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.

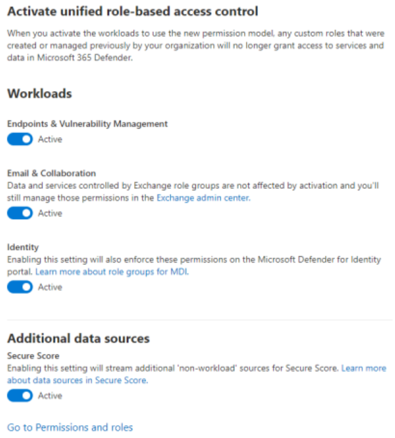
3. Tasks

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” → “Microsoft 365 Defender” → “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.



Activate unified role-based access control

When you activate the workloads to use the new permission model, any custom roles that were created or managed previously by your organization will no longer grant access to services and data in Microsoft 365 Defender.

Workloads

Endpoints & Vulnerability Management
Active

Email & Collaboration
Data and services controlled by Exchange role groups are not affected by activation and you'll still manage those permissions in the Exchange admin center.
Active

Identity
Enabling this setting will also enforce these permissions on the Microsoft Defender for Identity portal. Learn more about role groups for MDI.
Active

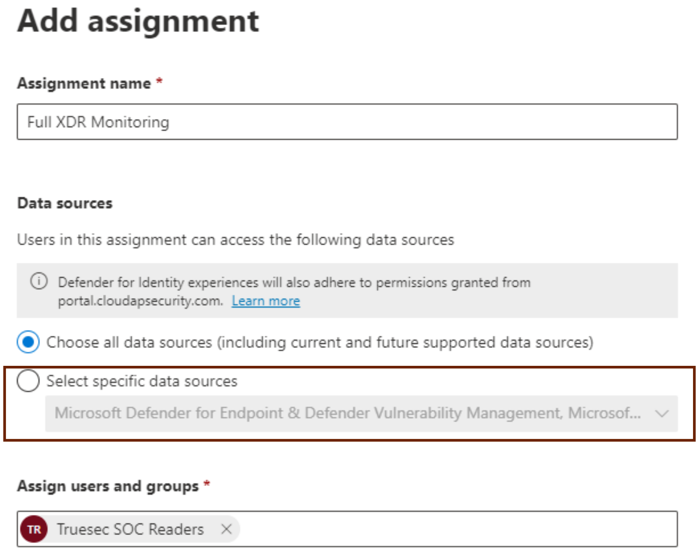
Additional data sources

Secure Score
Enabling this setting will stream additional 'non-workload' sources for Secure Score. Learn more about data sources in Secure Score.
Active

Go to Permissions and roles

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 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:



Add assignment

Assignment name *

Full XDR Monitoring

Data sources

Users in this assignment can access the following data sources

Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. Learn more

● Choose all data sources (including current and future supported data sources)

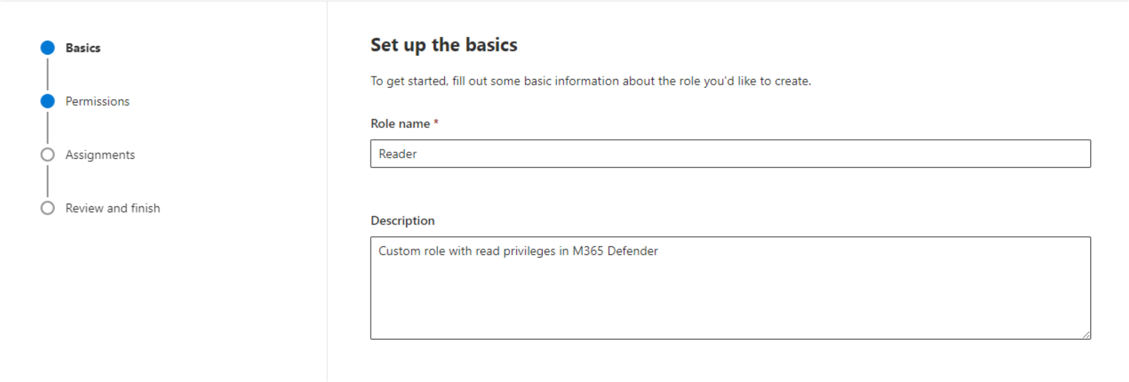
○ Select specific data sources

Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsof...

Assign users and groups *

TR Truesec SOC Readers

- 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.



Set up the basics

To get started, fill out some basic information about the role you'd like to create.

