INDEX	F/B ERROR	F/B direction	Causes	Troubleshooting suggestions or possible resolutions
1	Proxy web request failed. , inner exception: **An internal server error occurred. The operation failed**. LID: 59916 If you also Test-OauthConnectivity for EWS On-Premises endpoint (for autoD endpoint might be successful), you will see the following 500 Internal Server Error: `Test-OAuthConnectivity -Service EWS -TargetUri https://<On-Premises EWS URL>/ews/Exchange.asmx -Mailbox <Cloud Mailbox>` System.Net.WebException: The remote server returned an error: **(500) Internal Server Error.**	Cloud to On-Premises (Exchange 2016 CU8)	A known Exchange OAUTH issue	This was seen in Exchange 2016 CU8 (considered old now) and fixed in CU9. Please note that in a hybrid deployment, you should always install latest CU or the immediately previous CU. More info about this particular issue here. If you are running another Exchange Server Version (CU/ RU), please check if your Exchange Services are up and running (including EWS and AutoD Application Pools). You would make sure that you can browse the EWS and Autodiscover URLs and that you see the requests coming in IIS logs with 500 HTTP Status. If none of the situations above, please open a case with us for investigation.
2	**The remote user mailbox must specify the the explicit local mailbox in the header** *Note:* The double "the" in the error is not my typo	Cloud to On-Premises (Exchange 2013 CU12-CU14)	A known Exchange OAUTH issue	This particular error was seen in Exchange 2013 CU12-CU14 versions and this issue was fixed in Exchange 2013 CU15 (now considered old). References about this particular error here and here. Please note that in a hybrid deployment, you should always install latest CU or the immediately previous CU.
3	**An error occurred when verifying security for the message** "Autodiscover failed for email address joe@contoso.com with error System.Web.Services.Protocols.SoapHeaderException: An error occurred when verifying security for the message at System.Web.Services.Protocols. SoapHttpClientProtocol.ReadResponse(SoapClientMessage message, WebResponse response, Stream responseStream, Boolean asyncCall)at	Cloud to On-Premises, especially Exchange 2010 servers	WSSecurity Authentication issues	1) Refresh MFG metadata (reference) Run this command **twice** in Exchange Management Shell On-Premises: `Get-FederationTrust | Set-FederationTrust -RefreshMetadata` 2) *WSSecurity* authentication should be enabled on both Autodiscover and EWS virtual directories (*Get-AutodiscoverVirtualDirectory* and *Get-WebServicesVirtualDirectory*); if already enabled, try to toggle WSSecurity Authentication ON/OFF on the Autodiscover and EWS virtual directories on all Exchange On-Premises Servers. Follow this procedure to toggle WSSecurity on these virtual directories.

	System.Web.Services.Protocols.SoapHttpClientProtocol.EndInvoke(IAsyncResult asyncResult)"			WSSecurity is only used for cross-premises Free/Busy, so there should be no effect on other clients connecting to servers. If issue is still not resolved: 3) `IISreset /noforce` on all Exchange 2010 CAS or on all Exchange 2013/2016 Servers 4) Reboot all CAS Exchange 2010 or all Exchange 2013/2016 Servers If issue still not resolved: 5) Check Windows Time events (warnings or errors) in System logs for Time Skew issues 6) Set *TargetSharingEpr* (On-Premises External EWS URL) on Cloud Organization Relationship and check the free/busy issue (and error) after. By default, *TargetSharingEpr* is blank because we rely on Autodiscover (*TargetAutodiscoverEpr* in OrganizationRelationship or *DiscoveryEndpoint* in IntraOrganizationConnector) in order to retrieve EWS URL of the target user where we would make a second request to get the Free/Busy information. As a temporary troubleshooting step, we are bypassing Autodiscover process and we connect directly to EWS endpoint to rule out any Autodiscover issues. **EXO PowerShell** `Set-OrganizationRelationship "O365 to On-premises*" -TargetSharingEpr <On-Premises EWS External URL>` Also, make sure there is no mismatch between TargetApplicationUri in Organization Relationship and AccountNamespace configured for the Federation Organization Identifier. Check Test-OrganizationRelationship results and Baseline Configuration section of the first blog post.
4	**Unable to connect to the remote server** Proxy web request failed. , inner exception: System.Net.WebException: Unable to connect to the remote server ; System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection	Cloud to On-Premises	Network /Connectivity issues (EXO IP addresses blocked)	1) Verify that your firewall allows all O365 IPs to connect to your Exchange on-premises endpoints for Inbound direction. References here and here. You would check Firewall / Network logs when making Free/Busy requests from O365.

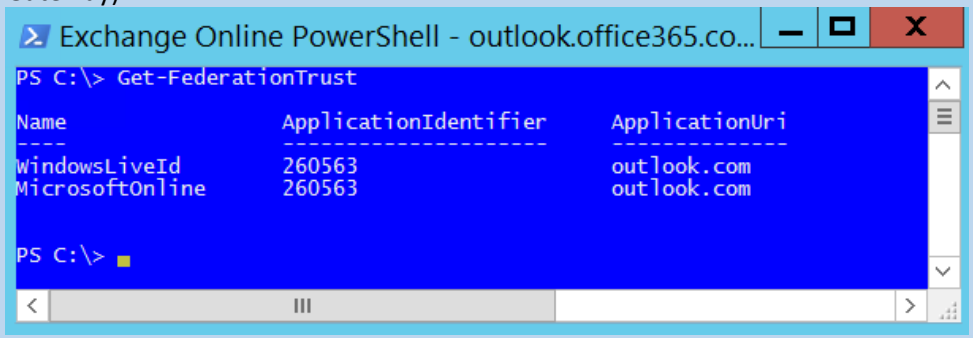
	failed because connected host has failed to respond CUSTOMER_IP:443 at System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult)			2) Also, you would verify *IIS logs* (W3SVC1 for Default Website) on Client Access Servers in the timeframe when you repro this F/B issue to see if the requests coming from Office 365 reach IIS servers / Exchange CAS on-premises. If you don't see these requests, this suggests that the Office 365 connection didn't reach your Exchange Servers (IIS). If you have Exchange 2013 or above server version, you would also look at *HttpProxy* logs for Autodiscover / EWS protocols. 3) In case you have set restrictions on inbound connections coming from the Internet to your on-premises endpoints, allowing only Office 365 IP addresses to connect to your EWS endpoint, you can do *Test-MigrationServerAvailability* command to test connectivity from Office 365 to the on-premises EWS endpoint. Keep in mind that your Exchange Online users are hosted on different Mailbox Servers and the Office 365 Outbound IP is thus different. You might have this Free/Busy error for some users or 1 user, depending on the O365 IP connecting to your on-premises endpoints. You would test this from when connected to Exchange Online PowerShell session: `Test-MigrationServerAvailability -RemoteServer mail.contoso.com -ExchangeRemoteMove -Credentials (get-credential)` #input Domain Admin credentials in the format domain\admin Reference Test-MigrationServerAvailability
5	**Autodiscover failed for email address user@contoso.fr with error System.Net.WebException: The request failed with HTTP status 404: Not Found.** Autodiscover failed for email address user@contoso.*fr* with error System.Net.WebException: The request failed with HTTP status 404: Not Found.
Cloud to On-Premises	AutoD Endpoints not configured ok or not functional	1) Browse Autodiscover endpoint specified on IntraOrganization Connector / Organization Relationship and see if you get “404 not Found” error. 2) Check the SMTP domain in the Target Address for the User if it exists in Target Domains in IntraOrganization Connector / Organization Relationship (example: Free/Busy cloudUser@contoso.com > onPremUser@contoso.fr, check if **contoso.fr** domain is there) 3) There might be cases where SVC handler mapping is missing from IIS manager. Make sure svc-integrated handler mapping is present both at the **/autodiscover** virtual directory level and **/EWS** virtual directory. References: here and here **Note**: You may see the AutodiscoverDiscoveryHander (*.svc) mapping. This is NOT the mapping we used for federation Free/Busy lookup.

