

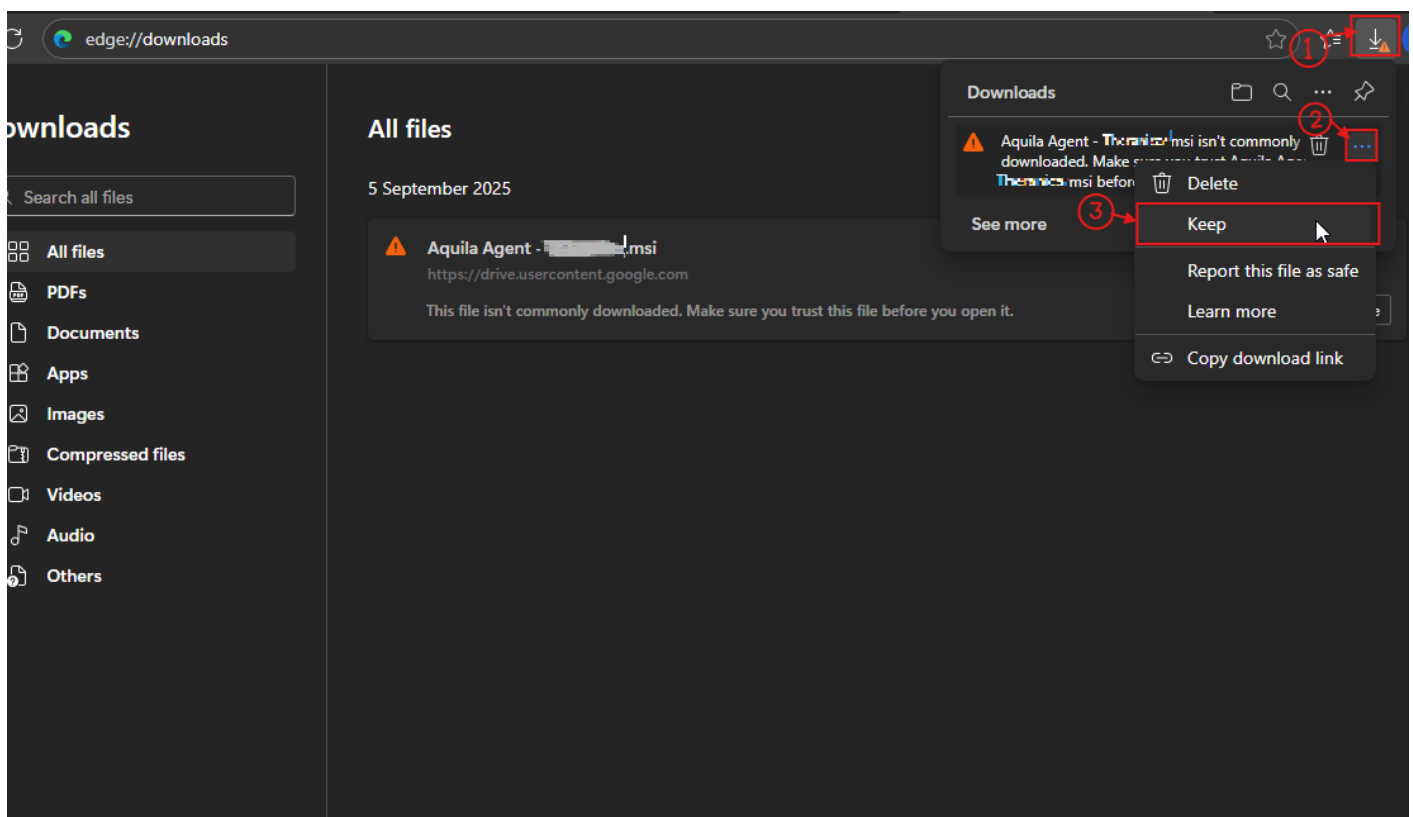
AQUILA - EDR MSI Aquila Agent

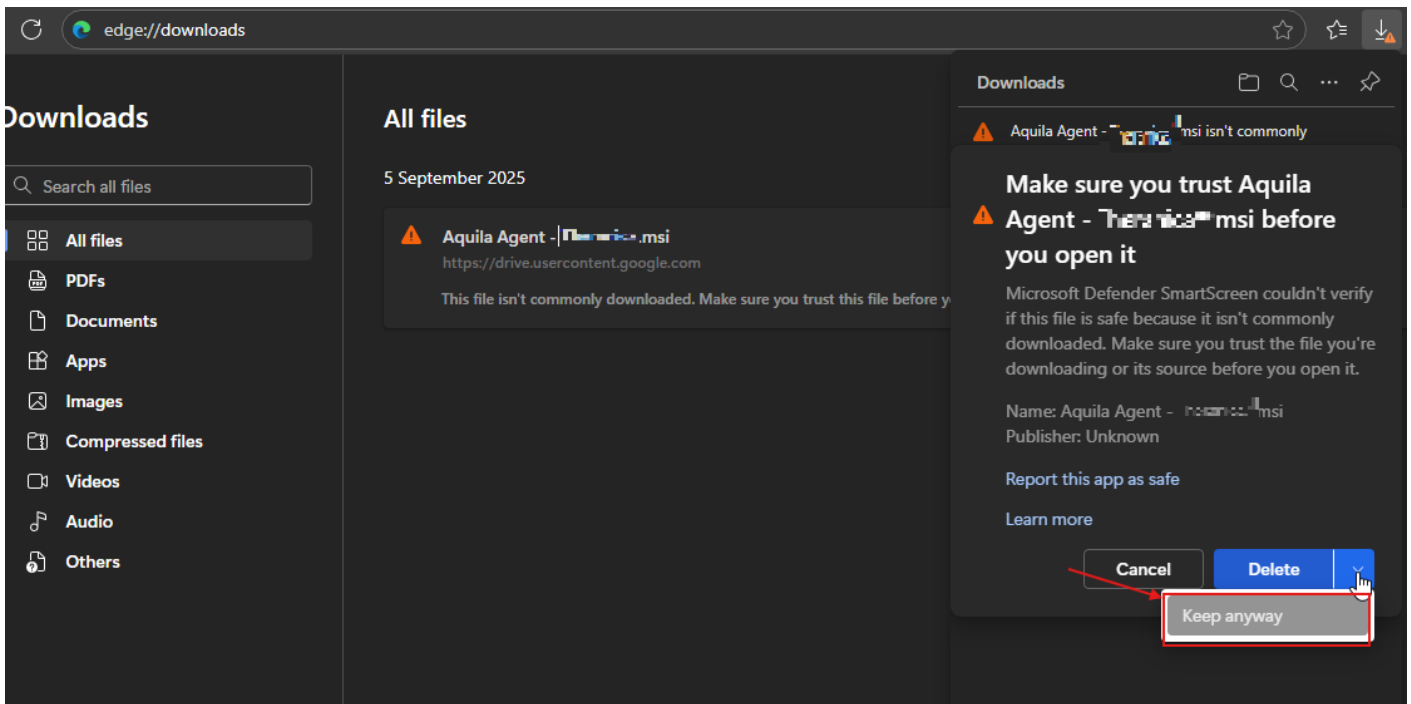
Aquila Agent MSI (EDR) - Manual Installation

