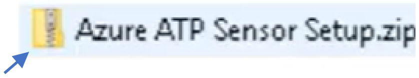
Lab Instructions Microsoft Defender for Identity sensor download and configuration

1. **Select the Next navigation button on the Introductory Screen**
2. **Click on Select a use name and password**
3. **Notice the the username, password and domain name must be entered**
4. **Click on Save to continue**
5. **Click on Download Setup to install your first sensor**
6. **Select the copy icon next the the access key to copy the access key. You will need to use it later**
7. **Now click on Download to download the sensor.**
8. **Look at the top right of the screen to see your downloaded zip file**
9. **Click on the File explorer icon on your task bar and right click on**



Azure ATP Sensor Setup.zip

10. **Click on Extract All, then click on Extract**
11. **Right click the exe file and select Run as Administrator**
12. **On the Defender for Identity page click on Next**
13. **Click Next on the Sensor page to continue**
14. **Click on the access key line, then right click to paste the key you copied previously**
15. **The install key will be selected for you (in your production environment make sure you select install buutton)**
16. **Click on Finish to complete the install**
17. **Click on the Edge icon on your task bar, notice the Service status**
18. **Select Directory Services again …….. wait for the scrolling to complete**
19. **Select Sensors from the left menu. Notice that the sensor is starting**
20. Under **Detection** select **Entity Tags** and type **jadamsadmin** for the entity name
21. Click on the down arrow by **sensitive accounts** and type **aaron** for the sensitive account name
22. Click the down arrow to the right of **suspected brute force attack.** Notice that you can choose to enter ip address or computer name
23. Select **Notifications**. Notice the available settings
24. Click on **Detections.**
25. Select **Manage Role Groups** then click on **Azure AD Admin Center**
26. Select **Azure Active Directory**

****End of Lab***