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.
- It is important to know that enabling of any of the Workloads (3.1) will deactivate RBAC and permissions created in MDE.
- This example will be for the onboarding of 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 *
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. <u>Learn more</u>
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 *
Search for any user or security group in your organization



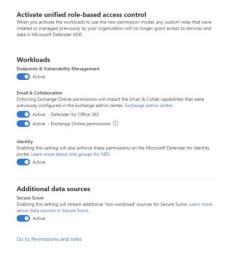


3. Tasks

Five roles must be created in the portal. These roles must be assigned to five security groups.

3.1. Activate RBAC for workloads

- Browse to https://security.microsoft.com/
- Click "Settings" → "Microsoft Defender XDR" → "Permissions and roles"
- Use the slider as listed below to activate workloads.



3.2. Create custom roles

- Click the blue text "Go to Permissions and roles" at the bottom of the page for Workloads.
- Create five custom roles with the level of access that correlates to the agreement between customer and Truesec.
- Click "Create custom role" and create the roles, one by one:

Readers

Operators

Privileged Operators

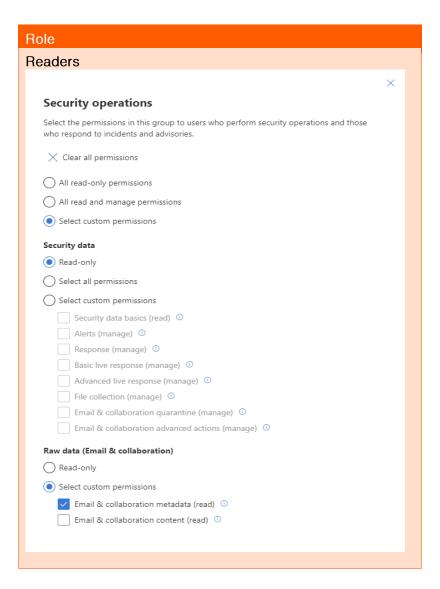
Live Responders

Admins

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

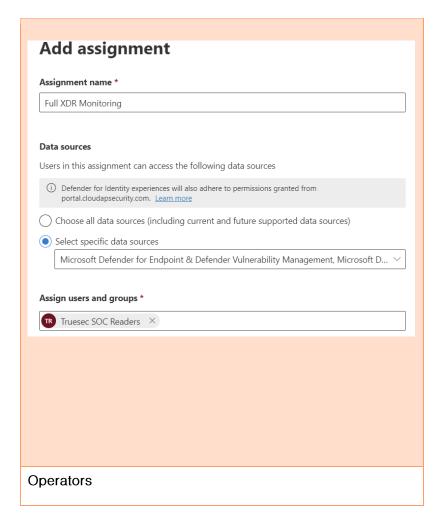
3







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) ①	
Exception handling (manage) ①	
Remediation handling (manage) ①	
Secure Score (read) ①	
Secure Score (manage) 0	
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 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	



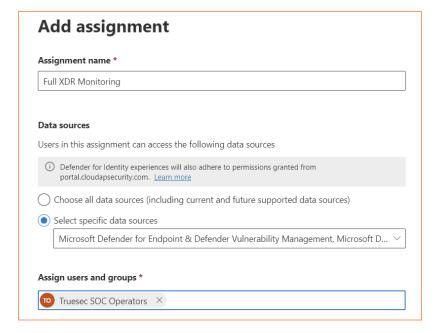
Author: Adam Helgesson Date: 2024-04-09 Classification: Internal Version: 1.3

Sweden

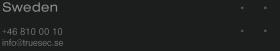
6

Sitti	×
Security operations	
Select the permissions in this group to users who perform security operations and thos who respond to incidents and advisories.	e
X 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) ①	
✓ Alerts (manage) ①	
Response (manage) ①	
Basic live response (manage) ①	
Advanced live response (manage) ①	
File collection (manage) ①	
Email & collaboration quarantine (manage) ①	
Email & collaboration advanced actions (manage) ①	
Raw data (Email & collaboration)	
Read-only	
Select custom permissions	
✓ Email & collaboration metadata (read) ①	
Email & collaboration content (read) ①	

