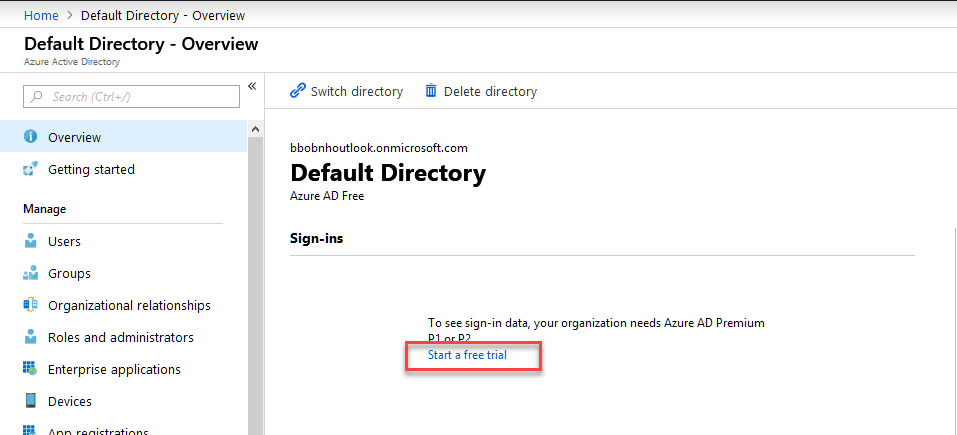
**LABS Day 5**

**Lab 1 Require MFA for specific apps with Azure Active Directory conditional access**

**Task 1 Enable Premium**

1. In the overview section of the Default Directory click on **Start a free trail.** Then click **Free Trial** for **Preimum2** and **Activate**



**Task 2 Create User**

1. Create a User for use in this lab named Billy Bob.

**Task 3 Test your sign-in**

The goal of this step is to get an impression of the sign-in experience without a conditional access policy.

**To initialize your environment:**

1. Sign in to your Azure portal as your new user.
2. Sign out.

**Task 4 Create your conditional access policy**

This section shows how to create the required conditional access policy. The scenario in this quickstart uses:

* The Azure portal as placeholder for a cloud app that requires MFA.
* Your sample user to test the conditional access policy.

In your policy, set:

| **Setting** | **Value** |
| --- | --- |
| Users and groups | Billy Bob |
| Cloud apps | Microsoft Azure Management |
| Grant access | Require multi-factor authentication |

**To configure your conditional access policy:**

1. Sign in to your [Azure portal](https://portal.azure.com/) as global administrator, security administrator, or a conditional access administrator.
2. In the Azure portal, on the left navbar, click **Azure Active Directory**.
3. On the **Azure Active Directory** page, in the **Security** section, click **Conditional Access**.
4. On the **Conditional Access** page, in the toolbar on the top, click **New policy**.
5. On the **New** page, in the **Name** textbox, type **Require MFA for Azure portal access**.
6. In the **Assignment** section, click **Users and groups**.
7. On the **Users and groups** page, perform the following steps:

a. Click **Select users and groups**, and then select **Users and groups**.

b. Click **Select**.

c. On the **Select** page, select the user you created, Billy Bob, and then click **Select**.

d. On the **Users and groups** page, click **Done**.

1. Click **Cloud apps**.
2. On the **Cloud apps** page, perform the following steps:

a. Click **Select apps**.

b. Click **Select**.

c. On the **Select** page, select **Microsoft Azure Management**, and then click **Select**.

d. On the **Cloud apps** page, click **Done**.

1. In the **Access controls** section, click **Grant**.
2. On the **Grant** page, perform the following steps:

a. Select **Grant access**.

b. Select **Require multi-factor authentication**.

c. Click **Select**.

1. In the **Enable policy** section, click **On**.
2. Click **Create**.

**Task 5 Evaluate a simulated sign-in**

Now that you have configured your conditional access policy, you probably want to know whether it works as expected. As a first step, use the conditional access what if policy tool to simulate a sign-in of your test user.

To initialize the **What if** policy evaluation tool, set:

* **Your user**
* **Microsoft Azure Management** as cloud app

# 

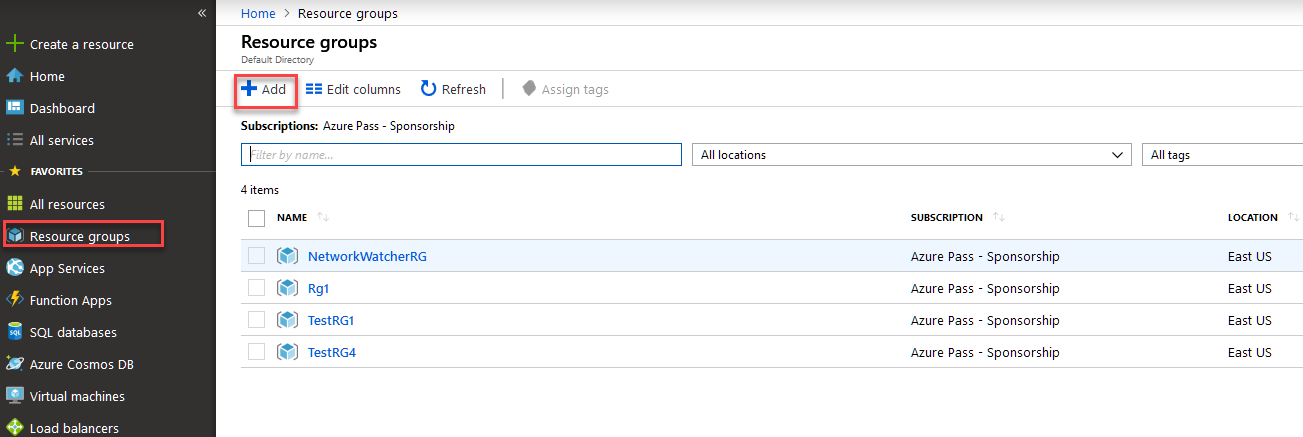
# **Lab 2A Grant access for a user using RBAC and the Azure portal**

## Task 1 Sign in to Azure

Sign in to the Azure portal at [http://portal.azure.com](http://portal.azure.com/).

