Must read before escalating to Data Collection team

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

Here are some things that you must do before escalating the ticket:

• Check each connector in the connectors excel list and open it to the listed team. If the connector isn't there open it to the 3rd party connectors team.

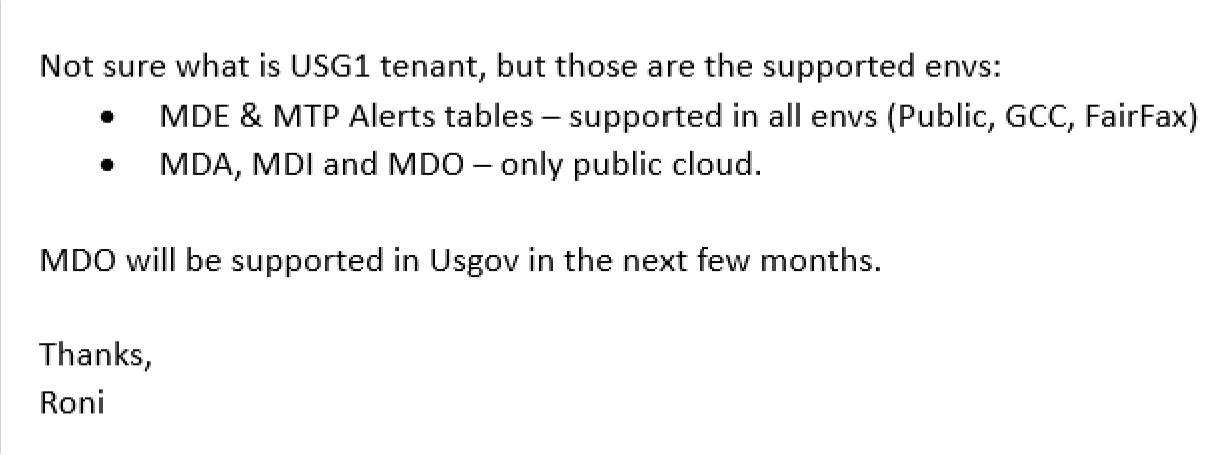
Another link

• In Office, Defender, and diagnostic settings connectors the customer always can access the source data (in Office audit logs portal, advance hunting portal etc.). Ask the customer to check that the missing data/field he is complaining about is present in the source, and if not open it to the relevant team there.

Here is a CRI for example: Incident-304074907 Details - IcM

• When you get complains about Sign In logs not ingested in Azure Active Directory connector please open the CRI to IDX/Data Insights and Reporting Service team. It's a known issue that repeat every week, PG have nothing to do with those tickets and they just transfer them to that team.

• For defender connectors see in the picture below which connectors supported in which environment:



Not sure what is USG1 tenant, but those are the supported envs:

- MDE & MTP Alerts tables – supported in all envs (Public, GCC, FairFax)
- MDA, MDI and MDO – only public cloud.

MDO will be supported in Usgov in the next few months.

Thanks,
Roni

You can check tenant scope by this link before they open the ticket:

https://login.microsoftonline.com/ <tenant-id>/.well-known/openid-configuration