

Libraesva EA v22.8: Release Notes

Changes in EA v22.8

Main Features

- Security bundle: urlsand integration

The Libraesva Email Archiver can now integrate with the Urlsand protection. This engine actively blocks malicious email URLs to protect against spear-phishing attacks, zero-day exploits and ransomware. This protection is available both when using the Archiver from browser or from the Outlook plugin. When running an export, the admin can choose whether to rewrite all the links to take advantage of the Urlsand protection. This integration requires the security bundle to be included in the base license and can be enabled tenant-based.

- Security bundle: antivirus support

The Archiver now supports three antivirus engines: Avira, Clamav and BitDefender. When consulting emails, it's possible to enable antivirus scan to protect users from infected attachment. If an antivirus engine detects an infected file, the Archiver prevents the user from downloading the attachment and forwarding or downloading the email. The user can optionally be allowed to perform these operation even if an antivirus detects something. The antivirus scan is available also when exporting emails from the Archiver. You can choose tenant-based which antiviruses to enable. The Antivirus protection requires the security bundle to be included in the base license. Avira and BitDefender are available with the per-mailbox license only, while Clamav is always available.

- E-Discovery

With the E-Discovery rules you can actively check for new specific emails coming to the Archiver. When configuring an E-Discovery rule you can select a saved search, in order to define the emails you are looking for, a frequency, according to which sending scheduled E-Discovery report and a list of email addresses to which sending the report to.

- Full SMTP Google Workspace Journaling support

The Libraesva Email Archiver now supports the native Google SMTP Journaling. There's no need to configure an hoc IMAP journaling mailbox anymore.

- Group and filter options to Google Workspace configuration

When configuring a Google directory service for fetching users it's now possible to define a group (which can be a group's email address, a group alias or an unique group ID) or some Google filtering to be applied when fetching users.

- Archived emails protocol number
The Libraesva Email Archiver assigns to each archived email a protocol number, which is an unique identifier of each archived emails. This protocol number is unique and immutable, so you can uniquely identify each email on your the Archiver by using it. The protocol number automatically applies to already archived emails, too.
- Directory service historical users
The Libraesva Email Archiver automatically records the details of the users coming from all directory service. This allows to keep track of the details of all the users ever archived on the Archiver (starting from the release 22.8 update day) and to setup Microsoft 365 delegation with historical and dismissed users, too.

Features

- Multiple words filter
When using the advances search, it's now possible to filter by multiple words
- Greater and lower than
When searching emails, it's possible to add a filter on the email size, to be greater or lower than a certain value.
- Syslog
The Archiver now supports the Syslog integration. You can configure it by inserting syslog server IP, port and protocol.
- User filter
When running a search, you can use an additional filter to match only the emails belonging to a particular user.
- Add OID for license info/usage
Some new OIDs are available to get information about license limits and license usage. You can find the detailed list of all available OIDs on the online documentation.
- Allow to clone saved search
Saved searches can now be cloned in order to create a copy which can be further modified.
- User folders report
A new report is now available. With the folders report you can list for each users (in a

tenant) the count of its folders.

- Check for IMAP and PEC single users credentials
The Libraesva Email Archiver periodically checks for credentials validity about connectors. IMAP and PEC single users credentials are now periodically checked, too.
- Export by folder
When exporting emails from the Archiver, it's now possible to export emails belonging to a specific folder of a specific user.
- MSP license overuse For the Archiver running with a MSP license, the Archiver allows to exceed license limit for 30 days. If the overuse lasts for more than a month, the archiving process is suspended.
- Extended Backup When configuring appliance backup, you can choose among single or extended backup. Simple backup is useful to backup the appliance configuration. Extended backup includes also information about users folder structure and a few emails meta-data.
- Connector report schedule
The connector report can be scheduled to retrieve data about the latest n days.
- Sessions page
In this new page the administrator can monitor all the active sessions on the appliance and possibly invalidate some of them.
- Multi-tenant report
This new report is particularly useful for MSP appliance. The reports contains aggregated information for each customer on the appliance.
- 365 Shared-mailbox import
The Graph connector can now synchronize 365 shared mailboxes even when they do not have an active license on 365.
- Google Workspace calendar
The Archiver can now deal with Google calendars and shared documents email notifications. The Archiver detects this type of emails and archives them.
- Allow to clean user synchronization status by connector

The user synchronization status for a specific connector can now be reset in order to collect information from scratch.

- Mailbox license overuse

For the Archiver running with a mailbox-based license, the Archiver allows to exceed license limit for 30 days. If the overuse lasts for more than a month, the archiving process is suspended.

- PST of journaling mails

The Archiver does now support the import of PST containing journaling emails. When running the import you have just to use a specific option for this type of archive.

- Contains words feature

When searching emails, this new filter type is available. You can provide a set of words and search for emails containing at least one of this words.

- Increase PEC connector frequency

The PEC connector synchronization, which was running hourly, is now launched every 30 minutes.

- Monitor listener and connector inactivity through SNMP

Some new OIDs are available to monitor listener and connector inactivity. You can find the detailed list of all available OIDs on the online documentation.

Bugfix

- Fixed expired legal hold rules shown as active

- Fixed multiple login buttons appearing when multiple directory services are configured

- Allow to assign super-admin role only for users with no tenant associated

- Fixed Archiver not importing emails with same message ID, folder within 24 hours

- Fixes PST logs not showing due to 500 errors

- Fixed URL too long when running a search

- Allow to authenticate local users only associated with active tenants

- Fixed IMAP importer skipping valid journaling emails when the attachment filename was missing

- Fixed duplicated folders
- Fixed volumes not readable for administrator users different than *admin*
- Fixed PST imports triggering out of memory
- Fixed archiving policies not working when saved with priority equal to 9999
- Fixed PEC connector not deleting emails from mailbox
- Fixed full-text search containing *null* word
- Fixed connector synchronization randomly crashing on zip upload

Improvements

- Folder alphabetical order on Outlook Addin
- Handle too big emails view on browser
- Add support to Wasabi volumes Object Locked
- Make users caching more resilient and prevent issues
- Forcing retention rules now requires OTP if configured
- Activate NTP by default on all appliances and make sure it's synchronized
- Show license overuse in dashboard card
- Show MFA indicator on users page
- Trigger high swap notification when swap usage is more than 75%
- Increase PST import processes timeout

How to update

The Libraesva Email Archiver will automatically send an email notification about this major release.

In the section *Settings > System > General*, the update could be scheduled for the next night or started immediately.

For the Archivers hosted in the Libraesva Cloud, please contact support@libraesva.com to get the Archiver updated.

LIBRAESVA
Email Archiver

Dashboard Search Archiver Settings Reports

Version and Updates SMTP Configuration SNMP Configuration

New major version available.

Main features:

- Antivirus support
- Urlsand integration
- E-Discovery
- Archived emails protocol number
- GSuite SMTP journaling and filtering on Google configuration
- Syslog support
- More search criteria

Update to new major version this night Update to new major version now

The indexing engine is updated!

Libraesva ESG v5.1: Release Notes

Main features of version 5.1

- Users with quarantine action "release-only" or "none" cannot manage white and black lists in the UI anymore
- Cluster: added replicate transport option for each domain (previously known as WAN cluster or Geo-Cluster option)
- Any trusted network defined by the administrator can be configured to accept only email originated by internal domains
- Outbound email traffic from Microsoft 365 and G Suite allows only email originated by internal domains (i.e. relay table)
- New administrative REST API (/api/v2), stateless, JSON/HAL based, with support for Impersonation and OTP
- Quarantine digest report: email addresses of other recipients are not listed for privacy protection

- More granular management of the privacy password to view sensitive data
- Message details now includes all URIs contained in the message and forensic data about them
- Show asynchronous job status and failures to administrator on the Web UI
- DMARC aggregated reporting can be enabled by the administrator
- Advanced Audit log which contains all the details of the modified data

Version 5.1.20 (Sep 16, 2025)

Security

- **Mail scanner:** fixed CVE-2025-59689
- **System upgrade:** new upgrade system with asymmetric signature validation and encryption
- **Passwordless:** removed old authentication systems (may need re-login)
- **API authentication:** removed old authentication systems (may need re-login)
- **Remote support:** removed the old remote support connection via port 25

Version 5.1.19 (Jul 31, 2024)

Security

- Bitdefender: update to version 3.7.1
- Savapi: update to version 4.15.22

Version 5.1.18 (Mar 5, 2024)

Security

- ClamAV: upgrade to version 0.103.11
- Bitdefender: update to version 3.5.5

- Savapi: update to version 4.15.20

Version 5.1.17 (Aug 29, 2023)

Security

- ClamAV: upgrade to version 0.103.10

Version 5.1.16 (Aug 21, 2023)

Security

- Quicksand: add RAR archive reconstruction on sanitization
- ClamAV: upgrade to version 0.103.9

Version 5.1.15 (Jun 27, 2023)

Improvements

- System Upgrade: show more details on failure

Bug fixes

- Microsoft 365: case insensitive username check on login

Version 5.1.14 (Apr 8, 2023)

Security

- Savapi: update to version 4.15.16
- Bitdefender: update to version 3.2.2

Improvements

- Learn Actions: always update Adaptive Trust Engine when learning as good or bad

Bug fixes

- SubmitToLabs: when submitting as bad, use learn-as-bad instead of forget
- Quarantine reports: allow actions from quarantine report for read-only admins with “mark for release” permissions
- ESG 5.2 upgrade: pre-install the upgrade file for user convenience

Version 5.1.13 (Apr 3, 2023)

Improvements

- Audit log: speed up logging during massive updates

Bug fixes

- Removed duplicated default/relay configuration
- Search: fixed export of search results when using advanced filters
- System Preferences: added validation of NTP server address
- Digest report: show links of configured actions for “Quarantine” users
- Report: fixed MTA Statistics report using advanced timing
- System Upgrade: keep local DNS resolved running during system upgrade

Version 5.1.12 (Mar 13, 2023)

Security

- QuickSand: block attachments in archive when unzip size is greater than 150MB

Improvements

- System Upgrade: require confirmation before upgrade

Bug fixes

- File System Replica: improved stability for “Large” appliances
- Message Viewer: hide Whitelist/Blacklist action for user with “Mark for Release” permission
- Smarthost: fixed migration of 4.9 configuration on address-based smarthost

API

- IMPROVED: `message-journal` reduced pagination to 150 records

Version 5.1.11 (Feb 21, 2023)

Security

- ClamAV: upgrade to version 0.103.8

Improvements

- TLS Certificate: validate certificate match with private key
- Fail2ban: ignore SASL auth failed from trusted networks
- ClamAV: increase timeout of signature update for slow connection

Bug fixes

- Backup: fix backup of TLS Certificates
- Database rotation: restore optimization of TxRep data
- Graymail Management: add validation on Blocked Graymail entries

- Top Sender Report: fix visualization of locally generated email
- Quarantine storage extension: fix GPT partition extension
- Search: fix “Last Hour” range to latest hour
- Report: increase timeout of PDF generation
- Message Details: fix popup of Dictionary rules triggered
- User Quarantine schedule: automatically order delivery and fixed duplicated hours

Version 5.1.10 (Jan 16, 2023)

Security

- Whaling Protection: verify SPF alignment before whaling checks

Improvements

- Check Firewall Ports: added detection of firewall inspection on http/https
- System Upgrade: implemented email notification after upgrade
- System Upgrade: improved check of upgrade pre-condition
- License Details: show contact email
- Dashboard: show all engines as “not active” when license is expired

Bug fixes

- Privacy Password: permit view for Read-Only Domain Admin
- Privacy Password: fixed UI regression of version 5.1.9
- Antispam action: fixed compile of High Spam forward rule
- RBL Filtering: re-activated RBL check flagged as enabled
- System notification: use absolute URL for generated email
- Database Rotation: fixed cleanup of old Message Uris
- Message details: show meaningful messages in pop-up when there are no results

- Mail log: properly log to database messages with more than 300 blocked files
- Search: fixed condition for all fields with value Yes/No

Version 5.1.9 (Dec 20, 2022)

Improvements

- Dashboard Cluster status checks both nodes
- FTP Backup: less disk space required before FTP upload
- FTP Backup: execute on both nodes of cluster
- Updated DDoS default limit for connection and message rate
- DMARC: changed reporting organization to appliance hostname

