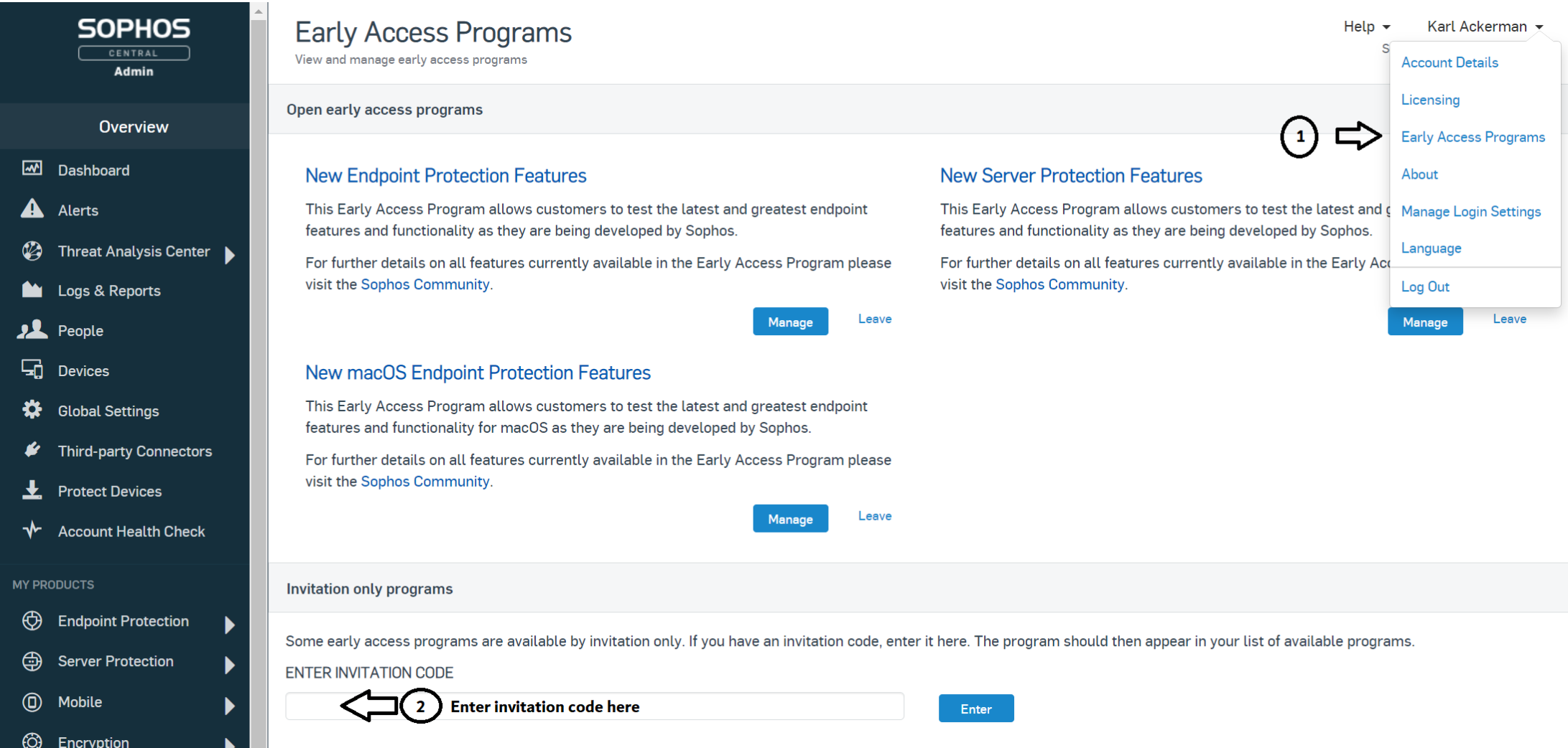
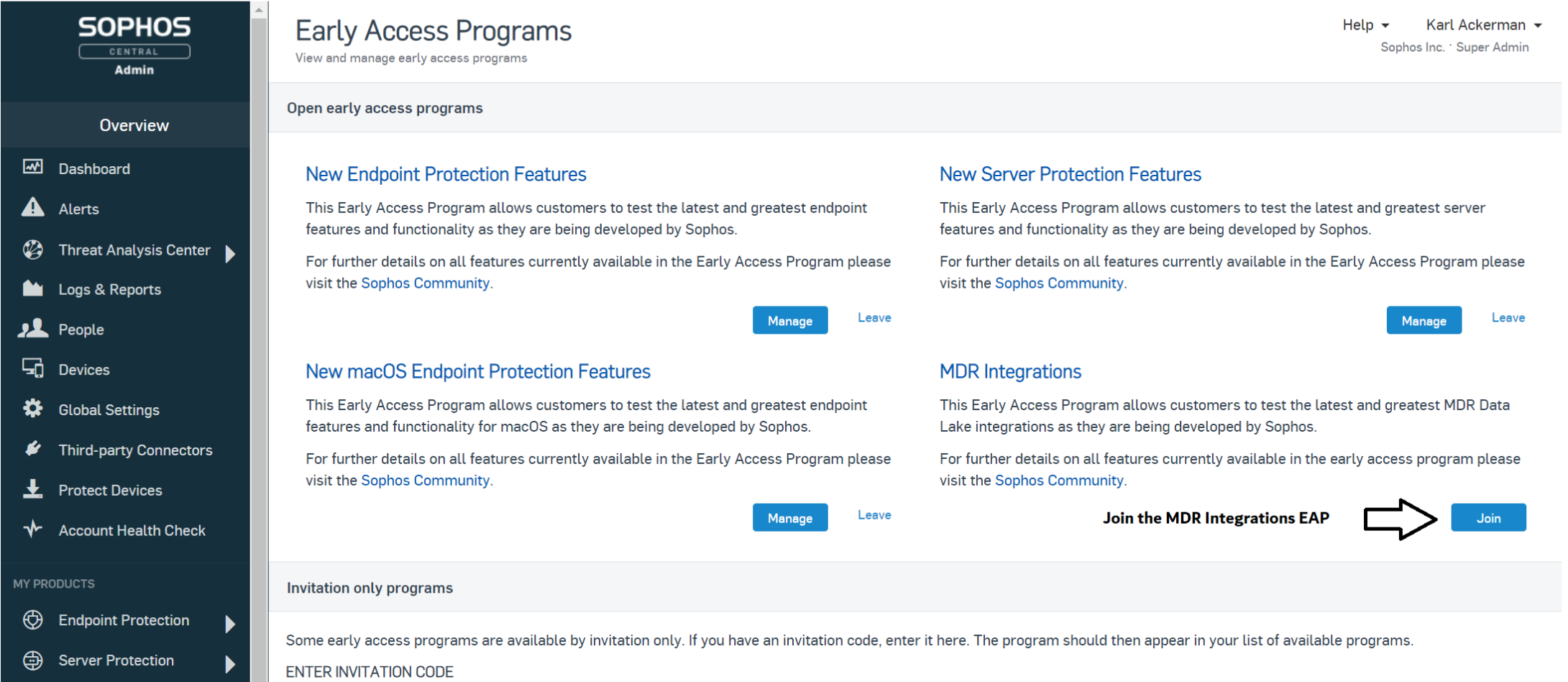
**How to Join the Sophos MTR - EAP Microsoft Graph Security EAP**

