

- update certificate to commercial (selfsigned only works if accepted for outlook manually before)
<https://github.com/jahube/PShell/blob/master/Oauth/update-certificate.PS1>
- letsencrypt is for free 3 month just add domains (mail servers autodiscover + domain / web / wildcard)
<https://github.com/jahube/PShell/blob/master/Oauth/letsencrypt.ps1>
- run HCW in **classic** to upload authconfig certificate to Azure **aka.ms/Hybridwizard**
Alternative: <https://docs.microsoft.com/en-us/exchange/configure-oauth-authentication-between-exchange-and-exchange-online-organizations-exchange-2013-help>
modern does not support Oauth
<https://docs.microsoft.com/en-us/exchange/hybrid-deployment/hybrid-agent#constraints>
- logs <https://github.com/jahube/PShell/blob/master/Oauth/Oauth-logs.ps1>
- Teams then uses EvoST authserver to forward authentication to cloud
- most important is
onprem get-authconfig | current thumbprint
assign S =SMTP (better also W=IIS) to used certificate
test-oauthconnectivity cloud > cloud mailbox vs onprem endpoint
- if 401 <https://github.com/jahube/PShell/blob/master/Oauth/update-certificate.PS1>
= scenario 17 > update certificate
https://techcommunity.microsoft.com/legacyfs/online/media/2019/01/FB_Errors.FixesV6.pdf
- **after that EXRCA**
Outlook <https://testconnectivity.microsoft.com/tests/Ola/input>
EWS <https://testconnectivity.microsoft.com/tests/EwsAccess/input>
expand > save as html
Teams only supports A Record or SRV for Autodiscover NOT CNAME
- Common issue: Test-oauth works but autodiscover EXRCA fails on redirect to webserver
check certificate <https://www.digicert.com/help/>
- if necessary update certificate in
IIS<https://github.com/jahube/Screenshots/blob/master/onprem/IIS-Bindings.png>
- **Windows Auth by default is disabled in IIS**
if negotiate is not offered make sure to enable
<https://github.com/jahube/Screenshots/blob/master/onprem/negotiate-A.png>
<https://github.com/jahube/Screenshots/blob/master/onprem/negotiate-B.png>
- **Script to test offered authentication on IIS**
<https://techcommunity.microsoft.com/t5/exchange-team-blog/troubleshooting-hybrid-migration-endpoints-in-classic-and-modern/ba-p/953006>
\$req = [System.Net.HttpWebRequest]::Create("https://mail.contoso.com/ews/MRSPoxy.svc")
\$req.UseDefaultCredentials = \$false
\$req.GetResponse()
Expected error: Exception calling "GetResponse" with "0" argument(s):
"The remote server returned an error: (401) Unauthorized."
\$ex = \$error[0].Exception
\$resp = \$ex.InnerException.Response
\$resp.Headers["WWW-Authenticate"]
- Rare issue: missing **linkedaccount in partnerapplication**
<https://github.com/jahube/PShell/tree/master/PartnerApplication>