How to integrate Azure ATP with Windows Defender ATP

(Please go to link below to view the contributors for this article)

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/integrate-wd-atp

Azure Advanced Threat Protection enables you to integrate Azure ATP with Windows Defender ATP, for an even more complete threat protection solution. While Azure ATP monitors the traffic on your domain controllers, Windows Defender ATP monitors your endpoints, together providing a single interface from which you can protect your environment.

By integrating Windows Defender ATP into Azure ATP, you can leverage the full power of both services and secure your environment, including:

- Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system (for example, process, registry, file, and network communications) and send this sensor data to your private, isolated, cloud instance of Windows Defender ATP.
- Cloud security analytics: Leveraging big-data, machine-learning, and unique Microsoft view across the Windows ecosystem (such as the Microsoft Malicious Software Removal Tool), enterprise cloud products (such as Office 365), and online assets (such as Bing and SmartScreen URL reputation), behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- Threat intelligence: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Windows Defender ATP to identify attacker tools, techniques, procedures, and generate alerts when these activities are observed in collected sensor data.

Azure ATP technology detects multiple suspicious activities, focusing on several phases of the cyber-attack kill chain including:

- Reconnaissance, during which attackers gather information on how the environment is built, what the different assets are, and which entities exist. They generally build their plan for the next phases of the attack here.
- Lateral movement cycle, during which an attacker invests time and effort in spreading their attack surface inside your network.
- Domain dominance (persistence), during which an attacker captures the information allowing them to resume their campaign using various sets of entry points, credentials, and techniques.

At the same time, Windows Defender ATP leverages Microsoft technology and expertise to detect sophisticated cyber-attacks, providing:

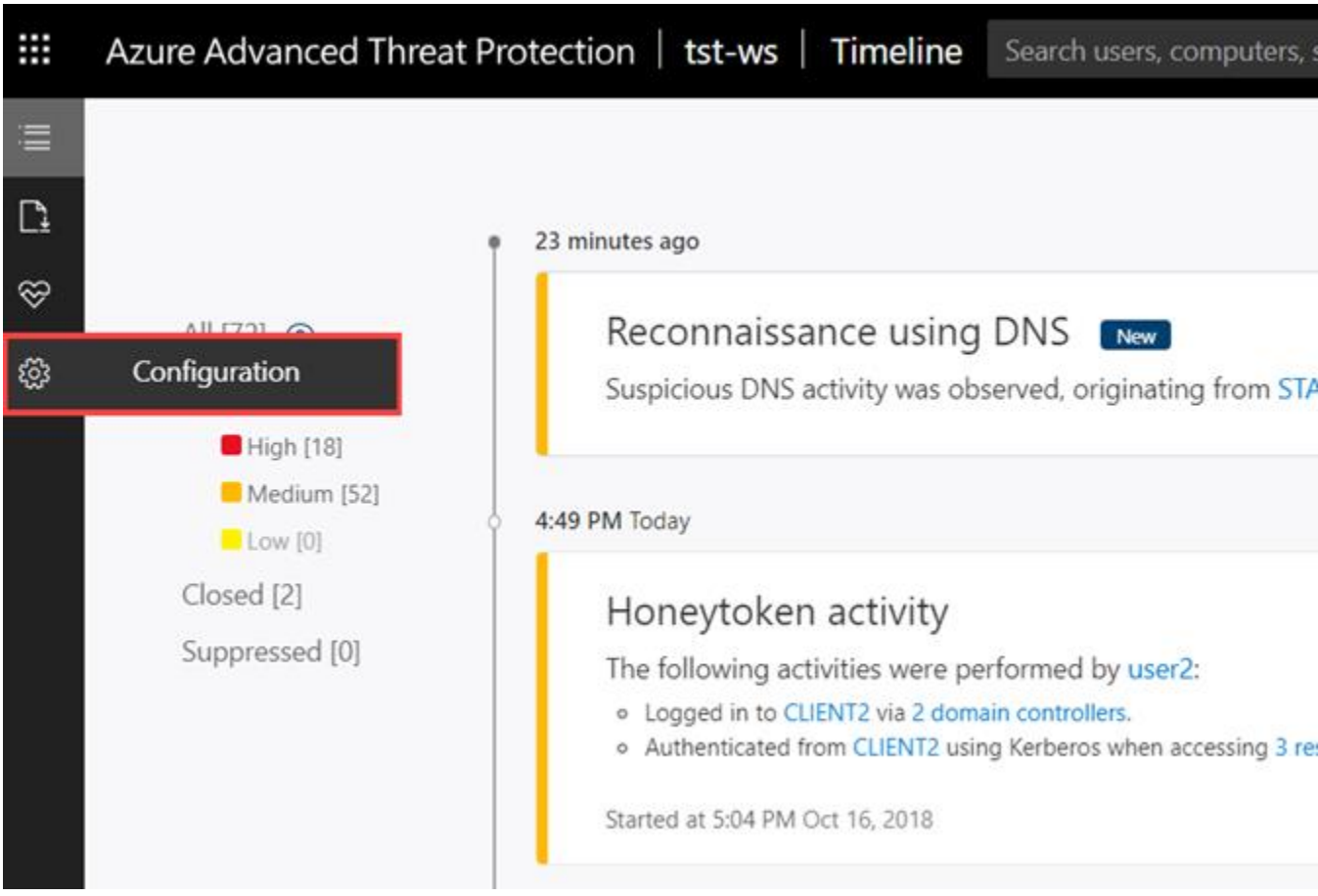
- Behavior-based, cloud-powered, advanced attack detection
  Finds the attacks that made it past all other defenses (post breach detection), provides actionable, correlated alerts for known and unknown adversaries trying to hide their activities on endpoints.
- Rich timeline for forensic investigation and mitigation
  Easily investigate the scope of breach or suspected behaviors on any machine through a rich machine timeline. File, URLs, and network connection inventory across the network. Gain additional insight using deep collection and analysis ("detonation") for any file or URLs.
- Built in unique threat intelligence knowledge base
  Unparalleled threat optics provides actor details and intent context for every threat intelligence based detection – combining first and third-party intelligence sources.

