Office 365: Secure email configuration

Published June 2019
Version 2

Contents

Purpose 3

Glossary of Terms 3

Overview 3

Before you start 4

Technical Configuration 4

- Overview 4
- Admin Center 4
- New Outbound Connector 6
- New Inbound Connector 9
- Anti-spoofing – DMARC 12
- Anti-spoofing – SPF 12
- Office 365 Inbound 12
- Notification Rules 13

Testing 14

- Additional TLS Verification 14

Purpose

This document details the configuration changes that you need to make to your Office 365 tenant configuration to enable secure email exchange between your secure.nhs.uk email service and NHSmail.

If your organisation is pursuing DCB1596 (Formally SCCI1596) then these settings must be made before applying for certification.

Glossary of Terms

Term / Abbreviation	What it stands for
DCB1596	Health and cares secure email standard - https://digital.nhs.uk/nhsmail/secure-email-standard
TLS	Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). For secure email, forced TLS means encrypt and fail if not possible, opportunistic TLS means encrypt if possible, send in the clear if not.
DMARC	Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication protocol.
MX Record	A mail exchanger record (MX record) is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient's domain, and a preference value used to prioritize mail delivery if multiple mail servers are available.
SPF	An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of the organisations domain. The purpose of an SPF record is to prevent spammers from sending messages with forged From: addresses at an organisations domain.

Overview

The document covers;

1. Forcing TLS (secure) connections for both inbound and outbound email.
2. Configuring anti-spoofing measures (DMARC).
3. Creating Rules to protect content.

Both points 1 and 2 above are required to gain and then maintain DCB1596 certification.

Before you start

1. Admin User – you must have a user account for your Office 365 instance that has administrative rights to make the changes listed later in this document.
2. Domain Name – your email services must be accredited to DCB1596. Once this is complete you will need to identify your organisation with a trusted domain e.g. <organisation>.secure.nhs.uk domain name assigned to you..
3. Ensure you have the permission of your organisation to make these changes and that disruption to operational email services is kept to a minimum.
4. When switching to Office 365 you should ensure you have no mail routing entries in DNS pointing to the relay service (relay.nhs.uk). This can create mail routing loops as well as potentially cause message authenticity failures where features like domain keys identified mail are used.

Technical Configuration

NOTE:	The screen shots were taken from the Office 365 Admin centre in April 2017 the screens may change in the interim.

Overview

In this section you will

- Open the Office 365 Exchange Admin Centre.
- Configure a new inbound email connector to only accept secure TLS encrypted email from NHSmail.
- Configure a new outbound email connector to encrypt any email going to NHSmail.

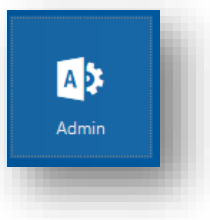
  Note: Office 365 will use opportunistic TLS for all other connections.
- Configure anti-spam/spoofing measures:
  - DMARC

Admin Center

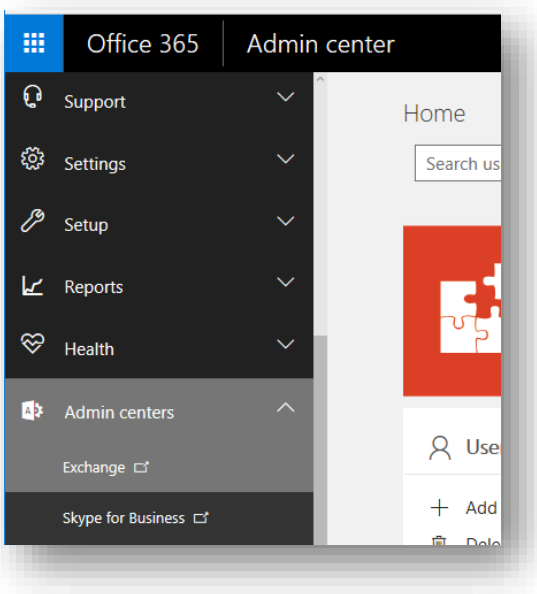
Login to Office 365 using your administrator user.