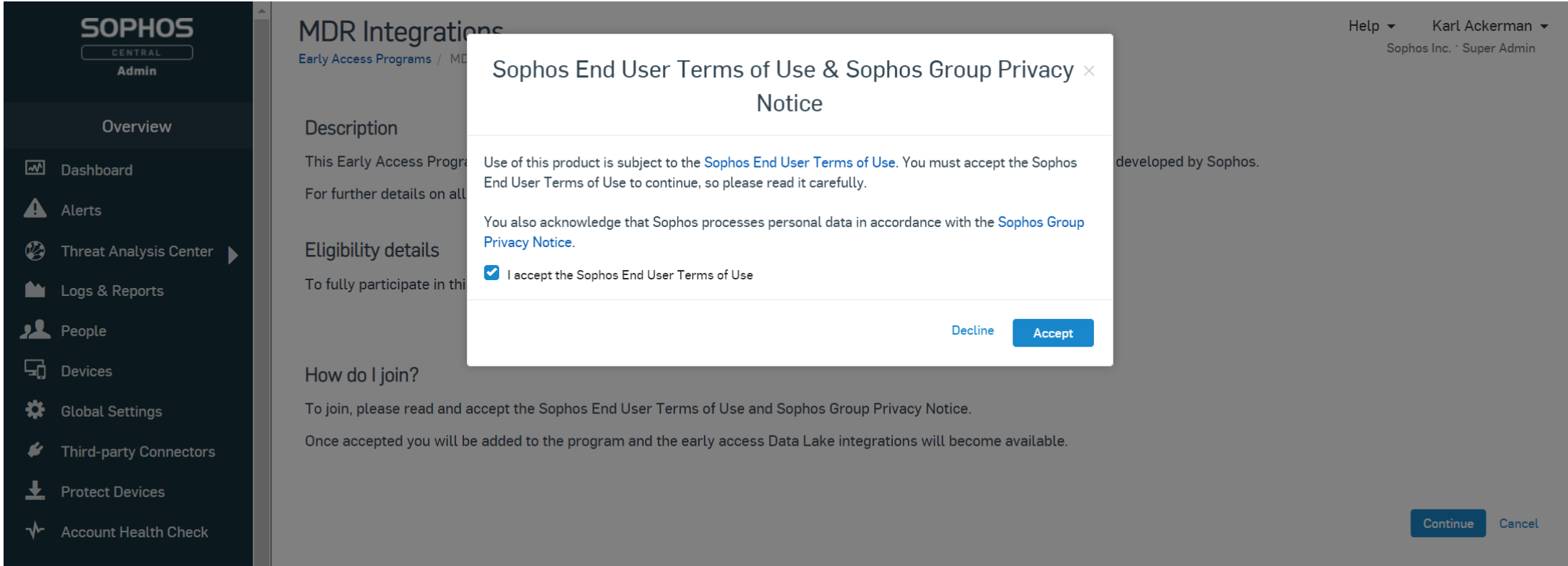
**STEP 1** - Enter the invitation code in the Central