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR), is a cybersecurity technology that focuses on detecting, investigating, and responding to suspicious activities and threats on endpoints, such as workstations, laptops, and servers. EDR solutions provide visibility into endpoint activities and help security teams identify and mitigate potential threats before they can cause significant harm.

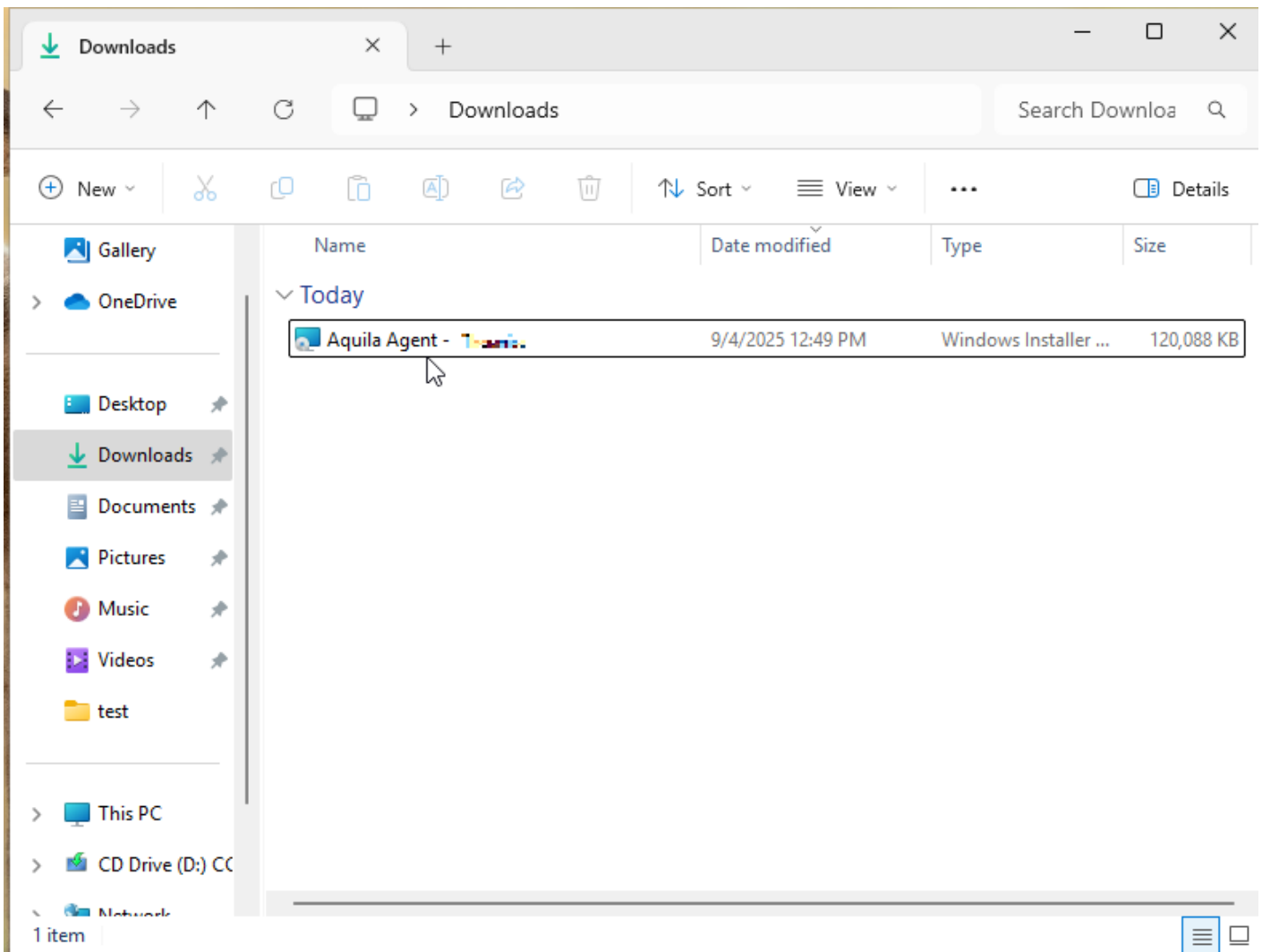
Follow the number of steps to keep the AQUILA EDR installer.



