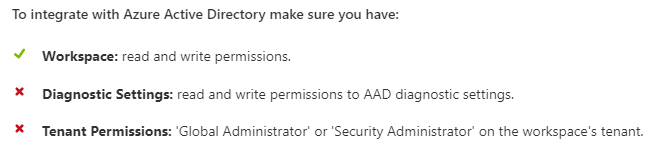
**Azure Native log Source integration to Sentinel**

1. **Azure Active Directory Log Ingestion to Sentinel**

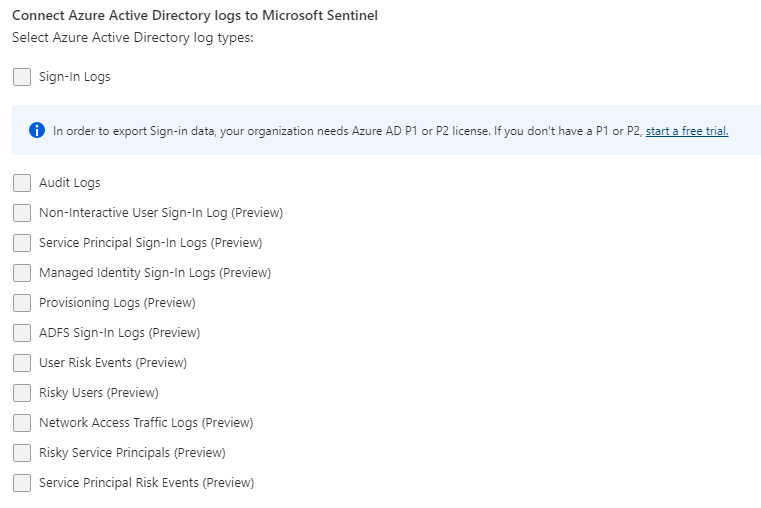
**Description**

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self-Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

**Prerequisites**-



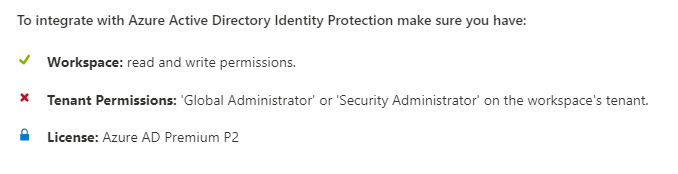
**Configuration**



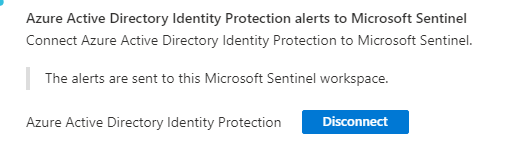
1. **Azure Active Directory Identity Protection Log Ingestion to Sentinel**

**Description-**  
Azure Active Directory Identity Protection provides a consolidated view at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft’s experience protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day. ​ Integrate Microsoft Azure Active Directory Identity Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation.​

