Be a shepherd for your data, Protect- and prevent data leaks.

It's that simple!

Pim Jacobs
Principal Consultant
InSpark

Ronny de Jong
Security Technical Specialist
Microsoft

Workplace Ninja Summit 2022

Thanks to our sponsors!

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_
SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

APPMANAGEVENT.COM
2022
October 7
NETHERLANDS

dinext.

About “Pim Jacobs”

Focus

Azure Active Directory

Microsoft Entra

Microsoft Endpoint Manager

From

The Netherlands

My Blog

https://identity-man.eu

Certifications

Microsoft MVP

Hobbies

Blogging, Watching Soccer, (trying) to play soccer myself & spending time with my family.

Contact

https://www.linkedin.com/in/pimjacobs89/

https://twitter.com/pimjacobs89

About “Ronny de Jong”

Focus

Zero Trust, Microsoft (365) Defender
Making the Netherlands more secure

From

Netherlands

My Blog

https://ronnydejong.com

Certifications

Former Microsoft MVP
Cybersecurity Architect

Hobbies

Relaxing, Fishing, BBQ, CrossFit, F1

Contact

https://www.linkedin.com/in/ronnydejong/
https://twitter.com/ronnydejong

Agenda

Introduction of Defender for Cloud Apps

Key features and importance as organizations are licensed but aren’t using DfCA 😐

Retrieving data by enabling integration

Learn how to retrieve data, enable integrations and work with the gathered data

Defender for Cloud App Policies

Learn what policies are available and how to enable or create policies yourself

Considerations & next steps

Tips & tricks to get you kick started

Questions

…and hopefully we have some answers 😜

Key takeaways:

- **Start retrieving data by enabling integrations today**
- **Start exploring policies and more advanced data protection methods**
- **Implement newly created policies for your pilot user group**

Introduction of Defender for Cloud Apps

What is Defender for Cloud Apps

Defender for Cloud Apps:

- Is the gatekeeper to **broker access** in real time between your enterprise users and **cloud resources** they use (anywhere, anyplace, any device).
- Can **discover** and provide visibility into **Shadow IT** and app use, **assesses** the compliance of cloud services and **monitors** anomalous behaviours
- Can **controls access** to resources, provides the ability to classify and **prevent** sensitive information leak and **protects** against malicious actors.
- Can with the above address **security** & **compliance** gaps in an organization's use of **cloud services**, whereby this goes further than just Microsoft services!
- Therefore, helps your IT Team to find the right **balance** of supporting **access** while **protecting** data and helps to **discover** Shadow IT.

Defender for Cloud Apps use-cases

This is super cool but what are my use cases?

- **Getting insights**
  - Know which apps are used in your organization and by whom
  - Use of Dropbox within your organization
  - Use of over privileged applications
- **Helps to make decisions**
  - Are these apps allowed?
  - Are these apps complaint?
  - Setup Single Sign-on for protection and new functionality
- **Improving your protection level**
  - Conditional Access is great, but it can be better and more granular
  - Restrict cut/copy & paste from browser sessions
- **Getting alerts**
  - Mass downloads or worse mass deletes
  - Stale externally shared files
  - And much more!

Retrieving data by enabling integration

Getting Defender for Cloud Apps data

Ways to get data into Defender for Cloud Apps:

- Defender for Endpoint*
- App Connectors
  - Office 365 & Microsoft Azure (out of the box)
  - 3rd Party app Connectors
- Microsoft Purview Information Protection
- Log collectors
  - Docker instance deployed next to your firewall
  - Firewall syslog against Docker instance
  - Docker instance uploads data to Defender for Cloud Apps to get visuals and insights

* Microsoft Defender for Cloud Apps + Defender for Endpoint P2

Enable Microsoft Integrations

Which Microsoft integrations are available:

- **Defender for Endpoint**
  - For uploading data from Defender for Endpoint to Defender for Cloud Apps to **get insights**
- **Defender for Identity**
  - To enable a complete protection and investigation experience for users in **hybrid** environments
- **Identity Protection**
  - For unified alerts view and **enhanced investigation experience** for identity alert
- **Microsoft Information Protection**
  - Enables the use of file policies and being able to set sensitivity labels automatically.