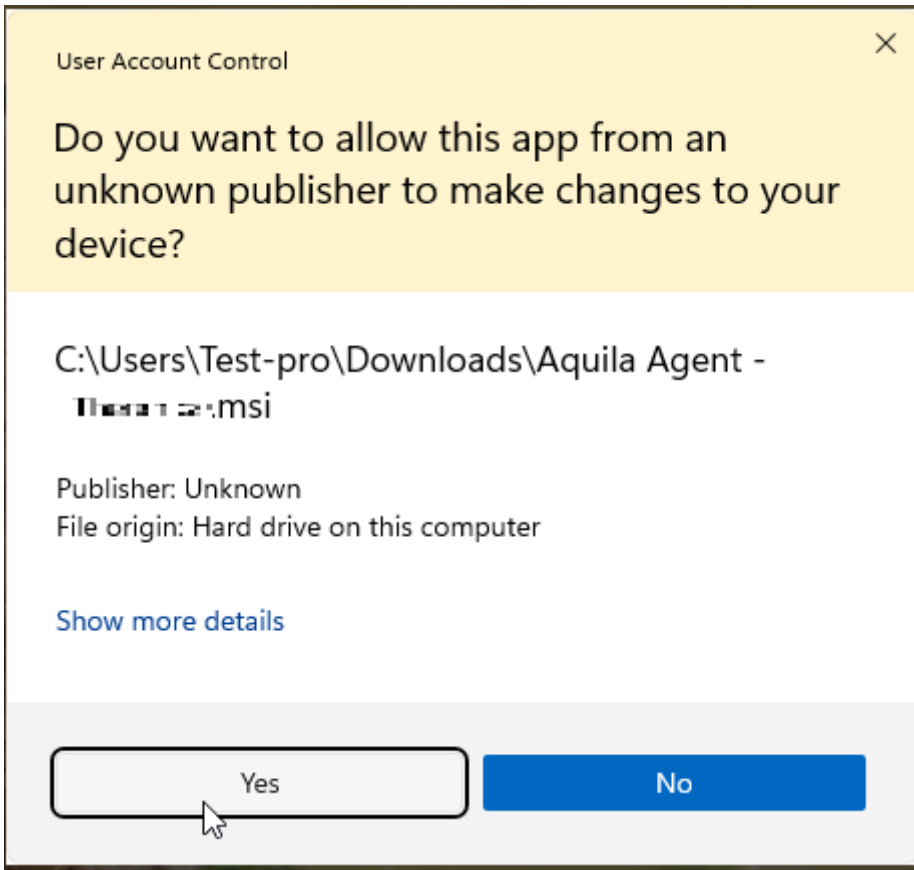


Please follow the instructions below and refer to the images below:

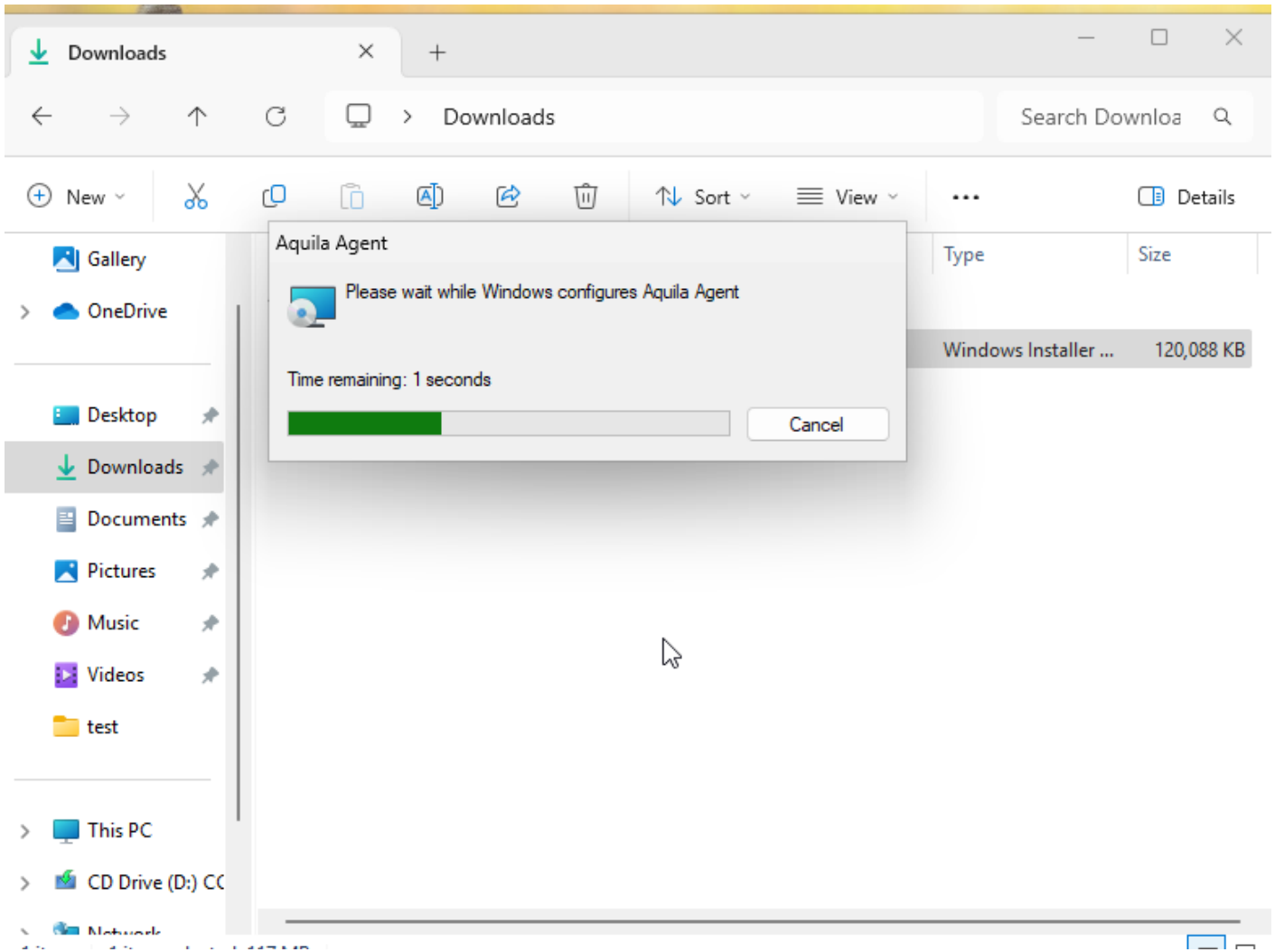
Step 1: After downloading the AQUILA Agent Setup installer. Run the setup file to start the installation wizard.



