Cloud App Security

Proof of Concept Playbook

Learn how to quickly implement Microsoft Cloud App Security

Prepared by

Yoann Mallet

Sr Program Manager,

C+E Security Customer Experience Team

Contributors

Shalini Pasupneti, Sr Program Manager, C+E Security Customer Experience Team

Version 1.0 Final

Executive Summary

This document provides guidelines to explore different features of Cloud App Security in a Proof of Concept (POC). The intended audience of this document is Security administrators, IT Professionals, and System Integrators.

Content

Training and Community Resources

aka.ms/SecurityCommunity

Microsoft Cloud App Security On-demand Training

How to use this play book?

1. Use the Theme section and pick the areas of interest based on your needs.
2. Scope the PoC by choosing the scenarios which aligns best with your business goals. We recommend as short and concise as possible to convey the value to the stakeholder, while minimizing the complexity.
3. Use the PoC Implementation section to understand the scenarios and what would they mean for your environment. In each scenario, we describe how to set it up (what we call building blocks), and how to navigate.
4. Each building block explains the pre-requisites needed, as well as an approximate time to complete. This can help you during the planning process.
5. Based on 1-3 above, define the environment in which to execute. We encourage to strive for a production environment to get a good feel of the experience for your users.

POC Ingredients / Intro

Theme / Scenarios overview

Microsoft Cloud App Security (MCAS) can help organizations gain control over cloud applications currently in use. Leveraging its capabilities, we can use it in the following three scenarios:

- Discover Shadow IT
- Data Control over Sanctioned Apps
- Threat Protection - Using MCAS in an Incident response scenario

Defining the main scenario(s) for this POC will assist focusing efforts with the organization's main goal in implementing MCAS.

More info on MCAS can be found here: https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security

Environment

Choosing the proper environment is essential to the success of a POC deployment. The following can be used:

- Production: using actual Firewall logs, containing user data, and connecting to production SaaS applications.
- Lab / Trial: using a temporary environment to evaluate the product or one of its features using Firewall logs in a test environment or test tenants of SaaS applications in use within the organization.

Due to the non-invasive way MCAS operates we strongly recommend to deploy it directly within a production environment. This will provide more relevant results and analytics in order to understand the product.

Pilot Target

The target of the PoC must be defined clearly prior to deployment. Depending on the selected scenario, it can be one of the following:

- One Site Pilot: having a pilot for the Firewall logs coming from one Firewall device, or one site initially, to have a clear understanding of the discovery process.
- One Application Pilot: having a MCAS pilot connecting directly to a SaaS application used in the environment will give an overview of the product's capabilities.

The different scenarios described below are not mutually exclusive and can be combined.

POC Implementation Scenarios

Foundation: Setting up the Cloud App Security portal

To begin implementing a PoC of MCAS, you must first sign up for a MCAS tenant and set up the portal.

Signing up can be done a couple of ways:

- Free trial: can be converted into a paid subscription
    - You can sign up for a free trial here: https://www.microsoft.com/en-us/cloud-platform/cloud-app-security-trial
- As part of a licensing package, such as EMS E5

While anyone can setup a trial, enabling the subscription included with EMS E5 will require an administrator's credentials.

The portal can be customized by providing access to additional administrators or configuring a custom logo.

Scenario #1: Discover shadow IT

Nicholas, an IT security administrator at Contoso, was asked to investigate the use of shadow IT within the organization. He is well aware of older mechanisms to prevent shadow IT, such as requiring encryption for USB storage, or preventing non-corporate managed assets to reach critical resources.

However, Nicholas knows a new type of shadow IT is spreading out using cloud applications, and he wants to assess his environment for any modern threats. To do this, he will enable Cloud Discovery.

Cloud Discovery analyzes your traffic logs against our catalog of over 13,000 cloud apps. These are ranked and scored based on more than 50 attributes, to provide you with ongoing visibility into cloud use, Shadow IT, and the risk Shadow IT poses into your organization.

Upload a cloud Discovery log

1. Nicholas requests Firewall logs from Bob, one of the network administrators.
2. He opens the Cloud App Security portal and creates a snapshot report by uploading the Firewall log provided by Bob.
3. Nicholas can review the report of utilized applications and understand the security posture of each application by reviewing the risk score.

More info on setting up Cloud Discovery is available here:

- https://docs.microsoft.com/en-us/cloud-app-security/working-with-cloud-discovery-data
- https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery

Unsanctioning an application

1. Nicholas notices a number of users are using OneDrive personal, which is not a sanctioned cloud application, and wants to identify them.
2. He unsanctions the application on the MCAS portal.
3. He exports a script to apply on Contoso's Firewall in order to blocks access to this application.
4. Nicholas works with Andrew, from the network team, in order to have the script applied to the Firewall.

Configuring automatic Firewall logs upload

1. Nicholas sees the high importance of Firewall logs' analysis by Cloud App Security and wants the process to be automated.
2. He connects to the Cloud App Security Portal and downloads the Log Collector VM.
3. He works with Andrew, the network administrator, to configure the auto upload of the Firewall logs.
4. Nicholas creates reports to identify trends in discovery of the cloud applications.
5. He configures alerts for unsanctioned applications and will now receive notifications when they are used.

