Setup Guide
Revision F

Using McAfee SaaS Email Protection to Secure Microsoft Office 365

Setting up Microsoft Office 365

Use this guide to configure Microsoft Office 365 and Microsoft Exchange Online for use with McAfee® SaaS Email Protection.

Perform these steps at a time when the volume of email traffic is low to minimize the impact on your users. Also, follow your standard maintenance procedures and notify your users ahead of time of potential interruptions in service.

About Microsoft Office 365

Microsoft Office 365 is a cloud-based service that offers online mail hosting and productivity software, including hosted Microsoft Exchange (Exchange Online). Securing Exchange Online with McAfee® SaaS Email Protection provides superior threat protection, spam filtering, and the latest encryption, DLP, and click-time technologies.

Securing inbound mail flow

To secure inbound mail flow, configure your MX Records and inbound servers in Email Protection. Then, create rules in Exchange Online to restrict email flow to your hosted server.

How inbound email is routed

The MX records for your domain determine the email server that is responsible for accepting inbound email for your users. With Office 365, the MX records point to the Exchange Online service in the cloud. However, when you secure Office 365 with Email Protection, your MX records point to the

McAfee SaaS service. McAfee SaaS then filters and relays inbound email to Exchange Online and your users. The following examples explain each process.

Inbound mail without McAfee SaaS Email Protection

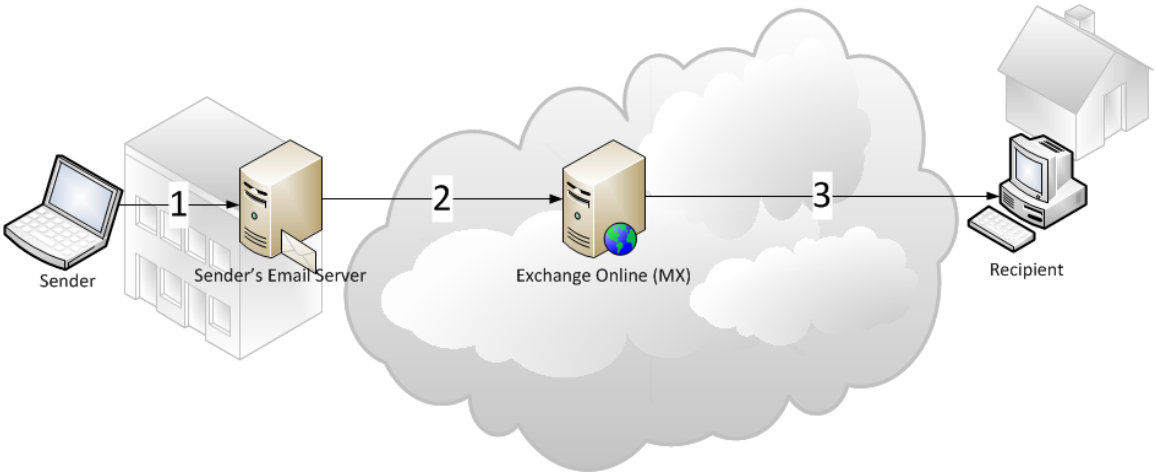


Figure 1 Inbound mail with Office 365

1. Someone sends an email to an Exchange Online recipient.
2. Their email server performs an MX Record lookup and determines that Exchange Online is the destination for the message. Exchange Online receives and stores the email in the cloud.
3. The recipient's email client communicates with Exchange Online so that the user can access their email. The recipient opens the email using Microsoft Outlook or the Outlook Web Application (OWA).

Inbound mail with Office 365 secured by Email Protection

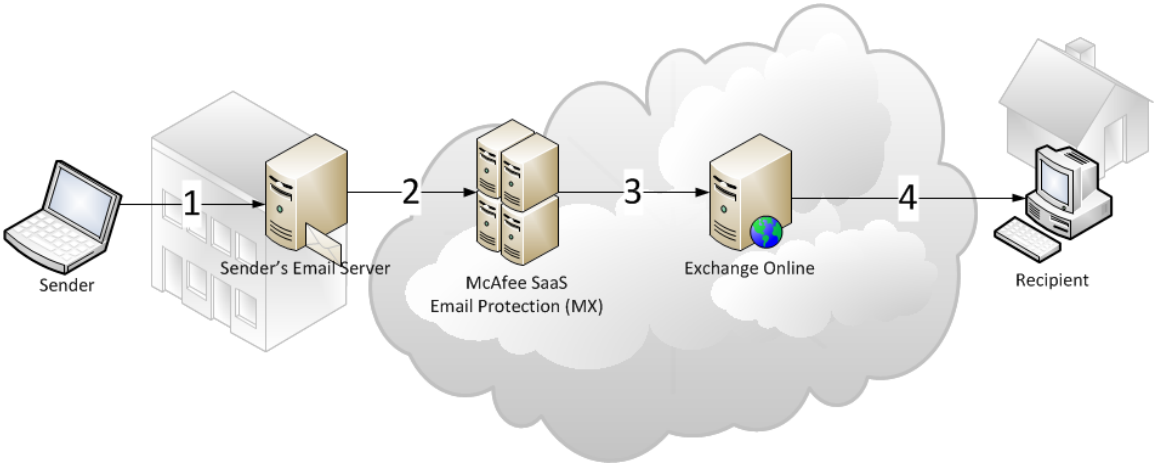


Figure 2 Inbound mail with Office 365 secured by Email Protection

1. Someone sends an email to an Exchange Online recipient who is secured by McAfee SaaS Email Protection.
2. An MX record lookup determines that McAfee SaaS Email Protection is the destination for the message.

3 McAfee SaaS Email Protection scans the email and then forwards it to Exchange Online.

4 The recipient's email client communicates with Exchange Online so that the user can access their email. The recipient opens the email using Microsoft Outlook or the Outlook Web Application (OWA).

Set up inbound servers in SaaS Email Protection

Add an inbound server in Email Protection so that filtered email is routed to Exchange Online.

Before you begin

- Add or migrate all your domains to Office 365.
- Make sure you can access your DNS provider's administrative application.

Repeat this process for each of your domains.

Task

1 Locate and copy the MX record for the domain in Office 365.

Microsoft generates MX records for your domains when you set them up in Exchange Online.

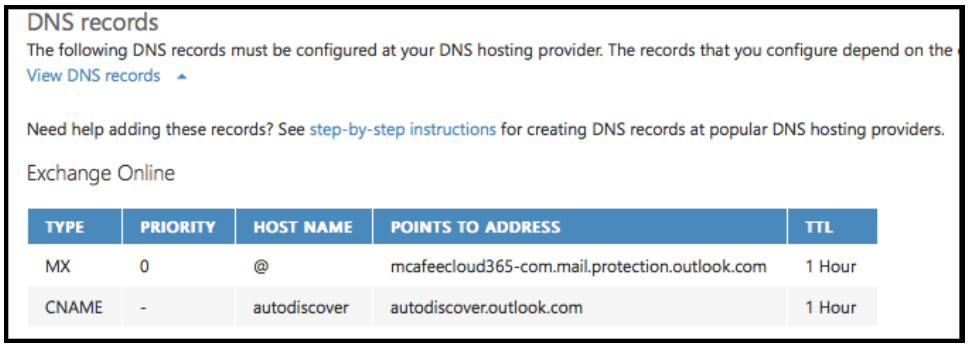
a Log on to your Microsoft Office 365 account as an administrator.

b Select **Admin** | **Office 365**.

c In the left pane, click **Domains**.

d Select the domain, click **Manage DNS**.

e Under **Exchange Online**, find the MX row in the table and copy the value from the **Points to address** column.


