

# Microsoft Office 365 Courseware

Version 4.2



# 70-346 Identities and Requirements

## Office 365 Setup, ADFS and DirSync

To setup Office 365:

- Setup an Office 365 plan
- Configure the Global Administrator account recovery information
- · Configure the custom domain and DNS

An Office 365 E3 Trial has 25 licenses

To add a custom domain to Office 365 the first thing you need to do is add the custom domain and verify it.

Create a new custom domain in Office 365 using Power Shell:

- Install Windows Azure Active Directory module for Windows Power Shell
- Connect to Office 365
- · Run New-MsolDomain
- Get-MsolDomainVerificationDns
- · Conform-MsolDomain
- Set-MsolDomain

To use Windows Power Shell to manage Office 365, you need to download the Microsoft Online Services Sign-In Assistant first.

To give an external user just access to SharePoint and Office Web Apps Only when you do not want to use existing E3 licenses

- Sign in to the Office 365 Admin center
- Select the purchase Option
- Add the Office Web App with the SharePoint (Plan 1)
- · Select the users and groups option
- · Assign license to user

The prerequisites for the Azure Active Directory module for Windows Power Shell installed on Server 2012 are:

- Microsoft Online Services Sign-In Assistant
- · Microsoft .Net Framework 3.5
- Windows Azure Active Directory module for Windows Power Shell

#### DirSync Requirements:

- Microsoft .Net Framework 3.5 SP1 and Microsoft .Net Framework 4.0
- A member server running 2008 or 2012
- Forest functional level of 2003

If you have 2 servers in you network, one is domain joined the other one isn't and you want to deploy DirSync:

- Activate user synchronization in Office 365
- · Install Windows Azure Active Directory Sync on the domain joined computer
- · Activate synchronized users



The following three filtering configuration types can be applied to the Directory Synchronization tool:

- Organizational-unit (OU)-based: You can use this filtering type to manage the properties
  of the SourceAD Management Agent in the Directory Synchronization tool. This filtering
  type enables you to select which OUs are allowed to synchronize to the cloud.
- Domain-based: You can use this filtering type to manage the properties of the SourceAD
  Management Agent in the directory synchronization tool. This type enables you to select
  which domains are allowed to synchronize to the cloud
- User-attribute-based: You can use this filtering method to specify attribute-based filters
  for user objects. This enables you to control which objects should not be synchronized to
  the cloud.

When User synchronization is used all users' information such as department etc. must be maintained in the on premise Active Directory. The only exception is the mobile number.

FIM is used to assign filters to Azure Active Directory Sync. To exclude users from being synced use FIM:

- Populate an attribute in Active Directory, cause you need a filter argument
- Configure a filter based on that attribute
- Perform a full synchronization

If Azure Active Directory Sync is not used to create accounts in Office 365 and you still want to use a bulk import mechanism to create users in the cloud export the users from your on premises Active Directory and then create a Power Shell script.

After deploying ADFS; tenant password policies are handled by the local Active Directory Environment and note Office 365. So even if you got 2 different password policies all the users will be synched by Azure Active Directory Sync.

To only sync the some users with a routable UPN suffix <u>firebrand.com</u> to Office 365 using DirSync:

- Add firebrand.com UPN suffix using Active Directory Domains and Trusts
- Use Active Directory Users and Computers to change the UPN for the users
- Use a user attribute- based filter to exclude all the firebrand.local users

The required roles for the AD FS Proxy Server are:

- Web Server (IIS)
- AD FS Role

To deploy ADFS server farm on Server 2012:

- Install the Active Directory Federation Service server role
- Use the AD FS Federation Server Configuration Wizard to configure the first server and the farm
- Use the AD FS Federation Server Configuration Wizard to add the second server

To deploy ADFS on server 2008

- Install .Net Framework 3.5 with SP1
- Install ADFS 2.0 (ADFS RTW)
- Install Rollup 3 for AD FS 2.0
- · Configure trust between the 2 environments



To prepare the domain <u>firebrand.com</u> for ADFS, you need at least to deploy one Federation Server. Then configure the local Active Directory to use the UPN <u>firebrand.com</u> and create a server authentication certificate for the federation server using <u>firebrand.com</u> in the subject and subject alternative name field.

You need two certificates for ADFS:

- Secure Socket Layer (SSL)
- Token Signing

The ADFS Proxy Server uses port 443 to communicate with the ADFS Server.

The minimum amount of servers you need to deploy high available ADFS infrastructure is four. We use 2 servers for the Federation Server and 2 for the Federation Proxy Server.

The basic steps to deploy ADFS are:

Deploy a federation server farm

Run the Windows Power Shell cmdlet Convert-MsolDomaintoFederated to active ADFS For this domain.

Given the following scenario when you deploy ADFS

Cluster DNS Name
Server node in cluster

You need to add the cluster FQDN fs.firebrand.com in the subject name for the certificate.

If you are getting an Error 393 during ADFS Deployment you should reenter the credentials to establish the trust.

Change ADFS Service Account Password:

- Logon to each Federation Server
- Modify the application pool identity by using the IIS manager
- Modify the Services Account for in the Services MMC-Snapin

The ADFS Server Website can get your corporate branding. There are the important sites to modify:

Change the overall appearance for all pages

Authenticate users

Change the list of trusted claims providers that are displayed

MasterPage.master

IdpInitiatedSignOn.apsx

HomeRealmDiscovery.aspx

When you deploy two federation proxy servers in the DMZ, it is required to add the cluster DNS name and IP addresses of the federation server to the hosts file.

#### DNS Record examples:

Helps prevent outbound email messages from being flagged as SPAM
Configures email message routing
Outlook autodiscover record is used to help user to configure client

TXT

MX

CNAME

Create the correct record for SharePoint public facing website you need to create another subdomain record, for example <a href="www.firebrand.com">www.firebrand.com</a>. When it is verified you need to create the DNS Record

**CNAME** <u>www.firebrand.com</u> <u>firebrand-public.sharepoint.com</u>

The DNS Record to verify the domain is mainly the TXT record. If your provider doesn't support TXT records you can use the MX record as well.



## User Administration, Rights Management and Monitoring

If you want to create an Office 365 user account using Powershell the only arguments for New-MSOLUser you need is the UPN and the DisplayName.

The user location settings are defining, what features a user can have in Office 365.

Get-MSOLUser can be used to identify users who do not have an Exchange Online license.

The longest time in days before the password expires is 730 days and the days before the user gets notified is 30 days.

To determine if a company is ready to use Office 365 you can use the OnRamp for Office 365 tool.

