

Review and Respond to DLP Alerts

At the end of this episode, I will be able to:

1. Review and respond to DLP alerts, events, and reports

Learner Objective: *Review and respond to Data Loss Prevention (DLP) alerts, events, and reports in Microsoft Purview*

Description: In this episode, you will learn the basics of how to configure and respond to alerts, events, and reports regarding DLP in Microsoft Purview.

-
- Microsoft Purview Data Loss Prevention (DLP) policies can take protective actions to prevent unintentional sharing of sensitive items.
 - When an action is taken on a sensitive item, you can be notified by configuring alerts for DLP.
 - The DLP alert management dashboard:
 - Located in the Microsoft Purview Compliance Portal
 - Show alerts for Exchange, SharePoint, OneDrive, Teams, and Devices
 - Advanced alert configuration options - part of the DLP policy authoring flow; these permit the creation of rich alert configurations; you can create single-event alerts or aggregated alerts based on the number of events or the size of the leaked data
 - Prerequisites include:
 - Ensure proper licensing
 - Ensure required permissions (roles)
 - All eligible tenants for Office 365 DLP can access the DLP alert management dashboard
 - To work with the DLP alert management dashboard:
 - Launch the Microsoft Purview Compliance Portal
 - Go to Data Loss Prevention
 - Select the Alerts tab
 - Access the DLP Alerts Dashboard
 - There is an Events tab to view all of the events associated with the alert
 - Once you investigate the alert - you can choose Manage Alerts to change the status:
 - Active
 - Investigating
 - Dismissed
 - Resolved
-

Additional Resources:

Configure and view alerts for data loss prevention policies

<https://learn.microsoft.com/en-us/purview/dlp-configure-view-alerts-policies>