DNS records

The following DNS records must be configured at your DNS hosting provider. The records that you configure depend on the

View DNS records

Need help adding these records? See step-by-step instructions for creating DNS records at popular DNS hosting providers.

Exchange Online

TYPE	PRIORITY	HOST NAME	POINTS TO ADDRESS	TTL
MX	0	@	mcafeecloud365-com.mail.protection.outlook.com	1 Hour
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour

Figure 3 Exchange Online MX record

Use this value in the next step.

2 Go to the Control Console and configure an inbound server using the value you copied in the **SMTP Host Address** field.

a Select **Email Protection** | **Setup** | **Inbound Servers.**

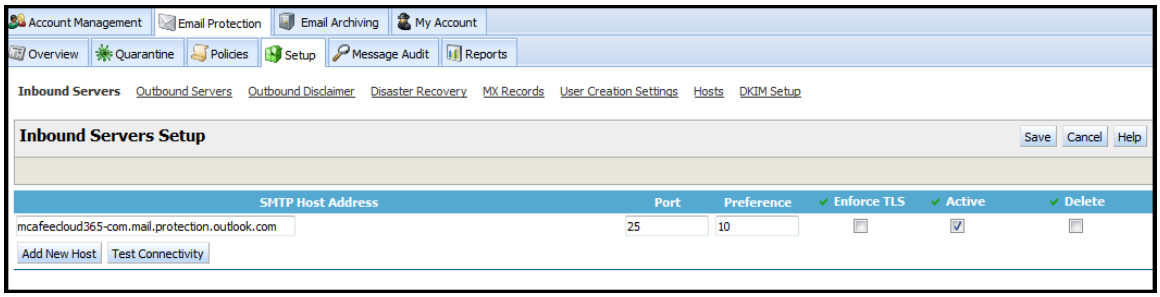


Figure 4 Inbound Servers Setup

b Click **Add New Host.**

A new row appears.

c In the **SMTP Host Address** field, paste the value you copied in Office 365.

d In the **Port** field, enter `25` (default value).

e In the **Preference** field, enter `10` (default value).

f Select **Active** to enable the inbound server.

g Click **Save**.

The inbound server is now setup and active, and filtered email is relayed to Office 365. However, no email will flow through Email Protection until the next step.

3 Determine the MX records to use for your region.

a In the Control Console, select **Email Protection** | **Setup** | **MX Records**.

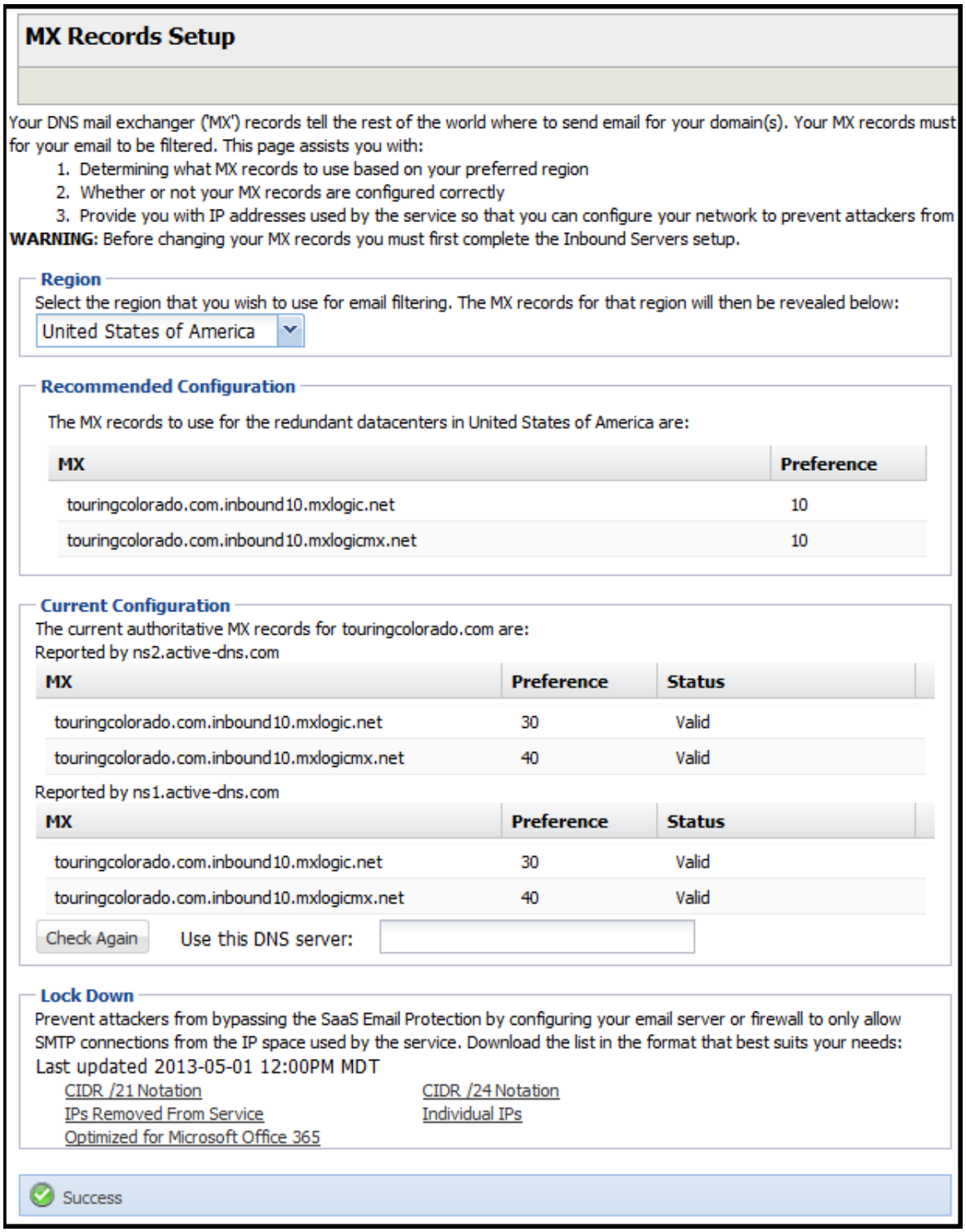


Figure 5 MX records setup page with sample values

b Select your preferred region.

The page refreshes with the recommended MX records for your region. Have this information ready for the next step.

4 Configure your DNS provider's administrative application.

   a In a separate window, open your DNS provider's administrative application.

   b Copy and paste the recommended MX records found in the Control Console as the MX values in your DNS provider's administrative application.

   Your MX record setup is complete. Email is now flowing through Email Protection to Office 365 and Exchange Online. However, due to DNS caching, some DNS servers might not recognize the change for up to three days or longer.

Add a mail flow rule to bypass spam filtering

Create a mail flow rule to turn off spam filtering in Exchange Online and use SaaS Email Protection exclusively.

Before you begin

Allow 72 hours for your MX records to update before activating rules in Office 365.

- Copy the **CIDR /21 Notation** values from the **Lock Down** section of the **MX Records Setup** page in SaaS Email Protection.
- Access your Exchange Online Protection (EOP) Console.

