AQUILA - Endpoint Detection and Response (EDR) Automatic Installation

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.

Pre-requisites

1. **Access to CyTech - AQUILA**
   - Only users assigned the **"Owner"** or **"Admin"** role can access the Log Collector installation resources within the platform.

Steps to Add AQUILA EDR

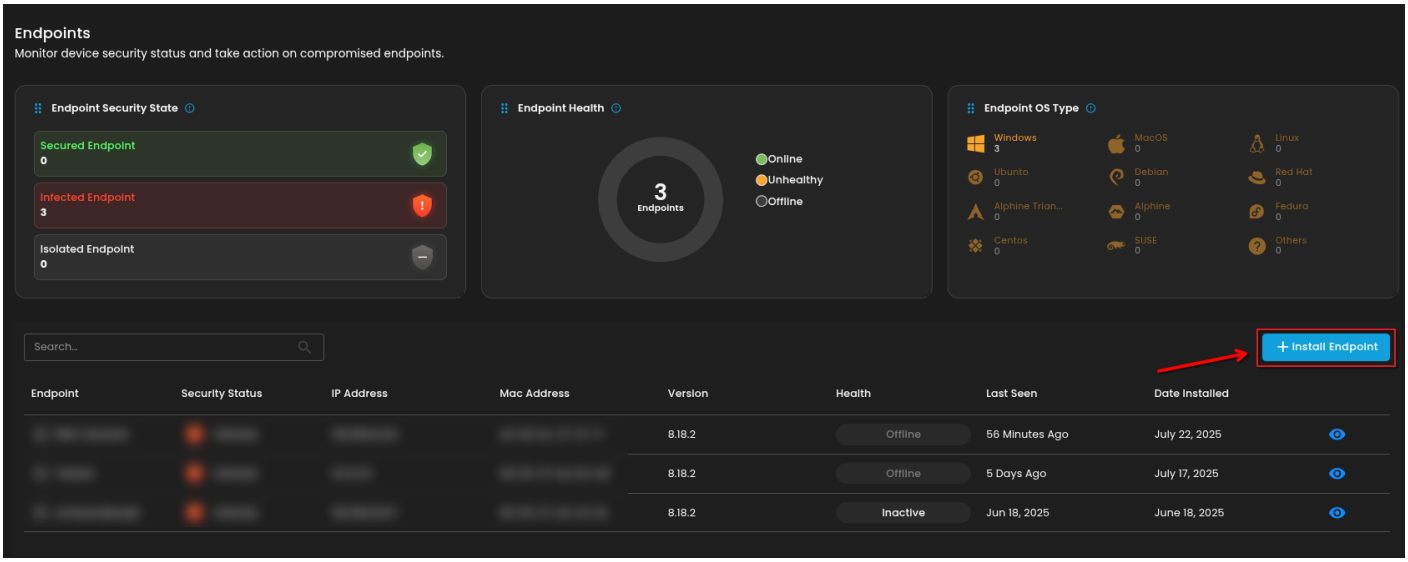
Please follow the steps below to add a Log Collector using Windows Environment.

1. Log in to **CyTech - AQUILA**. Click here: **usdc.cytechint.io**

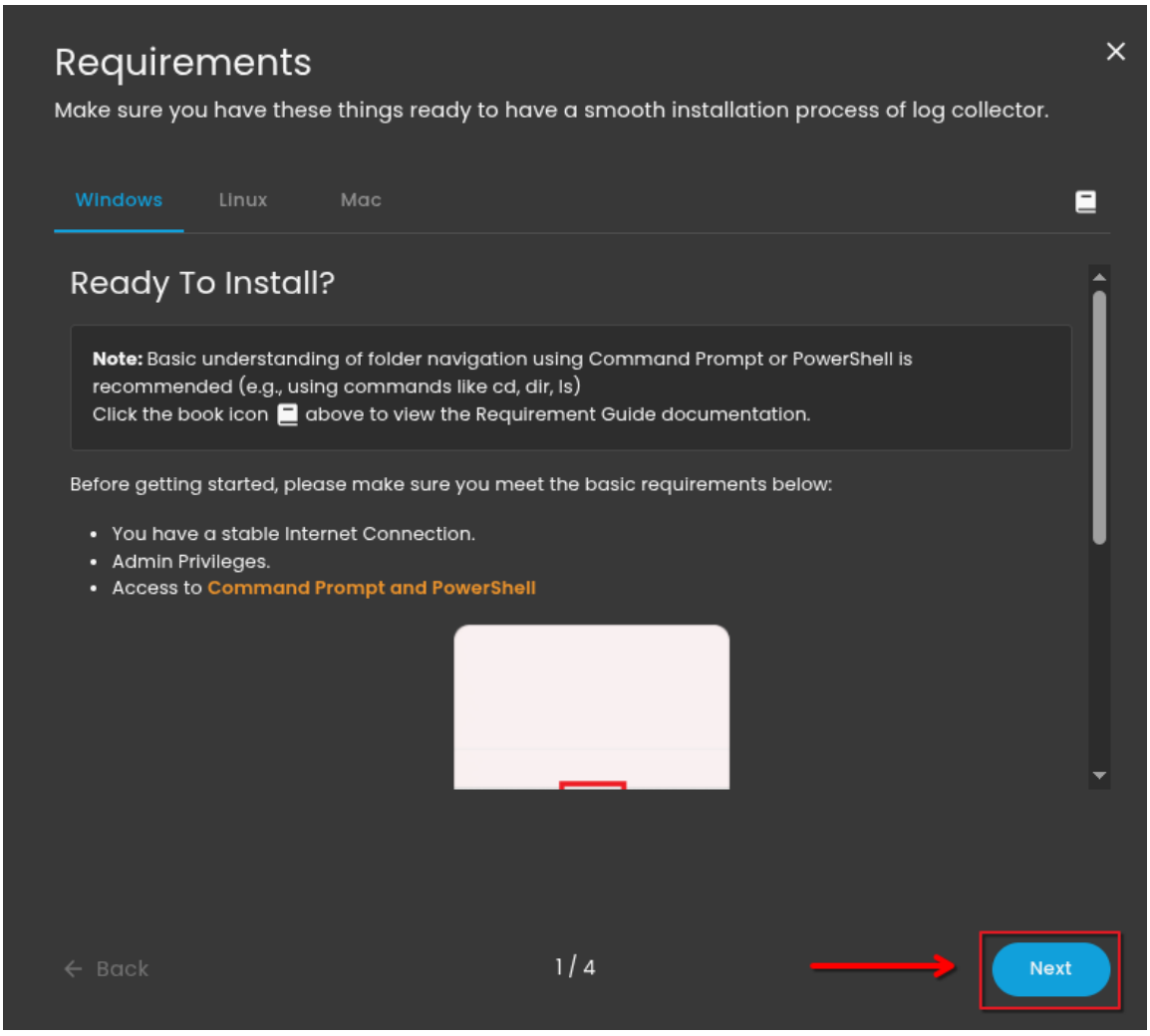
- Click **Collapse** to view side panel. Then navigate through **Domains>Cyber Monitoring>Endpoint Detection and Response>Endpoints**.



