Falcon Sensor for Windows Deployment

Last updated: Jan. 24, 2024

Introduction

Falcon sensor for Windows stops breaches by unifying true next-generation antivirus (NGAV) endpoint detection and response (EDR), identity protection, managed threat hunting, and threat intelligence automation, all within a single, lightweight sensor.

This solution combines simple deployment with ease of management, and eliminates the need for additional resources.

System requirements

Supported operating systems

Only these operating systems are supported for use with the Falcon sensor for Windows.

> **Note**: For identity protection functionality, you must install the sensor on your domain controllers, which must be running a 64-bit server OS. Windows Server 2008 R2 SP1 is supported for Falcon sensor versions 6.51 or later.

Supported 64-bit server OSes

64-bit Windows Server OSes	Version	Build	LTSC Release?	Minimum Sensor Version	Falcon EOS Date
Server 2022	21H2	20348	Yes	6.30.14406[1]	April 13, 2032
Server Core 2022	21H2	20348	Yes	6.30.14406[1]	April 13, 2032
Server 2019	1809	17763	Yes	All supported sensor versions	July 8, 2029
Server Core 2019	1809	17763	Yes	All supported sensor versions	July 8, 2029
Server 2016	1607	14393	Yes	All supported sensor versions	July 11, 2027
Server Core 2016	1607	14393	Yes	All supported sensor versions	July 11, 2027
Server 2012 R2	—	9600	—	All supported sensor versions	April 11, 2027
Storage Server 2012 R2	—	9600	—	All supported sensor versions	April 11, 2027
Server 2012	—	9200	—	All supported sensor versions	April 11, 2027
Server 2008 R2 SP1	—	7601	—	All supported sensor versions	July 9, 2025

[1]The minimum sensor version required to enable Identity Protection Traffic inspection is 6.53.16705.

Supported desktop OSes

Windows Desktop OSes	Version	Codename	Marketing Name	Build	LTSC Release?	64-bit Support?	64-bit IOT Enterprise Support?	32-bit Support?	ARM64 Support?	Minimum Sensor Support	Falcon Date
Windows 11	23H2	Sun Valley 3	2023 Update	22631	— [3]	Yes	—	—	Yes[4]	7.05.17706	May 9,
Windows 11	22H2	Sun Valley 2	2022 Update	22621	— [3]	Yes	—	—	Yes[4]	6.45.15907	April 1 2026
Windows 11	21H2	Sun Valley	N/A	22000	— [3]	Yes	—	—	Yes[4]	6.31.14505 ARM64: 6.38.15205	April 7 2025
Windows 10	22H2	22H2	2022 Update	19045	—	Yes	Yes	Yes[2]	Yes[4]	6.47.16103	Nov 0 2025
Windows 10	21H2	21H2	November 2021 Update	19044	Yes	Yes	Yes	Yes[2]	Yes[4]	6.33.14704 ARM64: 6.44.15803	July 11 2027 (Enter July 11 2032 (Enterp
Windows 10	21H1	21H1	May 2021 Update	19043	—	Yes	Yes	Yes [2]	Yes[4]	All supported sensor versions ARM64: 6.44.15803	June 1 2023
Windows 10	20H2	20H2	October 2020 Update	19042	—	Yes	Yes	Yes [2]	Yes [4]	All supported sensor versions ARM64: 6.44.15803	Noven 5, 202
Windows 10	1809	Redstone 5 ("RS5")	October 2018 Update	17763	Yes	Yes	Yes	Yes [2]	—	All supported sensor versions	July 8, 2029
Windows 10	1607	Redstone 1 ("RS1")	Anniversary Update	14393	Yes	Yes	—	—	—	All supported sensor versions	April 2 2027
Windows 10	1507	Threshold 1	N/A	10240	Yes	Yes	—	—	—	All supported sensor versions	April 1 2026
Windows 7 SP1	—	—	—	7601	—	Yes	—	Yes	—	All supported sensor versions	July 9,

Windows Desktop OSes	Version	Codename	Marketing Name	Build	LTSC Release?	64-bit Support?	64-bit IOT Enterprise Support?	32-bit Support?	ARM64 Support?	Minimum Sensor Support	Falcon Date
Windows 7 Embedded POS Ready	—	—	—	7601	—	Yes	—	Yes	—	All supported sensor versions	July 9,

[2] Additional User Mode Data (AUMD) and Script Control are not supported on Windows 10 32-bit operating systems.