http://portal.office365.com

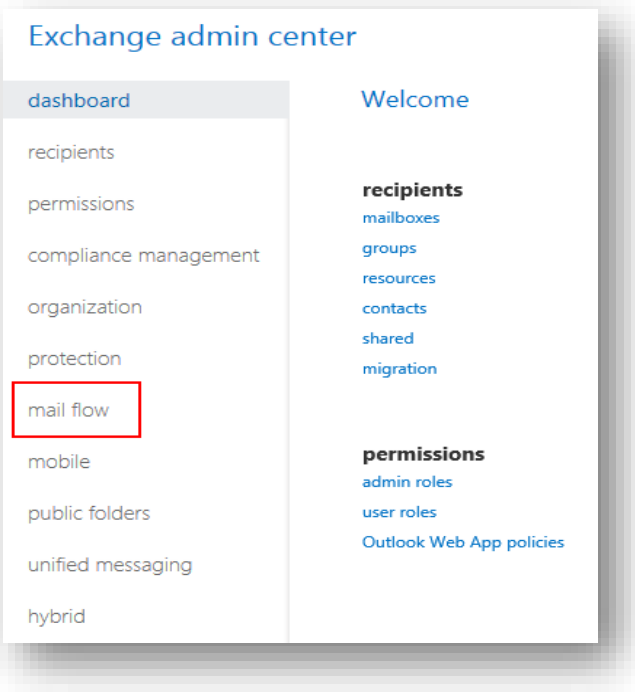
Then click on the waffle menu, usually top left hand corner, and click the Admin icon



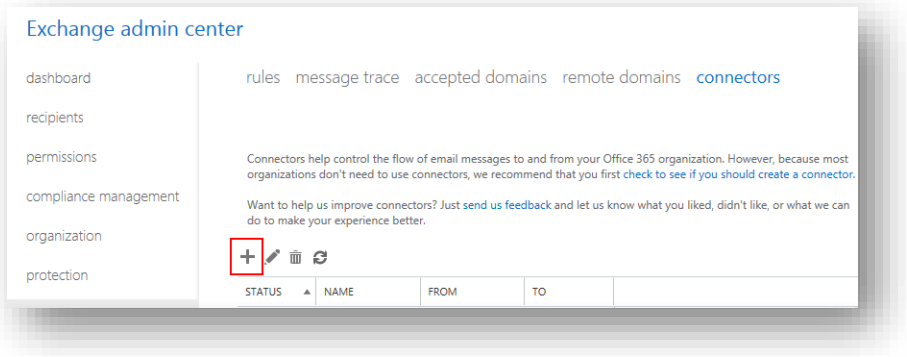
Then in the menu on the left-hand side click on '*Admin center'* to expand the list and then 'Exchange'.



Once the '*Exchange admin center*' opens click on 'mail flow' in the left-hand column.



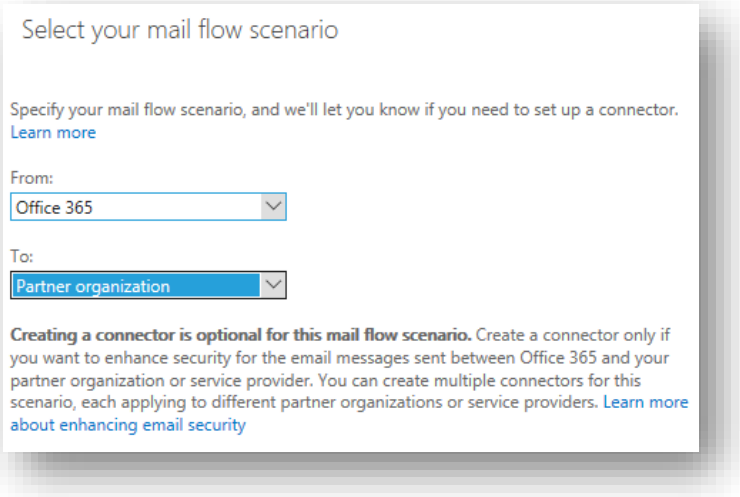
Now click on 'connectors' and then the '+' to create a new connector.