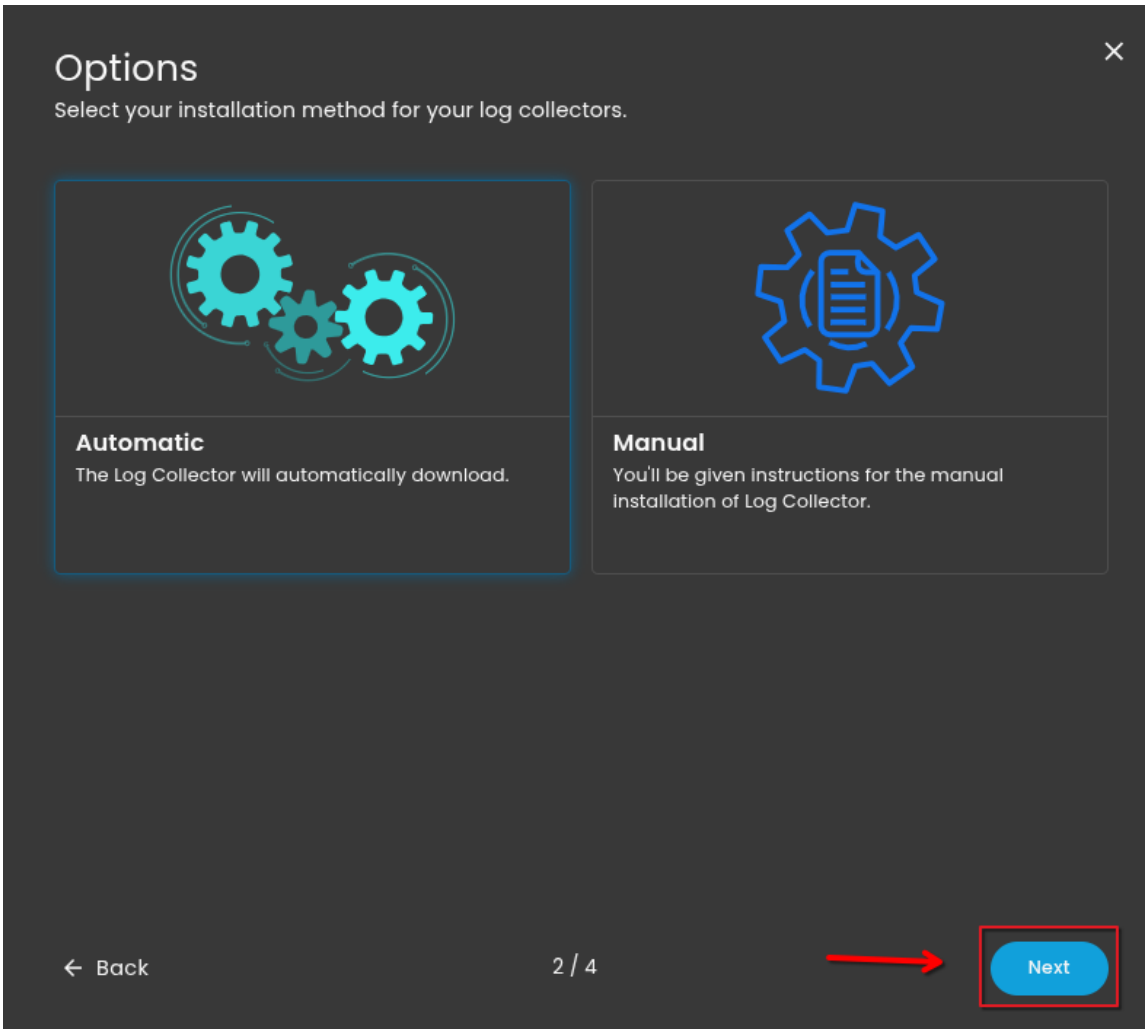
2. Click "**Install Endpoint**" to start installation window.



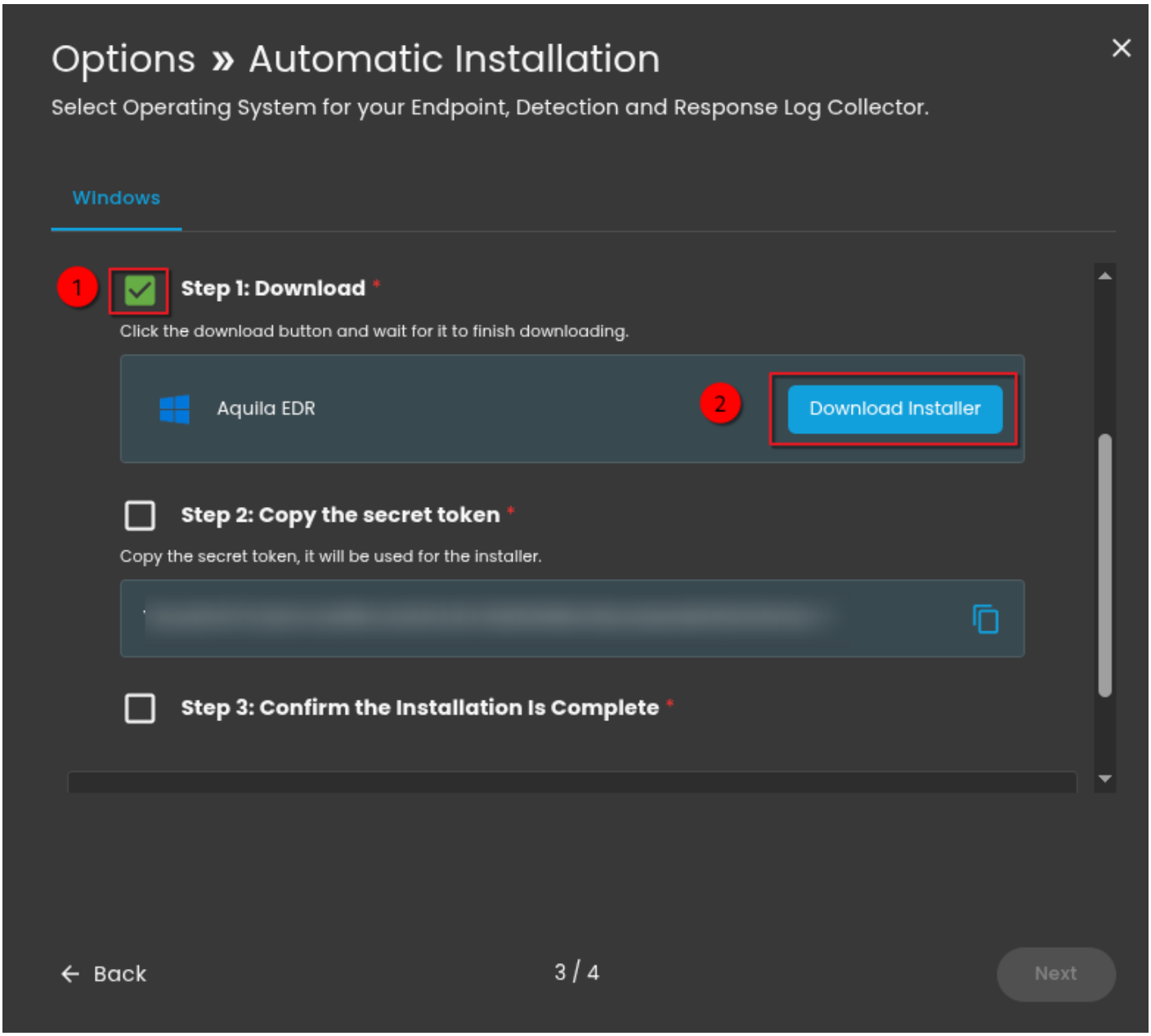
3. Review the needed requirements for each Operating Systems and click "Next".



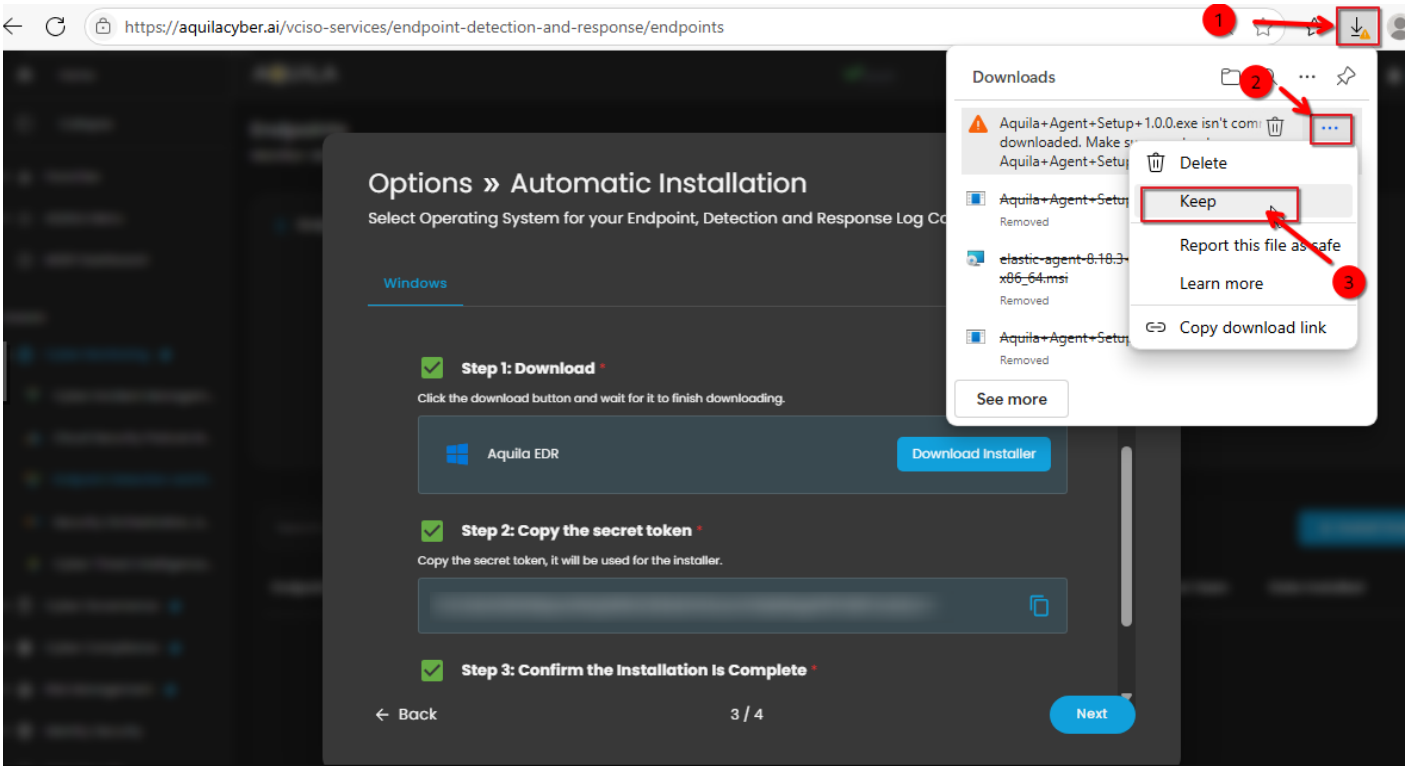
4. Choose "Automatic" installation and click "Next".

