

CyTech - AQUILA EDR Automatic

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

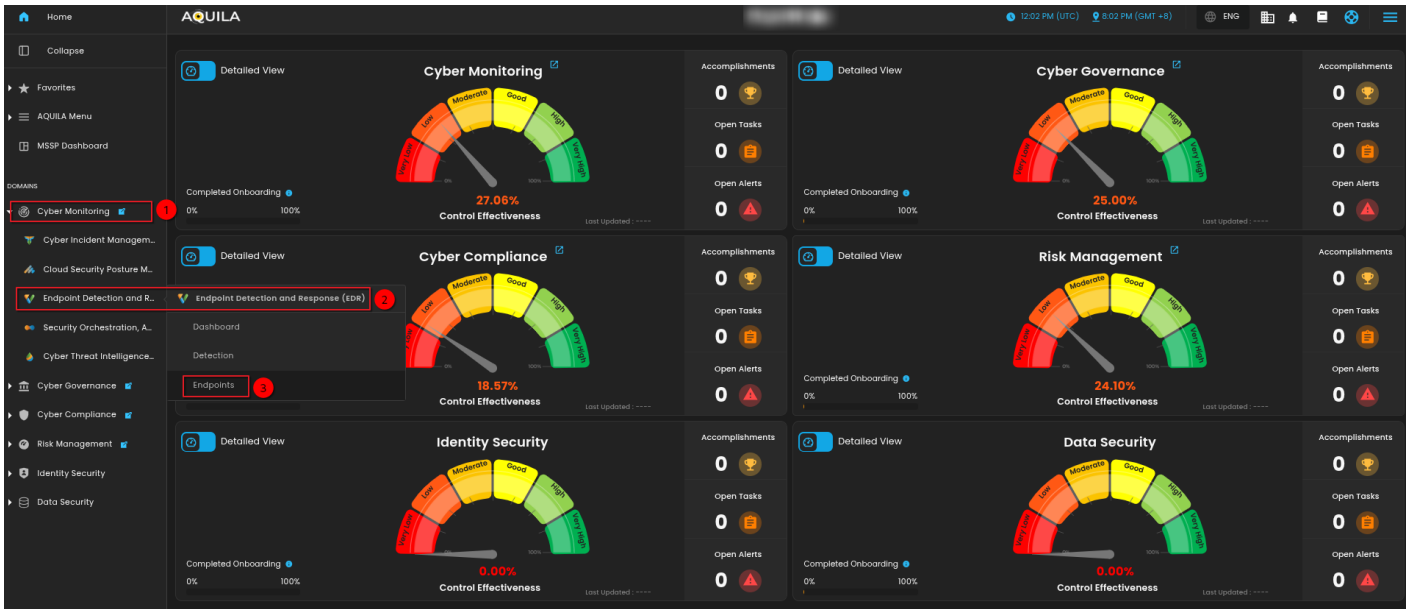
1. Access to CyTech - AQUILA

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

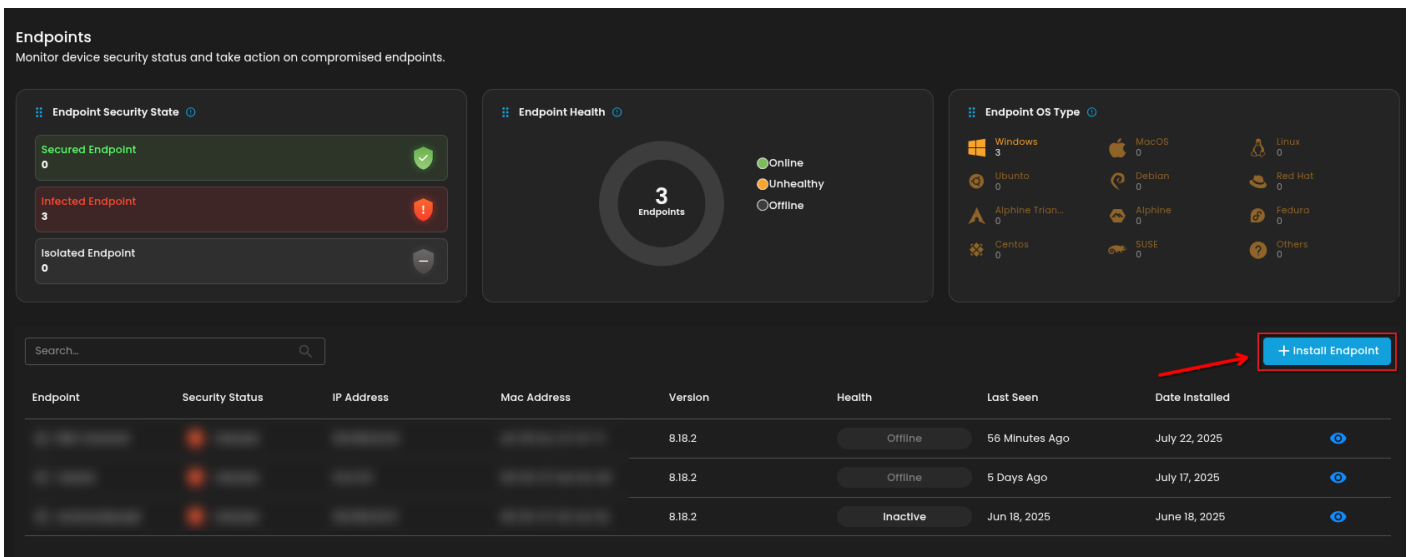
Steps to Add AQUILA EDR

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"**.

Requirements

Make sure you have these things ready to have a smooth installation process of log collector.

Windows


Linux

Mac



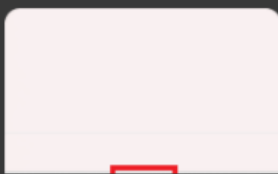
Ready To Install?

Note: Basic understanding of folder navigation using Command Prompt or PowerShell is recommended (e.g., using commands like cd, dir, ls)

Click the book icon  above to view the Requirement Guide documentation.

Before getting started, please make sure you meet the basic requirements below:

- You have a stable Internet Connection.
- Admin Privileges.
- Access to **Command Prompt and PowerShell**



← Back

1 / 4



Next

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

Options

Select your installation method for your log collectors.



Automatic

The Log Collector will automatically download.



Manual

You'll be given instructions for the manual installation of Log Collector.

← Back

2 / 4



Next

5. Download the AQUILA EDR installer.

Options » Automatic Installation



Select Operating System for your Endpoint, Detection and Response Log Collector.

Windows

1



Step 1: Download *

Click the download button and wait for it to finish downloading.



Aquila EDR

2

Download Installer



Step 2: Copy the secret token *

Copy the secret token, it will be used for the installer.