Step 2: If prompted with a User Account Control (UAC) dialog stating that the app is from an unknown publisher, click **'Yes'** to allow the installer to make changes and proceed with the installation.



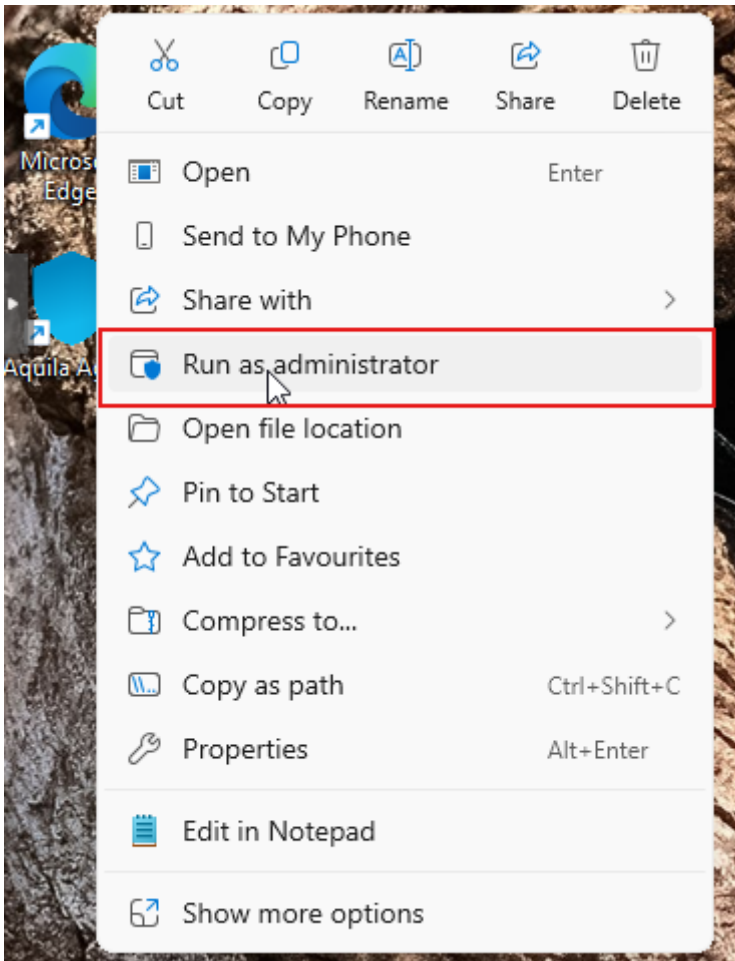
Step 3: Wait for a moment to install the Aquila Agent.



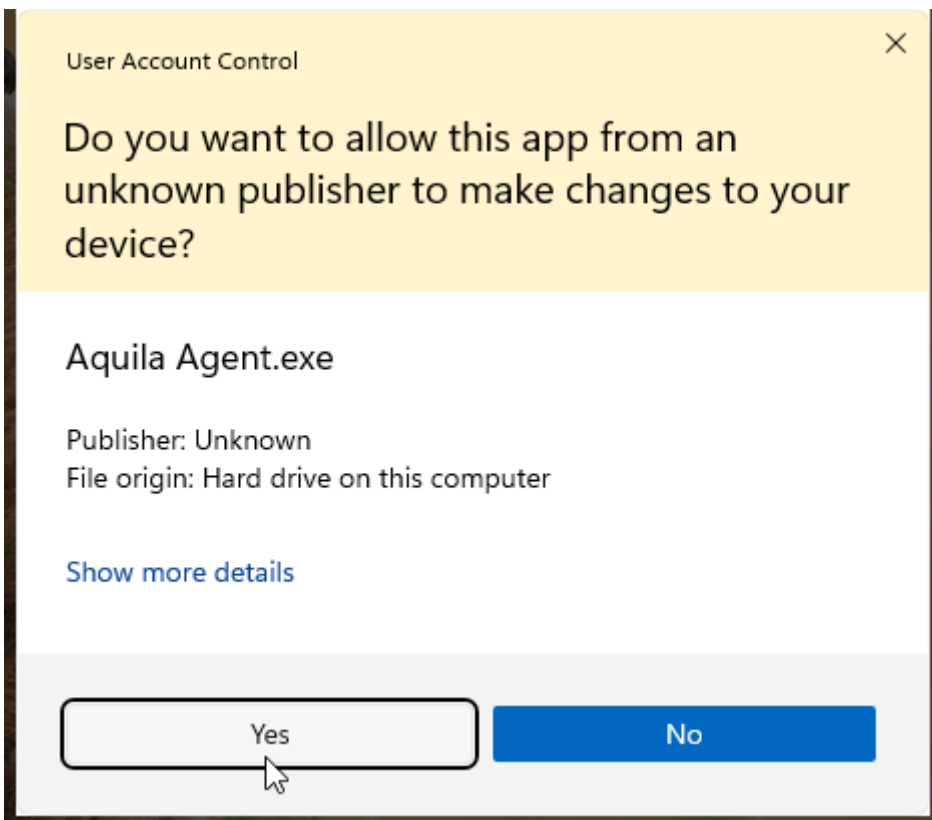
Step 4: After the installation finished, the AQUILA Agent would now be displayed on the Desktop,



