



# Lab – Microsoft Cloud App Security

Moving to the cloud increases flexibility for employees and IT alike. However, it also introduces new challenges and complexities for keeping your organization secure. To get the full benefit of cloud apps and services, an IT team must find the right balance of supporting access while maintaining control to protect critical data.

Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

Microsoft Cloud App Security natively integrates with leading Microsoft solutions and is designed with security professionals in mind. It provides simple deployment, centralized management, and innovative automation capabilities.

Want to learn more, click [here](#).

## Lab Parts

This lab contains three activities, as shown below:

- Pre-requisites
- Part 1 – Ingest Data
- Part 2 – Explore a Snapshot Report
- Part 3 - Blocking Risky Apps
- Part 4 – Shadow IT Discovery Report

## Pre-requisites

### Step 1 – Create Demo Tenant

Before you start you should have completed the “Getting started with Labs”. If you have not completed this, you will not be able to do this lab. You can find this document which you can download from <https://aka.ms/secpractice-labs>.

Each tenant can take up to 24 hours to provision so it’s important that you complete this prior to when the labs are to be run.

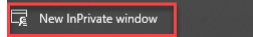
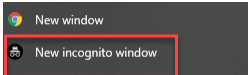
NB – If you already created your demo tenant as part of the Identity Labs you **DO NOT** need to do this again.

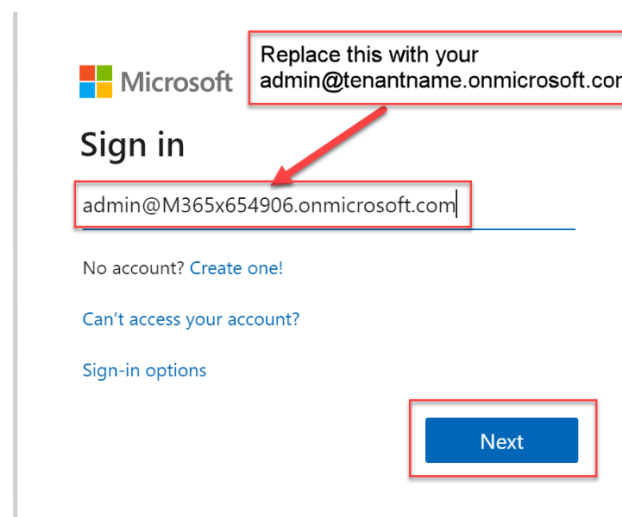
## Step 2 – Create yourself an Admin account for your demo tenant.

*NB – If you already created your **ADMIN ACCOUNT** as part of the Identity Labs you **DO NOT** need to do this again. Please use the same account that you created in the Identity labs. [Go straight to Part 1](#)*

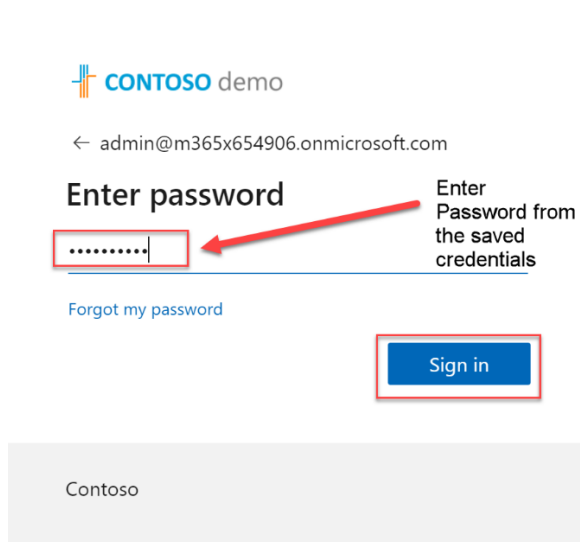
In this task, you will create a Microsoft 365 user account for yourself, and assign your account the Microsoft 365 Global Administrator role, which gives you the ability to perform all administrative functions within Microsoft 365.

**Important:** As a best practice in your real-world deployments, you should always write down the first global admin account's credentials (in this lab, the MOD Administrator) and store it away for security reasons. This account is a non-personalized identity that owns the highest privileges possible in a tenant. It is **not** MFA activated (because it is not personalized) and the password for this account is typically shared among several users. Therefore, this first global admin is a perfect target for attacks, so it is recommended to create personalized service admins and keep as few global admins as possible. For those global admins that you do create, they should each be mapped to a single identity, and they should each have MFA enforced.

1. Open an In-private browser (Edge)  or New in-Cognito (Chrome)  on your machine and then go to <https://admin.microsoft.com/>
2. Enter the admin account username that you saved in "Getting started with Microsoft Labs" to gain credentials.
3. Enter your admin credentials in the sign in as below and click NEXT



4. Enter the password and then click "Sign in"



5. In the **Microsoft 365 admin center**, in the left navigation pane, select **Users** and then select **Active users**.
6. In the **Active users** list, you will see the default **MOD Administrator** account as well as some other user accounts.
7. In the **Active Users** window, select **Add a user**.
8. In the **Set up the basics** window, enter the following information:
  - First name: **Your First Name**
  - Last name: **Your Last Name**
  - Display name: When you tab into this field, **YOUR NAME** will appear.
  - Username: When you tab into this field, **YOURFIRSTNAME-LASTNAME** may appear; if not enter this as the username

**IMPORTANT:** To the right of the **Username** field is the domain field. select the **M365xZZZZZ.onmicrosoft.com** cloud domain.

