



Email Defense Optional Features

With Email Defense, we are committed to you having the best protection suited to your needs. With this in mind, we offer some optional features for you to customize your experience with us. They are:

- Email Defense protection for non-LuxSci hosted accounts
- Outbound Message Filtering
- Fail Safe Message Recovery

Protection for non-LuxSci Accounts

Simply put, Email Defense is among the best in email filtering technology. Even if you do not have a LuxSci-hosted account, purchase and setup of Email Defense through LuxSci is quick.

How does this work?

Even if a company other than LuxSci provides your email hosting services, you can still purchase Email Defense from LuxSci and use it to filter your email. Service provisioning and implementation requires no data migration or integration. You simply point your Mail Exchange (MX) records located within their DNS infrastructure to our Email Defense servers. Recipient auto-discovery technology provides for a seamless method of managing end-user filtering data and policies with no additional integration. You can use Email Defense with no change to your existing email infrastructure or practices!



Outbound Message Filtering

What are the reasons for ordering this option?

Clean and secure emails are something we all want. With Email Defense, you are assured the best in email filtering technology. But while inbound email threats receive the bulk of attention from network administrators, outbound email can cause tremendous problems for organizations. Through outbound email, confidential information can get into the wrong hands, servers can crash from dangerously-sized attachments, and organizations face risk a liability from the distribution of emails containing inappropriate content.

How does this work?

Outbound Message Filtering enables businesses and service providers to proactively integrate email policy enforcement for all messages leaving corporate networks en route to valued customers or business partners.

- Prevent company-sensitive information from being distributed.
- Stop inappropriate content from being sent from and within your domain.
- Strip oversized attachments to avoid causing server lag.
- Block the transmission of harmful viruses and worms with customizable filtering rules.



Let Outbound Message Filtering protect your domain by:

- Eliminating the risk of infecting business partners or customers, thus preserving the integrity of your business.
- Protecting information assets by preventing the accidental or intentional distribution of proprietary corporate information.
- Reducing legal liabilities associated with emails containing inappropriate content.
- Establishing and enforcing policies around bandwidth-draining attachments.
- Filtering by content keywords or phrases and by attachment type and size.

Outbound Message Filtering gives your outbound emails the same treatment as your incoming mail gets; using industry-leading software from Sophos, McAfee, and Authentium, Outbound Message Filtering makes sure that your email traffic is secure.



Fail Safe Message Recovery

What are the reasons for ordering this option?

In the case of a server emergency, emails sometimes can get lost in the shuffle. If they can't be delivered, more often they'll just get bounced; with Fail Safe Message Recovery, you can get your messages delivered with no extra effort once your server is back online.

How does this work?

Fail Safe Message Recovery ensures that your company will never lose an email in the event your business is struck by an unforeseeable outage or malfunction, or during planned maintenance by providing automatic email backup. With Fail Safe, organizations no longer risk email delays, interception, damage or loss.



- Provides automated, worry-free email delivery protection
- Minimizes productivity loss in the event of a disaster
- Engages automatically for instantaneous protection
- Provides manual start-up option to accommodate system maintenance
- Offers outage notifications and regular system updates
- Includes five rolling days of unlimited storage
- Automatically delivers all spooled email upon outage completion

Fail Safe provides easy administration through the Control Console our convenient Web-based administrative portal that is also central to management of the Email Defense Service. Through the Control Console, users can:

- Set the service for automatic or manual startup
- Determine whether mail is flowing normally, being spooled in Fail Safe, or being released following an outage
- Test the connection between their mail server(s) and LuxSci
- Set up notification delivery options

Your organization can be protected from email threats and the loss of email messages due to unexpected or planned outages in less than one business day with the Email Defense Service and Fail Safe Message Recovery.



Message Continuity

What are the reasons for ordering this option?

Sometimes simply storing emails during a server outage isn't sufficient. With Message Continuity, not only is your period and amount of rolling storage extended, but you also can access and use your email through our special portal. This product is an extended version of our Fail Safe Message Recovery option.

How does this work?

Message Continuity is delivered through a convenient managed service that enables businesses to access and use email during server outages.

- Automatically begins once outage is detected.
- Delivers outage notifications and system updates
- Queues messages for up to 60 days
- No limit on the amount of email queued
- Users can read and reply to queued email, as well as send new messages through our secure portal.

Your privacy is important to us. Because of this, administrators and support do not have access to your personal queued email.