Admin Role Examples:

Reset users password of other administrators
Perform purchasing operations
Create and manage user views

Open Tickets and Communicate with Customer Service S

Global Administrator Billing Administrator

User Management Administrator

Service Administrator

Only the global administrator can change passwords for others administrators.

To view the service health and maintenance reports of the past seven days you can use the Service Health Page in the Office 365 Admin Center or subscribe to the RSS Notification Feed.

You can use System Center Operations Manager with the Office 365 Management Pack and a Watcher Node PC to configure notification if Microsoft plans a Maintenance for Office 365.

You can use the Remote Connectivity Analyzer to verify your external Lync and Exchange Settings too.

This is an example from the Office 365 services Window.

SERVICE	TODAY	NOV 13
Exchange Online 💂	0	0
Identity Service 🕶	~	4
Lync Online 🕶	~	~
Office 365 Portal 🕶	~	4
Office Subscription 🔻	· ·	~
Rights Management Service	*	~
SharePoint Online 🕶	0	0
Yammer Enterprise	~	~

Right here, SharePoint is available and Exchange is degraded. The earliest date that a post incident review will be available for SharePoint Online is November 13th.

To configure Active Directory Rights Management run:

- Import-Module Aadrm
- · Connect-AadrmService
- Enable-Aadrm



You need to modify the users and groups who are authorized to administer the Rights Management service.

- Import-Module Aadrm
- Connect-AadrmService
- Enable-Aadrm
- Remove-AadrmRoleBasedAdministrator

To get the Administration Logs for Active Directory Rights Management:

- · Import-Module Aadrm
- · Connect-Aadrm
- Get-AadrmAdminLog

To decrypt the files secured with the rights management service with 3rd Party

- Import-Module Aadrm
- · Connect-AadrmService
- Enable-Aadrm
- Enable-AadrmSuperUserFeature

With Enable-AadrmSuperUserFeature you can activate the Super User function in Active Directory Rights Management. This is not enabled by default. If it is turned on you can configure who is authorized to decrypt the files secured with the rights management service.

Add-AadrmAdministrator and Remove-AadrmRoleBasedAdministrator defines administrators for the Aadrm Service.

## Exchange Online / Multifactor

To analyze the trends for email messages received over the past 60 days and get SPAM statistics use the Mail Protection Reports

The prerequisites to view the Online Protection Reports for Exchange Online are:

- .Net Framework 4.5
- Microsoft Excel 2013

To get all the features in Exchange Online you need to create the following records:

- CNAME
- MX

If you want to grant the permissions to a user to monitor Exchange Online Services in Office 365, assign the Service Administrator role and grant this user administrative permissions in Exchange Online. You need to do these two steps as a signed in Global Admin Account.

To troubleshoot Exchange Online and Exchange on premise problems for example if a user can not see free / buys information of other users, use the Remote Connectivity Analyzer with Office 365 tab selected.

The Role Assignment Policy can be used to prevent the user to change his display name by using Outlook Web App.

To track the sending of confidential information you can use DLP Policies. To get a report of any sent mail matching a DLP look for the:

- · Rule matches for sent mail
- DLP Policy matches for sent mail



To control, who can sent emails to a distribution group in Exchange Online, create a distribution group and configure mail flow settings.

To deploy MFA for mobile users:

- Enable multi-factor authentication for the user
- Instruct the user to use a mobile phone to complete the registration
- Instruct User 1 to create an app password

#### Basic steps to deploy MFA

- · Enable multi-factor authentication for the user
- Instruct the user to use a mobile phone to complete the registration
- Instruct users to obtain a single-use password to complete the registration process

Use an IP whitelist to exempt internal IP addresses if you are deploying ADFS and multi factor authentication.

You implement single sign-on (SSO) with Office 365 by using Active Directory Federation Services (AD FS). You need to implement Windows Azure multi-factor authentication.

- On the AD FS federation server, run PhoneFactorAgentSetup.exe.
- On the AD FS Federation server, run WindowsAzureSDK-x64.exe.
- On the AD FS Federation server, run the Windows PowerShell cmdlet Register-AdfsAuthenticationProvider.

# Lync Online

Port Ranges for Lync Online:

443 TCP Audio, video, and application sharing sessions

 5223 TCP
 Lync Mobile

 50000 - 50019 UDP
 Audio Sessions

 50020 - 50039 UDP
 Video Sessions

 50040 - 50059 UDP
 Application Sharing

The Lync Bandwidth Analyzer can be used to estimate the post migration network traffic of Lync Online.

If you are migrating SIP Domains to Lync Online, don't forget that you must have a public routed domain suffix. For Example a lot of companies are using mycompany.local. A .local suffix is at the moment a nonpublic routed DNS Suffix. So suffixes such as firebrand.local or a Netbios Name such as firebrand cannot be migrated.

#### Client Installation

General Port:

SMTP Relay TCP 587 Office 365 Admin Center TCP 443

If a user is not connecting to Microsoft Office 365 once within 30 days, Microsoft Office goes to limited functionality mode. To get the whole functionality again, Install the recent Microsoft Online Sign In Assistant and verify the users license.

If rendition tags are not working in Outlook, instruct the user to recreate his Outlook profile.



## Power Shell examples during the course

#### Bulk remove all unlicensed users:

Get-MsolUser -UnlicensedUsersOnly | Remove-MsolUser -Force

#### **Disabled Password expiration**

Set-MsolUser -UserPrincipalName test01@mcsauk.onmicrosoft.com -PasswordNeverExpires 1

#### **Deactivate Directory Synchronization**

Set-MsolDirSyncEnabled 0

#### Set password for one user and force to change when next login

Set-MsolUserPassword -UserPrincipalName test01@mcsauk.onmicrosoft.com

#### **Bulk Disabled password expiration**

Import-Module -MsOnline \$Cred = Get-Credential Connect-MsolServer -cred \$cred Get-MsolUSer | Set-MsolUser -PassWordNeverExpires \$true

#### Disable SharePoint License for users from the DEV department

\$license = New-MsolLicenseOptions -AccountSkuID "Training:ENTERPRISEPACK"
-DisabledPlans SHAREPOINTSTANDARD
Get-MsolUser -MsolUser -All -Department "DEV" | Set-MsolUserLicense -LicenseOptions \$license



# 70-347 Enabling Office 365 Services

# Lync Online / Exchange Online Lync Config

To allow Lync federation only with a list of domains in Lync Online.

- In the Lync Admin Center set External Access to the option On only for allowed domains
- Add the domains to the Blocked or Allow Domains List

The Lync Basic Client requires an E1 license instead of an E3.

To customize the Lync 2010 client use the communicator.adm file

To deny a user to chat with external users in Lync online, go to the external communication settings of this user and clear people on Public IM.

