**Lab – 32: Use the investigation tools in Cloud App Security.**

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

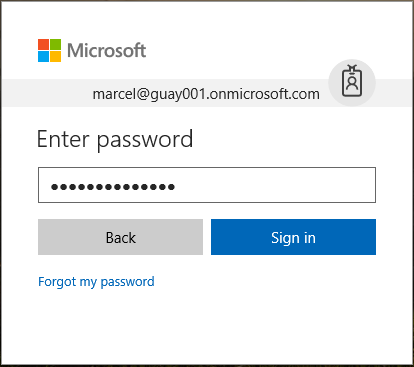
* To learn how to use the investigation tools in Cloud App Security.

Use the investigation tools in Cloud App Security to gain a deeper understanding of what's happening in your cloud environment. Basically, based on your particular environment and how it's being used, you can identify the requirements for protecting your organization from risk.

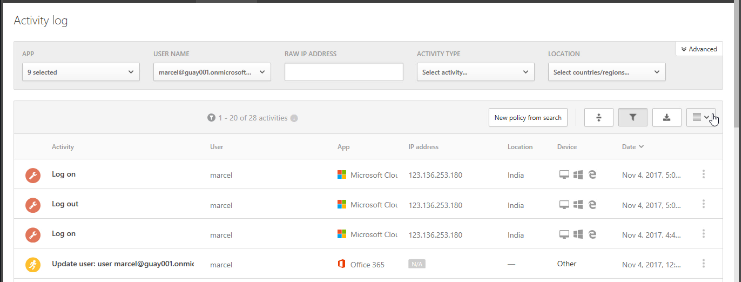
**Prerequisite:** EMS Enterprise Mobility + Security E5. To set up Cloud App Security, you must be a Global Administrator, a Compliance Administrator or a Security Reader in Azure Active Directory or Office 365.

**Steps:**

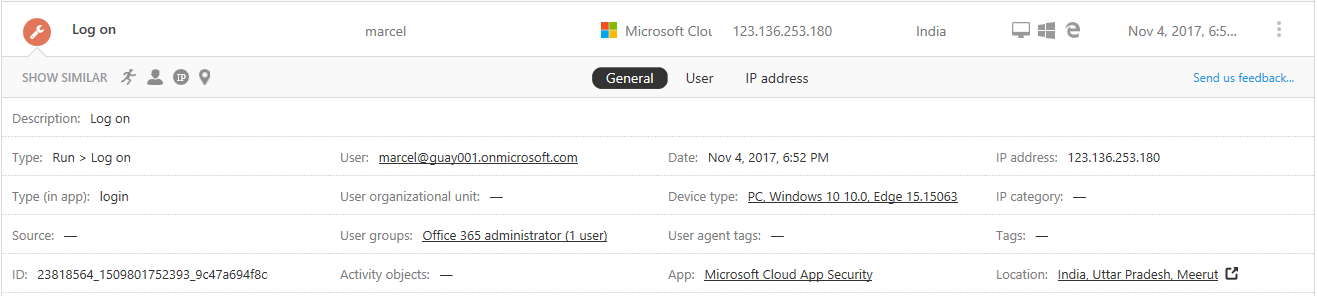
1. To access the Cloud App Security portal, go to <https://portal.cloudappsecurity.com>.



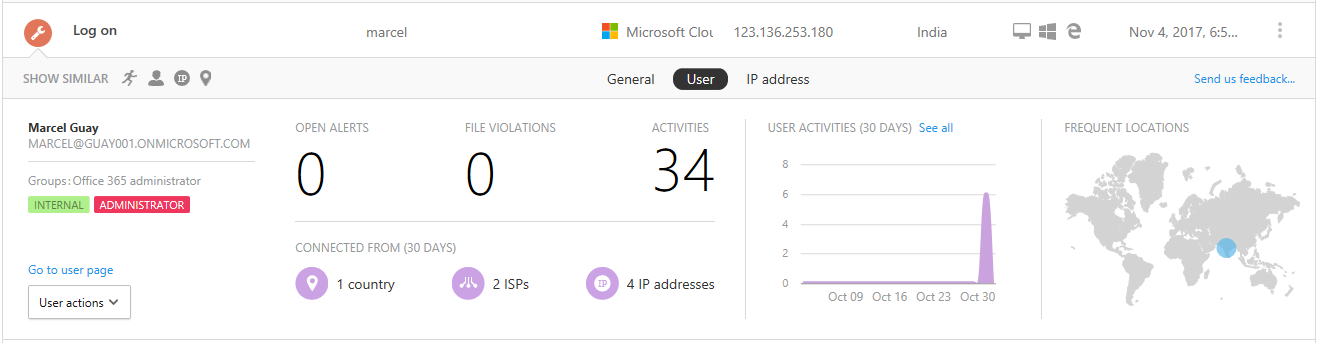
1. When you sign-in to Cloud App Security a general dashboard will be shown.
2. In the Cloud App Security portal, go to **Investigate** and then look at the **Activity log** and filter by a specific app and choose a specific user. And, Check the information like - Who is accessing your cloud environment, From what IP ranges, What is the admin activity, From what locations are admins connecting, Are any outdated devices connecting to your cloud environment, Are failed logins coming from expected IP addresses?



