

<https://avionteboldsupport.zendesk.com/hc/en-us/articles/4415878586387>

Overview

Updated 01/21/2022

This needs to be performed from your O365 Administration panel and your Exchange Online Administration Console. The person making these changes should be a global Admin within O365. This change will allow all users in O365 to use BOLD SMTP feature with no action needed to be performed by the user.

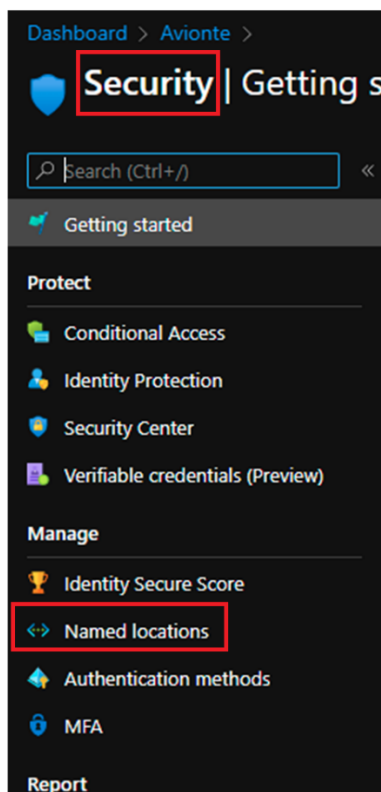
- [Click here for information on using MFA and app passwords](#)
- [Click here for information on changing your MFA settings](#)

[Add a trusted IP Address](#)

[Add Exchange Online Connector](#)