You can archive Lync traffic, bust juste IM and conference IM traffic. So you can archive:

- · Multiparty instant messages
- Audio and video for peer-to-peer chat traffic
- content upload activities in meetings

Set-CsPushNotificationConfiguration configures Lync Push Notification for mobile phones.

#### Exchange Migration scenarios overview

Existing organization	Number of mailboxes to migrate	Do you want to manage user accounts in your on- premises organization?	Migration type
Exchange 2013, Exchange 2010, Exchange 2007, or Exchange 2003	Less than 2,000 mailboxes	No	Cutover Exchange migration
Exchange 2007 or Exchange 2003	Less than 2,000 mailboxes	No	Staged Exchange migration
Exchange 2007 or Exchange 2003	More than 2,000 mailboxes	Yes	Staged Exchange migration or remote move migration in an Exchange hybrid deployment
Exchange 2013 or Exchange 2010	More than 2,000 mailboxes	Yes	Remote move migration in an Exchange hybrid deployment
Exchange 2000 Server or earlier versions	No maximum	Yes	IMAP migration
Non-Exchange on- premises messaging system	No maximum	Yes	IMAP migration

The Exchange Server Deployment Assistant helps you when you are migrating from on Premises to the cloud. He can generate a custom step-by-step checklist for multiple migration types.



The company has the following migration requirements:

- During the migration, do not change the existing Microsoft Outlook profiles and .ost files used by the employees.
- Ensure that email messages sent between on-premises mailboxes and online mailboxes during the migration are secure.
- Do not send email messages between on-premises mailboxes and online mailboxes over the Internet in plain text.

The best migration for the scenario above is **Remote Move**, because one of the requirements is that the transfer is secured.

If you do not want to migrate contacts, custom folders etc., you can use the **IMAP migration**.

You see free / busy information during the following Exchange migrations

• Remote Move

You will not see him in the following migrations

- IMAP
- Cutover
- Staged

#### Migration Examples

Exchange 2010 SP3 15000 users using Replication Remote Move Non Exchange System IMAP

#### Exchange protection

You can sent a notification to employees if they sent mails with confidential information. This can be configured with a Data Loss Prevention policy. You can use eSearch to look for mails of the kind and the people in the discovery management group can perform searches.

Active Sync can be used if you want to ensure that employees can access their Microsoft Exchange content offline.

The NDR backscatter SPAM setting is preventing you from experiencing an NDR bounce.

To accomplish that message from a domain or server from a datacenter bypass your spam:

- Create a connection filter to allow the data center IP address range
- Configure a mail flow rule to bypass spam filtering for the fabrikam.com domain

#### SPAM Protection examples:

Filter messages based on language Content Filter International SPAM Filter based on country and region Content Filter International SPAM

To turn on these features on for your Exchange Online

- Reverse DNS lookup
- Sender open proxy test
- HELO/EHLO analysis
- Analysis of spam confidence level (SCL) ratings on email messages from a specific sender use

Set-SenderReputationConfig -ExternalMailEnabled \$true -InternalMailEnabled \$true



#### **Exchange Objects**

External user with no access to Office 365. He must appear in the GAL External user with access to Office 365. He must appear in the GAL Any department member must be able to open the mailbox and reply to mail Messages sent to that recipient must be sent to every member.

Mail Contact Mail User SharedMailbox Distribution Group

Exchange Admin Roles Overview:

Place Mailbox in Litigation Hold Discovery Management

Create Retention Tags Record Management

Create and Manage Resource Mailbox Recipient Management

Update User Display names Help Desk

Create and Manage Security Groups Organization Management

#### Additional Exchange configuration

To disable contact synchronization for mobile devices configure the email, calendar and contacts and the mobile access section in the services window.

To control the ActiveSync password Policy and the control of the presence information configure the IM, meetings and conferencing section and the mobile access options in the services window.

You need to add the label "External" to the subject line of each email message received by your organization from an external sender from the Exchange Control Panel, run the New Rule wizard.

To delete a mailbox when directory synchronization is activated, delete his on premises account.

With Set-Mailbox –LitigationHoldEnabled you can configure that's emails are accessible to members of the audit department for 60 days, even if Test5 permanently deletes the messages.

# Office 2013 Client Deployment

#### **Telemetry**

If you want to get usage data from different Office versions on different system and you are using telemetry. The only thing you need to do is use the different platforms to get data for the statistics.

Telemetry processor should be installed on a server operating system for production environments.

Collecting data from more than 20 clients, Telemetry processor must be run on an Windows Server.

In the telemetry dashboard you are getting the document name, title and path of the Office documents.

To disguise file names and document titles, obfuscate the document name, title, and path in the Telemetry Dashboard.

Information collected by telemetry:

- The names of add-ins and solutions interacting with Microsoft Office
- The file names of Office files that are in the Most Recently Used list
- System information such as user name and computer name



You need to enable telemetry and immediately trigger data collection.

- Modify AgentInitWait and AgentRandomDelay in the registry
- Configure Group Policy and turn on telemetry in the user options

https://technet.microsoft.com/en-us/library/jj591589.aspx

#### Install Office

When you are receiving the error "Windows cannot find 'C:\Program Files\Microsoft Office 15 \clientX64\integratedOffice.exe' manually remove any previous installation of Office and clean the registry sub keys.

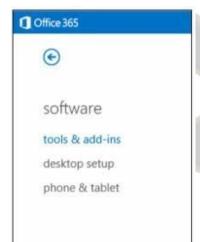
When you are using 32 and 64 Bit Versions and you are experiencing problems with add-ins or Share Point Data sheet views, try to use just the 32 Bit version to check for architecture problems.

A user has a new notebook and wants to user his existing Office2013 ProPlus version.

Go to Office 365 and deactivate the old notebook, because in total one Office 365 License allows 5 simultaneously client activations.

A Microsoft Surface is a normal client and requires a license for Office 365. If a user can't work with a surface, instruct the user to login and deactivate unused clients.

If a user's Software tab in Office 365 looks like this:



Assign an Office 365 ProPlus license to the user.

To install Office 365 on a local computer you must have Global Admin rights and the minimum connection frequency to the Internet is 30 days.