**Prerequisites**-



**Configuration**-

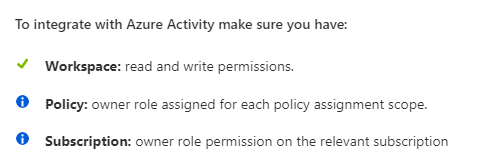


1. **Azure Activity Log Ingestion to Sentinel**

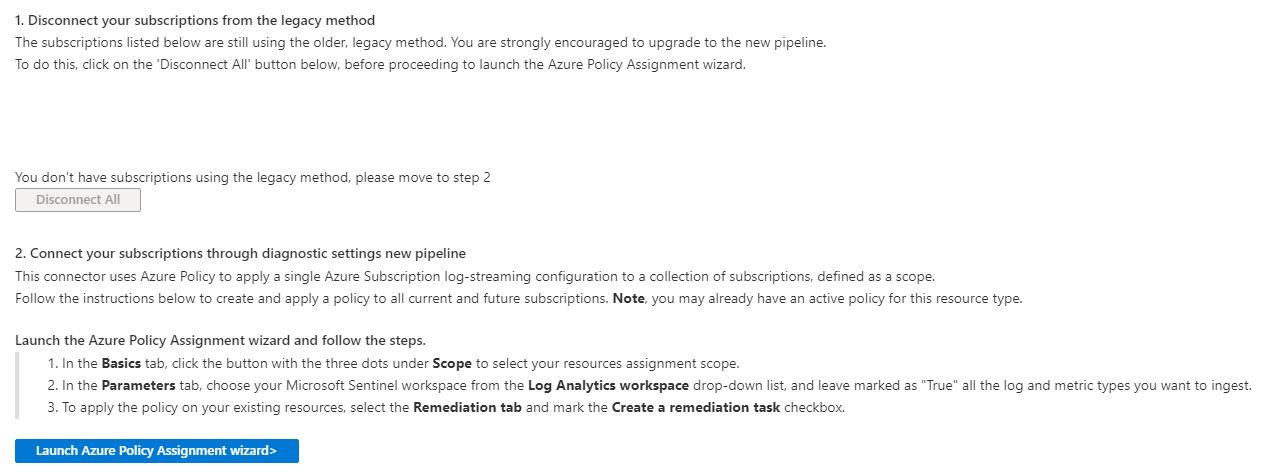
**Description**-

Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

**Prerequisites**-



**Configuration**-

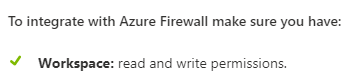


1. **Azure Firewall Log Ingestion to Sentinel**

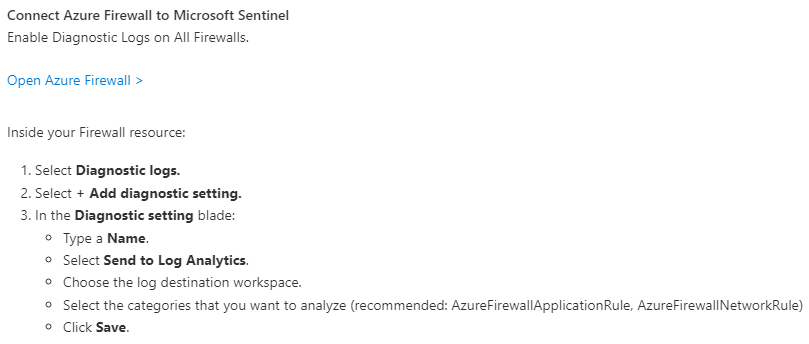
**Description-**

Connect to Azure Firewall. Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

**Prerequisites**-



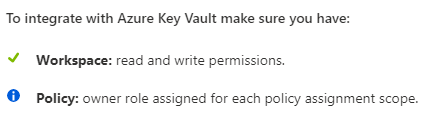
**Configuration**-



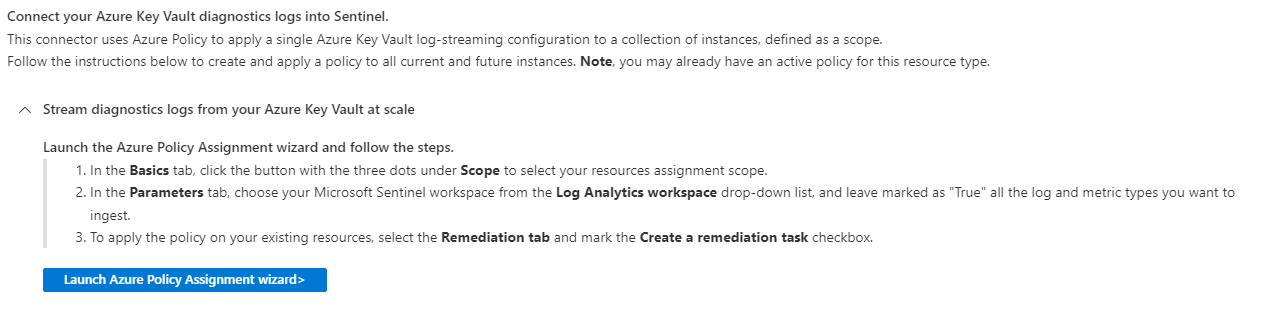
1. **Azure Key Vault Log Ingestion to Sentinel**

**Description**  
Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. This connector lets you stream your Azure Key Vault diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances.