6	Exception Proxy web request failed. , inner exception: **The request failed with HTTP status 401: Unauthorized** diagnostics: 2000005;reason= **"The user specified by the user-context in the token is ambiguous."** ;error_category="invalid_user" LID: 43532	Cloud to On-Premises, OAUTH used	Duplicate users	1) Use LDP.exe or Active Directory Users and Computers snap-in with a custom LDAP query to find the object with the duplicate UPN / SMTP /SIP address. For example, this would be the LDAP filter for user with UPN: user@corp.contoso.com, SMTP: user@contoso.com, SIP: user@contoso.com `(|(userPrincipalName=user@corp.contoso.com)(proxyAddresses=SMTP:user@contoso.com)(proxyAddresses=sip:user@contoso.com))` For more information of using LDP.exe or Active Directory Users and Computers to find AD objects, see this. Once you find the on-premises user with the duplicate address, either change the address for that on premises user or delete the duplicate.
7	**An existing connection was forcibly closed by the remote host** "Proxy web request failed. , inner exception: System.Net.WebException: The underlying connection was closed: An unexpected error occurred on a **receive** . System.IO.IOException: Unable to read data from the transport connection: An existing connection was forcibly closed by the remote host. System.Net.Sockets.SocketException: An existing connection was forcibly closed by the remote host"	Cloud to On-Premises	Usually firewall blocking Office 365 outbound IP	1) Check if the request coming from Office 365 Exchange Online reaches IIS / Exchange Server, look for at least one of these 2 entries in IIS logs when you reproduce the issue: a. Autodiscover request: **"ASAutoDiscover/CrossForest/EmailDomain"** b. EWS Request: **"ASProxy/CrossForest/EmailDomain"** Note: If you had manually set the TargetSharingEpr (EWS URL) on the Cloud Organization Relationship / Cloud IntraOrganization Connector, then you would see only the EWS request in IIS logs because TargetSharingEpr (EWS Request) bypasses TargetAutodiscoverEpr / DiscoveryEndpoint (Autodiscover Request). 2) Check if the firewall is blocking connection from Office 365 IP. References here and here. 3) Check if the Federation Certificate is in place on the Exchange Servers (*installed*) or if you get an error /warning when retrieving Federated Organization Identifier: **Exchange Management Shell:** `Test-FederationTrustCertificate` `Get-FederatedOrganizationIdentifier -IncludeExtendedDomainInfo |FL`

				4) Toggle *WSSecurity* on Autodiscover and EWS virtual directories and recycle Autodiscover and EWS App Pools in IIS and if not solved with recycling, perform also *iisreset /noforce*. Reference. 5) If you see this error for 1 or 2 users, there might the situation where those users are hosted on Exchange Online Mailbox Server that has an Outbound IP that you don't allow to connect to your on-premises. If not this cause, then check the 1:1 personal sharing settings on them. If there is 1:1 personal sharing, we will use that and not the organization relationship. Possibly there is a problem or bad entry on the personal sharing. You would see this with MFCMAPI (Sharing) but really you should reach Microsoft Support if you got this far with troubleshooting.
8	**An existing connection was forcibly closed by the remote host (2)** "Exception: Autodiscover failed for email address user@Notes.Domain.com with error Microsoft.Exchange.InfoWorker.Common.Availability.AutoDiscoverFailedException: The underlying connection was closed: An unexpected error occurred on a **send..** The request information is Discovery URL : https://notes.server.com/AutoDiscover/AutoDiscover.xml, EmailAddress : SMTP:user@notes.domain.com System.Net.WebException: The underlying connection was closed: An unexpected error occurred on a **send.** ; System.IO.IOException: Unable to read data from the transport connection: An existing connection was forcibly closed by the remote host System.Net.Sockets.SocketException: An existing connection was forcibly closed by the remote host"	Cloud to On-Premises Lotus Notes Server	Usually firewall blocking Office 365 outbound IP	If the on-premises server is Lotus Domino and not Exchange, you would check Availability Address Space from Cloud to On-Premises In EXO PowerShell run: `Get-AvailabilityAddressSpace |FL` Check if the firewall is blocking connection from Office 365 IP. Reference here.
9	**Configuration information for forest/domain could not be found in Active Directory**	Cloud to On-Premises	Probably a misconfiguration	1) Check if the Target Domain for the user we want to lookup free/busy for is found in the Source Organization Relationship or Source IntraOrganization Connector (IOC). For example, suppose CloudUser@contoso.com will lookup Free/Busy for On-Premises user On-PremUser@**contoso.ro.** You would check in EXO PowerShell if the domain **contoso.ro** is present in IOC /Org Relationship:

				`Get-IntraOrganizationConnector | fl TargetAddressDomains` **TargetAddressDomains** - This should be your federated domains. Example: contoso.com. You can find the domains name by cross-check Exchange Online's (Get-IntraOrganizationConfiguration).OnPremiseTargetAddresses `Get-OrganizationRelationship "Exchange Online to on premises Organization Relationship" | fl DomainNames` **DomainNames** - This should be your federated domains. Example: contoso.com. You can find the domains name by cross-check On-Prem's `(Get-FederatedOrganizationIdentifier).Domains` In the example given, we would need that **contoso.ro** to be present in TargetAddressDomains (IOC) or in DomainNames (Organization Relationship). If this were to be missing, you would need to add your domain, in this example would be "contoso.ro". `Set-IntraOrganizationConnector "HybridIOC*" -TargetAddressDomains @{add="contoso.RO"}` 2) It might also be the scenario where Minimal HCW was configured instead of Full HCW and in Minimal HCW there is no Organization Relationship / Federation Trust or IntraOrganization Connectors. Reference.
10	**Proxy web request failed.,inner exception: The request failed with HTTP status 401: Unauthorized.** Proxy web request failed. , inner exception: System.Net.WebException: The request failed with HTTP status 401: Unauthorized. at System.Web.Services.Protocols.SoapHttpClientProtocol.ReadResponse(SoapClientMessage message, WebResponse response, Stream responseStream, Boolean asyncCall) at System.Web.Services.Protocols.SoapHttpClientProtocol.EndInvoke(IAsyncResult asyncResult) at Microsoft.Exchange.InfoWorker.Common.Availability.Proxy.Service.EndGetUserAvailability(IAsy	Cloud to On-Premises	Usually pre-authentication issues	As mentioned before, "proxy web request failed" suggests EWS request failed but you might see this error also for Autodiscover request (and in this case the error message would be "Autodiscover failed for email address"), so I will refer to both failed Autodiscover and EWS with 401 Unauthorized. "401 Unauthorized" error is perhaps one of the most common free/busy errors in Cloud to On-Premises Free/Busy direction and these are the main troubleshooting suggestions: 1) Pre-authentication is not supported in Hybrid deployments for both Autodiscover and EWS virtual directories. Pre-authentication means that something which is sitting in front of Exchange Server is asking for authentication (username and password). The request from Office 365 should pass thru to Exchange server directly.