The Office installation can be automated. The answer file has the name configuration.xml. There is an example which silently installs office

configuration.xml:

< Display Level="None" AcceptEULA=,,TRUE/>

Syntax for running a custom install:

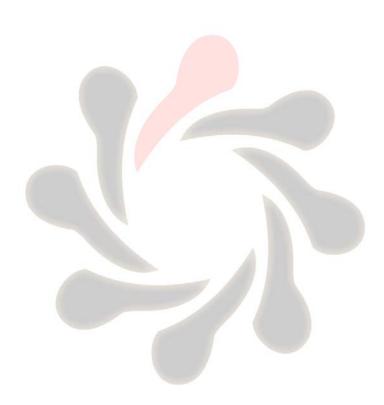
\\filesvr\office\setup.exe /configure \\filesvr\office\configuration.xml

Syntax for running a click to run:

\\filesvr\office\setup.exe /download \\filesvr\office\configuration.xml



The lowest version which can be used for Office 365 is on the client side Windows 7 SP1. Office 2010 is not working anymore.





#### SharePoint 2013

Microsoft Yammer is a Social Media Add on for Office 365.

When any user must be able to post an event, to join groups and receive project updates, use **Yammer**.

To provide access to the public facing Share Point Website you first have to create a new domain with the defined purpose Share Point online.

You only can create one public facing website URL. Anyway if you want to have 2 public facing websites, you can work with a redirect in order to get this done.

Only the Global Administrator can create Site Collections

To add another person as Global Administrator

- Sign in as a Global Administrator
- From the SharePoint admin center select the correct site collection
- Add the person as a site collection administrator

Contributors can edit content inside of SharePoint site collections.

If you have content and you want to share this content to external users so can edit the content without affecting your existing security,

- create a new site collection
- add the content,
- share it
- add the external people to the contributors group.

Inside a Share Point library change the require documents to be checked out before they can be edited to no to enable the coauthoring feature.

If you want to provide external users the possibility to add content to a site collection in SharePoint 2013 Online, create a new site use the external invite feature and add them to the contributors group.

To revoke access to an external shared document

- Open the SharePoint library that contains the shared document
- Display the Site Settings page
- · Click on Access requests and invitations
- Point to the user and click the associated Open Menu button
- In the properties window, click Withdraw

Change Permissions for external users for a document inside a document library

- Open the SharePoint library that contains the shared document
- Display the Site Settings page
- Click on Access requests and invitations
- Point to the user and click the associated Open Menu button
- In the permissions list chose the new permission
- Click Resend

Remove external users with PowerShell

- Open the SharePoint Online Management Shell
- Connect to the Admin Center using Connect-SPOService
- Remove the external users with Remove-SPOExternalUser

Only 32-bit Version of Office supports the **Datasheet view** in the SharePoint lists.



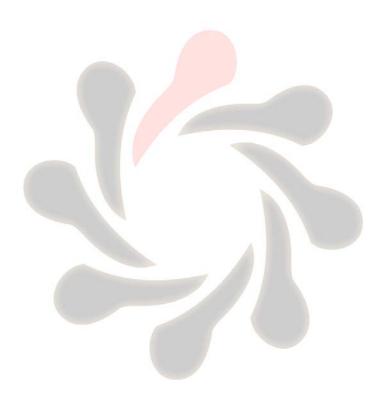
# Office 365 ADFS

You can use the AD FS 2.0 Management Console to identify which certificate is used for token signing between the on premises environment and Office 365.

To verify the functionality of ADFS 2.0 open Internet Explorer and browse to: <a href="https://adfs.firebrand.com/adfs/fs/federationserverservice.asmx">https://adfs.firebrand.com/adfs/fs/federationserverservice.asmx</a>

To change the authentication mechanism from Windows to Forms, modify the Web.config file in the %systemroot%\inetpub\adfs\fs directory

After the installation of Azure Active Directory Synchronization the miisclient can be used to troubleshoot directory synchronization.





# Power Shell examples during the course SharePoint

#### To create a SharePoint Site with the following parameters:

Site name <a href="https://firebrand.sharepoint.com/site/hr">https://firebrand.sharepoint.com/site/hr</a>
Site Collection Administrator <a href="user1@firebrand.com">user1@firebrand.com</a>
Storage Quota 1000
Resource Quota 300
Title HR

Open SharePoint Management Shell

 $Run\ Connect-SPOService\ \underline{https://firebrand-admin.sharepoint.com}\ -credential\ admin@firebrand.com$ 

Run New-SPOSite -Url <a href="https://firebrand.sharepoint.com/sites/hr">https://firebrand.sharepoint.com/sites/hr</a> -Owner <a href="mailto:user1@firebrand.com">user1@firebrand.com</a> StorageQuota 1000 -ResourceQuota 300 -Title HR

#### **Create a French SharePoint Site:**

New-SPOSite -Url https://firebrand.sharepoint.com/sites/paris -Owner administrator@firebrand.com -StorageQuota 1000 -template STS#0 -LocaleId 1036

#### Exchange

#### Add email addresses for all employees

```
$mailboxes = Get-Mailbox
foreach ($mailbox in $mailboxes)
{
$newadress = $mailbox.alias + "@contoso.com"; $mailbox.EmailAdresses += $newadress
Set-Mailbox -Identity $mailbox.alias -EmailAdresses $mailbox.EmailAdresses
}
```

#### Creating a shared mailbox and granting SendAs permissions

New-Mailbox -Shared -Name "Support" -Alias "Support" -PrimarySmtpAddress support@firebrand.com

Add-RecipientPermission -Identity "Support" -AccessRights SendAs -Trustee student@firebrand.com

#### Overview about ActiveSync enabled users and their devices

Get-CASMailbox -Filter ,{HasActiveSyncDevicePartnership -eq \$True }" \$ActiveSyncUsers | Select-Object DisplayName,@Name="Device"; Expression={(Get-ActiveSyncDevice -Mailbox \$ .ldentity).DeviceType\}}

#### **Enable Litigation Hold**

Set-Mailbox -Identity "test01" -LitigationHoldEnabled 1

#### **Activate Archiving**

Get-Mailbox –resultsize unlimited –filter {(RecipientTypeDetails –eq 'UserMailbox')} | Enable-Mailbox -Archive

#### Create and apply a retention policy with one Tag

New-RetentionPolicy Policy-90

New-RetentionPolicyTag Tag-90 –Type DeletedItems –RetentionEnabled \$true –AgeLimitFor Retention 90 –RetentionAction DeleteAndAllowRecovery Set-RetentionPolicy Policy-90 –RetentionPolicyTagLinks Tag-90 Get-Mailbox | Set-Mailbox –RetentionPolicy Policy-90



# Apply a new retention policy to all archive mailboxes and ensure that the new retention policy tags are applied as soon as possible.