Role name *

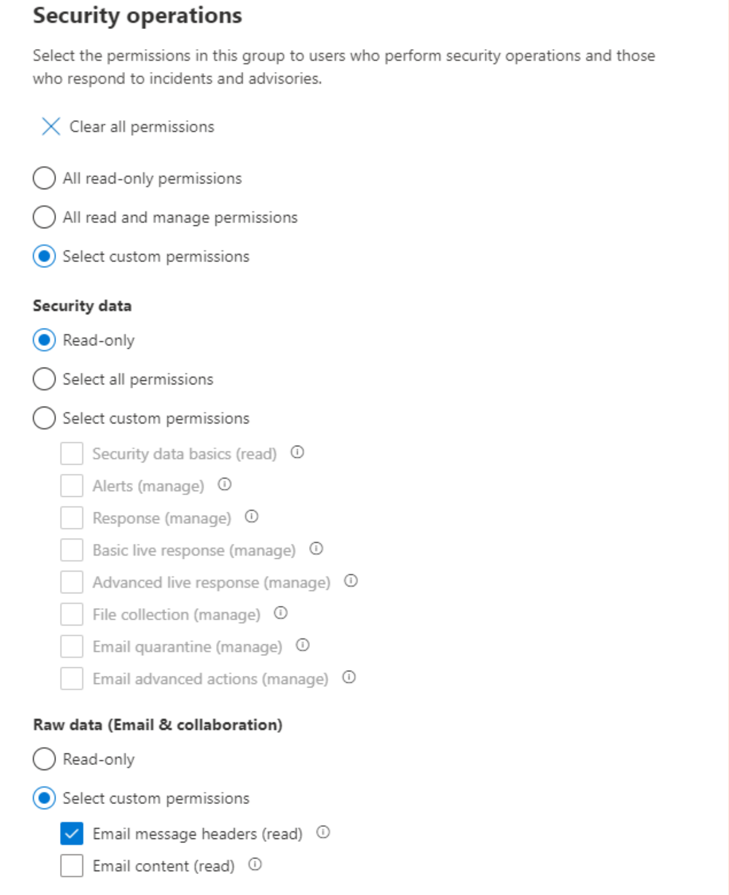
Reader

Description

Custom role with read privileges in M365 Defender

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

Role
Readers



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

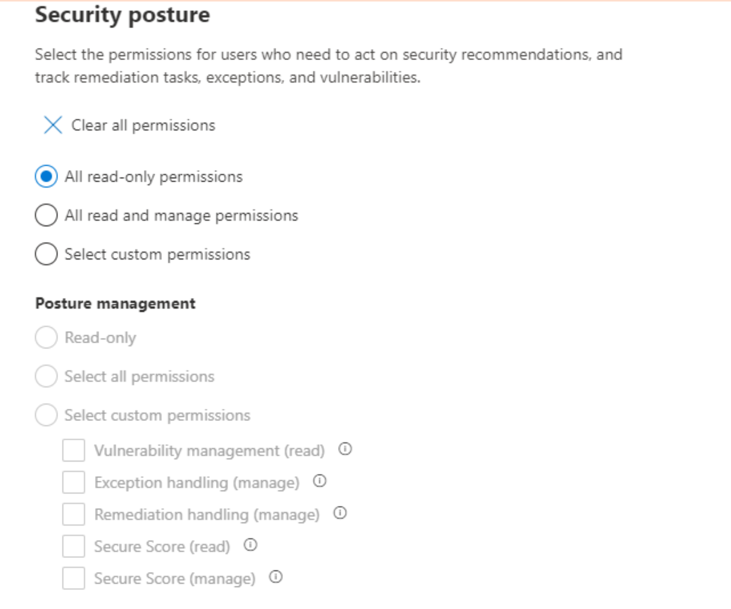
● Read-only
○ Select all permissions
○ Select custom permissions

- ☐ 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.

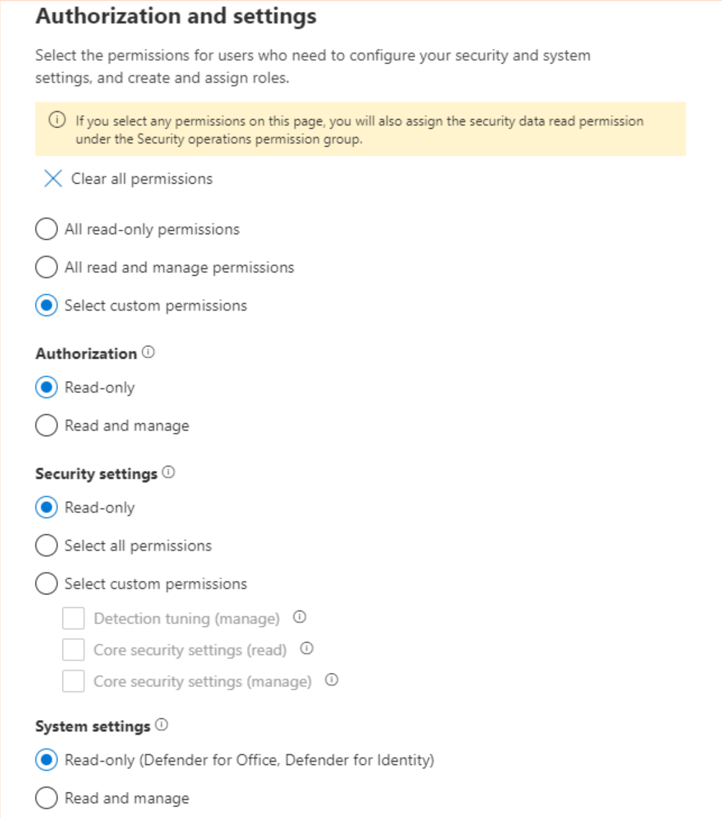
✕ Clear all permissions

● 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)



Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

ⓘ If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

✕ Clear all permissions

○ All read-only permissions

○ All read and manage permissions

● Select custom permissions

Authorization ⓘ

● Read-only

○ Read and manage

Security settings ⓘ

● Read-only

○ Select all permissions

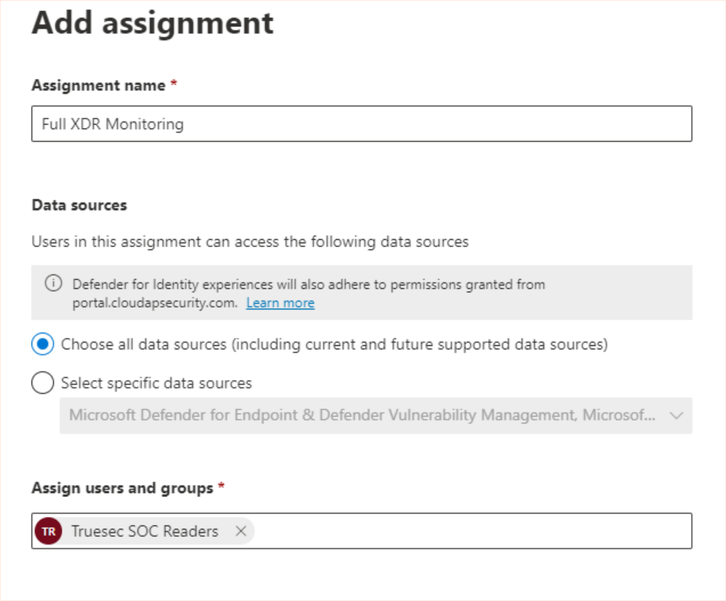
○ Select custom permissions

- □ Detection tuning (manage) ⓘ
- □ Core security settings (read) ⓘ
- □ Core security settings (manage) ⓘ