Bug fixes

- Quicksand: fixed sanitization of nested archives
- Cluster: fixed option “replicate transport” for some instances
- Cluster: fixed notification of file replica down
- Message Details: show correct DKIM information when domain use mixed case sensitivity
- MTA Certificate: correctly apply fallback self-signed certificates
- FTP Backup: check disk space before execution
- Web UI: custom pagination detail when there are no records
- Microsoft Azure: add agent server IP to trusted IPs in firewall configuration
- Microsoft Azure: changed keepalive settings to avoid stale support connections
- Privacy Password: hide spurious read-only records from Domain Admin view
- ESG4 migration: correctly configure CRM114 permission
- ESG4 migration: check let's encrypt configuration before migrate

API

- ADD: added validation and other options to `/relay`
- FIXED: avoid 500 error on `/relay` updates due to auditing issues of impersonated users
- FIXED: avoid 500 error on `/integration/imap` and `/integration/pop3` updates due to digest report options
- IMPROVED: increased allowed memory and timeout for `GET /messages/message-soar`

Version 5.1.8 (Nov 14, 2022)

Improvements

- Firewall check: only use local resolver for outbound DNS port test (53)
- User console: improved storage speed test
- ISP Panel: add accounted email addresses count
- License Usage: add more fields to exported data
- Login auth test: show logs from all user providers (M365, IMAP, ...)
- Cluster auto-recover: added new auto-recover scenarios
- Integrations: when import is triggered from the UI, forward the request to the primary node
- Message details: contextualize WebUI notice for ignored whitelist entries
- OpenDMARC: don't replicate data between node so that reports are appliance based.
- RSyslog: increase rate limit to 2048 to accommodate large appliance
- Cluster: add the replica node to trusted IPs by default
- Add support for Enterprise Linux 8.7

Bug fixes

- Summary Report: date interval extremes are now included in date range
- Improve reliability of watchdog scripts notifications
- Microsoft 365 auth: catch server errors when the connector is badly configured

- ESG4 migration: correctly migrate disabled antivirus customizations
- firewall: maintain netfiltering rules during cluster setup
- Fix audit message on TLS certificate deletion
- Use correct DN on user import
- Backup: added SMTP Auth users to archive
- Antispam settings: fix saving of high spam score
- Fail2ban: recover logging to rsyslog (as it was in ESG 4.x)

API

- FIX: allow creation of relay based entities (regression from 5.1.4 fixed)

Version 5.1.7 (Oct 17, 2022)

Security

- Improves RBL detection sub-domains below 3rd level
- Quicksand: improves www-links detection in PDF
- Update Bitdefender license
- Relay: bounce messages sent by M365/G Suite are considered trusted (when the relative option is enabled)

Improvement

- Whaling: improved performance of domain selection during scanning
- Cluster auto-recovery: reduce timer interval to recover minor error faster
- System upgrades: show estimate time in advance and use animated progress bars when upgrade is active
- HA Proxy: locally generated email are sent directly, not through the proxy

Bug fixes

- Outlook add-in: remove reference to a deprecated API call
- User Manager: add JS validation for empty username on creation
- User Manager: on user removal, cleanup job statuses owned by that user
- UI: remove the about link which conflict with white labeling
- Improved trial license upload
- Passwordless: remove Libraesva from signature when white labeling is enabled

API

- IMPROVED: added user `_permissions` property to message details
- IMPROVED: allow domain admins to access `/api/v2` documentation page
- FIX: add headers content-type x-requested-with to CORS headers

Changes in v5.1.6 (Oct 3, 2022)

Improvements

- ESG 4.x migration: prevent timeout and memory exhaust on historical data restore

Bug fixes

- System Definitions: fixed automatic update of blacklisted URL hashes
- Release requests: fixed Domain Admin notification of release requests
- License Usage: fixed display of accounted license
- Login Authorized Networks: properly check login network on current IP before save or modify it

API

- FIXED: properly apply page size on GET /message API

Changes in v5.1.5 (Sep 20, 2022)

Improvements

- Report: show more data in reports and improve accuracy
- Logwatch: reduce noise due to irrelevant log entries
- Web UI: menu is collapsible from mobile device

Bug fixes

- Message listing: shows to users email sent from restricted trusted network
- Message logging: logs URI/attachment with very long names
- Message details: fixed negative delay time due to timezone conversions
- Summary report: count as outgoing email sent from restricted trusted network
- OpenDKIM: always add restricted trusted networks as source for OpenDKIM signatures
- Release requests: show disabled form settings to read-only users
- Release requests: fixed selection of domain admins for a domain
- Backup: hide non-working edit buttons to read-only admins
- Backup: increase timeout for TAR command
- Whitelist: allow creation of whitelist to SafeLearn network

API

- NEW: added /report/{name} methods to query historical data (e.g. license usage /report/per_domain_mailbox_use?search=all)
- IMPROVED: collections GET /messages order data by received date
- IMPROVED: empty response from POST /user-message return 204 instead of 200

Changes in v5.1.4 (Sep 05, 2022)

Security

- Add CSRF protection to all user quarantine actions
- Message forwarding requires privacy password authorization
- Extended quarantine links validity to 31 days

Improvement

- Dashboard: add filtering by “last hour” and “last 3 hours”
- Rejected message: show more message details
- Search export: added many fields and fixed recipient numbering
- Cluster auto-recovery: added notification when the procedure fails to auto-recover
- Cluster: improved the auto-recovery procedure when an appliance is powered off for a very long time
- Safe-learn web UI: describes advantages and drawback of the feature
- Add forward compatibility for Clamd configuration of ESG > 5.1
- System upgrades: show estimate time in advance and use animated progress bars when upgrade is active
- API user: use automatic password generation to enforce strong password policy

Bug fixes

- Backup: restored manual backup creation which was failed due to a missing table
- License settings: cleanup license no longer generates memory errors
- License settings: restore searching by email address
- M365/G suite: resolved a race condition which may interfere with cluster replication
- Data Loss Prevention: resolved the 503 caused by custom rule names
- Spam Actions UI: add a better description for bounce action

- Job status: remove stale job entries when certificate creation fails
- Message details: after quarantine storage delete flag the message as “deleted”
- Whitelist: fix javascript validation in some complex situation
- Login networks: added advanced audit logs
- Mail Encryption: auto-apply settings on save
- Export no longer generate errors if executed by read-only or quarantine admins
- Cofence: fixed auto learn of notified samples (regression from 5.1.3)
- Release: show a message to the user when a message release fails
- User Messages: show success message on completed save action
- First boot wizard: handle non-FQDN before to initial bootstrap is completed
- Local RBL: don't consider quicksand sanitized as definitive threat
- Message actions: update all leftover links in user report to the new ESG 5.x format
- Phishing safe sites are now mirrored only by Libraesva ESG first-party mirror
- Custom spam policy: fix javascript validation for body rules
- LDAP import: fix manual import triggered from the WebUI
- User manager: fixed saving of option “Can change spam settings”
- Release requests: the notification email is optional

API

- NEW: read-only access to saved search using “GET /saved-search”
- NEW: added resource “/user-message” to allow email-continuity implementation
- ADD: added property “senderIp” to message listing “GET /message”
- ADD: added many properties to “GET /message/{id}”
- ADD: added filtering by recipients and or relay filtering on many resource listing
- Increased the default item per page
- Improved speed of journal/soar calls when messages contain many URIs

Changes in v5.1.3 (Aug 08, 2022)

Improvements

- Privacy password: show session expiration details in profile menu when permission is granted
- Reduce web-server memory usage, especially for small appliance
- Cluster: auto-recover cluster replication when an appliance is powered off for a very long time
- Outlook Addin: added support for “Mark for Release” User Permission

Bug fixes

- Custom Antispam Rule: when adding a rule for a single domain, consider both “envelope to” and “header to” to select the domain
- Fix web-interface redirection when DKIM is disabled
- Release request: fix auto-removal of already managed requests
- Content filtering: removed web-ui combination add custom header on body matches, which isn't available in the engine
- Mail Logs Real-Time View: better visualization for filter and reset buttons
- ESG status: remove visualization artifact during status update
- Mail Logs Real-Time View: stop real-time view on logout to avoid DoS
- System Upgrade: fixed prefetch of all packages before upgrade
- Increased timeout for quarantine report generation
- Associate delivery to the most recent MTA message id, to avoid issues on high-traffic instances
- Automatically apply and reload Mail Scanner configuration when changing Mail Intercept configuration and Attachment Filters
- ESG 4.x migration: reset cache after Adaptive Truste Engine import
- DKIM Signing: fixed generation of DKIM keys

Changes in v5.1.2 (Jul 26, 2022)

Security

- ClamAV: upgrade to version 0.103.7

Improvements

- Delivery details: add DSN column
- Cluster: allow hostname change when cluster is already setup
- Cluster setup wizard: add button to quickly copy-paste IPs
- ESG system upgrades: better identification and feedback on Layer-7 inspection

Bug fixes

- Adaptive Trust Engine: fixed a bug which prevented the relay age cache to be used
- Report: pie chart used in "Per Domain Mailbox Use" defaults to licenses count not email address
- Delivery details: delay seconds are displayed correctly
- Reports: disabled the menu for raw data export (use export or copy instead)
- Cluster setup: show replica IP in flashed message during first initialization
- Database logger: fixed a bug that caused some delivery not to be bound to scanned messages
- Local RBL: use transactional update to improve accuracy
- Queues: ignore temporary files when computing queued message counts
- Privacy password: fixed the flashed messages on wrong password
- DOS prevention: when an abuser is blocked, prevent access to mail encryption portal too
- Backup: ignore a cache table during backup
- Cluster reload: added proper distributed reload in many pages
- API: boolean property "user releasable" was negated in the output

Changes in v5.1.1 (Jul 20, 2022)

Security

- URLSand: handle URI with a protocol name containing special chars

Improvements

- Firewall checks includes cluster connectivity check
- URI: log all URI also when message is blocked as spam
- Quicksand: improve cache hit rate of clean PDF and Documents
- User manager: quarantine permissions for all admin types are explicitly shown when editing users
- Show a custom "410 gone" page for all quarantine action URL no longer available on ESG 5.x
- File replication: send email notification also when SSH connection repeatedly timeouts
- TLS certificates: show expiration date of active certificates

Bug fixes

- Quicksand: a silently disarmed PDF no longer hides other files disarmed reports
- Mail Intercept: enable/disable button is recovered
- Email continuity: restore JS warning on invalid data
- Advanced logging: correctly set "null" values in audit messages
- Mail log: strip invalid UTF-8 character from security report and spam report
- Web UI: fixed removal of Passwordless Authorized Devices
- make sure graymail plugin is restarted on database reload
- Quarantine settings: immediately apply per domain customization of language
- Local RBL: make sure statistics are updated only on primary node
- ESG 4.x migration: reset file permissions after quarantine import
- Domain admin: allow domain names up to 256 character

- Backup/Restore: avoid errors if quarantine files changes during a hot backup
- Prevent creation of new domain admin password (see upgrade to version 5.1)
- Update documentation of Whitelist and Blacklist import

Changes in v5.1.0 (Jul 11, 2022)

Security

- TLS policy: changed default policy for new installation from "High Compatibility" to "Medium"
- TLS policy: "Medium" policy requires TLS encryption for SMTP Authentication (as in strict policy)
- TLS policy: "Strict" policy disables TLS renegotiation
- Postfix: prevent DoS when multiple email to the same domain are hanging in outgoing (i.e active) queue
- Improve detection of sender hosts in backscatter plugin
- Web Portal Authentication: allow multiple authentication set per domain (e.g. combining G Suite with Microsoft 365 and LDAP)

Improvements

- Quicksand and URLSand: allow default configuration at appliance level which also applies to new relays
- Add OTP support to APIv1 login
- Syslog: service is not restarted on "apply" when configuration is unchanged
- Faster license usage cleanup operation through asynchronous deletion
- Disk space monitor: notify by email when older data is removed because of critical disk threshold
- Message details: increased readability of security reports
- Message details: when a message is trusted, log if it's trusted by IP, by SMTP-auth or Authorized relay
- Backup: "User Messages" configuration is now added to backup by default

- Relay: automatic apply of engine configurations on every change
- Cluster: the Web UI highlights all the configurations that are not replicated automatically
- Web UI: "risky operations" are highlighted with a "danger" style (red color)
- Mail log viewer: faster and cleaner filtering
- Integration: improved memory consumption of Microsoft 365 and G-Suite import operations
- User Messages: "External Warning" can now be customized
- Asynchronous import from Microsoft 365, G-Suite and LDAP when started from the Web UI
- Compose: show the list of available sender addresses for the logged user
- Compose: hide main menu button when the user has no usable sender email
- Subject tags: replaced all prefixed {tag?} with user friendlier [tag]
- External warning: use the definition of "unusual correspondent" rather than "first time sender"

Bug fixes

- Search page: by default search is performed as "exact match" rather than "contains" to maximize performance
- Syslog: prevent double logging of some entries
- G-Suite: handle Google API rate limiting to prevent issues when importing big user base
- Wizard: allow manual configuration of Short and Long organization name
- SNMP: only show major release in sysLocation OID
- MTA: use hostname instead of domain for locally generated email to better distinguish generating servers
- MTA: don't automatically add domain to envelope sender for email generated from fully-trusted IP

Breaking changes

This version introduces some changes which require your attention.

