-847, BNESS-1033, BNESS-2193, BNESS-2340, BNESS-2577, BNESS-2641, BNESS-2692, BNESS-2721)

Web Interface

- Ability to limit synchronization of primary and linked addresses to the current domain. Takes effect starting after the new option on the Directory Services section of the **DOMAINS > Domain Manager > Settings** page is selected. (BNESS-1798)
- Ability for administrators to initiate password resets for their users. (BNESS-935)
- Multiple improvements to the web interface, including to the handling of entries on the Filters page. (BNESS-990, BNESS-1919, BNESS-2104, BNESS-2394, BNESS-2704, BNESS-2718, BNESS-2720, BNESS-2724, BNESS-2726, BNESS-2733, BNESS-2742, BNESS-2770)

Fixed in Version 2.5.2

- Bulk deletion of users works as expected. (BNESS-2735)
- Repaired report generation. (BNESS-2675)

What's New in Version 2.5.1

Mail Processing

- *Received* headers now include TLS information, when appropriate.
- More detail provided for outbound message log entries when inbound side (Barracuda Email Security Service customer) blocks messages based on a DNSBL/RBL.

Web Interface

- Improved Barracuda Message Center user experience.
- New outbound attachment type / extension filter.
- New **Whitelist** option in users' quarantine confirmation screen.

Fixed in Version 2.5.1

Mail Processing

- Improved handling of duplicate emails. (BNESS-2673)
- Improved handling of HTTP queries during intent checks. (BNESS-2681)
- Fixed bug in handling of bulkmail setting. (BNESS-2682)

Spam Accuracy

- Allow content blocks to override defer actions found earlier in intent. (BNESS-2699)
- Improved spam-accuracy around content intent. (BNESS-2700)
- Continue to look for multilevel intent block action even if there is already a **Defer** action for the message. (BNESS-2701)

User Management

- Correctly display default quarantine notification interval for users. (BNESS-1836)
- Ensure deleting linked users when deleting primary user email addresses. (BNESS-1858)
- Prevent creation of users that conflict with existing linked users. (BNESS-2657)

Web Interface

- The **Check Archives** option works as expected for Inbound Attachment filter. (BNESS-1329)
- Avoid local cache for certain web interface checks of customer DNS. (BNESS-2484)
- Improved user/administrator session handling. (BNESS-2641, BNESS-2702)
- Correct wording in Email Categories web interface elements on the **INBOUND SETTINGS > Anti-spam/Antivirus** page. (BNESS-2690)

Message Log

- Improved message rendering. (BNESS-2558, BNESS-2697)
- Improved message log search function. (BNESS-2577)
- Improved Saved Searches function. (BNESS-2644)

Miscellaneous

- More robust DNS queries. (BNESS-2569)

What's New in Version 2.5

Mail Processing

- **Email Categorization**. This feature gives administrators an additional way to decide what to do with various types of emails from senders on the Barracuda Reputation Whitelist. These emails are separated into different categories such as Transactional Emails, Corporate Emails, and Marketing Materials, each of which can have a different delivery action associated with it from the **INBOUND SETTINGS > Anti-spam/Antivirus** page. See Barracuda Reputation and Email Categorization for more details.
- **Sender Policy Framework (SPF) Exemptions**. You can exempt trusted/known IP addresses from SPF checks by clicking **Add Exemption** and adding the IP address(es) and associated netmask(s) to the table. Mail from these IP addresses will still be scanned for spam.
- Optional user notification when that user's password is changed by an account or domain admin.
- Saved searches now indicate the search type (inbound, outbound)

Fixed in Version 2.5

Mail Processing

- Ability to block a message from the Message Details view. (BNESS-611)
- Ability to exempt IP addresses from SPF checking. (BNESS-2442)
- LDAP test now takes user filter into consideration. (BNESS-2618)
- Improvements to the **Request IP Exemption** feature on the **OUTBOUND SETTINGS > Abuse Monitor** page. (BNESS-1317)

Domain Management

- When a domain admin manages multiple domains, the **Settings** page shows correct information for each domain. (BNESS-2634)
- Domain admins that add a new domain are automatically granted management permissions for that domain. (BNESS-1188)

