How - To Guide

Install the Logcollect Sensor for Windows

Publication Date:

Nov 17, 2025

© Copyright Logcollect. All Rights Reserved.

Abstract

The Logcollect sensor for Windows deployment procedures is described in detail in this document. The Logcollect sensor for Windows can be deployed using GUI or Command Line or through GPO. The purpose of this document is to provide step by step instructions to deploy the sensor using distinct methods.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Logcollect 9.4 or later.

Audience

Users and system administrators, who want to deploy the Logcollect sensor for Windows.

© Copyright Logcollect. All Rights Reserved.

Table of Contents

1 Overview 4

2 Software Requirement 4

3 Resource Requirement 5

4 Deploying the Logcollect Sensor through GUI Mode 5

5 Deploying the Logcollect Sensor through Command Line (in Silent Mode) 8

5.1 Installing Using Sensor.exe 8

5.2 Installing Using SensorInstaller.exe 9

6 Deploying the Logcollect Sensor via Group Policy Organization (GPO) 10

6.1 Creating an Installation Batch File 13

6.2 Creating an Installation Batch file for the Customer with Existing etaconfig.ini 15

7 Uninstalling the Logcollect Sensor through GPO (in Batch file) 15

8 Uninstalling the Logcollect Sensor through Command Line 24

8.1 Uninstalling Using Sensor.exe 24

8.2 Uninstalling Using SensorInstaller.exe 25

© Copyright Logcollect. All Rights Reserved.

1 Overview

The Logcollect sensor for Windows is the front-line telemetry collection component on the Logcollect platform which provides detailed visibility of the endpoint. The sensor collects and normalizes logs, monitors your endpoint, and collects information about your assets and IT environment.

The Logcollect sensor delivers the following essential capabilities:

- Log collection.
- High-degree monitoring of application log files, TCP/UDP network activities, and USB devices.
- Observes network traffic non-intrusively to identify hosts.
- Software install/uninstall.
- Finds services start/stop.
- Sends events with guaranteed delivery via TCP mode.
- Monitor files and registry changes on the system.
- Monitor/ terminate suspicious activity.
- Provides immediate visibility into the attacks against your systems.
- Syslog relay.

2 Software Requirement

Windows Server	2022, 2019, 2016, 2012 R2
Windows	11, 10
Microsoft .NET Framework 3.5 and above	

Note:

Versions other than those listed above are not supported.

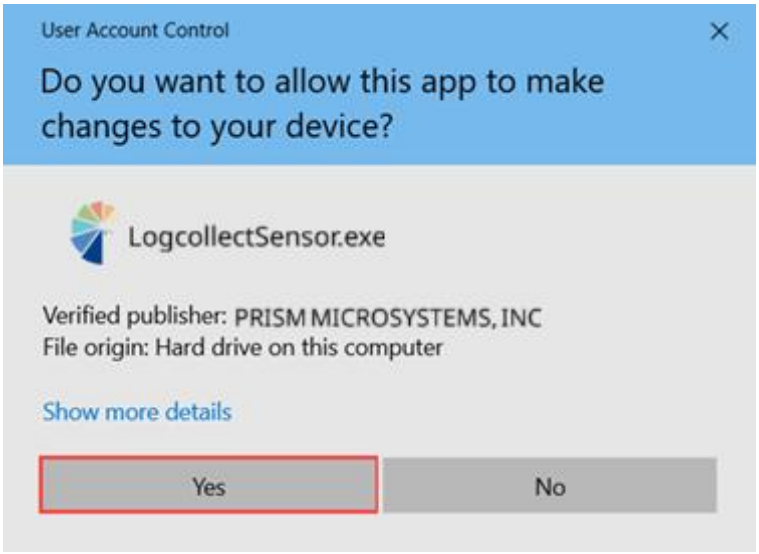
© Copyright Logcollect. All Rights Reserved.

3 Resource Requirement

Minimum Configuration			Resource Utilization (in a typical environment)		
CORE	RAM	DISK	CPU		MEMORY
			AVG	MAX	
4	8 GB	200 MB	1-2 %	10 %	50 MB

4 Deploying the Logcollect Sensor through GUI Mode

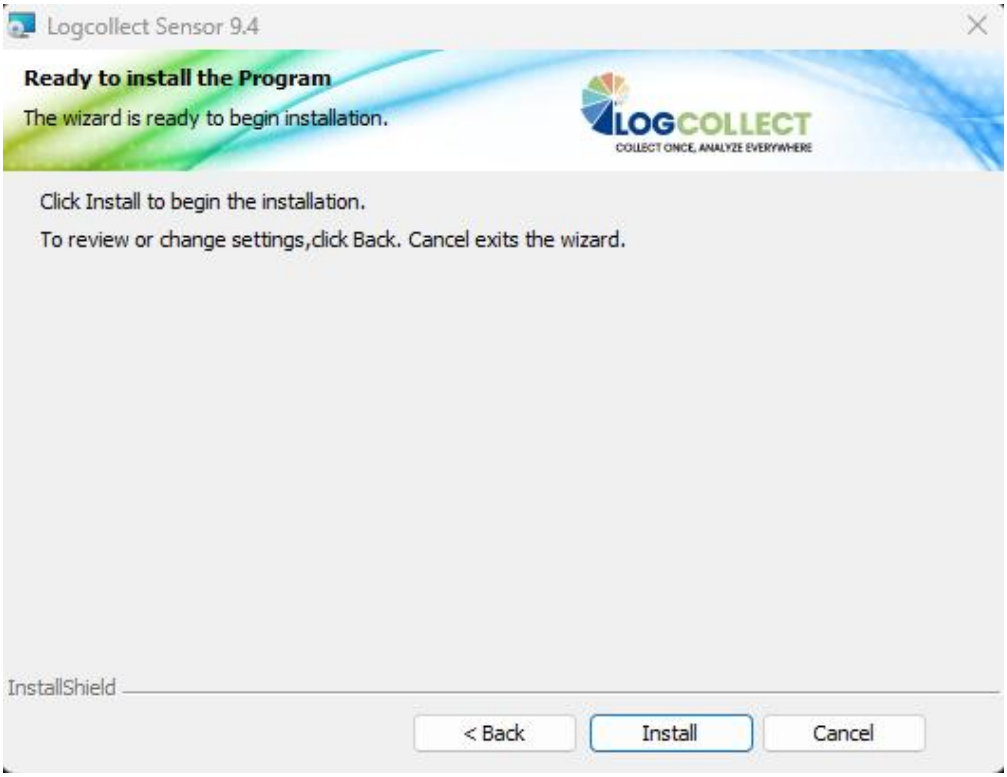
1. Download the installation file from the link delivered via email.
2. Save the installation file to a location on the Windows device on which the installation is to be done.
3. Right-click the downloaded file and click **Run as administrator**. Click **Yes** to continue.



© Copyright Logcollect. All Rights Reserved.

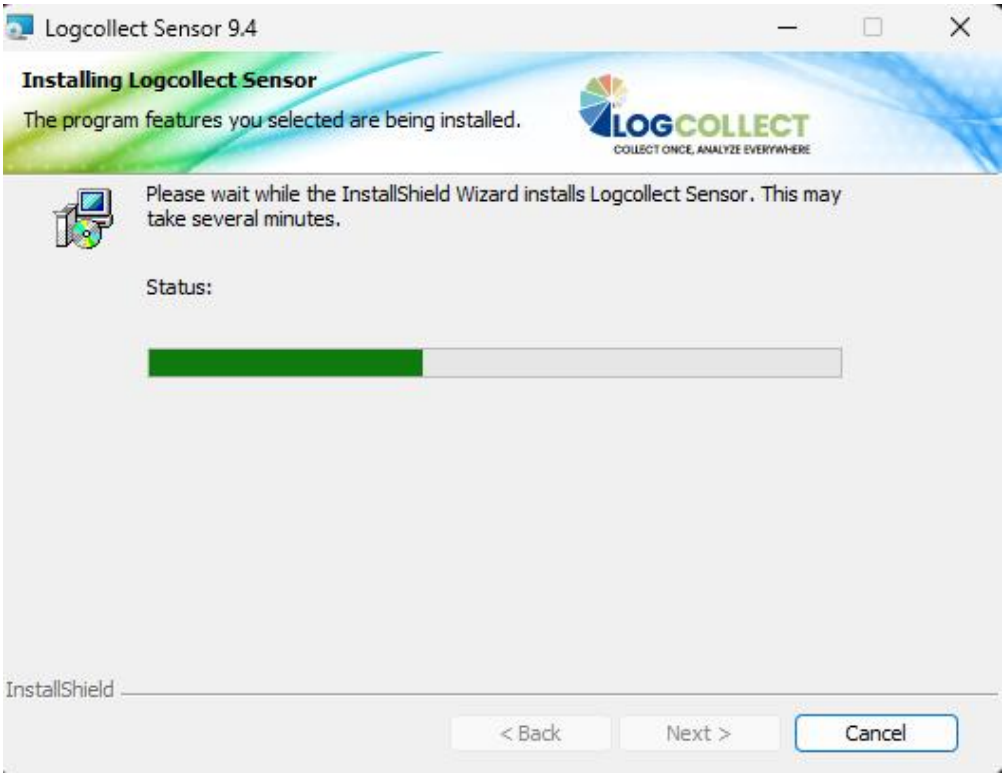
4. In the **Welcome to the installation of Logcollect Sensor** window, click **Next >**.