1. **Email from M365/G-Suite sent from unmanaged domains will go through additional SMTP transport checks.** For incoming email, this will improve security since all SMTP reputation checks are always enabled. For outgoing email you have to make sure that all your domains used as "envelope sender" are listed into relay table page. Take extra care for subdomains of your relay domains, which MUST be explicitly added.
2. **Restricted user permissions for whitelist and blacklist.** The web UI will honor the user's "Quarantine Action" configuration in all pages. Some users will not be able to manage whitelists and blacklists anymore if they are not explicitly given this permission. Change the "Quarantine Action" user's configuration to include whitelists and blacklists if needed. From the user manager page you may bulk update this setting for multiple users.
3. **Changed format of default subject tags.** Subject prefixes added from ESG are now formatted as [Tag], while in previous versions were formatted as {Tags?}.
4. **Removed old API for ISP Panel.** If this appliance is controlled by an external ESG with version 5.1, after the upgrade the appliance needs to be associated again using a new API token generated from the API v2.

Version 5.0

All upgrades from previous versions are included. See the full release notes of Libraesva ESG version 5.0.

Libraesva EA v21.12: Release Notes

Changes in EA v21.12

Main Features

- Report scheduling

In the report section, it's now possible to schedule reports. When scheduling a report it's possible to choose the report type, the email addresses to which the report will be sent and the frequency. Supported frequencies are daily, weekly and monthly. For all the

schedules it's possible to set the time of report generation (hour and minute) and for weekly and monthly frequency it's possible to respectively configure the day of week or day of month, too. Please note that the time corresponds to the generation time of the report, if the report involves complex computation it may take some minutes to generate and send it.

- Indexing engine automatic optimization

In order to allow the Libraesva Email Archiver to run with optimal performance, an automatic daily index optimization has been introduced. The index is organized into chunks. A new page *Settings > System > Indexing* engine shows the optimal number of chunks based on the current hardware resources, along with the current number of chunks. The nightly optimization service progressively compacts the index by reducing the number of chunks.

- Log volumes

This new type of volume has been added in order to keep all the logs the Libraesva Email Archiver generates. Before release 21.12, logs were rotated and old logs were deleted after some time in order to preserve space on the local disk. When configuring a log volume, the Archiver will upload nightly the new logs to all the configured log volumes.

- Dedicated PEC connector

In addition to the existing Exchange, M365, Graph, Google, Zimbra and IMAP connectors, a new dedicated "Italian PEC" connector has been added. The synchronization of PEC connectors is completely independent from the synchronization of the other connectors and runs hourly. Currently the configuration of a PEC connector is identical to an IMAP connector. Existing IMAP connectors can be transformed into PEC connectors. Migration is very easy: when opening the configuration of the IMAP connector, the Archiver will automatically check if the connector could be a valid PEC connector and it will show a migration button. If the button does not show up where you think it should please raise a ticket to support@libraesva.com

- Multi-factor authentication

Local users can optionally configure multi-factor authentication through T-OTP (time-based one-time-password). This can be configured for all local users, without any restriction or limitation about the role.

- Download, restore, forward from Home view

When a user logs in the Libraesva Email Archiver, the buttons Download, Forward and Restore are now available also in the "Home" section. Through these buttons it's possible to download an email in EML, MSG or PDF format, forward an emails to any email address or restore an email if the configured connector supports this feature.

- PEC friendly name

When archiving an "Italian PEC" email, the Libraesva Email Archiver automatically indexes the email address displayed in the friendly name. PEC emails are identified by

the *X-Trasporto* or *X-Ricevuta* headers. Emails indexed with this new feature will be searchable also by the email address in the friendly name.

Features

- M365 key expiration notification

Microsoft introduced App registration client secrets expiration. The client secret is mandatory for configuring authentication, directory service and M365 connector. The Libraesva Email Archiver will automatically send a notification 15 days before the expiration.

- Update license button on license page

On the license page, in the *Settings > System > License* page, a button “License update check” checks if a new license is available and automatically installs it. The Libraesva Email Archiver will continue, as before, to check nightly if a new license is available.

- Report with multiple emails

When generating a report or when adding a configuration for a scheduled report, it’s possible to add multiple email addresses as recipients for the report.

- PST import advanced option

When running an import, two advanced options are available. The option “Replace already imported emails” replaces the already archived email with the new one. The option “Check exact email size” requires that the size of two emails must be exactly the same in order to infer that the two emails are actually the same emails. These options have been introduced also in release 21.8 starting from October 2021.

- New major release notification

The Libraesva Email Archiver nightly checks if a new major release is available for the configured release tier (early-adopter or stable) and sends a notification.

- Postpone major release update

When updating the Libraesva Email Archiver to the new available major release, the Archiver asks you whether to update immediately or to postpone the update to the next night to avoid service downtime for the users.

- High swap usage notification

The Libraesva Email Archiver periodically checks for RAM memory and swap usage. If an high swap usage is detected, a notification suggesting to upgrade RAM is sent to the administrators.

- Configurable number of inactivity days for connector

Until release 21.8, the engine that checks for connectors inactivity used a 7 days threshold to infer whether a connector is inactive. This threshold is now customizable

and can be configured from the connector settings page.

- Directory service caching information

The Libraesva Email Archiver keeps the directory service information and users list cached locally for faster access. The caching status of such information is now displayed in the directory services pages. The cache is automatically refreshed whenever configuring a new directory service or when updating an existing one. It's also possible to manually run a refresh of a specific directory service.

- Reindex retry

When a reindex process fails, it's now possible to re-run the process with the failed zip files only.

- Reindex priority

When launching a reindex job, it's possible to configure the priority of the process. Available priorities are normal, high and urgent. When setting an high or urgent priority, the Libraesva Email Archiver will run the reindex taking advantage of multi-core processing.

- Indexing engine status page

In the *Settings > System* section, a new "Indexing engine" page is available. This page shows information about the current status of the indexing engine and the index optimization status.

- Jobs page

In the section *Archiver > Compliance*, a new "Job" page is available, showing information and status about current and past jobs.

- Authentication with equivalent directory services

When a user is listed in multiple directory services, the Archiver will try to perform user login with all directory services. If the user is disabled on a specific directory service, the next directory service will be tried.

- Add capability to display raw mail from Mail detail

When opening an emails, it's now possible to consult also the raw headers.

Bugfix

- Fixed failing passive FTP server behind NAT

- Fixed missing emails retention when opening email from QR code

- Fixed PEC not validated when opened from QR code

- Fixed DNS settings update not working from user interface

- Fixed connector notifications not removed on problem solved
- Fixed batch import not considering uppercase file extension
- Fixed IMAP connector email deletion failing when deleting a lot of emails
- Fixed race condition lowering performance of PST batch import
- Fixed users caching engine losing some users for big directory services
- Fixed mailbox licensing counting M365 users without mailbox or Exchange online plan
- Fixed job's log file retrieval failing for old jobs
- Fixed exports by saved search including folder structure references
- Fixed M365 connector validation failing on known non-critical warning
- Fixed missing M365 login url
- Fixed user interface bug inhibiting to save legal hold
- Fixed Archiver nightly updated preventing connectors to synchronize new users
- Fixed user interface showing misleading negative emails number in a volume
- Fixed license update service deadlock
- Fixed LDAP search failing because of Domino not supporting paginator
- Fixed command to expand disks failing with GPT table headers
- Fixed Zimbra connector synchronizing only first level of folder structure mailbox
- Fixed notification settings not showing appliance level option when only a tenant is configure

Improvements

- Increased timeout for connector synchronization jobs
- Improved index mismatch email message
- Improved performance when listing folder-structure for specific user
- Improved performance when listing emails in specific folder
- Improved PST import progress percentage by using also percentage of single archive
- Improved log verbosity when deleting a customer (hard mode)
- Encourage splitting archives when running PST batch import

- Improved performance of PST archive extraction during PST import
- Improve volume credentials check trigger false positives notifications
- Decrease by 70% storage usage for folder structure volumes
- Retry upload on export volume when failing the first time
- Added alphabetical ordering for connector running users list
- Display only authentication buttons for directory services the user can authenticate with
- Force at least 1 domain on tenant configuration
- Allow to kill timed out jobs
- Hidden disable services tab for cloud Archivers
- Improved memory usage for zip cleaner service
- Optimized memory usage for directory service users caching engine
- Improved directory service users caching engine by preventing multiple refresh to run concurrently
- Improved zip cleaner service by preventing multiple execution to run concurrently
- Use data disk when extracting zip file for reindex instead of using `/tmp`
- On reindex failure, mark as failed only the specific email and not the entire zip
- Move zip cleaning percentage to advanced options
- Prevent OOM situation when running a batch import with a lot of archives
- Fixed UI overflow when visualizing postfix raw emails detail
- Renamed Google and Microsoft services to Google Workspace and Microsoft 365
- Improved performance when loading tenants page
- Added check for SPF when configuring a listener for Microsoft 365 or GSuite

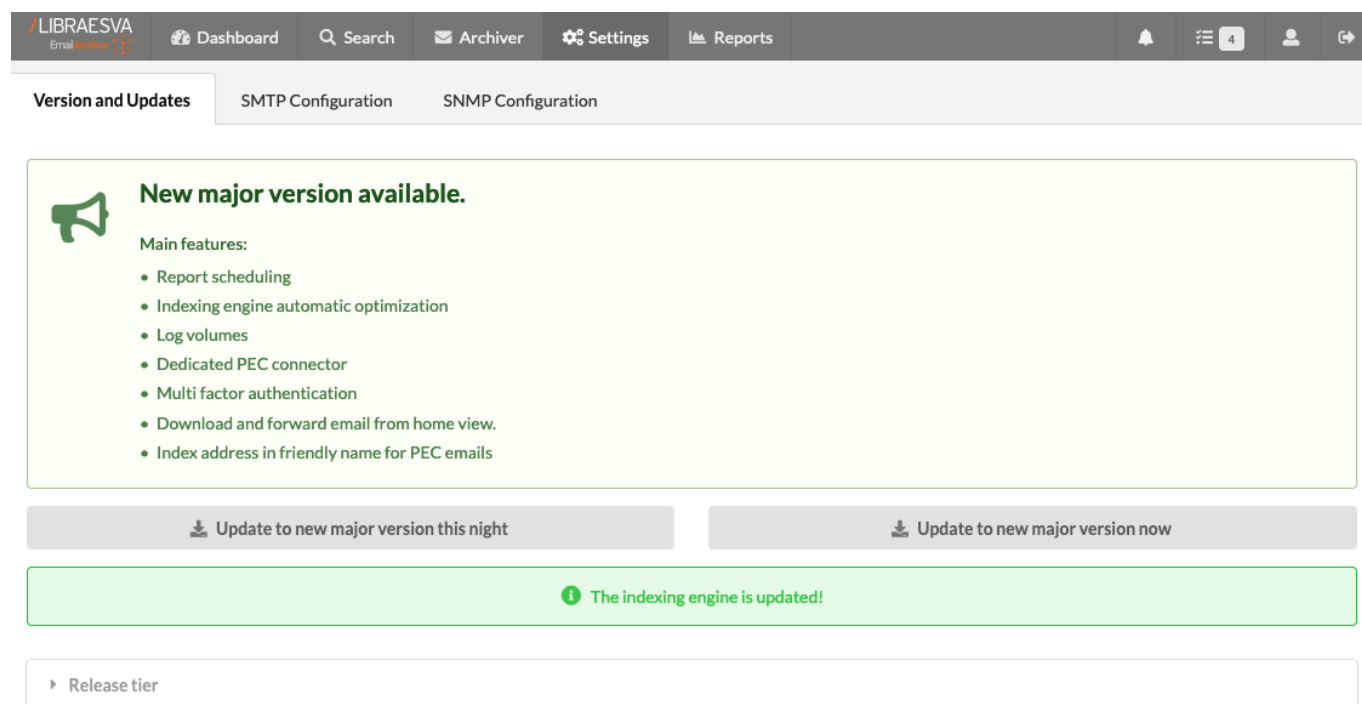
How to update

The Libraesva Email Archiver will automatically send an email notification about this major release.