	ncResult asyncResult) at Microsoft.Exchange.InfoWorker.Common.Availability.FreeBusyApplication.EndProxyWebRequest(ProxyWebRequest proxyWebRequest, QueryList queryList, IService service, IAsyncResult asyncResult) at Microsoft.Exchange.InfoWorker.Common.Availability.ProxyWebRequest.EndInvoke(IAsyncResult asyncResult) at Microsoft.Exchange.InfoWorker.Common.Availability.AsyncWebRequest.EndInvokeWithErrorHandling</td>			You can use Remote Connectivity Analyzer, Free/Busy test in Office 365 tab and run it from Cloud to On-premises. This will tell you if pre-authentication is disabled (pass-thru authentication step will be green against the endpoint). There might be cases where even this is green, you might still have pre-authentication issues or network devices interfering. You would confirm this by looking in the IIS logs. If you see the 401 error (instead of expected 200) in the IIS logs for the Autodiscover / EWS Request, this means that the Free/Busy request failing with 401 Unauthorized reached IIS/Exchange and this is likely not a Reverse Proxy / Firewall issue. IIS entry for Autodiscover request: **401 "ASAutoDiscover/CrossForest/EmailDomain"** IIS entry for EWS Request: **401 "ASProxy/CrossForest/EmailDomain"** If you don't see these requests in IIS logs around the time you queried Free/Busy Request, then you would check Reverse Proxy /Firewall logs to understand where the request is stuck. Keep in mind that IIS logs are UTC time. 2) If not a pre-authentication issue, you need to make sure that you have WSSecurity (Exchange 2010) / OAuth (Exchange 2013+) authentication methods enabled on EWS and Autodiscover virtual directories and that you have default authentication methods in IIS on EWS and Autodiscover virtual directories (Reference Ex2013/2016, Ex2010). 3) If authentications are ok in Exchange and IIS for EWS and Autodiscover, then try Suggestions from Error "*An error occurred when verifying security for the message*", especially the WSSecurity toggle part. If using Oauth (and not WSSecurity), toggle Oauth on Autodiscover and EWS virtual directories: `Set-WebServicesVirtualDirectory "<ServerName>\ews (Exchange Back End)" -OAuthAuthentication:$False`

				Set-WebServicesVirtualDirectory "<ServerName>\ews (Exchange Back End)" -OAuthAuthentication:$True Set-AutodiscoverVirtualDirectory "<ServerName>\Autodiscover (Exchange Back End)" -OAuthAuthentication:$False Set-AutodiscoverVirtualDirectory "<ServerName>\Autodiscover (Exchange Back End)" -OAuthAuthentication:$True 4) Check Get-FederationTrust output from your EXO tenant. If you run Get-FederationTrust cmdlet in Exchange Online PowerShell) you would see two trusts: “WindowsLiveId” (Consumer Instance of Microsoft Federation Gateway) and “MicrosoftOnline” (Business Instance of Microsoft Federation Gateway).  Make sure the Application Identifier is “**260563**” and the Application Uri is “**outlook.com**” for both; in case you have a different App ID (292841) and a different App URI (outlook.live.com) for a Cloud trust, this means your tenant has an old reference pointing to MFG and most probably Free/Busy from on-premises to cloud would fail with a quite generic **401 Unauthorized** error or with “failed due to an error in user setting 'ExternalEwsUrl' Error message: InvalidUser.” (**error #11**). If you were to find yourself in a such situation (outdated federation trust in Office 365), please open a support case with Microsoft to get it resolved.
11	**The response from the Autodiscover service at 'https://autodiscover/autodiscover.svc/WSSecurity' failed due to an error in user setting 'ExternalEwsUrl'. Error message: InvalidUser.**	Cloud to On-Premises	Probably Misconfiguration	You might see this error also in Remote Connectivity Analyzer - Free/Busy test. 1) Check if the cloud user has a secondary smtp address **user@contoso.mail.onmicrosoft.com** present in EmailAddresses.

	Autodiscover failed for email address user@contoso.com with error Microsoft.Exchange.InfoWorker.Common.Availability.AutoDiscoverInvalidUserException: The response from the Autodiscover service at 'https://autodiscover/autodiscover.svc/WSSecurity' failed due to an error in user setting 'ExternalEwsUrl'. Error message: InvalidUser.. Name of the server where exception originated: DB3PR02MB0345 . LID: 33676.			To fix this issue, you need to add user@contoso.mail.onmicrosoft.com in email addresses of the cloud user. If the cloud user is synced from on-premises, you would add the email address in the on-premises AD and force directory sync. 2) You can also set TargetSharingEpr on the Organization Relationship and check again the issue /error. **EXO PowerShell:** `Set-OrganizationRelationship "O365 to On-premises*" -TargetSharingEpr <On-Premises EWS External URL>`
12	**Microsoft.Exchange.InfoWorker.Common.Availability.NoFreeBusyAccessException: The caller does not have access to free/busy data**	Cloud to On-Premises	Misconfiguration	1) Check calendar folder permissions using **Get-MailboxFolderPermission user:\calendar** and see if **Default** user has **None** permissions. Default user should have "AvailabilityOnly" or "LimitedDetails". 2) When the request is done from Cloud, the Cloud User's FROM address would be in the format user@tenant.mail.onmicrosoft.com and if the on-premises organization doesn't locate an organization relationship for the FROM domain **tenant.mail.onmicrosoft.**com in the on-premises Exchange, it will reject the request with this same error. Therefore, make sure the on-premises organization relationship contains tenant.mail.onmicrosoft.com domain.
13	**Proxy web request failed. , inner exception: The request failed with HTTP status 403: Forbidden (The server denied the specified Uniform Resource Locator (URL). Contact the server administrator.). LID: 43532**	Cloud to On-Premises	Pre-authentication issues from TMG/ISA	Pre-authentication is not supported in Hybrid deployments for both Autodiscover and EWS virtual directories. Pre-authentication means that something which is sitting in front of Exchange Server is asking for authentication (username and password). The request from Office 365 should pass thru to Exchange server directly, which instead is responsible to do the authentication (ask for username and password and authenticate the user). You can use Remote Connectivity Analyzer, Free/Busy test on the Office 365 tab and run it from Cloud User to On-premises User. This will tell you if pre-authentication is disabled (pass-thru authentication step will be green). This error is specific to TMG/ISA pre-authentication.