Prerequisites

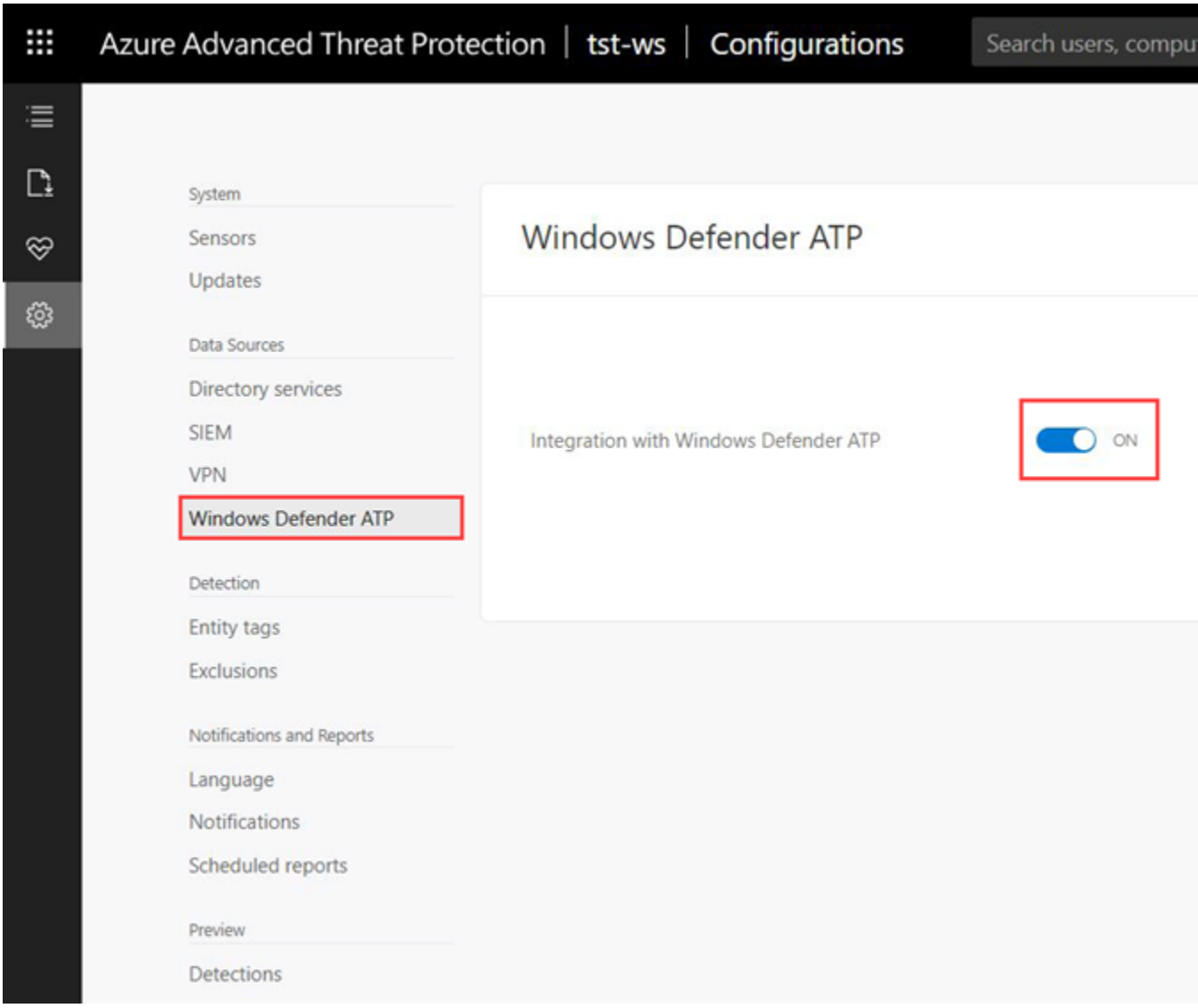
To enable this feature, you need a license for both Azure ATP and Windows Defender ATP.

