Office 365

- 365 Exchange MFA
- 365 Password Settings
- AD Connect
- Add_SMTP_365_Proxy_Email.ps1
- Azure/Office 365 - Convert from ADConnect to Online Only
- Email Cutover to Office 365
- Exporting PST from Office 365
- Google email in Outlook
- Manage who can create Office 365 Groups
- Office 365 and scan to email
- Office 365 Exchange Hybrid Migration -Decom
- Office 365 Exchange Migration - Hybrid
- Office 365 Exchange Migration Cutover
- OneDrive Grant Access
- OneDrive Redirection
- OneDrive Sync Issues
- Outlook Credential Windows Disappears
- Password WriteBack
- PowerShell Add to Global Admin
- routable domain
- SSO
- SSPR
- Troubleshoot Missing Emails

365 Exchange MFA

2FA

Connect-EXOPSSession -UserPrincipalName Accent@bb.summersphc.com

Connect-EXOPSSession -UserPrincipalName adminkeith@faztek.net

Get-PSSession | Remove-PSSession

365 Password Settings

https://admin.microsoft.com/AdminPortal/Home#/Settings/Services/:/Settings/L1/PasswordPolicy

AD Connect

Provide the password of the AD DS Connector account

1. Start the Synchronization Service Manager (START → Synchronization Service).
2. Go to the Connectors tab.
3. Select the AD Connector that corresponds to your on-premises AD. ...
4. Under Actions, select Properties.
5. In the pop-up dialog, select Connect to Active Directory Forest:

From <
https://www.google.com/search?q=AD+Connect+change+synchronization+account&rlz=1C1ONGR_enUS963US963&oq=AD+Connect+change+synchronization+account&aqs=chrome..69i57.8829j0j7&sourceid=chrome&ie=UTF-8>

AD ADD Sync

Start-ADSyncSyncCycle -PolicyType Delta

Get-date

Reinstall:

Found problems with reinstall and today I was able to work around it by removing these items to allow the installation to think it was not installed prior:

Prior to today (4/5/2022) yesterday I uninstalled and then restarted the server overnight.

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products

Inside of this key was a couple of entries that linked to AD Connect. In removed the sub-keys (not "Products")

This folder must also be empty:

C:\Program Files\Microsoft Azure AD Sync\Data

Once those 2 areas were cleared I was able to get it to install.

Add_SMTP_365_Proxy_Email.ps1

```
#Variables

$Domain = "accentconsultingservices.mail.onmicrosoft.com"



#Get all users in ActiveDirectory

$Users = Get-ADUser -Filter * -Properties ProxyAddresses



#Some output is always nice

Write-Host "Processing $Users.Count users..." -ForegroundColor Green



#Go through all users

foreach ($User in $Users) {



#Check if <domain>.mail.onmicrosoft.com alias is present, if not add it as an alias

if ($User.Proxyaddresses -like "*$Domain*") {

Write-Host "$User.SamAccountName has an alias matching $Domain..." -ForegroundColor Yellow

}

else {

$Alias = "smtp:" + $User.SamAccountName + "@" + $Domain

Set-ADUser $User -Add @{Proxyaddresses="$Alias"}

Write-Host "Alias addded to $User.SamAccountName..." -ForegroundColor Green
```

```
}

}

Write-Host "Done" -ForegroundColor Green
```

Azure/Office 365 - Convert from ADConnect to Online Only

When you are ready to turn off DirSync, and all exchange mailboxes are in the cloud, the next steps will be turning off DirSync:

https://docs.microsoft.com/en-us/microsoft-365/enterprise/turn-off-directory-synchronization?view=o365-worldwide

You need to connect to MSOL with your global admin credentials:

connect-msolservice

Set-MsolDirSyncEnabled -EnableDirSync $false

Next, you can uninstall AD Connect cleanly:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-uninstall

Please let me know if you have any additional questions or if you wish to archive your case for now?

Thank you and have a great day.

This will switch AAD_AD sync accounts to cloud ONLY accounts. If sync runs after this it will create duplicate accounts.

Email Cutover to Office 365

This is intended as high level generic overview, nothing more

Prep

- Prep MS 365
  - Add domains
  - Add users
  - Add and apply licensing
  - Ensure all objects in old source are in new one
    - Contacts
    - Distribution lists
    - Shared Mailboxes
- User Tool (VEEAM/FLY) to create initial copy of all email from source email to MS 365 EOL
  - Resolve all errors and problems

Get Access to all DNS

- Update SPF Record to include old and new sources
- Reduce TTL

- Identify all email sources
  - Phones
  - Computer email clients
  - Email generating software
  - Scan to email devices
  - Marketing and 3rd party sources
- Prep for company communications
  - How to update your phone
  - What to do to get your Outlook client to update
  - What is the URL for MS 365 EOL
  - How to validate your MS 365 password

Cutover

- Day before
  - Lower TTL on DNS
  - Conduct incremental data sync
- Execution
  - Update MX records
  - Update AutoDiscover Record
  - Validate mail flow
  - Final cutover sync
  - Disable source email access (if possible)
  - Work with end users client access
  - Update non-standard email source devices.

Exporting PST from Office 365

The export must be done in IE or Edge!

Initial export

1. Login to Office 365 with the Company specific admin login
   Note: If you go back to the office portal page click Login again to fully sign in.
2. Click Admin
3. On the left side click "Show all"
4. Click Security
5. On the left side click "Permissions"
6. Sort the results by name and then click "eDiscovery Manager"
7. Verify that under "Assigned roles" you see "Export", If Export does exist go to Step 8
   1. click "Edit" besides "Assigned roles"
   2. Click "Edit", then click "+ Add"
   3. Search for Export, check the box, and click "Add"
   4. Click "Done" then click "Save"
8. Scroll down and click "Edit" beside "eDiscovery Administrator"
9. Click "Choose eDiscovery Administrator"
10. Click "+ Add"
11. Search for the user that we login as (I.E. Admin, O365Admin, etc…)
12. Once located check our user and click "Add"
13. Click "Done", then click "Save", and lastly click "Close"
14. Scroll to the top of the window and click the hyperlink on the line that reads;

"To assign permissions for archiving, auditing, and retention policies, go to the Exchange admin center."

15. Look for a "Role Group" called "Import Export", Skip to step 16 if this exists
    1. Click”+” to create a new role.
    2. Name the role Import Export.
16. Edit the "Import Export" rule to add our user that we login as (I.E. Admin, O365Admin, etc…)
17. Click Save and close the Role Groups tab

User PST Export Steps

1. Login to Office 365 with the Company specific admin login
   Note: If you go back to the office portal page click Login again to fully sign in.
2. Click Admin
3. On the left side click "Show all"
4. Click Security
5. On the left side Click "Search"
6. Click "Content Search"
7. Click "+ New search"
8. Beside "Specific Locations" click "Modify"
9. Click "Choose users, groups, or teams"
10. Click "Choose users, groups, or teams"
11. Search for the user you wish to export.
12. Check the box and click "Choose", Click "Done", and click "Save"
13. Click "Save & run"
14. Name the search "{Date YYYY-MM-DD} {Username} Export" and click "Save"
15. Click on "Searches" at the top of the screen, and then click "Refresh" You should now see your search
16. Click on the newly created search, and click Export Results
    NOTICE: If Export Results is not an option, and you recently added the Admin user to have permission for this you may need to log out and back into O365, or wait for a duration of time as it can take up to 24 hours to update the settings.
17. Keep the Default settings and click "Export"
18. Click "Close:, then Click the "Exports" option at the top.
19. Click "Refresh" and you should see your new Export.
20. Click on the option and verify the "Preparing data ..." process has started under "Status".
    Note: You may need to refresh this a couple of times before you see progress.
21. Now wait for that process to complete as you will not be able to download the PST file until it has.