[3] Microsoft has stated that a Windows 11 LTSC release is a future deliverable.

[4] Some features and prevention policy settings aren't supported on Windows ARM64-based hosts. For more info, see Unsupported features on ARM64-based hosts [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#p89d53de].

Unsupported features on ARM64-based hosts

These features and prevention policy settings aren't supported on any Windows ARM64-based hosts:

- Additional User Mode Data (AUMD)
- BIOS Deep Visibility
- Device Control
- Engine (Full Visibility)
- Interpreter-Only

These prevention policy settings aren't supported on Windows 10 ARM64-based hosts:

- Script-Based Execution Monitoring
- Suspicious Scripts and Commands

Unsupported Windows versions

All other Windows OSes are ***unsupported***, including but not limited to:

- All pre-GA versions/builds of Windows – Windows Insider Preview, beta, etc – unless specifically stated in a Release Note.
- Windows Server IoT 2022/2019, which are OEM versions for appliances
- Windows Server 2008 (non-R2), which is based on the Vista kernel
- Windows Server Core, all versions other than 2016, 2019, and 2022
- Windows 10 64-bit v1511, aka Threshold 2
- Windows 10 64-bit v1703, aka Redstone 2 ("RS2")
- Windows 10 64-bit v1709, aka Redstone 3 ("RS3")
- Windows 10 64-bit v1803, aka Redstone 4 ("RS4")
- Windows 10 64-bit v1903, aka 19H1
- Windows 10 64-bit v1909, aka 19H2
- Windows 10 64-bit v2004, aka 20H1
- Windows 10 64-bit v21H1
- All 32-bit versions of Windows 10 not listed above
- All versions of Windows 8.1
- All versions of Windows 8

- Container-based Windows OS solutions, including but not limited to Docker, are not currently supported.
- Windows Embedded Standard 7 is unsupported. This version is independent from Windows 7 Embedded POS Ready, which is the only Embedded version we do support.
- Windows 10 & 11 running in S mode [https://supportportal.crowdstrike.com/s/article/ka16T000000wxiWQAQ]

Services

These services must be installed and running:

- **LMHosts**
  Note: LMHosts might be disabled on your host if the **TCP/IP NetBIOS Helper** service is disabled.
- **Network Store Interface (NSI)**
- **Windows Base Filtering Engine (BFE)**
- **Windows Power Service** (sometimes labeled **Power**)

On Windows Server 2016 and 2019, Windows Defender is enabled by default. To use Falcon's Next-Gen Antivirus quarantine setting, you must disable Windows Defender. You can use this Powershell command to disable Defender:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

Network protocols

The Falcon sensor requires TLS 1.2 to communicate with the CrowdStrike cloud. Other protocols, including SSL or earlier versions of TLS, are not supported.

Additional services for hosts using proxies

- **WinHTTP AutoProxy**
- **DHCP Client**, if you use Web Proxy Automatic Discovery (WPAD) through DHCP

Local audit policy setting

To better capture logon-related events, the Falcon sensor for Windows requires the **Logon** local audit policy to have a setting of `Success and Failure`. If the actual policy setting does not match this setting, the sensor changes it to match. Often, this policy is managed by a group policy object, or GPO. If you use a GPO to manage the **Logon** policy, consider updating your GPO to match the required setting to minimize conflict between your GPO enforcement and the sensor enforcement.

To view your **Logon** local audit policy setting, use this `auditpol` command:

```
auditpol.exe /get /category:Logon/Logoff
```

Certificates

The Falcon sensor requires certain certificates. For more information, see
Verify that your host trusts CrowdStrike's certificate authority [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#of5bce8d].