**Prerequisites-**



**Configuration-**

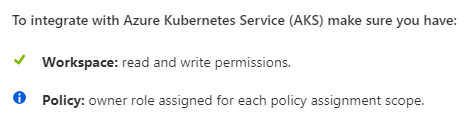


1. **Azure Kubernetes Services Log Ingestion to Sentinel**

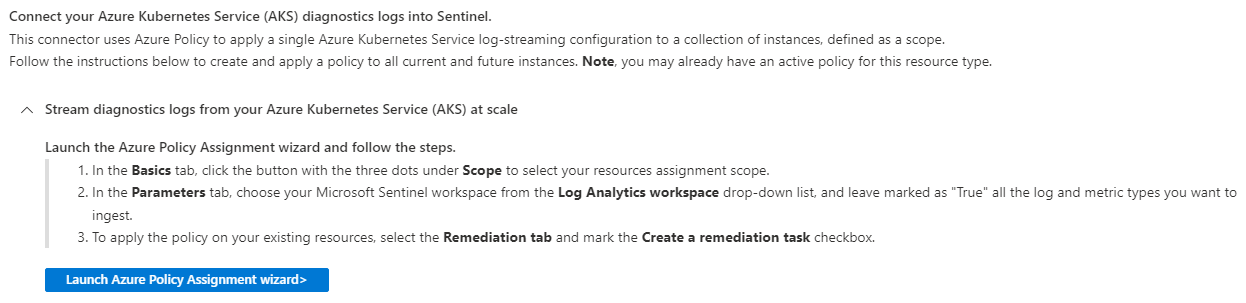
**Description-**

Azure Kubernetes Service (AKS) is an open-source, fully managed container orchestration service that allows you to deploy, scale, and manage Docker containers and container-based applications in a cluster environment. This connector lets you stream your Azure Kubernetes Service (AKS) diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances.

**Prerequisites**-



**Configuration**-

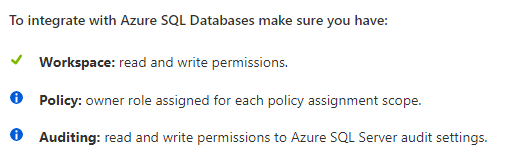


1. **Azure SQL Databases Log Ingestion to Sentinel**

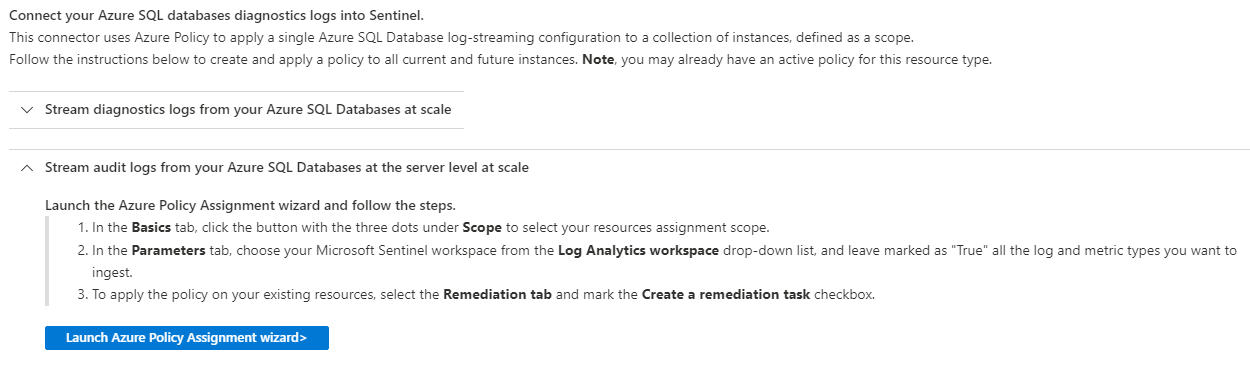
**Description**-

Azure SQL is a fully managed, Platform-as-a-Service (PaaS) database engine that handles most database management functions, such as upgrading, patching, backups, and monitoring, without necessitating user involvement. This connector lets you stream your Azure SQL databases’ audit and diagnostic logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances.