Task

1 Log on to your Microsoft Office 365 account.

2 From the title bar, select **Admin** | **Exchange** to open the **Exchange admin center** page.

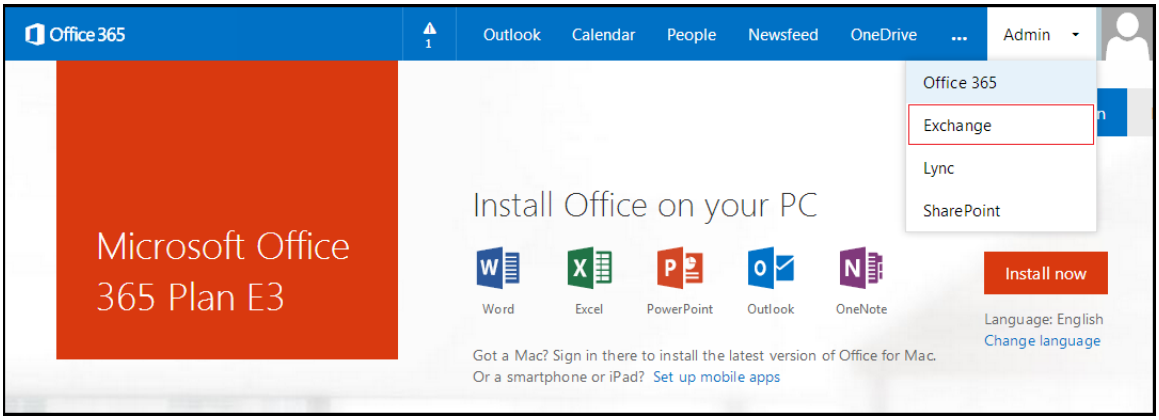


Figure 6 Admin menu

3 In the left navigation, click **mail flow**. Select **rules**.

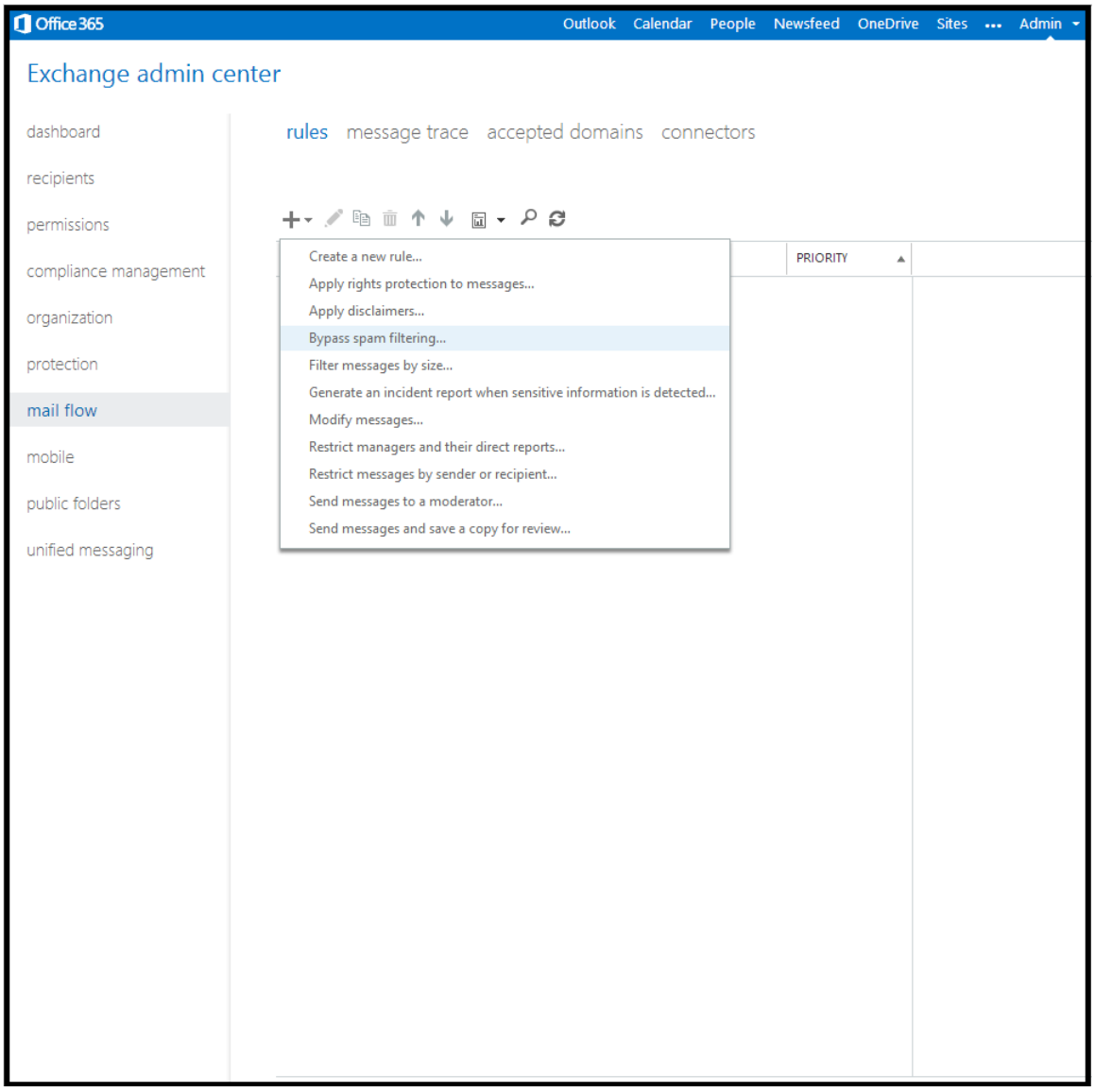


Figure 7 mail flow | rules

4 Click the pull-down menu for the add icon and select **Bypass spam filtering**.

5 In the **Rule** window, complete the required fields.

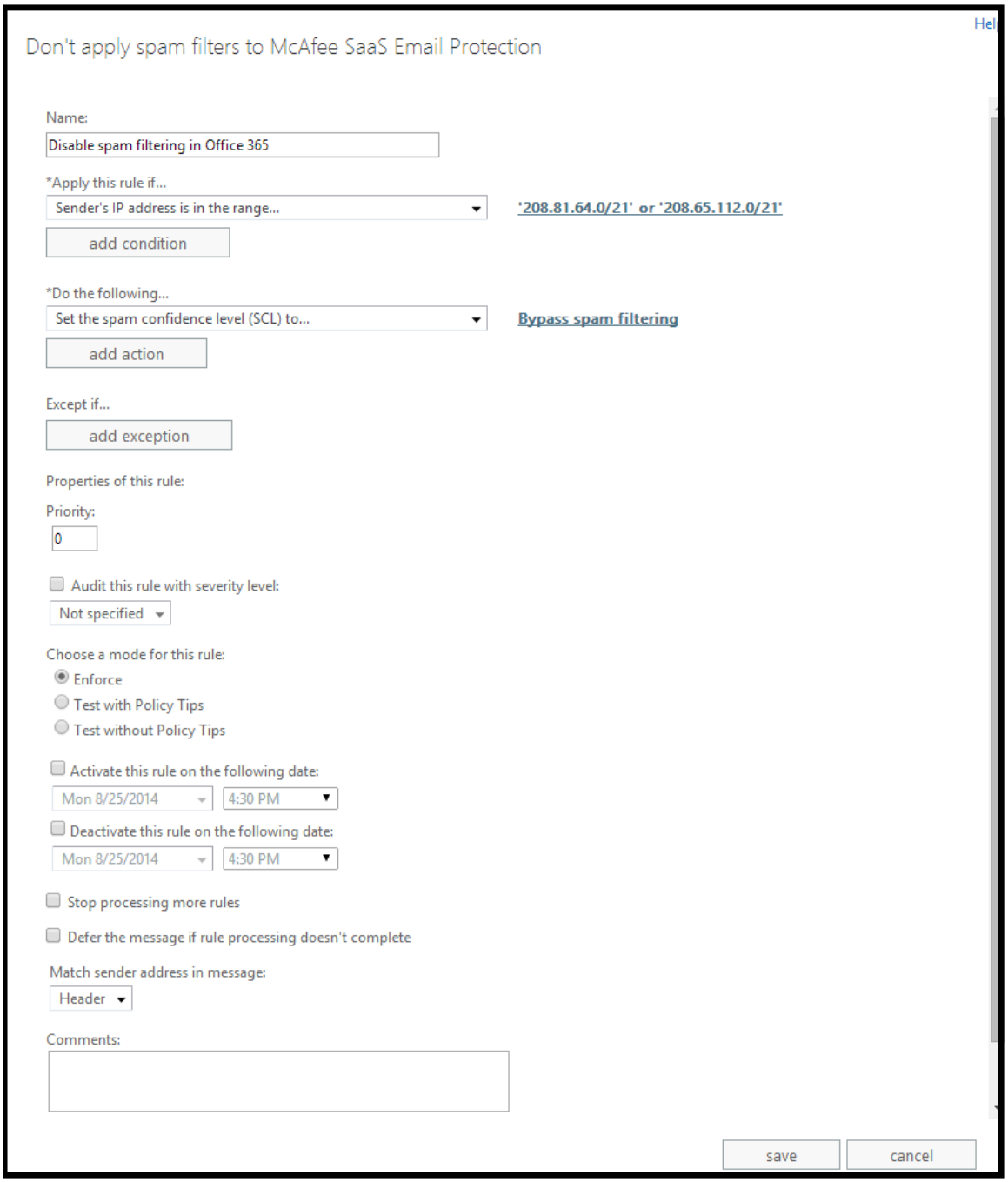


Figure 8 new rule

Option	Instructions
Name	Enter a name for the rule. For example, `Disable spam filtering in Office 365`.
Apply this rule if	1 Select **The sender** | **IP address is in any of these ranges or exactly matches**. 2 In the **specify IP address ranges** window, enter the /21 IP address range you copy and paste from the **Lock Down** section of the **MX Records Setup** page in the Control Console. 3 Click the add icon for each range. 4 Click **ok**.
Do the following	**Set the spam confidence level (SCL) to...** — **Bypass spam filtering** (Default Values).
Except if	Do not add an exception.
Audit this rule with severity level	Deselect.
Choose a mode for this rule	Select **Enforce**.

6 Click **save**.

The **rules** list updates with the new rule. You can review the rule logic in the right side of the page.

Add a mail flow rule to lock down Exchange Online

Create a mail flow rule that only accepts email from SaaS Email Protection. This change ensures that spammers cannot bypass the service.

Before you begin

Allow 72 hours for your MX records to update before activating rules in Office 365.

- Copy the **CIDR /21 Notation** values from the **Lock Down** section of the **MX Records Setup** page in SaaS Email Protection.
- Access your Exchange Online Protection (EOP) Console.