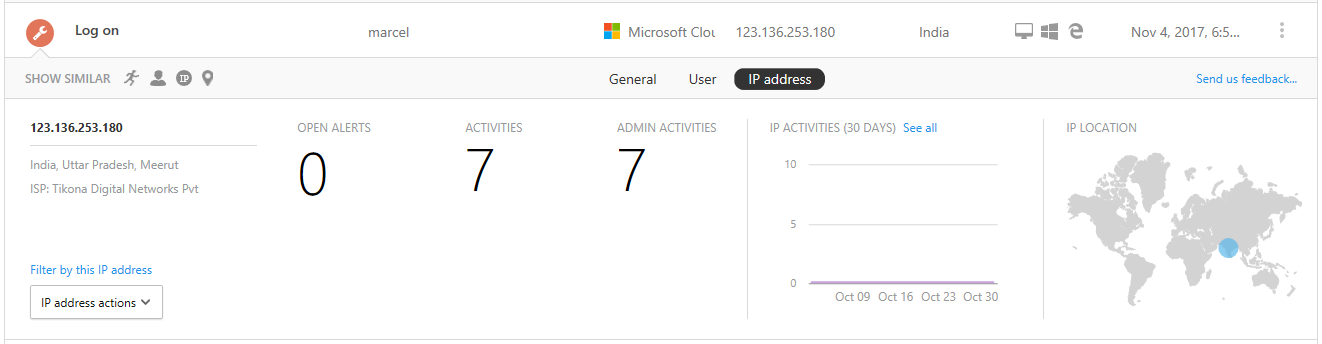
1. Select any activity from the list and in the general tab get information like – Description, Type, User, Date, IP address, User organizational unit, Device type - PC, Windows 10 10.0, Edge 15.15063, IP category, Source, User groups, User agent tags, Tags, ID, Activity objects, App - Microsoft Cloud App Security, Location, ISP.



1. Then select **User** tab, and get information like – user, groups (internal or administrator), open alerts, file violations, activities, connected from (Country, ISPs and IP Addresses), user activities graph and frequent locations.

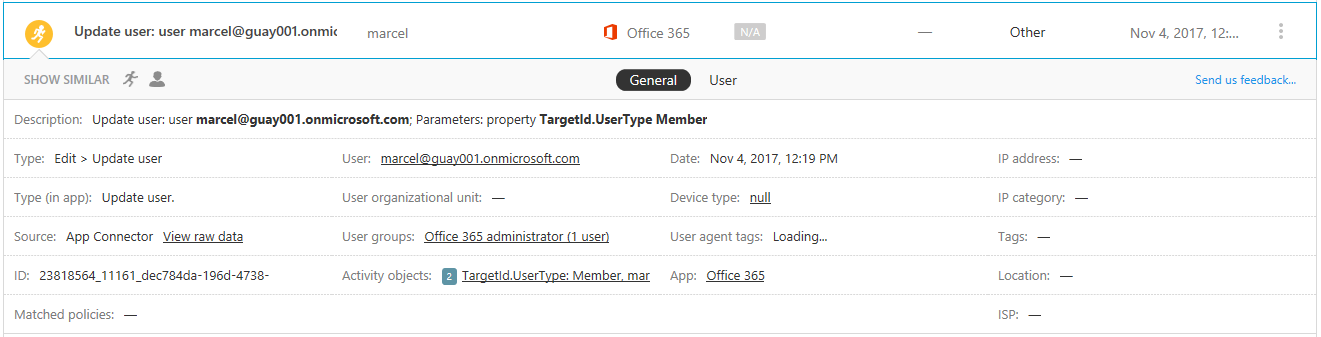


1. Then select IP address tab, and get information like – IP address of the log on machine, location, ISP, open alerts, activities, admin activities, IP activities and IP Location.