**Prerequisites**-



**Configuration**-



1. **Microsoft 365 Defender Log Ingestion to Sentinel**

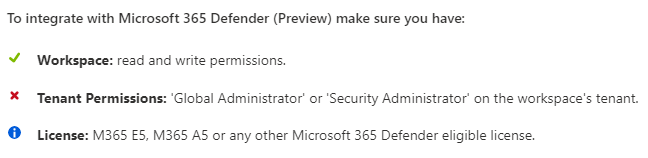
**Description-**

Microsoft 365 Defender​ is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

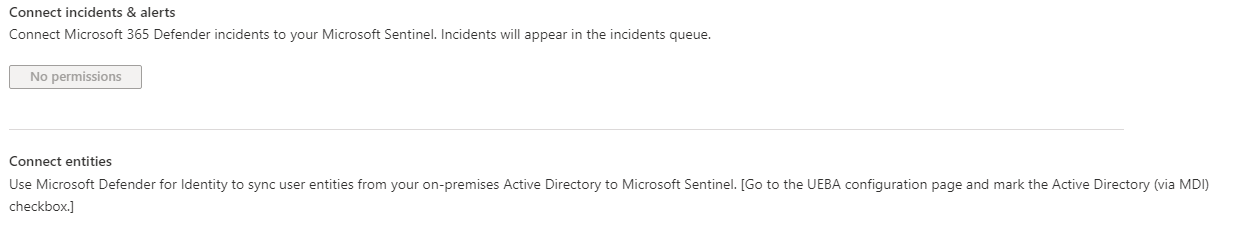
Microsoft 365 Defender suite includes:

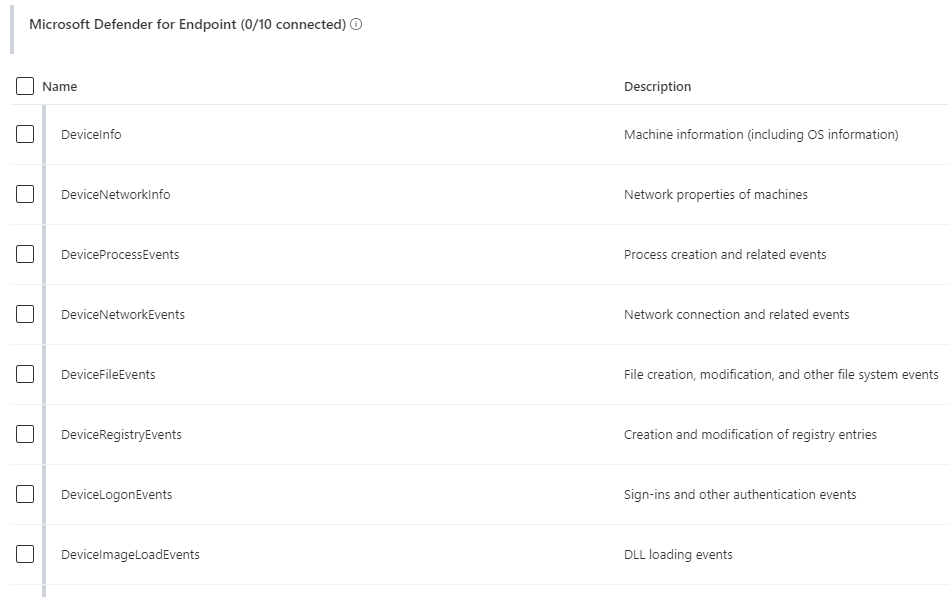
* Microsoft Defender for Endpoint
* Microsoft Defender for Identity
* Microsoft Defender for Office 365
* Microsoft Defender for Cloud Apps
* Microsoft Defender Alert Evidence
* Microsoft Defender Vulnerability Management

