# Email Security for Microsoft 365

Email is one of the most common attack vectors, most likely because it's one of the easiest entry points for cyberattacks. It's also the tool most rely on to get their jobs done. More businesses are choosing cloud-based solutions, like Microsoft 365™, as the center point of their business systems for greater organizational flexibility, cost savings, and ease of collaborating across multiple offices and locations. But assuming Microsoft 365 will handle all your security and data retention needs can lead to a false sense of security. N-able™ Mail Assure seamlessly integrates with Microsoft 365 via an add-in and the new Microsoft 365 sync functionality is designed to help you effortlessly onboard multiple Microsoft 365 users fast!

Q. How does the Microsoft 365 add-in work?

- The Mail Assure add-in, available at Microsoft AppSource®, is designed to give Microsoft 365 users greater control over and transparency into their email flow while enjoying the benefits of Mail Assure email protection. The add-in enables users to:

  1. Mark messages as **spam** or **not spam** from Outlook®, on the web, macOS® or Windows® PC, iOS®, iPadOS®, or Android®.

  2. Easily sign into their Mail Assure dashboard from both Microsoft 365 Apps and Azure® Active Directory® using single sign-on (SSO).
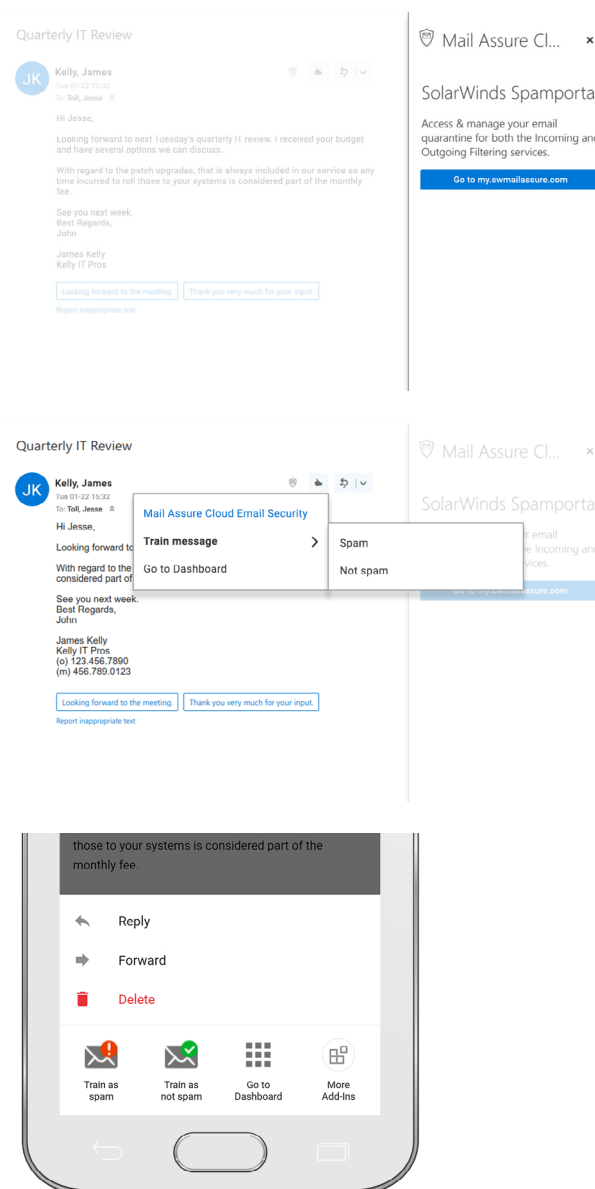
## Q. How does the Microsoft 365 sync functionality work?

- The Microsoft 365 sync functionality is designed to simplify onboarding of Microsoft 365 customers to Mail Assure. Once logged into the new Mail Assure interface using your SSO credentials, a Microsoft 365 wizard (available from the Domains Overview page) will help you get your Microsoft 365 customers protected fast.