Task

1 Log on to your Microsoft Office 365 account.

2 From the title bar, select **Admin** | **Exchange** to open the **Exchange admin center** page.

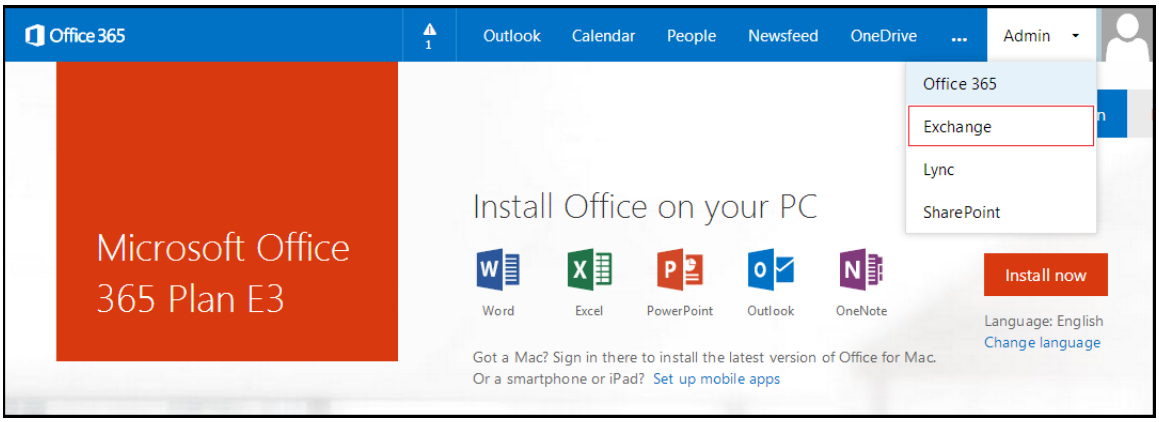


Figure 9 Admin menu

3 In the left navigation, click **mail flow**. Select **rules**.

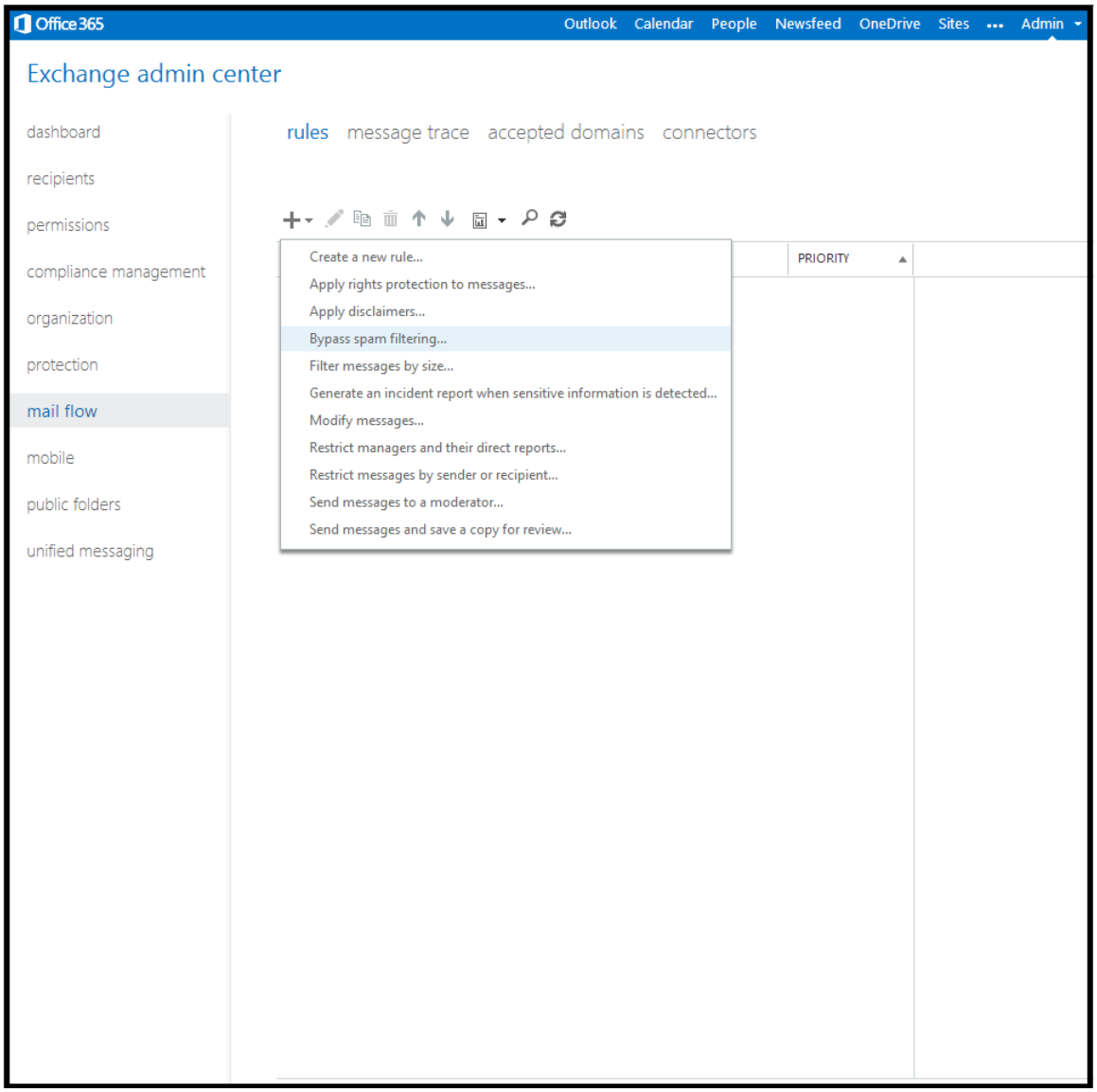


Figure 10 mail flow | rules

4 Click the pull-down menu for the add icon and select **Restrict messages by sender or recipient...**.

5 In the **Rule** window, complete the required fields.

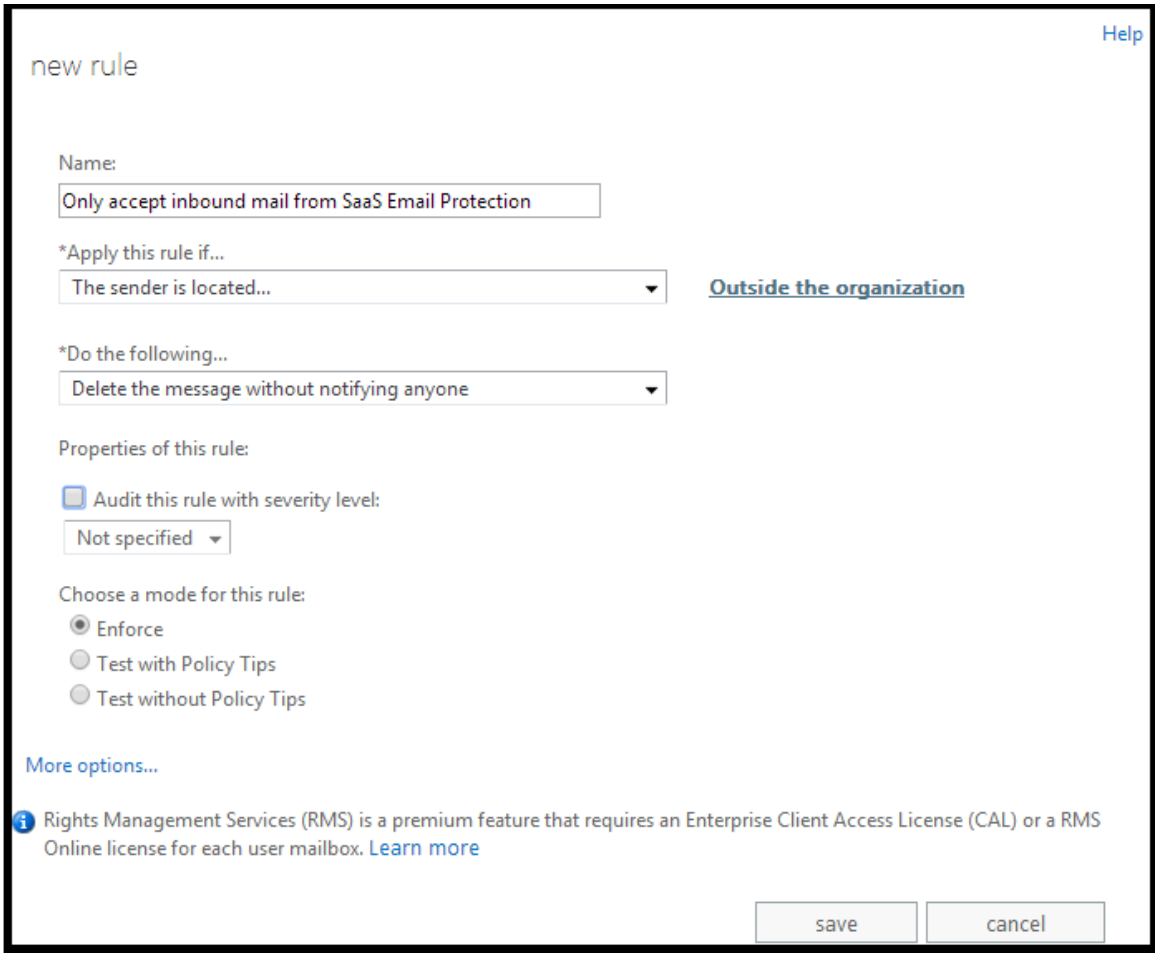


Figure 11 new rule

Option	Instructions
Name	Enter a name for the rule. For example, `Only accept inbound mail from SaaS Email Protection`.
Apply this rule if	1 Select **The sender is located**. 2 In the **select sender location** window, select **Outside the organization**. 3 Click **ok**.
Do the following	Select **Delete the message without notifying anyone**.
Audit this rule with severity level	Deselect.
Choose a mode for this rule	Select **Enforce**.

You have completed the basic form requirements. The rule as it is written blocks all incoming email.