System settings ⓘ

● Read-only (Defender for Office, Defender for Identity)

○ Read and manage



Add assignment

Assignment name *

Full XDR Monitoring

Data sources

Users in this assignment can access the following data sources

ⓘ Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. Learn more

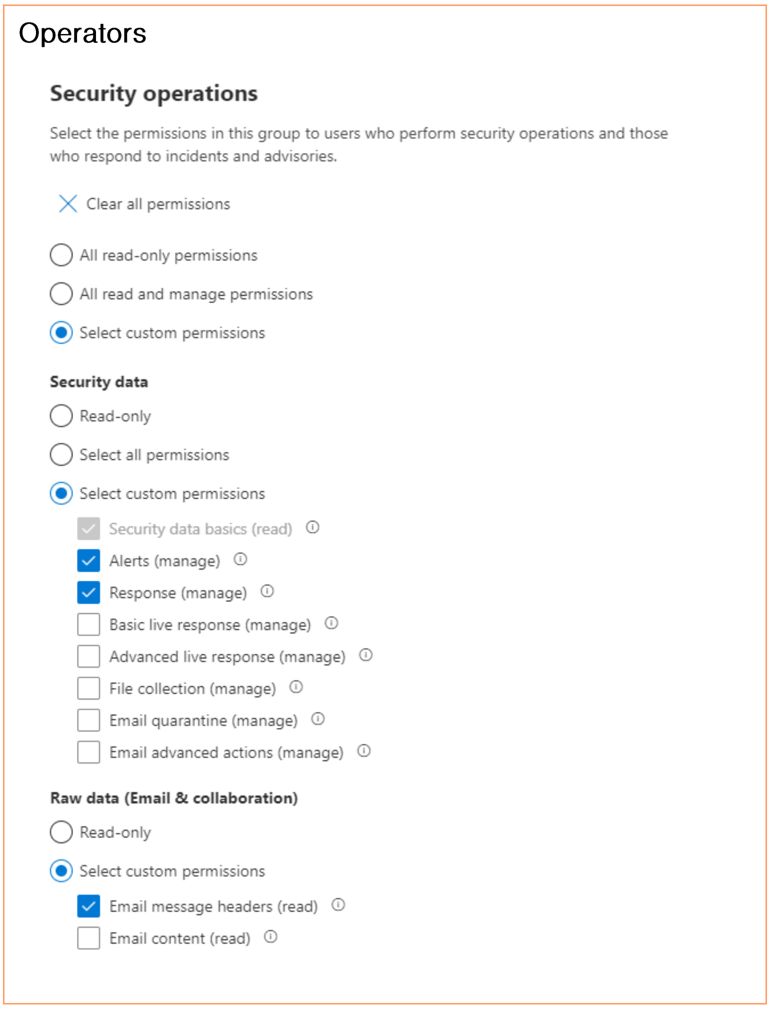
● Choose all data sources (including current and future supported data sources)

○ Select specific data sources

Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsof...

Assign users and groups *

TR Truesec SOC Readers ✕



Operators

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

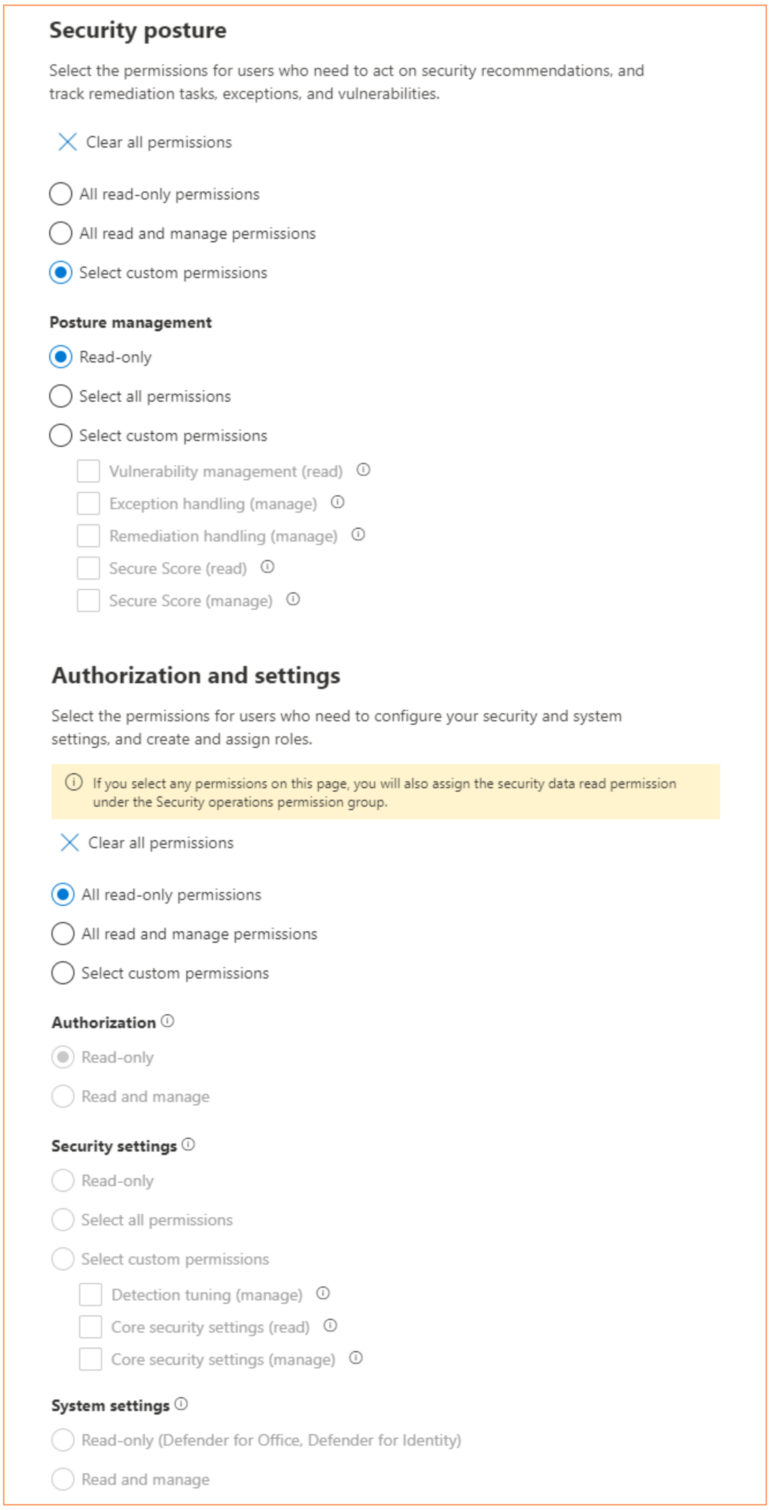
- ☑ Security data basics (read) ⓘ
- ☑ Alerts (manage) ⓘ
- ☑ Response (manage) ⓘ
- □ Basic live response (manage) ⓘ
- □ Advanced live response (manage) ⓘ
- □ File collection (manage) ⓘ
- □ Email quarantine (manage) ⓘ
- □ Email advanced actions (manage) ⓘ