5. In the **Ready to install the program** window, click **Install** to initiate the installation.



© Copyright Logcollect. All Rights Reserved.

The following image represents the installation progress of the Logcollect sensor.



6. Click **Finish** to complete the Logcollect sensor installation process.

© Copyright Logcollect. All Rights Reserved.

Once the installation is complete, the Server Connectivity window displays the connection established status information.

7. Click **Close** if it displays a successful connection.

> **Note:**
>
> If it displays connection issues, contact the Logcollect support team.

5 Deploying the Logcollect Sensor through Command Line (in Silent Mode)

5.1 Installing Using Sensor.exe

1. Download the installation file (Sensor.exe) from the link given in the email.
2. Save the installation (**.exe**) file to a location on the Windows device on which you want to install.
3. Run the Command Prompt in the Admin mode.
4. Type in the command **`<cd> <installation file location>`**

> **Command syntax** `<cd> <installation file location>`

In the above command, change the directory to the file path where the installation (.exe) file is located.

5. Press **Enter** to go to the next line and press **Tab** to retrieve the **.exe** file.
6. Press **Space** and type in **/qn** and press **Enter** to run the installation in Silent mode.

In the following example, the installation (.exe) file is located in C drive. The location may differ on your machine, depending on the installation (.exe) file location.

© Copyright Logcollect. All Rights Reserved.

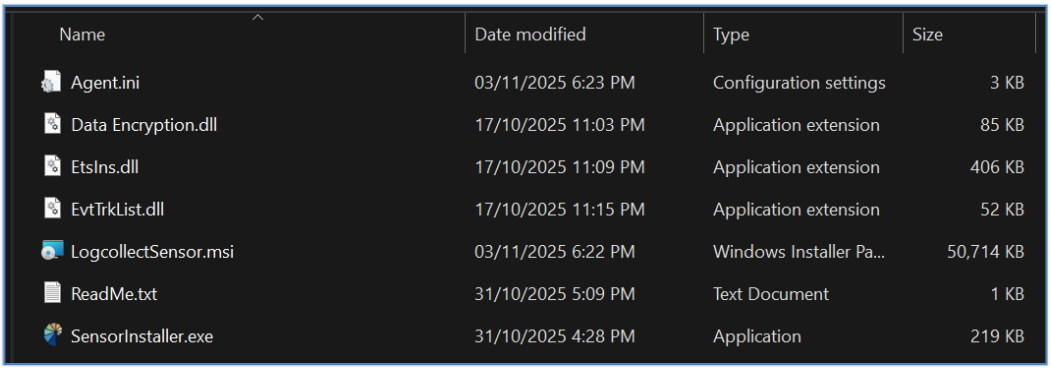
```
C:\Windows\system32>cd C:\Users\        \Documents\Sensor

C:\Users\        \Documents\Sensor> Sensor-BANGALORE-14505-0194-1685702422.exe /qn
```

Command syntax `<executable file name.exe> /qn`

5.2 Installing Using SensorInstaller.exe

1. Download the installation (Sensor.exe) file from the link shared via email.
2. Save the installation (.exe) file to a location on the Windows device on which the package will be installed.
3. Go to the saved location and extract the installation (.exe) file.



Name	Date modified	Type	Size
Agent.ini	03/11/2025 6:23 PM	Configuration settings	3 KB
Data Encryption.dll	17/10/2025 11:03 PM	Application extension	85 KB
EtsIns.dll	17/10/2025 11:09 PM	Application extension	406 KB
EvtTrkList.dll	17/10/2025 11:15 PM	Application extension	52 KB
LogcollectSensor.msi	03/11/2025 6:22 PM	Windows Installer Pa...	50,714 KB
ReadMe.txt	31/10/2025 5:09 PM	Text Document	1 KB
SensorInstaller.exe	31/10/2025 4:28 PM	Application	219 KB

4. Run the Command Prompt in Admin mode.
5. Type in the command **<cd> <extracted file location>**

Command Syntax `<cd> <extracted file location>`

In the above command, change the directory to the file path where the installation (.exe) file is located.

6. Press **Enter** to go to the next line and press **Tab** to retrieve the **SensorInstaller.exe** file.
7. Press **Space** and type in the following command as mentioned in the example below, and then press **Enter** to run the installation in Silent mode.

```
SensorInstaller.exe CUSTOMCONFIG=4 EA=1 CA=1 EM=ET00.LOGCOLLECT.COM
EP=14221 MIN_GUI=1 IR=1 LS=ET00.LOGCOLLECT.COM LP=14503 CM=LOCALHOST
SUFFIX=BK-PPPP-NS1 IS_SUFFIX=2
PKG_UID=c2d0bce2scvb22624b2cb69f6dc9b8de328376ecc8 /qn
```

```
C:\Program Files\Sensor\Sensor-NETSURION-14505-0194-1685469164>SensorInstaller.exe
CUSTOMCONFIG=1 EA=1 CA=1 EM= ET00.LOGCOLLECT.COM   EP=14221 MIN_GUI=1 IR=1 LS=ET00.
LOGCOLLECT.COM  LP=14503 CM=LOCALHOST SUFFIX=BK-PPPP-NS1 IS_SUFFIX=2 PKG_UID=c2d0bc
e2scvb22624b2cb69f6dc9b8de328376ecc8 /qn
```

© Copyright Logcollect. All Rights Reserved.

Arguments used for Command Line Installation

The **Agent.ini** contains the following sensor configurations and the same details needs to be provided in the command line.

Argument	Description
CUSTOMCONFIG	**0** - Default
EM	Enterprise Manager Name
EP	Enterprise Port Number
CM	Change Audit Manager Name
LS	License Server Name
LP	License Server Port
EA	**1** - Default
CA	**1** - Default
PIP	Public IP
PKG_UID	Package UID
IS_SUFFIX	**1** - Default
SUFFIX	Suffix string present as “Location ID” in the ReadMe.txt

6 Deploying the Logcollect Sensor via Group Policy Organization (GPO)

1. Download the installation file from the link shared via email.
2. Create the installation batch file.

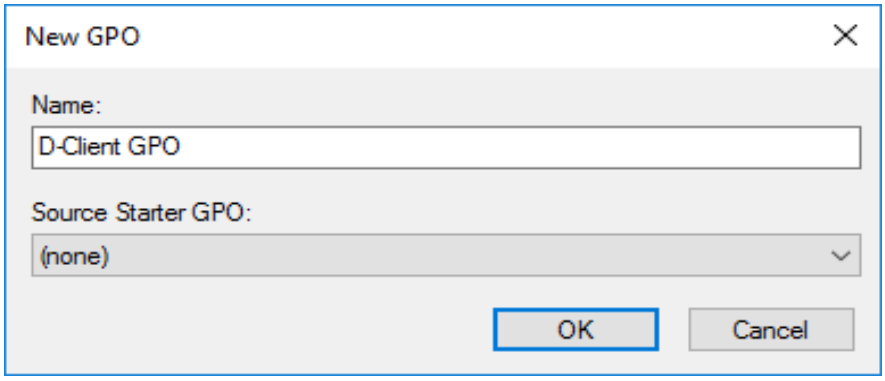
> **Note:**
>
> Refer to the **Creating an Installation Batch File** section to deploy the sensor.
>
> Refer to **Creating an Installation Batch file for the Customer with existing etaconfig.ini** section to deploy the sensor with existing etaconfig.ini file.

3. Save the installation batch file to the Startup Script folder.
4. Save the batch file and the .exe file in a location that is accessible to all Windows devices used by the organisation.
5. Log in to the Domain Controller (DC) and start the Microsoft Group Policy Management Console (GPMC).
6. In the GPMC tree, right-click the Organization Unit (OU) in which the D-Client must be deployed.

© Copyright Logcollect. All Rights Reserved.

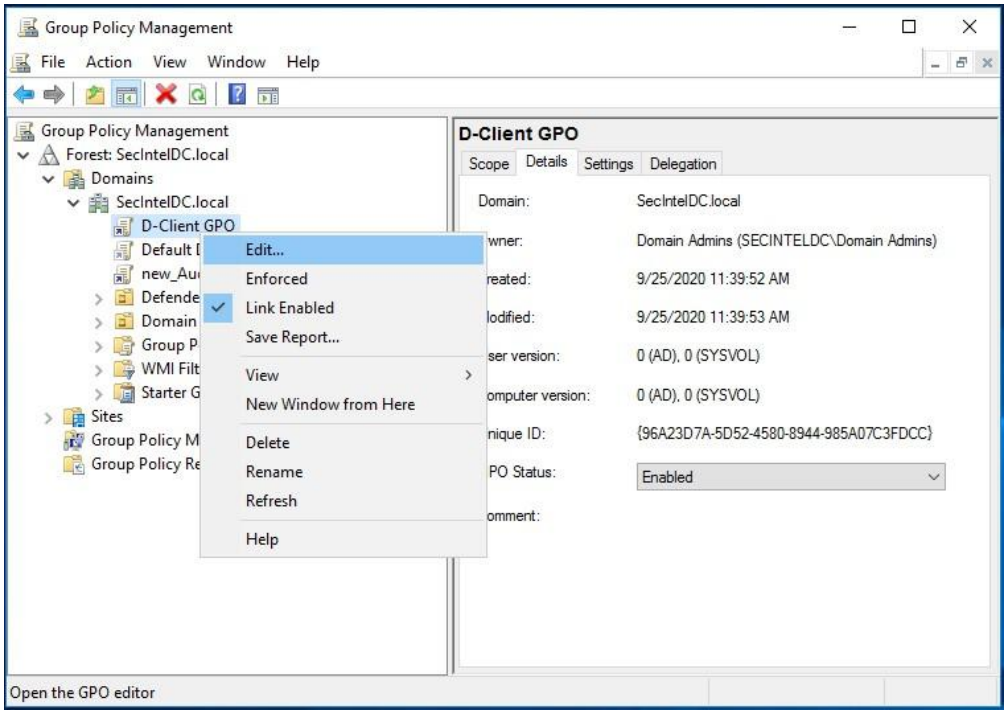
7. Click **Create a GPO** in this domain and click **Link it here** to create a new GPO.

