**How to Deploy Azure Advanced Threat Protection**

**High Level Steps:**

Prepare Domain for AATP operation.

Install Sensors for Domain Controllers

Configure AATP

Troubleshoot and Test.

**Prepare Domain for Azure ATP (ATTP):**

Creating The Group Managed Service Accounts (GMSA) For ATTP.

Gmsa's are created in powershell With these steps:

To Create KDS Root Key: (this takes time to replicate through all DCs)

Add-KdsRootKey -EffectiveImmediately

To Create A GMSA Using the New-ADServiceAccount command

steps:

New-ADServiceAccount (name of gmsa)'

* DNSHostName accountname.dnssuffxix
* ManagedPasswordIntervalInDays x

You can add on additional configurations with

Set-adserviceaccount -identity accountname -option etc etc

* PrincipalsAllowedToRetrieveManagedPassword Server group allowed to install gmsa
* KerberosEncryptionType RC4, AES128, AES256 `
* ServicePrincipalNames spns

**Installing Sensor for All Domain Controllers**

Prerequisites For Domain Controllers:

Microsoft .Net Framework 4.7 or later

The following CPU and Random Access Memory (RAM) capacity refers to the sensor’s own consumption, not the domain controller capacity.

Packets per second CPU (cores)\* Memory\*\* (GB)

0-1k 0.25 2.50

1k-5k 0.75 6.00

5k-10k 1.00 6.50

10k-20k 2.00 9.00

20k-50k 3.50 9.50

50k-75k \3.50 9.50

75k-100k 3.50 9.50

The recommended and simplest way to determine capacity for your Azure ATP deployment is to use the Azure ATP Sizing Tool downloadable from Github, see the Domain controller traffic estimator

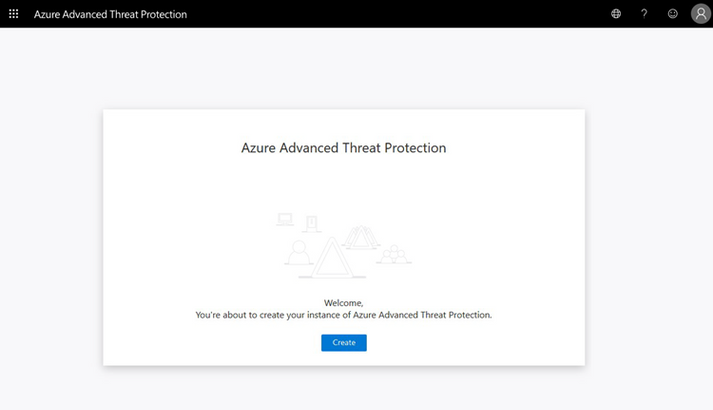
**Sizing tool** - https://gallery.technet.microsoft.com/Azure-Advanced-Threat-a11343c4

**DC Traffic Estimator -** https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning#manual-sizing

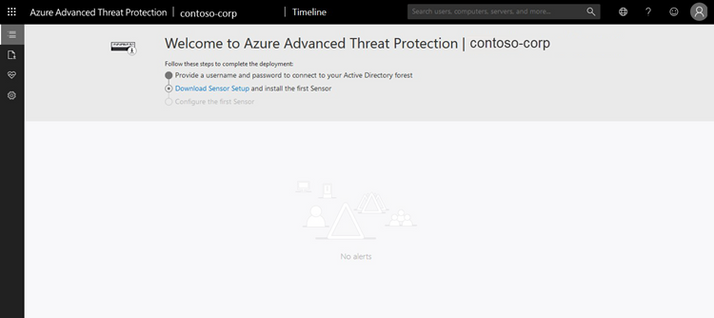
**Create Azure ATP Instance**

Sign in to https://portal.atp.azure.com with the Azure Account used as AATP administrator

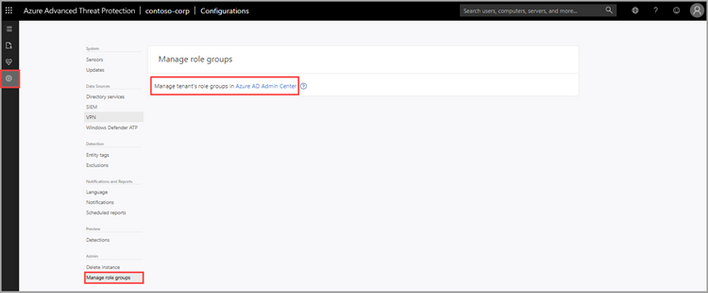
Create a new AATP Instance will be created:



Your Azure ATP instance is automatically named with the Azure AD initial domain name and created in the data center located closest to your Azure AD.