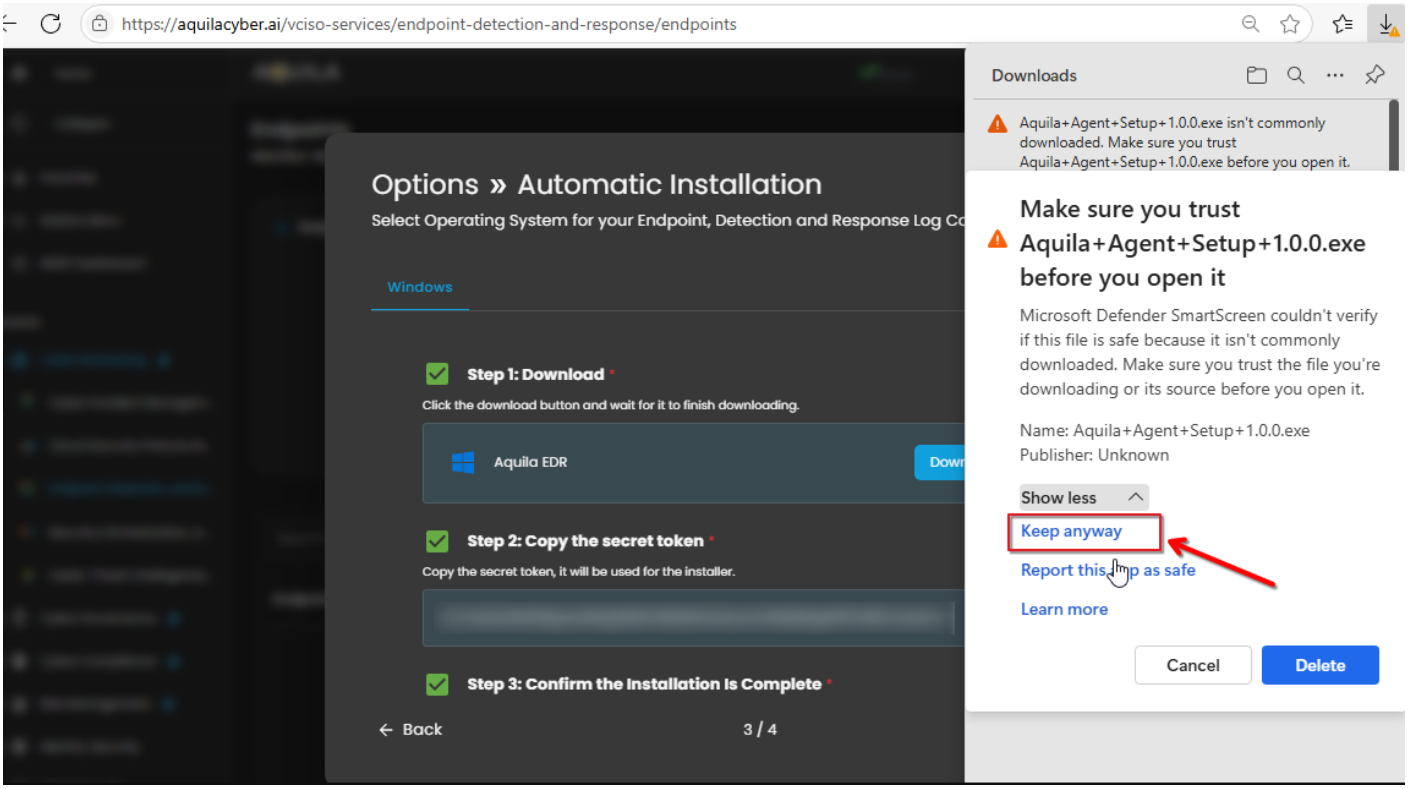


5. Download the AQUILA EDR installer.



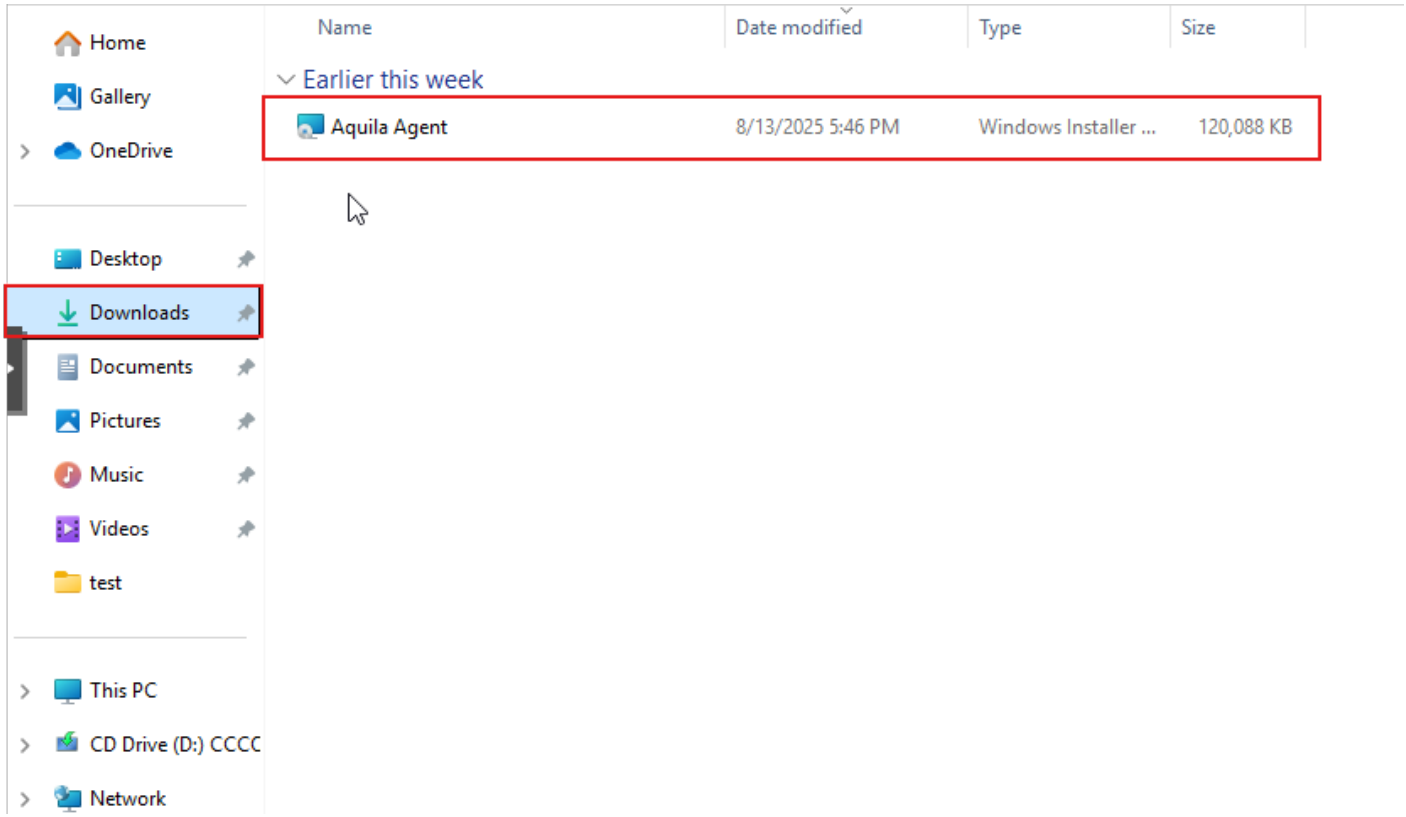
6. Follow the number of steps to keep the AQUILA EDR installer.





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.

