- Fixed an issue where the SwissSignREST MPKI connector settings were not loaded in the Admin GUI.
- Updated the GlobalSign root CA certificate chain so that GlobalSign certificates can be issued correctly.
- Certificate orders via the SwissSignREST connector that are not issued in time are now kept as pending requests and completed later, preventing duplicate certificates.

Operating system:
- Fixed a regression in 15.1.0.1 where external DNS names could no longer be resolved after a local DNS zone was configured with the built-in DNS resolver.

Outlook Add-In:
- Removed the HIN ACS support from the COM Outlook Add-In, as HIN now provides its own software.

RestAPI:
- Fixed the error handling of PUT /v1/ssl, which returned an internal server error instead of the actual error message.
- Fixed PUT /webmail/domain/{domainName} failing with an internal server error when "Initial password via SMS" is enabled.

Rule engine:
- If signing or encryption is requested and no key material exists, a key or certificate is now generated automatically (and a local user created if necessary) instead of bouncing the message, provided automatic key generation and user creation are enabled.
- Fixed an issue in the make_lft() RuleSet function that occurred when an LFT had multiple recipients and only some of them were permitted to make the LFT.

S/MIME:
- If "Delete expired certificates automatically" and "Automatically check revocation status every day" are enabled, revoked certificates are now deleted automatically as well.
- Fixed an issue where the result of a CRL check did not override the OCSP check result, so revoked certificates were not marked as revoked.

Security:
- **Affected versions**: <15.1.1 · **CVE-ID**: CVE-2026-114424 · **CVSS Score**: 9.2
Description: Improper handling of replacement values in address replacement rules could allow a remote sender to execute arbitrary commands on the appliance if a ruleset uses values taken from the message as replacement.
Fix Description: The evaluation of replacement values in address replacement rules was hardened to prevent code execution.
- **Affected versions**: <15.1.1 · **CVE-ID**: CVE-2026-114425 · **CVSS Score**: 9.2
Description: Specially crafted attachment metadata in an incoming message could cause the Large File Transfer processing to read or delete arbitrary files on the appliance.
Fix Description: Attachment metadata received with a message is now validated before any file is accessed.
- **Affected versions**: <15.1.1 · **CVE-ID**: CVE-2026-114421 · **CVSS Score**: 6.9
Description: Insufficient input escaping in account lookups combined with missing validation in the password recovery process could allow an unauthenticated attacker to discover GINA accounts without a password and take them over.
Fix Description: LDAP filter values are now escaped, and the password recovery only asks registered users with configured security questions.
- **Affected versions**: <15.1.1 · **CVE-ID**: CVE-2026-114420 · **CVSS Score**: 8.3
Description: Insufficient input escaping in account lookups combined with missing validation in the password recovery process could allow an unauthenticated attacker to discover GINA accounts without a password and take them over.
Fix Description: LDAP filter values are now escaped, and the password recovery only asks registered users with configured security questions.

users with configured security questions.

- **Affected versions**: <15.1.1 · **CVE-ID**: CVE-2026-114426 · **CVSS Score**: 8.7
Description: The file upload interface processed request data before checking authentication, which could allow an unauthenticated attacker to exhaust disk space and worker processes.
Fix Description: Authentication is now checked before upload data is processed, and the upload size is limited.
- Removed the acceptance of PGP keys with user IDs that are not self-signed.
- PGP messages that are not actually encrypted (NULL encryption) are now detected and no longer marked as encrypted.

Virtualization:
- Added support for the QEMU guest agent (qemu-ga).

Webmail:
- Fixed an issue where GINA read receipts were only sent for the first recipient of a message sent to multiple recipients.

Hotfix release 15.1.0.1, 2026-09-29

Admin:
- Fixed internal server error in edit GINA domain page.

Feature release 15.1.0, 2026-09-28

(new in 15.1)

Admin:
- Improved monitoring of LDAP database growth to help detect abnormal storage increases before available disk space becomes critical.
- Improved tenant-specific administration so delegated administrators can access only the accounts associated with their assigned tenant.
- Added a connection test for external keyserver settings to simplify configuration verification.

Background tasks:
- Added improved administrator notification when an email backup cannot be completed.
- Added support for notifying communication partners about expiring certificates and facilitating certificate renewal.
- Extended disk-space monitoring to provide notifications when the LFM storage area approaches its configured capacity limit.

Database:
- Adjusted LDAP synchronization settings to improve operation on medium and large installations.

Libraries:
- Update OpenSSL to version 3.5.8
- Update OpenSSH sshd to version 10.4

RestAPI:
- Added auditing capabilities for REST API requests to improve traceability of API activity.
- Corrected an incomplete API definition for cryptographic certificate information.

Rule engine:
- Added message metadata that records actions performed during mail processing, allowing downstream applications to identify how a message was handled.

- Added PostgreSQL integration capabilities for Rule Engine custom commands, enabling controlled database lookups and updates for supported use cases.

Refactoring:
- Modernized the internal implementation used for certificate revocation checks.

Security:
- Updated internal command execution to use safer command-handling mechanisms.

- **Affected versions**: <15.0.6.1 · **CVE-ID**: Pending · CVSS Score: 9.9

Description: Insufficient authorization controls in a cryptographic management API could allow an authenticated user with limited permissions to perform operations beyond their intended scope, potentially affecting system-wide trust configuration.

Fix Description: Restrict access to the REST endpoint /crypto/rootca to MSP tokens.

- **Affected versions**: <15.1.0 · **CVE-ID**: Pending · **CVSS Score**: 7.1

Description: Insufficient output sanitization in the log viewer could allow specially crafted message data to execute unintended browser-side content when viewed by an administrator.

Fix Description: Escape all external data to prevent content execution.

Webmail:
- Corrected the styling of generated email notifications to ensure a consistent appearance.
- Added support for restricting file types that external communication partners can upload through GINA.

Patch release 15.0.7, 2026-09-02
(new in 15.0.7)
This release will be the last release in the 15.0 branch and enable the update to version 15.1.

Admin:
- Fixed an issue that could prevent a local user from being deleted when associated certificate revocation was processed.
- Fixed an issue that prevented time zone settings from being changed or saved correctly.

Background tasks:
- Improved handling and logging of previously running background processes, preventing overlapping processes from contributing to excessive resource consumption and system instability.

Cfgserver:
- Fixed an issue that prevented time zone settings from being changed or saved correctly.

Clustering:
- Fixed an issue in the connector.pl service which failed to stop first run injection connections.

Libraries:
- update OpenSSL to version 3.0.22 to address the following security findings:
  - CVE-2026-63072
  - CVE-2026-63076
  - CVE-2026-54874
  - CVE-2026-63074
  - CVE-2026-75803

- Fixed checking of authentication tags for empty ciphertexts for AEAD ciphers in CCM cipher mode.

Operating system:
- Updated SSH-related configuration and warning handling to avoid unnecessary warnings when displaying cluster member status.

RestAPI:
- Corrected the API documentation so requests generated according to the specification are accepted as expected.

Rule engine:
- Corrected temporary directory handling to ensure required processing data remains available while the Rule Engine instance is in use.
- Fixed an issue where generated LFT messages could be missing encrypted attachments due to incorrect output directory handling.
- Improved logging to provide a clearer explanation when a revocation check is intentionally skipped.

Security:
- **Affected versions**: <15.0.7 · **CVE-ID**: CVE-2026-84830 · **CVSS Score**: 8.6
Description: SEPPmail Secure Email Gateway before 15.0.7 contains a command injection vulnerability that allows authenticated administrators to execute commands with elevated privileges.
Fix Description: All affected values will be escaped not.
- **Affected versions**: <15.0.7 · **CVE-ID**: CVE-2026-84831 · **CVSS Score**: 7.7
Description: Under certain conditions, the authentication process could allow access before all required multi-factor authentication steps had been completed.
Fix Description: The authentication flow was tightened to ensure all required MFA checks are completed before access is granted.
- **Affected versions**: <15.0.6 · **CVE-ID**: CVE-2026-84832 · **CVSS Score**: 8.6
Description: A vulnerability in the processing of specially crafted input could potentially lead to unintended command execution in the affected component.
Fix Description: Additional validation and safer command-handling mechanisms were introduced to prevent malicious input from being executed.

Webmail:
- Corrected an issue where cached webmail data could be validated using an incorrect value, potentially preventing it from being processed correctly.
- Corrected session handling where certain values were not applied as expected, which could cause a session to remain in an incorrect state.

Hotfix release 15.0.6.1, 2026-07-22

(new in 15.0.6.1)

RuleEngine:
- fixed an issue where an undefined value prevented the message object from writing log entries to the mail log
- added direction detection for archived emails to ensure correct delivery handling

Patch release 15.0.6, 2026-07-21

(new in 15.0.6)

Admin:
- always use a valid time zone; the default is Europe/Zurich
- add a separate MFA input field as MFA no longer needs to be appended to the password

- add a separate MFA input field so MFA no longer needs to be appended to the password
- add Admin GUI authentication against an external LDAP server
- add a "Trigger AutoRenew..." button to the MPKI connector settings
- validate the System Object ID under System >> Advanced View >> Comment as a valid OID

Backup:
- add an additional corrupt database check before daily snapshot creation

Clustering:
- fix an issue where an existing CARP IP blocked the IP settings of a new cluster member
- prevent password rehashing when cluster members use different firmware versions

Libraries:
- update OpenSSH to version 10.4 to address the following security findings:
  CVE-2025-61984
  CVE-2025-61985
  CVE-2026-35385
  CVE-2026-35386
  CVE-2026-35387
  CVE-2026-35388
  CVE-2026-35414
  CVE-2026-59995
  CVE-2026-59996
  CVE-2026-59997
  CVE-2026-59998
  CVE-2026-59999
  CVE-2026-60000
  CVE-2026-60001
  CVE-2026-60002

- update OpenSSL to version 3.0.21 to address the following security findings:
  CVE-2026-45447
  CVE-2026-34182
  CVE-2026-45445
  CVE-2026-7383
  CVE-2026-9076
  CVE-2026-34180
  CVE-2026-42766
  CVE-2026-42770
  CVE-2026-45446

Logging:
- fix mail log date sorting that incorrectly used alphabetical order
- fix the displayed size of LFT messages
- improve handling of already running background tasks during DB-based mail log cache refresh
- no longer log access to missing X-headers

MPKI:
- improve CertCentral connector handling of input and REST errors

RestAPI:
- fix handling of undef/null values in the GET /system/ifaliasconfig endpoint
- fix access configuration for the /system/applySysconfig endpoint
- fix domain certificate uploads through the /crypto/domain/{domainName} endpoint
- fix issues in the GET and POST /ssl/csr endpoints

- fix issues in the GET and PUT /ssl/csr endpoints
- increase the REST call timeout from 300 to 900 seconds for long-running requests

RuleEngine:
- fix subject handling when the encoding is unknown
- bounce messages when signing is explicitly requested but cannot be performed
- send archive mail through deliver() to add ARC headers
- ignore MDC errors when the PGP message contains no MDC data

Webmail:
- fix automatic deletion of unregistered webmail accounts after the configured grace period
- fix a false-positive decryption result in the hashdecrypt function
- fix an issue where adding an attachment in the Webmail GUI cleared the To and CC fields
- fix time output in SMS logs

Patch release 15.0.5, 2026-05-30
(new in 15.0.5)

Admin:
- fixed an issue where a CSR could not be displayed in the detail view
- enforce new admin password after initial login
- check that the private key and the certificate match when importing an SSL certificate that was issued on the basis of a generated CSR
- disable all DNS local zone input field if "use DHCP settings" is selected

System Services:
- fixed an issue in the auto reocation process
- fixed failing ruleset generation at sartup on HIN appliances

Clustering:
- extend the connector service to support more complex cluster configurations

Logging:
- fixed an issue in the DB based logging when there are no entries in the database

MPKI:
- successful access to an EJBCA via SCEP

OpenPGP:
- switch crypto backend for Sequoia-PGP to provide support for legacy algorithms
- fixed an issue whereby a failed PGP decryption was treated as successful

RestAPI:
- fixed an issue in the /mailsystem/template endpint when adding templates/disclaimers
- fixed an issue in the /system/dns/localzones/{domainName} whith operation DELETE
- fixed an issue with setting a customers maximumEncryptionLicenses and maximumLFTLicenses settings
- fixed an issue with an empty response for Crypto/Keymaterial
- fixed an issue when creating a webmail user
- fixed an issue with a path parameter in PUT and DELETE of endpoint /mailsystem/manageddomain/{domainName}/group/{groupName}

Security:

- fixed a possible path traversal vulnerability in PDF generation, found by Infoguard (CVE-2026-8811). With the same vulnerability disclosure Infoguard found some SSH configuation issues for our update server.
- base64 encode all PGP decrypted content to prevent MIME structure injection
- refactor hashencrypt function, used by pwsend and cache mode, to use AES-256-CBC with PBKDF2 (CVE pending). Since we already had planned the refactoring, this function was also criticised by ETH.

Webmail (GINA):
- fixed an issue in the webmal password reset pro
- use PBDKF2-512 as password hashing algorithm (CVE pending). The old hashing algorithm was criticised in the ETH findings.

Hotfix release 15.0.4.3, 2026-05-11
(new in 15.0.4.3)

CfgServer:
- fixed an array access error in the Fetchmail module which caused the CfgServer to stop

OpenPGP:
- add all PGP allowed algorithms to Sequoia-PGP crypto policy to allow usage of old PGP keys

Webmail (GINA):
- fixed a SAML login issue which resulted in an "unexpected render Page" error

Hotfix release 15.0.4.2, 2026-05-08
(new in 15.0.4.2)

Database:
- fixed an issue which prevented the webserver for the LDAP encryption password input to come up

Interim Certificate Service:
- fixed an issue with interim cert process caused by a change of the DB schema

Libraries:
- update to OpenLDAP 2.6.13
- update to OpenBSD 7.7 errata 42
- update to OpenSSL version 3.0.20 to fix a list of security findings:
  CVE-2026-31790
  CVE-2026-28387
  CVE-2026-28388
  CVE-2026-28389
  CVE-2026-28390
  CVE-2026-31789
- update to Apache 2.4.67 to fix a list of security findings:
  CVE-2026-23918
  CVE-2026-24072
  CVE-2026-28780
  CVE-2026-29168
  CVE-2026-29169
  CVE-2026-33006

CVE-2026-33007
CVE-2026-33523
CVE-2026-33857
CVE-2026-34032
CVE-2026-34059

MPKI:
- Add support for static subject handling to SCEP

RuleEngine:
- fixed an issue with Sequoia-PGP which is able to create a freeze situation inside the kernel

Security:
- CVEs published for the vulnerabilities found by Infoguard and fixed in 15.0.4
  * Exposure of Sensitive Information to an Unauthorized Actor (CVE-2026-7864)
  * Local File Inclusion (LFI) and Arbitrary File Deletion (CVE-2026-44127)
  * Unauthenticated Remote Code Execution (CVE-2026-44128)
  * Server-Side Template Injection (CVE-2026-44129)
  * Missing Authorization in GINAv2 (CVE-2026-44125)
  * Insecure Deserialization (CVE-2026-44126)
- remove login redirect to prevent disclosure of session token information (CVE- pending)

Hotfix release 15.0.4.1, 2026-04-28
(new in 15.0.4.1)

RuleEngine:
- a missing waitpid() after fork() causes the system to run out of available PIDs which results in a system freeze

Patch release 15.0.4, 2026-04-24
(new in 15.0.4)

Admin:
- fixed "Copy to Clipboard" for the ruleset to prevent invalid indention characters
- fixed an error while saving SwissSign REST MPKI settings
- fixed an issue where "Delete From Mailqueue" deleted all mails in the queue, not only the selected
- fixed an issue with incomplete SNMP System Contact information
- fixed an issue where a customer admin could not see the customer's users
- added a per-customer user limit for the GINA account list
- removed GINA cleanup settings because they are now controlled per customer
- prevent deletion of GINA domains that are still in use and added a warning if messages exist for that GINA domain.
  Since GINA mails can only be decrypted by the GINA domain they were created for, deleting a GINA domain will make all its mails unreadable.
- added comment fields for users, managed domains, GINA accounts, GINA domains, and mail processing groups
- added an input under Mail System to add specific SpamAssassin settings

MPKI:
- fixed an issue with '+' characters in names
- added new Harica TLS certificates for HTTPS REST connections

Protectionpack:
- fixed an issue with the update process for unofficial ClamAV signatures when using a proxy

RestAPI:
- fixed an issue in the OpenAPI specification for the /crypto/rootca endpoint

RuleEngine:
- fixed the make_lft() function

Security:
- fixed several vulnerabilities found by Infoguard
  * Exposure of Sensitive Information to an Unauthorized Actor
  * Local File Inclusion (LFI) and Arbitrary File Deletion
  * Unauthenticated Remote Code Execution
  * Server-Side Template Injection
  * Missing Authorization in GINAv2
  * Insecure Deserialization

- fixed the next batch of vulnerabilities found by ETH Zurich
  We switched to Sequoia-PGP. For now, we will still support older and weaker algorithms. The next releases will gradually become more restrictive. We will inform you about the changes.

SOAP interface:
- fixed an issue in the attachment length calculation

Webmail (GINA):
- fixed an issue causing a "Proxy Error" when writing a mail in the GINA GUI
- fixed an issue in GINA account activation that caused an infinite loop
- fixed an issue in the ZIP download of mail written in the GINA GUI. The file names were encoded in base64.
- fixed an issue when replying to a GINA mail. After adding an attachment, the CC address field was shown.

Patch release 15.0.3, 2026-03-03

(new in 15.0.3)

Admin:
- hide the CARP password
- fixed an issue in the System settings where verification of the bind IP for the Admin GUI web interface failed
- fixed an issue with umlauts in webmail domain names

Backup:
- fixed an issue where a double quote (") in the backup password caused an encryption problem

Libraries:
- updated OpenBSD 7.7 to Errata 23

Logging:
- when the DB-based logging database is regenerated, we now show a proper message instead of an error notification
- fixed an issue in mail log rotation that caused the mail log to be rotated four times between 00:00 and 01:00

MPKI:
- restricted CN length to 64 characters in the SwissSignREST MPKI connector; also added a product check and the option to override pseudo-attribute handling and transliterate special characters
- added the new GlobalSign R45 Root and R45-based ICA to the GlobalSign certificates; you can add them to the list of trusted CA certificates by clicking "Add or update..." in the GlobalSign MPKI settings

RestAPI:
- fixed a bug in user creation where the user was not added to the specified groups

Security:
- fixed a possible path traversal issue found by Infoguard (CVE-2026-2743)

- next batch of vulnerabilities found by ETH Zurich, fixed
  * High: S/MIME Signature Additional Certificate (CVE-2026-29140)
  * High: Bounded Subject Tag Sanitization (CVE-2026-29141)
  * High: Plaintext secure-mail.html (CVE-2026-29142)
  * High: S/MIME Decryption Impersonation (CVE-2026-29143)
  * High: Unicode Subject Tags (CVE-2026-29144)
  * High: GINA State Confusion Account Takeover (CVE-2026-29139)
  * Medium: PGP Decryption Recipient LDAP Injection (CVE-2026-29131)
  * Low: ESWmail-Verify Bypass (CVE-2026-29132)
  * Low: UID Regex Bypass (CVE-2026-29133)
  * Low: GINA Domain Switch (CVE-2026-29134)
  * Low: Webmail Password Tag Sanitization Bypass (CVE-2026-29135)
  * Low: CA Notification HTML Injection (CVE-2026-29136)
  * Low: Long Subject Untagging (CVE-2026-29137)
  * Low: PGP Decryption Sender LDAP Injection (CVE-2026-29138)

SOAP interface:
- fixed an issue where a call to an undefined function caused an exception

Webmail (GINA):
- added more French translations
- added new HTTP headers
  * Documents (HTML)
    Cross-Origin-Opener-Policy: same-origin
    Cross-Origin-Embedder-Policy: require-corp
  * Static assets (JS/CSS/fonts/images/assest/... except mobiletest.css)
    Cross-Origin-Resource-Policy: same-origin
  * Logout response:
    Clear-Site-Data: "cache", "cookies", "storage", "executionContexts"
  * Legacy hardening:
    X-Permitted-Cross-Domain-Policies: none

Hotfix release 15.0.2.1, 2026-02-06

Libraries:
- update to OpenSSL version 3.0.19 to fix a list of security findings:
  CVE-2025-15467
  CVE-2025-68160
  CVE-2025-69418
  CVE-2025-69419

CVE-2025-69420
CVE-2025-69421
CVE-2026-22795
CVE-2026-22796

Patch release 15.0.2, 2026-01-06
(new in 15.0.2)

Admin:
- fixed an issue where enabling "Disallow insecure ciphers" caused an error when saving the GINA settings
- added new filter options for the "Mail currently in queue" list
- display the correct timezone in the GINA account detail view

Backup:
- fixed an issue in daily snapshot restore handling for full snapshots
- the configured postmaster email address is now used as the envelope sender for daily backups and digests

CA:
- certificates generated by the local CA now include the keyCertSign and cRLSign KeyUsage flags
- fixed an issue that prevented automatic renewal of certificates issued by the local CA

MPKI:
- SwissSign: given name and surname are only required for Gold products

RestAPI:
- fixed a filtering issue in the /crypto/user/{email} and /crypto/domain/{domainName} endpoints
- fixed the /customer endpoint to allow empty strings for maximumEncryptionLicenses and maximumLFTLicenses

RuleEngine:
- fixed an issue in the header reprocessing mechanism that inadvertently changed the "next rule" value this mainly caused issues with HIN decryption, where successfully decrypted mail was handled as unsuccessfully decrypted
- fixed an issue where parsing a MIME-decoded email address caused an "invalid mail address" error
- added the correct mail size for LFT bypass attachments
- log all explicit header changes (add, set/replace, delete)

System Services:
- frontend systems now clear the local GINA cache

Webmail (GINA):
- fixed issues affecting mainly French translations in the GINA GUI
- re-added mobiletest.css; its absence prevented older GINA mails from opening
- log the X-Forwarded-For header for all web accesses
- improved cache link access speed for S3 storage
- defang form tags in GINA mails in the GINA GUI
- fixed an issue where some text in GINA mails was duplicated

Patch release 15.0.1, 2026-01-06

(new in 15.0.1)

Admin:
- added the ability to disable Vioscsi on non-QEMU and non-Nutanix systems
 Newer Nutanix installations do not have a problem with Vioscsi but on older installations it will result in a hanging VM during boot for ~2 hours.
 To prevent this, disabling Vioscsi before migrating to Nutanix will be a good idea.
- fixed an issue in the GINA domain view when disabling the "Use settings from master template" setting would allow saving invalid values
- fixed an issue with the manual license import
- added "use UTF-8 encoding" setting to SMS settings for HTTP_GET and XML mode
- allow import of S/MIME certificates with RSASSA-PSS, RSA-OAEP, RSAES-OAEP and ECDSA key type
- suppress notification of missing seconds disk for database snapshots on hardware appliances >= 1000B because they have an LFT partition on the first disk
- set minimum password length to 16 on BSI mode appliances
- add a warning in the Admin GUI and prevent switching to DB based logging if there is not enough space available on the Device's log partition

CfgServer:
- added "Autorenew" and "Autorevoke" prefix to auto-renew and auto-revoke log output

Clustering:
- fixed the "backend failover" handling, the situation when a frontend loses its backend

Logging:
- fixed an issue with the DB based log cache generation where a not deleted flag file lead to unspecified behaviour
- better notification messages in case of an empty mail log filter result
- SMTPd.pl will write its error log to /var/log and no longer to /tmp which will prevent the deletion of the logfiles on restart
- the mail log is rotated at least once a day to provide a time-based search window of at least one day

Mail transport:
- enable "Require TLS encryption" by default in BSI mode

MPKI:
- check for SwissSign domain certificate generation if the certificate's CN is not longer than 64 characters
- added ability to transliterate special characters and umlauts to avoid problems with non-ASCII character for the HARICA MPKI connector
- add setting to enable and disable the auto-revocation process of user certificates

Reporting:
- fixed an issue with the nrpe_telnet_static test

RuleEngine:
- relaying behaviour for outgoing and internal mails over submission port is now the same
- fixed an issue in the textual RuleSet generation
- added special handling of Incamail test email address mta@check.incamail.ch

Security:
- closed several vulnerabilities

(thank you to Andris Suter-Dorig working under the supervision of Matteo Scarlata and Prof. Kenny Paterson from the Applied Cryptography Research Group at ETH Zurich)

System Services:
- added a keep-alive check for the support connection to prevent unexpected disconnects, primarily in Azure environments

Webmail (GINA):
- fixed an issue where the GINA accounts' login history was not being cleaned up
- show company logo in pwsend.ap
- disable available size check for S3 storage in cache mode
- remove account's name from pwsend_smstext

Feature release 15.0.0, 2025-11-04
(new in 15.0)

Admin:
- fixed "Save and apply all" button in the advanced system settings
- added the ability to regenerate DKIM and ARC keys
- added the option to skip user certificate revocation when deleting a customer
- fixed an issue where language settings of a Webmail Domain were not saved

Libraries:
- Apache version: 2.4.63
- ClamAV version: 1.4.2
- Dovecot version: 2.3.21.1
- Fetchmail version: 6.4.39
- LibreSSL version: 4.1.0
- OpenBSD version: 7.7 Errata 14
- OpenLDAP version: 2.6.9
- OpenSSL version: 3.0.18
- GPG version: 2.4.7
- Perl version: 5.40.1
- Postfix version: 3.10.1
- OpenSSH version: OpenSSH_10.0, LibreSSL 4.1.0

Logging:
- added the logging of the X-Forwarded-For header for webmail accesses

Mail transport:
- added the option to disable client certificate verification for submission port

MPKI:
- added the ability to issue new domain certificates via the SwissSign CMC MPKI connector
- added Harica MPKI connector
- added SwissSign REST based MPKI connector
- added auto revocation of user certificated for users who are no longer licensed (manually or by 90 days inactivity)
- given name and surname are no longer mandatory for SwissSign Silver products

RestAPI:
- corrected the User List for License Limiter number
- added encryption policies endpoint

- added the ability to import a non-multi-customer backup as new customer
- delete all managed domain references if managed domain is deleted

RuleEngine:
- added two functions to the ruleset: make_lft() for enforcing LFT and revert_lft() for reverting LFT
- added function getuserattr() to read user entry specific attributes into variables
- enhanced memory consumption of CSM module
- add important headers X-SM-outgoing, X-SM-incoming, X-SM-internal, X-SM-encrypted and X-SM-decrypted via RuleEngine, not RuleSet

System Services:
- set revoked root CA certificates to state untrusted

Webmail (GINA):
- fixed an issue where invalid login attempts were not recorded when internal authentication was active
- removed the functionality to use client certificate authentication
- added meaningful return messages for the file.app when a LFT bypass upload failed

Patch release 14.1.4, 2025-10-01

(new in 14.1.4)

This release will be the last release in the 14.1 branch and enable the update to version 15.0.

