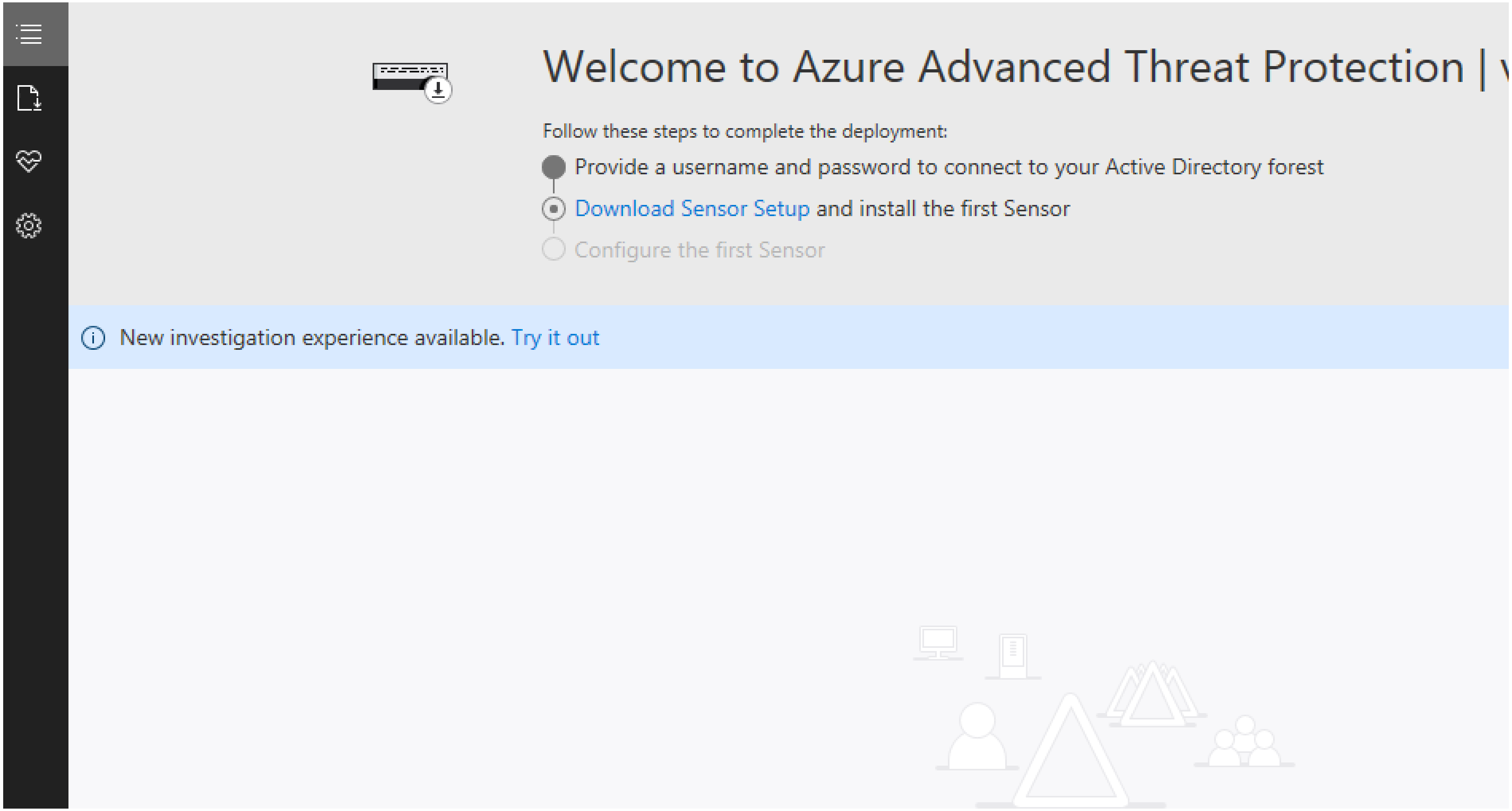
INSTALLING AZURE ATP

Azure ATP monitors your domain controllers by capturing and parsing network traffic and leveraging Windows events directly from your domain controllers, then analyzes the data for attacks and threats.

Utilizing profiling, deterministic detection, machine learning, and behavioral algorithms Azure ATP learns about your network, enables detection of anomalies, and warns you of suspicious activities.



Welcome to Azure Advanced Threat Protection | v

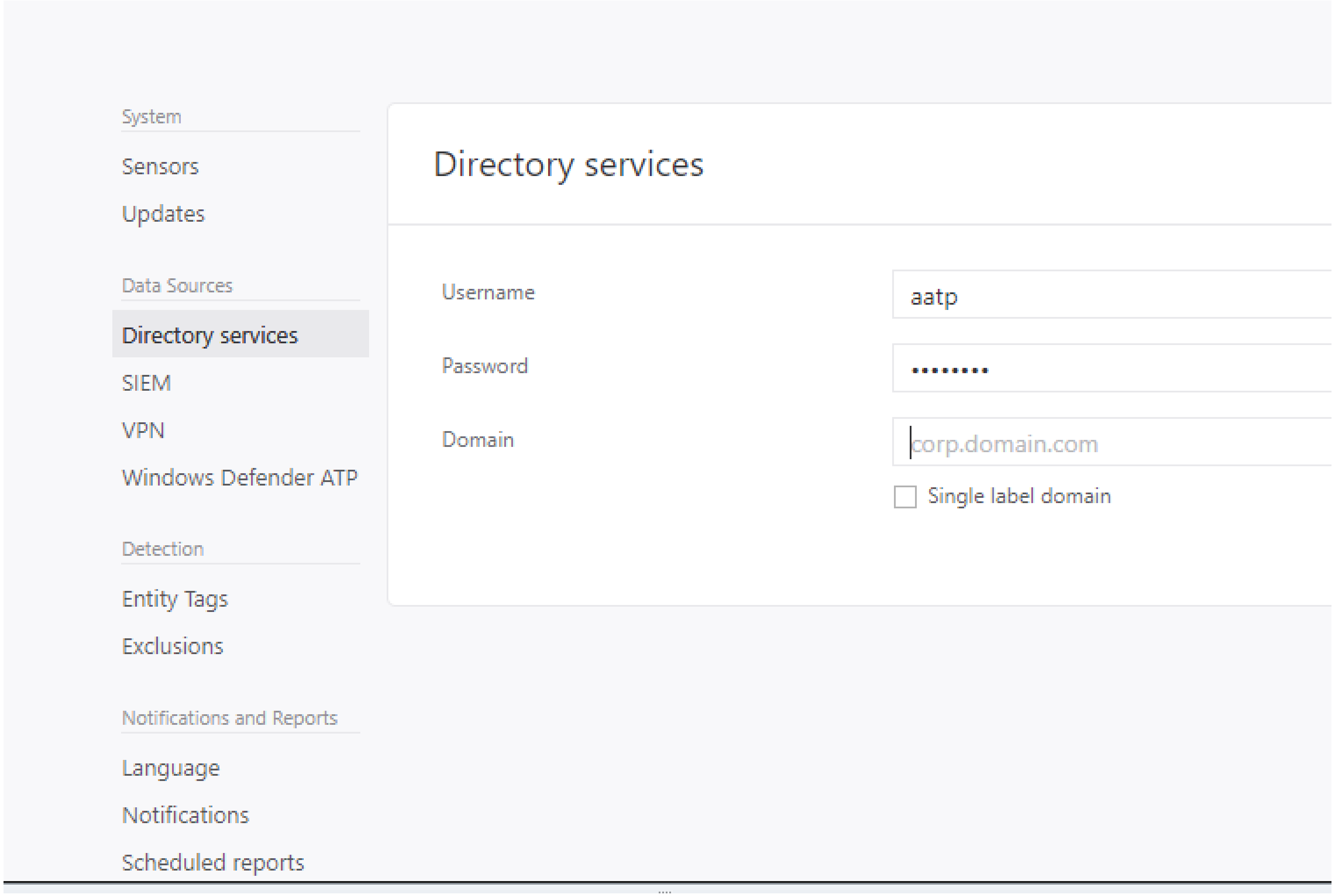
Follow these steps to complete the deployment:

● Provide a username and password to connect to your Active Directory forest

◉ Download Sensor Setup and install the first Sensor

○ Configure the first Sensor

ⓘ New investigation experience available. Try it out



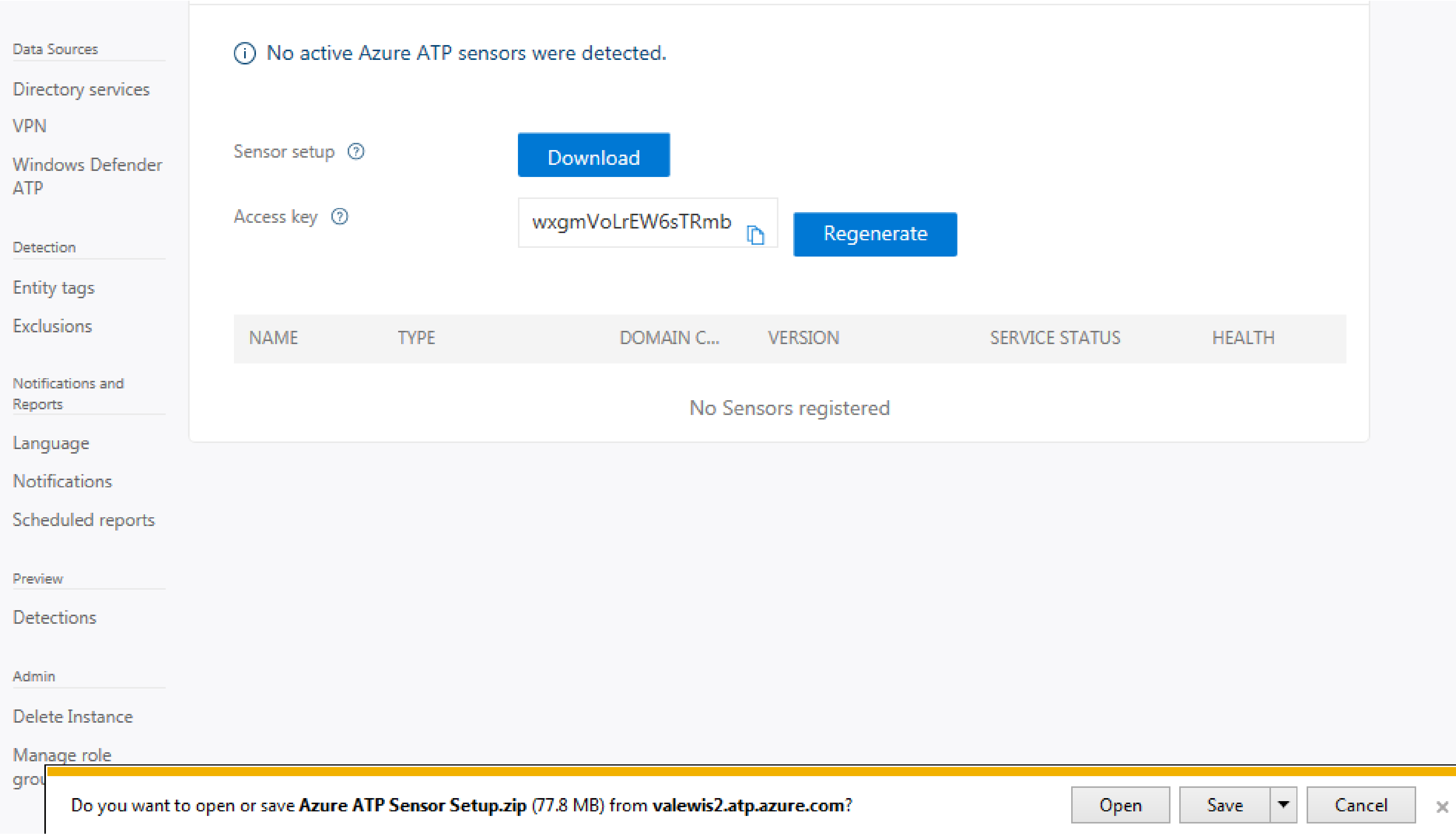
Directory services

Username: aatp

Password: •••••••••

Domain: corp.domain.com

□ Single label domain



ⓘ No active Azure ATP sensors were detected.