Security posture	
Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities.	
X 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) ①	
Exception handling (manage) ①	
Remediation handling (manage) ①	
Secure Score (read) ①	
Secure Score (manage) ①	
If you select any permissions on this page, you will also assign the security data read permission	
① If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.	
under the Security operations permission group.	
under the Security operations permission group. X Clear all permissions	
under the Security operations permission group. X Clear all permissions All read-only permissions	
under the Security operations permission group. Clear all permissions All read-only permissions All read and manage permissions	
under the Security operations permission group. Clear all permissions All read-only permissions All read and manage permissions Select custom permissions	
under the Security operations permission group. Clear all permissions All read-only permissions All read and manage permissions Select custom permissions Authorization ①	
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	
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	
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	
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	
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	
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	
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 Detection tuning (manage) ①	
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 Detection tuning (manage) ① Core security settings (read) ①	
under the Security operations permission group. Clear all permissions All read-only 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 (manage) ①	



Author: Adam Helgesson Classification: Internal Date: 2024-04-09 Version: 1.3



8

9

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 Security data Read-only Select custom permissions Select dustom permissions Security data basics (read) Read-only Select (manage) Response (manage) Basic live response (manage) Final & collaboration quarantine (manage) Email & collaboration advanced actions (manage) Email & collaboration advanced actions (manage) Read-only Select custom permissions Email & collaboration operations Email & collaboration operations Cermical & collaboration operations All read-only Select custom permissions All read-only permissions All read-only permissions Select custom permissions Select custom permissions All read-only permissions Select custom permissions	Privileged Operators	
Select the permissions in this group to users who perform security operations and those who respond to incidents and advisories. X Clear all permissions All read-only permissions Select custom permissions Security data Read-only Select all permissions Select dustom permissions Security data basics (read) Alerts (manage) Alerts (manage) Basic live response (manage) File collection (manage) File collection (manage) Email & collaboration quarantine (manage) Email & collaboration advanced actions (manage) Email & collaboration advanced actions (manage) Email & collaboration on the collaboration (manage) Email & collaboration on the collaboration (manage) Security posture Select custom permissions Email & collaboration metadata (read) Email & collaboration content (read) Security posture Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities. X Clear all permissions All read-only permissions Select custom permissions Posture management Read-only Select all permissions Select custom permissions Select custom permissions Select custom permissions Osture management Read-only Read-only Select custom permissions	Security operations	×
All read and manage permissions All read and manage permissions Security data Read-only Select custom permissions Security data Read-only Select all permissions Security data basics (read) ① Alerts (manage) ② Response (manage) ② Activanced live response (manage) ② Activanced live response (manage) ② File collection (manage) ② Email & collaboration quarantine (manage) ③ Email & collaboration advanced actions (manage) ③ Email & collaboration advanced actions (manage) ③ Email & collaboration metadata (read) ③ Email & collaboration metadata (read) ③ Email & collaboration content (read) ③ Security posture Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities. X Clear all permissions All read-only permissions All read and manage permissions Select custom permissions Posture management Read-only Select all permissions Vulnerability management (read) ② Exception handling (manage) ③ Remediation handling (manage) ③ Remediation handling (manage) ③ Remediation handling (manage) ③	Select the permissions in this group to users who perform security operations and those	
All read and manage permissions Select custom permissions Security data Read-only Select all permissions Security data basics (read) Active (manage) Active (manage) Advanced live response (manage) Advanced live response (manage) Email & collaboration quarantine (manage) Email & collaboration advanced actions (manage) Email & collaboration content (read) Select custom permissions I email & collaboration content (read) Email & collaboration 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 custom permissions Select custom permissions Posture management Read-only Select custom permissions	X Clear all permissions	
● Select custom permissions Security data Read-only Select custom permissions ● Select custom permissions ● Select custom permissions ● Response (manage) ① Response (manage) ② Passic live response (manage) ② File collection (manage) ② Email & collaboration quarantine (manage) ③ Email & collaboration advanced actions (manage) ③ Email & collaboration advanced actions (manage) ③ Raw data (Email & collaboration) Read-only ● Select custom permissions ● Email & collaboration metadata (read) ③ Email & collaboration content (read) ③ 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 Vulnerability management (read) ④ Exception handling (manage) ④ Remediation handling (manage) ④ Remediation handling (manage) ④ Remediation handling (manage) ④ Secure Score (read) ④		
Read-only Select all permissions Select custom permissions Security data basics (read) ① Alerts (manage) ② Response (manage) ② Basic live response (manage) ① Advanced live response (manage) ② File collection (manage) ② Finail & collaboration quarantine (manage) ③ Email & collaboration advanced actions (manage) ③ Email & collaboration advanced actions (manage) ③ Email & collaboration metadata (read) ③ Email & collaboration metadata (read) ③ Email & collaboration content (read) ③ Email & collaboration content (read) ③ All read and manage permissions All read and manage permissions Select custom permissions All read and manage permissions Select custom permissions Select all permissions Select custom permissions		