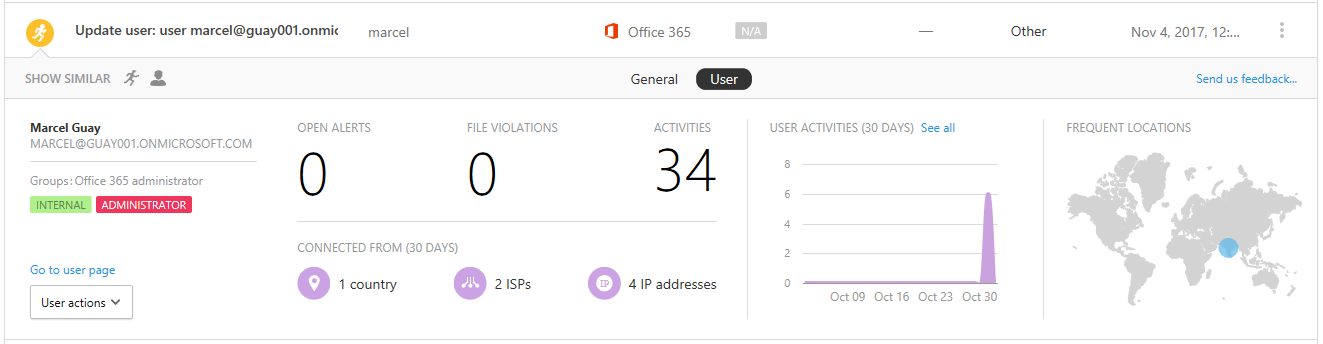


1. In this way, you can investigate for each activity. Select any other activity and investigate according to their information tabs.

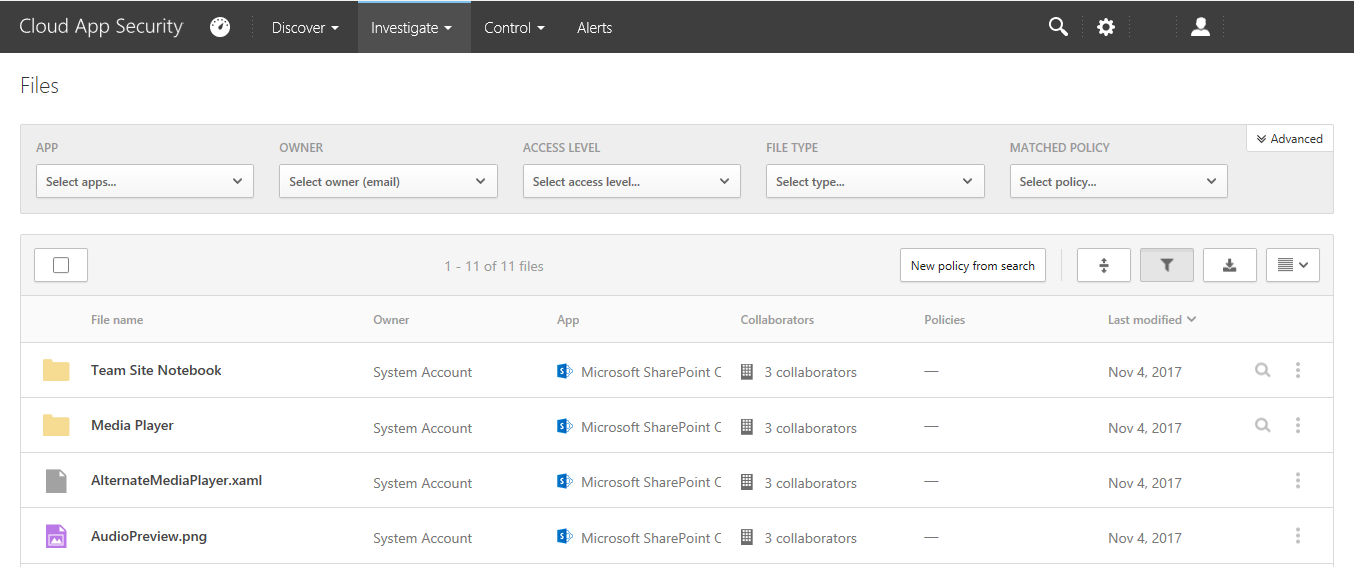
In general tab:



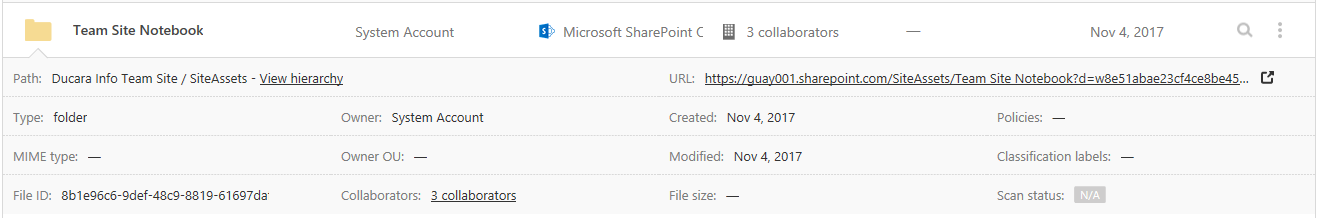
In User tab:



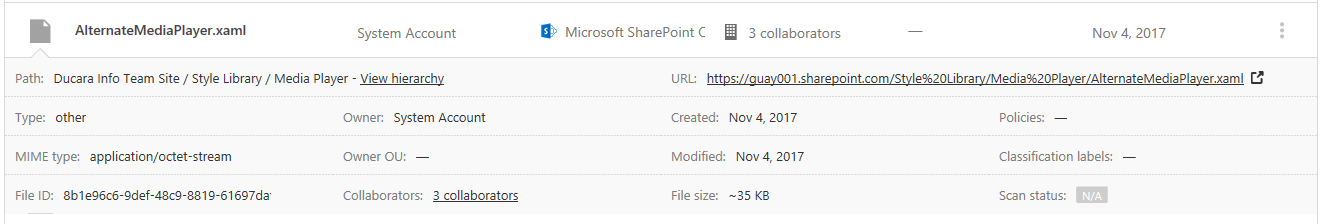
1. Select activities, it will redirect you to the activity log page.
2. Go to **Investigate** and then **Files**, and check the information - How many files are shared publicly so that anyone can access them without a link, With which partners are you sharing files (outbound sharing), Do any files have a sensitive name, Are any of the files being shared with someone's personal account?



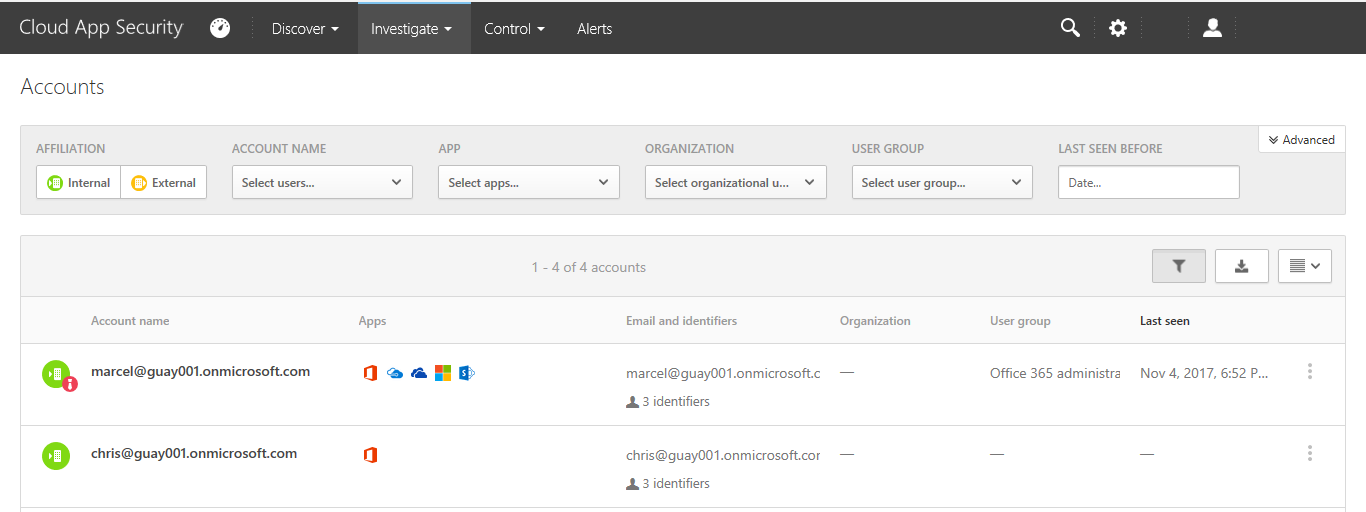
1. You can also apply filter for app, owner, access level, file type and matched policy. Select any file to get the complete information – path, type, MIME type, File ID, Owner, collaboration, URL, Created, Modified, File size, policies, classification labels and scan status.