After configuring this field, **YOUR username** should appear as:

[YOURNAME@M365xZZZZZ.onmicrosoft.com](mailto:YOURNAME@M365xZZZZZ.onmicrosoft.com)

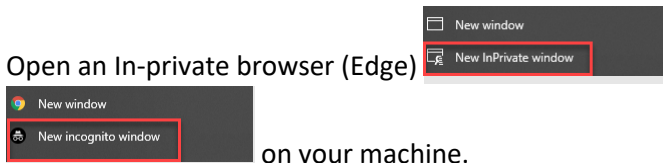
- Password settings: select the **Let me create the password** option.
  - Password: **Set your own complex Password**
  - Uncheck the **Require this user to change their password when they first sign in** checkbox.
9. Select **Next**.
  10. In the **Assign product licenses** window, enter the following information:
  11. Select location: **United States (Your Location)**
  12. Licenses: Under **Assign user a product license**, select **Office 365 E5** and **Enterprise Mobility + Security E5** or if you have **Microsoft 365 E5** select this instead.
  13. Select **Next**.

14. In the **Optional settings** window, in the Roles section select **Admin center access** By doing so, all the Microsoft 365 administrator roles are now enabled and available to be assigned.
15. Select **Global Admin** and then select **Next**.
16. On the **Review and finish** window, review your selections. If anything needs to be changed, select the appropriate **Edit** link and make the necessary changes. Otherwise, if everything is correct, select **Finish adding**.
17. Once your new username **has been added to active users** page, select **Close**.

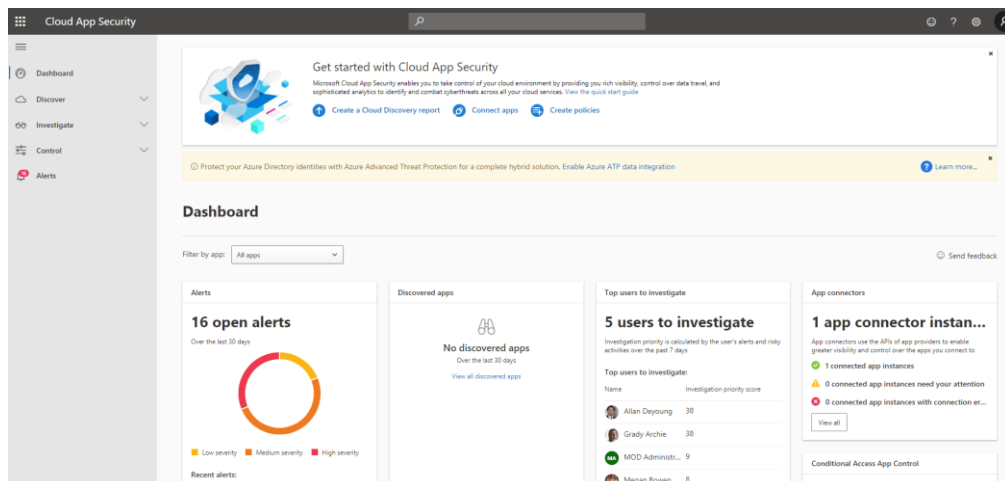
# Part 1 – Ingest Data, Generate Snapshot Report -

In this part you will download a demo log file from a data source and then proceed to create a new Snapshot report using that data as the source. This will give you a rich set of data to explore and demo the product.

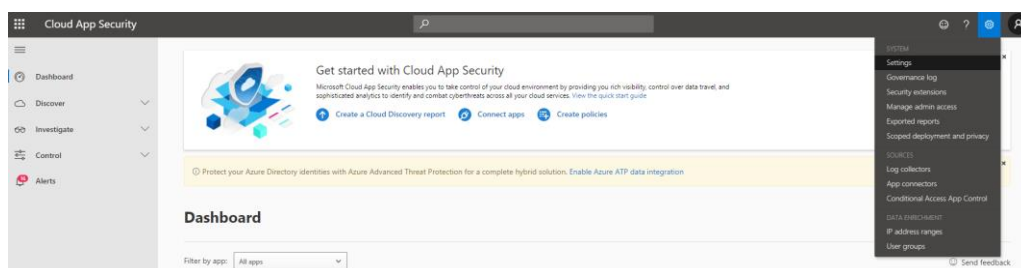
1. Open an In-private browser (Edge) or New in-Cognito (Chrome)



2. Navigate to <https://portal.cloudappsecurity.com/>.
3. Sign in with **Global Admin** account that you created in the Pre-requisites.



4. Navigate to the cog in the top right-hand corner and click on Settings.



5. Within Settings, click on Automatic Log Upload and then click on Add Data Source.

## Settings

Search

System

- Organization details
- Mail settings
- Export settings
- Automatic sign out
- Activity privacy
- Cloud Discovery
- Score metrics
- Snapshot reports
- Continuous reports
- Automatic log upload**
- App tags
- Exclude entities
- Microsoft Defender ATP
- User enrichment

### Automatic log upload

**Data sources** | Log collectors

Create and manage your organization's data sources.  
[Terms](#) | [Privacy statement](#)

No data sources found

**Add data source...**

Name	Source	Receiver type	Uploaded logs	Last data received	Modified date
------	--------	---------------	---------------	--------------------	---------------

There are no data sources

- Under Source, open the drop down and scroll down to and select Microsoft Forefront Threat Management Gateway (W3C).

