Configure Audit Logging in Microsoft 365 for Umbrella Cloud Malware Scanning

Contents

Introduction

This document describes how to enable Audit Logging in Microsoft 365 for Umbrella Cloud Malware scanning.

Overview

To integrate Cisco Umbrella with Microsoft 365 (formerly Office 365) for Cloud Malware scanning, the auditing of user events must be enabled in Microsoft 365 (which might not be enabled by default). This article explains how to enable audit logging in the Microsoft Purview compliance portal.

For more information on the Cloud Malware feature, please read the Cisco Umbrella Documentation.

Enable audit logging

To enable audit logging in Microsoft 365:

1. In the Microsoft Purview compliance portal at https://compliance.microsoft.com, go to **Solutions** > **Audit**.
   - Or to go directly to the **Audit** page, use https://compliance.microsoft.com/auditlogsearch.
2. If auditing is not turned on for your organization, a banner is displayed prompting you to start recording user and admin activity.
3. Select the **Start recording user and admin activity** banner.

Note that it can take about 24 hours for auditing to begin working. For assistance with audit logging, please read the Microsoft Documentation or contact your MS support partner.

For the Cloud Malware Report to work in Cisco Umbrella, auditing related to user/file activity must appear on the **Audit** page in Microsoft 365's Purview compliance portal.

For example:

4404249123348