Some Time Later . . .

22. Once the Export Process has completed.
23. Click "Copy to clipboard" under "Export Key:"
24. Click "Download results" at the top of the screen.
25. A new program will launch called "eDiscovery Export Tool" (Install if needed)
    1. Paste the Export Key
    2. Then choose the download location.
    3. Click the Down arrow next to "Advanced options" to change the name of the PST being exported.

4. Click Start
5. Now wait for the download to complete . . .

Some Time Later . . .

26. Once complete you now have a PST that you can import into another mailbox.

Google email in Outlook

How to set up Gmail in Outlook

Gmail is a popular choice for email, and you can get this as part of the Google Apps suite to use as email at your domain. See this tutorial for how to get Google Apps free for nonprofits!

Your Gmail account can be accessed anywhere using an email app on your phone or by logging on to Gmail.com, but you may prefer to use Outlook to access your email. This tutorial will walk you through the setup process in Outlook for your Gmail account.

1

Enable IMAP and Outlook access in Google

In order to connect Outlook to Gmail, you'll need to first enable the IMAP connection that Outlook will use.

1. Log in to your Google Apps account at Gmail.com, and click the gear button to access your settings
2. Click "Settings"
3. Go to the "Forwarding and POP/IMAP" tab
4. Click the radio button to "Enable IMAP". You can leave the default settings for the additional options that appear, unless you specifically want to change them.
5. Save your changes

Machine generated alternative text:

6. Now, you'll need to click this link to allow Outlook to log in to your account:

   https://www.google.com/settings/security/lesssecureapps

Machine generated alternative text:

If you're unable to complete this step, you'll need to have your admin log into http://admin.google.com and change a setting. The admin will need to do a search for less secure and click on the less secure apps result. Then just change the setting to the middle option as pictured below:

7.

8. Next, make sure your account is unlocked by visiting this link and clicking "Continue":
   https://accounts.google.com/b/0/DisplayUnlockCaptcha

Now you're ready to set up the account in Outlook!

2

Add a new IMAP account in Outlook

These instructions assume you are starting from scratch to set up an new email account in Outlook. If you are switching to Gmail but are keeping an email address that you already have set up as POP3, you will still need to create a new one, since Outlook won't let you modify the account type.

Settings Quick Reference:

Type	IMAP
Full Name or Account Name	[your name]
Email address	full email address for Google Apps (username@yourdomain.org)
Username	full email address for Google Apps (username@yourdomain.org)
Password	your Google Apps account password
Require authentication (SPA)	checked
Incoming server	imap.gmail.com
Port	993
Encryption Type	SSL
Outgoing server	smtp.gmail.com
Port	587 (or 465)
Encryption type	TLS (or SSL)
Use the same settings as incoming server	checked

Setup Steps:

1. Open Outlook and go to File >> Account Settings and click New to add an account (or Change an existing IMAP account)

2. Choose "Manual Setup" and then choose "POP or IMAP"

3. Enter the settings as summarized in the table above, or use the following screenshot for reference:

4. Click "More Settings" and continue entering the information:

5. Click "OK" and then "Next" and correct any errors, then "Finish"

You're all set! Be sure to visit the Google Apps support page for IMAP setup if you run into any problems, and double-check your settings. If you still can't figure it out, our friendly support team would be happy to lend a hand!

Once you sign in you may get a error message. I sent an email out and it prompted for access and once authenticated to GOOGLE and accepted control that error went away. 0x800CCC0E

From <https://help.ecatholic.com/article/155-how-to-set-up-gmail-in-outlook>

Manage who can create Office 365 Groups

https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/manage-creation-of-groups?view=o365-worldwide

Manage who can create Office 365 Groups

03/02/2020

5 minutes to read

Because it's so easy for users to create Office 365 Groups, you aren't inundated with requests to create them on behalf of other people. Depending on your business, however, you might want to control who has the ability to create groups.

This article explains how to disable the ability to create groups in all Office 365 services that use groups:

Outlook

SharePoint

Yammer

Microsoft Teams

Microsoft Stream

StaffHub

Planner

PowerBI

Roadmap

You can restrict Office 365 Group creation to the members of a particular security group. To configure this, you use Windows PowerShell. This article walks you through the needed steps.

The steps in this article won't prevent members of certain roles from creating Groups. Office 365 Global admins can create Groups via any means, such as the Microsoft 365 admin center, Planner, Teams, Exchange, and SharePoint Online. Other roles can create Groups via limited means, listed below.

Exchange Administrator: Exchange Admin center, Azure AD

Partner Tier 1 Support: Microsoft 365 Admin center, Exchange Admin center, Azure AD

Partner Tier 2 Support: Microsoft 365 Admin center, Exchange Admin center, Azure AD

Directory Writers: Azure AD

SharePoint Administrator: SharePoint Admin center, Azure AD

Teams Service Administrator: Teams Admin center, Azure AD

User Management Administrator: Microsoft 365 Admin center, Yammer, Azure AD

If you're a member of one of these roles, you can create Office 365 Groups for restricted users, and then assign the user as the owner of the group. Users that have this role are able to create connected groups in Yammer, regardless of any PowerShell settings that might prevent creation.

Licensing requirements

To manage who creates Groups, the following people need Azure AD Premium licenses or Azure AD Basic EDU licenses assigned to them:

The admin who configures these group creation settings

The members of the security group who are allowed to create Groups

The following people don't need Azure AD Premium or Azure AD Basic EDU licenses assigned to them:

People who are members of Office 365 groups and who don't have the ability to create other groups.

Step 1: Create a security group for users who need to create Office 365 Groups

Only one security group in your organization can be used to control who is able to create Groups. But, you can nest other security groups as members of this group. For example, the group named Allow Group Creation is the designated security group, and the groups named Microsoft Planner Users and Exchange Online Users are members of that group.

Admins in the roles listed above do not need to be members of this group: they retain their ability to create groups.

Important

Be sure to use a security group to restrict who can create groups. If you try to use an Office 365 Group, members won't be able to create a group from SharePoint because it checks for a security group.

In the admin center, go to the Groups > Groups page.

Click on Add a Group.

Choose Security as the group type. Remember the name of the group! You'll need it later.

Finish setting up the security group, adding people or other security groups who you want to be able to create Groups in your org.

For detailed instructions, see Create, edit, or delete a security group in the Microsoft 365 admin center.

Step 2: Install the preview version of the Azure Active Directory PowerShell for Graph

These procedures require the preview version of the Azure Active Directory PowerShell for Graph. The GA version will not work.

Important

You cannot install both the preview and GA versions on the same computer at the same time. You can install the module on Windows 10, Windows Server 2016.

As a best practice, we recommend always staying current: uninstall the old AzureADPreview or old AzureAD version and get the latest one.

In your search bar, type Windows PowerShell.

Right-click on Windows PowerShell and select Run as Administrator.

Open PowerShell as "Run as administrator."

Set the policy to RemoteSigned by using Set-ExecutionPolicy.

Copy

```
Set-ExecutionPolicy RemoteSigned
```

Check installed module:

Copy

```
Get-InstalledModule -Name "AzureAD*"
```

To uninstall a previous version of AzureADPreview or AzureAD, run this command:

Copy

```
Uninstall-Module AzureADPreview
```

or

Copy

Uninstall-Module AzureAD

To install the latest version of AzureADPreview, run this command:

Copy

Install-Module AzureADPreview

At the message about an untrusted repository, type Y. It will take a minute or so for the new module to install.