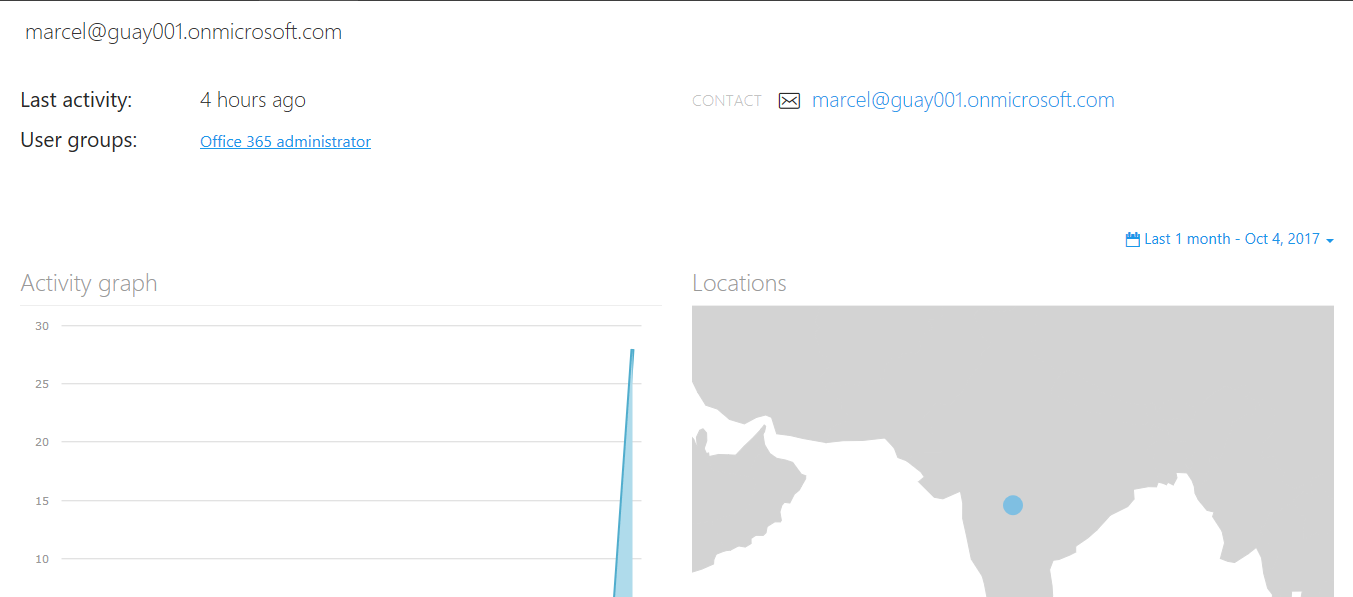
1. In the same way, select any other file and investigate.



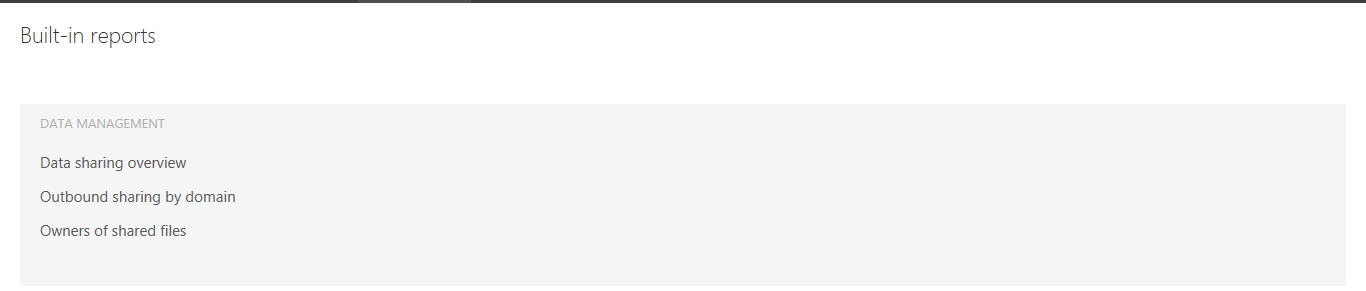
1. Now go to **Investigate** and then **Accounts**, and check the information - Have any accounts been inactive in a particular service for a long time? (Maybe you can revoke the license for that user to that service?), Do you want to know which users have a specific role?, Was someone fired but they still have access to an app and can use that access to steal information?, Do you want to revoke a user's permission to a specific app or require a specific user to perform multi-factor authentication? Get a list of accounts having their details - account name, apps, email and identifiers, organization, user group and last seen