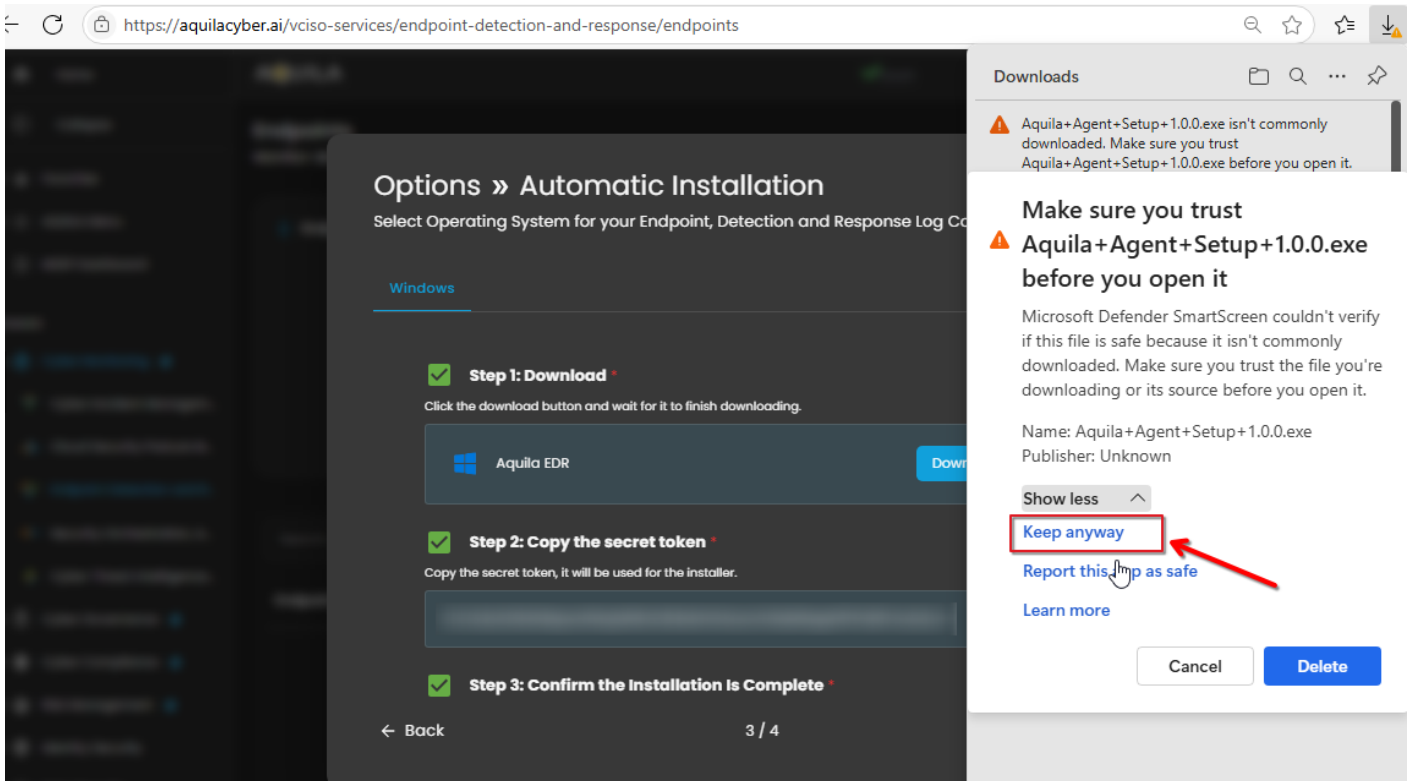
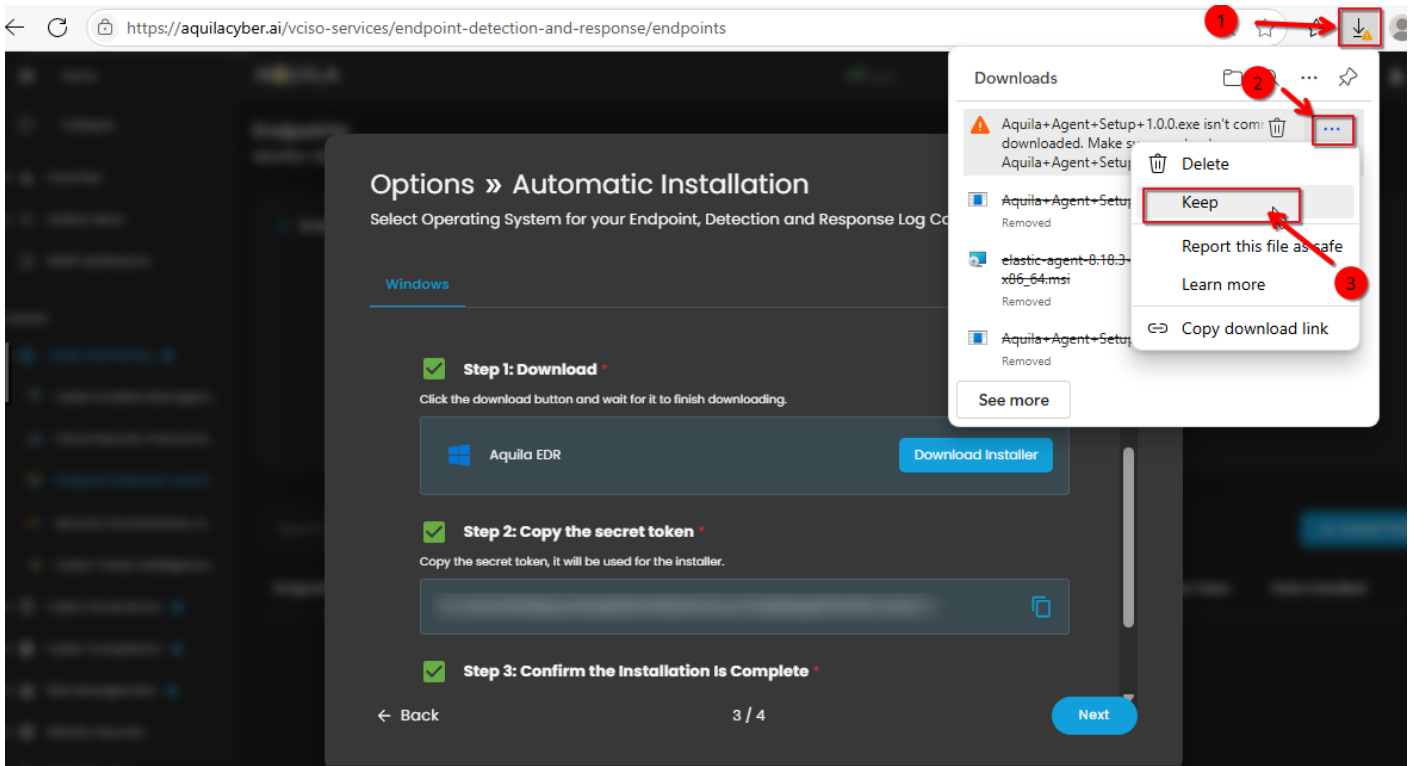
Step 3: Confirm the Installation Is Complete *