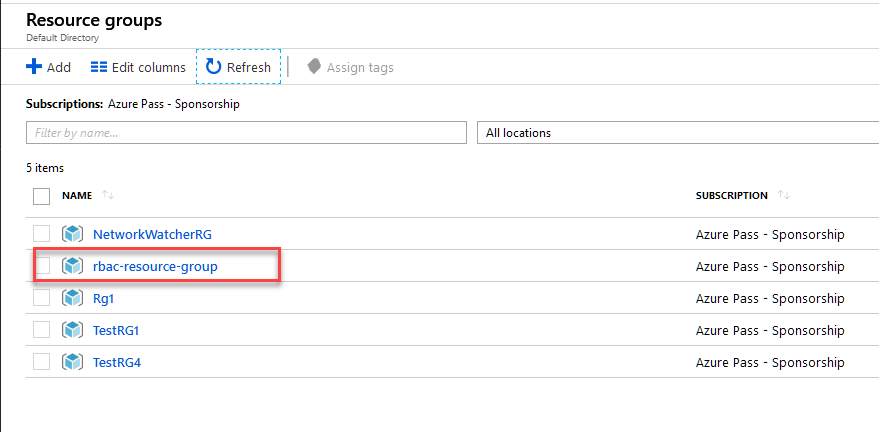
## Task 2 Create a resource group

1. In the navigation list, choose **Resource groups**.
2. Choose **Add** to open the **Resource group** blade.



1. For **Resource group name**, enter **rbac-resource-group**.
2. Select a subscription and a location.
3. Choose **Review+Create**, then **Create** to create the resource group.
4. Choose **Refresh** to refresh the list of resource groups.

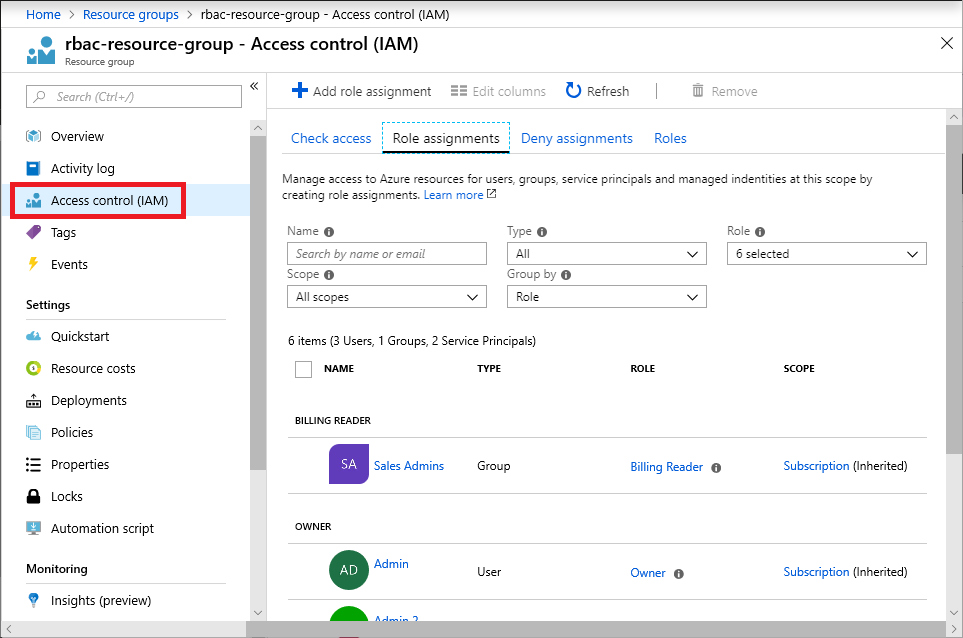
The new resource group appears in your resource groups list.



## Task 3 Grant access

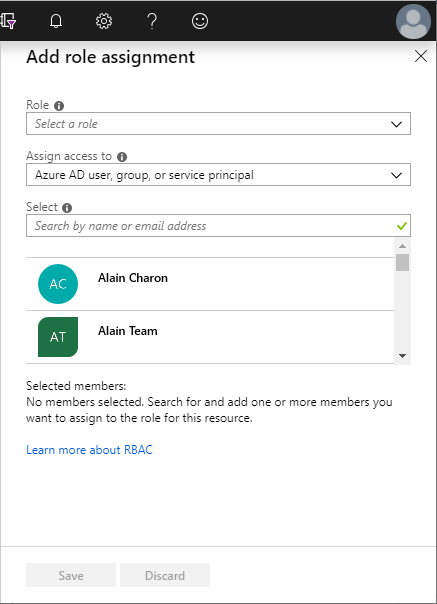
In RBAC, to grant access, you create a role assignment.