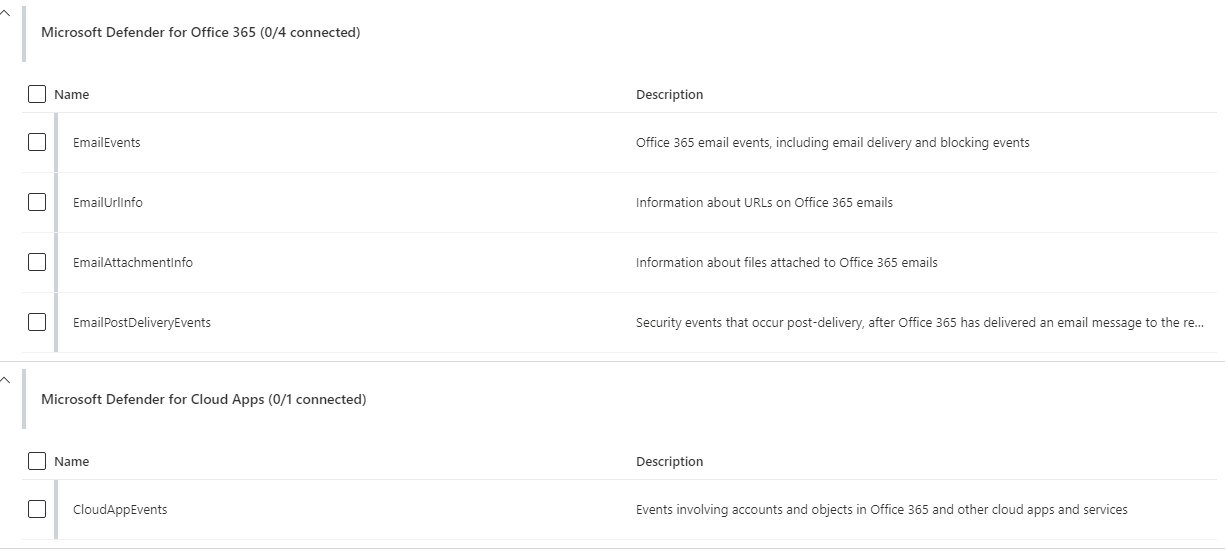
**Prerequisites-**

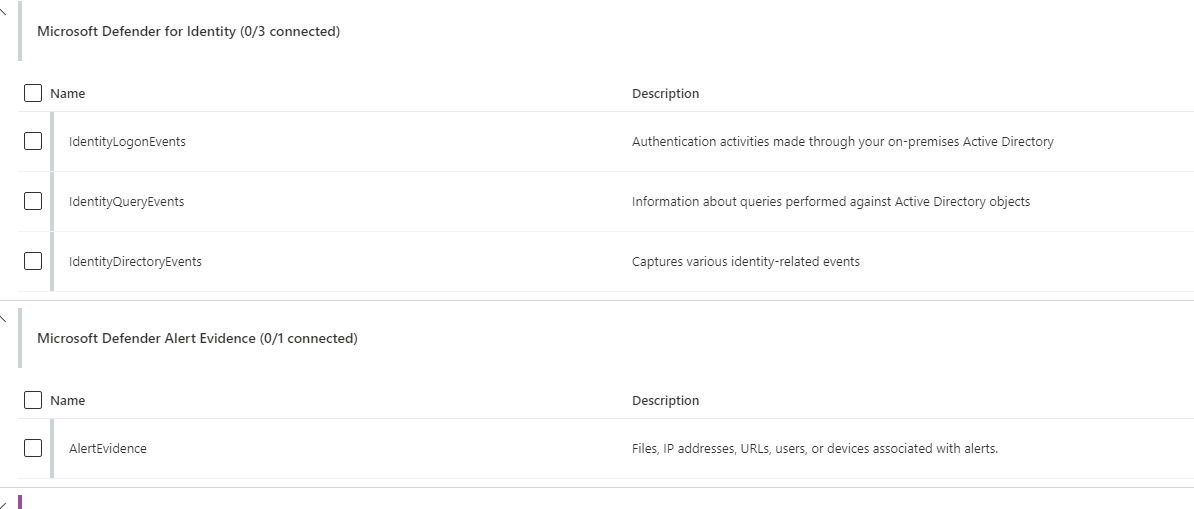


**Configuration**-









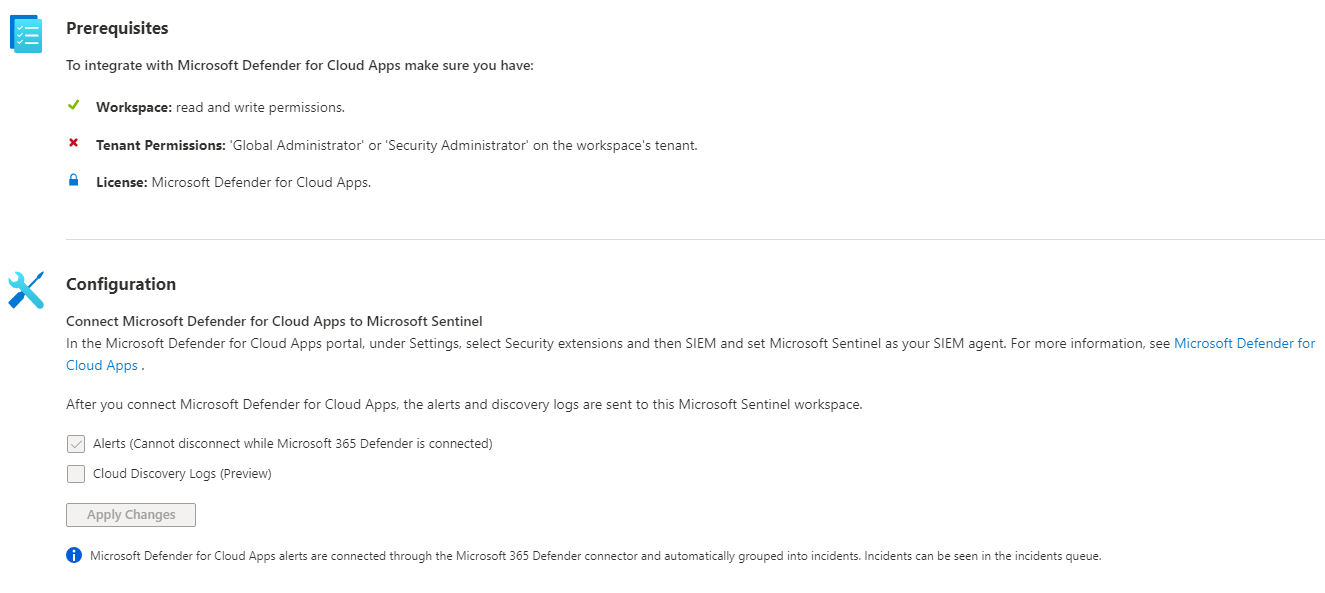
1. **Microsoft Defender for Cloud Apps Log Ingestion to Sentinel**

**Description-**

By connecting with [Microsoft Defender for Cloud Apps](https://aka.ms/asi-mcas-connector-description) you will gain visibility into your cloud apps, get sophisticated analytics to identify and combat cyberthreats, and control how your data travels.

* Identify shadow IT cloud apps on your network.
* Control and limit access based on conditions and session context.
* Use built-in or custom policies for data sharing and data loss prevention.
* Identify high-risk use and get alerts for unusual user activities with Microsoft behavioral analytics and anomaly detection capabilities, including ransomware activity, impossible travel, suspicious email forwarding rules, and mass download of files.
* Mass download of files