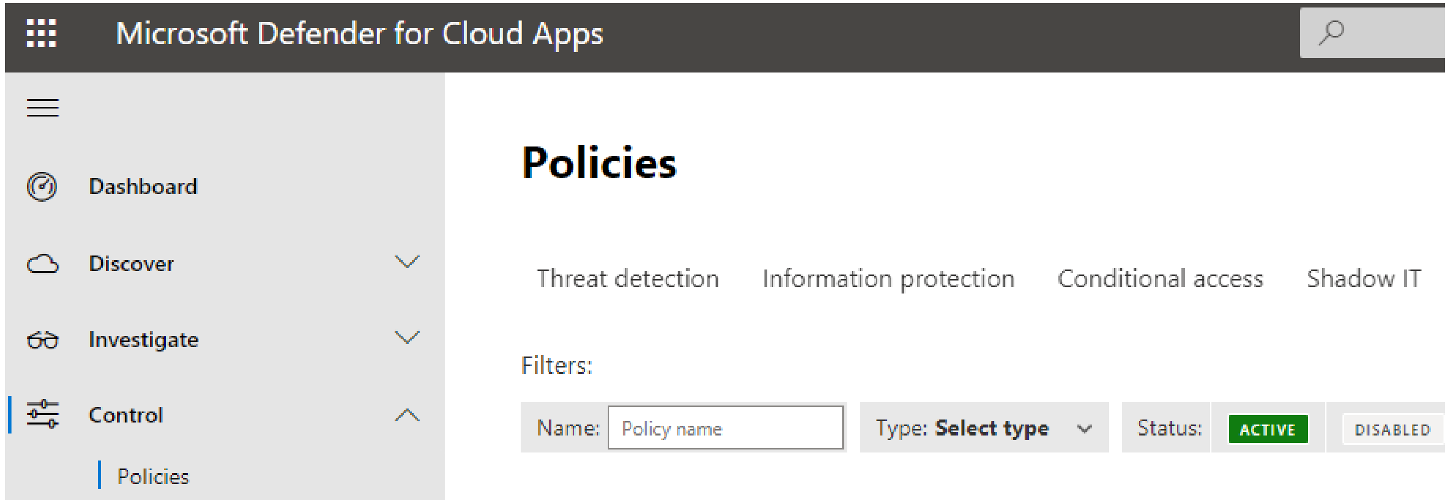
Demo

- Learn how to configure the basics
- Learn how to enable integration(s)
- Learn how to work with the gathered data in Defender for Cloud Apps.

Defender for Cloud App Policies

Available policy types

- **Shadow IT**
  - App discovery policy
  - Cloud Discovery anomaly detection policy
- **Conditional access**
  - Access Policies
  - Session Policies
- **Threat detection**
  - Activity Policies
  - OAuth app policies
- **Information Protection**
  - File Policies