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) ⓘ

Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

ⓘ If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

✕ Clear all permissions

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

Authorization ⓘ

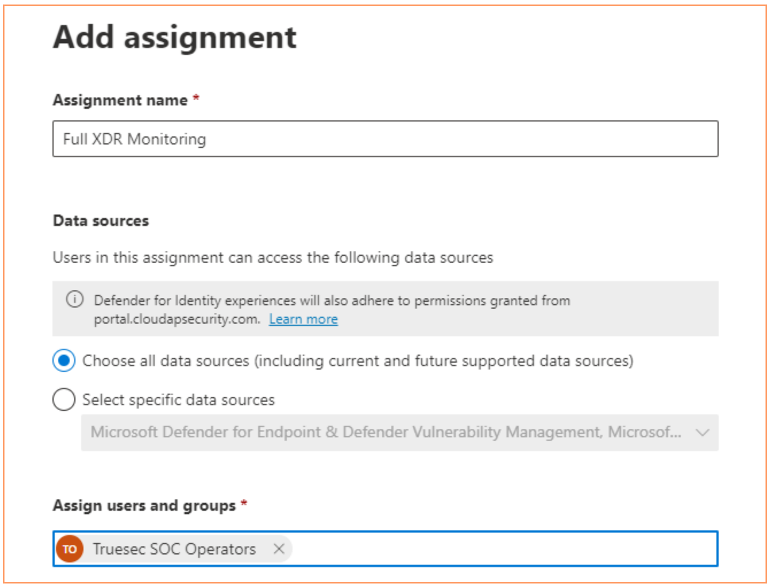
● Read-only
○ Read and manage

Security settings ⓘ

○ Read-only
○ Select all permissions
○ Select custom permissions
- □ Detection tuning (manage) ⓘ
- □ Core security settings (read) ⓘ
- □ Core security settings (manage) ⓘ

System settings ⓘ

○ Read-only (Defender for Office, Defender for Identity)
○ Read and manage



Add assignment

Assignment name *

Full XDR Monitoring

Data sources

Users in this assignment can access the following data sources

ⓘ Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. Learn more

● Choose all data sources (including current and future supported data sources)

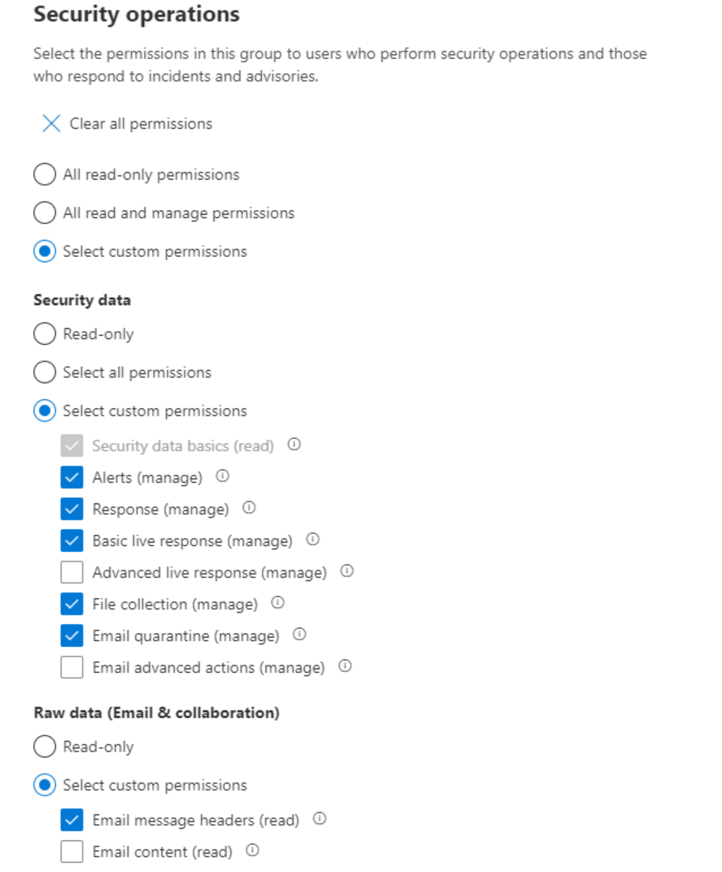
○ Select specific data sources

Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsof...

