

Log Collector Installation - Ciso Workplace(old)

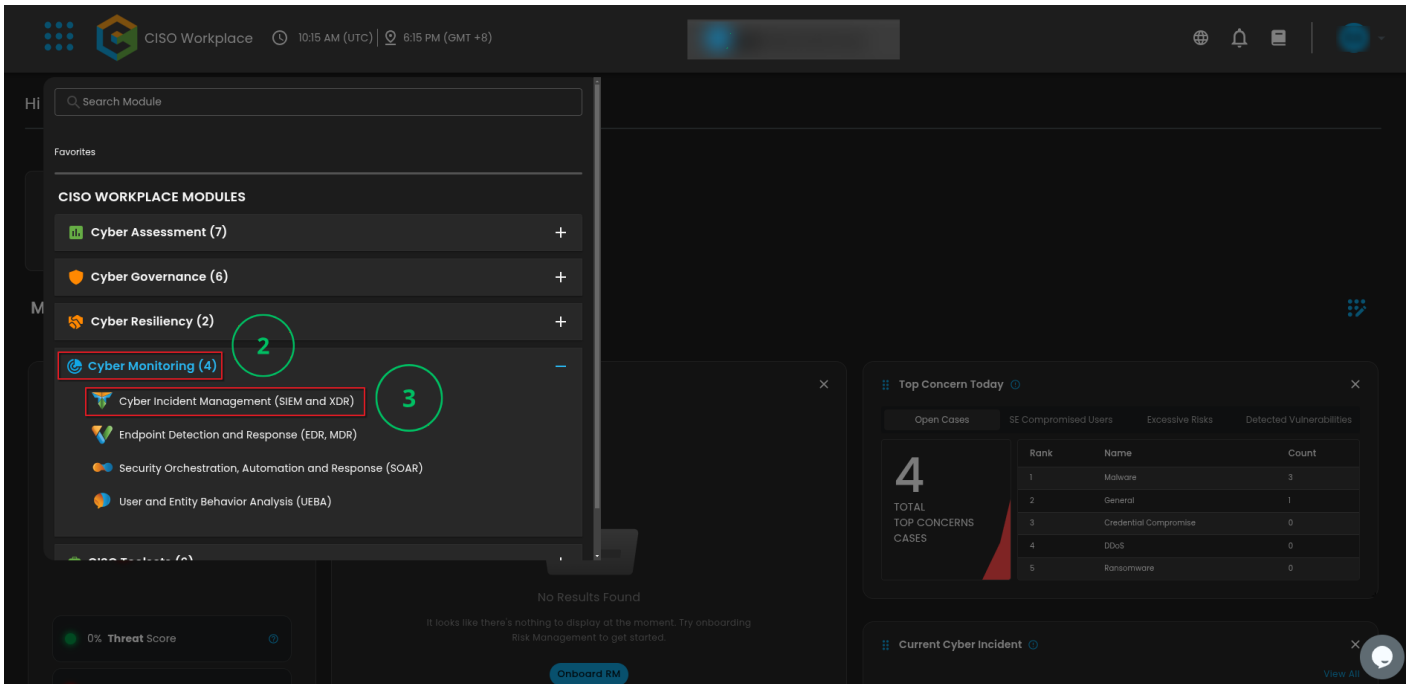
Please follow the steps below to manually add a Log Collector using Windows Environment.

Step 1: Log in to your **CISO Workplace** and click the **rectangular dots**.