Name: Policy name

Type: Select type

Status: ACTIVE

DfCA Shadow IT policies

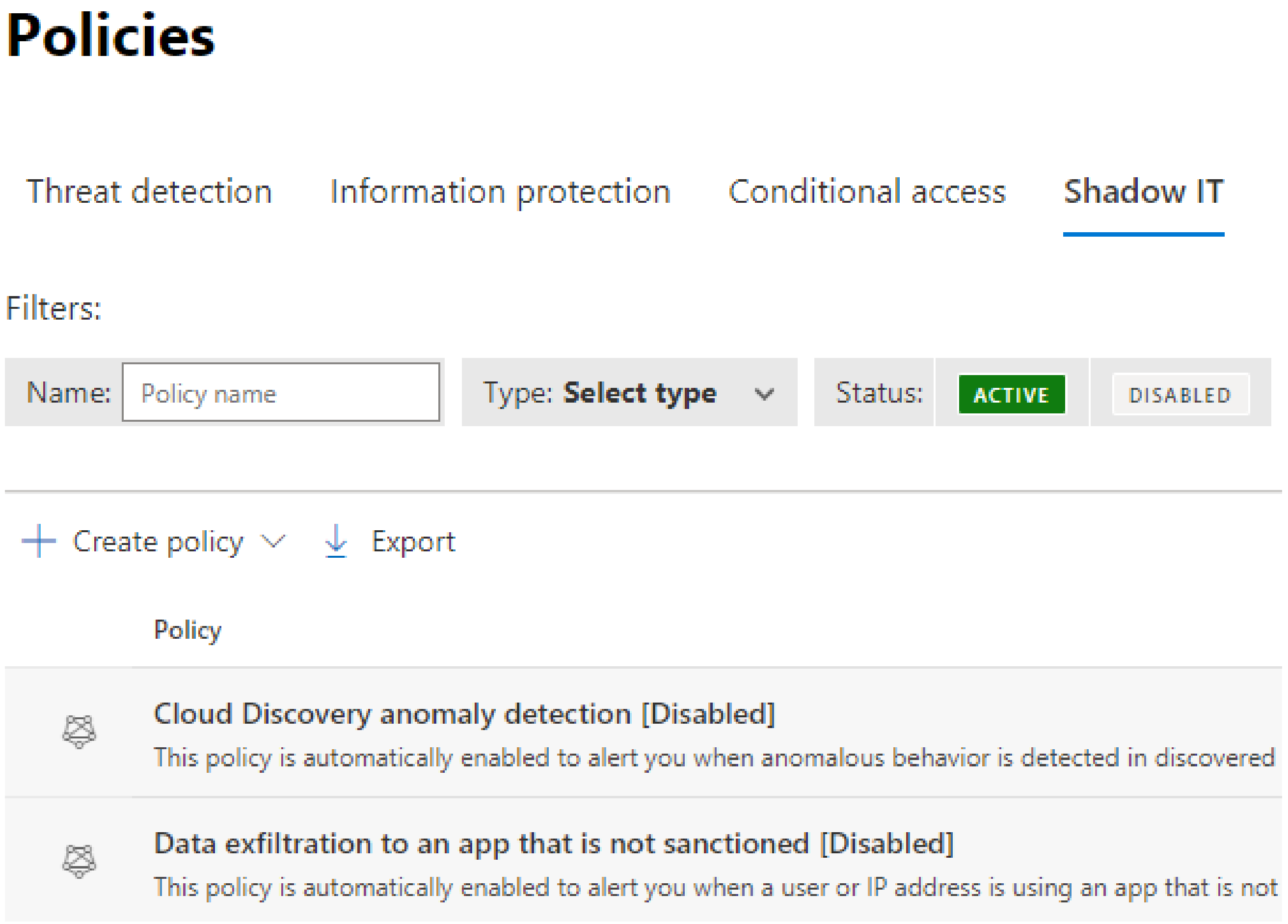
www.wpninjas.eu

What can we do with DfCA Shadow IT policies?

- Monitor anomalies and newly discovered apps

From the field examples:

- New risky app
- New cloud storage app
- New collaboration app
- Anomaly detection in large amount of uploaded data compared to other users or user’s history



Policies

Threat detection | Information protection | Conditional access | **Shadow IT**

Filters:

Name: Policy name | Type: **Select type** | Status: ACTIVE | DISABLED

Policy

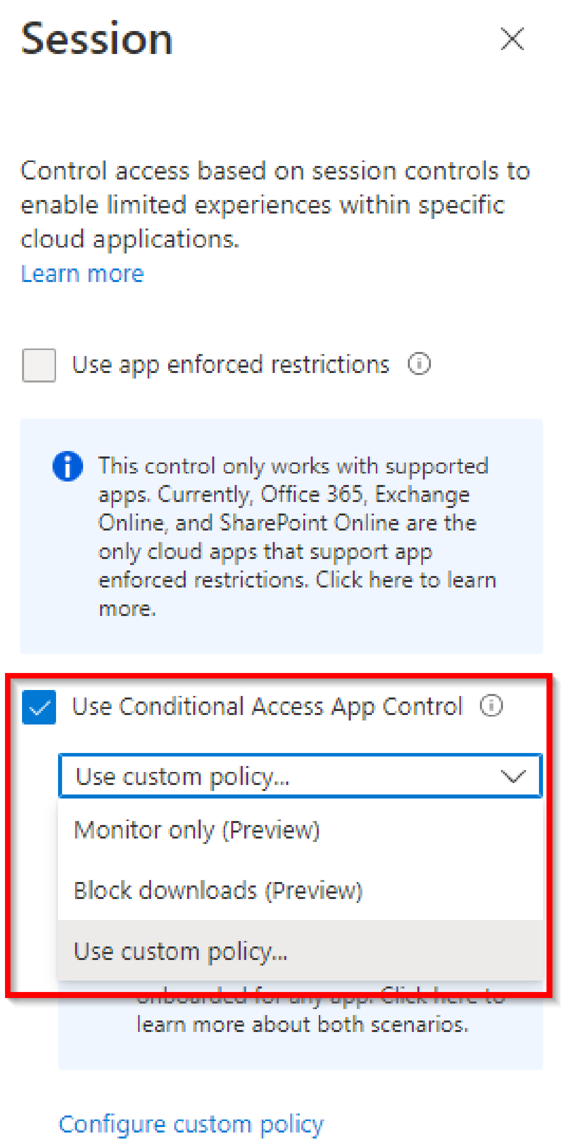
Cloud Discovery anomaly detection [Disabled]
This policy is automatically enabled to alert you when anomalous behavior is detected in discovered

Data exfiltration to an app that is not sanctioned [Disabled]
This policy is automatically enabled to alert you when a user or IP address is using an app that is not

Azure AD Conditional Access policies

Conditional Access Session Access Controls

- Available within Conditional Access to:
    - Monitor only
    - Block downloads
    - Use a custom policy
- Only when using the custom policy setting it will look at your self-made DfCA Conditional Access policies



Session

Control access based on session controls to enable limited experiences within specific cloud applications.
Learn more

□ Use app enforced restrictions ⓘ

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

☑ Use Conditional Access App Control ⓘ

Use custom policy...

Monitor only (Preview)

Block downloads (Preview)

Use custom policy...

onboarded for any app. Click here to learn more about both scenarios.