Leave the PowerShell window open for Step 3, below.

Step 3: Run PowerShell commands

Copy the script below into a text editor, such as Notepad, or the Windows PowerShell ISE.

Replace <SecurityGroupName> with the name of the security group that you created. For example:

$GroupName = "Group Creators"

Save the file as GroupCreators.ps1.

In the PowerShell window, navigate to the location where you saved the file (type "CD ").

Run the script by typing:

.\GroupCreators.ps1

and sign in with your administrator account when prompted.

PowerShell

Copy

```
$GroupName = "<SecurityGroupName>"

$AllowGroupCreation = "False"

Connect-AzureAD

$settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id

if(!$settingsObjectID)

{

  $template = Get-AzureADDirectorySettingTemplate | Where-object {$_.displayname -eq "group.unified"}

    $settingsCopy = $template.CreateDirectorySetting()

    New-AzureADDirectorySetting -DirectorySetting $settingsCopy

    $settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id

}
```

```
$settingsCopy = Get-AzureADDirectorySetting -Id $settingsObjectID

$settingsCopy["EnableGroupCreation"] = $AllowGroupCreation



if($GroupName)

{

$settingsCopy["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString
$GroupName).objectid

}

 else {

$settingsCopy["GroupCreationAllowedGroupId"] = $GroupName

}

Set-AzureADDirectorySetting -Id $settingsObjectID -DirectorySetting $settingsCopy



(Get-AzureADDirectorySetting -Id $settingsObjectID).Values
```

The last line of the script will display the updated settings:

This is what your settings will look like when you're done.

If in the future you want to change which security group is used, you can rerun the script with the name of the new security group.

If you want to turn off the group creation restriction and again allow all users to create groups, set $GroupName to "" and $AllowGroupCreation to "True" and rerun the script.

Step 4: Verify that it works

Sign in to Office 365 with a user account of someone who should NOT have the ability to create groups. That is, they are not a member of the security group you created or an administrator.

Select the Planner tile.

In Planner, select New Plan in the left navigation to create a plan.

You should get a message that plan and group creation is disabled.

Try the same procedure again with a member of the security group.

Note

If members of the security group aren't able to create groups, check that they aren't being blocked through their OWA mailbox policy.

Related articles

Getting started with Office 365 PowerShell

Set up self-service group management in Azure Active Directory

Set-ExecutionPolicy

Azure Active Directory cmdlets for configuring group settings

Office 365 and scan to email

How to set up a multifunction device or application to send email using Office 365

Exchange Online

Applies to: Exchange Online

Topic Last Modified: 2016-05-04

You can use SMTP submission, direct send, or SMTP relay to allow a multifunction device, printer, or application to send email using Office 365 and Exchange Online.

This topic explains how to send email from devices and business applications when all of your mailboxes are in Office 365. For example:

- You have a scanner, and you want to email scanned documents to yourself or someone else.
- You have a line-of-business (LOB) application that manages appointments, and you want to email reminders to clients of their appointment time.

Use this article to choose the option that meets your requirements, then configure your device or application to send email:

Image not found or type unknown

Note:

This document helps you set up email for multifunction printer devices and business applications only. If you want to set up a mobile device, such as a smart phone, or other email clients to send and receive from an Office 365 mailbox, see Settings for POP and IMAP access for Office 365 for business or Microsoft Exchange accounts.

Use your own email server to send email from multifunction devices and applications

If you have mailboxes in Office 365 and an email server that you manage (also called an on-premises email server), always configure your devices and applications to use your local network and route email through your own email server. For details about setting up your Exchange server to receive email from systems that are not running Exchange (such as a multifunction printer), see Create a Receive connector to receive email from a system not running Exchange.

How can devices and applications send email to recipients?

If all of your mailboxes are in Office 365, here are the options for sending email from an application or device:

- Option 1 (recommended): Authenticate your device or application directly with an Office 365 mailbox, and send mail using SMTP client submission
  Configure your device or application to authenticate with an Office 365 mailbox, and use Simple Mail Transfer Protocol (SMTP) client submission. In this scenario, the device or application uses an email account to send email to recipients just like an email client.
- Option 2: Send mail direct from your printer or application to Office 365 (direct send)
  Configure your device or application to send mail directly to recipients in your organization. When you set up your device or application, configure it to point to your mailboxes in Office 365 using your mail exchange (MX) endpoint record.
- Option 3: Configure a connector to send mail using Office 365 SMTP relay
  Configure a connector so your device or application can send email to Office 365. Office 365 can then relay email to your organization mailboxes and to external recipients.

Note:

If you have already configured email for printers or devices and want to troubleshoot an issue, see the article Troubleshoot email sent from devices and business applications.

Descriptions of each method and configuration instructions follow.

Option 1 (recommended): Authenticate your device or application directly with an Office 365 mailbox, and send mail using SMTP client submission

If your device or application can authenticate and send email using an Office 365 mailbox account, this is the recommended method. The device or application sends mail using SMTP client submission. In the following diagram, the application or device in your organization's network uses SMTP client submission and authenticates with a mailbox in Office 365.

Using SMTP client submission

To send mail using SMTP client submission, each device or application must be able to authenticate with Office 365. Each device or application can have its own sender address, or all devices can use one address, such as printer@contoso.com. If you want to send email from a third-party hosted application or service, you must use SMTP client submission. In this scenario, the device or application connects directly to Office 365 using the SMTP client submission endpoint smtp.office365.com.

Features of SMTP client submission

- SMTP client submission allows you to send email to people in your organization as well as outside your company.
- This method bypasses most spam checks for email sent to people in your organization. This can help protect your company IP addresses from being blocked by a spam list.
- With this method, you can send email from any location or IP address, including your (on-premises) organization's network, or a third-party cloud hosting service, like Microsoft Azure.

Requirements for SMTP client submission

- Authentication: You must be able to configure a user name and password to send email on the device.
- Mailbox: You must have a licensed Office 365 mailbox to send email from.
- Transport Layer Security (TLS): Your device must be able to use TLS version 1.0 and above.
- Port: Port 587 (recommended) or port 25 is required and must be unblocked on your network. Some network firewalls or ISPs block ports—especially port 25.

Note:
For information about TLS, see How Exchange Online uses TLS to secure email connections in Office 365 and for detailed technical information about how Exchange Online uses TLS with cipher suite ordering, see Enhancing mail flow security for Exchange Online.

Limitations of SMTP client submission

You can only send from one email address unless your device can store login credentials for multiple Office 365 mailboxes. Office 365 imposes a limit of 30 messages sent per minute, and a

limit of 10,000 recipients per day.

Set up SMTP client submission by following How to configure SMTP client submission.

Option 2: Send mail directly from your printer or application to Office 365 (direct send)

If SMTP client submission is not compatible with your business needs or with your device, consider using direct send. Direct send makes it easy to send messages to recipients in your own organization with mailboxes in Office 365.

In the following diagram, the application or device in your organization's network uses direct send and your Office 365 mail exchange (MX) endpoint to email recipients in your organization. It's easy to find your MX endpoint in Office 365 if you need to look it up.

Using direct send

You can configure your device to send email direct to Office 365. However, in this case, Office 365 does not relay messages for external recipients and will only deliver to your hosted mailboxes. If your device sends an email to Office 365 that is for a recipient outside your organization, the email will be rejected.