Admin:
- fixed a bug in the support console menu's when setting routes
- if no password for the system support user has been configured go back to the old behaviour and use the default password
- fixed an issue in a script that caused the process to abort when adding a new cluster member, leaving an inconsistent cluster configuration

Libraries:
- update to OpenSSL 3.0.18

Licensing:
- since the end of September, we have switched to a new update and license server. In rare cases, delays may occur

Logging:
- fixed a log rotation issue that caused the maillog index to not be generated
- show the Log-view even if there is a DB error in DB based logging

MPKI:
- fixed another issue with spechial characters for thr GlobalSign MPKI connector
- fixed a TLS connection issue of the DigiCert MPKI connector
- fixed an issue with the DigiCert Connector where the default value of the fullname regex was not used in the domain specific settings

RestAPI:
- fixed the schema definition for authtoken objects for Webmail user

RuleEngine:
- fixed the handling of ED25519 keys for ARC
- remove MIME epilogue befor adding S/MIME signature

System Services:
- added check_smtp command for nrpe

Webmail (GINA):
- added autocomplete=off for E-mail and Password on the Webmail login page
- fixed an issue where selecting search jumped to the profile settings
- fixed an issue in the password reset process where the given phone number was ignored
- removed the mechanism in the secure-email attachment to check the current environment, to allow Edge browsers in iOS to open the attachment

Patch release 14.1.3, 2025-08-26
(new in 14.1.3)

Admin:
- fixed an issue where the Blocked Mails log could not be shown
- add missing table heading in customer overview
- fixed search filter in Domain Certificates view to only search for SEPPmail Managed Domain Service domains
- fixed an issue in the SSL request page where a wrong regex created an invalid list of country codes
- added ability in the Cluster view to specify the cluster's maintenance node
- Admin Email field is now mandatory for webmail domains

Libraries:
- update to OpenSSL 3.0.17

MPKI:
- some rectifications for the new SectigoEU MPKI connector
- fixed some UTF-8 encoding problems in the SwissSign CMC MPKI connector
- fixed an issue in the DigiCert MPKI connector where the full name regex could not be found
- adjustments for the GlobalSign MPKI connector to correctly handle the CommonName information

RestAPI:
- fixed an issue where a typo prevented the API to reset the password of a webmail account
- fixed an issue where the GET request for the certificates of managed domains returned an empty array
- fixed an issue with processing managed domain deletion that caused all extended fields to be deactivated
- general maintenance

RuleEngine:
- fixed an issue in the user creation code where an email with a leading whitespace caused the RuleEngine to reject the email address
- added a timeout of 5 seconds for LDAP keyserver searches

System Services:
- added a system status message when unofficial ClamAV signatures could not be updated

Webmail (GINA):
- fixed an issue where the anonymous key search was not displayed in the login screen
- implemented a new LFTAuthToken rotation mechanism
- added possibility for line breaks in SMS templates
- when resetting the password via SMS, 3 SMS messages can now be sent (instead of 1 SMS) before the user has to contact support
- specifying an incorrect file size during a bypass upload no longer results in the uploaded data being silently discarded

Hotfix release 14.1.2.1, 2025-08-04

System Services:
- prevented race conditions between two tasks that would otherwise terminate each other and thereby prevent the watchdog from running

Webmail (GINA):
- fixed an issue to allow anonymous certificate search

Patch release 14.1.2, 2025-07-30
(new in 14.1.2)

Note: Version 14.1.2 will most likely generate new Diffie-Hellman parameters after the update, which may take up to 20 (or more) minutes.

Admin:
- added check if swapctl fails in Administration>>System Update page

Database:
- added daily snapshot restore to support console menu
- save parsed ASN.1 data and information of X.509 certificates to speed up certificate handling

Logging:
- fixed an issue with the logrotation where a missing HUP signal did not restart the syslog daemon

MPKI:
- added given name, surname and pseudonym handling for DigiCert/CertCentral MPKI connector
- fixed an issue where the certificate generation triggered by the RuleEngine failed because of an incomplete DN
- fixed "method not found" bug in GlobalSign MPKI connector
- fixed DigiCert/CertCentral skip_approval problem
- added new Sectigo EU MPKI connector

RestAPI:
- fixed customer import by REST
- fixed an issue in the password reset via SMS endpoint which caused a re-registration of the user
- SSL endpoints added that cover the SSL area of the Admin GUI

RuleEngine:
- added triple wrapping for encryption policies (if activated)
- better detection of attachment file names for script detection to prefent false-positives

Webmail (GINA):
- fixed an UFT8 character issue in the "Download all attachments" function
- fixed an issue where styles were not replaced correctly in GINA mails
- fixed an issue where a wrong placeholder lead to wrong texts in GINA password mails
- implemented a redirect after login to prevent caching of credentials
- fixed several potential security issues in file.app

Hotfix release 14.1.1.2, 2025-07-03

Logging:
- fixed an issue in the logrotation code where an error was thrown because of a non-existing PID file

Webmail (GINA):
- fixed an issue where unintentionally too many generated LFMKeys lead to an LDAP overload because every LFMKey object did an LDAP bind

Hotfix release 14.1.1.1, 2025-06-27

GUI Alert regarding new update mechanism

For many customers, there is currently an alert in the SEPPmail Secure E-Mail Gateway GUI with the text "We are changing to a new update mechanism for SEPPmail appliances. Connection attempt to new server failed - please make sure this device is able to connect via port 22 to 94.130.170.135. (This message will vanish as soon as the successful connection has been made.)"



Explanation: SEPPmail is preparing the migration of the licence and update server (LuS) from Neuenhof in Switzerland to the new LuS called Kronos in the Hetzner data centre in Germany. This is a Kronos connection test, which performs a simple ssh access from the respective SEPPmail Secure E-Mail Gateway via IP address to Kronos via IP.

As the corresponding Firewall rules are IP-based for most of our customers, this test is explicitly IP-based. The FQDN (targets update.seppmail.ch and support@seppmail.ch, see Setting up the firewall / router) will not be changed until the changeover date.

As soon you open the access from your SEPPmail Secure E-Mail Gateway to the specified IP 94.130.170.135 via port 22 SSH, the message will disappear.

Admin:
- fixed an issue in the clone device script

System:
- fixed a syntax error in root's crontab that prevented cron jobs from being executed

Patch release 14.1.1, 2025-06-24

(new in 14.1.1)

Admin:
- fixed an issue where the account password complexity settings for a webmail domain could not be saved
- fixed an issue that prevented user settings from being saved
- fixed an issue where read-only admins could not use the mail log filter
- added a message history table to the webmail (GINA) account details view

Backup:
- only one cluster member will now perform the database backup

CfgServer:
- fixed an issue in password handling for additional smarthost credentials
- ensure that the [default] and [none] customers are created

Logging:
- suppress false-positive MPKI error message in daily digest
- fixed a potential race condition in mail log cache creation for db-based logging when log file rotation occurs during cache generation

MPKI:
- added a space between the pseudo tag and value for SwissSign certificate generation
- added support for given name, surname, and pseudo fields in the GlobalSign mpki connector

RuleEngine:
- improved error logging for S/MIME signature verification failures

Feature Release 14.1.0 (Released 2025-05-27)
(new in 14.1.0)

Additional Services:
– keyserver now supports LDAP filter attributes
– add additional locking in expired LFM message cleanup to prevent race conditions in a cluster setup
– move monitoring of cluster LDAP connections from watchdog into the responsible connector service

Admin:
– added the ability to copy the ruleset to the clipboard
– added the option to set the MTU during initial network setup
– added a "copy log entry" button to copy all relevant information to the clipboard
– added hint and progress information in the admin GUI after switching from file-based to database-based logging
– added the ability to select the update channel
– removed postscreen settings from the admin GUI as they are no longer used
– unified settings for CertCentral and DigiCert MPKI
– implemented certificate chain validation before import, including expiry date checks
– introduce maintenance node attribute. In a cluster setup some tasks only have to run once and not on all cluster members.
The member with the maintenance node setting will be responsible for this kind of tasks.

Logging:
– improved verbosity of startup logs
– enhanced logging for service scripts

MPKI:
– adapted SwissSign MPKI connector to use surname, given name, and pseudonym attributes

RuleEngine:
– added more meaningful log messages indicating whether an encryption policy was applied

RestAPI:
– added /mailprocessing/processmail endpoint

– added endpoints for ruleset configuration
  - /mailprocessing/ruleset
  - /mailprocessing/ruleset/upload
  - /mailprocessing/ruleset/misc
  - /mailprocessing/ruleset/settings
– added /webmail/user/smshistory endpoint
– completed implementation of the /webmail/domain endpoint
– added partial match support for GET /webmail/user requests

System:
– all appliances will become multi customer systems

System Services:
– added MAILTO="" to crontab to suppress cron job email notifications

Webmail (GINA):
– fixed an issue with local LFT storage synchronization, which failed to delete messages older than the configured retention period
– added support for multiple seppmailSymmkey attributes for webmail accounts, allowing customer merges without losing access to encrypted messages
– password reset emails are now signed
– added SMS statistics for webmail accounts
– introduced the "virtual mailbox" feature
– enabled hard encryption for cached links to prevent decryption errors in cluster setups with different SSL certificates on cluster members

Patch release 14.0.7, 2025-05-27
(new in 14.0.7)

This release will be the last release in the 14.0 branch and enables the update to version 14.1.

Admin:
– fixed an issue where the user password policy settings were not saved
– added guidance to the update page to assist with checking resource requirements

CfgServer:
– fixed an issue on systems with disabled GINA GUI where the GINA mail encryption could not access necessay files

Reporting:
– remove empty addresses from the list of recipients before sending the daily digest to prevent mail format errors

RuleEngine:
– fixed an issue with the parsing of DSN Notify entries

Webmail (GINA):
– fixed an issue with the "lft used" functionality which caused to always ignore LFT settings

Patch release 14.0.6, 2025-04-30
(new in 14.0.6)

System:
- OpenBSD 7.5 Errata 25

CfgServer:
- fixed typo in mail template apply which prevented a cluster wide apply

RestAPI:
– implemented periodic restarts of ResAPI workers to reduce memory consumption
– fixed an issue in the /info/encryption endpoint where expired domain certificates were ignored
– fixed an error in the /statistics/license endpoint where incorrect user counts per customer were returned
– fixed an issue in the /webmail/domain endpoint where the "password recipient" could not be set to "last sender"
– fixed an issue in the /webmail/domain endpoint to handle "multiple cluster assigned to domain" situations
– added publishLocalCA to POST and MODIFY of the /webmail/domain endpoint
– /crypto/*: add the mail address used for the import of keymaterial to the imported key
– /crypto/*: add "public" query-parameter for GET and POST

RuleEngine:
– ensured that the ARC chain is always validated

Webmail (GINA):
– fixed a security issue in GINA's "Download as PDF" feature
– fixed an issue with UEP emails where the initial password length was set to 0
– fixed an issue where the total size of a GINA message was miscalculated, leading to error situations
– implemented periodic restarts of web.app workers to reduce memory consumption

Hotfix release 14.0.5.1 2025-04-04

Additional Services:
– fixed issue in supportconnection script which prevented the support connection from being established
– fixed device ID generation to prevent ID collisions
– watchdog will now check for running ssh-daemon

RuleEngine:
- fixed Runtime Error in HIN-Connector code

Patch release 14.0.5, 2025-04-01
(new in 14.0.5)

Libraries:
- update to OpenSSL 3.0.16
- update to nrpe 4.1.3
- update to samhain 4.5.2

Admin:
- Fixed an issue on the customer overview page where the number of GINA accounts and valid S/MIME certificates was not displayed.
- Fixed an issue in the log view that prevented customer admins from seeing log entries for their managed domains.
- Fixed a bug in notifications and warnings (daily report) for version 14.0.2.2.

- Added the ability to push SSL and CA certificates from frontend systems to cluster members.

Additional Services:
- Added a timeout for mdb_copy checks to prevent infinite loops.
- Fixed an issue in the ldapproxy filter string handling by using the baseDN for searches.
- Fixed an issue in the watchdog that caused an incorrect retrieval of "keyserver.enabled".
- Fixed an issue in fetchlicense that prevented the system from fetching a license.
- cleanCache now only runs once a day.

MPKI:
- Prevented certificate autorenew from stopping after three consecutive errors.

RestAPI:
- Fixed an issue in the /v1/info/encryption endpoint on HIN systems.
- Fixed a problem in the statistics endpoint.
- The backend now only starts if REST is enabled.
- Restart the backend process after every 100 connections to free memory.

RuleEngine:
- Added the option to specify the GINA domain in webmail_keys_avail() and webmail_keys_gen().

Webmail (GINA):
- Dynamically set the footer's position to prevent it from being partially off-screen.
- Fixed cache mode cleanup for never-expiring cache links.
- Fixed an issue with the password reset functionality.
- Switched to using POST requests in preview.app.
- Improved the alignment of input field labels.
- Added streamed ZIP download functionality.
- Fixed an issue in the S3 backend where the chunked download range overlapped.
- Fixed an issue with UEP mails that unnecessarily requested a mobile number.
- Fixed an issue with encoding attachment names in file.app.

Patch release 14.0.4, 2025-02-25
(new in 14.0.4)

Admin:
- fixed an issue where not all actions applied to an email were displayed in the DB-based log view
- RestAPI secrets will now be stored as SSH512. As a result, the secret can only be viewed when initially generated
- the S3 connectivity and speed test now correctly displays results in minutes and seconds

Additional Services:
- fingerprintd will no longer run on frontends and will be monitored by the watchdog
- the transferLFMarchives script will now check for a valid LFT license to prevent unnecessary log entries in the system log
- slapd will now be limited to a maximum of 32 threads
- adjusted log rotation 'when' for MPKI error logfile
- fixed another issue with filter string handling in the ldapproxy

Cluster:
- removing a cluster member will now trigger the regeneration of the slapd configuration file on the remaining cluster members to prevent synchronization attempts with the removed member

RestAPI:
- fixed an issue with the attribute name for serverSideCaching

RuleEngine:
- better detection of almost existing and registered Webmail accounts to prevent the RuleEngine to complain about not being able to create already existing accounts
- fixed filter escaping in both customer account searches and customer searches
- added better detection for PGP/MIME encrypted emails

System:
- increased the number of inodes in /var/run to handle more files
- implemented log rotation for watchdog.log

Webmail (GINA):
- use storage abstraction layer for every webdomain separately, resolving issues with LFT mail attachments not expiring on S3 storage
- increased the number of allowed connections to the Webmail GUI for improved responsiveness
- cache mode will use /tmp for cache size files
- fixed an issue with not working preview in the Webmail GUI
- Webmail's directory structure will no longer be generated if Webmail is not enabled
- fixed an issue where changes to the language settings for "Insecure Mail Text" were not being saved
- added support for specifying a URL for the metadata XML of a SAML IdP; this URL will also be used to update the XML file automatically once per day
- fixed two penetration test vulnerabilities in web.app

Patch release 14.0.3, 2025-01-28
(new in 14.0.3)

A happy new year to all. We skipped the New Year's Eve release on 2024-12-31 and will now continue to release a patch release on every last Tuesday of the month. The most important issues we are currently working on are PGP encryption/decryption issues, DB corruption problems and the new GINA.

Admin:
- removed irrelevant but annoying error message about not receiving extended system fields due to missing domain name when adding a managed domain
- add a hint in the Admin GUI that the change of the domain name requires a restart
- fixed an issue in the DigiCert CertCentral MPKI connector configuration that prevented users from deleting domain-specific parameters

Additional Services:
- fixed an issue in mailgraph.app where a corrupted statistics database could cause Statistics.pm to delete /dev/null
- the web.app is no longer restarted after the rotation of the SEPPMaillog logfile
- added LDAP database corruption checks
  If a corrupted LDAP database is detected, the administrator will receive a watchdog email, and all further backups and daily snapshot creations will be halted.
  This ensures that the last working backup is not overwritten by a faulty one.
- fixed an issue with filter string handling in the ldapproxy

CfgServer:
- fixed an issue with not escaped LDAP filter values in the daily digest generation

RuleEngine:

- fixed an issue where the last header of a mail was not processed by the RuleEngine
- fixed an issue with enabled ExO relaying that allowed an external tenant to relay emails to another external tenant through the appliance

Webmail (GINA):
- fixed an issue where temporary LFT-related files were saved in the wrong folder, causing session cleanup issues
- fixed an issue with the handling of initial password emails when the initial password length is set to 0
- fixed an issue with the "Powered by SEPPmail" link in the new GINA
- fixed an issue with the reply-to-all function.
  When sending a reply-to-all email, we now verify that all recipients can receive an encrypted email. To qualify, recipients must have one of the following: a GINA account, a personal public S/MIME certificate or PGP key, a domain public S/MIME certificate or PGP key, or support TLS encryption. Previously, only GINA accounts and personal public S/MIME certificates or PGP keys were checked. As a result, recipients with, for example, domain encryption were incorrectly flagged as "not possible to encrypt" and therefore rejected.
  This issue has been resolved by including all supported encryption mechanisms in the check.
- we now dowload LFT attachments for the ZIP download in parallel to speed up the overall download process

Hotfix release 14.0.2.2, 2024-12-07

Apologies for the necessity of the next hotfix release, but the changes to favour OpenSSL introduced some issues which had to be fixed quickly, especially the creation of CSRs and the handling of P7 data in a MPKI connector response. The reason for this change of the default behaviour was that LibreSSL has some problems to parse the validity dates in X.509 certificates.

SSL:
- explicitly set default_md to sha265 for all kind of requests and prevent unsupported parameters for openssl calls. PKCS12 exports will no longer use des3.

Webmail (GINA):
- fixed an issue with the download of searched certificates

Hotfix release 14.0.2.1, 2024-11-29

Database:
- adapt the number of threads used by LDAP to the number of available CPU cores

Network Services:
- add the complete list of MIB files to fix some snmp issues

RuleEngine:
- use OpenSSL in favor of LibreSSL because LibreSSL sometimes has problems to parse the validity dates in X.509 certificates

Webmail (GINA):
- fixed an S3 issue where the message metadata were not written to the database
- fixed an issue where the new GINAv2 was always configured in httpd.conf for non-virtualhosting GINA domains

Patch release 14.0.2, 2024-11-26

(new in 14.0.2)

Admin:
- fix issue with backup/restore where the "Keep current system settings instead of restoring them from backup" failed with empty current settings

Additional Services:
- implemented a better filter attribute parsing for the LDAP key proxy

Backup:
- fixed an issue where the customer backup could be sent up to 80 times per day

RuleEngine:
- fixed an issue where a bad charset decoding causes the RuleEngine to bounce an LFT message
- prevent CAs with a wrong ASN.1 encoding to be added to the trusted CA file
- fixed an issue where no more Extended Fields could be added

Webmail (GINA):
- fixed an issue where language selection did not work
- fixed an issue where the mobile number was always a mandatory input fild in the registration process
- connector service and bypass LFT issues (was: File App request denied - unable to load api session > Message Rejected. (431 Secure E-mail gateway exception - encryption failed) [Not secured by HIN])
- fixed an issue the registration date was not set for self registered users
- fixed an issue in the self registration process where the registration was rejected because of a missing security question/answer, even if no question/answer was necessary
- add random "Server" header to disguise the user server version
- only return certificates/keys in the certificate/key search with the ability to decrypt mails
- fixed an issue where the password reset mail could not be sent to the last sender

Patch release 14.0.1, 2024-10-29

(new in 14.0.1)

Admin:
- fix an issue where the GINA account menu would not load
- fix issue where multiple internal server errors were occurring due to missing internal system extended fields
- fix issue where details were not loading in the new DB-based log view
- fix issue where the daily customer backup was not sent
- fix an issue in mailgraph.app that caused an error when creating the statistics graphs and also prevented the daily digest from being sent
- added MPKI connector errors for certificate generation to the daily digest

RuleEngine:
- added ability to check CA validity for certificates found on a remote keyserver
- use size of uploaded bypass LFT attachments for LFT quota calculation

Mail transport:
- fix issue with mails injected by fetchmail

Webmail (GINA):
- force mandatory fields in the registration form as required
- do not show SMS PIN confirmation field if not required
- fix issue with searching for user certificates

- fix issue with domain certificate download

Hotfix release 14.0.0.1, 2024-10-09

Webmail (GINA):
- fix issue with not working SAML login button in Webmail GUI

Feature Release 14.0.0 (Released 2024-09-24)
(new in 14.0.0)

Major changes:
- OpenBSD 7.5 as system base errata 10

System:
- add the ability to view, add and delete routes in the support consolemenu
- Apache version: 2.4.59
- ClamAV version: 1.4.0
- Dovecot version: 2.3.21
- Fetchmail version: 6.4.37
- LibreSSL version: 3.9.0
- OpenLDAP version: 2.6.7
- OpenSSL version: 3.0.15
- GPG version: 2.4.4
- Perl version: 5.36.3
- Postfix version: 3.8.6
- OpenSSH version: OpenSSH_9.8, LibreSSL 3.9.0

Admin:
- when changing the IP address of the appliance, check whether the IP address is already being used by a cluster member
- fix missing close "X" for modals
- added account status filter to Webmail account search
- logview for CfgServer log and added filter and limit options for system, audit and CfgServer log
- ability to import P7B files as response after CSR creation
- one-time option to download the private SSL key after the SSL certificate has been generated
- add ability to to set a validity time range for manual blocklisting / welcomelisting entries
- added the ability to specify the From-address for watchdog emails
- added the need to enter a security code before an update can be triggered in the Admin GUI
- added ability to set system support user's password (not the support user in the LDAP)
- added "Certificate expires on" row to the domain_stats.csv
- add Message-ID to backup emails
- update external libraries: jquery 3.7.1, bootstrap 5.3.3
- prevent mailgraph.app access whithout active login
- more audit logs for changes done in the Admin GUI

RuleEngine:
- add ability to specify the returned error code in preempt mode

Webmail (GINA):
- added S3 as storage for LFT and cache mode
- prevent option to download public key material of local users if not enabled
- add option to enable/disable "copy to myself" button
- quota handling for LFT
- log time and date for unsuccessful Webmail logins

- log time and date for unsuccessful Webmail logins
- add a more detailed webmail account registration status
- add specific email headers for Webmails:
  X-ESWmail-Type-Init: initial password mail
  X-ESWmail-Type-Auth: authorization email
  X-ESWmail-Type-Pwreset: password reset mail
  X-ESWmail-Type-Zip: zipped attachment
  X-ESWmail-Type-Pdf: encrypted PDF attachment
  X-ESWmail-Type-Lft: plain LFT
  X-ESWmail-Type-Sec: secure LFT

RestAPI:
- System settings
- ability to get/add/modify/delete root CA certificates
- LFT disk usage statistics
- cluster monitoring

System Services:
- speedup of maillog indexing
- database snapshot history (only if LFT partition is present)

Version 13.1 (Released 2024-06-27)
See also the Version 13.1 Extended release notes (ERN).

Patch release 13.1.3, 2024-09-24
(new in 13.1.3)
This release will be the last release in the 13.1 branch and enables the update to version 14.0.

Admin:
- sorting by status in the user list view fixed
- fix LDAP key server certificate search

Webmail (GINA):
- file.app (used for the LFT bypass upload of the Outlook AddIn) will use the correct direction to determine the size limits to be used
- do not defang embedded date-URL images in Webmail emails

RuleEngine:
- fix decryption handling of "internal" HIN emails

MPKI:
- add missing SSL CA certificates for CertCentral MPKI connector communication

Patch release 13.1.2, 2024-08-27
(new in 13.1.2)

Admin:
- better check for IP addresses configured under "System > Advanced Setting > Admin GUI > Bind to IP addresses"

MPKI:
- DigiCert connector: always use email address for the common name to prevent malformed JSON problems

RestAPI:

- fix issue in DELETE TLS domain endpoint that prevented the deletion of a TLS domain

RuleEngine:
- prevent relaying of external emails (coming from and going to not managed domains) from ExO IPs
- the use of the attribute "use_lfm" to recognize LFM emails in the rule engine is possible again
- better detection for disclaimer position in reply emails

Webmail (GINA):
- fix of several issues in cache mode
- fix issue where the "Copy to myself" email could not be read in the Webmail GUI
- general bug fixes and improvements for GINAv2
- update Bootstrap version to 5.3.3
- added "frame-ancestors" to the CSP
- replace all inline Javascript in Webmail

Patch release 13.1.1, 2024-07-30
(new in 13.1.1)

Admin:
- the watchdog will use the mail address <watchdog@HOSTNAME> as the FROM address
- mail address is no longer mandatory for the SSL certificate generation
- dark mode for the admin GUI

RuleEngine:
- fix bug in PGP signature verification
- prevent domain encryption from encrypting calendar emails if "Exclude calendar entries and RTF mails (winmail.dat)" is activated

Webmail (GINA):
- general bugfixes and improvements for GINAv2
- fix issue where the "download all" ZIP file will contain only one attachment if two attachments have the same name
- handle opaque signed mails in GINA to fix display issues
- fix issue where the quote from the previous mail was not displayed in a GINA replay mail
- allow writing GINA mails to external recipients without the need of an LFT or IME license
- only show "404 Page not found" if strict SNI checking is enabled

RestAPI:
- fix issue where getting the CSR data of a managed domain will not return the private key data inside the admin GUI. This caused an 'Invalid Key' error in the admin GUI.

