

Endpoint Detection and Response (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.

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

Step 1: Login to CyTech - Aquila "cytechint.io" and navigate to Aquila Modules at leftmost corner of the dashboard.

Step 2: Go to Cyber Monitoring > Endpoint Detection and Response (EDR, MDR).

The screenshot shows the AQUILA dashboard interface. At the top, there is a header with the AQUILA logo, a clock showing 7:55 AM (UTC), and a location indicator showing 3:55 PM (GMT +8). Below the header is a 'Favorites' section. The main content area is titled 'AQUILA MODULES' and lists several modules with expandable options:

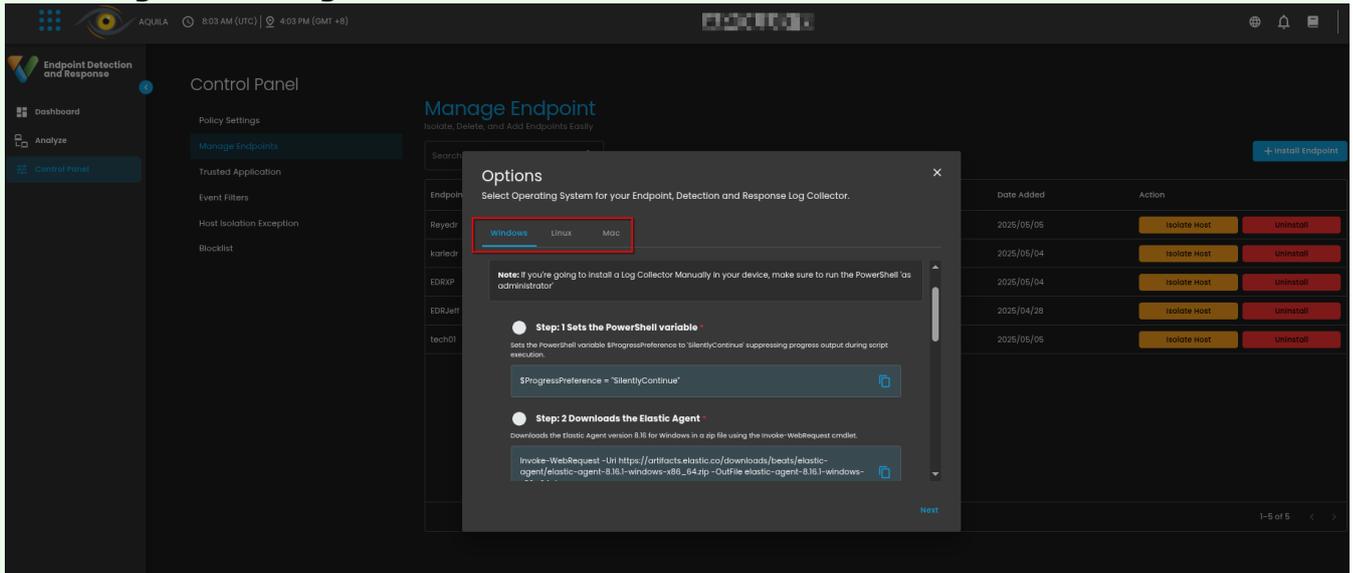
- Cyber Assessment (7) +
- Cyber Governance (6) +
- Cyber Resiliency (2) +
- Cyber Monitoring (4) -** (highlighted with a red box)
 - Cyber Incident Management (SIEM and XDR)
 - Endpoint Detection and Response (EDR, MDR)** (highlighted with a red box)
 - Security Orchestration, Automation and Response (SOAR)
 - User and Entity Behavior Analysis (UEBA)
- CISO Toolsets (6) +

Step 4: Navigate through Control Panel > Manage Endpoints > Install Endpoint > Choose Manual.

