Table of Contents

[AZURE ACTIVE DIRECTORY 2](#_Toc122527640)

[AD TERMINOLOGIES 2](#_Toc122527641)

[SUBSCRIPTION AND AD 2](#_Toc122527642)

[CONFIGURING THE TRUST BETWEEN AD AND SUBSCRIPTION 2](#_Toc122527643)

[CREATING USER 4](#_Toc122527644)

[ROLE BASED ACCESS CONTROL (RBAC) 5](#_Toc122527645)

[BASIC BUILD-IN ROLES 6](#_Toc122527646)

[ROLE BASED ASSIGNMENT – READER ROLE 6](#_Toc122527647)

[ROLE BASED ASSIGNMENT – RESOURCE GROUP LEVEL 8](#_Toc122527648)

[ROLE BASED ASSIGNMENT – SUBSCRIPTION LEVEL 8](#_Toc122527649)

[ROLE BASED ASSIGNMENT – CONTRIBUTOR LEVEL 8](#_Toc122527650)

[ROLE BASED ASSIGNMENT – USER ACCESS ADMIN ROLE 9](#_Toc122527651)

[CUSTOM ROLES 9](#_Toc122527652)

[CREATING USER GROUP 11](#_Toc122527653)

[CREATING DYNAMIC USER GROUP 11](#_Toc122527654)

[AZURE AD ROLES 11](#_Toc122527655)

[JOINING A VM TO AD 11](#_Toc122527656)

[MULTIFACTOR AUTHENTICATION 13](#_Toc122527657)

[SETTING UP PER USER MFA 13](#_Toc122527658)

[ADMINISTRATIVE UNITS 13](#_Toc122527659)

# AZURE ACTIVE DIRECTORY

It an identity provider in Azure. With the help of active directory, we can create identities such as users.

With the help of role-based access control, we can actually give permissions to these users over resources as part of Azure subscription.

The key benefit of Azure Active Directory is that we don’t need to implement any infrastructure.

Using active directory, we can CREATE USERS, USER GROUPS

## AD TERMINOLOGIES

|  |  |
| --- | --- |
| TENANT | * When we create an azure account by default, we get an instance of Azure AD. Every such instance is called tenant. * It a dedicated and trusted instance of Azure AD |
| DEFAULT DIRECTORY | * Each tenant has a dedicated and trusted Azure AD directory * This includes tenant user, group and used to perform identity and access management of Azure resources. |

* In Azure Portal, apart from default directory we create a new directory as well. Creating a new directory is same s creating a new tenant itself.

WHY AN ORGAINIZATION WILL CREATE NEW DIRECTORY RATHER THAN USING THE DEFAULT DIRECTORY?

***User-case***: Let's say if an organization has many other companies under that organization, so they can create directories for each of the companies in that organization. Hence rather than creating the users under this one directory, we can create uses company’s directory.

## SUBSCRIPTION AND AD

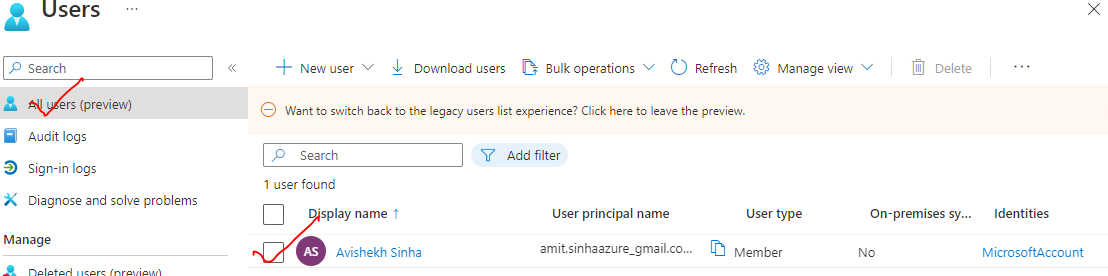
* The subscription is used for grouping of resources and used for the billing aspect. All the resources are built against a particular subscription.

