**If your Dealership is hosting email in office 365 Promax recommends that you set the following up in your office365 tenant (Office 365 exchange online) to ensure email deliverability of lead notifications.**

**Going through the instructions below from Microsoft. Please add the domain promaxonline.com and ip addresses 192.158.25.66 and 192.158.25.65**

**Connectors for mail flow with a partner organization**

<https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/use-connectors-to-configure-mail-flow>

You can create connectors to add additional security restrictions for email sent between Microsoft 365 or Office 365 and a partner organization. A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, antispam, and so on. You can create a partner connector that defines boundaries and restrictions for email sent to or received from your partners, including scoping the connector to receive email from specific IP addresses, or requiring TLS encryption.

### Example use of connectors with a partner organization

The diagram below shows an example where ContosoBank.com is a business partner that you share financial details with via email. Because you are sharing financial information, you want to protect the integrity of the mail flow between your businesses. Connectors with TLS encryption enable a secure and trusted channel for communicating with ContosoBank.com. In this example, two connectors are created in Microsoft 365 or Office 365. TLS is required for mail flow in both directions, so ContosoBank.com must have a valid encryption certificate. A certificate from a commercial certification authority (CA)that's automatically trusted by both parties is recommended.



### Additional partner organization connector options: specify a domain or IP address ranges

When you create a connector, you can also specify the domain or IP address ranges that your partner sends mail from. If email messages don't meet the security conditions that you set on the connector, the message will be rejected. For more information about creating connectors to exchange secure email with a partner organization, see [Set up connectors for secure mail flow with a partner organization](https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner).

### Create a partner organization connector

<https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner>

To create a connector in Microsoft 365 or Office 365, select **Admin**, and then select **Exchange** to go to the **Exchange admin center**. Next, select **mail flow** and then **connectors**. If any connectors already exist for your organization, you can see them listed here.

To start the wizard, click the plus symbol **+**. To create a connector for email you receive from a partner organization, use the options depicted in the following screenshot:



Once you choose this mail flow scenario, you can set up a connector that will apply security restrictions to email that your partner organization sends to you. For some security restrictions, you might need to talk to your partner organization to obtain information to complete some settings. Look for the examples that best meet your needs to help you set up your partner connector.

### Example 1: Require that email sent from your partner organization domain contosobank.com is encrypted using transport layer security (TLS)

To do this, specify your partner organization domain name to identify mail from that partner, and then choose transport layer security (TLS) encryption when you create your partner to Microsoft 365 or Office 365 connector. Use these options during setup:



Use this screen to enter your partner organization's domain name(s) so the connector can identify mail sent by your partner:



Choose this setting to require encryption for all email from ContosoBank.com using TLS:



When you choose these settings, all email from your partner organization's domain, ContosoBank.com, must be encrypted using TLS. Any mail that is not encrypted will be rejected.

### Example 2: Require that email sent from your partner organization domain ContosoBank.com is encrypted and uses their domain certificate

To do this, use all the settings shown in Example 1. Also, add the certificate domain name that your partner organization uses to connect with Microsoft 365 or Office 365. Use this option during setup:



When you set these restrictions, all mail from your partner organization domain must be encrypted using TLS, and sent from a server with the certificate name you specify. Any email that does not meet these conditions will be rejected.

### Example 3: Require that all email is sent from a specific IP address range

This email could be from a partner organization, such as ContosoBank.com, or from your on-premises environment. For instance, the MX record for your domain, contoso.com, points to on-premises, and you want all email sent to contoso.com to come from your on-premises IP addresses only. This helps prevent spoofing and makes sure your compliance policies can be enforced for all messages.

To do this, specify your partner organization domain name to identify mail from that partner, and then restrict the IP addresses that you accept mail from. Using an IP address makes the connector more specific because it identifies a single address or an address range that your partner organization sends mail from. Enter your partner domain as described in Example 1, then use this option during setup:



When you set these restrictions, all email sent from your partner organization domain, ContosoBank.com, or from your on-premises environment must be sent from the IP address or an address range you specify. Any mail that does not meet these conditions will be rejected.

### Example 4: Require that all email sent to your organization from the internet is sent from a specific IP address (third-party email service scenario)

Mail flow from a third-party email service to Microsoft 365 or Office 365 works without a connector. However, in this scenario you can optionally use a connector to restrict all mail delivery to your organization. If you use the settings described in this example, they will apply to all email sent to your organization. When all email sent to your organization comes from a single third-party email service, you can optionally use a connector to restrict all mail delivery; only mail sent from a single IP address or address range will be delivered.

**Note**

Make sure you identify the full range of IP addresses that your third-party email service sends mail from. If you miss an IP address, or if one gets added without your knowledge, some mail will not be delivered to your organization.

To restrict all mail sent to your organization from a specific IP address or address range, use these options during setup:







When you set these restrictions, all mail sent to your organization must be sent from a specific IP address range. Any internet email that does not originate from this IP address range will be rejected.

### Example 5: Require that all mail sent from your partner organization IP address or address range is encrypted using TLS

To identify your partner organization by IP address, use these options during setup:





Add the requirement for TLS encryption by using this setting:



When you set these restrictions, all mail from your partner organization sent from the IP address or address range you specify must be sent using TLS. Any mail that does not meet this restriction will be rejected.