14	**Unable to resolve e-mail address user@notes.domain.com to an Active Directory object** Recipient: user@notes.domain.com Exception: Unable to resolve e-mail address user@notes.domain.com to an Active Directory object. LID: 57660 Server Name: DBXPR05MB0655 Exception Type: MailRecipientNotFoundException Response Code: ErrorMailRecipientNotFound	Cloud to On-Premises Lotus Notes (no Exchange)	Probably Misconfiguration	Create a mail enabled user or a mail contact in Exchange Online for target users - Lotus Notes users (Example: user@notes.domain.com). Notes.domain.com would be the domain from `Get-AvailabilityAddressSpace` in Exchange Online (this is created manually by administrators in Exchange Online).
15	ProxyWebRequestProcessingException ErrorProxyRequestProcessingFailed Proxy web request failed. , inner exception: **An error occurred when processing the security tokens in the message.** LID: 59916	Cloud to On-Premises		1) Check if the on-premises federation trust certificates are OK (expiration and thumbprints) with: `Get-FederationTrust |FL` `Test-FederationTrust` `Test-FederationTrustCertificate` 2) Trigger a refresh of MFG metadata (Reference). Run this command **twice** in EMS On-Premises: `Get-FederationTrust | Set-FederationTrust -RefreshMetadata`
16	**The cross-organization request for mailbox yyy@contoso.com is not allowed because the requester is from a different organization** Recipient: yyy@contoso.com Exception Type: CrossOrganizationProxyNotAllowedForExternalOrganization Exception Message: The cross-organization request for mailbox yyy@contoso.com is not allowed because the requester is from a different organization. LID: 39660	Cloud to Cloud Hybrid	Probably misconfiguration	1) This error is likely to be encountered in a Hybrid Mesh Scenario. You can read more about Hybrid Mesh here, with the difference that for this scenario the Source and Target Organization are both Cloud Exchange Organizations and one of them is Hybrid. In the blog mentioned, both organizations are On-Premises Exchange and one goes hybrid. Consider the following scenario: `xxx@adatum.com` is an Exchange Online user querying free busy of another Exchange Online user from a different tenant `yyy@contoso.com`. The target Organization Contoso.com is a Hybrid Exchange Organization and Autodiscover for contoso.com points to on-premises Exchange.

				In Adatum (Source Organization) we have 2 organization relationships: one for contoso.com (Exchange On-Premises Organization of Contoso) and another one for contoso.mail.onmicrosoft.com (Exchange Online Organization of Contoso). Suppose that in Adatum (Source organization), user `yyy@contoso.com` (Target User from Target Org) is represented as a mail user with target address `yyy@contoso.com` But `yyy@contoso.com` is a cloud user and Autodiscover for contoso.com points to Exchange On-Premises. Being a cloud user in Hybrid Deployment, `yyy@contoso.com` will have also a proxy address `yyy@contoso.mail.onmicrosoft.com` and Autodiscover for contoso.mail.onmicrosoft.com will always point to cloud (correct way). When `xxx@adatum.com` queries free/ busy for `yyy@contoso.com`, the user `xxx@adatum.com` gets the following message: "*The cross-organization request for mailbox* `yyy@contoso.com` *is not allowed because the requester is from a different organization*". To work around this issue, either `xxx@adatum.com` will query free busy for this email address `yyy@contoso.mail.onmicrosoft.com` (where Autodiscover for contoso.mail.onmicrosoft.com points to Exchange Online) , either tenant admin changes Target Address / External Email Address to `yyy@contoso.mail.onmicrosoft.com` on the target user, represented as mail user or mail contact in their source organization. Either way, Adatum organization needs to know which users from Contoso Organization are hosted in cloud and what is their target address where domain's autodiscover points to cloud (example alias@tenant.mail.onmicrosoft.com). 2) You might also encounter this error after you switched Autodiscover for your Hybrid Organization SMTP domains from Exchange On-Premises to Exchange Online and there are still mailboxes hosted in Exchange On-Premises with SMTP @Domain whose Autodiscover points to cloud.
17	**System.Net.WebException: The request failed with HTTP status 401: Unauthorized.**	Cloud to On-	OAuth certificate	1) Check certificate in *AuthConfig* in On-Premises Exchange Management Shell: `(Get-AuthConfig).CurrentCertificateThumbprint`

	And if you do `Test-OAuthConnectivity -Service AutoD -TargetUri <OnPremises Autodiscover.svc endpoint - https://mail.domain.com/autodiscover/autodiscover.svc> -Mailbox <Exchange Online Mailbox> -Verbose | fl` , it will give you this exception: **Microsoft.Exchange.Security.OAuth.OAuthTokenRequestFailedException: Missing signing certificate.**	Premises, Oauth		2) Check thumbprint of OAuth certificate (if one exists) if matching CurrentCertificateThumbprint from AuthConfig: `Get-ExchangeCertificate -Thumbprint (Get-AuthConfig).CurrentCertificateThumbprint | fl` If no OAuth certificate: 1. Create a new OAUTH certificate and update it on Auth Config: `New-ExchangeCertificate -KeySize 2048 -PrivateKeyExportable $true -SubjectName "CN=Microsoft Exchange Server Auth Certificate" -FriendlyName "Microsoft Exchange Server Auth Certificate" -DomainName <Domain> -Services smtp` *** Do not accept to replace the SMTP certificate when prompted 2. Note the thumbprint of the new certificate. Let us assume it is: 1A39741F8DF58D4821567DD8F899B27410F7C096 `$a=get-date` `Set-AuthConfig -NewCertificateThumbprint 1A39741F8DF58D4821567DD8F899B27410F7C096 -NewCertificateEffectiveDate $a` *** Accept to continue despite the fact that the certificate effective date is not 48 hours into the future `Set-AuthConfig -PublishCertificate` 3. Make sure to remove any potential reference to the previous certificate (which might not exist anymore) by doing: `Set-AuthConfig -ClearPreviousCertificate.` If you have a different thumbprint, just follow steps 2-3.
18	System.Web.Services.Protocols.SoapException: **The application is missing a linked account for RBAC roles, or the linked account has no RBAC role assignments, or the calling users account is logon disabled.**	Cloud to On-Premises	Probably Misconfiguration	1) Check if the "Exchange Online Application Account" is missing from on-premises Get-PartnerApplication Linked Account: `(Get-PartnerApplication).LinkedAccount` 2) If user is there, check RBAC assignments in EMS:

```
Get-ManagementRoleAssignment -RoleAssignee "Exchange
Online-ApplicationAccount" | ft Name,Role -AutoSize
```

```
Name                                                Role
----                                                ----
UserApplication-Exchange Online-ApplicationAccount  UserApplication
ArchiveApplication-Exchange Online-ApplicationAccount ArchiveApplication
LegalHoldApplication-Exchange Online-ApplicationAccount LegalHoldApplication
Mailbox Search-Exchange Online-ApplicationAccount   Mailbox Search
TeamMailboxLifecycleApplication-Exchange Online-ApplicationAccou TeamMailboxLifecycleApplication
MailboxSearchApplication-Exchange Online-ApplicationAccount MailboxSearchApplication
MeetingGraphApplication-Exchange Online-ApplicationAccount MeetingGraphApplication
```