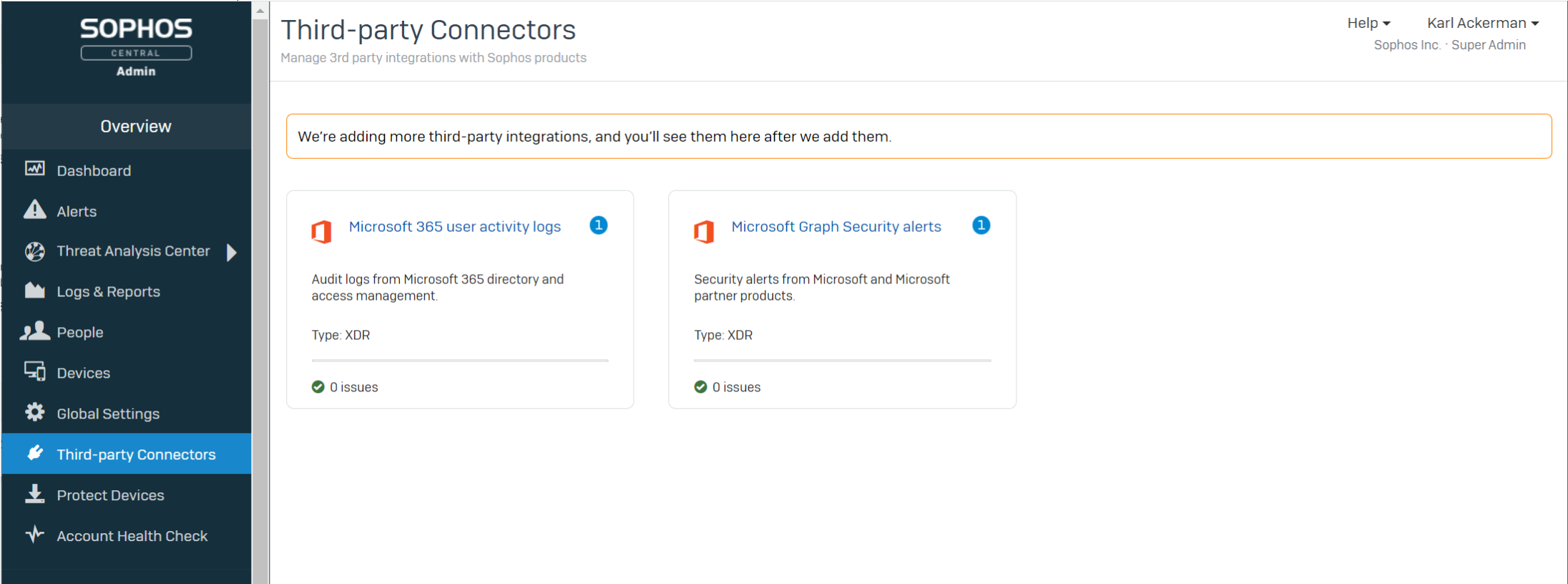
**STEP 2** - The early access program should become available and you need to JOIN the program