In the section *Settings > System > General*, the update could be scheduled for the next night or started immediately.

For the Archivers hosted in the Libraesva Cloud, please contact support@libraesva.com to get

the Archiver updated.



The screenshot shows the top navigation bar of the LIBRAESVA ESG v5.0 interface. The navigation bar includes the logo 'LIBRAESVA Email Archiver 5.0' and menu items for 'Dashboard', 'Search', 'Archiver', 'Settings', and 'Reports'. On the right side of the navigation bar, there are icons for a notification bell, a hamburger menu with a '4' badge, a user profile, and a share icon. Below the navigation bar, there are tabs for 'Version and Updates', 'SMTP Configuration', and 'SNMP Configuration'. The 'Version and Updates' tab is active, displaying a green notification box with a megaphone icon. The notification text reads: 'New major version available.' followed by 'Main features:' and a bulleted list of features: 'Report scheduling', 'Indexing engine automatic optimization', 'Log volumes', 'Dedicated PEC connector', 'Multi factor authentication', 'Download and forward email from home view.', and 'Index address in friendly name for PEC emails'. Below the notification box are two buttons: 'Update to new major version this night' and 'Update to new major version now'. Below the buttons is a green status bar with an information icon and the text 'The indexing engine is updated!'. At the bottom of the notification area is a dropdown menu labeled 'Release tier'.

Libraesva ESG v5.0: Release Notes

Main features of version 5.0

- **New modern web interface**, with dynamic responsive dashboard and highly detailed scan result report
- **Message classification** through new message badges: **phishing**, **bulk**, **spoofing**, **BEC**, **malicious**, etc...
- **Adaptive trust engine** improvements: UI representation of historic data, improved AI
- **Advanced analysis result** with **Risk Confidence** and **Spam Confidence** indicators
- Unified **Advanced search**, a single place to search rejected and accepted messages
- **New Reports** that can also be exported as PDF
- **Unified TLS management**, allows certificate validation, rapid renewal and service assignment from a single page

- **LDAP sets can be managed in groups**, to allow flexibility when merging user information from different tenants

Version 5.0.31 (Sep 16, 2025)

Security

- **Mail scanner**: fixed CVE-2025-59689
- **System upgrade**: new upgrade system with asymmetric signature validation and encryption
- **Passwordless**: removed old authentication systems (may need re-login)
- **API authentication**: removed old authentication systems (may need re-login)
- **Remote support**: removed the old remote support connection via port 25

Version 5.0.30 (Aug 29, 2023)

Security

- ClamAV: upgrade to version 0.103.10

Version 5.0.29 (Aug 21, 2023)

Security

- Quicksand: add RAR archive reconstruction on sanitization
- ClamAV: upgrade to version 0.103.9

Version 5.0.28 (Mar 13, 2023)

Security

- QuickSand: block attachments in archive when unzip size is greater than 150MB

Version 5.0.27 (Feb 21, 2023)

Security

- ClamAV: upgrade to version 0.103.8

Version 5.0.26 (Oct 17, 2022)

Security

- Improves RBL detection sub-domains below 3rd level
- Quicksand: improves www-links detection in PDF
- Update bitdefender license

Bug fixes

- Outlook add-in: remove reference to a deprecated API call

Changes in v5.0.25 (Sep 05, 2022)

Improvement

- Add forward compatibility for Clamd configuration of ESG > 5.1
- System upgrades: show estimate time in advance and use animated progress bars when upgrade is active

Bug fixes

- Whitelist: fix javascript validation in some complex situation
- Export no longer generate errors if executed by read-only or quarantine admins

Changes in v5.0.24 (Aug 08, 2022)

Security

- ClamAV: upgrade to version 0.103.7

Bug fixes

- Mail Logs Real-Time View: stop real-time view on logout to avoid DoS
- System Upgrade: fixed prefetch of all packages before upgrade
- Increased timeout for quarantine report generation
- Associate delivery to the most recent MTA message id, to avoid issues on high-traffic instances
- Automatically apply and reload Mail Scanner configuration when changing Mail Intercept configuration and Attachment Filters
- ESG 4.x migration: reset cache after Adaptive Truste Engine import
- DKIM Signing: fixed generation of DKIM keys

Changes in v5.0.23 (Jul 20, 2022)

Security

- URLSand: handle URI with a protocol name containing special chars

Improvements

- Show a custom "410 gone" page for all quarantine action URL no longer available on ESG

5.x

- File replication: send email notification also when SSH connection repeatedly timeouts
- TLS certificates: show expiration date of active certificates

Bug fixes

- Mail log: strip invalid UTF-8 character from security report and spam report
- Web UI: fixed removal of Passwordless Authorized Devices
- make sure graymail plugin is restarted on database reload
- Quarantine settings: immediately apply per domain customization of language
- Local RBL: make sure statistics are updated only on primary node
- ESG 4.x migration: reset file permissions after quarantine import
- Domain admin: allow domain names up to 256 character
- Backup/Restore: avoid errors if quarantine files changes during a hot backup
- Prevent creation of new domain admin password (see upgrade to version 5.1)
- Update documentation of Whitelist and Blacklist import

Changes in v5.0.22 (Jul 05, 2022)

Security

- Defend against file extension evasion techniques targeting Windows machines

Improvements

- Backup Tools: add User Messages to “configuration” backup

Bug fixes

- Properly enable all the service after licence upload if the previous was expired
- Import 4.9: apply dkim configuration after import

- Content Filtering Rules: correctly apply modifier for “regex” filter expression
- Search: fixed “not equal” operator on “Delivery status” field
- Threat Remediation: permit multiple connector on the same domain with Zimbra mail server
- Backup Tool: fixed restore of manually-uploaded certificates
- Valid Recipient: properly check duplicate during text import

Changes in v5.0.21 (Jun 15, 2022)

Security

- Update kernel to release 5.4

Improvements

- Cluster: improved auto-recovery procedure for updates on message tables
- Cluster: added popup to better explain Hard Reset behaviour
- Quarantine Digest: speed up digest email retrieval
- User Management: show Quarantine Action in user details popup

Bug fixes

- Always use MTA configured double-bounce address for Dynamic Verification test
- Quarantine Test: show all address and domain owned by the User
- Quarantine Digest: always generate the report for all hours, even if the previous job is not completed
- Quarantine Digest: skip users with invalid data
- LDAP Import: honor user configuration for quarantine recipient (regression in 5.0)

Changes in v5.0.20 (May 23, 2022)

Security

- Update operative system to upstream RHEL version 8.6

Improvements

- Automatically reboot appliance after Time Zone changes
- Adaptive Trust Engine: improved speed of Trust score algorithm
- Sort domains alphabetically in the drop-down selections

Bug fixes

- Fixed Delete action from View Body page
- Email Continuity: fixed reply action
- SMTP Auth SASL: removed un-supported CRAM-MD5 mechanism
- Quarantine Retention: restore cleanup of Database data according to its retention
- Message Details: limit ATE graph history to database retention
- Properly identification of First Time Sender for messages with multiple headers X-Envelope-From
- Google Workspace: fixed login when user doesn't exist yet

Changes in v5.0.19 (May 09, 2022)

Security

- Quicksand: identify suspicious action write+execute without autoexec
- SAVAPI: upgrade to version 4.15.7
- ClamAV: upgrade to version 0.103.6

Improvements

- MailScanner Engine: preload license options on batch start to reduce overhead
- Reordered and randomized scheduled tasks to distribute and avoid spike of resource usage
- License Count: cleanup BATV from accounted addresses

Bug fixes

- Whaling: fix identification of whales for related (alias) domains
- Backup Download: Increased timeout for very large backups
- ESG4 migration: keep domain admin without credentials but quarantine report enabled
- Per Domain Mailbox Use: fix domain license count
- Quarantine Disk: fixed cleanup of duplicated data
- Cluster Setup: prevent error on scheduled task start
- Graymail: ignore messages without from header
- Network Setting: allow DNS change on cloud appliance
- Spam Engine: reduce cache timeout of result for messages with the same hash
- Address Rewriting: properly save “Rewrite Header” options

Changes in v5.0.18 (Apr 19, 2022)

Improvements

- Web UI: faster visualization of navigation tabs
- Skip whaling check when scan mode is “virus only”
- Message details: add warning for failed SPF beside whitelist result label
- Relay: don't use pop-ups to notify saved changes

Bug fixes

- User Messages: preserve active tab when changing language or domain
- URLSand: always executes HTML analysis, even when preliminary tests have found no A-tags
- First setup: remove special chars from generated company short name

Changes in v5.0.17 (Apr 11, 2022)

Improvements

- System memory: improve speed by avoiding swap area as far as possible
- System upgrade: add user-friendly message when uploading invalid upgrade file
- Web UI: enable sorting in Valid Recipients List, Whitelist, Blacklist, User Manager and Whaling.

Bug fixes

- G Suite integration: continue import in case one or more user failed to import
- M365 Authentication: add openid scope
- Saved Search: restore delete functionality
- Whilist/Blacklist: display invalid email errors
- TLS certificates: avoid permission error when generating CSR certificate
- Cluster: disable job replicator on destroy
- Quarantine digest: hide “send” button when there are no messages to notify via email
- Database logger: prevent automatic stop during log rotation

Changes in v5.0.16 (Mar 29, 2022)

Improvements

- add “System Upgrade” page to allow manual upgrade to next releases
- improved message in error pages (e.g. 403)
- improved message logging from ESG application

Bug fixes

- Antispam settings: correctly show as customized domain
- correctly log graylisted email when only some of multiple recipients cause the delay
- fix missing logo when not using the default one
- remote syslog: fix a duplicated configuration on apply
- Restore description of SPF exceptions in the Web UI
- fix TLS certificate file removal
- FTP backup: remove double appliance name prefix from admin notices
- licensing: allow setting aliases to username without explicit domain
- ESG4 migration: avoid connection timeout when migrating huge appliances
- ESG4 migration: restore letsencrypt renewal files from previous version if missing

Changes in v5.0.15 (Mar 14, 2022)

Security

- protect backups from un-authorized access
- add DNS lookup to esvalabs when IP is blacklisted for DoS attempt

Improvements

- upgrade parser of PDF documents
- Upgrade Letsencrypt certbot

- Dashboard: cleaner cluster status box in dashboard
- Halves memory usage of web server scripts
- Graylist plugin: add inline documentation
- IspMonitorController: up to 6x faster requests to remote server (also prevents timeouts)
- ESG4 migration: reduce memory usage for xlarge appliances

Bug fix

- Smarthost: use most specific configuration when mixing domain based smarthost and default smarthost
- User text import: replace variable HOST URL with value configured in quarantine report
- Quicksand: fix disarming of external resources in office documents
- Policy quota: prevent duplicate names in webui
- Logs rotation: use signals to restart database email writer daemon
- Upgrade from ESG 4.8: fix a version conflict which may block the upgrade

Changes in v5.0.14 (Mar 07, 2022)

Features

- Country Policies: configurable policies to allow/block web interface access from specific countries (see also Geo-Blocking)

Improvements

- Backup/Restore: increase timeouts to accommodate huge backups
- Valid recipient import: reword web interface to improve UX
- SNMPd: inline help for available custom OID
- Details: show quicksand result even when running in dry-run mode
- LetsEncrypt: update certbot

Bug fix

- Cluster file replica: removed a memory leak (may free up to 1GB RAM)
- Details: show “not analyzed” status of quicksand and URLSand
- Shutdown sequence: ensure all logging is stopped before storage unmount
- Log to database email delivered via internal relay service (i.e. fix messages left in active state in the UI)
- Improve UI when changing option “block email on attachment removed”
- Viewmail: properly identify attachments filenames if defined in MIME Entity headers
- Threat Remediation: always try the recall for all recipients, and log failure tentative
- Disabled password-less login when domain authentication is configured to “No Access”
- Message Detail: fixed report parsing for Deutsche language
- Use native select in popup to show more field validation errors
- SNMPd: prevent usage of reserved community name “public”
- Release request: better feedback on MTA transport errors
- Relay test: change user feedback on invalid email
- Logwatch: remove some noisy unmatching logs