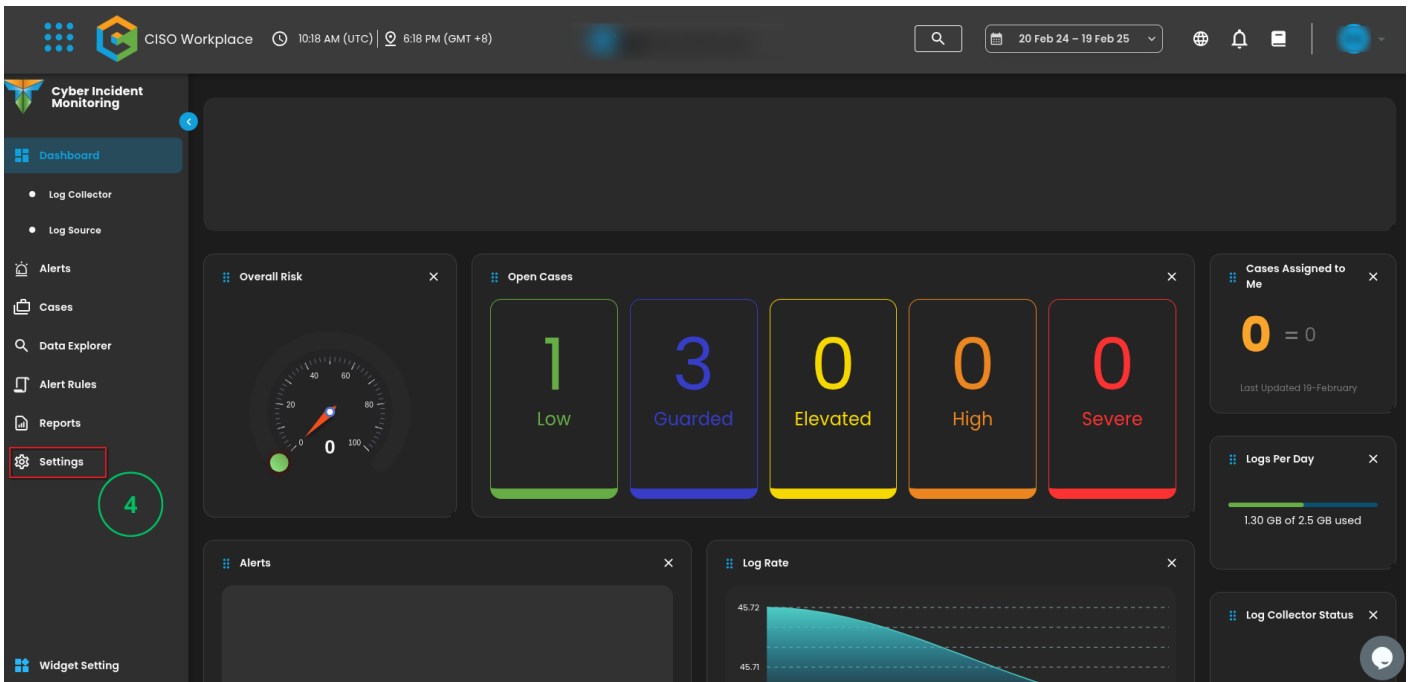
The screenshot displays the CISO Workplace interface. At the top, the header includes the CISO Workplace logo, a grid icon (rectangular dots) circled in red, and the text 'CISO Workplace'. Below the header, a greeting 'Hi [User], Good Evening' is shown. The main dashboard area is titled 'My Dashboard' and contains several widgets: 'Cyber Incident Monitoring' (Recent Action: 19 minutes ago), 'Risk Score' (0% Threat Score, Minimal), 'CRAM™ live' (No Results Found), 'Top Concern Today' (4 TOTAL TOP CONCERNS CASES), and 'Current Cyber Incident' (View All).

Step 2: Click "**Cyber Monitoring**".

Step 3: Go to "**Cyber Incident Management (SIEM and XDR)**".

