



SINGTEL EMAIL PROTECT

Provisioning Guide

Table of Contents

About This Document	2
1 Pre-Provisioning	2
1.1 Email Acceptance	2
1.2 Incoming Port.....	2
1.3 IP Address Range To Allow	2
1.4 SPF Record Include Text.....	3
2 Setup After Provisioning	3
2.1 Licensed Users	3
2.2 Inbound MX Record	3
2.3 Console URL.....	3
3 Configuring G Suite Email	4
3.1 Set up an Outbound Mail Gateway to deliver outgoing messages to Email Protect	4
3.2 Set up an Inbound Mail Gateway to accept incoming messages from Email Protect	4
4 Configuring Exchange Online	5
4.1 Set up a connector to send outgoing messages through Email Protect.....	6
4.2 Set up a connector to accept incoming messages from Email Protect	9
4.3 Set up Connection Filter Exclusions	11

About This Document

Singtel Email Protect is an email gateway product that protects against spam and malware.

This document highlights configuration items you must complete in your existing environment before your Email Protect account can be provisioned.

This document does not cover the required details you supplied on the provisioning form, such as the location where Email Protect will send your incoming processed email.

For full details of the product features and web interfaces, see the Customer Console guide and Help.

Singtel Email Protect is Powered by Trustwave SEG Cloud (lite).

1 Pre-Provisioning

This section describes items that must be completed before Email Protect is provisioned and activated.

1.1 Email Acceptance

You must configure your firewall and email server (or cloud service) to accept incoming messages from Email Protect. You must complete this task before your account is provisioned because the email will be sent through Email Protect immediately upon provisioning.

Email sending through Email Protect is a separate item that you can only complete after provisioning is complete.

1.2 Incoming Port

Your email server must accept email on **port 25**, the standard SMTP port.

1.3 IP Address Range To Allow

Inbound messages from Email Protect to your servers may originate from addresses in the following IP CIDR blocks:

20.40.125.96/28

20.40.161.176/28



Note: Ensure that your internal email system always accepts messages from these IP blocks. For example, if you use IP reputation services, whitelist these IP addresses.

If you use Microsoft Exchange Online as your mail server, you should exclude the IP ranges from filtering temporarily. After the Email Protect service is live, you should configure a connector so that incoming mail can **ONLY** be sent from Email Protect.

1.4 SPF Record Include Text

To include Email Protect in a SPF record for your email domain, use this text:

```
include:spf.seg.au.twsegcloud.com
```

For example

```
v=spf1 include:spf.seg.au.twsegcloud.com -all
```

If your email service is hosted on Office365, also include the Office365 SPF record:

```
include:spf.seg.au.twsegcloud.com include:spf.protection.outlook.com
```

2 Setup After Provisioning

2.1 Licensed Users

As part of the provisioning process, once you have access to the Customer Console you must enter or upload a list of all valid email addresses within your organization. You can upload the information using a simple text file with one address per line. For details, see the Customer Console guide.

2.2 Inbound MX Record

To have incoming mail delivered through Email Protect, set your MX record as follows:

MX Record	Priority
mx.au.twsegcloud.com	10

- You (the customer) or your DNS provider must make this setting.
- Make sure you only have one MX record. If you have more than one record, then email might bypass Email Protect.

2.3 Console URL

Customers use the following URL to connect to connect to the Console, for setup of licensed users and email management:

<https://seglite.apac.twsegcloud.com/>

3 Configuring G Suite Email

If you use Google G Suite for cloud email hosting, you will set up two gateways to route email between Email Protect and G Suite Email. To complete this step, you must have an Administrator credential for the G Suite service.

3.1 Set up an Outbound Mail Gateway to deliver outgoing messages to Email Protect

1. From the G Suite dashboard, go to Apps > G Suite > Gmail > Advanced settings.
2. In the Organizations section, highlight the top-level org.
3. Scroll down to the Outbound gateway section.