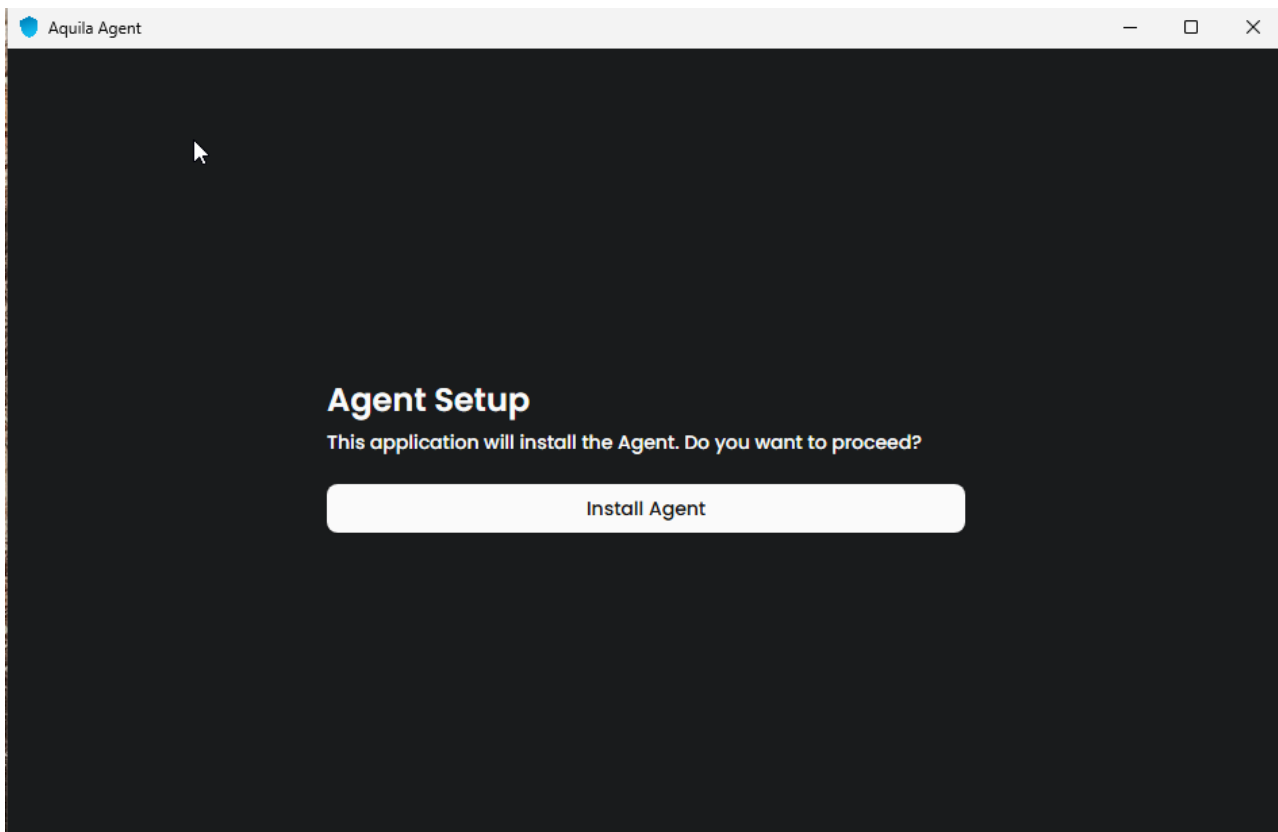
Step 5: Right click or click Mouse 2 on the AQUILA Agent then run it as Administrator.



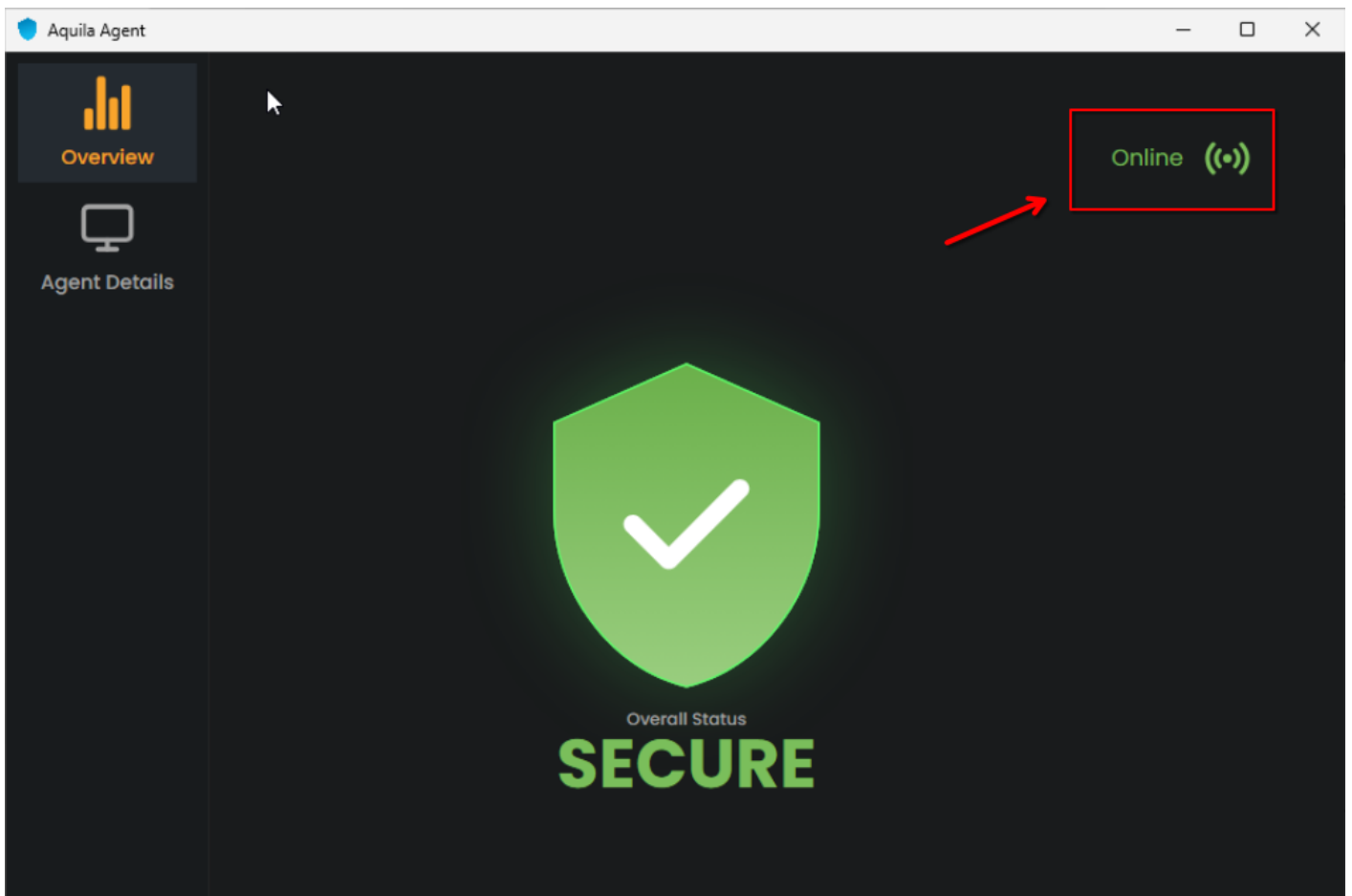
Step 6: If prompted with a User Account Control (UAC) dialog stating that the app is from an unknown publisher, click **'Yes'** to allow the installer to make changes and proceed with the installation.