Pasting here only the Role Column as each name will comprise the role name:

```
Role
----
UserApplication
ArchiveApplication
LegalHoldApplication
Mailbox Search
TeamMailboxLifecycleApplication
MailboxSearchApplication
MeetingGraphApplication
```

3) If user not present on Partner Application, follow these steps:

1. Look for the user in on-premises AD.
   Example:

```
Set-ADServerSettings -ViewEntireForest $true
Get-User "Exchange Online-ApplicationAccount"
```

2. If user found in AD, set it on Partner Application:

```
Set-PartnerApplication "Exchange Online" -LinkedAccount
"<rootdomainFQDN>/users/Exchange Online-
ApplicationAccount"
```

   After you set the Linked Account, you need to do an *IISreset* or even *reboot* the Exchange 2010 CAS servers or Exchange 2013/2016 Mailbox Servers.

3. If user not found in AD, check if user was deleted and if so try to recover with ADRstore.exe. If you manage to restore the user, do step #2

				4. If not able to recover the user, run prepareAD and see if this brings back the user. If not, create the user in AD manually. Add the RBAC roles mentioned above. Proceed with step #2.
19	Soap fault exception received. **The entered and stored passwords do not match**	Cloud to on-premises	Issue with particular cloud user(s)	This suggests a mismatch of the Azure user credentials (password). Specific cloud user is unable to see Free /Busy of the on-premises users with the error mentioned. Also, if we run `Test-OrganizationRelationship -Identity "O365 to On-premises*" -UserIdentity <Cloud Mailbox>` we would get same error when retrieving Delegation Token. Here are some suggestions that could fix this issue: 1) Reset cloud user password with same password or different password. 2) Flip UPN of the cloud user to onmicrosoft.com and then set it back to initial UPN (reference) If connecting to Azure AD (`Connect-AzureAD`) `Set-AzureADUser -ObjectID user@federateddomain.tld -UserPrincipalName user@tenant.onmicrosoft.com` `Set-AzureADUser -ObjectID user@tenant.onmicrosoft.com -UserPrincipalName user@federateddomain.tld` If connecting to MSOL service (`Connect-MSOLservice`) `Set-MsolUserPrincipalName UserPrincipalName user@federateddomain.tld NewUserPrincipalName user@tenant.onmicrosoft.com` `Set-MsolUserPrincipalName UserPrincipalName user@tenant.onmicrosoft.com NewUserPrincipalName user@federateddomain.tld` 3) Open Exchange Management Shell and check the following: o Ensure the ImmutableID value for the on-premises user object is null. `Get-RemoteMailbox <Cloud Mailbox> |FT userprincipalname, immutableID` o If the ImmutableID is already null, follow these steps:

				a) Set the ImmutableID on the remote mailbox object to the UPN of the user: `Set-RemoteMailbox <User> -ImmutableID <user@contoso.com>` b) Sync the change to the cloud and verify the user object has been updated in cloud. To force the sync, you can use these commands: `Import-Module ADSync` `Start-ADSyncSyncCycle -PolicyType Delta` In Exchange Online PowerShell, check if the immutableID has been updated: `Get-mailbox <Cloud Mailbox> |FT userprincipalname, immutableID` c) Set back the ImmutableID to null: `Set-RemoteMailbox <User> -ImmutableID $null` d) Sync the user object to the cloud and verify the user object has been updated. `Start-ADSyncSyncCycle -PolicyType Delta` In Exchange Online PowerShell, check if the immutableID has been updated: `Get-mailbox <Cloud Mailbox> |FT userprincipalname, immutableID`
20	**The password has to be changed.** OR **The password for the account has expired**	Cloud to on-premises	Issue with few or more cloud user(s)	This again suggests an inconsistency on the Azure User(s). You can also run *`Test-OrganizationRelationship`* in the Cloud side to see if you get the same error when retrieving the federation token (*`Test-FederationTrust`* is not available in Exchange Online) `Test-OrganizationRelationship -Identity "O365 to on-premises*" -UserIdentity <Cloud Mailbox> -Verbose` **Workarounds** Connect to Azure AD PowerShell and run the following commands for the affected users. 5. Usually for the error "**The password for the account has expired**", we fix it like this: If you Connect-MSOLService `Set-MsolUser -UserPrincipalName <UPN of the account> -PasswordNeverExpires $true`

				If you Connect-AzureAD `Set-AzureADUser -ObjectId <UPN of the account> -PasswordPolicies DisablePasswordExpiration` 6. And for the error "**The password has to be changed**", we fix it like this: Connect-MSOLService `Set-MsolUserPassword -UserPrincipalName <UPN> -ForceChangePassword $false` More info here These issues seem to be caused if we don't have Password Sync Enabled for Synced Users (with or without ADFS/ Identity Federation in place) and you can enable password sync to see if this fixes the issue. More details here.
21	**Provision is needed before federated account can be logged in.** ErrorWin32InteropError	Cloud to on-premises	Issue with few or multiple users	This also suggests an inconsistency on the Azure AD side regarding those federated users. You can also run `Test-OrganizationRelationship` in the Cloud side to see if you get the same error when retrieving the federation token (`Test-FederationTrust` is not available in Exchange Online) `Test-OrganizationRelationship -Identity "O365 to on-premises*" -UserIdentity <Cloud Mailbox> -Verbose` Workaround: Flip UPN of the cloud user to onmicrosoft.com and then set it back to initial UPN (federated domain). Reference. If connecting to Azure AD (`Connect-AzureAD`) `Set-AzureADUser -ObjectID user@federateddomain.tld -UserPrincipalName user@tenant.onmicrosoft.com` `Set-AzureADUser -ObjectID user@tenant.onmicrosoft.com -UserPrincipalName user@federateddomain.tld` If connecting to MSOL service (`Connect-MSOLservice`)