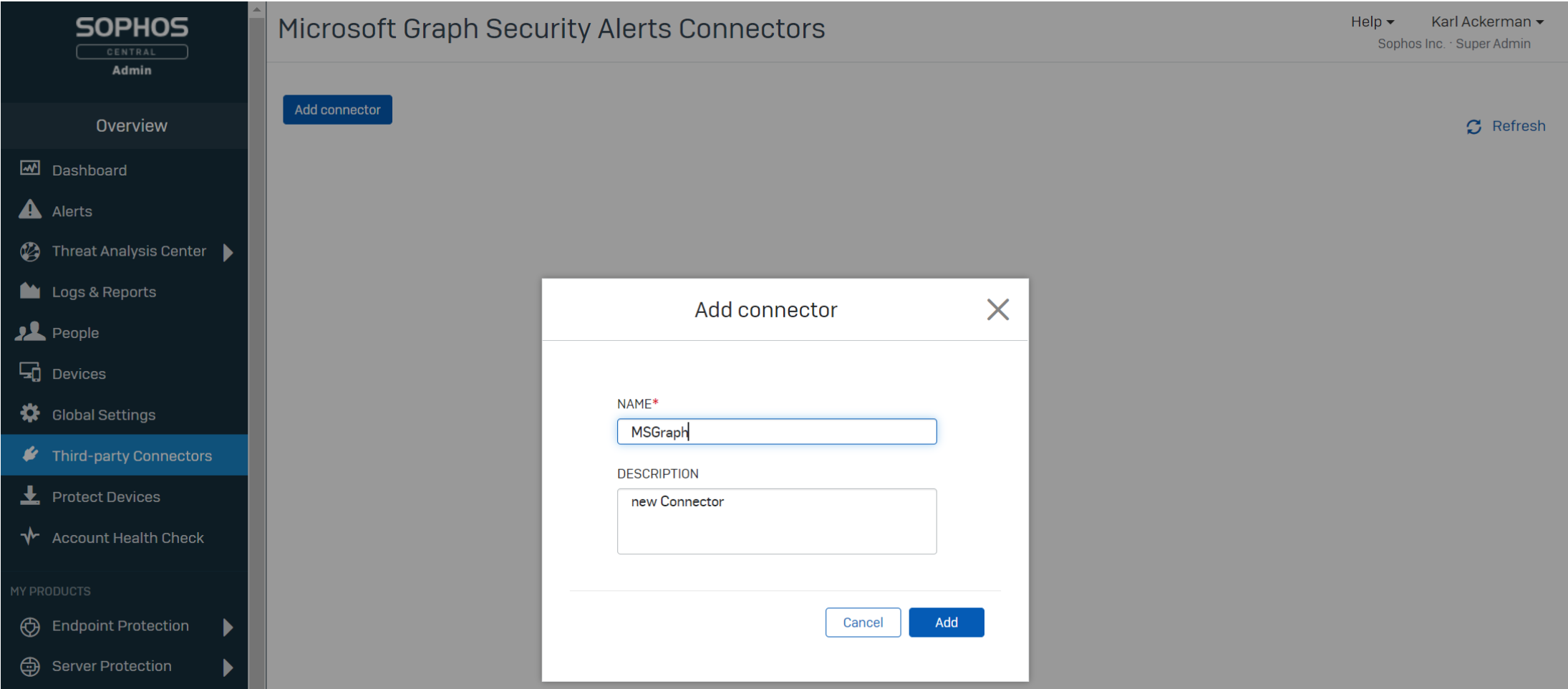
**STEP 3** - Review and Accept the terms and conditions for the EAP.



