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).

Security Level Requirements

While there is no strict minimum security level required for MDR SOC implementation, a mature security posture significantly enhances the effectiveness of SOC operations. The following recommendations outline key security controls that should be in place or planned prior to onboarding.

Please note that this list is not exhaustive and assumes fundamental IT hygiene policies, routines, and practices are already established within the environment.

Microsoft 365 Environment

Organizations with Microsoft Security E5 add-on licenses should maintain a Secure Score of 80%, a combined 750 points, or higher for identity and device security, including:

- **Privileged Account Separation** – Privileged accounts must be maintained separately from regular user accounts to mitigate privilege escalation and lateral movement risks
- **Conditional Access Policies** – Comprehensive coverage should include:
  - Multi-factor authentication (MFA) enforcement
  - User risk-based access controls
  - Operating system compliance requirements
- **Application Consent Controls** – User-level application consent should be disabled
- **Authentication Protocol Hardening** – Legacy and insecure authentication methods must be disabled

On-Premises Environment

- **Active Directory Tiering** – Implement an AD tiering model (or equivalent administrative segmentation strategy)
- **Vulnerability Management** – Establish comprehensive vulnerability management processes covering Windows patching, third-party application updates, and end-of-life (EOL) server replacement
- **Security Hardening** – Apply security hardening configurations using Microsoft Security Baselines or equivalent industry-standard frameworks

DEGEA
En del av Aderian Group

Endpoint Security

- **Least Privilege Access** – Standard users should not possess local administrator privileges
- **Vulnerability Management** – Maintain comprehensive patch management for Windows updates, third-party applications, and EOL endpoint replacement
- **Security Hardening** – Implement endpoint security hardening using Microsoft Security Baselines or equivalent frameworks

Settings

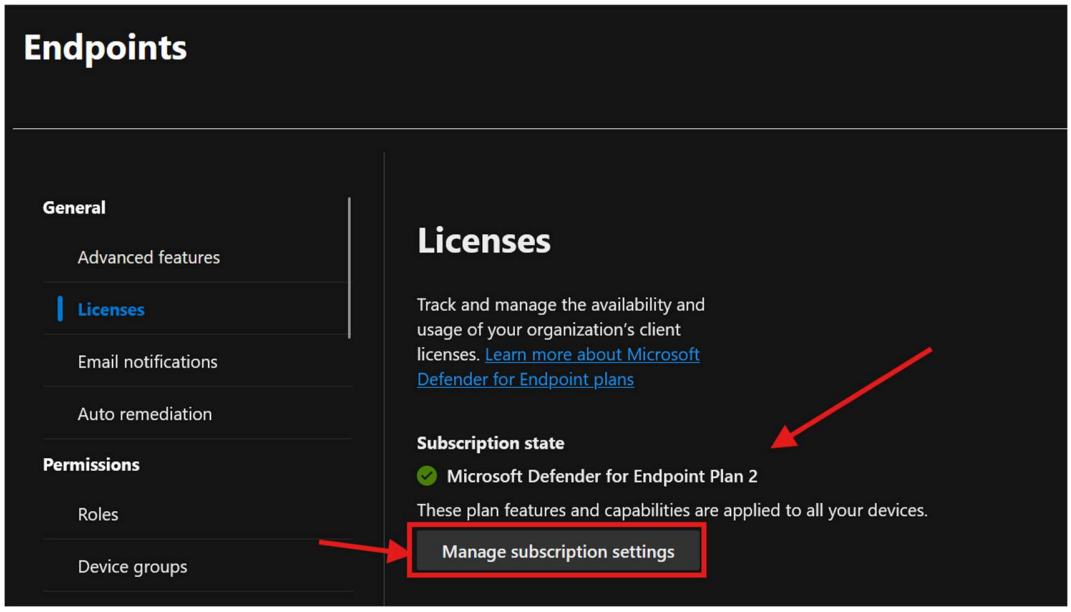
Change subscription state to Defender for Endpoint Plan 2

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



DEGEA
En del av Aderian Group

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.