Networking requirements

Internet access

Windows sensor version 6.22 and later

Hosts must connect to the CrowdStrike cloud on port 443 during initial installation. If your environment restricts internet access, allow traffic to CrowdStrike cloud IP addresses and FQDNs. For more info, see Cloud IP Addresses and FQDNs [/documentation/page/e87d1418/cloud-ip-addresses].

We strongly recommend ensuring hosts remain online after installation to download supplementary data.

Windows sensor version 6.21 and earlier

Hosts must remain connected to the CrowdStrike cloud throughout installation, which is generally 10 minutes. If your environment restricts internet access, allow traffic to CrowdStrike cloud IP addresses and FQDNs. For more info, see Cloud IP Addresses and FQDNs [/documentation/page/e87d1418/cloud-ip-addresses]. A host unable to reach and retain a connection to the cloud within 10 minutes will roll back the installation and then exit the installer.

If your host requires more time to connect, you can override this by using the `ProvWaitTime` parameter in the command line to increase the timeout to 1 hour.

```
<installer_filename> /install /norestart CID=<your CID> ProvWaitTime=3600000
```

In this example, replace `<installer_filename>` with the name of the install file you downloaded and `<CCID>` with the CCID from **Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads]**.

Allow additional network access from domain controllers

For customers with Falcon Identity Protection, the domain controllers require the following additional port communications:

- For Windows Defender Firewall and Falcon Firewall we suggest adding the following *allow* rules:
  - Outgoing traffic to *any* remote port from local TCP ports 3389, 88, 135, 389, 636, 3268, 3269
  - Outgoing traffic to *any* remote port from local UDP ports 88, 389, 3268
  - Outgoing traffic to *any* from RPC dynamic ports range (for example: 49152-65535)
  - Outgoing traffic to *any* remote port from CSFalconContainer
- For Guardicore firewall we suggest adding the following *allow* rules:
  - For Guardicore versions earlier than 5.42:
    - Outgoing traffic to *any* destination from *any* process
  - For Guardicore versions 5.42 and later:
    - Outgoing traffic to *any* destination from system
    - Outgoing traffic to *any* from CSFalconContainer

Any host-based firewall software running on domain controllers must have rules to allow the required traffic prior to enabling Falcon Identity Protection.

Note: Failure to allow required traffic from the domain controllers prior to enabling Falcon Identity Protection will impact authentication traffic — up to and including preventing authentication to the domain.

When installed on a domain controller, the sensor uses NetBIOS to resolve hostnames on your network. You should allow traffic on UDP port 137 between your domain controllers and all endpoints.

The sensor requires that network ports (TCP and UDP) in the range between 49000 and 49100 are available for use on domain controllers. The sensor uses these ports to redirect network traffic to itself for inspection, before forwarding it to its destination.

Note: The installer attempts to automatically open this port range if the domain controller uses Windows Firewall.

In order to support enforcement (block, MFA) using the Identity Protection policy for Remote desktop (RDP) to DC, Network Level Authentication (NLA) must be enabled on the domain controllers.

Avoid interference with certificate pinning

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Some network configurations, such as deep packet inspection, interfere with certificate validation.

Disable deep packet inspection (also called "HTTPS interception," or "TLS interception") or similar network configurations. Common sources of interference with certificate pinning include antivirus systems, firewalls, or proxies.

Allow TLS traffic

After agent installation, an agent opens a permanent TLS connection over port 443. The connection is kept open until the endpoint is turned off or the network connection is terminated.

Depending on your network environment, you might need to allow TLS traffic on port 443 between your network and our cloud's network addresses.

If your network only allows traffic by destination IP address instead of FQDN, allow TLS traffic on port 443 over the static IP addresses. For more info, see Cloud IP Addresses and FQDNs [/documentation/page/e87d1418/cloud-ip-addresses].

