



# Discover What Your Users Are Really Doing in the Cloud

Using Microsoft Defender for Cloud  
Apps – Cloud Discovery and Log  
Integration




[Home](#) > [Perparims Cloud Solutions](#) >

Perparims Cloud Solutions ...





# What Is Cloud Discovery?

-  **Collects Logs**  
From firewalls, proxies, and network appliances
-  **Detects Risky SaaS Usage**  
Identifies unsanctioned or shadow IT apps (like personal Dropbox)
-  **Improves Visibility**  
Gives insights into cloud app usage across your org

# Discovery Methods

- ✓ Manual snapshot report (upload a log file)
- ✓ Automatic upload (configure appliances)



# What Does Cloud Discovery Do?

The screenshot displays the Microsoft Defender Cloud App Security dashboard. The left sidebar contains navigation options: Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log, Policies, Policy management, Policy templates, Reports, Audit, Health, and Permissions. The main content area is titled 'Cloud Discovery' and features an illustration of a person with a magnifying glass. Below the illustration, it states: 'Cloud Discovery enables you to: Gain continuous visibility over Shadow IT, Analyze cloud app usage, Dive into a specific app, user or IP address, Get notifications about new discovered apps'. Three buttons are present: 'Create a new report', 'Configure automatic upload', and 'View sample report'. At the bottom, a detailed dashboard is shown with metrics: 128 Apps, 5875 Users, 3861 IPs, and 9.5 TB Traffic. It includes a bar chart for App categories (Collaboration, Cloud storage, Webmail, Social media, Online meeting) and a risk level gauge showing 890 users at high risk. A table of discovered apps and top users/IP addresses is also visible.

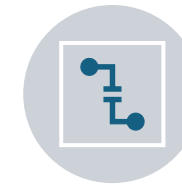
- Identify risky or unsanctioned SaaS apps
- Discover apps by user, IP, and traffic
- Visualize app categories and usage
- Launch reports or configure automatic uploads

# Upload Logs or Discover Apps Automatically

👉 “You can upload logs manually or configure continuous log collection from firewalls/proxies.”



MICROSOFT DEFENDER FOR CLOUD APPS LETS YOU DISCOVER APP USAGE BY IMPORTING LOG DATA MANUALLY OR SETTING UP AUTOMATIC COLLECTION.