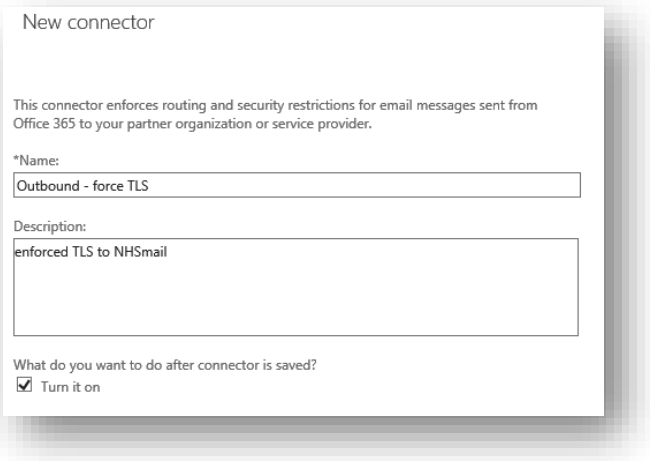
New Outbound Connector

This will set up a connector to send TLS encrypted email to NHSmail.

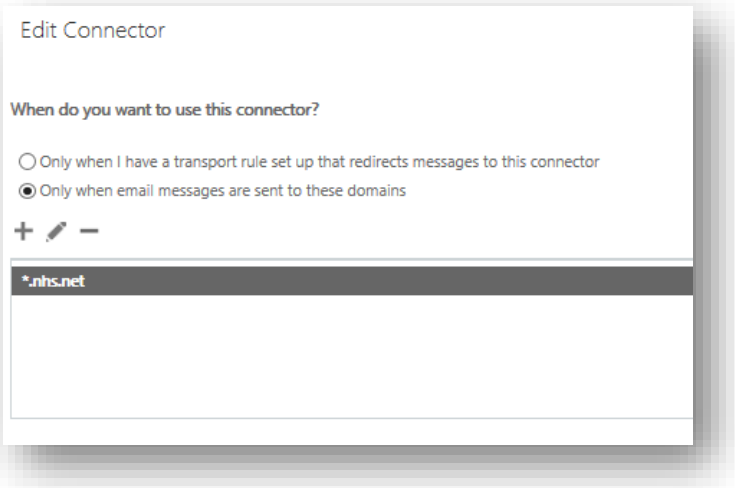
When prompted to enter your mail flow scenario in the ‘From:’ drop down select ‘Office 365’ and in the ‘To:’ drop down select ‘Partner Organization’.



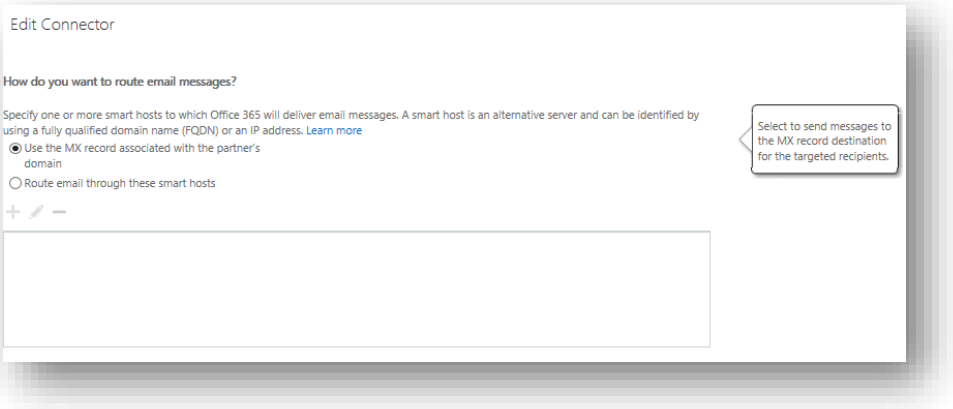
Click on ‘Next’ and enter a name and description for the connector. Make sure that ‘Turn it on’ remains checked.



Click ‘Next’.



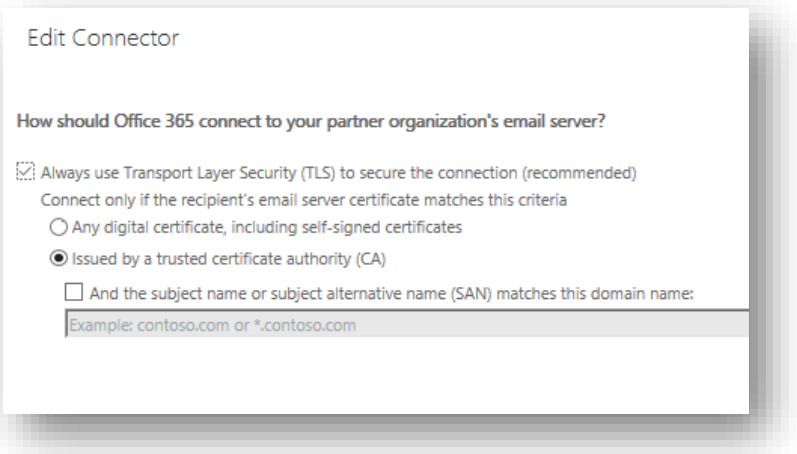
In the next dialogue select ‘Use the MX record associated with the partner’s domain’.