Configure custom policy

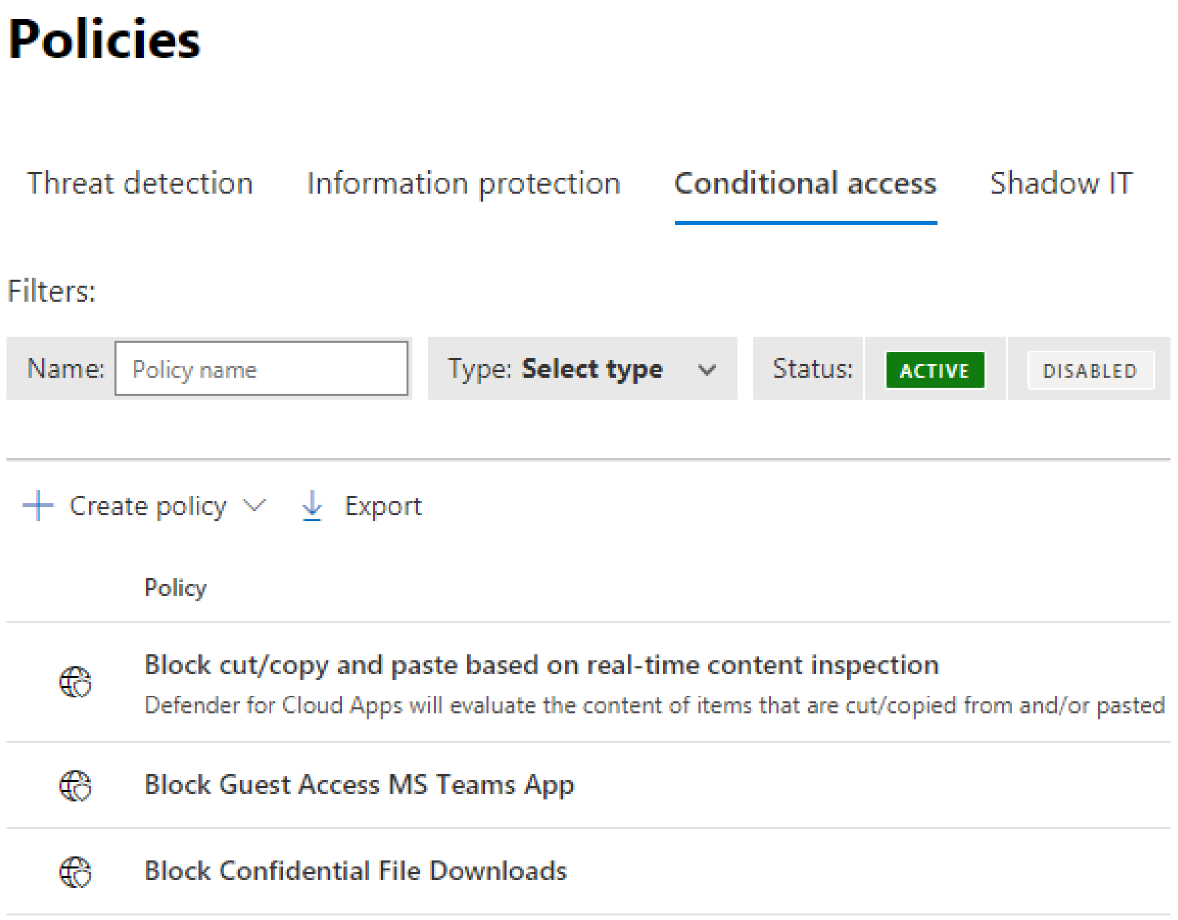
DfCA Conditional Access policies

What can we do with DfCA Conditional Access policies?

- Monitor Access and Sessions
  - Access is used for mobile and desktop apps
  - Session is used for browser-based apps
- Apps must support Conditional Access App Control

From the field examples:

- Restrict cut/copy/paste for users without a managed / compliant device
- Block downloads on noncompliant devices
- Limit restrictions for guest users (just protection your end users is not enough ☹)



Policies

Policy
Block cut/copy and paste based on real-time content inspection Defender for Cloud Apps will evaluate the content of items that are cut/copied from and/or pasted
Block Guest Access MS Teams App
Block Confidential File Downloads