Cloud domains for US-1

```
ts01-b.cloudsink.net
lfodown01-b.cloudsink.net
lfoup01-b.cloudsink.net
https://falcon.crowdstrike.com
https://assets.falcon.crowdstrike.com
https://assets-public.falcon.crowdstrike.com
https://api.crowdstrike.com
https://firehose.crowdstrike.com
```

CrowdStrike cloud US-2 domains

```
ts01-gyr-maverick.cloudsink.net
lfodown01-gyr-maverick.cloudsink.net
lfoup01-gyr-maverick.cloudsink.net
https://falcon.us-2.crowdstrike.com
https://assets.falcon.us-2.crowdstrike.com
https://assets-public.falcon.us-2.crowdstrike.com
https://api.us-2.crowdstrike.com
https://firehose.us-2.crowdstrike.com
```

CrowdStrike cloud EU-1 domains

```
ts01-lanner-lion.cloudsink.net
lfodown01-lanner-lion.cloudsink.net
lfoup01-lanner-lion.cloudsink.net
https://falcon.eu-1.crowdstrike.com
https://assets.falcon.eu-1.crowdstrike.com
https://assets-public.falcon.eu-1.crowdstrike.com
https://api.eu-1.crowdstrike.com
https://firehose.eu-1.crowdstrike.com
```

CrowdStrike cloud US-GOV-1 domains

```
ts01-laggar-gcw.cloudsink.net
sensorproxy-laggar-g-524628337.us-gov-west-1.elb.amazonaws.com
lfodown01-laggar-gcw.cloudsink.net
ELB-Laggar-P-LFO-DOWNLOAD-1265997121.us-gov-west-1.elb.amazonaws.com
https://falcon.laggar.gcw.crowdstrike.com
laggar-falconui01-g-245478519.us-gov-west-1.elb.amazonaws.com
https://api.laggar.gcw.crowdstrike.com
https://firehose.laggar.gcw.crowdstrike.com
falconhose-laggar01-g-720386815.us-gov-west-1.elb.amazonaws.com
```

CrowdStrike cloud US-GOV-2 domains

```
ts01-us-gov-2.cloudsink.crowdstrike.mil
lfodown01-us-gov-2.cloudsink.crowdstrike.mil
https://falcon.us-gov-2.crowdstrike.mil
https://api.us-gov-2.crowdstrike.mil
https://firehose.us-gov-2.crowdstrike.mil
```

Standard installation

In most cases, you can install the Falcon sensor for Windows using either a manual GUI installation or an automated command-line installation.

To ensure that sensors function as expected, don't shut down or reboot the host while the sensor is being installed. Doing so can cause the host to repeatedly crash on boot or omit the uninstall option.

> Note: If this occurs, you'll need to boot in safe mode to fix the Windows registry.

For information about other installation considerations, see Advanced installation options [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#xaf55505].

After installation, the sensor runs silently and is invisible to the user.

Manual installation

If you have a small number of installs to do, manual installation might be your best option.

1. Use the Google Chrome browser to download the sensor installer from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].
2. Copy your customer ID checksum from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].
   If you're a trial user, skip this step.
3. Double-click the sensor installer.
4. Accept the license agreement and enter your customer ID checksum.
   If you're a trial user, skip this step.
5. If your OS prompts to allow the installation, click **Yes**.

Automatic installation

To automate silent installations on many devices, including installations using a deployment tool such as Windows System Center Configuration Manager (SCCM), complete these steps.

1. Use Google Chrome to download the sensor installer from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].
2. Copy your customer ID checksum (CCID) from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].
3. Run or configure your deployment tool to use this command, replacing `<installer_filename>` with the name of the install file you downloaded, and `<CCID>` with the CCID from step 2 :
   `<installer_filename> /install /quiet /norestart CID=<CCID>`

For information about these parameters and their functions, see Appendix A [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#e61915d1].

Post-installation steps

Verifying sensor installation

You can verify an installation by using the Falcon console or a command prompt on the host.