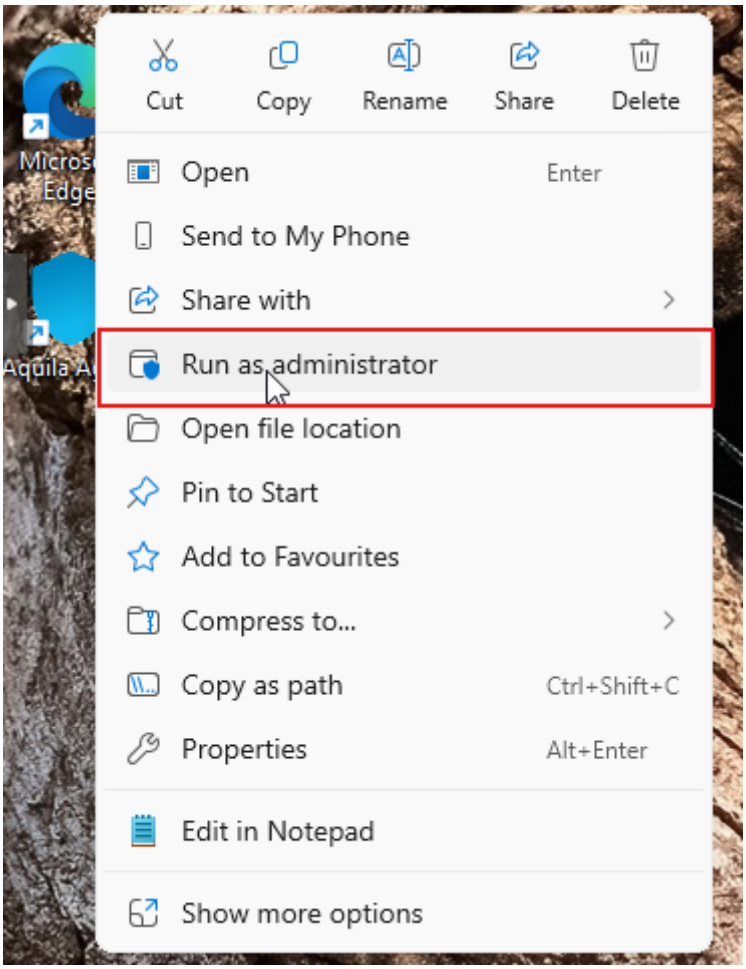


> If prompted with a User Account Control (UAC) dialog stating that the app is from an unknown publisher, click **'Yes'** to allow the installer to make changes and proceed with the installation.

Step 2: After the installation finished, the AQUILA Agent would now be displayed on the Desktop,

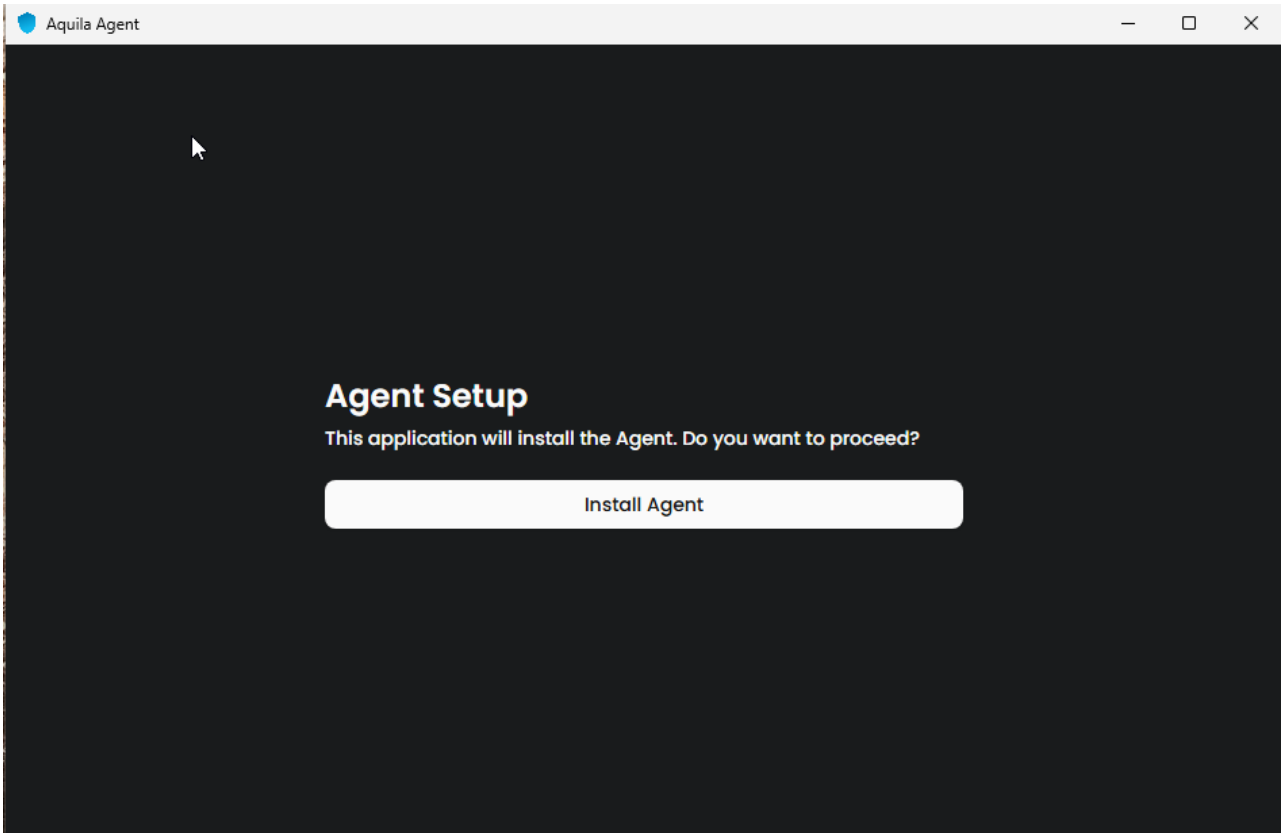


Step 3: Right click or click Mouse 2 on the AQUILA Agent then run it as Administrator.

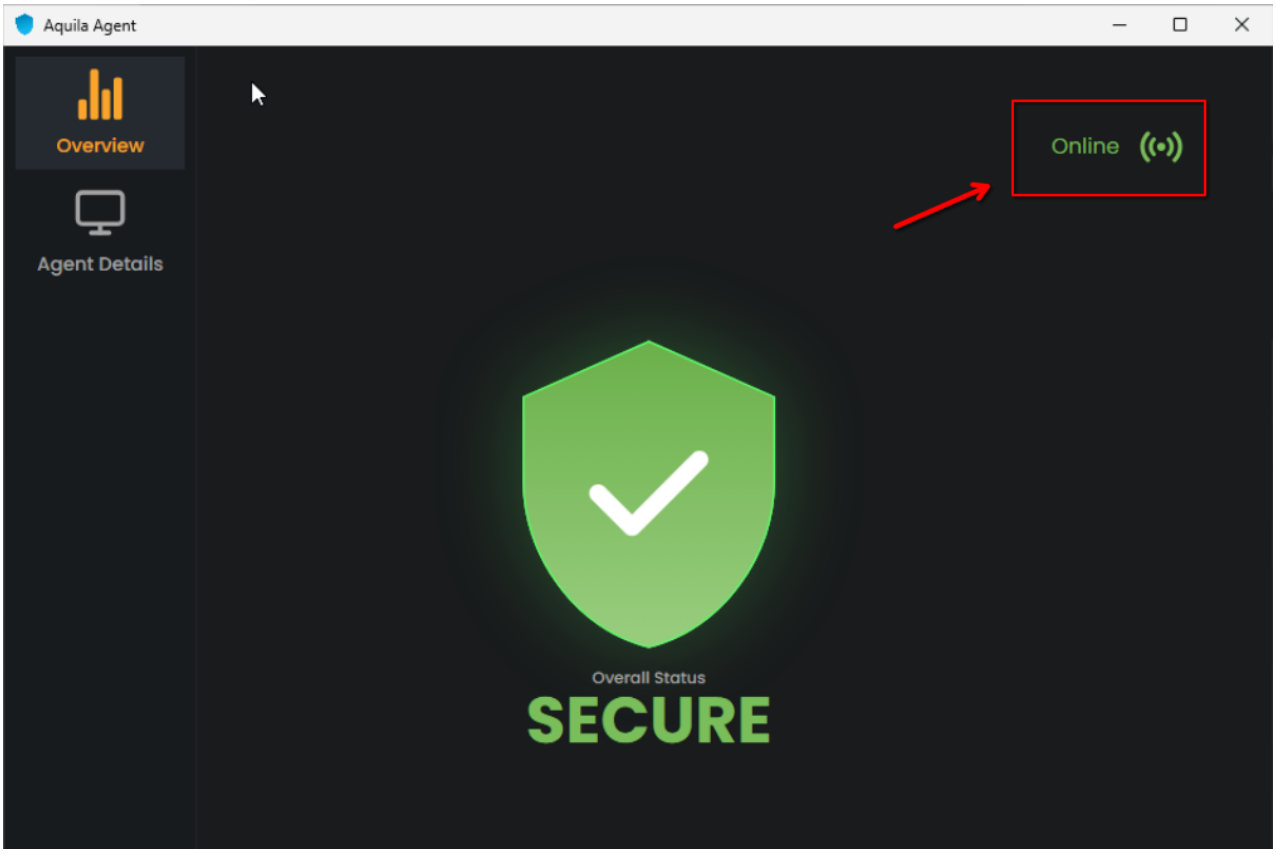


> If prompted with a User Account Control (UAC) dialog stating that the app is from an unknown publisher, click **'Yes'** to allow the installer to make changes and proceed with the installation.