Changes in v5.0.13 (Feb 22, 2022)

Security

- ClamAV: upgrade to version 0.103.5 LTS
- Block aggressive bulk email even when Graymail plugin is disabled
- (notice: unaffected to PwnKit security issue)

Improvements

- Asynchronous system upgrade, which can now be easily and safely called from web-ui and system cron jobs
- Asynchronous application of MTA settings to improve service stability and reliability

- Periodical cleanup of unusual values in message score normalization
- Increase “unusual correspondent” interval from 12h to 24h
- Spam rule report: add column “Determined Spam %” to highlight the most influent rules
- Add more logging to digest report generator to give more feedback on support tickets
- Search: allow the user to search bounce messages and add more validation for email addresses
- Local RBL: add engine documentation on the web UI
- Mail Encryption reply: allow bigger reply message (up to 100M)
- License usage: show mailbox count variation to MSP
- ESG4 migration: import user customized MTA settings
- User text import: improved quarantine report options
- Search: results are displayed by “received date” instead of “analyzed on”
- Reports: when displaying license usage count, consider all licensing model options
- Search modal: improved UI, with autofocus and button reordered
- Message details: add column “user / machine learning” to antispam report
- Data Loss Prevention: cleanup UI and show report in a modal
- First install: when network is available, wait for a full upgrade before starting webserver
- Increase logging of verbosity for system jobs
- HTTPd: increase server timeout for long running searches
- HTTPd: reduce server authorization by moving to backend job sensible tasks
- ESG4 migration: improve user feedback while importing data

Bug fixes

- Dashboard: adjust count of delivered messages in mail flow
- Log rejected messages due to MTA configuration errors
- Log rejected messages to multiple recipients due to message size limit
- Implemented edit feature in wildcard TLS certificates
- Bulk release: make sure sent email are limited to addresses owned by the logged in user
- URLSand rewrite: handle & character correctly in HTML text parts

- Avoid email notification on slow storage when doing log rotation
- License count: when deleting license avoid removal of quarantined messages
- FTP backup: auto-delete backup after upload (either on success or failure)
- Reboot: avoid multiple reboot when some error are generated by the shutdown process
- Outlook addin: generate a unique ID per appliance, to avoid issue on hardware migration
- Data loss prevention: schedule engine reload after “apply” action
- Mail Encryption: show authentication problem on login
- Backup restore: converted to a system service to avoid restore issues
- LDAP: fix user/email address DN selection and properly display authentication errors
- Summary Report: restore total percentages
- Message details: add all missing rules descriptions
- Remember login target path when authenticating via M365 or G Suite
- Quarantine: mark messages as “not available” when cleaning storage files
- Search: prevent timeout when displaying multiple email with many recipients
- Increase timeout for User import
- Message Details ATE: ignore bounce messages
- ESG4 migration: fix quarantine domain admin permission
- ESG4 migration: avoid timeout on configuration import
- ESG4 migration: cleanup duplicate whitelist and blacklist on import
- ESG4 migration: import greylist database from ESG 4.x

Changes in v5.0.12 (Jan 10, 2022)

Security

- Bitdefender server: update to version 3.0
- Avira SAVAPI: update to version 4.15
- ESG Bitdefender integration: drops high-privileges while scanning
- ESG Savapi integration: drops high-privileges while scanning

- Quicksand: increase the Office Document scan limits to intercept more threats

Improvements

- ESG Bitdefender integration: nearly halves RAM usage during scanning
- ESG Savapi integration: nearly halves RAM usage during scanning
- Install license: replicate license installation in cluster setup

Bug fixes

- MailIntercept: do not monitor for messages received from localhost
- System preferences: fix a UI issue when using three-level timezones (e.g. America/North_Dakota/Center)
- Report: add UI feedback when using “Per Domain Mailbox Use” with date ranges
- System preferences: fix audit message for timezone changes
- Social graph: fix a server error when searching by empty email address
- Graymail: prevent duplicate record creation
- PDF Report: display correct datetime interval
- Custom spam policy: avoid errors when adding an policy with empty description
- ESG4 migration: copy LetsEncrypt account information to authorize automatic renewal

Changes in v5.0.11 (Dec 28, 2021)

Security

- Message detail page: stricter validation of message ownership of logged user
- ClamAV SaneSecurity: changed enabled databases based on Libraesva security review
- Passwordless: double check server-side secret on token verification
- Disable httpd lua module (CVE-2021-44790)

Improvements

- ISP Instance Monitor: integrate with ESG4 appliance and use faster queue length evaluation
- Scheduled report: new email template with whitelabelling and explicit report type in subject
- Release request: new email template with direct detail page link
- User messages: allow signatures bigger than 64k
- Message details: show delivery information of messages imported from ESG4
- Add audit log in Account takeover protection
- Disk expansion: warn about possible expansions left
- ClamAV monitor: wait more time when doing service availability tests
- Whitelabelling: remove Libraesva signatures from email notifications
- Hypervisor Console: add “pause incoming mail” command as in web ui
- WebUI: better vertical alignment of all forms

Bug fixes

- Quarantine actions: avoid redirect to login when session is expired and passwordless cookie is available
- Quarantine actions: quarantine administrators always have action “release” instead of “ask to release”
- Dashboard: last messages honor the global settings, instead of using a fixed 20 results limit
- Disk expansion: minimal increase is set to 1GB (to avoid almost null expansions)
- LDAP: enable pagination only when server announce it in the banner
- User text import: restore notification email, and document quarantine address selection
- History import from ESG4: enable import of deliveries logs
- Reports: evaluate all saved search filters on “per domain email usage” report
- LetsEncrypt: when server verification fails due to network issues, do not retry validation on remote server

- SocialGraph: show proper UI feedback when searching by empty email
- Deferred message: show full deferred status as reported by the MTA

Changes in v5.0.10 (Dec 15, 2021)

Security

- QuickSand: handle PDF files with random file preamble or filename containing “..”
- SNMP: disable basic information access when SNMPd is enabled for one IP
- Adaptive Trust Engine: fully handle UTF-8 to better identify first time senders

Improvements

- Add UI feedback on Threat Remediation recall actions
- LDAP: allow anonymous access to external sets when bind user is left empty
- Integration: performance speedup (up to 10x)
- UI: show delivery status as bounce when there's at least one recipient with bounce
- Quarantine Actions: show user-friendly 410 gone page for old quarantine link actions
- CRM114: improve learning routine, and avoid useless “forget” actions
- Enable Threat Analysis Portal registration (license dependent)

Bug fixes

- Restore release permission for “Quarantine” Admin/Domain Admin
- Mail Encryption portal: allow loading of images on reply
- Replicate Bayes learn action in cluster environment
- prevent cluster setup failure when letsencrypt directory is missing
- Message details: delivery path interpolate hop without Geo-localization
- Integration: avoid duplication errors when valid recipients are found on multiple sources
- LDAP import: always set a page size when supported by remote server to avoid server

import limiting results transparently

- LDAP synchronization: correct loading email and users from Domino servers
- LDAP on domino: properly filter email addresses based on domain
- Avoid a configuration errors on engine which caused messages to became marked as other infected
- Fix a race condition which caused some message to be left in “active” delivery status
- Permission check against bounce messages for domain admin no longer generate UI errors
- WebUI: align graphics for all modal

Changes in v5.0.9 (Dec 1, 2021)

Security

- Adaptive Trust Engine: increase accuracy by normalizing header from
- Quarantine action: restrict permissions on forwading

Improvements

- ClamAV: halves RAM usage during signature reload
- Quarantine action: properly blacklist from header when available
- Quarantine action: improve feedback on release
- LDAPS: allow using self-signed certificates on remote host
- Integration: separate import of users and valid recipients for G Suite, Microsoft365 and LDAP, to better compute licensed mailbox
- Message detail: add audit logging as in ESG 4
- Wizard: add validation when using IP address instead of hostname
- Bitdefender: use proper brand spelling

Bug fixes

- Encryption: resolve issues with multipart/signed and multipart/encrypted MIME which caused some email to become plain/text
- Quarantine action: add modal for “ask to release” when viewing email
- URLSand: fix licensing hash on link generation
- Database mail logger: avoid issues when importing reports with size above 4 kilobytes
- Graymail: fix a database permission error which prevented newsletter identification
- Backup: change audit log messages
- Antispam engine: resolve accuracy issue when interpreting rare UTF-8 character (i.e. high level pages)
- System Preferences: use system administrator email for system email (i.e. sent to root)
- Threat Remediation: avoid failing when no mailbox was found
- Relay domain: fix an error when enabling dynamic verification

Changes in v5.0.8 (Nov 18, 2021)

Security

- update operative system to upstream RHEL version 8.5
- reduce session TTL on server-side

Improvements

- WebUI: spinners icons review
- scanning engine maximum message size is kept in sync with MTA max message size
- re-enable email encryption portal (license needed)
- graceful reload of HTTPd configurations
- email samples are sent to esvalabs.com to improve deliverability
- faster mail queues length calculation on dashboard

Bug fixes

- avoid CPU high utilization when reading messages in active queue
- avoid memory exhausted when generating Spam rules hit reports on large dataset
- add backward compatibility with encrypted links generated by ESG 4.x
- mail queue logger can handle remote server messages up to 8192 chars

Changes in v5.0.7 (Nov 02, 2021)

Improvements

- Syslog: configuration isn't replicated in cluster setup
- Microsoft365/GSuite: faster import of users (at least 2x)
- Allow readonly access to relay and user page when the license is expired
- Whitelabelling: rollback to previous theme, should the generation fail
- Allow cluster destroy should the license expires

Bug fixes

- IMAP/POP3: prevent a 500 error on user login
- Import 4.9: cleanup old configuration to avoid clamav engine failures
- Whitelabelling: don't reset theme on updates
- Release requests: allow empty notification email
- Release requests: remove loading browser popup on successful release
- Digest Report: fix selection of options in bulk actions
- User preference: read default values for new user when creating on login
- Email continuity: use new security policy system to validate user from addresses
- ATE: prevent errors when from header is not set in a message

Changes in v5.0.6 (Nov 09, 2021)

Security

- Hardened configuration for SSH daemon

Improvements

- Chrony: if the offset is above 30 minutes, just set the current time
- Check for update after network first configuration
- Cluster: better status monitor for file replica
- automatically reload mail scanner engine after configuration changes
- added confirm modal for shutdown/reboot/suspend cluster actions

Bugfix

- First run: wait for database initialization before scheduling reboot
- Console: reset fallback address in issue file on first boot
- restore release requests functionality
- cluster setup: fixed file synchronization of TLS keys
- compile smtp check override after migration from 4.9
- When creating users inherit all configured default
- Fix signature saving error on some configuration
- Fix widget for color selection in system preferences
- Restored SNMP OID for SMTP traffic
- Remove errors on whitelist and blacklist insertions for users with multiple addresses in recipients
- Remove errors on whitelist and blacklist insertions for safe-learn users
- LDAP set of type other are correctly identified as such
- prevent a page error when decrypting links generated by ESG 4.9

Changes in v5.0.5 (Oct 19, 2021)

Security

- **Abuser lockout:** implement incremental lockout for recidive abuser
- **Adaptive Trust Engine:** support BATV address and domain with more than 4 levels
- **Adaptive Trust Engine:** separated history age for different relays
- **DKIM key:** upgrade to 2048 bit
- **DNS:** prevent DoS on SERVFAIL by adding a short term cache
- **Webapp:** force HTTPS with TLS > 1.2
- **Mail transport agent:** disable TLS 1.0 and 1.1 on strict/medium TLS mode
- **RBL:** don't disclose RBL name on rejection
- **User Manager:** all domain admins are now multi domain admins (no longer restrict the username format)
- **User Manager:** increase password security for Users, by using high-end caching algorithm for user passwords.