				Set-MsolUserPrincipalName UserPrincipalName user@federateddomain.tld NewUserPrincipalName user@tenant.onmicrosoft.com Set-MsolUserPrincipalName UserPrincipalName user@tenant.onmicrosoft.com NewUserPrincipalName user@federateddomain.tld If affecting many /all users, please open a support case with us.
22	**The request timed out** **Request could not be processed in time. Timeout occurred during 'Waiting-For-Request-Completion'.**	On-Premises to Cloud	Usually network issues or temp timeouts	This can be a temporary error, make sure your try several times and you always get this timeout error (consistent repro). 1. Check if you can get the federation token or any other failure when running the following commands in Exchange Management Shell: Test-OrganizationRelationship -Identity "On-premises to O365*" -UserIdentity <On-Premises Mailbox> -Verbose #test-federationtrust should be executed from all Exchange Servers Test-FederationTrust -UserIdentity <On-Premises Mailbox> -Verbose Test-FederationTrustCertificate 2. From on-premises Exchange to Office 365, the 2010 MBX & CAS or 2013 MBX (backend) or 2016 would need outbound Internet access to the Microsoft Federation Gateway or Authorization server (if using OAuth) in additions to https://outlook.office365.com/ews/exchange.asmx (the availability URL in Office 365). References here and here. 3. Verify the Machine /System account can access these URLs below. You will use **PsExec.exe** (with **-s -i**) switches from PSTools/Windows 2000 Resource Kits to launch an Internet browser session to test the URLs. C:\Tools\pstools>PsExec.exe -i -s "c:\Program Files\Internet Explorer\iexplore.exe"

				Microsoft Federation Gateway (without OAuth) • https://nexus.microsoftonline-p.com/federationmetadata/2006-12/federationmetadata.xml [<-- You should see an xml page.] • https://login.microsoftonline.com/extSTS.srf [<-- You should be prompted to download the file.] • https://domains.live.com/service/managedelegation2.asmx [<-- You should see the operations supported by ManageDelegation2.] **Microsoft Authorization Server (with OAuth)** • https://outlook.office365.com/ews/Exchange.asmx [<-- We should be getting a cred prompt.] • https://login.windows.net/common/oauth2/authorize [<-- We should be getting Sorry, but we're having trouble signing you in.] • https://accounts.accesscontrol.windows.net/<tenant guid>/tokens/OAuth/2 [<-- We should be getting HTTP 400.] This is a quite generic error and usually it requires further troubleshooting.
23	**The specified member name is either invalid or empty**. S:Fault xmlns:S="http://www.w3.org/2003/05/soap-envelope"><S:Code><S:Value>S:Sender</S:Value><S:Subcode><S:Value>wst:FailedAuthentication</S:Value></S:Subcode></S:Code><S:Reason><S:Text xml:lang="en-US">**Authentication Failure**</S:Text></S:Reason><S:Detail><psf:error xmlns:psf="http://schemas.microsoft.com/Passport/SoapServices/SOAPFault"><psf:value>0x80048821</psf:value><psf:internalerror><psf:code>0x80041034</psf:code><psf:text>**The specified member name is either invalid or empty**.</psf:text></psf:internalerror></psf:error></S:Detail></S:Fault> Microsoft.Exchange.Net.WSTrust.SoapFaultExce	Cloud to on-premises	Issue with few or multiple users	This suggests an inconsistency on the Azure AD side for those users requesting a Delegation Token but there might be also a problem with your ADFS (if logon domain is federated). Some suggestions: 1) Flip UPN of the cloud user to onmicrosoft.com and then set it back to initial UPN. Reference. If connecting to Azure AD (`Connect-AzureAD`) `Set-AzureADUser -ObjectID user@federateddomain.tld -UserPrincipalName user@tenant.onmicrosoft.com` `Set-AzureADUser -ObjectID user@tenant.onmicrosoft.com -UserPrincipalName user@federateddomain.tld` If connecting to MSOL service (`Connect-MSOLservice`) `Set-MsolUserPrincipalName UserPrincipalName user@federateddomain.tld NewUserPrincipalName user@tenant.onmicrosoft.com`

	ption: Soap fault exception received. at Microsoft.Exchange.Net.WSTrust.SecurityTokenService.EndIssueToken(IAsyncResult asyncResult) at Microsoft.Exchange.InfoWorker.Common.Availability.ExternalAuthenticationRequest.Complete(IAsyncResult asyncResult)			`Set-MsolUserPrincipalName UserPrincipalName user@tenant.onmicrosoft.com NewUserPrincipalName user@federateddomain.tld` 2) Check ADFS rules /endpoints/ ADFS logs 3) If you run test-organizationrelationship for the cloud user and you see an error related to Immutable ID of that user, then check in on-premises Shell `get-remotemailbox <migrated user> |FL immutableID` and in Exchange Online PowerShell `Get-Mailbox <cloud mailbox> | FL immutableID`. There should be no ImmutableID set here. Example of ImmutableID error when running `Test-OrganizationRelationship -Identity "O365 to On-premises*" -UserIdentity CloudMailbox@contoso.com -Verbose` *The email address "XGuNpVunD0afQeVNfyoUIQ==" isn't correct. Please use this format: user name, the @ sign, followed by the domain name. For example, tonysmith@contoso.com or tony.smith@contoso.com.* *+ CategoryInfo : NotSpecified: (:) [Test-OrganizationRelationship], FormatException* If you see this error above, ensure the ImmutableID value for the on-premises user object is null. `Get-RemoteMailbox <Cloud Mailbox> |FT userprincipalname, immutableID` If the *ImmutableID* is already *null*, follow these steps: a. Set the ImmutableID to the UPN of the user: `Set-RemoteMailbox <User> -ImmutableID <user@contoso.com>` b. Sync the user object to the cloud and verify the user object has been updated in cloud. To force the sync, you can use these commands: `Import-Module ADSync` `Start-ADSyncSyncCycle -PolicyType Delta`

				In Exchange Online PowerShell, check if the immutableID has been updated: `Get-mailbox <Cloud Mailbox> |FT userprincipalname, immutableID` c. Set back the *ImmutableID* to *null*: `Set-RemoteMailbox <User> -ImmutableID $null` d. Sync the user object to the cloud and verify the user object has been updated. `Start-ADSyncSyncCycle -PolicyType Delta` In Exchange Online PowerShell, check if the immutableID has been updated: `Get-mailbox <Cloud Mailbox> |FT userprincipalname, immutableID` If the user is not synced from On-Premises then you would clear the value on the cloud object directly with command executed in EXO PowerShell: `Set-mailbox <cloud user> -immutableID $NULL` 4) Check organization relationship settings (baseline configuration is in part 1 of this blog post) 5) If you have this error for the other direction (On-Premises to Cloud), you can also run command `Test-FederationTrust -UserIdentity OnPremMBX@contoso.com -verbose -debug` and you can try recreating federation trust in on-premises.
24	Exception: **The result set contains too many calendar entries.** The allowed size = 1000; the actual size = 5009. LID: 54796	Cloud to cloud	Issue with particular user(s)	The previous allowed limit of events was set to 1000 and we were using this KB for workarounds: https://support.microsoft.com/help/2962513/you-can-t-view-free-busy-information-on-another-user-s-calendar-in-exc The limit has been raised and the logic changed. If you still encounter this error, please open a support case with us.
	Microsoft.Exchange.InfoWorker.Common.InvalidParameterException: **Work hours start time must be less than or equal to end time.**
at Microsoft.Exchange.InfoWorker.Common.Meeti	Cloud to Cloud	Users are unable to see F/B for Room Lists	Review the value of **WorkingHoursStartTime; WorkingHoursEndTime ;WorkingHoursTimeZone** in the Mailbox Calendar Configuration of the rooms. Make sure **WorkingHoursEndTime** does not happen before **WorkingHoursStartTime** and **WorkingHoursTimeZone** is set.

