

How to use ExchangeDefender Bypass

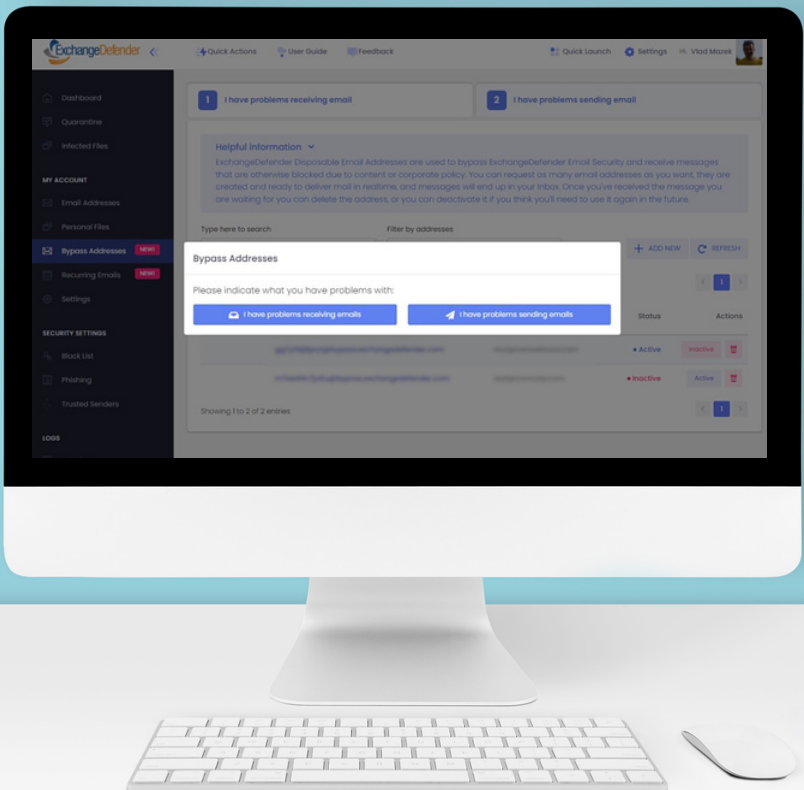


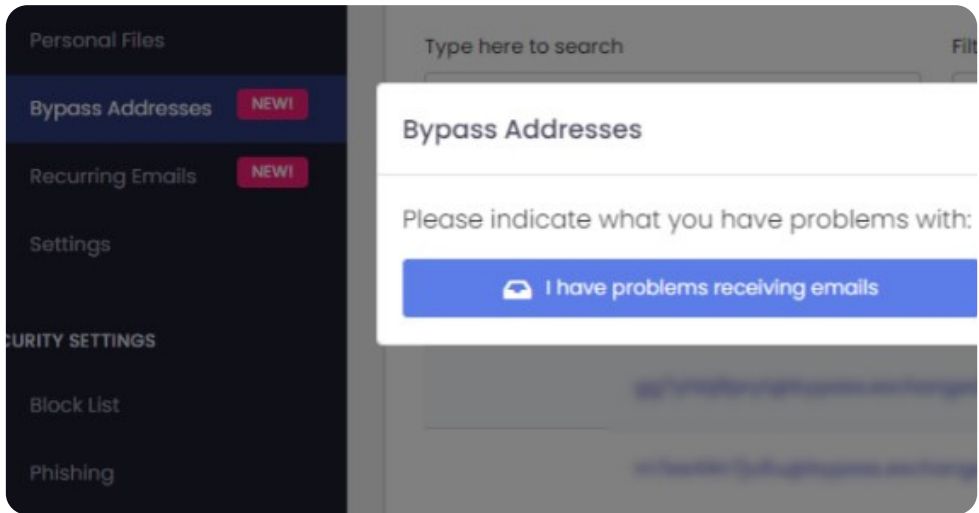
Table of Contents



| | |
|--|-----------|
| Common Scenarios for Inbound Mail | 03 |
| How to Use Bypass Inbound Mail (Incoming mail, sent to you) | 04 |
| Common Scenarios for Outbound Mail | 05 |
| How to Use Bypass Outbound Mail (Outgoing mail, sent from you) | 06 |
| Frequently Asked Questions (FAQs) | 07 |

What is Bypass?

ExchangeDefender Bypass is a powerful tool that allows quick email delivery when IT/tech policies pose challenges.