Improvements

- **AntiSpam settings:** defaults for new users are explicitly configured and no longer inherited from the domain admin's configurations
- **Appliance Sizing:** automatic configuration of all resource-intensive services
- **Backup and Restore:** new data importer from ESG 4
- **Backup and Restore:** FTP backup supports TLS
- **Branding:** new Libraesva logo and hypervisor themes
- **Cluster Setup:** simplified setup wizard
- **Cluster:** simplified monitoring and recovery UI
- **Console:** add full ANSI-color support to hypervisor console
- **Console:** interactive console with dynamic data
- **Crash auto-recovery:** auto-repair services for most disk crash situation
- **DKIM:** disabled signature for empty envelope from

- **Dashboard Threat Map:** high level threat distribution like phishing, spoofing and whaling
- **Details page:** quick summary for rejected email
- **Details page:** threat or indicators identified by the internal engines
- **Disk expansion:** support for 60 disk expansions
- **Licensing:** new licensing system
- **MailIntercept:** new dedicated configuration page
- **Machine Learning:** new page with statistical records of CRM114 machine learning engine
- **Machine Learning:** new page with statistical records of Bayes machine learning engine
- **Message Actions:** all actions can be executed from all message views
- **Message details:** add DSN and description to all SMTP reject listing, to distinguish temporary from permanent failures
- **Message details:** new analytical representation of email path
- **Message details:** new delivery status badges, which includes all statuses (e.g. recalled, released, ...)
- **NTP:** system clock synchronizations is always enabled and synchronized
- **Network:** refactored network management with multiple interface and route configurations
- **Phishing Highlight:** removed some options which are now managed directly by the ESG security team
- **Quarantine list:** show scan results and delivery status
- **Quarantine settings:** explicit configuration of default settings for new users (no longer inherit domain admin configuration)
- **Reboot/Shutdown:** prompt feedback of the progress of the reboot
- **SASL:** automatic realm initialization and asynchronous configuration
- **Sandboxes:** URLSand and Quicksand configurations are on distinct pages
- **Scan result:** Dictionary and DNSBL reporting has been improved
- **Scan result:** new "Archive Encrypted" scan result
- **Scan result:** new "QuickSand URI Disarmed" scan result
- **Scan result:** "OFF" messages (not scanned because of exception rules) are displayed in

message lists

- **Search page:** searches with advanced filters can be saved to be used with report pages
- **Search page:** can now search also among rejected messages
- **Social graph:** refined interface and interactions
- **System preferences:** increased the default value of records displayed in message lists
- **System preferences:** new color palettes and new color picker
- **System resource:** new dedicated page, with detailed resource statistics
- **TLS Certificates:** TLS certificate can be shared in a cluster setup
- **White-labelling:** logo automatic scaling from many raster formats
- **Wizard:** brand new first-run wizard, with configuration loader from ESG 4.9

VM hardware improvements

- Use EFI in all hypervisors which support it
- Add Secure boot and security options in VMware 6.7+
- Add IOMMU in VMware 6.7+
- Use GPT partitioning which allows up to 60 disk expansions
- Support for in-place operating system migration
- Fully automated build-chain for many target hypervisors. Supported vSphere 6.0-6.5, vSphere 6.7+, Proxmox KVM, Hyper-V, Xen

Bug fixes

- **User Manager:** Read-Only administrator can modify their own profile
- **Mail transport agent:** default email max size lowered to 25 MB, to avoid delivery issues to M365 and GSuite
- **Licensing:** atomically switch license without services restart

Breaking Changes

- **License file:** license file for ESG 4.x isn't valid on ESG 5.x. You should have received the updated license from your channel, if you haven't please contact us.
- **Scheduled reports:** not migrated from ESG 4.9, must be recreated manually
- **Quarantine link:** links generated from ESG 4.9 are no longer valid. Messages can be released from WebUI after migration process for history and quarantine is completed.
- **Legacy end-user API (URL /esva-api/myemail.php)** (new user API for mobile applications to be used instead. URL: /api/v1)
- **Administrative API (URL /esva-api/)** for system configuration (available from ESG 5.1. URL: /api/v2)
- **Distributed setup:** not available, will be released in a future release.

Libraesva EA: Critical bug notification (potential data loss) – Oct 2021

Affected product versions

- Libraesva EA Backend from version 21.3.4020
- Libraesva EA Backend from version 21.8.4619

The current backend version can be found in Settings > General > Backend

Brief description

A bug has been discovered in the volume cleanup service which performs the hard deletion of emails that have been soft-deleted manually by the administrator or automatically by

configured retention rules.

Additional conditions

In the mentioned product versions the bug arises when emails are deleted either manually by the administrator or by retention rules. The bug does not arise if no email is deleted.

If you don't have configured any retention rule and did not perform any manual deletion you are not affected by this issue.

Consequences

Email bodies and attachments may have been accidentally deleted. Such emails are still indexed and can be searched for, but the email body is not available.

This is limited to emails stored in proximity of emails that have been deleted manually by the administrator or automatically by configured retention rules.

Detailed description

Email deletion is performed through a soft-delete followed by an asynchronous hard-delete.

When the administrator or a retention rule deletes an email, the email is flagged as deleted making it invisible to the searches but the email metadata is still available in the archiver and the email content is still available in the volumes.

At a later time a scheduled cleanup process performs the hard deletion by removing the email content from the archive volumes and the email metadata from the archiver.

A bug in this cleanup process caused some emails, which were not been soft-deleted, to be deleted from the volumes. Metadata about these emails is not deleted from the archiver.

The result is that such emails can be searched for in the archiver but the content of the email is not available.

For such email the metadata which includes sender, recipients, subject, date and message-id is still available while the email body and attachments are not.

Mitigation

Libraesva released an “emergency update” to stop the cleanup process on all affected product versions until a fix of the software bug will be developed and released.

The “emergency update” is a mechanism through which Libraesva can release a software update to be installed immediately on the appliances. The process has been designed to handle unexpected and urgent issues like this.

The emergency update brings the backend version to 21.3.4945 or 21.8.4833. Starting from these versions the problem is not present.

Assessment

The Libraesva support service can assess whether the customer is affected by this problem or not.

The assessment can be done through the “remote support” feature of the product.

Should the customer be affected, the Libraesva support will perform an in-depth assessment and will provide the following information:

- how many emails have been deleted (phase 1)
- how many have been recovered by the mail service connector (phase 2)
- the list of email that eventually have not been recovered (phase 3)

Customers can contact the Libraesva support through the usual channels. The issue will be managed with high priority.

Remediation

The engineering team disabled the cleanup service through an “emergency update”, automatically installed on all appliances, thus no more email loss can happen.

The cleanup service will be re-enabled by the engineering team when the issue will have been fixed.

Timeline

- Engineering: Investigation started on the 2nd of October at 9:15 CET
- Engineering: Bug discovered on the 2nd of October 2021 at 10:58 CET
- Engineering: Mitigation action through an “emergency update” released on the 2nd of October at 11:18 CET
- Technical Support: Initial assessment on all appliances hosted in Libraesva’s cloud completed on the 2nd of October at 16:30 CET (phase 1)
- Technical Support: In-depth assessment on all appliances hosted in Libraesva’s cloud completed on the 4th of October at 18:13 (phase 2)
- Engineering: Released the new cleanup process through standard automatic update on the 30th of November at 06:00
- Engineering: Recovery completed confirmation from the last customer affected by this issue, Jan 27 2022

Incident closed

Libraesva EA v21.08: Release Notes

Changes in EA v21.08

Main Features

- Connector statistics per user

In the connectors page it's now possible to check statistics about the users synchronized by each connector. For each user useful information is provided: the email address, the synchronization status (running, completed, errored) and the time of the last update. For each user it's also possible to see more advanced statistics about number of mails imported, moved, deleted or expired. Please note that in order to fully gather this information, the Archiver needs a full execution of the connector with the 21.8 version.

- Journaling statistics and inactive journaling notification

The Archiver keeps track of the timestamp of the last imported email for each of the configured listeners. This information is shown in the listeners page. When configuring a listener the `Allowed inactivity hours` is used to trigger a notification if the Archiver detects that no mail has been imported from a specific listener in the configured number of last hours. The default value is 48 hours.

- Launch single user connector from UI

The Archiver allows to manually launch the execution of a connector for a specific user. This can be done through the connector page by launching a synchronization job and specifying the user's mailbox you want to synchronize. It's still possible to launch the execution of the connector for all the users but this is not recommended due to performance reasons.

- Connector report

In the Report section it's now possible to generate a new connector report. This report shows the list of the users synchronized by the connector and includes some counters: the new emails imported by the connector, the emails for which the Archiver has registered a variation about the position in the folder structure, the emails deleted by the user in the mailbox and the emails deleted in the mailbox by the Archiver due to connector cleaning configuration. These counters can be filtered by date.

- Mailbox licensing

Full support for mailbox licensing. If the Archiver is running with a storage-based license storage tenants limits are available. When the Archiver is running with a mailbox-based license mailbox tenants limits are available.

- Updated index engine

The indexing engine has been updated in order to provide better performance and to better handle the growth of the index.

- Cloud Archivers: automatically configure volumes

The Cloud Archivers are now distributed with an internal configuration about volumes. When creating a new tenant, a `Automatically create and configure Libraesva`

Cloud Volumes option is available. By using this option, the Libraesva Email Archiver will automatically configure data volumes and folder structure volumes for the new tenant. It will be still possible to edit the volumes configuration at any time.

Features

- New email deletion management
Send notification on retention rules creation, update, deletion. See details at <https://docs.libraesva.com/document/how-to-delete-email-from-the-libraesva-email-archiver/>
- Allow to delete exported files in export volume
When browsing an export volume, it's now possible to delete exported files.
- Allow to update DNS servers from the hypervisor console
When configuring network from the hypervisor console, also primary and secondary DNS server are configurable.
- Add stop button on connector synchronization jobs
After launching a connector synchronization jobs, the job can be killed.
- New page about disks
In this page details about disks are shown. Information about SCSI controllers are shown, too.
- Allow to reprocess all deferred messages
In case of troubles when setting up listeners, the email queue can grow very fast. When listeners configuration has been fixed, all the messages can be reprocessed.
- Show details about skipped mails for PST/zip
When a PST/zip import process skips some of the emails to be imported, it's possible to analyze which mails were skipped and why.
- Add notification for full index disk
When the index disk is full or almost full, a notification to the administrator is triggered.
- Send a notification when a tenant has no volumes configured
When archiving is stopped for a tenant because no volumes have been configured, a notification describing the problem is triggered.
- In the update page, show if the Archiver is updating
In the **Settings > System > General** section you can see if there is already an upgrade running. In this case, the Archiver prevents to run again an upgrade.
- Send a notification on backup failure
When the backup (scheduled or manually launched) fails, a notification describing the

issue is triggered.

- Tenant limits for mailbox licensing

If the Archiver has a mailbox-based license, tenant mailbox limits are available for all the tenants.

- Send a notification when the IMAP journaling is trying to import a too big email
IMAP journaling can be blocked when trying to import a too big email. In this case a notification describing the issue is triggered.
- Allow to search users in case insensitive mode
In every page of the Archiver, when searching for a user, the search is always case insensitive.
- Directory service equivalence (beta) Allow to define an equivalent class for directory services. This is useful especially when migrating users (for example from Exchange to Microsoft365). The archiver will be able to match the users in different directory services.

