Onboard Microsoft 365 Defender

1. Prerequisites

- Activated Microsoft Defender for Endpoint license with the instance running in the correct location
- Representative with Global Administrator and Security Administrator role access
- Successfully completed “TSD SOP - 03 Onboard Azure tenant guest access”

2. General information

This guide does not include device grouping scenarios. It is important to understand that any device group that does not include all the access groups described below, will cut the visibility for the SOC to those devices. It is ok to leave the assigned access empty on the device group, it will then apply the global RBAC privileges.

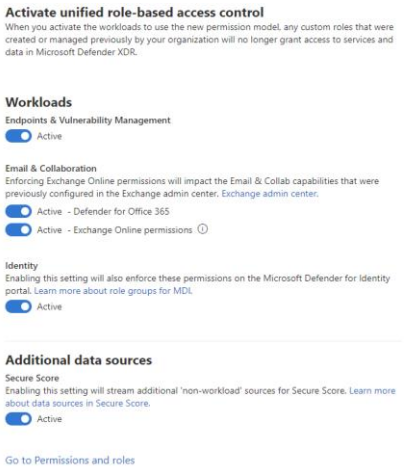
3. Tasks

Five roles must be created in the portal. These roles must be assigned to five security groups according to this pattern:

- Browse to https://security.microsoft.com/

3.1. Activate RBAC for workloads

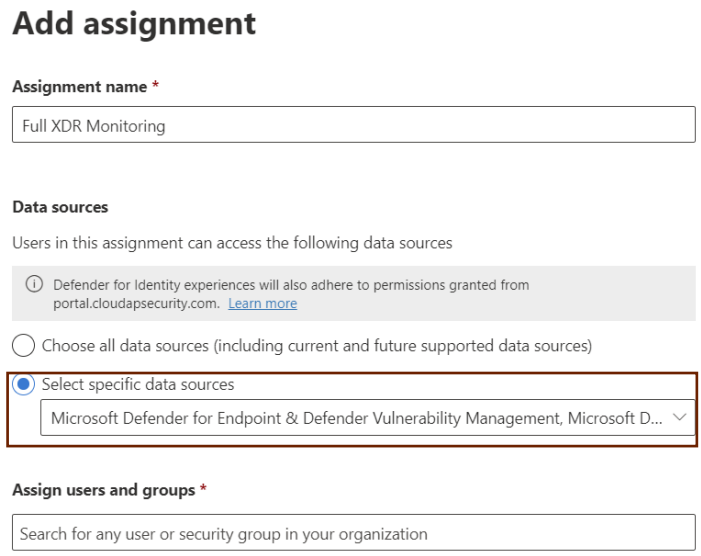
- Click “Settings” → “Defender XDR” → “Permissions and roles”
- Use the slider as listed below to activate workloads. It is important to know that enabling of any of the following workloads will deactivate and RBAC permissions created in MDE.



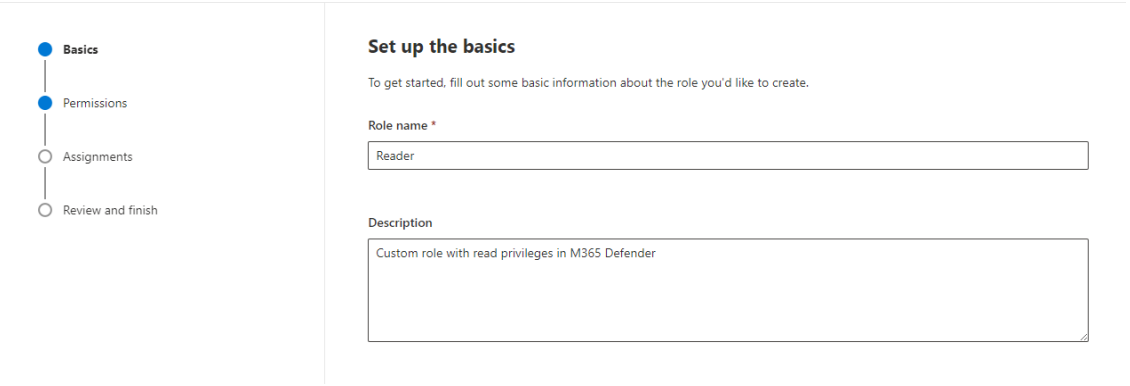
Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se

3.2. Create custom roles

Create four custom roles with the level of access that correlates to the agreement between customer and Truesec. This example will be onboarding full XDR + Defender for Cloud monitoring with extended access for live responders to act on mail flows (Move or Delete email to the junk email folder, deleted items or inbox, including soft and hard delete of email). For alternative scopes the following settings should be configured:



- Click “Permissions” in the left side navigation -> “Microsoft 365 Defender, Roles”.
- Click “Create custom role” and create: Reader, Operator, Privileged Operator, Live Responder
- Start off with assigning a name and description that corresponds to the role that you are configuring.