Note:
If your device or application has the ability to act as a mail server and deliver to Office 365 as well as other mail providers, consult your device or application instructions; there are no Office 365 settings needed for this scenario.

There are several scenarios where direct send can be the best choice:

- If the device or application is only sending email to your own Office 365 users and SMTP client submission is not an option, this is the simplest method as there is no Office 365 configuration needed.
- You want your device or application to send from each user's email address and do not want each user's mailbox credentials configured to use SMTP client submission. Direct send allows each user in your organization to send email using their own address. When you use direct send, avoid using a single mailbox with Send As permissions for all your users. This method is not supported because of complexity and potential issues.
- Your device or application does not meet the requirements of SMTP client submission, such as TLS support.
- Office 365 does not allow you to send bulk email or newsletters via SMTP client submission. Direct send allows you to send a higher volume of messages. However, there is a risk of your email being marked as spam by Office 365. You might want to enlist the help of a bulk email provider to assist you. There are best practices for bulk email, and bulk email providers can help ensure that your domains and IP addresses are not blocked by others on the Internet.

Features of direct send

Direct send:

- Uses Office 365 to send emails, but does not require a dedicated Office 365 mailbox.
- Doesn’t require your device or application to have a static IP address. However, this is recommended if possible.
- Doesn’t work with a connector; never configure a device to use a connector with direct send, this can cause problems.
- Doesn’t require your device to support TLS.

Direct send has higher sending limits than SMTP client submission. Senders are not bound by the 30 messages per minute or 10,000 recipients per day limit.

Requirements for direct send

- Port: Port 25 is required and must be unblocked on your network.
- Static IP address is recommended: A static IP address is recommended so that an SPF record can be created for your domain. This helps avoid your messages being flagged as spam.

Limitations of direct send

- Direct send cannot be used to deliver email to external recipients, for example, recipients with Yahoo or Gmail addresses.
- Your messages will be subject to antispam checks.
- Sent mail might be disrupted if your IP addresses are blocked by a spam list.
- Office 365 uses throttling policies to protect the performance of the service.

Set up direct send by following How to configure direct send.

Option 3: Configure a connector to send mail using Office 365 SMTP relay

Office 365 SMTP relay uses a connector to authenticate the mail sent from your device or application. This allows Office 365 to relay those messages to your own mailboxes as well as external recipients. Office 365 SMTP relay is very similar to direct send except that it can send mail to external recipients. Due to the added complexity of configuring a connector, direct send is recommended over Office 365 SMTP relay, unless you must send email to external recipients. To send email using Office 365 SMTP relay, your device or application server must have a static IP address or address range. You can't use SMTP relay to send email directly to Office 365 from a third-party hosted service, such as Microsoft Azure.

In the following diagram, the application or device in your organization’s network uses a connector for SMTP relay to email recipients in your organization.

Using Office 365 SMTP relay

The Office 365 connector that you configure authenticates your device or application with Office 365 using an IP address. Your device or application can send email using any address (including ones that can't receive mail), as long as the address uses one of your Office 365 domains. The email address doesn’t need to be associated with an actual mailbox. For example, if your domain is contoso.com, you could send from an address like do_not_reply@contoso.com.

Features of Office 365 SMTP relay

- Office 365 SMTP relay does not require the use of a licensed Office 365 mailbox to send emails.
- Office 365 SMTP relay has higher sending limits than SMTP client submission; senders are not bound by the 30 messages per minute or 10,000 recipients per day limits.

Requirements for Office 365 SMTP relay

- Static IP address or address range: Most devices or applications are unable to use a certificate for authentication. To authenticate your device or application, use one or more static IP addresses that are not shared with another organization.
- Connector: You must set up a connector in Exchange Online for email sent from your device or application.
- Port: Port 25 is required and must not be blocked on your network or by your ISP.
- Licensing: SMTP relay doesn’t use a specific Office 365 mailbox to send email. This is why it’s important that only licensed users send email from devices or applications configured for SMTP relay. If you have senders using devices or LOB applications who don’t have an Office 365 mailbox license, obtain and assign an Exchange Online Protection license to each unlicensed sender. This is the least expensive license that allows you to send email via Office 365.

Limitations of Office 365 SMTP relay

- Sent mail can be disrupted if your IP addresses are blocked by a spam list.
- Reasonable limits are imposed for sending. For more information, see Higher Risk Delivery Pool for Outbound Messages.
- Requires static unshared IP addresses (unless a certificate is used).

Set up SMTP relay by following How to configure Office 365 SMTP relay

Summary of options for sending email from a device or application

The following table will help you decide which one of these options will meet your needs. Detailed information and setup steps follow each method.

	SMTP client submission	Direct send	SMTP relay
Features			
Send to recipients in your domain(s)	Yes	Yes	Yes
Relay to Internet via Office 365	Yes	No. Direct delivery only.	Yes
Bypasses antispam	Yes, if the mail is destined for an Office 365 mailbox.	No. Suspicious emails might be filtered. We recommend a custom Sender Policy Framework (SPF) record.	No. Suspicious emails might be filtered. We recommend a custom SPF record.
Supports mail sent from applications hosted by a third party	Yes	No	No
Requirements			
Open network port	Port 587 or port 25	Port 25	Port 25
Device or application server must support TLS	Required	Optional	Optional
Requires authentication	Office 365 user name and password required	None	One or more static IP addresses. Your printer or the server running your LOB app must have a static IP address to use for authentication with Office 365.
Limitations			
Throttling limits	10,000 recipients per day. 30 messages per minute.	Standard throttling is in place to protect Office 365.	Reasonable limits are imposed. The service can't be used to send spam or bulk mail. For more information about reasonable limits, see Higher Risk Delivery Pool for Outbound Messages.

How to configure SMTP client submission

Devices and applications vary in functionality and terminology use. However, these configuration settings will help you set up SMTP client submission.

Enter the settings directly on the device or in the application as the device guide or manual instructs. As long as your scenario meets the requirements for SMTP client submission, these settings will enable you to send email from your device or application.

Device or Application setting	Value
Server/smart host	smtp.office365.com
Port	Port 587 (recommended) or port 25
TLS/ StartTLS	Enabled
Username/email address and password	Login credentials of hosted mailbox being used

TLS and other encryption options

Determine what version of TLS your device supports by checking the device guide or with the vendor. If your device or application does not support TLS 1.0 or above:

- Use direct send or Office 365 SMTP relay for sending mail instead (depending on your requirements).
- If it is essential to use SMTP client submission and your printer only supports SSL 3.0, you can set up an alternative configuration called Indirect SMTP client submission. This uses a local SMTP relay server to connect to Office 365. This is a much more complex setup.

  Instructions can be found here: How to configure Internet Information Server (IIS) for relay with Office 365.

Note:
If your device recommends or defaults to port 465, it does not support SMTP client submission.

How to configure direct send

Devices and applications vary in functionality and terminology use. To configure direct send, enter the following settings on the device or in the application directly.

Device or application setting	Value
Server/smart host	Your MX endpoint, for example, contoso-com.mail.protection.outlook.com
Port	Port 25
TLS/StartTLS	Enabled
Email address	Any email address for one of your Office 365 accepted domains. This email address does not need to have a mailbox.