1. In the list of **Resource groups**, choose the new **rbac-resource-group** resource group.
2. Choose **Access control (IAM)**.
3. Choose the **Role assignments** tab to see the current list of role assignments.



1. Choose **Add role assignment** to open the Add role assignment pane.

If you don't have permissions to assign roles, the Add role assignment option will be disabled.



1. In the **Role** drop-down list, select **Virtual Machine Contributor**.
2. In the **Select** list, select yourself or another user.
3. Choose **Save** to create the role assignment.

After a few moments, the user is assigned the Virtual Machine Contributor role at the rbac-resource-group resource group scope.

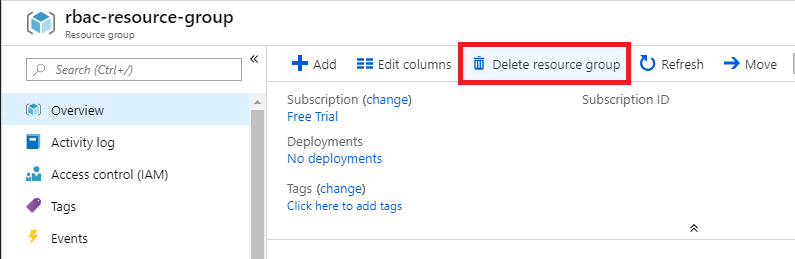
## Task 4 Remove access

In RBAC, to remove access, you remove a role assignment.

1. In the list of role assignments, add a checkmark next to the user with the Virtual Machine Contributor role.
2. Choose **Remove**.
3. In the remove role assignment message that appears, choose **Yes**.

## Task 5 Clean up

1. In the navigation list, choose **Resource groups**.
2. Choose **rbac-resource-group** to open the resource group.
3. Choose **Delete resource group** to delete the resource group.



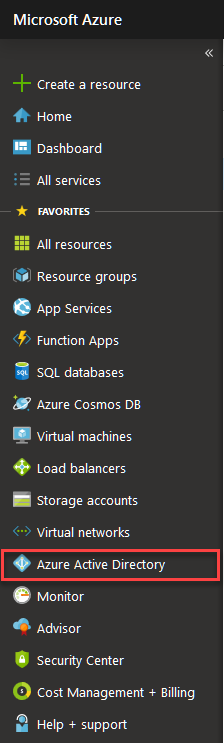
1. On the **Are you sure you want to delete** blade, type the resource group name: **rbac-resource-group**.
2. Choose **Delete** to delete the resource group.

**Lab 2B How to manage devices using the Azure portal**

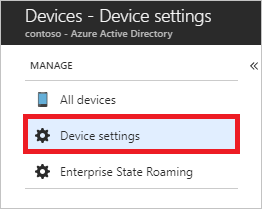
**Task 1 Manage devices**

The Azure portal provides you with a central place to manage your devices. You can get to this place by either using a [direct link](https://portal.azure.com/#blade/Microsoft_AAD_IAM/DevicesMenuBlade/Devices) or by following these manual steps:

1. Sign in to the [Azure portal](https://portal.azure.com/) as administrator.
2. On the left navbar, click **Active Directory**.



1. In the **Manage** section, click **Devices**.

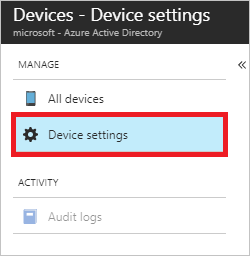


The **Devices** page enables you to:

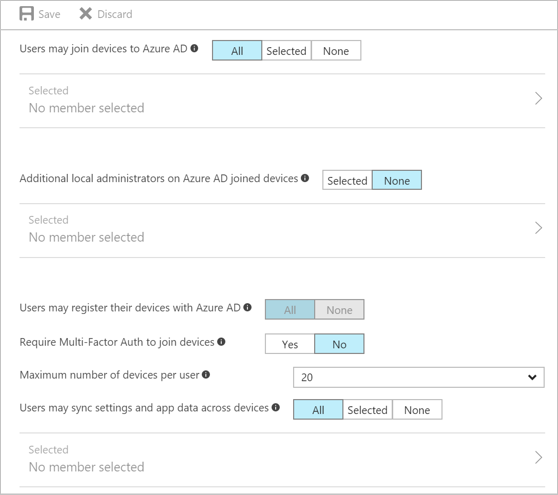
* Configure your device management settings
* Locate devices
* Perform device management tasks
* Review the device management related audit logs

## Task 2 Configure device settings

To manage your devices using the Azure portal, your devices need to be either [registered or joined](https://docs.microsoft.com/en-us/azure/active-directory/devices/overview#getting-devices-under-the-control-of-azure-ad) to Azure AD. As an administrator, you can fine-tune the process of registering and joining devices by configuring the device settings.



