**Lab – 10: Customize device settings in Azure.**

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

* To customize device settings in Azure.

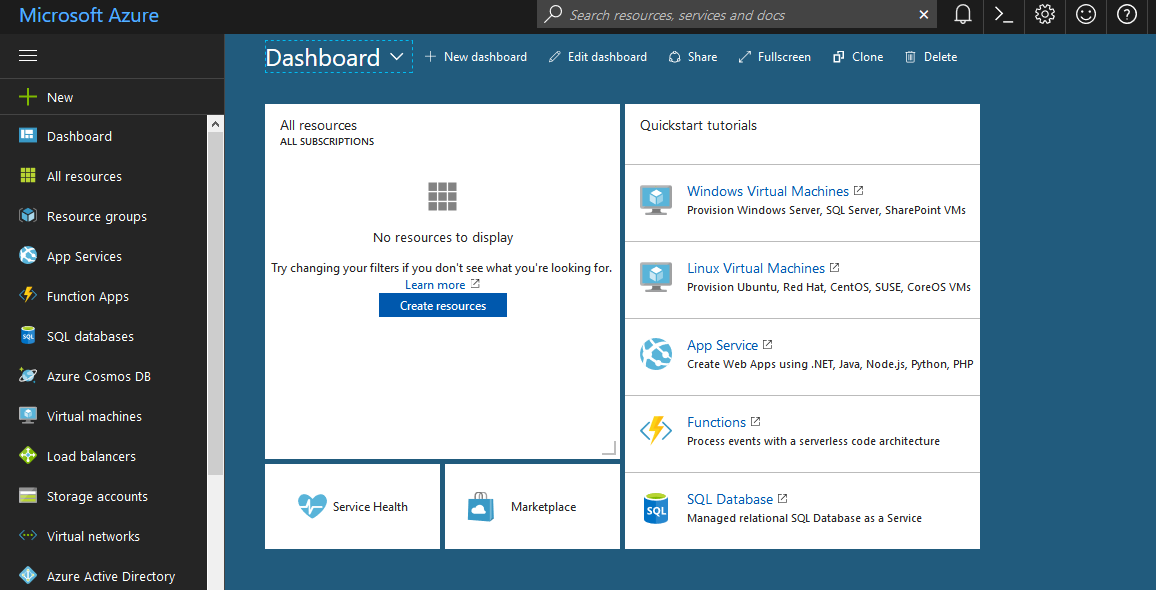
**Prerequisite:** EMS Enterprise Mobility + Security E5.

**Steps:**

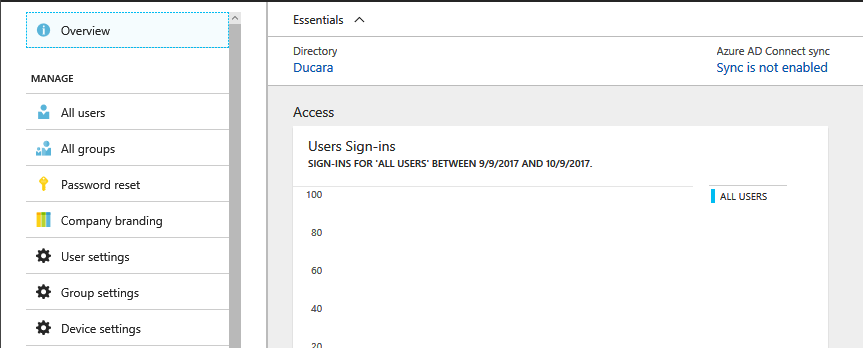
1. Sign in to your Azure Portal, by using the link - **https://portal.azure.com/**. Enter your credentials and click Sign In.