|  |  |
| --- | --- |
|  | * ***At any point in time, one subscription can trust one directory*** - so users are defined in this directory can be given access on resources that are defined in * It means that whatever users are defined in this directory can be given access on to the resources defined in that subscription. |

## CONFIGURING THE TRUST BETWEEN AD AND SUBSCRIPTION

|  |  |  |
| --- | --- | --- |
|  | Step 1: CREATE AN ACTIVE DIRECTORY(TENANT)   * Select Active Directory Service 🡪 Manage Tenant 🡪 Create * Select the Tenant type as “Azure Active Directory”   *Note - So if a company wants to have another directory in place for managing users separately, they can go out and create another as the Active Directory*.   * Once a new directory is created then we can go ahead and create user into the AD. * We can also change the directory for a subscription * The users in the AD will get an access to the resources created in that subscription | |
|  | To change the directory for a subscription   * Go to Subscription🡪 Change Directory 🡪 Select the directory | |
|  | | |
| DELETING A AD(TENANT) – Go to Active Directory 🡪 Manage Tenant 🡪 Select the tenant 🡪 Delete | | |
|  | |  |

## CREATING USER



|  |  |
| --- | --- |
|  | * To Create User🡪 New user 🡪 Create * The default domain is “*onmicrosoft.com*” * We can use the newly created user to login to Azure Portal * Note – When we login with the created user, by default it will have no access to any resource * The Access to the user has to be given explicitly |
|  | |

## ROLE BASED ACCESS CONTROL (RBAC)

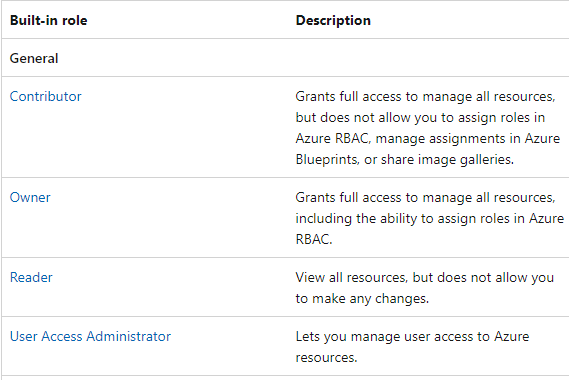
* When we created a user in Azure Active Directory then the user can be able to log into your account. This step was known as authentication to log into Azure account. But the user, we could not access any resource in the Azure account
* To give access - We must make use of ***role-based access control***. This step gives authorization to the user to access resources as part of the Azure account.

The role-based access can be given at

|  |  |
| --- | --- |
| RESOURCE LEVEL | Example - if we had a storage account, we can get access on to that user on to the storage account |
| RESOURCE GROUP LEVEL | This will then ensure that the user has access onto all resources that are part of the resource group. |
| SUBSCRIPTION LEVEL | The user will get access on to all the resource groups and in turn, all the resources that are part of that subscription. |

* Azure has number of in-built roles - <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>, but we can also create our own custom roles as well.