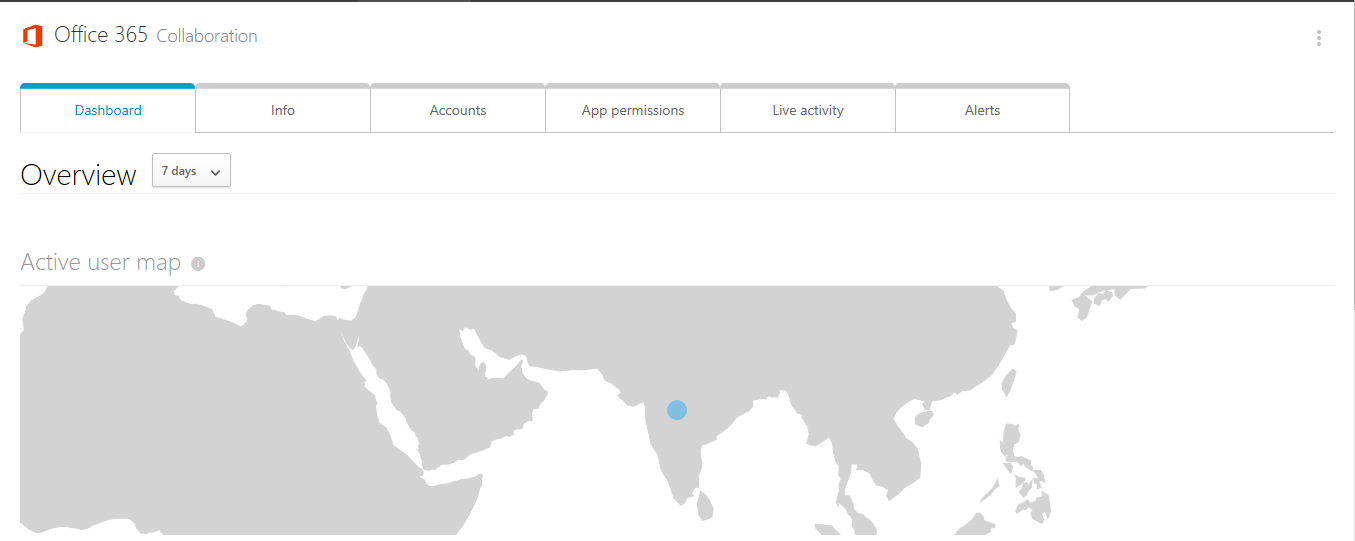
1. Select any account and get complete information about that account, like – last activity, user group, contact, activity graph, locations, apps, devices, accounts filtered by the username, alerts, activity log, files with policy matches filtered by the username and reports filtered by the username.



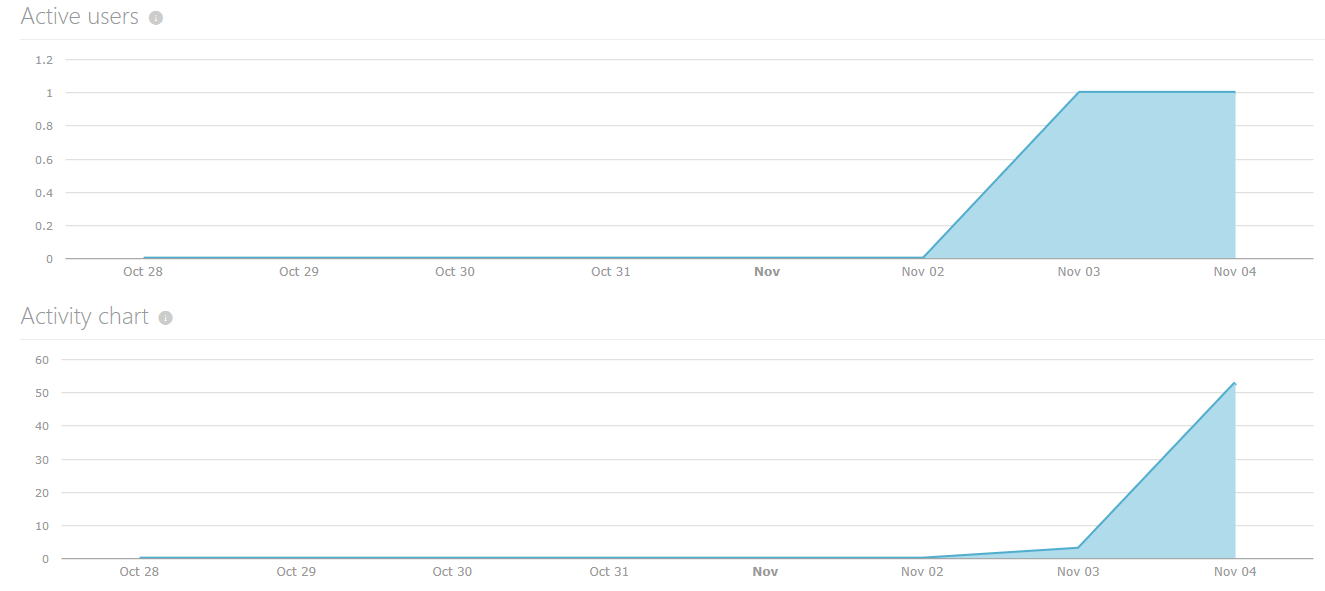
1. Then go to **Investigate** and then **built-in reports**. This information is categorized into – Data sharing overview, outbound sharing by domain and owners of shared files.



