CrowdStrike

☑ Installing the Falcon Sensor for Windows

1. Download the Falcon sensor installer

- Navigate to:
  `Host Setup and Management > Deploy > Sensor Downloads`
  URL (if you're in the Falcon UI): ***https://falcon.us-2.crowdstrike.com/hosts/sensor-downloads***

2. Copy your Customer ID Checksum (CID)

- You'll find this value on the **Sensor Downloads** page.

3. Silent Install Command

Use the following command:

<installer_filename> /install /quiet /norestart CID=<CCID>

 Replace:

- <installer_filename> with the actual file name you downloaded
- <CCID> with your actual CrowdStrike Customer ID

☑ Tagging for Windows

This command assigns two tags to the host: Washington/DC_USA and Production

```
<installer_filename> /install /quiet /norestart CID=<CCID>
GROUPING_TAGS="Washington/DC_USA,Production"
```

- Tags must be comma-separated
- Tags should not contain spaces
- You can set multiple tags at once

☑ Verifying Falcon Sensor Installation Windows

1. Open Command Prompt

- Run as Administrator (recommended).

2. Execute the Command

```
sc.exe query csagent
```

🔍 Expected Output If Sensor Is Running

You should see output similar to this:

```
SERVICE_NAME: csagent
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Key Indicator

Look for this line:

```
STATE              : 4  RUNNING
```

This confirms that the **csagent service is active**, which means the **Falcon sensor is running properly**.

☑ Uninstalling the Falcon Sensor for Windows

- **Download the Uninstall Tool:**
  - Go to:
    `Support > Tool Downloads`
    and download the:
    Falcon Windows Sensor Uninstall Tool
- **Retrieve the Maintenance Token:**
  - Follow instructions under:
    `Making changes to a single host`
    (linked in your CrowdStrike dashboard under sensor update policies).
- **Run the Uninstall Command:**
  - Open **Command Prompt as Administrator**
  - Run:

    ```
    CsUninstallTool.exe MAINTENANCE_TOKEN=<your_token_here> /quiet
    ```

📦 SCP Command to Transfer Falcon Sensor to Windows

```
scp <path_to_installer>\<installer_filename> <username>@<windows_host>:/C:/Temp/
```

🔧 Example:

```
scp C:\Installers\WindowsLegacySensor.exe admin@192.168.1.20:/C:/Temp/
```

🔁 **Replace the Placeholders:**

- `<path_to_installer>` — Local path to the sensor file (use `\` on Windows)
- `<installer_filename>` — The exact name of the `.exe` file
- `<username>` — SSH username on the Windows host