**Introduction**

* **Fix Connector authentication  
  (1) IP  
  (2) Certificate + Domain  
  (3) TLS + certificate**
* Fix/update **commercial certificate**- trusted root authority – **required for external mailflow**
* Fix self-**signed certificate   
  -** root authority stored locally
* Make sure the certificate is uploaded to Azure  
  [*https://docs.microsoft.com/en-us/exchange/configure-oauth-authentication-between-exchange-and-exchange-online-organizations-exchange-2013-help*](https://docs.microsoft.com/en-us/exchange/configure-oauth-authentication-between-exchange-and-exchange-online-organizations-exchange-2013-help)
* *Fix (intermediate local certificate chain (onprem)*

[*https://support.microsoft.com/de-de/help/954755/how-to-configure-intermediate-certificates-on-a-computer-that-is-runni*](https://support.microsoft.com/de-de/help/954755/how-to-configure-intermediate-certificates-on-a-computer-that-is-runni)

**Connector configuration scenarios**

* **Change Connector Certificate**

Get-ExchangeCertificate | Format-List FriendlyName,Subject,CertificateDomains,**Thumbprint**,Services  
  
$**TLSCert**=Get-**ExchangeCertificate** ##########**CODE**###########  
  
$**TLSCertName**="<I>$($**TLSCert**.Issuer)<S>$($**TLSCert**.Subject)"  
  
Get-ReceiveConnector "**SERVER1\Default Frontend SERVER1**" |  
Set-**ReceiveConnector** -TlsCertificateName **$tlscertname**  
<https://docs.microsoft.com/en-gb/archive/blogs/exchangechallengeaccepted/mail-not-routing-to-on-premise-exchange-2013-environment-from-o365-with-450-4-7-320-certificate-validation-failed-error>

**Change Connector Authentication Type**

* **(1) TLS** (inbound cloud)

$**TLSCert**=Get-**ExchangeCertificate** ##########**CODE**###########  
  
$**TLSCertName**="<I>$($**TLSCert**.Issuer)<S>$($**TLSCert**.Subject)"  
  
Set-InboundConnector –RequireTLS $true -TlsSenderCertificateName **$tlscertname**

* (2) restrict to **IP** (inbound cloud)

$IPs = “123.123.123.123”, “123.123.123.123”, “123.123.123.123”  
Get-InboundConnector|  
Set-**Inbound**Connector -RestrictDomainsToIPAddresses -SenderIPAddresses $IPs

* (3) restrict **domains to certificate** (inbound cloud)

$domains = “domain1”, “domain2”, “domain3”

Get-InboundConnector|  
Set-InboundConnector –RestrictDomainsToCertificate $true -SenderDomains $domains

* **TLS** (outbound cloud/to fix receive onprem receive issue)

Get-OutboundConnector |  
Set-OutboundConnector -TlsSettings EncryptionOnly -TlsDomain $null

[*https://docs.microsoft.com/en-us/exchange/configure-oauth-authentication-between-exchange-and-exchange-online-organizations-exchange-2013-help*](https://docs.microsoft.com/en-us/exchange/configure-oauth-authentication-between-exchange-and-exchange-online-organizations-exchange-2013-help)

* *Fix (intermediate local certificate chain (onprem)*

[*https://support.microsoft.com/de-de/help/954755/how-to-configure-intermediate-certificates-on-a-computer-that-is-runni*](https://support.microsoft.com/de-de/help/954755/how-to-configure-intermediate-certificates-on-a-computer-that-is-runni)

* Fix/update **commercial certificate**

Get-ExchangeCertificate | Format-List FriendlyName,Subject,CertificateDomains,Thumbprint,Services

enable-ExchangeCertificate -Thumbprint YourThumbprintCODE -Services POP,IMAP,IIS,SMTP

* Set the certificate to be used for server authentication by running the following commands:

Set-AuthConfig -NewCertificateThumbprint YourThumbprintCODE -NewCertificateEffectiveDate (Get-Date)

Set-AuthConfig –PublishCertificate  
Set-AuthConfig -ClearPreviousCertificate

* Restart the Microsoft Exchange Service Host Service.
* Either run the IISReset command to restart IIS or run the following commands (in elevated mode) to recycle OWA and ECP Application pools:

Restart-WebAppPool MSExchangeOWAAppPool  
Restart-WebAppPool MSExchangeECPAppPool

* Fix self-**signed certificate**

**1. Create a new OAuth certificate by running the following command:**

New-ExchangeCertificate -KeySize 2048 -PrivateKeyExportable $true -SubjectName "cn=Microsoft Exchange Server Auth Certificate" -FriendlyName "Microsoft Exchange Server Auth Certificate" -DomainName "contoso.com"

Note Change the value of the DomainName parameter in the example (contoso.com) to the SMTP domain that's used in your organization.

**2. Set the created certificate to be used for server authentication by running the following commands:**

Set-AuthConfig -NewCertificateThumbprint <ThumbprintFromStep1> -NewCertificateEffectiveDate (Get-Date)

Set-AuthConfig –PublishCertificate  
Set-AuthConfig -ClearPreviousCertificate

**3. Restart the Microsoft Exchange Service Host Service.**

**4. Either run the IISReset command to restart IIS or run the following commands (in elevated mode) to recycle OWA and ECP Application pools:**Restart-WebAppPool MSExchangeOWAAppPool  
Restart-WebAppPool MSExchangeECPAppPool  
  
**5.Export new certificate and uploaded it to Azure Auth.**https://docs.microsoft.com/en-us/exchange/configure-oauth-authentication-between-exchange-and-exchange-online-organizations-exchange-2013-help