The device settings page enables you to configure:

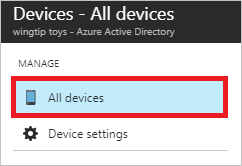


* **Users may join devices to Azure AD** - This setting enables you to select the users who can [join devices](https://docs.microsoft.com/en-us/azure/active-directory/devices/overview#azure-ad-joined-devices) to Azure AD. The default is **All**. This setting is only applicable to Azure AD Join on Windows 10.
* **Additional local administrators on Azure AD joined devices** - You can select the users that are granted local administrator rights on a device. Users added here are added to the Device Administrators role in Azure AD. Global administrators in Azure AD and device owners are granted local administrator rights by default. This option is a premium edition capability available through products such as Azure AD Premium or the Enterprise Mobility Suite (EMS).
* **Users may register their devices with Azure AD** - You need to configure this setting to allow devices to be [registered](https://docs.microsoft.com/en-us/azure/active-directory/devices/overview#azure-ad-registered-devices) with Azure AD. If you select **None**, devices are not allowed to register when they are not Azure AD joined or hybrid Azure AD joined. Enrollment with Microsoft Intune or Mobile Device Management (MDM) for Office 365 requires registration. If you have configured either of these services, **ALL** is selected and **NONE** is not available.
* **Require Multi-Factor Auth to join devices** - You can choose whether users are required to provide a second authentication factor to [join](https://docs.microsoft.com/en-us/azure/active-directory/devices/overview#azure-ad-joined-devices) their device to Azure AD. The default is **No**. We recommend requiring multi-factor authentication when registering a device. Before you enable multi-factor authentication for this service, you must ensure that multi-factor authentication is configured for the users that register their devices. For more information on different Azure multi-factor authentication services, see [getting started with Azure multi-factor authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-whichversion). This setting does not impact hybrid join for Windows 10 or Windows 7. This is only applicable to Azure AD Join on Windows 10 and BYO device registration for Windows 10, iOS, and Android.
* **Maximum number of devices** - This setting enables you to select the maximum number of devices that a user can have in Azure AD. If a user reaches this quota, they are not be able to add additional devices until one or more of the existing devices are removed. The device quote is counted for all devices that are either Azure AD joined or Azure AD registered today. The default value is **20**.
* **Users may sync settings and app data across devices** - By default, this setting is set to **NONE**. Selecting specific users or groups or ALL allows the user’s settings and app data to sync across their Windows 10 devices. Learn more on how sync works in Windows 10. This option is a premium capability available through products such as Azure AD Premium or the Enterprise Mobility Suite (EMS).

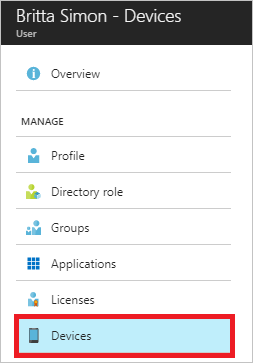
## Locate devices

You have two options to locate registered and joined devices:

* **All devices** in the **Manage** section of the **Devices** page

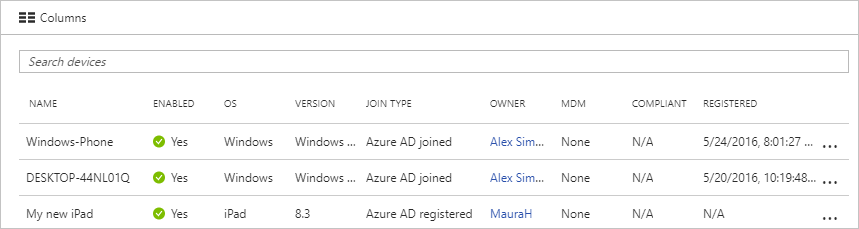


* **Devices** in the **Manage** section of a **User** page



With both options, you can get to a view that:

* Enables you to search for devices using the display name as filter.
* Provides you with detailed overview of registered and joined devices
* Enables you to perform common device management tasks



For some iOS devices, the device names containing apostrophes can potentially use different characters that look like apostrophes. So searching for such devices is a little tricky - if you are not seeing search results correctly, please ensure that the search string contains matching apostrophe character.

## Task 4 Device management tasks

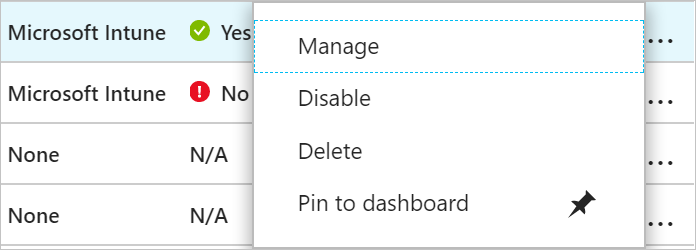
As a global administrator, you can manage the registered or joined devices. Intune Service administrators can:

* Update devices - Examples are daily operations such as enabling/disabling devices
* Delete devices – When a device is retired and should be deleted in Azure AD

This section provides you with information about common device management tasks.

### Manage an Intune device

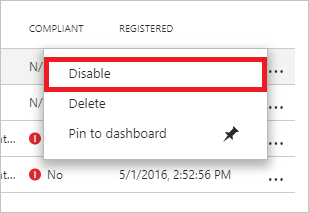
If you are an Intune administrator, you can manage devices marked as **Microsoft Intune**.



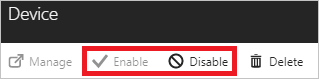
### Enable / disable an Azure AD device

To enable / disable a device, you have two options:

* The tasks menu ("...") on the **All devices** page



* The toolbar on the **Devices** page



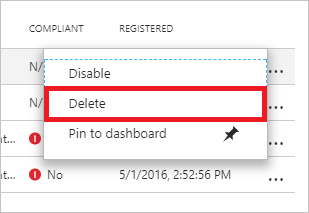
**Remarks:**

* You need to be a global administrator in Azure AD to enable / disable a device.
* Disabling a device prevents a device from successfully authenticating with Azure AD, therby preventing the device from accessing your Azure AD resources that are guarded by device CA or using your WH4B credentials.