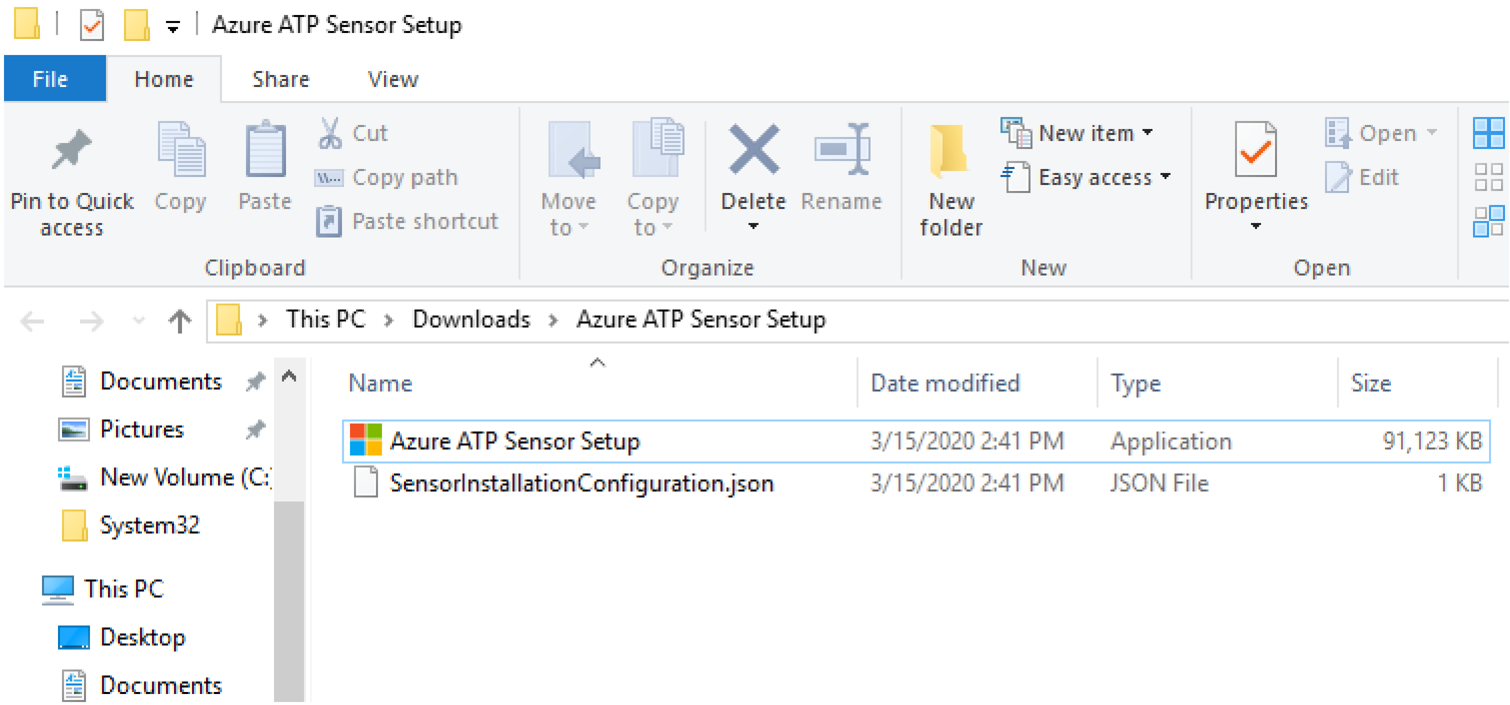
Sensor setup ⓘ **Download**

Access key ⓘ wxgmVoLrEW6sTRmb **Regenerate**

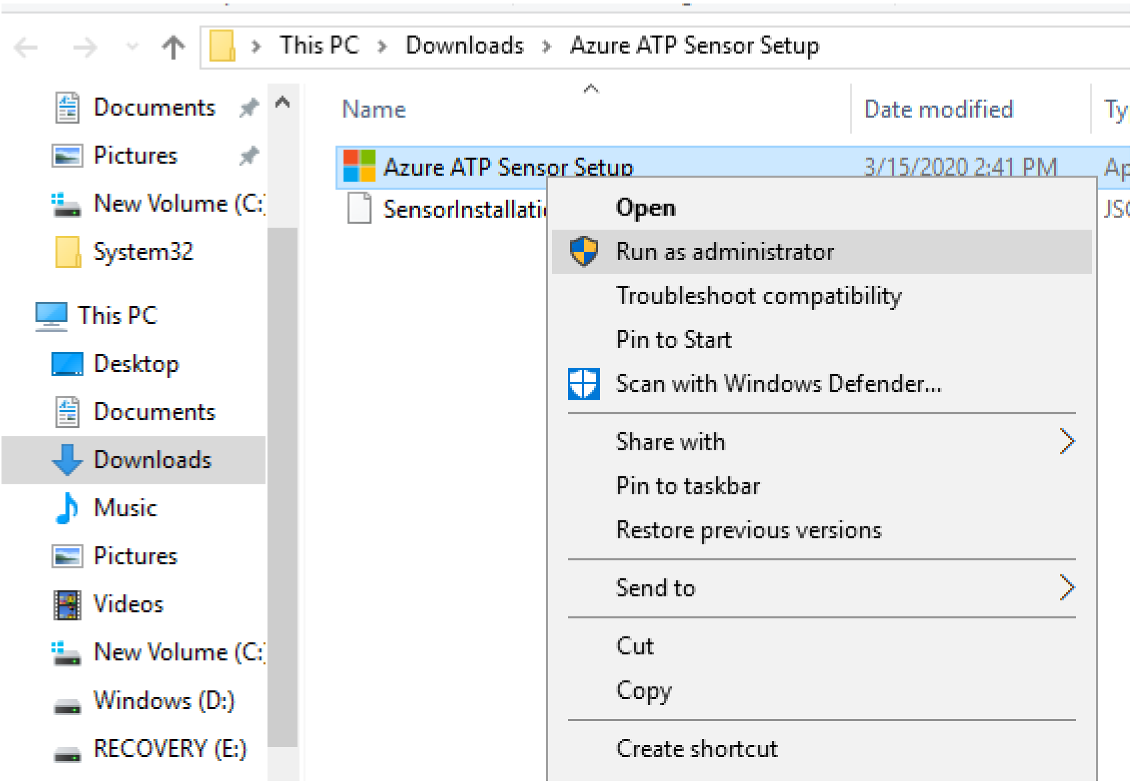
NAME	TYPE	DOMAIN C...	VERSION	SERVICE STATUS	HEALTH