Message Delivery

- Encrypted messages now display only the message headers when viewed from the Message Log and when downloaded. (BNESS-720)
- Redelivery for encrypted messages is now disabled. (BNESS-2076)
- Delivering from a user's quarantine delivers to only that recipient. (BNESS-2589)
- Avoid redelivery of empty messages. (BNESS-2431)
- Now blocking mail with no subject and no body. (BNESS-2626)
- Improved detection of HTTPS URLs in multi-level intent checking. (BNESS-2632)
- Messages blocked due to recipient verification are now logged with action 'Blocked' and reason 'Invalid Recipient'. (BNESS-2645)

Miscellaneous

- Find (and use) primary account if user logs in with linked account (BNESS-2637)

What's New in Version 2.4.2

Web Interface

- Improved validation of entered data, including for incorrectly-formatted domains and other entries made via bulk edit. (BNESS-943, BNESS-2188, BNESS-2500)
- The **USERS > User List** page now includes the total number of users, displayed in **Results** number above the users list. (BNESS-1028)
- Statistics for messages classified as Bulk Email are now included in the **Emails Processed by Action** section of the **BASIC > Status** page. (BNESS-2509)
- The Domain level **Status** page now only displays the information relevant to that domain. (BNESS-1086)
- The **User** column on the **INBOUND SETTINGS > Sender Policies** page has been renamed to **Sender**. (BNESS-1424)

- Added **Quarantine Status** column to **USERS > Users List** page for account and domain admins, indicating whether or not each user in the list receives a quarantine digest (e.g. the Quarantine Notification Interval for the user is either Daily, Weekly, Custom or Never). (BNESS-1887)
- The **Sender Policy** time stamp now reflects the Last Modified Time of that entry. (BNESS-2161)
- The version number at the bottom of the status page now links to this Release Notes page. (BNESS-1869)

Message Log

- Added a **Reason** column to the **Message Log** that indicates why a message had the listed action taken with it. (BNESS-2232)
- A link for each domain within the Top Domains by Volume (30 days) report on the **BASIC > Status** page now leads to a 30-day Message Log search. (BNESS-856)
- Expanded contents of Exported Logs. (BNESS-1266)
- Quarantined items now show as yellow in the **Action** column. (BNESS-1760)

Fixed in Version 2.4.2

- Improvements to multilevel intent analysis (BNESS-2533, BNESS-2573)
- Improved LDAP synchronization of user lists (BNESS-2563)
- Improved delivery of New User Welcome Emails.
- Improved scanning of extracted content. (BNESS-2344)
- Restored ability for all users to specify their own Quarantine Notification interval. (BNESS-2574)
- Encryption honored on explicitly allowed messages. (BNESS-2462)
- Addressed rare situation where mail was sent to a domain's A record entry. (BNESS-2572)
- Corrected display of special characters like **%** and **+** in recipient addresses in the **Message Log**. (BNESS-2106)

Security

- Resolved the following vulnerabilities:
- High severity: Unauthenticated; remotely exploitable; account takeover; brute force [BNSEC-3196 / BNESS-2541)
- Medium severity: Cross-site request forgery (CSRF) [BNSEC-2339 / BNESS-2480, BNESS-2542)

What's New in Version 2.4.1

Mail Processing

- Trusted Forwarders. Ability to specify one or more IP addresses of machines that you have set up to forward email (i.e. Trusted Forwarders) to the Barracuda Email Security Service from outside sources. The Barracuda Email Security Service exempts any IP address in this list from Rate Control, SPF checks and IP Reputation. In the Received headers, the Barracuda Email Security Service will continue looking beyond a Trusted Forwarder IP address until it encounters