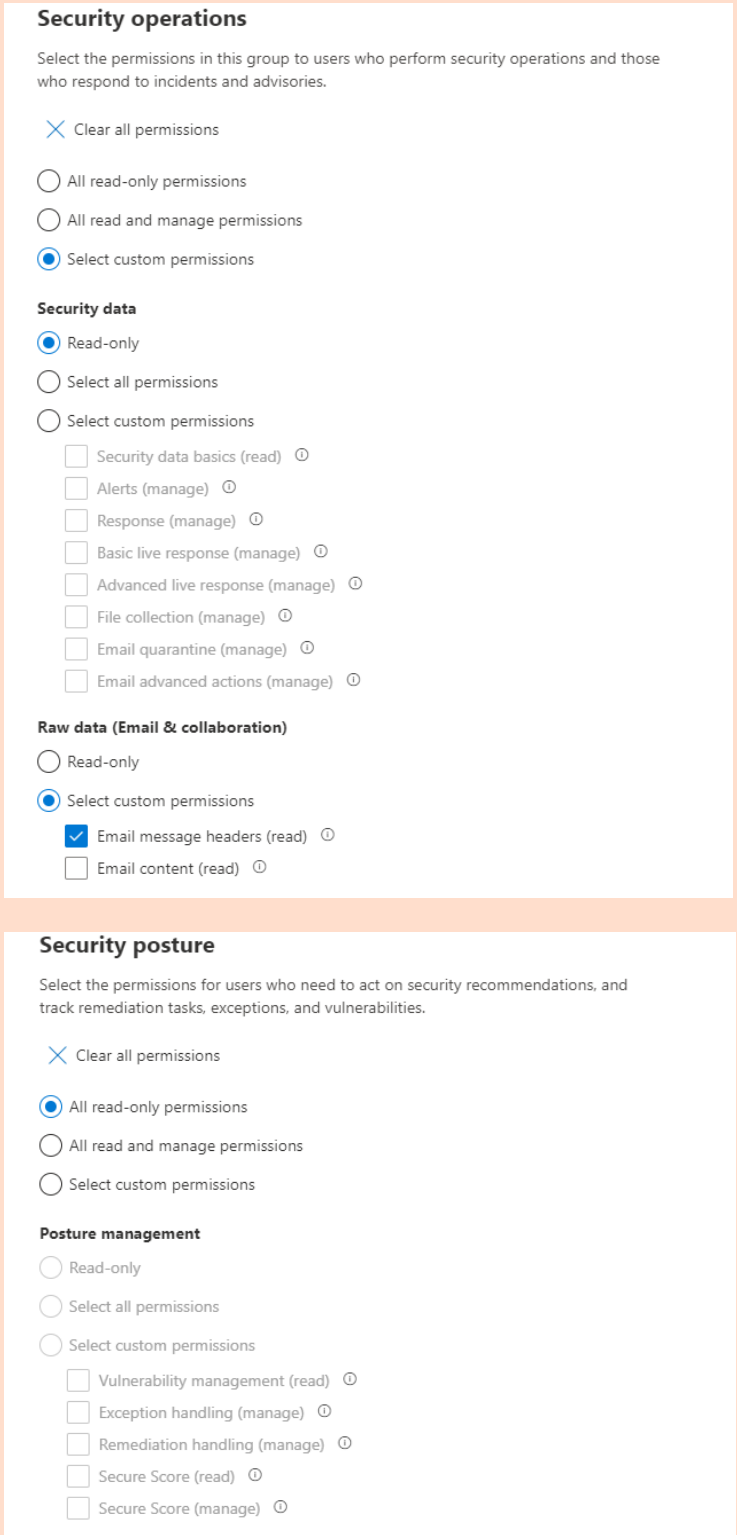


- Follow the wizard for each of the roles that you are configuring with the following attributes.

Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se

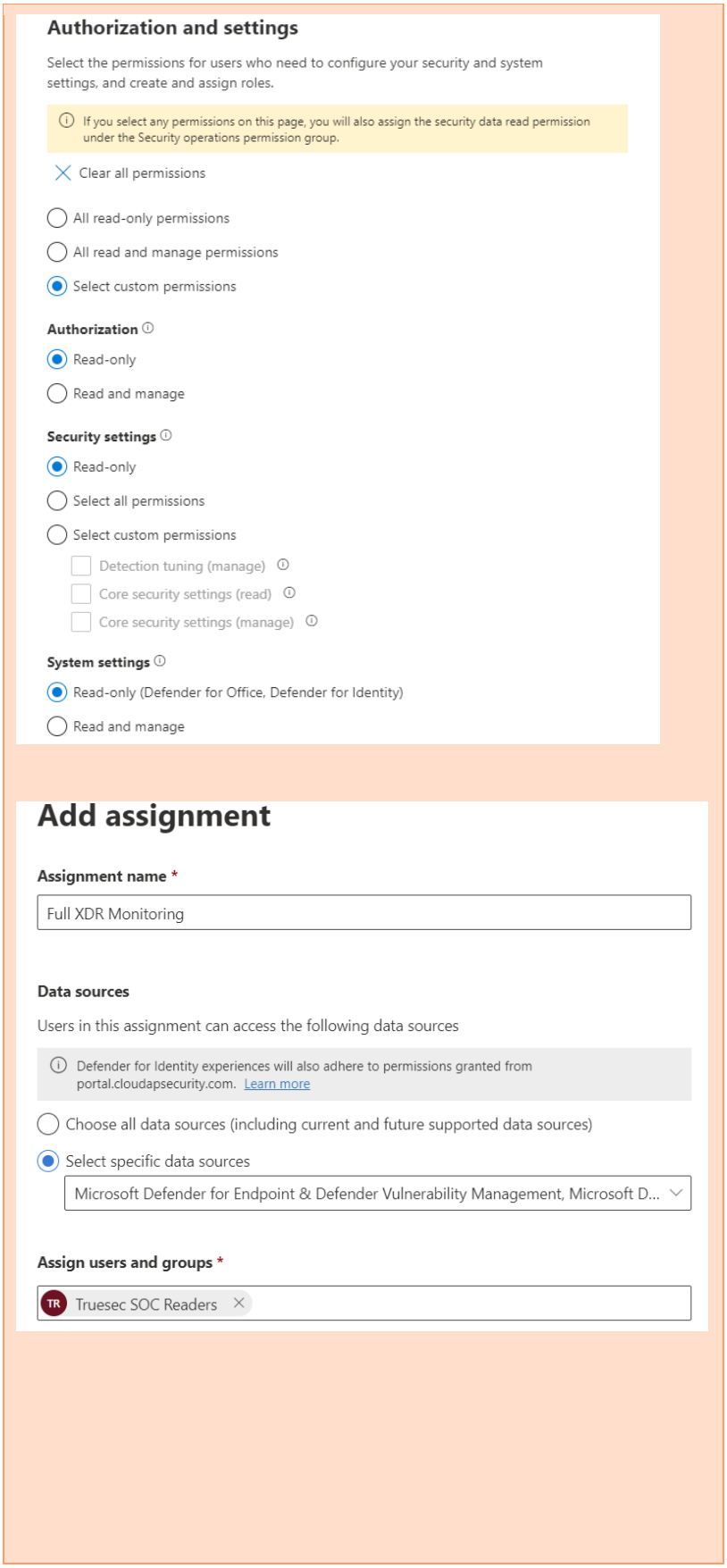
Role

Readers



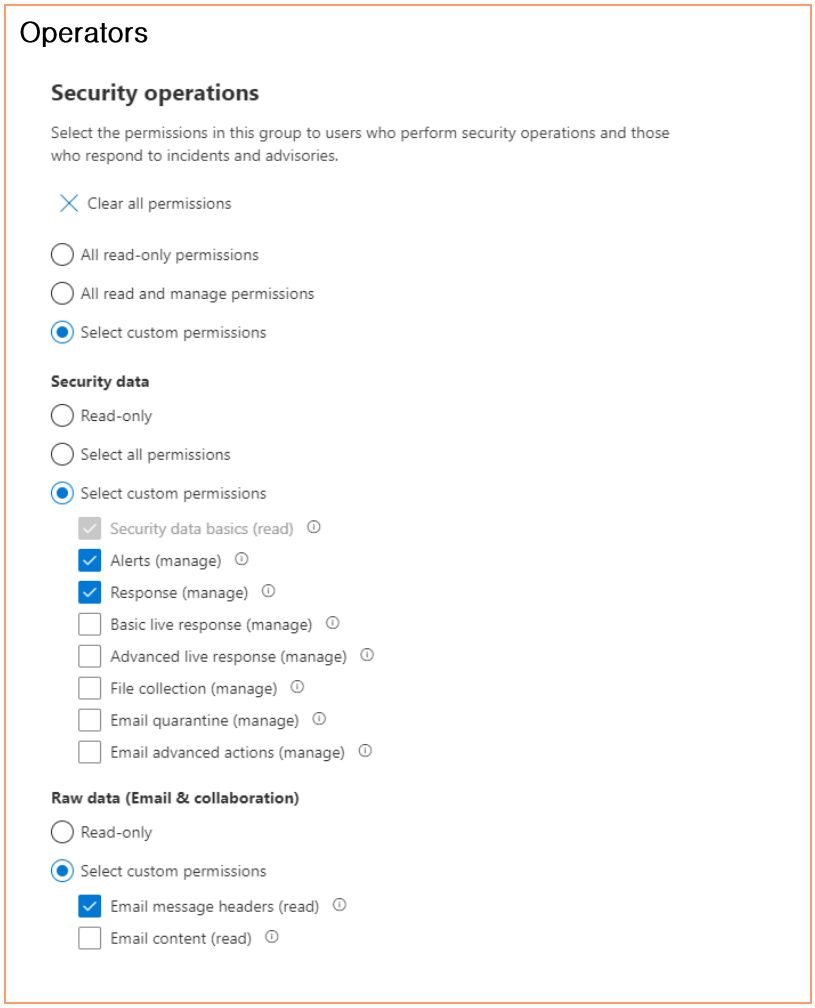
Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