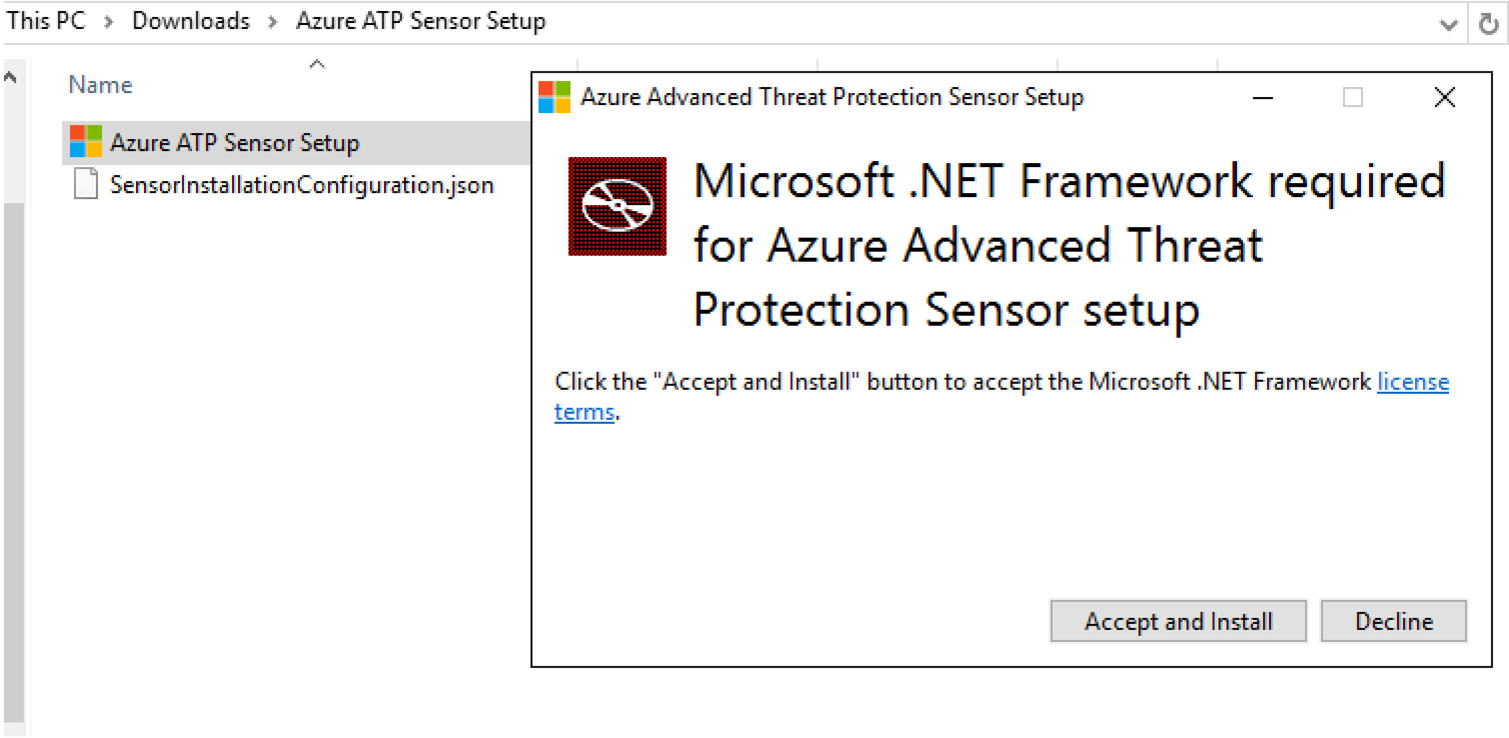
No Sensors registered

Do you want to open or save **Azure ATP Sensor Setup.zip** (77.8 MB) from **valewis2.atp.azure.com**?



Name	Date modified	Type	Size
Azure ATP Sensor Setup	3/15/2020 2:41 PM	Application	91,123 KB
SensorInstallationConfiguration.json	3/15/2020 2:41 PM	JSON File	1 KB


This PC › Downloads › Azure ATP Sensor Setup
Documents
Pictures
New Volume (C:)
System32
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
New Volume (C:)
Windows (D:)
RECOVERY (E:)
Name
Date modified
Ty
Azure ATP Sensor Setup
3/15/2020 2:41 PM
Ap
SensorInstallati
JS(
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
Scan with Windows Defender...
Share with
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut



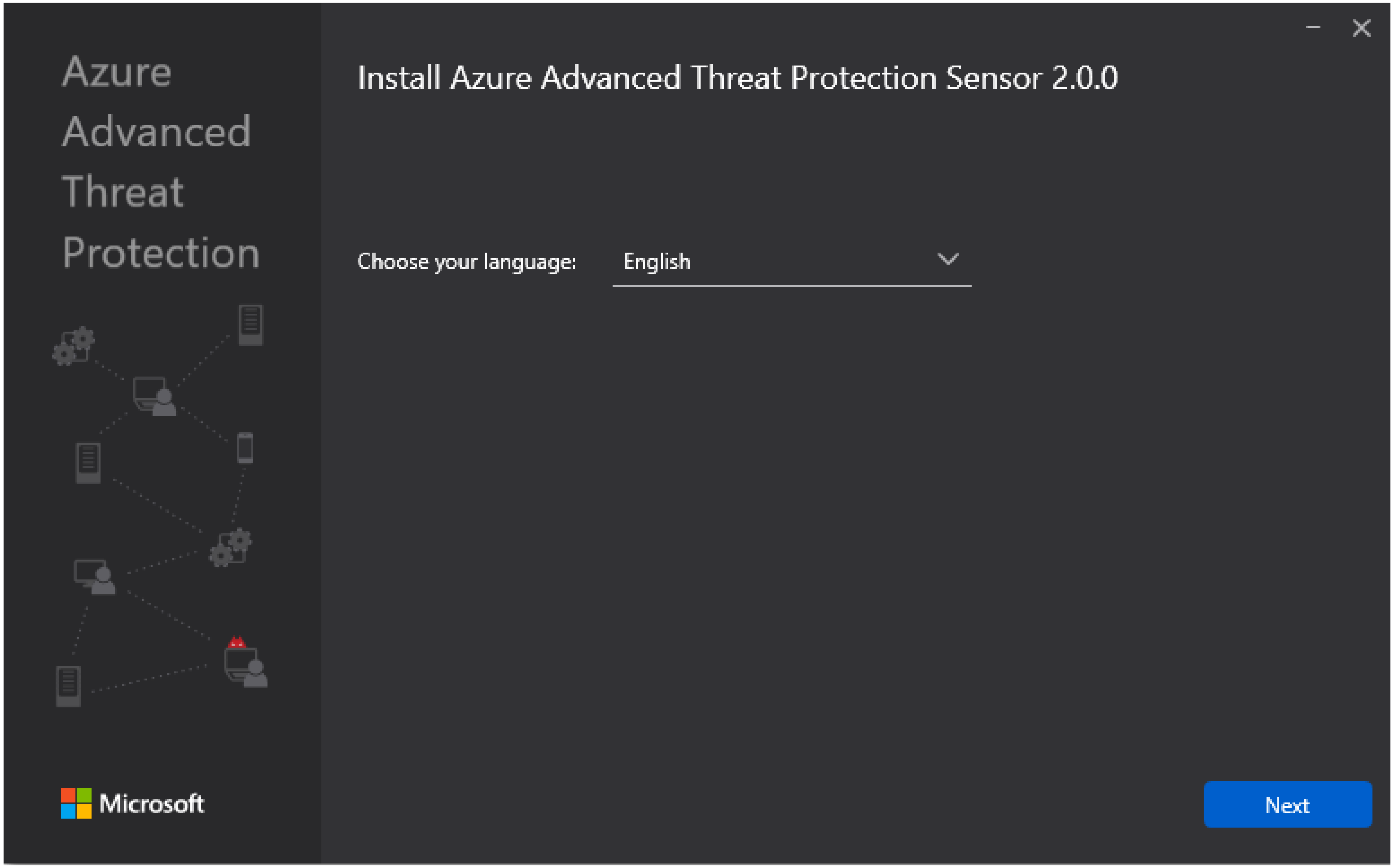
This PC > Downloads > Azure ATP Sensor Setup
Name
Azure ATP Sensor Setup
SensorInstallationConfiguration.json

Azure Advanced Threat Protection Sensor Setup

Microsoft .NET Framework required for Azure Advanced Threat Protection Sensor setup