### Add data source

**Name \***

**Source \***


Select appliance...

- Juniper SRX Welf
- Juniper SSG
- McAfee**
- McAfee Web Gateway
- Microsoft**
- Microsoft Forefront Threat Management Gateway (W3C)**
- Palo Alto
- PA Series Firewall
- PA Series Firewall LEEF
- Sophos

**Comment**

**Add** **Cancel**

- Once selected you can click on View sample of expected log file.

 Add data source

Name \*

Source \*

Microsoft Forefront Threat Management Gateway (W3C) ▼

[View sample of expected log file, and compare it with yours](#)

Receiver type \*

Select receiver type... ▼

☐ Anonymize private information  
Store and display only encrypted usernames.

Add Cancel

8. On the next screen, click on Download sample log.

## Verify your log format

In order to successfully parse your log, it must match the following format:

### Microsoft Forefront Threat Management Gateway (W3C)

#### FTP (Supported in snapshots and automated upload)

```
#Fields: c-ip cs-username c-agent sc-authenticated date time s-svcname s-comp s-username cs-re
192.168.1.1 USERNAME Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

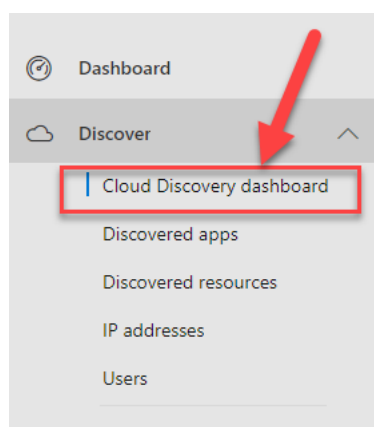
If your log file doesn't match this format, reconfigure your data source settings to enable this format.

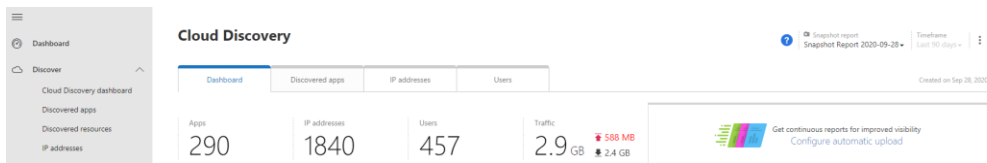
**Logs with a different format will fail to process.**

Download sample log

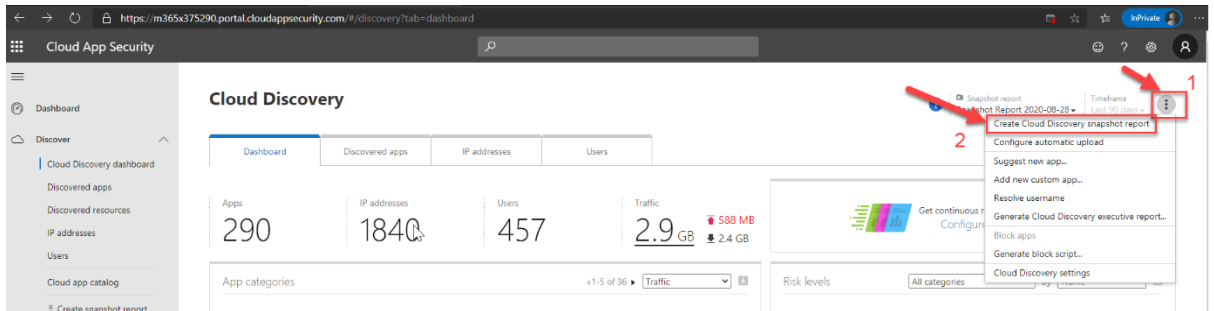
Close

9. The sample log will download – take note of the download location.
10. Return to the Cloud Discovery Dashboard.





11. Near the top-right of the Dashboard – Click on the down Elipse and select “Create Cloud Discovery Snapshot report”



12. Create a new Cloud Discovery snapshot report.

- Provide a Report name, e.g. MCAS Lab Report Demo.
- Description – leave blank
- Data Source – Select Microsoft Forefront Threat Management Gateway (W3C).
- Anonymize private information – leave unchecked.
- Choose traffic logs – click on Browse and navigate to the log file you downloaded in step 8.



## Create new Cloud Discovery snapshot r...



Fill in the following details and upload recent traffic logs from your organization to create a new report.

[Privacy statement](#)

Report name

MCAS Lab Report Demo.

Description

Enter description (optional)

Data source

Microsoft Forefront Threat Management Gateway (W3C)

### Verify your log format

Important: make sure your logs are in the right format.

**Logs with a different format will fail to process**

[View and verify...](#)



Anonymize private information

Store and display only encrypted usernames.

Choose traffic logs

microsoft-forefront-threat-management-gateway-w3c\_dei



1 GB maximum size per log, from the last 90 days

Cancel

Create

### Report creation process

⌚ Analysis takes up to 24 hours | [Track status](#)

- Upload
- Parse
- Data analysis
- Generate report



[View sample report](#)

13. Click on Create.

14. You will then be taken to the Snapshot reports screen where you can see the status of the report you just created.

### Snapshot reports

Snapshot reports provide visibility into your cloud app activity and use by analyzing traffic logs that you upload.

[Terms](#) | [Privacy statement](#)

[View sample report](#)

1 - 5 of 5 snapshot reports					
Create snapshot report					
Name	Data source	Logs	Date added	Added by	Status
MCAS Lab Report Demo	Microsoft Forefront Threat Mana...	1	Sep 29, 2020	admin@M365x504983.onmicroso...	Processing