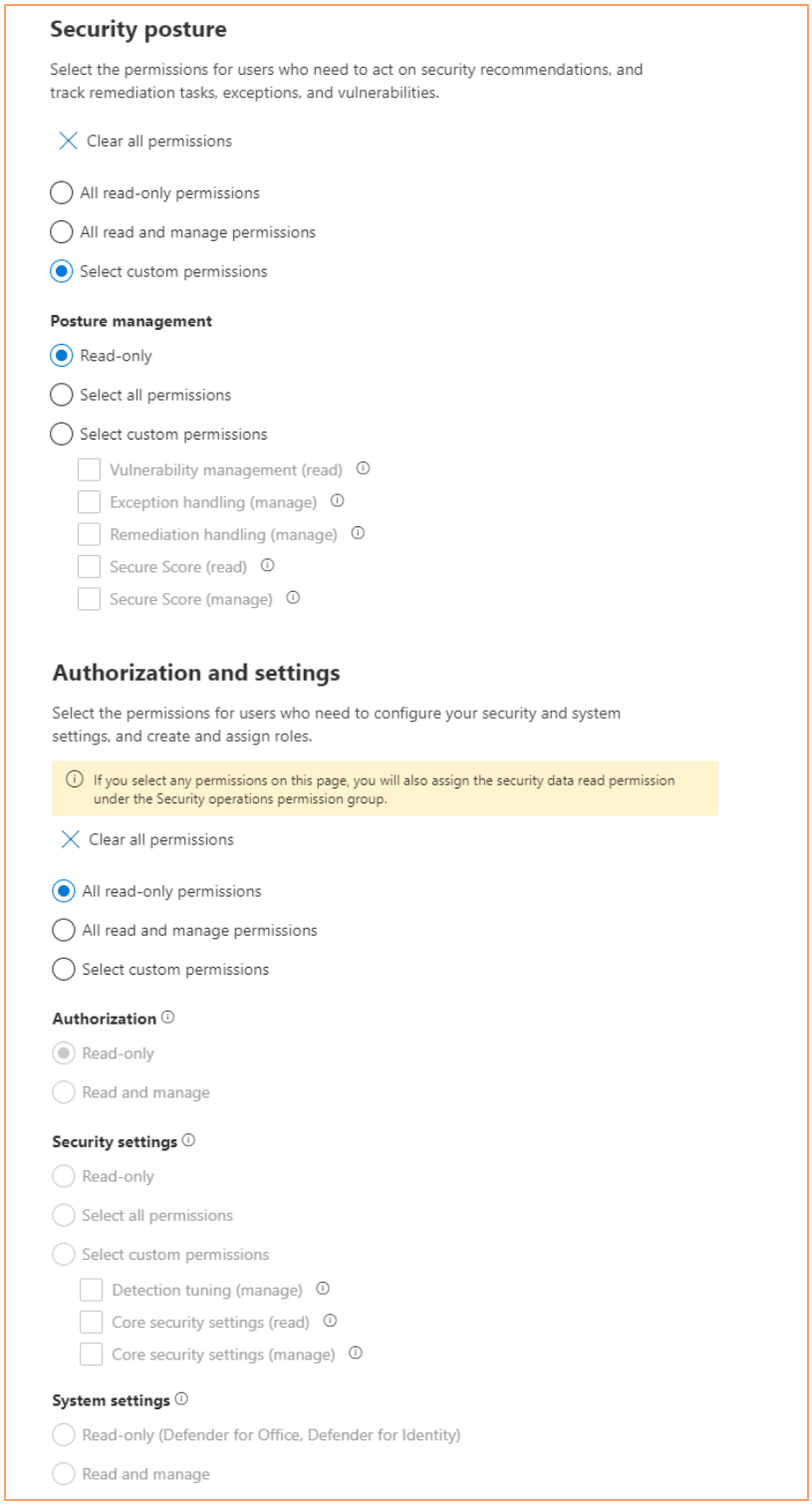


Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se

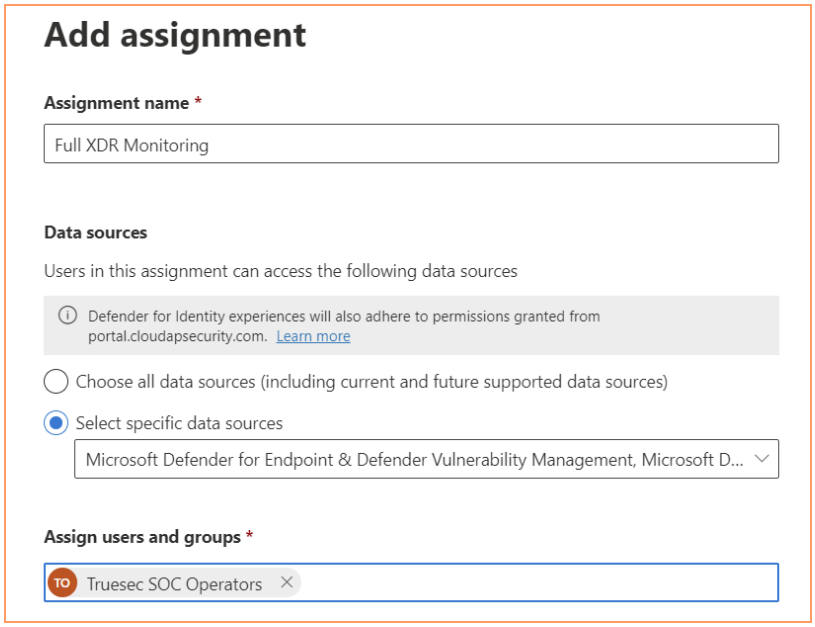
Operators



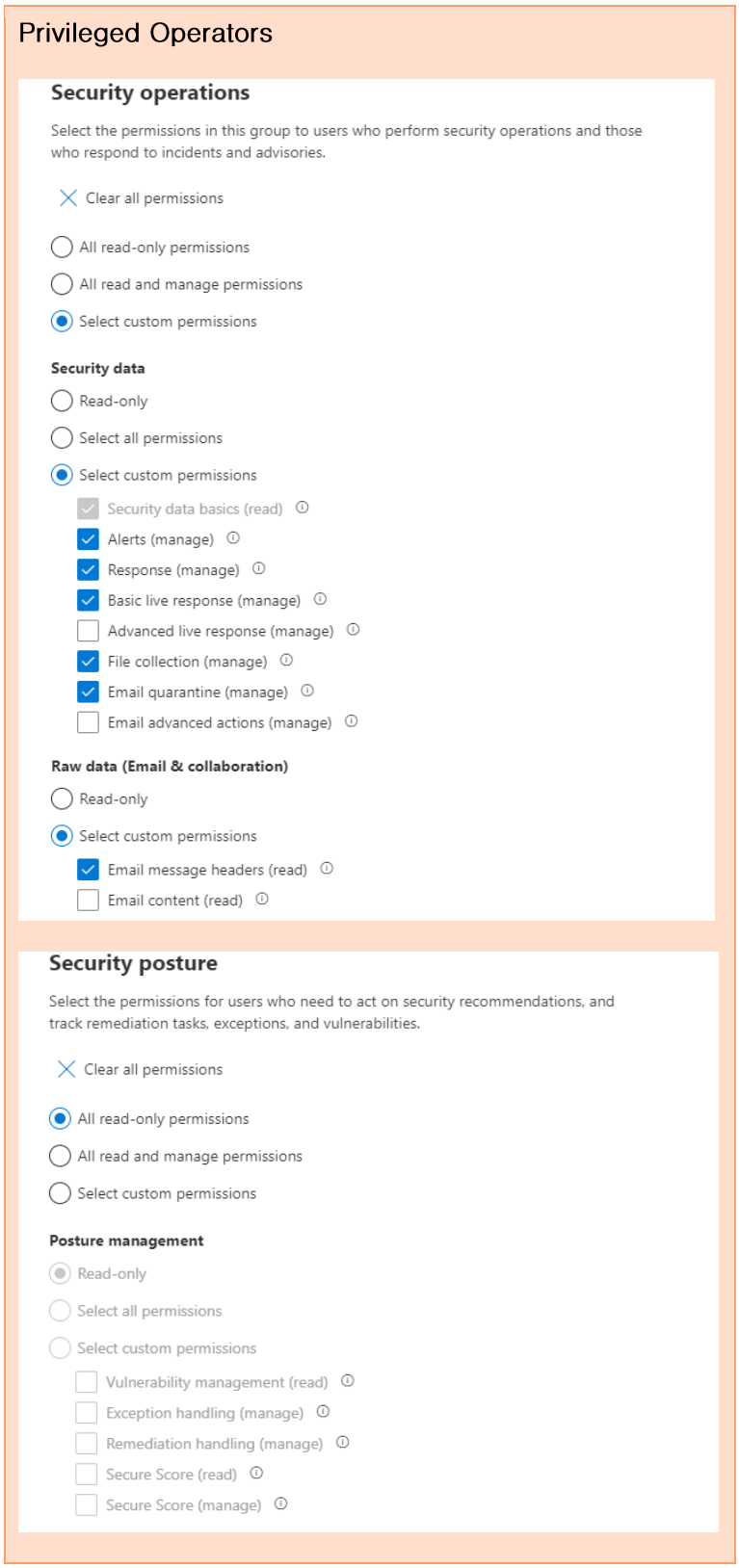
Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se