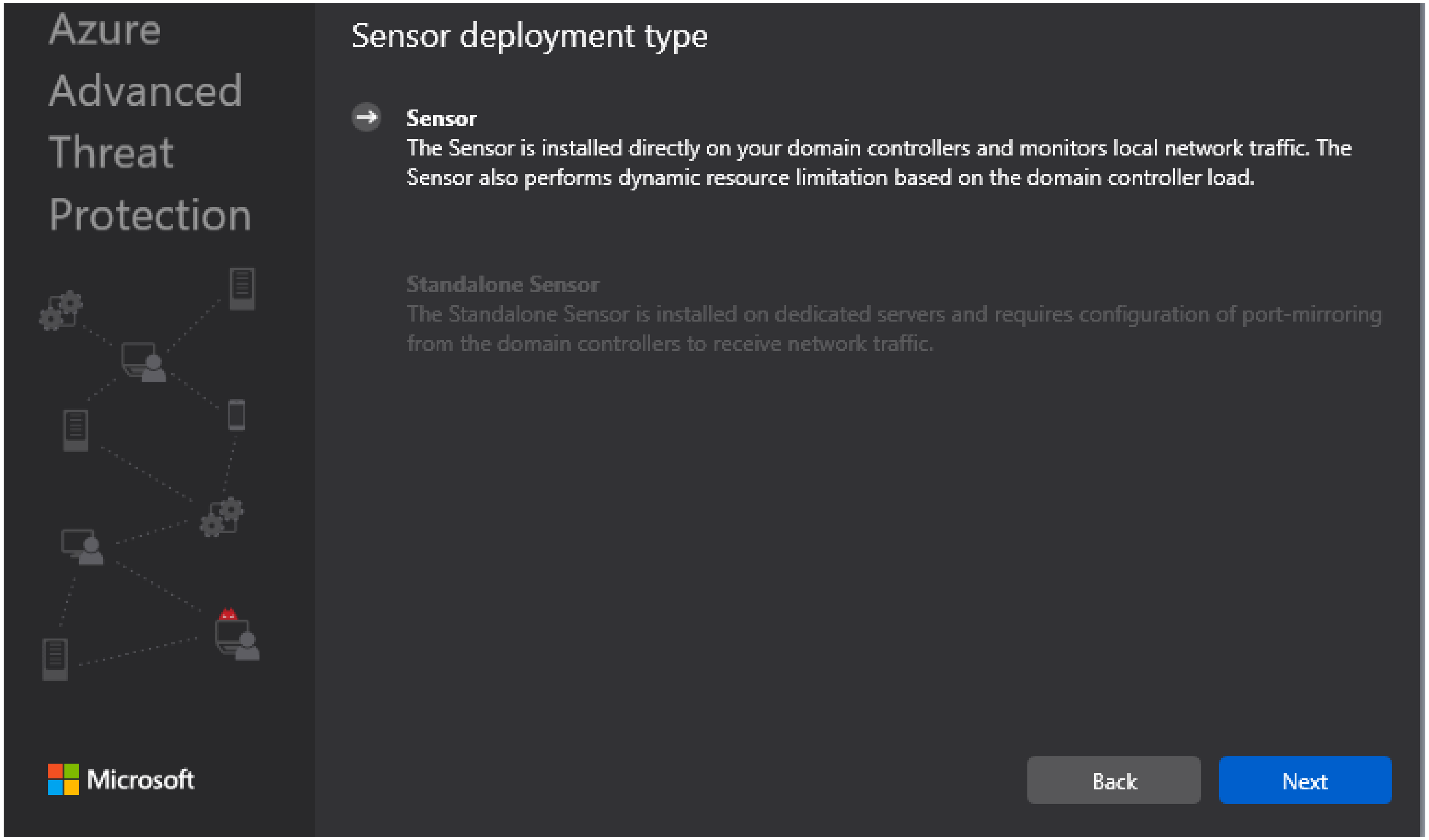
Click the "Accept and Install" button to accept the Microsoft .NET Framework license terms.

Accept and Install
Decline



Install Azure Advanced Threat Protection Sensor 2.0.0

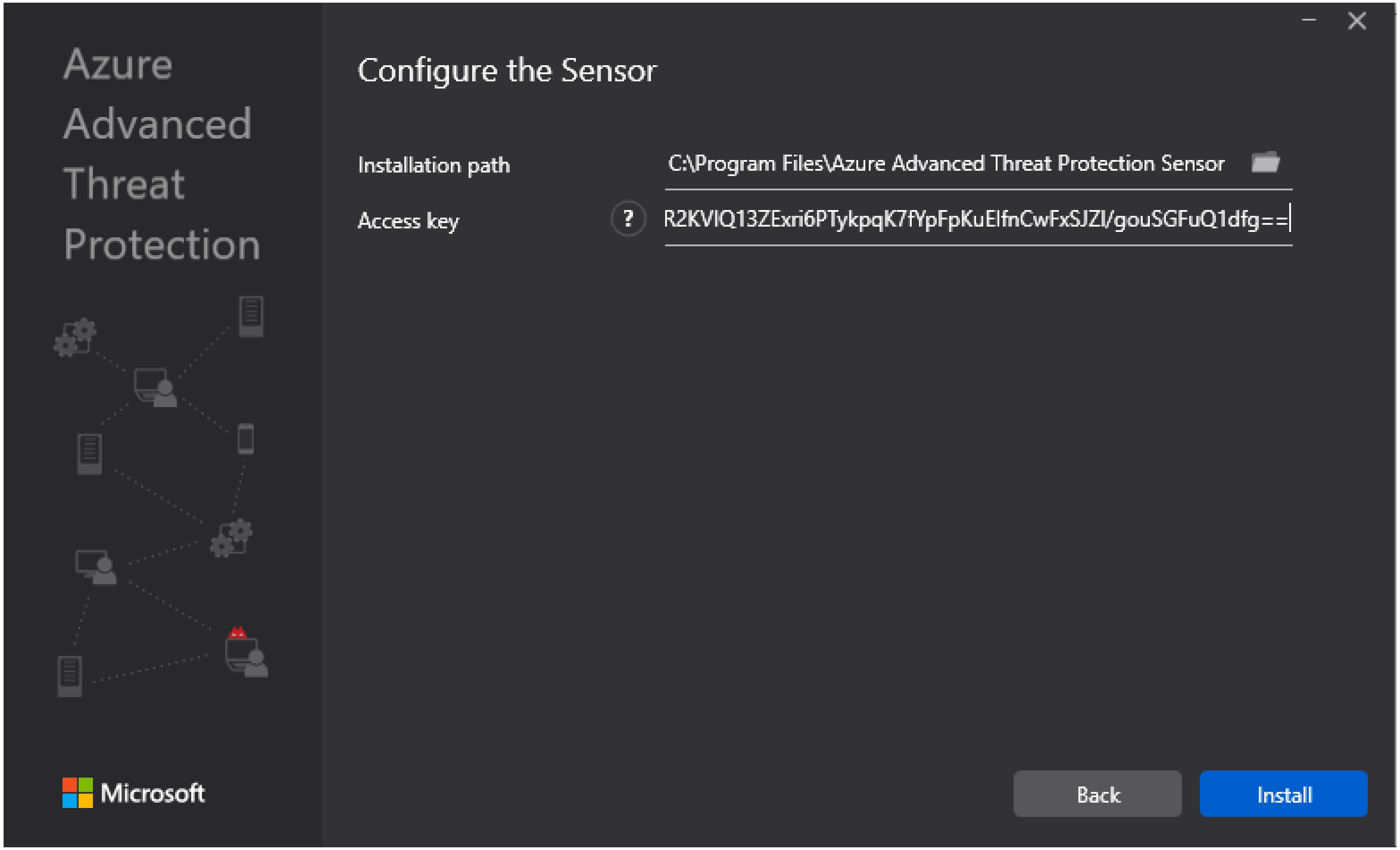
Choose your language: English



Sensor deployment type

→ **Sensor**
The Sensor is installed directly on your domain controllers and monitors local network traffic. The Sensor also performs dynamic resource limitation based on the domain controller load.