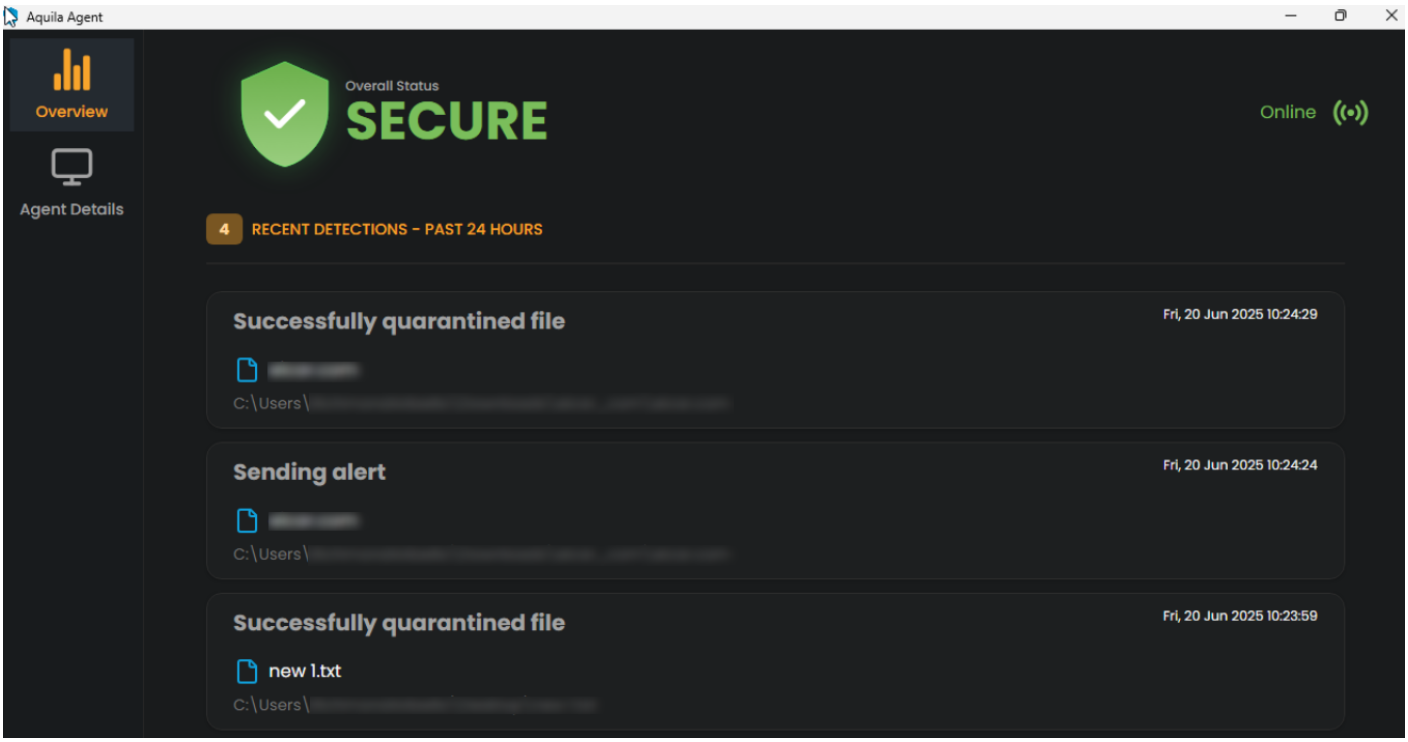
Step 4: Proceed with the installation. Click "**Install Agent**" to proceed. Please wait a few minutes for the installation process to complete. This will automatically initiate enrollment into the CyTech - AQUILA platform.



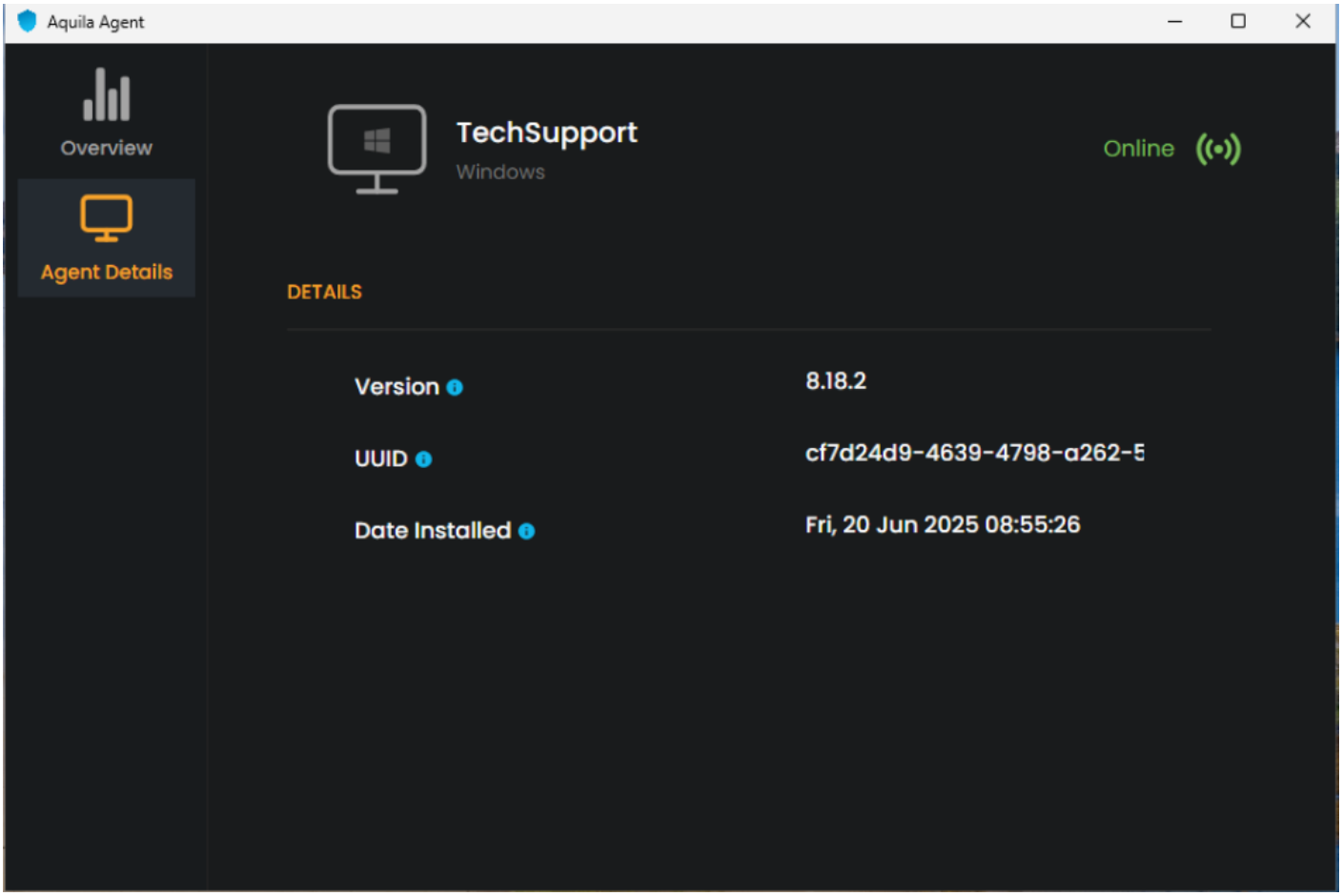
Step 5: After successful enrollment, an overview window will be displayed. Please note that it may take some time for the device to reflect an online status. Ensure the device remains connected to the network for the EDR policy to be properly applied.



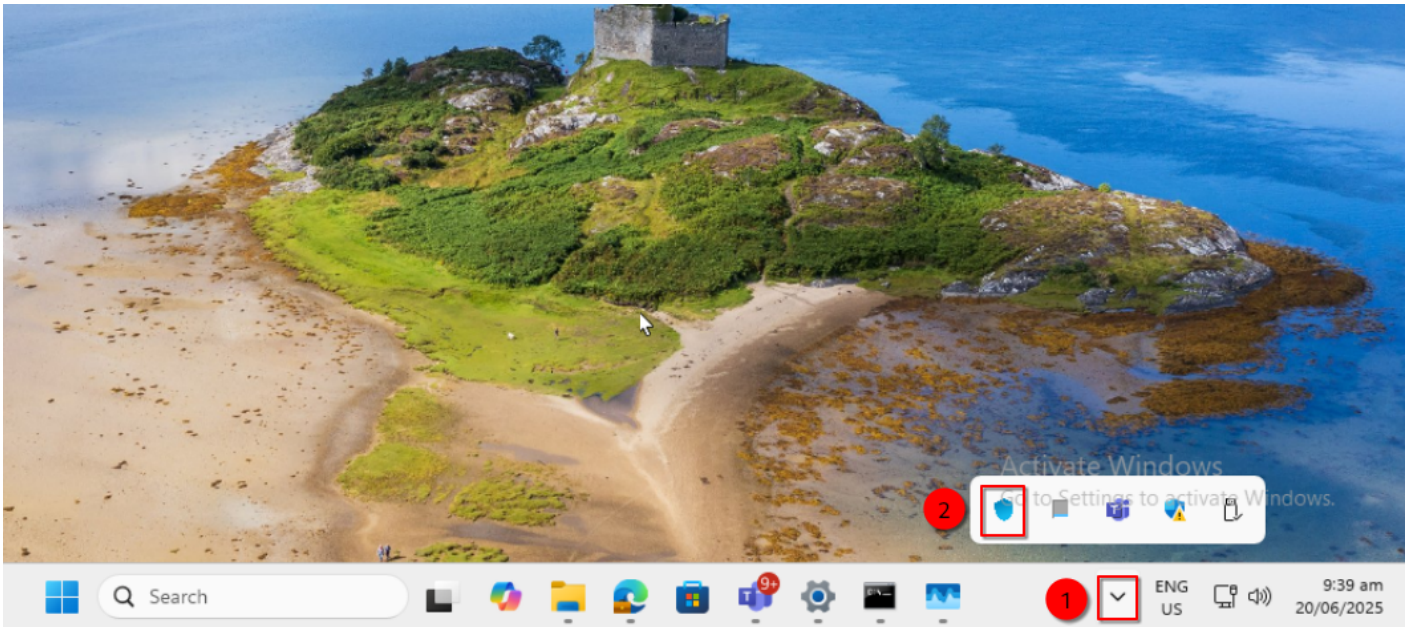
The Overview page provides a centralized dashboard displaying all recent detections related to your endpoint devices. This real-time monitoring allows security teams to quickly identify potential threats, analyze attack vectors, and prioritize response efforts based on severity and impact. By consolidating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



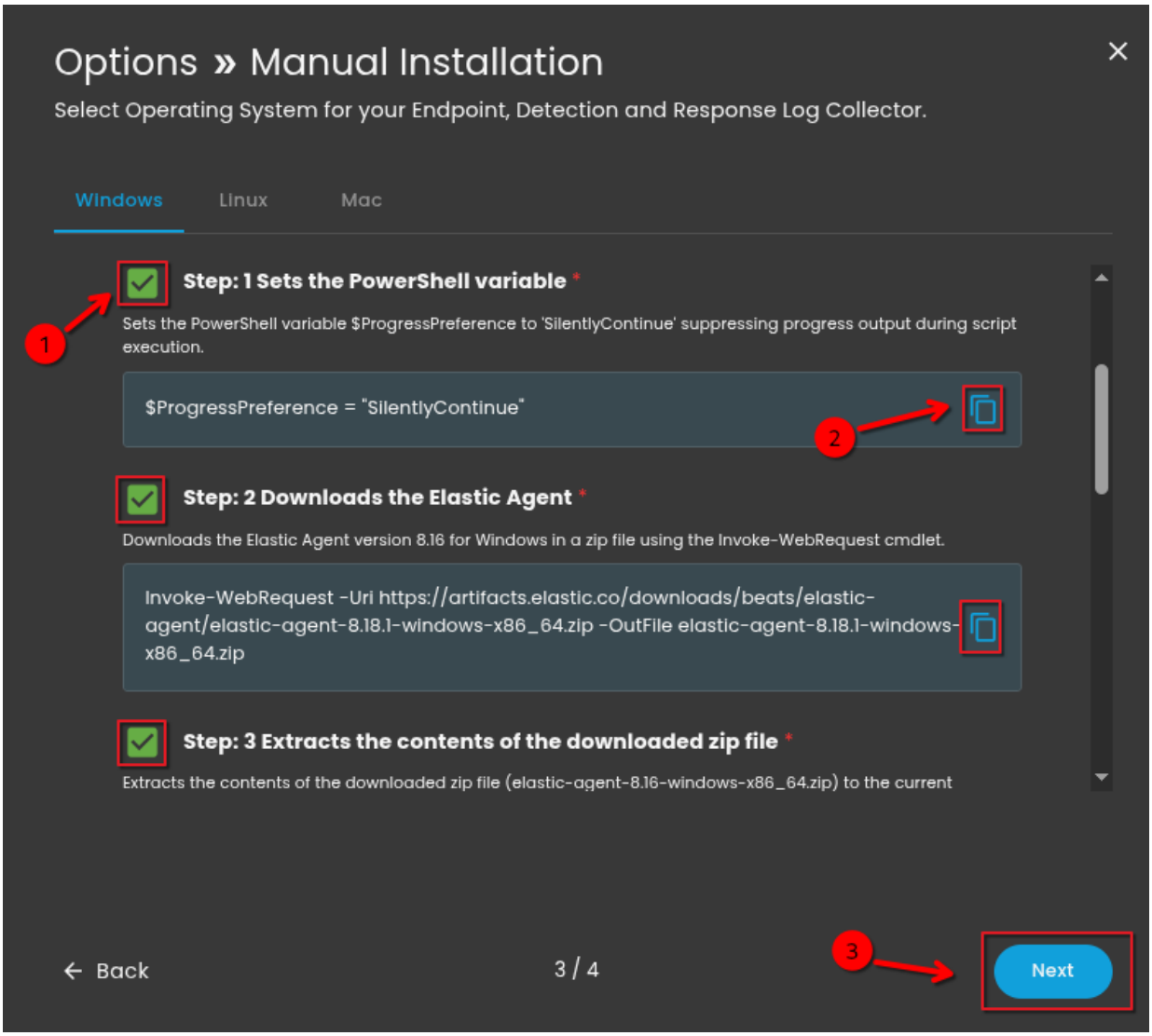
The Agent Details panel allows you to verify the status and identity of your endpoint device.



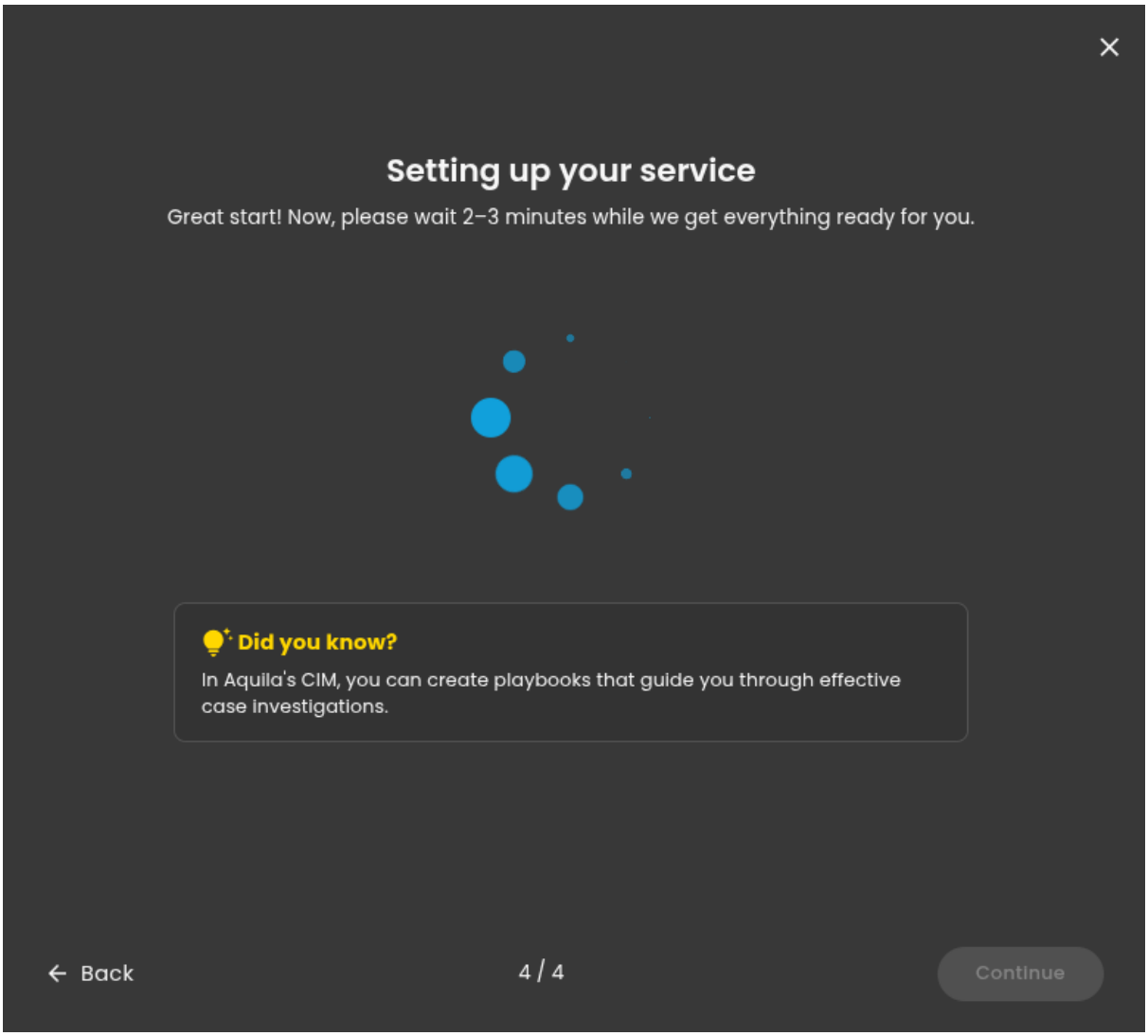
You may also access AQUILA Agent Secure through the Windows taskbar's side dock panel.



