

# FAQ: What do I do if I have Cortex XDR which causes unsuccessful installation of the Log Collector?

## Elastic Agent Main installation path (windows)

When installing Elastic Agent on a Windows machine, the installation files are placed in specific directories. Below are the important paths to know for managing and troubleshooting the Elastic Agent.

### Temporarily Disable Cortex XDR Antivirus

To allow for a smooth installation, you may need to temporarily disable the Cortex XDR antivirus:

- **Disable Cortex XDR Antivirus:**
  - Start a CMD Prompt, PowerShell, or Windows Terminal as an **ADMINISTRATOR**
  - Type **cytool protect disable** and press **ENTER**
  - Type in the password
    - The default password for Cortex XDR cytools is **Password1**
  - Wait for the tool to disable the Cortex services

## Main Installation Path

- The Elastic Agent's main installation folder on Windows is located at:

```
C:\Program Files\Elastic\Agent
```

This directory contains the core Elastic Agent files, including the binaries necessary for the agent to function, configuration files, and various modules.

### Configuration Files

- After installation, Elastic Agent's configuration files can be found under:

```
C:\Program Files\Elastic\Agent\elastic-agent.yml
```

The `elastic-agent.yml` file contains important configuration settings for data collection, integrations, and connectivity to the Elastic Stack.

## Log Files

- Log files generated by Elastic Agent during its operation are stored at:

`C:\Program Files\Elastic\Agent\logs`

These logs are useful for monitoring the health of the agent and diagnosing any issues that arise during operation.

## Data Directory

- The Elastic Agent stores its temporary data and downloaded module files in the following path:

`C:\Program Files\Elastic\Agent\data`

This directory is used to manage the agent's internal state, cache data, and more.

## Uninstall Path

- To uninstall Elastic Agent from the system, you can find the uninstallation files and services within the same main installation directory (`C:\Program Files\Elastic\Agent`), or you can uninstall it via the **Control Panel > Programs and Features**.

By understanding and utilizing these paths, you can easily manage the Elastic Agent on a Windows machine, adjust configurations, troubleshoot issues, or perform updates and uninstallation.

**After locating the Installation path of Elastic Agent, proceed to the whitelisting step.**

# Whitelist the Elastic Agent Installer in Cortex XDR

- **Find the executable:** Determine the path or the exact name of the Elastic Agent installer or any processes it spawns.
- **Create an Allow List:**
  1. Log in to the Cortex XDR management console.
  2. Navigate to **Endpoints > Policies**.
  3. Locate the policy that is enforcing restrictions on software installations.
  4. Go to the **Allow List** section.
  5. Add the **Elastic Agent installer** to the allow list by specifying its executable path or file hash.

# Temporarily Disable Certain Cortex XDR Modules

- Some Cortex XDR modules might block certain operations or files. You can temporarily disable specific modules rather than turning off Cortex XDR completely:
  - **Disable Exploit Prevention:** If this module is causing the block, disable it temporarily during the installation.
  - **Disable Behavioral Threat Protection:** This can also interfere with installations.
- After the installation, turn the protection modules back on.

## Run the Installation in Exclusion Mode

- You can try running the installer in a way that bypasses Cortex XDR monitoring for certain directories or processes. In the Cortex XDR management console, you can:
  1. Create a **Folder Exclusion** for the folder where you're installing the Elastic Agent.
  2. Go to **Endpoints > Endpoint Protection**.
  3. In the **Exclusions** section, add the directory where Elastic Agent is being installed.

Cortex XDR file and folder exclusion link:

[File and Folder exclusion link](#)

---

Revision #11

Created 3 October 2024 05:51:25

Updated 4 October 2024 01:56:27