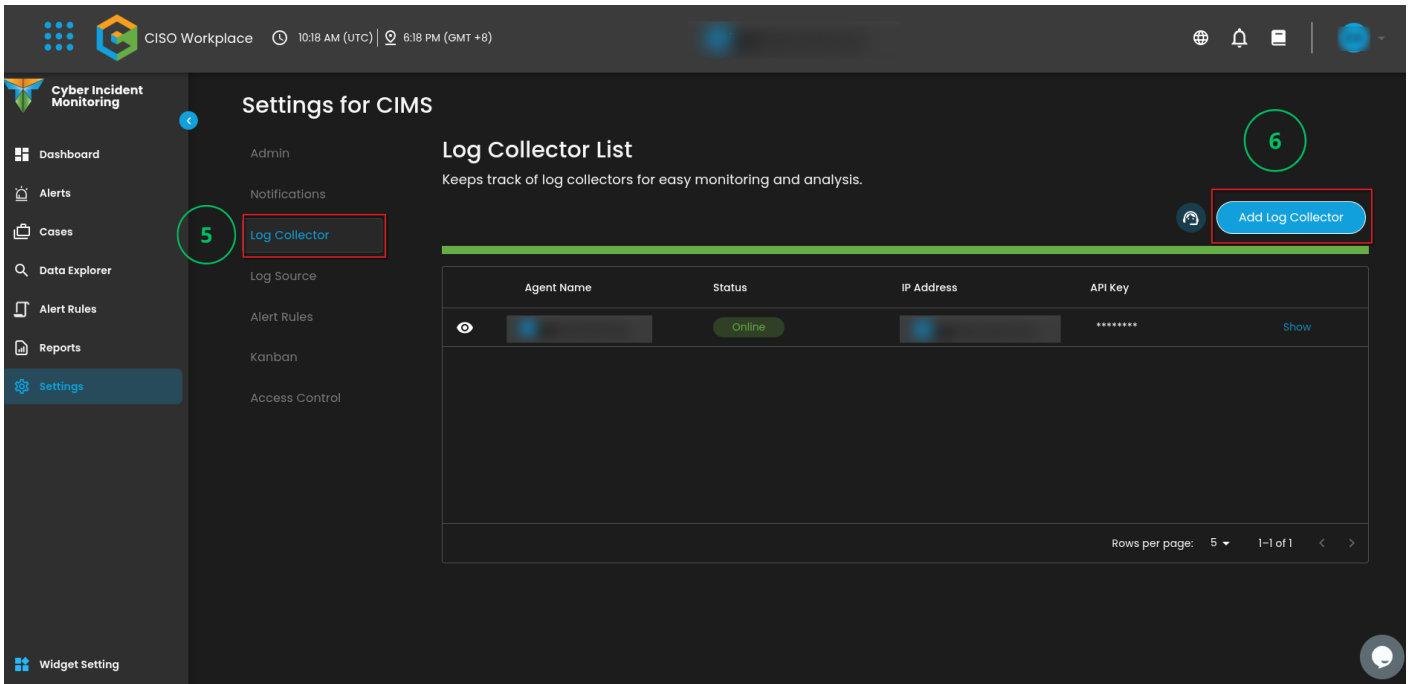


Step 4: Go to "Settings".



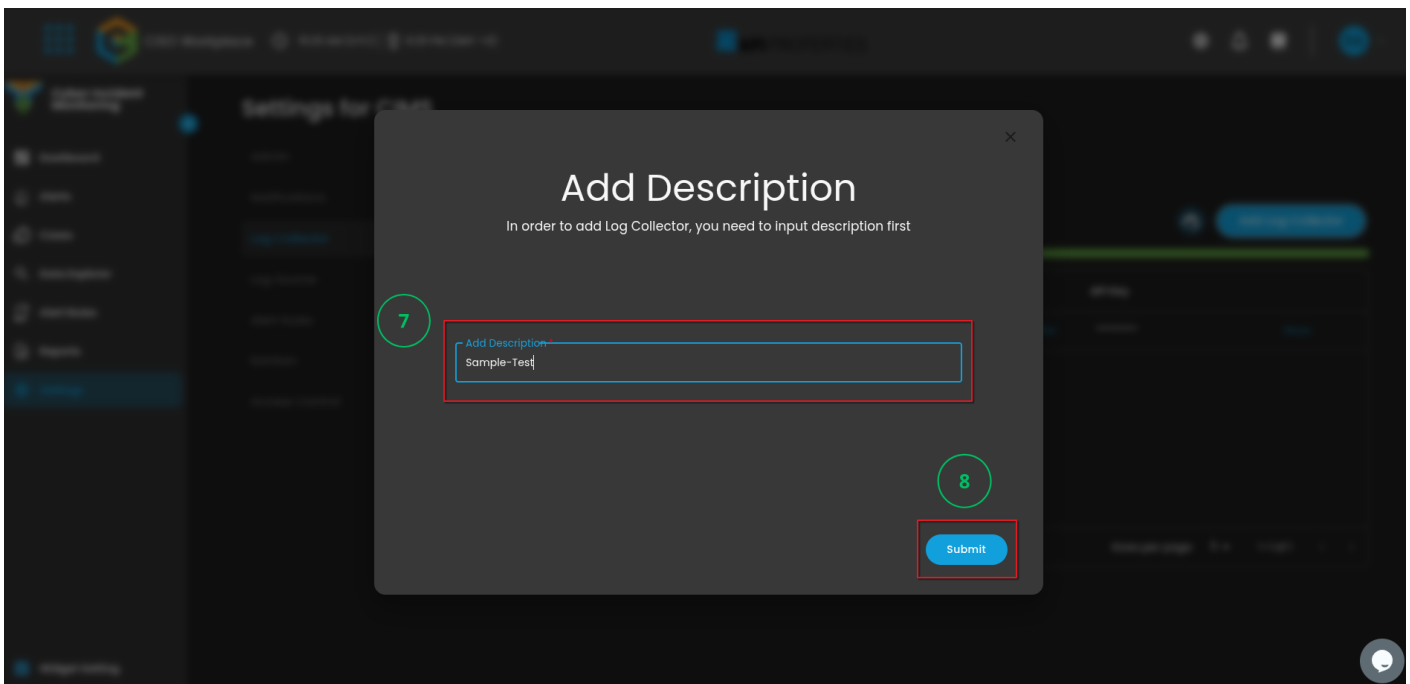
Step 5: Go to "Log Collector".

Step 6: Click "Add Log Collector".



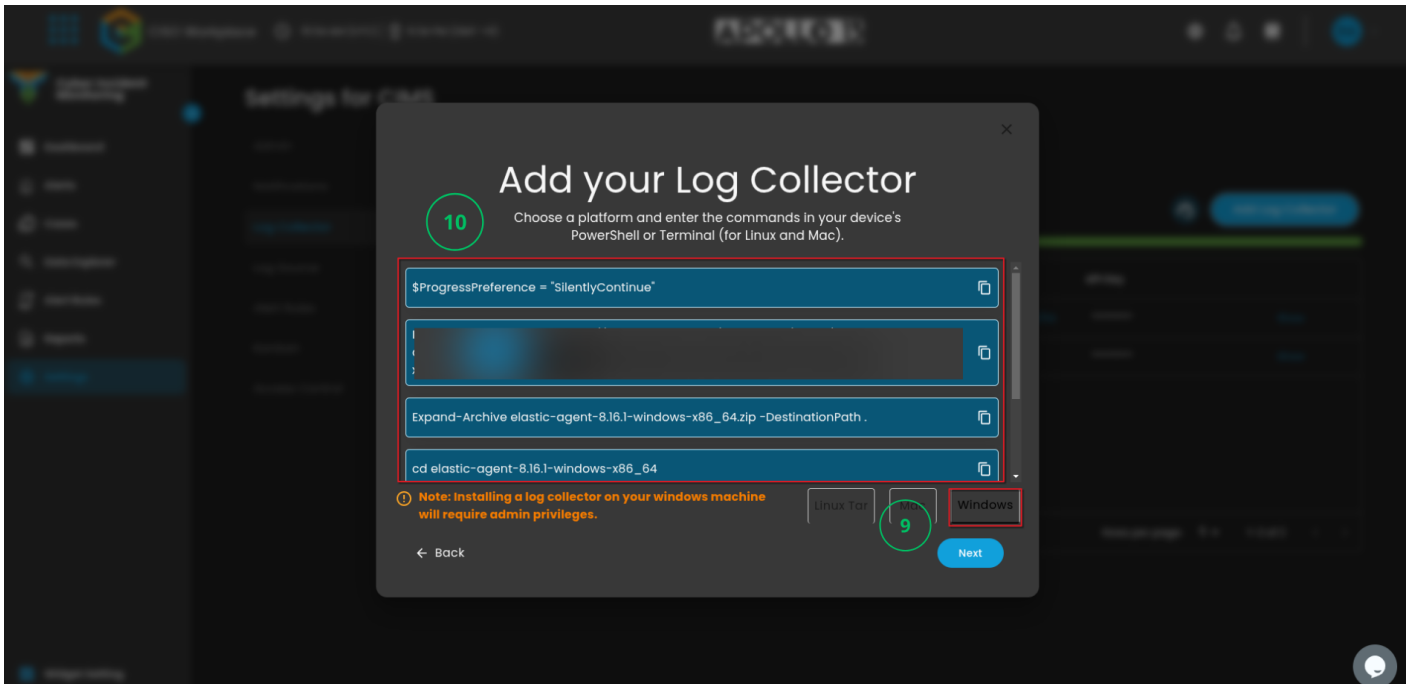
Step 7: A pop window will show. **Add a description** that can easily identify the Log Collector.

Step 8: Click "**Submit**".

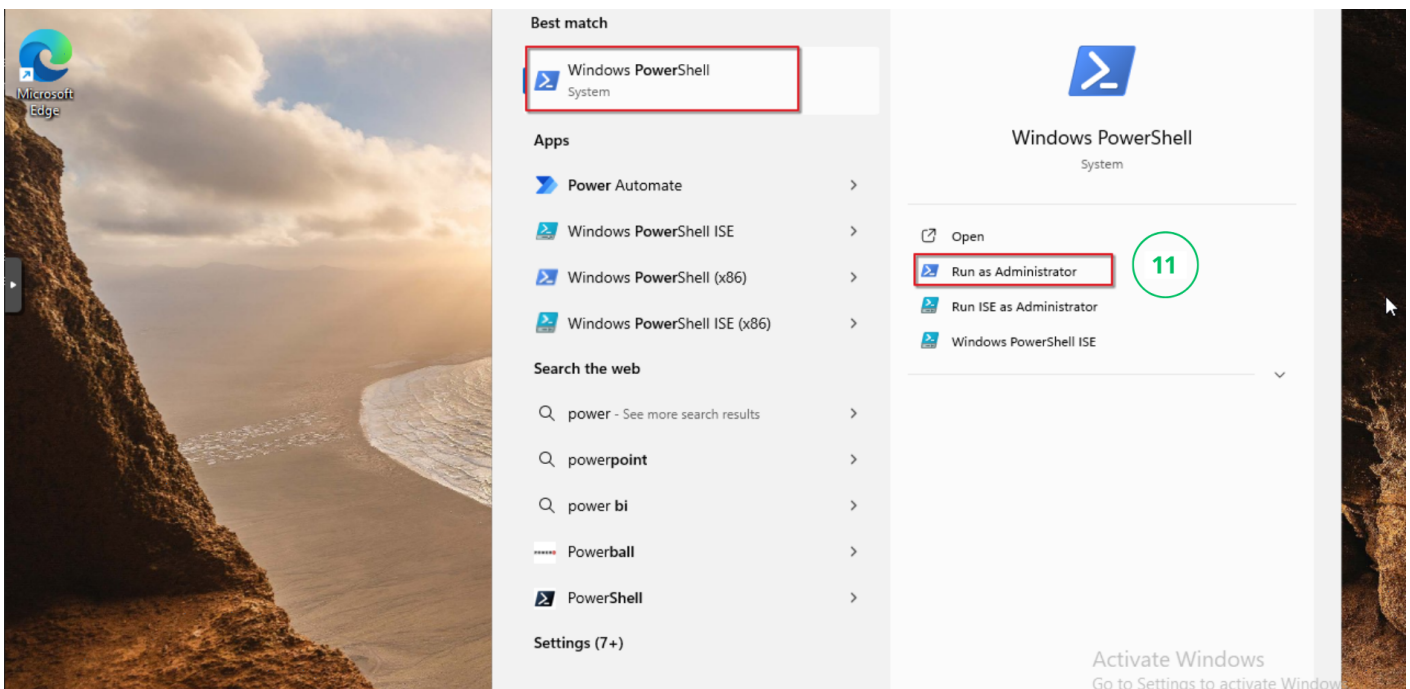


Step 9: After proceeding to the next page. Click on the "**Windows**" panel to display the windows command needed for installing the Elastic Agent.

Step 10: Take **NOTE** of the commands. You will need it in Step 12.



Step 11: Go to your Windows Environment and **Run PowerShell as Administrator**.



Step 12: **Copy and Paste** the command from Step 10. Make sure to copy it correctly. **Individually execute the commands** in PowerShell CLI to avoid unexpected errors. Some commands will take time executing. So, wait for it to process. A successful execution of the commands results in a new line as shown in the image.

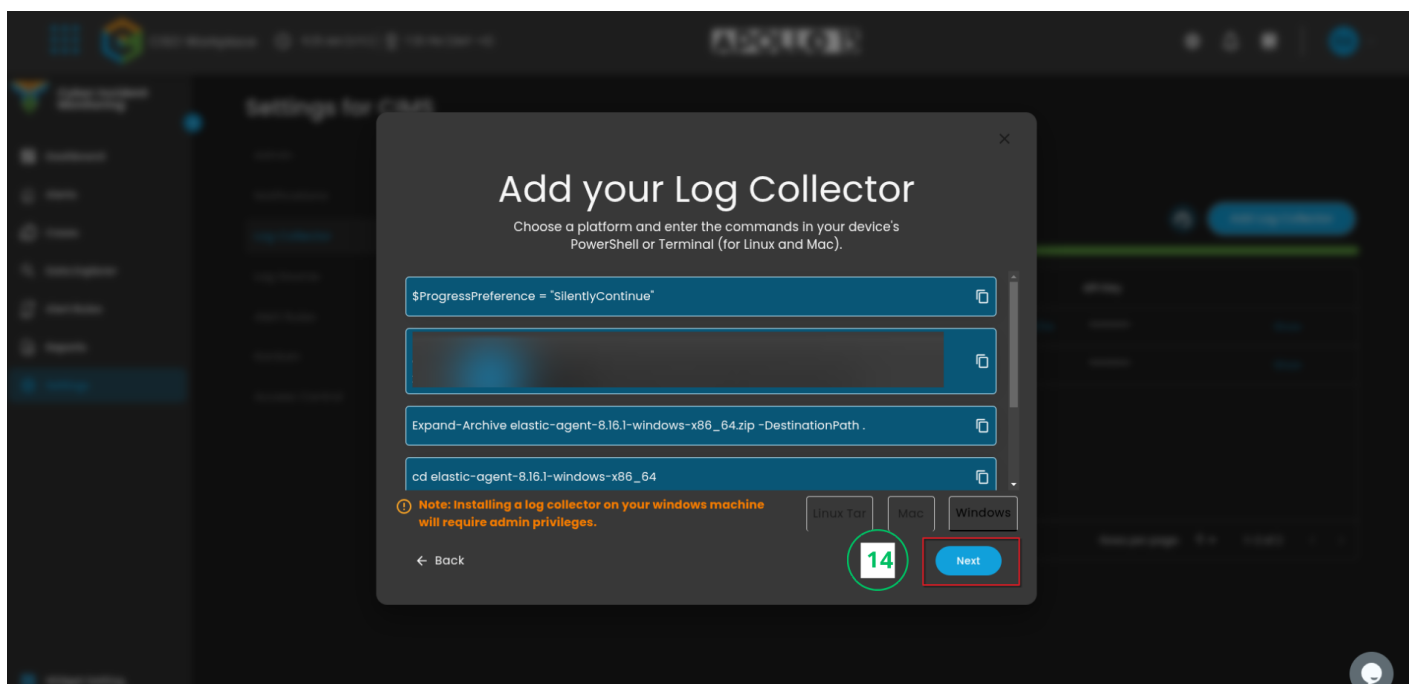
When prompted "Elastic Agent will be installed at", just type "Y" to proceed with the installation.

Step 13: After installing the Elastic Agent, you will see a "Successfully enrolled the Elastic Agent" and "Elastic Agent has been successfully installed".

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> $ProgressPreference = 'SilentlyContinue'
PS C:\WINDOWS\system32> Invoke-WebRequest https://artifacts.elastic.co/downloads/elastic-agent-8.16.4-windows-x86_64.zip
PS C:\WINDOWS\system32> Expand-Archive .\elastic-agent-8.16.4-windows-x86_64.zip
PS C:\WINDOWS\system32> cd elastic-agent-8.16.4-windows-x86_64
PS C:\WINDOWS\system32\elastic-agent-8.16.4-windows-x86_64> .\elastic-agent.exe --url=https://fleet.elastic.co --ecs-version=1.6.0
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
[+] Service Started [1s] Elastic Agent successfully installed, starting enrollment.
[+] Waiting For Enroll... [2s] {"log.level":"info","@timestamp":"2025-02-19T20:05:18.282+0800","log.origin":{"function":"github.com/elastic/elastic-agent/cmd/enroll","file.line":520},"message":"Starting enrollment to URL: https://fleet.elastic.co"}
[+] Waiting For Enroll... [4s] {"log.level":"info","@timestamp":"2025-02-19T20:05:20.662+0800","log.origin":{"function":"github.com/elastic/elastic-agent/cmd/enroll","file.line":301},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
[+] Done [4s] Elastic Agent has been successfully installed.
PS C:\WINDOWS\system32\elastic-agent-8.16.4-windows-x86_64>
```

Step 14: Go to back to **CISO Workplace** and proceed with the installation.

Just click "**Next**" to proceed.



Step 15: After proceeding in the next page. It will show "**Checking Agent**" and "**Successfully added:_____**". An Agent Name will show with its corresponding IP Address and Status. You should have the same output in the picture below. Showing a successful installation of the Elastic Agent and a successful addition in CISO Workplace.

CISO Workplace 12:33 PM (UTC) 8:33 PM (GMT +8)

Cyber Incident Monitoring

Settings for CIMS

Admin

Notifications

Log Collector

Log Source

Alert Rules

Kanban

Access Control

Log Collector List

Keeps track of log collectors for easy monitoring and analysis.

Add Log Collector

	Agent Name	Status	IP Address	API Key	
	[blurred]	Online	[blurred]	*****	Show
	[blurred]	Online	[blurred]	*****	Show
	[blurred]	Offline	[blurred]	*****	Show

17

Rows per page: 5 1-3 of 3

Widget Setting

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

Revision #7

Created 19 February 2025 13:04:29 by Richmond Abella

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