Configuring a Cloud App Discovery Policy

1. Nicholas wants to receive an alert if a new "risky" app is used within the environment.
2. He creates a new Cloud App Discovery Policy.
3. He chooses the proper policy template: "New Risky App", and tweaks its configuration if needed.
4. Nicholas saves the new policy. Now, any app with a security rating under 5 will generate an alert.

Scenario #2: Protect sanctioned apps

Hayden, the CISO, is having a discussion with Steve, the Office 365 administrator.

While the company very quickly adopted the new features offered by cloud technologies, Hayden is concerned users are not complying with the cloud service usage policies, such as:

- Require Office documents uploaded to OneDrive to be protected using Azure Information Protection (AIP).
- Do not upload data with PCI data, such as credit card numbers to cloud providers used by Contoso.
- Monitor their Office 365 and Salesforce users for non-approved data.

In addition to those compliance policies, Hayden wants to ensure no software resides on cloud data store, and to be alerted if this happens. She works on this with Nicholas, who is in contact with Steve, the messaging administrator, and Laura, the Salesforce administrator.

Connecting to a cloud application

1. Nicholas works side by side with Steve to connect MCAS with Office 365.
2. Andrew provides administrative credentials to Nicholas, so he can connect MCAS to Office 365.
3. Nicholas logs on to the MCAS portal and adds a connector.
4. He then works with Laura and repeats the same operation for Salesforce.

5. Laura and Andrew revoke Nicholas' admin access on Office 365 and Salesforce.
6. A number of policies such as abnormal upload are configured by default in MCAS and take effect automatically.

Configuring policies

1. Nicholas identifies the actual need for an alert: PCI information being uploaded to OneDrive and Salesforce.
2. He creates a new File policy and selects the proper template: "File Containing PCI Detected in the Cloud".
3. He tweaks additional settings if needed and saves the policy.
4. Alerts will now be sent to Nicholas, by MCAS, if it detects a file with PCI information, such as PCI data, in OneDrive or any other managed cloud application.

Scenario#3: Using MCAS in an incident response scenario

A less utilized, but very valuable scenario for Cloud App Security, is to leverage its Firewall analysis capability in case of a security incident.

The analysis of the traffic going out can provide some insight of potential data exfiltration.

Signing up for a free trial and uploading logs

1. Nicholas, our security administrator, signs up for a Cloud App Security free trial.
    a. Alternatively, if he already has a MCAS tenant, he can use it.
2. He works with Bob, the network administrator, to gather Firewall logs for the past 90 days in the sites where the incident is believed to have occurred.
3. He uploads them to the MCAS portal as previously discussed in Scenario 1.

Review uploaded report

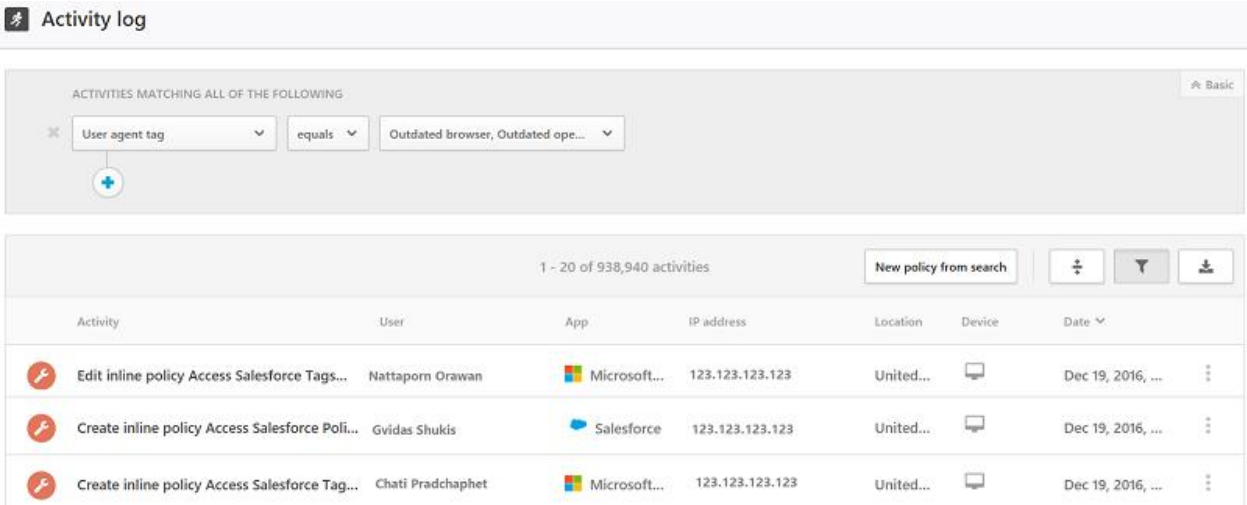
1. Nicholas reviews the dashboard in MCAS.
2. He identifies data storage apps that are not sanctioned by the organization.
3. He reviews application usage, and identifies any risky or unexpected behavior.