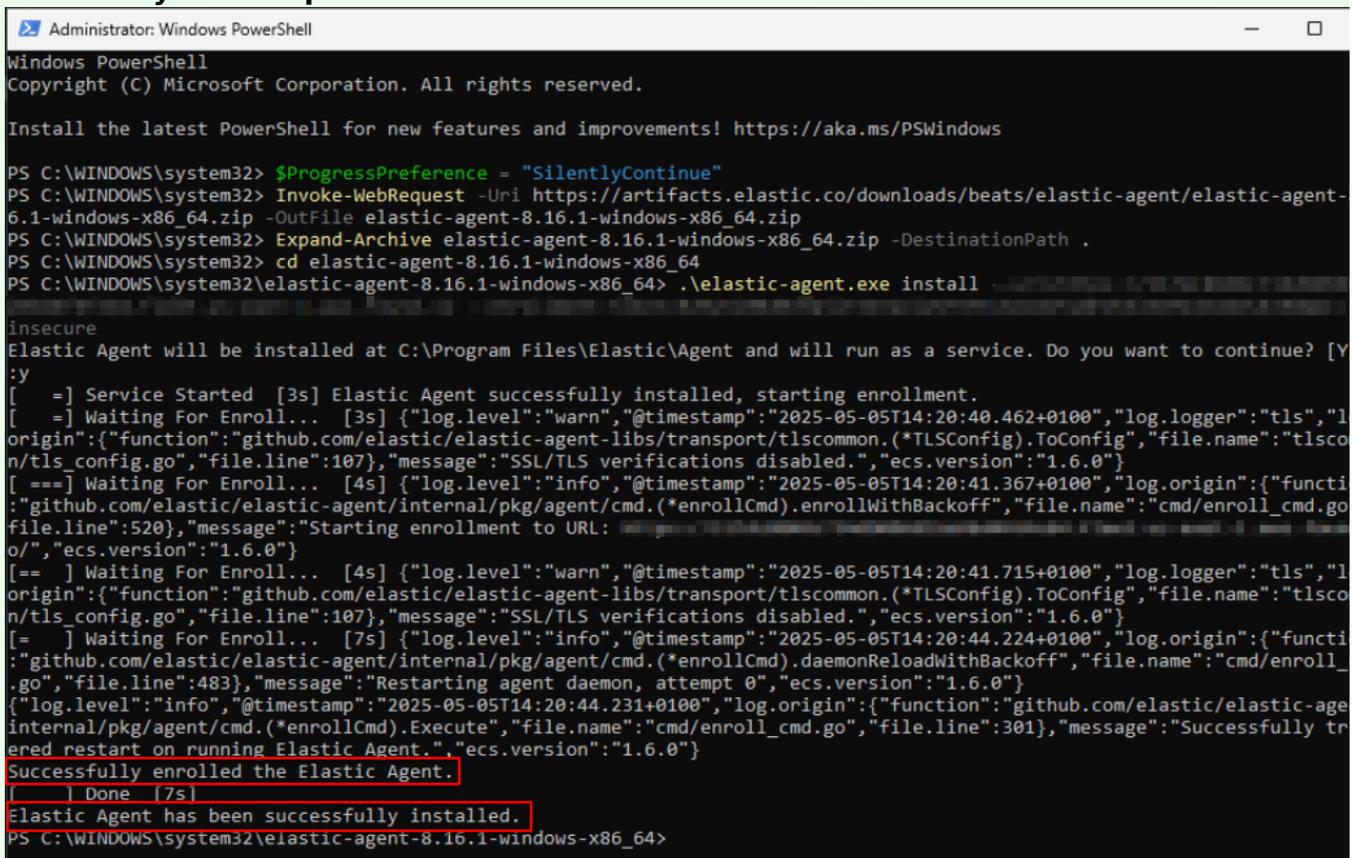
The screenshot shows the 'Manage Endpoint' control panel in the AQUILA interface. The left sidebar has 'Control Panel' highlighted with a red box. The main content area is titled 'Manage Endpoint' and includes a search bar and a table of endpoints. The 'Install Endpoint' button in the top right corner is highlighted with a red box, and the 'Manual' option is also highlighted with a red box.

Endpoint	Last Seen	Operating system	Status	Date Added	Action
[Icon]	6 hours ago	Linux	Offline	2025/05/05	Isolate Host Install Endpoint Automatic Manual
[Icon]	1 day ago	Linux	Offline	2025/05/04	Isolate Host Uninstall
[Icon]	2 days ago	Linux	Offline	2025/05/04	Isolate Host Uninstall
[Icon]	7 days ago	Linux	Offline	2025/04/28	Isolate Host Uninstall
[Icon]	2 minutes ago	Linux	Healthy	2025/05/05	Isolate Host Uninstall