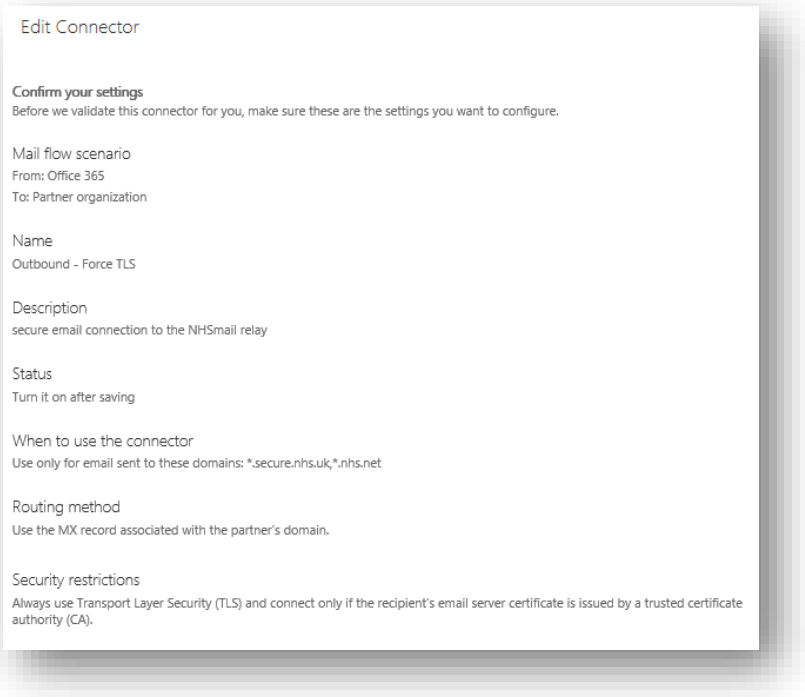
Office 365 will determine what this address is - you do not need to provide it.

Click ‘Next’

Configure the connector to always use TLS and only if the email server certificate is ‘Issued by a trusted certificate authority (CA)’.

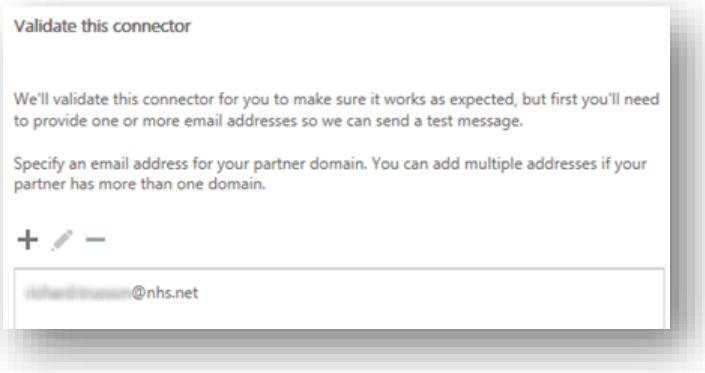


Click ‘Next’ and you will be presented with a summary of the connector settings. If you need to change any click ‘Back’, otherwise click ‘Save’.

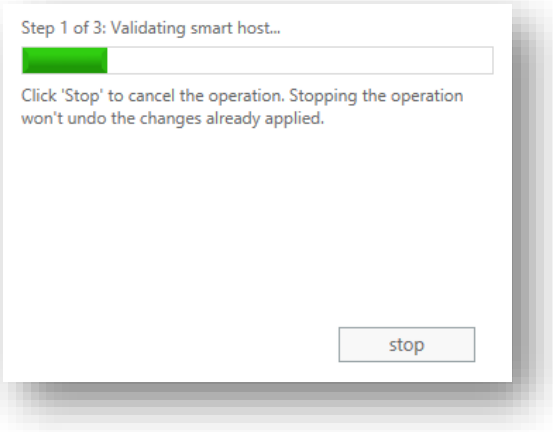


You will be prompted to validate the connector. This is optional but recommended.