In the Outbound gateway text box, enter the externally resolvable hostname of the Email Protect server:
`seg-outbound.au.twsegcloud.com`

4. Save your changes.

3.2 Set up an Inbound Mail Gateway to accept incoming messages from Email Protect

1. From the G Suite dashboard, go to Apps > G Suite > Gmail > Advanced settings.
2. In the Organizations section, highlight your domain (top-level org).
3. Scroll down to Inbound gateway (you can also enter Inbound gateway in the search field).
4. Hover the cursor to the right of Inbound gateway. To create a new inbound gateway setting, click Configure. To edit an existing setting, click Edit.
5. Under Gateway IPs, enter the IP address range of the Trustwave Email Protect servers. See the "IP Ranges To Allow" earlier in this document.
6. Also select Reject all mail not from gateway IPs and Require TLS for connections from the email gateways listed above.
7. Save your changes.

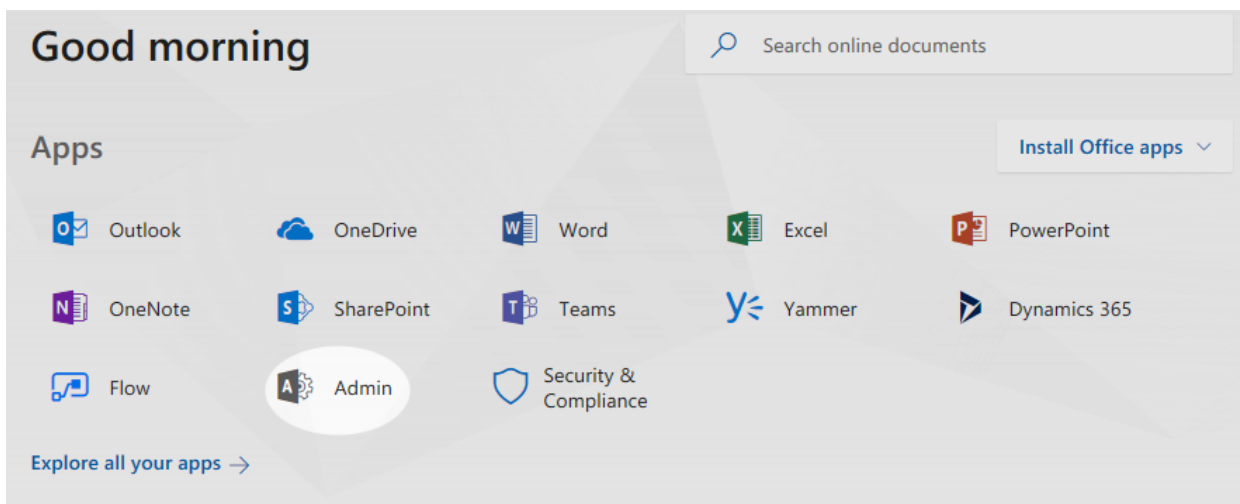
4 Configuring Exchange Online

If you use Office 365 Exchange Online to host email, you will set up two connectors to route email between Email Protect and Exchange Online.

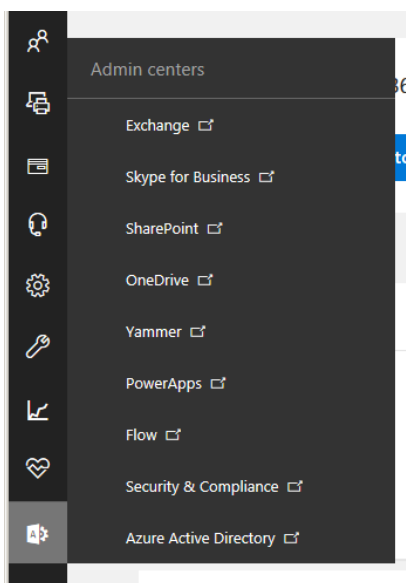
To complete this step, you must have an Office 365 Administrator credential with permission to create connectors. You may find that the validation process only works with a Microsoft browser.

To create a connector in Office 365:

8. From the Office home page, click **Admin**.



9. From the Admin left menu, click **Exchange** to go to the Exchange Admin Center.



10. Next, click **mail flow**, and then click **connectors**.

4.1 Set up a connector to send outgoing messages through Email Protect

11. To start the Connector wizard, click the plus symbol **+**.

12. On the first screen, choose a connector as follows:

From:

Office 365

To:

Partner Organization

Click **Next**.