### BASIC BUILD-IN ROLES



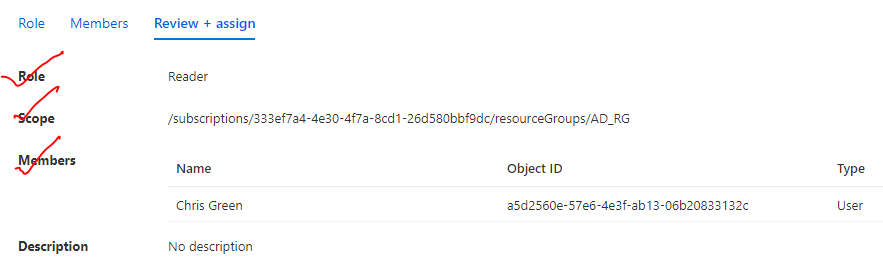
### ROLE BASED ASSIGNMENT – READER ROLE

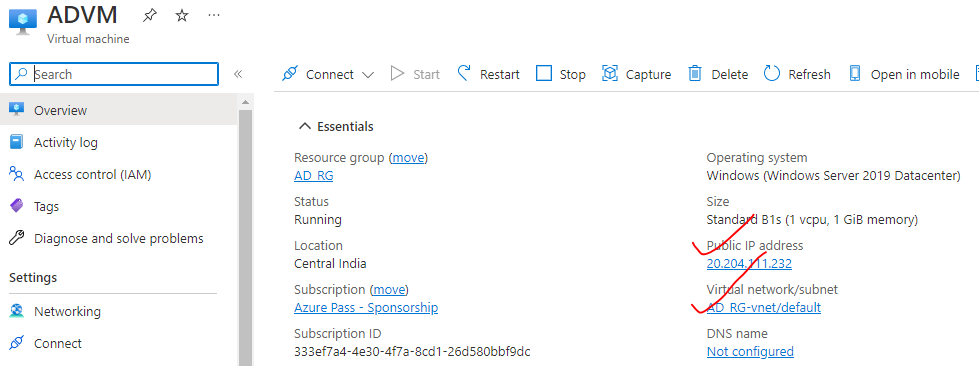
* Example – if we want to give access the Reader permission on VM level(Resource level)

|  |  |  |
| --- | --- | --- |
|  | * *Navigate to VM 🡪 IAM🡪 Add 🡪 Add Role Assignment* | |
|  | | * Select member to whom we want to give access to. * Review and Assign |
| * The VM(resource) has a user with a reader role | | |
| * Note - The user will have read permission on the VM but no access to public IP , VNET and DNS – as they are separate resources in Azure- which needs a separate role assignment. | | |

### ROLE BASED ASSIGNMENT – RESOURCE GROUP LEVEL

* Navigate to resource group and assign the permission (reader permission for this example) on the resource
* If we assign a role at a resource group level, it will apply to all of the resources within the resource group.





### ROLE BASED ASSIGNMENT – SUBSCRIPTION LEVEL

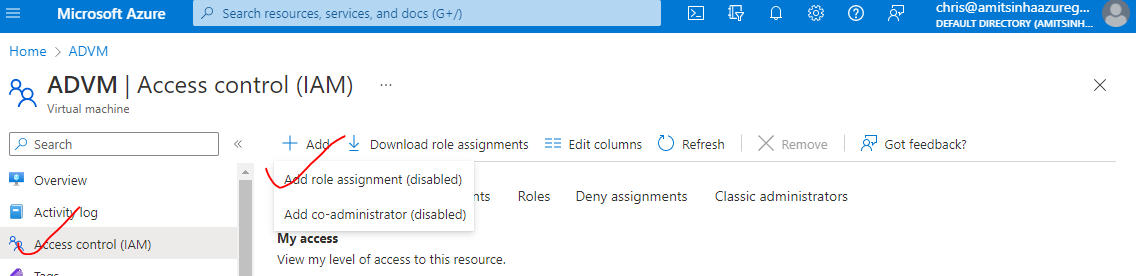
* If we give access at the subscription level, then the role gets applied to all resource groups that are part of that subscription.

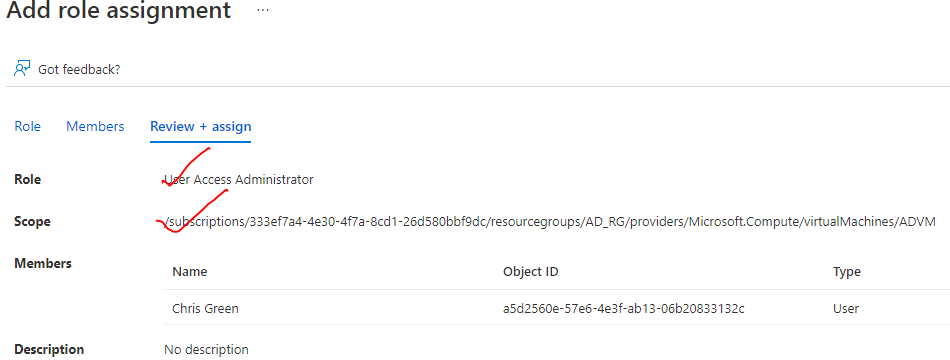
### ROLE BASED ASSIGNMENT – CONTRIBUTOR LEVEL