More info is available here: https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports

Another feature of MCAS can be leveraged for Incident Response scenarios by using API Integration for managed applications.

Reviewing Activity

1. Nicholas is receiving alerts from MCAS that abnormal activity is occurring on a user.
2. He opens the MCAS portal and reviews the alert's details.
3. He then looks in the users activity to review the suspicious activity and determine its criticity. Activity screen is depicted below:



Optional Scenario: SIEM integration, AIP Integration, IP range Tagging

SIEM Integration

The organization now needs to have a single unified view of all operational events across the environment. The requirement is to have the minimum amount of portals to review when monitoring for incidents.

Their preferred solution is to have everything reported within their SIEM, which currently already aggregates logs from several services.

To achieve this, Nicholas configures the following:

1. Setup a standard Windows or Linux machine (can be a VM, and must have JAVA 8 installed).
2. Configures SIEM integration in the MCAS portal.
3. Installs the SIEM agent on his VM, and configures it to point to his MCAS tenant.
4. He configures a policy to receive all alerts and activity.
5. His operations team now has a single view point for all incidents and activity in the environment.

Azure Information Protection Integration

Nicholas has recently started to use Azure Information Protection and configured classification labels and protection on his corporate data.

He would like to be able to identify when any confidential information is shared over the OneDrive for Business.

Nicholas configures the following steps:

- He configures Cloud App Security to automatically scan files for Azure Information Protection Labels.
- He creates a file policy that matches the label “Confidential” and the OneDrive for Business app.
- He configures an alert to be notified by email if someone stores them over OneDrive or Box.

Configuring IP Range Tagging to identify risky sources

Nicholas has had a few users affected by ransomware, requiring them to pay money to access their data. Often they had to connect to those malicious resources using the Tor browsers.

Nicholas wants to be alerted immediately if any user attemps such activity.

He use Cloud App Security doing the following:

- Creates a new activity policy.
- Has the policy match traffic coming from IP addresses with the "Tor" tag.
- Configures the proper notification for him.

He will still be able to tag any additional IPs as part of the Tor network at a later time.

POC Building blocks

Catalog of actors

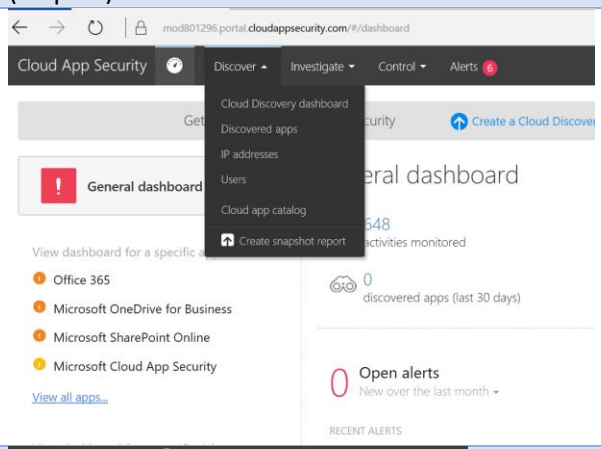
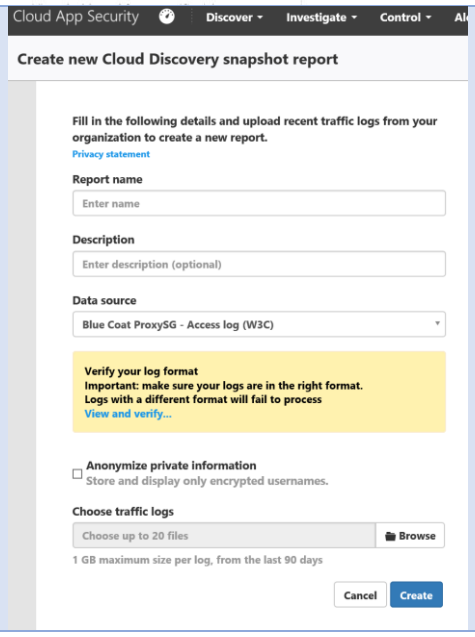
Actor	Description	PoC Responsibility
Information Security Team	This team manages the security of the information systems. It defines security strategies and policies for other teams within the organization. It also administers and monitors security solutions	Main actor responsible for configuring, maintaining and monitoring Cloud App Security. They will work with connecting teams when needed.
Network Team	Owners of the network infrastructure and Firewall devices.	Provide Firewall log, as needed, and assistance to configure Firewall logs auto-upload.
Messaging team	In charge of managing the cloud service providers used for email messaging (Office 365, Google Apps, etc.)	Helps the MCAS admin to connect the messaging application to MCAS using vendors' APIs.
Cloud Application owners	Own and manage cloud applications such as Service-Now, Salesforce or Box, etc.	Help the MCAS admin to connect these additional cloud applications to MCAS.
Operations team	Manage daily operations and monitor alerts from various monitoring systems (including security).	Work with the security team to understand the alerts coming from MCAS and how to respond to them.