MPKI:
- SwissSign intermediate CA certificates "SwissSign RSA SMIME MV ICA 2024", "SwissSign RSA SMIME SV ICA 2024" and "SwissSign RSA SMIME OV ICA 2024" added to the list of SwissSign certificates, which can be updated in the SwissSign-MPKI settings under Settings using "Add or update ..."

Feature release 13.1.0, 2024-06-27
(new in 13.1.0)

Major changes:
- beta version of the new GINA

Admin:
- fix issue that prevented groups from being deleted
- fix issue that prevented Webmail accounts from being assigned to a new customer
- fix issue with the filter in the user list view
- fix issue with showing DKIM keys with CNAME DNS entries
- improvement of the possibility to limit and filter the output of the system log
- copy/past feature for IP address input fields
- prevent RBL from using SORBS lists

RuleEngine:
- use From-header of original mail as recipient for Webmail password mails if the original mail has no envelope sender
- fix issue with not creating new CA file after adding an automatically trusted root CA
- shorten timeout and reduce retry count for LDAP key server lookups to prevent mail flow problems if key server is not available

Webmail (GINA):
- add primary default VirtualHost as catch all with error page
- fix missing subtitle issue in cache mode
- add input field for virtual paths in Webmail domain settings
- add lang attribute to Webmail pages to match selected language

RestAPI:
- license data endpoint added
- system extended fields endpoints added (will be used later)

CfgServer:
- fix issue that prevented the local CA to be pushed to the cluster members

MPKI:
- "Special" section removed from the SwissSign MPKI connector settings
- improved product selection for CertCentral/DigiCert

Version 13.0 (Released 2023-05-04)

See also the Version 13.0 Extended release notes (ERN).

Jump release 13.0.17 (2024-07-02)

This release is the last release in the 13.0 branch and enables the update to version 13.1
(all changes are also included in 13.1)

Admin:
- fix issue that prevented groups from being deleted
- fix issue that prevented Webmail accounts from being assigned to a new customer
- fix issue with the filter in the user list view
- fix issue with showing DKIM keys with CNAME DNS entries
- prevent RBL from using SORBS lists

RuleEngine:
- fix issue with not creating new CA file after adding an automatically trusted root CA
- shorten timeout and reduce retry count for LDAP key server lookups to prevent mail flow problems if key server is not available

CfgServer:
- fix issue that prevented the local CA to be pushed to the cluster members

MPKI:
- improved product selection for CertCentral/DigiCert

Patch release 13.0.16, 2024-05-28

(new in 13.0.16)

Webmail (GINA):
- new directory structure for Webdomain cache mode entries to prevent the subdirectory limitation + speedup
- change Reader App name to "SEPPmail Viewer APP"
- add mail header X-ESWMail-Password with value Yes to all Webdomain password mails
- Bootstrap 4.0.0

Admin:
- MFA for Admin GUI
- fixed an issue where changes to custom Webdomain languages were not saved
- add option "Send to last sender" to "Webdomain >> Admin Settings"

RuleEngine:
- partoftype RuleEngine function will only accept valid MIME types or the legacy list of file types
- print the complete verification report if PGP signature verification fails
- always use CRLF as line ending for locally injected mails
- fixed an issue where the usage of a master ARC key prevented the RuleEngine from using the Authentication-Results header from ExO

RestAPI:
- RestAPI/Users: better filter for customer users

Patch release 13.0.15, 2024-05-14
(new in 13.0.15)

Webmail (GINA):
- fixed a character set encoding problem with file names in ZIP archives that were downloaded with the "Download all" option
- fixed an issue where the mobile number could not be saved in the profile
- fixed an issue where an already registered user could be treated as an unregistered user during password reset
- support Clickatell as an SMS service

Cluster:
- fixed an issue where cluster commands were not executed on the receiving cluster members

Admin:
- fixed an issue where the import of certificates led to an error

LFT:
- enforce LFT partiton file system check

RuleEngine:
- use of the ExO Authentication-Results header for the ARC seal for incoming mails with parallel connected managed domains to avoid SPF check problems.
  You must specify that a managed domain is connected in parallel in the settings of the managed domain.
- interruption-free reloading of the Ruleset
- content type of the attached PGP keys is now application/pgp-keys

Patch release 13.0.14, 2024-04-17
(new in 13.0.14)

General:
- add "Show network setup" to console menu
- rotate rc.log file
- checkdiskspace will look for almost full database
- create tmp partition on install
- fix issue wit customer license limit calculation

MPKI:
- CertCentral: add product selection
- CertCentral/DigiCert: use email address as CN to avoid problems with validation
- SCEP: fix usage of wrong configuration data
- SCEP: convert MPKI connector's certificates into PEM format
- SwissSign: always evaluate and display CMC response status

Webmail (GINA):
- add ability for local users (with passwords) to login to webmail GUI
- add webmail domain information to the cache mode folder
- do not offer IME certificates for download
- fix missing subtitle in cache mode webmail messages
- fix an issue where the reply with attachment in the GINA GUI was not possible
- the order of the downloaded domain certificates in the download file has been changed so that the domain certificate comes first
- add download all for attachments
- add cache mode text templates
- add Cache-control HTTP header

LFT:
- in the case of LFT, the expiry time for a cache link is the same as the expiry time of the LFT messages

Admin:
- add error message in managed domain overview if one forwarding server is configured with different TLS policies
- add ability to resize database
- add zip to the list of accepted types under X.509->Import
- use Perl module for DNS lookup to get public DKIM key to prevent special character escaping
- add ZIP to the list of possible file formats for the X.509 certificate import

RuleEngine:
- Crypto: lower case SrvID for ARC to prevent "No authentication results seen" behaviour
- escape regex to prevent problems with email addresses with special characters
- allow creation of users with '&' in the email address
- always add Job-ID to "ok, queued as ..." log messages
- allow relaying for users of managed domains authenticated via SMTP
- add AES-GCM encryption ciphers to support SMIME/4
- do SPF checks before ARC sealing and add SPF check result into ARC seal

CfgServer:
- log package and pid for controls
- do not reuse Config::Client objects to prevent DB-connection timeouts
- also reopen logfile after rotation in running child processes

RestAPI:
- more worker
- Customer: correct log output

- Customer: correct log output
- Info/Encryption: escape filter email
- Webmail/Domain: fix wrong value for initial password recipient
- Webmail/Domain: fix internal server error on PUT with languageSettings
- Mailsystem/Domain: fix an issue where the disclaimer could not be set to the value "-NONE-"

Cluster:
- setclusterinfo: reparse the cluster data if cluster members file is newer than the cluster data file
- connector: sort backend UUIDs tor prevent balancer restarts which resulted in "queue file write error" messages

Patch release 13.0.13, 2024-02-21
(new in 13.0.13)

General:
- enforce running session cleanup if the lock file is older than 1 hour
- restart apache after regeneration of Diffie Hellman parameters without restarting the backends
- improve update behaviour for big jumps from version 12 to 13.0.13 in cluster environments. The last updating device with a local LDAP database will run the migrate_db process
- fix OCSP Proxy issues
- fix OEM link creation

MPKI:
- additional fixes for CertCentral to correctly handle subdomains

Webmail (GINA):
- reworked cache mode mail texts
- do not allow download of domain certificates issued by the non-trusted internal fallback CA which is used if no local CA is configured
- do not check for mandatory fields for plain LFT mails

LFT:
- fix LFT attachment synchronization issue

Admin:
- fix disclaimer inline and attachment removal issue
- fix display issue with UTF8 encoded subject parts for S/MIME certificates

RuleEngine:
- add crlf IO layer for reprocessed mails to prevent SMTP smuggling
- show SHA256 fingerprint in encryption/signature info
- process duplicated messages in deliver
- fix issue with mail address parsing
- use CrossTenant-AuthAs 'Anonymous' as indicator for incoming and only force smarthost for outgoing

CfgServer:
- speed up adding smimeFingerprint256 in migrate_db

Patch release 13.0.12, 2024-01-30
(new in 13.0.12)

General:
- improved maxsize estimation for the LDAP database to prevent disk-sync hiccups because of a too large database

Admin:
- fix "Autopublish switched off" display issue under Mail System

MPKI:
- fix handling of subdomains in the CertCentral MPKI connector

RuleEngine:
- fix problem with incorrect mail address parsing which leads to an incorrect mail direction detection

Webmail (GINA):
- fix GINA mail generation which triggered SMTP smuggling detection

Patch release 13.0.11, 2024-01-17
(new in 13.0.11)

Special note for ExO tenants:
There are still some issues with invalid ARC signatures. Actually, the ARC signature attached by the SEPPmail is not invalid, but ExO seems to ignore the ARC signature if the mail is a multi-part message (which is the case in 99.9%). We are still working on this issue to find out under what circumstances this happens, why it happens and how to correct it.
We are still in contact with Microsoft to resolve this issue.

MPKI:
- fix error in P7 parsing of MPKI responses which prevents the import of issued certificates

CfgServer:
- problem with incorrectly started rule engine fixed

Patch release 13.0.10, 2024-01-15
(new in 13.0.10)

Special note for ExO tenants:
There are still some issues with invalid ARC signatures. Actually, the ARC signature attached by the SEPPmail is not invalid, but ExO seems to ignore the ARC signature if the mail is a multi-part message (which is the case in 99.9%). We are still working on this issue to find out under what circumstances this happens, why it happens and how to correct it.
We are still in contact with Microsoft to resolve this issue.

General:
- update Postfix to 3.5.23 (fix SMTP smuggling). With this update we by default set the following options
  smtpd_forbid_bare_newline = yes
  smtpd_forbid_bare_newline_exclusions = $mynetworks
  You can overwrite them in the extended MTA settings in the Mail System settings
- update and patch to OpenSSH 9.5 (fix Terrapin attack)
- slapd will now do a checkpoint every minute (was every 60 minutes before)
- connector.pl will now first kill all relevant running ssh connections on startup/restart
- rc.update will write log entries
- drop support for LDAP's bdb and hdb backends
- correctly unbind an disconnect from LDAP
- increase thread and reader count for LDAP

Admin:
- fix bug in color customizing for the new Webmail GUI

- fix bug in color customizing for the new Webmail GUI
- fix settting issue for the sender notfication
- not specifying a smart host when creating a managed domain is OK again
- rename misleading term 'cache' in syslog details to 'index'
- fix issue with adding an empty port for additional smarthost credentials

CfgServer:
- delay some cluster commands to prevent parallel execution on all remaining cluster members
- fix issues with mail routing and additional credentials settings

RestAPI:
- usage of compact IPv6 representation in mailsystem settings and managed domains no longer results in an error
- fix OpenAPI schema for ARC objects
- always use lowercase hostnames
- fix a problem in the crypto/keymaterial endpoint with the incorrect use of C, CN and O of the issuer for revocation requests
- fix CustomCommandType description
- add ability to add/modify default recipients in webmail/domain endpoint

Rule Engine:
- fix an error when using the ARC master key. Now the domain specified for the master key is used.
- only use envelope recipients for ARC
- only the headers "content-transfer-encoding:subject:from:to:content-language:user-agent:mime-version:date:message-id"
  will be used for the ARC-Message-Signature (this setting will be configurable in the future)
- several changes in SMTPd.pl to enhance health detection
- catch DKIM verify exceptions
- use internal message number to create new Message IDs
- always add DKIM to altered outgoing mails
- print more details to the maillog if DKIM has invalid results
- skip DKIM check if there is no DKIM header
- no special treatment for HIN messages if incoming and coming from managed domain

Webmail (GINA):
- fix the use of cds_lock in situations without DBENV
- various improvements and fixes for the new Webmail GUI
- password secure color changed to css

Patch release 13.0.9, 2023-11-21

(new in 13.0.9)

Special note for ExO tenants:
In a MIME-structured mail there might be some additional lines for non-MIME clients like "This is an S/MIME signed message" or "This is a multi-part message in MIME format." These lines are included in the ARC-Message-Signature. Unfortunately, we do not know why, ExO removes these lines which will result in an invalid ARC-Message-Signature and therefore the mail will not pass Microsofts DMARC check.
We are currently in contact with Microsoft to solve this issue.

Administration:
- delete user statistics when the user is deleted

RuleEngine:
- fix bug in mail routing to default outgoing server

- better exception handling for DKIM verification
  do not evaluate the DKIM policy since we will not reject/drop the mail

Patch release 13.0.8, 2023-11-20
(new in 13.0.8)

Libraries:
- update to OpenSSL 3.0.12
- update to nrpe 4.1.0
- update to samhain 4.5.0

Webmail (GINA):
- add a default file extension for all layout images
- make the "Login with SAML" button hideable for the GINA GUI
- fixed LinkedIn Oauth IDP to use new LinkedIn profiles

Administration:
- add ability to input 0.0.0.0/0 as a relaying network under Mail System and in managed domains
- show missing autorenew settings in MPKI configuration
- add ability to filter users by activity level (active, inactive, all)
- add DNSSEC support in System >> DNS
- add ARC sealing for incoming mails configurable in Mail System and in the managed domains (please read the manual on how to setup)
- add support for SSL certificates per managed domain, used as client certificates for SMTP connections
- add ability to set user validation status to HIGH for Sectigo MPKI connector
- remove static subject part settings for DiiCert and CertCentral becaus it is not used by them
- always user the SHA256 fingerprint for identifying S/MIME certificates (admin GUI, RuleEngine logs, ...)

MPKI:
- solve an issue with umlauts in the DigiCert MPKI connector

RestAPI:
- add ability to assign customer admins to a customer even if the admin does not belong to the customer
- fix an character encoding issue in the custom command upload
- Crypto/KeyMaterial: fix issue with incorrectly shown revocation date
- Crypto/KeyMaterial: fix issue with PKCS12 download
- MailProcessing/ExtendedFields: handle situations where deleted tenants/domains/mailprocessing groups/users results in a
- tenants/domains/mailprocessing groups/users does not exist error. These entries are now silently removed
- Mailsystem/Settings: modify will now also modify relaying, relayingForManagedDomains, rbl, blwl and dovecot settings

RuleEngine:
- make HIN's spoof text regex less greedy
- the RuleEngine now logs information about the attachments: name, size, content-type
- using ldap_compare will now explicitly ask the LDAP server for the requested attibute.
- Some LDAP server do not replay all attributes of an entry. By explicitly asking for that attribute the LDAP server will reply these attributes.

Patch release 13.0.7, 2023-09-25
(new in 13.0.7)

When you upgrade a cluster, the change to SSHA512 may cause you to no longer log on to the pre-13.0.7 appliances after upgrading a
cluster member to 13.0.7 and logging on to the upgraded cluster member.
This is because after a successful login we convert the password to SSHA512 and the appliances before 13.0.7 are not able to handle this type of password hash.
The solution to this issue is to either not log in to any of the updated appliances until all cluster members are updated, or use
the update functionality of the CLI by using the support login on the console.

- update to OpenSSL 3.0.10
- update to jquery 3.7.0
- add DigiCert CertCentral MPKI connector
- fixed issue with Apache not restarted after certificate change
- fixed issue with incorrectly displayed TLS level in managed domain settings
- SSHA512 is now used as default password hash mechanism
- moved customer import handling completely into RestAPI functionality
- fix bug in Webmail's "No Password" mode
- watchdog now also looks for zombie processes blocking a clean restart of services
- fixed issue in RuleEngine where the revoked status was not saved after revocation check
- RestAPI: add revocation check and ignore expired certificates in /info/encryption endpoint
- added possibility to specify a smart host for HIN MGWs
- PGP: use last expiring key for mail signatures
- removed 63 character limitation for syslog server input fields in system settings
- RestAPI: fix handling of webmail domains when importing a customer
- fixed multiple issues with waagent for Azure environments

Patch release 13.0.6, 2023-08-24
(new in 13.0.6)

In case of upgrading from 12.1.19 to 13.0.6, please ensure to update to the newest Hypervisor drivers first.

- extend maximum content length for originatorOrgs field in Mail System
- fix issue with not starting reverse proxy for GINA
- fix issue with sscep not able to get address information

Patch release 13.0.5, 2023-08-21
(new in 13.0.5)

- graceful restart of all Apache instances after log rotation
- subjectAltName=email:copy now default requested extension for certificate requests in all OpenSSL configurations
- enhanced caching in internal X509 parsing module
- fix issue with wrong cluster member data shown in details view
- fix issue with incorrectly handled time server data
- disclaimer and templates can now be deleted on Customer deletion
- possibility to select managed domains and webmail domains on customer import
- trigger user license count after manipulations by the means of the RestAPI
- RestAPI/KeyMaterial: fix double reference access
- RestAPI/KeyMaterial: fix usage of wrong data for SAN
- ExtendedFields: add ability to handle users which are no members of a managed domain
- RestAPI: add ability to generate the ruleset and GET or MODIFY the custom commands
- remove SOPA specific X-headers on incoming mails
- fix issue with wrongly loaded language
- fix issue with GINA cache mode content search
- fix all tool-scripts to parse the argument switches case sensitive

- fix LFT sync script to create storage directory if it does not exist
- do not log RuleEngine log entries to /var/log/messages
- distribute checkallcerts-script's load to all cluster members
- fix issue with getting PIDs of running processes
- fix issue where the CfgServer loops in creating domain certificates
- fix issue with not being able to issuing certificates with the SCEP or DTrust MPKI
- fix issue with not being able to issuing certificates with Sectigo MPKI
- fix issue with not being able to set a new customer backup password
- fix logfile parsing issue in mailgraph
- fix issue in file.app with simultaneously uploaded bypass attachments
- add ability for the LFT attachment sync script to only sync to configured cluster members and only sync attachments if LFT or Cache Mode is enabled
- fix a possible LDAP search injection in track.app
- fix issue where the pwsend.app, responsible for initial passwords by SMS, shows an empty form
- fix some spelling mistakes in the Admin GUI
- fix an issue where additional smarthost credentials were ignored
- fix an issue where PGP signatures could not be created
- fix issue where the default TLS level of 'may' was ignored
- fix issue with an Internal Server Error in "Managed Accounts" in the customer settings page
- fix issue where the SwissSign MPKI settings are not shown
- add support for SMTPUTF8 in postfix.
- This can be enabled within the "Extended Postfix MTA settings..." by setting smtputf8_enable to yes.
- add managed domain and GINA domain selection for customer import
- add functionality for every cluster member (frontend or backend) to inject mails on every other cluster member (frontend or backend)
- This is important for bypass LFT mails.
- DKIM signatures only for outgoing mails
- show expiry date for GINA cache links
- prevent CfgServer from generating pending certificates more than once
- do not call 'sync' in /etc/nonvol handling to avoid the system freezing for some seconds

Patch release 13.0.4, 2023-06-16

(new in 13.0.4)

Before updating to version 13.0.4 first read the extended release notes for version 13.0.4 because of changed mailrouting behaviour

- OpenSSL 3.0.9
- fix issue with initially using DHCP in Azure environment
- fix issue with customer admin login causing an internal server error
- add setting to Mail System and Managed Domain to select if mails between managed domains (aka internal traffic) should be sent to the configured smarthost.
  Currently this is only done for mails between ExO hosted managed domains if the X-OriginatorOrg is set.
  This settings is off by default and will change the internal mail handling to the behaviour as it was before version 13.0.
- fix issue with backup download
- fix issue with SVG logos in webmail
- fix issue with expiring MPKI operator certificate in daily report

Patch release 13.0.3, 2023-06-01

(new in 13.0.3)

- OpenSSL 3.0.8

- OpenSSL 3.0.8
- postfix with UTF8 support
- fix license limit counting
- fix issue with admin user not being editable
- fix issue with continous webmail apply
- fix user filter
- fix issue with lost SMTP authentication data
- fix issue with public key search in GINA GUI
- fix issue with "syntax error" in DNS section while saving System settings
- fix issues with DigiCert MPKI connector not being able to obtain certificates
- fix issue with user login
- fix issue with setting DNS server in the console
- fix display error in user settings for "may not sign mails"
- fix issue with getting data for the Sectigo MPKI connector
- fix issue with SMS not being sent
- fix issue with 'internal' routing between EXO tenants
- fix issue with clamv not starting
- fix issue with double '<<>>' around 'copy to myself' address

Patch release 13.0.2, 2023-05-12

(new in 13.0.2)

This patch release is important for all running a fronend/backend constellation

- fix issue with fetchmail restart through watchdog due to wrong PID file parsing
- fix issue with the maillog index cron job
- fix issue with migrate_db after backup restore
- fix issue with frontend system freeze
- collect local information of the device even on non-cluster systems
- fix issue with not saving keyserver settings under Mail Processing
- show cluster setup on not clustered backend systems
- fix issue with not added PGP key information after an upload in GINA

Patch release 13.0.1, 2023-05-12

(new in 13.0.1)

- fix internal server error when configuring Micsosoft as IDP for GINA domains
- fix issue with snmp configuration
- fix issue preventing cron jobs to run

Release 13.0.0, 2023-05-04

(new in 13.0.0)

Major changes:

- introduction of extended fields

Administration:

- fixed an issue where a bulk user import set the "last mail sent" date which automatically acquired a license
- fixed an issue where "Server requires authentication" under "Mail System" could not be deactivated
- fixed issue with X.509 Root CA trust inheritance in cases of two or more certificates with the same common name
- fixed an issue where a temporary creates main.cf could interrupt the mail processing
- fixed issue with erroneously shown "GINA Domain ... used by more than one customer" warning
- apply extended mta settings last, otherwise they may be overwritten

- apply extended mta settings last, otherwise they may be overwritten
- graceful restart for Admin GUI if settings have changed
- prevent [default] GINA domain from being deleted if an assigned Customer is deleted
- allow frontend to create and import backups (the database will be ignored)
- change all size units from KiB, MiB, ... to kb, MB, ... to avoid confusion for users
- add input field in Mail System for custom ExO IPs
- every cluster member has now the full knowledge of all other cluster members. This information are shown in the Cluster section.
- prevent the admin from deleting pre-defined groups
- check CSS syntax before saving it under GINA Domain >> Layout
- only show virtualization tools suitable for the host system
- Device-UUID introduction (for information purposes only for now)
- Tenant-UUID introduction (for information purposes only for now)
- use PKCS12 for HIN domain certificate import
- advanced configurability of the network settings
- added postcreen-proxy
- added configuration settings to use relaying settings of managed domains in global relay settings
- added Cluster Identifier protection
- added selection of TLS versions and Cipher Suites configurable for IMAP and POP3 (important for satellite installations)
- enforce a certain password strength for backup passwords
- user defined DKIM-selector input
- do not disable rfc1323 extension via sysctl
- improve nonvol mount behaviour

Large files:
- replace RC4 with AES256 for LFM attachment encryption

Mail transport:
- set hop count limit in master.cf to 48
- postfix will use a cidr map for mynetworks

REST-API (1.0.4):
- fixed an issue where the RestAPI was not started after log rotation
- fixed issues with UTF-8 vs. Unicode
- fixed token information cleanup to prevent invalid token errors
- added endpoint fpr Mail System / Settings
- added endpoint for Mail System / Domain
- added endpoint for Mail System / TLSDomain
- added endpoint for GINA Domains / Settings
- added endpoint for GINA Domains / Domain
- added endpoint for MPKI
- added endpoint for crypto
- added endpoint for authentication
- more fine grained token module access

Reporting:
- log SMTPd.pl's PID in maillog like "SMTPd.pl[6897]"
- add sequence numbers and split information to RuleEngine log output.
  The job ID for each message is now extended by a sequence number and additional split information.
  This means that the job ID, e.g. 2188437, is now followed by the sequence number of the log line.
  After the sequence number comes the split information, which gives you an indication of which message you are following.
  This then looks like this: 2188437-54-1 (Job ID 2188437, protocol line 54, message not split).
  A split will happen in the RuleEngine, e.g. with an rmatchsplit function or if a message should be

A split will happen in the RuleEngine, e.g. with an rmatchsplit function or if a message should be encrypted, but this was not possible for all recipients. In this case, additional split information is added. An rmatchsplit on a message with two recipients RA and RB, which only matches the recipient RA, is continued for RA with e.g. 2188437-55-1-1 and RB 2188437-56-1-2. Internally, the message is duplicated and the "original" message receives the "1" and the duplicate receives the "2".