Assign users and groups *

TO Truesec SOC Operators ✕

Privileged Operators



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

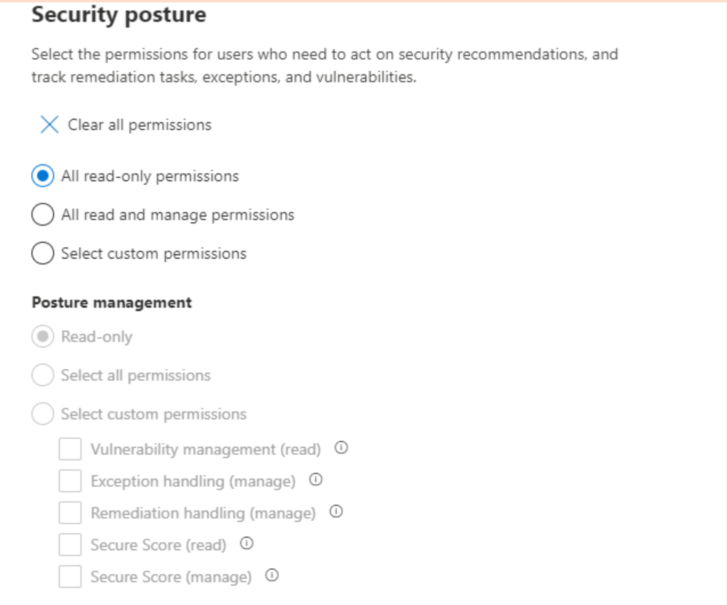
○ Read-only
○ Select all permissions
● Select custom permissions

- ☑ 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.

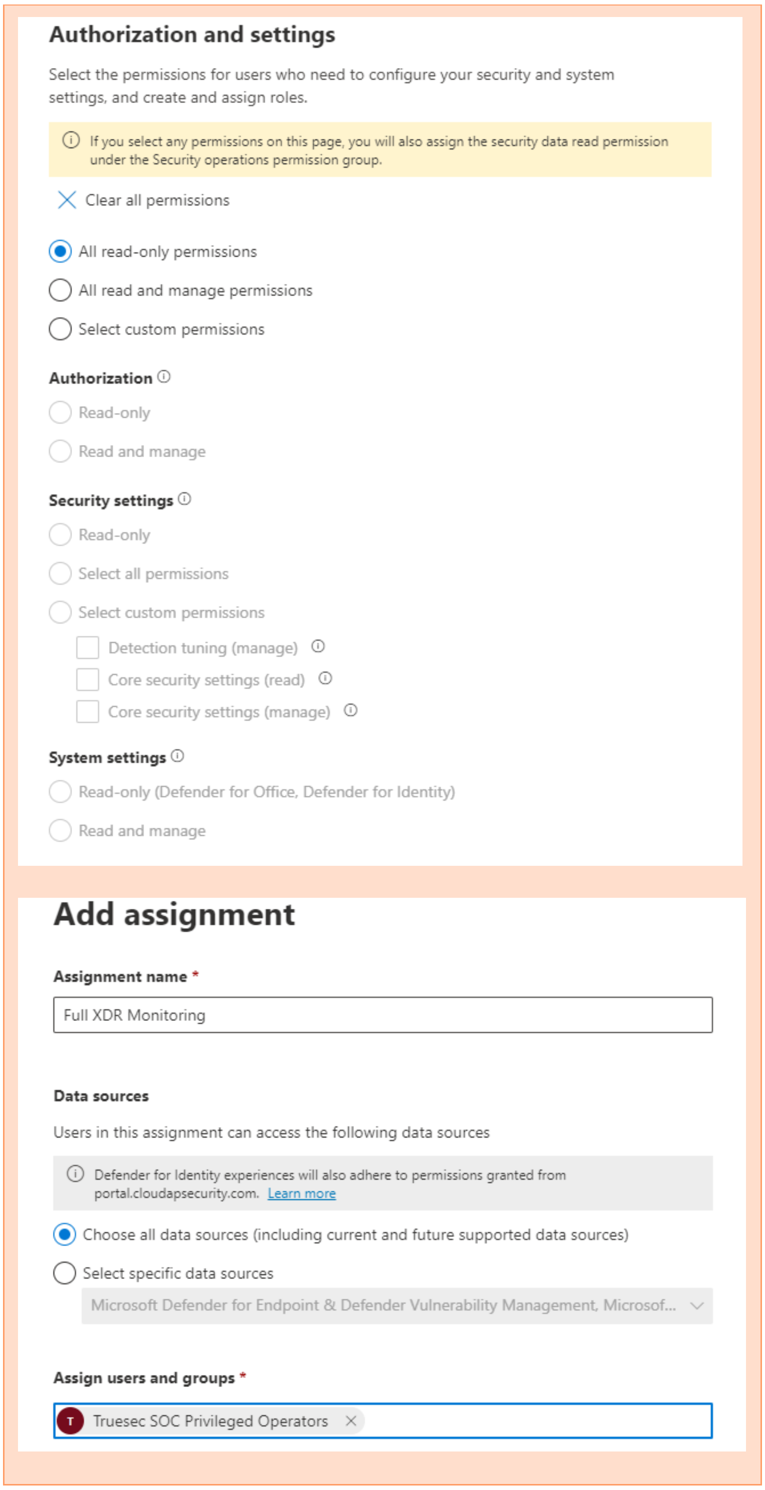
✕ Clear all permissions

● 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) ⓘ



Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

ⓘ If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

✕ Clear all permissions

● All read-only permissions

○ All read and manage permissions

○ Select custom permissions

Authorization ⓘ

○ Read-only

○ Read and manage

Security settings ⓘ

○ Read-only

○ Select all permissions

○ Select custom permissions

- □ Detection tuning (manage) ⓘ
- □ Core security settings (read) ⓘ
- □ Core security settings (manage) ⓘ

