Automatic Sensor Installation

Use this installation path if you want to automate silent installations on many devices, including installations via a deployment tool such as Windows System Center Configuration Manager (SCCM).

1. Download the sensor installer from Hosts > Sensor Downloads. Use the Chrome browser.
2. Copy your customer ID checksum (CCID) from Hosts > Sensor Downloads.
3. Run or configure your deployment tool to use this command, replacing <your executable file name> with the name of the install file you downloaded, and <CCID> with the CCID from step 2 :

**<your executable file name>.exe /install /quiet /norestart CID=<CCID**

### Assigning Sensor Tags During Installation

Sensor tags are user-selected identifiers you can use to group and filter hosts. You can assign one or more tags to a host using the GROUPING\_TAGS parameter (case sensitive). You must set tags at installation time.

Tags can include alphanumeric characters, hyphens (-), underscores (\_), and forward slashes (/). To use multiple tags, separate each tag with commas. Tags can't include spaces ( ) or commas (,). All tags for a host, including any comma separators, must be a total of 256 characters or less.

WindowsSensor.exe /install /norestart CID=<your cid> GROUPING\_TAGS="Washington/DC\_USA,Production"

This sets two tags: Washington/DC\_USA and Production.

Tags can be added or changed after sensor installation by editing a registry key.

### Installing the Sensor with IE Proxy Detection

On hosts using IE proxy detection, install the sensor from the command line using the ProvNoWait parameter. The sensor acquires proxy settings from the user registry hive with the next user login.

WindowsSensor.exe /install /norestart CID=<your CID> ProvNoWait=1

### Installing the Falcon Sensor on a Virtual Machine Template

Follow these steps to set up a virtual machine template with a Falcon sensor.

Do not perform a normal install on a template: If you perform a normal installation on your virtual machine template, all hosts that use the template will be assigned the same agent ID (AID). The Falcon console will display activity from all these hosts as if the activity came from a single host.

#### **INSTALLING ON A VM TEMPLATE**

To install on a virtual machine (VM) template:

1. Prepare your VM template.
2. Install the sensor with the NO\_START=1 parameter:

**WindowsSensor.exe /install /quiet /norestart CID=<your CID> NO\_START=1**

1. Shut down the VM.
2. Use your virtualization software to convert the VM to a template image.

When a VM created from this template first starts up, the CrowdStrike cloud assigns it a unique AID.

#### **MODIFYING A VM TEMPLATE**

To modify a VM template that has an existing sensor installation:

1. Prepare your VM template.
2. Remove these registry values to remove the AID from the VM template:
   * HKEY\_LOCAL\_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default\AG
   * HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CSAgent\Sim\AG
3. Shut down the VM.
4. Use your virtualization software to convert the VM to a template image.

### Installing the Falcon Sensor in a Virtual Desktop Infrastructure (VDI) Environment

When installing in a Virtual Desktop Infrastructure (VDI) environment, the sensor runs from a shared, read-only OS image. The CrowdStrike cloud assigns the correct AID based on the host's fully qualified domain name (FQDN) and other characteristics.

To install the Falcon sensor for Windows on your VDI master image:

1. Prepare your VDI master image.
2. Install the sensor with the VDI=1 parameter:

**WindowsSensor.exe /install CID=<your CID> VDI=1**

Update your VDI master's sensor: We recommend regularly updating your VDI master image to use the latest Falcon sensor version. This minimizes the risk of new VDI instances running outdated Falcon sensors, as well as network traffic caused by sensor updates.

### Verify that the Sensor is Running

To verify that the sensor is running on your host:

1. Open a command prompt with administrative privileges on the host.
2. Run this command: sc query csagent

The following output is displayed if the sensor is running:

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

Verify the Host's Connection to the CrowdStrike Cloud

You can verify that the host is connected to the cloud using the Falcon console or a command line on the host.

* Falcon console: Use the Sensor Report to search for the host.
* Host: Run this command from a command line with administrative privileges:

netstat -f

The following output is displayed if the sensor can connect to the CrowdStrike cloud:

Active Connections Proto   Local Address State     Foreign Address TCP     192.0.2.130:49790    ec2-54-219-145-181.us-west-1.compute.amazonaws.com:https  ESTABLISHED

In this example, ec2-54-219-145-181 indicates a connection to a specific IP address in the CrowdStrike cloud, 54.219.145.181. SeeCloud IP Addresses for a full list of CrowdStrike cloud IPs.

If your host uses a proxy, the Foreign Address shows the proxy address, such as proxy.example.com, instead of the CrowdStrike Cloud address.