6 Add an exception to allow email flow from SaaS Email Protection.

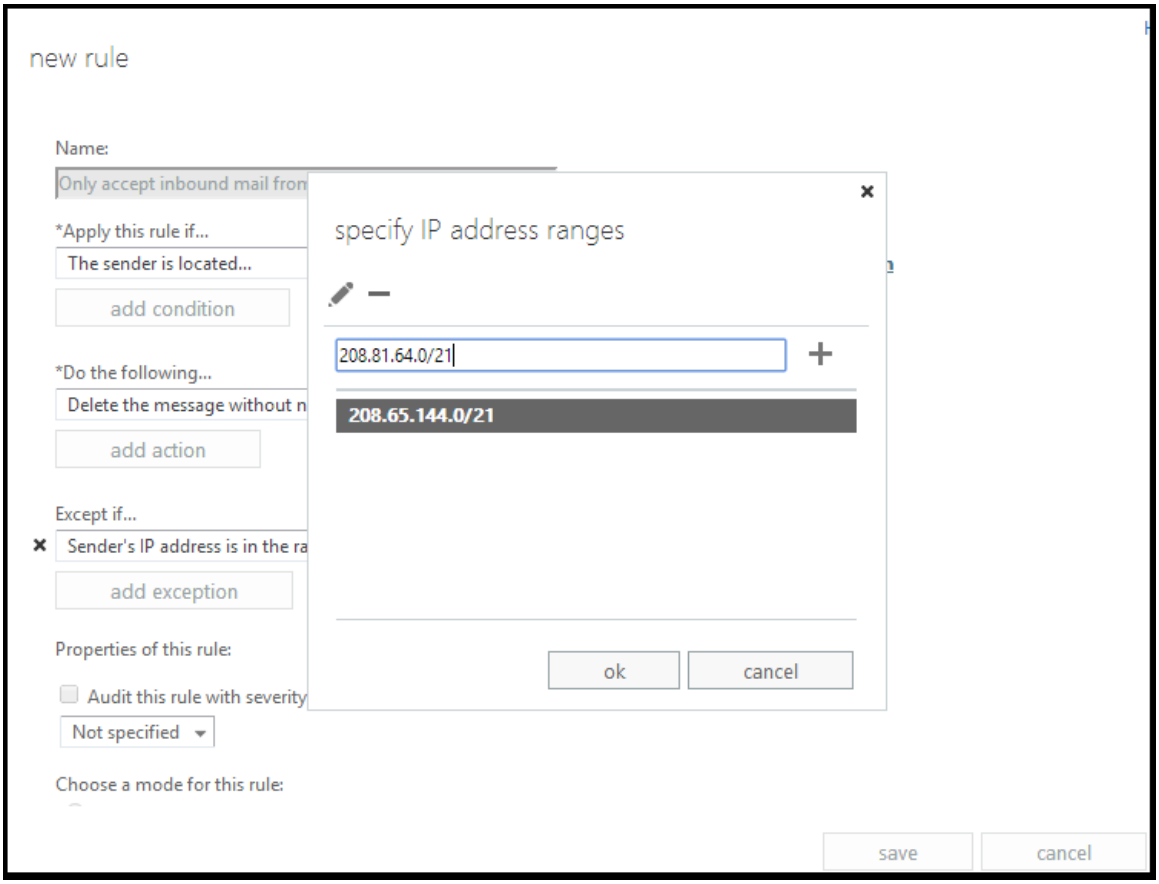


Figure 12 new rule — Except if — specify IP address ranges

a Click **More options**.

New fields appear.

b Under **Except if**, click **add exception**.

A new drop-down menu appears.

c Select **The sender... | IP address is in any of these ranges or exactly matches**.

d In the **specify IP address ranges** window, enter the /21 IP address range you copy and paste from the **Lock Down** section of the **MX Records Setup** page in the Control Console.

e Click the add icon for each range.

f Click **ok**.

The window closes and the new exception logic appears in the **Except if** field.

7 Click **save**.

The **rules** list updates with the new rule. You can review the rule logic in the right side of the page.

Securing outbound mail flow

To secure outbound mail, configure your outbound servers in the McAfee SaaS Control Console and add an outbound connector in Exchange Online.

The outbound mail setup process is optional. Follow these steps if you have purchased outbound service.

How outbound mail is routed

To secure your outbound mail, relay your email through the McAfee SaaS service using an outbound connector in Exchange Online. The following examples explain each scenario.

Outbound mail without McAfee SaaS Email Protection

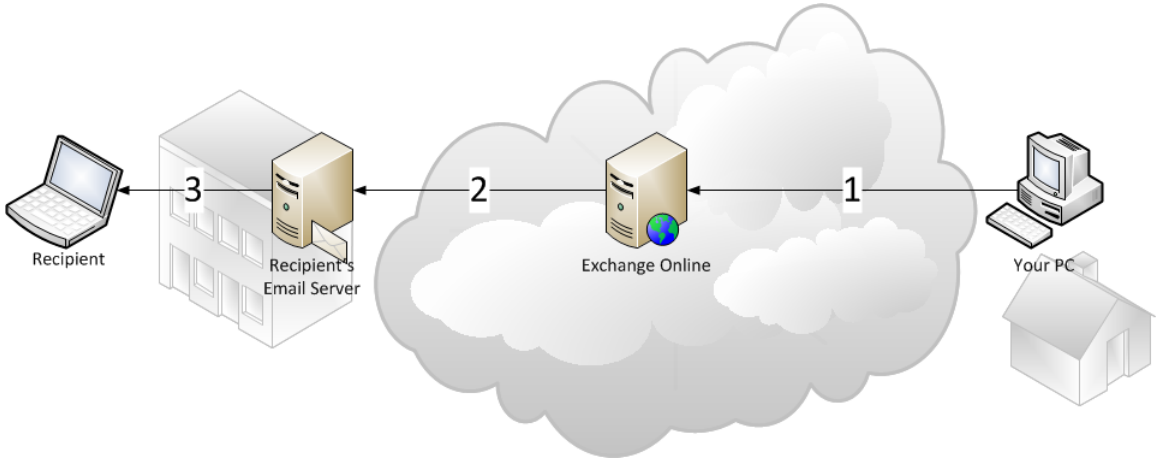


Figure 13 Outbound mail with Office 365

1. You send an email to an external recipient using the Microsoft Outlook desktop application or the Outlook Web Application (OWA).
2. Office 365 performs an MX lookup and sends the email to the recipient's email server.
3. The recipient opens the email in their email client.

Outbound mail with Exchange Online secured by McAfee SaaS Email Protection

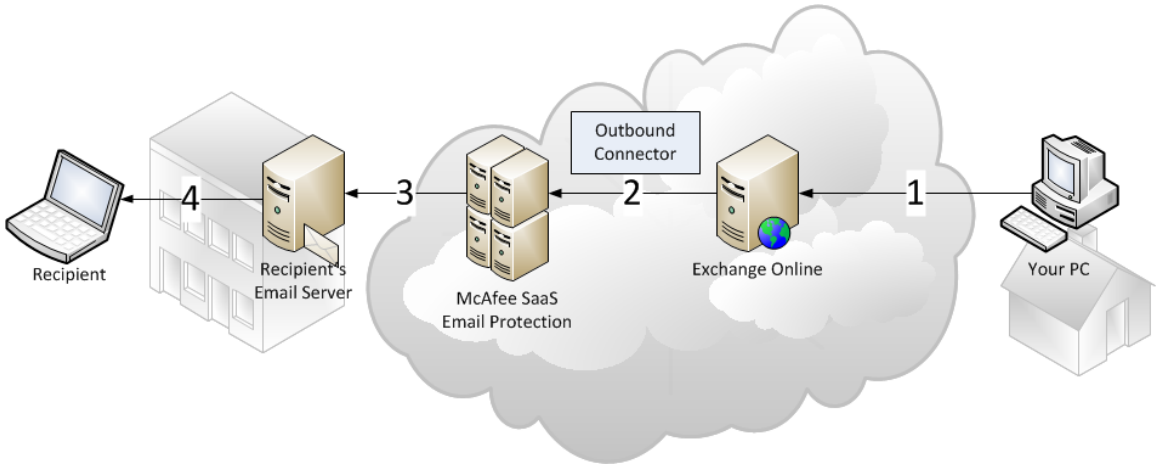


Figure 14 Outbound mail with Office 365 secured by McAfee SaaS Email Protection

1 You send an email using the Microsoft Outlook desktop application or the Outlook Web Application (OWA).

2 Office 365 uses the outbound connector to route all outbound messages through Email Protection.

3 Email Protection performs the MX lookup and sends the email to the recipient's email server.

4 The recipient opens the email in their email client.

Set up outbound servers in SaaS Email Protection

In the **Outbound Server Setup** page, allow Email Protection to filter email from Microsoft Office 365. Repeat this process for each of your domains.

> **Before you begin**
>
> Outbound server configuration is region aware. Before adding outbound servers, select your region by going to **Setup** | **MX Records**.

