**Cloud Discovery**

In this lab, we will create and view a Cloud Discovery Dashboard where you can:

* Analyze which cloud apps are being used in your organization
* Understand Office 365 use and adoption trends
* Compare data to other cloud apps that are being used in your organization

1) Log into you tenant

<https://login.microsoftonline.com/>

2) Click on the Admin Center 'App'

Machine generated alternative text:
MOD Administrator 
Good afternoon 
Search online documents 
Install Office 2016 
Other installs 
Power 31 
Mail 
Delve 
Calendar 
People 
Word 
i; 
Teams 
Yammer 
Dynamics 365 
PowerPoint 
Store 
OneDrive 
OneNote 
MyAnaIytics 
SharePoint 
Admin 
Planner 
Security & 
Compliance 
Tasks 
PowerApps 

3) In the left navigation, click on **Admin Centers** then click on **Cloud App Security**

Machine generated alternative text:
Office 365 
Billing 
Support 
Settings 
Setup 
Reports 
Health 
Admin centers 
Exchange cf 
Skype for Business cf 
SharePoint cf 
oneDrive cf 
Yammer 
PowerApps cf 
Flow cf 
Security & Compliance 
Azure AD cf 
Intune cf 
Cloud App Security cf 
Admin center 
Home v' 
Search users, groups, settings or tasks 
Office 365 Enterprise E5 setup is incomplete. Get someone to help you. 
Go to setup 
? MOD Administrator 
Contoso EMS932138 
Users > 
Add a user 
Delete a user 
Edit a user 
Reset a password 
Videos 
Admin center overview 
What's new 
> Admin mobile app 
•oooo 
Suggested features 
Billing > 
Total balance: None 
In trial: Buy now 
Message center > 
Office software 
Install my software 
Share the download link 
Software download settings 
Troubleshoot installation 
Domains > 
Add a domain 
Delete a domain 
Edit a domain 
Check health 
Service health > 
Some services have posted advisories 
3 advisories 
Active users 
Q Support 
— 
'Planned Maintenance: SharePoint Online Read... 
O Updated feature: Office 365 App launcher 
New feature: Guest access in Microsoft Teams 
sep 12 
sep 12 
sep 12 
x 
x 
x 
36 unread messages 
Help users get started 
Setup guides 
New service request 
View service requests 
O Need help? 
Feedback 

4) From the Cloud App Security Home Page, From the **Discover** menu, select **Create a snapshot report**

Machine generated alternative text:
Cloud App Security 
Discover 
Investigate 
Cloud Discovery dashboard 
Discovered apps 
IP addresses 
Users 
Control • 
Alerts @ 
Get started with Cloud App Security 
ral dashboard 
7K 
-twities monitored 
Create a Cloud Discovery report 
files monitored 
5 
Connect apps 
Create policies 
General dashboard 
Cloud app catalog 
Create snapshot report 
Learn more... 
0 112 
accounts monitored 
user notifications sent 
View dashboard for a specific a 
e 
Office 365 
O 
Microsoft OneDrive for Business 
O Microsoft SharePoint Online 
e 
Microsoft Cloud App Security 
View all apps... 
View dashboard for a specific risk type 
6b o 
discovered apps (last 30 days) 
Open alerts 
New over the last month • 
RECENT ALERTS 
2 
BY ALERT TYPE 
8 
Custom 
Microsoft 
o 
e 
O 
O 
e 
O 
Threat detection 
Privileged accounts 
Compliance 
DLP 
Cloud Discovery 
Sharing control 
Access control 
Configuration control 
u 
File containing PCI detected in the cloud (built-in DLP engine) 
meganb@emsg32138.onmicrosoft.com 
Microsoft SharePoint Online 
Publicly shared confidential files 
meganb@emsg32138.0nmicrosoft.com 
Microsoft SharePoint Online 
Publicly shared confidential files 
meganb@emsg32138.0nmicrosoft.com 
Microsoft SharePoint Online 
View all alerts in the last month... 
governance actions taken 
g days ago 
g days ago 
g days ago 
BY SEVERITY 
5 
High 
Top 3 alert types 
File policy alert 
Activity policy alert 
File policy alert 

5) Complete the Name and Description and choose **Cisco IronPort WSA** as the data source then click **"view and verify"** so that we can get a sample log file to test from the web security appliance / firewall / gateway. Notice all the different data sources that you could use.

Machine generated alternative text:
Create new Productivity App Discovery snapshot report 
Upload logs to discover cloud app activity and use. 
Productivity App Disccrvery is powered by Microsoft Cloud App Security which is a 
Report creation process 
O Analysis takes up to 24 hours I Track statuse 
separate online service. Terms I Privacy statement 
Report name 
Cisco IronPort WSA Discovery 
Description 
Enter description (optional) 
Data source 
Cisco IronPort WSA 
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... 
Choose traffic logs 
Choose up to 20 files 
1 G8 maximum size per log, from the last 90 days 
Cancel 
• 
• 
Upload 
Parse 
Data analysis 
Generate report 
View sample report 
Browse 
Create 

6) Click **Download sample log** and save it locally to your device. Close the dialog when done.