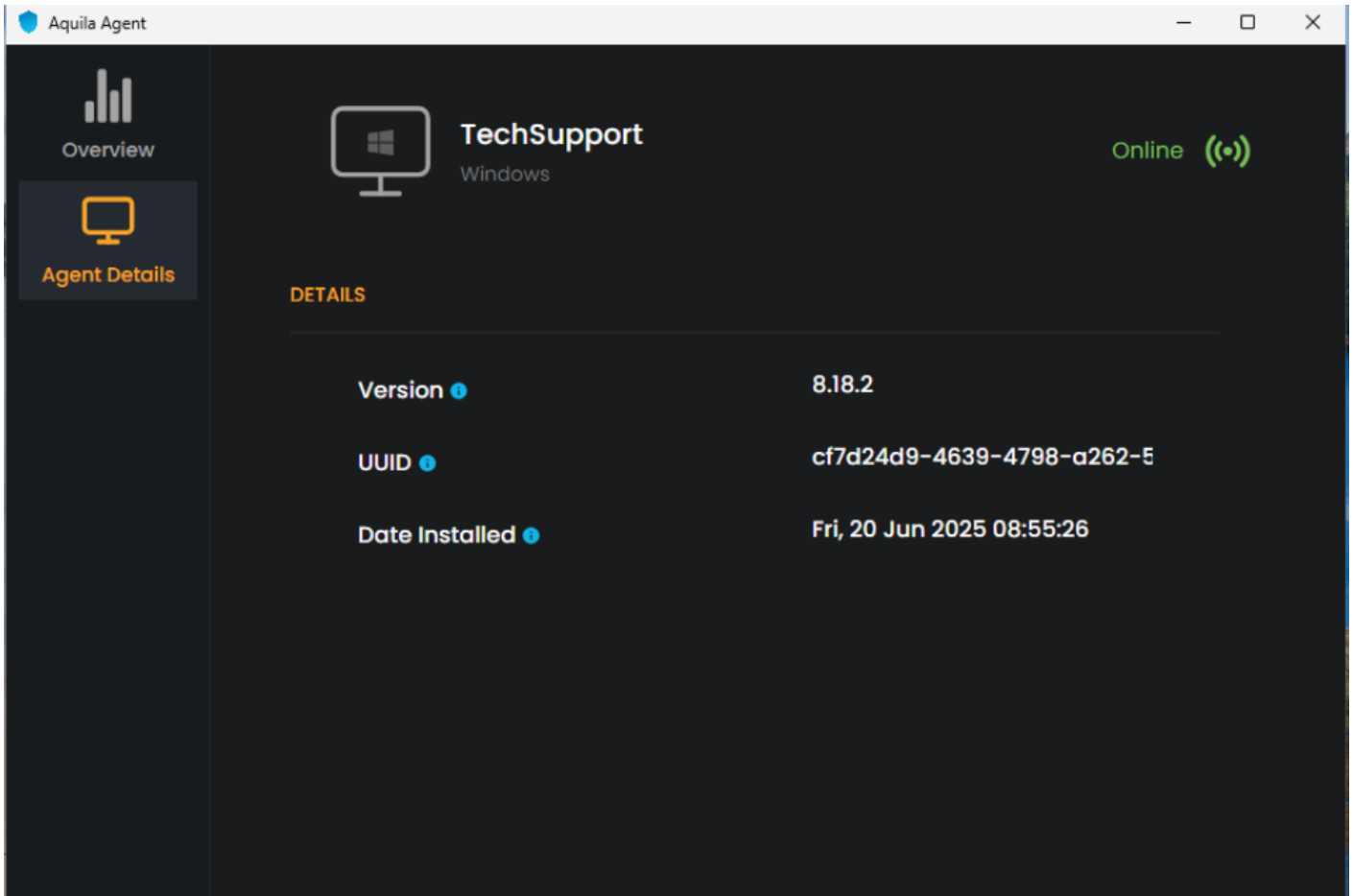
Step 7: Proceed with the installation. Click "**Install Agent**" to proceed. Please wait a few minutes for the installation process to complete. This will automatically initiate enrollment into the CyTech - AQUILA platform.