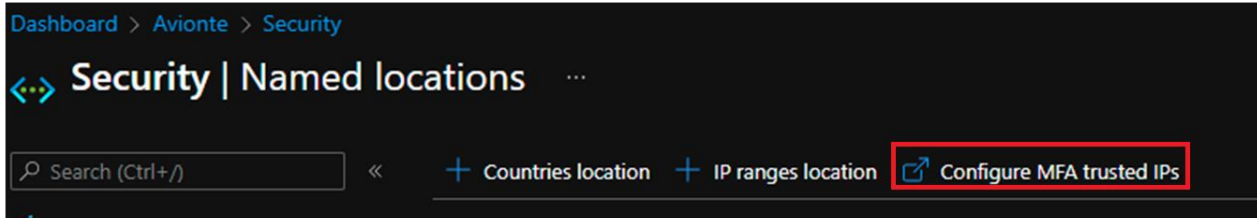
Add a trusted IP Address

1. Azure AD, go to Security and then Named Locations

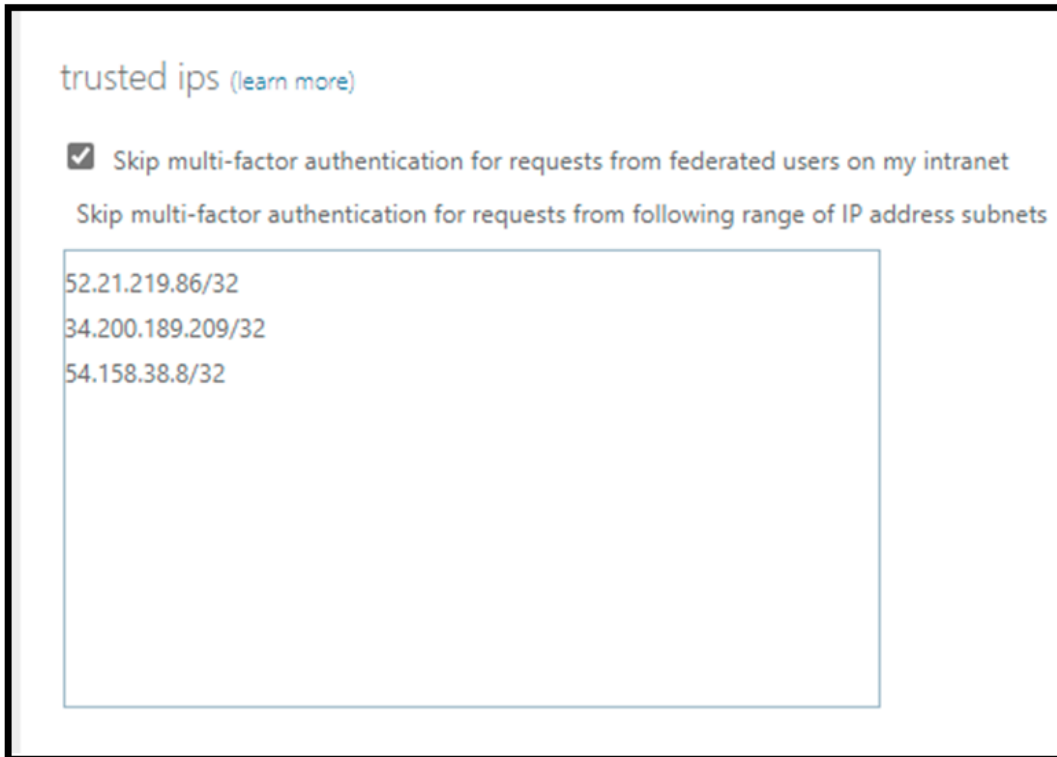


How to configure O365 with BOLD SMTP AVIONTÉ

2. Click Configure MFA Trusted IP's and a new Tab will open



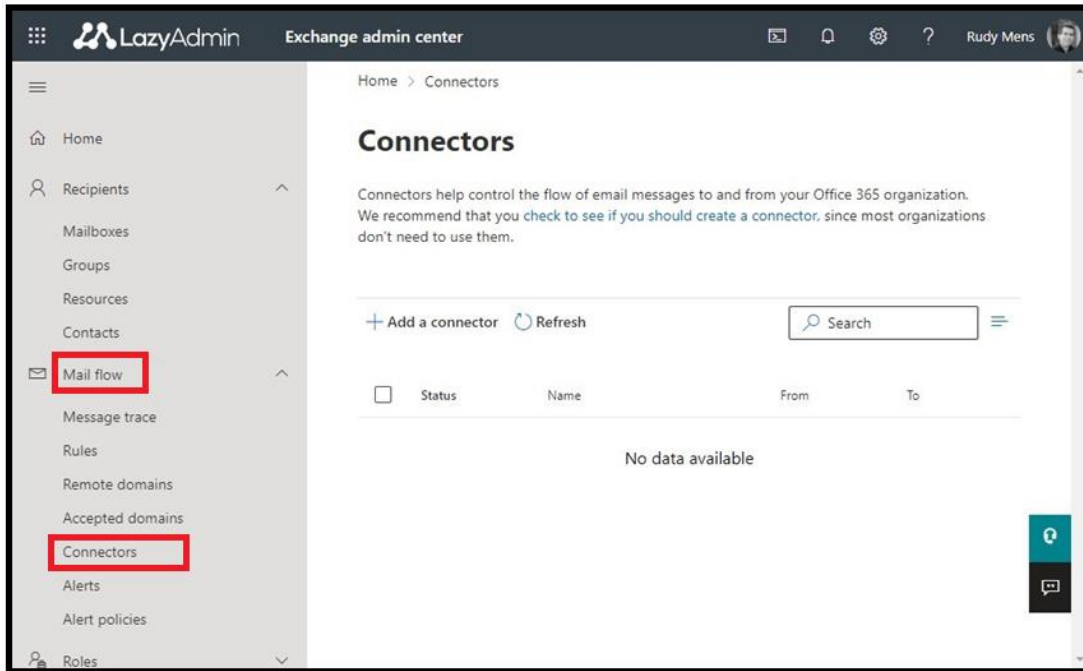
3. In Trusted IP section, check the box for Skipping MFA and external Bold IP's click save at the bottom.