	ngSuggestions.AttendeeWorkHours.Validate(TimeSpan startTime, TimeSpan endTime)
at			You can run the below command for example to export this information for a room list: `Get-DistributionGroupMember -Identity "Rooml list A" | Get-MailboxCalendarConfiguration | FL`
25	System.Net.WebException: **The request failed with HTTP status 401: Unauthorized**. And if you do `Test-OAuthConnectivity -Service EWS -TargetUri https://mail.contoso.com/ews/exchange.asmx -Mailbox cloudmbx@contoso.com -Verbose | fl`, it will give you this exception: System.Net.WebException: The remote server returned an error: (401) Unauthorized. Boolean reloadConfig), diagnostics: 2000000;reason="The token has an invalid signature.";error_category="**invalid_signature"**	Cloud to On-Premises, Oauth	Functional or configuration issue	In the On-Premises Exchange Shell run a command similar to this to refresh metadata for Auth: `Set-AuthServer <name of the auth server for exchange> -RefreshAuthMetadata` You would need to wait a few or you can run *IISreset* on all Exchange servers and then check again this issue. Below is an expected output of *Get-AuthServer* so that you can check other settings. `Get-AuthServer | fl Name,IssuerIdentifie,TokenIssuingEndpoint,AuthMetadataUrl,Enabled` `Name : WindowsAzureACS` `IssuerIdentifier : 00000001-0000-0000-c000-000000000000` `TokenIssuingEndpoint : https://accounts.accesscontrol.windows.net/XXXXXXXX-5045-4d00-a59a-c7896ef052a1/tokens/OAuth/2` `AuthMetadataUrl : https://accounts.accesscontrol.windows.net/contoso.com/metadata/json/1` `Enabled : True` In the next error, we show also Auth Certificate issue, in case if related.
26	System.Net.WebException: **The request failed with HTTP status 401: Unauthorized.** And if you do `Test-OAuthConnectivity -Service EWS -TargetUri https://outlook.office365.com/ews/exchange.asmx -Mailbox`	On-Premises to Cloud, Oauth	Usually, issues with Certificates	The cause can be that the Auth Certificate with thumbprint *'XXX'* present in *CurrentCertificateThumbprint* from *Get-AuthConfig* | fl is not found in Azure (in *Get-MsolServicePrincipalCredential)* The quickest way to check this certificate mismatch is to look at the certificate dates (*StartDate* and *EndDate* from *Get-MsolServicePrincipalCredential*) and see if they match

	`onpremMailbox@domain -Verbose | fl` in EMS, it will give you this exception: System.Net.WebException: The remote server returned an error: (401) Unauthorized. Error:Unable to get token from Auth Server. Error code: 'invalid_client'. Description: 'AADSTS70002: Error validating credentials. AADSTS50012: **Client assertion contains an invalid signature. [Reason - The key was not found., Thumbprint of key used by client:** 'XXXXXXXXXXXXXXXXXXX'			*NotBefore* and *NotAfter* from *Get-ExchangeCertificate*). You would run this command in Exchange On-Premises to see the details of the On-Premises Exchange Certificate used for OAuth: `Get-ExchangeCertificate -Thumbprint (Get-AuthConfig).CurrentCertificateThumbprint | fl` (look especially at *NotBefore* and *NotAfter* values) Then in Azure PowerShell (*Connect-MsolService)* you would run command `Get-MsolServicePrincipalCredential -ServicePrincipalName "00000002-0000-0ff1-ce00-000000000000" -ReturnKeyValues $true` and here you would look first at *StartDate* and *EndDate* to see if they match *NotBefore* and *NotAfter* dates. If you want to make sure it is the same certificate, you would copy the "Value" data from *Get-MsolServicePrincipalCredential* to a Notepad and save that file as *.cer.* Then you would open the *.cer* file and you would see other details of the certificate like *Issuer* and *Thumbprint.* 1) If the certificate is not being uploaded to Azure (suppose *Value* is empty in *Get-MsolServicePrincipalCredential*), you will need to export the On-Premises Certificate with (*CurrentCertificateThumbprint*) from *Get-AuthConfig* and Upload it to Azure (steps 3 and 4 from here) 2) If certificate thumbprint in *Get-AuthConfig* 'XXX' is different from the one you see in *Get-MsolServicePrincipalCredential* 'YYY', then you would either change the Certificate Thumbprint on Auth Config (commands below), either you would export and upload the *Auth Certificate* to Azure (as mentioned above in #1). Commands to set the Certificate Thumbprint on *AuthConfig:* `$a=get-date` `Set-AuthConfig -NewCertificateThumbprint YYY -NewCertificateEffectiveDate $a`

				* Accept to continue despite the fact that the certificate effective date is not 48 hours into the future `Set-AuthConfig –PublishCertificate` * Make sure to remove any potential reference to the previous certificate (which might not exist anymore) by doing `Set-AuthConfig -ClearPreviousCertificate`
27	**Proxy web request failed. , inner exception: Response is not well-formed XML.**	Cloud to On-Premises, DAUTH	Unknown	This looks like an issue with External EWS (you wouldn't normally have this issue with Internal EWS), if you run the Remote Connectivity Analyzer test for EWS for on-premises user, you will most probably see this error: *"The response received from the service didn't contain valid XML"* Application logs from Exchange Server Event Viewer could help in troubleshooting this issue only if the request reaches to Exchange / IIS. IIS logs will help you check this. If you don't see the F/B entries in IIS logs, then check the Reverse Proxy logs to see if the device is rejecting the request. Causes for this error might be IIS misconfigurations (for example Anonymous authentication missing from EWS in IIS), Network devices (Reverse Proxy), EWS crash. For this error, we recommend you open a case with Exchange on-premises support if the above suggestions don't help.
28	**Failed to communicate with https://login.microsoftonline.com/extSTS.srf., inner exception: Unable to connect to the remote server**	On-Premises to Cloud, DAUTH	Network issues	This suggests we cannot connect to MFG URL(s) from one or more Exchange Servers 1) Check if you can get the federation token or any other failure when running the following commands in Exchange Management Shell: `Test-OrganizationRelationship –Identity "On-premises to O365*" -UserIdentity <On-Premises Mailbox> -Verbose` `Test-FederationTrust -UserIdentity <On-Premises Mailbox> -Verbose` `Test-FederationTrustCertificate`