**MANUAL UPLOAD:** IMPORT LOGS FROM FIREWALLS & PROXIES



**AUTOMATIC UPLOAD:** CONTINUOUSLY GATHER DISCOVERY LOGS








**SUPPORTS MAJOR VENDORS** LIKE PALO ALTO, FORTINET, CHECK POINT







**LOG COLLECTORS:** CONFIGURE EXTERNAL DATA SOURCES VIA IP/URL

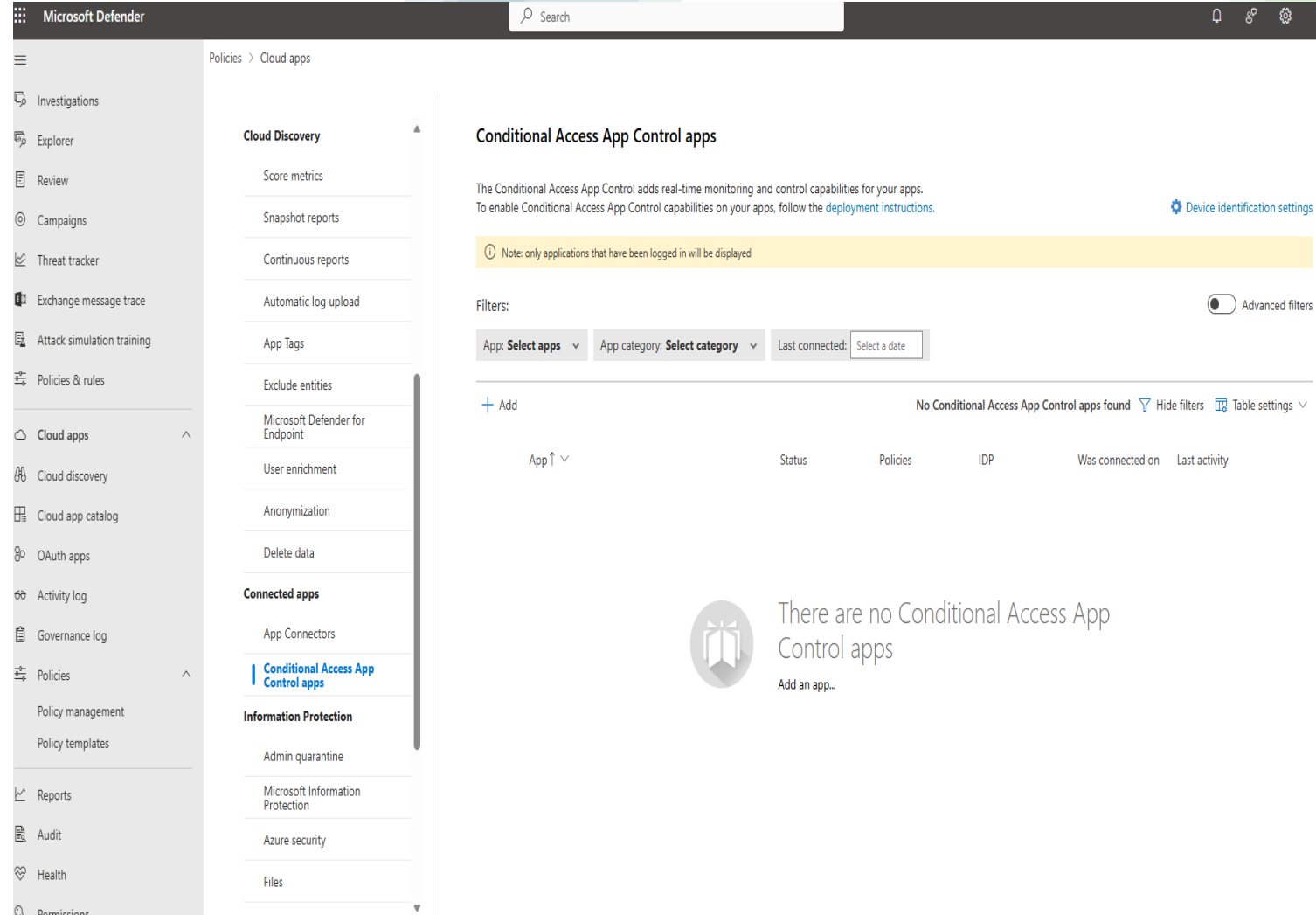
# App Connectors: Deep Integration with SaaS Platforms

-  **Connects Defender to sanctioned SaaS apps**
  -  **Enables deep visibility into app usage & file activity**
  -  **Supports Microsoft 365, Dropbox, Salesforce, and more**
  -  **Enables governance features like DLP, file control, and session monitoring**
-  **Note: In this lab, no connectors were linked — but in production, App Connectors integrate key business SaaS platforms for detailed control and monitoring.**

# Conditional Access App Control: Real-Time Policy Enforcement

-  **Enforce access and session policies in real-time**
-  **Block sensitive file downloads on unmanaged devices**
-  **Detect risky behavior and enforce session re-authentication**
-  **Integrates with Microsoft Entra Conditional Access**

We used Microsoft Defender to demonstrate how Conditional Access App Control helps restrict risky activities like file downloads, sharing, or session hijacking.



The screenshot displays the Microsoft Defender web interface. The left sidebar contains navigation options: Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps (expanded), Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log, Policies (expanded), Policy management, Policy templates, Reports, Audit, Health, and Permissions. The main content area is titled 'Policies > Cloud apps'. It features a 'Cloud Discovery' section with options like Score metrics, Snapshot reports, Continuous reports, Automatic log upload, App Tags, Exclude entities, Microsoft Defender for Endpoint, User enrichment, Anonymization, and Delete data. Below this is a 'Connected apps' section, which includes 'App Connectors' and 'Conditional Access App Control apps' (highlighted with a blue bar). The 'Information Protection' section includes Admin quarantine, Microsoft Information Protection, Azure security, and Files. The right-hand pane is titled 'Conditional Access App Control apps'. It contains an introductory text, a note about logged-in applications, filter controls (App, App category, Last connected), and a table. The table currently shows 'No Conditional Access App Control apps found' and includes columns for App, Status, Policies, IDP, Was connected on, and Last activity. A message at the bottom states 'There are no Conditional Access App Control apps' with an 'Add an app...' link.

# Summary & Takeaway

- **Cloud Discovery** helps detect Shadow IT and risky SaaS usage
- **Automatic Upload** connects firewall/proxy logs for real-time insights
- **App Connectors** integrate services like Microsoft 365 for visibility
- **Conditional Access App Control** enforces granular session and access policies

Microsoft Defender for Cloud Apps empowers organizations to uncover hidden app usage, enforce data protection, and strengthen overall security posture in the cloud.

[Home](#) > [Perparim Cloud Solutions](#) >  
Perparim Cloud Solutions