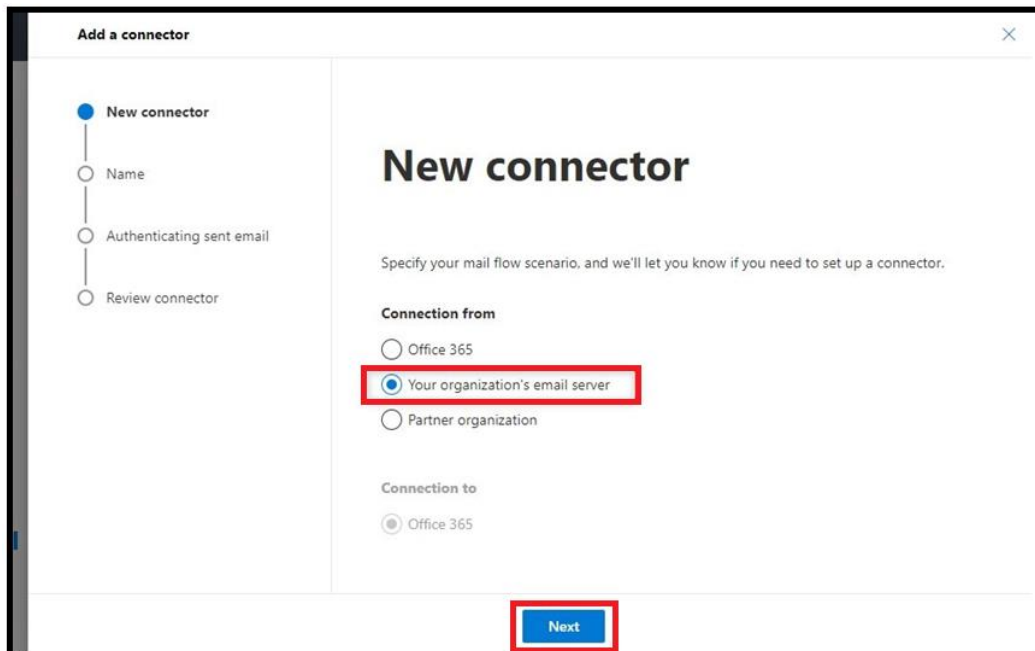
4. You will also need to add the IP's to your Exchange Online as a separate connector.

