**Lab – 29: Set up Cloud Discovery.**

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

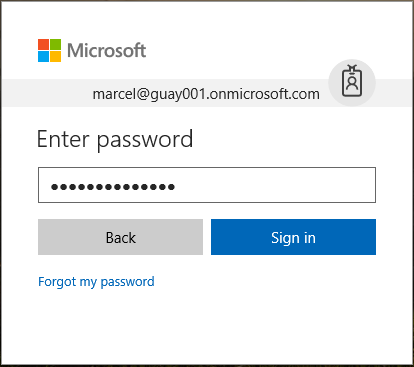
* To set up Cloud Discovery.

Cloud App Security can help you take advantage of the benefits of cloud applications while maintaining control of your corporate resources. It works by improving visibility of cloud activity, and helping to increase the protection of corporate data. In this lab, we are going to set up Cloud Discovery.

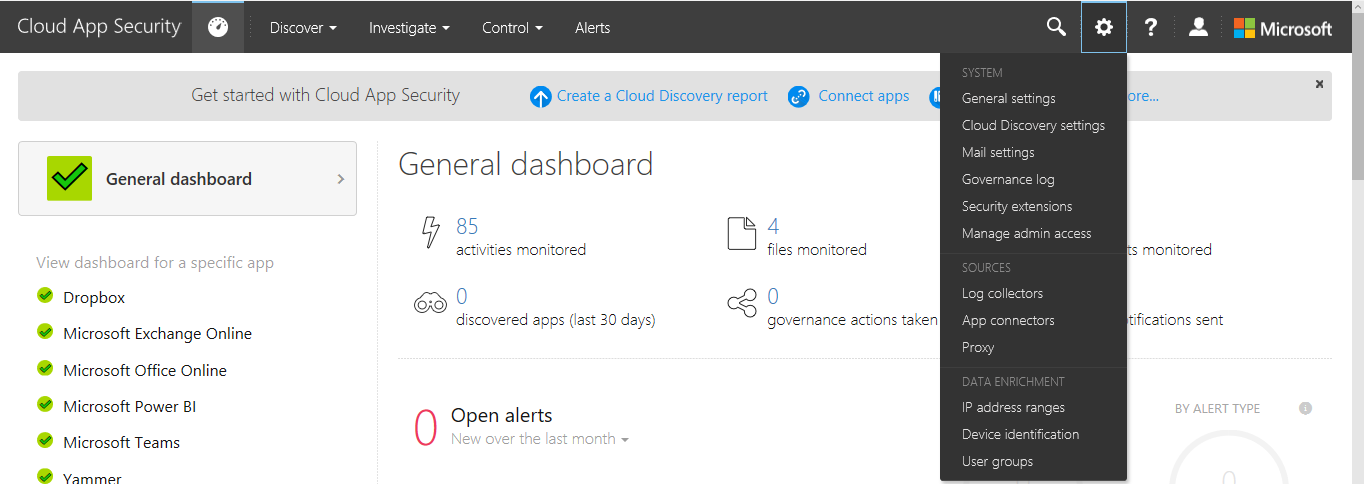
**Prerequisite:** EMS Enterprise Mobility + Security E5. To set up Cloud App Security, you must be a Global Administrator, a Compliance Administrator or a Security Reader in Azure Active Directory or Office 365.