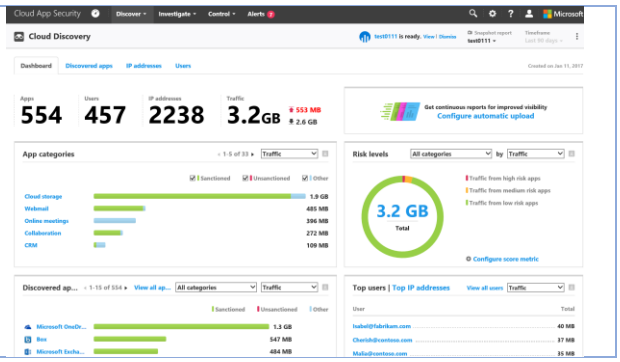
Discovery

Manual log upload

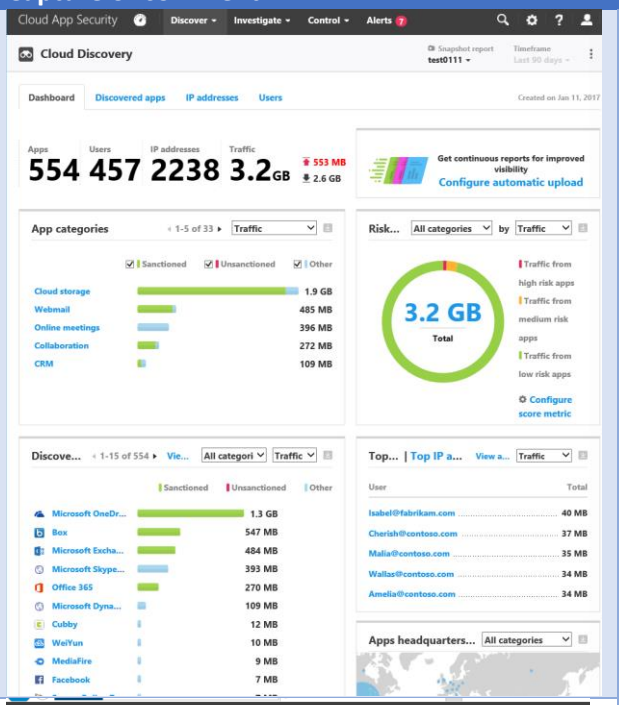
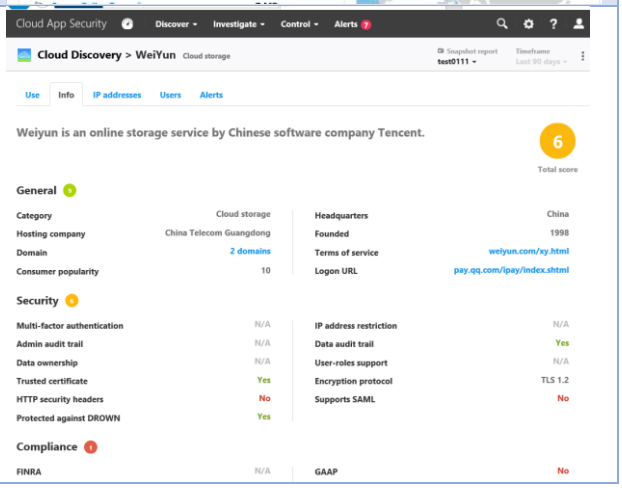
This procedure requires the following:

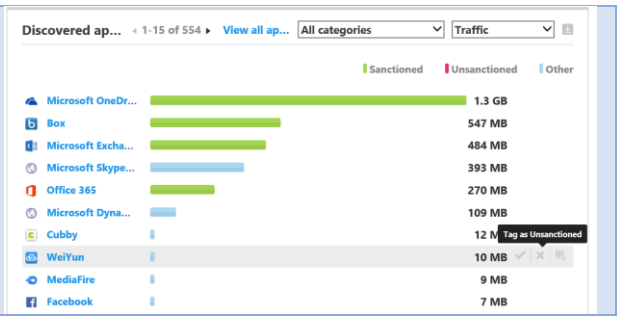
- Request Firewall logs from network administrator.
- Identify the type of Firewall before uploading logs.

Instruction	Capture or comment
1. Open the Cloud App Security portal and create a snapshot report by uploading the Firewall log provided by the network administrator.	Sample Firewall logs are available on the MCAS portal. More info: https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports (step #5)
2. On the top right, the network adminstrator clicks on the Discover menu and chooses Create snapshot report.	
3. Fill out the report name / description, and choose the proper Firewall from the dropdown list. 4. Data can be anonymized for additional compliance requirements. This option forces MCAS to store and display only encrypted usernames. 5. Click Create. 6. Wait until the data is processed and analyzed (can take several minutes).	