Rule Engine:
- fixed INCAmail tag handling
- introduction of Extended Fields for Mail Processing, Customer, Managed Domains, Mailprocessing Groups, and Users
- add mail address to "420 an encryption key for your account will be available shortly" message

WatchDog:
- more and better monitoring

WebMail (GINA):
- customer separated key search
- add support for PNG, JPG and SVG logos
- support direct key download via link
- introduce cache mode
- limit password length ti 2048 characters
- adapt password strength determination for more secure user defined passwords
- add IPDs Microsoft and Google
- no registration process for users authenticated by IDP

Version 12.1 (Released 2021-09-18)
(new in 12.1)

If you are running this SEPPmail in a cluster environment, using virtual IP addresses, please go to System ==> IP ALIAS Addresses
and check if the interface binding entry is bound to a named interface. We had cases where the interface names got lost and the bind
did not work anymore.

See also the Extended release notes.

Patch release 18, 2023-03-15
(new in 12.1.18)

Starting with 12.1.18 an update will only be possible if the LDAP uses the MDB backend.
You easily can switch under Administration >> Maintenance > > LDAP >> Migrate LDAP to MDB backend.

- OpenSSL 1.1.11
- ClamAV 0.103.8 to fix CVE-2023-20032 and CVE-2023-20052
- digits only passwords for event logins
- MDB migration path
- case insensitive X-OriginatorOrg match in RuleEngine
- prepare SwissSign CMC mPKI connector for new SwissIgn CA
- fix GINA issue with ignored additional hostnames
- add information to secure mail upload hint
- fix bug in MPKI connectors using SOAP in MPKI-proxy environments
- protect RuleEngine from using old PGP-2 keys
- fix Sectigo MPKI connector by correctly parse decoded result content
- Fix problem when opening certain GINA messages
- fix issue with too big customer imports in Admin GUI

- fix a problem in the watchdog log where only the first word of a log message was displayed
- fix a GINA problem where a normal user is created in the self-registration process

Patch release 17, 2022-09-28
(new in 12.1.17)

- OpenSSL 1.1.1q
- static functions for WebMaiDomain's used_by_... functions which will speed up Admin GUI for Mail System, GINA Domains and Customer
- GINA Session: do not use file lock for serialization if DB is not bound
- fix error message handling which results in "ARRAY(...)" messages on the home screen
- do not run the migrate_db task in frontend systems
- fix GINA account creation for mail addresses containing a '+'
- fix template creation
- prevent remote code execution in Admin GUI
- do not show CC-field after adding an attachment in GINA if editing recipient is not allowed
- fix issue with not used translations and empty labels in GINA
- disallow CBC ciphers in PCI compliance mode

Patch release 16, 2022-09-07
(new in 12.1.16)

- fix for missing Tenant ID in Exchange online mails. For details check Microsoft Tenant-ID Mailflow Solution
  If you use Exchange Online Integration with 'tenant ID' authentication, you must change to the new 'Exchange Online Originator Organisation Header' authentication in all managed domains after update
- fix LFT bypass upload issue

Patch release 15, 2022-08-05
(new in 12.1.15)

- fix Fatal Runtime error in protection pack/RuleEngine

Patch release 14, 2022-08-02
(new in 12.1.14)

fix Fatal Runtime error in RuleEngine
harden RestAPI authentication header usage

Patch release 14, 2022-08-02
(new in 12.1.14)

- fix Fatal Runtime error in RuleEngine
- harden RestAPI authentication header usage

Patch release 13, 2022-08-01
(new in 12.1.13)

- only show GINA confirmation password settings on HIN systems
- fix possible Remote Code Execution vulnerability in RuleEngine
- hide LFM settings in GINA settings if LFT is not licensed
- fixes issue with ampersand in GINA account name
- fix issue with slowly filling /tmp partition
- fix issue in GINA GUI with deactivated 'reply' button with activated setting "Only allow GINA users to write new e-mails to default recipients"
- introduce restricted ports for internal backends
- fix disclaimer positioning for Apple Mail, Gmail and GroupWise
- fix issue where file.app does not find GINA account
- fix SwissSign special task version guard
- fix Fatal Runtime Error in RuleEngine
- fix issue where changes in texts were not applied in the GINA settings
- fix issue with custom smarthost credentials
- fix several security issues as a result of a pentest
- fix issue with incorrectly used PGP key expiry date
- fix issue with kernel panic because of write operations on read only file system

Patch release 12, 2022-06-02
(new in 12.1.12)

- OpenSSL 1.1.1o
- fix with keyserver not returning PGP keys
- fix Incamail handling
- public keys are available in GINA satellite systems
- fix version number comparison in DB migration to prevent unnecessary adaptions
- locking mechanism for session DB to prevent concurrent access problems
- fix fatal error in RuleEngine
- fix PGP key import
- fix encryption policy filter
- fix internal server error if CA is not configured
- OEM specific changed in language files
- fix cluster redirect of LFT-bypass messages

Patch release 11, 2022-05-03
(new in 12.1.11)

- fixed an issue where a secure GINA attachment would display "preview mode" information in addition to the normal content.

Patch release 10, 2022-04-28
(new in 12.1.10)

- fix System>>Advanced view freeze

Patch release 9, 2022-04-27
(new in 12.1.9)

- installed patch to fix zlib vulnerability
- always add hostname in sslog messages
- fix broken link in SPF bounce messages
- add user agent in httpd's access logfiles

- fix issue with as empty shown GINA messages in gmail's inline preview
- show entropy data of /dev/urandom in home screen
- add means to bulk-issue new SwissSign certificates
- make web.app session ID regeneration configurable
- deactivate TLS 1.1 for all httpds
- fix not showing GINA user log
- fix web.app's CGI object usage
- fix reverse proxy configuration
- fix wrong TO mail address delimiter in daily report mails

Patch release 8, 2022-03-23
(new in 12.1.8)

- OpenSSL 1.1.1n
- fix issue with domain certificate renewal
- fix issue with internal server error in pwsend.app
- add missing CA certificates for DFN MPKI connector

Patch release 7, 2022-03-11
(new in 12.1.7)

- GINA now uses a backend which results in a massive speedup
- rewrite of the domain certificate renew code
- add more HTTP securitiy headers
- add "validity in days" setting for HIN domain certificate generation
- more an better information for iOS users for GINA mails
- configurable "Powered by ..." link for GINA
- add new DigiCert root certificates necessary for ExO
- setvar and ldap_read now can handle JSON data. For more information please refer to the manual.
- added domain specific account name settings for the SwissSign MPKI connector
- force the GINA user to set mandatory fields if missing
- better preview for GINA mails on mobile devices
- fixes PGP key import error when data to import are not a PGP key
- fixes an internal perl bug where an authenticated user can not login to GINA
- fixes an X.509 certificate import issue where the same email address is in the SAN multiple times, but is case sensitive
- fixes the return message of the RestAPI's LDIF import
- fixes a race condition where log rotation and the watchdog could interfere with each other.
- fixes PGP key import of keys with multiple same IDs (but case sensitive) in ldap_getpgpkeys
- fixes an issue in ldap_getcerts where the userCertificate has not the ";binary" option

Patch release 6, 2022-01-12
(new in 12.1.6)

- add LDIF import to RestAPI
- fix for HIN signature verification
- fix customer backup dispatch
- fix issue where IDP settings were not taken from master template
- fix GINA portal PGP key download
- fix PGP key bulk import

Patch release 5, 2021-12-20
(new in 12.1.5)

- fix PGP key usage for not expiring keys
- use passphrase for PGP secret key export
- fix for SAML authentication to correctly pasre metadata XML

Patch release 4, 2021-12-14
(new in 12.1.4)

- improve customer overview page loading behaviour
- fix MPKI issue with incorrect SN/GN splitting
- fix issue where triple wrapping tagged unsigned mails as [signed INVALID]
- fix internal sever error when generating certificates over SCEP
- fix configuration issue with smtp submission port
- fix RestAPI /group output
- fix issue with unescaped DN in automatic S/MIME generation
- fix invalid master.cf generation for submission port
- fix handling of no longer supported PGP-2 keys
- remove mail address length limitation for SCEP

Patch release 3,2021-11-10
(new in 12.1.3)

- allow an empty NRPE daemon listen address to listen on all interfaces on IPv4 and IPv6
- adapt Sectigo MPKI connector to Sectigo's REST API changes
- fix handling of no longer supported PGP-2 keys
- fix footer position in GINA portal
- fix CSV statistics export by adding HIN Global counters
- fix file.app's LFT bypass upload authentication error
- fix postfix configuration error
- fix issue with self-registration on GINA portal
- fix COM-Addin LFT login with enabled external LDAP authentication

Patch release 2, 2021-10-27
(new in 12.1.2)

- fix problem with GINA encryption

Patch release 1, 2021-10-20
(new in 12.1.1)

- add new SwissSign root CAs (can be added via "Add or update..." in MPKI sessings)
- reenable processing of mails with missing mandatory from and date header but reject signing mails with missing from header
- fix SPF welcomelist checks
- fix reverse proxy location match for IDP icons
- fix possible deadlock in config server
- fix maillog index deletion

Release 12.1 (Released 2021-09-18)
(new in 12.1)

Major changes:

- RESTful API
- OAuth and SAML authentication for web domains

Administration:

- Protect 'Cluster identifier' downloads with password
- Show correct X.509 root certificate chains
- Show "trust state set by" for X.509 root certificates
- Trust state set for X.509 root certificates gets inherited to chained root certificates
- Full configuration option when adding managed domains
- Users, GINA users and customers now show when they were created by what and by whom (Liste)
- Automatic periodic OSCP/CRL checks for certificates (user, X.509 and X.509 root certificates)
- Show all PGP subkey-IDs in the Admin-GUI and Logs
- The validity in days of domain certificates to generate is now configurable
- New kind of Multi-Select in the Admin GUI for better handling of a large ammount of entries
- RESTful API
- Restart GINA GUI after SSL certificate change
- Fix display error of empty section tables
- Fix removing of "LDAP connect to" error message in admin GUI

Large files:

- Fix handling of attachments if "copy to myself" is used

Mail transport:

- Server Name Indication (SNI) is now configurable via checkbox in "SMTP settings"
- Fetchmail now uses the combined list of trusted CAs of OpenBSD and all trusted X.509 root certificates

Multi-tenancy:

- New Customers overview Page
- Remove, import or export a customer from the customer overview page

OpenPGP:

- Switch to gpg2 which includes Support for PGP 2.0 ECC keys

REST-API:

- manage users (local and web accounts)
- manage groups
- manage manged domains
- manage customers
- manage templates/disclaimer
- get statistics
- get encryption information
- a more detailes definition can be found under swagger hub

Reporting:

- HIN Global Counter

Rule Engine:

- Support for Triple wrapping (RFC 2643)
- Drop mails if mandatory headers (requested by RFC 5322) are not present

- Drop mails if mandatory headers (requested by RFC 5322) are not present
- E-mails, infected by a virus which has to be sent to a specfied email, are now no longer encrypted anymore
- Fix handling of message headers when using reprocess to decrypt a message again

WatchDog:

- web.app is now monitored by the watchdog
- Watchdog uses active pages for memory usage calculation

WebMail (GINA):

- Automatic creation of user-accounts for internal GINA-Users when externally authenticated or registered
- Support of external IDPs (OAuth: Facebook, LinkedIn, FideasIAM; SAML) for GINA user authentication
- Saving an LFT message as PDF now shows attachment and their size
- Country-specific redirection of GINA default forward page
- Mobile phone number and full name can now be set mandatory in a GINA registration
- "CC" field for GINA mails
- Automatic logout after manual GINA passwort resets
- GINA-SessionID is changed after login to avoid session hijacking
- Special error page for GINA to prevent "internal server error" page anymore
- Use of user agent to prevent session hijacking can be switched off
- GINA Certificate download - Show hex values instead of decimal for serial numbers
- Any HTTPS configuration uses now HSTS headers
- Improved load behavior for the GINA Interface
- GINA GUI code hardening
- Fix "Confirmation password usage" from GINA Domain is used from master if configured
- Fix quoting of the display name in to address in passwort reset e-mails
- Fix: In rare cases the "reply secure" button was missig for some recipients of GINA Mails
- Fix use admin e-mail for all SMS to send
- Fix parsing of X-FORWARDED-FOR HTTP header to prevent session mismatch
- Fix missing date and message-id header in "displayed" notification mails

MPKI:

- MPKI only accepts valid SSL client certificates as operator certificate
- Update of SOAP API for DFN (Deutsches Forschungsnetz)
- More appropriate errormessage if MPKI request fails to MPKI endpoint
- Always add the e-mail address as SAN in CSRs
- Settings to clear challenge password and make use of 'nombstr' in requests for SCEP
- Fix certificate creation via SCEP failed with password error
- Fix automatic renew of D-Trust certificates

Version 12.0 (Released 2020-11-13)
(new in 12.0)

Upgrade is only possible for appliances with a log partition size of at least 2 GB and must otherwise be cloned to a new appliance using the "clone device" feature found under "Administration".

Warning for customers with HIN connector using GLOBAL encryption: The current update corrects a misbehaviuor of the old ruleset that led to GLOBAL encryption for users without a local account even ignoring the settings in "Mail processing". Please check that GLOBAL encryption still works as expected after creating a new ruleset.

The following rule set macros are provided for replacement of legacy variables:

- @ADDDISCLAIMER@ -> $disclaimer;
- @ARCHIVE@ -> $archive;
- @KEYSERVER@ -> $keyserver;
- @LOGSUBJECT@ -> $logsubject;
- @PLUGIN@ -> $plugin;
- @RELAY@ -> $relay;
- @REMOVELFMTAGS@ -> $removelfmtags;
- @VSCAN@ -> $vscan;
- @VSCANSEL@ -> $vscan_crypt_only;

Administration:

- Allow public X.509 certificates, root CAs and OpenPGP key bulk export
- Make sure the system time is in sync when using hardware sensors
- Automatic frontend sync for mail processing and GINA
- Show more relevant information in blocked mails log
- Allow frontends to update vendor domain certficates
- Test mail console menu option

Processing:

- Runtime disclaimer selection using extended signature marker
- Log reject code and message for internally rejected mails
- Option to trust imported CA certificates automatically
- Properly tag non-managed domain encryption in log
- Domain-based default and reply disclaimer
- Skip PTR check if sender is authenticated

GINA:

- New GINA password reset option: SMS or hotline without question/answer
- Disable reply button when reply to default recipient list is empty
- Confirmation password feature for additional authentication factor
- Provide relevant local issuer CA along with certificate on search
- Improved GINA secure attachment lanuage selection and support
- Allow to disable strict Server Name Indication (SNI) checks
- Allow multiple authentication methods in one GINA domain
- Limit session access to User Agent / IP combination
- Prevent error when uploading empty keys to GINA
- Prevent improper log entries in GINA user log
- Implement 12 hour hard timeout

MPKI:

- GlobalTrust MPKI connector

System:

- Update to OpenBSD 6.8 / LibreSSL 3.2
- OpenSSL 1.1.1h

Patch release 1, 2020-11-13

(new in 12.0.1)

- Interpret waiting status in D-TRUST MPKI revoke as success
- Correctly handle private S/MIME RSA keys in PKCS#8 format
- Prevent display of invalid entries in mail log overview
- Remove LDAP bind failed message when LDAP is reachable
- Improve CSV user imports

Patch release 2, 2020-11-17
(new in 12.0.2)

- Correctly recover mail service on unrelated watchdog error
- Allow HIN domain-encrypted subjects to appear in mail log
- Properly replace subject tags for plugin use
- Fix issue with external GINA authentication
- Fix fetchmail startup issue

Patch release 3, 2020-11-27
(new in 12.0.3)

- nslookup for all record types in consolemenu
- Fix issue with registration process

Patch release 4, 2020-12-14
(new in 12.0.4)

- Show lock for HIN encrypted mails
- Do not allow PKCS7 in SSL import
- Allow frontend server backups
- Disable vioscsi and correctly detect Nutanix Hosts
- Do not set accountLastUsed for domain for internal mails
- Fix sporadic syntax error in system view
- Fix race condition in watchdog starting GINA portal
- Fix missing fromemail in GINA secure attachment
- Fix customer/mailroute assignment issue

Patch release 5, 2021-01-05
(new in 12.0.5)

- Better error handling for all MPKI connectors
- Read vioscsi with manual disable possibility
- Fix azure provisioning
- Fix bad formating in tracker
- Fix case where frontends are detected as cluster members

Patch release 6, 2021-01-27
(new in 12.0.6)

- GINA GUI code hardening
- improved license usage for LFT users
- notify() with parameter 'admin' now also notifies the postmaster of the managed domain
- Improve GINA domain configuration speed with large number of installed managed domains
- Add SMS provider prosms.dds.a1.net
- Fix issue where where smarthost redentials are used for internal delivery

- Fix bad DN formating for S/MIME certificates issued by rule engine
- Fix bad encoding in D-Trust MPKI connector
- Fix IncaMail tag handling
- Fix ldap proxy crash

Patch release 7, 2021-02-01
(new in 12.0.7)

- Fix issue with appliances that have a very old ruleset

Patch release 8, 2021-03-08
(new in 12.0.8)

- Fix issue with not starting GINA portal
- Fix issue with GINA replies from unknown domains

Patch release 9, 2021-03-08
(new in 12.0.9)

- generate internal CA list after a transfer of a CA from a cluster member
- session invalid message after session timeout in GINA portal
- suppress logging of the value in setvar()
- allow import of domain PGP keys without email
- add waring mesage for Hyper-V appliances with a legacy network controller
- Fix GINA portal configuration issue with virtual hosting
- Fix issue with GINA portal registration
- Fix service restart on frontend/backend system
- Fix memory leak in system libraries

Patch release 10, 2021-03-26
(new in 12.0.10)

- Enhance connection stability when using a proxy to connect to the update/license server
- Add new policy to emulate a HIN MGW
- Correct handling of long MIME lines (RFC 2821)
- Correctly remove forbidden headers from decrypted S/MIME mails
- Fix display problem with CRL and CA Issuers URI in S/MIME details
- Fix GINA language text file handling with master template dependency
- Update ClamAV to 0.103.1
- Update OpenSSL to 1.1.1j
- Update OpenLDAP to 2.4.58

Patch release 11, 2021-04-29
(new in 12.0.11)

- Update root hints for bind
- Sync CRL from backend to frontend
- better TLS compatibility for external LDAP authentication
- Fix CRL generation for local CA
- Fix PKCS12 password encoding
- Fix managed domain assignment in customer settings
- Fix header handling in GINA mails
- Fix PGP secret key import
- Fix sporadic PGP signature verification failure
- Fix handling of long MIME lines (RFC 2821)

- Fix handling of forbidden headers from decrypted S/MIME mails
- Prevent welcomelisting for auto-reply messages
- Update OpenSSL to 1.1.1k

Patch release 12, 2021-06-11
(new in 12.0.12)

- Update ClamAV to 0.103.2
- Use gaurd pattern to prevent time consuming PGP signature detection in large HTML mails
- CSM module improvements
- Fix search for LFT partition
- Fix rare case when a mail has to be redirected to a cluster member because of a bypass LFT upload
- Fix access rights for MPKI operator certificates
- Fix creation of local CRL to track all revoked certificates
- Fix verification of static subject inputs in the admin GUI
- Fix rare case of currupted mail structure after S/MIME decryption
- Fix nrpe SSL handshake failure

Patch release 13, 2021-08-19
(new in 12.0.13)

Version 12.0.13 fixes a possible path traversal attack issue in the GINA frontend. We recommend to install this update as soon as possible,
The system automatically checks if an attack has been performed or tried on the appliance and will issue a warning if traces are found.
If this warning is issued please contact the vendor for further investigation and log analysis.

- fix security issue in web.app

Patch release 14, 2021-08-23
(new in 12.0.14)

- fix GINA attachment handling in reassemble

Patch release 15, 2021-09-30
(new in 12.0.15)

- Update OpenSSL to 1.1.1l
- Update OpenLDAP to 2.4.59
- remove user agent in originator for GINA to prevent iOS issues
- fix attachment handling over SOAP interface
- Prepare for the update to version 12.1

Version 11.1 (Released 2019-11-14)
(new in 11.1)

DKIM use prior to version 11.1 requires correcting the DNS entries due to compatibility improvements.

Major changes:

- Substantial S/MIME performance improvements
- Microsoft 365 relay and tenant ID support
- Outlook Addin 2.0 with IME and LFT integration

Administration:

- DKIM DNS entry changes for better compatibility
- Show last license refresh date in home screen
- Allow to refresh license from home screen
- Do not restrict password field input length in admin GUI
- Fix overflow of serial number in OpenSSL-generated S/MIME certificates
- Show MPKI use in mail domain overview
- Added port probe feature to support console menu
- Added web services restart feature to support console menu
- Added support for Office365 tenant ID and automatic relay
- List public OpenPGP keys and X.509 certificates as "DISABLED" when manually disabled
- Allow optional admin GUI login with user mail address instead of ID
- S/MIME certificate and OpenPGP key aliases are only valid for encryption recipients
- User-based IP alias passwords can now be set as an alternative to the hardwired default
- External authentication tester in managed domain now supports direct password login test
- Prevent firmware update download being stuck on download aborts
- Warn about managed domain fingerprint mismatch in edit page
- Prevent deletion of managed domain when fingerprint certificate is active
- Show statistics about top level domains provided by managed domain encrption
- Fix issue with CRL fetch on GUI-based certificate check
- Fix possible GUI not available issue on mail processing reload
- UX improvements for SCEP integration

Logging:

- Support Postfix "enable_long_queue_ids" parameter and use it by default
- Log structural errors in MIME when scanning for S/MIME encrypted mails
- Send new CA certificate notifications to members of "x509rootcertificatesadmin" group
- Do not store custom user creation ruleset when it is equal to the default ruleset
- Move MPKI auto-renew error message to top warning messages
- Allow manual deletion of GINA logs like mail logs
- Improve read speed of log archive files

Processing:

- Reusable macros for user creation in rule engine (see manual for details)
- Autofill comment for X.509 certificates origin imported via incoming mails
- HIN connector will now also sign mails for HIN domain recipients
- Rewrote S/MIME subsystem for maximum performance
- Allow shared smarthost with different credentials per mail domain
- Remove internal control headers from managed domain encrypted mails
- Protect Thread-Topic and Thread-Index headers for managed domain encrypted mails
- Header tagging option for internal mails
- Archiving option now triggers before encryption policies and custom rules
- Allow import of S/MIME certificates with duplicated mail addresses in SAN
- Send watchdog message when user-based license pool is depleted
- Improve scanning for disclaimer markers
- Support legacy mail address format in header From
- Reprocess encrypted mails from Lotus Notes

GINA:

- No longer require user accounts for local GINA messages
- Allow configuration of initial GINA password sender address
- Start of GINA portal is now asynchronous for faster appliance boot

- ~~Start of GINA portal is now asynchronous for faster appliance boot~~

Large files:

- Introduce token-based authentication for server-side LFT API / plugin support

Patch release 1, 2019-12-11
(new in 11.1.1)

- Allow access to variables $user_name and $user_mail currently selected by authenticated()
- Append user stats to user currently selected by authenticated() if possible
- Correctly treat LFTs as secure as per user request when using LFT API
- Stray CA certificates in LDAP imports no longer force a runtime error
- When using tagsubject() with multi-word regex only use the first word
- Prevent log index generation failures by detecting log rotation
- Use configured admin address in hotline password reset mails
- Fix rule engine fatal error on malformed mail address
- 1-year log read would sometimes stop prematurely
- Improve disclaimer positioning and add a timeout
- Switch MPKI RSA key generator to 4096 bit keysize
- Do not show date for unread LFT messages
- Fix per-certificate revocation check
- Fix manual IME certificate import
- ClamAV 0.101.5, WALinuxAgent 2.2.45

Patch release 2, 2019-12-19
(new in 11.1.2)

- Support console can now force a reinstall of an already installed version
- Remove unnecessary hidden form values on GINA self-registration
- Fix cleanup of unregistered customer GINA accounts
- Fix key server response on frontend servers
- Fix special encoding read in certificates
- Assorted LFT API improvements

Patch release 3, 2020-01-15
(new in 11.1.3)

- Show "implicit" trust of previously imported root certificates
- Allow select / edit of OpenPGP key delivery template
- Fix edge cases with X.509 certficate import
- Fix crafted GINA registration form disabled bypass
- Fix GINA reply check for default customer domains
- Properly add disclaimer to Addin-based LFT mails
- Add timeout for stuck PGP key generation issue
- Correct chain certificates on signature write
- Use stored postmaster to deliver OpenPGP key

Patch release 4, 2020-02-05
(new in 11.1.4)

- Improve validation of Office 365 forwarding server hostnames
- Indicate encrypted status of secure GINA-based replies
- GINA portal auto-keepalive to prevent LFT timeouts
- Fix parsing of leading zeros in serial numbers

- Fix import of unknown OID in cert DNs

Patch release 5, 2020-03-25
(new in 11.1.5)

- SMS empty from address will now use configured GINA admin address
- Fix SNMP queue statistics read for "enable_long_queue_ids" use
- Improve mail index write on appliances with many log archives
- Fix truncated bulk export of PGP keys and S/MIME certificates
- Keep special characters in full name during user creation
- Warn about expired state of MPKI operator certificate
- Rewrote log index generation to use multiple CPUs
- Relax validation on S/MIME certificate import
- Fix OCSP check fatal error in rule engine
- Validate GINA proxy target input
- Improve SPF input validation

Patch release 6, 2020-04-16
(new in 11.1.6)

- Improved tagsubject() parsing of regular expression input
- Allow ruleset policy to use same GINA sattelite settings
- Skip RSA-specific options on EC certificate actions
- Prevent locked users from authenticating via SMTP
- Fix possible error in customer backup creation
- Rewrote queue handling in rule engine
- Event-based SMS OTP support for GINA
- Sectigo MPKI connector
- OpenSSL 1.1.1f