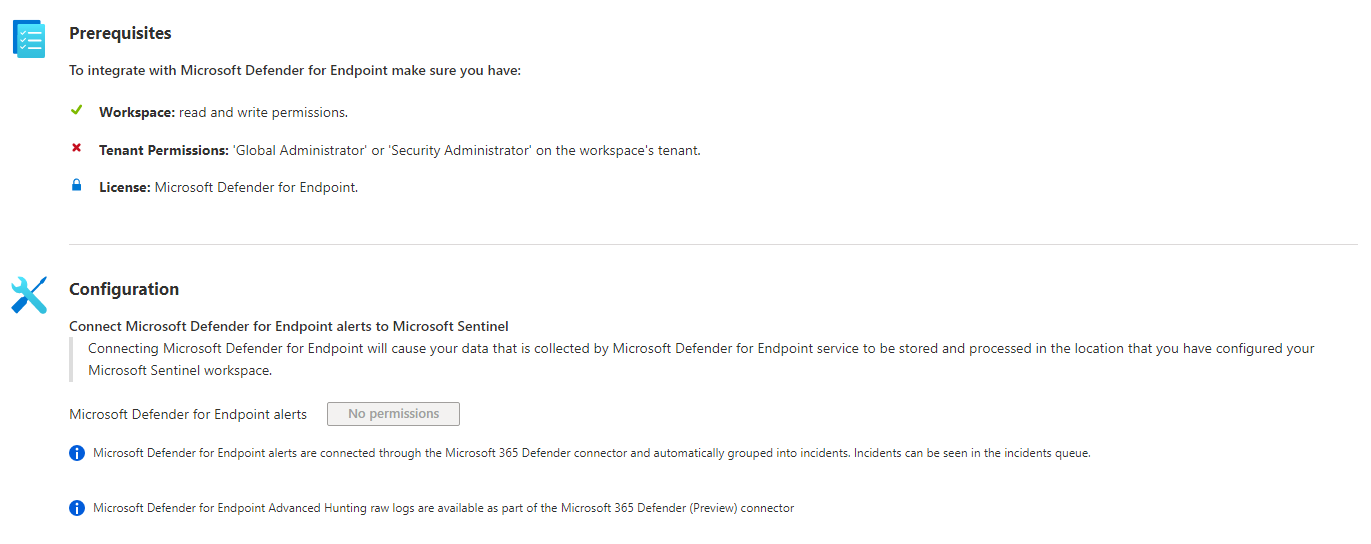
**Prerequisites**-



1. **Microsoft Defender for Endpoint Log Ingestion to Sentinel**

**Description**

Microsoft Defender for Endpoint is a security platform designed to prevent, detect, investigate, and respond to advanced threats. The platform creates alerts when suspicious security events are seen in an organization. Fetch alerts generated in Microsoft Defender for Endpoint to Microsoft Sentinel so that you can effectively analyze security events. You can create rules, build dashboards and author playbooks for immediate response.

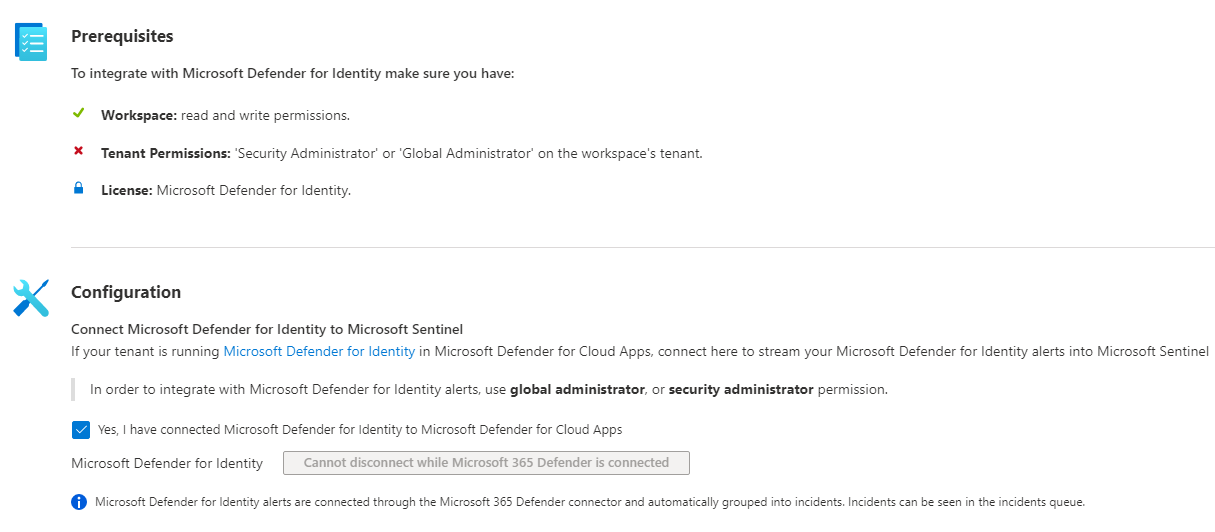


1. **Microsoft Defender for Identity Log Ingestion to Sentinel**

**Description**

Connect Microsoft Defender for Identity to gain visibility into the events and user analytics. Microsoft Defender for Identity identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Microsoft Defender for Identity enables SecOp analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