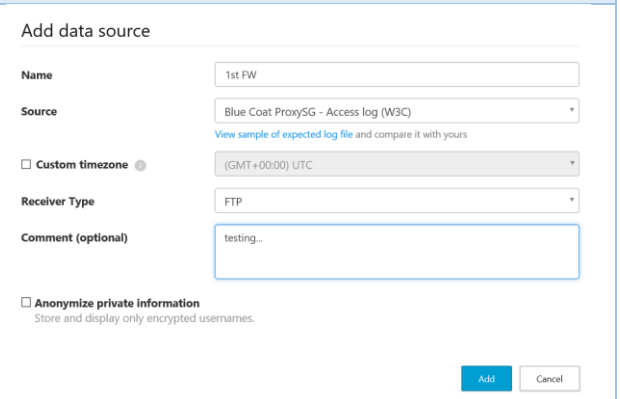
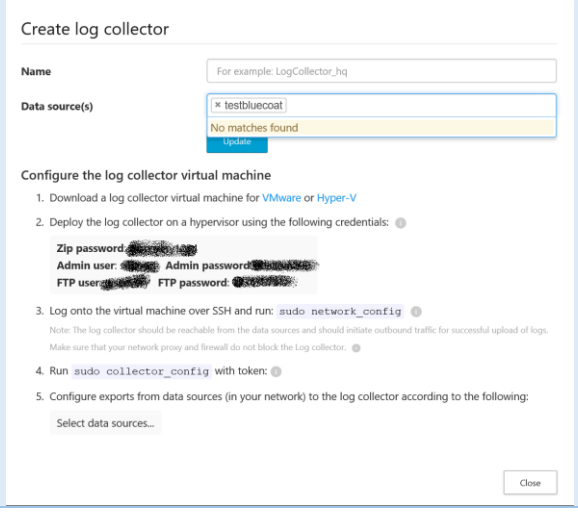
7. Click on the Discover menu and on Cloud Discovery Dashboard. 8. You can review the report of utilized applications and define which applications are sanctioned or unsanctioned.	

Investigate and Unsanctioning a cloud app

Instruction	Capture or comment
1. Looking at the Cloud Discovery Dashboard, we notice a number of unexpected cloud apps and decide to evaluate their risk level: a. Click the Discover menu and Cloud Discovery Dashboard. b. Review the security risk related to “WeiYun” by Clicking on it.	
2. Click on the info tab. The apps security score is “6”. This is below what the security policy tolerates and and it must be unsanctioned.	

3. Back on the dashboard, hover your mouse over the app and click Tag as unsanctioned.	

Automatic upload

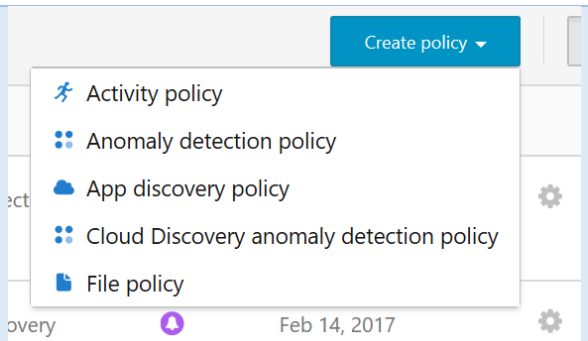
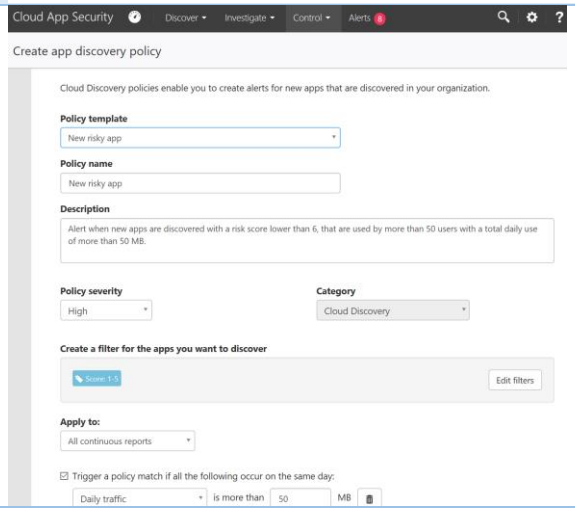
Instruction	Capture or Comment
1. Click on the setting icon ( ) and select Log Collectors to open the automatic upload page.	
2. For each Firewall, from which you want to upload logs, click Add Data Source. Provide a name and in the Source field select the Firewall type. Select the appropriate settings in the window.	
3. Go to the Log Collectors tab, and add a log collector. Click Update. Type a name and select a data source. Download the proper image (VMWare or Hyper-V), and write down the password, logon information, as well as the token that appears in #4. Click Close.	
4. Configure the Virtual Machine, using the downloaded virtual disk file, and using	Hardware requirements: • Hypervisor: HyperV or VMware

the recommended hardware requirements.	• Disk space: 250 GB • CPU: 2 • RAM: 4 GB • Firewall settings: • Allow the log collector to receive inbound FTP and Syslog traffic • Allow the log collector to initiate outbound traffic to the portal (for example contoso.cloudappsecurity.com) on port 443
5. Start the newly created VM and connect to it.	*Connection over SSH is possible. Password should be changed from default configuration.*
6. Run the Collector Config Utility with the access token provided in step 3, above.	sudo collector_config <access token>
7. Enter your console domain (such as: contoso.portal.cloudappsecurity.com). This is available from the URL you see after logging into the Cloud App Security portal.	
8. Enter the name of the collector previously configured.	
9. Configure your network Firewalls and proxies to periodically export logs to the dedicated Syslog port of the FTP directory according to the directions in the dialog.	Example: `London Zscaler - Destination path: 614` `SF Blue Coat - Destination path: \\CloudAppSecurityCollector01\BlueCoat\` 0020