Bugfix

- Export mail list is fixed at the moment the job is launched, it will not change during the export process
- Fixed bug when retrieving owner of saved searches
- Fixed DNS update from UI
- Allow to run configuration backup manually, even if there are no rules configured
- Fixed inconsistent behavior of To date selector for searches and export
- Fixed issues related to timed-out jobs
- Fixed issues related to network configuration updates
- Allow to update tenant limits only when same tenant connectors are not running
- Fixed firewall page crash when no rules are configured
- Fixed kill job feature
- Fixed bug during tenant hard deletion
- Fixed tenant limits information in tenant report
- Fixed bug in mail view for mails imported by an Exchange connector
- Allow to re-import soft-deleted mails
- Fixed connector current status information

- Fixed multiple notifications deletion
- Fixed configuration backup time-out for big databases
- Added check for priority when inserting new retention rule

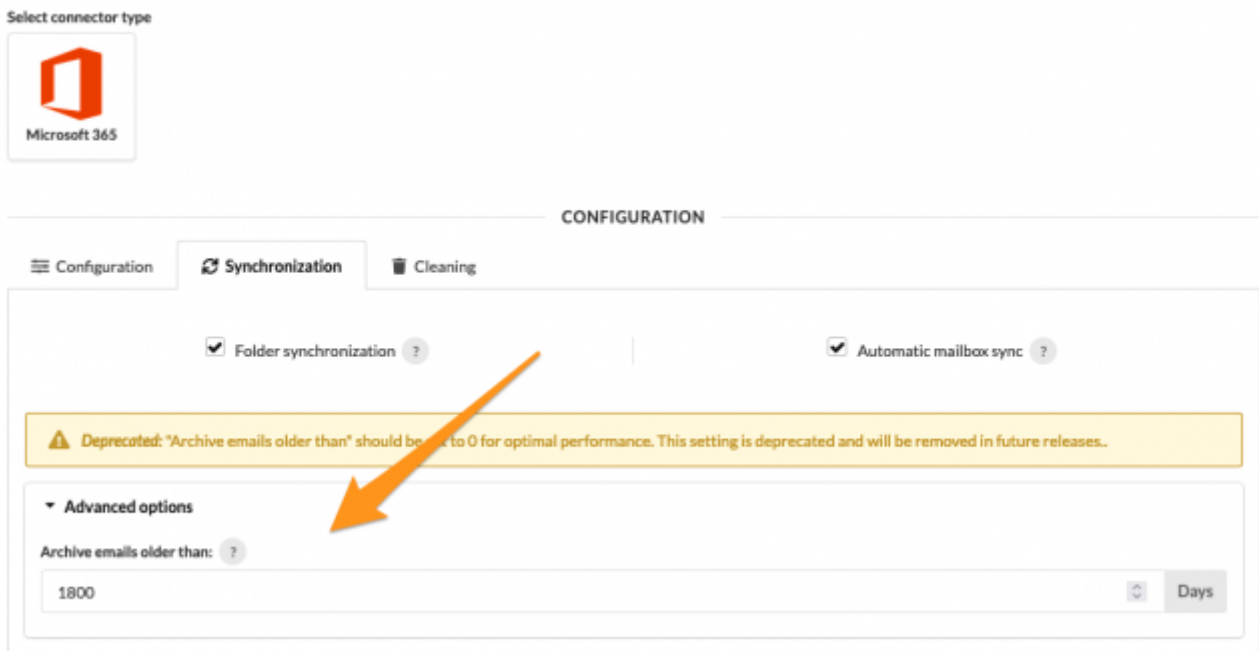
Improvements

- Improved mail forward to make it fully RFC compliant
- Moved reindex out of system disk and use /mnt disks instead
- Improved restore feature for Exchange mailboxes
- Hidden network settings for Libraesva's cloud Archivers
- Improved automatic configuration for Libraesva's cloud Archivers
- Improved folder structure dump disk usage and performances on folder structure volumes
- Prevent local user usernames from being modified
- For manually launched connector synchronization, show the list of skipped users
- Improved performance of volumes page
- Exchange connector is now more resilient to connectivity issues
- Added tenant information in OTP mail
- Added check on deletion mode type when configuring deletion rules on connectors
- Added pagination in notifications page
- Prevent Anacron emails to end up in deferred queue
- Improved directory service attribution during login
- Added mail source extra header (records the source of the import)

Deprecation notice

- The `archive older than` option for connectors, which was deprecated since the 21.3 release, **has been completely removed**. This applies to existent connectors, too. You can see if the option is active in each connector page (see picture below). If the advanced options are not visible, the `archive older than` option is not used.
- The security thresholds about disks has been changed. From this release on, an alert notification is triggered when a disk usage is more than 90% and archiving services stop

when a disk usage is more than 95% (99% for /mnt/disk disks).



"Archive emails older than" option

Prerequisite

- Updated indexing engine
The Libraesva Email Archiver 21.8 requires the new indexing engine to be installed.

Libraesva PhishBrain v1.0 Release Notes

Changes in PhishBrain 1.0.1757 (Oct 6 , 2025)

Changes

- Added text on Test button in campaign wizard's final step that explains what happens when test mail is sent.
- It is now easier check who reported the email in campaign summary.
- Some style changes on reset password page and email.

Bug fixes

- Fixed link that prevent the final landing page after the "fake" landing page in QR code campaigns.
- Fixed reset password page.

Changes in PhishBrain 1.0.1693 (Jun 17 , 2025)

Features

- **New: Users: Single Sign On using SAML for MS 365.** In Users section there is a new tab SAML, where it is possible to setup single sign on for microsoft 365 users using SAML. Check also the documentation at <https://docs.libraesva.com/document/how-to-setup-saml-for-365-entra-id/> to setup it.

Bug fixes

- Table rows hover have been standardised, if the elements are clickable the background will be highlighted and the cursor will become a pointer.
- When a scheduled campaign has an error and the campaign can not be started it shows the error status in the campaigns scheduled list and in the campaign summary page too (clicking the edit button from the list).
- The campaign summary page now provides links to documentation on how to setup sending IP and send domains and setup Microsoft 365 and Gmail Applications.

Changes in PhishBrain 1.0.1674 (May 27 , 2025)

Features

- Create new filtered list changed style, checkboxes became toggle buttons.

Bug fixes

- Fixed behaviour on addresses import that let user to import wrong email addresses. They are now validated and the user is warned if any address is wrong.
- Fixed file picker UI and text on addresses import modal.
- Pointers on new list are now standardised.
- In user section the microsoft 365 button is missing if you go in local users. Now it's fixed
- The new microsoft 365 connector is pointing to main tenant is you go in a subtenant; now this behaviour is fixed too.
- Fixed the menu selector relative to microsoft 365 user's section.
- Template lists filtered for private/owned did not produced expected results. Now it does.
- Campaign and User's statistics are now standardised.

Changes in PhishBrain 1.0.1628 (May 7 , 2025)

Features

- Enabled saas-relay cluster and worker in round-robin configuration.
- Admin can force users to change password (and eventually enable OTP) at next login.

Bug fixes

- Fixed the 0 value on % in pdf reports.

Changes in PhishBrain 1.0.1610 (Mar 27 , 2025)

Features

- **New: Exercises: a teaching feature on spotting phishing attempts.** It is now possible to create and send exercise campaigns.

Bug fixes

- Fixed several minor style issues on PhishBrain's UI.

Changes in PhishBrain 1.0.1541 (Feb 19, 2025)

Changes

Completely revamped user interface for Phishbrain! Here's what you can expect from this exciting update:

- **Say Goodbye to the Top Menu:** We've replaced it with an intuitive side menu for improved navigation.
- **Cleaner and More Readable Design:** Enjoy a sleek, modern look that makes everything easier to read.
- **More Responsive Interfaces:** The new UI is designed to be reactive and adaptive across various screen mediums.
- **Leveraging the Latest Bootstrap Version:** We've implemented the latest version of Bootstrap to ensure a smooth and visually appealing experience.

Changes in PhishBrain 1.0.1487 (Jan 27, 2025)

Features

- Username are now limited to alphanumeric chars and @ . _ - signs
- **New: Campaigns: auto send of report email when campaign ends.** It is now possible to send an email to a specified mail address when to campaign ends.
- **New: Domains: move domain to sub tenant.** It is now possible to create, verify and move a domain from a parent to sub tenant in case of multitenant account.
- **New: Users: Single Sign On MS 365.** In Users section there is a new tab Microsoft 365, where it is possible to setup single sign on for microsoft 365 users.

Bug fixes

- Fixed several minor issues and typos.

Changes in PhishBrain 1.0.1395 (Nov 21, 2024)

Features

- Changed styles in campaign wizard tables
- Added more informative flashes when some actions are done (i.e: forbidden actions, errors and so on).
- **New: Templates: added attachment capability to templates.** At the moment it is NOT possible to create or edit attachments.

Bug fixes

- Fixed several minor issues, typos and added fallbacks in checks.

Changes in PhishBrain 1.0.1262 (Jul 22, 2024)

Bug fixes

- Fixed several inconsistencies when users and admin tries to navigate in not their own sections
- Fixed typo in campaign wizard
- When a smishing campaign has been launched it is possible to see the real Delivery status

Changes in PhishBrain 1.0.1235 (Jul 11, 2024)

Features

- Improved performances on CI/CD
- Various optimizations on backend processes (i.e.: launching highchart, checking and managing saving files in directories)
- **New: Campaigns: filter list / re-target user** (when the campaign is completed it is possible to create a sublists from the list used for the campaign that just ended)
- **New: Campaign wizard step 2 list searchbar** (campaign wizard step 2 has a new interface and it's now possible to filter the lists using a searchbar)

Bug fixes

- Fixed bug that prevent the user to select too many templates in campaigns
- Fixed memory usage on templates data

Changes in PhishBrain 1.0.1160 (Jun 12, 2024)

Features

- Improved campaign assets data storage and retrieval

Bug fixes

- Fixed bug that prevent the tenant owner impersonating a sub tenant to send campaigns to sub tenant

Changes in PhishBrain 1.0.1149 (Jun 6, 2024)

Features

- Phishbrain passed to PHP 8.2 and Symfony 6,4; this led to the revamp of all the other packages and code for better security.
- **New** Templates can be cloned
- **New** Sub tenants can now send campaigns to tenant owner (parent tenant set this); also, parent tenant can impersonate and send campaigns to himself as parent
- missing timezone is shown under Suggestion card in dashboard

Bug fixes

- QR code in preview is now shown
- Azure/office365 list of addresses show now first name and surname the right way
- minor bugfixes in launch and deletion of a campaign
- OTP is back again
- Validation in WYSIWYG editor is displayed correctly

- You can't save a template with no selected language
- minor UI fixes

Changes in PhishBrain 1.0.859 (Feb 13, 2024)

Features

- **New** QRishing feature: available new placeholder to add phishing link as QRCode
- Improved address list CSV import interface

Changes in PhishBrain 1.0.802 (Jan 15, 2024)

Features

- Campaign with no redirect or page 404 are now redirected to the same domain of the phishing campaign website

Bug fixes

- Username can be anything and is not tied to email anymore
- Password enforcing rules check now at least one lowercase character too
- Fixed case when having a single target campaign with multiple template does not randomize the template

Changes in PhishBrain 1.0.777 (Jan 2, 2024)

Bug fixes

- Fixed missing custom logo in email and other branding issues

Changes in PhishBrain 1.0.763 (Nov 24, 2023)

Features

- Added template languages support for French, Spanish and German

Changes in PhishBrain 1.0.757 (Oct 23, 2023)

Bug fixes

- Fixed issue with domain verification during user creation

Changes in PhishBrain 1.0.752 (Aug 1, 2023)

Bug fixes

- Fixed user impersonation issue

Changes in PhishBrain 1.0.751 (Jun 27, 2023)

Bug fixes

- Fixed default timezone on new tenants and subtenants accordingly to node region

Changes in PhishBrain 1.0.745 (May 30, 2023)

Bug fixes

- Fixed missing PDF Report generation

Changes in PhishBrain 1.0.742 (Apr 18, 2023)

Bug fixes

- Fixed repeated campaigns issue

Changes in PhishBrain 1.0.740 (Apr 13, 2023)

Bug fixes

- Fixed misalignment between risk score counters and data shown in event type charts

Changes in PhishBrain 1.0.736 (Apr 5, 2023)

Features

- Improved import and managing of big address lists (> 1000 addresses)

Changes in PhishBrain 1.0.729 (Mar 29,

2023)

Bug fixes

- Fixed minor issues

Changes in PhishBrain 1.0.704 (Feb 24, 2023)

Bug fixes

- Fixed sms service issue

Changes in PhishBrain 1.0.684 (Feb 13, 2023)

Bug fixes

- Fixed occasional sms status “Errored”

Changes in PhishBrain 1.0.680 (Jan 16, 2023)

Bug fixes

- Reduced smishing url length in sms text (overall limited to 160 characters) to improve user available space

Changes in PhishBrain 1.0.671 (Jan 10,

2023)

Features

- Added detection of events originated by automatic scanning systems, added notification on the event and excluded from results processing

Changes in PhishBrain 1.0.666 (Dec 6, 2022)

Bug fixes

- Fixed timezone issue in reschedule action from campaign list

Changes in PhishBrain 1.0.662 (Nov 22, 2022)

Features

- Added timezone setting on User

Changes in PhishBrain 1.0.656 (Nov 4, 2022)

Bug fixes

- Improved portal performance and reliability
- Improved password recovery process
- Fixed editing of campaign scheduling properties when the campaign is already launched
- Improved default setting and localization consistent with selected node

Changes in PhishBrain 1.0.642 (Oct 17, 2022)

Features

- Improved teachable moment UI when displayed on mobile device

Bug fixes

- Fixed security issue when using custom URL redirect

Changes in PhishBrain 1.0.637 (Oct 3, 2022)

Bug fixes

- Fixed license check issue

Changes in PhishBrain 1.0.630 (Aug 30, 2022)

Features

- Improved UX while switching nodes on login page

Changes in PhishBrain 1.0.626 (Aug 23, 2022)

Features

- Ability to customize sender name (local part) in addition to sender domain in template (default: noreply@)

- Added query field to filter addresses in Google Directory address list synchronization
- Improved UX to discern between scheduled and repeated campaigns

Bug fixes

- Check branding logo format to prevent Print PDF issues

Changes in PhishBrain 1.0.611 (Aug 16, 2022)

Bug fixes

- Fixed public templates region sync issue

Changes in PhishBrain 1.0.608 (Aug 10, 2022)

Features

- PhishBrain is now multi-region.