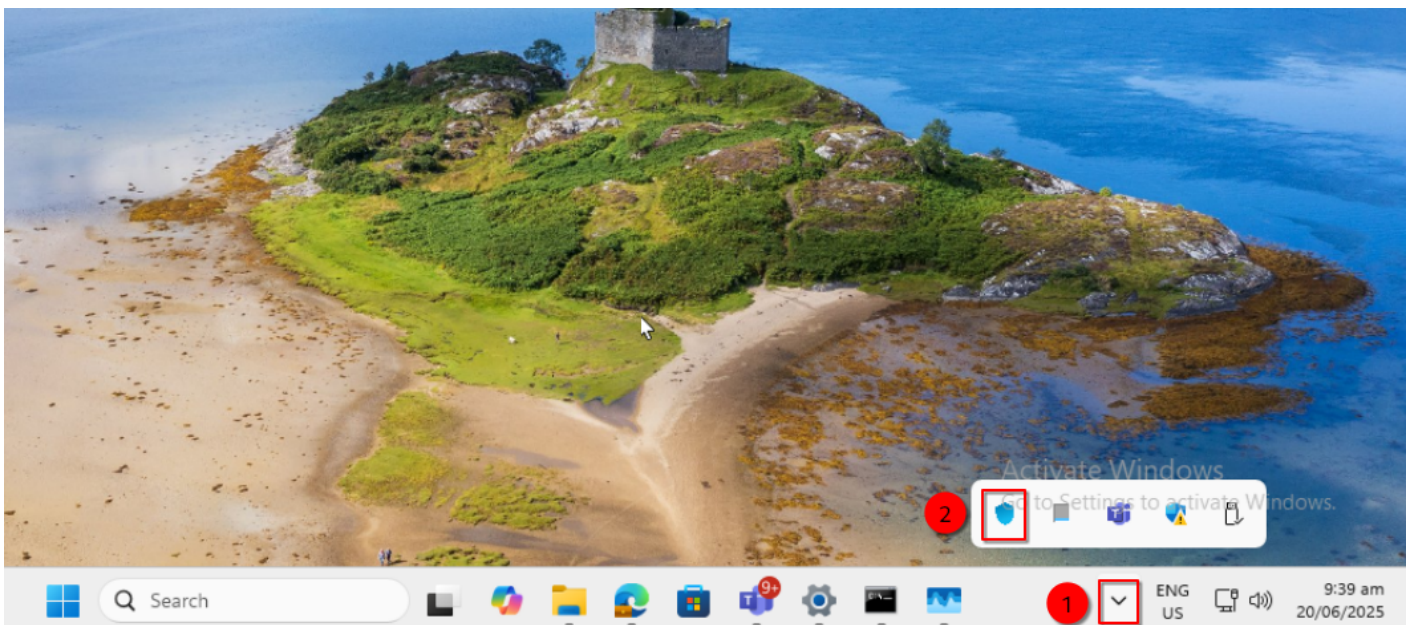
Step 8: After successful enrollment, an overview window will be displayed. Please note that it may take some time for the device to reflect an online status. Ensure the device remains connected to the network for the EDR policy to be properly applied.



Step 9: The Agent Details panel allows you to verify the status and identity of your endpoint device.



Step 10: You may also access AQUILA Agent Secure through the Windows taskbar's side dock panel.



Step 11: The Overview page provides a centralized dashboard displaying all recent detections related to your endpoint devices. This real-time monitoring allows security teams to quickly identify potential threats, analyze attack vectors, and prioritize response efforts based on severity and impact. By consolidating detection data, the Overview page supports proactive threat hunting and continuous endpoint security management as part of a comprehensive cybersecurity monitoring

strategy.