More info available here: https://docs.microsoft.com/en-us/cloud-app-security/configure-automatic-log-upload-for-continuous-reports

Create an App Discovery Policy

Instruction	Capture or Comment

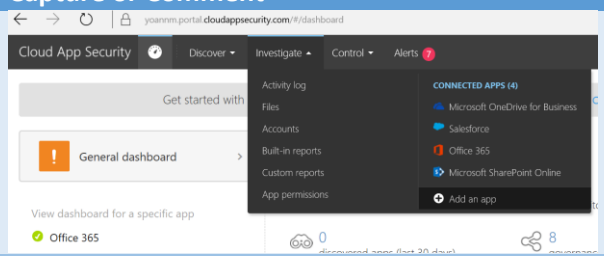
1. In the MCAS portal, click the Control menu / Policies. 2. Click the Create Policy Button and select App discovery policy.	
3. Either select a template (as in captured screenshot here), or manually configure policy settings. Here we are discovering Risk Apps (security score below 6). 4. Scroll down and configure alert settings. 5. Click Create.	

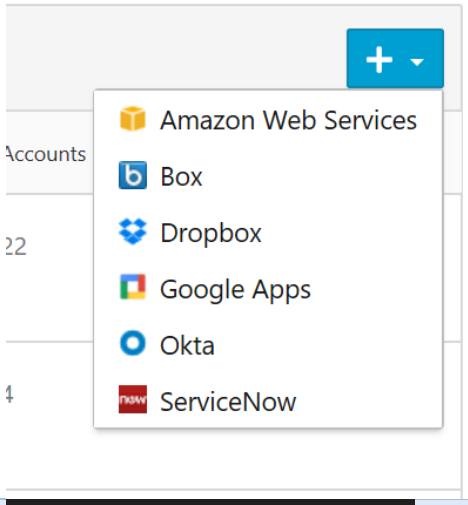
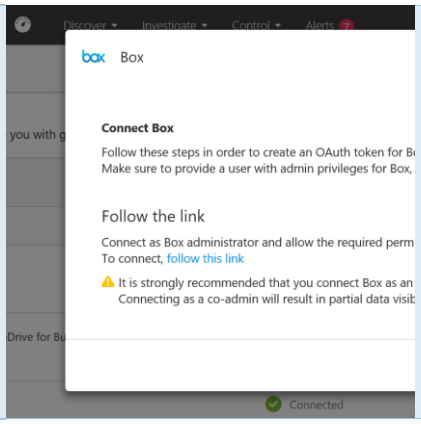
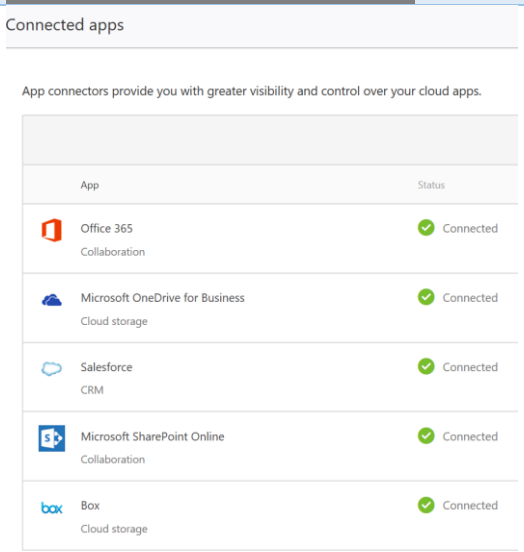
More info available here: https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-policies

Working with Sanctioned Apps

Connecting an application through API Connectors (Box)

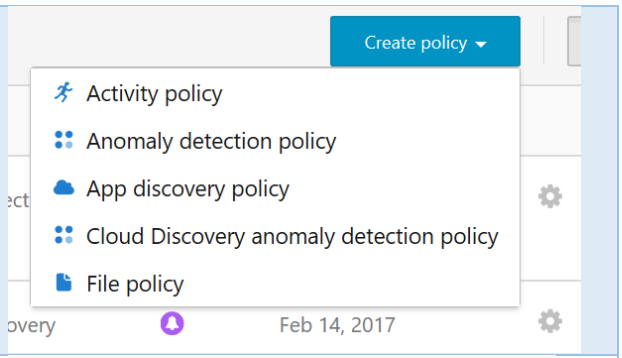
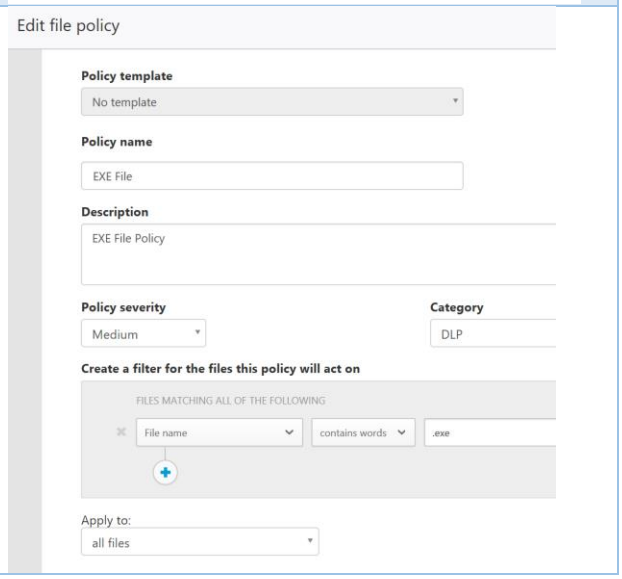
The following procedure requires an administrative account to your Box subscription. For a test deployment, this can be done using a developer account.