← Back

3 / 4

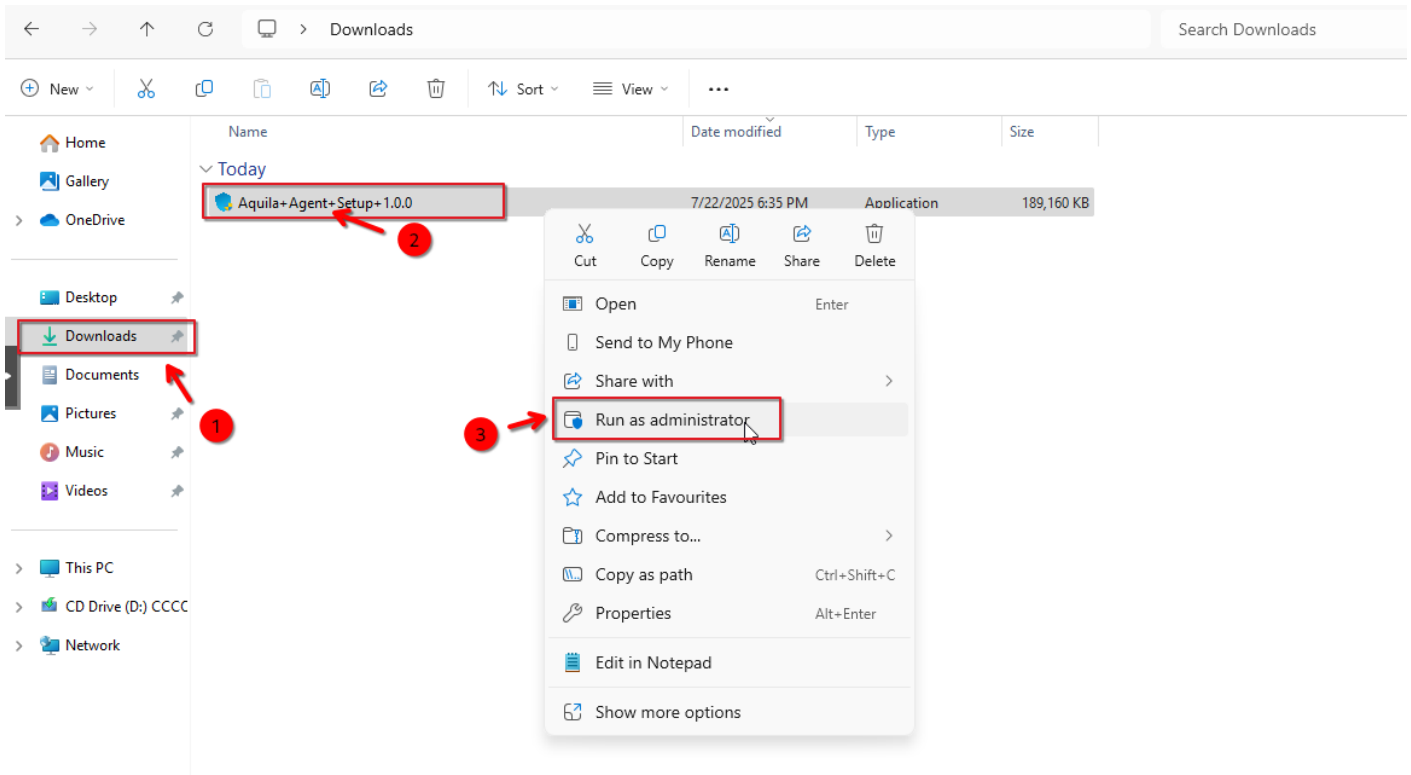
Next

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



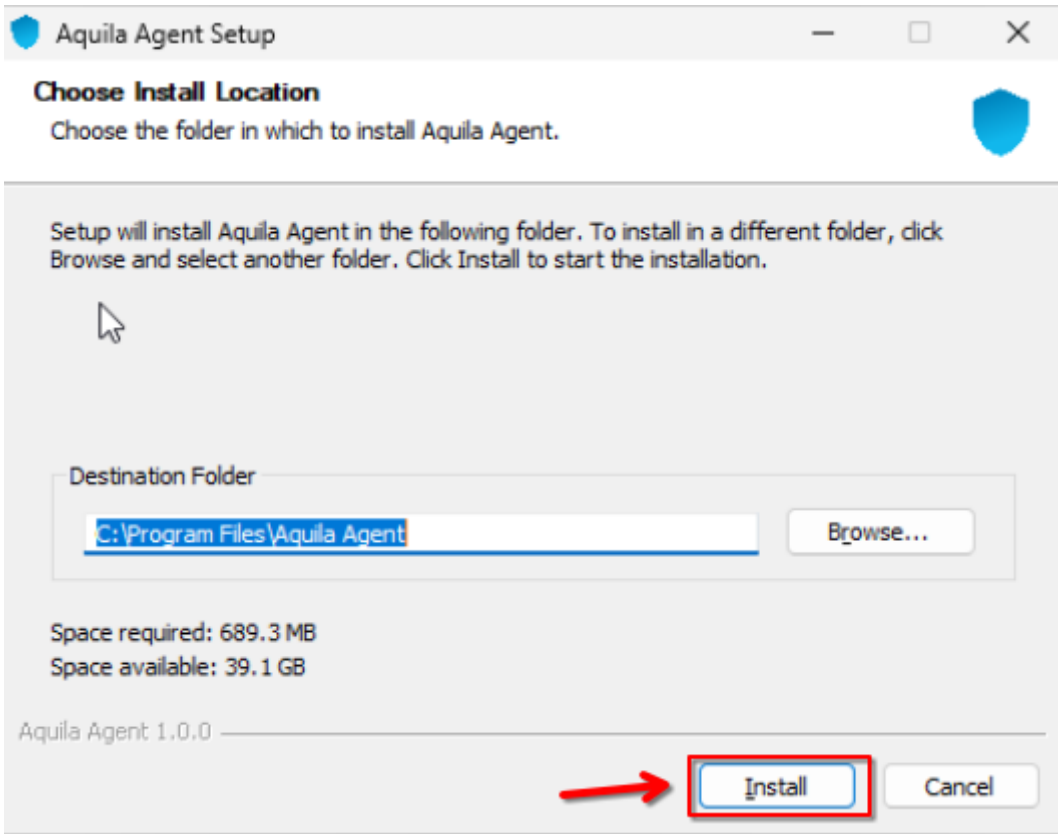
Please follow the instructions below and refer to the images below:

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

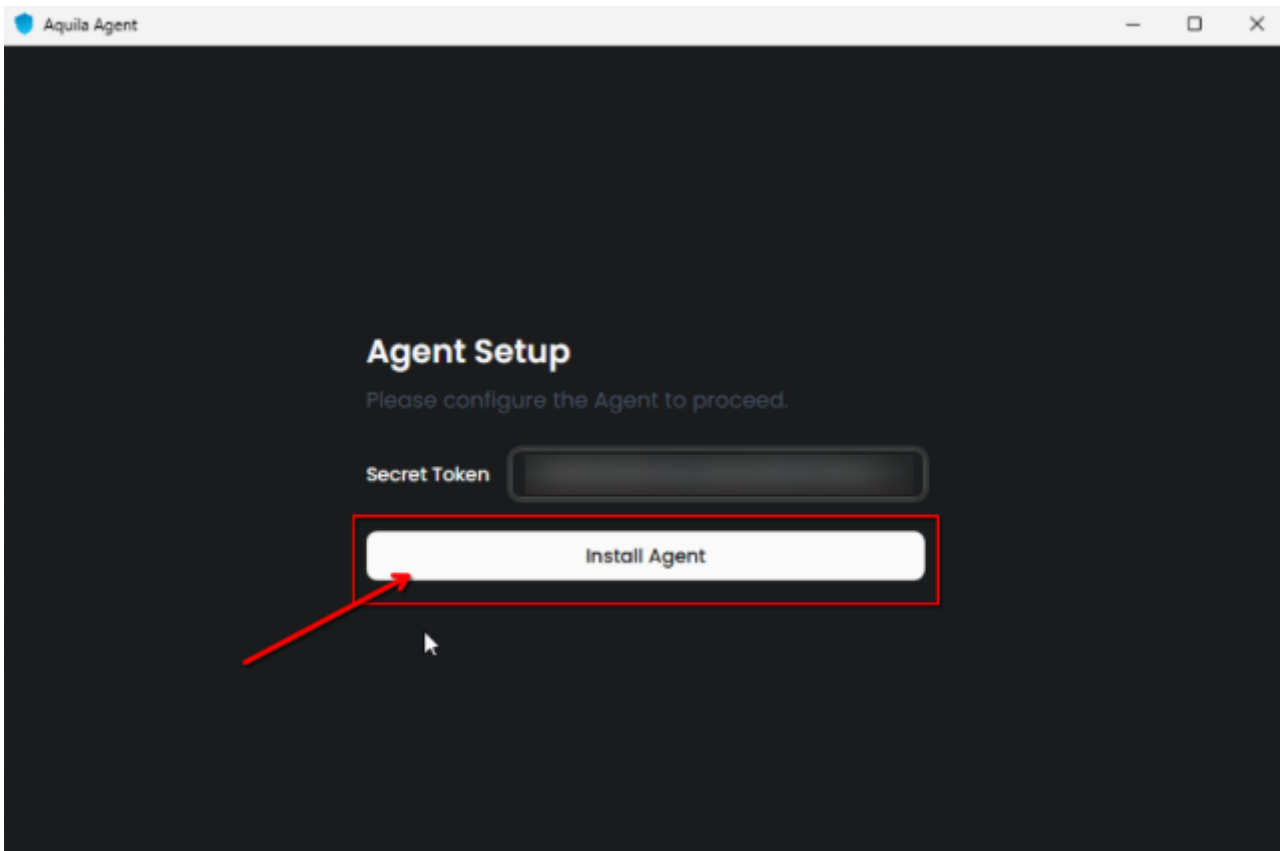


If prompted with a User Account Control (UAC) dialog stating that the app is from an unknown publisher, click **'Yes'** to allow the installer to make changes and proceed with the installation.

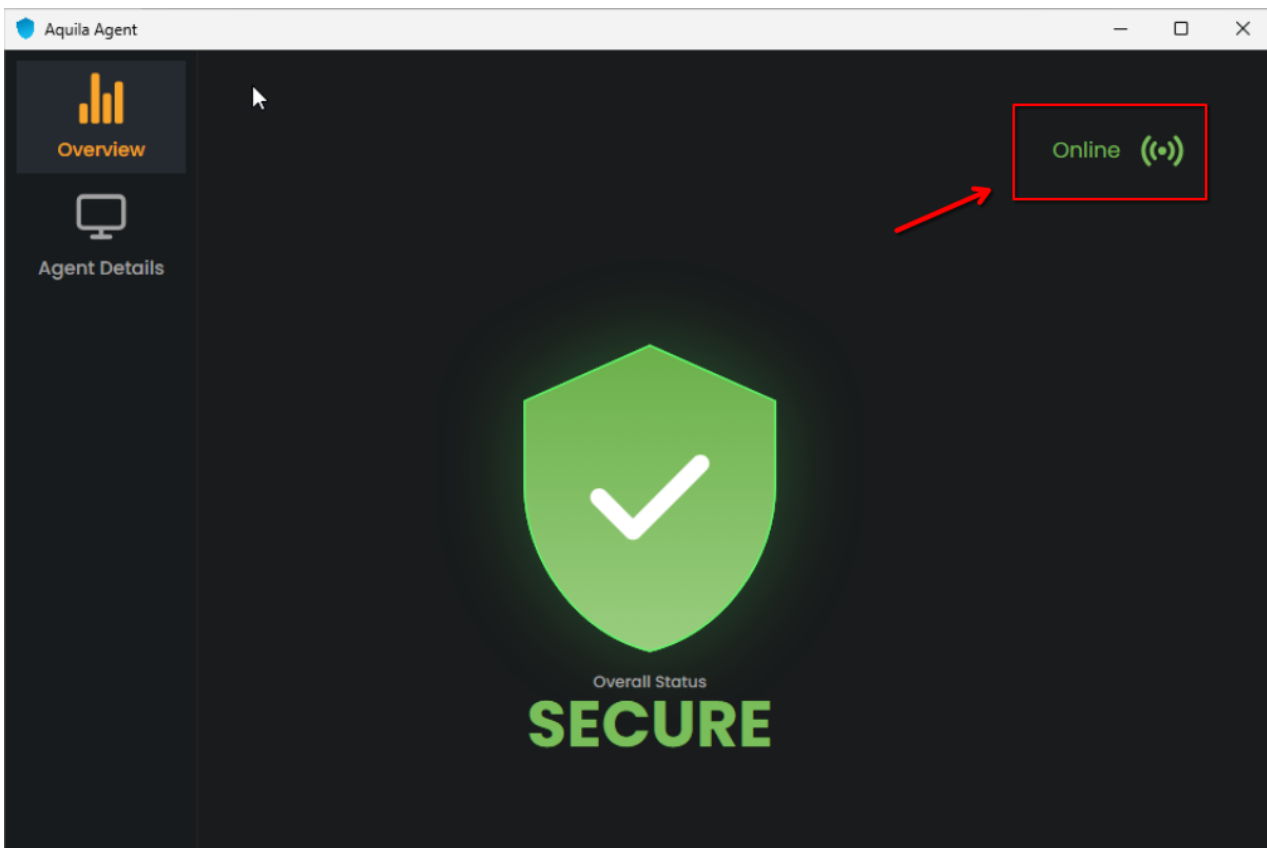
Step 2: You may specify a custom installation directory or proceed with the default path. Click **'Install'** to continue with the installation process. Wait for a moment to install the Aquila Agent. After AQUILA Agent has been successfully installed. Click **"Finish"** to close installation wizard.