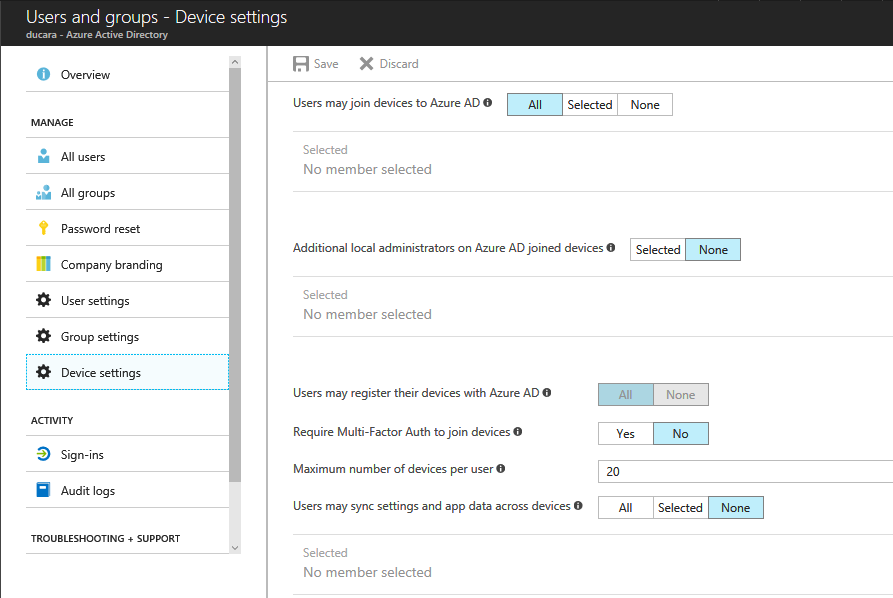
1. Microsoft Azure AD Dashboard will open.



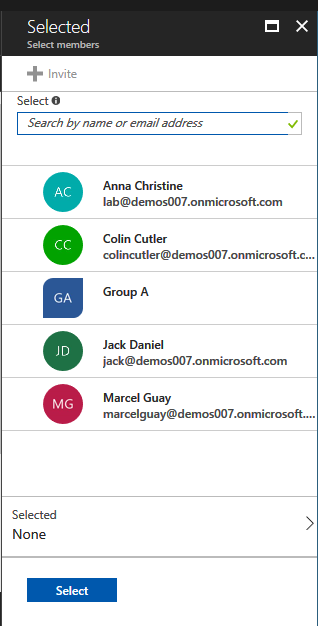
1. Now click **Azure Active Directory** from left-hand pane, and then select **Users and Groups** then select **Device Settings** in the **Manage** section.



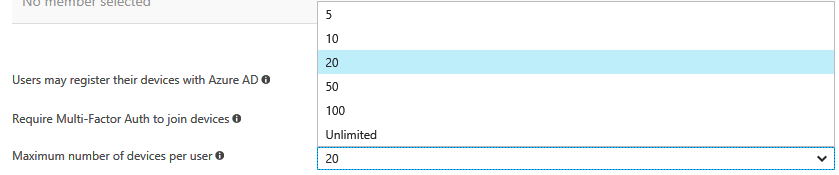
1. Device settings page will open, which will show you the configuration settings for the device.



1. Like –
   1. Users may join devices to Azure AD - This setting enables you to select the users who can join devices to Azure AD. We have three options for this – All, Selected and None. The default is All. You can also select a particular member or number of selected members who can join their devices to Azure AD. For this click **Selected**, then you will get Select members page from where you can select members by checking the box of the users or the groups and then click **Select**.



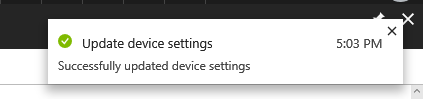
* 1. Another setting is, Additional local administrators on Azure AD joined devices - You can select the users that are granted local administrator rights on a device. Users added here are added to the Device Administrators role in Azure AD. Global administrators in Azure AD and device owners are granted 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). By default, it is **None**.
  2. Users may register their devices with Azure AD – you need to configure this setting to allow devices to be registered 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 for Office 365 requires registration. If you have configured either of these services, ALL is selected and NONE is not available.
  3. Require Multi-Factor Authentication to join devices - You can choose whether users are required to provide a second authentication factor to join their device to Azure AD. By default, it is **No**. Click **Yes**, to enable multi-factor authentication to join devices.
  4. 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 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. You can select maximum number of devices from the menu.



* 1. Users may sync settings and app data across devices - Selecting specific users or groups or All allows the user’s settings and app data to sync across their Windows 10 devices. This option is a premium capability available through products such as Azure AD Premium or the Enterprise Mobility Suite. By default, this setting is set to **None**.



1. After setting, click **Save**. It will show you notification, that **successfully updated device settings**.



1. So, this is how you can configure device settings in Azure AD.