Select all permissions Security data basics (read) ① Alerts (manage) ① Response (manage) ① Alerts (manage) ① Basic live response (manage) ① File collection (manage) ② File collection (manage) ② Finali & collaboration quarantine (manage) ① Email & collaboration advanced actions (manage) ① Raw data (Email & collaboration) Read-only Select custom permissions Email & collaboration metadata (read) ① Email & collaboration content (read) ② Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities. Clear all permissions All read and manage permissions All read and manage permissions Select custom permissions Posture management Read-only Select all permissions Vulnerability management (read) ② Exception handling (manage) ① Remediation handling (manage) ① Remediation handling (manage) ① Remediation handling (manage) ① Remediation handling (manage) ① Secure Score (read) ②		
Security data basics (read) ○ Alerts (manage) ○ Response (manage) ○ Basic live response (manage) ○ File collection (manage) ○ Email & collaboration quarantine (manage) ○ Email & collaboration advanced actions (manage) ○ Raw data (Email & collaboration) Read-only Select custom permissions Email & collaboration metadata (read) ○ Email & collaboration content (read) ○ Email & collaboration content (read) ○ 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 tall permissions Vulnerability management (read) ○ Exception handling (manage) ○ Remediation handling (manage) ○		
Response (manage) ① Basic live response (manage) ① Advanced live response (manage) ① File collection (manage) ① Email & collaboration quarantine (manage) ① Email & collaboration advanced actions (manage) ① Email & collaboration advanced actions (manage) ① Raw data (Email & collaboration) Read-only Select custom permissions Email & collaboration metadata (read) ① Email & collaboration content (read) ① Email & collaboration content (read) ① 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 Vulnerability management (read) ① Exception handling (manage) ① Remediation handling (manage) ① Remediation handling (manage) ① Remediation handling (manage) ①		
■ Basic live response (manage) □ Advanced live response (manage) □ File collection (manage) □ Email & collaboration quarantine (manage) □ Email & collaboration advanced actions (manage) □ Raw data (Email & collaboration) Read-only Select custom permissions Email & collaboration metadata (read) □ Email & collaboration content (read) □ Email & collaboration 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 Select all permissions Posture management Read-only Select all permissions Select custom permissions Vulnerability management (read) □ Exception handling (manage) □ Remediation handling (manage) □ Remediation handling (manage) □ Remediation handling (manage) □	✓ Alerts (manage) ①	
File collection (manage) Email & collaboration quarantine (manage) Email & collaboration advanced actions (manage) Raw data (Email & collaboration) Read-only Select custom permissions Email & collaboration metadata (read) Email & collaboration content (read) Email & collaboration content (read) Email & collaboration 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) Remediation handling (manage) Remediation handling (manage) Secure Score (read) Secure Score (read)	Basic live response (manage) ①	
Email & collaboration advanced actions (manage) Raw data (Email & collaboration) Read-only Select custom permissions Email & collaboration metadata (read) Email & collaboration content (read) Email & collaboration 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	File collection (manage) ①	
Read-only Select custom permissions Email & collaboration metadata (read) Email & collaboration content (read) Email & collaboration 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 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 (read)		
Email & collaboration metadata (read) Email & collaboration content (read) Email & collaboration 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 Select custom permissions Posture management Read-only Select all permissions Vulnerability management (read) Exception handling (manage) Remediation handling (manage) Secure Score (read) Secure Score		
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 and manage permissions Select custom permissions Posture management Read-only Select all permissions Vulnerability management (read) Exception handling (manage) Remediation handling (manage) Secure Score (read)		
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 Select custom permissions Posture management Read-only Select all permissions Vulnerability management (read) Exception handling (manage) Remediation handling (manage) Secure Score (read)		
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 Select custom permissions Posture management Read-only Select all permissions Vulnerability management (read) Exception handling (manage) Remediation handling (manage) Secure Score (read)	Cognity posture	
 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) ○ 	Select the permissions for users who need to act on security recommendations, and	
 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) ① Exception handling (manage) ① Remediation handling (manage) ① Secure Score (read) ① 		
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 (rea		
Posture management Read-only Select all permissions Select custom permissions Vulnerability management (read) Exception handling (manage) Remediation handling (manage) Secure Score (read) Secure Score (read)	All read and manage permissions	
 ■ Read-only Select all permissions Select custom permissions Uulnerability management (read) □ Exception handling (manage) □ Remediation handling (manage) □ Secure Score (read) 		
Select custom permissions Vulnerability management (read) ① Exception handling (manage) ① Remediation handling (manage) ① Secure Score (read) ①		
Vulnerability management (read) ① Exception handling (manage) ① Remediation handling (manage) ① Secure Score (read) ①	Select all permissions	
Exception handling (manage) ① Remediation handling (manage) ① Secure Score (read) ①		
Remediation handling (manage) ① Secure Score (read) ①		
Secure Score (read) ①		