**STEP 4**- Now select Third-party Connectors from the left side navigation in central and select the Microsoft Graph Security alerts connector

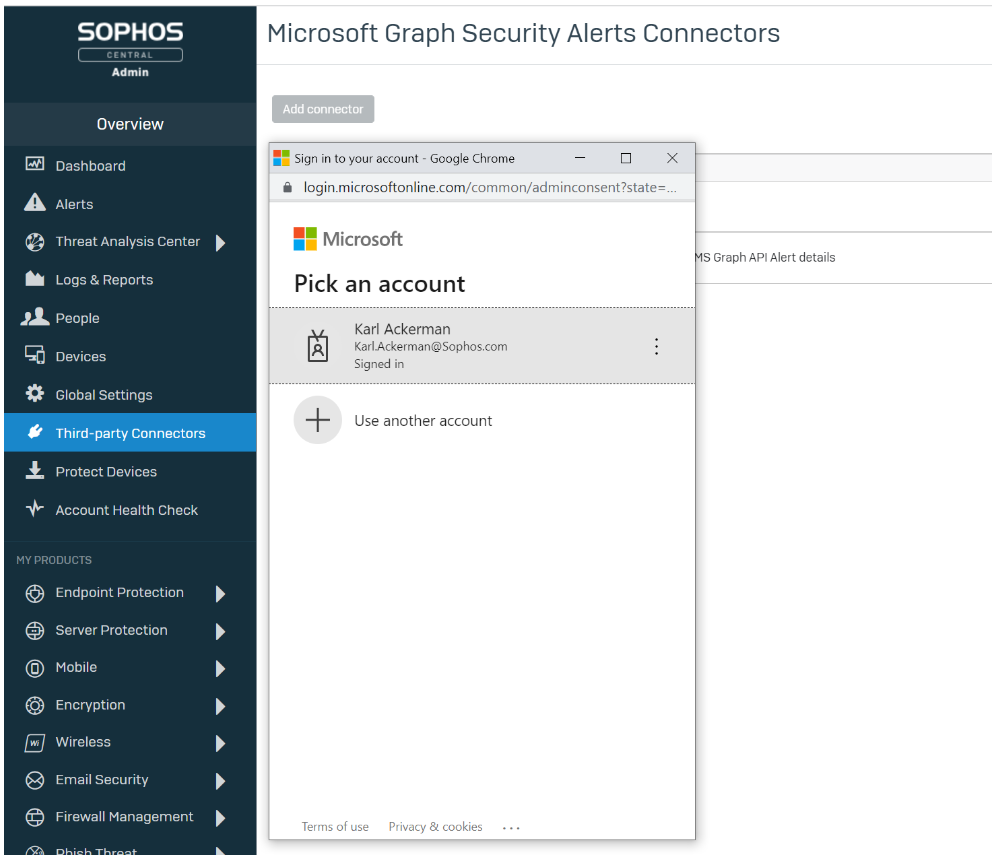


**STEP 5**- Add the connector



**STEP 6** - Select continue and you will be prompted for your Microsoft Security Center password.

* We are not storing your account credential; You are simply authorizing Sophos to setup a read-only connection the the MS Graphs Security API.