- Hotfix 1: Fix GUI bug while setting up Sectigo connector
- Hotfix 2: Fix regression in ruleset handling

Patch release 7, 2020-05-20
(new in 11.1.7)

- Improve reprocess() for Lotus Notes so that only RFC-compliant mails are processed
- Only append "<>" to sender address in change_webmail_sender() if not already found
- Fix check for valid certificate during domain decrypt with HIN connector
- Fix incorrect handling of "<tab>$" character sequence in custom rulesets
- Check MPKI state before revoking certificates to avoid spurious errors
- Automatically add X.509 Root Certificates from issued MPKI certificates
- Only offer users with passwords when adding new group members
- Sign LFT mails in the same way that GINA mails are handled
- Fix incompatibility with newer customer backups during import
- Fix possible external auth tester error on too many results
- Fix missing user creation in ruleset generator edge case
- Fix issue with password escaping during PKCS#12 import
- Fix recently used domain certificate details display
- Fix PGP inline signed status on multiple parts
- Allow collapse/expand in admin GUI for main tables
- Tweak GINA HTTPS server settings
- Add disclaimers to internal mails
- Virus scan internal LFT mails

Patch release 8, 2020-05-29
(new in 11.1.8)

- Allow independent OCSP/CLR bulk check for public and root certificates
- Properly add Sectigo MPKI to nightly auto-renewal
- Avoid double-escape of PKCS#12 in relevant spots
- Fix possible duplicated parts in PGP decryption
- Allow relay servers in Office 365 hybrid setups
- Scrub trigger tags on default encrypt deliver

Patch release 9, 2020-07-16
(new in 11.1.9)

- Provide root certificates that cannot be downloaded from trust store if available
- Better handling of incoming and internal relay of managed Exchange Online domains
- LFT bypass can now create new users with external authentication
- Provide manual flush button for address verification cache
- Fix file type extension handling on multiple MIME parts
- Prevent LDAP import of non-encryption S/MIME certificates
- Do not abort OpenPGP key import after invalid first key
- Add new Sectigo intermediate CA to MPKI connector
- Separate fetchmail from local injection queue
- Prevent deadlocks in background task handler
- Fix saving additional PGP key addresses
- Do not sign to be modified LFT content
- Fix issue with OpenPGP public key bulk export
- Fix OCSP check before revoke
- OpenSSL 1.1.1g

Patch release 10, 2020-09-10
(new in 11.1.10)

- encrypt_webmail() second parameter allows to skip password mail if SMS can be sent
- When renewing S/MIME MPKI certificates skip imported disabled certificates
- Select proper smarthost credentials for mails with empty SMTP sender
- Authentication log was mistakenly called "audit" log for a long time
- Use exception for edge case logging instead of connection check
- New function getheader() can store header content in variable
- disclaimer() can now auto-position in GINA carrier mails
- Allow company/footer logo opt-out in GINA carrier mails
- Allow to disable WAAgent in Azure without disabling DHCP
- Correctly remove revoked certificates in deduplication
- Allow domain-encrypted subjects to appear in mail log
- Improve whitespace trim for email address reading
- Fix revocation date display in S/MIME certificates
- Check S/MIME revocation status on signature verify
- Allow browser auto-complete in GINA login form

Patch release 11, 2020-11-11
(new in 11.1.11)

- Users without accounts now correctly trigger domain encryption only in manual user creation
- Function reprocess() now supports attached message only mode
- Always replace revoked certificates in key server lookup

- CRL/OCSP check via X.509 user and root certficate details
- Delete last update for domain keys when importing a backup
- Restrict internal() and external() From header fallback
- Optionally allow group member selector for all users
- Fix selective smarthost parsing with port number
- Allow to specify the mail log search limit
- Do not alter effective plugin subject tags
- Support UFT-8 characters in PKCS12 export
- Correct initial statistic graph content
- Use multiple CRL/OCSP URI if necessary
- Prepare for the update to version 12.0

Version 11.0 (Released 2019-06-20)
(new in 11.0)

Major changes:

- New policy editor features and ordering support
- Improved spoofing detection
- GINA GUI security hardening
- D-TRUST MPKI
- DKIM support

Adminstration:

- Prevent creation of wildcard managed domains
- Allow selection for MPKI-capable managed domains
- S/MIME bulk import advanced usage options
- Let S/MIME certificate deduplication default to off in new installs
- Unofficial antivirus signatures now default to off in new installs
- Validate maximum message size value
- Support bulk imports in X.509 certificates and OpenPGP public keys
- Remove non-user bulk imports in administration section
- Show current ruleset creation data
- List mobile number in GINA account overview
- Reject SSL certificate upload if non-server certificate was presented
- Allow use of internal CA for virtual host SSL certificate creation
- Create PGP keys immediately when requesting them in the GUI
- Added D-TRUST MPKI connector
- Policy editor now supports selecting GINA template
- Allow reordering policies in policy editor
- Add mail disclaimers to policy editor
- Updated layout of key server input
- Automatically delete non-managed users after 6 months of inactivity
- Improve import to accept OpenPGP user IDs without "<>" characters
- Indicate managed domain participation value correctly when global setting is used
- Remove carriage returns from templates to avoid spurious newlines
- Correct fetchmail SSL support
- Fix edit bug in multiple customer management
- Add SEPPmail version to backup file name
- Warn about auto-renew issues in daily report
- Warn on version mismatch in cluster

Logging:

- Allow filtering mail logs by encryption, signature, large file or unencrypted property
- Audit and system log now always display 1 full year of log entries
- Make message ID column optional in mail log overview
- Fix property display mismatch in mail log overview
- Improved parsing in technology statistics generation
- Log ruleset version in mail log

Processing:

- Add separate dispatch queue for locally injected mails
- Distinguish between external and outgoing communication
- Wait for internal database to come up instead of failing to process mails
- Defer creation of S/MIME certificates to keep mail processing responsive
- Automatic managed domain relay checks now also enforce global relay permission
- Allow managed domain request header check result to persist
- Improved check_sender() mail header validity check
- Allow variable replacement in setvar() and empty()
- Change LDAP import to add new addresses to existing certificates on key match
- Fix calculation of mail size when reassembling GINA attachments
- Allow reversal of large file processing in deliver()
- Removed obsolete getcustomer() function
- Added support for opaque S/MIME signature creation
- iscalendar() will now treat RTF just like plain calendar entries
- Optional DKIM support for managed domains
- Allow precise disclaimer positioning with "##MAILDISCLAIMER##" placeholder
- Always remove [emptypw] tag from processed mails
- Fix MIME-Version Header misplacement in domain encryption
- Do not allow notify() delete the original message in edge case
- Improved recipient rewrite internals

GINA:

- Use HTML instead of text part when generating a PDF download
- Optionally disallow manual input of GINA recipients
- Create unique message ID for all GINA mails
- Use minimal UTF-8 encoding in mail headers
- GINA GUI code, script and object security hardening
- Add viewport meta values to secure attachment
- Improved GINA GUI responsiveness
- Update to Bootstrap 3.4.1

Large files:

- New LFT disks will now require a size of at least 30 GB
- Split LFT maximum size for outgoing and incoming mails

System:

- Update to OpenBSD 6.5 / LibreSSL 2.9
- Hardening of NTP configuration
- Improved Azure integration

Patch release 1, 2019-06-24

(new in 11.0.1)

- Validate sender addresses before processing starts
- archive() usage now correctly appears in mail log
- Fix issue in periodic domain certificate update

Patch release 2, 2019-06-27
(new in 11.0.2)

- Let vscan() check if antivirus deamon is off to avoid spurious mail bounces
- Wrap GINA header from and to addresses in "<>" for better spam avoidance
- Fix PDF preview with new GINA content security policies
- Do not check global relay servers for incoming/internal mails
- DFN MPKI connector awareness for email/email-host setting
- Fix pending rule engine S/MIME certificates mismatch
- Correct domain name in GINA message ID headers
- Fix import of S/MIME certificates

Patch release 3, 2019-07-10
(new in 11.0.3)

- Let isspam() check if antispam engine is off to warn about skipped spam check
- Correctly attach mail body or header report in bounce() and nofity()
- Show potential errors in CRL/OCSP certificate check fetch
- CA root addition notification with details about new certificate
- Daily report lists all undefined CA root certificates
- Correct error in default recipient display on GINA send
- Fix saving miscellaneous options in mail processing
- Do not support auto-customer option in encryption policy
- Fix processing of mails from mails starting with a plus sign
- Let admin decide about customer association on user/bulk import
- Always clear previous daily report MPKI autorenew error
- Retain advanced MTA settings on mail system edit
- Correct error in DKIM signature append
- Add ability to scan LFT attachment for viruses
- Fix missing LFT in split recipient scenario

Patch release 4, 2019-07-31
(new in 11.0.4)

- Avoid incorrect HIN domain certificate fingerprint mismatches
- Properly remove subject tags in "do not encrypt" policies
- Add domain encryption-only users to daily CSV report
- Allow to skip createkeys() deferral with custom rule
- Fix regression in saving attributes in setuserattr()
- Fix migration of policies to new position-based approach
- Do not list unlocked GINA accounts in daily report
- Allow secure LFT bump via Outlook sensitivity header
- Fix issues with user creation and deletion
- Show user language GINA account details

Patch release 5, 2019-08-08
(new in 11.0.5)

- Fix OpenPGP key generation where the secret key was not saved

- Fix issue where the list of users could not be displayed
- Fix GINA issue where the dsn notification was not sent
- Fix regression in saving GINA accounts
- Fix restore of pre version 11 backups

Patch release 6, 2019-09-10
(new in 11.0.6)

- Do not mark daily reports with undefined root certificates as important
- Follow-up change for HIN domain certificate fingerprint mismatches
- Fix import edge case with Arbeitsagentur S/MIME certificates
- Make it possible to distinguish licensed users in daily CSV
- Proper enforcement of multi-tenancy customer license limits
- Header validity checks now allow superfluous whitespaces
- Show account and last message status in GINA details
- Better mobile number validtion on GINA CSV import
- Support encryption policies in GINA remote setups
- Show issuer in GINA S/MIME certificate display
- Add confirmation dialog to OpenPGP key deletion
- Fix a faulty certificate issue in D-TRUST MPKI
- Refuse import of unspported ECC OpenPGP keys
- Fix save delay for GINA domain settings
- Allow import of OpenPGP keys of unusual size
- Custom generation for EDIFACT mail reports
- Fix GINA frontend OCSP HTTP proxy URL
- Log S/MIME retention check in system log
- Add support for new aspsms SMS interface
- Fix issue with Azure agent service
- ClamAV 0.101.4

Patch release 7, 2019-10-01
(new in 11.0.7)

- Fix customer association in multi-tenancy GINA portals for uppercase mail addresses
- Only add encrypted attached mail as separate mail on incoming direction
- S/MIME digest selection is now effective in "do not encrypt" policies
- Rule engine key and certificate generation now correctly sets CN attribute
- Do not append disclaimers to calendar entries (requires ruleset reload)
- Only get host name and domain name from Azure DHCP if not set manually
- Optionally allow static subject override for SwissSign MPKI
- Improve parsing of sloppy whitespace patterns in mail headers
- OpenSSL 1.1.1d

Patch release 8, 2019-10-24
(new in 11.0.8)

Only send passwords mails via private mail queue to avoid potential deadlocks
Remove trigger tags on plain or already encrypted messages
Expire stale pending certificate/key requests
Always try to skip approval in DigiCert MPKI
Only create DKIM keys per user request
Fixed MSG format export encoding issue
Prepare for the update to version 11.1

Version 10.1 (Released 2018-11-29)

(new in 10.1)

Major changes:

- Improved ease of use for SSL certificate import, renewal and cluster distribution
- Improved logging capabilities and log view analysis for custom rulesets and policies
- Elliptic-curve encryption support for imported S/MIME certificates
- Optional removal of OpenPGP signatures during mail processing
- Support console menu with network and administration utilities
- Improved performance of file type scanning
- Full OCSP stapling support in GINA proxy
- Removed unsupported SignTrust MPKI
- QEMU and Xen host integration

New admin group priviliges "readonlyuser" are not being added to existing installations, but can be added manually by using this exact name if required.

You can reach the support console via user "support" and password "support". The menu will allow you to open a support connection even when the GUI is unavailable.

Administration:

- Check SSL import for matching private key and automatically handle it as the primary certificate
- Allow to import a renewed certificate without private key as long as the previous one matches
- Allow to push current SSL and CA settings to all other cluster members
- Allow to set CRL validity for local CA
- Vendor domain services are now indicated by "managed", "unmanaged", and "mismatch"
- Delete all domain keys after confirmation of deletion of a managed domain
- Allow to test a managed domain's external authentication settings
- Several new and updates notes as well as clarified option names
- Prevent overlapping GUI output when using administration tools
- Allow to restore a backup without overwriting system-specific settings
- Allow to trigger a backup mail via administration tools
- Support console menu with network and administration utilities
- Manual domain encryption overview now shows active column in overview
- Mail disclaimer and templates can now be forced to UTF-8 for maximum compatibility
- Mail disclaimer and templates relocated to mail system category
- Importing a previously known domain key will yield a more descriptive error message
- Allow bulk import of X.509 root certificates
- Fix edit language encoding issue on save
- New "readonlyuser" group for selective GUI access in combination with existing groups
- Fixes for "readonlyadmin" group usage
- QEMU host integration (no settings necessary)
- Xen host integration (no settings necessary)
- Action button support and other visual tweaks

Logging:

- Internally encrypted mail recipients are now properly indicated as encrypted
- Allow policies and custom rulesets to indicate encrypted and signed status as well
- Use "S/MIME" and "certificate" instead of "smime" and "key" in log messages
- Administrative mails generated by the appliance are now visible in the logs
- Protection pack software now logs to system log instead of mail log
- Remote logging now sends system log along with mail log
- Added CC and Date header to message metadata logging option

- Added CC and Date header to message metadata logging option
- Distinguish between incoming and internal communication
- Regenerate mail log index after updates
- Local mail logging may be disabled completely

S/MIME:

- Automatically add SAN to generated S/MIME domain certificates
- SHA-256 is now the signature message digest default
- Support import of elliptic-curve certificates
- Correct CSR creation for wildcard domain

OpenPGP:

- Honour OpenPGP key capabilities, e.g. refuse encryption if capability is not available
- PGP/MIME now prefers AES-256, SHA-512, ZLIB (or lower depending on recipient key)
- Force the use of MDC even when the recipient key does not meet the criteria
- Optional removal of OpenPGP signatures is now available

MPKI:

- Fix internal selected MPKI mismatch for connectors added in version 10
- Only issue certificates for users from managed domains
- Trust all GobalSign chain certificates via GUI button
- Trust all DigiCert chain certificates via GUI button
- Trust all DFN chain certificates via GUI button
- Unsupported SignTrust connector has been removed

Rule engine:

- Removed obsolete functions smime_create_key(), swisssign_create_key() and signtrust_get_cert()
- Fix issue with stripped secure tag on "Consider internally routed mails as encrypted"
- Move custom outgoing ruleset before encryption in front of encryption policies
- Function createaccount() no longer creates keys, see createkeys()
- Key server checks are now done before starting encryption policies
- Add ldap_init() function for maintenance tasks such as cache flush
- Allow key generation even when user creation is set to manual
- Allow use of variables in replace_rcpt() and replace_sender()
- Allow tags to be appended to the beginning of the subject by default
- Implement $one_recipient and $all_recipients in ldap_read()
- Implement custom search filter support in ldap_getpgpkeys()
- Implement custom search filter support in ldap_getcerts()
- Warn when RTF-formatged MIME parts have been detected
- Case-insensitive match of incoming() domain check
- Removed obsolete function webmail_password()
- File type scan speedup

GINA:

- Support web.app?subject= parameter in Base64 encoding to prefill the subject field after login
- Warn when GINA domain is associated with managed domains of more than one customer
- Add setting to prevent registration of GINA accounts for associated managed domains
- Always use message arrival time as base for read time in notification message
- Extended MSG support will now show address book entries for sender and recipients
- Optional HTTPS proxy now logs correct user IP regardless of proxy request header setting

- Optional HTTPS proxy now logs correct user IP regardless of proxy request header setting
- Log TLS protocol and cipher for user login when using GINA via direct HTTPS
- Do not advertise revoked domain certificates in domain key listing
- Change transfer-encoding of attached EML files to 8-bit
- Allow to publish local CA on the certificate search page
- Use more robust MIME structure in generated GINA mails
- Allow indirect OCSP stapling only via OCSP HTTP proxy
- Optional HTTPS proxy now supports OCSP stapling

Large files:

- Allow override of configured LFT plain and secure mode via several control headers and subject tags
- Plain LFT is no longer indicated as encrypted in mail log

Patch release 1, 2018-12-07
(new in 10.1.1)

- Prevent display of unassociated partial mail entries for customer admins
- Fix external GINA authentication test when multiple servers were given
- Prevent invalid characters when creating a new GINA domain
- Fix mixed charset detection when displaying GINA messages
- Always decode disclaimer text like HTML variant
- Separated mail log indicator for general LFT message usage
- Create persistent backup copy for support-based recovery
- Only create internal users for managed domains
- Fix truncating large DNS zone configurations

Patch release 2, 2019-01-07
(new in 10.1.2)

- Remove spurious case-insensitive markers from internal compare() statements
- Improve local HTTPS GINA proxy interoperability in Exchange environments
- Avoid potential truncation of long certificates when reading from system
- Also escape characters ";" and "\" in ldap_read() and ldap_compare()
- allow replace_rcpt() to use variables with multiple enclosed recipients
- Storing variables using setvar() no longer accepts names starting with a number
- Compare LDAP certificates e-mail addresses as case-insensitive
- Option to use remote POP3 mail fetch with pure SSL port
- Only create one message abstraction for all associated GINA messages
- Fix a regression in customer association for GINA users
- Send daily report even when individual statistics are damaged
- Hardening of OpenSSL S/MIME key encryption parameters
- Use configured welcomelisted subnets to skip SPF check
- Do not store empty values in system configuration
- Fix import of binary LDAP certificates
- Allow IncaMail and HIN connector to coexist
- Fix faulty year wrap in statistics parser
- Show OpenPGP subkey ID on detail page
- Show IPv6 source address in mail logs
- Sort local DNS zones alphabetically

Patch release 3, 2019-01-09
(new in 10.1.3)

- Automatically trust previously known MPKI certficates on "add or update"

- Correct issue in new SPF welcomelist range check
- Avoid partial display of listed user state

Patch release 4, 2019-01-23
(new in 10.1.4)

- Only replace certificates from remote LDAP if expire date is higher
- Correctly load and store disclaimer parts as UTF-8 in the GUI
- Correctly load and store custom rules sets as UTF-8 in the GUI
- Only accept MPKI P12 password when uploading a new P12 or old password is wrong
- Log relevant S/MIME signature information when detecting or signing
- Exclusively use latest OpenSSL 1.1.1 in S/MIME operations
- Allow to turn off archive scanning in executable and script file scans
- Do not automatically issue or renew keys for users who may not sign or encrypt
- Fix MSG render error by providing an additional codepage mapping
- Fix PDF render error for file names with umlauts
- Fix customer license limiter regression in version 10.1
- Remove default relay network from factory reset
- Prevent use of disclaimer names with "#" characters
- Use charset from original part when decoding

Patch release 5, 2019-03-06
(new in 10.1.5)

- Allow to hide domain certificates from GINA by disabling signing capability
- Immediately restart ClamAV on connection failure
- Do not reorder DNS servers on system settings save
- Use all available CRL points to check revocation status
- Treat sender "<>" as empty to allow fallback to "From" header
- Accept non-conforming RFC 2045 quoted-printable parts
- Fix operating system panic on heavy statistics write
- Do not MIME-encode "<>" in "From" header
- Fix race in internal statistics increment
- Correctly handle HIN Global in policy editor
- Fix export encoding of GINA translation files
- Update DFN MPKI certificate authority chain
- Prevent storing duplicated local DNS zones
- Add NTP sensor mode for virtual machines
- Improve traditional NTP synchronisation
- Increase S/MIME bulk import speed
- Update to OpenSSL 1.1.1b

- Hotfix 1: Bring back missing log messages

Patch release 6, 2019-03-29
(new in 10.1.6)

- Remove duplicated counter values to avoid cluster sync issues
- compareattr() "M_Sender" attribute changed to "SENDER"
- Warn when NTP cannot find qualified servers to sync with
- Fix import of certificates with telephone numbers
- Fix setting multiple DNS servers via DHCP
- Improved performance of background tasks
- Add SMS provider certificall.net

- Use correct PDF encoding for date

- Hotfix 1: Prevent library error on GINA read
- Hotfix 1: Correct license calculation

Patch release 7, 2019-04-15
(new in 10.1.7)

- Fix sending daily report when MPKI operator certificate expires
- Fix empty initial GINA password user in conjunction with external auth
- Ignore pseudo domain @local in daily reports
- Retain sender behaviour from 10.1.4 and below
- Policy sender match now works for empty sender using "<>"
- Avoid sporadic background service exit
- Support "/" in local mail address part
- Amazon Web Services support
- Add SMS provider playSMS
- ClamAV 0.101.2

Patch release 8, 2019-05-23
(new in 10.1.8)

- Allow creating users with a previous user ID but different mail address
- Special variable $from in LDAP functions now replaces correctly with empty envelope sender
- Correctly disable SNMP R/W community when no password was set
- Do not show logs for customer admins without managed domains
- Properly quote LDAP attribute for search in ldap_compare()
- Add missing timeout setting for OCSP HTTP proxy
- Always properly generate mail log index
- Prepare for the update to version 11.0

Version 10.0 (Released 2018-07-05)
(new in 10.0)

Major changes:

- Performance improvements in mail processing, GINA and admin GUI
- Preempt mode to temporarily stop mail flow through appliance
- OpenPGP subject tags for positive and negative signature verification
- Assorted improvements in frontend / backend clustering
- Allow to specify credentials for each smarthost
- Added a number of new policy editor conditions
- Allow to sign an arbitrary CSR with local CA
- New MPKI connector for Deutsches Forschungsnetz
- New MPKI connector for GlobalSign
- Allow to specify different modes for incoming and outgoing LFT mails
- GINA legacy layout has been removed

New admin group priviliges "webmaildomainsadmin" and "mpkiadmin" are not being added to existing installations, but can be added manually by using these exact names if required.

(Groups -> Create new user group)

Please take note that the old GINA design was removed from this version. All remaining users will automatically switch to the new GINA layout and may require a manual style update.

(GINA Domains -> Change GINA Settings -> Edit GINA layout)

Before proceeding with this update, make sure to back up your device.