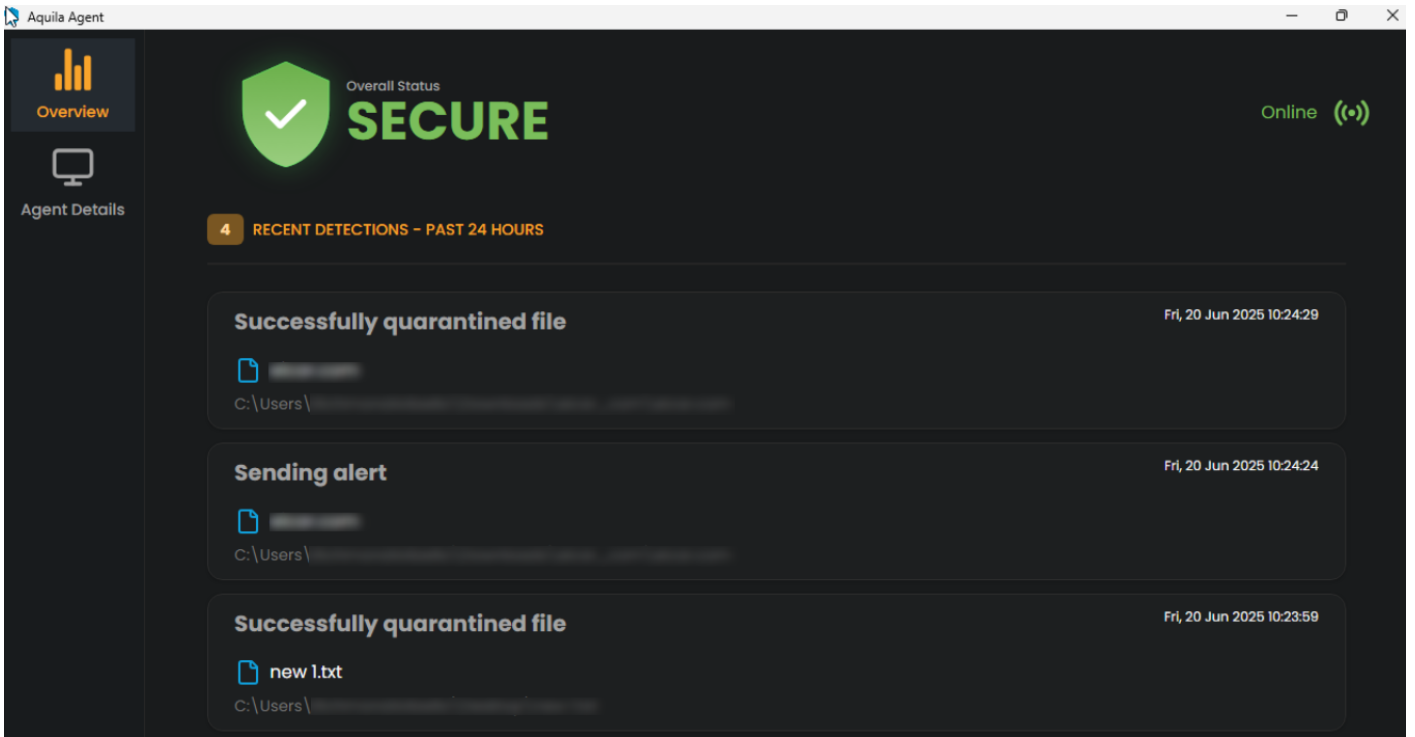
Step 3: Provide the required Secret Token to authorize and proceed with the installation. Click "**Install Agent**" to proceed. Please wait a few minutes for the installation process to complete. This will automatically initiate enrollment into the CyTech - AQUILA platform.



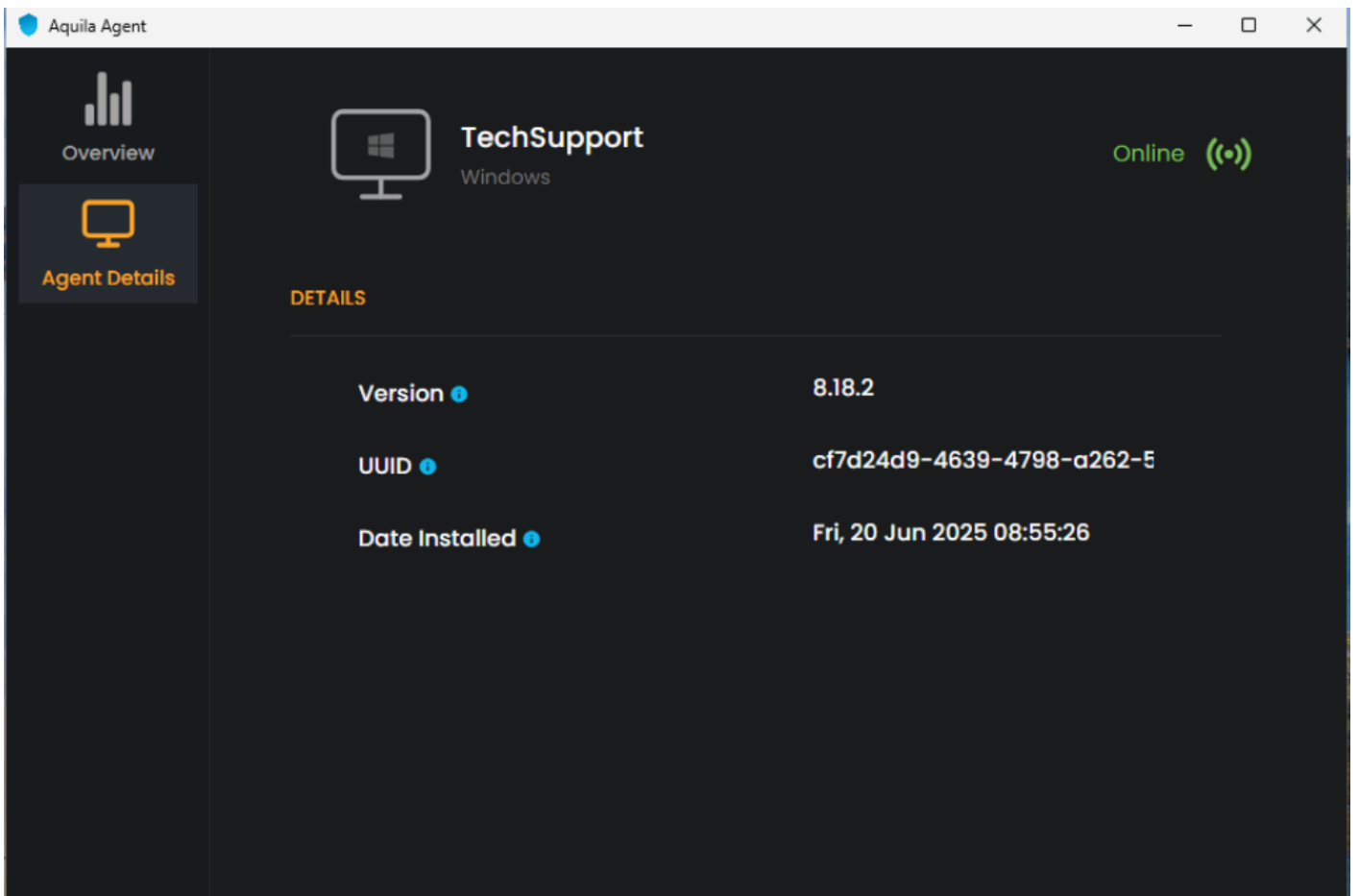
Step 4: After successful enrollment, an overview window will be displayed. Please note that it may take some time for the device to reflect an online status. Ensure the device remains connected to the network for the EDR policy to be properly applied.