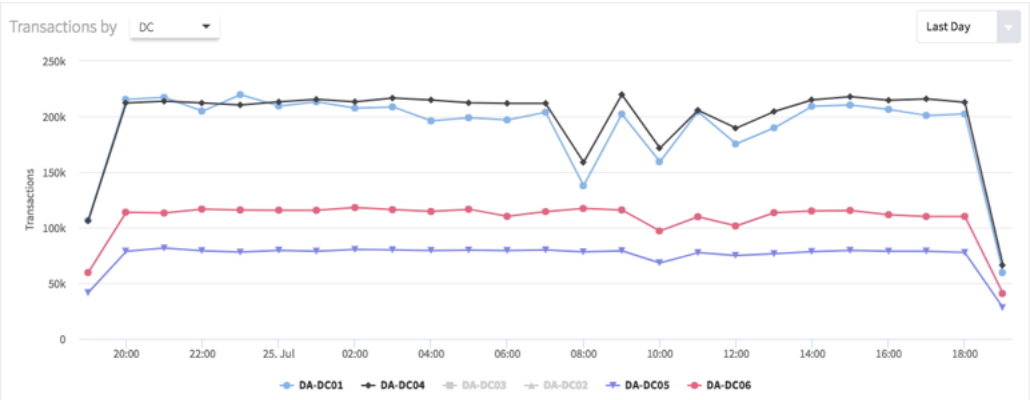
Falcon console

After the sensor is installed, the host connects to the Falcon console. You can confirm a sensor installation by reviewing your hosts.

To view a complete list of newly installed sensors, use the Sensor Report [/investigate/events/en-US/app/eam2/sensor_app] in the Falcon console.

To verify deployment of a sensor on a domain controller in the console:

1. In the Falcon console, go to Identity Protection > Configure > Domains [/identity-protection/administration/domains].
2. On the **Domains** tab, view the amount of authentication traffic being monitored for each domain controller in the **Transactions by DC** graph.



Any traffic flow in the graph represents a clear indication that the Falcon sensor for Windows is configured correctly to work with the domain controller. If there is no traffic flow, see
Allow additional network access from domain controllers [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#f9a109e3].

Host

To validate that the Falcon sensor for Windows is running on a host, run this command at a command prompt:

```
sc.exe query csagent
```