|  |  |
| --- | --- |
| This role allows the user to manage the VM and also the virtual networks that the VMS are hosted in. | * When a user is assigned a role of reader – then no operation can be performed by the user except view. * To enable this capability – we need to assign contributor role to the user. * For example - VM contributor role (To perform VM operations). In the below example - we are assigning *VM contributor Role* on resource group level |

### ROLE BASED ASSIGNMENT – USER ACCESS ADMIN ROLE

* The role allows the user to give access to other users / add role-based access to other user. The “User Access Admin Role” – enable the user for role-based assignments.



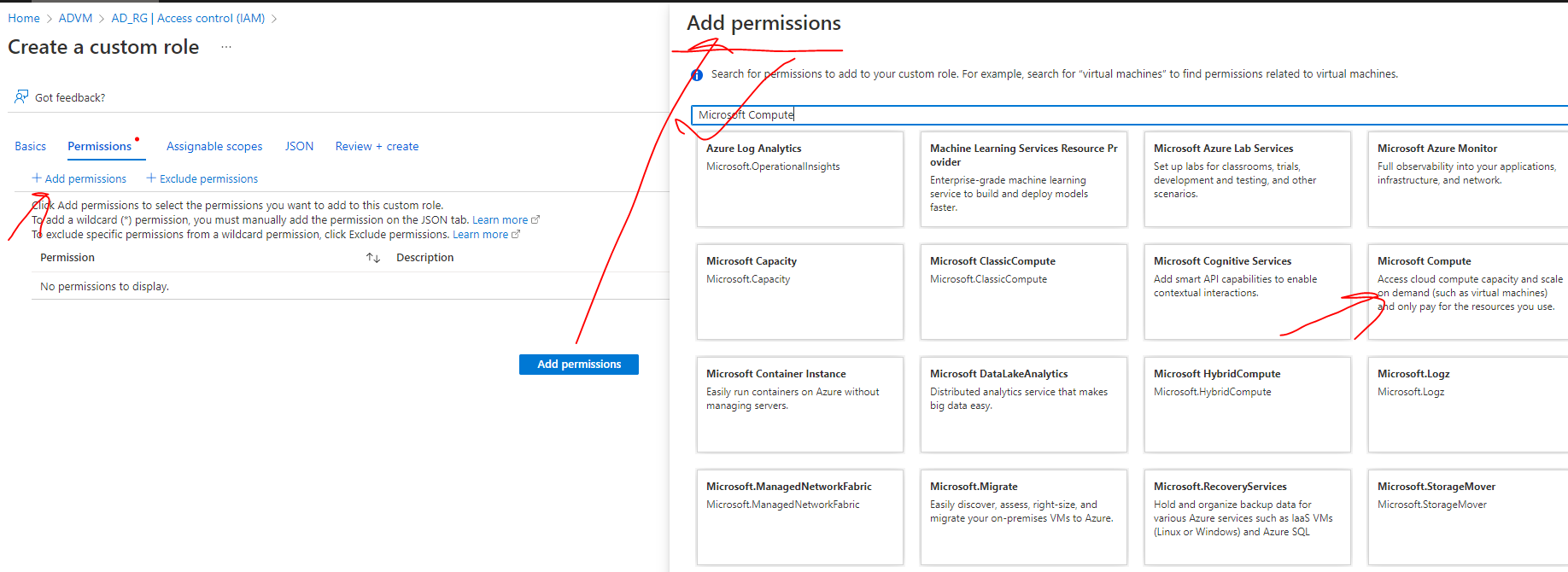


### CUSTOM ROLES

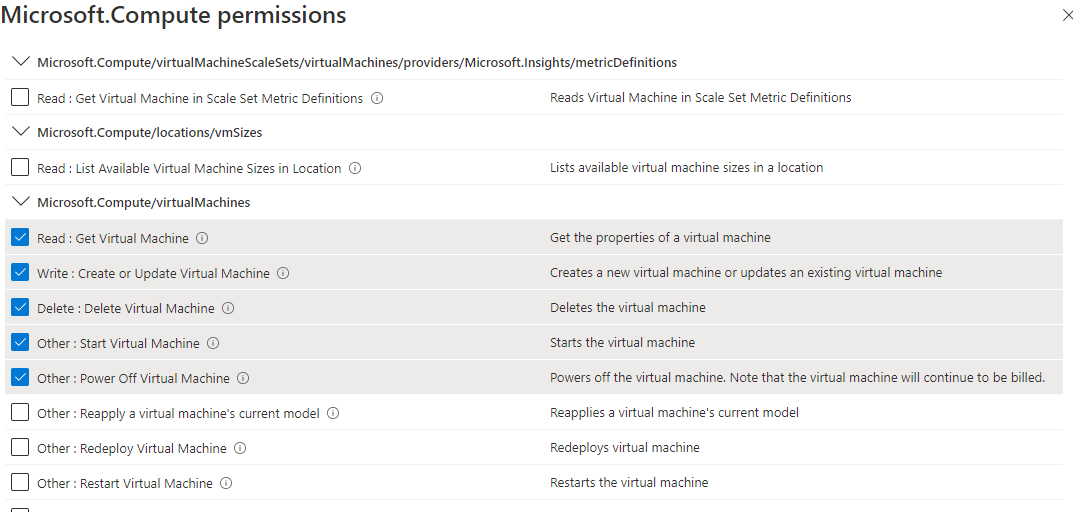
* Apart from build in roles -we can create custom roles too. For example to assign a custom role on resource group level.

|  |  |
| --- | --- |
|  | * Navigate to IAM🡪 Add custom rule * While creating a custom role – we have an option to   + Clone a role   + Start from scratch   + Start from JSON |
|  | * Let’s select “start from scratch”🡪 next |

* Let’s say we want to create role for a VM 🡪 select Microsoft Compute



* Select the required permission from the Compute permission list



|  |  |
| --- | --- |
|  | * Once the custom role is created – it can be then assigned to any level |

### CREATING USER GROUP

|  |  |
| --- | --- |
|  | * Go to Azure AD 🡪 Groups 🡪 New Group * Note – members can be added while creating the group itself or later too. |
| * To add member to the group 🡪 Go to the group 🡪 Members 🡪 Add members | |

### CREATING DYNAMIC USER GROUP

* In a user group we must manually assign members onto a group. But you also have this facility of dynamic groups wherein users can automatically be added onto a group.