Task

1 In the Control Console, select **Email Protection** | **Setup** | **Outbound Servers**.

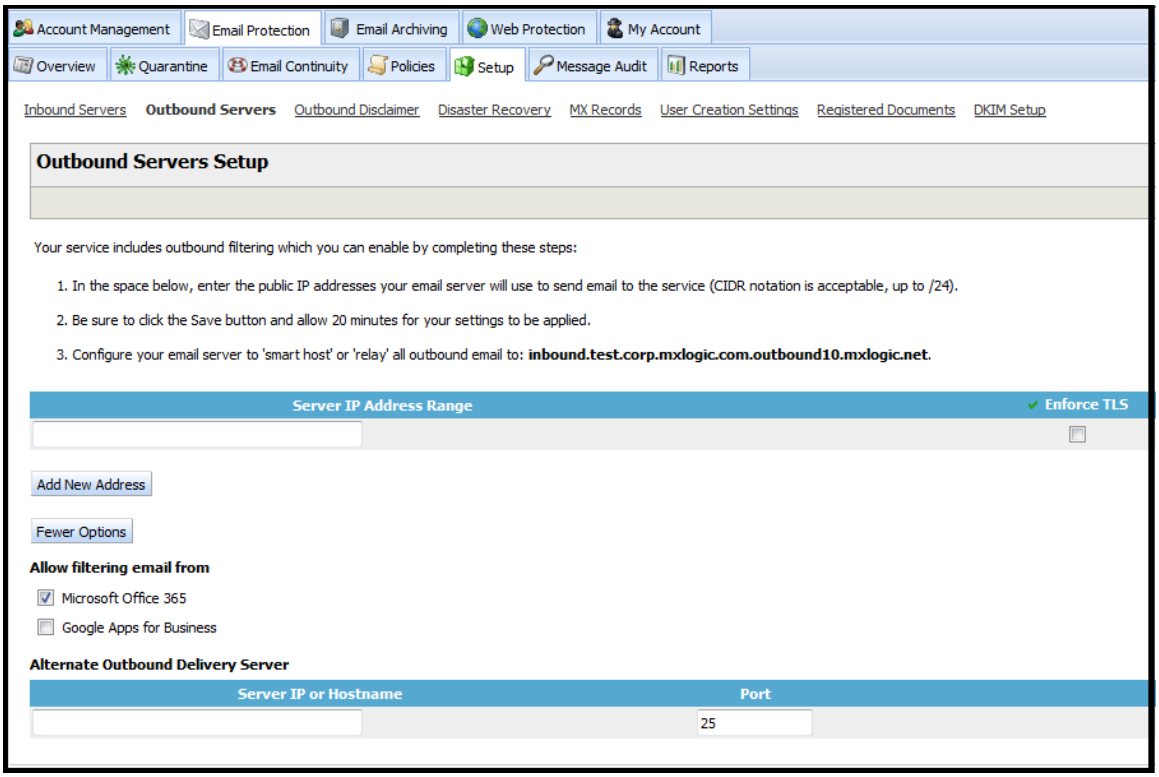


Figure 15 Outbound Server Setup — Office 365

2 If necessary, use the domain link in the upper right to change domains.

3 Click **More Options...**.

4 Under **Allow filtering email from**, select **Microsoft Office 365**.

5 Click **Save**.

Wait at least 30 minutes for your new settings to take effect.

Add an outbound connector to set up your outbound server

Configure Microsoft Office 365 to route outbound email to Email Protection.

Before you begin

- Set up your **Outbound Servers** in Email Protection before configuring Office 365.
- Copy the host name (in bold text) from the **Outbound Servers Setup** page in Email Protection.