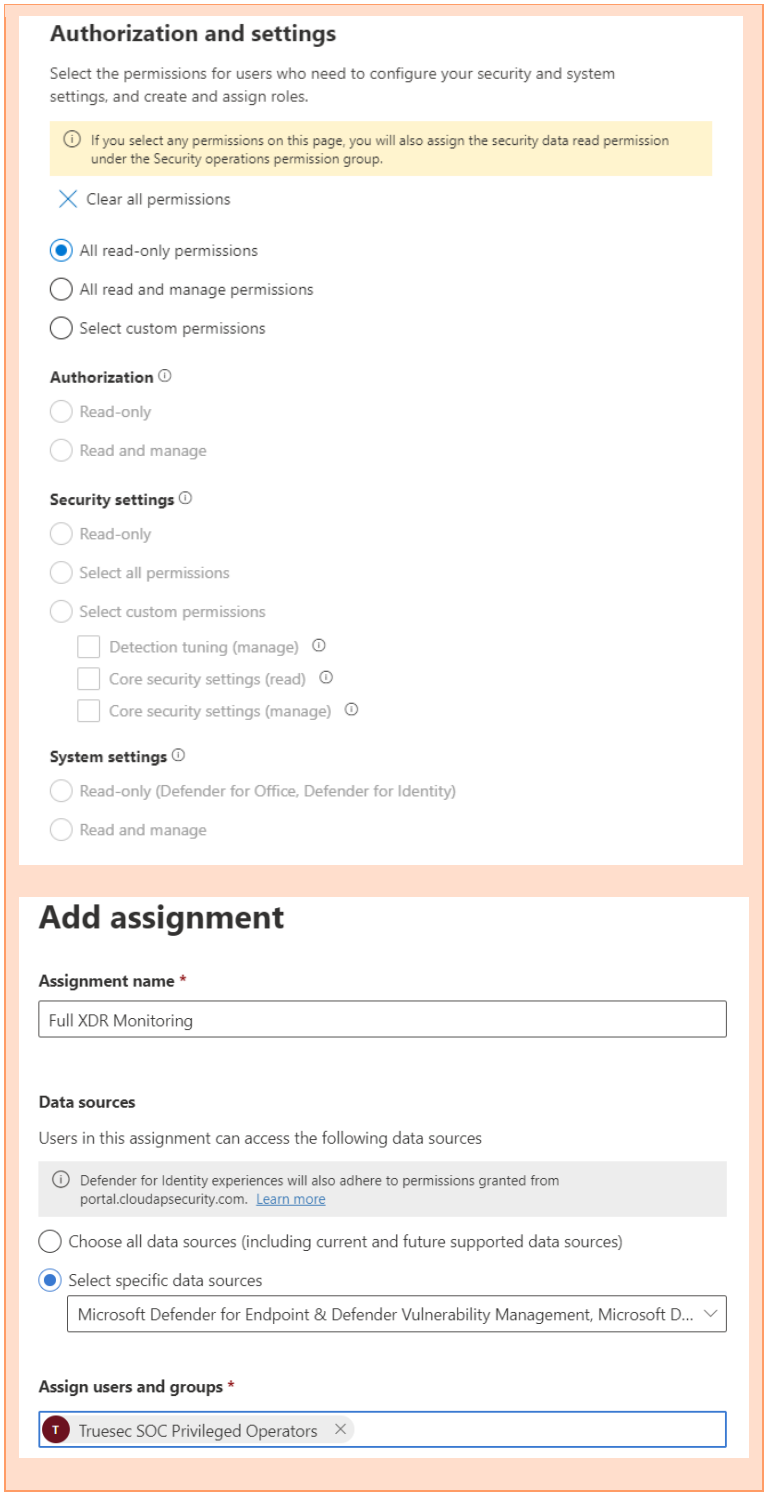
Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se

Live Responders

Security operations

Select the permissions in this group to users who perform security operations and those who respond to incidents and advisories.

Clear all permissions

- ○ All read-only permissions
- ○ All read and manage permissions
- ◉ Select custom permissions

Security data

- ○ Read-only
- ○ Select all permissions
- ◉ Select custom permissions
  - ☑ Security data basics (read)
  - ☑ Alerts (manage)
  - ☑ Response (manage)
  - ☑ Basic live response (manage)
  - ☑ Advanced live response (manage)
  - ☑ File collection (manage)
  - ☑ Email quarantine (manage)
  - ☑ Email advanced actions (manage)

Raw data (Email & collaboration)

- ○ Read-only
- ◉ Select custom permissions
  - ☑ Email message headers (read)
  - ☐ Email content (read)

Security posture

Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities.