Admin:

- Require confirmation on user removal and delete/revoke all certificates automatically
- Show current user and device name in footer when logged in
- Redirect users to first viable page after login
- Show user lock state in list (bad password count, locked)
- Redirect to home section when performing a firmware update and show reboot status afterwards
- Do not redirect to logout page after logging back in after logging out there
- Added "webmaildomainsadmin" group access privilege for GINA domains section
- Added "mpkiadmin" group access privilege for MPKI section
- Allow read-only admin to view and filter mail logs
- Add summary to individual mail log detail view
- Add sign and encrypt indicator icons in mail log
- Performance improvements in mail log view
- Avoid temporary purge of SSL trust bundle on frontend servers on save
- Create backup file on startup to allow immediate SCP backup
- Properly encode certificate or key file names on export
- Assorted improvements in frontend / backend clustering
- Preempt mode to temporarily stop mail flow through appliance
- Allow to disable DNS resolver prefetch disable
- GINA 30 day log and full archive download
- Optimized visual spacing used between GUI elements
- Use monospace font in statistics images
- Statistics reset button

Mail System:

- Allow to specify credentials for each smarthost
- Never rate-limit local mail relay
- Added option for mandatory TLS

SSL/CA/MPKI:

- Automatically add CA certificate to internally created SSL certificates on export
- Show correct SSL certificate details if import contained multiple certificates
- Allow to sign an arbitrary CSR with local CA
- Immediately propagate trusted MPKI CA chain during manual update via button
- Use a negative grace period of 30 days for renewing previously expired MPKI certificates
- Warn about expiring MPKI operator certificate in daily report
- New MPKI connector for Deutsches Forschungsnetz
- New MPKI connector for GlobalSign
- Send all MPKI requests to system log
- Verify given MPKI static subject

Rule Engine:

- Sign mail in "do not encrypt" policy if requested

- Properly validate CIDR welcomelist ranges in spam and spoof checks
- Fix encoding issues in user-generated notifications
- Improve spoof check to test for match in relay domain
- Authentication header checks must also pass relay network check to succeed
- Always use 30 seconds timeout for LDAP certificate and key lookups
- Allow to use a manual flag as a policy trigger
- Filter policy according to sender too
- Use internal flag mechanism to avoid tagging a subject temporarily
- Always replace the emptypw tag according to the user setting
- "mpkiSubjectPart" attribute support for setuserattr()
- Prevent excessive substitution in compare()
- Accept flat RFC 822 messages in reprocess()
- Allow to force disclaimer usage even when message does not contain the necessary parts
- Automatic disclaimer placement for Microsoft Outlook, Apple Mail and Mozilla Thunderbird
- Domain-sign is no longer available from the ruleset generator
- Properly generate accounts in policies when account creation for all users is selected
- Improve parsing of the message disposition notification header
- Performance improvements for reading incoming messages
- File detection performance improvements

S/MIME:

- Allow to refuse use of certificates that can not be checked for a number of days
- Optionally refuse the import of certificates using SHA-1 or lower
- Optionally refuse to use expired certificates for encryption
- Certificates now have a default validity of 825 days
- Properly escape special characters in common name
- Avoid generating multiple domain certificates in a cluster environment
- Unhide same-subject certificates in X.509 Root Certificates
- Separate page for manual domain encryption management
- Show prominent expired warning for certificates in detail view
- Allow immediate check of certificates in detail view
- Limit the number of external certificates shown by default
- Managed domain encryption switches to OAEP
- Also treat non-multipart message as S/MIME

OpenPGP:

- Properly trust all known keys in PGP/MIME to align with inline PGP behavior
- Make PGP/MIME the default mode for OpenPGP encryption if not set otherwise
- Optional subject tags for positive and negative signature verification
- Allow selection of OpenPGP mode in policy editor as a fallback
- Show prominent expired warning for keys in detail view
- Separate page for manual domain encryption management
- Added validation of signatures

GINA:

- Notifications now default to domain setting, but individual user settings can override
- Do not submit question / answer when it is no longer required by password reset mode
- Do not provide disabled or revoked user certificates in search
- Clarify error message when encryption was requested but account is missing
- Send all password mails to envelope sender to fix an "in behalf of" case
- Automatically add "On ... wrote:" to reply text

- Automatically add "On ..., ... wrote:" to reply text
- SMS support for vapi2.infinite-convergence.com
- Do not generate accounts for HIN GLOBAL
- Add originating IP to authentication log messages
- CSS handling improvements for secure attachment customization
- EML / MSG downloads now have their date and subject in the file name
- Fix character encoding in MSG export
- Add insecure mail text to basic translation edit view
- Adjust secure copy mail text for clarity
- Annotate use of background images in CSS / LESS file
- Correct time offset in GINA delivery status page
- Added GINA proxy health check to watchdog
- Allow sending GINA logs to remote syslog server
- Allow optional virtual hosting per domain
- GINA legacy layout has been removed
- Performance improvements

Large Files:

- File API version 1.0 can receive files without having to attach them to the initial mail
- Allow to specify different modes for incoming and outgoing files

Patch release 1, 2018-07-09
(new in 10.0.1)

- Correctly append system settings during boot up
- Fix MIME part parsing error during disclaimer add
- Fix SCP backup user login

Patch release 2, 2018-07-10
(new in 10.0.2)

- Add SOAP service alias to default GINA domain
- Fix VGA hardware boot for OEM hardware
- Fix manual S/MIME domain list display
- Fix Nagios service start
- Fix GINA PDF export

Patch release 3, 2018-07-16
(new in 10.0.3)

- Allow empty subject trigger tags to revert to their default
- Use cleaned from address in policies
- Fix GINA secure copy licensing error
- Fix error in external user creation
- Fix import of PGP keys from GINA
- Fix automatic fetch of license

Patch release 4, 2018-07-19
(new in 10.0.4)

- Do not fail on first action of special group member after login
- Improved robustness S/MIME certificate attribute parsing
- Allow to create domain keys without a local CA present
- Verify alternative mail addresses for S/MIME signer

- Handle malformed mail addresses in mail log

Patch release 5, 2018-08-02
(new in 10.0.5)

- Fix CVS user import for previously welcomelisted senders
- Correct domain encryption user count to license overview
- Assume default domain message delivery notification setting if not set
- HIN connector now always uses latest set of trigger texts
- Create default bounce templates during bootup if not found
- Fix case where message tracker was not loading its stylesheet
- Add GINA encryption user count to license overview
- Add SMS support for Interactive Digital Media
- Fix mixed encoding issue with GINA replies
- Improved faked HIN subject tag detection
- Fix possible hang in PGP/MIME encryption
- Fix nightly MPKI auto-renew
- ClamAV 0.100.1

Patch release 6, 2018-08-14
(new in 10.0.6)

- Fix boot hang in Windows Server 2008 R2 with Hyper-V 6.1
- Also parse elaborate message disposition notification header values
- Improved detection for incoming / outgoing direction in GINA / LFT
- Fix GINA resource path in preview, translations and password mail
- Align GINA secure reply envelope sender with from header change in 10.0.3
- Set proper permissions on work directory after nightly MPKI run
- Correctly search for external user certificate in edge case
- Only test each sender domain once in anti-spoof check
- Allow keyserver lookup in Internal Mail Encryption
- Further fixing for import of PGP keys from GINA

Patch release 7, 2018-09-11
(new in 10.0.7)

- Support GINA HTTPS OCSP stapling (incompatible with "Enable local https proxy")
- Do not warn about ruleset regeneration when using uploaded rulesets
- Do not emit final newline character in SMS password messages
- Tweak RAM usage according to available system resources
- Allow enabling serial console in system settings
- Fix possible decryption error with HTML parts in OpenPGP
- Make LFT tag removal case-insensitive

Patch release 8, 2018-09-20
(new in 10.0.8)

- Correct domain replacement issue in HIN connector
- GINA high-performance toggle option, now defaults to off
- Fix display error in Internet Explorer in log detail view
- Correctly delete datasets no longer used in version 10
- Backend task scheduler reworked

Patch release 9, 2018-10-17
(new in 10.0.9)

- Correctly skip expired certificates in smime_keys_avail() when required
- Improve GINA portal speed with large number of installed managed domains
- Correctly save and apply all extended MTA settings values
- Do not partially match on user certificate / key search in GINA
- Allow special HIN prefix on incoming encrypted mails in HIN connector
- Avoid a potential charset issues when displaying GINA messages
- Disable OAEP usage in managed domain encryption
- Improved background task cleanup in scheduler
- Fix customer backup decryption during import

Patch release 10, 2018-10-26
(new in 10.0.10)

- Allow HA backup to become master when master crashes and hangs at "syncing disks..."
- Raise limits for concurrent GUI access to make GINA and admin GUI more responsive
- Escape special characters in CN of locally generated certificates via mail processing
- Fix expire check when generating new OpenPGP keys via mail processing
- Fix IncaMail connector when sending mail to a real incamail.ch recipient
- Updates for ClamAV 0.100.2 and SpamAssasin 3.4.2

Patch release 11, 2018-11-09
(new in 10.0.11)

- Variables and flags are now appended and edited using their associated message only
- Improve accessiblity of HTTP-only admin GUI missed in patch release 10
- Fix issue with CID replacement of embedded images in disclaimers
- Use UTF-8 encoding for Infinite Convergence SMS service
- Correctly flag use of LFT subject tags for custom rulesets
- Fix OAEP decryption which would occur sporadiacally
- Create required accounts in sign-only policies

Patch release 12, 2018-11-22
(new in 10.0.12)

- Allow longer function argument strings in custom rule set
- Fix issue with disclaimer attach on very large messages
- Fix daily report calculation of MPKI operator certificate expire
- Fix off-by-one in X.509 root certificates expire GUI display
- Relax concurrent connection limits on all web servers
- Verify postmaster address input in mail settings
- Do match case when removing subject tags
- Prepare for the update to version 10.1

Version 9.6 (Released 2018-05-17)
(new in 9.6)

- Only show support connection message warning for users with access to the feature
- Reserve mail log green, orange and red status for remote server status
- Correctly abort mail processing when certificate generation fails
- Outlook Plugin header mode corrections for LFT
- Only log invalid Bind-DNs during LDAP operations
- Tweak LDAP multi-master synchronization configuration
- Display used product version in each mail log
- Fix queued mail log always being one entry short

- Fix memory leak in HIN connector
- Properly enable the Microsoft Azure integration service when selected
- Properly delete expired X.509 Root Certificates when selected
- Prevent removal of certificate bundles on frontend appliances
- Allow leading dot for TLS domain names
- Fix possible problems with LFT resize feature
- Fix special character encoding issue in generated GINA mails
- Display PGP user keys without expiry in GINA key search

Version 9.5 (Released 2018-03-06)
(new in 9.5)

Patch release 1 is a mandatory update for QuoVadis Swiss Advanced CA G3 S/MIME certificate interoperability. In case of QuoVadis MPKI usage please also refresh the chain certficates via MPKI: Settings: "Add or update".

- Domain encryption is now part of the default encryption in the policy editor
- Added IncaMail, RSA-OAEP and RSA-PSS options to policy editor
- Separate sign option to unify policy editor with ruleset generator
- Do not strip brackets from outgoing server when entering host names
- Prevent password reset for GINA users with empty initial passwords
- Do not mention password expiration during initial GINA registration
- Always update relevant master template settings during relevant GINA domain edits
- Correctly use domain encryption when user-based S/MIME and OpenPGP is disabled
- Speed up creation of multiple domains under mail system
- LDAP connector improvements for anonymous bind and mail-based Bind-DN
- Global switch for auto-publishing managed domain certificates
- Allow to specify the use of text and HTML disclaimer parts
- Disclaimer positioning tweaks for multiple mail clients
- Add disclaimer attachments to mails even when no disclaimer parts could be added
- Log metadata option now includes message from, sender and to headers
- Prevent logging large amounts of data per line
- Added confirmation dialog to full mail log delete
- Allowed deletion of mail log index
- Correct plugin header usage for [plain] and [noenc]
- Allow login for users with single statisticsadmin group
- Improve statistics write for more accurate results
- Unify GINA time format display between languages
- Allow IME certificate import
- Meltdown mitigation
- ClamAV 0.99.4

Patch release 1:
(new in 9.5.1)

- Correct import of QuoVadis Swiss Advanced CA G3 issued certificates
- Add QuoVadis Swiss Advanced CA G3 chain to optional MPKI trust bundle

Version 9.4 (Released 2018-02-01)
(new in 9.4)

- Fix translation of timestamp in GINA tracker
- Correctly handle ".asc" extension during PGP inline decrypt
- Always strip encryption tag on incoming mails
- Gracefully deal with an empty from header during account generation
- Added customer info to user CSV in daily report if applicable

- Use same sender extraction for initial key generation and subsequent regeneration
- Always convert PGP/MIME incompatible incoming mails to allow encryption thereof
- Fix an issue with PGP/MIME bulk sending
- Better error message on LDAP bind failures
- Fix GINA password reset mentioning e-mail if only SMS was set
- Do not show unused images in GINA preview
- Do not add unused inline attachments to disclaimers in e-mails
- Allow $rcptdomain and $rcptaddress in ldap_compare()
- Improved sender verification
- New OpenPGP public key bulk import
- Allow initial DHCP assignment and add agent for Azure deployments
- Update ClamAV to version 0.99.3

Patch release 1:
(new in 9.4.1)

- Allow e-mail address as bind DN in LDAP queries

Version 9.3 (Released 2017-12-14)
(new in 9.3)

- Wrap individual versions in release note viewer
- Correctly interpret all MPKI auto-renew failures
- Do not truncate content ID of disclaimer attachments
- Bring back usage of leading dot in mail domain
- Do not override key creation result during user creation
- Remove enabled subject tags from incoming mails
- Fix initial display of default recipients when writing a new GINA mail
- Fix user-based GINA ZIP support in mixed recipient list
- Fix GINA mobile number subject parsing for special encodings
- Fix spurious display of "=" characters in GINA messages
- Fix an error in device cloning that could prevent database replication
- Add CA certificate to exported SSL certificates if available
- Correctly preset disabled proxy and OSCP selection in system settings
- Do not search for disabled LFT tags
- Allow use of SwissSign Demo MPKI

Correct typo in LFT resize feature

Patch release 1:
(new in 9.3.1)

- Add rule generator option to prefer RSA-OAEP for S/MIME encryption

Patch release 2:
(new in 9.3.2)

- Add rule generator option to prefer RSA-PSS for S/MIME signatures
- Correctly verify the non-backwards-compatible RSA-PSS signatures
- Correct mails that are not compliant with PGP/MIME before encryption

Version 9.2 (Released 2017-11-27)
(new in 9.2)

- New LFT tag was set to enabled by default for backwards-compatibility
- If there are no LFT attachments use original mail for GINA mail download

- Allow master template selection during GINA domain creation
- Correct line endings in GINA mail download
- Fix the nested attachment parsing in GINA mails
- Allow obsolete protocol, cipher and key exchange in SMS connector
- Show correct search entries in domain certificates
- Prevent GINA login when clicking "Forgot password"
- Stripped spurious markup and whitespace from GINA text notifications
- Make internally secured subject tagging opt-in
- Show GINA SOAP connector 400 rejects as deferred in log view
- Always add inline file data for disclaimer
- Do not mention passwords in plain LFT mails
- Correct proxy usage in MPKI connectors
- Correct quoting during S/MIME sequence read
- Raised overall memory limit for mail processing

Version 9.1 (Released 2017-11-08)
(new in 9.1)

- Fixed SwissSignCMC connection problems
- Fetch correct product's name_id for DigiCert MPKI connector
- Add all languages in GINA notification mails
- Fixed runtime error when adding disclaimer
- Use UTF-8 charset for user import

Patch release 1:
(new in 9.1.1)

- Show HIN Global activation in managed domains if HIN connector is enabled
- Fix a bug with character sets in disclaimer

Version 9.0 (Released 2017-10-30)
(new in 9.0)

This major release contains a rework of the Large File Transfer feature. If you previously used LFT and set it to allow unsafe LFT for your domains, your mails will be sent as unsafe by default. If that is not what you expect, please disable the unsafe LFT mode prior to upgrade. Both modes can still be used flexibly using multiple new key words, see below for details.

Please also note that the old GINA design is no longer the default and will not be available in the next major release. All remaining users are encouraged to activate the new GINA layout.

(GINA Domains -> Change GINA Settings -> Edit GINA layout -> Use mobile-friendly web templates)

The database will be reorganized during this update. This means that the update can take longer than usually (up to 30 minutes on large installations)

The Legacy SwissSign connector has been removed. Please change to the new CMC connector before updating.

Before proceeding with this update, make sure to back up your device.

Admin:

- Look and feel of the UI has been improved for all of its elements and the menu
- Revamped disclaimer management with variable support, custom attachments / inline files (requires a

valid license)
- Policy editor allows to set fine-grained outbound encryption policies without custom ruleset
- Managed domain service participation can now be selected per mail domain
- Allow to specify subject alternative names for SSL certificates
- Allow to sign a SSL certificate with the local CA during creation
- Certificate usage can be restricted to not encrypt, not decrypt or not sign depending on its capabilities
- Make sure that S/MIME fingerprints are always calculated immediately after import
- Added internal user OpenPGP public key or S/MIME certificate bulk export tool under "Administration"
- Added LFT partition resizing tool under "Administration"
- Per-customer limits for encryption and large file license
- Templates can now set subject and add custom attachments / inline files
- A new system template for policy-based bounce was added
- System default templates can no longer be deleted
- System default templates may be customized per mail domain
- The system info on the "Home" page will now show current memory usage and load averages
- The "Home" page will periodically refresh and show firmware update progress
- Firmware update progress is now fully accurate in terms of percent downloaded
- The import and create pages for "SSL" and "CA" have been separated for clarity
- X.509 Root Certificates now has a retention policy setting for expired certificates
- The mail queue page under "Syslog" now shows a count of all (filtered) mails and their active / hold state
- Security hardening of the admin login process and authorization tokens

MPKI:

- Added support for DigiCert client premium
- MPKI settings move from "CA" to "MPKI" in the menu
- Replaced and unified the client used for issuing MPKI requests
- Treat expired certificates like revoked certificates during auto-renewal

GINA:

- GINA domain settings move from "Mail Processing" to "GINA domains" in the menu
- The user profile welcome page was removed from the GINA portal
- Login will now open the write mail page by default if this page is enabled in the settings
- Support web.app?rcpt= parameter in Base64 encoding to prefill the recipient field after login
- Secure attachment works by default since iOS 11, help button is no longer necessary
- A new password reset option was added: Reset by E-mail verification, no reminder question/answer
- The non-table e-mail layout has been removed as it is incompatible with the newer mobile layout
- Language selectors will now hide if no languages were selected and the default language is used exclusively
- Reduced downtime of GINA portal when reconfiguring GINA domains on installations with multiple domains
- The PDF format was added to the list of possible mail export formats
- Always show maximum attachment size in GINA portal
- Hide mail export in GINA when viewed via iOS
- Fixed ico file import in GINA layout editor

LFT:

- Available operational modes simplified to be either "secure" or "plain"
- The subject tags for "lfm:crypt" and "lfm:nocrypt" have been removed
- Two new customizable subject tags have been added to force or prevent LFT
- In plain mode, enabled GINA subject tag can force "secure" mode
- In secure mode, enabled plain subject tag can force "plain" mode

- In secure mode, enabled plain subject tag can force "plain" mode
- All previous improvements have also been made operable via headers
- Transfer can now be rejected via custom rules for unauthorized users without consuming a license
- Separated automated threshold for incoming and outgoing mails to be set individually
- All messages can now be exported like their GINA counterparts, but will not include the attachments

Rule Engine:

- Warnings are now issued after major upgrades to regenerate the ruleset for the current version
- Improved internal mail encryption to deliver fully encrypted mails to gateway via Outlook plugin
- New function createkeys() to ensure key creation without calling createaccount()
- Tag messages as secure when crossing customer domains on the same appliance
- PGP/MIME can now be set as the perferred outgoing mail format instead of inline PGP
- The reject() rule command alias has been removed, please use drop() instead
- It is now possible to declare reusable macros in the custom commands

Version 8.8 (Released 2017-10-30)
(new in 8.8)

This is the End-Of-Life release for version 8. Appliances with small disk sizes of under 5 GB (VM 500) are not able to perform the upgrade to version 9 due to lack of available disk space and must therefore be cloned to a new appliance using the "clone device" feature found under "administration".

Use a 9.x image to clone any existing 8.8 appliance which is not capable of upgrading.

- Fix a performance issue in GINA portal with large number of mail domains
- Always fall back to admin mail on GINA password reset if self-registered
- Correctly interpret MPKI generation result in all cases
- Target version 9 for subsequent firmware updates

Version 8.7 (Released 2017-09-27)
(new in 8.7)

- Restore secure tagging for internal GINA replies
- Fix an error on password reset in GINA interface
- Improved mail score of GINA mails
- Treat attached messages correctly during LFT processing
- Allow to import same GINA account for multiple customers
- Sort OpenPGP and S/MIME count in user listing numerically
- Improved S/MIME logging for undecipherable messages
- Make POP3 fetch interval configurable in mail system settings
- Reprocess attached S/MIME encrypted messages automatically
- Added managed domain encryption status to overview
- Show X.509 root certificates as undefined even when they are orphaned
- Correct edge case in subject tagging with multiple encodings
- Skip spam scan for known active correspondents
- Skip spam scan for mail size over 1 MB
- Always use first NTP server in forced time sync

Version 8.6 (Released 2017-08-31)
(new in 8.6)

- Improve S/MIME and OpenPGP import process
- Mark installed root chain certificates as orphaned if their signing certificate is missing
- OpenPGP keys without an expire date were falsely presented as expired

- Correctly restart the key server on a rules reload
- Use UTF-8 encoding for SMS connector when needed
- Add all currently locked GINA accounts to daily report
- Correct error in GINA user import
- Fix edit of relay hosts in managed domains
- Let user and certificate cleanup tasks log to the new system log
- Fix special character handling in SNMPv3 user name and password
- When user-based S/MIME and OpenPGP is turned off completely still create users required for GINA encryption
- Slightly change the subject MIME encoding to always preserve whitespaces between words
- Add additional hostnames for virtual hosting GINA domains
- Change the managed domain certificate update interval from 12 to 6 hours
- Allow to specify requested header in managed domains
- Allow larger input in recipient mask for key server search
- Remove JavaScript from secure GINA attachment to avoid false positives in antivirus software
- Fix GINA edge case in improper invalidation of criteria during password change
- Improved content type detection for PDF attachments in the GINA GUI
- Security hardening of the GINA GUI
- Shorten navigation link names in GINA GUI
- Allow to export secure LFT mail without attachments

Version 8.5 (Released 2017-07-21)
(new in 8.5)

- Allow selection of default S/MIME digest: SHA-1, SHA-256, SHA-512
- Fix certificate generation regression for internal CA
- Improve file system synchronisation in VM scenarios
- Add loading indicator for mail log detail dialog

Version 8.4 (Released 2017-07-14)
(new in 8.4)

Admin:

- Download GINA translation with all applied modifications
- Run GINA reconfiguration in the background for faster editing
- Made AlgorithmIdentifier optional in X.509 root CA import
- Better ZIP and PB7 handling in X.509 root CA import
- Added missing text inputs for S/MIME certificate and OpenPGP key imports
- Support for daily log file rotation and cleanup
- Show mail log entries even if they miss a host name
- Improved coloring of re-injected and bounced mails in mail log
- Fixed parsing of log files that resulted in wrong years to be shown
- Show mail log details in an embedded dialog to retain search filter
- Added a system services log file
- Added a lock/unlock history for GINA users to the daily report
- Fix OpenPGP key generation for e-mails with unusual characters
- UTF-8 support for GINA domain descriptions
- Allow to filter external S/MIME and OpenPGP domain keys
- Prevent the DNS resolver from sending queries in forward mode

Managed PKI:

- Fixed auto-renewal of local OpenPGP keys and SCEP certificates

- Improved error reporting on connection errors
- Abort auto-renewal after too many failures

GINA/LFT:

- New setting to allow self-deletion of GINA accounts
- Fix display of special characters in status mails
- Increased the size of the company logo in the default CSS
- Make inline images responsive so that they always fit the screen
- Interactive confirmation dialog for user key/certificate removal
- Added a preview button to each attachment for in-browser viewing
- Visually indicate password confirmation match during register, edit and reset
- Do not advertize expired S/MIME certificates and OpenPGP keys during search
- Prevent sending the same LFT notification multiple times in a cluster
- Unconditionally sign all messages and notifications when forced sender is set

Rule Engine:

- Allow selection of default S/MIME cipher: 3DES, AES-128, AES-192 and AES-256
- Allow CIDR notation for postfix access map
- Use access maps for HELO checks
- Improved detection for S/MIME encrypted mails
- Improved matching for user and domain certificates
- Log issuer and serial number of decrypted S/MIME messages
- Move user creation to the top of IME handling
- Stop renaming ASC files during OpenPGP decryption
- Better umlaut handling in subject tags for mixed encodings
- Allow override of subject in autoreply()

Version 8.3 (Released 2017-06-01)
(new in 8.3)

Admin:

- Permit bulk import of single PKCS#12 file
- Ask for old password to be able to set a new one
- Allow import of OpenPGP keys without email addresses
- Only allow download of public certificate in SSL settings
- GINA HTTPS proxy input field validates host name or IP
- Make X.509 User, Root and OpenPGP tables sortable
- Handle import of domain certificates case-insensitive
- Allow limited / unlimited search in mail log
- Show last mail sent in user list
- Correct CSV import of users
- Allow to filter TLS domain display
- Fix MPKI proxy setting affecting the proxy setting for updates
- Improved MPKI SSL connection error reporting

GINA:

- Prevent import of same GINA users into other multi-customer accounts
- Enable mobile layout automatically when no custom CSS is been specified
- Gracefully handle special characters in attachment names
- Show error when creating a new GINA domain without having a default host name set

- Alternative logging of proxied IP addresses
- Allow the HTTPS proxy to work with the new mobile layout
- Avoid UTF-8 file name encoding for secure attachment if possible
- Always use windows CR/LF when downloading EML file
- Correctly embed inlined images into encrypted mails
- Removed custom URL from SMS settings
- Support SMS link for e-mail passwords
- Added language preselection for SMS link

Rule Engine:

- Support IPv6 servers for mail relay
- Prefer resolving IPv6 servers in relay if DNS was set to prefer IPv6 also
- Warn about use of AES-256 as it may not always be supported by the receiver
- Factor GINA mail size into mail log size message
- Strip subject tag [priv] where [emptypw] is also stripped
- Allow to use the characters "{" and "}" in e-mail addresses
- Fix integrity issue with writing MIME structures
- Correct CR/LF in OpenPGP and GINA encryption
- Eliminate duplicate Message-ID header if present in encrypted mail
- Accept CIDR notation for welcomelisting spoofed/spam domains
- Allow specifying subject in notify headers
- Update Postgrey welcomelist domains and senders

Version 8.2 (Released 2017-03-29)
(new in 8.2)

- fix display of double-encoded UTF-8 in OpenPGP user ID
- sort drop-down selectors in multi-customer edit
- fix publishing of managed domain certificates
- improve error reporting in the SwissSign CMC connector
- solely use display name for GINA default recipient selection
- fix rare case of false positive invalid S/MIME signature
- force CR/LF line endings for increased S/MIME signature compatiblity
- slightly improve generated MIME headers

Version 8.1 (Released 2017-03-21)
(new in 8.1)

- Show outgoing mail server name port when not equal to 25
- Show correct setting for GINA initial mail password length
- Properly delete previous cluster inconsistency messages
- Fix import of PKCS#12 user key when CA certificate is present
- Revert Postfix hardening to prevent TLS handshake errors
- Create all existing partitions on device clone
- Allow "mobile-optional" to also remove mobile number from GINA profile
- Fix missing subject/message after file upload while writing GINA mail
- Avoid potential cropping of company logos in GINA attachments
- Properly detect PDF in GINA attachments

Version 8.0 (Released 2017-03-17)
(new in 8.0)

This release features a completely new GINA frontend. To activate it edit the GINA layout and select "Use mobile-friendly web templates". Please note that this will also reset all previously applied CSS changes.

The old GINA frontend is scheduled for removal in an upcoming major release.