\$users = Get-Mailbox -ResultsSize unlimited -Filter{(ArchiveStatus -eq ,,Active")}

\$users | ForEach-Object {Set-Mailbox \$\_.Identity -RetentionPolicy1"}

\$users | ForEach-Object {Start-MangagedFolderAssistant -Identity \$\_.Identity}

#### Remove a retention policy from all mailboxes.

\$UserMailboxes = Get-Mailbox -Filter {(RecipientTypeDetails -eq "UserMailbox")} \$UserMailboxes | SetMailbox -RetentionPolicy \$null

#### Modify a policy tag to increase the retention age for deleted email items to 90 days.

Set-RetentionPolicyTag "deleted items" -AgeLimitForRetention 90

#### **Creating Contacts based on CSV**

Import-CSV .\ExternalContacts.csv |%(New-MailContact -Name \$.\_Name -ExternalEmailAddress \$\_.ExternalEmailAddress -FirstName \$\_.Firstname -Lastname \$\_.LastName )

#### Add secondary mail address

Set-Mailbox -Identity <u>user@firebrand.com</u> -EmailAddresses <u>user@firebrand.com</u>", "alias@firebrand.com"

#### Add secondary mail address as new reply address

Set-Mailbox -Identity <u>user@training.onmicrosoft.com</u> -WindowsEmailAddress user@firebrandtraining.com

#### Lync

# To complete the process of updating the employee's Lync address without affecting any other addresses.

You have

- \$ID=User1@contoso.com
- \$OldAddress = SIP:User1@contoso.com
- \$NewAddress = SIP:User1-Sales@contoso.com

use

Set-Mailbox -Identity \$ID -EmailAddresses@{add = "\$NewAddress"; remove = "\$Old Address"}

#### **PSTN** callers can bypass the Lobby

Get-CsMeetingConfiguration | where-object { \$.\_AdmitAnonymousUsersbyDefault –eq \$false} | Set-CsMeetingConfiguration –PstnCallersBypassLobby \$true

#### Add Legal URL

Set-CsMeetingConfiguration –LegalUrl "<u>www.fb.com/disclaimer.html</u>" -CustomFooterText "This meeting may be recorded"

#### List all SIP addresses

Get-Mailbox -ResultSize Unlimited | Select-Object –ExpandProperty EmailAddresses |where-object {\$\_-match "SIP"}

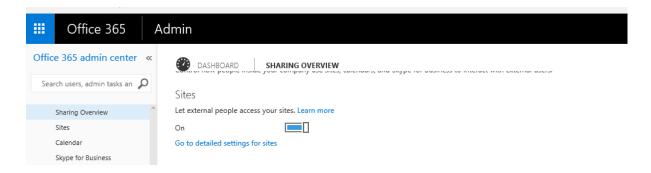


# Microsoft Office 365 Extra Material

# Contents

SharePoint External Sharing	2
SharePoint PowerShell Example	12
Exchange Online PowerShell Example	13
Exchange Migration Flow Chart	15
Azure AD PowerShell Examples	15

#### SharePoint External Sharing



You can configure external sharing at two levels within the SharePoint admin centre:

- 1. You can turn external sharing on or off globally for an entire SharePoint Online environment (or tenant). Additionally, if you turn on external sharing, you can specify if you want to allow sharing only with authenticated users, or if you want to allow users to share content with both authenticated users and anonymous users through guest links.
- 2. You can turn external sharing on or off for individual site collections. This provides you with the ability to secure content on specific site collections that you do not want to be shared. You can also specify which level of sharing you want to allow in a site collection (sharing with authenticated users, or sharing with both authenticated users and anonymous users through guest links).

#### External sharing features include:

- 1. The ability to turn external sharing on or off **globally** for an entire SharePoint Online environment (or tenant). Turning external sharing off at the tenant level means no documents, sites, or site collections can be shared externally.
- 2. The ability to turn external sharing on or off for **individual site collections**. This provides you with the ability to secure content on specific site collections that you do not want to be shared.
- The ability to share sites and documents with authenticated users. Authenticated
  users are those who are invited to sign in by using a Microsoft account or work or
  school account.
- 4. The ability to share documents with **guest users**. Guest users, also called anonymous users, don't need a Microsoft account or work or school account to access documents. They access the document via a guest link that you or your employees give to them.

External users can	External users can't
Use Office Online for viewing and editing	Create their own personal sites (what
documents. If your plan includes Office Pro	used to be referred to as My Sites), edit
Plus, they will not have the licenses to install	their profile, change their photo, or see
the desktop version of Office on their own	aggregated tasks. External users don't
computers.	

	get their own OneDrive for Business document library.
Perform tasks on a site consistent with the	Be an administrator for a site collection
permission level that they are assigned. For example, if you add an external user to the Members group, they will have Edit permissions and they will be able to add, edit and delete lists; they will also be able to view,	(except in scenarios where you've hired a partner to help manage Office 365. You can designate an external user as a designer for your Public Website.
add, update and delete list items and documents.	Note The SharePoint Online Public Website information in this article applies only if your organization purchased Office 365 prior to March 9, 2015. If you purchased Office 365 after March 9, 2015, use an Office 365 website hosting partner.
See other types of content on sites. For example, they can navigate to different subsites within the site collection to which they were invited. They will also be able to do things like view site feeds.	See the company-wide newsfeed
	Add storage to the overall tenant storage pool
	Access the Search Centre or execute searches against "everything." Other search features that may not be available include: Advanced Content Processing, continuous crawls, and refiners.
	Access site mailboxes
	Access Power BI features such as Power View, Power Pivot, Quick Explore, or Timeline Slicer. These features require an additional license, which is not inherited by external users.
	Use eDiscovery. This requires an Exchange Online license.
	Open downloaded documents that are protected with Information Rights Management (IRM).

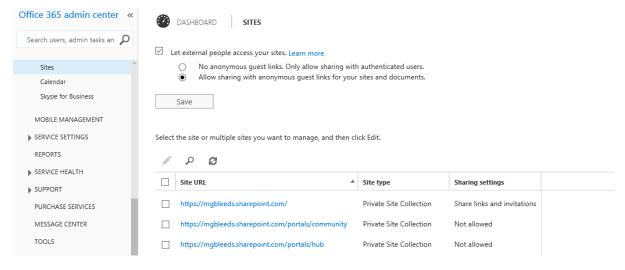


fig1

Fig 1 shows the sharing settings specifically for SharePoint online.