» Using the Microsoft 365 sync:

1. Add Microsoft 365 customers by securely connecting with your Microsoft 365 credentials.

2. Improve efficiency with automatic synchronization of new Microsoft 365 mailboxes, distribution lists, and shared mailboxes, as well as mailbox aliases.

3. Keep usage under control with scheduled automatic synchronization of added and deleted mailboxes.

4. Easily set timezone, date and time formatting, and reporting options for new mailboxes.

» **Note:** Configure your browser to allow pop-ups before clicking on **connect** in the wizard; you will need to authenticate to Microsoft 365 twice, once to allow the wizard to collect information and once to allow the scheduled sync.

Q. If I am an existing Mail Assure customer, how can I start using the Microsoft 365 sync?

1. If you already have domains and mailboxes configured in Mail Assure, you can start using the Microsoft 365 sync immediately, without any preparation work.

2. Simply log in to Mail Assure using SSO credentials, proceed to the **new interface** and **domains overview** section; from there, you can configure your Microsoft 365 customers using the Microsoft 365 sync.

» **Note:** It is important to log into your Mail Assure dashboard with SSO. This feature is only available in the new Mail Assure interface. Configure your browser to allow pop-ups before clicking on **connect** in the wizard and authenticate to Microsoft 365 twice—once to allow the wizard to collect information and once to allow the scheduled sync.

Q. What is the frequency of the automatic synchronization?

- By default, if automatic synchronization is enabled, it will sync every four hours with the following alternative options:

  › Every 12 hours

  › Every day

  › Every week
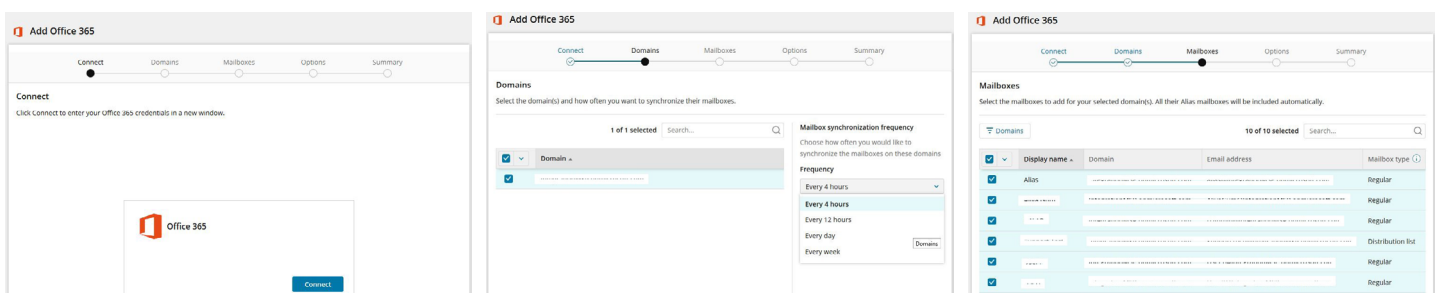
Q. What happens with my added and deleted mailboxes in Microsoft 365?

- When automatic synchronization is enabled:

  A. Added and deleted mailboxes in Microsoft 365 will automatically be added and deleted from Mail Assure.

  B. If you delete a mailbox in Microsoft 365, the Microsoft 365 sync functionality will automatically delete the mailbox from Mail Assure as well. Mail Assure will continue to attempt to deliver any queued email, even if a domain, or its mailbox(es), is removed. Any quarantined email will be removed within 24 hours after a mailbox has been removed from Mail Assure. Since archived email is stored at the domain level, all archived email of the deleted mailbox will still be available from the admin or domain level if the domain the mailbox belongs to has not been entirely removed. This is valuable for e-discovery of important security or critical business information.

  C. If you add a mailbox back in Microsoft 365, the Microsoft 365 sync functionality will automatically add the mailbox back into Mail Assure as well, and both the settings and services you have configured in your Microsoft 365 sync will apply.

  D. If you add any new mailboxes in Microsoft 365, the Microsoft 365 sync functionality will automatically add the mailbox into Mail Assure, and both the settings and services you have configured in your Microsoft 365 sync wizard will apply.