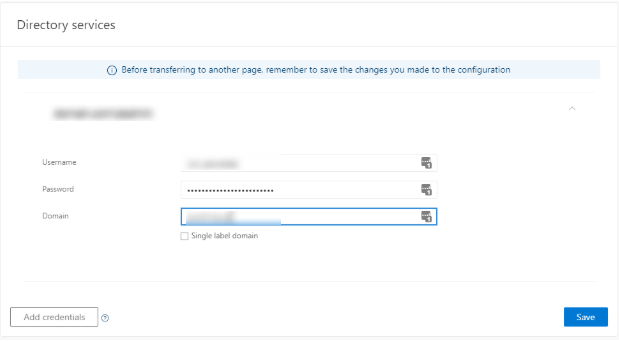


Click Configuration, Manage role groups, and use the Azure AD Admin Center link to manage your role groups.



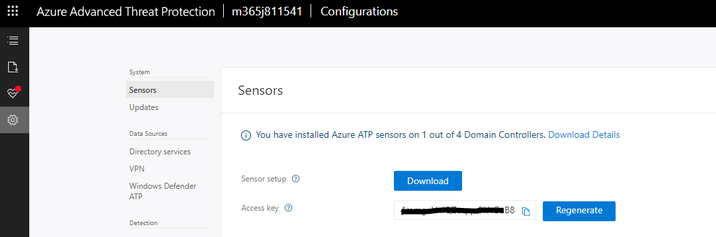
**Connect AATP Instance To AD Forest**

The first time you open the Azure ATP portal, the following screen appears:

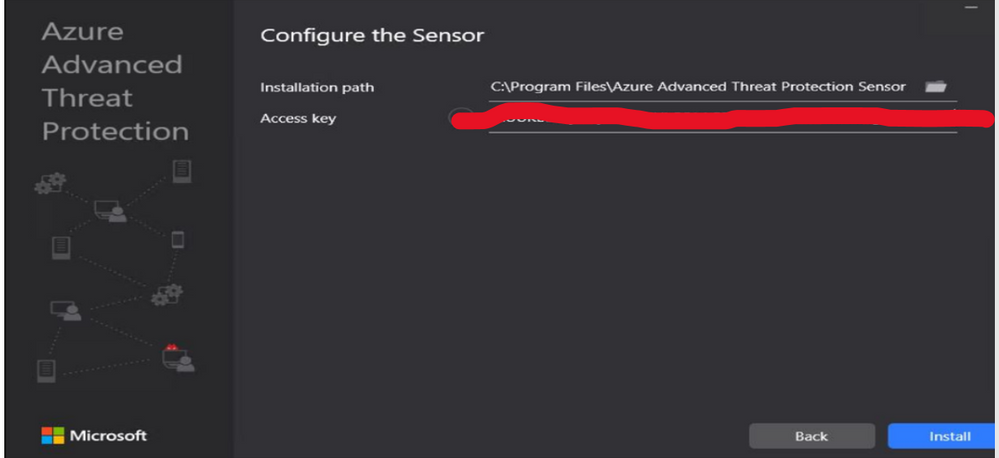


**Download And Install The Sensor To DC**

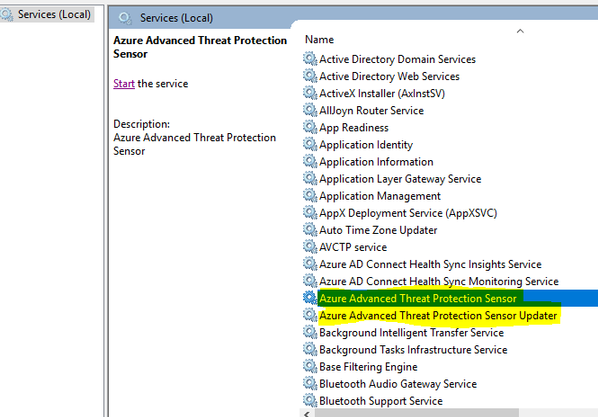
Download and copy the Access key. The access key is required for the Azure ATP sensor to connect to your Azure ATP instance (one-time-password for sensor deployment).