15. After a few moments refresh the screen and the status should update to Ready.

### Snapshot reports

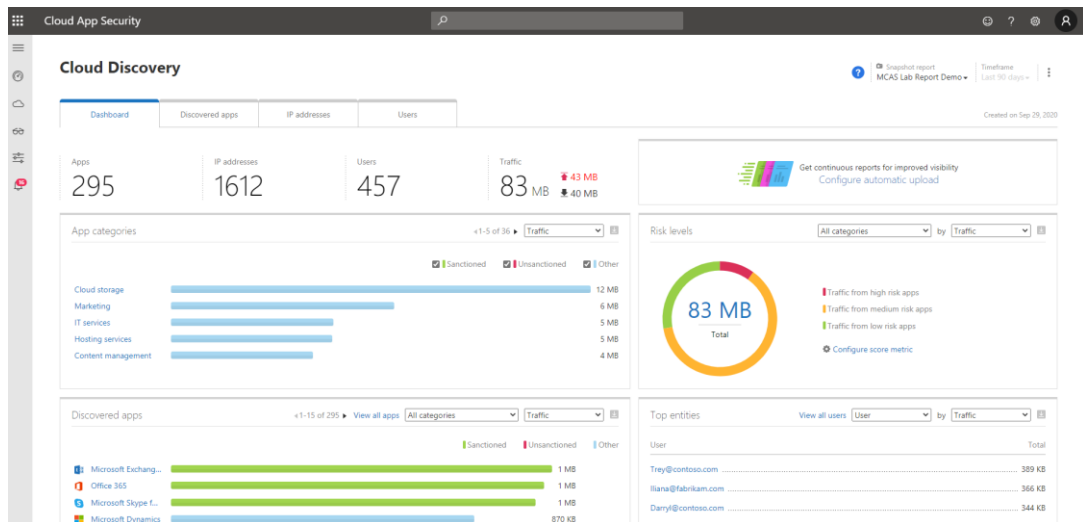
Snapshot reports provide visibility into your cloud app activity and use by analyzing traffic logs that you upload.

[Terms](#) | [Privacy statement](#)

[View sample report](#)

1 - 5 of 5 snapshot reports					
Create snapshot report					
Name	Data source	Logs	Date added	Added by	Status
MCAS Lab Report Demo	Microsoft Forefront Threat Mana...	1	Sep 29, 2020	admin@M365x504983.onmicroso...	Ready

16. Click on your report to view the data.

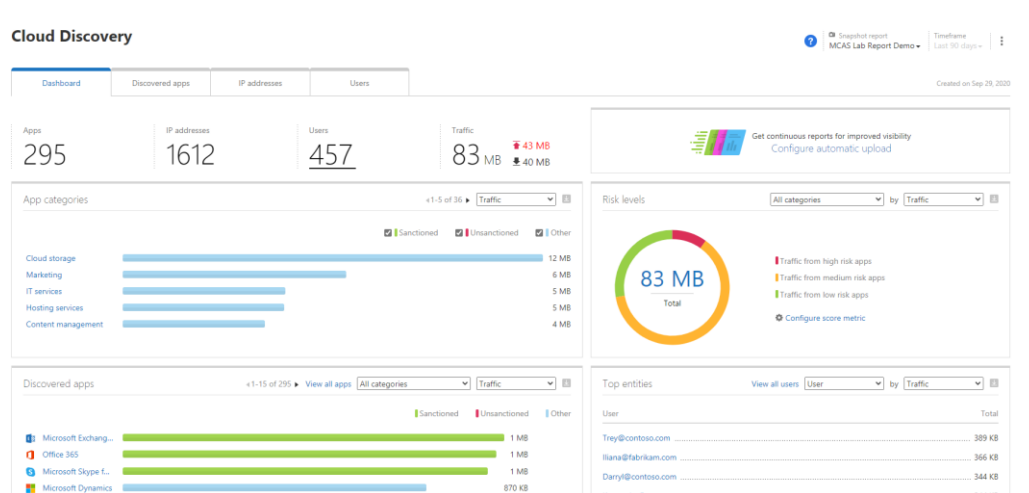


**Part 1 – Complete.**

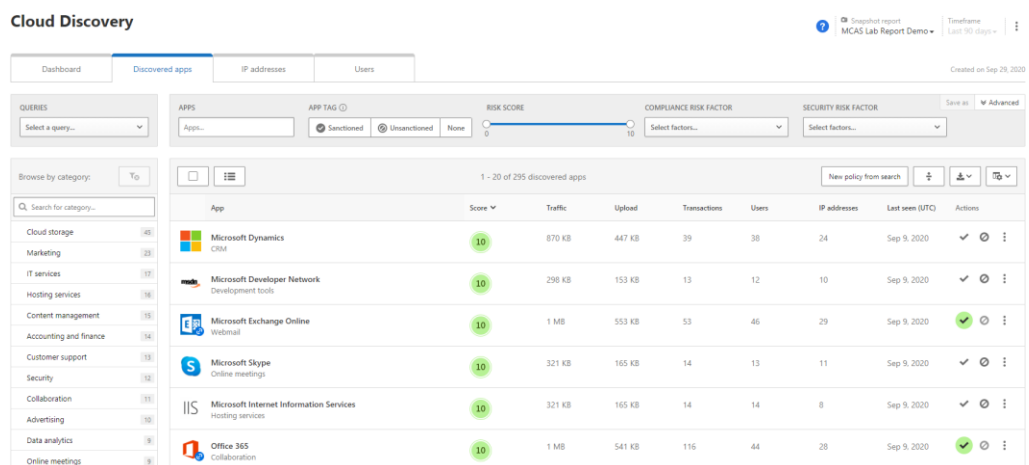
# Part 2 – Explore a Snapshot Report

Snapshot reports provide ad-hoc visibility on a set of traffic logs from your organization's firewalls and proxies. This allows you to see traffic at a point in time when trying to sleuth anomalous activities or detect specific data sets that would help pin down threat-based activities.

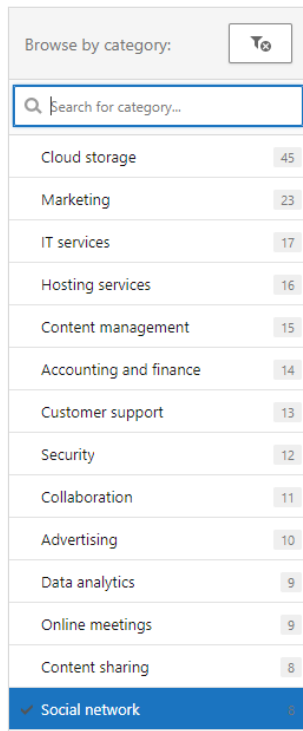
1. From the previous part you should be viewing the Snapshot Report you created.



2. The dashboard provides an all up view of the report. Here you can start exploring the discovered apps, users, and IP addresses. The dashboard page shows a summary of the discovered apps and their risks and categories.
3. Click on the **Discovered apps** tab to view more detailed information about the app information captured in the report.



4. Take the time to explore the various filters and options available on this tab.
5. Repeat for **IP Addresses** and **Users** tabs.
6. Return to the Discovered Apps tab. Click **Discovered apps** tab.
7. Under **Browse by category**, select **Social network**



- From the list of apps, click the whitespace next to **Facebook** (not the label itself) to show details.

In this example, the app **Facebook** was accessed by numerous users in the organization. MCAS has rated Facebook with a risk score of 5. Looking at the breakdown of this score, we can see that while Facebook scores highly for **security** factors, it scores a lowly 2 for **compliance** and **legal** factors. For example, this app does not fully preserve the user's ownership of uploaded data and does not comply with some GDPR policies. Hence, Facebook only scores an aggregate risk score of 5.

<b>SECURITY</b>			
Latest breach: Dec 8, 2019	Data-at-rest encryption method: AES	Multi-factor authentication	IP address restriction
User audit trail	Admin audit trail	Data audit trail	User can upload data
Data classification	Remember password	User-roles support	File sharing
Valid certificate name	Trusted certificate	Encryption protocol: TLS 1.2	Heartbleed patched
HTTP security headers	Supports SAML	Protected against DROWN	Penetration Testing
Requires user authentication	Password policy: Partial		
<b>COMPLIANCE</b>			
ISO 27001	ISO 27018	ISO 27017	ISO 27002
FINRA	FISMA	GAAP	HIPAA
ISAE 3402	ITAR	SOC 1	SOC 2
SOC 3	SOX	SP 800-53	SSAE 16
Safe Harbor	PCI DSS version: 1	GLBA	FedRAMP level: Not supported
CSA STAR level: Not supported	Privacy Shield	FFIEC	GAPP
COBIT	COPPA	FERPA	HITRUST CSF
Jericho Forum Commandments			
<b>LEGAL</b>			
Data ownership	DMCA	Data retention policy: Deleted within more th...	GDPR readiness statement: facebook.com/bu...
GDPR - Right to erasure	GDPR - Report data breaches	GDPR - Data protection	GDPR - User ownership: Partial

- Scroll to the **LEGAL** category, then hover mouse over and point to **Data Ownership** > info icon (i).

