How to Whitelist Email in Office 365 Security and Compliance

Whitelisting allows selected email addresses or domains to bypass spam filters and reach the intended recipients. Knowing how to whitelist email in Office 365 Security and Compliance ensures that important messages from trusted senders are not blocked or marked as junk by Security and Compliance features.

Improve Deliverability, Visibility, and User Experience

Whitelisting improves the deliverability and visibility of important messages from trusted senders, such as customers, partners, vendors, or internal communications. It also reduces the risk of missing or overlooking critical information due to spam filtering or user actions, such as deleting or ignoring junk mail.

Whitelisting also enhances the user experience by minimizing false positives (legitimate messages marked as spam) and diminishing the need to check the junk folder frequently. Finally, it saves time and resources by decreasing the workload of administrators and users who must deal with spam issues and complaints.

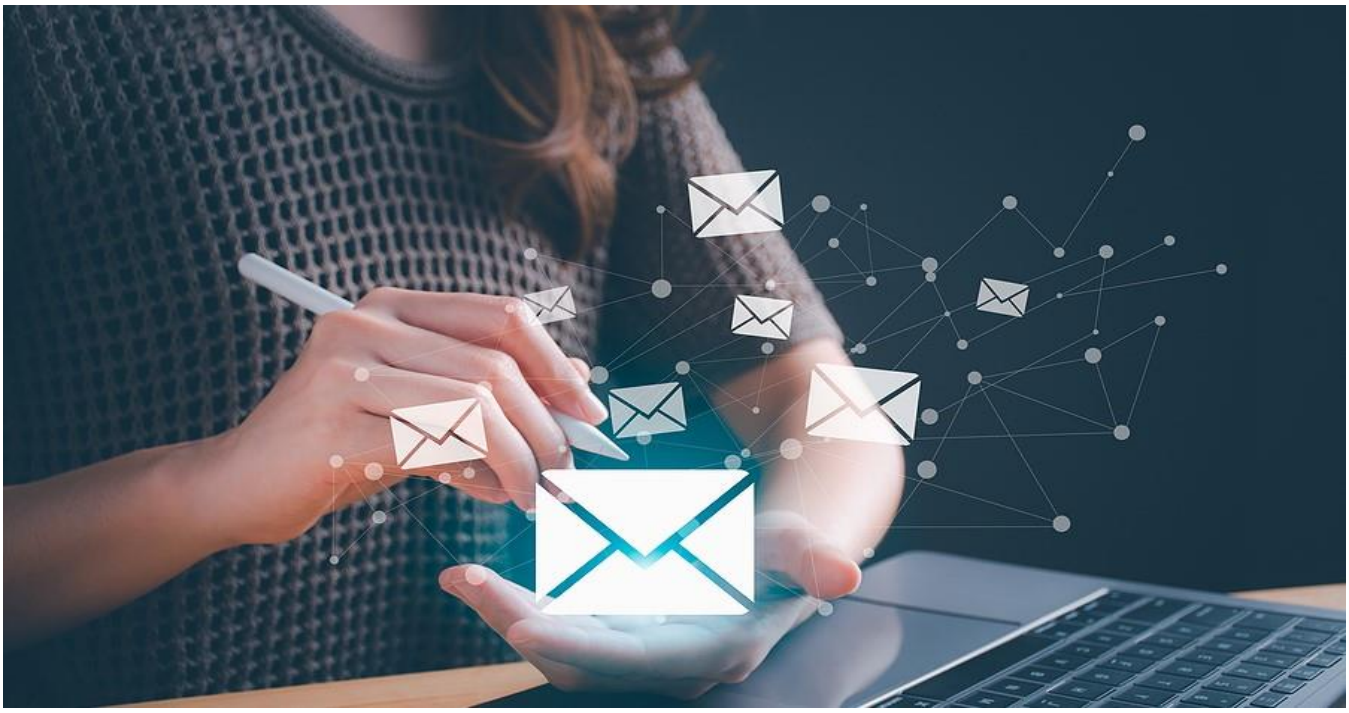
How to Whitelist Email in Office 365 Security and Compliance

Read on to see how to whitelist email in Office 365 Security and Compliance. We've included the steps to create a whitelist policy, apply it to specific users or groups, and manage the whitelist entries.

How to Create a Whitelist Policy

To create a whitelist policy in Office 365 Security and Compliance, you need to do the following:

1. Sign-in to the Office 365 Admin Center with your administrator account.
2. Go to Security & Compliance > Threat Management > Policy > Anti-Spam.
3. Click on the + icon to create a new policy.



4. Give your policy a name and a description and choose Custom from the drop-down menu.
5. Under Applied to, click on the + icon to select the users or groups to apply the policy to individual users, distribution lists, security groups, or dynamic distribution lists. You can also exclude some users or groups from the policy if needed.
6. Under Spam and bulk actions, click on Edit.
7. Under Allow lists, click on the + icon to add the email addresses or domains that you want to whitelist. You can enter up to 1,024 entries per policy.
8. You can also use wildcards (*) to match multiple subdomains or variations of an email address. For example, *@somewebsite.com will whitelist all email addresses from somewebsite.com and its subdomains.
9. Click on Save to save your changes.
10. Click on Save again to create your policy.

The new whitelist policy will take effect within one hour after you create it. You can view, edit, or delete your policy at any time from the Anti-Spam page.

Understand the Risks and Limitations of Whitelisting

Whitelisting is not a perfect solution. It comes with some risks and limitations that you should be aware of, such as:

- **Increasing exposure to phishing, spoofing, or other malicious attacks** that may originate from whitelisted senders (either intentionally or unintentionally).

  Whitelisting does not guarantee that an email is safe or legitimate. So, you should still exercise caution and verify the sender's identity and the message's content before opening any attachments or clicking on any links.

- **Reducing the effectiveness of spam filtering** and other security features that rely on machine learning and user feedback.

  Whitelisting may interfere with the ability of Office 365 Security and Compliance to learn from user actions (such as reporting spam) and adjust its algorithms accordingly. It may also override some default settings or policies designed to protect your organization from spam and other threats.

- **Creating management and maintenance challenges** for administrators who must create, update, and monitor multiple whitelist policies for different users or groups. Whitelisting may also cause confusion among users. This results when they receive different treatment for the same sender or message depending on their assigned policy.

Balance the Benefits and Risks of Whitelisting

Used properly, whitelisting becomes an effective tool for ensuring that important messages from trusted senders are not blocked or marked as junk by Office 365 Security and Compliance. Always balance the benefits of whitelisting with the risks of compromising your security and performance. Also review your whitelist policies regularly and adjust as needed based on changing needs and preferences.

In addition to showing you how to whitelist email in Office 365 Security and Compliance, the Office 365 email experts at Messaging Architects help you manage and optimize email deliverability, update email policies and rules, monitor compliance, and strengthen cyber security. Contact their experienced Microsoft Office consultants today to improve the productivity and security of email throughout the organization.