Under Configure the sensor, enter the installation path and the access key that you copied from the previous step, based on your environment:



Azure ATP sensor service and Azure ATP sensor updater service are now available in Windows Services as shown:

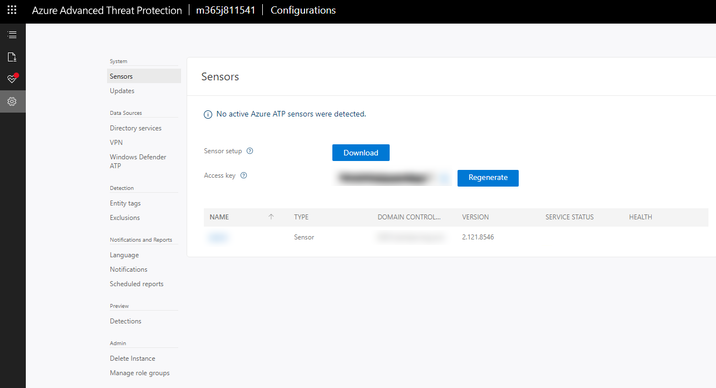


To finish, reboot the DC Sensor Server.

If the domain controller is the first deployed sensor, you will need to wait at least 15 minutes to allow the database backend to finish initial deployment of the necessary microservices.

**To Check If Sensor Is Working Correctly:**

Sign in to portal.atp.azure.com and check if sensor is working:



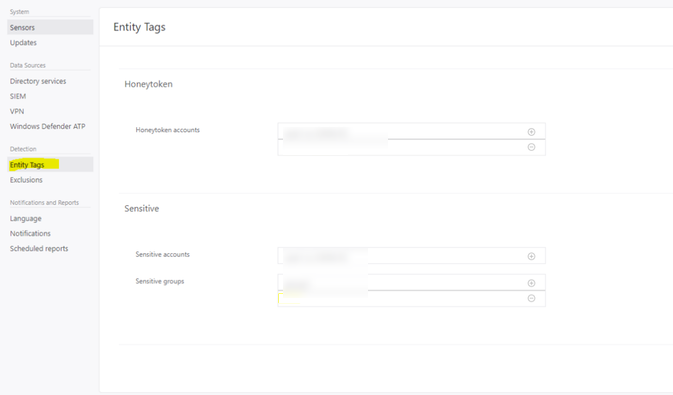
**Configure AATP**

**To Configure Detection Exclusions And Honeytoken**

Honeytoken accounts, which are used as traps for malicious actors – any authentication associated with these honeytoken accounts (normally dormant), triggers an alert.

Honeytokens can exist in many forms, from a dead, fake account to a database entry that would only be selected by malicious queries, making the concept ideally suited to ensuring data integrity. A particular example of a honeytoken is a fake email address used to track if a mailing list has been stolen.

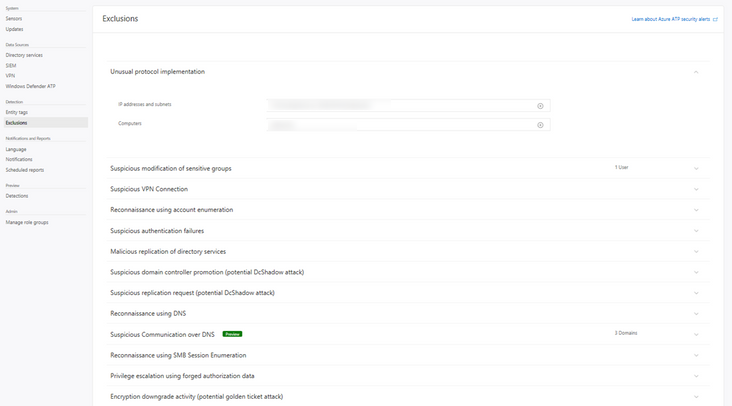
1. From the Azure ATP portal, click on the settings icon.
2. Under Detection, click Entity tags.
3. Under Honeytoken accounts, enter the Honeytoken account name and click the + sign. The Honeytoken accounts field is searchable and automatically displays entities in your network. Click Save.