### Data ownership

Does this app fully preserve the user's ownership of uploaded data?

**Possible values:** Yes, No, N/A

**Source:** App website

0 /10      14%  
Property score      Weight in category

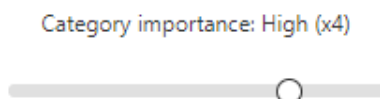
10. The risk aggregate scoring and prioritization can be customized to suit an organization's need. For example, if compliance factor is important, we can change the weighting accordingly.
11. Hover mouse over to the far-right of **LEGAL**, and then click **Configure score metric**.



12. In the **Score metrics** page, scroll down to **Compliance** category.

Compliance			Category importance: Medium (x2)
Field	Importance	N/A values	
<b>FINRA</b> Does this app comply with FINRA, a standard set by a non-profit organization authorized by the US Congress to regulate and enforce the protection of investors and safeguard market integrity?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	
<b>FISMA</b> Does this app comply with FISMA, the US legislation that defines a comprehensive framework to protect government information, operations and assets within federal agencies, against threats?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	
<b>GAAP</b> Does this app comply with GAAP, a collection of commonly-followed accounting rules and standards for financial reporting?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	
<b>HIPAA</b> Does this app comply with HIPAA, the US legislation that sets standards for protecting the confidentiality and security of individually identifiable health information?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	
<b>ISAE 3402</b> Does this app comply with ISAE 3402, the global standard providing assurance that a service organization has appropriate controls in place?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	
<b>ISO 27001</b> Is this app ISO 27001 certified, a certificate given to companies upholding internationally recognized guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	
<b>ITAR</b> Does this app comply with ITAR, regulations controlling the export and import of defense-related articles and services found on the US Munitions List?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	
<b>SOC 1</b> Does this app comply with SOC 1, reporting on controls at a service organization which are relevant to user entities' internal control over financial reporting?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As	

Here we set the **Compliance** category to x4 – twice the weighting compared to security and legal. Set the **Category importance** slider to High (x4).



13. Scroll to the bottom of the page and click on **Save**.

After an hour, all application risk scores will be updated to reflect the new weighting.

**Part 2 – Complete.**

# Part 3 - Blocking Risky Apps

Return to the Cloud Discovery dashboard / Snapshot report page. Select Discovered Apps tab

Cloud Discovery

Dashboard | **Discovered apps** | IP addresses | Users

QUERIES: Select a query...

APPS: APP TAG: Sanctioned, Unsanctioned, None. RISK SCORE: 0 to 10. COMPLIANCE RISK FACTOR: Select factors... SECURITY RISK FACTOR: Select factors...

Browse by category: Cloud storage (47), Marketing (22), IT services (17), Hosting services (16), Accounting and finance (14), Content management (14).

1 - 20 of 290 discovered apps

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Last seen	Actions