Common Scenarios for Inbound Mail

1 **Receiving Emails from Compromised/Spam Networks:**

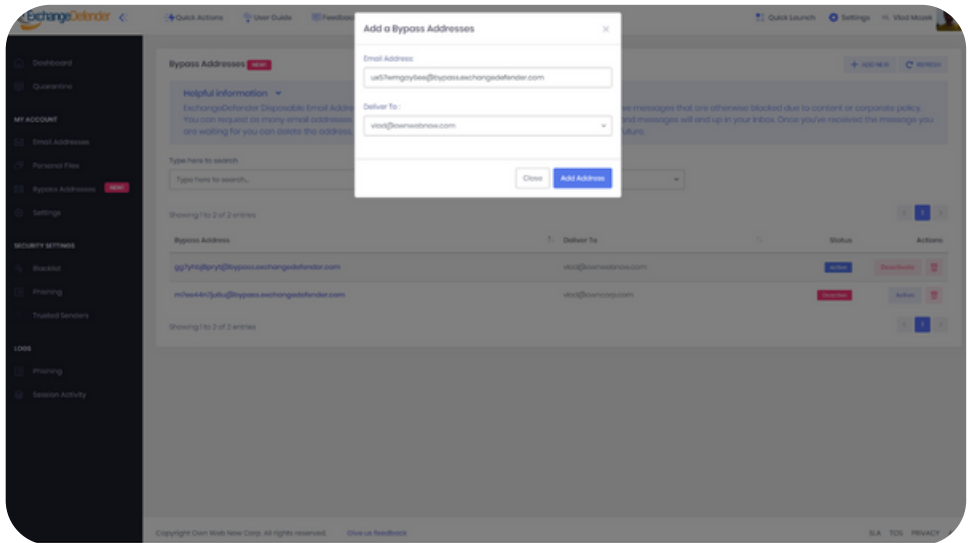
Spam and compromised emails threaten security. Legitimate emails can be blocked or marked as junk. Bypass ensures important messages reach your inbox.

2 **Your organization's corporate policy won't allow certain attachments**

Many organizations implement strict policies to protect against malicious attachments that could carry viruses or malware. While these policies are essential for security, they may inadvertently block legitimate attachments that are crucial for your business.

3 **Misconfigured SPF/DKIM Domains:**

If a domain is misconfigured or lacks proper SPF/DKIM records, some email servers might mark the messages as suspicious or reject them altogether.



How to Use Bypass for Inbound Mail

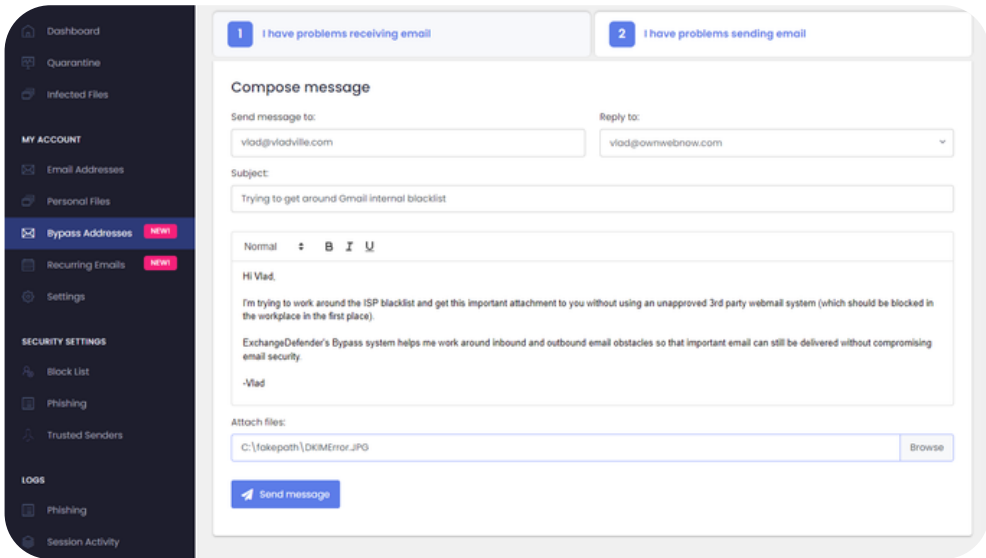
Bypass for Inbound Mail is a valuable tool that allows users to receive emails in scenarios where typical IT policies may pose restrictions or challenges.

1. Access the ExchangeDefender Admin portal at <https://admin.exchangedefender.com>.
2. **Log in** with your credentials.
3. Go to "**My Account**" and select "Bypass Addresses."
4. Click "**+ Add New**" to generate a random disposable email address.

Any mail sent to this address will be forwarded to your real email.

Did you know? ➤ You can **deactivate and reactivate** bypass email addresses if needed for future use.