New regional areas are available in the United Kingdom (uk.phishbrain.net) and the United States (us.phishbrain.net) along with the original Europe area.

New users can choose the region when they create an account. All data will remain within the chosen region. Current accounts in the European region cannot be migrated to other regions.

Note: links in PhishBrain emails are on a 3rd level domain related to the region. Example: uk.phishingdomain.tld. Landing pages are also have a regional 3rd level domain

Changes in PhishBrain 1.0.588 (Jul 28,

2022)

Features

- Added statistics CSV export by addresses/campaigns

Changes in PhishBrain 1.0.586 (Jul 20, 2022)

Bug fixes

- Fixed minor issues

Changes in PhishBrain 1.0.579 (Jun 22, 2022)

Bug fixes

- Fixed search issue on Campaign events

Changes in PhishBrain 1.0.578 (Jun 20, 2022)

Features

- Shown TOTP token during 2FA activation process below QRCode

Bug fixes

- Fixed Microsoft Graph query escaping chars issues in Office 365 connector
- Fixed error 500 on PhishBrian landing page

- Fixed visual inconsistency in campaign detail between overall values and data shown in event graphs by type
- Minor issues

Changes in PhishBrain 1.0.557 (May 4, 2022)

Features

- Added risk explanation on PhishBrain landing page. When risk category is set on template on PhishBrain landing page will be shown an explanation about what they missed to detect the phishing campaign, what threat they are facing and how to protect themselves (more info)

Changes in PhishBrain 1.0.546 (Apr 5, 2022)

Bug fixes

- Fix loading issue on activity list when show all items (per page) selected

Changes in PhishBrain 1.0.541 (Mar 30, 2022)

Features

- Added template details and preview images on campaign report PDF
- Added ability to export addresses statistics and risk data

Bug fixes

- Fix PDF report generation when customer is using his own logo

Changes in PhishBrain 1.0.530 (Mar 7, 2022)

Bug fixes

- Fixed template gallery privacy filter issue

Changes in PhishBrain 1.0.526 (Mar 1, 2022)

Bug fixes

- Improved performance in template gallery
- Minor issues

Changes in PhishBrain 1.0.515 (Feb 16, 2022)

Bug fixes

- Fixed issue while save customized template
- Minor issues

Changes in PhishBrain 1.0.511 (Feb 14, 2022)

Features

- Released “Submit as phishing” Outlook add-in to track campaign user’s ability to identify phishing awareness email

- License check and charge it (in case of *per sends* license) at message send time instead at campaign launch time. This allows you to close a campaign before all scheduled sends are executed without lose unused licensed sends
- Ability to select multiple templates on campaign wizard, each target from the list will randomly receive one of the selected templates
- Target lists (Google connector) ability to direct upload JSON file to populate service account data
- Campaign list, added *Scheduled* tab to show more clearly which campaign will be recreated by rescheduling
- Ability to create, with multiple selection, PDF report for specific user/campaign and send it via email
- Tuned risk score and considering campaign *Detection Difficulty*

Bug fixes

- Compatibility issues on Edge and Safari browsers
- Issue on adding private key for Google list service account
- Minor issues

Changes in PhishBrain 1.0.473 (Jan 24, 2022)

Bug fixes

- Already scheduled emails used to be sent even if the campaign was then set as manually completed, now the scheduled sending stops immediately when the campaign is set as completed
- The order of sending emails used to follow the order of the list, now it is randomized

Changes in PhishBrain 1.0.461 (Jan 19,

2022)

Bug fixes

- Improved UI on campaign activities grid
- Improved domain invalidation check

Changes in PhishBrain 1.0.442 (Jan 4, 2022)

Features

- New smishing campaign type (Phishing via SMS)
- Template type filter on template page
- Add NIST Detection Difficulty value on campaign details
- Recovery forgot password

Bug fixes

- Fix minor issues
- Improved performance on Stats grid
- Fix favicon

Changes in PhishBrain 1.0.369 (Dec 3, 2021)

Features

- Add new send domain *enelenergia.email*

Changes in PhishBrain 1.0.384 (Dec 1, 2021)

Features

- Add new send domain *a2a.email*

Bug fixes

- Fix compatibility issue while printing PDF report on Safari, Edge and Firefox browsers

Changes in PhishBrain 1.0.360 (Nov 22, 2021)

Features

- Add check to launch date and tracking timeframe consistency
- Add ability to change email address on user detail
- Add sort to risk score column
- Add preview generation to on custom templates

Bug fixes

- Fix multiple tracking of 'Open Email' events
- Ordered templates by newest
- Fix exclamation mark as password allowed symbols
- Fix minor issues

Changes in PhishBrain 1.0.264 (Oct 22, 2021)

Features

- Audit feature to log users activities

Bug fixes

- Fix campaign wizard test email differences on PhishBrain landing page respect campaign configuration
- Ordered templates by newest
- Fix minor issues

Changes in PhishBrain 1.0.239 (Oct 4, 2021)

Bug fixes

- Fixed minor issues

Changes in PhishBrain 1.0.226 (Sep 29, 2021)

Features

- Allowed to select what will happen once target click on email link or submit data on landing page
 - Redirect to blank page
 - Redirect to 404 Page Not Found
 - Redirect to Custom URL (URL must belong to a verified domain)
 - Classic PhishBrain landing page (eventually with teachable moment video)

- Added license assigned/used columns on tenant list

Bug fixes

- Fixed email static resources extraction issue
- Fixed missing translation in the template selection during the campaign creation wizard
- Increased OTP validation time window

Changes in PhishBrain 1.0.196 (Sep 21, 2021)

Features

- Improved image upload on template and email editor
- Improved CSV addresses list import with update ability on existing addresses

Changes in PhishBrain 1.0.190 (Sep 15, 2021)

Features

- Added user impersonation for tenant administrator
- Added NIST Phish Scale values on templates (Number of cues) and campaigns (Premise Alignment)
- Added code edit on template email and landing page

Bug fixes

- Fixed blank charts on user report PDF

Changes in PhishBrain 1.0.168 (Sep 1, 2021)

Features

- Added OTP activation suggestion badge
- Added activity and overall risk score charts on campaign page with print to PDF ability
- Added button in the lists of users and campaigns to open relative details

Bug fixes

- Minor issues and improvements
- Fixed logo and format in email notifications
- Fixed blank page on user report PDF

Changes in PhishBrain 1.0.138 (Aug 9, 2021)

Bug fixes

- Improved compatibility in address list CSV import
- Fixed broken images in phishing email when opened from Gmail interface

Changes in PhishBrain 1.0.123 (Aug 4, 2021)

Features

- Improved address list import from CSV file
- Implemented Two Factor Authentication (2FA) with One Time Password (OTP)

- Added ability to set custom teaching video
- Added ip address and user agent in campaign activities CSV export

Bug fixes

- Fixed Safari browser issue on campaign wizard
- Fixed page positioning in templates browsing
- Fixed teaching page inconsistency, localized texts and other improvements

Changes in PhishBrain 1.0.75 (Jul 27, 2021)

Features

- Add PDF report to risk score page
- Added template ranking (difficulty)

Bug Fixes

- Branding: allow removing your logo
- Click rate and Submit rate update issue

Changes in PhishBrain v1.0.0

First service release.

Libraesva EA v21.03: Release Notes

Changes in EA v21.03

Main Features

- New “report” feature to request a tenant statistic report
The report is an Excel spreadsheet with tenant usage information (emails and storage), per-user usage information (emails and storage), charts of usage over time (emails and storage)
- New native Zimbra connector
Uses the native Zimbra APIs to sync email, folders and for message restore
- Office 365 user delegation using custom schema extensions
A user can now be delegated to manage other mailboxes.
- Recipient-based SMTP listener authentication
The attribution to the tenant can be based on the recipient of the journal email. For example: journals delivered to `tenant1@archiver.mydomain.com` are attributed to `tenant1`, journals delivered to `tenant2@archiver.mydomain.com` to `tenant 2`

Features

- Delay update until all running jobs are completed
Automatic nightly system updates are postponed until all running import/export jobs are completed
- Automatically suspend services when engine disk usage is higher than 90%
In order to avoid data corruption, the archiver will stop ingesting more email if the disk is getting full. The administrator is notified in advance.
- Handle IMAP corrupted messages
Better support of less-than-perfect IMAP implementations
- Compress folder structure dump while preparing it
The backup of the folder structure requires much less disk space and reduces disk I/O
- Support mailbox-based licensing
Introduces a new license based on the number of mailboxes rather than on the storage size
- Compress logs to reduce engine disk usage
System logs are now stored in a compressed format reducing disk usage
- Add support for zip-based reindex

The granularity of the reindexing process is now higher

- Add tenant soft and hard deletion
Tenant deletion is performed through a quick soft-delete followed by a background process of hard-delete
- Add customer address list in tenant summary page
Besides showing the number of messages, addresses, listeners and connectors related to the tenant, now the tenant summary page can also list the addresses
- Add notification snooze settings
Notifications can be snoozed with a very high level of granularity
- Add support for additional data disks
The console menu allows to add disks to the Archiver VM
- Improve job error notifications and logging
More information available to the admin about job execution
- IMAP journaling skips duplicated, already imported, messages
After having verified that the message is actually already present in the archiver, the duplicate message is skipped
- Send notification on automatic index check failures
Index health checks are automatically performed and issues notified to the admin
- Keep historical, per tenant, disks usage and emails count statistics
Besides appliance-wide historical usage data, also per-tenant historical usage data is calculated and stored
- More logging for outlook-addin authentication failures and email parsing failures
Debugging these kind of issues is now faster thanks to more details provided to the admin
- Synchronization for a single connector can be launched
The admin can force a synchronization execution for a single connector, without waiting for the nightly sync
- Add message IDs dump to backup procedure to speed up the restore (and reindex) process
With this additional information in the backup, the restore is much faster
- Re-design SMTP listener configuration page
UI redesign for a better user experience
- Delegation support in outlook-addin
Delegated users can manage other mailboxes also from within the outlook-addin

Bugfix

- Fix user impersonation if user has a domain not configured under tenant domains
- Fix OTP token regeneration in tenant page
- Regenerate kerberos configuration after archiver update
- Use correct Content-Type header when downloading messages as msg, eml or pdf
- Remove : from folder struct dump file to prevent failures on SAMBA volumes
- Fix PST importer skipping folders starting with .
- Fix HTML email indexing not correctly handling invalid HTML emails
- Fix tenant selector keeping old selection even if it's no more valid

Improvements

- archiver update: stop if export jobs are running
- stop services if /var usage is higher than 90%
- improve IMAP connector memory managements
- skip IMAP corrupted messages
- limit maximum log lines shown in webinterface
- add appliance level OTP code
- improve folder structure creation
- improve user impersonation if user domain is not in tenant domains
- improve fix otp token regeneration
- improve SMB share volumes
- improve disk usage and indexes email stats collection
- disable connector cache if days filter is used
- improve kerberos configuration
- improve eml to pdf conversion
- improve html to text messages conversion
- add notification for failed jobs

Libraesva EA backend v20.5.3625: Release Notes

Changes in EA backend v20.5.3625

Features

- Microsoft 365 Graph connector: more improvements to performance and speed
- IMAP connector: improvements on expunge after delete messages.

Bugfix

- Folder structure dump: solved potential issue on data compression.

Libraesva EA backend v20.5.3426: Release Notes

Changes in EA backend v20.5.3426

Features

- More improvements to performance and speed of all connectors during periodic synchronization through improved process scheduling and resource management
- Improved connector logging to provide more information to the sysadmin
- Supporting archiving of huge email, up to the size of 150MB

Bugfix

- IMAP connector: Solved potential compatibility issues with some IMAP servers