We recommend adding an SPF record to avoid having messages flagged as spam. If you are sending from a static IP address, add it to your SPF record in your domain registrar's DNS settings as follows:

DNS entry	Value
SPF	v=spf1 ip4:<Static IP Address> include:spf.protection.outlook.com ~all

Full configuration instructions for direct send

1. If your device or application can send from a static public IP address, obtain this IP address and make a note of it. You can share your static IP address with other devices and users, but don't share the IP address with anyone outside of your company. Your device or application can send from a dynamic or shared IP address but messages are more prone to antispam filtering.
2. Log on to the Office 365 Portal.
3. Make sure your domain, such as contoso.com, is selected. Click Manage DNS, and find the MX record. The MX record will have a POINTS TO ADDRESS value that looks similar to cohowineinc-com.mail.protection.outlook.com, as depicted in the following screenshot. Make a note of the MX record POINTS TO ADDRESS value, which we refer to as your MX endpoint.

4. Check that the domains that the application or device will send to have been verified. If the domain is not verified, emails could be lost, and you won't be able to track them with the Exchange Online message trace tool.
5. Go back to the device, and in the settings, under what would normally be called Server or Smart Host, enter the MX record POINTS TO ADDRESS value you recorded in step 3.
6. Now that you are done configuring your device settings, go to your domain registrar's website to update your DNS records. Edit your sender policy framework (SPF) record. In the entry, include the IP address that you noted in step 1. The finished string looks similar to this:
   v=spf1 ip4:10.5.3.2 include:spf.protection.outlook.com ~all
   where 10.5.3.2 is your public IP address.

Note:
Skipping this step might cause email to be sent to recipients' junk mail folders.

7. To test the configuration, send a test email from your device or application, and confirm that the recipient received it.

How to configure Office 365 SMTP relay

This method allows Office 365 to relay emails on your behalf by authenticating using your public IP address (or a certificate). This requires a connector to be set up for your Office 365 account. If your device or application supports or requires user name and password authentication, consider the SMTP client submission method instead. Quick configuration details follow. If you prefer full instructions, check the next section.

Device or application setting	Value
Server/smart host	Your MX endpoint, e.g. yourcontosodomain-com.mail.protection.outlook.com
Port	Port 25
TLS/StartTLS	Enabled
Email address	Any email address for one of your Office 365 verified domains. This email address does not need a mailbox.

If you have set up Exchange Hybrid or have a connector configured for mail flow from your email server to Office 365, it is likely that no additional setup will be required for this scenario. Otherwise, create a mail flow connector to support this scenario:

Connector setting	Value
From	Your organization's email server
To	Office 365
Domain restrictions: IP address/range	Your on-premises IP address or address range that the device or application will use to connect to Office 365.

We recommend adding an SPF record to avoid having messages flagged as spam. If you are sending from a static IP address, add it to your SPF record in your domain registrar’s DNS settings as follows:

DNS entry	Value
SPF	v=spf1 ip4:<Static IP Address> include:spf.protection.outlook.com ~all

Full configuration instructions

1. Obtain the public (static) IP address that the device or application with send from. A dynamic IP address isn’t supported or allowed. You can share your static IP address with

other devices and users, but don't share the IP address with anyone outside of your company. Make a note of this IP address for later.

2. Log on to the Office 365 Portal.
3. Select Domains. Make sure your domain, such as contoso.com, is selected. Click Manage DNS and find the MX record. The MX record will have a POINTS TO ADDRESS value that looks similar to cohowineinc-com.mail.protection.outlook.com as depicted in the following screenshot. Make a note of the MX record POINTS TO ADDRESS value. You'll need this later.

4. Check that the domains that the application or device will send to have been verified. If the domain is not verified, emails could be lost, and you won't be able to track them with the Exchange Online message trace tool.
5. In Office 365, click Admin, and then click Exchange to go to the Exchange admin center.

Note:
If you have Microsoft Office 365 Small Business Premium, see the instructions here.

6. In the Exchange admin center, click mail flow, and click connectors.
7. Check the list of connectors set up for your organization. If there is no connector listed from your organization's email server to Office 365, create one.
   1. To start the wizard, click the plus symbol +. On the first screen, choose the options that are depicted in the following screenshot:

   Click Next, and give the connector a name.
   2. On the next screen, choose the option By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization, and add the IP address from step 1.
   3. Leave all the other fields with their default values, and select Save.
8. Now that you are done with configuring your Office 365 settings, go to your domain registrar's website to update your DNS records. Edit your SPF record. Include the IP address that you noted in step 1. The finished string should look similar to this: v=spf1 ip4:10.5.3.2 include:spf.protection.outlook.com ~all, where 10.5.3.2 is your public IP address. Skipping this step can cause email to be sent to recipients' junk mail folders.
9. Now, go back to the device, and in the settings, find the entry for Server or Smart Host, and enter the MX record POINTS TO ADDRESS value that you recorded in step 3.
10. To test the configuration, send a test email from your device or application, and confirm that it was received by the recipient.

From <https://technet.microsoft.com/en-us/library/dn554323(v=exchg.150).aspx>

Office 365 Exchange Hybrid Migration -Decom

NOTE: This page is for the cleanup of a Hybrid migration. This is expected to be the phase AFTER completing the mailbox migrations.

Office 365 Exchange Migration -Hybrid

qKzeWcMcrkNayZZW

Make sure no devices are using your old Exchange on-premise server

Exchange Powershell:

Get-Message

Coordinate with client and turn off the Exchange Server for a period of time to verify no email flow conclusively.

Prepare Your Office 365 Environment for the Removal of the Last Exchange On-Premises Server

Follow these steps to remove dependencies on your on-prem Exchange environment:

Confirm you have no public folders on your on-prem Exchange server (move them to Office 365 if they exist)

Confirm you have no more mailboxes on your on-prem Exchange server

Confirm that no scan-to-mail devices, applications, etc. are using your on-premises Exchange server to relay emails

DNS

MX

Autodiscover

SPF

Remove the Service Connection Point values from Exchange:

Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri $Null

Remove (or disable) Exchange on-prem inbound and outbound connectors from your Office 365 environment (done via the Connectors page in the EAC – the connectors created by the Hybrid Connection Wizard are named “Inbound from ” and “Outbound to “)

Remove the Organization Relationship from Office 365 using the Office 365 Portal (the Organization Relationship created by the Hybrid Connection Wizard is named “O365 to On-Premises – “

If OAuth is enabled make sure to disable it on both on-prem and in Exchange Online:

Get-IntraorganizationConnector -Identity ExchangeHybridOnPremisesToOnline | Set-IntraOrganizationConnector -Enabled $False

Get-IntraorganizationConnector -Identity ExchangeHybridOnlineToOnPremises | Set-IntraOrganizationConnector -Enabled $False

Once these steps are completed you can remove the on-prem Exchange server.

Clean Removal of the Last On-Premises Exchange Server

A clean removal of Exchange is the preferred solution. This will ensure relevant Active Directory objects are removed properly. The clean removal is started simply by uninstalling Exchange from

the last Exchange server in your organization (make sure you completed the steps in the previous section to prepare for the removal).

Launching the Exchange uninstaller (from Add/Remove Programs) will trigger a readiness check which checks for any remaining mailboxes, any remaining mailbox databases, etc. Make sure to get rid of your arbitration mailboxes to complete the uninstall:

Automate: Set to Maintenance Mode

See what mailboxes are left

Get-Mailbox

Get-Mailbox -Archive

Get-Mailbox -PublicFolder

Get-Mailbox -AuditLog

Get-Mailbox -Monitoring

Remove or Disable Mailboxes

Get-Mailbox | Remove-Mailbox

Disable-Mailbox

Get-OfflineAddressBook

Get-OfflineAddressBook | Remove-OfflineAddressBook

Get-Mailbox -Arbitration | Remove-Mailbox -Arbitration -RemoveLastArbitrationMailboxAllowed

Get-Mailbox -Arbitration | Disable-Mailbox –Arbitration –DisableLastArbitrationMailboxAllowed

Once the readiness check is successful it will remove the Exchange configuration from AD and remove Exchange binaries from the server.