Admin:

- new mail processing GINA domain table overview
- correct case sensitivity error in group editing
- correct problem with text input of OpenPGP keys
- option to disable the encryption feature for external S/MIME certificates during import
- option to disable the encryption feature for external OpenPGP keys during import
- add comment field to relay network entries
- correct problem with X.509 certificate import with long lifetimes
- simplify e-mail security settings to avoid ambiguous behaviour with account security section
- improved IPv6 handling in mail routes
- the language reset button for GINA domains moved to the overview page
- import all e-mail addresses within OpenPGP keys
- device clone feature for simplified hardware / virtual machine migration
- properly report that non-RSA X.509 certificates cannot be imported
- warn about in-use GINA domain during deletion confirmation
- warn about in-use disclaimer during deletion confirmation
- correctly handle out of range disk space system readings on home section
- changed active encryption user count to only include active users of the last 6 months
- allow to make each key server lookup optional via ruleset generator
- add group membership info to daily report CSV
- only one cluster member will automatically renew MPKI certificates
- various help text corrections and improvements

GINA:

- new mobile friendly and accessibility-aware layout based on Twitter Bootstrap
- always show native language in drop-down selection
- disable password reset link after first use or successful login
- allow removal of logout and key search menu items via CSS
- allow removal of name and mobile number during registration via CSS
- allow removal of previously set language selectors for login/registration via CSS
- optional contrast improvement for accessibility in mobile layout via CSS
- predefined security questions for new layout
- support multiple servers for external authentication
- the password send app is now translatable into the default domain language
- added feature to present default recipients when writing mail
- display of remaining attachment size when writing mail
- added upload progress bar in secure attachment
- provide both UTF-8 and ASCII fallback name for secure attachment
- suppress login page if logout was selected
- suppress login page if an error occurred while not logged in
- display mail server reject reason in user error message
- add password quality indicators in new layout
- make the initial password length a per-domain setting

LFT:

- add 24 hour pre-expiry notification delivery status notification
- clean up all cached incoming files after 4 hours
- fix potential upload problem with very large files

Rule Engine:

- fix disclaimer() top argument handling
- fully deprecate the use of reject() in favour of drop()
- prevent OpenPGP decrypt from consuming too much memory
- correctly match on ISO-encoded subjects with special characters in trigger text
- improved trigger text removal within subject lines
- compatibility fix in OpenPGP for K-9 mail app for Android
- partoftype() now completely removes ZIP files with matching content instead of rewriting the attachment
- clarify the bounce log entry by not mentioning recipients as the whole mail is being bounced
- allow use of variables in setheader()

Version 7.4.8 (Released 2016-11-22)
(new in 7.4.8)

Admin:

- corrected problematic encoding of characters in PGP keys
- user listings can now be sorted by each individual column
- correct spurious admin GUI errors on factory reset
- redirect to administrator page after issuing shutdown, reboot or factory reset
- support for downloading of log messages from the last 30 days only
- added confirm dialog for canceling a certificate signing request
- allow to assign / release all accounts for for a customer in multi-customer environments
- correct date and mime type in backup mail
- improved mail log filtering results display
- tweaked spacing in admin GUI header status messages
- correct default logout time in GINA settings
- added SFTP support to backup user login
- added SFTP support to LFT archiver

Managed PKI:

- fixed QuoVadis revoke to adhere to correct domain-specific setting
- added option to automatically request MPKI keys for users without certificates for QuoVadis and SwissSign CMC
- added root certificate import to QuoVadis and SwissSign CMC
- fixed encoding in certificate signing request for QuoVadis

GINA/LFT:

- switched translations to full UTF-8 for non-latin language support
- translations can now fallback to English if no translation was found
- added Russian and Czech translation
- fixed redirect for multiple hosted domains when URL was not ending with a trailing slash
- added help button in iOS Mail preview
- support iOS banner on GINA landing pages
- fixed possible truncated download in GINA attachments

Rule Engine:

- correct domain encryption when GINA and user-based S/MIME disabled
- splitrecipient() now supports setting To header for each CC entry
- generate unique message IDs for all duplicated emails
- adhere to RSA/4096 bits when generating PGP keys unless specified otherwise
- lowered threshold for recursion when checking archived files with partoftype()
- remove duplicated part in bounced emails
- bounce if signing fails before creating GINA account
- properly handle PGP decryption when malformed input was found
- added the autoreply() rule engine command
- run SPF checks after greylisting

Other:

- keep track of non-created users that send mails
- remove 3DES from allowed web server ciphers
- updated OpenSSL to version 1.0.2j

Patch Release 1 (Released 2016-11-25):
(new in 7.4.8.1)

- Re-enable Nagios plugin
- Revert backup to scp (sftp support will be added for next release)

Patch Release 2 (Released 2016-12-21):
(new in 7.4.8.2)

- correctly separate sessions for GINA domain edit pages in multicustomer mode
- build domain groups for S/MIME domain encryption to prevent duplicate mails
- direction indicators for sortable user listings
- New Ruleset compiler option to exclude calendar entries from opportunistic encryption
- auto-focus and enter key support in reboot/shutdown/factory reset
- fix display of active support connection hint after reboot
- correct SwissSign CMC revoke per product domain
- correct a bug that would prevent a backup restore
- remove [sign] from subject also when sign all is used
- do not include sender in reply-all recipient list in GINA
- correctly remove previous CC and Sender in bounce mail
- remove [nosign] from calendar entry
- only bounce header of mails in Postifx
- correct a bug that would prevent PGP key import

Version 7.4.7 (Released 2016-08-18)
(new in 7.4.7)

NOTE: If you are using OpenPGP signing, prompt update is recommended

- GINA password per email feature added, allows individual passwords per email without user registration
- New, enhanced rule compiler with support for comments, procedures etc.
- fix SMTP authentication
- SNMP now properly advertizes mail statistics
- Adjusted RAM warning threshold

- ignore NDRs for welcomelisting
- do not send identical watchdog messages every 10 minutes
- use postmaster address as virus scanner notification from address
- Security fix for OpenPGP: fix a rule engine bug that could result in sending unencrypted attachments in rare cases when legacy keys are used and attachments could not be signed

Version 7.4.6.1 (Released 2016-07-21)
(new in 7.4.6.1)

- POP3 fetcher
- Smarthost port
- backup copy using scp
- SSL CSR import
- save of system comments
- support for Kentix SMS gateway

Version 7.4.6 (Released 2016-07-08)
(new in 7.4.6)

Admin:

- Added Nagios Remote Executor Plugin support
- Show active support connection on every page
- x509 root certificates are now ordered per trust state and alphabetically
- Autofocus and enter support for various filters and login screen
- Filter for managed domains listing
- Read-only admins can now change their passwords
- Read-only admins can now apply mail log filters
- Rearranged mail log navigation
- Added feature to filter and delete queued mails

Managed PKI:

- Correctly set static subject in new SwissSign MPKI on manual override
- Product name can now be set per domain for new SwissSign MPKI
- Separate proxy settings for MPKI connectors

GINA:

- Allow users to disable their uploaded S/MIME certificates or OpenPGP keys
- Added customer association to user creation message in logs
- Attachment download now reports the download size
- Do not allow users to log in directly after a password reset trigger
- Can now set preferred type for user key upload to exclude a certain technology
- Language selection is no longer displayed if previously given in web interface
- Added Cc to displayed messages
- Allow change of secure attachment name per domain
- Fixed display of unicode characters in SSL certificates, CA and CSR
- Ruleset generator for script file blocking
- Proxy setting now honoured by spam filter update

LFT:

- Delete LFT users older than 30 days
- Added Cc to displayed messages

Rule Engine:

- Prefer sender header to from header for authentication
- Multiple alt names for email in S/MIME certificates and OpenPGP keys
- Immediately adhere to OSCP check outcome
- Allow to specify digest when signing mails

Protection Pack:

- Add unofficial signatures for ClamAV virus protection

Other:

- Base system update
- DNS service has been added to watchdog
- Webservers have been added to watchdog
- Low swap warning was added to watchdog
- Migrated SNMP from net-snmp to OpenBSD snmpd
- Activate sender verification for newer exchange servers
- Periodic time sync option to address clock skew in Hyper-V VMs

Version 7.4.5 (Released 2016-05-04)
(new in 7.4.5)

- The security patch applied in 7.4.4 was incompatible with some ASN structures. This leads to problems with some encrypted mails. This patch update resolves this problem. We apologize for any inconvenience there was only time for basic QA testing for 7.4.4

Version 7.4.4 (Released 2016-05-04)
(new in 7.4.4)

Security update. Fixes the following OpenSSL / LibreSSL issues:

- Memory corruption in the ASN.1 encoder (CVE-2016-2108)
- Padding oracle in AES-NI CBC MAC check (CVE-2016-2107)
- EVP_EncodeUpdate overflow (CVE-2016-2105)
- EVP_EncryptUpdate overflow (CVE-2016-2106)
- ASN.1 BIO excessive memory allocation (CVE-2016-2109)

We recommend all customers to update to 7.4.4 promptly.

Version 7.4.3 (Released 2016-04-26)
(new in 7.4.3)

- Significant performance enhancements (for all platforms)
- Enhancements in SwissSign and QuoVadis MPKI
- Allow to use mail queue partition on second disk
- Fix GINA without reminder/answer
- Allow to use expired PGP keys for encryption
- Fix authentication / user creation for users with subdomains
- Allow to disable GINA for a single managed domain

Version 7.4.2 (Released 2016-04-08)

(new in 7.4.2)

- Fix Preview of GINA layout in GUI
- Add sender based routing
- Fix display of Users in Admin GUI for large number of entries
- Allow automatic unregistered GINA account cleanups for single customer environments
- Allow to bind admin GUI to specific IP
- Enhancements in file type detection
- Allow to specify specific postfix settings in Admin GUI
- better error handling when local or remote LDAP fails

NOTE: unlike older versions, user authentication is done using the mail address in the "From" header instead of the envelope address. If you use LDAP lookups to check if a sender is allowed to encrypt mails you should use "$from" instead of "$sender" in LDAP queries.

Version 7.4.1 (Released 2016-03-10)
(new in 7.4.1)

NOTE: For security reasons, TLSv1 is diabled for the admin GUI (and the GINA GUI if PCI ciphers under mail processing is enabled) . Use a recent browser to access the GUI (e.g. IE 9 will not work)

Managed PKI:

- Added SwissSign CMC MPKI connector

Protection Pack:

- Added SPF (Sender Policy Framework) feature to Antispam
- Added check for spoofed domains

Admin GUI:

- Fixed rare case of GINA log dates not showing the correct year
- Encryption counter improvements, now also counts HIN and Incamail
- Fixed CSV import preview behaviour for users and GINA users
- Fixed time display on lockout messages in GINA GUI
- Fixed time display in audit log and reversed order for consistency
- Improved LFT settings behaviour on save in admin GUI
- Added settings to allow specific servers / networks to send from a specific domain
- Fixed display of full name in group listing and edit view
- Display users by ID in customer admin selection for unambiguous select
- Don't display disabled user / password input block when already logged in

Rule Engine:

- LDAP commands now failover if server not reachable / timed out
- Show details in log if S/MIME signature verify fails
- Allow emptypw param in subject when sending LFT from GINA
- Fixed replace of PLAINTEXT and CREATEGPGKEYS templates in custom rule set
- Corrections in ruleset if user-based S/MIME and PGP disabled
- Added option to consider forced TLS as encrypted
- Prefer stronger AES256 for OpenPGP when applicable

GINA technology:

- Moved "Send copy to myself" option beneath send button in GINA interface

Version 7.4.0 (Released 2016-02-15)
(new in 7.4.0)

Main features added:

- Added LDAP key server feature (S/MIME and PGP)
- LFT can now archive to an external server
- New security level for GINA: reset by SMS without question/answer
- Allow multiple NTP server entries
- Cache LDAP connections
- Avoid signing of Outlook calendar sharing requests
- Added audit log page
- Extend S/MIME certificate management to be able to automatically deduplicate certificates
- Extend S/MIME certificate management to be able to automatically delete expired certificates
- Allow automatic unregistered GINA account cleanups per customer
- Added a backup user to download backups via SCP
- Added GINA domain setting to override the sender for GINA emails

Admin GUI:

- Added comment fields for S/MIME certificates
- Allow leading numbers in domain names
- Allow to change a user's ID
- Allow to filter mail log entries by colour
- Cap number of user accounts displayed on overview pages
- Changed date formats in admin GUI to consistently use ISO 8601
- Fix certificate import with special control characters
- Increase file size restrictions of import forms
- Mail size in log now properly accounts for all types of attachments
- PGP Import and delete now properly refreshes the overview page
- Show log entry number on details page
- Correctly sort users when adding to group
- Allow to specify multiple syslog servers for forwarding

Crypto Engine:

- Don't corrupt PGP attachments on decrypt when files are incorrectly tagged as text files from sender
- Change default OpenPGP keysize to 4096

GINA technology:

- Added real IP to access log when using reverse proxy (X-Forwarded-For)
- Adjusted the GINA login failure messages to not leak account information
- Allow creation of local accounts from managed GINA domains that have external authentication enabled
- Alway set Strict-Transport-Security header with max-age 30 days
- Fix password reset link in e-mail verification
- Fixed GINA attachment filenames with special characters for IE11
- Fixed GINA email sending in IE 9 and below
- Further harden HTTP requests against XSS
- Restrict CORS headers to hostname and GET,POST,HEAD method if requested
- Verify phone number in GINA account details

Rule Engine:

- Adapt replace_sender() to work like replace_rcpt()
- Added rule set generator option to automatically sign using PGP after encryption
- Allow attachmail for bounces as well
- Allow evaluation of regular expressions in replace_rcpt()
- Allow usage of @NOSIGNTEXT@ and @NOENCTEXT@ in custom rule set
- Don't generate GINA accounts when license is invalid or sender is not allowed to encrypt
- Fix template selection in encrypt_webmail()
- Respect nosign flag for GINA mails

System:

- Added device ID to backup filename
- Added log message if no PGP key was found for a domain
- Allow to specify threshold for load balancer
- Automatically copy initial console network setup to GUI system settings
- Extended SMS service support
- Multi-customer support for backup features

Version 7.3.3 (Released 2015-12-04)
(new in 7.3.3)

- Make sure named is always restarted correctly when saving settings in system and local zones are defined

Version 7.3.2 (Released 2015-10-23)
(new in 7.3.2)

- Allow to specify threshold for load balancer, lower default threshold to 4 connections
- Add support for simmcomm sms provider
- Ignore revoked S/MIME certificates when signing
- Fix import of certificates with special characters

NOTE: Security update for libressl (CVE-2015-5333 and CVE-2015-5334)

Version 7.3.1 (Released 2015-08-27)
(new in 7.3.1)

- Fix a bug in the SwissSign MPKI for silver light certificates
- Fix shutdown by amdin GUI
- Increase stability of SNMP daemon

Version 7.3.0 (Released 2015-08-13)
(new in 7.3.0)

- Update base system
- Enhanced css templates for GINA mails (optimized for Outlook)
- Add support for www.sms4.de
- Allow to specify HELO
- IPV6 support
- Add support for Safenet HSM encrypted LDAP partition
- Allow to exclude specific ClamAV patterns
- Allow to block executable files in mails

- OCSP / CRL checks
- Enhanced S/MIME certificate information in GUI
- Allow to use $recipient as a variable in LDAP queries
- Add QuoVadis MPKI support
- Add SCEP MPKI support (e.g. for Microsoft CA)
- Add domain-specific paramters to SwissSign MPKI
- Enhancements in HIN connector

Version 7.2.4 (Released 2015-06-22)
(new in 7.2.4)

- Fix character set issues in GINA GUI
- Performance enhancements for Microsoft Hyper-V appliances
- Update ClamAV engine
- Security update for CVE-2015-1788,CVE-2015-1789 and CVE-2015-1792
- Correctly create user account for IME when sending from new account
- Changes in HIN connector

Version 7.2.3 (Released 2015-06-03)
(new in 7.2.3)

- Update apache to version 2.4.12
- Show creator in GINA account overview
- Add support for www.sms4.de sms provider
- Fix an error in max mail size calculation for LFT

NOTE: Security update for logjam vulnerability

Version 7.2.2 (Released 2015-05-09)
(new in 7.2.2)

- Fix decryption using expired OpenPGP keys
- Fix type check in archives
- Fix SOAP connector for attachments with special characters in name
- Allow to specify HELO name
- Add command to add SwissSign intermediate certificates

NOTE: If you use the SwissSign MPKI connector you should add the new SHA2 intermediate certificates. You can add them manually under "X.509 Root Certificates" or click "Add or update" in "CA" "External CA" "Configure MPKI" "SwissSign Connector" "Settings"

Version 7.2.1 (Released 2015-04-24)
(new in 7.2.1)

- Allow underscore in GINA admin mail address
- Show hint if password reset is attempted by locked GINA account
- Correct URL in GINA pw reset / init mails when using virtual hosting
- Fix log file download (remove trailing HTML code)
- Fix log search for IP addresses
- Fix load balancer activation when using chrome browser
- Fix backup import for multi-tenancy
- Fix sync of LFT files in cluster
- Limit uploaded certificates/openpgp keys to max 5 MB in GINA interface
- Add support for domain encryption for subdomains with one single key
- Allow to edit mail addresses for OpenPGP public keys
- Enhancements in LFT

- ~~Enhancements in LFT~~

Version 7.2.0 (Released 2015-03-30)
(new in 7.2.0)

- Add option to authenticate internal GINA or LFT against with LDAP / AD server
- Send Samhain messages to syslog server
- Allow to set max LFT message size (independant from SMTP max message size)
- Relallow GUI over http
- Enhancemenet in LFT file upload: Disable send and attach buttons during send/upload operations, add spinning waiting indicator
- Add audit user functionality (readonlyadmin group)
- Disable autocompletion in admin GUI
- Some cosmetic changes in admin GUI (mainly add some help texts)
- Make sure smtpd is correctly restarted after config changes
- Patch for CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288 and CVE-2015-0289 for libressl
- Patch https://www.openssl.org/news/secadv_20150319.txt (note: openssl is only used internally, no services unsing openssl are reachable over the network)
- Note for customers with reverse proxies: New file [URL]/img/waiting.gif, new elemets on write-mail page: id="messageBody", id="subjectText", id="input-add-recipient", id="submit-add-recipient"
- Automatically renew OpenPGP keys
- Add support for domain encryption for subdomains with one single key

Version 7.1.2 (Released 2015-03-06)
(new in 7.1.2)

- Revert change for signature algorithm for S/MIME as there are too many systems around which cannot handle SHA-256

Version 7.1.1 (Released 2015-02-15)
(new in 7.1.1)

- Update clamAV
- Stability / DOS enhancements for GINA / LFT interface
- Progress bar for File uploading in GINA GUI
- Performance enhancements for ESX (no multiprocessor support)
- Update apache to version 2.2.29
- Change default signature algorithm for S/MIME to SHA256

Version 7.1.0 (Released 2014-12-15)
(new in 7.1.0)

- Update base system
- Switch from OpenSSL to LibreSSL
- Enhancements in LFT
- LFT without authentication (use [lfm:nocrypt] in subject to trigger)
- "Reply all" function for GINA

Version 7.0.4.2 (Released 2014-12-03)
(new in 7.0.4.2)

- Correct log detail display for rejected mails
- Fix date and character set in msg download in GINA
- Fix SwissSign revocation for certificates with odd serial numbers

- Do not detect mails with spoofed domains as virus
- Monitor snmpd in watchdog

Version 7.0.4.1 (Released 2014-10-20)
(new in 7.0.4.1)

- Completely remove sslv3, even from opportunistic postfix TLS
- Correct a bug when tagging a subject that contains double quotation marks
- Repair statistics for GINA mails

Version 7.0.4 (Released 2014-10-10)
(new in 7.0.4)

- SNMP V3
- Enhancements in HIN connector
- Notify in GUI if important settings are missing (postmaster address, DNS)
- Add filter for GINA ausers in admin GUI
- Allow sending sms through proxy
- Enhancemenets in SOPA connector
- Make virus scan use less memory
- Final changes for PCI compliance
- Allow disks larger than 1TB for LFT partition
- Allow domain cert refresh over https

Version 7.0.3 (Released 2014-09-05)
(new in 7.0.3)

- Fix backup restore
- Check size of attachemnts uploaded in GINA GUI
- Allow to enable / disable vmware tools
- Allow firmware upload in admin GUI
- Include cutom files in backup
- Speed up display of log details
- Enhancements in outlook message download in GINA
- Make sure domain encryption counters are used for non-registered users (until now domain encryption was only counted if sent / received by a registered user)
- Optimize backup file size
- Show list of recently used managed domain keys
- PCI: Allow LDAP partition unlocking over network
- openssl security fixes (see http://www.openssl.org/news/secadv_20140806.txt for details)

NOTE: This update includes openssl security fixes. Prompt update is recommended

Version 7.0.2 (Released 2014-08-04)
(new in 7.0.2)

- Show LFT user in admin GUI
- Do not create Encryption users when using LFT
- Show max possible message size in GUI
- Introduce teaming for network adapters
- Updated CSS files for better compatibility
- Correct sms link in multi-tenancy environment

Version 7.0.1 (Released 2014-07-12)
(new in 7.0.1)

- Enhancements in mail-to-sms service
- Add auto-renewal function for LFT keys
- Log console commands to audit log
- Enhance postfix TLS (custom dhparams)
- Changes for 2500B and 5000B hardware
- Allow deletion of users with S/MIME or OpenPGP keys
- PFS for SMTP
- Fix splitrecipients command
- Fix backup download in GUI
- Fix a bug in OpenPGP decryption and key creation

Version 7.0.0 (Released 2014-06-27)
(new in 7.0.0)

- Make multi-tenancy available in default version
- Password rules for admin users including password history
- Password history / forced password change for GINA users
- Encrypted database directory with boot password
- CEF (Arcsight) Logging in admin GUI
- GUI timeout configurable
- Non-ambiguous initial passwords for GINA
- Samhain integration
- Update base system
- Support for ESX VMNET3
- Support for ESX paravirtual SCSI

Version 6.5.5.7 (Released 2014-07-16)
(new in 6.5.5.7)

- Allow deletion of users with keys / certificates

Version 6.5.5.6/6.6.5.6 (Released 2014-06-13)
(new in 6.5.5.6)
(new in 6.6.5.6) multitenant version

This update addresses CVE-2014-0224 and several other openssl security issues. Customers who are using the local proxy (under System/Advanced/GINA https Protocol/Enable local https proxy) should update as soon as possible.

Additional information: The openssl library used for normal operation (without local proxy) is known to be vulnerable, but appears not to be exploitable. If you are concerned about this security issue you should upgrade to this version and activate the local proxy.
If you are also concerned about the admin GUI, you can request an update to the (pre-)release version 7.0.0

Version 6.5.5.5/6.6.5.5 (Released 2014-06-03)
(new in 6.5.5.5)
(new in 6.6.5.5) multitenant version

- Fix SwissSign revocation
- Fix Reboot issue
- Fix OpenPGP key generation

Version:6.5.5.4/6.6.5.4 (Released 2014-05-20)
(new in 6.5.5.4)

(new in 6.6.5.4) multitenant version

(Info: 6.6.x is the multitenancy version)

- Add optional "restrictive" setting for Antivirus Check (Do not allow encrypted attachments)
- Allow specifying AES-256 / 3DES in ruleset. (set parameter 3 in encrypt_smime or parameter 1 in encrypt_domain_smime to 'aes256' if needed)

Note: You have to set AES256 / 3DES in ruleset generator AGAIN if you did so in a previous version
Note: Domain encryption always uses AES256

- Optimize ciphers for PFS
- Add new command "splitrecipients" to split up mails per recipient
- Enhancements in Outlook message download in GINA
- Add new languages (Dutch, Polish) to GINA GUI
- Add possibility to automatically delete old log archives
- Make GUI filter case-insensitive
- Show fingerprint in root certificates in GUI
- Only show GINA log in GUI when requested to speed up display
- Allow LFT users to use GINA GUI to send out large files
- Fix restore: apply system settings
- Fix root certificate import in GUI
- Fix hanging OpenPGP key creation if trying to issue a key for a user with an invalid mail address
- Fix cron job (automatic update of domain certificates, backup)

Version:6.5.5.3/6.6.5.3 (Released 2014-04-24)
(new in 6.5.5.3)
(new in 6.6.5.3) multitenant version

- Patch release: under certain circumstaces, issuing SwissSign certificates with firmware 6.5.5.1 or 6.5.5.2 / 6.6.5.1 or 6.6.5.2 crashes the applaince. This update corrects this bug.

Version:6.5.5.2/6.6.5.2 (Released 2014-04-09)
(new in 6.5.5.2)
(new in 6.6.5.2) multitenant version

- Patch for CVE-2014-0160.
- Update clamav

NOTE: CVE-2014-0160 ("Heartbleed") only affects the local proxy. Update is only necessary if you do not want (or cannot) disable the local proxy under System/Advanced/GINA https Protocol/Enable local https proxy..."

Version:6.5.5.1/6.6.5.1 (Released 2014-04-01)
(new in 6.5.5.1)
(new in 6.6.5.1) multitenant version

- Correct error in setting cipher
- Automatically create LFT parition
- Enhancemenets in HIN Connector
- Add function to delete expired X.509 certificates
- Disable OpenPGP Secret key download
- Enhancements in SMS interface
- Enhancements in ldap_getcerts: Handle multiple entries with same mail address

Version:6.5.5 (Released 2014-02-24)
(new in 6.5.5.)

