Prepare Intune for Windows Defender ATP

Configure Microsoft Defender ATP via Intune

BY ESHLOMO *ON* 18/03/2019 • (1)

Microsoft Defender Advanced Threat Protection is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Microsoft Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

Endpoint behavioral sensors Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Windows Defender ATP.
Cloud security analytics Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, 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, and procedures, and generate alerts when these are observed in collected sensor data.

With Intune, you can configure Microsoft Defender ATP as compliance for your environment. This means you can give the device access to your corporate resource by the status of Microsoft Defender ATP, based on risk scores.

If the device is not healthy or has to high-risk score in ATP then the access to the resources will be blocked by Azure Intune. Microsoft Defender ATP help prevents security breaches and helps limit the impact within your organization.

You need Microsoft Defender ATP subscription. This subscription has to be connected with Azure Intune. These are the steps on how to connect with Microsoft Defender ATP.

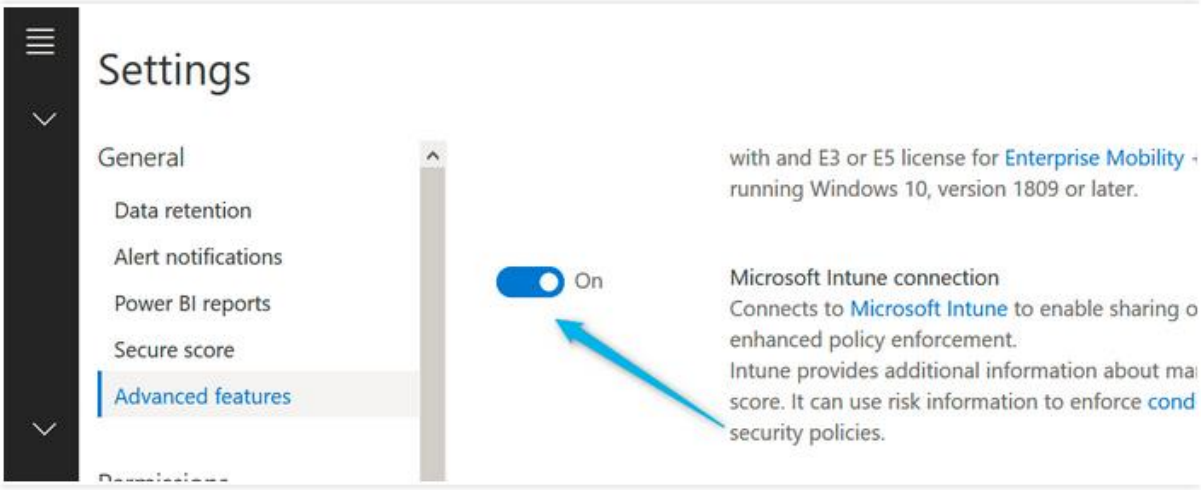
If you don't have a Microsoft Defender ATP subscription, you can create a trial subscription and use this one to connect with your Azure Intune environment.