All read and manage permissions Select custom permissions Authorization ① Read-only Read and manage Security settings ① Read-only Select all permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) ① Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *	-	uthorization and settings
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		
under the Security operations permission group. Clear all 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 all permissions Select custom permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) ② System settings ② Read-only (Defender for Office, Defender for Identity) Read and manage		
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 Read-only (Defender for Office, Defender for Identity) Read and manage	(
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 Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *	>	Clear all 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 Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *	•	All read-only 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 Read-only (Defender for Office, Defender for Identity) Read and manage) All read and manage permissions
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 Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *		Select custom permissions
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 Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *	٩ı	ithorization ①
Read-only Select all permissions Select custom permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) ① Read-only (Defender for Office, Defender for Identity) Read and manage		Read-only
Read-only Select all permissions Select custom permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) ① Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *		Read and manage
Select custom 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 signment name *	ie	curity settings ①
Select custom permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) ① Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *) Read-only
Detection tuning (manage) Core security settings (read) Core security settings (manage) System settings Read-only (Defender for Office, Defender for Identity) Read and manage		Select all permissions
Core security settings (read) Core security settings (manage) System settings Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *		Select custom permissions
Core security settings (manage) System settings Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *		Detection tuning (manage) ①
System settings ① Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment ssignment name *		Core security settings (read) ①
Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment signment name *		Core security settings (manage) ①
Read and manage Add assignment signment name *	у	stem settings ①
add assignment		Read-only (Defender for Office, Defender for Identity)
signment name *		Read and manage
signment name *		
signment name *	1	dd assignment
		, and the second
ull XDR Monitoring	si	gnment name *
	u	II XDR Monitoring
	t	a sources
ata sources	eı	rs in this assignment can access the following data sources
ata sources ers in this assignment can access the following data sources		
	ì	portal.cloudapsecurity.com. <u>Learn more</u>
ers in this assignment can access the following data sources Defender for Identity experiences will also adhere to permissions granted from		
Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. <u>Learn more</u> Learn more)	Choose all data sources (including current and future supported 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))	Choose all data sources (including current and future supported data sources) Select specific 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		Choose all data sources (including current and future supported data sources) Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D
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		Choose all data sources (including current and future supported data sources) Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D ign users and groups *