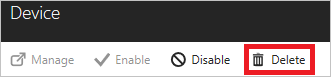
### Delete an Azure AD device

To delete a device, you have two options:

* The tasks menu ("...") on the **All devices** page



* The toolbar on the **Devices** page



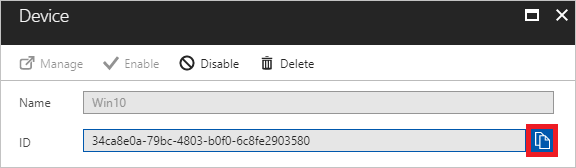
**Remarks:**

* You need to be a global administrator or an Intune administrator in Azure AD to delete a device.
* Deleting a device:
  + Prevents a device from accessing your Azure AD resources.
  + Removes all details that are attached to the device, for example, BitLocker keys for Windows devices.
  + Represents a non-recoverable activity and is not recommended unless it is required.

If a device is managed by another management authority (for example, Microsoft Intune), please make sure that the device has been wiped / retired before deleting the device in Azure AD.

### View or copy device ID

You can use a device ID to verify the device ID details on the device or using PowerShell during troubleshooting. To access the copy option, click the device.



### View or copy BitLocker keys

You can view and copy the BitLocker keys to help users to recover their encrypted drive. These keys are only available for Windows devices that are encrypted and have their keys stored in Azure AD. You can copy these keys when accessing details of the device.



To view or copy the BitLocker keys, you need to be either the owner of the device, or a user that has at least one of the following roles assigned:

* Global admins
* Helpdesk Admins
* Security Administrators
* Security Readers
* Intune Service Administrators

Note

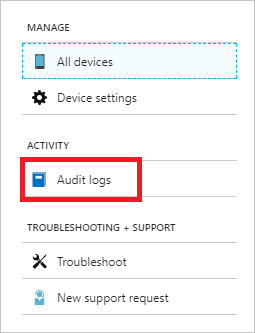
Hybrid Azure AD Joined Windows 10 devices do not have an owner. So, if you are looking for a device by owner and didn't find it, search by the device ID.

## Audit logs

Device activities are available through the activity logs. This includes activities triggered by the device registration service and by users:

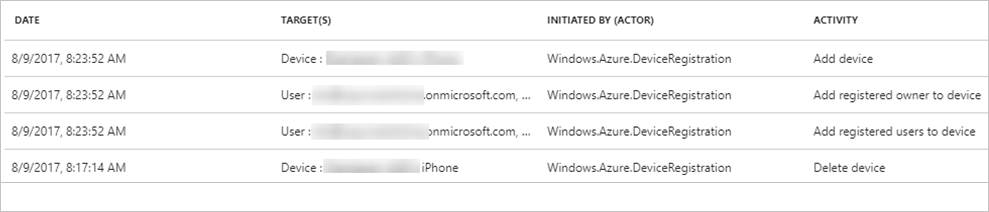
* Device creation and adding owners / users on the device
* Changes to device settings
* Device operations such as deleting or updating a device

Your entry point to the auditing data is **Audit logs** in the **Activity** section of the **Devices** page.



An audit log has a default list view that shows:

* The date and time of the occurrence
* The targets
* The initiator / actor (who) of an activity
* The activity (what)



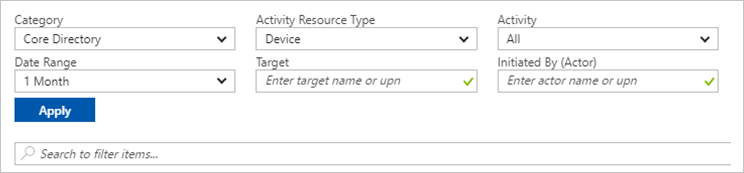
You can customize the list view by clicking **Columns** in the toolbar.

Audit logs

To narrow down the reported data to a level that works for you, you can filter the audit data using the following fields:

* Category
* Activity resource type
* Activity
* Date range
* Target
* Initiated By (Actor)

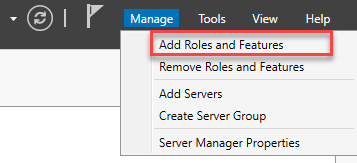
In addition to the filters, you can search for specific entries.



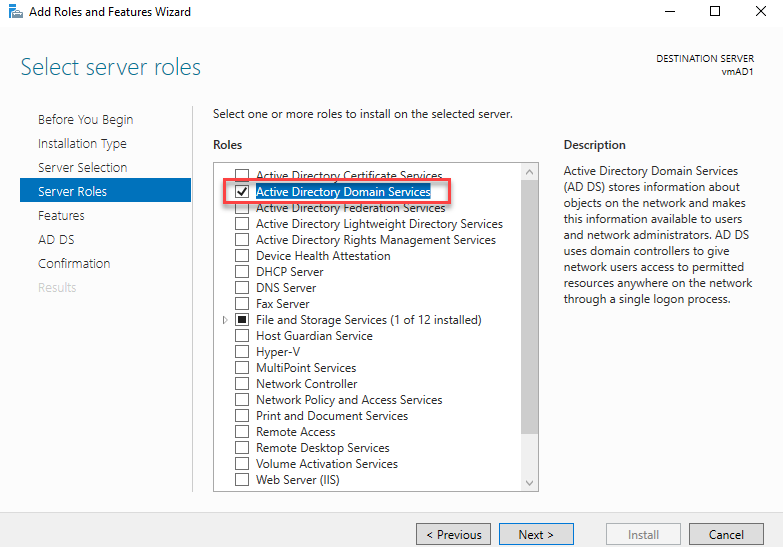
**Lab 3A Deploy AD Connect**

Exercise 1 Install A Domain Controller

1. Create a new Windows 2016 Server Datacenter
   1. Ensure Port 3389 is open
2. Connect to the Server using RDP
3. Install the Domain Service role
   1. From Server Manager choose Add Roles and Features