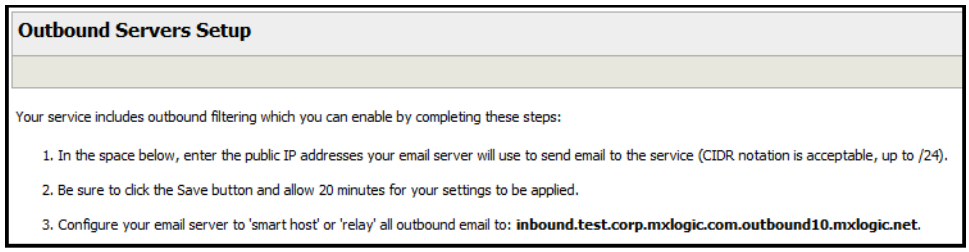


Figure 16 Copy the host name displayed in bold text

Task

1 Log on to your Microsoft Office 365 account.

2 Select **Admin** | **Exchange** to open the **Exchange admin center** page.

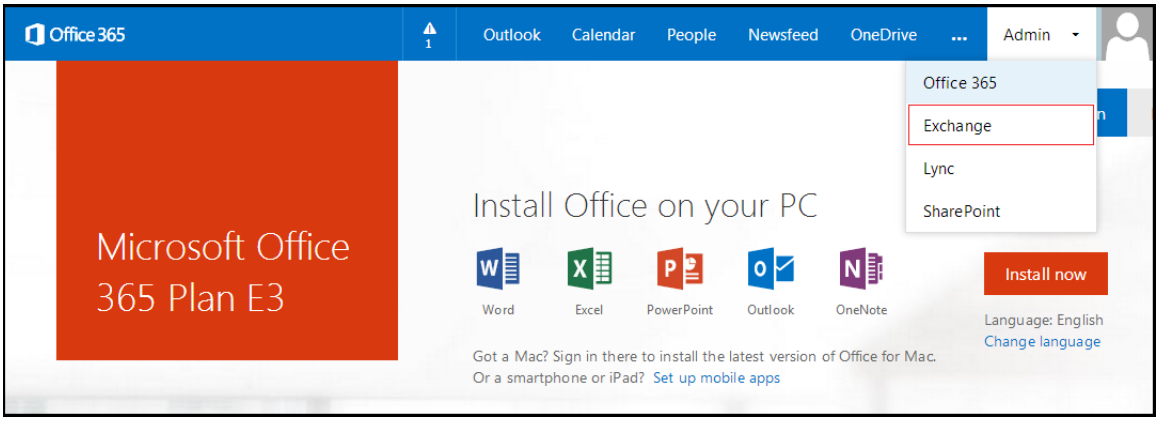


Figure 17 Admin menu

3 In the left navigation, click **mail flow**. Select **connectors**.

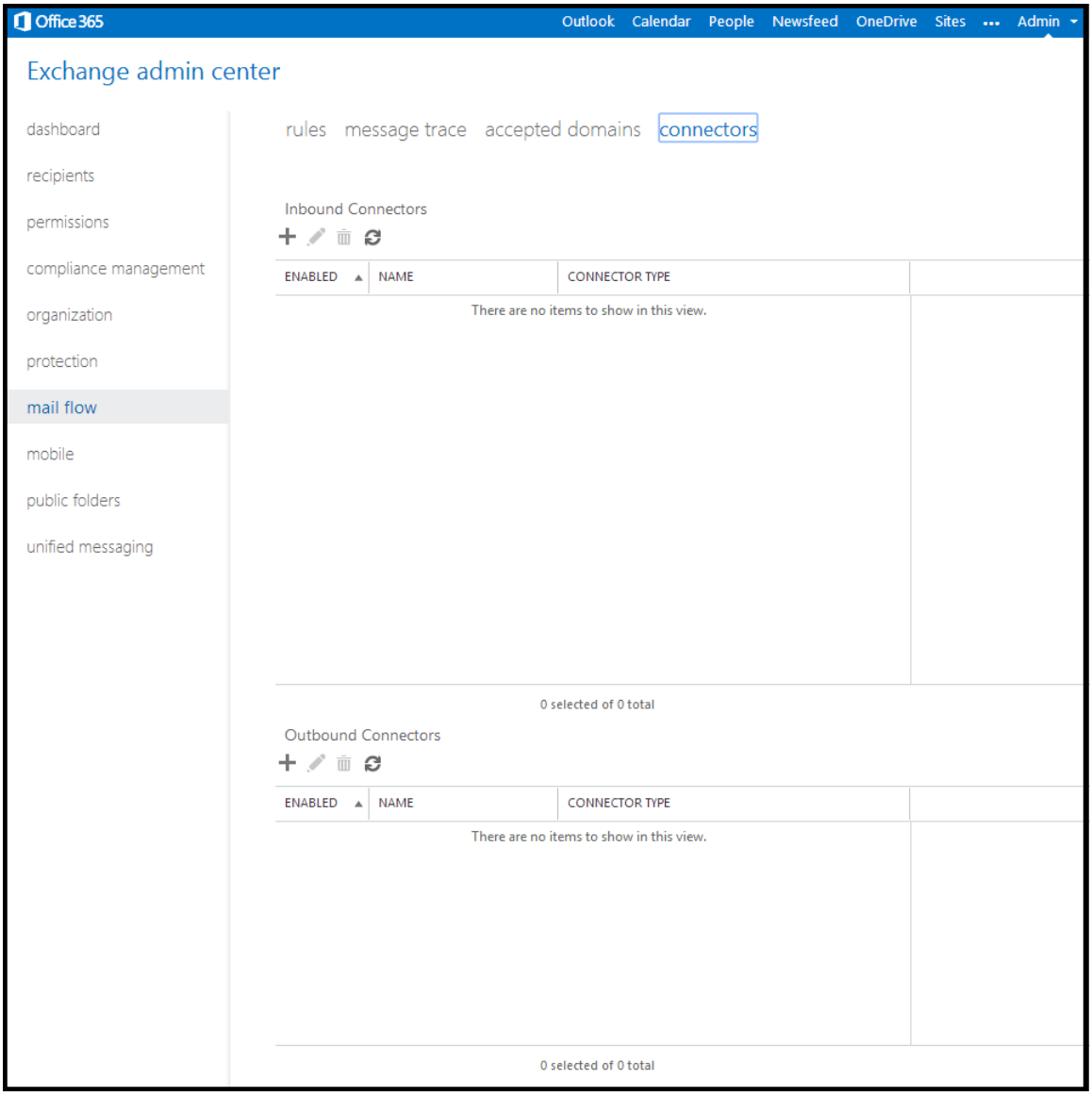


Figure 18 mail flow | connectors

4 Under **Outbound Connectors**, click the add icon.

5 In the **new outbound connector** window, complete the required fields.

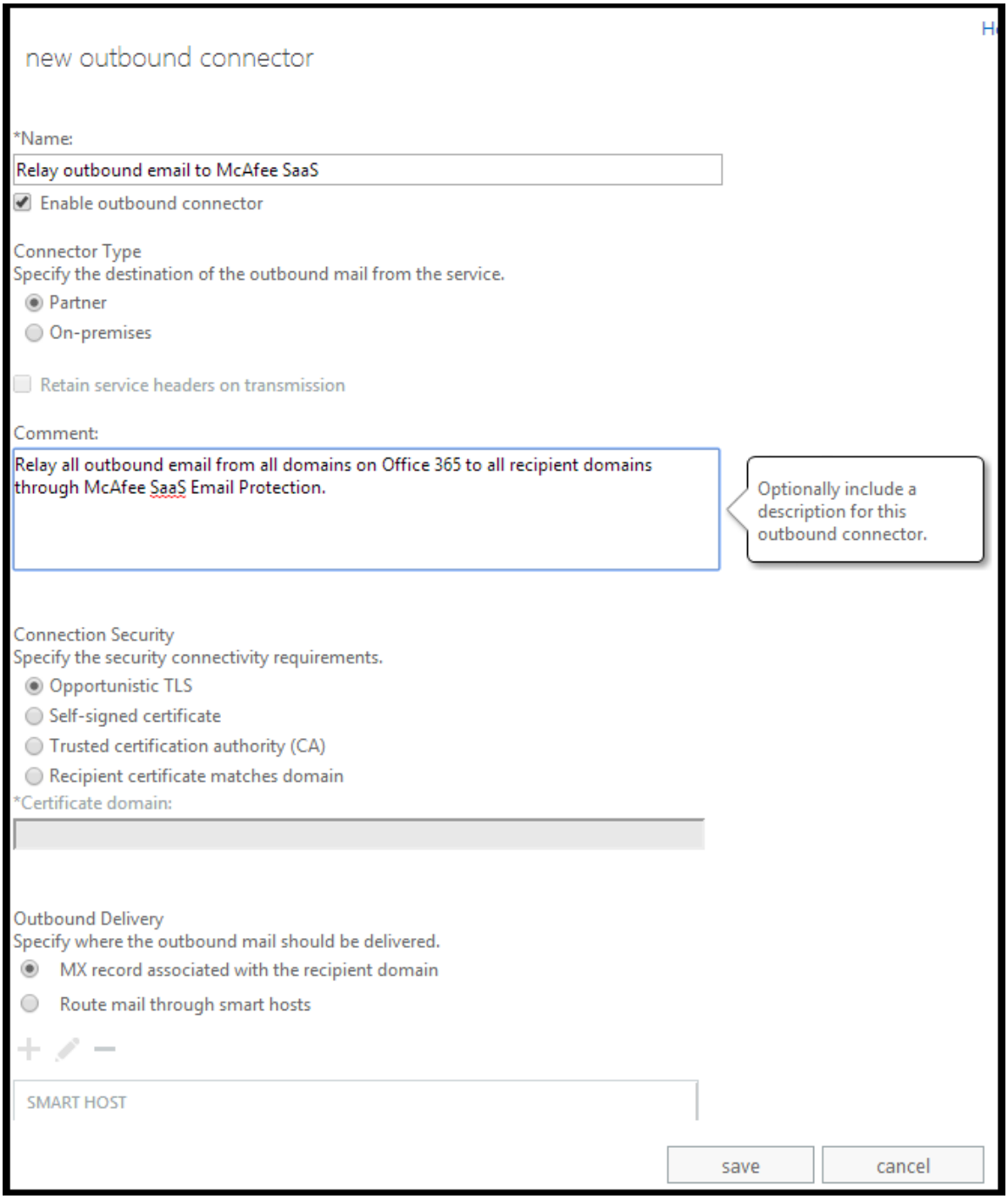


Figure 19 new outbound connector

Option	Definition
Name	Enter a name for the new outbound connector. For example, `Relay outbound mail to McAfee SaaS`.
Enable outbound connector	Select to enable (default value).
Connector Type	Select **Partner** (default value).

Option	Definition
Comment	Enter a description. For example, `Relays all outbound email from all domains on Office 365 to all recipient domains through McAfee SaaS Email Protection.`
Connection Security	Select **Opportunistic TLS** (default value).
Outbound Delivery	Select **Route mail through smart hosts** and add a smart host. 1 Click the add icon to add a smart host. 2 In the **add smart host** window, enter the host name that appeared in bold that you copied from the **Outbound Servers Setup** page. 3 Click **save**.
Recipient Domains	Add domains. 1 Click the add icon to add a domain. 2 In the **add domain** window, enter `*` to specify all domains. 3 Click **ok**.

6 Click **save**.

The page updates to display the new outbound connector.

Congratulations!

You have completed the installation process. Office 365 is now secured by McAfee SaaS Email Protection.