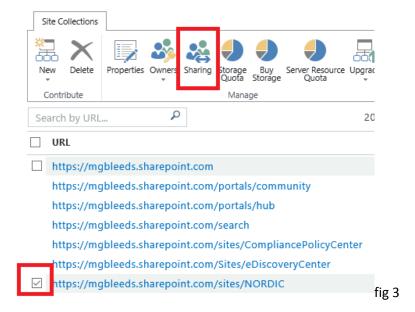
manage sharing setting for site: https://mgbleeds.sharepoint.com/sites/NORDIC

- Allow external users to access this site

  No anonymous guest links. Only allow sharing with authenticated users.
- Allow sharing with anonymous guest links for your sites and documents.

fig 2

Fig 2 shows the sharing settings for a site collection. You can disable external access to the site or enable it then allow anonymous guest links or not



From the SharePoint online administration console you can control how your users give access to people outside your organisation. Figures 4 through 7 show screens shots of this process

# sharing

#### Sharing outside your company

Control how users invite people outside your organization to access content

- O Don't allow sharing outside your organization
- O Allow external users who accept sharing invitations and sign in as authenticated users
- Allow sharing with all external users, and by using anonymous access links

#### Allowing non-owners to invite new users

Status: Allowed. This is the default setting for new sites.

Some sites in this site collection allow nonowners to grant permission to files, folders, or sites and sub-sites without requiring owner approval. Learn more Х

Turn off sharing for non-owners on all sites in this site collection.

fig 4



Some sites in this site collection allow nonowners to grant permission to files, folders, or sites and sub-sites without requiring owner approval. Learn more

Turn off sharing for non-owners on all sites in this site collection.

#### Changes will be applied to the following 1 site collections:



fig 5

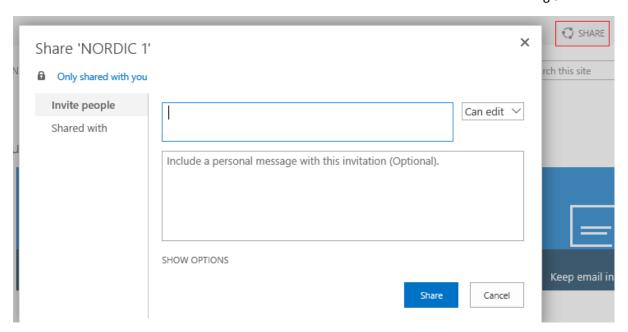


Fig 6

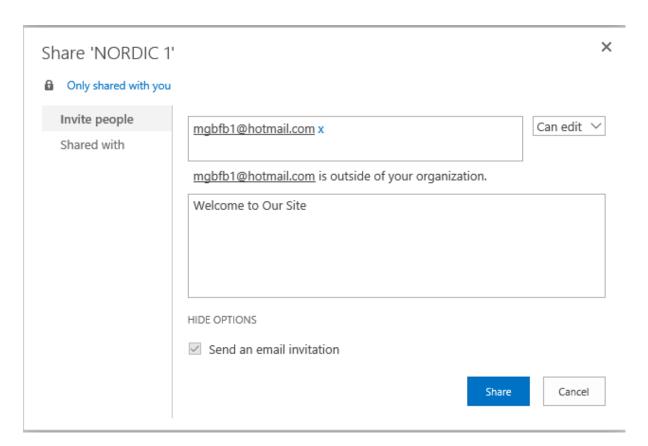


fig 7

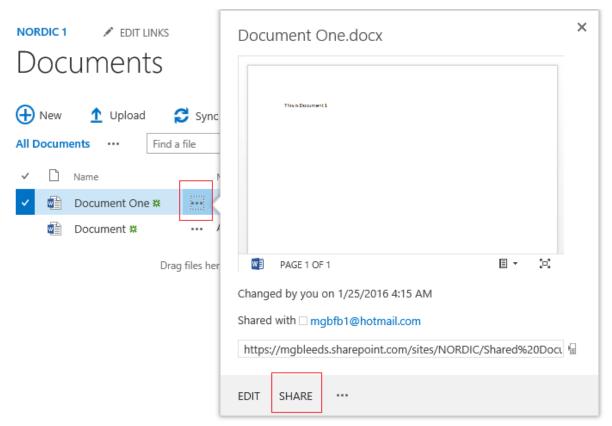


fig 8

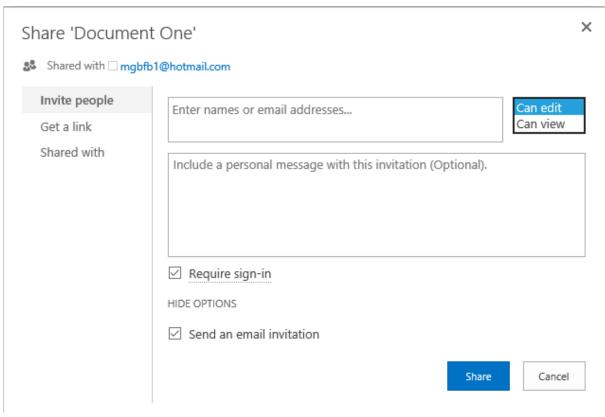


fig 9

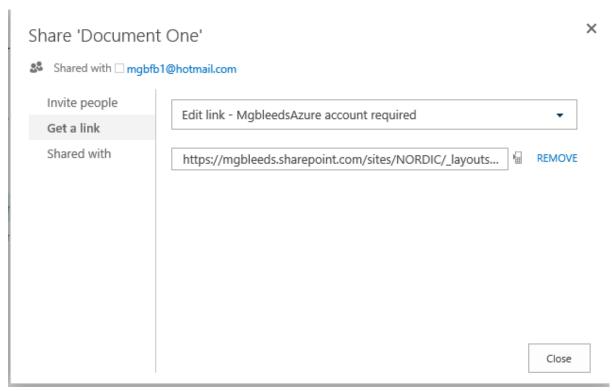


fig 10

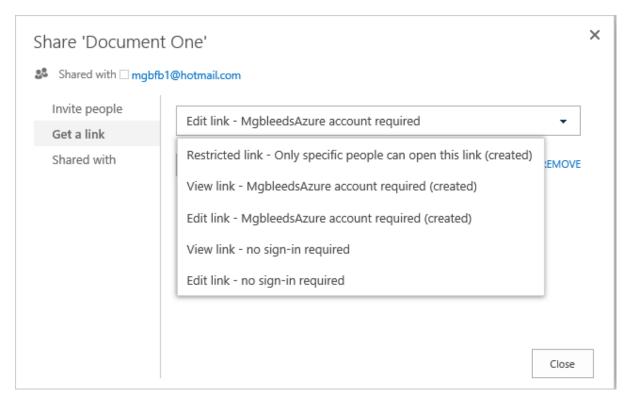


fig 11

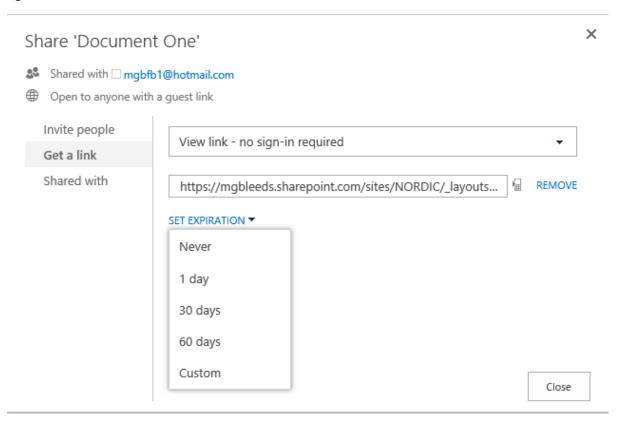


fig 12

Figures 8 through figure 12 show how to share an individual document in a SharePoint document library.