11

Live Responders	
Security operations	×
Select the permissions in this group to users who perform security operations and those who respond to incidents and advisories.	
X 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) ①	
✓ Alerts (manage) ①	
Response (manage) ①	
Basic live response (manage) ①	
✓ Advanced live response (manage) ①	
File collection (manage) ①	
Email & collaboration quarantine (manage) ①	
Email & collaboration advanced actions (manage) ①	
Raw data (Email & collaboration)	
Read-only	
Select custom permissions	
Email & collaboration metadata (read) ①	
Email & collaboration content (read)	
Security posture	
Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities.	
X 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) ①	
Exception handling (manage) ①	
Remediation handling (manage) ①	
Secure Score (read) ①	
Secure Score (manage) ①	

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 ③ All read-only permissions ④ All read and manage permissions ④ Select custom permissions Authorization ③ ⑥ Read-only ⑥ Read and manage Security settings ③ ⑥ Read-only ⑤ Select all permissions ④ Select custom permissions ⑤ Select custom permissions ⑤ Detection tuning (manage) ① ▼ Core security settings (read) ① □ Core security settings (manage) ① System settings ① ⑥ Read-only (Defender for Office, Defender for Identity) ○ Read and manage Add assignment sssignment name *	Select :	the permissions for users who need to configure your security and system
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 Add assignment name *		
All read and manage permissions All read and manage permissions Authorization ① Read-only Read and manage Security settings ① Read-only Select all permissions Select custom permissions Detection tuning (manage) ② Core security settings (read) ① Core security settings (manage) ① System settings ① Read-only (Defender for Office, Defender for Identity) Read and manage		
All read and manage permissions Select custom permissions Authorization ○ Read-only Read and manage Security settings ① Read-only Select all permissions Select custom permissions Detection tuning (manage) ○ 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 Add assignment name *	× c	lear all 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 	O All	read-only 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 *	O All	read and manage permissions
 Read-only Read and manage Security settings ① Read-only Select all permissions Select custom permissions ✓ Detection tuning (manage) ① ✓ Core security settings (read) ② ☐ Core security settings (manage) ① System settings ② Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment Assignment name *	Se	lect custom permissions
Read and manage Security settings ① Read-only Select all permissions Select custom permissions 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 *	Autho	rization ①
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 *	Re	ad-only
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 *	○ Re	ad and manage
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 *	Securi	ty settings ①
● 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 *	○ Re	ad-only
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 *	○ Se	lect all permissions
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 *	Se	lect custom permissions
Core security settings (manage) ① System settings ① Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment Assignment name *	~	
System settings ① Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment Assignment name *	~	
Read-only (Defender for Office, Defender for Identity) Read and manage Add assignment Assignment name *	_	,
Add assignment Assignment name *		•
Add assignment Assignment name *	_	
Assignment name *	O KE	au anu manage
Assignment name *	bbΔ	assignment
<u> </u>	10.0.	azzigi
	Assignm	ent name *
Full XDR Monitoring	Full XD	R Monitoring
	ata soı	ırces
Data sources	lsers in	this assignment can access the following data sources
Data sources Users in this assignment can access the following data sources		
		ose all data sources (including current and future supported data sources)
Users in this assignment can access the following data sources Defender for Identity experiences will also adhere to permissions granted from	Choo	
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)		ct specific 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	Sele	·