Remove from Domain

Turn off

Disable Backups, Notifications, & Reports

Disable any related processes that are no longer used (Barracuda)

Remove from CRM

https://www.easy365manager.com/remove-on-prem-exchange-from-hybrid-environment/

Notes found randomly that pertain but need reviewed:

```
#Remove default Public folders
Get-PublicFolder "\" -Recurse -ResultSize:Unlimited |
Remove-PublicFolder -Recurse -ErrorAction:SilentlyContinue

#Remove system Public folders
Get-PublicFolder "\Non_Ipm_Subtree" -Recurse -ResultSize:Unlimited |
Remove-PublicFolder -Recurse -ErrorAction:SilentlyContinue

#Remove Offline Address Book
Get-OfflineAddressBook | Remove-OfflineAddressBook

#Remove send connectors
Get-SendConnector | Remove-SendConnector
```

```
#Remove Public Folder database (SBS 2011/Exchange 2010 Only)
Get-PublicFolderDatabase | Remove-PublicFolderDatabase


#Remove arbitration mailboxes (SBS 2011/Exchange 2010 Only)
Get-Mailbox -Arbitration | Disable-Mailbox -Arbitration -DisableLastArbitrationMailboxAllowed


#Remove mailboxes
Get-Mailbox | Disable-Mailbox
```

From <https://www.itpromentor.com/sbs-remove-exchange/>

Office 365 Exchange Migration - Hybrid

qrW@-*5r2$+3BL3Qvm4*lLS0

Review cutover document to see what applies as it is a more comprehensive list

365 Exchange Cutover Migration

Create 365 domain

ID Exchange domains that will be needed

Add public domains as routable domains

Add public domains to 365

Update SPF & related

Create "365sync" group on premise

Set as Universal Group

Update users with email domain using script

Routable Domain

Setup sync between on-premise

Include option for Hybrid Exchange

Include SSO option

Setup SSO

Run on-premise Exch commands to sync permissions between on-premise and cloud

Set-OrganizationConfig -ACLableSyncedObjectEnabled $True

Create 2 test accounts. One for on-premise testing, the second to migrate to 365 Cloud for testing

Add all Exchange related accounts to "365sync" group or accounted for in other ways (duplicated in 365 EOL)

Users

Shared Mailbox

Contacts

Distribution groups

Dynamic Distribution Groups

On-premise need to add external email addresses

365 need to recreate groups and ensure external email addresses are included

Set Default domain within 365

Monitor and clear out any sync errors

Take documentation for rules, send connectors, receive connectors

Update RULES in Exchange Online 365 for:

Barracuda: '209.222.80.0/21' or '64.235.144.0/20'

Accent

Update 365 Security

https://security.microsoft.com/quarantinePolicies

https://protection.office.com/antispam

https://protection.office.com/antiphishing

Run Hybrid Configuration Wizard - Use correct link for download Run ELAVATED

Run from Exchange Shell before wizard to prevent MRP endpoint problems

Get-WebServicesVirtualDirectory | Set-WebServicesVirtualDirectory -MRSProxyEnabled $false

IISRESET

Get-WebServicesVirtualDirectory | Set-WebServicesVirtualDirectory -MRSProxyEnabled $true

IISRESET

https://aka.ms/hybridwizard

Update email address policy

Ensure all email address policy have '%domain%.mail.onmicrosoft.com' added

Run script to ensure all existing mailboxes that don't follow address policy get that email address

Add_SMTP_365_Proxy_Email.ps1

Duplicate related Exchange Rules from on-premise to 365

Update Firewall rules to allow secure connection between on-premise Exchange and MS 365 EOL/

https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

Purge all old Migration jobs

Get-MoveRequest | ? {$_.Status -eq "Completed"} | Remove-MoveRequest

Migrate test account to cloud

Test mail flow

External <-> 365 cloud

External <-> on-premise

365 clout <-> on-premise

Get full listing of mailboxes

Export On-Premise listing to CSV and provide to client with easy instructions on sorting purge/convert/keep

Once you get listing back strip down to just email address and header is "EmailAddress" for quick import to 365 Exchange

Migrate mailboxes

Check licensing

Be clear with client about expectations

Time

Outlook Problems

Mobile device setup

Outlook RULES

Update settings so that "Sent items" go to the correct mailbox for delegated items.

Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'SharedMailbox')} | set-mailbox -MessageCopyForSentAsEnabled $True

Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | set-mailbox -MessageCopyForSentAsEnabled $True

Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'SharedMailbox')} | set-mailbox -MessageCopyForSendOnBehalfEnabled $True

Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | set-mailbox -MessageCopyForSendOnBehalfEnabled $True

Update mail flow (MX records)

Update Autodiscover

Office 365 Exchange Hybrid Migration -Decom

Related Documents

https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps

https://docs.microsoft.com/en-us/exchange/permissions

Related commands

AD<->ADD sync

Start-ADSyncSyncCycle -PolicyType Delta

Office 365 Exchange Migration Cutover

0bf8fOnsJo05957fE7FBSnzPJEs3RXx0

PREPARATION:

1. See other document if Exchange Hybrid Migration is option
    1. 365 Exchange Hybrid Migration
2. MFA
3. Need to get login information for DNS and domains
4. Need to get login information for current email server
5. Work to get Office 365 account created for client
6. Start process to setup method of quick access to computers during cutover. AKA setup GPO for Automate.
7. Get listing of all current email accounts and provide to client to verify no unknown accounts they are unaware that will need to be migrated
8. Work with client to ID all devices where email is generated
    1. Outlook or similar desktop application
    2. Smartphones
    3. LOB applications that email
    4. MFD/Copier/Scanners that scan to email
9. Work with the client to ID all locations where email is generated (for SPF records)
    1. Current Exchange/email server location
    2. Office 365 SPF records
    3. If email is direct generated from LOB what is the public IP
    4. If email is direct generated from scanner/copier what is public IP
    5. If marketing email service is used, what IP need to be included for SPF
10. Link domains to Office 365
11. Increase licensing for Office 365 to appropriate number
12. Add user accounts to Office 365 and license
    1. AD Sync when possible
    2. Manual input when necessary
13. Ask client which personnel they want to have email on phone. Some companies do not want this.
14. Update SPF record to additionally include Office 365 SPF records

15. Review requirements for non-Outlook nor smartphone email processes
16. Create documents for email on phone
17. DNS TTL - Be aware and communicate the length of time it will take for changes
18. Once all is ready work with client to set expectations for process and schedule cutover

1. CUTOVER:
    1. Day Before: reduce TTL on all DNS records
    2. Day Before: Email all client personnel email on phone setup
    3. At designated time confirm with client that we are making change
        1. Client is not to email during this transition. This will reduce missed email during the process
    4. Update DNS and wait for TTL to expire. That way any transition email to the old server is captured.
    5. Update Internal AD Autodiscover location: Autodiscover Update
    6. Have full listing of users posted and coordinate which techs will address which users
    7. Outlook migration
        1. Remote to individual's computer
        2. Ensure all mail is downloaded. Verify it is not just caching recent messages, all message.