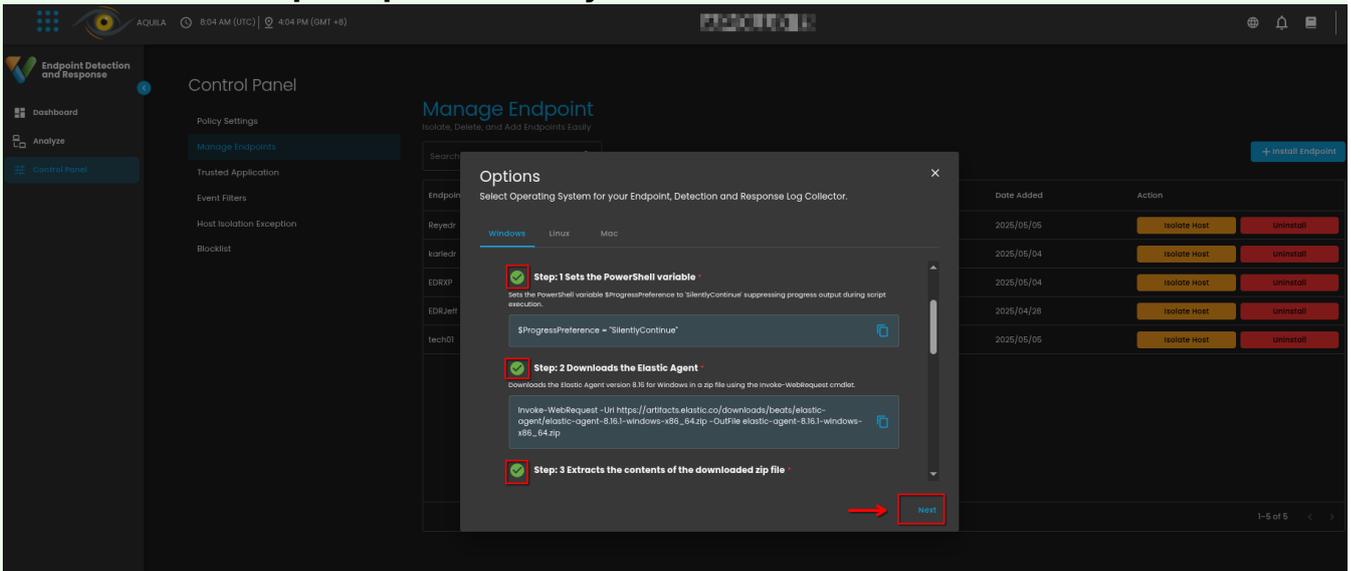
Step 8: Choose the correct Operating System for your endpoint. After choosing the type of your Operating System, the commands will display below needed for installing the EDR agent.



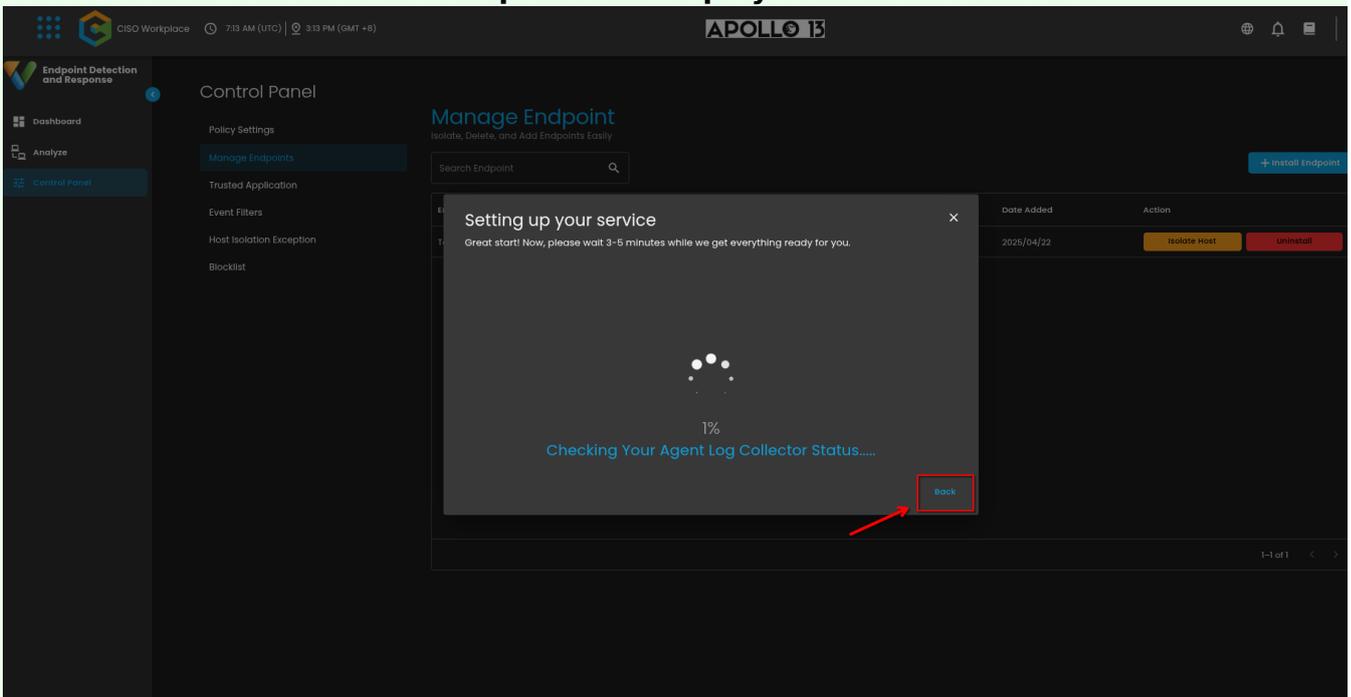
Step 9: Execute the command in your Endpoint environment using powershell or terminal under admin privilege. Once the commands are executed successfully, you should see an output similar to the example shown in the image below. Go back to Cytech - Aquila to finish manual installation.



