Real-Time SaaS Threat Protection with Microsoft Defender for Cloud Apps

Stop risky actions *as they happen* — not after the breach.

Home > Perparims Cloud Solutions >

Perparims Cloud Solutions ···

Why This Matters

- Icons + 1-liners:
- 🚫 Prevent data leaks in real time
- 🧠 Analyze risky user behavior
- 🔒 Apply access/session policies based on device, app, location

What is Conditional Access App Control?

- Extends Conditional Access to SaaS apps (e.g., Salesforce, Dropbox)
- Supports both **Access Policies** and **Session Policies**
- Policies apply *even without full device management*

Two Policy Types

- **Access Policies:**
- Block access from unmanaged devices
- Block specific app types (e.g., native Dropbox client)

- **Session Policies:**
- Block downloads of sensitive files
- Require labels or encryption on download

Setup Requirements

- 🛠️ You must:
- Have a **licensed SaaS app** like Salesforce, Dropbox, etc.
- Retrieve **SAML federation metadata** from that app
- Connect app via wizard in Defender

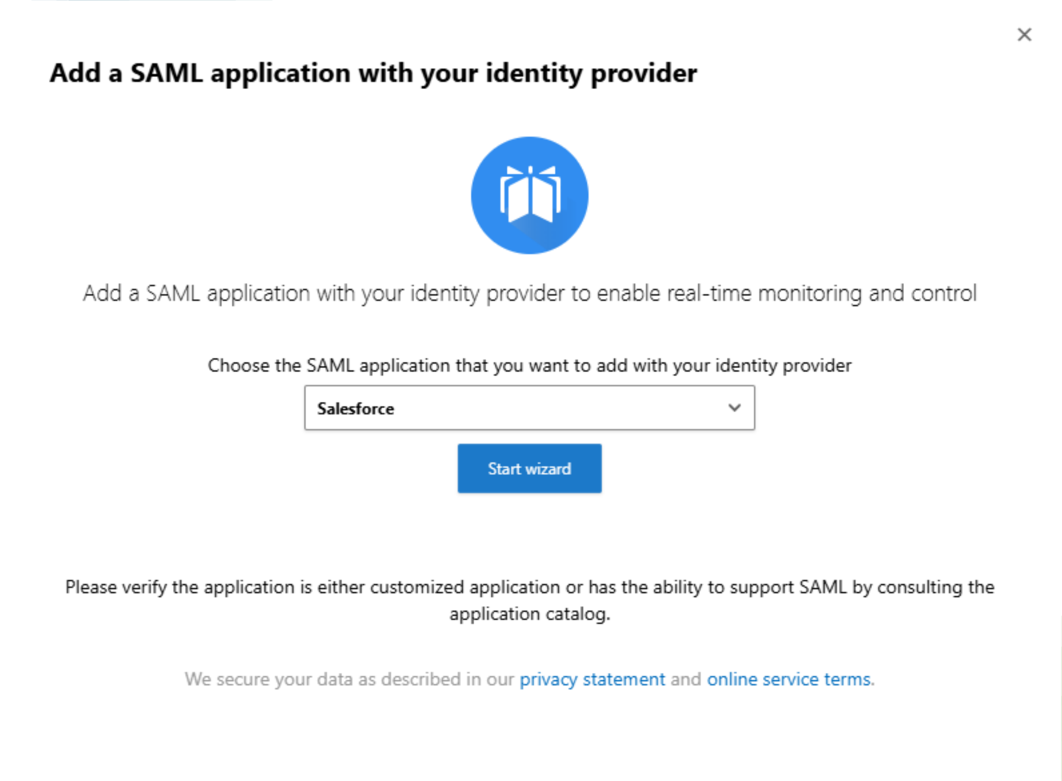
📌 NOTE: In a lab/demo, we *can't fully simulate this*, but we explain the steps.

We’re starting the wizard to add **Salesforce** as a SAML-integrated app.

Why It Matters:

Establishing a SAML trust allows **Defender for Cloud Apps** to monitor and control access in real-time.

- SAML = Security Assertion Markup Language
- This setup enables policies like **blocking sensitive file downloads** or **session monitoring**
- We’re preparing to create **Access** or **Session policies** once the connection is complete



Add a SAML application with your identity provider

Add a SAML application with your identity provider to enable real-time monitoring and control