Follow the instructions and enter a valid, NHSmail, address to send the test email to.



Click on ‘Validate’…



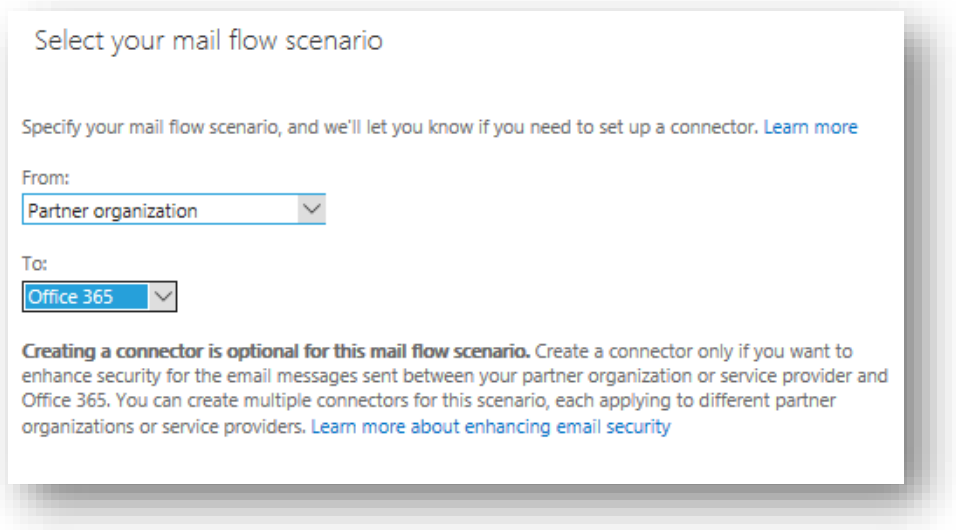
Click on ‘Close’ once the validation operation completes.

If the validation is successful your connector is setup and you can exit the dialogue. If validation fails please review your settings.

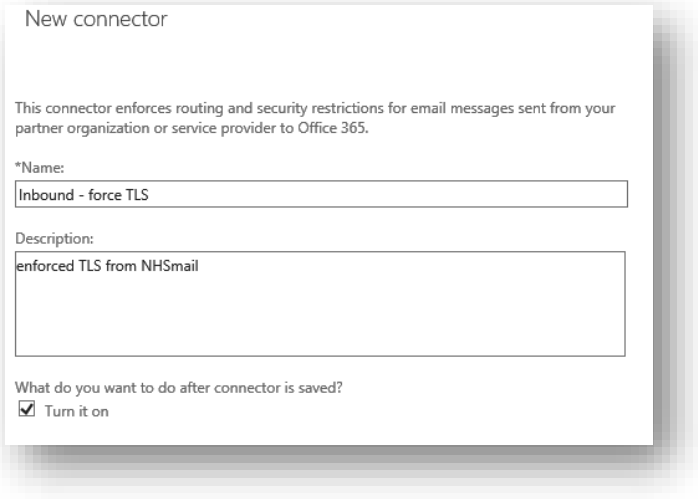
New Inbound Connector

This will create an inbound mail connector to ensure any email being received from NHSmail is encrypted.

From the Exchange Admin connectors dialogue, click on ‘+’ to create a new mail flow. Select ‘*Partner organization’* in the ‘From:’ list and Office 365 in the **‘**To:**’** list.

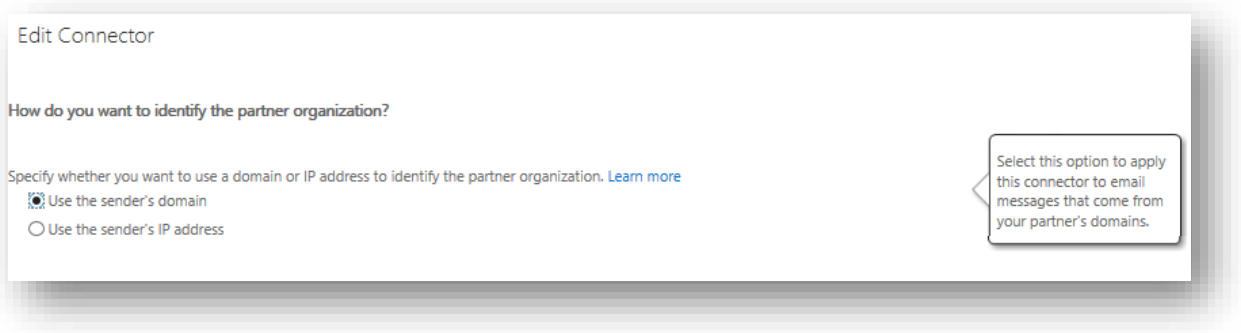


Enter a name and description for the connector.