Admins		
Security operations		
Select the permissions in this group to users who perform security operations and those who respond to incidents and advisories.		
X 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) ①		
✓ Alerts (manage) ①		
Response (manage) ①		
✓ Basic live response (manage) ①		
✓ Advanced live response (manage) ①		
✓ File collection (manage) ①		
✓ Email quarantine (manage) ①		
Email advanced actions (manage) ①		
Raw data (Email & collaboration)		
Read-only		
Select custom permissions		
✓ Email message headers (read) ①		
Email content (read) ①		
Security posture		
Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities.		
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) ①		
Exception handling (manage) ①		
Remediation handling (manage) ①		
Secure Score (read) ①		
Secure Score (manage) ①		

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 ③ All read and manage permissions ⑤ Authorization ② Read-only Read-only Read-only Select all permissions ⑤ Select and manage Security settings ③ Read-only Select all permissions ⑤ Detection tuning (manage) ③ Core security settings (read) ⑥ Core security settings (manage) ⑥ System settings ③ 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) ⑥ Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups * ⑥ Truesec SOC Admins PIM ×	Autilo	rization and settings
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 ② Read-only Read and manage Security settings ③ Read-only Select all permissions Detection tuning (manage) ② Core security settings (manage) ③ Core security settings (manage) ③ System settings ③ 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 mote Choose all data sources (including current and future supported data sources) Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *		
under the Security operations permission group. Clear all permissions All read-only 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 *	settings, a	nd create and assign roles.
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 Detection tuning (manage) ① Core security settings (read) ② Core security settings (manage) ② 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-cloud-specurity.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 *		
All read and manage permissions Select custom permissions Authorization ① Read-only Read and manage Security settings ① Read-only Select all permissions Detection tuning (manage) ① Core security settings (read) ② Core security settings (manage) ① System settings ② 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 cloud specurity.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 *	× Clea	all 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) ② Core security settings (manage) ① System settings ③ 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 *	O All rea	ad-only permissions
Authorization © Read-only Read and manage Security settings © Read-only Select all 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 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 *	All rea	ad and manage permissions
Read-only Read and manage Security settings ① Read-only Select all permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) ① System settings ② 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 *	Select	custom permissions
Read and manage Security settings ① Read-only Select all 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) ⑤ Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *	Authoriza	ution ①
Security settings ① Read-only Select all permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) 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 ② 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 *	Read-	only
Read-only Select custom permissions Detection tuning (manage) ① Core security settings (read) ① Core security settings (manage) 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 *	Read	and manage
Select custom permissions Select custom permissions Detection tuning (manage) ① Core security settings (read) 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 Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *	Security s	eettings ①
Select custom permissions Detection tuning (manage) ① Core security settings (read) 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 *	Read-	only
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 *	Select	all permissions
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 *	Select	custom permissions
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) ③ Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *		etection tuning (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 ② Choose all data sources (including current and future supported data sources) ③ Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *		ore security settings (read) 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 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 *		ore security settings (manage) ①
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) ② Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *	System se	ettings ①
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 *	Read-	only (Defender for Office, Defender for Identity)
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) ⑤ Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *	Read	and manage
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 ② Choose all data sources (including current and future supported data sources) ③ Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *		
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 *		
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 *	Full XDR	Monitoring
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 *		
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 *	Data sou	rces
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 *	Users in th	nis assignment can access the following data sources
Select specific data sources Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *		
Microsoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D Assign users and groups *		
Assign users and groups *	porta	al.cloudapsecurity.com. <u>Learn more</u>
	O Choo	eal.cloudapsecurity.com. <u>Learn more</u> se all data sources (including current and future supported data sources)
Truscar SOC Admins PIM X	Choo	al.cloudapsecurity.com. Learn more se all data sources (including current and future supported data sources) specific data sources
	O Choo	al.cloudapsecurity.com. Learn more se all data sources (including current and future supported data sources) specific data sources osoft Defender for Endpoint & Defender Vulnerability Management, Microsoft D



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 (Optional, recommended)

3.3.2. Make sure the following feature is disabled

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