**Lab – 7: How to check device Activity Logs in Azure?**

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

* To check device activity logs in Azure.

The device activities are available through the activity logs. This includes activities triggered by the device registration service or by the user such as - device creation and adding owners or users on the device, changes to device settings and device operations such as deleting or updating a device.

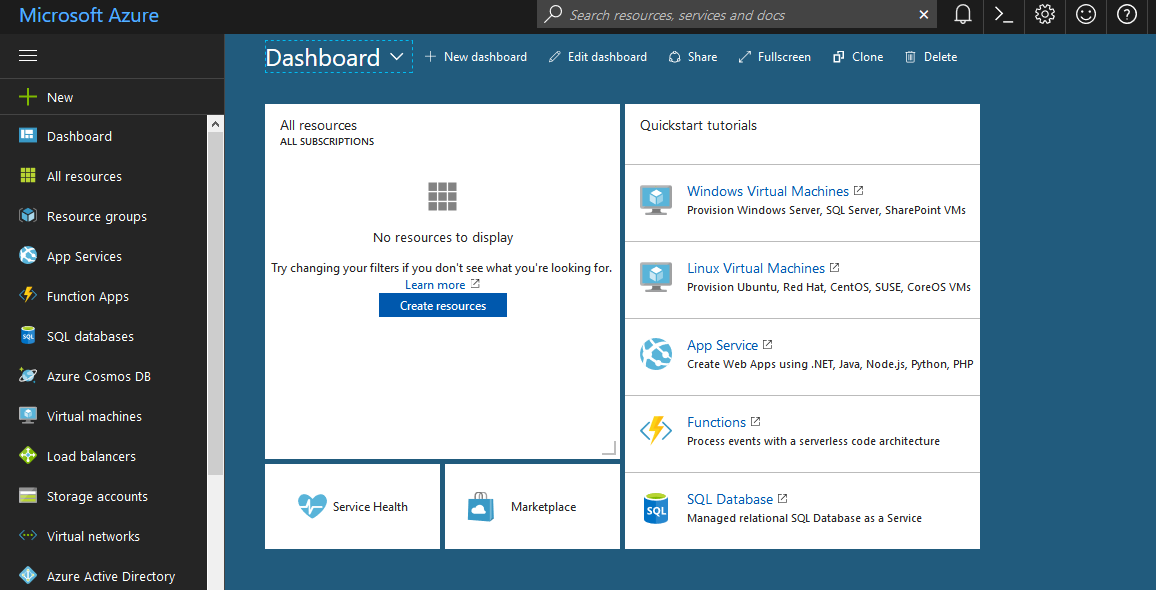
**Prerequisite:** EMS Enterprise Mobility + Security E5.

**Steps:**

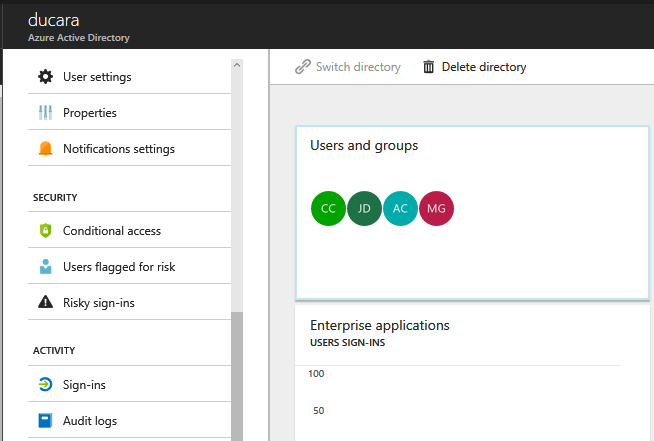
1. Sign in to your Azure Portal, by using the link - **https://portal.azure.com/**. Enter your credentials and click Sign In.



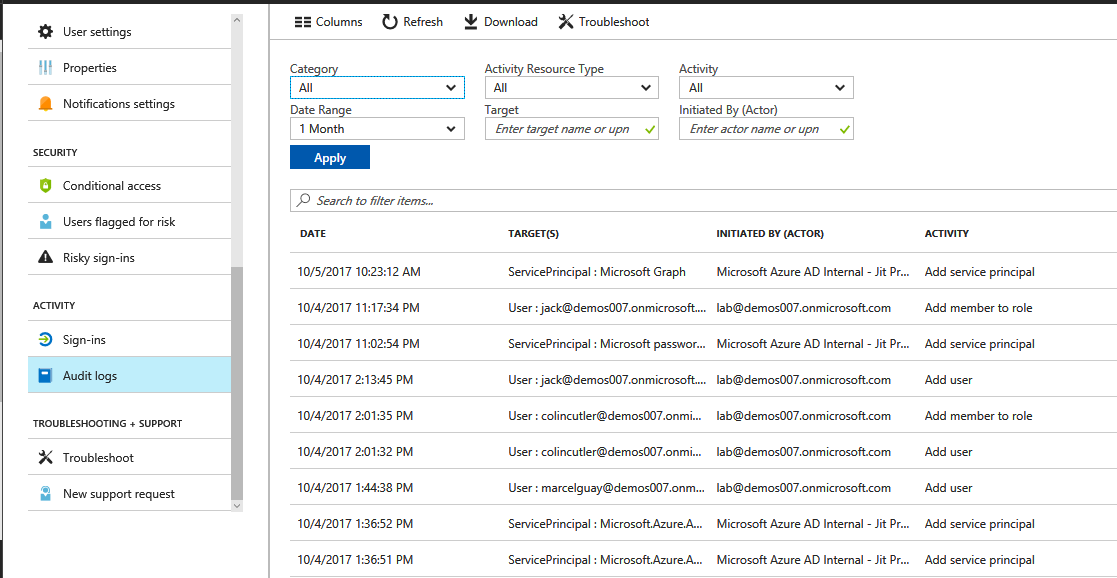
1. Microsoft Azure AD Dashboard will open.