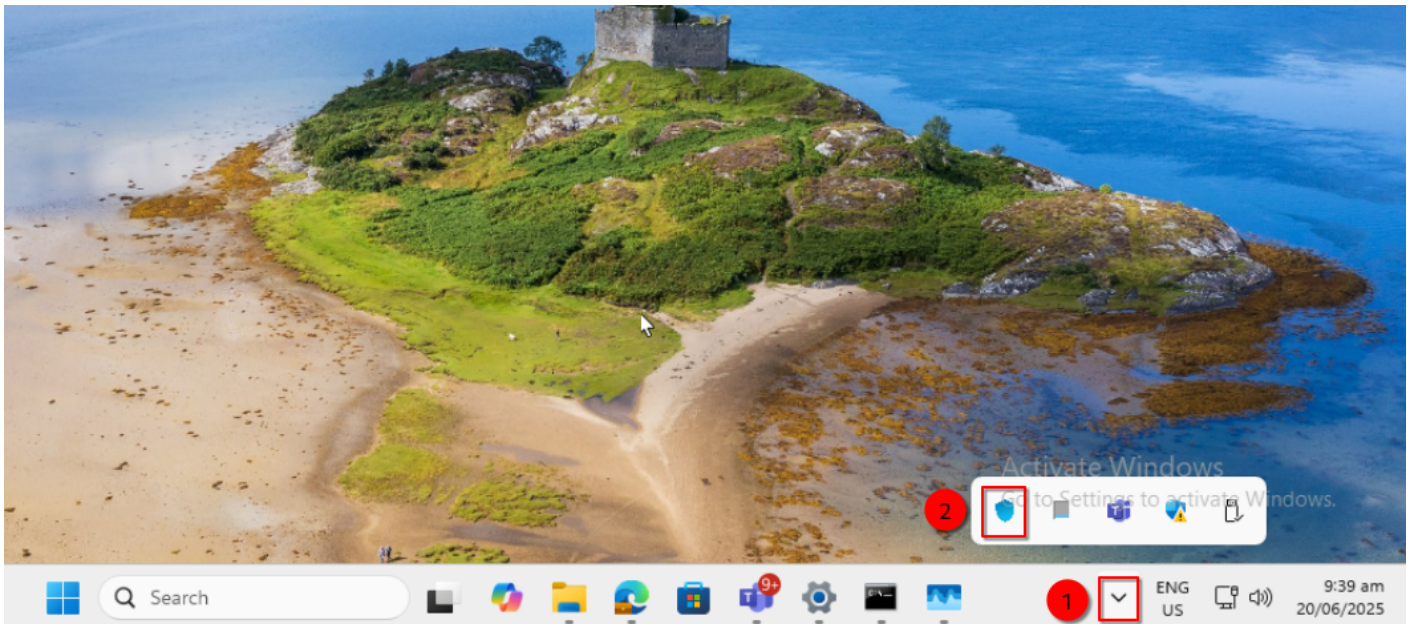
The Overview page provides a centralized dashboard displaying all recent detections related to your endpoint devices. This real-time monitoring allows security teams to quickly identify potential threats, analyze attack vectors, and prioritize response efforts based on severity and impact. By consolidating 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".

Options » Manual Installation

Select Operating System for your Endpoint, Detection and Response Log Collector.

Windows Linux Mac

Step: 1 Sets the PowerShell variable *
Sets the PowerShell variable \$ProgressPreference to 'SilentlyContinue' suppressing progress output during script execution.

```
$ProgressPreference = "SilentlyContinue"
```

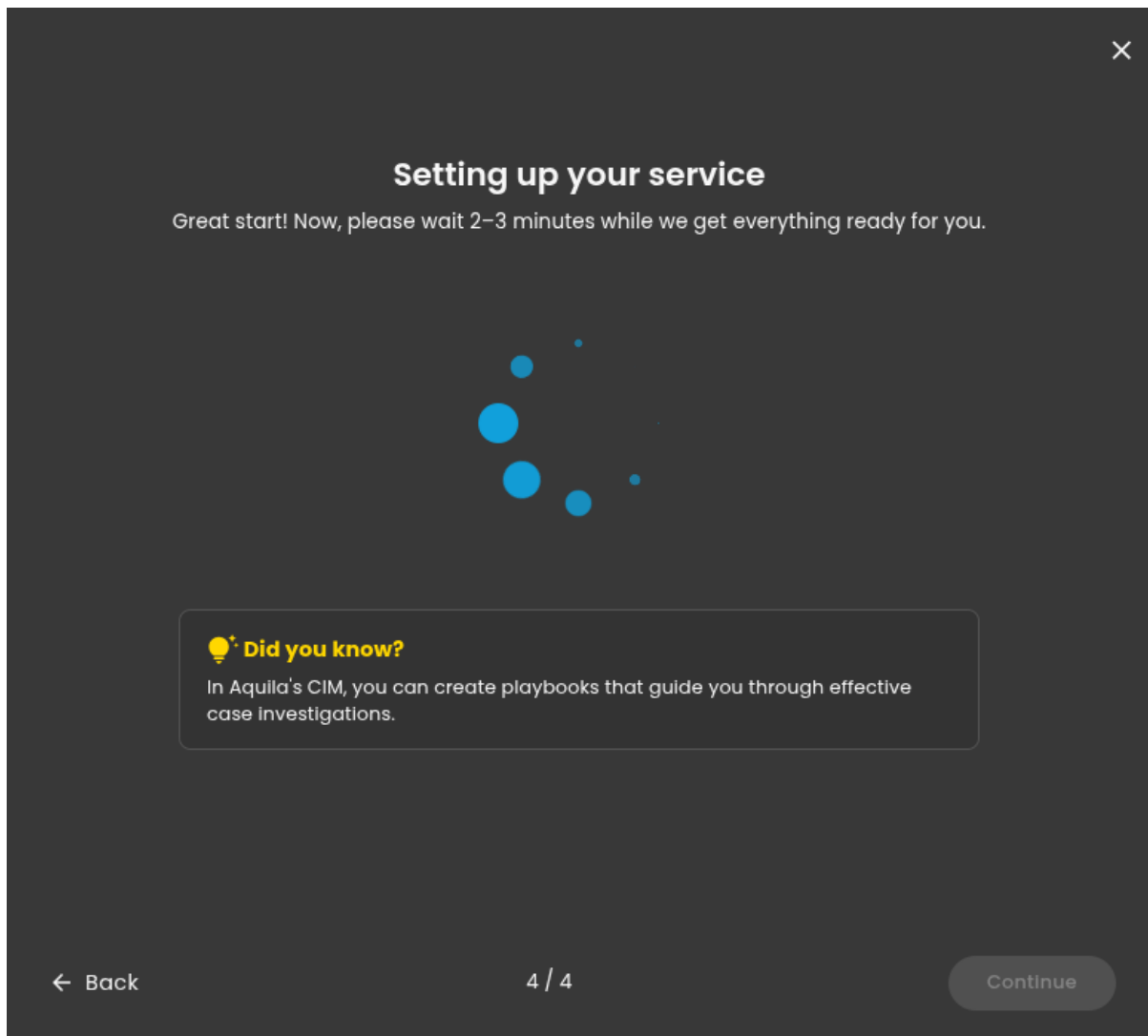
Step: 2 Downloads the Elastic Agent *
Downloads the Elastic Agent version 8.16 for Windows in a zip file using the Invoke-WebRequest cmdlet.

```
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.18.1-windows-x86_64.zip -OutFile elastic-agent-8.18.1-windows-x86_64.zip
```

Step: 3 Extracts the contents of the downloaded zip file *
Extracts the contents of the downloaded zip file (elastic-agent-8.16-windows-x86_64.zip) to the current

← Back 3 / 4 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 successful 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.