* Monitor users, entity behavior, and activities with learning-based analytics​
* Protect user identities and credentials stored in Active Directory
* Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
* Provide clear incident information on a simple timeline for fast triage



1. **Microsoft Defender for Office 365 Log Ingestion to Sentinel**

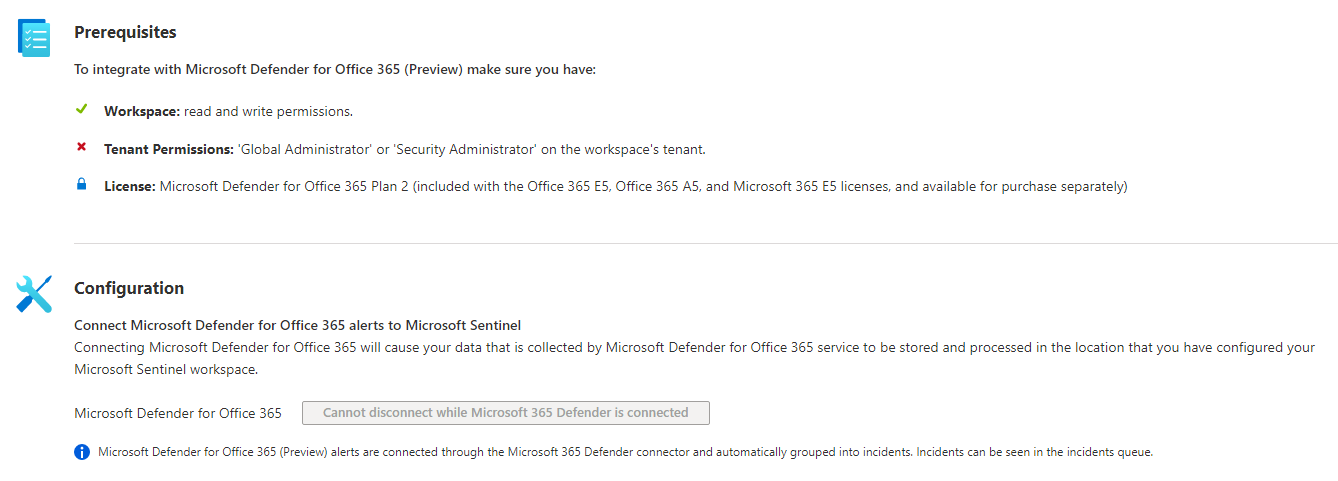
**Description-**

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools. By ingesting Microsoft Defender for Office 365 alerts into Microsoft Sentinel, you can incorporate information about email- and URL-based threats into your broader risk analysis and build response scenarios accordingly.

The following types of alerts will be imported:

* A potentially malicious URL click was detected
* Email messages containing malware removed after delivery
* Email messages containing phish URLs removed after delivery
* Email reported by user as malware or phish
* Suspicious email sending patterns detected
* User restricted from sending email

These alerts can be seen by Office customers in the **Office Security and Compliance Center**.

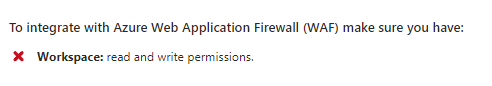


1. **Azure WAF Log Ingestion to Sentinel**

**Description-**

Connect to the Azure Web Application Firewall (WAF) for Application Gateway, Front Door, or CDN. This WAF protects your applications from common web vulnerabilities such as SQL injection and cross-site scripting, and lets you customize rules to reduce false positives. Follow these instructions to stream your Microsoft Web application firewall logs into Microsoft Sentinel.

**Prerequisites-**

****

**Configuration-**

****