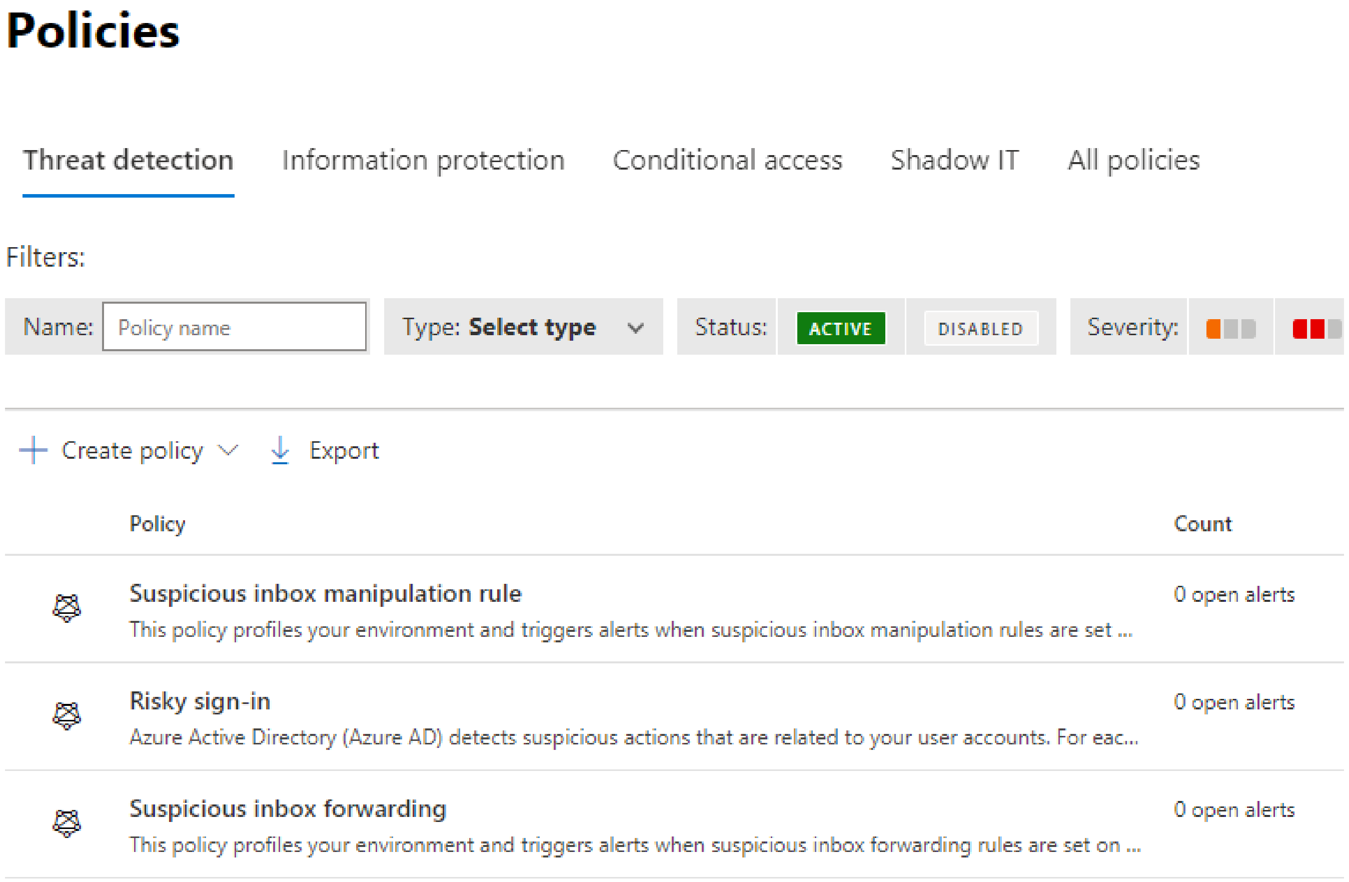
DfCA Threat detection policies

What can we do with DfCA Threat detection policies?

- Monitor activities & OAuth apps

From the field examples:

- Mass downloads
- Mass deletes
- Assigned Permissions
- Logon from Risky IP address
- Logon from an outdated browser
- Potential ransomware activity



Policies

Threat detection | Information protection | Conditional access | Shadow IT | All policies

Filters:

Name: Policy name | Type: **Select type** | Status: ACTIVE DISABLED | Severity:

＋ Create policy ⌵ ⤓ Export

Policy	Count
Suspicious inbox manipulation rule This policy profiles your environment and triggers alerts when suspicious inbox manipulation rules are set ...	0 open alerts
Risky sign-in Azure Active Directory (Azure AD) detects suspicious actions that are related to your user accounts. For eac...	0 open alerts
Suspicious inbox forwarding This policy profiles your environment and triggers alerts when suspicious inbox forwarding rules are set on ...	0 open alerts