fig 13

You can also create a QR code and use it to share you document

- If external sharing is turned off for the entire SharePoint Online environment, you will not be able to turn it on for specific site collections.
- The external sharing settings for individual site collections cannot be *less* restrictive than whatever is allowed for the entire SharePoint Online environment, but these settings can be *more* restrictive. For example, if external sharing is turned on for the entire SharePoint Online environment, but it is limited to allowing only authenticated users, then that will be the only kind of external sharing you can allow in a specific site collection. If external sharing through both sign-in and anonymous guest links is allowed for the entire SharePoint Online environment, you can opt to turn off external sharing entirely for a specific site collection or you can limit external sharing to authenticate users (no guest links).
- If external sharing is turned off globally in the SharePoint Online Admin center, any shared links will stop working. If the feature is later reactivated, these links will resume working. It is also possible to disable individual links that have been shared if you want to permanently revoke access to a specific document.
- If you change the external sharing settings for the My Site site collection, these
  changes will also apply to any existing or newly created personal sites (formerly
  called My Sites).
- Sharing settings on the -my site site collection (e.g., https://contoso-my.sharepoint.com) will apply to the OneDrive for Business sites for all users of the organization. You cannot selectively manage sharing for a particular user's OneDrive for Business site.

If you want to:	Select this option:	For this result:
Prevent all users on all sites from sharing sites or content with external users.	Don't allow sharing outside your organization	<ul> <li>Users will not be able to share sites or content with users who do not have licenses to your Office 365 subscription.</li> <li>External sharing cannot be turned on for any individual site collections.</li> </ul>
Require external users who have received invitations to view sites or content to sign-in with a Microsoft account before they can access the content.	Allow external users who accept sharing invitations and sign in as authenticated users	<ul> <li>Site owners or others with full control permission can share sites with external users.</li> <li>All external users will be required to sign in before they can view content.</li> <li>Invitations to view content can be redeemed only once. After an invitation has been accepted, it cannot be shared or used by others to gain access.</li> </ul>
Allow site users to share sites with people who sign in as authenticated users, but you also want to allow site users to be able to share documents through the use of anonymous guest links, which do not require invited recipients to sign in.	Allow both external users who accept sharing invitations and guest links	<ul> <li>Site owners or others with full control permissions can share sites with external users.</li> <li>All external users will be required to sign in before they can view content on a site that has been shared.</li> <li>Site owners or others with full control permissions can share documents and opt to require sign-in, or send an anonymous guest link for documents.</li> <li>When site users share a document, they can grant external users either view or edit</li> </ul>

- permissions to the document.
- External users who receive anonymous guest links can view or edit that content without signing in.
- Anonymous guest links could potentially be forwarded or shared with other people, who might also be able to view or edit the content without signing in
- If you turn off external sharing for your entire environment and later turn it back on, external users who previously had access to content or documents on sites will regain access to them. If you know that external sharing was previously turned on and in use for specific site collections and you do not want external users to be able to regain access if external sharing is ever turned on again globally, we recommend that you first turn off external sharing for those specific site collections.
- When you turn off external sharing at the site collection level, all external user permissions for that site collection will be permanently deleted.
- When you turn off external sharing at the site collection level, guest links will be disabled, but they could start working again if external sharing is ever turned on again. If you want to permanently revoke access to specific documents, you will need to disable the anonymous guest links.
- If you disable external access, or limit external access to a more restrictive form, external users will typically lose access within one hour of the change.

```
SharePoint PowerShell Example
Connect-SPOService -url https://mgbleeds-admin.sharepoint.com -Credential $cred

Get-SPOSite

New-SPOSite -url https://mgbleeds.sharepoint.com/sites/TODAY3 -Owner Admin@mgbleeds.onmicrosoft.com -Title "TODAY3" -StorageQuota 400
```

In the PowerShell example above we have used the **Connect-SPOService** cmdlet with the **-url** parameter to connect to our SharePoint online tenant. The **Get-SPOSite** cmdlet will show you a list of all your SharePoint online site collections. The **New-SPOSite** cmdlet will allow you to create a new Site Collection.

#### Exchange Online PowerShell Example

#### Example 1

This example is used to connect to your Exchange online tenant

Unlike with SharePoint online where you have install the sharepoint PowerShell module first, here we are connecting to a remote session then importing it so we can run the Exchange PowerShell commands without install the Exchange PowerShell module.

The –AllowClobber parameter imports the commands even if they have the same name as commands that exist locally.

#### Example 2

```
#Set email addresses and set primary
Set-Mailbox bob -EmailAddresses
SMTP:Bob@MgbleedsAzure.com, smtp:Bob@mgbleeds.onmicrosoft.com

#to assign an additional Email Address
$users = Get-Mailbox
foreach ($a in $users)
{$a.emailaddresses.Add("smtp:$($a.alias)@certificationandbeyond.com")}
$users | %{set-Mailbox $_.Identity -EmailAddresses $_.EmailAddresses}

#Assign using CSV
Import-CSV "C:\Users\Administrator\Desktop\AddEmailAddress.csv" | ForEach {Set-Mailbox
$_.Mailbox -EmailAddresses @{add=$_.NewEmailAddress}}
```

In Example 2 we have three examples that show how to add and mange email addresses. In the first example we use the **Set-Mailbox** cmdlet to give a user 2 email addresses. The address that uses the uppercase **SMTP** will be the primary email address. The second example here adds an additional email address to set of users. It uses the **Get-Mailbox** CMDLet, foreach loop and the **Set-Mailbox** cmdlet.

In the last example we use the **Import-CSV** cmdlet and a foreach loop.

#### Example 3

```
New-Mailbox -Name "Corporate Printing Services" -Alias corpprint -Shared Set-Mailbox bob -Type Regular
```

Here in example three we are showing the different types of mailbox that can be create. Using the **New-Mailbox** cmdlet we can set the type of the new mailbox being created. Using the set-mailbox we can change the type of an existing mailbox. The options for type are:

Regular Shared Room Equipment

The **Set-Mailbox** cmdlet can be used to change a mailbox type.