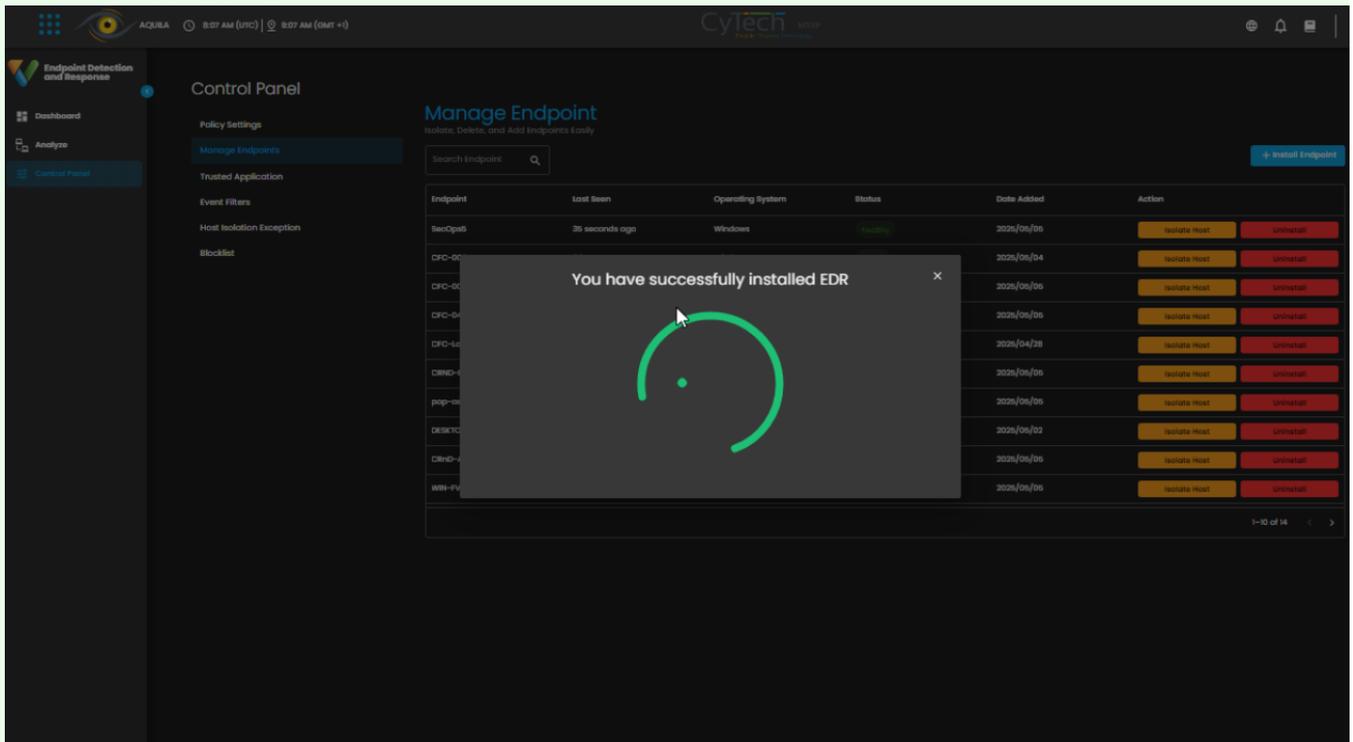
Step 10: Before you can proceed to the final installation set-up make sure you check off each steps required. Then you can click "Next".



Step 11: 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.



Step 12: This step confirms the successful installation and enrollment of the **EDR Agent** with the fleet server.



Revision #2

Created 22 April 2025 06:14:58 by Richmond Abella

Updated 28 May 2025 09:04:23 by Richmond Abella