        3. Export entire mailbox to C:\Accent\PST (Ensure all aspects including contacts, calendar, email)
        4. Duplicate file(s)
        5. Create a new mail profile
        6. Import old email and allow to process
    8. LOB/MFD - update per individual specifications
2. Decommission
    1. Review what steps will be needed to properly decommission the old system
    2. Review and remove newly unused anti-spam and other related services.

OneDrive Grant Access

OneDrive Termination

When someone is NLE terminated we may grant a different user access to that person's OneDrive

SharePoint Admin Center -> More featuers -> User profiles -> Manage User Profiles -> %user% Find -> select then Manage site collection owners -> update Site Collection Administartors

OneDrive Redirection

Baseline settings for stock OneDrive Redirection GPO

Computer Configuration

- Policies
  - Administrative Templates
    OneDrive
    - Block file downloads when user are low on disk space
      - 1024
    - Limit the sync app upload rate to a percentage of throughput
      - 70
    - Prevent users from redirecting their Windows known folders to their PC
      - Enabled
    - Prompt user to move Windows known folder to OneDrive
      - **TENAT ID***
    - Silently sign in users to the OneDrive sync app
      - Enabled
    - Use OneDrive Files On-Demand
      - Enabled
    - Warn users who are low on disk space
      - Enabled 768

User Configuration

- Policies
  - Administrative Templates
    - Desktop
      - Prohibit User from manually redirecting Profile Folders
        - Disabled

- Baseline GPO that you have to update the TENAT ID on:

  OneDriveSettings

OneDrive Sync Issues

If problem is rooted in dual sync accounts

- If logged into wrong OneDrive, download all files
- Log out
  - Log out of OneDrive
  - Log out of TEAMS
  - Log out of all other Microsoft Office Suite
  - Remove all Microsoft references from Windows Credential Manager
- Uninstall/Reinstall OneDrive

  OneDriveInstaller
- Reset OneDrive
  - %localappdata%\Microsoft\OneDrive\onedrive.exe /reset
- DO NOT LOG INTO ONEDRIVE FIRST
- Log into a web browser to the SharePoint site needed. This will allow you to specify the credentials required better than using OneDrive
- Click SYNC from the SharePoint webpage
  - That will force the signed in credentials to be transferred to OneDrive to setup the sync and that will log into OneDrive with the desired credentials
- VERIFY. Open OneDrive -> Settings -> Account and verify client and account
- Log into all the applications
- VERIFY everything again.

[Yesterday 4:32 PM] Everett Whiteman

Tech Tribe -

A lot of onedrive/sharepoint related sync issues have been coming up. Here is a helpful command that 'resets' onedrive as a service and clears it all out to be a clean slate that has been incredibly

helpful for me over the years. You dont neve need to run it as admin.

" %localappdata%\Microsoft\OneDrive\onedrive.exe /reset "

Run this, reboot the computer, you'll be prompted for sign-on credentials once login process has been completed.

This will most definitely break a few things on Azure joined PCs as they rely on OneDrive for so much. Just sign-in if prompted post reboot and it will all restore.

(3 liked)

<
https://teams.microsoft.com/l/message/19:9e5338205405476fbc65b1f13fc97255@thread.skype/1655929975392?tenantId=b3505bee-dd8d-4d90-b885-6d94317f097c&groupId=5ded7d5e-2cba-4f62-a605-f2186d21fe47&parentMessageId=1655929975392&teamName=Tech Tribe&channelName=General&createdTime=1655929975392>

[8:02 AM] Keith Johnson

At the end of the day yesterday Everett and I was working on Byron's computer. He had prior setup his email address with the old WCXG 365 tenant and each time we logged out and tried to log back in it would default to the old tenant.

We logged out of all of his old tenant accounts (TEAMS/OneDrive). Then we went to the perfval.com SharePoint site and logged in through the web browser. That allowed us to select the new account. Once we hit sync it transferred that account information into OneDrive and everything appeared to sync up properly.

The best way to tell is to go into OneDrive settings and check the Account:

If it is the new OneDrive you will see "perfval". The old one pointed to a "wcxg" tenant.

One thing we missed initially and please don't make the same mistake:

Byron had his known personal folders synced with his old account. When we broke the sync, all the desktop, document and pictures that were synced, but not downloaded were no longer accessible.

Make sure you force download of all files first.

Couple this information with the reset command from Everett's post and we should be able to resolve these issues.

Desktop

Everett Whiteman

John Worthman

<
https://teams.microsoft.com/l/message/19:e6b1696d66514f00a0450c947160f29d@thread.skype/1655985734874?tenantId=b3505bee-dd8d-4d90-b885-6d94317f097c&groupId=5ded7d5e-2cba-4f62-a605-f2186d21fe47&parentMessageId=1655911062783&teamName=Tech Tribe&channelName=PerfVal&createdTime=1655985734874>

Outlook Credential Windows Disappears

If a User reports that their Outlook isn't updating and that it needs a password, but the credential window disappears right after opening, then follow these steps:

I recently solved this issue in our environment (Windows 10 Pro with an Office 365 email account) by clicking the Windows button--> clicking the gear icon (settings)--> Accounts --> Access work or School (list on left side)--> If you see your any account under here other than the AD account remove it. Next time you open Outlook it will prompt for the password (actually pop up the prompt). After you enter the password, Outlook is going to ask you if you want to join it to your Windows account. Say skip for now (as if you join it to Windows, eventually the issue will return). This is an issue with two Microsoft systems not playing well together, and Microsoft really needs to find a solution as I receive a support call for this issue at least a couple of times a week. Screenshot below:

Image
Image not found or type unknown

Image
Image not found or type unknown

From <https://answers.microsoft.com/en-us/msoffice/forum/all/my-outlook-says-need-password-when-i-click-it-it/4d7494f9-a7dd-4ce4-959c-e504f397d230?page=1>

Password WriteBack

1. Setup Self Service Password Reset (SSPR)
    1. SSPR
    2. Requires P1 or P2 Microsoft licensing
2. Azure Active Directory -> Password Reset -> On-premises integration
    1. Enable password write back for synced users
    2. Allow user to unlock accounts without resetting their password?

    Screenshot of how to manage settings password writeback.
    
3. Enable Password Writeback on AD Connect

Configure Azure AD Connect for password writeback


PowerShell Add to Global Admin

Today I was working on adding all the new admin accounts we made for a client to the Global Admin Role for Microsoft 365 as part of the onboarding process. Prior I had added the accounts in the local AD accounts using PowerShell and set them to sync with AD Connect. We have a lot of admin accounts we are making and adding them one-by-one via GUI was not something I wanted to do anymore.

#I opened up PowerShell ISE on my local computer

#Connected to MS 365 for this client using a Global Admin account

```
Connect-AzureAD
```

#There are 2 variabled I needed for this command. The first is the ObjectID of the Global Admin group

```
Get-AzureADDirectoryRole | Where DisplayName -like "GL*" |  Select DisplayName, ObjectID
```

#copy out the Object ID

#The second is the ID of the user accounts you want. I used this command to narrow it down to just the names I was looking for

```
Get-AzureADUser | Where DisplayName -like "Admin*" | FT DisplayName, objectID

#the ObjectID for the user is the RefObjectID in the below commands



#The ObjectID of the role is the first ID. The second is the user ID.

Add-AzureADDirectoryRoleMember -ObjectId 2391f956-f330-4f76-854a-e57687457f54 -RefObjectId c354800b-db6b-46c3-a704-0f03da294b5b

Add-AzureADDirectoryRoleMember -ObjectId 2391f956-f330-4f76-854a-e57687457f54 -RefObjectId 3b9e26a9-b46c-43fb-8ed0-e9634f572f82
```

routable domain

Real world use. Updated Remington Seeds from RHSC.local to remingtonseeds.com for alternate domain name for their users so they sync properly.