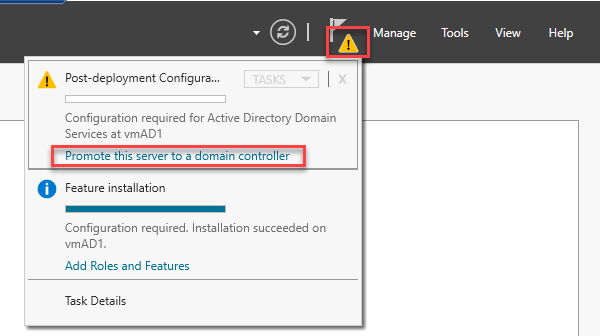


* 1. Select **Next** three times Active Directory Domain Services

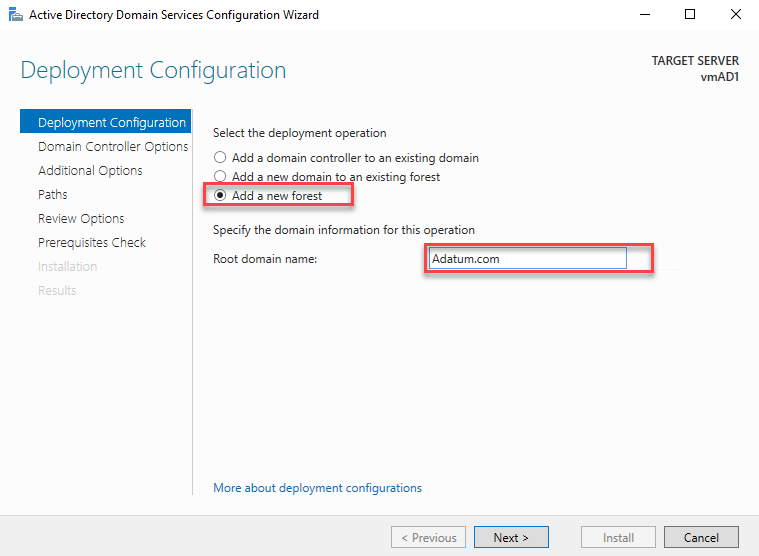


* 1. Hit **Next** three more time then select **Install**
  2. Once Finished select the **Close** Button

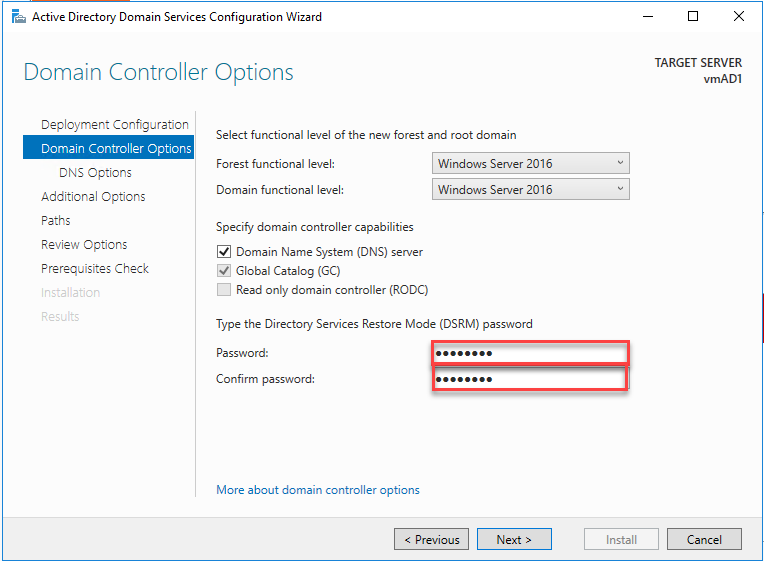
1. Promote the Server to a Domain Controller
   1. Select the warning Icon and then Promote this server o a domain controller.



