

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.

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 Defender XDR.

Workloads

Endpoints & Vulnerability Management

☒ Active

Email & Collaboration

Enforcing Exchange Online permissions will impact the Email & Collab capabilities that were previously configured in the Exchange admin center. Exchange admin center.

☒ Active - Defender for Office 365

☒ Active - Exchange Online permissions ⓘ

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 + 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:

Add assignment

Assignment name *

Data sources

Users in this assignment can access the following data sources

① 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 *

- 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.

Basics

- Permissions
- Assignments
- Review and finish

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.

① 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 ①

- ☒ Read-only
- ☐ Read and manage

Security settings ①

- ☒ Read-only
- ☐ Select all permissions
- ☐ Select custom permissions
- ☐ Detection tuning (manage) ①
- ☐ Core security settings (read) ①
- ☐ Core security settings (manage) ①

System settings ①

- ☒ 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

① 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 *

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, Microsoft D... ▾


Assign users and groups *

TO Truesec SOC Operators X

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, Microsoft D... 

Assign users and groups *

 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, Microsoft D... 

Assign users and groups *

 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


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, Microsoft D... 

Assign users and groups *

 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

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.

+ Connect an app ▾

App ▾	Status ▾
 Microsoft 365 Collaboration	✓ Connected
 Microsoft Azure Cloud computing platform	✓ Connected

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

- Select Office 365 components
- Great, Office 365 is connected

Select Office 365 components

Connect as Microsoft Azure administrator to gain full visibility and control.

ⓘ To connect this app, provide your access credentials. We secure your data as described in the [privacy statement](#) | [Terms](#)

- ☒ Azure AD Users and groups ⓘ
- ☒ Azure AD Management events ⓘ
- ☒ Azure AD Sign-in events ⓘ
- ☒ Azure AD Apps ⓘ
- ☒ Office 365 activities ⓘ
- ☒ Office 365 files ⓘ

Enable file monitoring before enabling Office 365 files.

3.5. Configure Entra ID Protection alert service

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

Microsoft Defender XDR

General	
Account	
Email notifications	
Alert service settings	Alert service settings
Permissions and roles	You can turn off alerts from the listed services. When you turn them off, alerts from the service no longer appear within incidents or in the alerts queue.
Streaming API	Microsoft Entra ID Protection
Multi-tenant content source	Choose which identity protection alerts will appear in the alerts and incidents pages.
	<input type="radio"/> High-impact alerts only (Default) Show only alerts about known malicious or highly suspicious activities that might require attention.
	<input checked="" type="radio"/> All alerts Show all alerts, including activity that might not constitute unwanted or malicious activity.