Common Scenarios for Outbound Mail



The screenshot displays the ExchangeDefender Bypass interface. On the left is a dark sidebar with navigation options: Dashboard, Quarantine, Infected Files, MY ACCOUNT (Email Addresses, Personal Files, Bypass Addresses (NEW!), Recurring Emails (NEW!), Settings), SECURITY SETTINGS (Block List, Phishing, Trusted Senders), and LOGS (Phishing, Session Activity). The main area shows a 'Compose message' form with two tabs: '1 I have problems receiving email' and '2 I have problems sending email'. The form includes fields for 'Send message to:' (vlad@vladville.com), 'Reply to:' (vlad@owmwebnow.com), and 'Subject:' (Trying to get around Gmail internal blacklist). The body text reads: 'Hi Vlad, I'm trying to work around the ISP blacklist and get this important attachment to you without using an unapproved 3rd party webmail system (which should be blocked in the workplace in the first place). ExchangeDefender's Bypass system helps me work around inbound and outbound email obstacles so that important email can still be delivered without compromising email security. -Vlad'. An 'Attach files:' section shows a file path 'C:\fakepath\DKIMError.JPG' and a 'Browse' button. A 'Send message' button is at the bottom.

Bypass for Outbound Mail is a feature that addresses common issues faced when sending emails. Here's more information about the scenarios where the Bypass feature can be useful:

Receiving NDR/Bounce Messages when Sending Mail:

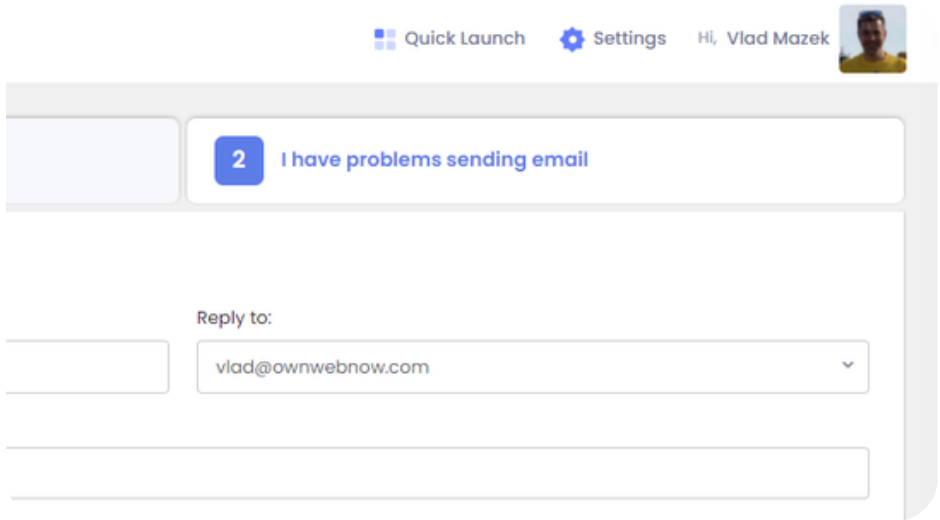


NDR stands for Non-Delivery Report, also known as a bounce message. It occurs when an email cannot be delivered to the recipient's mailbox for various reasons, such as an invalid email address, a full mailbox, or temporary server issues.

Messages Not Reaching the Recipient:



Sometimes, emails sent from your organization may not reach their intended recipients due to various reasons, such as blacklisting of IP addresses or domains, overzealous spam filters, or server misconfigurations.



How to Use Bypass for Outbound Mail

Bypass for Outbound Mail helps users overcome common delivery challenges, like bounced messages. To start emailing, **follow these simple steps:**

1. Access the ExchangeDefender Admin portal at **<https://admin.exchangedefender.com>**.
2. Log in and click on "**Bypass Addresses**."
3. Select "**I have problems sending emails**."
4. **Compose** and send the email as usual.
 - a. If you have multiple aliases, choose the reply-to address from the dropdown.
5. Click "**Send message**" to use the Bypass network.

PRO TIP



If the **message keeps bouncing**, the issue may be the recipient's server or message content.

Frequently Asked Questions

1. What is ExchangeDefender Bypass?

ExchangeDefender Bypass is a feature designed to facilitate email delivery in scenarios where IT/tech policies create obstacles. It allows users to create disposable email addresses to forward emails that might be blocked by spam filters, blacklisted domains, or other security measures, ensuring important messages reach the intended recipients.

2. How can Bypass for Inbound Mail benefit me?

Bypass for Inbound Mail is beneficial in various situations. If your organization's security policies block certain attachments or if you need to receive emails from compromised/spam networks, Bypass provides a workaround. It also helps when you encounter misconfigured SPF/DKIM domains that might otherwise prevent email delivery.

3. How do I set up Bypass for Inbound Mail?

Setting up Bypass for Inbound Mail is easy. Simply log in to the ExchangeDefender Admin portal, go to "My Account," select "Bypass Addresses," and click on "+ Add New." The system generates a random disposable email address, and any emails sent to this address will be forwarded to your real email. Once you receive the expected email, you can delete or deactivate the address.

4. How can Bypass for Outbound Mail help with email delivery issues?

Bypass for Outbound Mail is useful when you encounter email delivery issues, such as receiving NDR/bounce messages or messages not reaching the recipient. By utilizing Bypass, the email message takes an alternative route through a third-party email organization, avoiding potential blocks or misconfigurations that may have occurred when sending directly through the ExchangeDefender network.