How to Configure

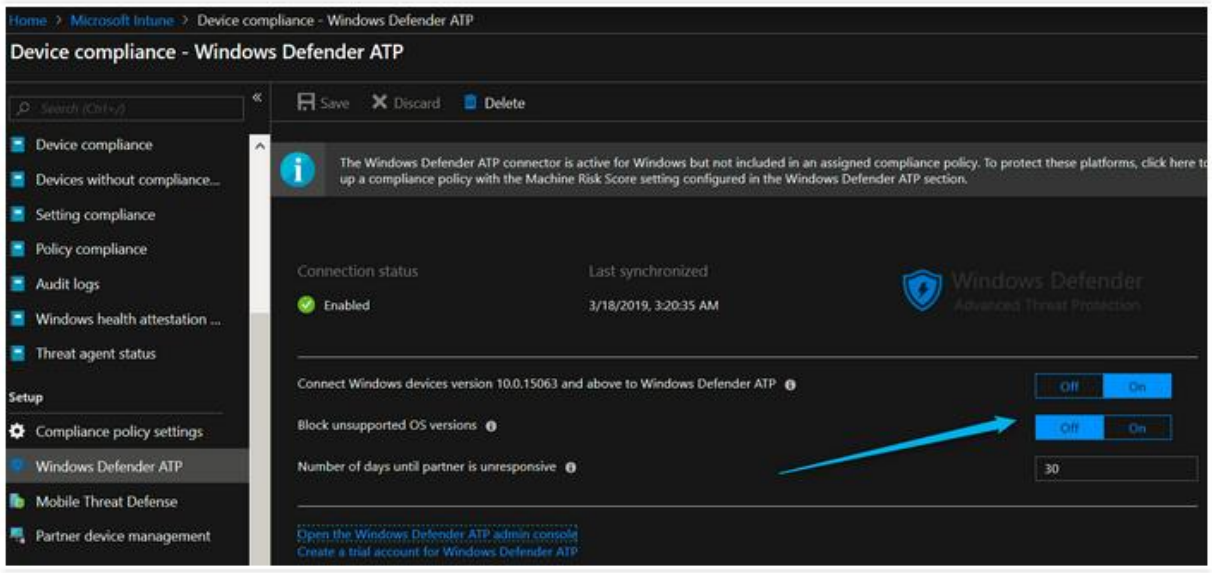
The following actions based on Microsoft Defender ATP and Intune integration with no requirements for onboarding files (the onboarding script already configured via SCCM)

- Go to Azure Intune portal -> Device compliance -> Microsoft Defender ATP and choose configure Windows Defender ATP
- Then click on the link Connect Microsoft Defender AP to Microsoft Intune in the Microsoft Defender Security Center.

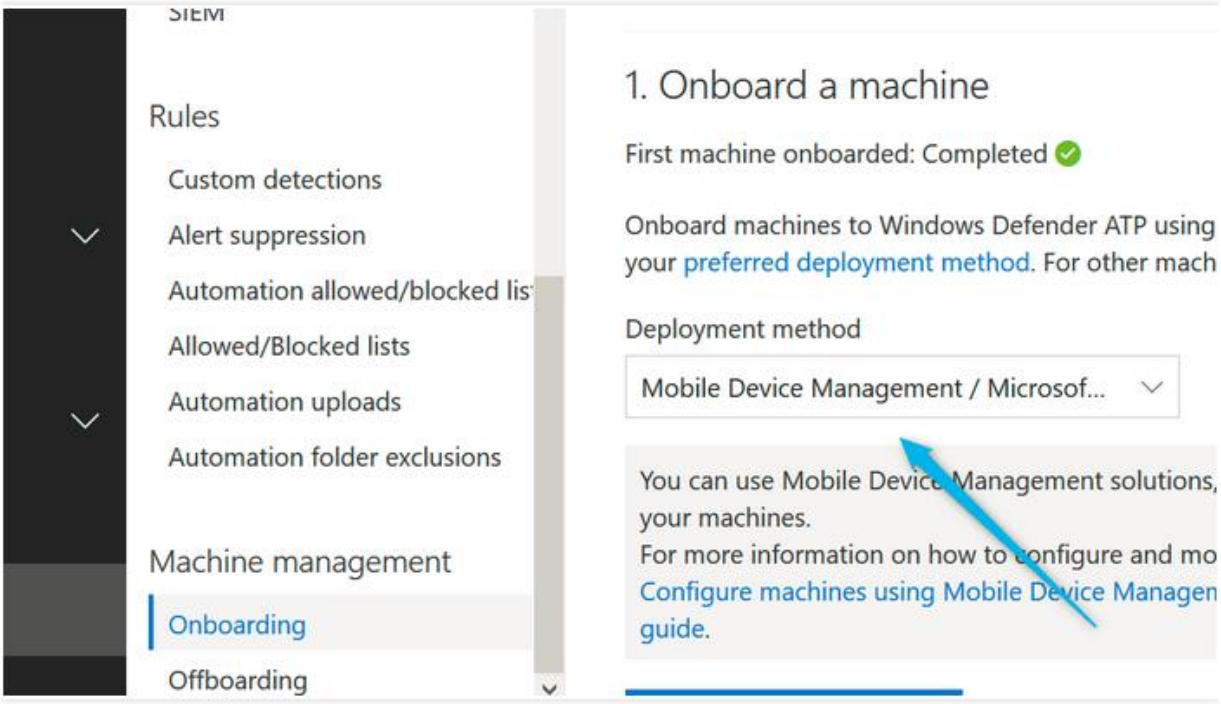
- Turn on the Microsoft Intune connection and click on the Save preference button



- Go back to the Azure and Intune portal and click on the refresh button, the connection has been made and the status is available. The status will change to Connected later.