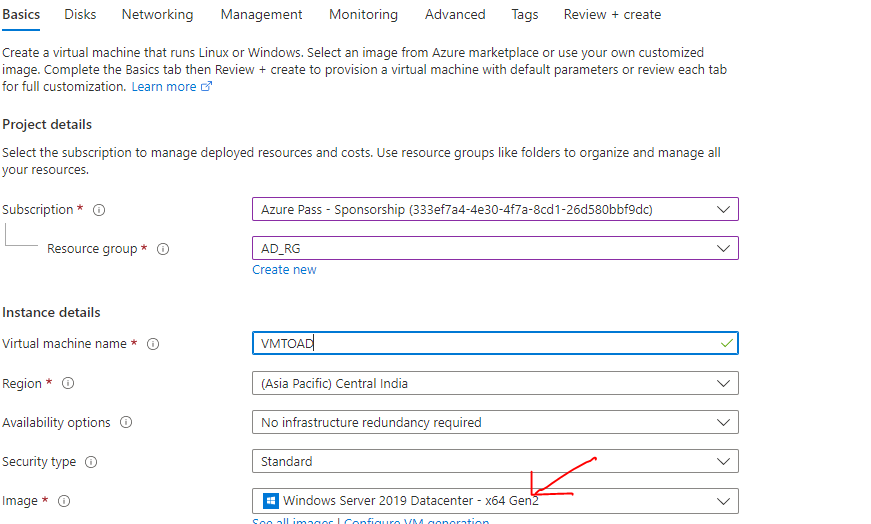
## AZURE AD ROLES

* AD roles are purely meant to carry out tasks in Azure Active Directory only. AD roles are dedicated to managing the Active directory itself. for example, to create an application, create a user, create a group etc. For example - In an organization, these activities are they typically delegated to administrators.
* On the other hand, the RBAC are used to give a user access to resources within Azure
* https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

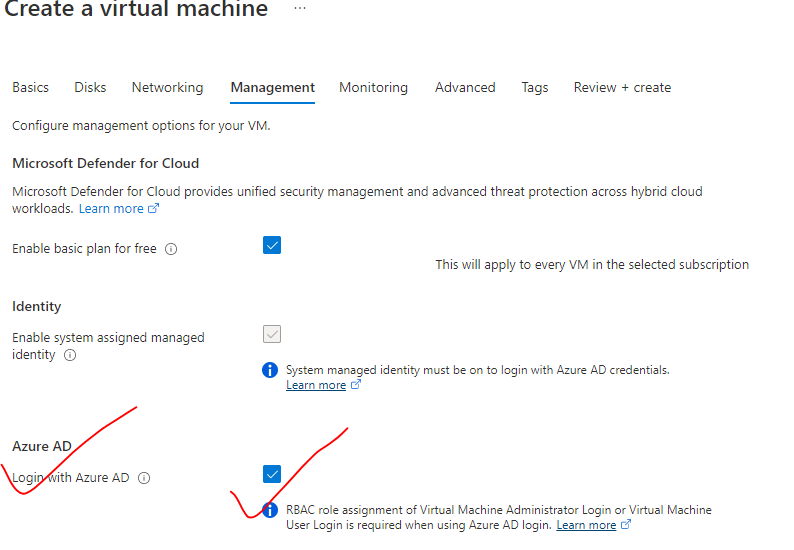
## JOINING A VM TO AD

* Windows 10 and based device, if you have Windows server 2019 can be joined to an Active Directory.

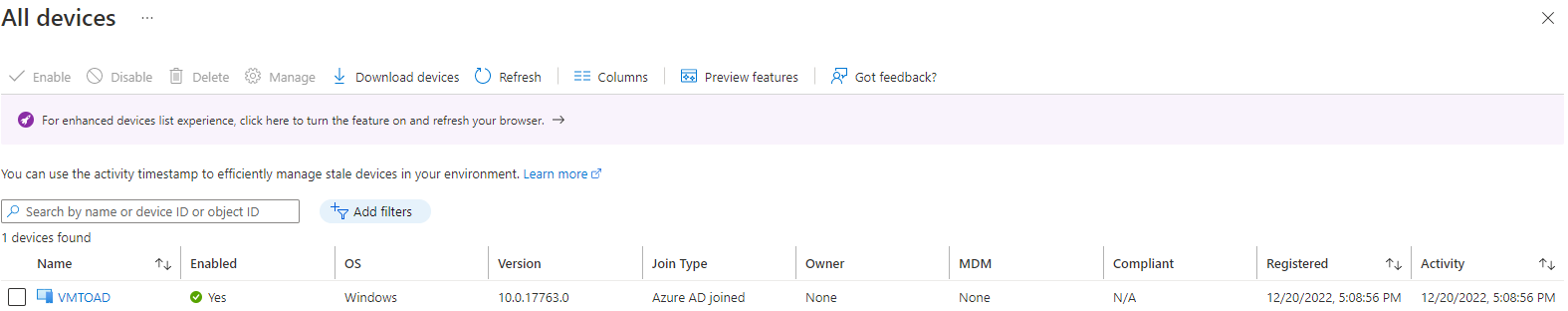
Step 1: Provision a Window 10 / Server VM



