CAPABILITIES REVIEW

# Unlimited | Secure Email

GFI™

Aurea SMB Solutions

GFI Unlimited|Secure Email provides key email and collaboration capabilities with the security protection companies need. It offers:

- Feature-rich email and collaboration tools: Secure platform delivers email integrated with shared calendars and scheduling, contacts management, tasks, notes, shared and public folders, and instant messaging
- Powerful multi-engine antivirus and more: Get 14 anti-spam filters, 4 antivirus engines, plus malware scanning, in one email security package
- Secure archiving to meet compliance regulations: Manage and access your organization's electronic communications history. This includes email, attachments, files, calendar entries, faxes, and SMS (text), and voice messages that are connected and logged via email.

Unlimited|Secure Email provides these through easy to use and easy to manage capabilities.  Here is an overview of some of the most critical security capabilities.

## Domain, email & connectivity encryption

Unlimited|Secure Email provides support to configure multiple domains along with DKIM authentication for each domain. In addition, sender anti-spoofing technology is built-in to protect vulnerable users from attack.

User authentication with Active Directory Integration (NTLM), Open Directory Integration, or Built-In (Digest & CRAM MD5) is available. Data encryption can be enabled on the mail stores, and finally TLS 1.3 for transmission. With access, data, and transmission fully encrypted, you can have an end-to-end secure system for all communications.

Email platform decure functionality includes:

- Password policy with complexity
- Password guessing protection
- Secure connectivity (TLS 1.3)
- Require secure connectivity
- Perfect Forward Secrecy support
- Signed and custom SSL certificates
- Encrypted email (S/MIME)
- DKIM signatures
- SMTP submission
- Directory harvest attack protection
- Sender anti-spoofing protection
- Remote mobile device wipe

## Integrated & secure access management

Active Directory and alternative directory services are available to manage users and groups, set permissions and access, ensuring you stay up-to-date with users and their status. In addition, security tools such as password expiration, complexity policies, and password-guessing prevention settings are also available.

## Multi-client & device support

Email communication, spam quarantine, and archiving user data are all available through existing clients that may be in use such as Outlook or Apple, as well as web and mobile device support. This makes it easier to use and requires less training for users.

Email client support, in addition to standard Imap/Pop clients, includes:

- Microsoft Outlook
- iOS | Windows | Android | macOS
- Apple Mail, Calendar, Contacts, Messages, and Reminders • iOS | macOS
- Android Mail • Article
- Windows 10 Mail and Calendar
- Kerio Connect Client (web based)
- Kerio Connect Desktop App Technology Preview (Mac)
- GFI Archive (web based)
- GFI Archive mobile apps (android , IOS)

Mobile device support also includes:

- Exchange ActiveSync 14.1 (option)
- CalDAV/CardDAV/IMAP client support
- Kerio Connect Sync app for Android
- Global address list synchronization
- Public and shared folders
- Automatic configuration for iOS

## Self-service email delegation & quarantine

Managing process mailboxes, shared mailboxes, and quarantines can all be provided directly to users, or to groups of users who can take action. This gives control and power to users for day-to-day simple operations and allows IT professionals more time to improve the business.

Email & calendar delegation can be provided to individual users, and those delegated users are easily managed inside email clients for easy switching. This is in addition to standard sharing capabilities which allow for shared folders, contacts, and calendars to even be visible from mobile devices.

Email security digests are sent based on frequency configured to end users: to view and release messages from being held. Only messages which are configured to be released by the administrator will have this ability, meaning user digests will not have the ability to release a message flagged as a virus.

Unlimited|Secure Email empowers users to leverage machine-learned spam detection with the Bayesian filter. It can be enabled to train continuously and automatically the advanced email threat functionality of what is, and is not, good email. By setting up public folders, users can “drag” questionable emails to train the functionality. This is all done without needing to create IT requests.

## Multi antivirus & malware protection

As Email traffic is a major source for viruses and malware, Unlimited|Secure Email uniquely provides advanced email threat protection using four antivirus engines (powered by industry winners Bitdefender, Avira, Kaspersky and Cyren).

This lets you take advantage of the strengths of each engine. Antivirus engine vendors have different response times to new viruses and malware. The multi-engine feature ensures your system can always detect new threats in the shortest possible time.

In addition to four antivirus engines, it also boasts 14+ configurable anti-spam engines which are pre-configured for optimal protection while allowing administrators to tailor them to their unique business.

- SpamRazer
- Anti-Phishing
- Director Harvesting
- Email Blocklist
- IP Blocklist
- IP DNS Blocklist
- URI DNS Blocklist
- Sender Policy Framework
- Anti-Spoofing
- Greylist
- Language Detection
- Header Checking
- Spam Keyword Checking
- Bayesian analysis
- Whitelist
- New Senders

## Advanced threat updates

Both the multiple antivirus engines and spam definitions are updated frequently to ensure you are protected from the most recent threats. The antivirus engines can be configured to check automatically for updates on the frequency you select, as well as enabling on-demand updates. You can be notified about updates for peace of mind that your security is functioning.

An “updates” tab is provided so that administrators can review and ensure their definitions are healthy and they are protected from new threats. All updates are put through a comprehensive test prior to release to ensure they pass GFI’s internal integration tests before releasing. This is conducted in nearly real-time by a team of security experts.