				2) From on-premises Exchange to Office 365, the 2010 MBX & CAS or 2013 MBX (backend) or 2016 would need outbound Internet access to the Microsoft Federation Gateway or Authorization server (if using OAuth) in additions to https://outlook.office365.com/ews/exchange.asmx (the availability URL in Office 365). References here and here. 3) Verify the Machine /System account can access these URLs below. You will use **PsExec.exe** (with **-s -i**) switches from PSTools/Windows 2000 Resource Kits to launch an Internet browser session to test the URLs. C:\Tools\pstools>PsExec.exe -i -s "c:\Program Files\Internet Explorer\iexplore.exe" **Microsoft Federation Gateway (without OAuth)** • https://nexus.microsoftonline-p.com/federationmetadata/2006-12/federationmetadata.xml [<-- You should see an xml page.] • https://login.microsoftonline.com/extSTS.srf [<-- You should be prompted to download the file.] • https://domains.live.com/service/managedelegation2.asmx [<-- You should see the operations supported by ManageDelegation2.] **Microsoft Authorization Server (with OAuth)** • https://outlook.office365.com/ews/Exchange.asmx [<-- We should be getting a cred prompt.] • https://login.windows.net/common/oauth2/authorize [<-- We should be getting Sorry, but we're having trouble signing you in.] • https://accounts.accesscontrol.windows.net/<tenant guid>/tokens/OAuth/2 [<-- We should be getting HTTP 400.]
29	**Autodiscover failed for E-Mail Address joe@contoso.com with error System.Net.WebException: The remote name could not be resolved: 'mail.contoso.com'**	Cloud to On-Premises	DNS issue	If you have this error for the Autodiscover Endpoint, you first need to check the `TargetAutodiscoverEpr` value from `Get-IntraOrganizationConnector |FL` OR `Get-OrganizationRelationship |FL` in Cloud Exchange Online PowerShell (direction in this case is Cloud to On-Premises). If the value for TargetAutodiscoverEpr is incorrect, in this example being https://mail.contoso.com/ and the correct one would be https://autodiscover.contoso.com/ , then you need the update the

				TargetAutodiscoverEpr (example below). You can also rerun HCW to restore default Autodiscover endpoint (based on Get-FederationInformation -DomainName “contoso.com” or On-Premises Get-IntraOrganizationConfiguration) `Set-IntraOrganizationConnector <Cloud IOC Identity> -DiscoveryEndpoint “https://autodiscover.contoso.com/autodiscover/autodiscover.svc”` or `Set-OrganizationRelationship <Cloud Org Rel Identity> -TargetAutodiscoverEpr “https://autodiscover.contoso.com/autodiscover/autodiscover.svc”` If the value for TargetAutodiscoverEpr is the one intended, then it means that the hostname mail.contoso.com (as per example above) is not resolvable in the public DNS (doesn't point to your on-premises Autodiscover Service). You should fix the DNS issue and publish your on-premises Autodiscover endpoint. If you can’t fix the Autodiscover or you need to work-around this free/busy issue while you are fixing it and if you have a resolvable hostname for the Exchange Web Services (EWS), then you can set that hostname as TargetSharingEpr in the Cloud IntraOrganizationConnector / Cloud Organization Relationship. Example: `Set-IntraOrganizationConnector <Cloud IOC Identity> -TargetSharingEpr https://<Resolvable_in_DNS_EWS_hostname>/EWS/Exchange.asmx` or `Set-OrganizationRelationship <Cloud Org Rel Identity> -TargetSharingEpr https://<Resolvable_in_DNS_EWS_hostname>/EWS/Exchange.asmx`

30	**Failed to get ASURL. Error 8004010F**	On-Premises to Cloud	Multiple	This is quite generic error and there can be multiple causes. Here are some troubleshooting suggestions: a) Make sure that Autodiscover works for the affected user and that is returning AS URL (Availability Service URLs = Exchange Web Services URLs) b) Make sure that the Client (Outlook for example) is able to get to the AS URL c) Make sure that Free/Busy works between on-premises users (hosted on different Exchange On-Premises Servers) d) If you have Load Balancers, you should point the Outlook Client Machine Hosts file to a specific Client Access Server when you reproduce the Free/Busy issue in Outlook to eliminate Load Balancers fault. e) If Free/Busy works between on-premises users, then you should make sure that all your on-premises Exchange Servers can access Office 365 and Exchange Online IP Addresses (outbound access). f) Also, you should check if each Exchange Server can get a Federation token, run Test-FederationTrust from each Exchange Server. If it fails at retrieving Federation token step, check again if the Exchange Servers are allowed to connect to Office 365 at proxy / firewall level If you still get this error after checking these suggestions, open a case with Microsoft Support to take some more advanced Exchange Traces
31	Proxy web request failed. , inner exception: System.Net.WebException: The request failed with the error message:
--
 <head><title>**Object moved**</title></head><body> Object Moved </body>
 --.
Cloud to On-Premises	Configuration	As mentioned before, if we see “proxy web request failed” in the Free/Busy error, this suggests an EWS issue. In this case, TargetSharingEpr was populated with an external EWS URL that was redirecting to something else, thus the “Object Moved” error. `Get-OrganizationRelationship | FL Identity, TargetSharingEpr, TargetAutodiscoverEpr` `Get-IntraOrganizationConnector | FL Identity, TargetSharingEpr, DiscoveryEndpoint` By default, HCW doesn’t populate TargetSharingEpr in the IntraOrganization Connectors or Organization Relationships because we rely on Autodiscover (TargetAutodiscoverEpr or DiscoveryEndpoint) to retrieve the External EWS URL of the user.

				If you see “proxy web request failed […] object moved”, you should therefore check the TargetSharingEpr URL that was manually set in the IntraOrganizationConnector or OrganizationRelationship and browse that to see where it redirects. Then you should fix the EWS URL.
32	**The request was aborted: Could not create SSL/TLS secure channel.**	Both directions	Configuration	If direction is Cloud to On-Premises, most probably TLS1.2 is not enabled in the on-premises servers where Office 365 servers are making the connections to (example TMG, Exchange Servers). Reference https://support.microsoft.com/en-us/help/4057306/preparing-for-tls-1-2-in-office-365 If direction is On-Premises to Cloud, can still be issues with TLS 1.2 not enabled but there can be also due to missing Office 365 certificates (example outlook.office365.com certificate) from Trusted Root CA Store or a mismatch of cypher suits or other related SSL/TLS protocols issues.
33	**"The user specified by the user-context in the token does not exist.";error_category="invalid_user". 401: Unauthorized**	On-Premises to Cloud, using OAUTH	Configuration	You would see this error also in `Test-OauthConnectivity` for the on-premises user. The error suggests that the on-premises user mailbox is not synced to the cloud (mail user object). Sync the on-premises user with AADConnect to cloud in order to provision the user in AAD.
34	**“The hostname component of the audience claim value 'https://<hybrid.domain.com>’ is invalid";error_category="invalid_resource” 401: Unauthorized**	Cloud to On-Premises, using OAUTH	Configuration	This is because SSL offloading does not work with OAuth. Workarounds: 1) disable SSL offloading for Autodiscover / EWS in the on-premises environment OR 2) disable Cloud IOC / OAuth and rely on Dauth.