- Allow to set cipher for S/MIME

NOTE: Default value is 3DES as quite a lot of recipients appear to have problems with AES-256

- Reprocessing support for OpenPGP has been added
- Bug fixes in SignTrust connector
- Enhancements in internal encryption
- Allow to specify key servers in ruleset generator
- Enhance GUI performance when DNS server not reachable

Version 6.5.4.1 (Released 2013-11-11)
(new in 6.5.4.1)

- Make sure sender address is used when replying to a GINA mail

Version 6.5.4 (Released 2013-11-08)
(new in 6.5.4)

- Allow https backends for local proxy
- Perfect Forward Security for most browsers if local proxy is enabled
- Allow pkcs12 upload for ssl certificates
- Update ClamAV Engine
- Fix some minor issues in GINA GUI
- Add loadbalancer for SMTP connections
- Add filter functionality for some parts of the admin GUI
- use AES256 as default cipher for S/MIME (replacing 3DES)
- Show information about used S/MIME cipher in log

Version 6.5.3 (Released 2013-09-23)
(new in 6.5.3)

- Add a certificate cleanup function to delete unneeded S/MIME certificates
- Add function to make GINA initial password change optional
- Fix domain certificate refresh invoked from GUI
- Fix an issue with domain encryption to recipients with solutions from another vendors
- Fix log detail display
- Move AV patterns to different location

Version 6.5.2 (Released 2013-08-22)
(new in 6.5.2)

- Changes in HIN Connector
- Use RFC-compliant S/MIME encryption for S/MIME domain encryption with other gateways
- Correct a bug when using more than one GINA domains (special settings not applied to different domains)
- Performance / stability enhancements

Version 6.5.1 (Released 2013-07-06)
(new in 6.5.1)

- Changes in HIN Connector
- Make proxy for GINA PCI compliant
- Update sms connector
- Send all public keys in daily statistics
- Import public key container for S/MIME and OpenPGP

- Ldap public key retrieval for S/MIME and OpenPGP
- Better memory management for GINA mail creation
- Allow use of variables in ldap queries
- Changes for 5000B appliances
- Corrections in S-TRUST connector (cn in automated user generation, leading zeroes in serial for key revocation)

Version 6.5.0 (Released 2013-04-04)
(new in 6.5.0)

- Update base system
- Large File Transfer: Allow to send large files by mail
- Disable legacy GINA interface (old messages can still be read)
- Add audit log

Version 6.1.6 (Released 2013-01-08)
(new in 6.1.6)

- Allow to change the SMTP greeting
- Make sure log index creation is only started once on very slow systems
- Correct a html error in the GINA attachment (better compatibility with some webmail systems like gmail)

NOTE: After the update, Expect about 30% more space requirement on the log partition.

Version 6.1.5 (Released 2012-12-13)
(new in 6.1.5)

- Enhanced log search
- Enhanced S/MIME v 3.1 support for decrypting

Version 6.1.4 (Released 2012-11-29)
(new in 6.1.4)

- Enhancements in HIN connector
- Allow / keep disclaimer in OpenPGP encrypted mails
- Correctly handle pgp encryption if mail part has no character set attribute
- Fix file upload in GUI (e.g. backup restore)
- Correctly display opaque signed mails in GINA
- Enhancements in HIN connector

Version 6.1.3 (Released 2012-10-31)
(new in 6.1.3)

- Update ClamAV
- Make sure /tmp partition gets cleaned up
- Add Device ID in subject of backup mail
- Do not display question / answer in GINA registration if no question / answer is required
- Corrections in SignTrust connector
- Make admin GUI cross-site scripting resistant
- Send authlog to syslog server, include GUI and GINA logins
- Enhancements in SMS sender
- SMS text for passwords can now be edited

Version 6.1.2 (Released 2012-10-03)
(new in 6.1.2)

(new in 6.1.2)

- Update ClamAV
- Re-enable GINA security level without reminder / question
- Correct "last used" date in daily statistics mail
- Always use utf-8 for OpenPGP encryption
- Prevent kernel panics when restarting services with active CARP connections

Version 6.1.1 (Released 2012-08-15)
(new in 6.1.1)

- Better recognition of OpenPGP encrypted mails
- Nicer Admin GUI
- is_calendar also recognizes Lotus Notes calendar entries
- Changes in HIN Connector
- Update Clam Antivirus
- Allow setting headers in ruleset generator
- Fix Backup Download

Version 6.1.0 (2012-05-22)
(new in 6.1.0)

- Completely remove cookies for GINA
- Allow Wildcard certificate creation for ssl
- Add Spanish as GINA language
- Add Support for S-Trust MPKI
- Add Support for SignTrust MPKI
- Enhanced sms password support (allow to specify mobile number in subject, pre-store numbers entered in sms link and subject, send sms from Admin GUI)
- Allow to add comments for CA and OpenPGP keys in GUI
- Enhanced group editing
- Enhancements for HIN connector
- Create nightly backup without restarting services
- Use signed domain certificates for domain encryption (instead of self-signed)
- *Note: If you are planning to use domain based encryption with java based secure e-mail gateways from other vendors, you should create new domain keys after updating. You do not need to revoke / delete the exiting keys.*
- Allow searching domain keys in GINA portal
- Enhanced sms support (allow sending OTP to sms from Admin GUI)
- Recipient does not have to enter mobile number if password reset is set to "let user choose between sms and hotline"
- GUI used to send sms can be made accessible in public interface
- Bulk import for S/MIME certificates

Version 6.0.0 (2011-11-10)
(new in 6.0.0)

- Base system update
- VMware tools
- New Enhanced Secure Webmail viewer (called GINA)
- Outlook plugin available (http://dl.seppmail.ch)

NOTE: To enable the new webmail interface "GINA", activate "Use extended Webmail functionality" in "Mail Processing"

Version 5.3.7 (2011-11-10)

(new in 5.3.7)

- Changes in HIN connector
- Enhanced SNMP support
- Allow update prefetch, show download status
- Move antivirus signatures to larger partition
- Allow update / support connections through SOCKS proxy
- Allow editing hosts file in GUI
- Show number of queued mails in GUI
- Enhanced OpenPGP filename detection
- Enable DSN for delayed mails

NOTE: You should check your time zone in System / Advanced after this update

Version 5.3.6.1 (2011-10-04)
(new in 5.3.6.1)

- Hotfix for 5.3.6 Release: Make sure header changes are always written
- Enhancements for 3000B hardware
- Changes in HIN Auditing
- Enhanced recognition of special charsets in Webmail viewer
- Add correction for leap seconds to ntp
- Add bulk import for S/MIME certificates
- Show e-mail size in GUI log
- retain leading comment lines in uploaded ruleset

Version 5.3.5 (2011-07-30)
(new in 5.3.5)

- Changes in HIN connector / HIN Auditing
- Allow local DNS overriding
- Update virus engine
- Correctly handle mails that are encrypted twice
- Do not re-encrypt mails that are already S/MIME encrypted
- Automatically repair simple cluster failuers
- Corrections in ESW viewer for special character sets

Version 5.3.4 (2011-04-14)
(new in 5.3.4)

- Enhancements in HIN connector
- Correctly change filenames when encrypting text attachemnts with OpenPGP
- Only activate proxy when a correct servername is specified
- Correct an error in webmail password reset
- Only use self-signed GUI certificate if the official certificate fails to load
- Add new Ruleset generator open "Do not encrypt, but sign"

Version 5.3.3 (2011-03-10)
(new in 5.3.3)

- Enhancements in HIN connector
- Enhancements in OpenPGP attachment handling / charset handling
- Enhancements in header encoding

Version 5.3.2 (2011-01-15)

(new in 5.3.2)

- Enhancements in HIN connector
- Check outgoing mails for virusses instead of only incoming
- Correct watchdog to ignore domain refresh errors if "Auto-Update S/MIME Domain Certificates" is not checked
- Make sure S/MIME and OpenPGP keys are used if a mail is marked as confidential and "Always use S/MIME or OpenPGP if keys are available" is not enabled

Version 5.3.1 (2011-01-15)
(new in 5.3.1)

- Enhancements in HIN connector
- Allow to attach disclaimers to "in-reply-to" messages

Version 5.3.0 (2011-01-12)
(new in 5.3.0)

- Add optional HIN (Health Information Net) connector
- Update Incamail Connector to support Incamail 3
- Add OpenPGP/MIME functionality for OpenPGP domain encrypted mails
- Switch to SHA1 for TLS fingerprint checking. *(Note: You must manually change fingerprint settings if you use fingerprint checking)*
- Allow same tag for "decrpyted" and "confidential"
- Clean up mail received headers (localhost)
- Show RAID status in GUI for 3000B hardware
- Add S/MIME Version 3.1 support
- Watchdog now also watches ntp daemon
- user-friendly colors in GUI
- Allow to edit user names

Version 5.2.2.1 (2010-09-15)
(new in 5.2.2.1)

- Add line breaks in long lines in Webmail Viewer text view

Version 5.2.2 (2010-09-15)
(new in 5.2.2)

- SuisseID support for Webmail authentication
- New web server for enhanced https Support
- Show RAID status in GUI on enterprise hardware
- Allow adding disclaimer in base64-encoded emails

Version 5.2.1 (2010-06-21)
(new in 5.2.1)

- Daily reports are sent to members of group statsadmins (and to members of gorup admin and the postmaster if they are important)
- Enhancements in displaying embedded graphics in secure webmails
- New rule engine wizard option "create all users"
- New rule engine command to parse email body
- Allow sending virus notifications to a pre-defined email address

Version 5.2.0 (2010-04-30)

(new in 5.2.0)

- Update base system
- Consolidated statistics in clustered environment
- Display embedded images in webmail viewer
- Strictly use POST instead of GET in webmail viewer
- Text-only webmail container
- Allow to disable msg download in webmail viewer (note: Defaults to on)
- New security level for simpler use (no question / reminder)
- PCI compliance for SMTP TLS in opportunistic mode
- Allow hiding mail subject in log files
- Enhanced watchdog with cluster connectivity checks
- New rule engine wizard option to delete smime signatures from incoming mail
- Per-user / per-domain usage counters
- New state "undefined" for unknown CA certificates
- Automatically renew locally issued Certificates if existing certificates are about to expire
- Automatically renew SwissSign Certificates if existing certificates are about to expire
- Daily status / troughput report mail
- Selective Reverse Proxy (for customers with one single IP address)
- Additional "undefined" state for auto-collected CA root certificates
- New rule engine command to disable a user

Version 5.1.7.3 (2010-01-20)
(new in 5.1.7.3)

- Revert Changes for normalized subjects in log as it leads to delayed delivery of emails if the subject is malformed

Version 5.1.7.2 (2010-01-18)
(new in 5.1.7.2)

- Allow to use non-selfsigned pgp keys
- Include Antivirus Engine in watchdog
- Display normalized subject in Log

Version 5.1.7.1 (2010-01-06)
(new in 5.1.7.1)

- Make sure spamassassin updates are fetched
- cosmetic change in SwissSign connector setup

Version 5.1.7 (2009-12-22)
(new in 5.1.7)

- Correct an issue with entering the phone number when the recipient forgets his password
- Re-schedule nightly domain certificates update to prevent update server overload
- Show last successful domain certificates refresh in GUI
- Correct an issue with S/MIME signed and encrypet mails in domain encryption mode

Version 5.1.6 (2009-12-10)
(new in 5.1.6)

- Strict input checking for Webmail viewer
- No RFC compliance check for incoming signed mails
- Template based webmail domains

- Enhancements in secure webmail password reset
- New ruleset wizard option: Do not sign single emails

Version 5.1.5 (2009-11-24)
(new in 5.1.5)

- Template-based webmail domains
- Enhancements in secure webmail password reset

Version 5.1.4 (2009-11-11)
(new in 5.1.4)

- Enhancements in pgp key generation
- Allow bulk import of OpenPGP secret keys
- Add header info about spam check
- Enhancements in disclaimer
- Prepare for base system upgrade

Version 5.1.3 (2009-10-27)
(new in 5.1.3)

- Add chain to signed emails
- Update root certificates
- Automatically purge expired root certificates
- Enhanced signature detection
- Stricter license Checking
- Allow SMTP recipient verification without antispam license
- Hide domain cert list
- Hide subject in domain encrypted emails

Version 5.1.2 (2009-09-27)
(new in 5.1.2)

- Enhanced detection of S/MIME signed / encrypted emails
- Enhanced detection of OpenPGP encrypted emails
- More detailed logging
- Display basic network configuration on console
- Small corrections in default disclaimer
- Do not sign outlook calendar entries if "sign all"
- Enhancements in SwissSign connector

Version 5.1.1 (2009-08-24)
(new in 5.1.1)

- Add support for OpenPGP/MIME for incoming mails
- Enhanced filename detection for pgp encrypted emails
- RFC conform headers in webmail viewer
- Prevent ntpd from blocking if network is unreachable
- Do not add disclaimer in replies
- Allow to trust untrusted root CAs
- Enhanced factory reset (overwrite data with random numbers)

Version 5.1.0 (2009-08-07)
(new in 5.1.0)

- New ruleset command "create key"
- Enhancements in CA including revocation and revocation lists
- Enhancements in SwissSign connectivity including revocation
- TLS logging in mail log
- Allow to disable encryption / signing for specific users
- Change pgp key sender
- Allow disabling automatic pgp key delivery for new users
- Easy "disclaimer per domain" settings
- Automatically add unknown root certificates as "untrusted"
- Added new command to remove S/MIME signatures
- Updated ruleset generator: Always use webmail accounts, mark signed mails
- Secure factory reset (10 x random overwrite of data partitions)
- Enhanced logging for certificate harvesting
- Enhanced certificate harvesting, now also works for "exotic" certificates
- Auto rollout for communication initiated by external communication partners
- Correct Carrige Return / Line feed for HTML headers

Version 5.0.6 (2009-07-02)
(new in 5.0.6)

- Include Extended user attributes in user display
- Include certificate chain in S/MIME signatures
- Correctly handle empty ldap attributes in ldap_read and ldap_compare
- Enhanced reprocess to re-decrypt emails
- change format of openpgp filenames to utf-8 when encrypting
- Enhancements in openpgp decryption
- Prepare for new Hardware with larger memory

Version 5.0.5 (2009-06-25)
(new in 5.0.5)

- New ruleset command to set extended user attributes
- enhancements in pgp compatibility
- add a workaround for PIX smtp proxy
- remember language chosen in webmail viewer
- add favicon
- CA parameters can be configured
- allow multi-value in ldap requests
- re-enable SMTP out for smarthost

Version 5.0.4 (2009-06-19)
(new in 5.0.4)

- Add zipped HTML can be activated on a per-user basis
- Automatically activate zipped HTML if the recipient uses OWA
- Optimized user generation in conjunction with ldap lookups
- Allow multivalue ldap compares
- Make sure pgp keys are only created once in clustered environments
- Re-enable disclaimer and template editor
- update some third party applications
- Use blocklist / welcomelisting entries for greylisting

Version 5.0.3.1 (2009-06-03)
(new in 5.0.3.1)

- Re-activate disclaimer
- Correct occasional problem in zipped webmail delivery

Version 5.0.3 (2009-06-01)
(new in 5.0.3)

- Allow to use SMS gateway to send webmail passwords
- Allow to use [zip] or [owa] in subject to force zipped webmail attachement
- Enhancemeents in queless mode
- Allow password reset in "Secure contact form"
- ASPSMS connection using xml to send password by sms
- Some cosmetic codepage corrections in webmail Viewer

Version 5.0.2 (2009-05-17)
(new in 5.0.2)

- Increase compatibilty for webmail with some webmail clients
- Correct display of text-only mails in webmail Viewer

Version 5.0.1 (2009-05-13)
(new in 5.0.1)

- Queueless mode can be configured with GUI
- Allow to configure default language for webmail viewer
- Allow to completely change webmail display using CSS and additional images
- Allow querying redundant LDAP servers
- Include message subjects in log display
- Allow to enable "send copy to myself" by default
- More detailed license display
- Prepare webmail for arabic language
- New "Secure Contact Form" allows user initiated webmail communication

Version 5.0.0 (2009-04-14)
(new in 5.0.0)

- Complete Incamail integration
- New ruleset wizard option: Reject mails that cannot be decrypted
- Optimize service start order
- Restrict https to high security ciphers
- Allow to specify TLS settings for internal domains
- webmail password complexity can be specified
- Additional cookie security for webmail viewer
- Add "Change Password" to login page
- Prepare for PCI compliance audit
- Optionally add webmail HTML messages in ZIP file (for OWA compatibility)
- Welcomelisting entries for greylisting
- Allow different webmail templates for same domain
- Correct bug: password mail if more than one webmail user is created
- Correct bug: Display of queued mails
- Correct bug: complex filenames in OpenPGP encrypted emails

NOTE: For PCI compliance, IE 7 or higher must be used for GUI access

Version 4.8.2 (2009-02-08)
(new in 4.8.2)

- Enhanced Frontend server
- Correct Error in Watchdog
- Disable spam checking for mails fetched from remote POP3 server
- New feature to re-process old emails that were received encrypted

Version 4.8.1 (2009-02-02)
(new in 4.8.1)

- Allow definition of sender mail addresses in password mails
- Less restrictive syntax checking for webmail replies

Version 4.8.0 (2009-01-26)
(new in 4.8.0)

- Enhancements in SwissSign connector
- Enhanced pgp key generation
- "Secure contact" frontend for external users
- Allow disabling "Powered by..." logo in User frontend

Version 4.7.1 (2008-12-31)
(new in 4.7.1)

- SNMP Support
- Automatic SwissSign CA certificate rollout
- Enhanced Rule Generator
- Queue-less mode for reinjection
- Enhanced signing key selection
- Frontend server without local database
- Include VMWare tools
- Restrict user access to defined GUI sections
- New rule engine commands for direct LDAP / AD connection

Version 4.7.0 (2008-07-25)
(new in 4.7.0)

- Antivirus Engine Update
- Enhanced virus scanning
- Exchange 2007 compatibility imporvements
- Enhanced memory management
- Minor improvements in webmail viewer
- Introduce bridging mode
- Improvements in cluster environment.

Version 4.6.1 (2008-05-12)
(new in 4.6.1)

- Better support for OpenPGP keys
- Support for intermediate certificates for ssl
- Enhanced log search
- Some cosmetic changes in webmail viewer
- Update base system
- Enhanced anti-spam features

Version 4.6.0 (2008-03-31)

(new in 4.6.0)

- Automatically fetch new license files
- Enhanced license management
- Enhancements in Antispam
- Allow site-specific TLS setup
- Allow to specify alternate SMTP port
- New, enhanced webmail viewer
- Automatically reboot after update
- Allow webmail download as outlook message files (beta)

Version 4.5.3 (2008-03-04)
(new in 4.5.3)

- allow automatic issuing of OpenPGP keys
- accelerated OpenPGP key generation
- correct small bug in Backup routine
- Allow ssh connections through http proxy
- add subject tagging of decrypted emails

Version 4.5.2 (2008-02-24)
(new in 4.5.2)

- correct small bug in Backup routine

Version 4.5.1 (2008-02-20)
(new in 4.5.1)

- Include license violation display
- New ruleset option: Do not auto-encrypt with S/MIME or oepnGPG
- Allow disabling console login
- Update notification in home section
- Introduced virtual appliances flavours
- Allow to specify a syslog server for maillogs

Version 4.5.0 (2008-01-10)
(new in 4.5.0)

- Change position of "Powered by..." logo
- Update AV Engine
- Allow to specify webmail pw length in ruleset
- Allow specification of "[emptypw]" in default ruleset
- Cleanup trigger values in subject before sending

Version 4.4.1 (2007-12-21)
(new in 4.4.1)

- Show network / carp status in GUI
- Allow mail addresses with underscore for users
- Correct statistics for domain encryption
- Correct error in GUI when first carp disabled
- Enable direct SMS delivery for webmail passwords
- Update S/MIME root certificates
- Add "Powered by..." logo to webmail display

Version 4.4.0 (2007-11-22)
(new in 4.4.0)

- Introduced a learning mode for Greylisting
- Enhanced webmail confirmations
- Allow specification of SMTP port
- Add new ruleset command "rmatch" to check recipients
- Add new ruleset command "webmail_password" to re-send password to sender
- Support for new hardware platform
- Added spam information to log files
- Added dcc and pyzor functionality to VSPP
- Include SSL/CA Certificates in Backup

Version 4.3.3 (2007-10-10)
(new in 4.3.3)

- Increase stability of SMTP daemon under high load
- Enhanced watchdog
- Optimize webmail for Firefox

Version 4.3.2 (2007-10-04)
(new in 4.3.2)

- Small bug fix (enable password reset for locked accounts)

Version 4.3.1 (2007-09-31)
(new in 4.3.1)

- Enable Postmaster warnings
- correct bug in pgp_detect
- Include mail fetcher for POP3 accounts
- Allow "low security" password retrevial for webmail
- New "queue-less" mode

Version 4.3.0 (released 2007-09-10)
(new in 4.3.0)

- Internal CA / RA
- Enhanced webmail logging
- webmail Delivery Reports
- Only accept emails for existing users
- Optional internal mailserver
- Enhanced antispam settings (PTR check)
- Ruleset enhancements: Allow force webmail encryption

Version 4.2.4 (2007-05-14)
(new in 4.2.4)

- Update base system to OpenBSD 4.1
- Enhanced performace for Appliances with CF cards
- Added italian support in webmail
- Added a rule for LDAP lookups on remote hosts
- Enhanced statistics, include CPU and memory load
- Fixed condition with non-restarting mail daemon after backup
- Fixed "too many recipients" error
- Fixed condition on the which CARP interface did not acquire host IP

- Fixed condition under which CARP interfaces did not reclaim lost IP
- Add handling for aliases in OpenPGP keys
- Minor bug fixes

Version 4.2.3 (2007-05-14)
(new in 4.2.3)

not released, see 4.2.4

Version 4.2.2
(new in 4.2.2)

not released, see 4.2.4

Version 4.2.1
(new in 4.2.1)

not released, see 4.2.4

Version 4.2.0
(new in 4.2.0)

not released, see 4.2.4

Version 4.1.0 (2007-03-26)
(new in 4.1.0)

- Generate S/MIME certificates
- S/MIME-based domain encryption
- S/MIME-based domain signature
- Anti-Spam / Anti-Virus module
- Corrected error in SMTP authentication for outgoing emails
- No clear text password in GUI for webmail passwords
- Creator of webmail accounts stored
- introduced an "expired" flag for webmail passwords
- allow http protocol for webmail
- allow specification of webmail port(s)
- Enhanced error handling in webmail reply
- Allow adding multiple managed domains in one step
- Implemented process for automated reset of forgotten passwords
- Allow permanent change of root password
- Added a restricted backup user
- Added a tmp partition on S3000 systems
- Added a permanent partition for user-specific data
- Major performance improvements
- Added functionality to archive emails
- Possibility to request a copy of a webmail reply to the sender
- Auto-generate and publish / download domain certificates
- (note: activated by default!)
- Only user with an account can encrypt E-mails

Version 4.0.0 (2007-01-31)
(new in 4.0.0)

- Registration

- Drivers for new Hardware
- Allow easy remote support connection (reverse ssh tunnel)
- Allow removal of webmail domain settings
- Add support for user-defined mail disclaimers
- Multi master cluster / load balancing
- Virtual IP Addresses based on CARP for failover
- optimized openldap indexes
- speed enhancements in webmail encryption
- allow specifying password length for webmail passwords in GUI
- allow empty webmail passwords (must be set by recipient on first use)
- Enhancements in ssl certificate generation (well, actually fixed some bugs)
- remove Windows CR/LF in cert Upload
- removed obsolete lcd driver for pyramid displays
- Allow deletion of IP addresses in GUI (thus allowing specifying empty name servers)
- fixed problem of non-responding appliance if no DNS server can be found
- Update base system to OpenBSD 4.0
- Update postfix to 2.3.6
- Update openldap to 2.3.31
- Allow webmail recipients to specify a password reminder
- changed NIC name convention
- introduced TLS support
- include revision history
- Disable password-based ssh login

Version 3.3.0 (2007-01-24)
(new in 3.3.0)

- Registration
- Drivers for new Hardware (SEPPmail 3000)
- Allow easy remote support connection (reverse ssh tunnel)
- Allow removal of SEPPmail domain settings
- Add support for user-defined mail disclaimers
- Multimaster cluster / load balancing
- Virtual IP Addresses based on CARP for failover
- optimized openldap indexes
- speed enhancements in seppmail encryption
- allow specifying password length for seppmail passwords in GUI
- allow empty SEPPmail passwords (must be set by recipient on first use)
- enhancements in ssl certificate generation (well, actually fixed some bugs)
- remove Windows CR/LF in cert Upload
- removed obsolete lcd driver for pyramid displays
- Allow deletion of IP addresses in GUI (thus allowing specifying empty nameservers)
- fixed problem of non-responding appliance if no DNS server can be found
- Update base system to OpenBSD 4.0
- Update postfix to 2.3.6
- Update openldap to 2.3.31
- Allow SEPPmail recipients to specify a password reminder
- changed NIC name convention
- introduced TLS support

Version 3.2.222 (2006-11-02)
(new in 3.2.222)

- Group management
- graphical statistics for mail throughput based on rrd

- license management / import
- Allow CSV import / batch creation for webmail Users
- introduced webmail domains ("Mandantenfaehigkeit")
- HTML support in webmail messages display
- allow empty passwords for standard users
- support for multiple relay networks
- send pgp public key by mail
- include domain encryption in standard ruleset
- enhanced log display with search / archive
- allow upload of ssl certificates
- log rotation
- added smime root certificate manager
- added trustcenter and quovadis root certificates in base installation
- initial page with basic mail statistics
- webmail logs on per-user basis
- allow specification of max mail size
- webmail recipient interface in french

Version 3.2.0 (2006-07-21)
(new in 3.2.0)

- LDIF Import
- Support for Pyramid LCD Displays
- Update to OpenBSD 3.8
- Enhancements in Backup procedure (Backup is sent by email)