* 1. On the Deployment Configuration page select the valus in the picure

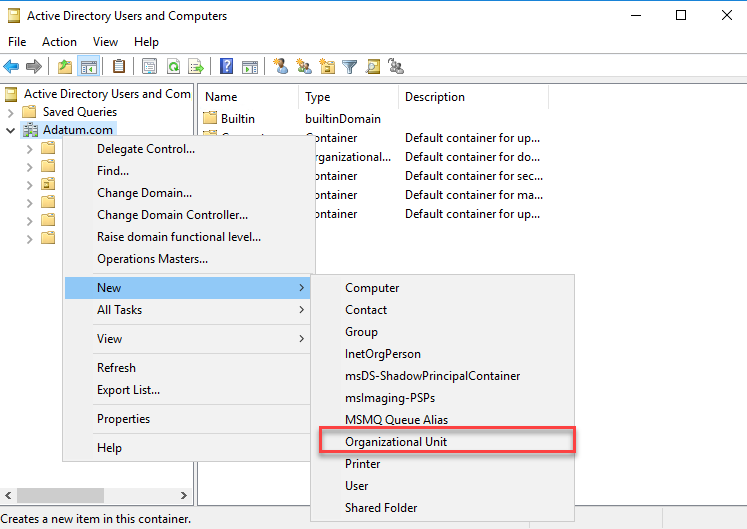


* 1. Click Next then enter password



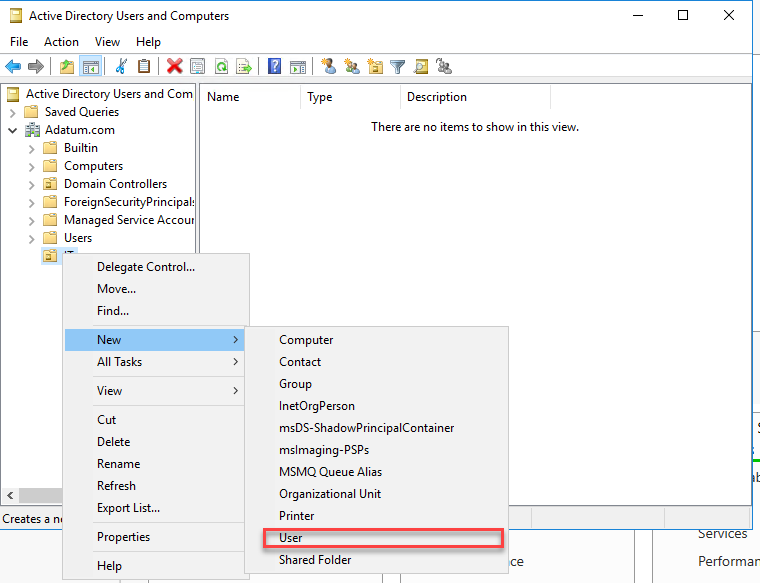
* 1. Click **Next** five times then click **Install**

1. Once the server has restarted, reconnect to it.
2. Using Server Manager open up **Tools >> Active Directory Users and Computers**
3. Right click on Adatum.com, then slect New, then select Organizational Unit

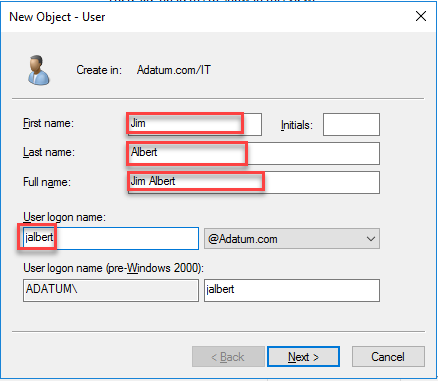


* 1. Type **IT** for the name and then click **OK**

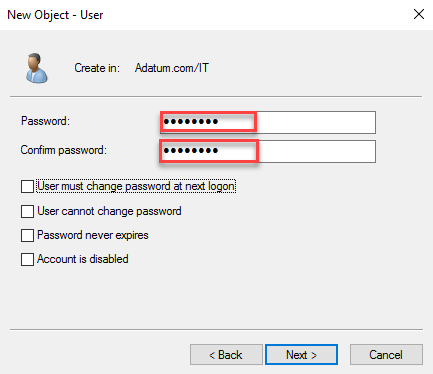
1. Right click on the OU IT, then slect New , then select User



1. File out the New Object User as follows:



* 1. Then Click **Next** and enter a Password



* 1. Click **Next** then **Finished**

1. On your PC In the Portal Select **Azure Active Directory** then under **Manage** select **Azure Ad Connect**
2. Click **Download Azure AD Connect** then select **Download.**
3. Save the file and the copy it to a folder on your Server.
4. Create a new Global Administrator and log into the protal as that user forcing the change of the password.
5. The run the **AzureADConnect.MSI** file
   1. Agree and select **Continue**
   2. Select **Use express setting**
   3. Enter your Global Admin’s Credentials
   4. Enter your Admin user account
   5. Since we do not have a custom domain verified select Continue, and then select **Next**.
   6. Select **Exit** when complete.
6. From the portal go to the **Azure Active Directory**, then **Users**
   1. Notice your new User is there.

Lab 3B Azure Active Directory Pass-through Authentication

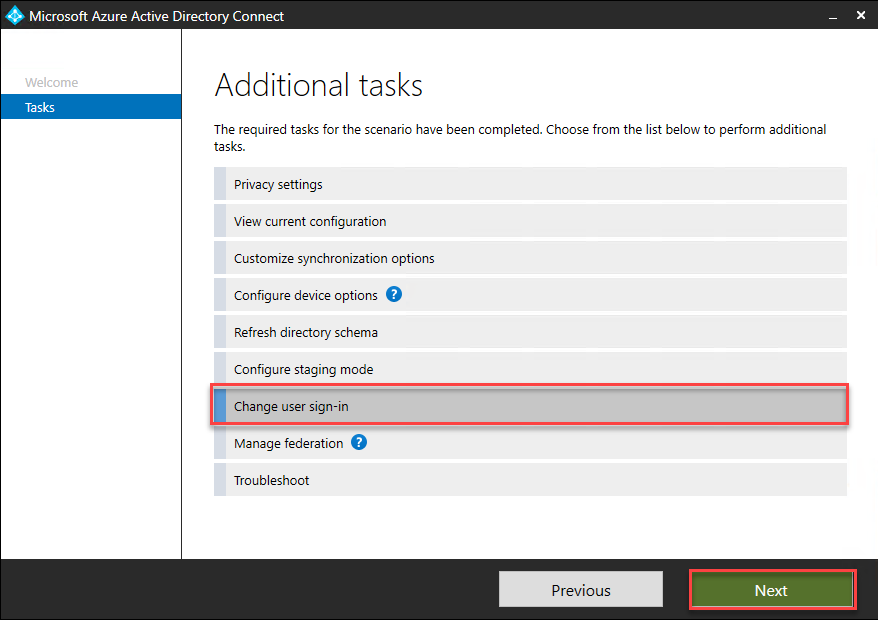
## Deploy Azure AD Pass-through Authentication