Instruction	Capture or Comment
1. In the Cloud App Security portal, click on Investigate / Add an app. 2. On the connected app page, click the "+" button.	

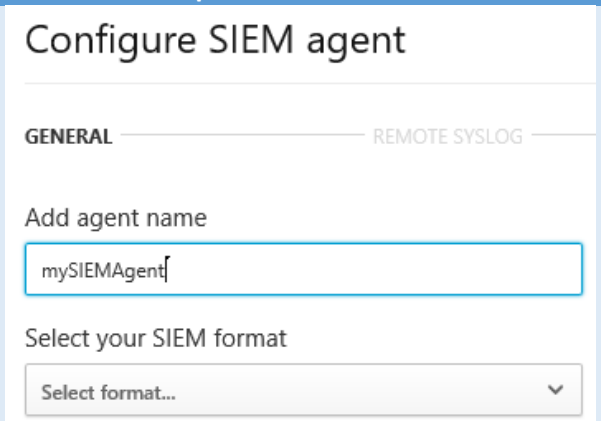
3. Select Box.	
4. A new window pops up, click Connect Box 5. Ensure you have an administrative account and follow the link required. 6. A box window will open. Ensure you are logged in with proper credentials, or enter them now and click "Grant Access to Box".	
7. Test connectivity. 8. Monitor that the connector appears.	

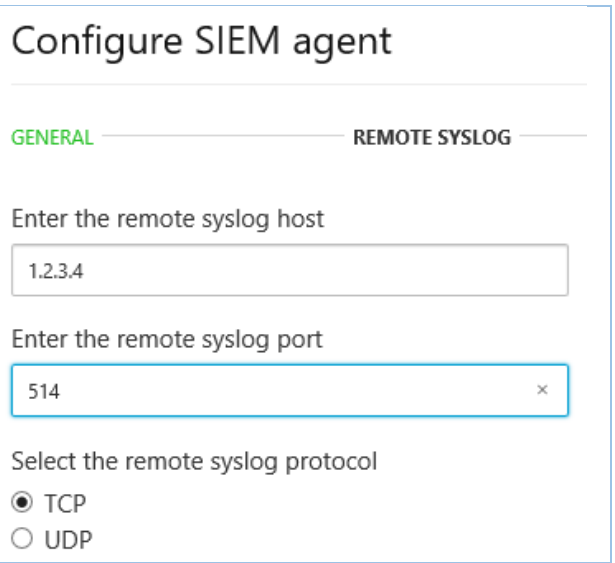
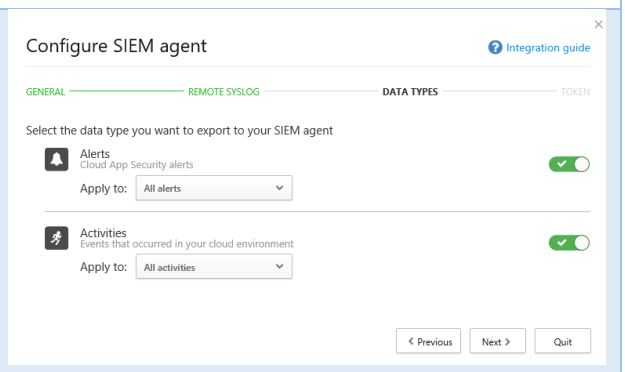
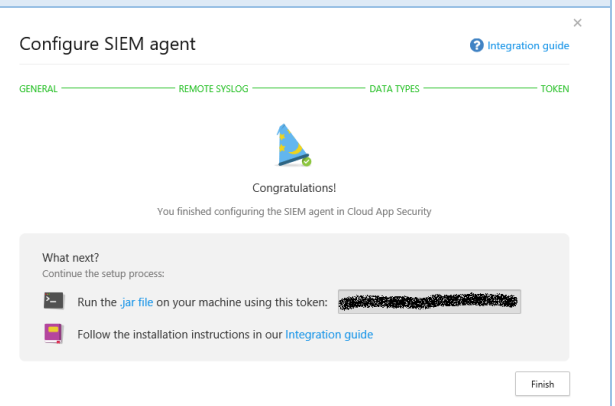
Create a File Policy