Update the OU for the specific OU of the personnel you want to update.

All domestic:

$ou = "OU=RHSC,DC=RHSC,DC=local"

All International:

$ou = "OU=RSI,DC=RHSC,DC=local"

Script saved at:

RHSC-00-VSRV18\C:\Accent\Scripts\UpdateAlternateDomain.ps1

Import-Module ActiveDirectory

$oldSuffix = "RHSC.local"

$newSuffix = "remingtonseeds.com"

$ou = "OU=RHSC,DC=RHSC,DC=local"

$server = "RHSC-00-VSRV18"

Get-ADUser -SearchBase $ou -filter * | ForEach-Object {

$newUpn = $_.UserPrincipalName.Replace($oldSuffix,$newSuffix)

$_ | Set-ADUser -server $server -UserPrincipalName $newUpn

}

$env:USERDNSDOMAIN

$env:LOGONSERVER

NOTE: domain is case sensitive

Prepare a non-routable domain for directory synchronization

- 02/19/2019
- 3 minutes to read
- Contributors

When you synchronize your on-premises directory with Office 365 you have to have a verified domain in Azure Active Directory. Only the User Principal Names (UPN) that are associated with the on-premises domain are synchronized. However, any UPN that contains an non-routable domain, for example .local (like billa@contoso.local), will be synchronized to an .onmicrosoft.com domain (like billa@contoso.onmicrosoft.com).

If you currently use a .local domain for your user accounts in Active Directory it's recommended that you change them to use a verified domain (like billa@contoso.com) in order to properly sync with your Office 365 domain.

What if I only have a .local on-premises domain?

The most recent tool you can use for synchronizing your Active Directory to Azure Active Directory is named Azure AD Connect. For more information, see Integrating your on-premises identities with Azure Active Directory.

Azure AD Connect synchronizes your users' UPN and password so that users can sign in with the same credentials they use on-premises. However, Azure AD Connect only synchronizes users to domains that are verified by Office 365. This means that the domain also is verified by Azure Active Directory because Office 365 identities are managed by Azure Active Directory. In other words, the domain has to be a valid Internet domain (for example, .com, .org, .net, .us, etc.). If your internal

Active Directory only uses a non-routable domain (for example, .local), this can't possibly match the verified domain you have on Office 365. You can fix this issue by either changing your primary domain in your on premises Active Directory, or by adding one or more UPN suffixes.

Change your primary domain

Change your primary domain to a domain you have verified in Office 365, for example, contoso.com. Every user that has the domain contoso.local is then updated to contoso.com. For instructions, see How Domain Rename Works. This is a very involved process, however, and an easier solution is to Add UPN suffixes and update your users to them, as shown in the following section.

Add UPN suffixes and update your users to them

You can solve the .local problem by registering new UPN suffix or suffixes in Active Directory to match the domain (or domains) you verified in Office 365. After you register the new suffix, you update the user UPNs to replace the .local with the new domain name for example so that a user account looks like billa@contoso.com.

After you have updated the UPNs to use the verified domain,you are ready to synchronize your on-premises Active Directory with Office 365.

Step 1: Add the new UPN suffix

1. On the server that Active Directory Domain Services (AD DS) runs on, in the Server Manager choose Tools > Active Directory Domains and Trusts.
   Or, if you don't have Windows Server 2012
   Press Windows key + R to open the Run dialog, and then type in Domain.msc, and then choose OK.
2. On the Active Directory Domains and Trusts window, right-click Active Directory Domains and Trusts, and then choose Properties.
3. On the UPN Suffixes tab, in the Alternative UPN Suffixes box, type your new UPN suffix or suffixes, and then choose Add > Apply.

Choose OK when you're done adding suffixes.

Step 2: Change the UPN suffix for existing users

1. On the server that Active Directory Domain Services (AD DS) runs on, in the Server Manager choose Tools > Active Directory Active Directory Users and Computers.
   Or, if you don't have Windows Server 2012
   Press Windows key + R to open the Run dialog, and then type in Dsa.msc, and then click OK
2. Select a user, right-click, and then choose Properties.

3. On the Account tab, in the UPN suffix drop-down list, choose the new UPN suffix, and then choose OK.
4. Complete these steps for every user.

   Alternately you can bulk update the UPN suffixes You can also use Windows PowerShell to change the UPN suffix for all users.

You can also use Windows PowerShell to change the UPN suffix for all users

If you have a lot of users to update, it is easier to use Windows PowerShell. The following example uses the cmdlets Get-ADUser and Set-ADUser to change all contoso.local suffixes to contoso.com.

Run the following Windows PowerShell commands to update all contoso.local suffixes to contoso.com:

Copy

```
$LocalUsers = Get-ADUser -Filter {UserPrincipalName -like '*contoso.local'} -Properties userPrincipalName -ResultSetSize $null
```

Copy

```
$LocalUsers | foreach {$newUpn = $_.UserPrincipalName.Replace("contoso.local","contoso.com"); $_ | Set-ADUser -UserPrincipalName $newUpn}
```

See Active Directory Windows PowerShell module to learn more about using Windows PowerShell in Active Directory.

From <https://docs.microsoft.com/en-us/office365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization>

SSO

Setting up Microsoft Azure/365 to an existing AD can be eased by implementing SSO between the systems

Setup sync w/ AD/AAD

- The Seamless SSO box has to be checked in AD Connect
- GPO (we can temple with Accent)
  - The Azure AD URL has to be added to the users intranet zone settings via Group Policy or manually
  - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start
  - GPO Settings:
    - User Configuration -> Policies -> administrative Templates -> Windows components -> Internet Control Panet -> Security page -> Intranet Zone
      - Allow updates to status bar via script - Enabled
        - Status bar updates via script - Enabled
    - User Configuration -> Preferences -> Windows Settings -> Registry
      - New Registry item
        - Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\microsoftazuread-sso.com\autologon
        - Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\microsoftonline.com\login\device
        - Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\microsoftonline.com\login
        - Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\sharepoint.com\accentconsultingservices
        -
        - Machine generated alternative text:https Properties General Common Action: Key Pa
- Users have to be logging in with their email to their computer so it matches the 365 account.

You can import the baseline settings and then update the GPO from:

Azure SSO - Trusted Zones

SSPR

Self Service Password Reset

Requires P1 or P2 MS Licensing

Azure Active Directory -> Password Reset -> Properties

If Hybrid Sync need to setup Password Writeback

Troubleshoot Missing Emails

- Login to Office365 portal as administrative user.
- Click on Admin

Machine generated alternative text:Admin

- Click on "... Show All"

Machine generated alternative text:Microsoft 365 admin center Home Users Groups Billing Customiz

- Click on Security & Compliance

Machine generated alternative text:Microsoft 365 admin center Home Users Groups Roles Resource

- Click through the following

1. Mail Flow
2. Message Trace
3. The Down arrow next to "Default Queries"
4. "Messages received by my primary domain in the last day"

- Fill out the necessary information to try and locate the emails and click search.
  - If you see the messages here it will give you a status of them.
  - If you do not see the message here it is a decent indication that it was:
    1. Blocked by a spam filter before reaching O365 (via Barracuda or other service)
    2. Blocked by a server on the sender's side.