#### **Example 4**

```
Set-Mailbox BOB -RetentionPolicy Polciy1

Get-Mailbox -ResultSize unlimited | Set-Mailbox -RetentionPolicy Polciy1

$old = Get-RetentionPolicy -Identity Polciy1 | Select -Property distinguishedname Get-Mailbox -Filter {RetentionPolicy -eq $old} -Resultsize Unlimited | Set-Mailbox -RetentionPolicy Policy2

Get-Mailbox Dave | Select RetentionPolicy
```

In example 4 we have several examples of working with retention policies. In the first we use the **Set-Mailbox** cmdlet to select a mailbox and set a retention policy of Policy1. In the next example we use the **Get-Mailbox** cmdlet to get a list of mailboxes, we use the **ResultSize** parameter to get the number of results we need. By default the **Get-Mailbox** cmdlet will return the first 1000 results with the **-unlimited** property it will return all mailboxes. In the third example we use the **Get-Retention** policy cmdlet to get a policy called **Policy1** we then use the **Get-Mailbox** Cmdlet to find a list of mailboxes that use **Policy1** then the **Set-Mailbox** Cmdlet to apply a policy called **Policy2** to those mailboxes.

#### Example 5

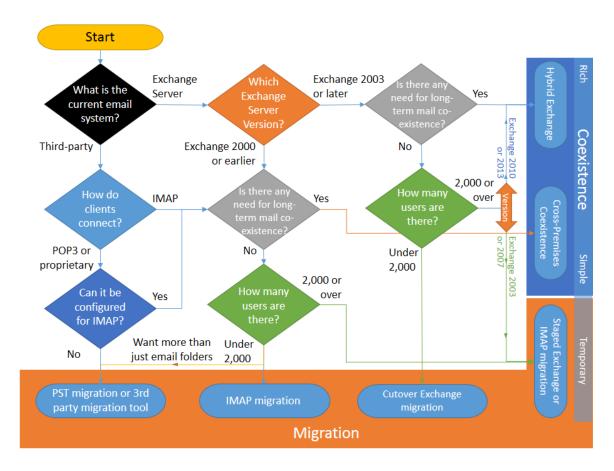
```
New-RetentionPolicyTag "Tag3" -Type All -AgeLimitForRetention 90 -RetentionAction DeleteAndAllowRecovery

New-RetentionPolicy Policy2 -RetentionPolicyTagLinks Tag1,Tag2,TAG3

Start-ManagedFolderAssistant -Identity
```

This example is used to create a Retention Policy Tag called **Tag3** using the **New-RetentionPolicyTag** Cmdlet. It also shows an example of using the **New-RetentionPolicy** cmdlet to create a new retention policy called **Policy2**. The cmdlet **Start-managedFolderAssistant** is used to run the managed folder assistant against one of or a set of mailboxes. The managed folder assistant is used to apply and run a retention policy.

#### **Exchange Migration Flow Chart**



### Azure AD PowerShell Examples

In order to run the Azure AD PowerShell cmdlets you will need to install the Azure AD PowerShell module and the Microsoft Online Sign in Assistant.

```
#Connect to Azure AD
$cred = Get-Credential
Connect-MsolService -Credential $cred
#Create and edit an Azure AD User
New-Msoluser -DisplayName User200
             -UserPrincipalName User200@mgbleeds.onmicrosoft.com
Set-Msoluser -ObjectId "e3795b04-8c29-41af-abbd-8ad1ae1aa930"
                                                               -Department SALES
Get-Msoluser | fl DisplayName, ObjectID
#get Object ID
$USER = Get-Msoluser -UserPrincipalName User200@mgbleeds.onmicrosoft.com
Set-Msoluser -ObjectId $USER.ObjectId -Department ACCOUNTS
Set-MsolUser -UserPrincipalName User200@mgbleeds.onmicrosoft.com -Department SALES
#create and delete a Group
New-MsolGroup -DisplayName GROUP1
$groupID = Get-MsolGroup -SearchString GROUP1
```

```
Remove-MsolGroup -ObjectId $groupID.ObjectId
#Bulk Import
Import-Csv -Path C:\newusers.txt
              foreach {New-MsolUser -DisplayName $_ DisplayName
            -UserPrincipalName $_ UserprincipalName}
# disable password complexity and block user and set password to never expire
Get-Msoluser -UserPrincipalName User1@mgbleeds.onmicrosoft.com | Set-Msoluser -StrongPasswordRequired $false
  -PasswordNeverExpires $true -BlockCredential $true
#MSOL Password Policy
Get-MsolPasswordPolicy -DomainName mgbleeds.onmicrosoft.com
Get-MsolPasswordPolicy -DomainName mgbleedsazure.co.uk
Set-MsolPasswordPolicy -DomainName mgbleedsazure.co.uk -ValidityPeriod 40 -
NotificationDays 10
Set-MsolPasswordPolicy -ValidityPeriod 100 -NotificationDays 10
#Get a list of users 500 by default
Get-Msoluser -all
Get-Msoluser -UnlicensedUsersOnly
#why might we use both together?
Get-Msoluser -all -UnlicensedUsersOnly
#if you want to remove all unlicensed users what would you type?
#what does this cmd do?
Get-Msoluser | Set-Msoluser -StrongPasswordRequired $true
# to export a list of all user and their licenses
Get-MsolUser -all | ft Displayname, Licenses | Out-File c:\userlicenses.csv
#to assign a license, usage location might need to be set to add a licence
Get-MsolAccountSku
Set-MsolUserLicense -UserPrincipalName "bobby@mgbleedsazure.com" -AddLicenses
"Mgbleeds:0365_BUSINESS_ESSENTIALS
Set-MsolUser -UserPrincipalName bobby@mgbleedsazure.com -UsageLocation GB
#to assign a licence subset
Get-MsolAccountSku | Where-Object {$_.skupartnumber -eq 'enterprisepack'} |
ForEach-Object {$_ Servicestatus}
Get-MsolAccountSku | Where-Object {$_.skupartnumber -eq 'o365_business_essentials'}
| ForEach-Object {$__Servicestatus}
$options = New-MsolLicenseOptions -AccountSkuId
MGBLEEDSAZURE: 0365_BUSINESS_ESSENTIALS -DisabledPlans SHAREPOINTSTANDARD
Set-MsoluserLicense -UserPrincipalName "SALLY@MGBLEEDS.ONMICROSOFT.COM" -
LicenseOptions $options
```