1. Now click **Azure Active Directory** from left-hand pane, and then select **Audit Logs** in the **Activity** section.



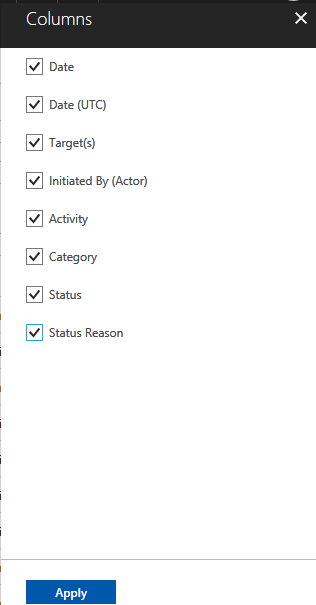
1. After clicking **Audit Logs**, an audit log table will open that has a default list view that shows: the date and time of the occurrence, the targets, the initiator or the actor (who) of an activity and the activity (what).



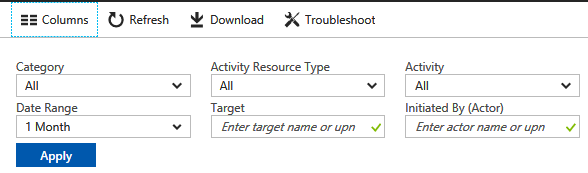
1. You can customize the list view by clicking **Columns** in the toolbar.



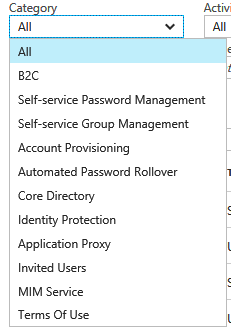
1. You can check/uncheck the options like – Date, Date (UTC), Targets, Initiated By (Actor), Activity, Category, Status, and status reason. And, click **Apply**.



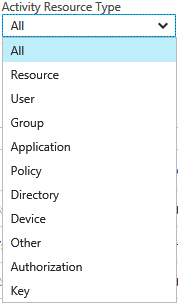
1. To narrow down the reported data to a level that works for you, you can filter the audit data using the fields: Category, Activity resource type, Activity, Date range, Target and Initiated By (Actor).



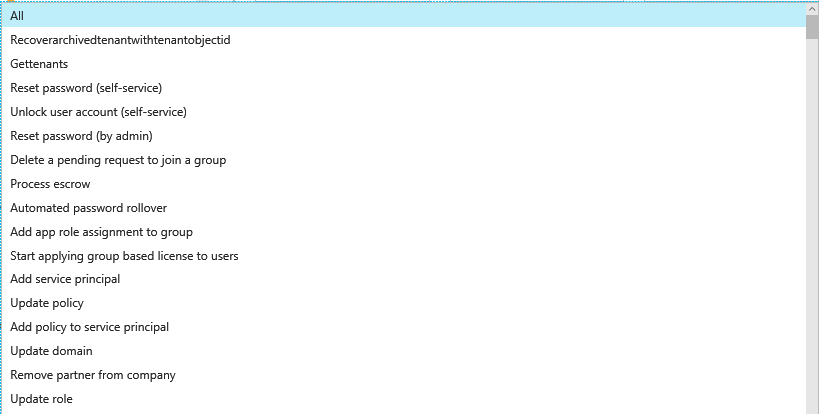
1. You can select a Category list menu and choose which type of activity you want to get. Like – B2C, Self-service Password Management, Self-service Group Management, Account Provisioning, Automated Password Rollover, Core Directory, Identity Protection, Application Proxy, Invited Users, MIM Service and Terms of Use.



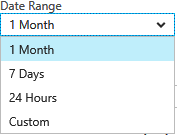
1. In Activity Resource Type, you will get – Resource, user, group, application, policy, directory, device, other, authorization, and key.



1. In Activity, you can select which type of audit data you want to filter. Like – Gettenants, Reset Password (Self-service), unlock a user account, Rest Password (by admin) etc.



1. In data range, you will get – 1 month, 7 days, 24 hours and also you can customize.



1. In the target field, you can enter can enter the target name.



1. And, in the Initiated By (Actor) field, you can enter the actor name.



1. You can also download the audit logs by clicking **Download** in the toolbar.



1. So, in this way you can check device activity logs in Azure AD.