Microsoft Developer Network Development tools	10	2 KB	1 KB	11	10	10	Aug 28, 20...	✓ ⚙ ⋮
Microsoft Dynamics 365 CRM	10	200 MB	96 MB	47	44	31	Aug 28, 20...	✓ ⚙ ⋮
Microsoft Exchange Online Webmail	10	329 MB	8 MB	82	44	25	Aug 28, 20...	✓ ⚙ ⋮

Based on risk factors, administrators can use MCAS to determine which apps are sanctioned or unsanctioned.

A green checkmark indicates that this app has been marked as sanctioned by IT. Select Microsoft Exchange Online, then select the Info Tab

Risk scores are calculated using different criteria, such as general, security, compliance, and legal capabilities of the apps. The Microsoft Exchange Online app scores 10 points based on this evaluation. Review the Microsoft Exchange Online app in the list.

Cloud Discovery > **Microsoft Exchange Online** Webmail

Usage | **Info** | IP addresses | Users | Alerts

1 connected instance. Microsoft Exchange Online is the hosted version of Microsoft's messaging platform, Exchange Server. Exchange Online gives companies a majority of the same benefits that on-premises Exchange deployments provide.

Suggest an improvement | Disclaimer | **10**

GENERAL			
Category: Webmail	Headquarters: United States	Data center: Ireland	Hosting company: Microsoft Corporation
Founded: 1975	Holding: Public	Domain: *.outlook.office.com *.outlook-off...	Terms of service: go.microsoft.com/fwlink/Link...
Domain registration: Jul 9, 2002	Consumer popularity: 10	Privacy policy: go.microsoft.com/fwlink/Linkid...	Logon URL: login.microsoftonline.com
Vendor: Microsoft	Data types: Documents, Media files, Databa...	Disaster Recovery Plan	

SECURITY			
Latest breach: —	Data-at-rest encryption method: AES	Multi-factor authentication	IP address restriction
User audit trail	Admin audit trail	Data audit trail	User can upload data
Data classification	Remember password	User-roles support	File sharing
Valid certificate name	Trusted certificate	Encryption protocol: TLS 1.2	Heartbleed patched
HTTP security headers	Supports SAML	Protected against DROWN	Penetration Testing
Requires user authentication	Password policy		

COMPLIANCE			
ISO 27001	ISO 27018	ISO 27017	ISO 27002
FINRA	FISMA	GAAP	HIPAA
ISAE 3402	ITAR	SOC 1	SOC 2
SOC 3	SOX	SP 800-53	SSAE 16

Return to the Cloud Discovery Dashboard and click on Discovered Apps Tab

Cloud Discovery also allows IT Administrators to easily identify risky, unsanctioned apps in use by their users. For example, filtering for cloud storage apps that scored 3 points or less in risk score, we see a handful of such apps.

At the top of the page, move the RISK SCORE slider from 10 down to 4.

The screenshot shows the 'Discovered apps' tab in the application management interface. At the top, there is a 'RISK SCORE' slider with a red box highlighting it, set to 4. Below the slider, there is a table of discovered apps. The first row shows 'Chrome Web Store' with a score of 4. The second row shows 'The Wall Street Journal' with a score of 4. The table has columns for App, Score, Traffic, Upload, Transactions, Users, IP addresses, Last seen (UTC), and Actions.

Under Browse by category, select Cloud storage.

Click the whitespace in the row corresponding to the PowerFolder app.