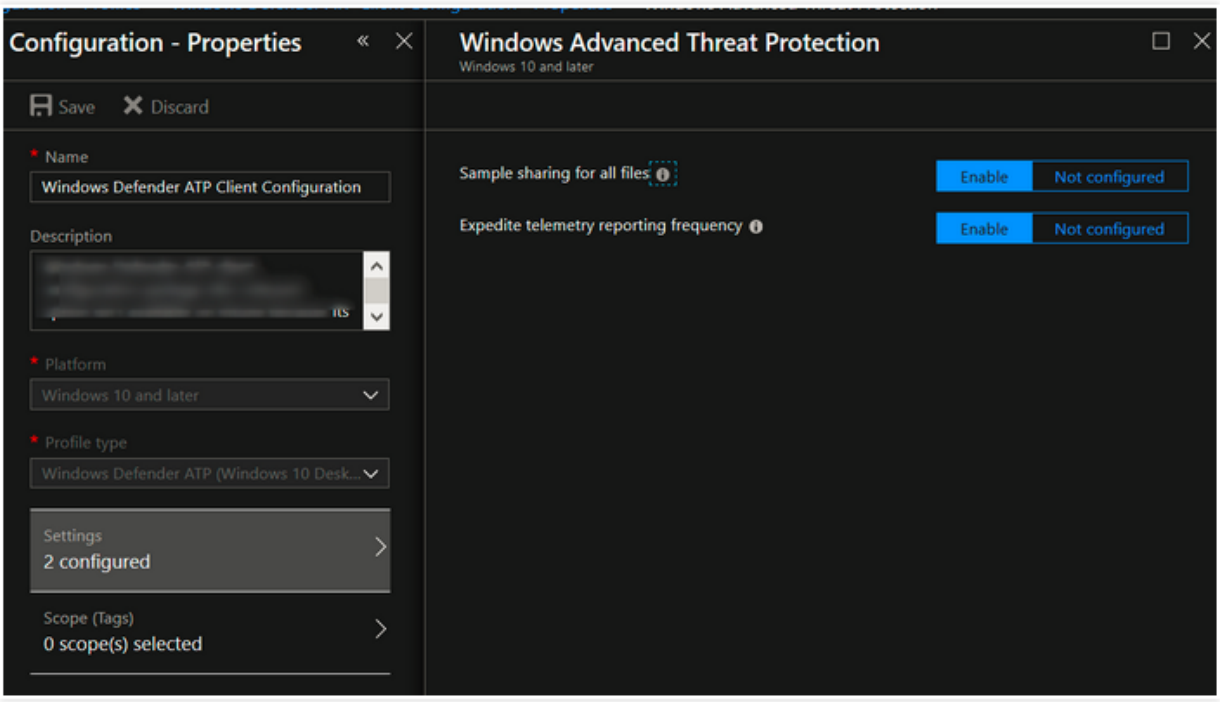


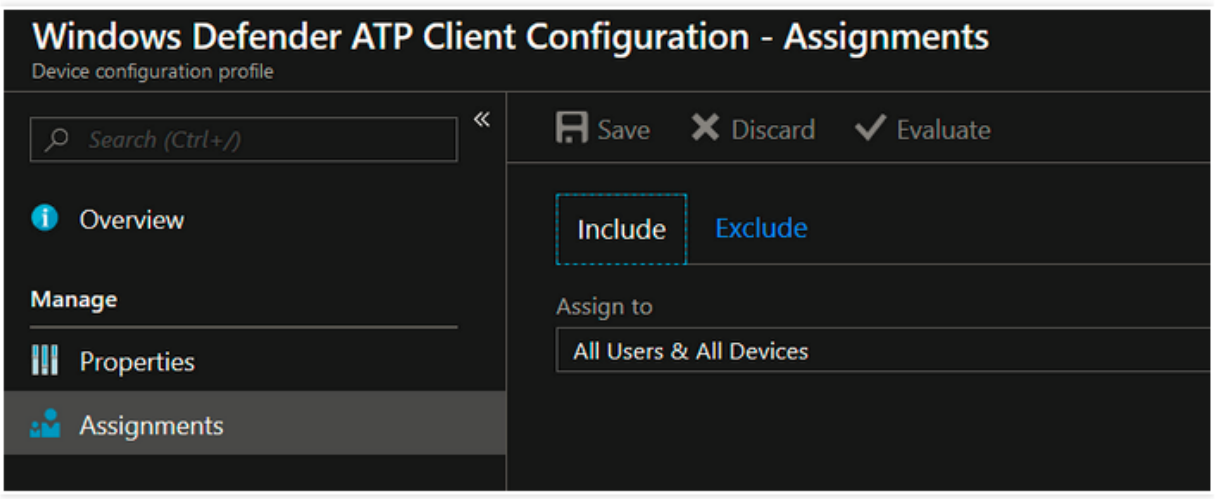
- Turn on the options Connect Microsoft devices and click on the save button.
- The next step is to onboard your test device into Microsoft Defender ATP. Go to the Microsoft