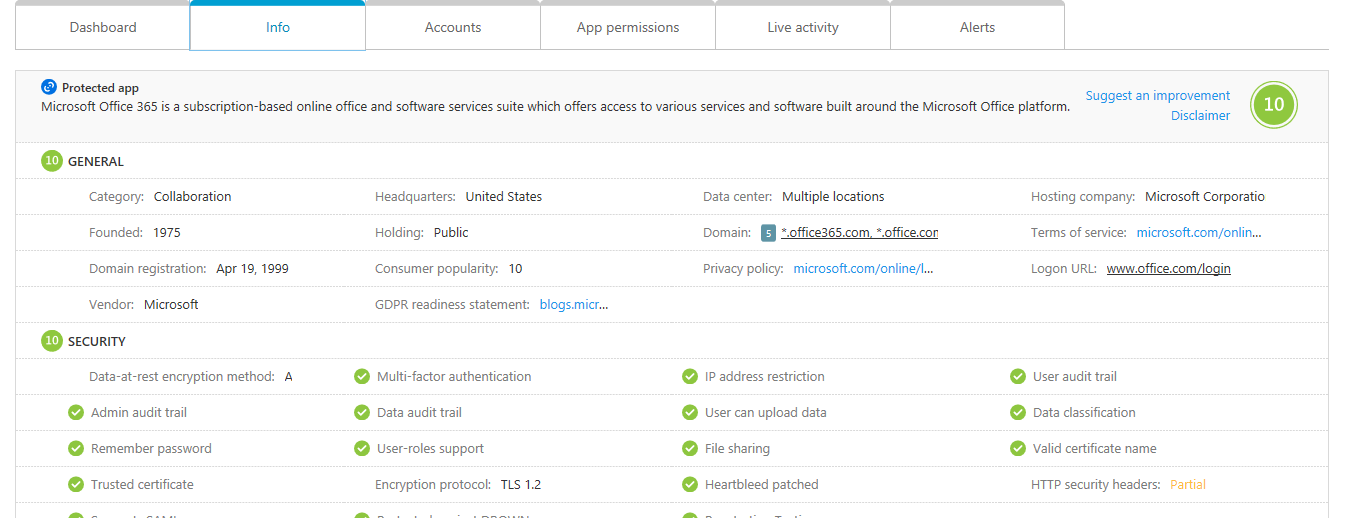
1. Go to **Investigate** and then select an app. The app dashboard opens and gives you information and insights. You can use the tabs across the top to check the complete information - What kind of devices are your users using to connect to the app?, What types of files are they saving in the cloud?, What activity is happening in the app right now?, Are there any connected third-party apps to your environment?, Are you familiar with these apps?, Are they authorized for the level of access they are permitted to?, How many users have deployed them? How common are these apps in general?



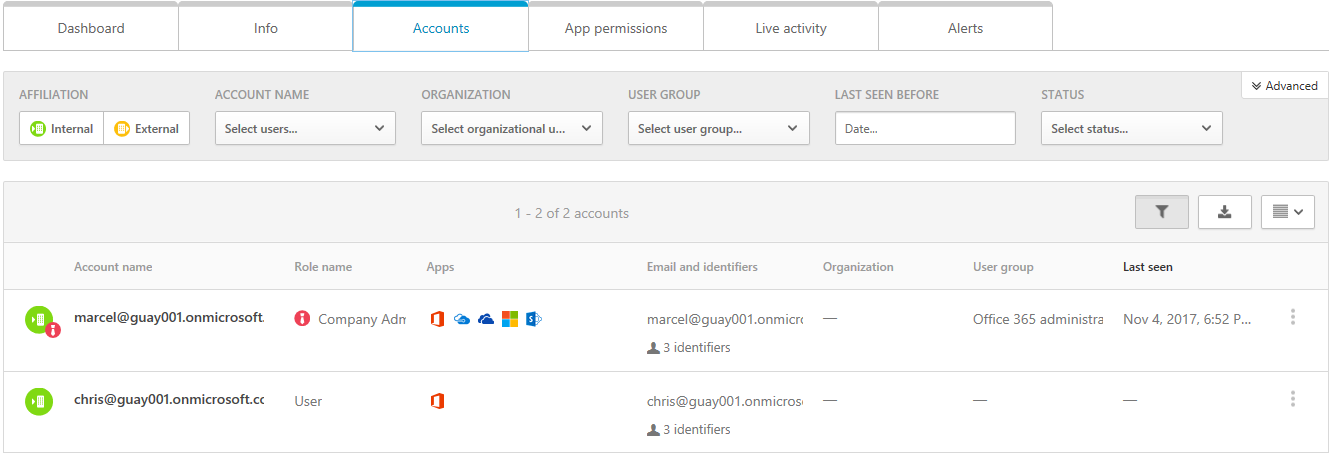
1. In the **dashboard** view of an app, see active user map, active users and activity chart.