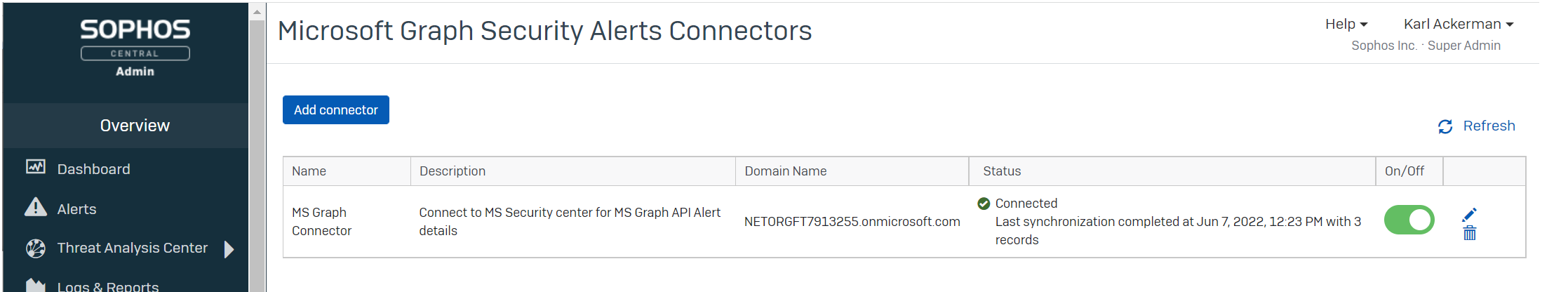


**STEP 7**- Confirm the connector is working correctly

After the connector, has been configured it will take some time before the first MS Graph alerts will be visible. Depending on the activity in your environment this may be from a quickly as 15 min to much longer if no detections are being generated.

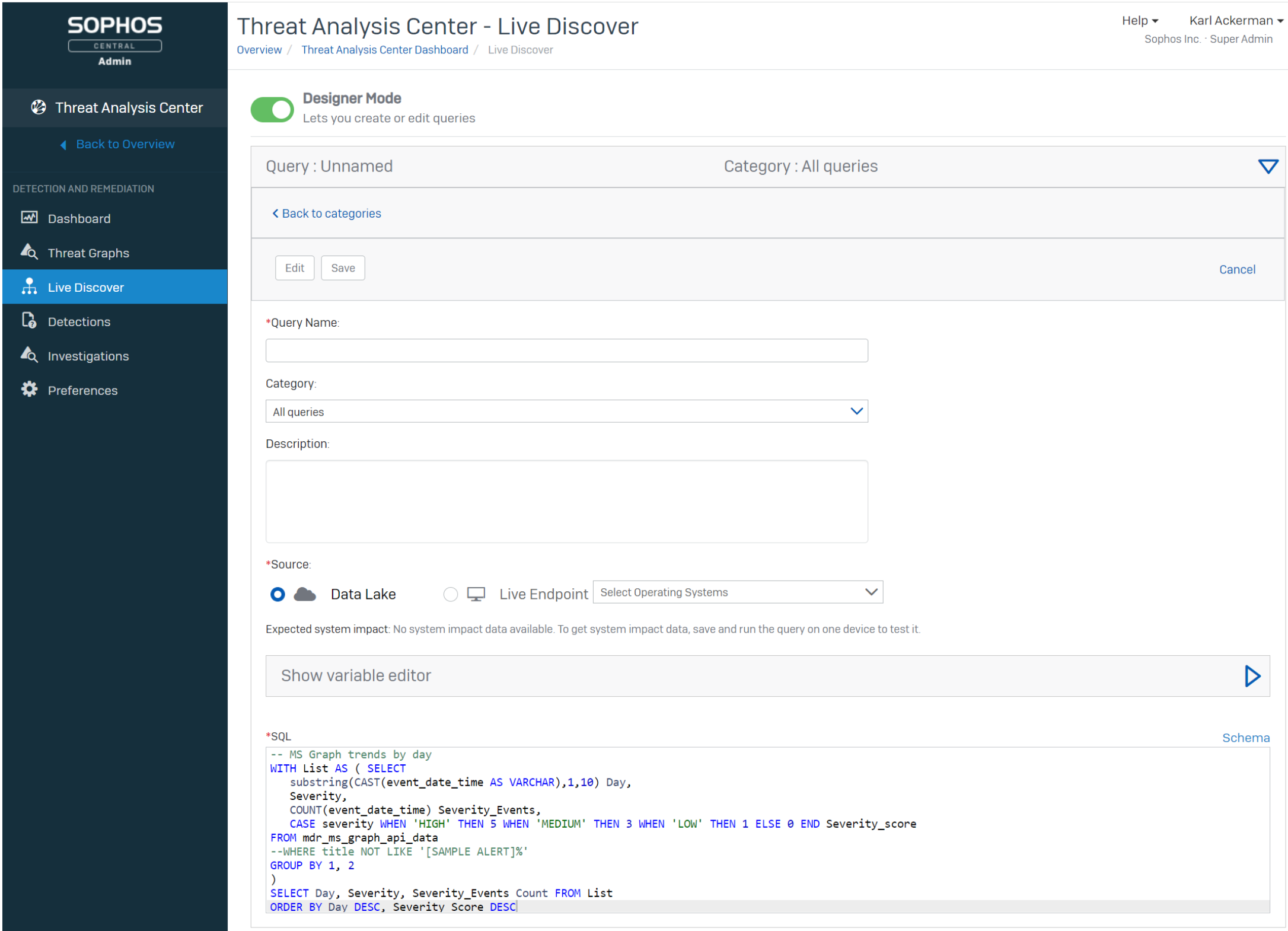
If the connection fails please reach out to us at **mdreap2@sophps.com**with the details.