System settings ⓘ

○ Read-only (Defender for Office, Defender for Identity)

○ Read and manage

Add assignment

Assignment name *

Full XDR Monitoring

Data sources

Users in this assignment can access the following data sources

ⓘ Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. Learn more

● Choose all data sources (including current and future supported data sources)

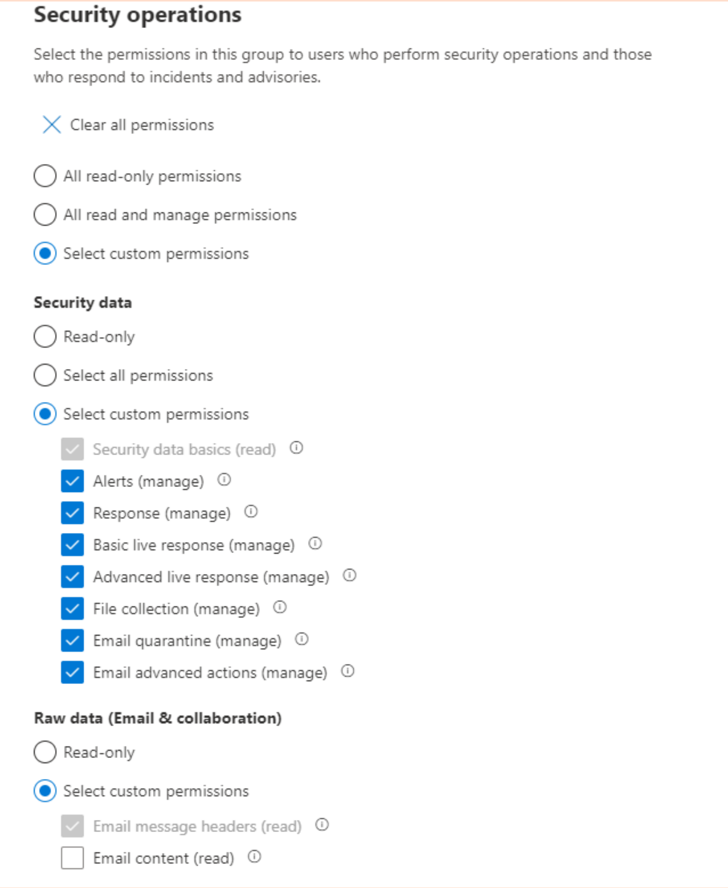
○ Select specific data sources

Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsof...

Assign users and groups *

T Truesec SOC Privileged Operators ✕

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

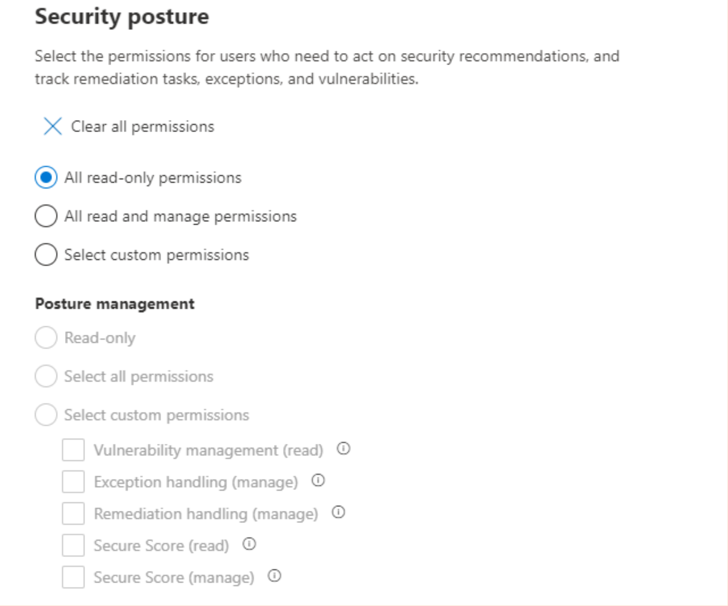
○ Read-only
○ Select all permissions
● Select custom permissions

- ☑ 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.

