**Lab – 12: Managing device using the Azure Portal.**

**Objective:** The objective of this lab is –

* To manage device using the Azure Portal.

With device management in Azure Active Directory (Azure AD), you can ensure that your users are accessing your resources from devices that meet your standards for security and compliance.

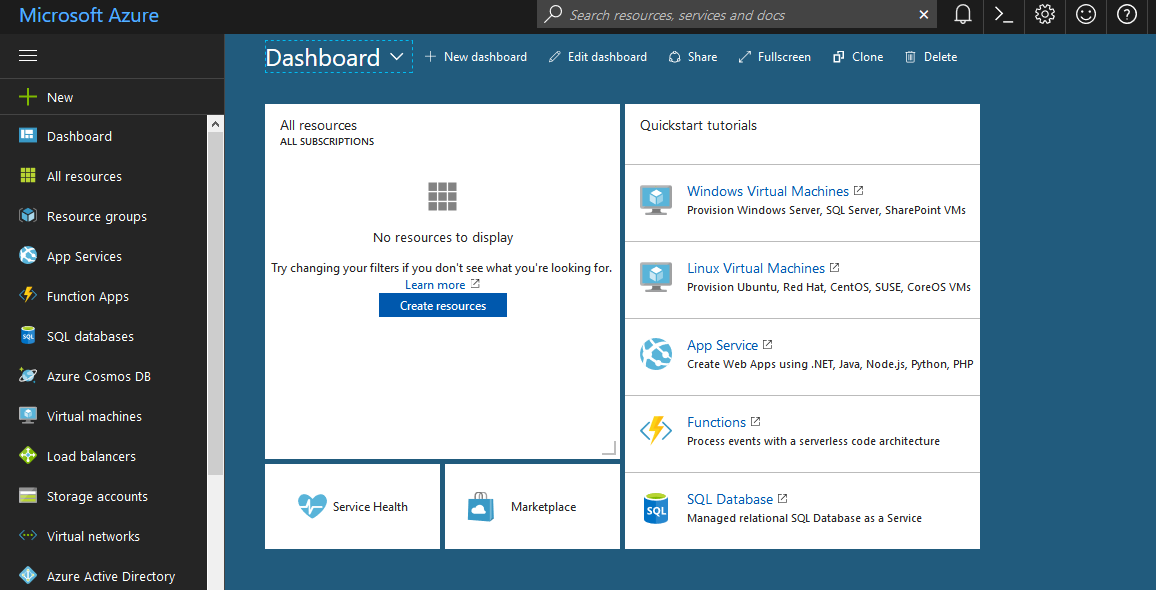
**Prerequisite:** EMS Enterprise Mobility + Security E5.

**Steps:**

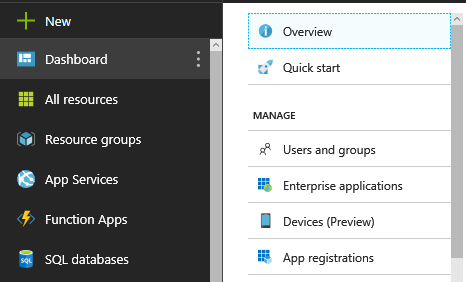
1. Sign in to your Azure Portal, by using the link - **https://portal.azure.com/**. Enter your credentials and click Sign In.



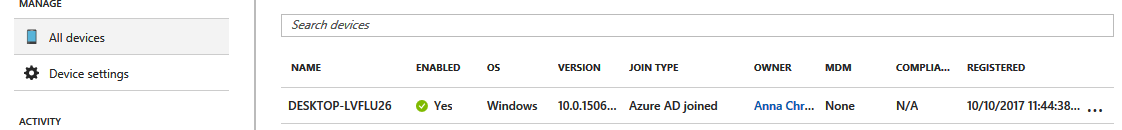
1. Microsoft Azure AD Dashboard will open.



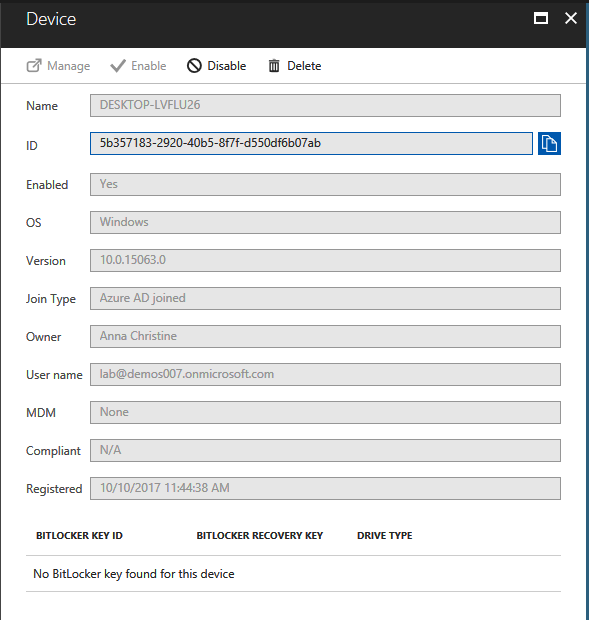
1. Now click **Azure Active Directory** from left-hand pane, and then select **Devices (preview)** in the **Manage** section.



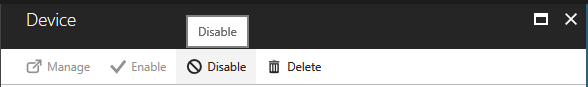
1. Here you can see all the registered devices with your Azure AD.



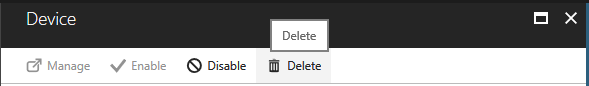
1. For additional details, click the Device.



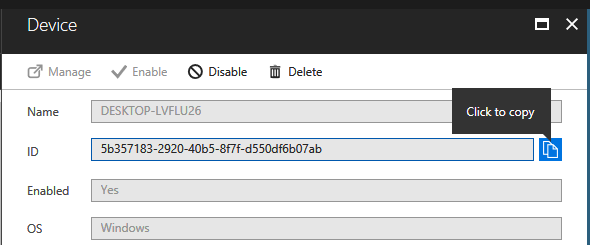
1. From here, you can view all the details.
2. To enable or disable a device, you need to be a global administrator in Azure AD. Disabling a device prevents a device from accessing your Azure AD resources. Click **Disable** to disable the device.



1. To delete a device, you need to be a global administrator in Azure AD. Deleting a device: prevents a device from accessing your Azure AD resources. It removes all details that are attached to the device, for example, BitLocker keys for Windows devices. It represents a non-recoverable activity and is not recommended unless it is required. If a device is managed by another management authority (e.g. Microsoft Intune), please make sure that the device has been wiped / retired before deleting the device in Azure AD. To delete the device, click **Delete**.



1. To view or copy the 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.



1. If you are an administrator, 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.



1. So, in this way, you can set up Azure Active Directory joined devices and you can manage it.