ATP dashboard/portal: https://securitycenter.windows.com/



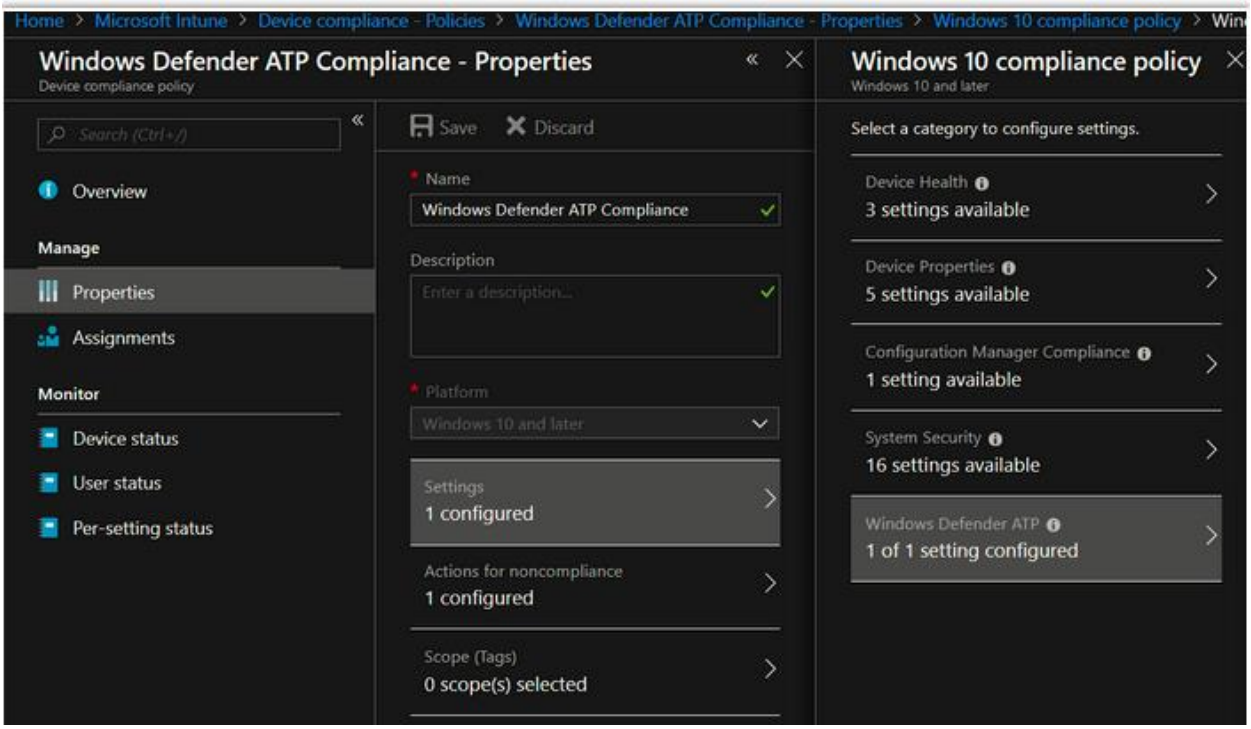
- Now go to the Azure Intune portal. You need to create a new device configuration profile. From Azure Intune portal -> Device Configuration -> Profiles