1. Add Sensitive Accounts:

* Sensitive Accounts: Enter the account you want to monitor lateral movement, modification change, high privilege accounts.
* Sensitive groups: Enter the account you want to monitor lateral movement, modification change, high privilege administrative group.

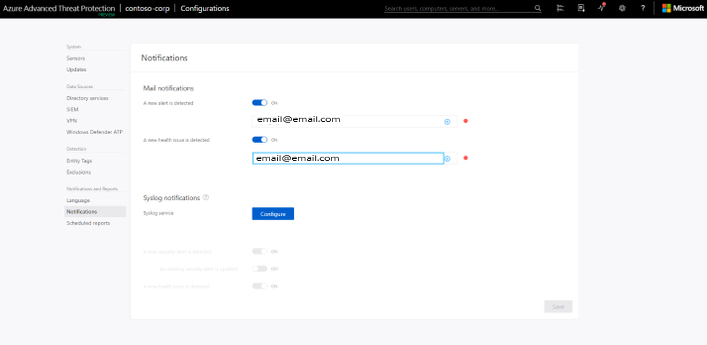
1. Click Exclusions. Enter a user account or IP address to be excluded from the detection, for each type of threat.
2. Click the plus sign. The Add entity (user or computer) field is searchable and will autofill with entities in your network. For more information, see Excluding entities from detections and the security alert guide.



1. Click Save.

**Notifications To A Specific Email Address:**

1. In the Azure ATP portal, select the “settings” icon
2. Click Notifications.
3. Under Mail notifications, specify which notifications should be sent via email – they can be sent for new alerts (suspicious activities) and new health issues.
4. Click Save.



**Configure The Collection Of Audit Events In GPO**

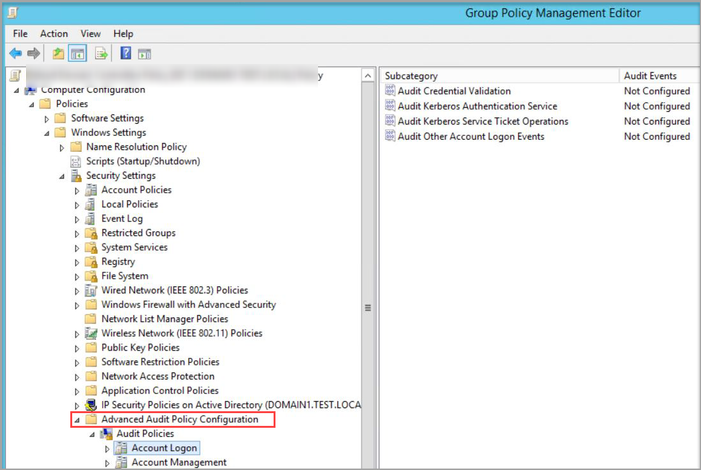
Azure Advanced Threat Protection (Azure ATP) detection relies on specific Windows Event log entries to enhance some detections and provide additional information on who performed specific actions such as NTLM logons, security group modifications and others.

You can use the Default Domain Controllers Policy or a dedicated GPO to set the following audit policies:

Go to Computer Configuration > Policies > Windows Settings > Security Settings

Go to Advanced Audit Policy Configuration

Audit Policies.



Under Audit Policies, edit each of the following policies select Configure the following audit events for both Success and Failure events.

