Degea SOC access

Information and instructions

Access Requirements

We require access via Granular Delegated Admin Privileges (GDAP). Learn more: https://learn.microsoft.com/en-us/partner-center/customers/gdap-introduction

The roles below represent our recommended configuration. Optional roles can be removed if needed, but they enable us to view additional settings beyond Global Reader and take limited action on certain threats.

Required Roles

- **Global Reader** – View all tenant configurations
- **Security Administrator** – Full access to the Defender portal for incident management and limited threat response

Optional Roles

- **Exchange Administrator** – View threat policies to correlate alerts and enable limited threat response
- **Intune Administrator** – View device configurations for enhanced alert and incident investigation

Onboarding Process

- Send your tenant ID (GUID) to your Degea technician
- Approve the onboarding link we provide (requires Global Administrator account)