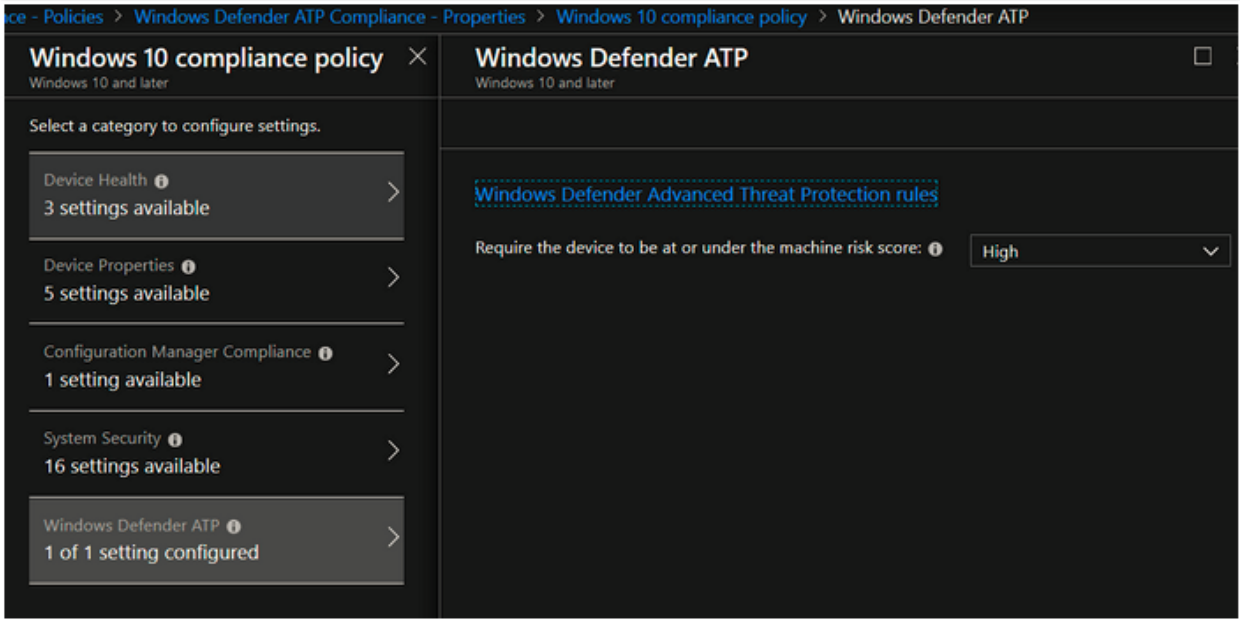
- Name the profile. The platform is Windows 10 and later. Profile type is Microsoft Defender ATP with Windows 10 Desktop.





- Then you have to make a new compliance policy based on device health. Go back and go to Device compliance -> Policies. Click on the Create Policy button.





You have got a few options to choose from:

Secured: This level is the most secure. The device cannot have any existing threats and still access company resources. If any threats are found, the device is evaluated as noncompliant.
Low: The device is compliant if only low-level threats exist. Devices with medium or high threat levels are not compliant.

Medium: The device is compliant if the threats found on the device are low or medium. If high-level threats are detected, the device is determined as noncompliant.
High: This level is the least secure, and allows all threat levels. So devices that with high, medium or low threat levels are considered compliant.

Next, go to the Windows Defender ATP portal. Click Machines list in the menu. Here you have to see your device.

If not, then you have to wait longer. The devices must be on this list. The device is now also managed by Windows Defender ATP