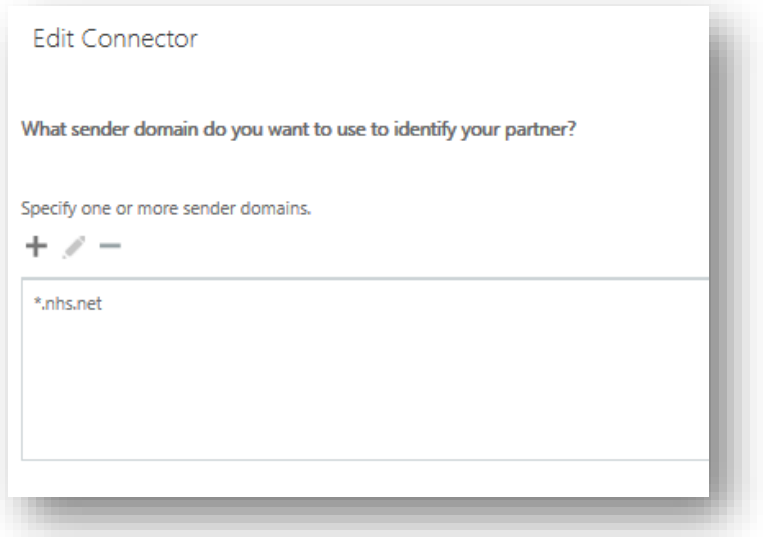
Click Next.

Select ‘Use the sender’s domain’ to identify the partner organisation.

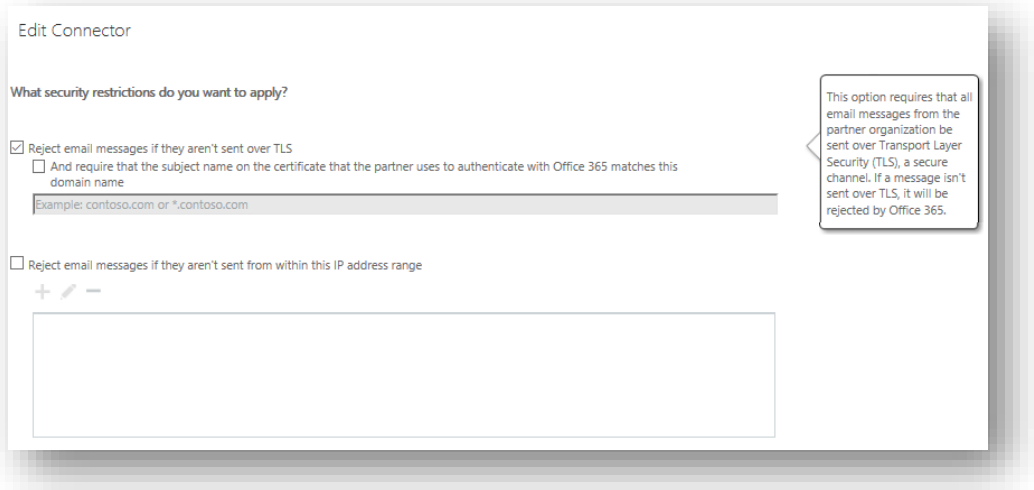


Enter the list of domains you want to apply this connector to. At a minimum, this includes *.nhs.net; see below.

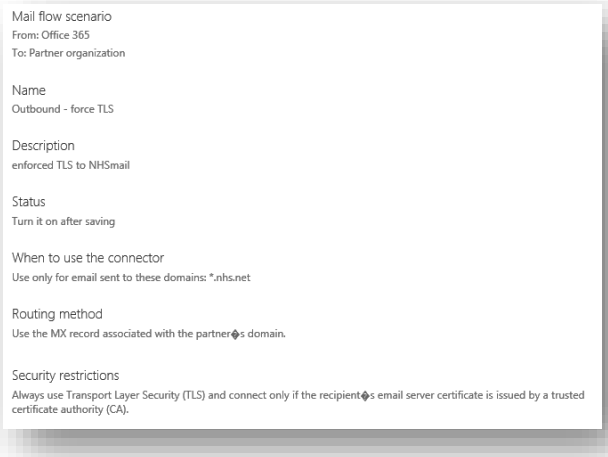
You MUST remove the default entry of ‘*’. Not doing so could result in failure to receive mail from domains that do not use encryption, (TLS).