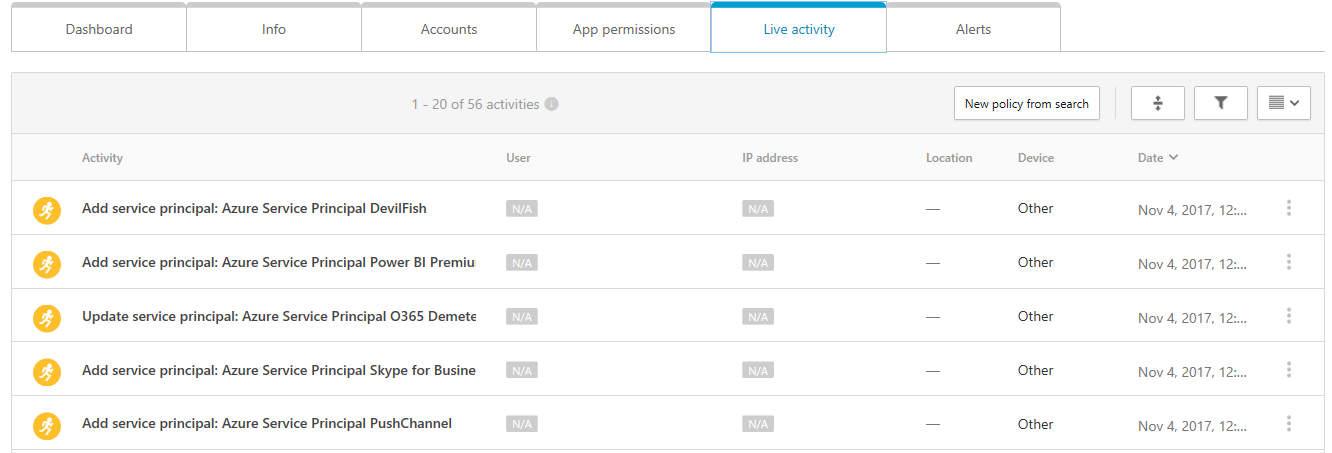
1. Click **Info** tab and view information about the selected app in the general, security and compliance section.



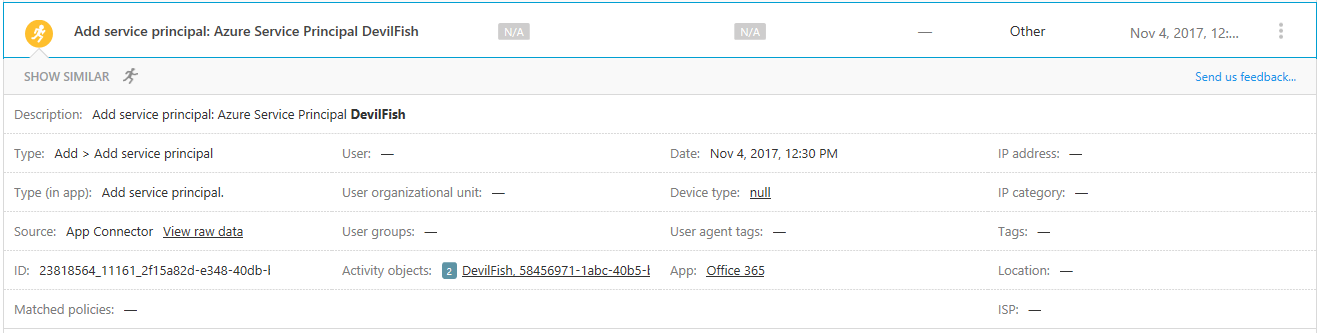
1. Click **Accounts** tab and view accounts information like – account name, role name, apps, email and identifiers, organization, user group and last seen.



1. Click **App permissions** tab to get apps details.
2. Then select live activity tab, to view the live activity information.



1. Select any activity to get complete view of that activity.



1. Then select **Alerts** tab, to get the information about the alerts.
2. So, in this way you can use the investigation tools in Cloud App Security to gain a deeper understanding of what's happening in your cloud environment.