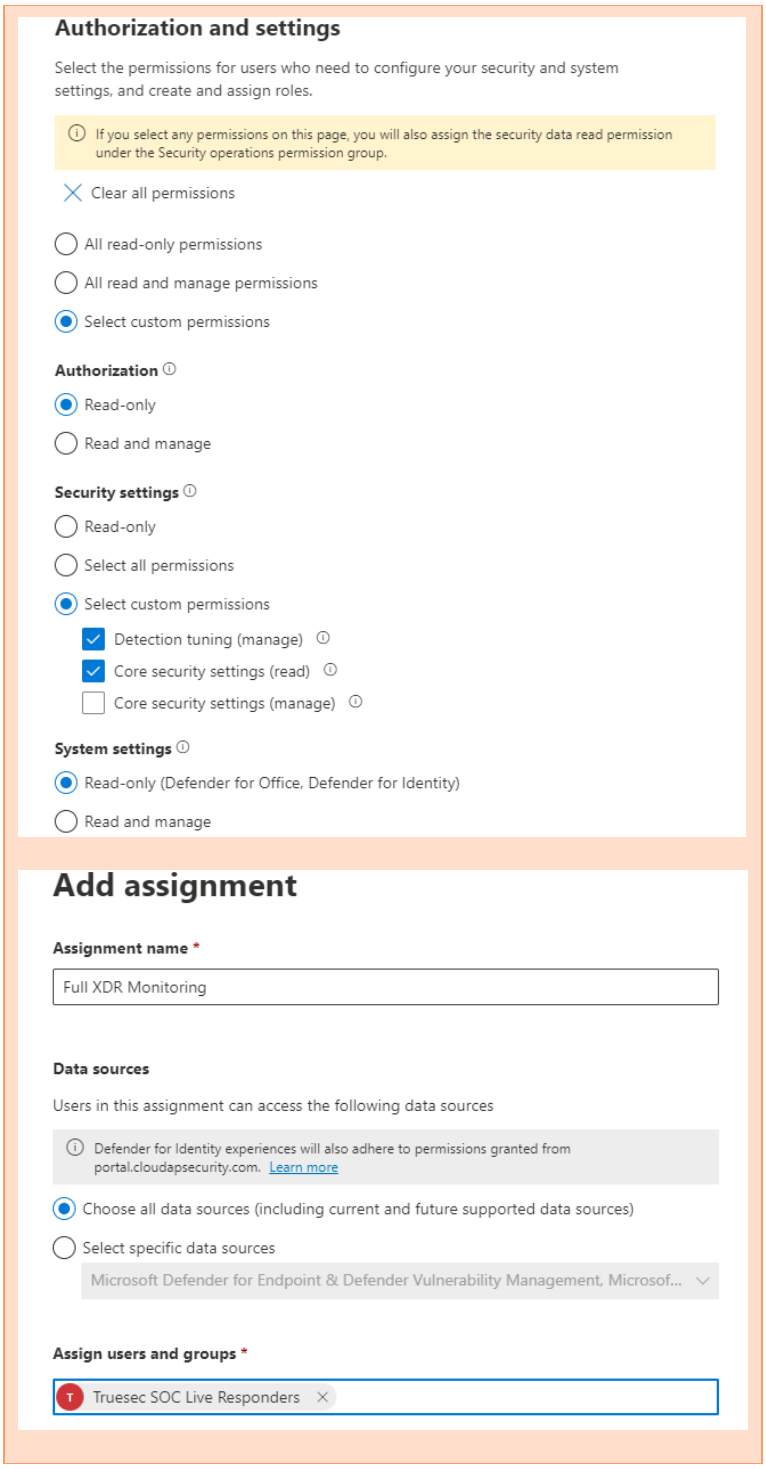
✕ Clear all permissions

● 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) ⓘ



Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

ⓘ If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

✕ Clear all permissions

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

Authorization ⓘ
● Read-only
○ Read and manage

Security settings ⓘ
○ Read-only
○ Select all permissions
● Select custom permissions
☑ Detection tuning (manage) ⓘ
☑ Core security settings (read) ⓘ
□ Core security settings (manage) ⓘ

System settings ⓘ
● Read-only (Defender for Office, Defender for Identity)
○ Read and manage

Add assignment

Assignment name *

Full XDR Monitoring

Data sources

Users in this assignment can access the following data sources

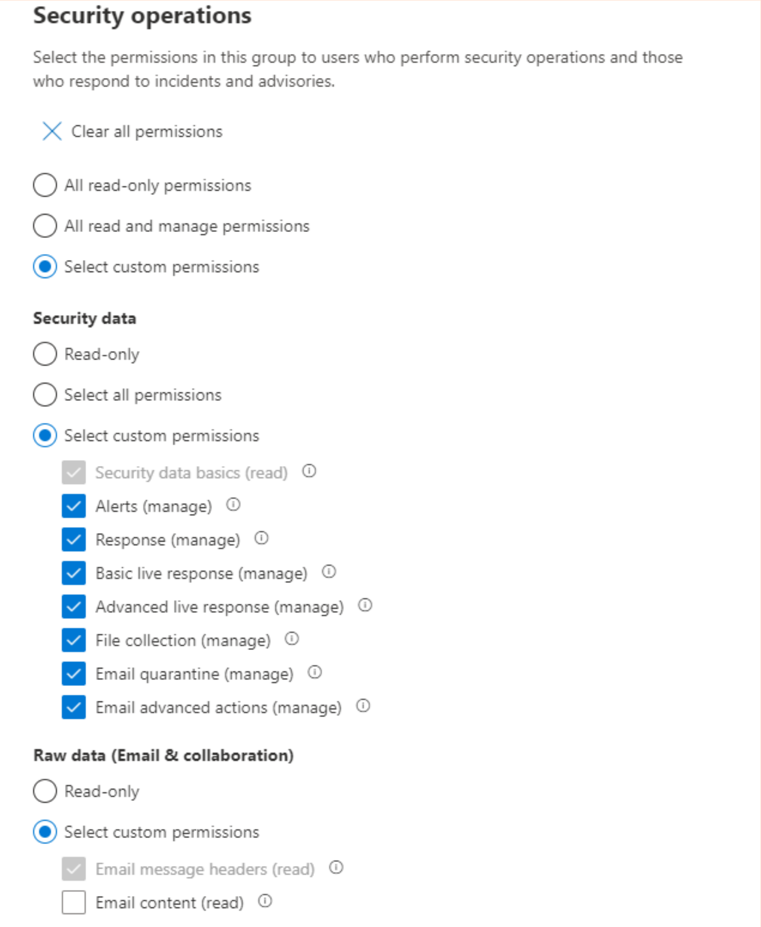
ⓘ Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. Learn more

● Choose all data sources (including current and future supported data sources)
○ Select specific data sources
Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsof...