Configure the connector to always use TLS, rejecting messages if the connection is not encrypted and only if the email server certificate is ‘Issued by a trusted certificate authority (CA)’.



After clicking ‘save’, you will be presented with a summary of the settings. If you need to change any click back, otherwise click ‘save’.



Anti-spoofing – DMARC

DMARC is read by external organisations to determine what to do with email that is spoofing your email address. Therefore it only applies to email received by external organisations. (Except for Office 365 – see the section title Office 365 inbound DMARC). As part of the secure email standard you are required to have a reject record in place.

Enter a DNS TXT record for your domain to set the DMARC policy. The policy is specified by the 'p' tag in the string. The options are;

- P=none – do nothing with the incoming spoofed email (recommended initially)
- P=quarantine – the incoming spoofed email is quarantined (delivered to the junk mail folder)
- P=reject – the incoming spoofed email is rejected by the receiver. No notification is sent to the sender but will be included in the daily aggregate report. It is recommended that you, initially, set p=none then move to p=quarantine to address any spoofing before moving to p=reject.

An example of a DMARC DNS record would be…

```
_dmarc.<trust>.nhs.uk 3600 IN TXT "v=DMARC1; p=none; pct=100; rua=mailto:
dmarc-rua@dmarc.service.gov.uk; ruf=mailto:report.forensic @ trust.nhs.uk;
fo=1"
```

This sets the policy to none, checks 100% of the inbound email (pct=100) and sends aggregate data reports to a mail box dmarc-rua@dmarc.service.gov.uk (the NCSC Mail Check tool) and forensic reports ruf to report.forensic@trust.nhs.uk if any of the authentication mechanisms failed to produce a pass result; fo=1. The fo tag (forensic) is only valid if the ruf tag is specified.

More information can be found at https://dmarc.org/overview/ and https://dmarc.org/wiki/FAQ

Reports can be analysed in the National Cyber Security Centre (NCSC) Mail Check tool.

For further information on the NCSC Mail Check tool click here.

Anti-spoofing – SPF

Sender Policy Framework (SPF) lets you publish a DNS record of all the domains or IP addresses you use to send email. Receiving email services check the record and know to treat email from anywhere else as spam.

It is recommended that you configure an SPF record for your email domain, further information on how to do this can be found at https://support.nhs.net/knowledge-base/spf-dkim-dmarc-configuration/ and at https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf

Office 365 Inbound

If you set up DMARC records, you can create an Exchange Transport Rule (ETR) that marks messages as spam for spoofed messages of *your* company that fail DMARC. This means that all spoofed email of your domain into Office 365 will be marked as spam, but anywhere else – at Gmail, Yahoo, AOL – will not be marked as spam (at least not due to DMARC). Some legitimate email may be marked as spam, but to get around this either ensure that the email is;

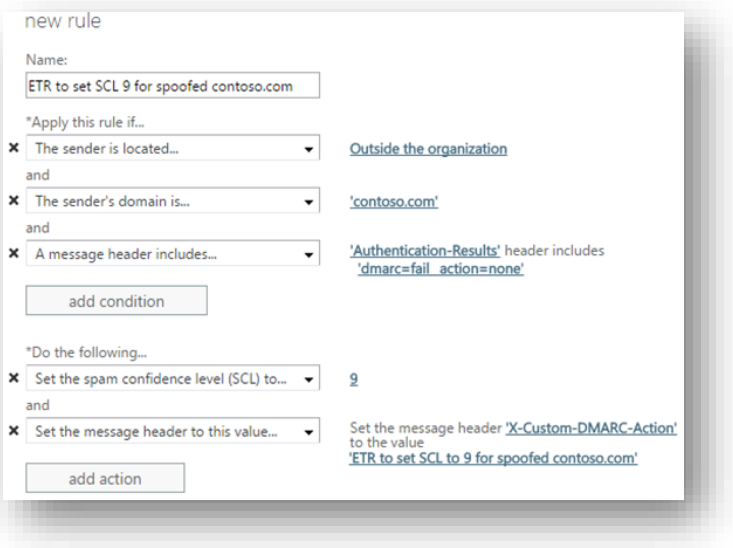
- authenticated by updating SPF records
- or signing it with DKIM
- or, add a safe sender

- or ETR allow rule for the sender

The ETR will look something like the following. You may want to add exceptions to the rule for known senders who spoof your domain but are not malicious.