Clear all permissions

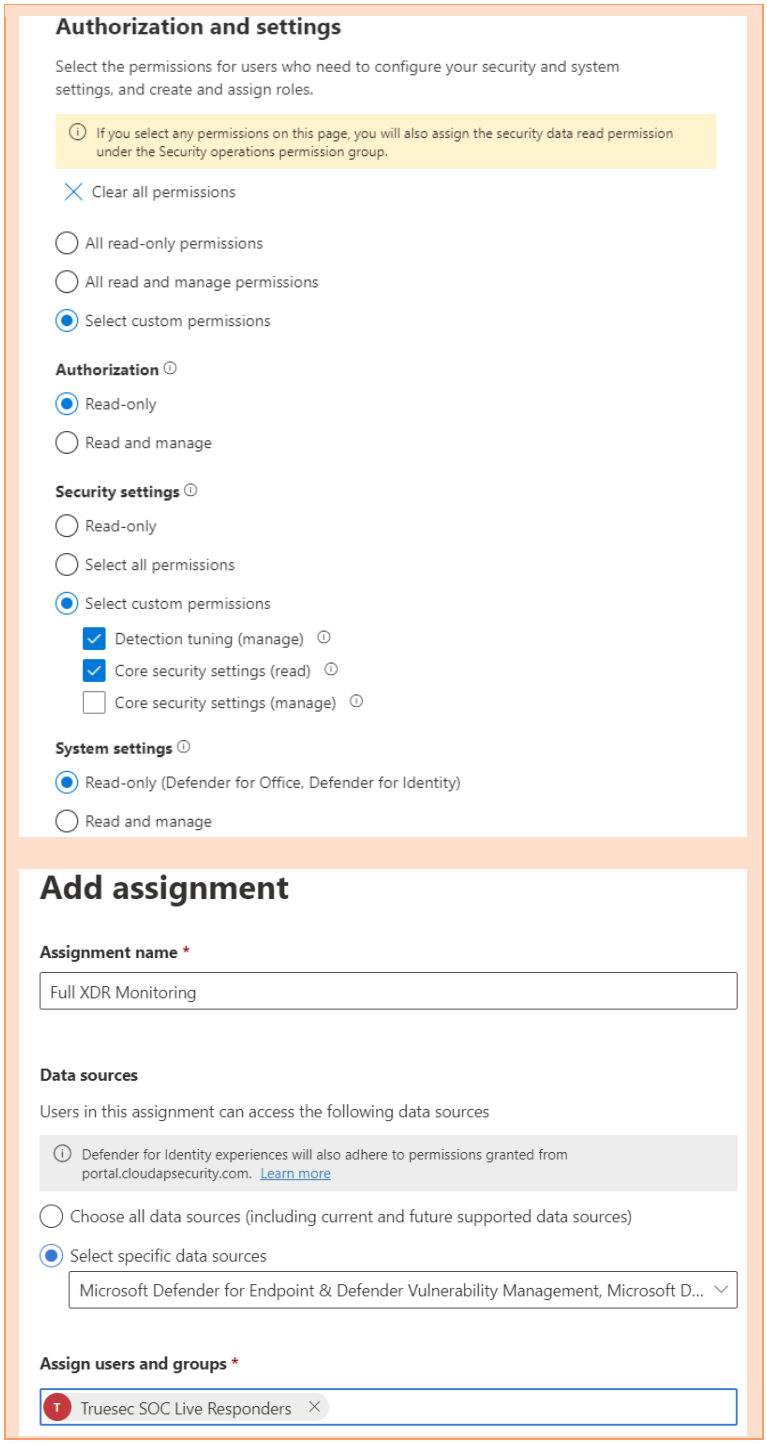
- ◉ All read-only permissions
- ○ All read and manage permissions
- ○ Select custom permissions

