Azure ATP health center

(Please click on the link below to view the contributors to this article)

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-health-center

The Azure ATP health center lets you know how your Azure ATP instance is performing and alerts you when there are problems.

Working with the Azure ATP health center

The Azure ATP health center lets you know that there's a problem by raising an alert (a red dot) above the Health Center icon in the menu bar.

Managing Azure ATP health

To check up on the overall health of your Azure ATP instance, click the Health Center icon in

the menu bar

- All open issues can be managed by setting them to **Close**, or **Suppress**, by clicking the three dots in the corner of the alert and making your selection.
- **Open**: All new suspicious activities appear in this list.
- **Close**: Is used to track suspicious activities that you identified, researched, and fixed for mitigated.

  Note

  Azure ATP may reopen a closed activity if the same activity is detected again within a short period of time.

- **Suppress**: Suppressing an activity means you want to ignore it for now, and only be alerted again if there's a new instance. If there's a similar alert Azure ATP doesn't reopen it. But if the alert stops for seven days, and is then seen again, you're alerted again.
- **Reopen**: You can reopen a closed or suppressed alert so that it appears as **Open** in the timeline again.
- **Delete**: From within the security alert timeline, you also have the option to delete a health issue. If you Delete an alert, it is deleted from the instance and you will NOT be able to restore it. After you click delete, you'll be able to delete all security alerts of the same type.

All [2] ⓘ

Open [1]

🟥 High [0]

🟨 Medium [0]

⬜ Low [1]

Closed [1]

Suppressed [0]

Now

Domain synchronizer not assigned

OPEN ⋮

The domain synchronizer is not assigned to any Sensor in: **contoso.com**. This may happen if there is no Sensor configured as domain synchronizer candidate. When the domain is not synchronized changes might cause entity information to become out of date or missing.

Started at 3:04 PM Feb 14, 2018

Recommendations

○ Configure at least one Sensor that monitors a domain controller as domain synchronizer candidate, for each domain.