## Policy based content & spam filtering

Email traffic content is filtered using four advanced content filtering engines. Advanced user-based filtering rules enable flexible and granular filtering of any part of the email message--message headers, subject, body, attachment name and attachment content--using different types of pattern matching methods, including regular expressions.

You could, for example, use the keyword checking functionality to scan emails for keywords that are inappropriate, vulgar, racial, sexual or offensive. This can also serve as another spam filter if configured to block common spam keywords.

Email content filtering can also be applied to outbound emails to prevent data leakage of personal or private information using keywords related to credit cards, personal identification numbers and more.  This is in addition to filtering outbound messages in the event of having been exploited as an smtp relay.

## Automated archive management

Once your email platform is configured for journaling, you can create and select your archive stores and easily manage them. Storage options you can select from include MS SQL + files, MS SQL, MS SQLExpress, or for testing a built in DB, you can then schedule your archive management.

By setting automatic storage roll-over, you can ensure that you have management data sets based on time (monthly, bi monthly, quarterly, half yearly, yearly). This lets you create an archive management strategy and optimize mail server performance.  For example, you can archive and roll-over your databases on a monthly basis, and set your organizational strategy to:

- Store only 24 months of email data on your mail server
- Hold 48 months of email data active, indexed, and useable from your archive
- Securely backup and move “off site” to a lock box any data which is >48 months.

Unlimited|Secure Email lets you customize this strategy for any business size or email usage size.

In addition, the archives can be easily added or attached back to the system to be used for e-discovery, recovery, or simply to find that lost email attachment that is critical to your business.

## Tamper-proof archiving

Unlimited|Secure Email archiving allows administrators to set up an auditing activity database. Only application services have permissions to make changes to the stored information, in addition to recording all activity on the database for auditing.

In addition, user-interaction auditing can be enabled to create a log of all activity which has taken place in the archive and the searches against the data. Audit reports can be quickly produced to create complaint-level evidence of your data. These reports include

- Configuration Management Auditing
- Access Control Auditing Report
- Archived items Auditing Report
- Bulk Import Auditing Report
- Retention Policy Auditing Report
- Data Leakage Prevention Auditing
- User Audit Trail Auditing Report
- Data Integrity Auditing Report

## Advanced search & eDiscovery

When searching for archived items, such as emails, files, calendar items or faxes, Unlimited|Secure Email archive functionality queries the email index and retrieves any matching item with its respective attachment. Within Archiver, you can search using a Quick Search, Simple Search, or Advanced Search. You can specify the exact search criteria required to extract the data you need. This includes the use of wild cards, nested filters. With all search types, it will query inside email attachments, so you are not limited to just the email text.

Administrators will also have access to an export tool allowing them to conduct specific searches and retrieve large data sets, outputting them with multiple format options. This is a key tool for eDiscovery or responding to legal requests.

Users will have multiple clients, from Outlook connectors, web clients, and mobile apps, to search within their own data. This puts archived data at their fingertips from the tools they already use, and will prevent IT requests for lost emails.

# Capabilities Cheat Sheet

## Domain, email & connectivity encryption

Provides support to configure multiple domains along with DKIM authentication for each domain, sender anti-spoofing, and user authentication with Active Directory Integration (NTLM), Open Directory Integration, or Built-In (Digest & CRAM MD5) is available. Data encryption can be enabled on the mail stores, and finally TLS 1.3 for transmission. With access, data, and transmission fully encrypted you can have an end-to-end secure system for all communications.

## Integrated & secure access management

Active Directory and alternative directory services are available to manage users and groups, set permissions and access. In addition, security tools such as password expiration and complexity policies, and password-guessing prevention settings are also available.

## Multi-client & device support

Email communication, spam quarantine, and archiving user data are all available through existing clients (such as Outlook or Apple) that may be in use, as well as web and mobile device support. Native clients with 10+ languages supported.

## Self-Service email delegation & quarantine

Email delegation to users, shared mailboxes & calendars, as well as self managed email threat digests, puts control in the users hands and prevents noisy IT requests. Combined with additional  self-service tools like archive client access, and machine learning spam filters, IT administrators can focus more on improving the business.

## Multiple antivirus & malware protection

Advanced email threat protection using four antivirus engines (powered by industry winners Bitdefender, Avira,  Kaspersky and Cyren).

## Advanced threat updates

The multiple antivirus engines and the spam definitions are updated frequently to ensure you are protected from the latest threats, up to the hour. Antivirus engines can be configured to check automatically for updates on the frequency you select.

## Policy-based content & spam filtering

Email traffic content is filtered using four advanced content filtering engines. Advanced user-based filtering rules enable flexible and granular filtering of any part of the email message: message headers, subject, body, attachment name and attachment content using different types of pattern matching methods, including regular expressions.

## Automated archive management

Create and select your archive stores and easily manage them. Storage options include MS SQL + files, MS SQL, MS SQLExpress, or for testing an built in DB.  you can then schedule and automate your storage/archive rollovers.

## Tamper-proof archiving

Set up an auditing activity database, such that only the SQL server has permissions to make changes to the data, and records trace files which are also secured with only access to the services, and full auditing reports for compliance

## Advanced search & eDiscovery

Search includes the use of wild cards, nested filters, available for searches inside of email attachments--so you are not limited to simply the email text. Used from e-discovery bulk tools, admin web console, or end user clients.