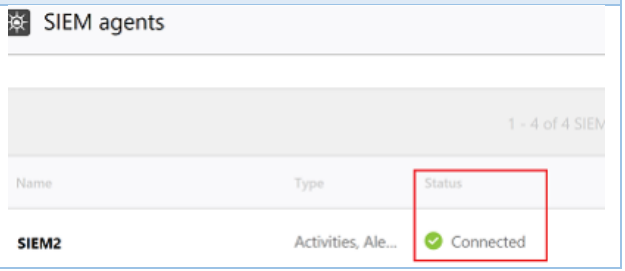
Instruction	Capture or Comment

1. In the MCAS portal, click the Control menu / Policies. 2. Click the Create policy button and select File policy.	
3. Either select a template or manually configure policy settings. 4. Here we configured a policy generating an alert each time an EXE file is stored in a cloud storage provider such as Box or OneDrive. 5. Scroll down and configure alert settings. 6. Click Create.	

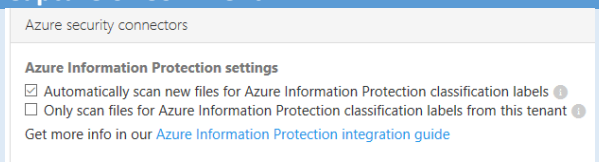
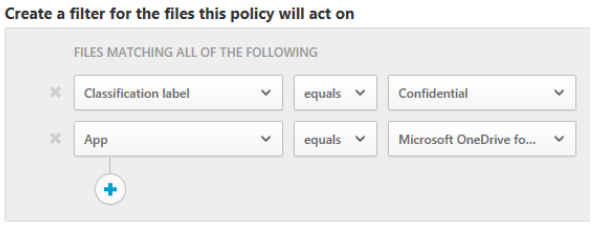
Configuring SIEM Integration

Instruction	Comment or Capture
1. In the Cloud App Security portal, under settings, select SIEM agents. 2. Click Add SIEM agent to start the wizard. 3. Configure an agent name and select a format (Generic or ArcSight). 4. Click Next.	

5. Configure the remote syslog host connection information, and click Next.	
6. Select the type of activities you would like sent to your SIEM (alerts and/or activities). 7. Click Next.	
8. Save the token presented in this step. 9. Download the .JAR file to your machine. Click Finish.	
10. Unzip the .JAR file to the previously configured machine. 11. Run the following command with the variables below: • DIRNAME is the path to the directory you want to use for local agent debug logs.	`java -jar mcas-siemagent-0.87.20-signed.jar [--logsDirectory DIRNAME] [--proxy ADDRESS[:PORT]] --token TOKEN`

• ADDRESS[:PORT] is the proxy server address and port that the server uses to connect to the Internet. • TOKEN is the SIEM agent token you copied in the previous step.	
12. Validate that the SIEM agent is shown as connected, and no error is currently affecting its status. 13. Verify events are arriving into your SIEM.	

Configuring AIP integration

Instruction	Capture or Comment
1. In the Cloud App Security portal, click the settings icon and select general settings. 2. Under Azure Information Protection settings, click Automatically Scan new files for Azure Information Protection classification labels.	
3. Create a new file policy. 4. Configure the filter to match a classification label (as per screenshot).	
5. Configure the appropriate notification mechanism if required.	

IP Range tagging and alerting

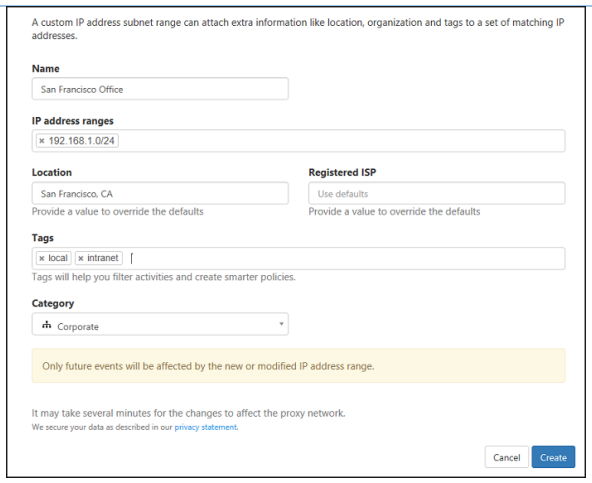
Instruction	Capture or Comment
1. In the Cloud App Security portal, click the settings icon and select IP Address Ranges. 2. Click Add IP address range.	

3. Type a name, for the IP range.

4. Enter the IP address range you wish to configure and then click on the "+" button. You can add as many IP addresses and subnets as you want using CIDR notation, for example 192.168.1.0/32.

5. Configure the additional optional settings as required (location, ISP, Tag).

6. Click Create.



7. In order to view traffic from a specific tag, click the Investigate menu in the Cloud App Security portal, and select Activity Log.

8. Click Advanced on the top right corner, to be able to configure a query based on IP Tagging.

9. Select IP address.

10. Select the Tag filter.

11. Select the required tag (ex: Tor).