How to integrate Azure ATP with Windows Defender ATP

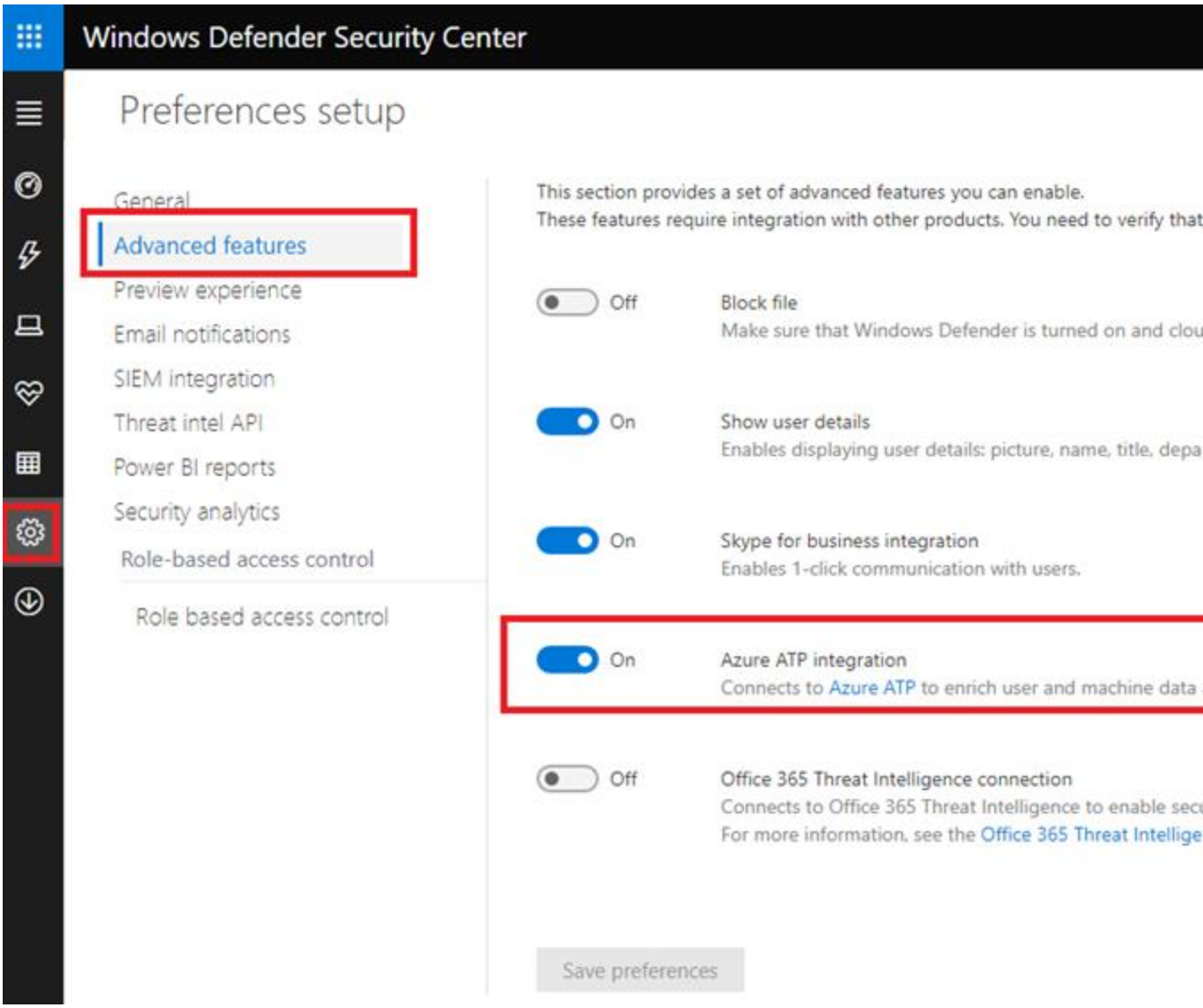
1. In the Azure ATP portal, open **Configuration**.