the first non-trusted IP address. At this point, Rate Control, SPF checks and IP Reputation checks will be applied. Configure on the **INBOUND SETTINGS > IP Address Policies** page.
- Sender Policy Framework (SPF) blocking options. When enabling SPF, you must specify one of two options:
  - **BLOCK FAIL** - The SPF FAIL (also referred to as Hard Fail) response indicates that the IP address of the message sender does not match the IP address or range of IP addresses specified in the sending domain name's SPF record, and that the real owner of the domain has specifically indicated that such messages should be rejected (blocked) as spoofed.
  - **BLOCK FAIL, SOFTFAIL** - The SPF SOFTFAIL response indicates that the message sender's IP address does not match the IP address or range of IP addresses specified in the sending domain name's SPF record. A SOFTFAIL means that the domain owner did not specify how such messages should be handled. Selecting this option means that messages in either the SPF SOFTFAIL or FAIL state are blocked.
- Improved recipient verification process.
- Improved spam accuracy.

Web Interface

- The **Blocked** action in the **Emails processed by action** section of the **STATUS** page now includes the **Bulk** reason.

Message Log

- The **Date** field is now included in the Message Log export file.
- Improved message search performance for related domains.

Miscellaneous

- Extended medical dictionary (HIPAA) for Predefined Filters (see the **OUTBOUND SETTINGS > Content Policies** page).

Fixed in Version 2.4.1

- When the sender and recipient domain are both protected by the Barracuda Email Security Service, a blocked message from/to the same domain shows the Reason for the block *only* in the inbound Message Log. (BNESS-2348)
- On the **DOMAINS > Settings** page, clicking the **Synchronize Now** button does not product an error message if the synchronization with the specified LDAP server is successful. (BNESS-1812)

What's New in Version 2.4.0

- **Dynamic Bulk Email Detection**. Enables taking action with messages that contain anything that looks like unsubscribe links or unsubscribe instructions in the message body. Configurable on the **INBOUND SETTINGS > Anti-Spam/Antivirus** page.

- Option to create exemptions for predefined filters. See the **OUTBOUND SETTINGS > Content Policies** page.
- Ability to scan more attachment types.

Message Log

- Added time/date as a filter in Message Log. (BNESS-2407, BNESS-2445)
- Adjusted Action **Reasons** for increased clarity and consistency, as displayed in Message View details in the Message Log. (BNESS-2185, BNESS-2297)
- Improved rendering of messages, including those with absent or malformed content. (BNESS-2414, BNESS-2446)
- Downloaded messages now include X-BESS-* headers. (BNESS-2420)
- Improved search performance in the Message Log. (BNESS-2449)

Spam Accuracy

- Improved detection of suspect URLs in message body. (BNESS-2443)
- Improved interaction between Trusted Forwarder and Sender Policy Framework (SPF). (BNESS-2459)

What's New in Version 2.3.5

Mail Processing

- All messages going through the Barracuda Email Security Service will now be subject to a size limit of 300MB. (BNESS-1082)
- Enhancements to spam detection, including improved URL scanning and handling of embedded URLs.
- Improved support for customer domains that rely on suspect nameservers. (BNESS-2419)
- Improved handling of emails sent to multiple recipients of different suspect domains. (BNESS-2426)
- Improved outbound TLS functionality. (BNESS-2428)

Search

- Ability to search through MIME-encoded From, To, Subject header fields (only for messages received using version 2.3.5 and later). (BNESS-2370)

Administration

- Confirmation now required when deleting users. (BNESS-2400)
- "451 possible mail loop" events are now logged. (BNESS-2311)

Web Interface

- Improved performance when displaying information for accounts with a large number of emails. (BNESS-2415)
- Improved display of messages encoded in UTF-8. (BNESS-2418)
- Filtering for aliases (on the **USERS > Users List** page) is no longer case sensitive. (BNESS-2434)

Fixed in Version 2.3.5

- Handling of emails with lines greater than 990 characters. (BNESS-2187)
- Whitelist function in the Users' Message Log. (BNESS-2408)

What's New in Version 2.3.4

Improved Spam Accuracy

- Enhanced the algorithms for detecting spams in attachments, multi-level intent, and URL detection.

LDAP Support Enhancements

- New **User Filter** setting in the **Directory Services** section of **DOMAINS > Domain Settings** page. This allows the administrator to better manage which accounts should be synced with the LDAP server.