GPO SETTINGS

Audit policy Subcategory Triggers event IDs

Account Logon Audit Credential Validation 4776

Account Management Audit Computer Account Management 4743

Account Management Audit Distribution Group Management 4753, 4763

Account Management Audit Security Group Management 4728, 4729, 4730, 4732,

4733, 4756, 4757, 4758

Account Management Audit User Account Management 4726

System Audit Security System Extension 7045

Configure The Collection Of Event 8004 NTLM Authentication:

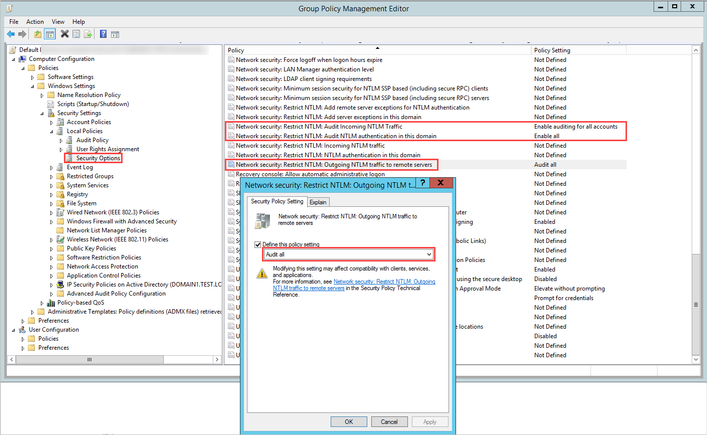
* Go to Local Policies > Security Options.

Under Security Options, configure the specified security policies, as follows:

Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers Audit all

Network security: Restrict NTLM: Audit NTLM authentication in this domain Enable all

Network security: Restrict NTLM: Audit Incoming NTLM Traffic Enable auditing for all accounts



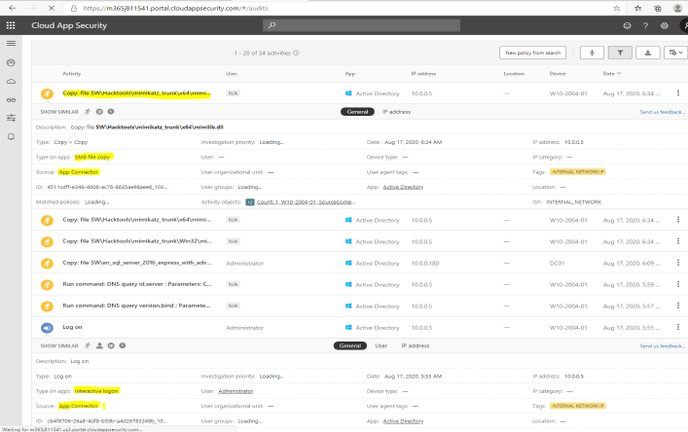
**Troubleshoot and Test AATP result**

**To Test AATP**

You could simulate the attacks from fake virus script and files at the following link: https://securitycenter.microsoft.com/tutorials/all

View responses from AATP portal at https://portal.cloudappsecurity.com

InvestigateActivity logs



**Troubleshooting**

**AATP logs ‘ locations:**

**Azure ATP Deployment logs**

The Azure ATP deployment logs are located in the temp directory for the user who installed the product. C:UsersAdministratorAppDataLocalTemp (or one directory above %temp%).

**Azure ATP logs**

C:Program FilesAzure Advanced Threat Protection Sensor version numberLogs.

Microsoft.Tri.Sensor.log – This log contains everything that happens in the Azure ATP sensor (including resolution and errors).

Microsoft.Tri.Sensor-Errors.log – This log contains just the errors that are caught by the ATP sensor.

Microsoft.Tri.Sensor.Updater.log – This log is used for the sensor updater process (automatically updated).

**Installing AATP Sensor On Server Core (No GUI)**

**Support for Windows 2016, 2019 Server Core**

“Azure ATP sensor Setup.exe” /quiet NetFrameworkCommandLineArguments=”/q” AccessKey=”<Access Key>”

Or by Powershell: ./”Azure ATP sensor Setup.exe” /quiet NetFrameworkCommandLineArguments=”/q” AccessKey=”<Access Key>”

To Update Sensor: “Azure ATP sensor Setup.exe” [/quiet] [/Help] [NetFrameworkCommandLineArguments=”/q”]