The screenshot shows the details for the 'PowerFolder Cloud storage' app. The app has a score of 2. Below the app name, there is a description: 'PowerFolder 1TB file sync Cloud now with Cloud Malware Protect for advanced protection Learn more buy now Advanced File Sync and Share for your Business in the cloud or within your company PowerFolder'. Below this, there is a 'GENERAL' section with details like Category (Cloud storage), Headquarters (Germany), Data center (Germany), Hosting company (SCHLUND), Domain (powerfolder.com), and Terms of service (powerfolder.com/legal-notice). There is also a 'SECURITY' section with details like Latest breach (—), Data-at-rest encryption method (AES), Multi-factor authentication (—), IP address restriction (—), User audit trail (—), Admin audit trail (—), Data audit trail (—), User can upload data (—), Data classification (—), Remember password (—), User-roles support (—), File sharing (—), Valid certificate name (—), Trusted certificate (—), Encryption protocol (TLS 1.2), and Heartbleed patched (—).

Here is an example of a risky app that has been in use by Contoso users. We can clearly see the reasons why this app is deemed risky: lack of data audit trail, lack of MFA support, no compliance with major industry standards, etc.

Since the **PowerFolder** app does not meet Contoso's organization's security requirements, an IT Administrator can take actions to discourage or block the usage of such apps. For example, we can tag this app as **unsanctioned** with just a click.

Click the block icon, , in the row corresponding to the PowerFolder app.

The screenshot shows the 'PowerFolder Cloud storage' app row in the table. The app has a score of 3. The 'Actions' column shows a checkmark, a block icon (highlighted with a red box), and a three-dot menu icon.

## Block app

Are you sure you want this cloud app to be blocked?

OK

Cancel

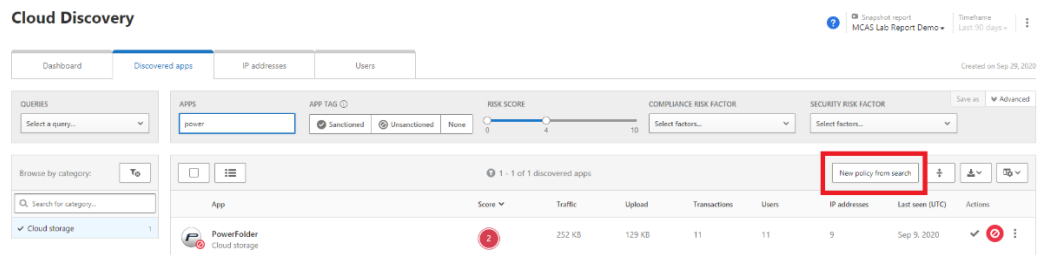
Click Ok.

The screenshot shows the 'PowerFolder Cloud storage' app row in the table. The app has a score of 2. The 'Actions' column shows a checkmark, a block icon (highlighted with a red box), and a three-dot menu icon.

Similarly, we can define a policy to automatically tag a risky app as unsanctioned as soon as the use of such an app is detected from end users.

This policy will mark any apps that fit the search criteria as “unsanctioned”.

**In the top-right corner of the page above the list of apps, click New policy from search.**



**In the Create app discovery policy page, type in a Policy name, e.g. “Automatically block risky Cloud Storage apps”.**

**Under the section APPS MATCHING ALL OF THE FOLLOWING, you can see that the filters are pre-applied.**

## Create app discovery policy

Cloud Discovery policies enable you to create alerts for new apps that are discovered in your organization.

Policy template \*

No template

Policy name \*

Automatically block risky Cloud Storage apps

Policy severity \*



Category \*

Cloud Discovery

Description

APPS MATCHING ALL OF THE FOLLOWING [Edit and preview results](#)

☒ Category  equals

☒ Risk score  equals

☒ Apps and domains  in

[+](#)

Apply to:

All continuous reports

**Under Governance actions, select Tag app as unsanctioned.**

**Click Create.**



### Governance actions

☐ Tag app as sanctioned

☒ Tag app as unsanctioned

☐ Tag app with custom tag

We secure your data as described in our [privacy statement](#).

Create

Cancel

### Policies

NAME	TYPE	STATUS	SEVERITY	CATEGORY	Advanced	
<input type="text" value="Policy name..."/>	<input type="text" value="App discovery policy"/>	<input checked="" type="checkbox"/> ACTIVE <input type="checkbox"/> DISABLED	<input type="text" value="Low"/> <input type="text" value="Medium"/> <input type="text" value="High"/>	<input type="text" value="Select risk category..."/>		