Machine generated alternative text:
Verify your log format 
In order to successfully parse your log, it must match the following format: 
Cisco IronPort WSA 
FTP (Supported in snapshots and automated upload) 
*Version: I. a 
*Date: 2015-a1-13 
*System: 55. les .27 .2m - location.corp.contoso.com 
*Software: AsyncOS for Web 8.0.6-123 
*Fields: SUSPECT USER AGENT,mOUITOR SUSPECT USER AGE 
1432771585.331 6 la.1e.5.37 TCP DENIED ssL/4Ø3 le GET https://www.microsoft.com:443 
Syslog (Supported in automated upload only) 
1432771585.331 6 la.1e.5.37 TCP DENIED_ssL/4Ø3 le GET https://www.microsoft.com:443 
UONE/ 
NONE / 
If your lag 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 
BLOCK 
BLOCK 
Close 

7) That will return you to the **Create new Cloud Discovery snapshot report** page where you can click **Browse** under **Choose traffic logs** and upload the sample file you just downloaded. Then click **Create**

Machine generated alternative text:
Create new Cloud Discovery snapshot report 
o 
A report is being processed 
You will be able to create a new one when the process completes (usually takes up to 10 minutes per 50 MB). 
Track status I Go back 
Fill in the following details and upload recent traffic logs from your 
organization to create a new report. 
Privacy statement 
Report name 
Enter neme 
Description 
Enter description {optional) 
Data source 
Choose applierce.. 
D Anonymize private information 
Store and aisplay only encrypted usernames. 
Choose traffic logs 
Choose up to 20 files 
1 Ga maximum size per lag, from the last 90 days 
Report creation process 
@ Analysis takes up to 24 hours I Track status % 
• 
Upload 
Parse 
Data analßis 
Generate report 
View sample report 
Cancel 
Browse 
Create 

*8) You should now be in the* ***Manage Snapshot Reports*** *screen where your snapshot should have a "Processing" status. You can return to this in about 15 minutes when it is done but note it could take up to 24 hours to process the logs.*

Machine generated alternative text:
Cloud App Security 
Cloud Discovery settings 
Configure score metric 
Manage snapshot reports 
Upload logs automatically 
Manage continuous reports 
Manage app tags 
Exclude entities 
User enrichment 
Anonymization 
Delete data 
Discover • 
Investigate 
Control • 
Alerts @ 
2 
Microsoft 
Manage snapshot reports 
Snapshot reports provide visibility into your cloud app activity and use by analyzing traffic logs that you upload. 
Terms I Privacy statement 
Cisco Iron Port WSA - 3 
Cisco IronPort WSA log 
Cisco IronPort WSA log discovery 
Demo Snapshot Report 20170904 
Auto provisioned by Demo Provisioning 
Platform 
1 - 3 of 3 snapshot reports 
Logs 
Data source 
Cisco IronPort WSA 
Cisco IronPort WSA 
Cisco IronPort WSA 
Date added v 
sep 13, 2017 
sep 13, 2017 
sep 3, 2017 
Added by 
admin@ems932138.onmicrosoft.con 
admin@ems932138.onmicrosoft.con 
admin@ems932138.onmicrosoft.con 
View sample report 
Create snapshot report 
Status 
O Processing 
Ready 
Ready 

9) In the meantime - check out the **Demo Snapshot Report 20170904** (list shown above) that should be included with a "Ready" status in your demo tenant. Click on that report to view.

Machine generated alternative text:
Cloud App Security 
Cloud Discovery' 
Apps 
300 
App categories 
Clc•ud storage 
6.1 GB 
Webmail 
Online meetings 
Collaboration 
Discovered apps 
Disco.'er • 
Discovered a PPS 
Investigate • 
Control • 
IP addresses 
457 
IP addresses 
1858 
.1-1Sof300» 
Traffic 
3.0 
605 MB 
GB 
.1-Sof35» Traffic 
View all apps 
Sardoned 
A I cetegares 
C] Unsaxtioned 
'Other 
4.4 Ga 
402 Ma 
377 Ma 
227 Ma 
• Other 
Risk levels 
Top users Top IP addresses 
Tripp@contoso.com 
Makai@contosocom 
Jamison@contoso.com 
Wlliam@contoso.com 
Karissa@contosoxom 
Apps headquarters location 
Get continuous repots for improved visibility 
Configure automatic upload 
Traffic from high risk apps 
I Traffc from medium risk apps 
Traffic from low risk apps 
Configure score metric 
all users 
I Saxtioned 
Traffic 
Ursanctioned 
1.5 GS 
620 MB 
329 MB 
200 MB 
186 MB 
113 MB 
Cisco IronPort WSA is ready. 
Traffic 
40 MB 
36 MB 
32 MB 
29 
28 MB 
Microsoft OneDrtv... 
Wcrosoft Exchang.„ 
Wcrosoft Dynami.„ 
Office 365 
Secure Online Des... 
Oxygen Cloud 
Open Drive 
Flunom 
Cubby 
SecureSafe 
SugarSync 
Send itcertified 
AJI categories 

10) Spend some time exploring the different filtering options and tabs. For example, in the Discovered apps, try selecting the Productivity or Cloud Storage apps and seeing how many users are using unsanctioned apps.