Step 2: Register the device with AD



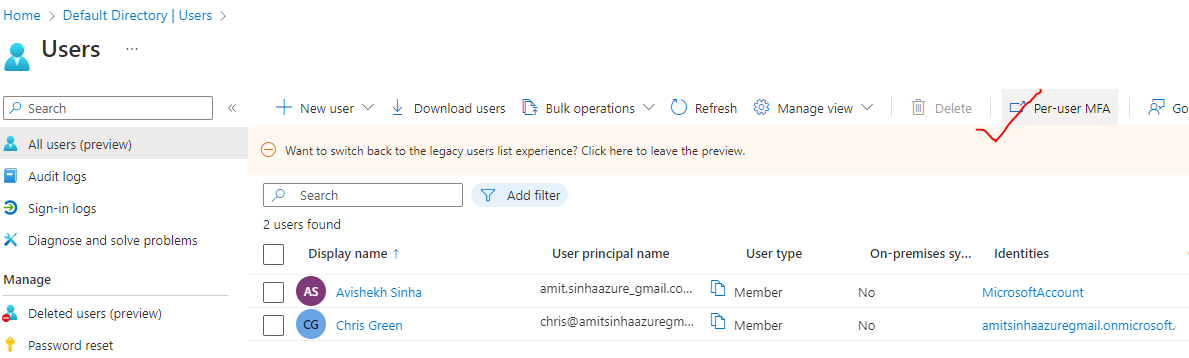
* To check the connected device – Active Directory 🡪 Devices



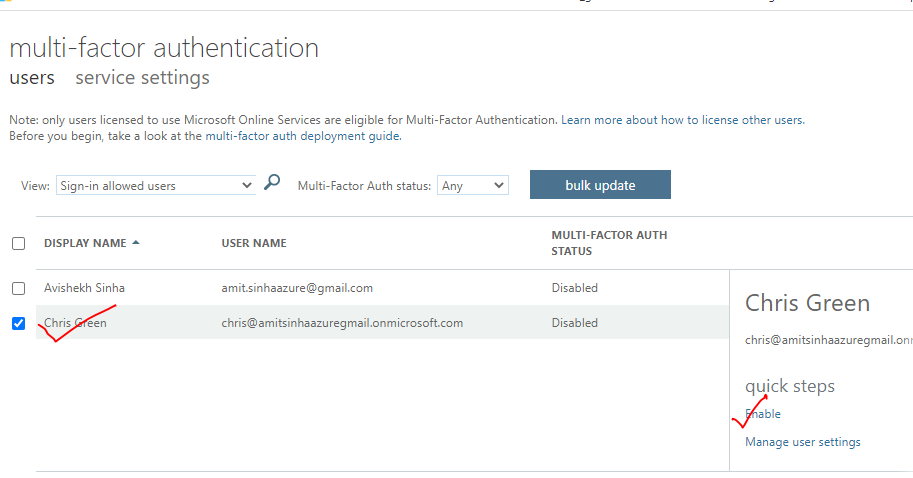
## MULTIFACTOR AUTHENTICATION

### SETTING UP PER USER MFA

* Go to Active directory 🡪 Per user MFA



* Select user 🡪 Enable



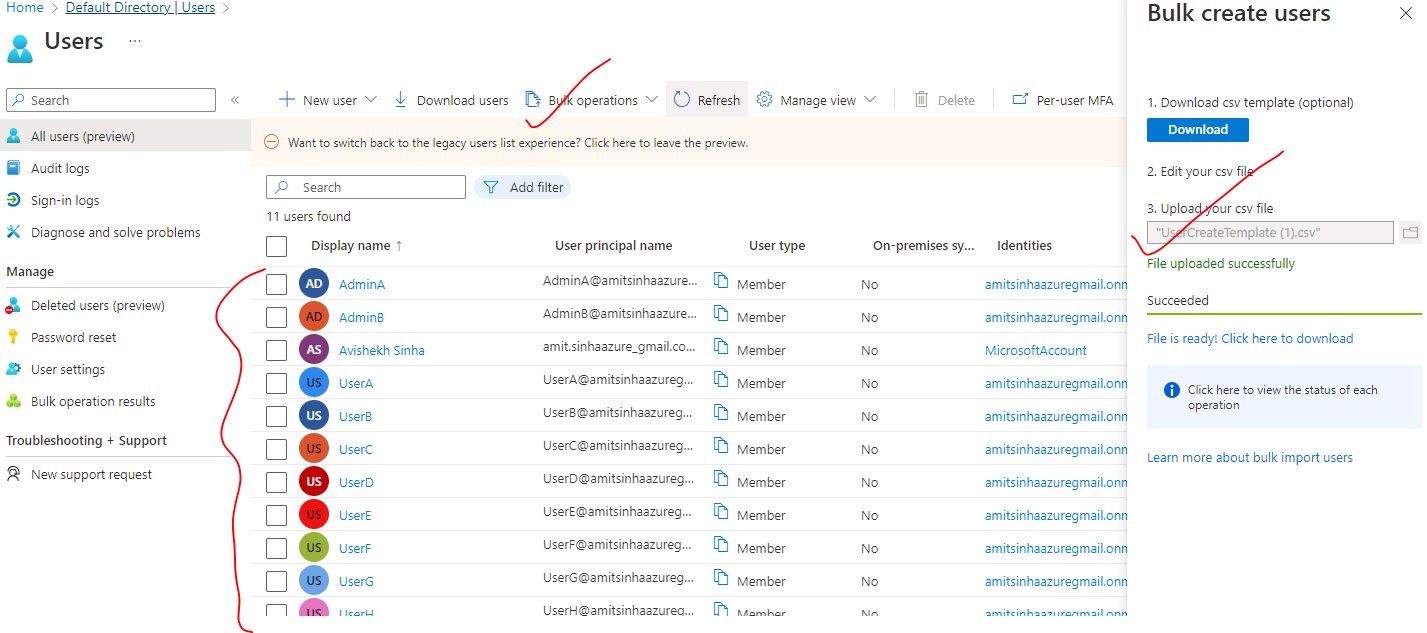
## ADMINISTRATIVE UNITS

|  |  |
| --- | --- |
|  | * In Azure AD we create uses and assign roles/permission to them   **USER CASE**   * Let's say that we have multiple departments in a company, and we want to create a admin for each department – who will only go ahead and manage the subset of users within that particular department. * Since Azure AD is a global directory. If we start creating users in global AD – it will be difficult to manage them all * Hence to manage the users department wise – we can make use administrative units for each department. |

### LAB -ADMINISTRATIVE UNITS

|  |  |
| --- | --- |
|  | * We are going to have two users who are going to be part of an administrative unit. * We are also going to have another user known as admin that is going to behave as the user administrator for the administrative unit. * We'll have two more users that are going to be part of a group(logistic-grp). * That group is going to be part of administrative unit * We're going to create some other users who are not going to be part of that unit. * Some of these users are going to be part of another group known as general-grp. |

***Step 1:*** *Create user (Bulk Operation) – for the bulk creation of user Azure provides a template(as .xlsx) 🡪 Download the template 🡪 Add the data of users 🡪 Upload the sheet*



**Step 2:** Create the user groups

|  |  |
| --- | --- |
| Logistic Group – User C and User D | General Group – User G and User H |
|  |  |

**Step 3:** Create the Administrative Unit –

So the entire idea is - Admin A can able to manage

1. Logistic Group (this group is part of Administrative Unit)
2. User A and User B (Will be members of Admin Unit)
3. But - should not have the ability to manage other users that are outside the administrative unit.