The advantage of this is that your domain cannot be spoofed by outside senders for inbound messages to your organization which is common in spear phishing, yet marketing messages that go over the Internet are not affected.

You should still properly authenticate your email because it reduces false positives and it shrinks the list of exceptions. If you publish p=reject you will no longer need this rule.

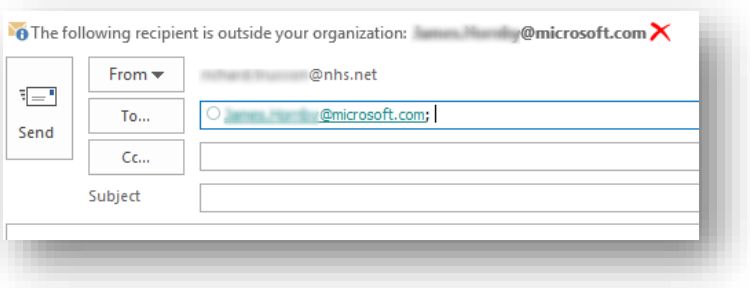


Notification Rules

Office 365 can apply rules to an email based on a number of properties such as; recipient name, recipient domain, content (NHS Number presence for example) and many other conditions. A variety of actions can be taken from presenting a tool tip to the user to blocking the email out right and sending an alert to an individual mailbox or group.

It is recommended organisations create a rule to alert users when they are sending emails outside of the organisation to insecure mail domains. Exceptions can be added for those domains listed as being secure.

An example of the external notification rule is below.



Testing

Throughout this configuration if any of the sections fail to load or fail it is likely that there is a problem. Carefully review the steps taken to ensure they match the documentation. If the configuration still fails contact your local support provider.

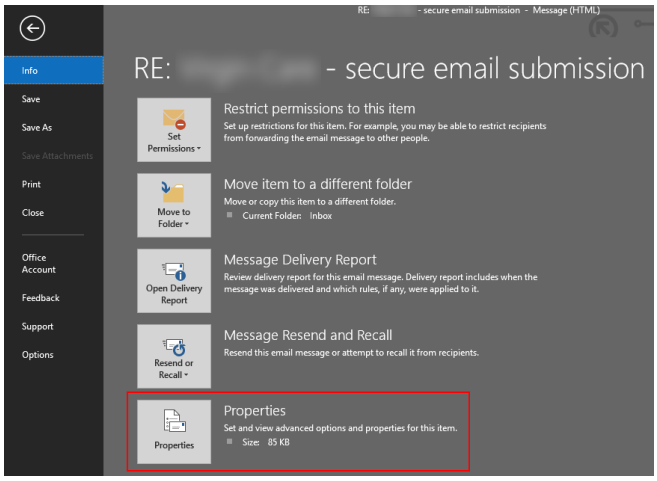
Once the settings are in place, email a test to feedback@nhs.net. State this is a test email and require notification of receipt. NHS Digital will respond to confirm receipt. If no confirmation email is received within 3 working days, then it is likely that the set up failed.

Additional TLS Verification

You can complete an additional manual verification step by having a colleague send a test email to your O365 account.

Once you receive the email, in Outlook 2016;

- Open the message in its own window
- Click File and the Properties in the main window, the red box below.



- In the ‘Internet Headers’ box at the bottom of the properties dialogue search for the phrase TLS or Cipher. You may find it easier to copy the text and paste it into a word processor. If there is text similar to;

  ```
  SMTP Server (version=TLS1_2,
  cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256)
  ```

  Then TLS has been used to encrypt the email and the configuration is working. The above example shows that TLS version 1.2 was used with an AES 256 cipher. This is an example; the TLS and cipher entries in your headers may be different.

You should use the NCSC Mail Check tool to check your configuration which will be used by other organisations to verify your configuration.

For domains not listed on the NCSC Mail Check service tools such as https://www.checktls.com and www.hardenize.com will also check if TLS is in use.