You can check the status of the connector and see how many alerts have been synchronized.



**STEP 8 -** After you have confirmed events are being synchronized you can view the detection by running a query in central.

Simply navigate to Threat Analysis Center -> Live Discover enable designer mode and add a new DataLake query.



SQL CODE TO ADD:

-- MS Graph trends by day

WITH List AS ( SELECT

   substring(CAST(event\_date\_time AS VARCHAR),1,10) Day,

   Severity,

   COUNT(event\_date\_time) Severity\_Events,

   CASE severity WHEN 'HIGH' THEN 5 WHEN 'MEDIUM' THEN 3 WHEN 'LOW' THEN 1 ELSE 0 END Severity\_score

FROM mdr\_ms\_graph\_api\_data

--WHERE title NOT LIKE '[SAMPLE ALERT]%'

GROUP BY 1, 2

)

SELECT Day, Severity, Severity\_Events Count FROM List

ORDER BY Day DESC, Severity\_Score DESC

Additional queries are available on the community forum.

**For more information on the Microsoft Graph Security Connector**

* Sophos MDR Community forum: <https://community.sophos.com/mdr-community-channel>
* Sophskills presentation: <https://community.sophos.com/mdr-community-channel/mtr-connector-eap/b/announcements/posts/presentation-deck-from-sophskills-for-ms-graph-connector>

|  |  |
| --- | --- |
| [https://community.sophos.com/cfs-file/__key/communityserver-blogs-components-weblogfiles/00-00-00-00-90/sophskills-_2D00_-msgraph-pptx.jpg](https://community.sophos.com/mdr-community-channel/mtr-connector-eap/b/announcements/posts/presentation-deck-from-sophskills-for-ms-graph-connector) | [Presentation Deck from Sophskills for MS Graph Connector](https://community.sophos.com/mdr-community-channel/mtr-connector-eap/b/announcements/posts/presentation-deck-from-sophskills-for-ms-graph-connector)  Attached below is the presentation deck used in the Sophskills demo from June 1 and 2.  community.sophos.com |