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

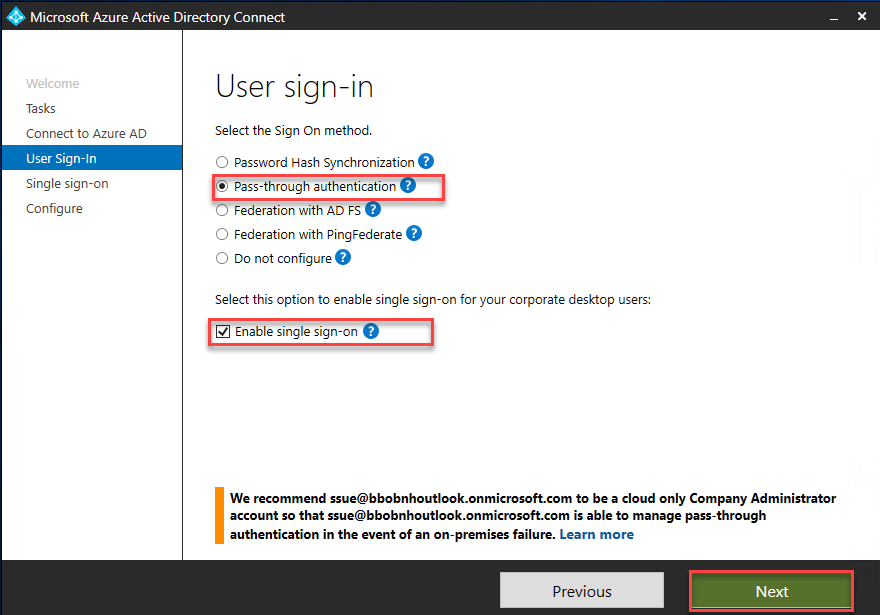
Follow these instructions to deploy Pass-through Authentication on your tenant:

## Task 1: Enable the feature

1. Launch the AD Connect program from the desktop on the Server
   * 1. Then Choose Change user sign-in



* + 1. Enable **Pass-through authentication**



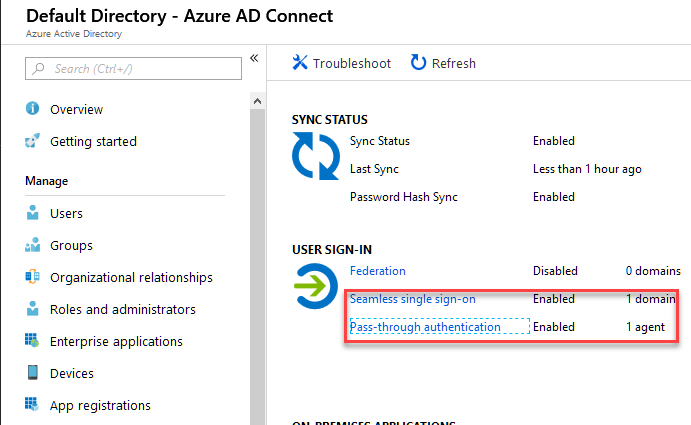
* + 1. Enter the Credentials required on the next two steps.
    2. Select Configure

## Task 3: Verify the feature

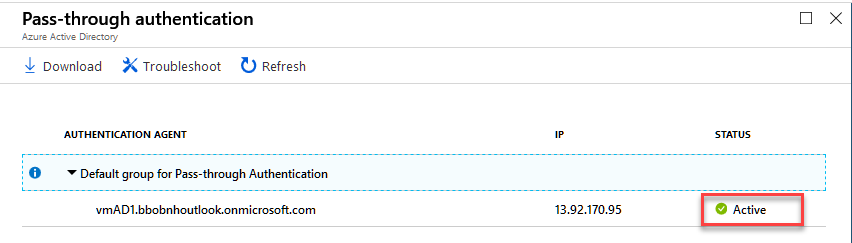
Follow these instructions to verify that you have enabled Pass-through Authentication correctly:

azureuser

1. Sign in to the [Azure Active Directory admin center](https://aad.portal.azure.com/)with the global administrator credentials for your tenant.
2. Select **Azure Active Directory** in the left pane.
3. Select **Azure AD Connect**.
4. Verify that the **Pass-through authentication** feature. It will take an hour to see it enabled.



1. Select **Pass-through authentication**. The **Pass-through authentication** pane lists the servers where your Authentication Agents are installed.



At this stage, users from all the managed domains in your tenant can sign in by using Pass-through Authentication. However, users from federated domains continue to sign in by using AD FS or another federation provider that you have previously configured. If you convert a domain from federated to managed, all users from that domain automatically start signing in by using Pass-through Authentication. The Pass-through Authentication feature does not affect cloud-only users.