Q. Can I change my settings after I've configured mailboxes in the Microsoft 365 sync?

- Yes, it is possible to go back at any point in time and adjust settings for all mailboxes or selected mailboxes.

Q. What happens if I make changes to Microsoft 365 mailboxes in-product (i.e., in the mailbox configuration)?

- If you make changes in-product—other than adding or removing the protection or archiving services—for Microsoft 365 mailboxes, your changes will be reverted to match what you have set up in the Microsoft 365 sync.

» Example: You manually flag a mailbox as a distribution list in-product within the mailbox configuration section, but the mailbox is not a distribution list in Microsoft 365. The next time the sync runs, your change will be reverted to match Microsoft 365. We are looking to further improve this capability.

Q. How do I configure mailboxes if I have Microsoft 365 customers and customers using other email platforms?

- If you have Microsoft 365 customers and customers using other email platforms or tools, you should use the Microsoft 365 sync to get your Microsoft 365 users onboarded and the mailbox configuration function or LDAP sync for your other customers. In summary, if you have one domain with Microsoft 365 mailboxes and one with other mailboxes, you can make use of both the Microsoft 365 sync, the mailbox configuration function, and LDAP to suit the needs of different users.

Q. Can I select a specific region for storing my logs, quarantines, and archive data with the Microsoft 365 sync?

- Currently, this option is not available in the Microsoft 365 sync wizard but we are working to add this. All domains added in the Microsoft 365 wizard will, by default, have the global region of choice selected. We utilize various data centers to ensure a global, redundant email security platform. The global region remains the optimal choice for email routing and redundancy.

- If a domain already exists within Mail Assure, it will use the region you selected upon adding the domain. If you or your customers need to use data centers located in specific regions, Mail Assure offers the option to select storage for your logs, quarantines, and archive data in the U.S., E.U., U.K., Australia, Canada, and global. To benefit from these options, you need to add the domain(s) first, using the **add domain** (see the screenshot below) functionality in your dashboard, and then proceed to the Microsoft 365 sync wizard to configure your Microsoft 365 users.
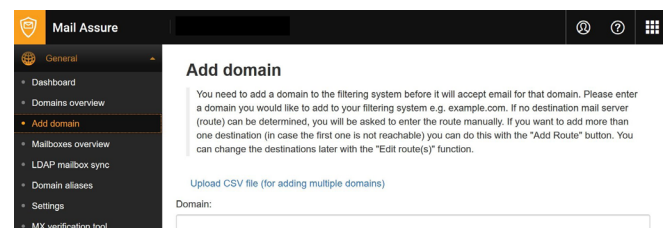
Q. Why choose N-able Mail Assure email security for your Microsoft 365 users?

- Mail Assure is a cloud-based email security solution that seamlessly integrates with Microsoft 365 via an add-in. Using collective threat intelligence, 24/7 email continuity, and long-term email archiving, Mail Assure provides an additional email security gateway to protect against:

  A. Spam, viruses, ransomware, malware, and other email-borne threats with advanced threat protection that uses proprietary email filtering technology—with near 100% filtering accuracy and close to zero false positives—with 2B+ spam messages blocked per month.

  B. Phishing, spear phishing, impersonation, and business email compromise with real-time pattern threat recognition that leverages a variety of filtering technologies and statistical systems to capture known and emerging threats.

  C. Spoofing and display-name spoofing with sender policy framework support (SPF), domain keys identified mail (DKIM) and domain-based-message authentication, reporting and conformance (DMARC).

  D. Dangerous attachments with hidden executables and macros to help prevent zero-day attacks.

  E. IP block listing and damage to company reputation with abuse management.

  F. Email server outages and downtime with 24/7 built-in email continuity that enables users to continue to receive and send email.

  G. Data loss using robust, encrypted email archiving with an unlimited retention period. Email archiving for Microsoft 365 also helps users easily retrieve messages and addresses compliance requirements from industry-related regulatory bodies like FRCP, SOX, and HIPAA.

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com