2. In the Configurations list, select **Windows Defender ATP** and set the integration toggle to **On**.



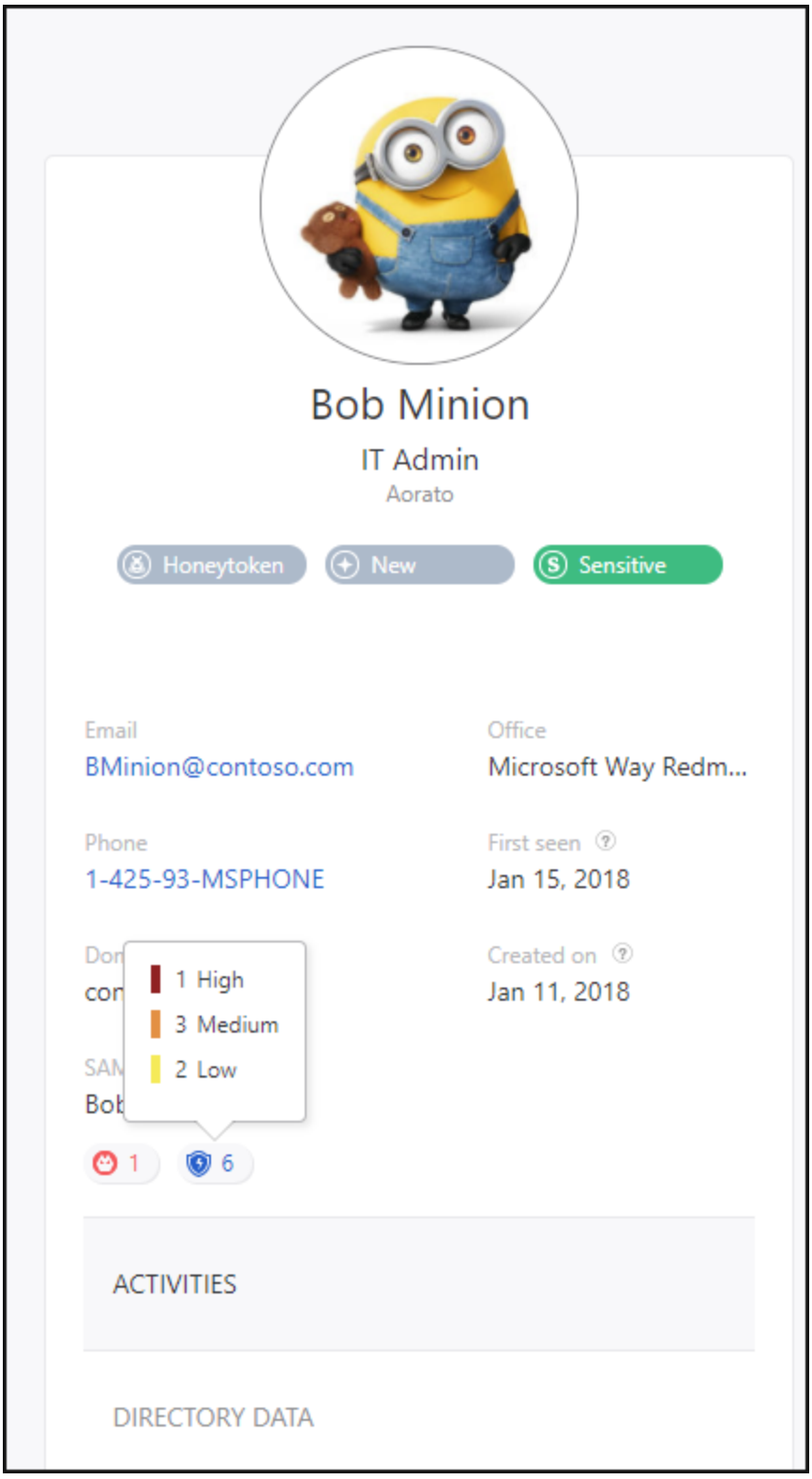
3. In the Windows Defender ATP portal, go to **Settings**, **Advanced features** and set **Azure ATP integration** to **ON**.