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. [Learn more](#)

From:

To:

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

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, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For outbound email, it refers to

Next Cancel

13. On the next screen, give the connector a name and a detailed description. If you want to enable this routing immediately, check the box **Turn it on**. Click **Next**.

New connector

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

*Name:

Description:

What do you want to do after connector is saved?
 Turn it on

Next Cancel

Optionally include a description for this connector.

14. On the following screen (When do you want to use this connector?), select *Only when email messages are sent to these domains*.

Click **+** to add recipient domains. On the **Add domain** window, enter ***** (to signify all domains), and then click **Next**.

New connector Help

When do you want to use this connector?

Only when I have a transport rule set up that redirects messages to this connector

Only when email messages are sent to these domains

+ ✎ -

Select this option only if you created a rule that redirects email messages to this connector.
[Learn more](#)

add domain -- Webpage Dialog x

<https://outlook.office365.com/ecp/Connectors/DomainEntry.aspx?mode=multiple&\new=true> Help

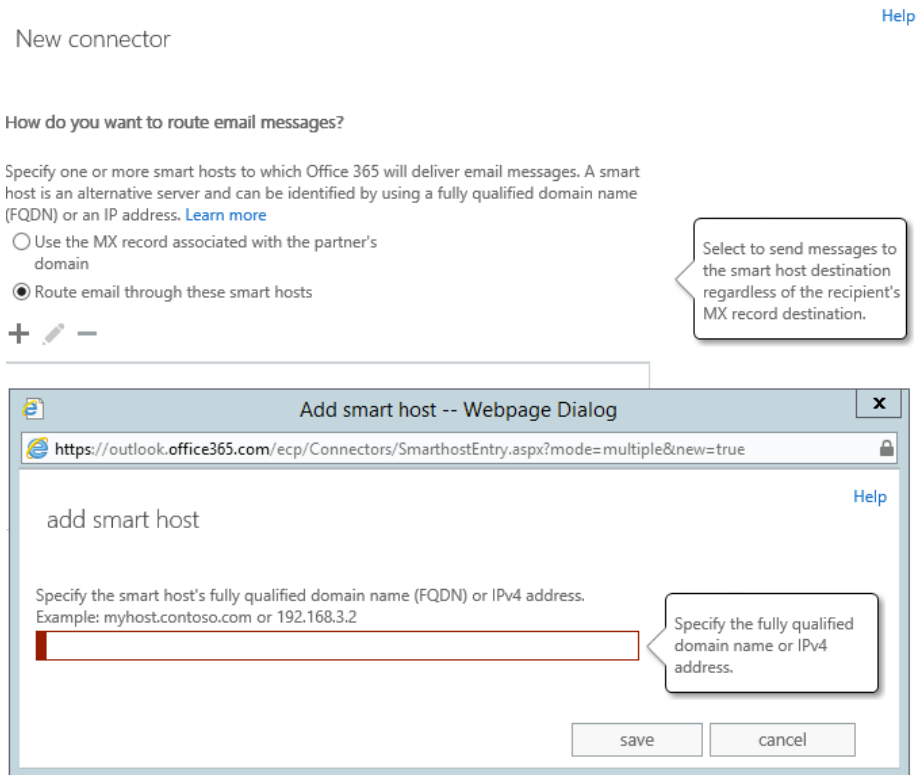
add domain

Specify the domain name, with or without wildcards.
 Example: * or *.contoso.com or *.com

Specify the fully qualified domain name. Example: myhost.contoso.com

ok cancel

15. On the next screen How do you want to route email messages?, select Route email through these smart hosts.
16. Click + to add a smart host.
17. Enter the externally resolvable hostname of the Email Protect server:
seg-outbound.au.twsegcloud.com.



18. On the following screen How should Office 365 connect?., The Transport Layer Security box should be selected.

19. Ensure that your connector validates. You will need to add a deliverable email address where a message can be sent for validation. Because this connector is used for all outbound messages, you can enter any address outside your managed domains.

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

Specify an email address for your partner domain. You can add multiple addresses if your partner has more than one domain.