Assign users and groups *

T Truesec SOC Live Responders ✕

Admins



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

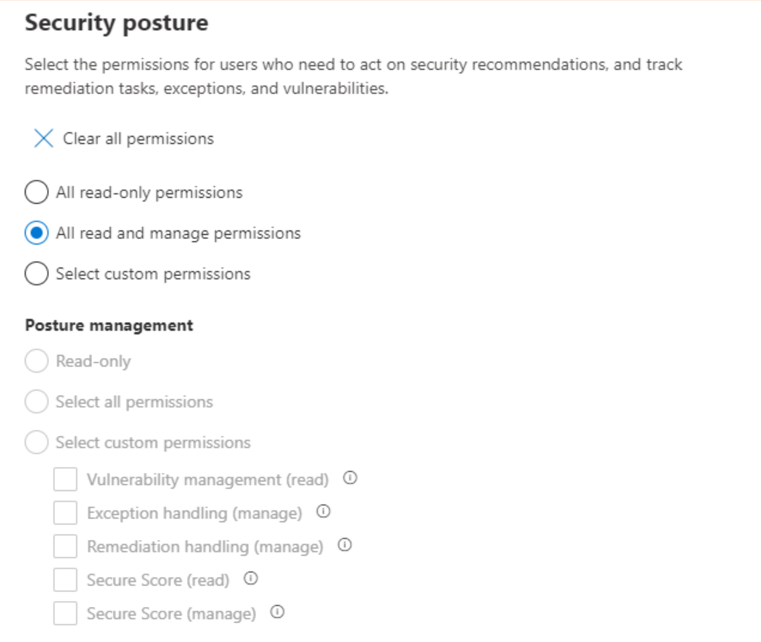
○ Read-only
○ Select all permissions
● Select custom permissions

- ☑ 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.

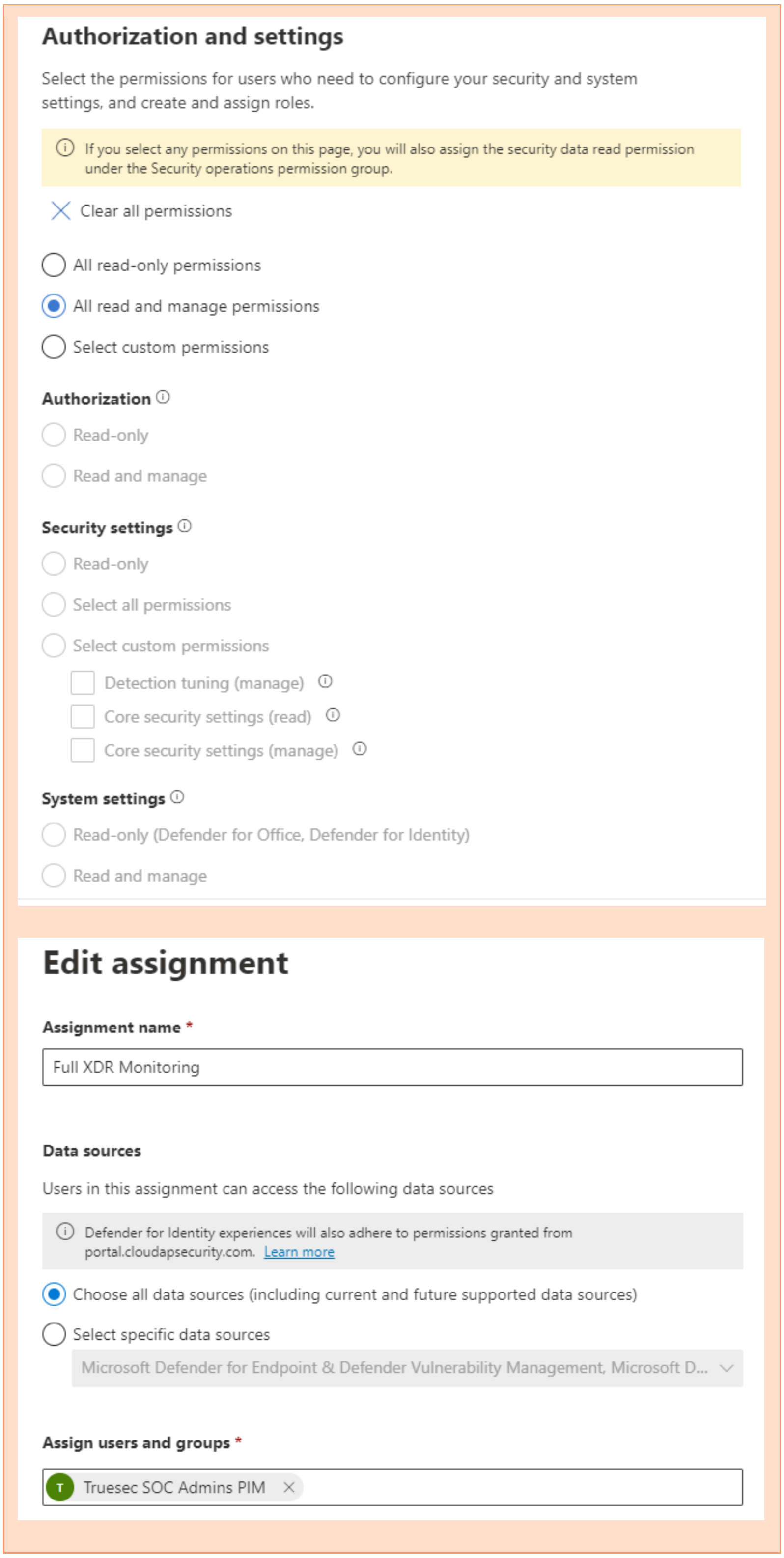
✕ Clear all permissions

○ 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)



Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

ⓘ If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

✕ Clear all permissions

○ All read-only permissions

● All read and manage permissions

○ Select custom permissions

Authorization ⓘ

○ Read-only

○ Read and manage

Security settings ⓘ

○ Read-only

○ Select all permissions

○ Select custom permissions

- □ Detection tuning (manage) ⓘ
- □ Core security settings (read) ⓘ
- □ Core security settings (manage) ⓘ

System settings ⓘ

○ Read-only (Defender for Office, Defender for Identity)

○ Read and manage

Edit assignment

Assignment name *

Full XDR Monitoring

Data sources

Users in this assignment can access the following data sources

ⓘ Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. Learn more

● Choose all data sources (including current and future supported data sources)

○ Select specific data sources

Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D...

Assign users and groups *

T Truesec SOC Admins PIM ✕

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