DEGEA
En del av Aderian Group

MDR SOC Onboarding Prerequisites

Steps required for onboarding

About

This document details all requirements before Degea can assist with SOC onboarding.

Licensing

For full XDR onboarding the following licenses are required:
All licenses are included in Microsoft 365 E5 Security addon

Services:

- Defender for Endpoint
    - Defender for Endpoint P2
- Defender for Office
    - Defender for Office P2
- Defender for Identity
    - Defender for Identity
- Defender for Cloud Apps
    - Defender for Cloud Apps
- Entra ID Protection
    - Entra ID P2

Functionality:

- User isolation
    - Entra ID P2
    - Defender for Cloud Apps

Services

- A dedicated pay-as-you-go Azure Subscription for Microsoft Sentinel (if Microsoft Sentinel is already deployed you can use the existing setup).

Settings

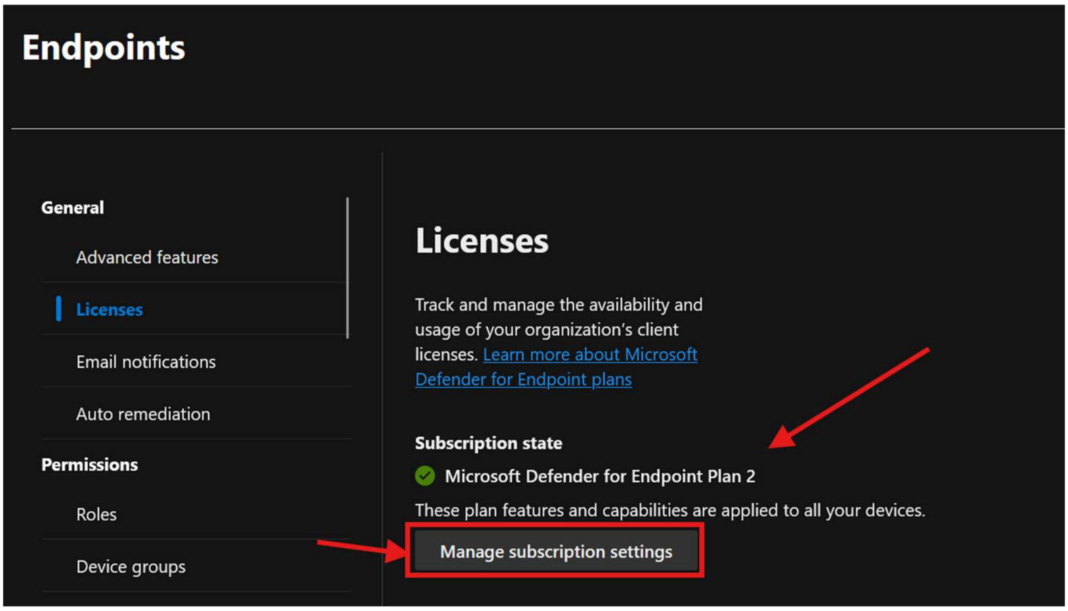
Change subscription state to Defender for Endpoint Plan 2

Requires sufficient Defender for Endpoint P2 licenses to cover all endpoints.

- **Minimum requirement:** 1 license per 5 endpoints to enable the licensing model
- **Microsoft compliance requirement:** 1 license per workstation user

Note: This change takes up to 24 hours to take effect.

https://security.microsoft.com ➔Settings ➔ Endpoints ➔ [General] Licenses



Licenses

Track and manage the availability and usage of your organization's client licenses. Learn more about Microsoft Defender for Endpoint plans

Subscription state

✓ Microsoft Defender for Endpoint Plan 2

These plan features and capabilities are applied to all your devices.

SOP Setup

We can assist with setup according to our SOP documents. If all requirements are met, we offer fully managed onboarding, which requires:

- **Global Administrator account (temporary)** – Needed to consent to applications and configure Sentinel delegation across all subscriptions
- **Contact person for test alert generation** – The final onboarding step requires generating a test alert on a user endpoint. Since fallback methods may need local administrator privileges, the contact must have elevation capabilities (see "9-DEG SOP - Generate a test alert")

Mandate

By default, the SOC is authorized to isolate users, endpoints, and servers when threats are detected. Any exceptions to this mandate should be discussed and agreed upon before onboarding is complete. Without explicit exclusions, we will proceed with standard authorization.

Contact list

Provide contact information for at least two individuals from both your company and your MSP (if applicable). Contacts should have organizational oversight and authority to approve services such as incident response and root cause analysis.