+ ✎ -

testuser@example.com

Back Validate Cancel

20. Save the connector.

4.2 Set up a connector to accept incoming messages from Email Protect



Note: When you set up a connector as described in this section, Exchange Online will ONLY accept incoming SMTP messages that are sent from the Email Protect servers at the IP addresses you specify. Messages from any other source will be refused.

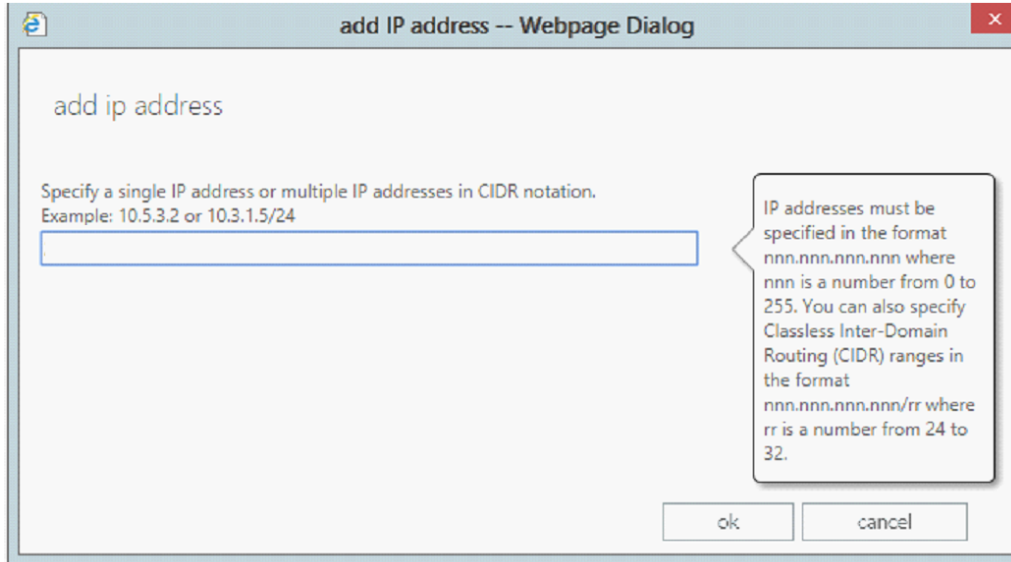
This connector is required to ensure that malware or spam cannot bypass Email Protect. You should only enable the connect AFTER you have updated MX records and confirmed email is flowing through Email Protect to Exchange Online.

The steps to accept incoming messages are similar to those for outgoing messages.

21. To start the Connector wizard, click the plus symbol +.
22. On the first screen, choose a connector as follows (**note the direction**):
From:
Partner Organization
To:
Office 365
23. Give the connector a name and verbose description.
24. On the screen *How do you want to identify the partner organization?*, select *Use the sender's domain*.
 - Click + to add sender domains. On the **Add domain** window, enter * (to signify all domains)

25. On the screen *What security restrictions do you want to apply?*, select *Reject email messages if they aren't sent from within this IP address range*

- Click **+** to add an IP address. On the **Add ip address** window, enter the IP address ranges mentioned earlier in this document.



26. Repeat until you have added all required ranges.

27. Choose to *Reject email messages if they aren't sent over TLS*. **Do not require a subject name on the certificate.**

28. Save the connector.

4.3 Set up Connection Filter Exclusions

Exchange Online includes a “connection filtering” function that limits the number of messages received from each IP address. You must exclude Email Protect from this filtering to ensure that all incoming messages can be delivered.

To set up exclusions:

1. From the Exchange Admin Center, click **protection** and then **connection filter**.

Exchange admin center

malware filter **connection filter** spam filter outbound spam quarantine action center
dkim

✎ 🗑️ ↺

NAME	
Default	Default


Scoped to:
All domains

Summary

IP Allow list:
Configured

IP Block list:
Not configured

Safe list:
Enabled

2. Select the default filter and then click  to edit.
3. On the Connection Filtering tab, in the Allowed IP Address list, add the IP address ranges for Email Protect, as in the connector setup.

4. Click **Save**.

The filtering information may appear as below:

