AQUILA EDR Deployment via GPO on Windows Server AD

This document provides a step-by-step guide for deploying **AQUILA Endpoint Detection and Response (EDR)** on Windows Server environments using **Group Policy Objects (GPO)**. The purpose of this guide is to streamline the installation process, ensure consistent configuration across domain-joined systems, and simplify centralized management of the EDR agent. By leveraging Group Policy, administrators can enforce deployment at scale, reduce manual installation efforts, and maintain stronger security coverage across the organization's Windows Server infrastructure.

Scope & Audience

This guide is intended for **system administrators, IT operations teams, and security engineers** responsible for managing Windows Server environments within an Active Directory domain. The deployment process outlined here applies to Windows Server editions that support Group Policy and assumes administrative privileges within the domain.

The scope of this document covers:

- Preparing the Windows Server environment for **AQUILA EDR** deployment
- Configuring and applying Group Policy Objects (GPO) for automated agent installation
- Ensuring consistent and secure deployment across domain-joined systems

This document does not cover post-deployment tasks such as advanced policy tuning, threat hunting, or incident response workflows.

Prerequisites

Before beginning the deployment of **AQUILA EDR** via Group Policy, ensure the following requirements are met:

1. **Administrative Permissions**
   - Domain Administrator or delegated privileges to create and manage Group Policy Objects (GPOs).
   - Local Administrator rights on the Windows Server hosting the installer.
2. **Windows Server Environment**
   - Active Directory domain configured and operational.
   - Supported Windows Server editions (2016, 2019, 2022).
   - Network connectivity between domain controllers and target machines.
3. **AQUILA EDR Installer Package**
   - Latest version of the **AQUILA EDR ZIP** file obtained

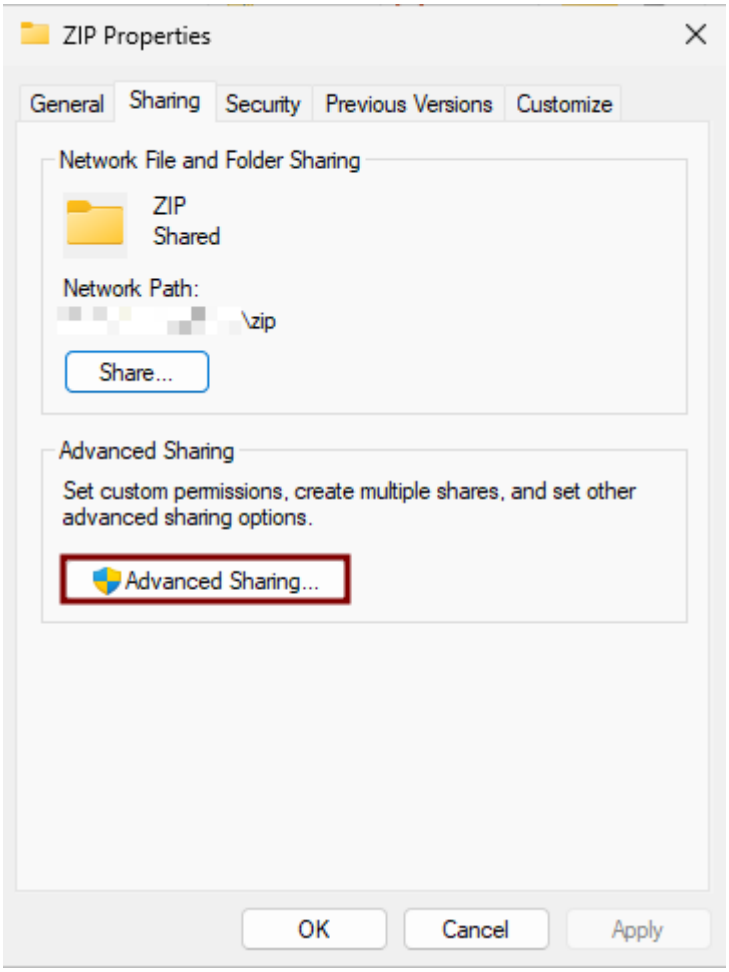
- Obtained the **script** to be setup on the GPO
- Installer stored in a **shared network location (UNC path)** accessible to all domain-joined endpoints.

4. **Group Policy Management Tools**
   - Group Policy Management Console (GPMC) installed on the Windows Server or administrator workstation.
5. **Security & Firewall Considerations**
   - Ensure that outbound communication to **AQUILA EDR cloud services** is allowed.
   - Verify no local security policies block software installation.
6. **Testing Environment**
   - At least one test machine joined to the domain to validate deployment before organization-wide rollout.

Creating a UNC Path for the AQUILA EDR ZIP file and for Centralize Logs

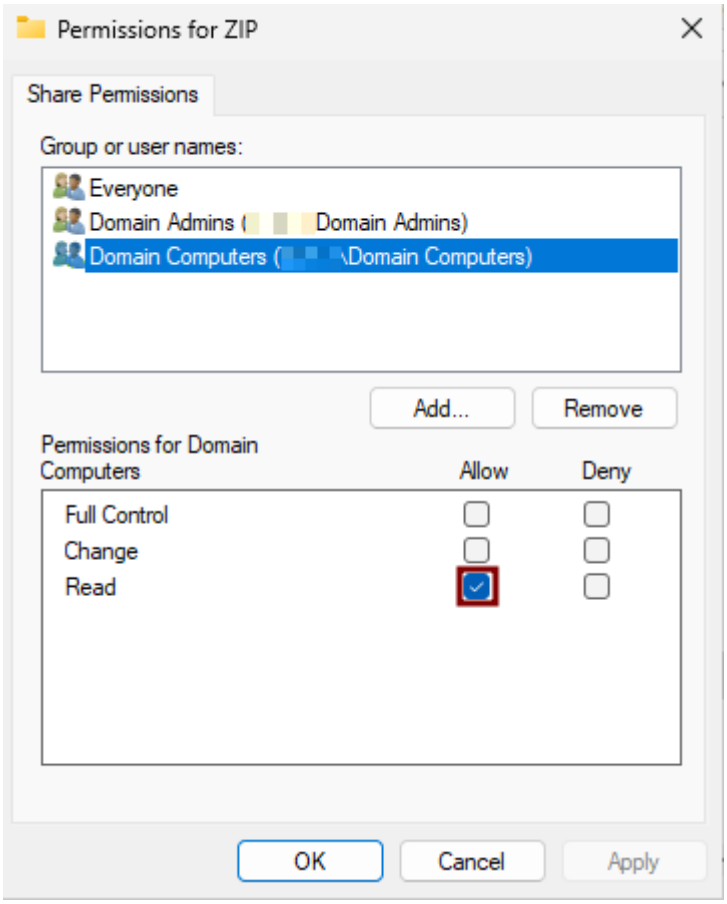
To ensure domain-joined computers can access the **AQUILA EDR ZIP** file package and folder for centralizing logs, create a shared network folder and configure appropriate permissions.

1. **Create a ZIP Folder**
   - On a file server, create a folder (e.g., `C:\ZIP`).
   - Copy the `edr-agent-8.18.1-windows-x86_64.zip` file into this folder.
2. **Enable Folder Sharing**
   - Right-click the `ZIP` folder and select **Properties**.
   - Navigate to the **Sharing** tab and click **Advanced Sharing**.

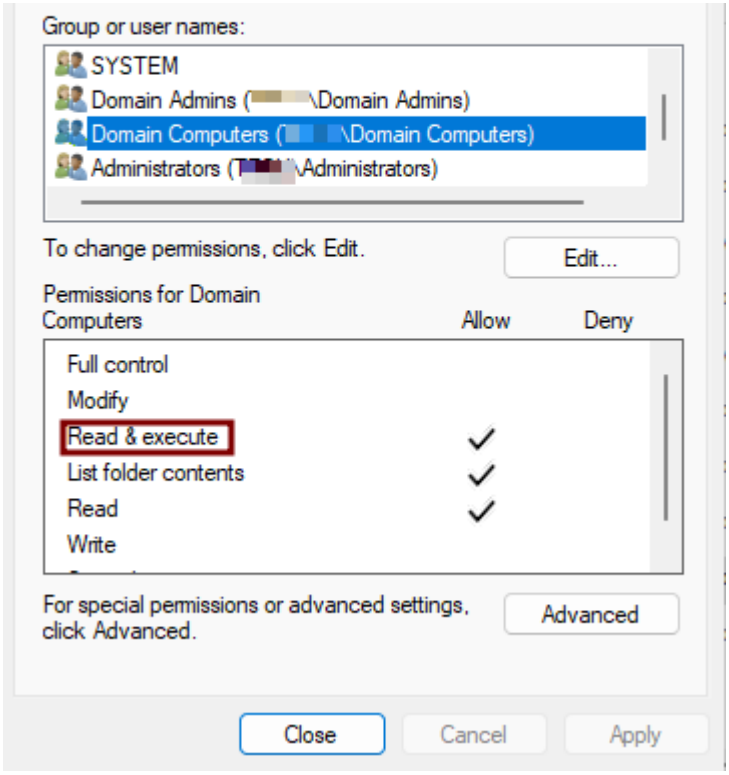


    - Check the box **Share this folder**.

3. **Set Permissions**
    - Click **Permissions**.
    - Grant the **Read** permission to `Domain Computers`.
    - Grant the **Full Control** permission to `Domain Admins`.



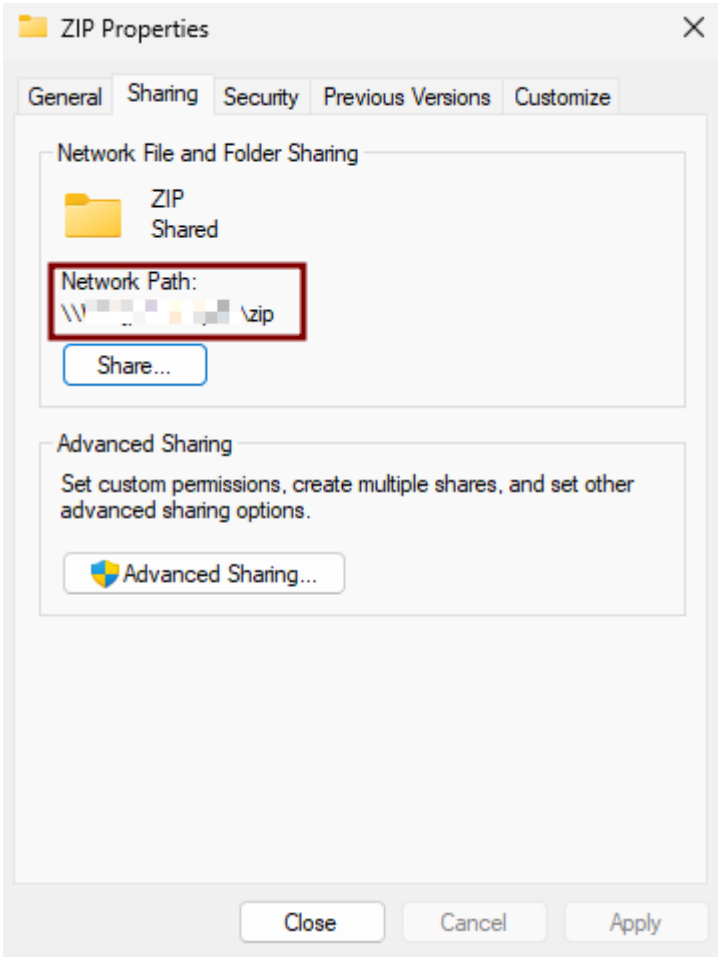
- Also, in the **Security** tab, grant the **Read & execute** permission to `Domain Computers` and **Full control** permission to `Domain Admins`.



- Click **Apply**, then **OK** to confirm the changes.

4. **Save the Network Path**

    - Note the **Network Path** displayed in the Sharing tab (e.g., `\\<ServerHostName>\ZIP`).
    - This UNC path will be required when configuring the script for the Group Policy Object (GPO) deployment.



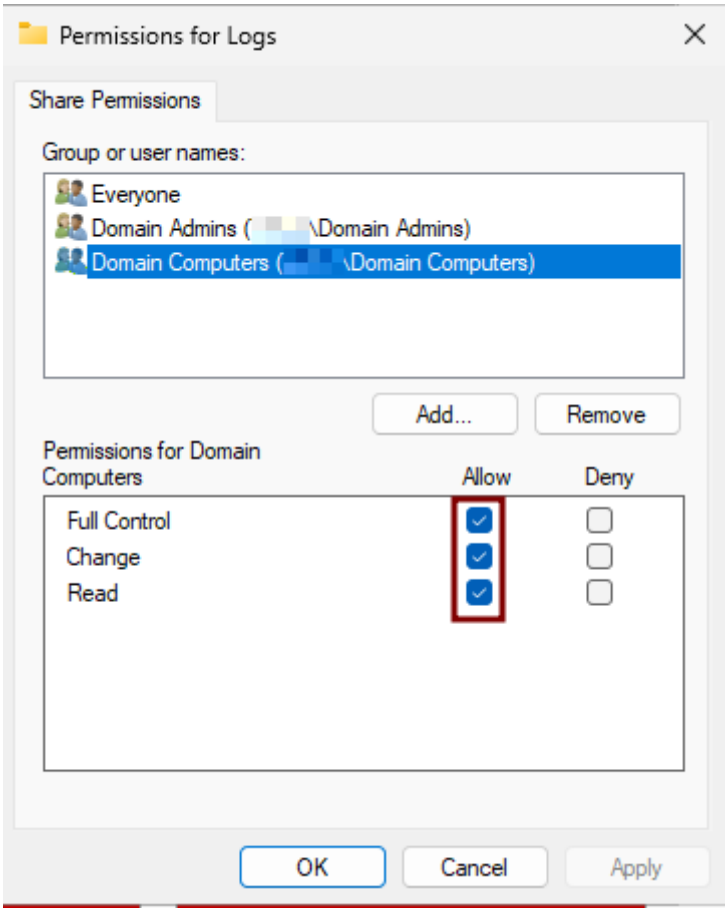
5. **Create the Logs Folder**

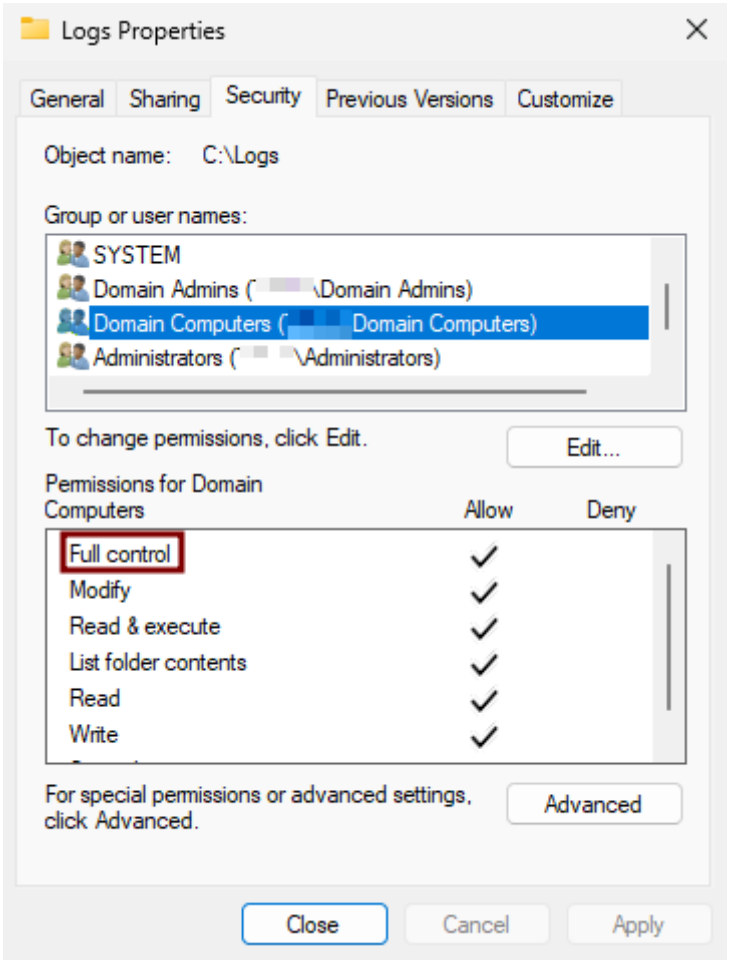
The purpose of this **Logs** folder is to centralize all log processes from every endpoint where the EDR is deployed within the domain. This setup allows us to verify whether each endpoint has successfully installed the EDR and to easily identify and troubleshoot any errors that may occur during deployment.

- On a file server, create a folder (e.g., `C:\Logs`).

6. **Set Permissions**

- Grant the **Full Control** permission to both `Domain Computers` and `Domain Admins`.
- Do the same on the **Security** tab.
- Note the **Network Path** displayed in the Sharing tab (e.g., `\\<ServerHostName>\Logs`)


Permissions for Logs
Share Permissions
Group or user names:
Everyone
Domain Admins (\Domain Admins)
Domain Computers (\Domain Computers)
Add...
Remove
Permissions for Domain Computers
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply


Logs Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Logs
Group or user names:
SYSTEM
Domain Admins (\Domain Admins)
Domain Computers (Domain Computers)
Administrators (\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Domain Computers
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
Close
Cancel
Apply

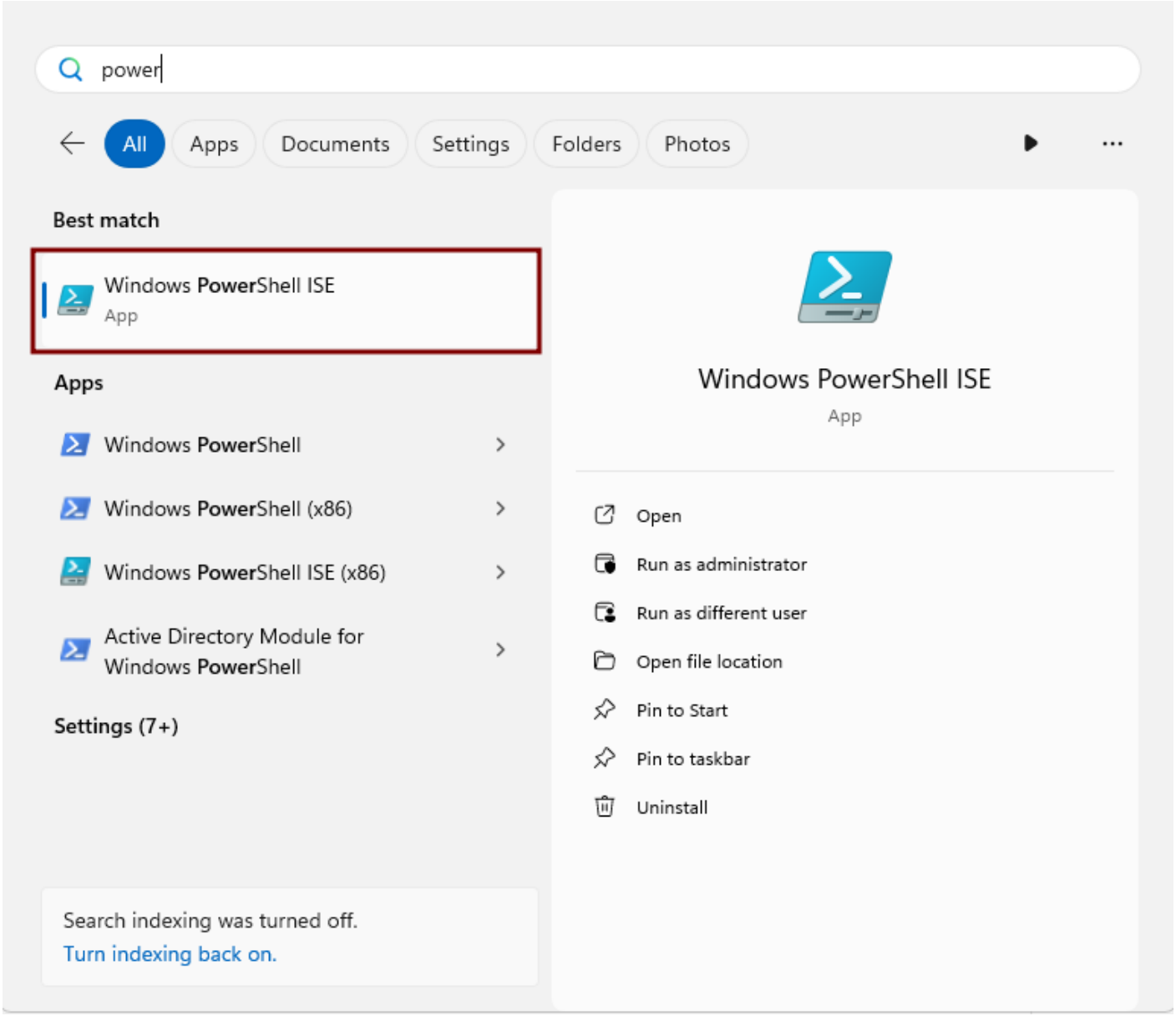
- Also don't forget to create one folder where you can save the **script** and should be shared advance and that has the same permission as the **ZIP** folder since when creating a GPO policy, it only accepts **UNC Path**.

> **NOTE:**
> **If you already have a dedicated folder for storing the ZIP file and centralized logs, we can use that location. Just make sure to take note of its UNC path, as we'll need it when updating the deployment script later.**
>
> **Alternatively, we can update the script for you and send it back—so all you need to do is save the script and configure the Group Policy to deploy it. If you prefer this option, please email us at support@cytechint.com.**

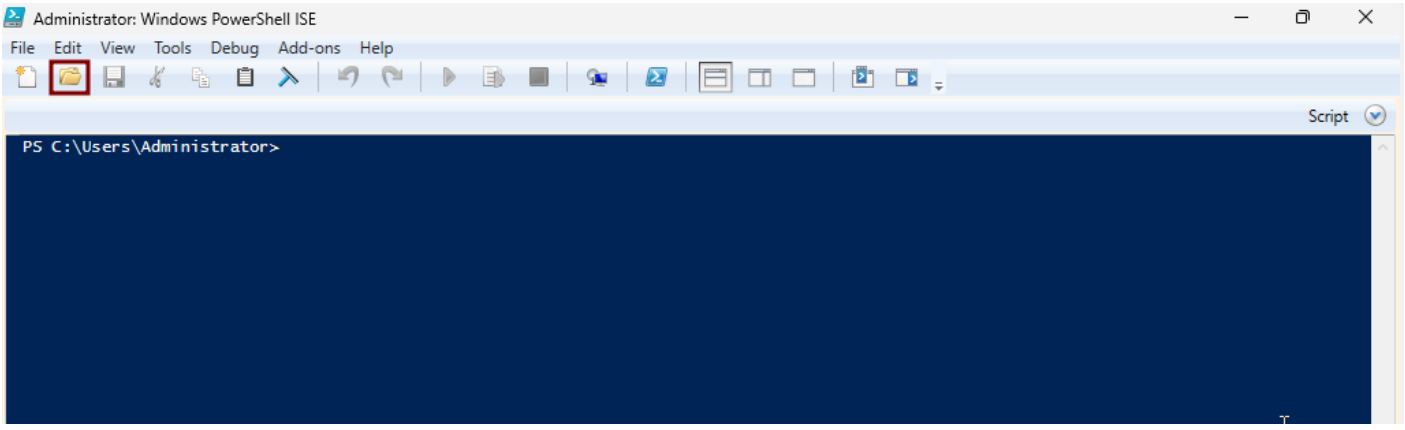
Editing the Script

To edit the provided script, you can use **PowerShell ISE** by following these steps:

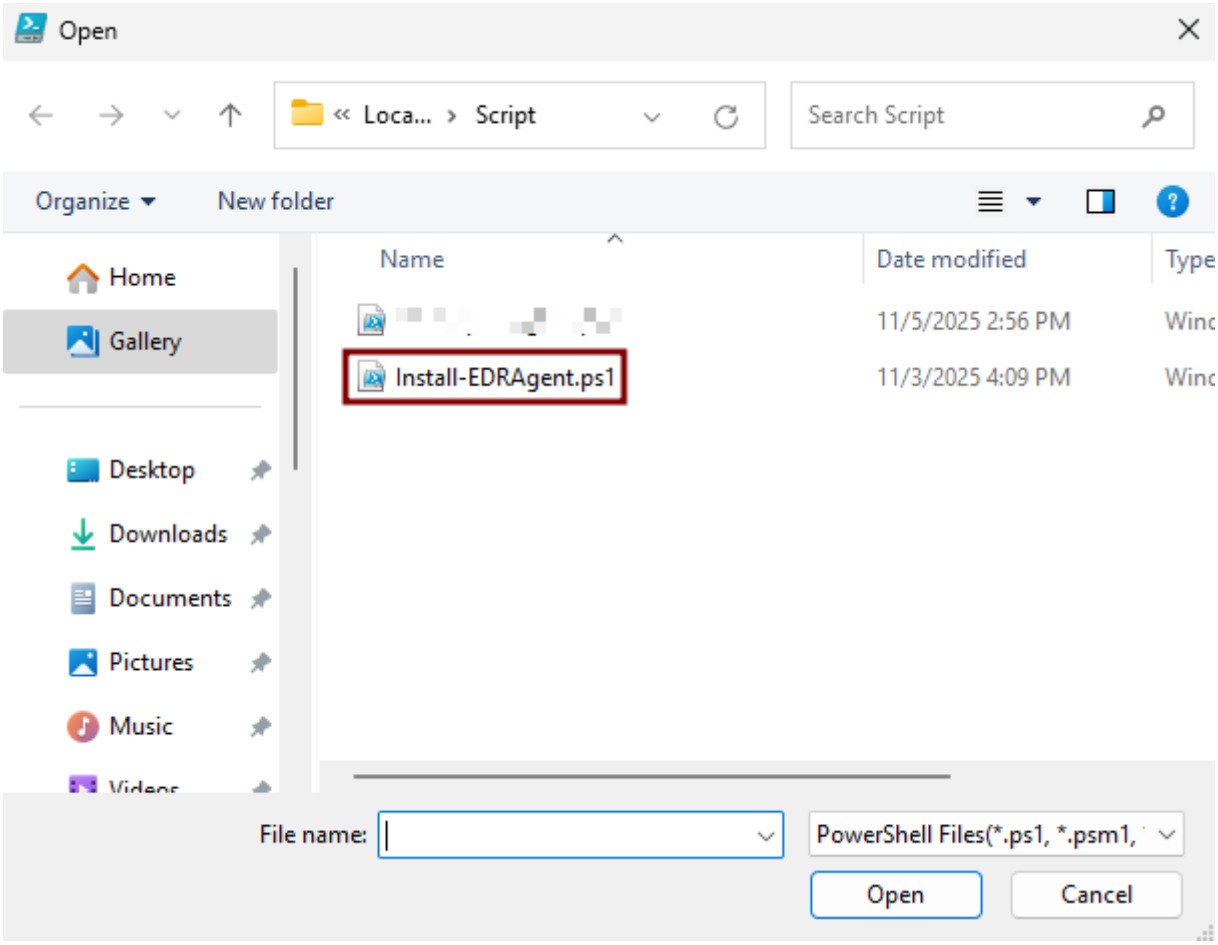
- Click the **Start** menu and type **PowerShell ISE**.



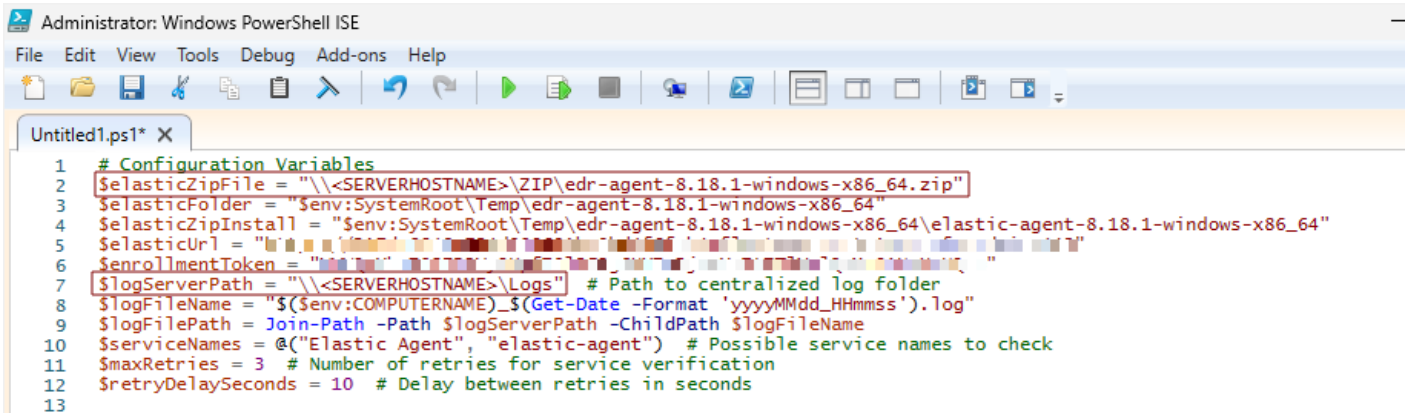
- In the upper-right corner, click the **Open Script** icon (folder symbol).



- Navigate to the folder where the script was saved, then open the file.



- Variables need to change:
  - **$elasticZipFile:** put the UNC path where the ZIP file was saved. *(e.g. \\WINJDHSGFYR\ZIP\edr-agent-8.18.1-windows-x86_64.zip).*
  - **$logServerPath:** put the UNC path of the created Logs folder. *(e.g. \\WINJDHSGFYR\Logs).*

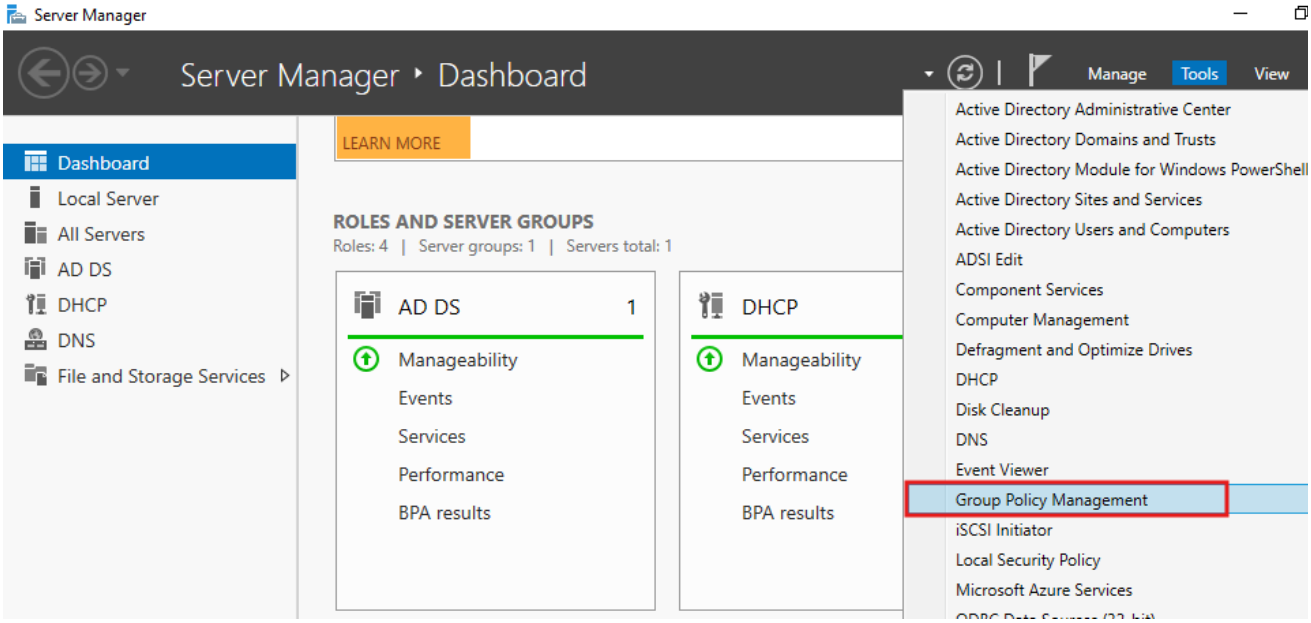


- Then **Save Script.**

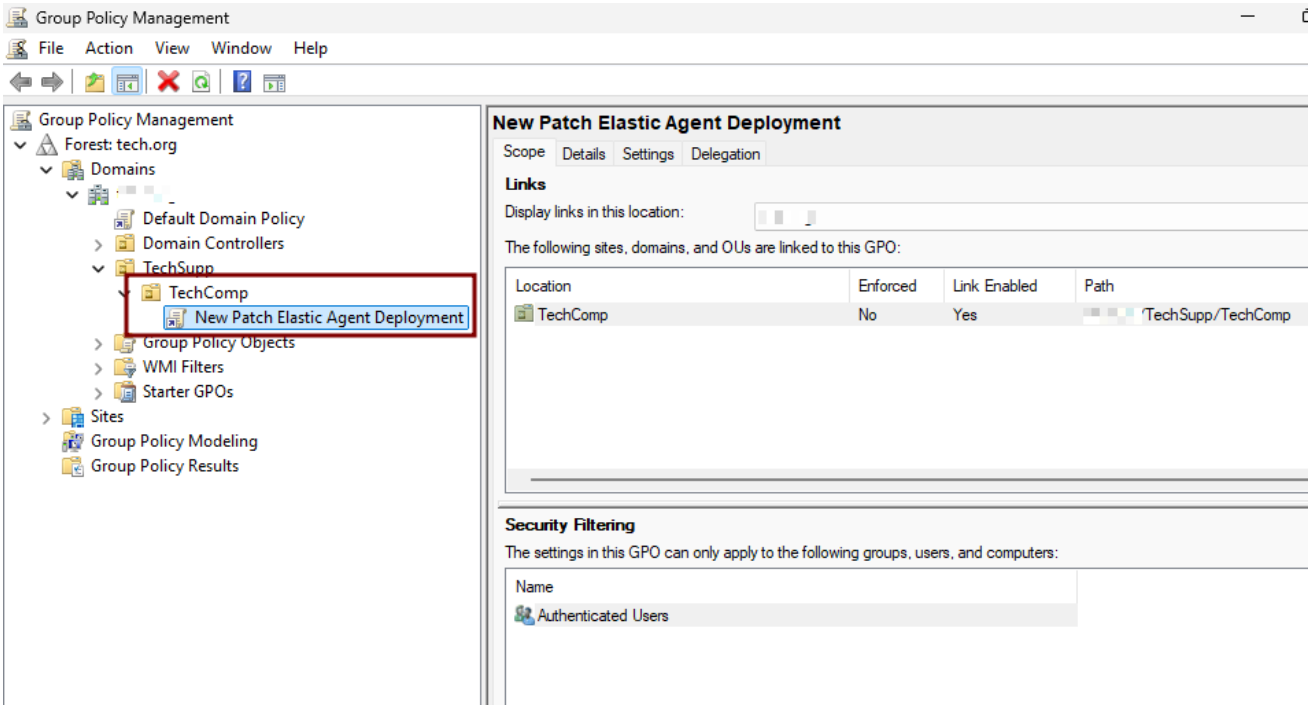
Deploying AQUILA EDR via Group Policy

Use Group Policy Management to create and link a Group Policy Object (GPO) that deploys the **AQUILA EDR** agent to domain-joined computers.

1. **Open Group Policy Management**
   - In **Server Manager**, go to **Tools → Group Policy Management**.

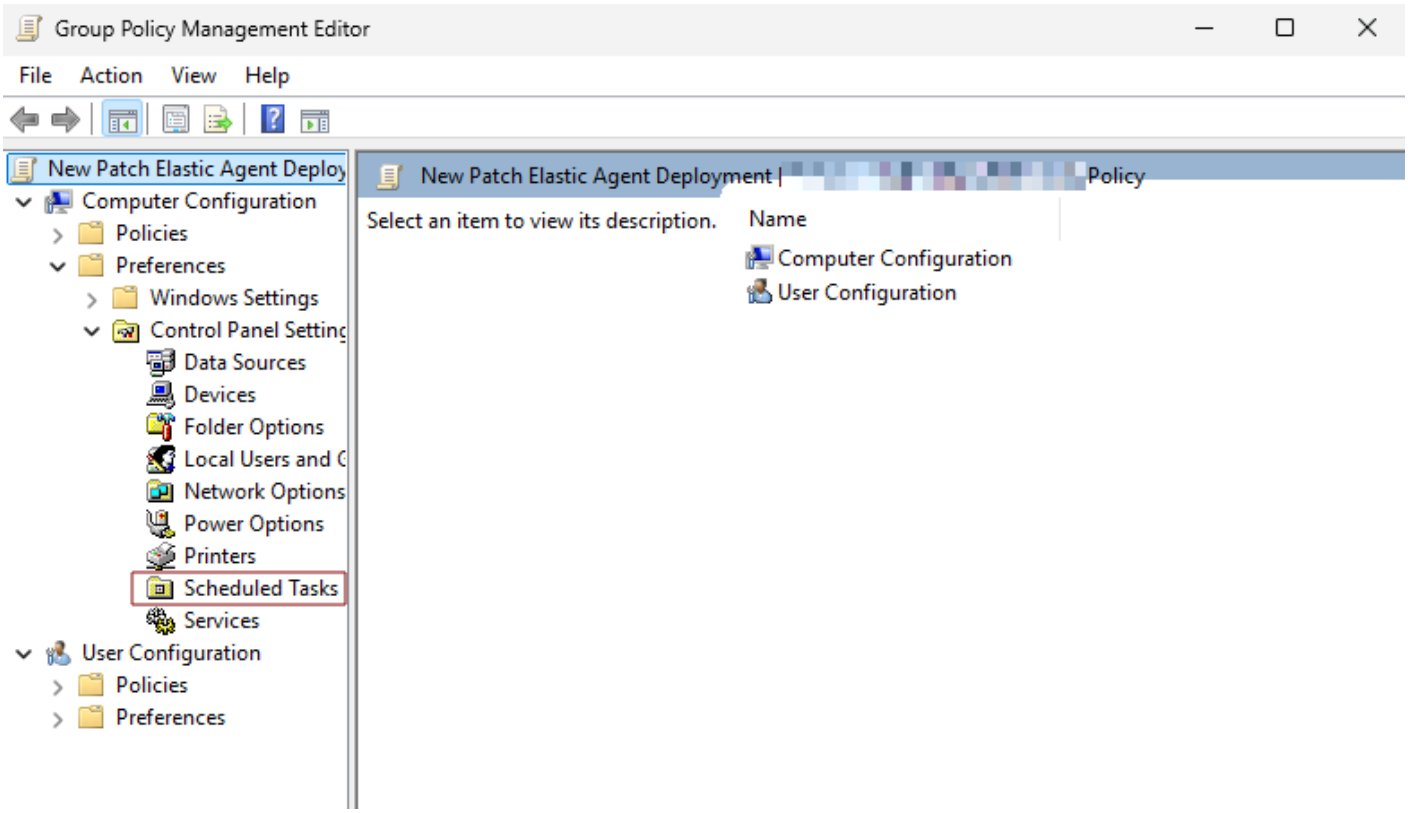


2. **Create a New GPO**
   - In the Group Policy Management Console, expand your domain and right-click the **Domain Controllers** container (or the appropriate **Organizational Unit (OU)**).
   - Select **Create a GPO in this domain, and Link it here**.
   - Provide a descriptive name (e.g., *New Patch Elastic Agent Deployment*), then click **OK**.

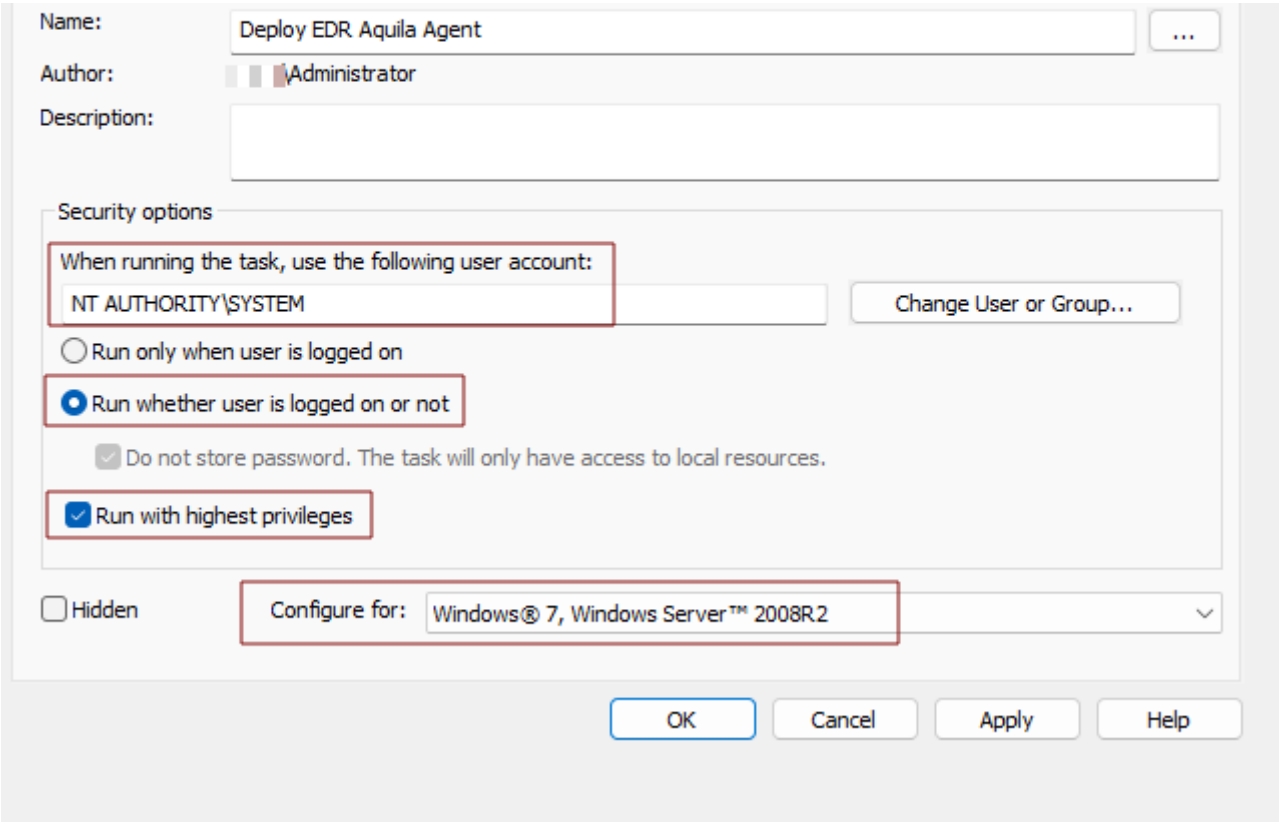


3. **Edit the GPO**
   - Right-click the newly created GPO and select **Edit**.

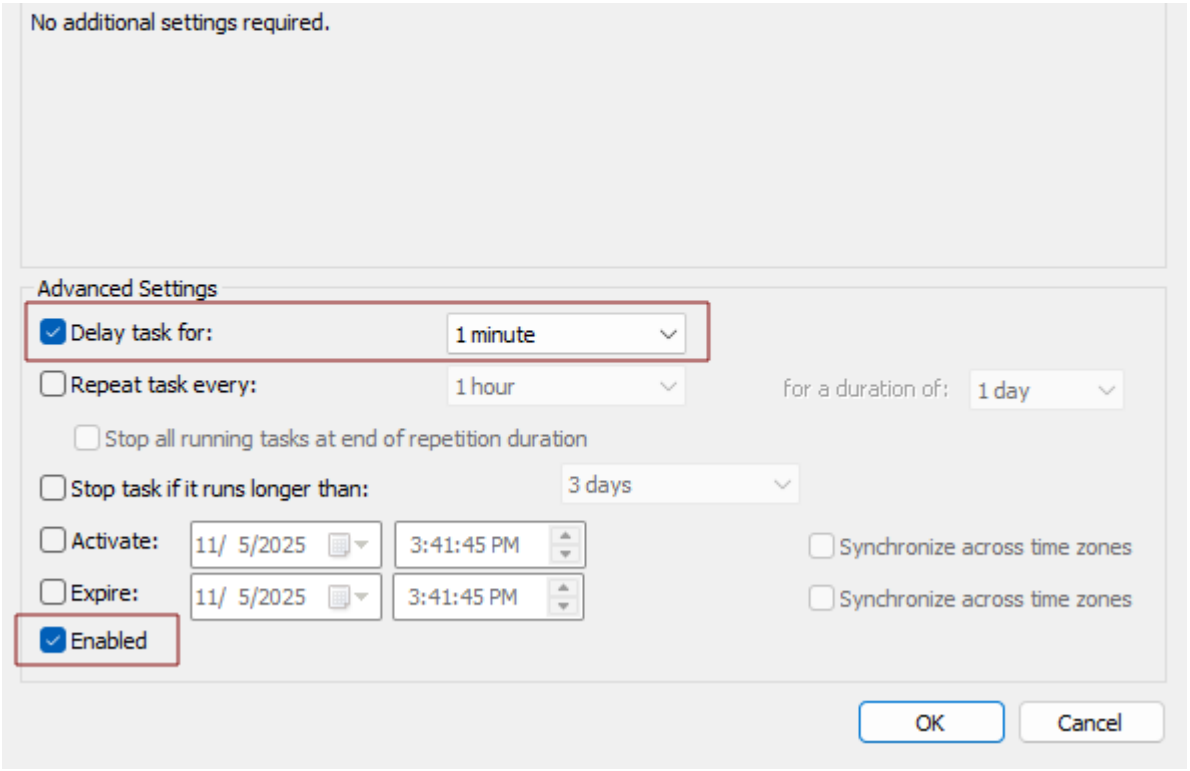
- In the Group Policy Management Editor, navigate to:
  Computer Configuration → Preferences → Control Panel Settings → Scheduled Tasks



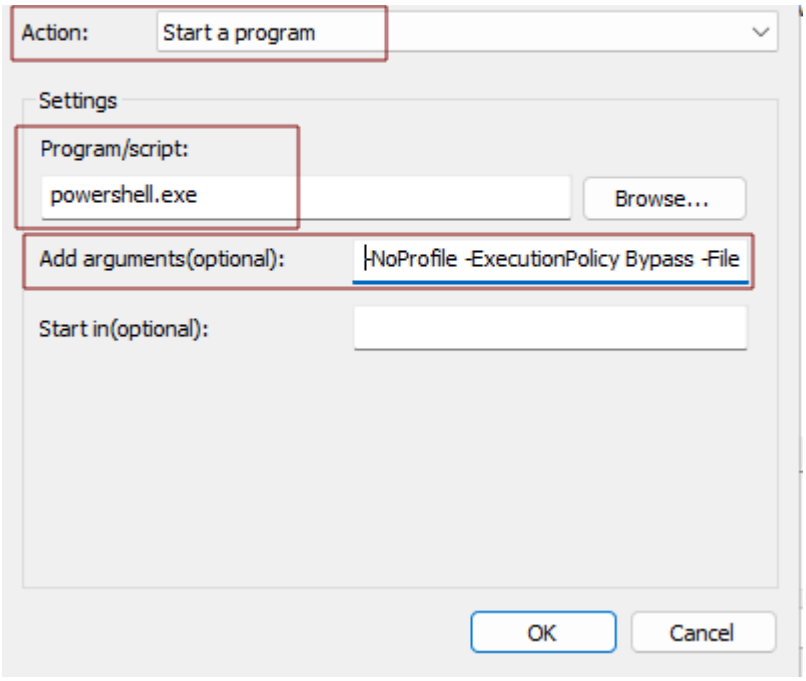
1. **Scheduled Tasks**
   - Right-click then choose **New** → **Scheduled Task (At least Windows 7)**.
   - **General Tab**
     - **Action:** Create
     - **Name:** you can set a name of the scheduled task. *(e.g. Deploy EDR Aquila Agent)*
     - **When running the task, use the following user account:** NT AUTHORITY\SYSTEM
     - Enable **Run whether user is logged on or not**
     - Enable **Run with highest privileges**
     - **Configure for:** Windows 7, Windows Server 2008R2



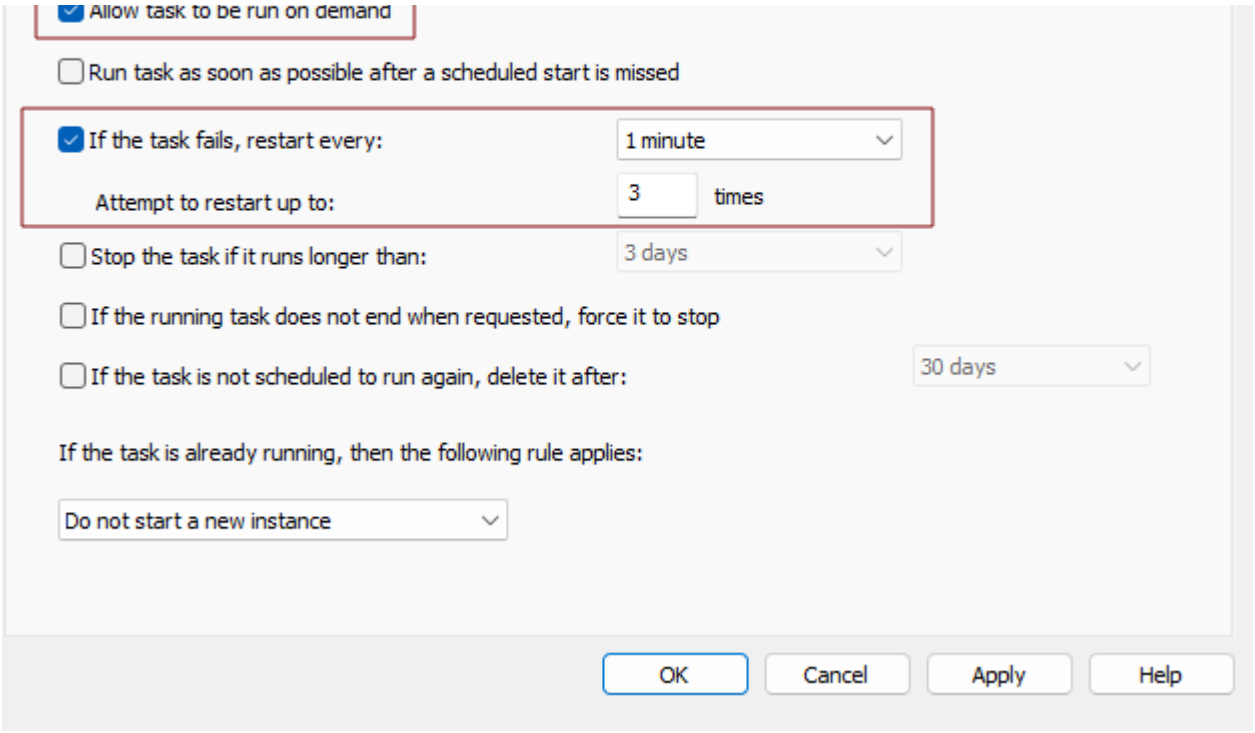
- **Triggers Tab**
  - Click **New**
  - **Begin the task:** At startup
  - **Delay task for:** 1 minute
  - **Enabled**



- **Actions Tab**
  - Click **New**
  - **Action:** Start a program
  - **Program/script:** powershell.exe
  - **Add arguments(optional):** -NoProfile -ExecutionPolicy Bypass -File "\\<SERVERHOSTNAME>\Script\Install-EDRAgent.ps1" *(e.g. \\WINSJHGJDHR\Script\Install-EDRAgent.ps1)*



- **Settings Tab**
  - Enabled **Allow task to be run on demand**
  - **If the task fails, restart every:** 1 minute
  - **Attempt to restart up to:** 3 times



1. **Finalize the GPO**
   - Close the Group Policy Management Editor.
2. **Test in the Client Computer before Deployment**
   - Go to the test client computer that is connected to the domain.
   - Open **Powershell** as administrator
   - Run the command:
     gpupdate /force
   - Running it refreshes the Group Policy on the server itself.
   - Open **Task Scheduler** and check if the scheduled task was reflected on the **Task Scheduler Library.**
   - If confirmed go back to **Powershell**
   - Run the command:
   - **shutdown /r /t 0**
   - To restart the test client computer
3. **Verify Installation**
   - Login to the test client computer and wait for the 1 minute to run the task.
   - You can open the **Task Scheduler** again and check **Task Scheduler Library** if the task is successful.
   - Confirm the agent, check **Task Manager** and search for **elastic-agent** and **elastic-endpoint**.

Test the Script via PsExec

Why This Method Is Necessary

Running the script through PsExec simulates how it will execute when deployed via GPO Scheduled Task—specifically under the **NT AUTHORITY\SYSTEM** context. This helps identify issues that may not appear when running the script as a regular user.

Prerequisites

- Administrative privileges on the test computer and on the script's UNC path.
- The test computer must be online and reachable.
- Verify that the script (e.g., `Install-EDRAgent.ps1`) is accessible via a UNC path such as `\\SERVER\Share\Install-EDRAgent.ps1`.

Step-by-Step Guide (Test Computer)

1. **Download PsExec**
   Download the PsExec utility from the official Microsoft Sysinternals website and save the ZIP file to your workstation. Download here.
2. **Extract the ZIP**
   Extract the ZIP file and open the extracted folder.
3. **Copy PsExec.exe**
   Locate `PsExec.exe` and copy it to a local folder on the test computer (e.g., `C:\Tools\PsExec\`).
4. **Open an Elevated Command Prompt**
   Right-click **Command Prompt** and choose **Run as administrator**.
5. **Open a SYSTEM-Level PowerShell Session**
   Navigate to the folder where the **PsExec** was copied (e.g., cd C:\Tools\PsExec).
   Run the following command:
   `psexec -s -i powershell.exe`
   Note: The first run may display the Sysinternals license prompt. To avoid this, you may use:
   `psexec -accepteula -s -i powershell.exe`

6. **Execute the Script Under SYSTEM Context**
   Inside the SYSTEM PowerShell window, run:
   `powershell.exe -ExecutionPolicy Bypass -File "\\<FILE-SERVER>\<Share>\<Install-EDRAgent.ps1>"`
   Example:
   `powershell.exe -ExecutionPolicy Bypass -File "\\WIN-JPFCK15QVMI\Script\Install-EDRAgent.ps1"`
7. **Monitor Output and Collect Errors**
   Observe the PowerShell output for any installation errors.
   If the installer generates logs, please collect them for review.

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

Revision #6
Created 21 August 2025 13:26:36 by Jeff Saguing
Updated 15 November 2025 11:33:48 by Jeff Saguing