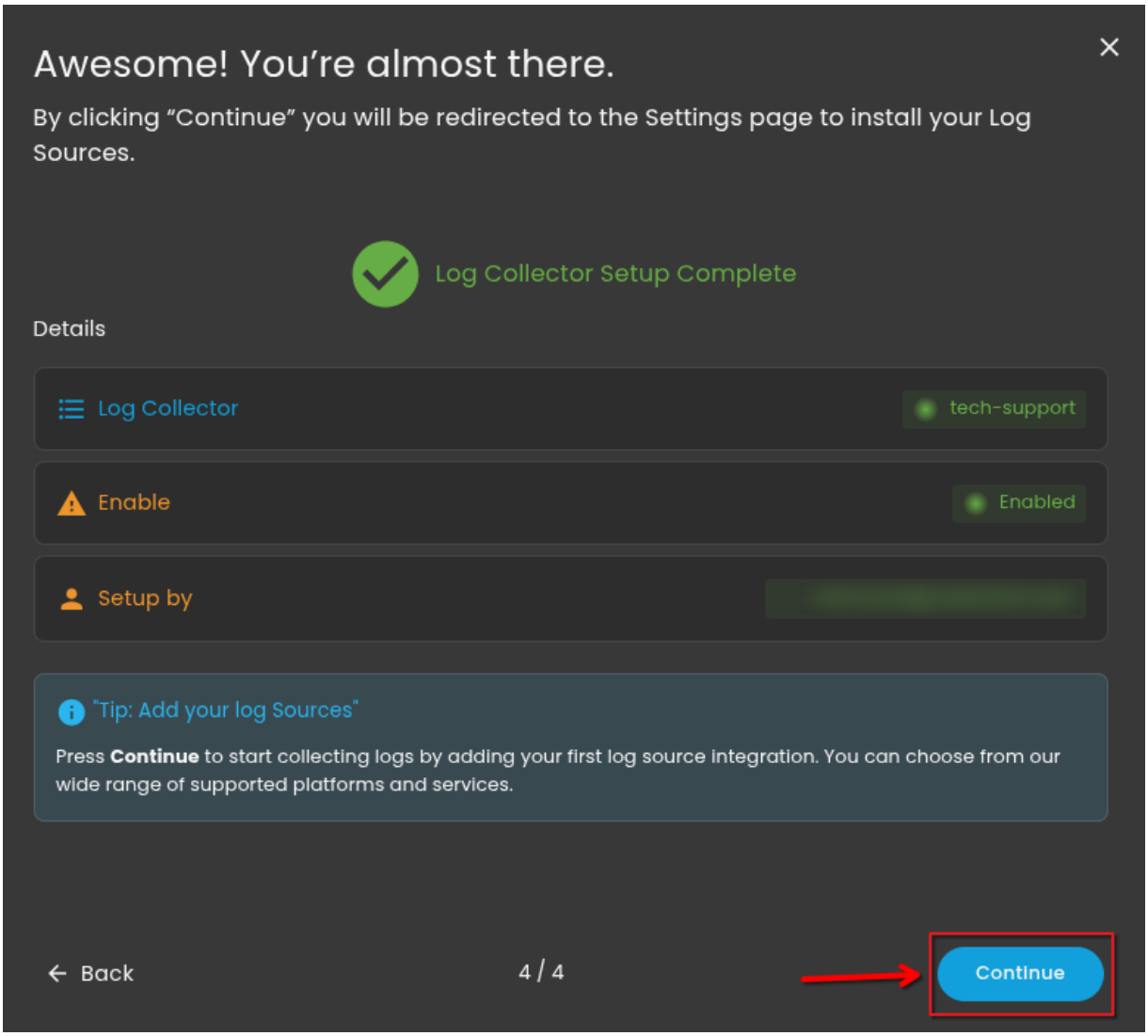
7. **Before you can proceed to the final installation set-up make sure you check off each steps required. Then you can click "Next".**



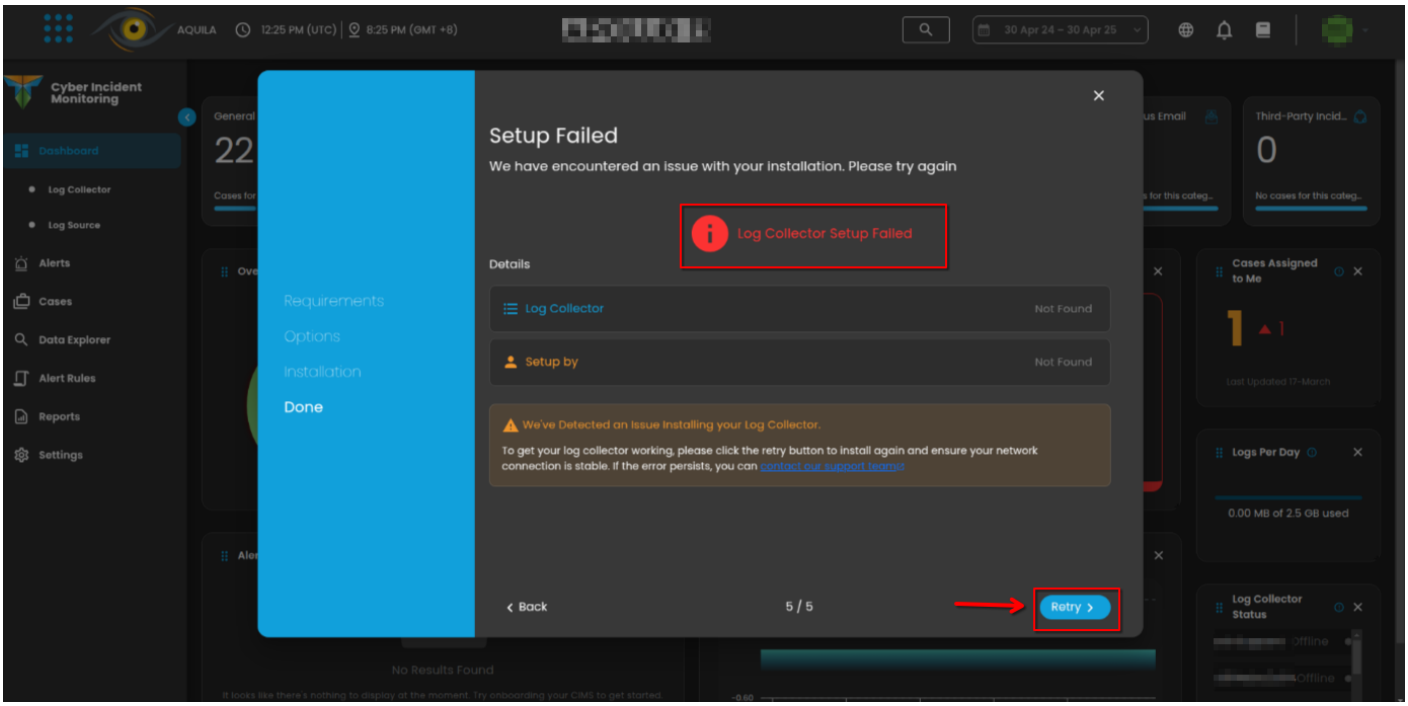
8. **A new window will appear and will check the log collector status and update the latest installation of EDR agent. Wait for it to finish and after successfull installation the endpoint will displayed in the dashboard.**