Add Exchange Online Connector

1. Open the Exchange Admin Center
2. Click on Mail Flow
3. Click on Connectors

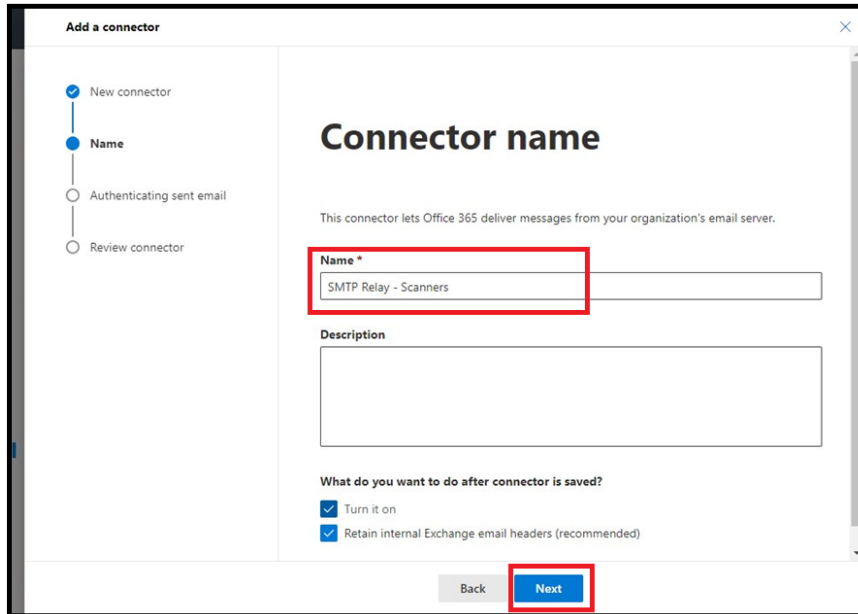


4. Select **Your organization's email server** option
5. Click on the **Next** button



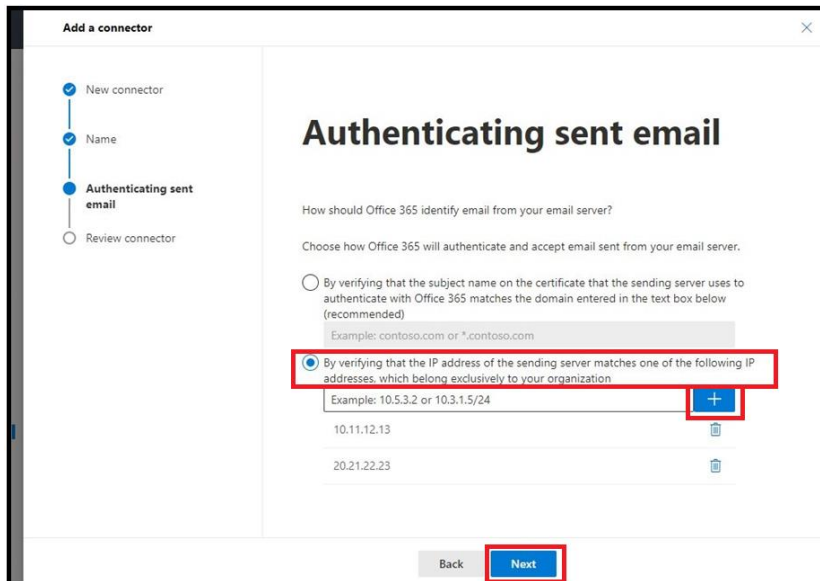
How to configure O365 with BOLD SMTP

- Put in a name for the Connector in the **Name** field.
 - Leave the selected options on.
- Click on the **Next** button



The screenshot shows the 'Add a connector' wizard in the 'Connector name' step. The left sidebar has four steps: 'New connector' (checked), 'Name' (active), 'Authenticating sent email', and 'Review connector'. The main area is titled 'Connector name' and contains a description: 'This connector lets Office 365 deliver messages from your organization's email server.' Below this is a 'Name *' field with the text 'SMTP Relay - Scanners' and a 'Description' text area. At the bottom, there are two checked options under 'What do you want to do after connector is saved?': 'Turn it on' and 'Retain internal Exchange email headers (recommended)'. At the very bottom are 'Back' and 'Next' buttons.

- The next step is to configure the authentication that we want to use. It's possible to use a certificate for authentication, but more common is to do the verification based on the public IP Address of the device.
- Add Bold Three external IP addresses
 - Click the **Plus** button to add IP addresses:
 - 52.21.219.86
 - 34.200.189.209
 - 54.158.38.8
- Click on the **Next** button



The screenshot shows the 'Add a connector' wizard in the 'Authenticating sent email' step. The left sidebar has four steps: 'New connector', 'Name', 'Authenticating sent email' (active), and 'Review connector'. The main area is titled 'Authenticating sent email' and contains the question: 'How should Office 365 identify email from your email server?' Below this is a sub-question: 'Choose how Office 365 will authenticate and accept email sent from your email server.' There are two radio button options. The first is 'By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches the domain entered in the text box below (recommended)' with an example 'contoso.com or *.contoso.com'. The second is selected: 'By verifying that the IP address of the sending server matches one of the following IP addresses, which belong exclusively to your organization'. Below this is a text input field with the example '10.5.3.2 or 10.3.1.5/24' and a blue '+' button. Below the input field are two IP address entries: '10.11.12.13' and '20.21.22.23', each with a trash icon. At the bottom are 'Back' and 'Next' buttons.

- The last step is to review your settings and create the connector. Double-check the IP Addresses and click on **Create connector**.