Posture management

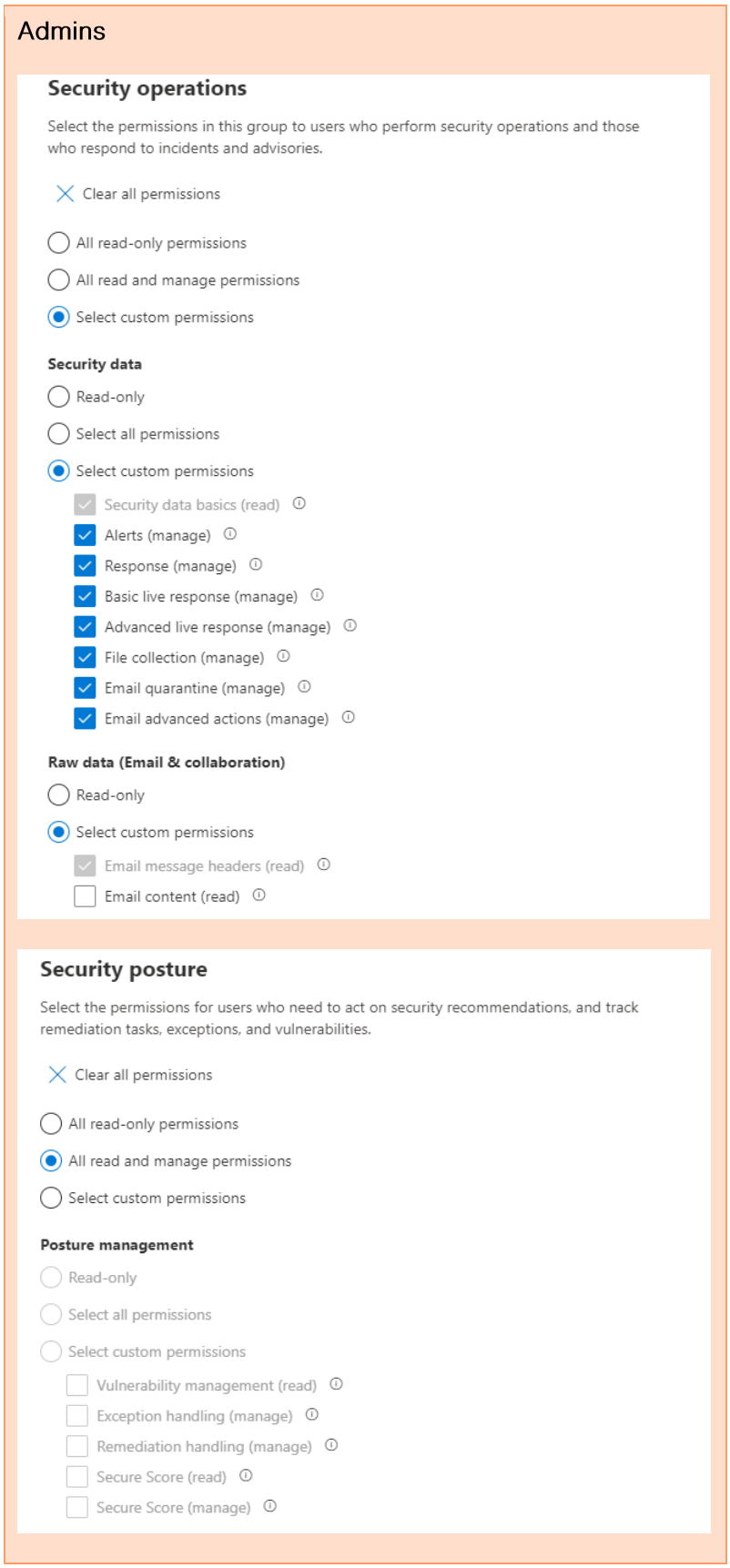
- ○ Read-only
- ○ Select all permissions
- ○ Select custom permissions
  - ☐ Vulnerability management (read)
  - ☐ Exception handling (manage)
  - ☐ Remediation handling (manage)
  - ☐ Secure Score (read)
  - ☐ Secure Score (manage)

Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com

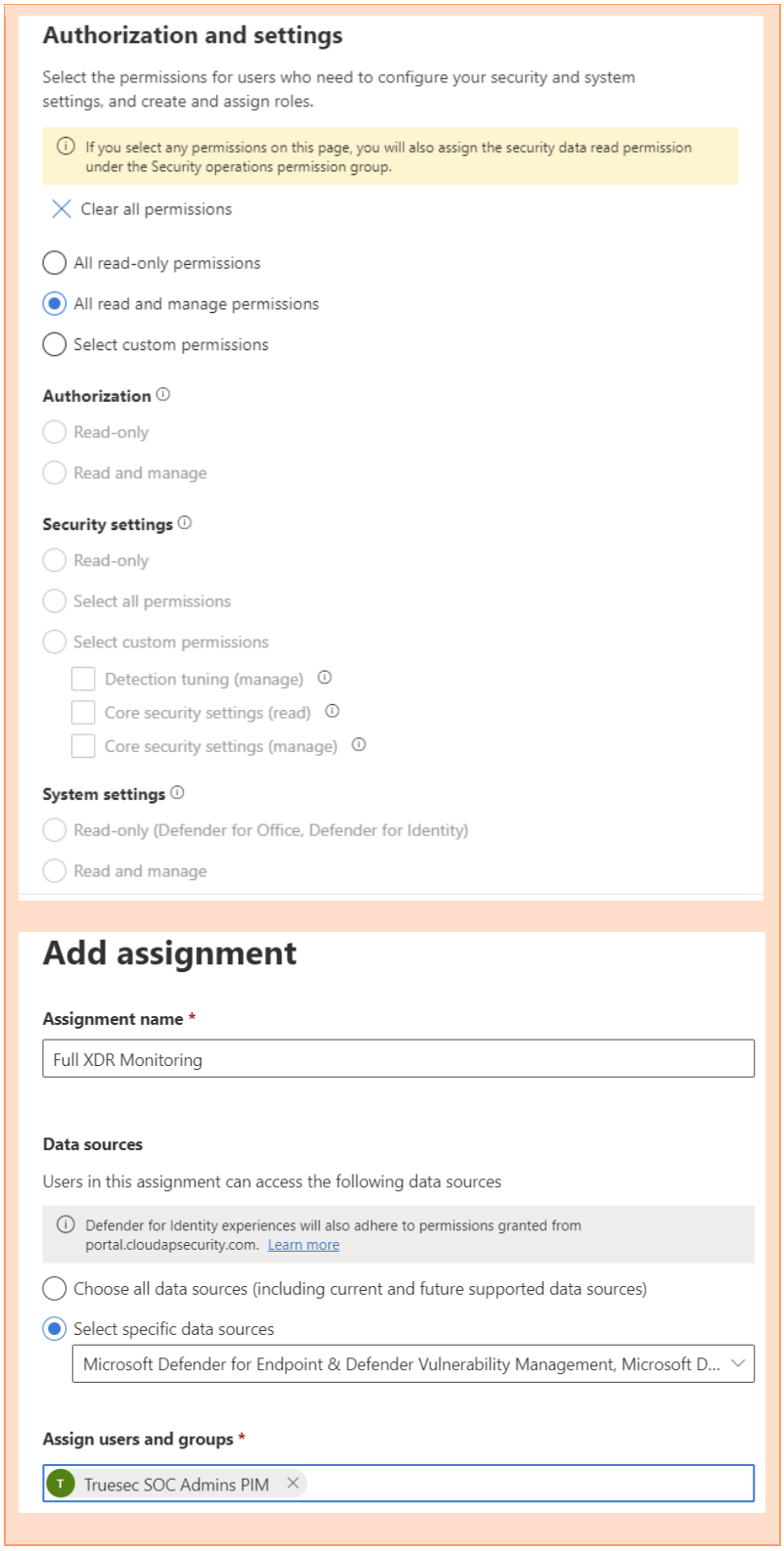
Sweden
+46 810 00 10
info@truesec.se



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se

3.3. Configure Advanced features

- Under “Settings” → “Endpoints”, click “Advanced features”

