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

Four roles must be created in the portal. These roles and the default admin role must be assigned to five security groups according to this pattern:

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

3.1. Configure Roles

- Click “Settings” → “Endpoints” → “Roles”
- Click “Turn on roles” if applicable
- Assign the default admin role (“Microsoft Defender for Endpoint administrator (default)”) to the security group “Truesec SOC Admins”
    - If the group “Truesec SOC Admins PIM” was created earlier, then add this group **instead** of “Truesec SOC Admins”.
- Click “+ Add item”
    - Create four new roles with permissions and assigned security groups as described below:
        - Readers
        - Operators
        - Privileged Operators
        - Live Responders

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

Sweden
+46 810 00 10
info@truesec.se

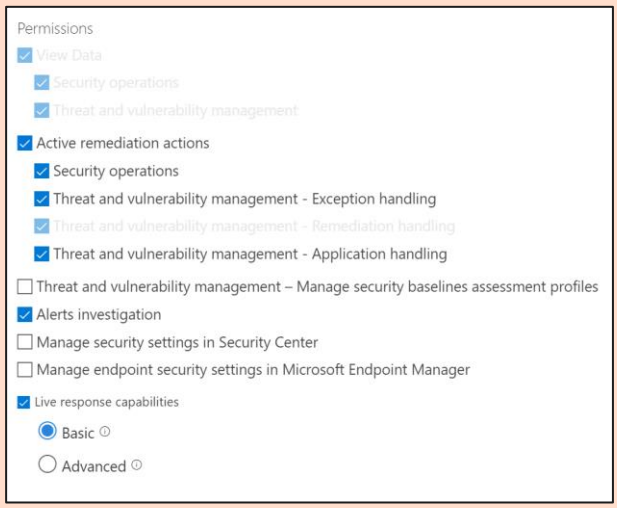
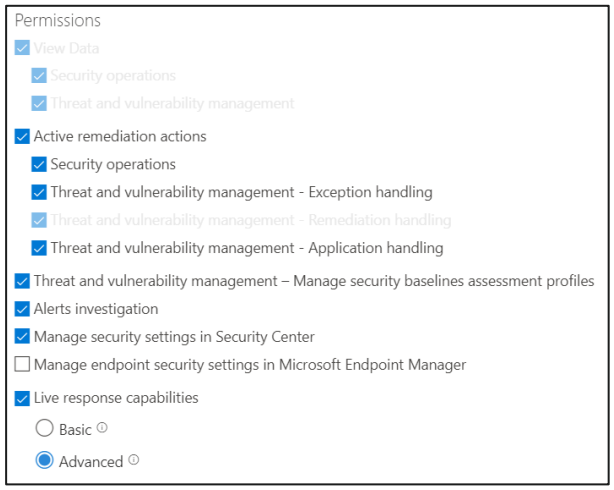
US
+1 (425) 818-8044
info@truesec.com

Role	Assigned to security group
Readers 	Truesec SOC Readers
Operators 	Truesec SOC Operators

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

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

Privileged Operators	Truesec SOC Privileged Operators
	
Live Responders	Truesec SOC Live Responders
	

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

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

3.2. Configure Advanced features

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

3.2.1. Make sure the following features are enabled

- Live Response
- Live Response for Servers
- Live Response unsigned script execution
- Enable EDR in block mode
- Preview features

3.2.2. Make sure the following feature is disabled

- Automatically resolve alerts

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

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com