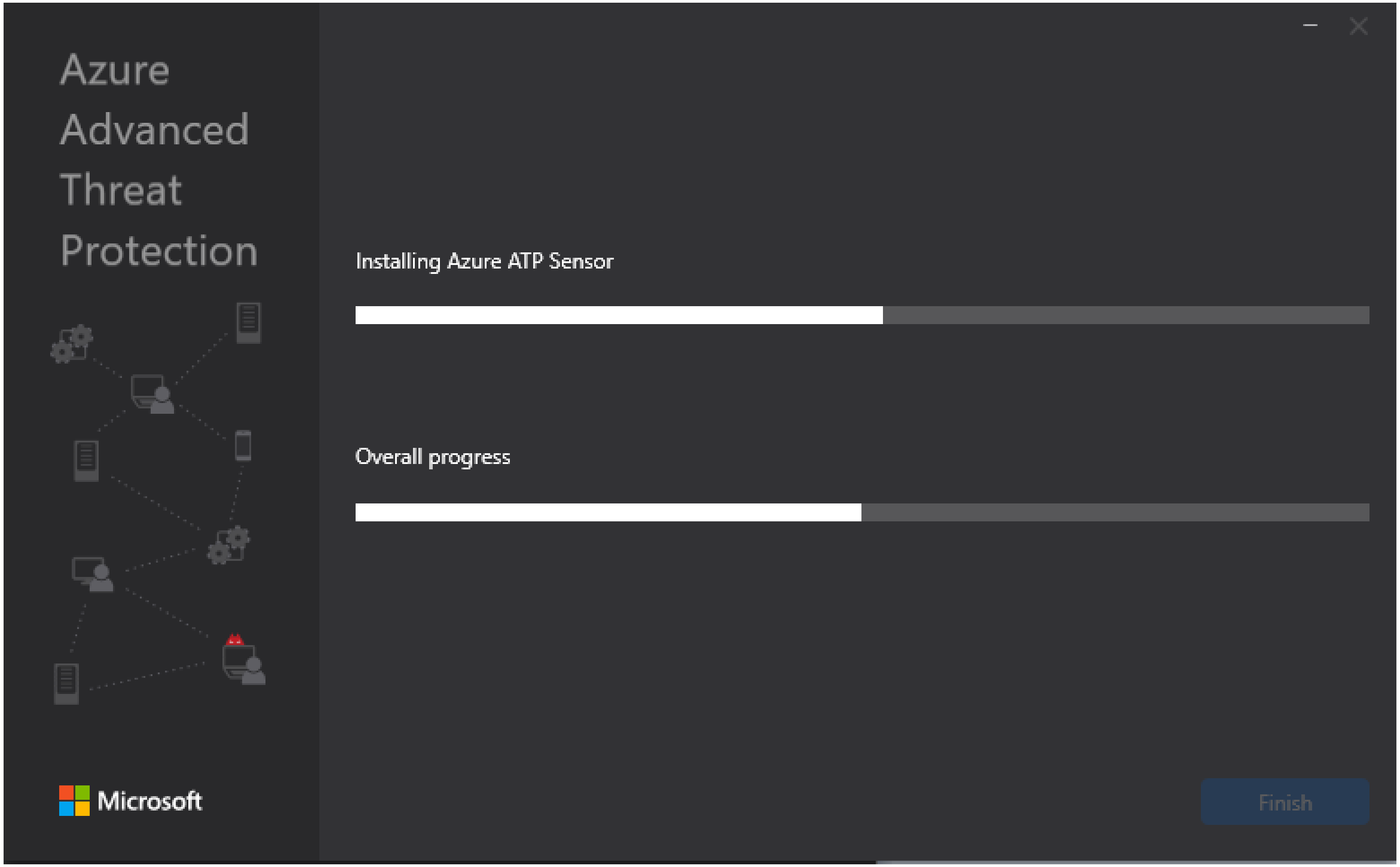
Standalone Sensor
The Standalone Sensor is installed on dedicated servers and requires configuration of port-mirroring from the domain controllers to receive network traffic.



Configure the Sensor

Installation path C:\Program Files\Azure Advanced Threat Protection Sensor

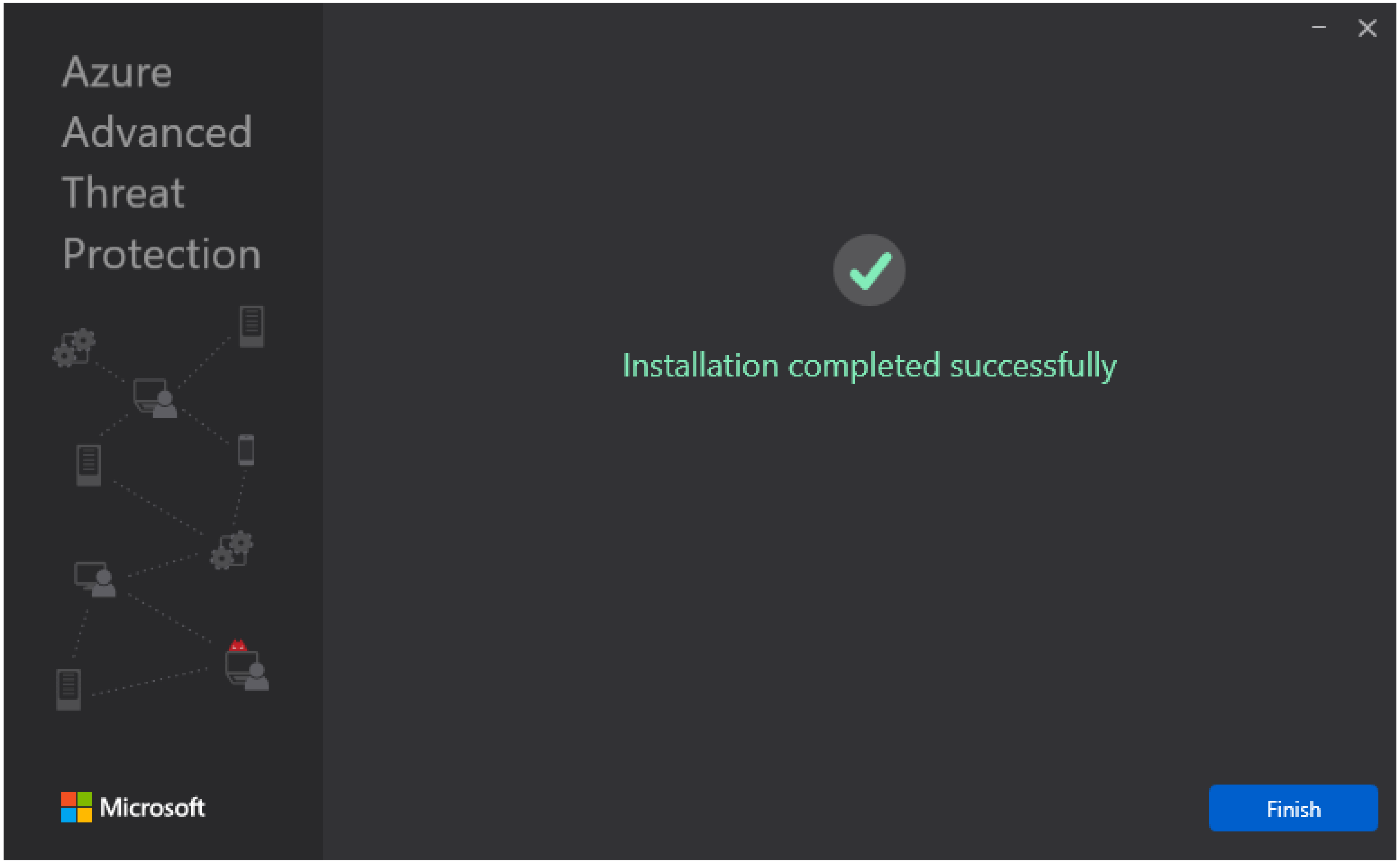
Access key R2KVIQ13ZExri6PTykpqK7fYpFpKuElfnCwFxSJZI/gouSGFuQ1dfg==



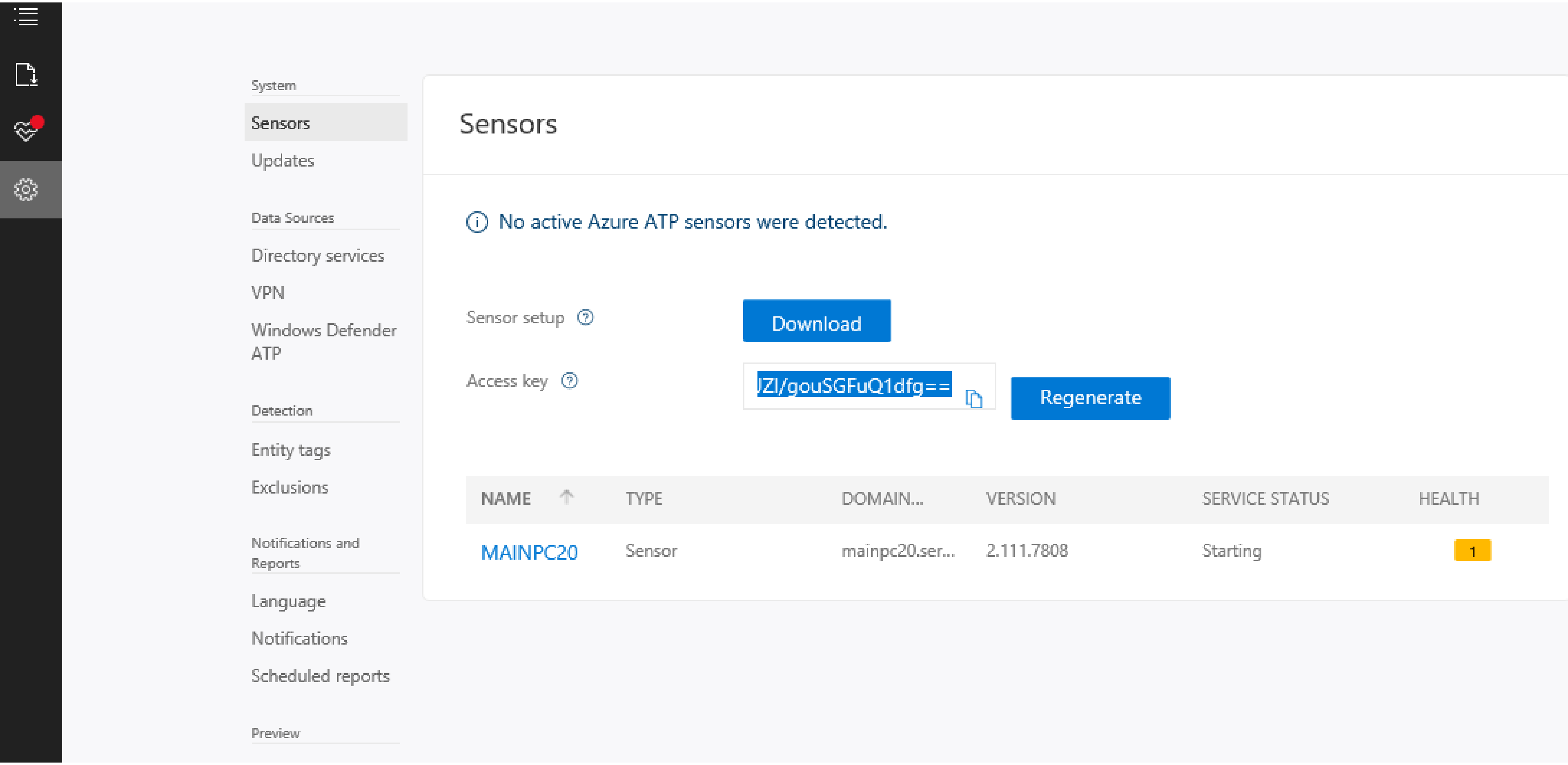
Azure Advanced Threat Protection

Installing Azure ATP Sensor

Overall progress



Installation completed successfully



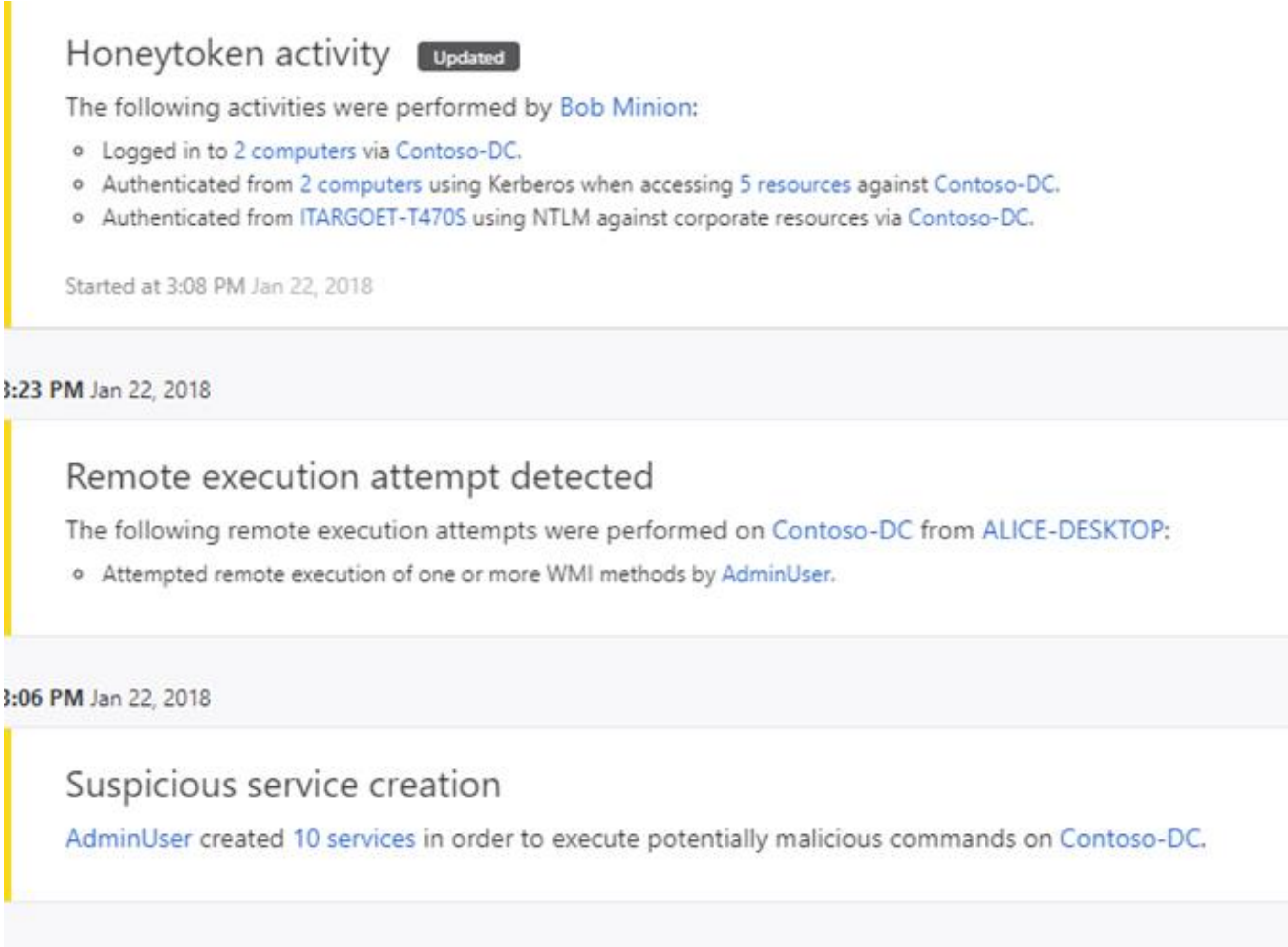
Sensors

ⓘ No active Azure ATP sensors were detected.

Sensor setup ⓘ

Access key ⓘ JZI/gouSGFuQ1dfg==

NAME ↑	TYPE	DOMAIN...	VERSION	SERVICE STATUS	HEALTH
MAINPC20	Sensor	mainpc20.ser...	2.111.7808	Starting	1



Honeytoken activity

The following activities were performed by Bob Minion:

- Logged in to 2 computers via Contoso-DC.
- Authenticated from 2 computers using Kerberos when accessing 5 resources against Contoso-DC.
- Authenticated from ITARGOET-T470S using NTLM against corporate resources via Contoso-DC.

Started at 3:08 PM Jan 22, 2018

3:23 PM Jan 22, 2018

Remote execution attempt detected

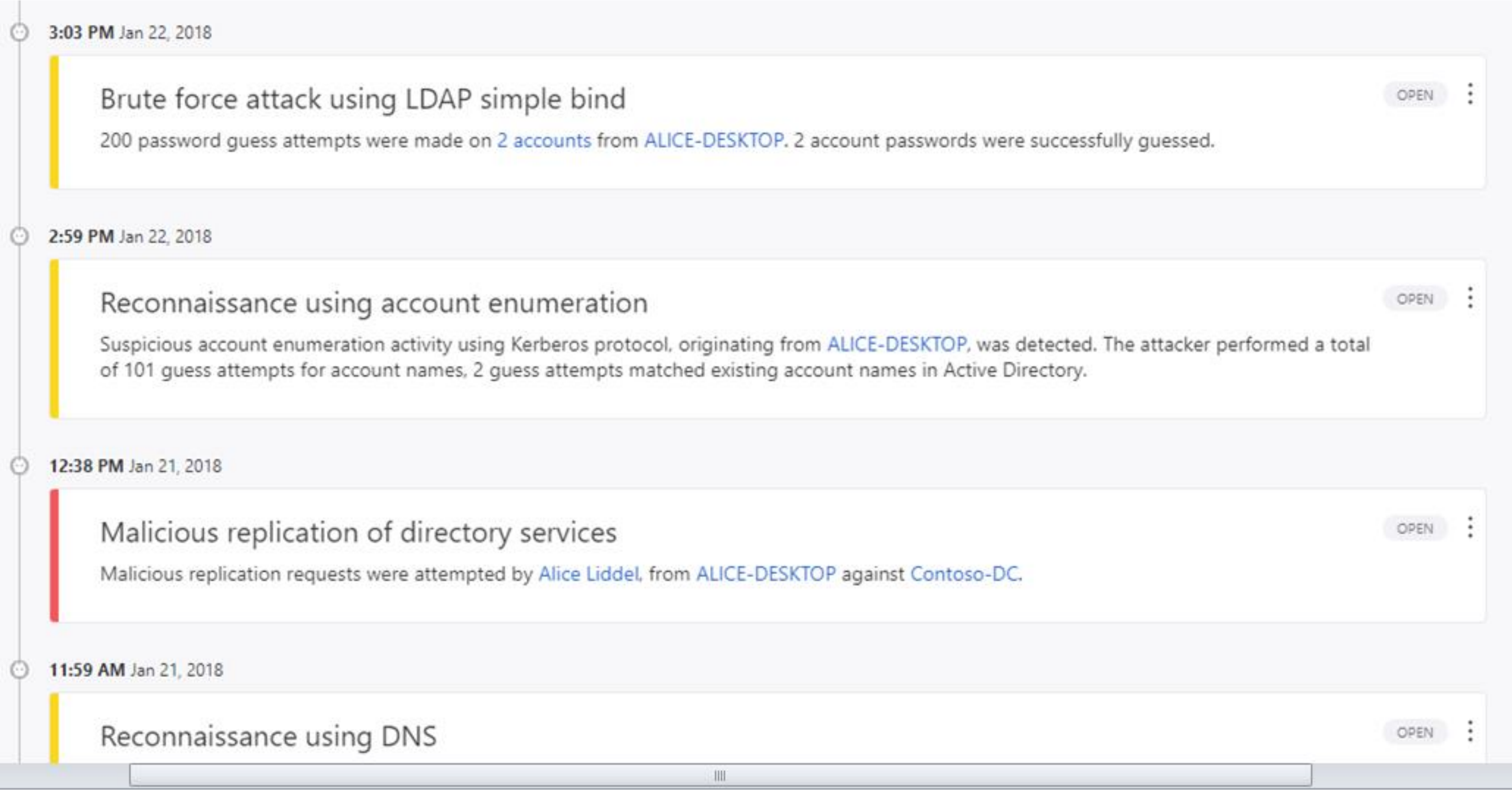
The following remote execution attempts were performed on Contoso-DC from ALICE-DESKTOP:

- Attempted remote execution of one or more WMI methods by AdminUser.

3:06 PM Jan 22, 2018

Suspicious service creation

AdminUser created 10 services in order to execute potentially malicious commands on Contoso-DC.



3:03 PM Jan 22, 2018

Brute force attack using LDAP simple bind

200 password guess attempts were made on 2 accounts from ALICE-DESKTOP. 2 account passwords were successfully guessed.

2:59 PM Jan 22, 2018

Reconnaissance using account enumeration

Suspicious account enumeration activity using Kerberos protocol, originating from ALICE-DESKTOP, was detected. The attacker performed a total of 101 guess attempts for account names, 2 guess attempts matched existing account names in Active Directory.

12:38 PM Jan 21, 2018

Malicious replication of directory services

Malicious replication requests were attempted by Alice Liddel, from ALICE-DESKTOP against Contoso-DC.

11:59 AM Jan 21, 2018

Reconnaissance using DNS