3.3.1. Make sure the following features are enabled

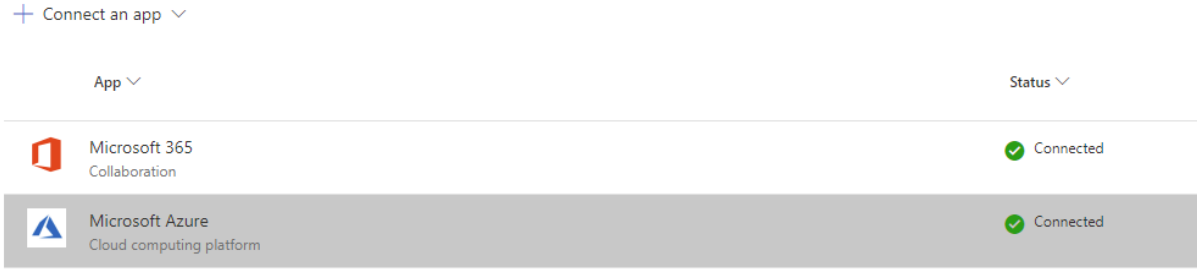
- Live Response (mandatory for MDR services)
- Live Response for Servers
- Preview features

3.3.2. Make sure the following feature is disabled

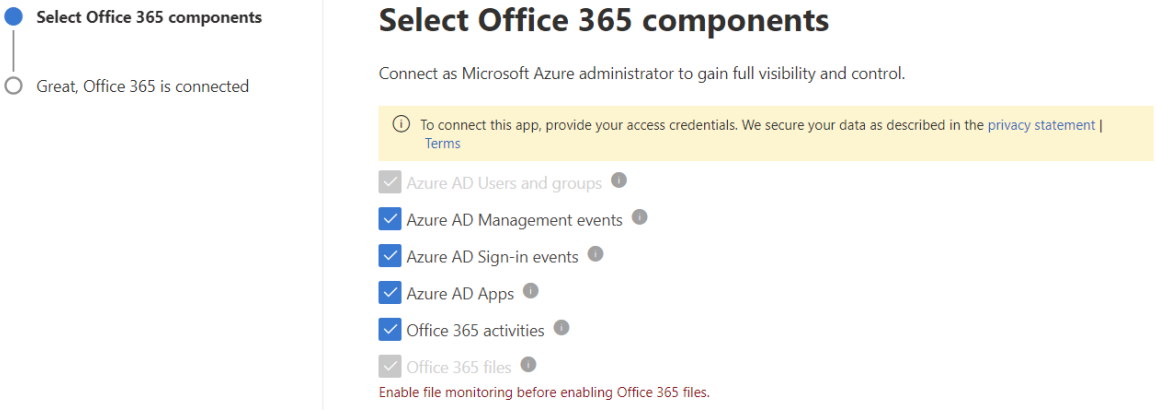
- Automatically resolve alerts (mandatory for MDR services)
- Live Response unsigned script execution

3.4. Configure Cloud Apps Connector

- Under “Settings” →”Cloud apps”, click “App Connectors”
- Make sure that “Microsoft 365” and “Microsoft Azure” are connected and that both are receiving data.



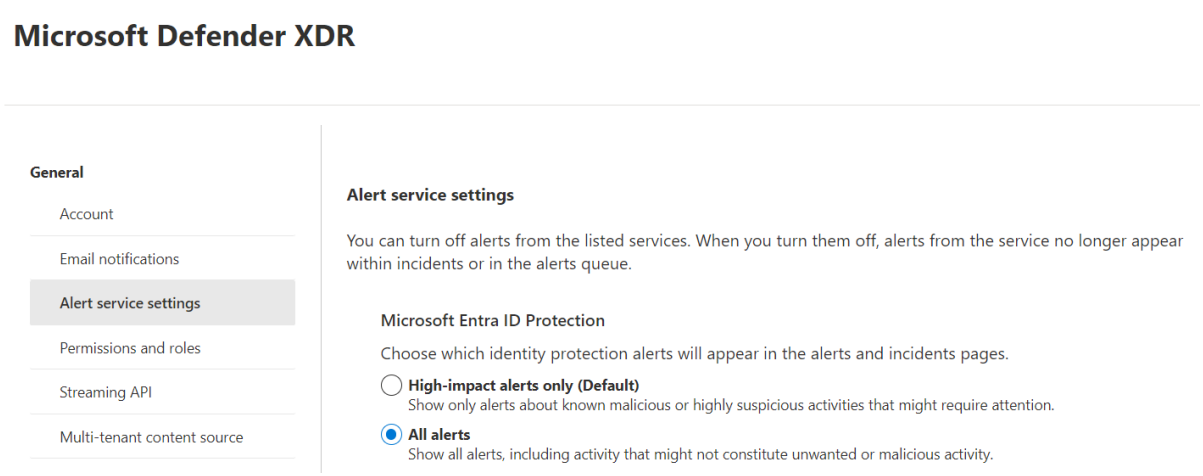
- Edit settings for the Microsoft 365 connector and select all available data sources.



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se

3.5. Configure Entra ID Protection alert service

- Under “Settings” →”Microsoft Defender XDR”, click “Alert service settings”
- Make sure that “All alerts” is selected



Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se