Choose the SAML application that you want to add with your identity provider

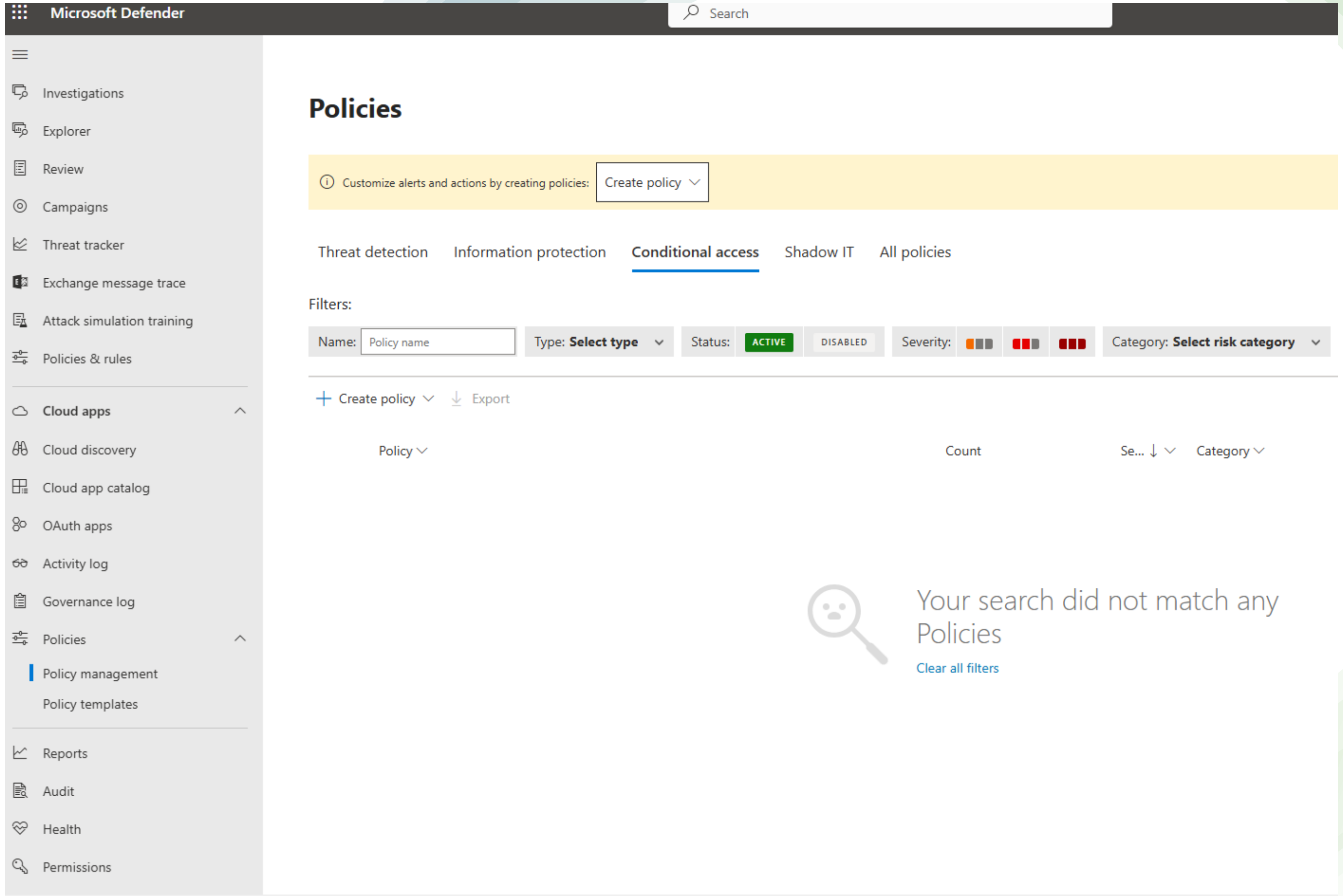
Salesforce

Please verify the application is either customized application or has the ability to support SAML by consulting the application catalog.

We secure your data as described in our privacy statement and online service terms.

Define Conditional Access App Control Policies

- **Policy Types:**
- **Access Policies** – Block access to risky apps or from unmanaged devices
- **Session Policies** – Monitor and control in real time (e.g., block downloads, enforce MFA)
- **Use Case Examples:**
- Block Dropbox access from unmanaged devices
- Prevent sensitive file downloads from OneDrive on personal laptops



Your search did not match any Policies

We're now ready to enforce security by defining **Access** and **Session Policies**—tailored to app risk, device status, and user behavior.

Home > Perparims Cloud Solutions >

Perparims Cloud Solutions ...

Key Takeaways: Secure SaaS with Conditional Access App Control

- 🧠 **What We Learned:**
- Connected SAML-based apps like Salesforce to Microsoft Defender for Cloud Apps
- Understood **Access Policies** vs **Session Policies**
- Explored **real-time monitoring** and **controls** to prevent data exfiltration, enforce MFA, and block risky behaviors
- 🔐 **Why It Matters:**
  This integration strengthens **zero trust** strategies by giving admins deep visibility and control over cloud app behavior—even on unmanaged devices.

#MicrosoftDefender #CloudAppsSecurity #ConditionalAccess #ZeroTrust #PerparimLabs