Awesome! You're almost there.



By clicking "Continue" you will be redirected to the Settings page to install your Log Sources.



Log Collector Setup Complete

Details

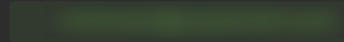
☰ Log Collector

tech-support

⚠ Enable

Enabled

👤 Setup by



📘 "Tip: Add your log Sources"

Press **Continue** to start collecting logs by adding your first log source integration. You can choose from our wide range of supported platforms and services.

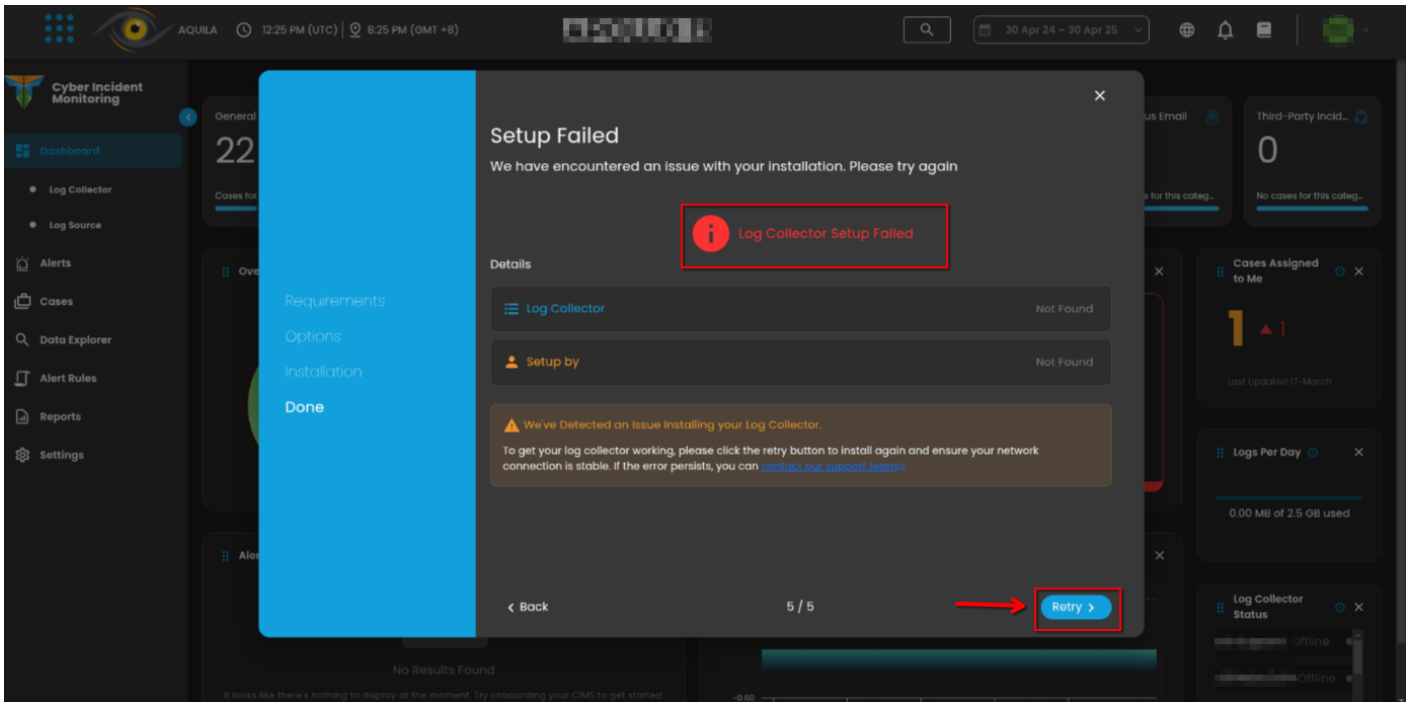
← Back

4 / 4

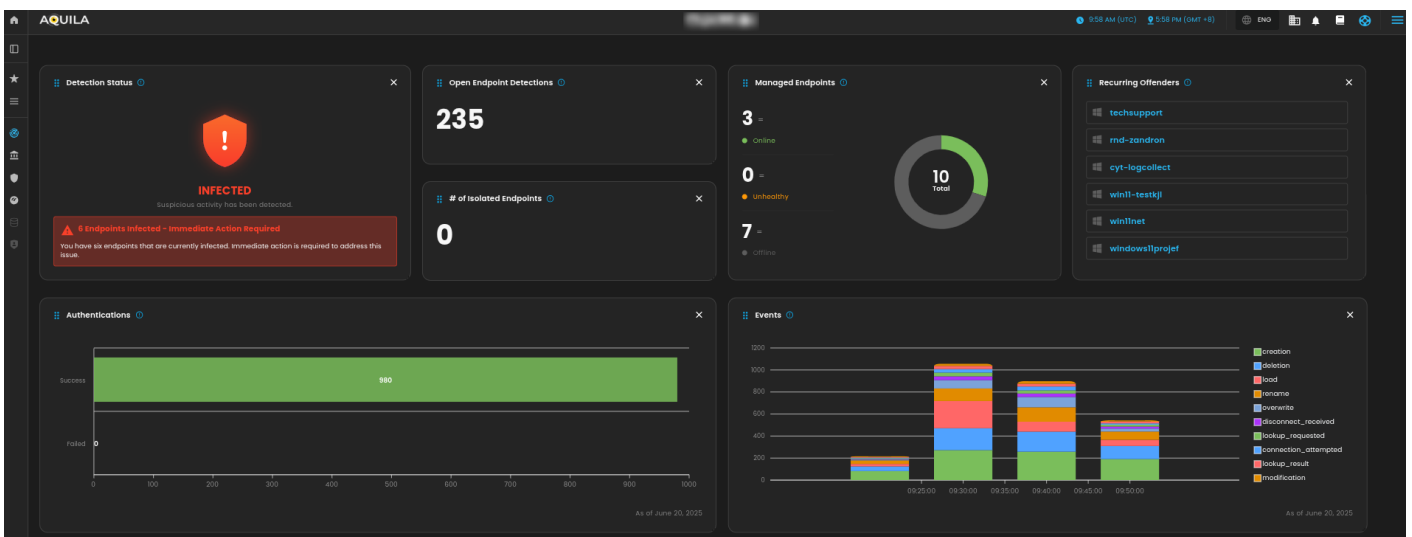


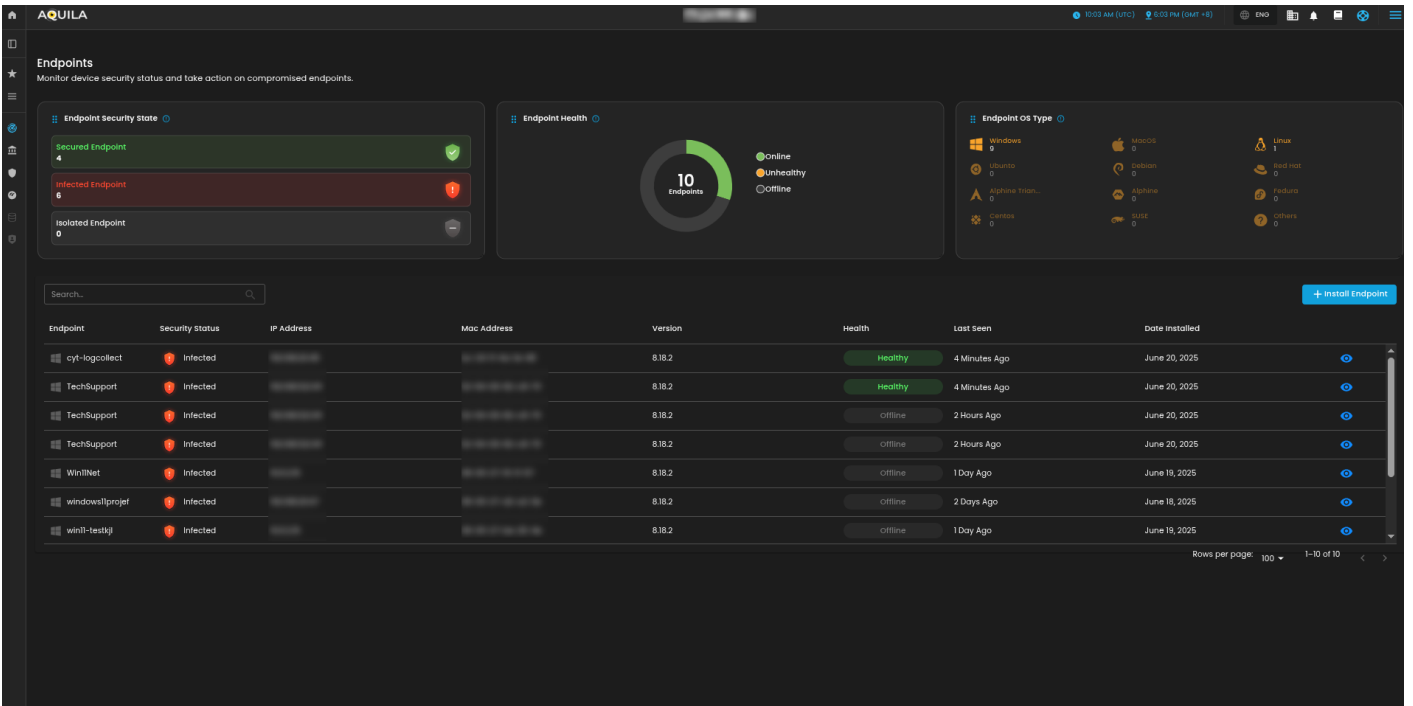
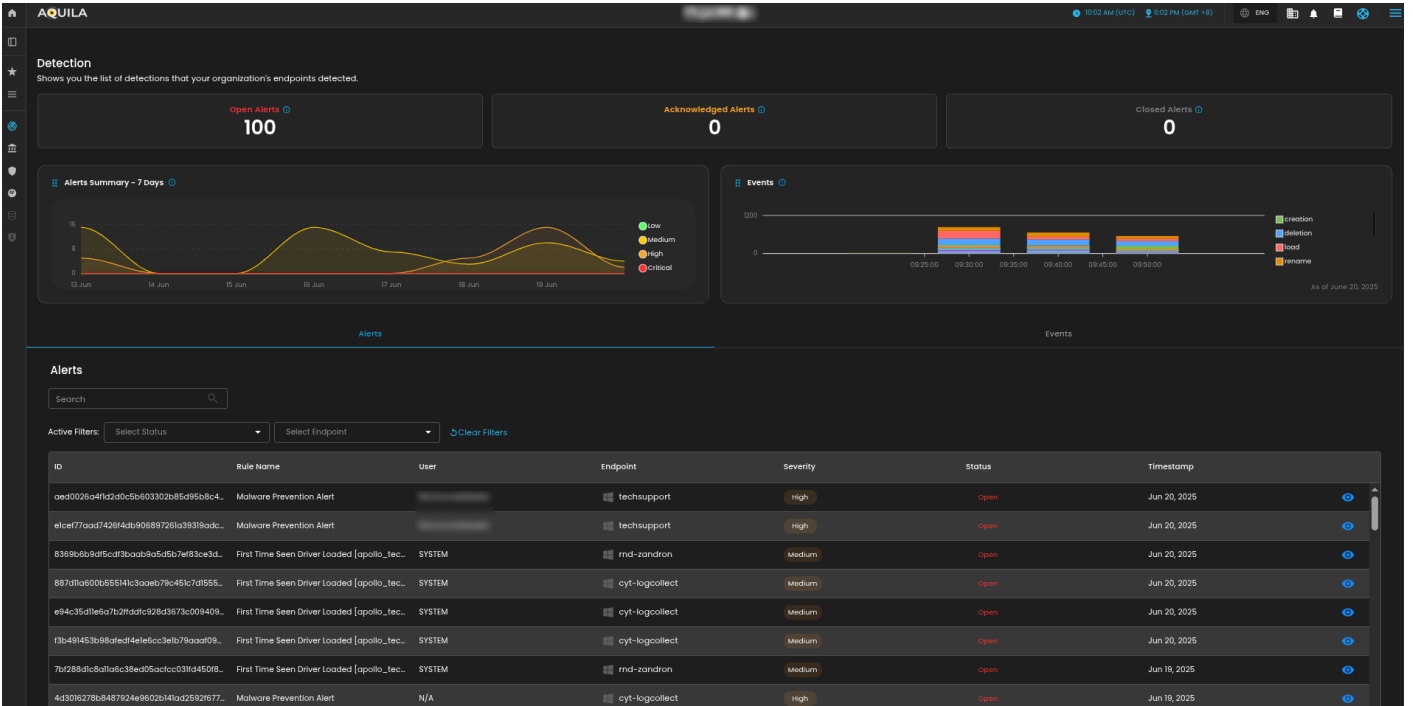
Continue

*****If you encounter *Log Collector Setup Failed*. Please click "Retry" and carefully go back 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 #10

Created 20 June 2025 09:44:15 by Richmond Abella

Updated 18 November 2025 06:20:52