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

ⓘ 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 *

Search for any user or security group in your organization

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

1

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.
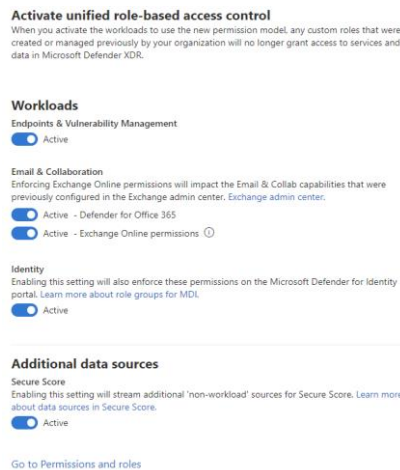
3.2. Create custom roles

- 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:

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

2

- **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

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 & 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) ⓘ

TRUESEC

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

Operators

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

5

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 & 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) ⓘ

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

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

7

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 ✕

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 & 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) ⓘ

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) ⓘ

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

9

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 *

🔴 T Truesec SOC Privileged Operators ✕

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

10

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 & 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) ⓘ

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) ⓘ

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

11

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 ✕

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

12

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) ⓘ

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

13

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 (Optional, recommended)

3.3.2. Make sure the following feature is disabled

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

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

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

+46 810 00 10
info@truesec.se

15