**Steps:**

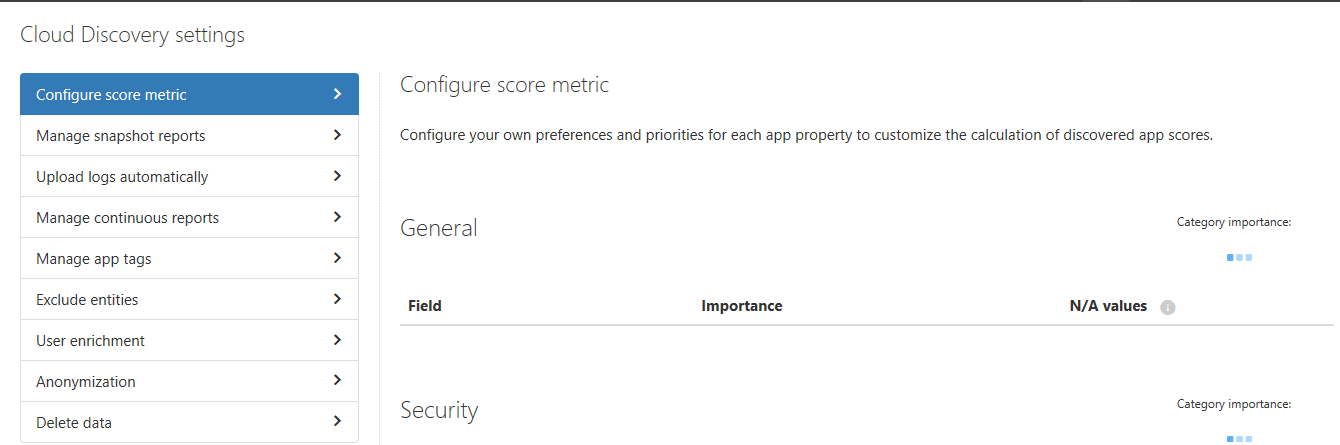
1. To access the Cloud App Security portal, go to <https://portal.cloudappsecurity.com>.



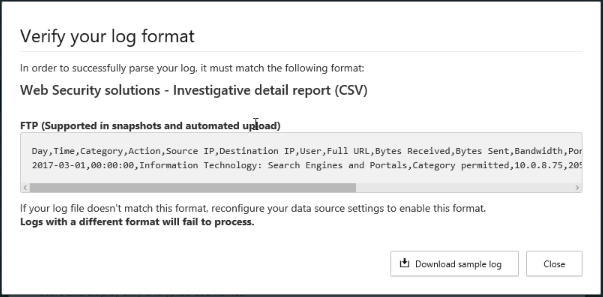
1. When you sign-in to Cloud App Security a general dashboard is shown.
2. Go to **Settings** > **Cloud Discovery settings**.



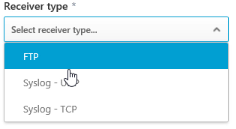
1. Choose **Upload log automatically**, from the left-hand side menu.



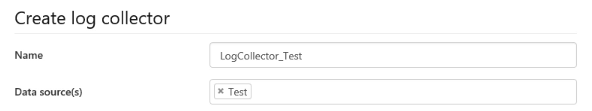
1. To create and manage your organization's data sources. On the **Data sources** tab, in Upload log automatically page **add data sources**. Click **add data source**, then enter the field **Name**, select data **Source** from the menu from which you want the log files.
2. Click **view sample of expected log file and you can compare it with yours**, click **Download sample log** and save this sample log file in your PC. The FTP sample format is supported in snapshots and automated upload while syslog is supported in automated upload only. Downloading a sample log will download a sample FTP log.



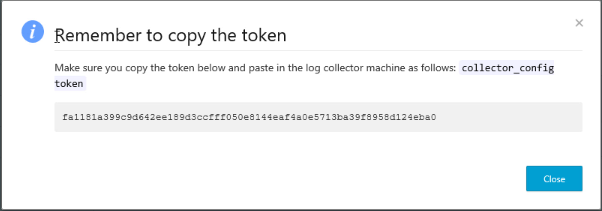
1. Then select **Receiver type**. You have three options – FTP, Syslog-UDP and Syslog-TCP. And, click **Add**.