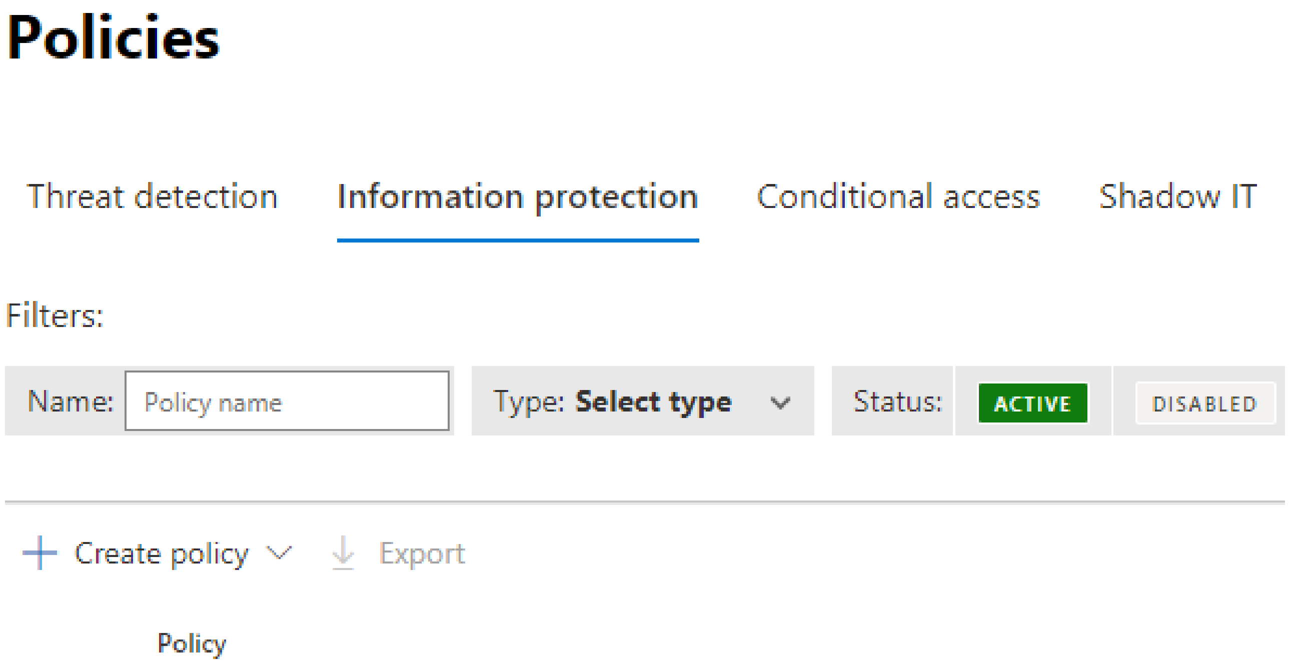
DfCA Information Protection policies

What can we do with DfCA Information Protection policies?

- Monitor Activity on files within your tenant.

From the field examples:

- Confidential files shared with personal email addresses
- Stale externally shared files
- File shared with unauthorized domain(s)



Policies

Threat detection | Information protection | Conditional access | Shadow IT

Filters:

Name: Policy name

Type: **Select type**

Status: ACTIVE DISABLED

+ Create policy

Export

Policy

Demo

- Learn the difference between App Enforced Restrictions and DfCA Policies
- Learn how to protect web-based access to your data
- Learn how to protect data access by Desktop Apps

Tips & Tricks

And start being a shepherd for your data!

How & where to start tomorrow?

- Start **enabling integrations** with Defender for Cloud Apps
- **Review high risk apps** with ‘over privileged’ permissions
- Review build in policies and **setup alerts where needed**
  - Especially Shadow IT & Threat detection are important here.
- If **sensitivity labels** are in need make sure those are **available** for use
- **Create your Access and Session policies** within Defender for Cloud Apps
  - For end users **AND** Guest users!
- Start with a **small pilot group** which you’re targeting in Conditional Access.
- **Fine tune** where this is needed and required
- Roll-out to **full production**

Q & A

Thank You

Wednesday, September 14 • 08:00 - 09:00

✓ Attack Surface Reduction rules... your best ally against ransomware!

Please rate my session!

😀 😐 🙁

○ ○ ○