Administration

- Ability to disable notifications when adding aliases (linked addresses) to user accounts. (BNESS-2308)

Miscellaneous

- Support for using CNAMEs in PTR records. IP addresses that resolve to a CNAME record can now be used as an outbound IP address, avoiding lack of Reverse DNS errors. (BNESS-2294)

Fixed in Version 2.3.4

Enhancements

- Message Log
  - Improved layout for usability. (BNESS-2306)
  - Updated the **Reason** filters. (BNESS-1244)
- Various documentation updates. (BNESS-2323, BNESS-2322, BNESS-1005)
- Improved font size consistency in Quarantine Notifications. (BNESS-2325)
- Improved deferral deduplication with multi-recipient messages. (BNESS-2355)

What's New in Version 2.3.3

Message Log

- Long domain or email address entries do not run into the **Policy** column. (BNESS-1009)
- The Message Log properly displays large HTML-rich messages. (BNESS-2279)
- The **Saved Searches** section has been moved to the right of **Advanced Filters**. (BNESS-2270)
- Improved search performance. (BNESS-946)

Improved description of multilevel/intent action reasons

- URL blocking for Multi-Level Intent is correctly reported. (BNESS-2295)

Quarantine Notifications

- Improved rendering of non-English text in Subject and From fields.
- Quarantine Notifications render character encodings as expected. (BNESS-1036), (BNESS-1767)

Fixed in Version 2.3.3

Enhancements

- Length of domain names is now limited. (BNESS-1126)
- When a domain administrator adds a new domain, it is immediately visible in the domain administrator's view. (BNESS-1188)

Fixes:

- Count for graph **Emails processed in the last 30 days** no longer repeat when the range is 0k - 3k. (BNESS-1026)
- Email notification to alias (Linked) address is no longer blocked when *UnManaged Users* are set to BLOCK. (BNESS-1098)
- One alias email address cannot be linked to multiple BESS users. (BNESS-2194)
- The **Return to Previous Page** link in the Printable View works as expected. (BNESS-2272)
- Destination server priority defaults to the current priority instead of *10*. (BNESS-2293)
- Selecting (No Content) messages and clicking the **SPAM** button works as expected. (BNESS-2296)
- Clicking the **SPAM** button for a selected message does not show the message as *Delivered* in the Message Log. (BNESS-2305)
- Trying to deliver a blocked message changes the **Delivery Status** in the Message Log list and in the Message Details page as expected. (BNESS-2315)
- Immediate notification in web interface if an IP address the admin enters is on the BRBL. (BNESS-2206)
- Message Content Filter matching attachments works as expected for PDFs. (BNESS-2115)
- Predefined Filtering blocks PDF attachments containing a valid credit card number, as expected.

(BNESS-2170)
- LDAP syncing of user names works as expected, preventing incorrect blocking of legitimate users when *UnManaged Users* is set to BLOCK. (BNESS-2286)
- When a message includes a domain which indicates suspicious intent, then Multi-Level Intent correctly defers the message instead of blocking it. (BNESS-2300)
- The IP address owner is correctly identified when applying outbound rate control. (BNESS-2317)

What's New in Version 2.3.2

- Enhancements to the Message Log functionality including:
  - Sender's email address is now displayed in the **From** column instead of display name. (BNESS-2212)
  - Resizable columns. (BNESS-1825)
  - Message preview pane, which can be configured for location on the screen or can be turned off.
  - Double clicking on a message now opens a new web page.
- Ability to edit Mail Server configuration. (BNESS-1856)
- Ability to define action (*Defer, Block, Quarantine*, or *No Action*) on Multi-Level Intent scanning from the **INBOUND SETTINGS > Anti-Spam/Antivirus** page. (BNESS-2247)
- Ability to print Message Log & Help screens. (BNESS-2251)
- Support for multiple Barracuda Cloud Control accounts. (BNESS-2264)

Fixed in Version 2.3.2

- Ensure duplicate entries are not being created (BNESS-987) E
- Email addresses that have underscores work as expected. (BNESS-2216)
- Ensure rate control is applied even to trusted forwarders. (BNESS-2215)
- PTR records are cached correctly. (BNESS-2143)