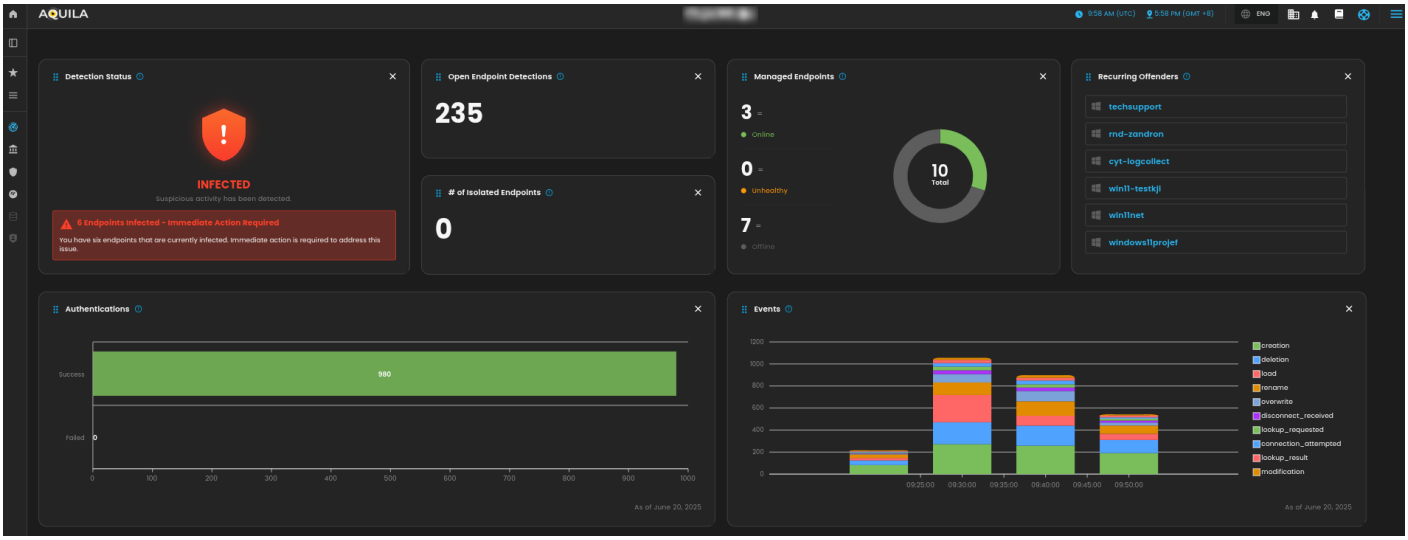
9. This step confirms the successful installation and enrollment of the EDR Agent with the fleet server.

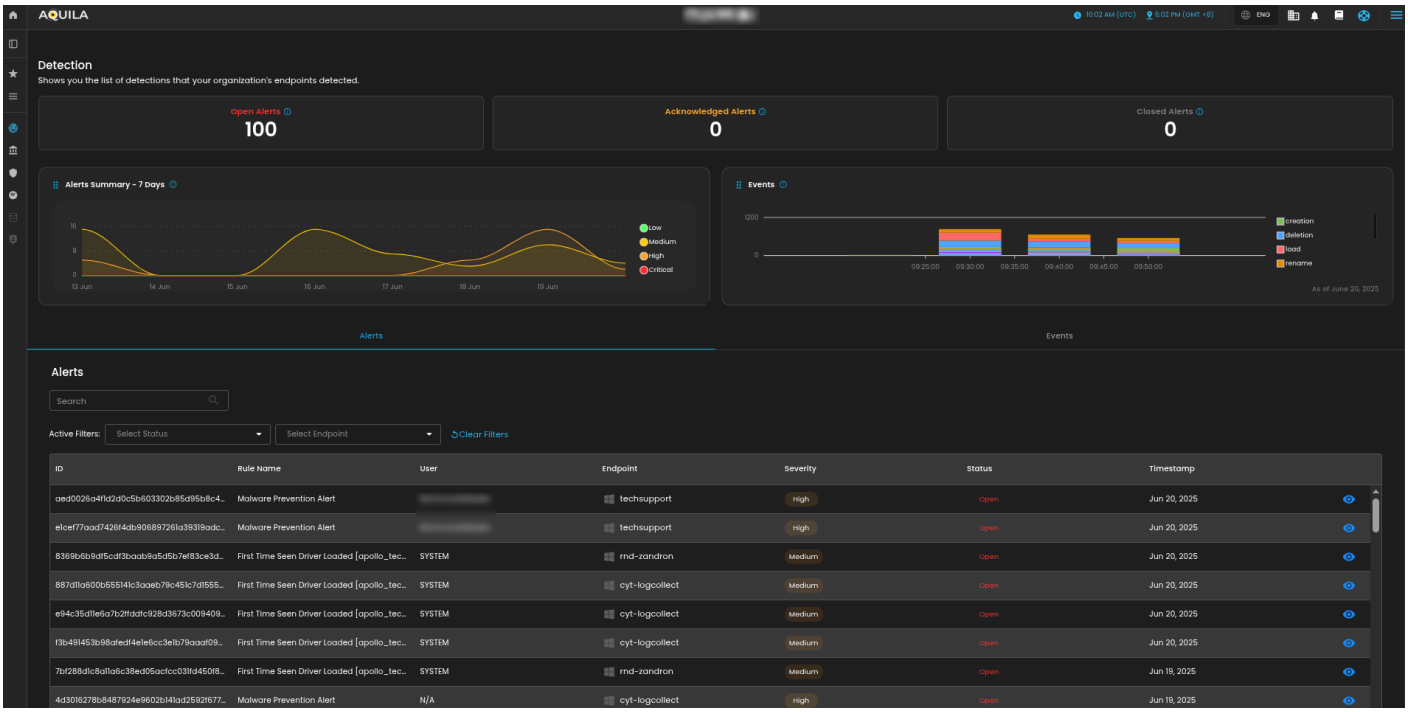


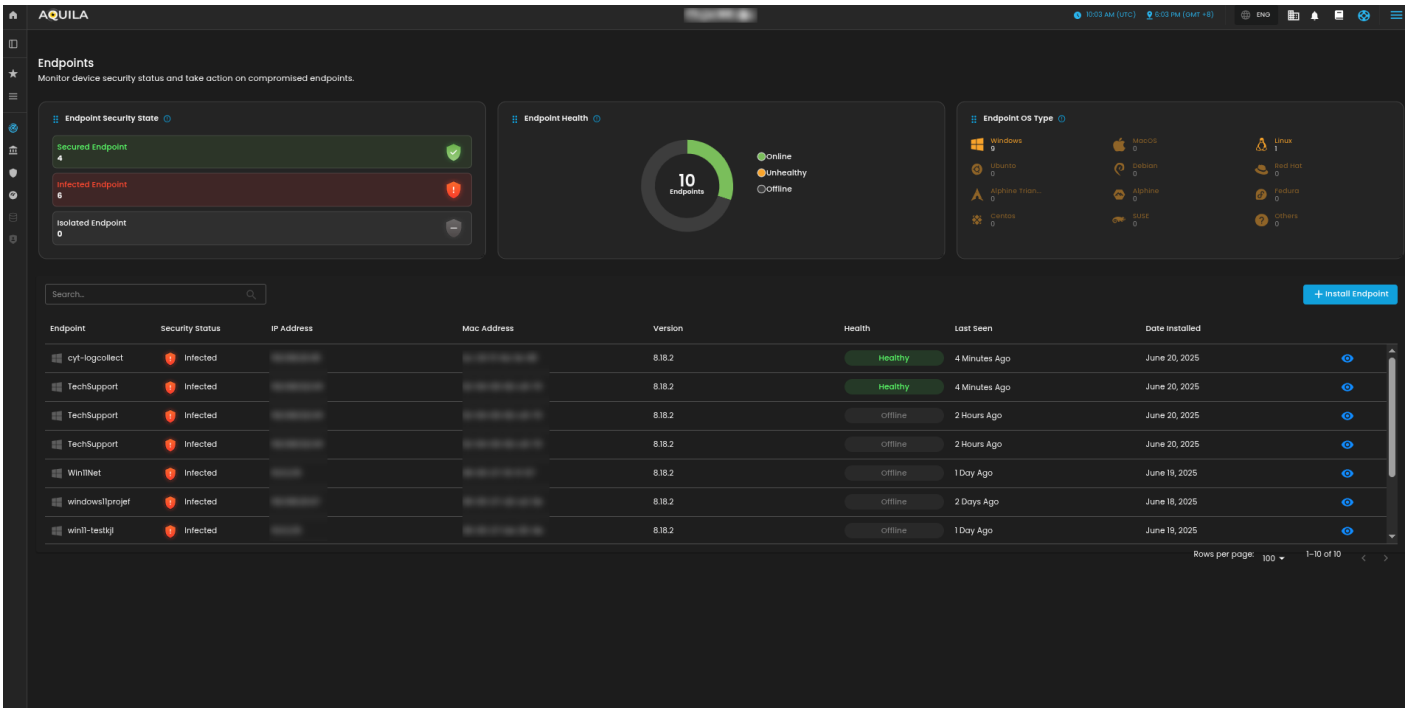
> ***If you encounter ***Log Collector Setup Failed***. Please click "Retry" and carefully go gack to Steps 5 or 6. You can also try "***Manual***" installation. If issues persist please contact our technical support at ***support@cytechint.com*** for prompt assistance and guidance.*



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.







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

Revision #4
Created 15 August 2025 14:44:59
Updated 19 November 2025 16:51:09 by Richmond Abella