

Information Protection Data Connector

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Information Protection Data Connector


The Azure Information Protection Data Connector works by pulling data from the same workspace where the Azure Information Protection's analytics stores its data.

From the Azure Information Protection portal within Azure Portal, it may be verified what Log Analytics workspace the Data Connector is reporting to, before configuring the Data Connector. It can be checked at Manage – Configure Analytics (preview).

Upon configuring the Data Connector, the selected workspace must be the one where Sentinel resides. If that workspace is different from the one that analytics is using from Azure Information Protection, then the system will automatically change the AIP workspace to be the one that is selected from the Data Connector.

So, upon the case that AIP used a different workspace, and then when configuring the Data Connector was changed to Sentinel, only the new data from the moment the connector was enabled will be visible to Sentinel.

It is important to bear in mind that AIP will store label changes logs only for desktop versions of Office. Any changes done at the web Office version will not be logged by AIP.

The compliance portal (compliance.microsoft.com ) handles data of AIP and other sources. So, be aware that if the customer expects to see data from the compliance portal, they will only see that relevant to AIP which comes only from the Desktop version of Office.