1 - 1 of 1 Policies						<a href="#">Create policy</a> <input type="button" value="Filter"/> <input type="button" value="Export"/> <input type="button" value="Refresh"/>
Policy	Count	Severity	Category	Action	Modified	
Automatically block risky Cloud Storage apps	0 open alerts	<input type="text" value="Low"/> <input type="text" value="Medium"/> <input type="text" value="High"/>	Cloud Discovery		Sep 25, 2020	

**Please note – this policy will take a few hours to take effect. Feel free to come back later and to see apps that were automatically tagged as unsanctioned as a result.**

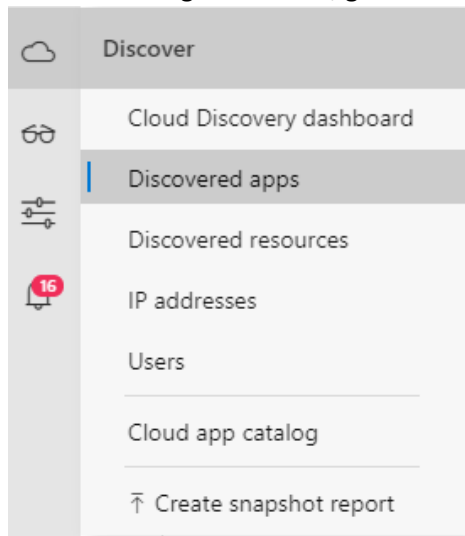
**Part 3 – Complete.**

## Part 4 – Shadow IT Discovery Report

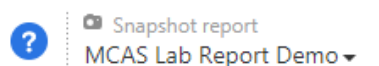
Now that you have blocked access to unsanctioned apps, let us generate an executive report about the discovered apps.

When IT Administrators are asked how many cloud apps they think their employees use, on average they say 30 or 40, when in reality, the average is over 1,000 separate apps being used by employees in their organization! Shadow IT helps identify which apps are being used and what each app's risk level is. 80% of employees use non-sanctioned apps that no one has reviewed and may not be compliant with their organization's security and compliance policies.

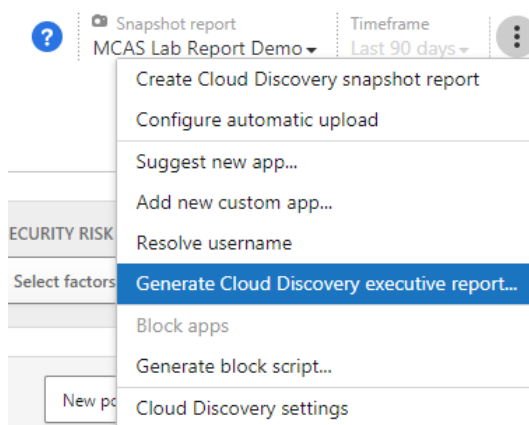
1. In the left navigation menu, go to **Discover > Discovered apps**.



2. Confirm you still have the **Snapshot report** you created in this lab selected.



3. At the top-right, click the vertical ellipsis menu (⋮) next to the drop-down, and then select **Generate Cloud Discovery executive report**.



4. Leave the **Report name** as default.

5. Click on **Generate**.

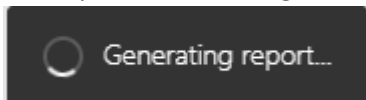
### Generate Cloud Discovery executive report

Snapshot report: MCAS Lab Report Demo | Timeframe: Last 90 days

Report name ⓘ

GenerateCancel

6. The report will now be generated.



7. Once complete the file will be automatically downloaded.
8. Open the generated **PDF** file located in your downloads folder.



Feel free to peruse the report to understand the contents and the value it would provide to a customer.

**Part 4 – Complete.**

# **End lab**

Thank you for taking the time to complete this lab, we hope you enjoyed it.

Please visit <https://aka.ms/secpractice-labs> to access further labs.

# Appendix

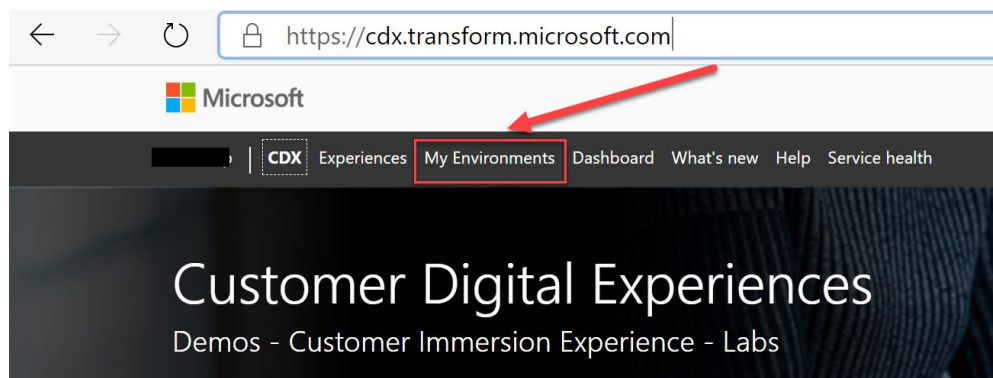
If you wanted to continue to test this with **real users** you need to add Cloud App security Add-on in order to get a licence to demo it

## Add Microsoft Cloud App Security Add-On

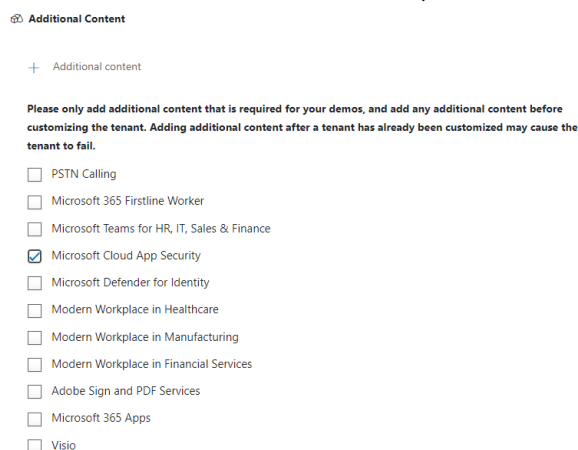
To be able to complete this lab your demo tenant will need the Microsoft Cloud App Security add-on enabled.

Please be aware – this may take time to provision, so please ensure you do it as early as possible before starting the lab thus to ensure it is provisioned in time.

1. Logon to <https://cdx.transform.microsoft.com/> You should use your partner email address and password that you use to connect to <https://partner.microsoft.com>
2. At the top of the page select My Environments Tab as shown below



3. Click on your tenant name in the list of your environments.
4. Scroll down to + Additional Content, select Microsoft Cloud App Security and click on Add.



5. Back on the main page you will now see the progress status of the addon pack provisioning.