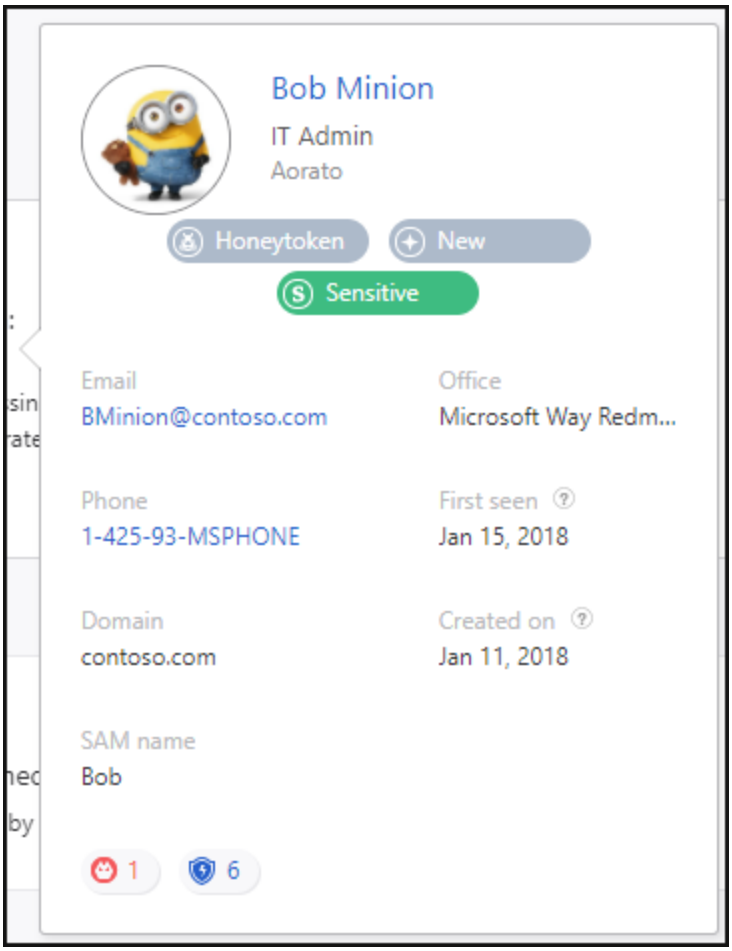
4. To check the status of the integration, in the Azure ATP portal, go to **Settings** > **Windows Defender ATP integration**. You can see the status of the integration and if something is wrong, you'll see an error.

How it works

After Azure ATP and Windows Defender ATP are fully integrated, in the Azure ATP portal, in the mini-profile pop-up and in the entity profile page, each entity that exists in Windows Defender ATP includes a badge to show that it is integrated with Windows Defender ATP.



If the entity contains alerts in Windows Defender ATP, there is a number next to the badge to let you know how many alerts were raised.