   The window for creating a New GPO appears.



8. Type the name of the new GPO and click OK. The new GPO is now added to the list of Linked Group Policy Objects.

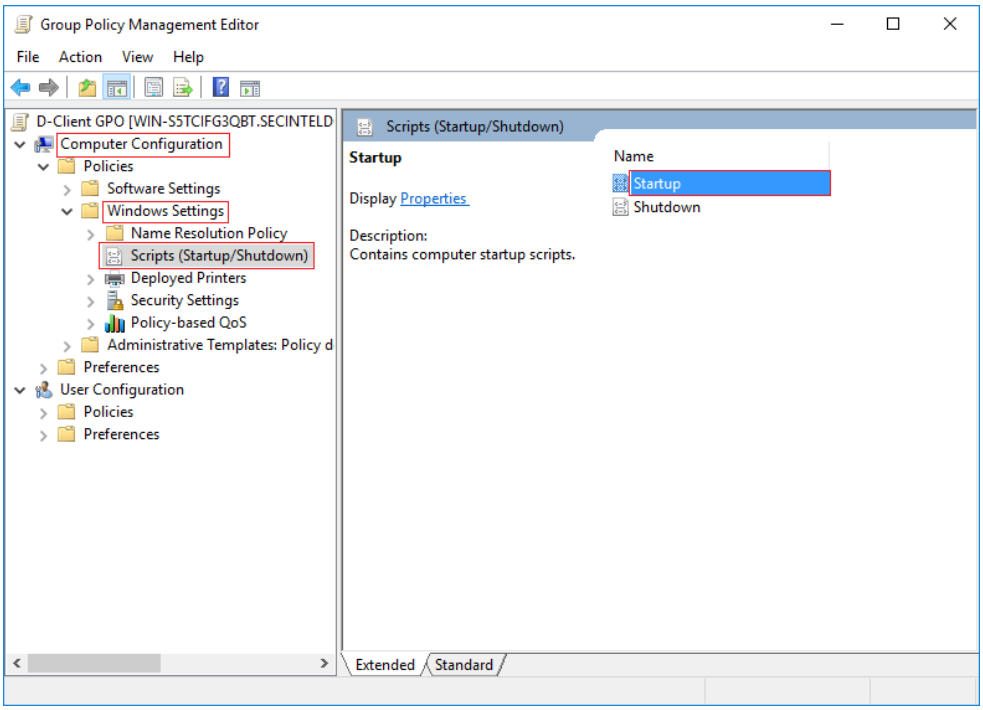
9. Right-click on the new GPO and click **Edit**.



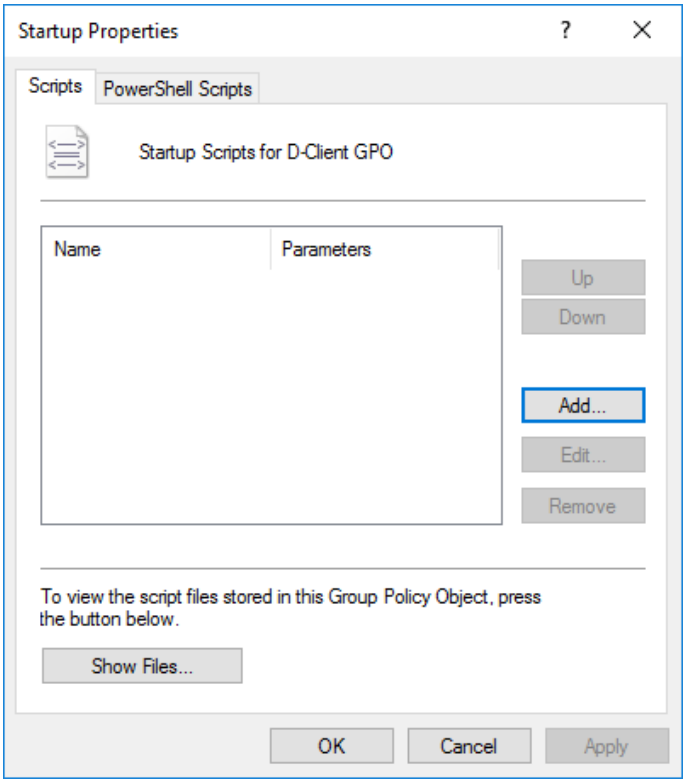
10. In the GPMC tree, under Computer Configuration, expand **Policies** and expand **Windows Settings.**

11. Then, under **Windows Settings**, click **Scripts (Startup/Shutdown)** and double-click **Startup** (located in the right panel).

© Copyright Logcollect. All Rights Reserved.

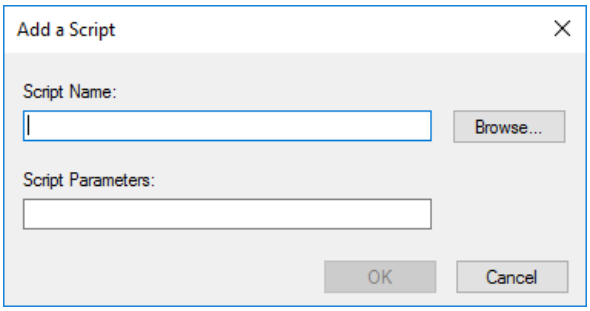


The **Startup Properties** dialog box opens.

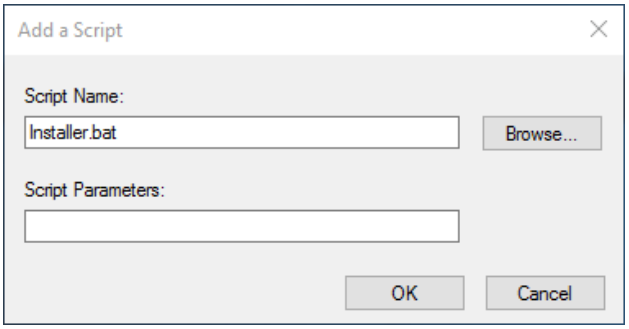


12. Click **Add** and the window for adding a script appears.

© Copyright Logcollect. All Rights Reserved.



13. Click **Browse** and select the installation batch file, and then click **OK** to add the script.



14. Then, click **OK** and exit the Microsoft Group Policy Management console. The Logcollect sensor will be deployed on each device whenever the device restarts.

    Perform the following steps, if you want to install the Logcollect sensor immediately on an endpoint.

    a. In the **Command Prompt** window, execute the command **`gpupdate /force`** to update the policy.

       The following message appears indicating that the policy is updated successfully.

    b. Type **Y** to restart the device and complete the Logcollect sensor deployment on this device.

6.1 Creating an Installation Batch File

Prior to deploying the Logcollect sensor package with GPO, an installation batch file must be created.

© Copyright Logcollect. All Rights Reserved.

Note:

The batch file can be created with a text editor, such as Notepad.

The following steps describe the procedure to create the installation batch file.

1. Download the Logcollect sensor Windows EXE installation file.
2. Save the installation file to a location where all the Windows devices have access.
3. Open the text editor and type the following command in the first line of the file.

Command Syntax

```
<exe path><installation file> /qn
```

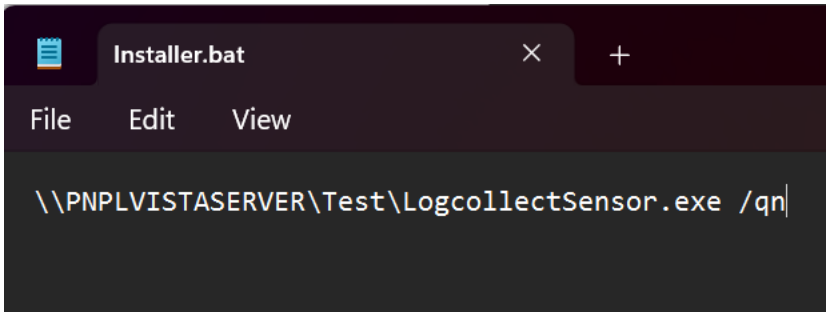
Command Description

Parameter	Description
`<exe path>`	Path for the appropriate installation file, where all the Windows devices have access
`<installation file>`	File name of the Logcollect sensor package

4. Save the file with the name **installer.bat**.

The following is an example:

- EXE path - **`\\PNPLVISTASERVER\Test\`**
- Installation file - **`LogcollectSensor.exe`**



5. Copy the batch file to the same location where the installation file was saved (the location where the Windows deployment tools have access).

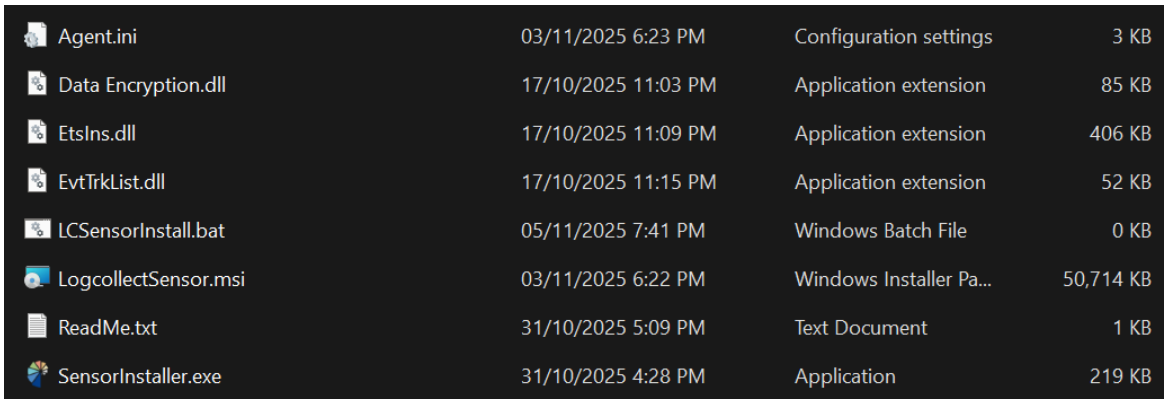
Note:

Refer to Deploying the Logcollect Sensor via Group Policy Organization (GPO) section to deploy the sensor via GPO.

© Copyright Logcollect. All Rights Reserved.

6.2 Creating an Installation Batch file for the Customer with Existing etaconfig.ini

1. In this case, first, place the existing **etaconfig.ini** in the extracted MSI package path.
2. Open the **Agent.ini** file and provide the parameter **Agentini=0**.



3. Open the **LCSensorInstall.bat** file and modify as shown in the below example.
4. When the user is using the customized **etaconfig.ini** file, they should not provide any parameters in the **LCSensorInstall.bat** file, except the below command.

Command Syntax

```
msiexec /i "%~dp0LogcollectSensor.msi" /qn EA=1 CA=0 CUSTOMCONFIG=4
PKG_UID=5947c59b27f7891eaac2f90fdf8659195340122.
```

Note:

The PKG_UID is available in readme.txt file.

5. After providing the command in the batch file, save the file.

Note:

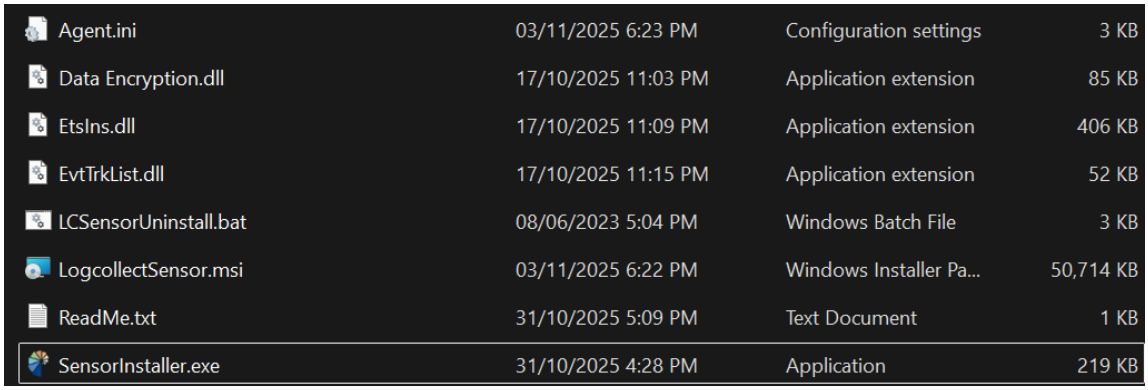
Refer to **Deploying the Logcollect Sensor via Group Policy Organization (GPO)** section to deploy the sensor via GPO.

7 Uninstalling the Logcollect Sensor through GPO (in Batch file)

1. Get the un-installation batch file from the following LCSensorUninstall.zip link to uninstall the sensor.
2. Download and save the **LCSensorUninstall.zip** and then extract it.
3. Copy the batch file and paste it in the extracted Sensor package path.

   For the Logcollect sensor 9.4

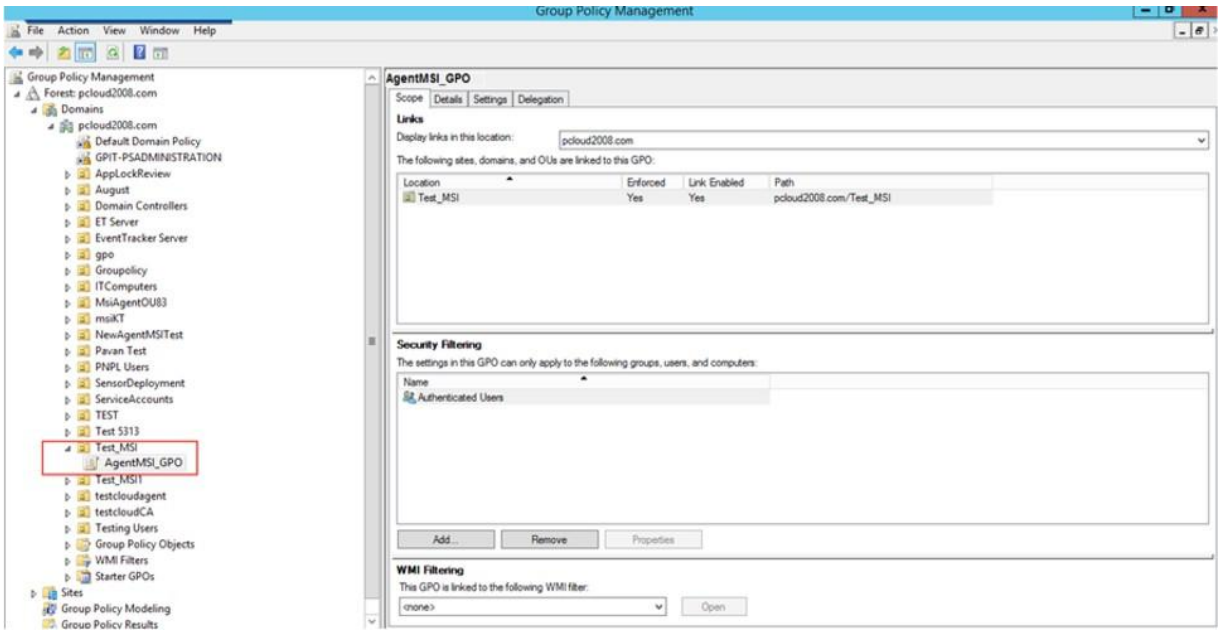
© Copyright Logcollect. All Rights Reserved.



4. The next step to uninstall the Logcollect Sensor through GPO mode is to remove the installation configuration in the Group Policy Management wizard.

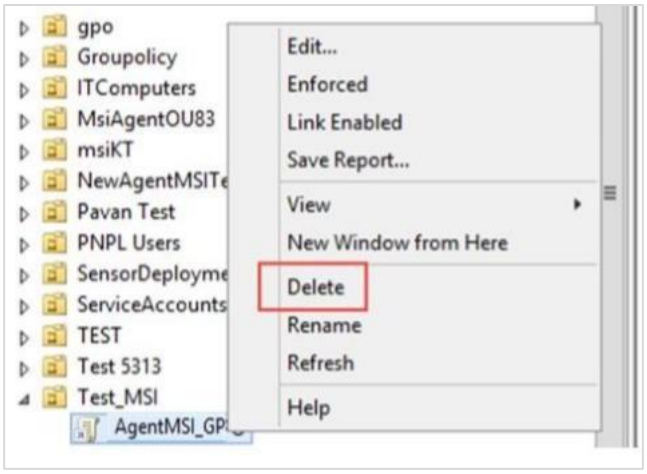
Note:

If you want to re-install the Logcollect Sensor, you will have to remove the un-installation configuration in the **Group Policy Management** wizard.



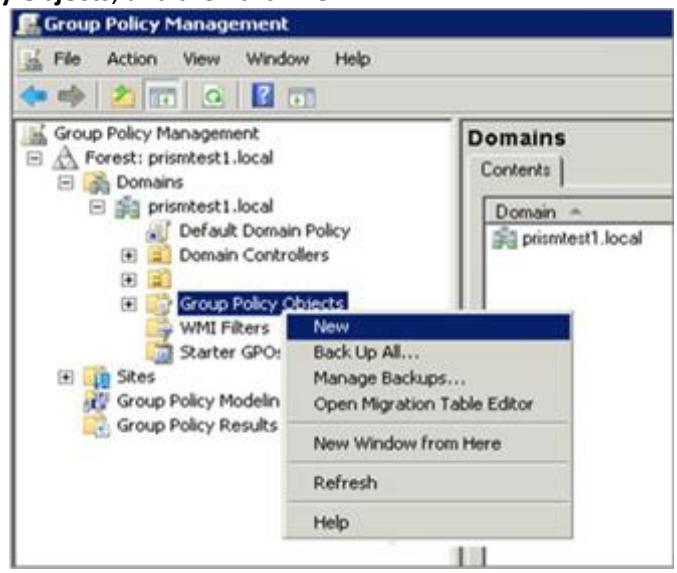
5. Right-click the **AgentMSI_GPO** and uncheck the **Enforced** and **Link Enabled** options.
6. Right-click the **AgentMSI_GPO** and delete it.

© Copyright Logcollect. All Rights Reserved.

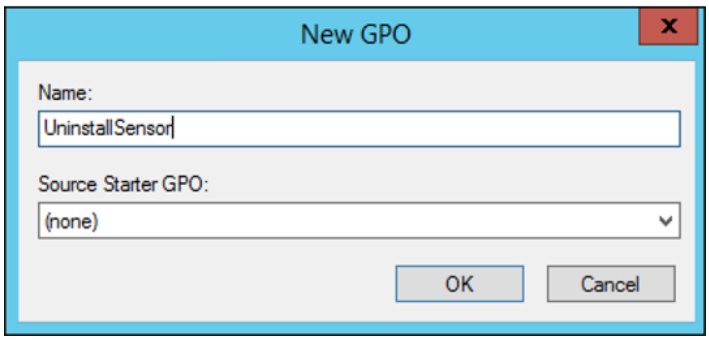


7. In the Group Policy Management pane, expand **Domains** node, and then expand the domain system node.

8. Right click **Group Policy Objects**, and then click **New**.

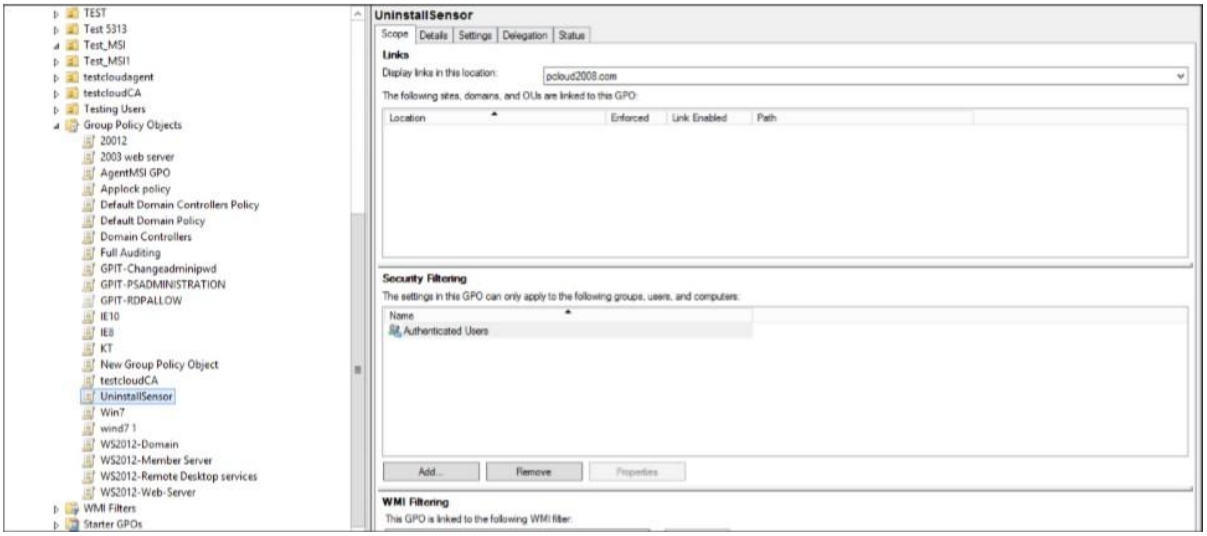


9. Enter a name for this new **GPO** (for example, UninstallSensor) and then click **OK**.

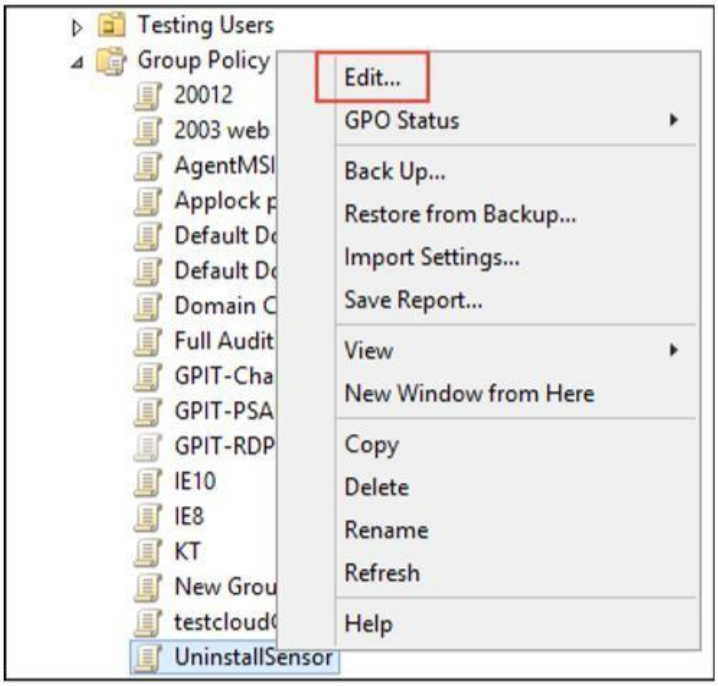


© Copyright Logcollect. All Rights Reserved.

10. Click the name of the newly created GPO. In this case, it is **UninstallSensor**.

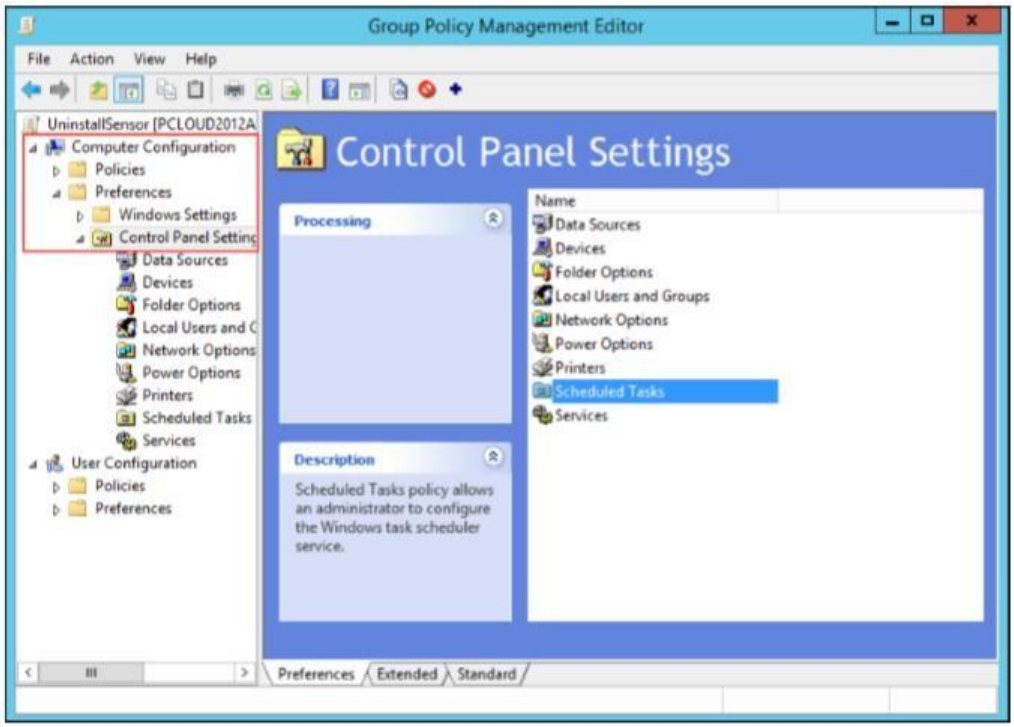


11. Right click on the created object and click **Edit**.

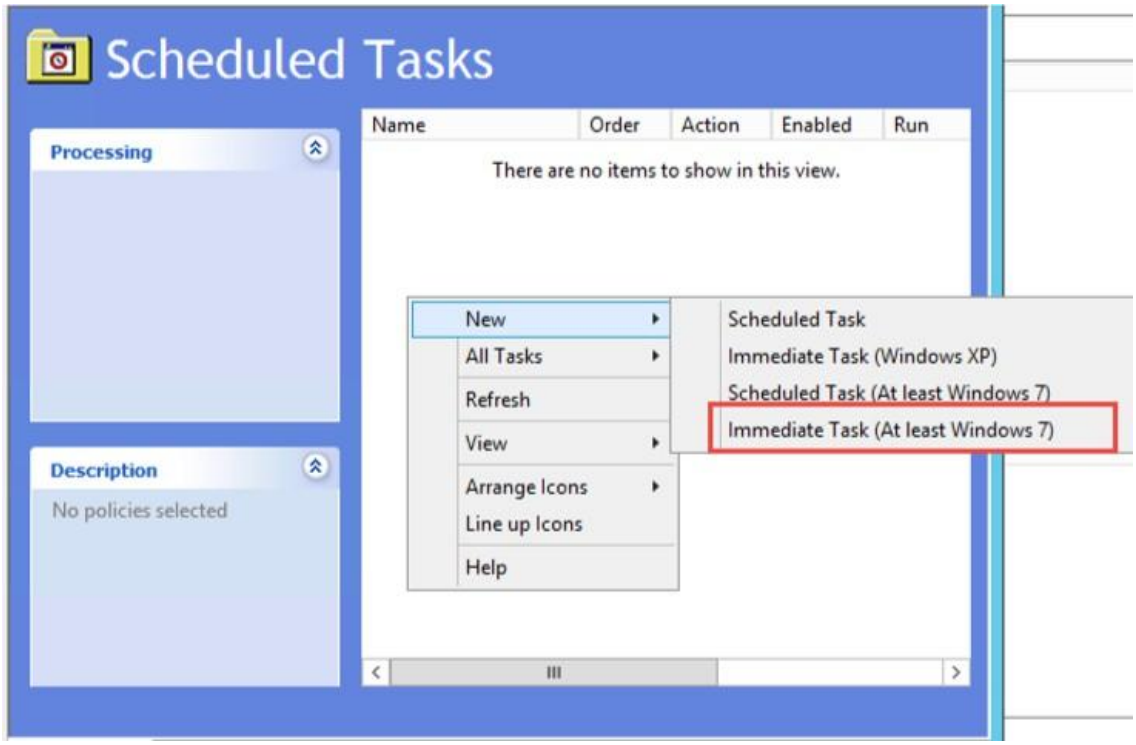


© Copyright Logcollect. All Rights Reserved.

12. In the next window, select **Preferences** under **Computer Configuration**. Then, choose **Control Panel Settings** > **Scheduled Tasks.**

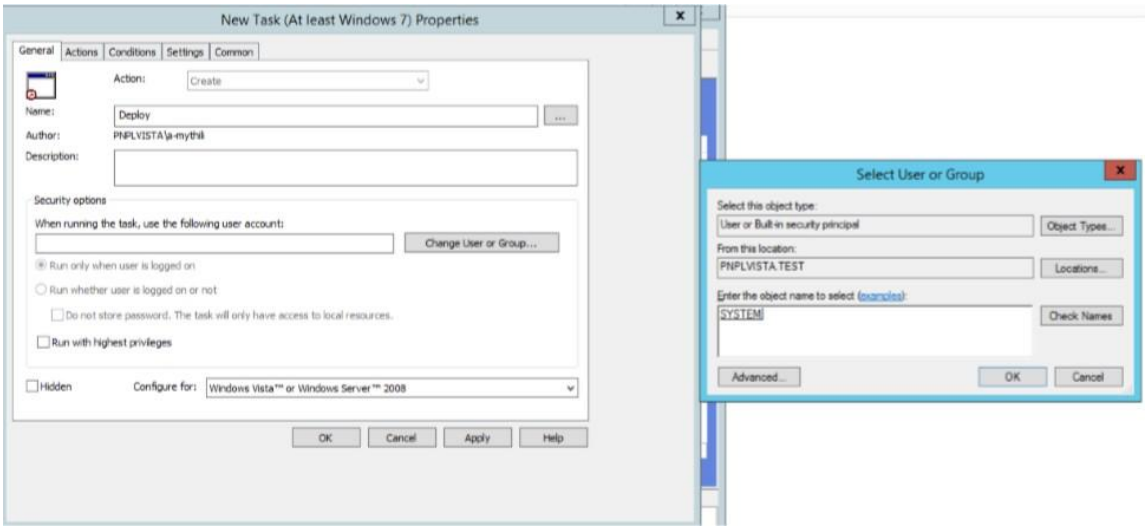


13. In the Scheduled Task screen, **Right Click** > **New** > **Immediate Task (**At Least Windows 7**).**

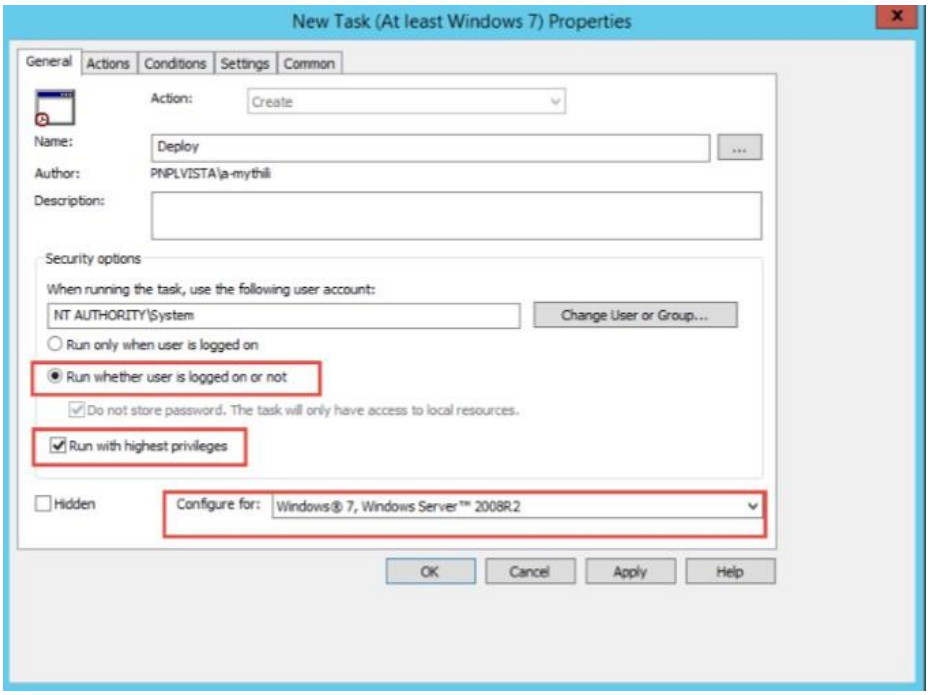


© Copyright Logcollect. All Rights Reserved.

14. Enter the name and click the **Change User or Group**. Search for **Systems** and click **OK**.

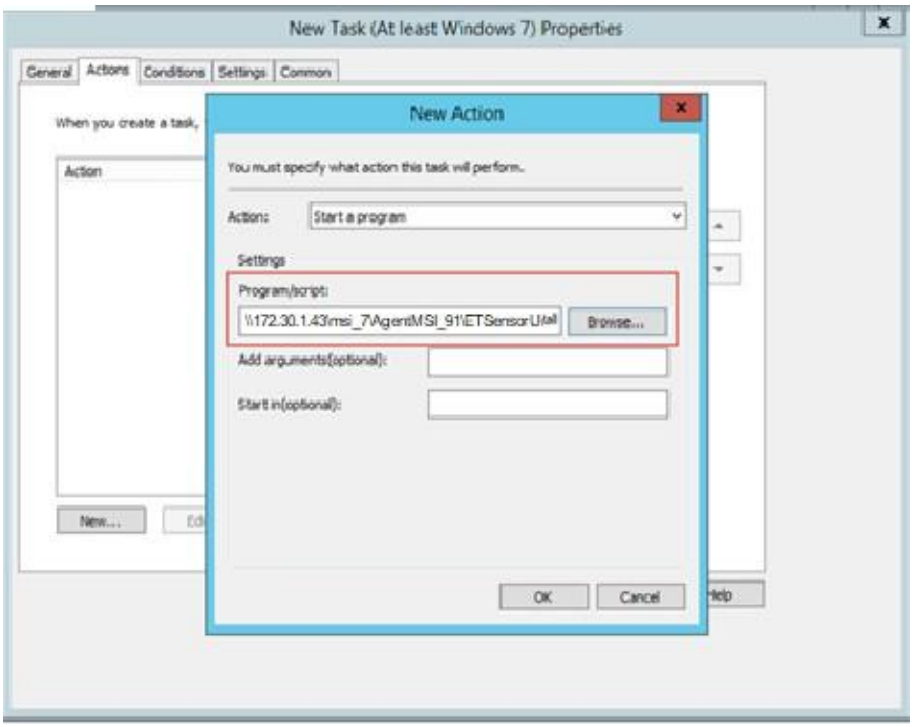


15. Select the check boxes shown below.

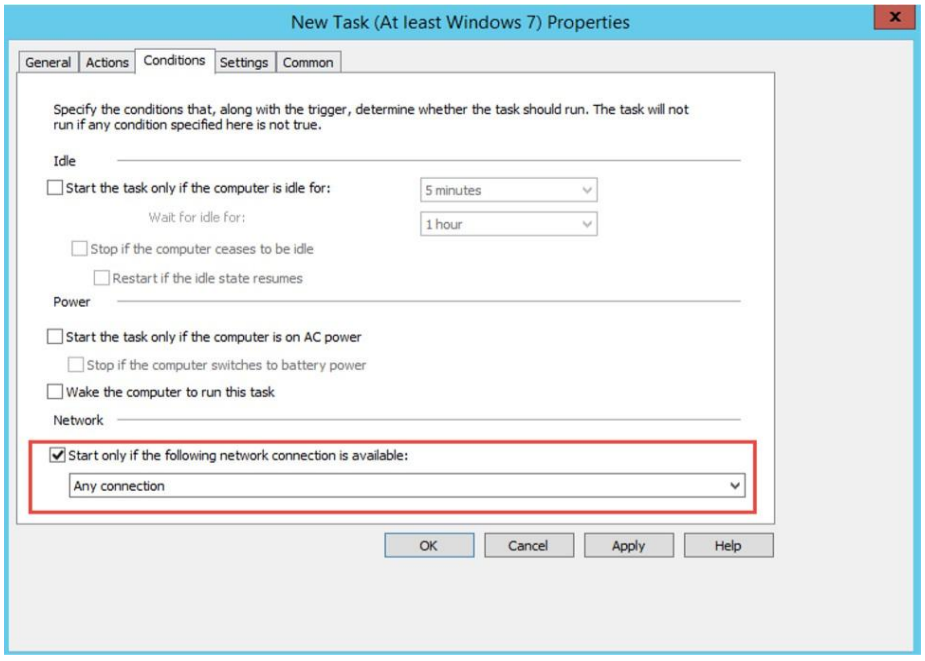


© Copyright Logcollect. All Rights Reserved.

16. In the Actions tab, click **New** and browse the network shared path where the Sensor package is available.



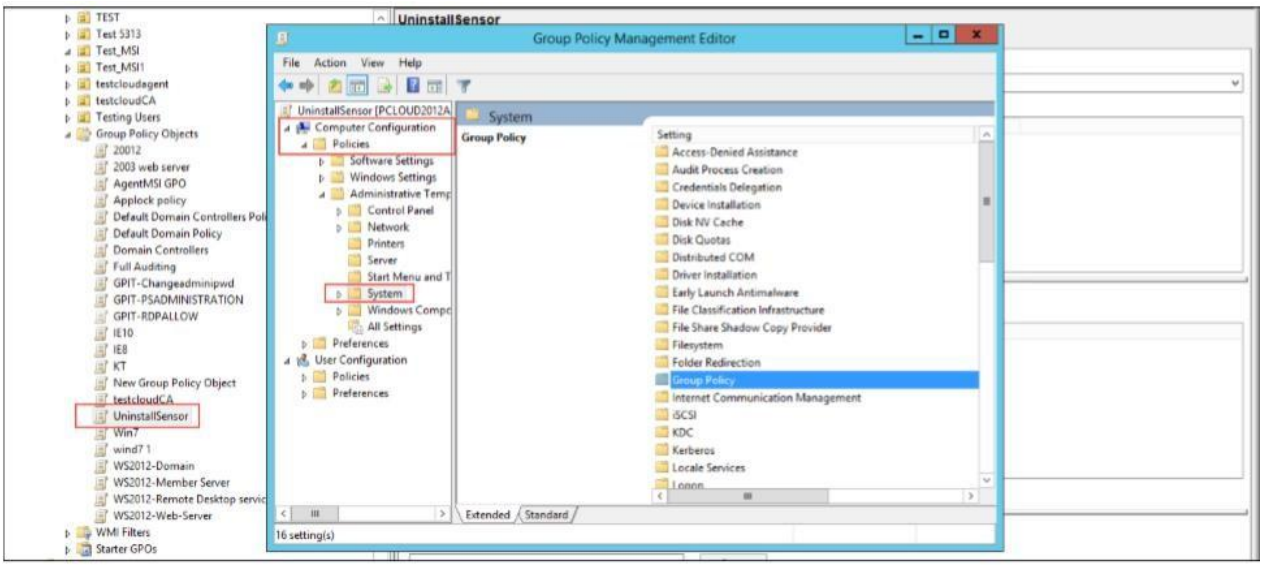
17. In the **Conditions** tab, select the checkbox, shown in the figure below:



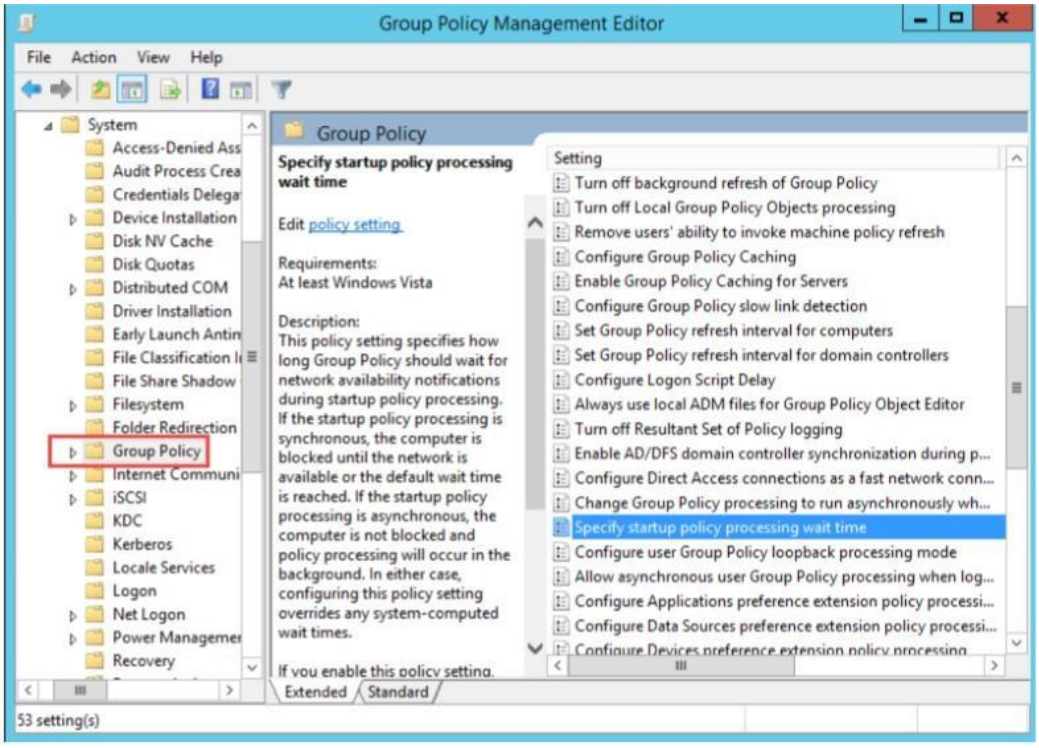
18. Click **Apply** and click **OK**.

© Copyright Logcollect. All Rights Reserved.

19. Again, select the newly created GPO and **right click** > **Edit**. Go to **Computer Configuration** > **Policies** > **Systems** and then select **Group Policy.**

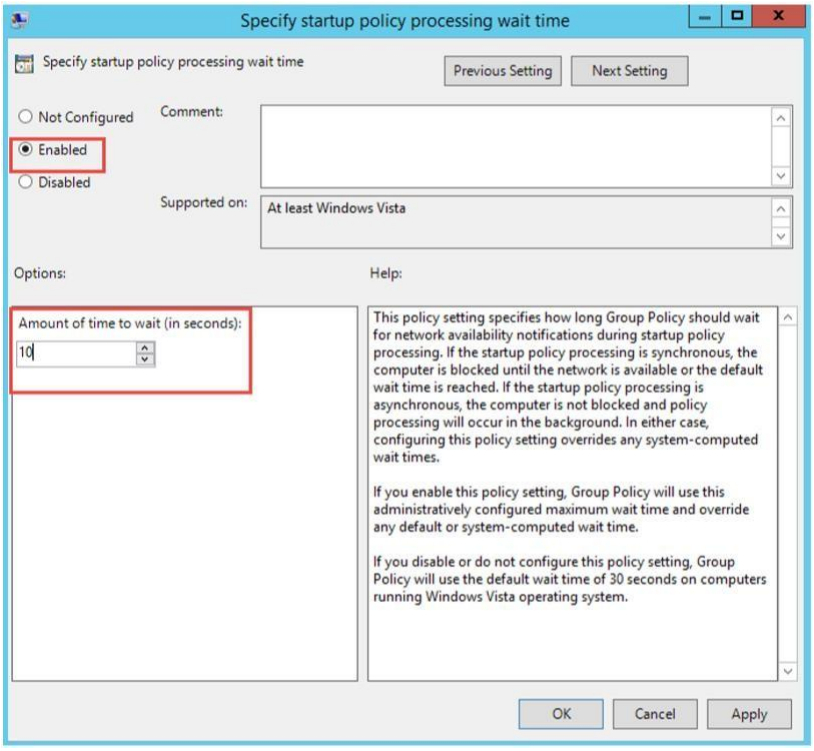


20. Under **Group Policy**, select **Specify Startup Policy Processing Wait Time.**



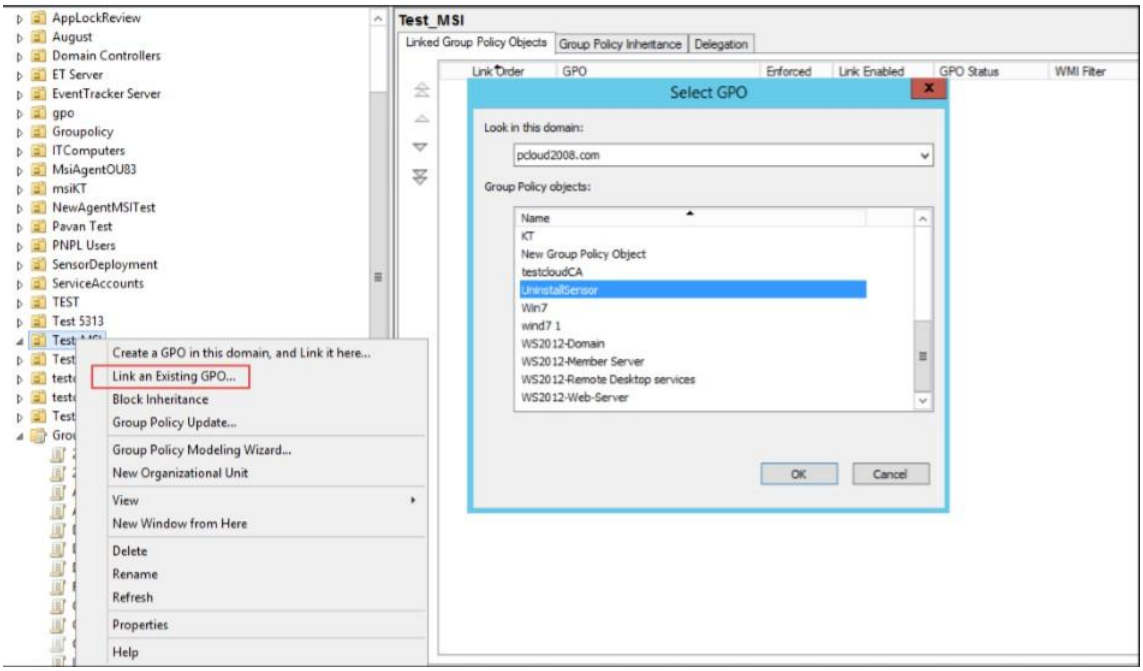
© Copyright Logcollect. All Rights Reserved.

21. Double click the policy and select the enabled radio button and provide the wait time, for example, 10 seconds.



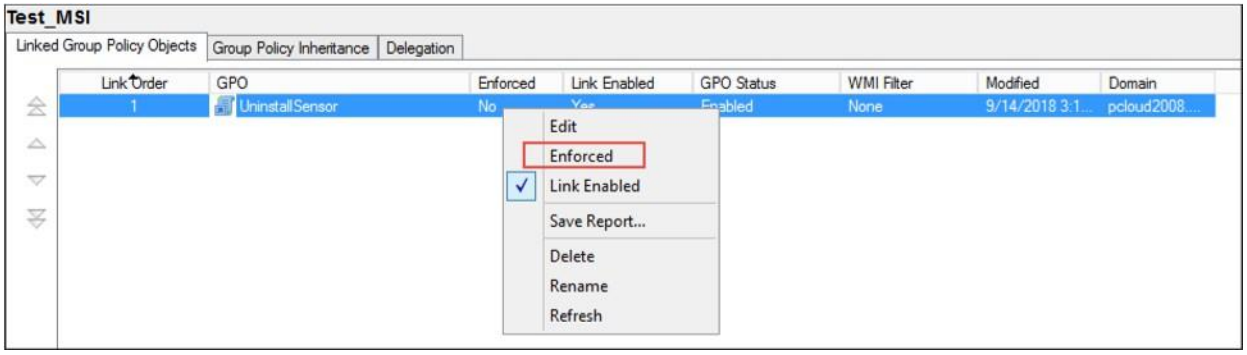
22. Click **Apply** and then **OK**.

23. Once it is done, select the created OU for example, **Test_MSI** and link it to the configured GPO.

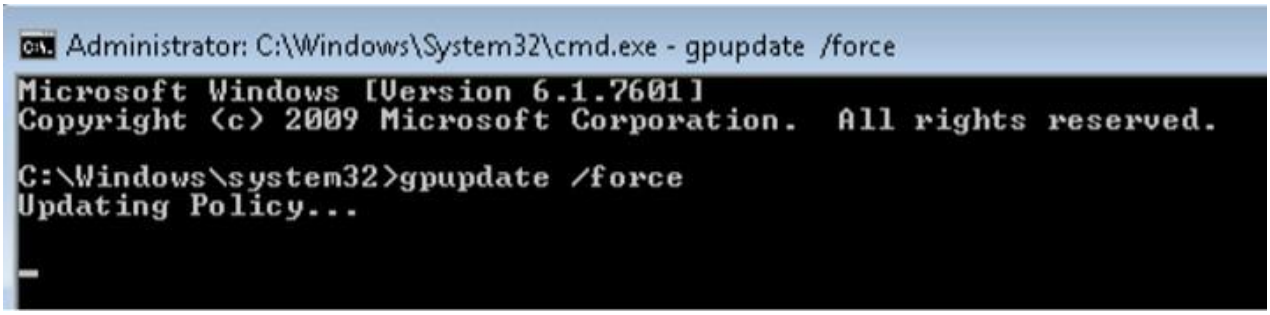


© Copyright Logcollect. All Rights Reserved.

24. Once it is added, right click, and select **Enforced**.



25. Now the user can go to the agent machine and update the **Group policy** by using the command in command prompt. **gpupdate /force**



26. After the policy is successfully applied in the agent machine, the Logcollect sensor gets uninstalled.

8 Uninstalling the Logcollect Sensor through Command Line

8.1 Uninstalling Using Sensor.exe

1. Run the Command Prompt in the Admin mode.
2. Type in the `<cd> <installation file location>`

Command syntax: `<cd> <installation file location>`.

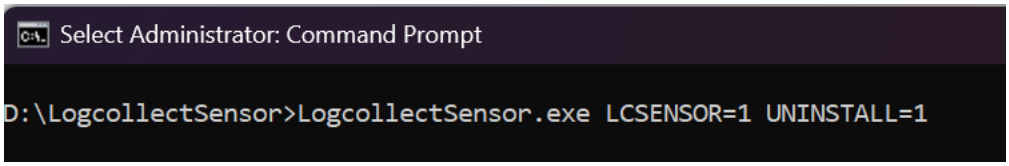
In the above command, change the directory to the file path where the installation (.exe) file is located.

3. Press **Enter** to go to the next line and press **Tab** to retrieve the **.exe** file**.**

© Copyright Logcollect. All Rights Reserved.

4. Press **Space** and type in **`LCSENSOR=1 UNINSTALL=1`** and press **Enter.**

In the following example installation (.exe) file is located in C drive, it may be different on your computer depending on the installation (.exe) file location.



It starts uninstalling the Logcollect sensor in the background.

Command Syntax: `<executable file name.exe> LCSENSOR=1 UNINSTALL=1`

8.2 Uninstalling Using SensorInstaller.exe

1. Extract the installation (.exe) file.
2. Open the Command Prompt in the Admin mode.
3. Type in the **<cd> <extracted file location>**

Command Syntax:

```
<cd> <extracted file location>
```

In the above command, change the directory to the file path where the extracted (.exe file) is located.

4. Press **Enter** to go to the next line and press **Tab** to retrieve the **SensorInstaller.exe** file.
5. Press **Space** and type in the command as mentioned in the example below .

Command Syntax:

```
SensorInstaller.exe CUSTOMCONFIG=1 EA=1 CA=0 EM=ET00.LOGCOLLECT.COM
EP=14515 MIN_GUI=1 IR=1 LS=ET00.LOGCOLLECT.COM LP=14503 CM=LOCALHOST
SUFFIX=BK-PPPP-NS1 IS_SUFFIX=2
PKG_UID=6e7b8611db393e7184f518e27bb130985271a312 LCSENSOR=1 UNINSTALL=1
```

```
D:\LogcollectSensor>SensorInstaller.exe CUSTOMCONFIG=1 EA=1 CA=0 EM=ET00.LOGCOLLECT.COM
EP=14515 MIN_GUI=1 IR=1 LS=ET00.LOGCOLLECT.COM LP=14503 CM=LOCALHOST SUFFIX=BK-PPPP-NS1
IS_SUFFIX=2 PKG_UID=6e7b8611db393e7184f518e27bb130985271a312 LCSENSOR=1 UNINSTALL=1
```

It starts uninstalling the Logcollect sensor in the background.

© Copyright Logcollect. All Rights Reserved.

About Logcollect

Logcollect is a software-only telemetry pipeline which supports the collection, enrichment, transformation and routing of security data from sources to multiple destinations. It is targeted to security operations that are struggling with distributing large volumes of disparate data, high operational costs, alert fatigue and missed threats. It is available as a software license or hosted in AWS. It is backed by a team that has extensive experience with security logging, SIEM and regulatory compliance. Collect once, analyze everywhere.

Headquartered in Ft. Lauderdale, FL, Logcollect is a leader in Log Collection. Learn more at www.Logcollect.com.

Contact Us

Corporate Headquarters

Prism Microsystems
920 NE 17th Way
Fort Lauderdale, FL 33304

https://www.Logcollect.com/support

© Copyright Logcollect. All Rights Reserved.