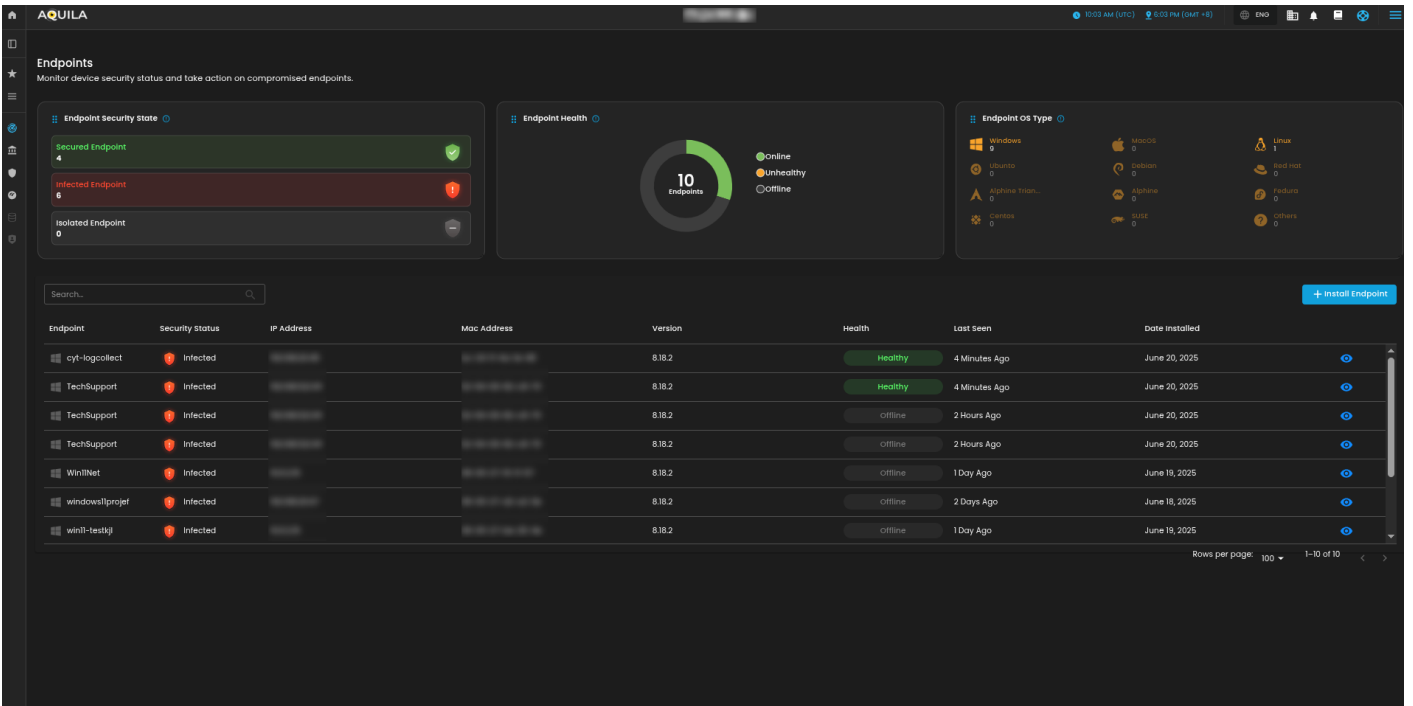
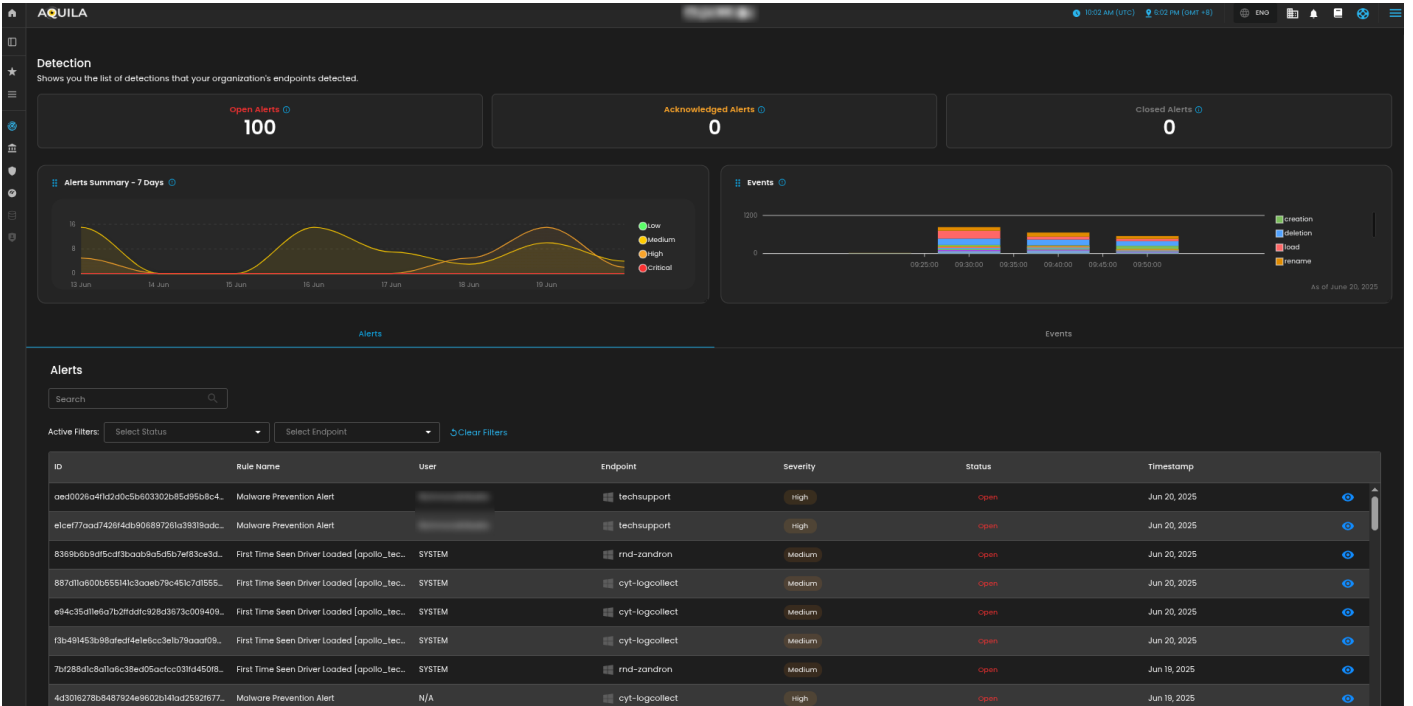
The screenshot shows the Aquila Agent interface. At the top left, there's a navigation menu with 'Overview' and 'Agent Details'. The main header displays 'Overall Status SECURE' with a green checkmark icon and 'Online' with a status icon. Below this, a section titled '4 RECENT DETECTIONS - PAST 24 HOURS' lists three events:

- Successfully quarantined file** (Fri, 20 Jun 2025 10:24:29): A file icon and a path starting with 'C:\Users\'.
- Sending alert** (Fri, 20 Jun 2025 10:24:24): A file icon and a path starting with 'C:\Users\'.
- Successfully quarantined file** (Fri, 20 Jun 2025 10:23:59): A file icon labeled 'new 1.txt' and a path starting with 'C:\Users\'.

For a more detailed report and in-depth analysis, navigate to **CyTech - AQUILA > Cyber Monitoring > Endpoint Detection and Response(EDR)**. This section provides comprehensive visibility into endpoint activity, detection timelines, threat classifications, and response actions to support advanced threat analysis and incident investigation.

The screenshot shows the AQUILA dashboard with several panels:

- Detection status:** Shows a red shield icon with 'INFECTED' and 'Suspicious activity has been detected.' Below it, a red alert box states: '6 Endpoints infected - Immediate Action Required. You have six endpoints that are currently infected. Immediate action is required to address this issue.'
- Open Endpoint Detections:** A large number '235' and a sub-panel for '# of Isolated Endpoints' showing '0'.
- Managed endpoints:** A donut chart showing '10 Total' with '3' Online, '0' Unhealthy, and '7' Offline.
- Recurring offenders:** A list of usernames: techsupport, rnd-zandron, cyt-logcollect, win11-testkj, win11net, and windowwallprojct.
- Authentications:** A bar chart showing 'Success' at 990 and 'Failed' at 0.
- Events:** A stacked bar chart showing event counts over time from 09:25:00 to 09:50:00. The legend includes: creation, deletion, load, rename, overwrite, disconnect_received, lookup_requested, connection_attempted, lookup_result, and modification.



If you need further assistance, kindly contact our technical support at support@cytechint.com for prompt assistance and guidance.

Revision #9

Created 4 September 2025 07:35:53

Updated 12 January 2026 15:30:02 by Benjie Janlay Jr.