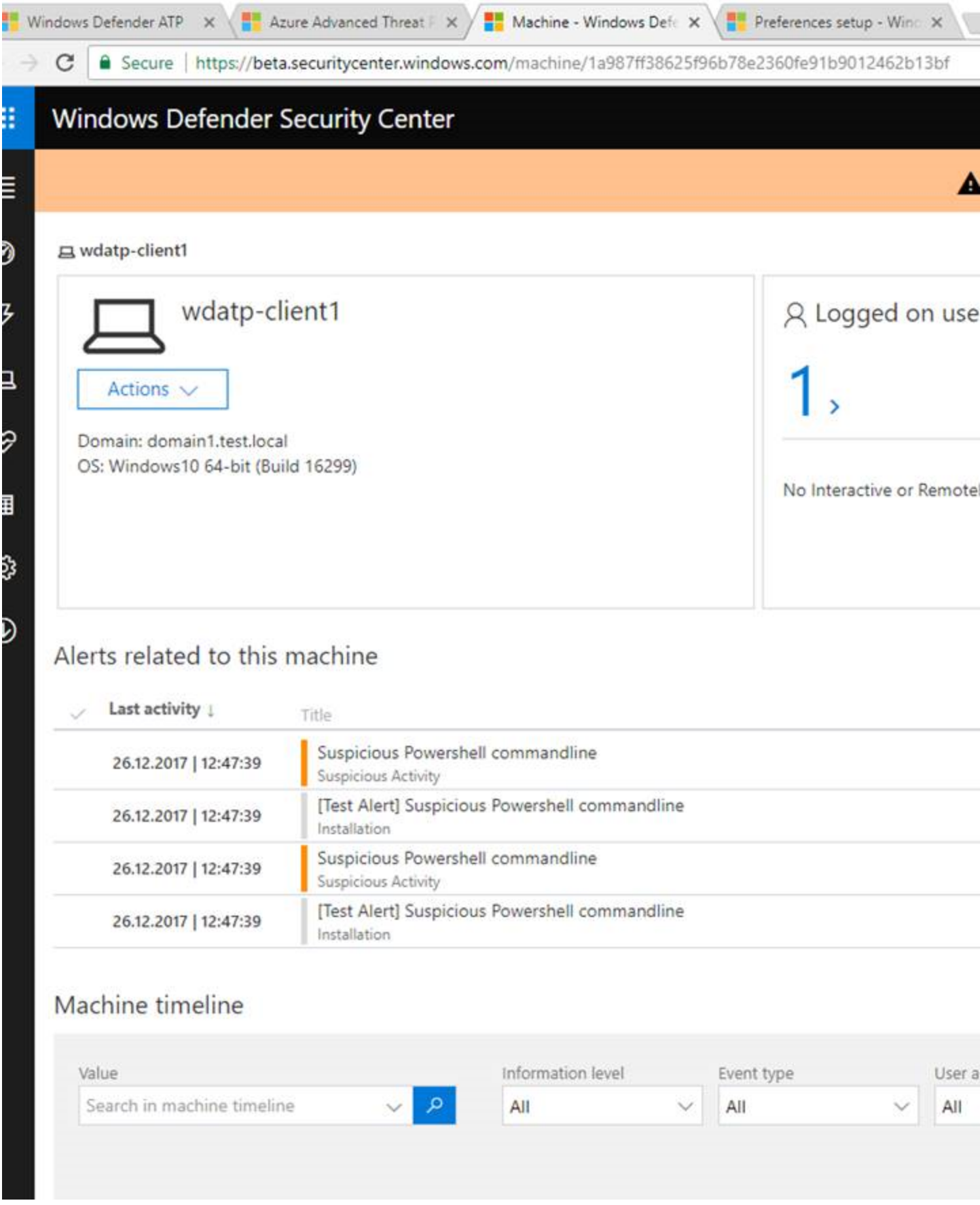


If you click on the badge, you are brought to the Windows Defender ATP portal where you can view and mitigate the alerts. If the entity is not recognized by Windows Defender ATP, the badge is grayed out.

From the Windows Defender ATP portal, click on an endpoint to view Azure ATP alerts. If you click on the alerts for this entity in Windows Defender ATP, the entity's profile page opens in Azure ATP.

Note

Currently, Azure ATP integration with Windows Defender ATP supports only users and machines from the on-premises AD. Users from Azure AD and virtual machines that are managed in Azure will not be displayed as part of the integration


Windows Defender ATP
Azure Advanced Threat
Machine - Windows Def
Preferences setup - Win
Secure | https://beta.securitycenter.windows.com/machine/1a987ff38625f96b78e2360fe91b9012462b13bf
Windows Defender Security Center
wdatp-client1
wdatp-client1
Actions
Domain: domain1.test.local
OS: Windows10 64-bit (Build 16299)
Logged on use
1
No Interactive or Remotel
Alerts related to this machine
Last activity
Title
26.12.2017 | 12:47:39
Suspicious Powershell commandline
Suspicious Activity
26.12.2017 | 12:47:39
[Test Alert] Suspicious Powershell commandline
Installation
26.12.2017 | 12:47:39
Suspicious Powershell commandline
Suspicious Activity
26.12.2017 | 12:47:39
[Test Alert] Suspicious Powershell commandline
Installation
Machine timeline
Value
Search in machine timeline
Information level
All
Event type
All
User a
All