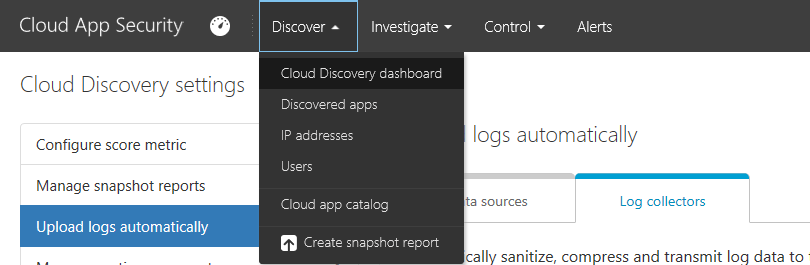
1. Now, a log collector machine needs to be deployed. On the **Log collectors** tab, configure the log collector to automatically sanitize, compress and transmit log data to the portal. Click **Add Log Collector** and enter the field **Name** and select a **data source**(s) that you have created. Then click **Update** and **Close**.



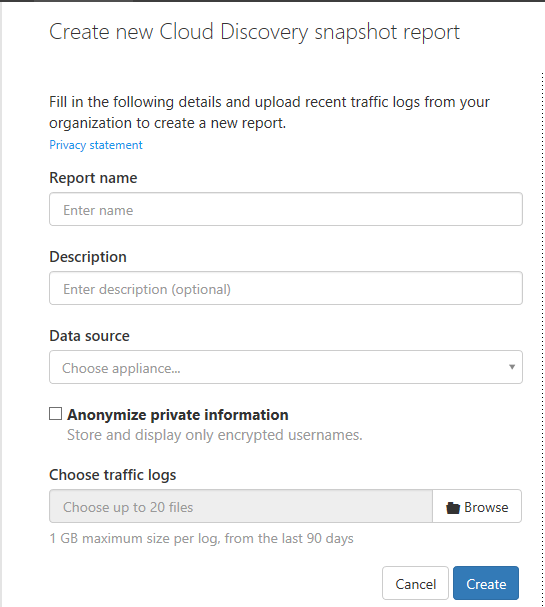
1. Remember to copy the token pop-up will appear, make sure to copy this token and paste it in the log collector machines. Click **Close**.



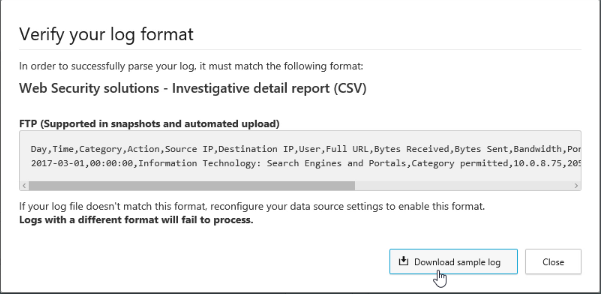
1. So, in this way you can create and manage your organization’s data sources.
2. Now go to **Discover** > **Create new snapshot report (Create Snapshot report)**.



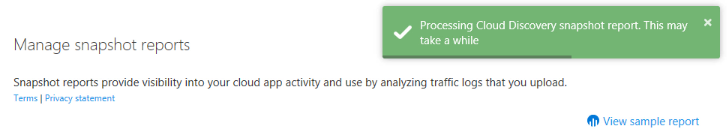
1. Create new Cloud Discovery snapshot report page will open. Here, fill in the details and upload recent traffic logs from your organization to create a new report.



1. Enter Report Name, Description.
2. Select the **Data source** from which you want to upload the log files.
3. Verify your log format to make sure that it is formatted properly according to the sample you can download. Click **View and verify** and then click **Download sample log**. Then compare your log with the sample provided to make sure it's compatible. The FTP sample format is supported in snapshots and automated upload while syslog is supported in automated upload only. Downloading a sample log will download a sample FTP log.



1. **Choose the traffic logs** that you want to upload. You can upload up to 20 files at once. Compressed and zipped files are also supported. Click **Create**.
2. After upload completes, the status message will appear at the top right corner of your screen letting you know that **Cloud Discovery snapshot report is in process, this may take a while**.



1. Table will show Name, Data Source, Logs, Date added, Added by and Status. After processing of your log files completes, you will receive an email to notify you that it is done.