This output will appear 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
```

If your output is different, see Troubleshooting an Installation [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#dfc6324a].

Enabling Identity Protection traffic inspection

When installed onto a domain controller, the Falcon sensor for Windows automatically begins to capture identity-related data to populate the monitoring pages that Identity Protection provides, including Active Directory users and endpoints.

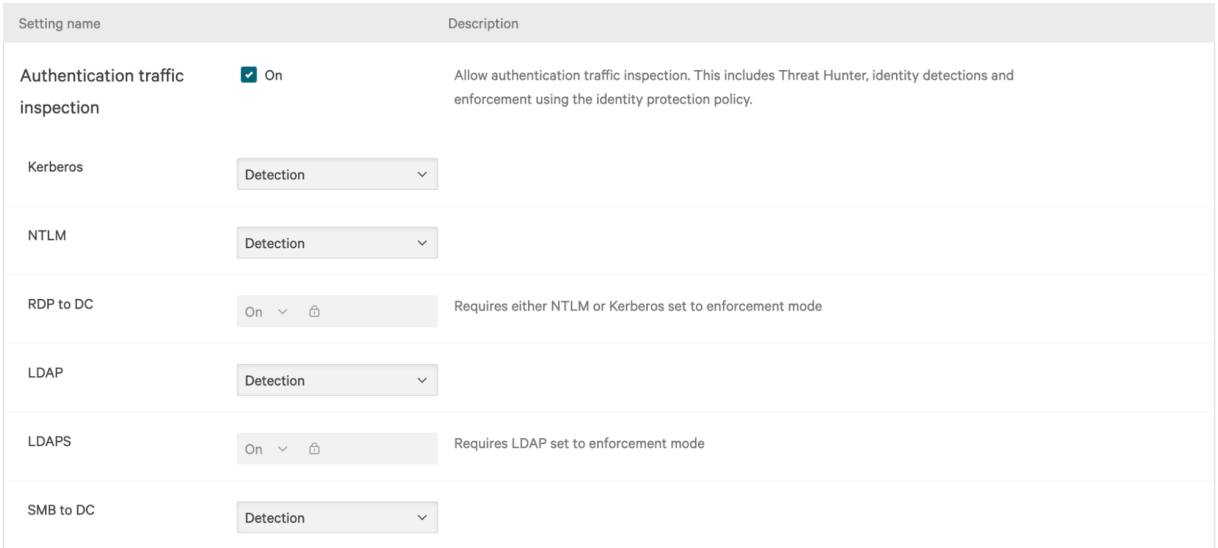
To use the full functionality of Identity Protection, you must enable the Falcon sensor to inspect authentication traffic on every domain controller.

Note: To avoid performance issues, ensure all domain controllers have a minimum of 2CPU and 8GB RAM before enabling Identity Protection traffic inspection.

Inspecting authentication traffic on domain controllers enables Identity Protection to populate Threat Hunter, create identity-based detections, and the enforcement of identity-based policy rules.

Follow these steps to enable inspection of authentication traffic on domain controllers:

1. In the Falcon Console, go to Identity Protection > Configure > Identity configuration policies [/policies/identity-protection] .
2. To edit an existing policy, click its **Name**, or to create a new policy, click **Create Policy**, provide a name and description, and then click **Create Policy**.
3. On the **Sensor Settings** tab, set **Authentication traffic inspection** to **On**.
4. For the available protocols on the **Sensor Settings** tab, choose the setting to match the required coverage level:
    - **Enforcement** allows for full operation with all features, including policy, detections, and Threat Hunter. Before allowing traffic to reach the DC, it is checked against the Identity Protection policy rules to see if it should be blocked or held until the end user approves via MFA.
    - **Detection** enables partial operation and includes only detections and Threat Hunter. In this mode, Identity Protection policy rules will not be enforced even when configured. Performance is significantly faster than **Enforcement** mode, as the traffic is not delayed for policy evaluation.
    - **Off** turns off traffic inspection so there is no visibility, detection, or enforcement.
      Note: When the **RDP to DC** or **LDAPS** dropdown selection appears dimmed, the protocol is actually set to **Off**, even though **On** might be displayed in the dropdown.



5. In the **Assigned host groups** tab, assign host groups that contain your domain controllers.

For information on creating host groups, see Managing host groups [/documentation/page/f8a0f751/host-and-host-group-management#l0e9728c].

6. To finish setup and apply the policy, click **Enable policy**.

Advanced installation options

Enabling uninstall protection for the Falcon sensor

Protect sensors from unauthorized uninstallation by enabling **Uninstall and maintenance protection**. This requires a maintenance token when unloading, uninstalling, repairing, or manually upgrading the sensor. For more info, read our Sensor Update Policies [/documentation/page/d2d629cf/sensor-update-policies] guide.

In sensor version 6.11.12502 and later, you can also stop users or processes from performing actions that tamper with key sensor components on the endpoint, such as deleting or renaming sensor files. The **Sensor tampering protection** setting is enabled by default for new installations.

Sensor upgrades with uninstall protection enabled and cloud updates disabled

Use this upgrade path if you don't use cloud updates and want to automate silent sensor upgrades on uninstall-protected devices. You might manage installations using a deployment tool like Windows System Center Configuration Manager (SCCM).

1. Use Google Chrome to download the sensor installer from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].
2. In the sensor update policy you want to update, turn on **Bulk maintenance mode**. Make sure the **Sensor version updates off** build version is selected and **Uninstall and maintenance protection** is turned on.
3. Retrieve the bulk maintenance token to include in the deployment package. This token doesn't change, so you don't need to modify your deployment package each time you enter bulk maintenance mode.
4. Run or configure your deployment tool to use this command, replacing`<installer_filename>` with the name of the install file you downloaded:
   `<installer_filename> MAINTENANCE_TOKEN=<bulk maintenance token> /install /quiet /norestart`
5. For increased security, turn off bulk maintenance mode after completing your upgrades. This restores the per-sensor maintenance token and disables the bulk maintenance token.

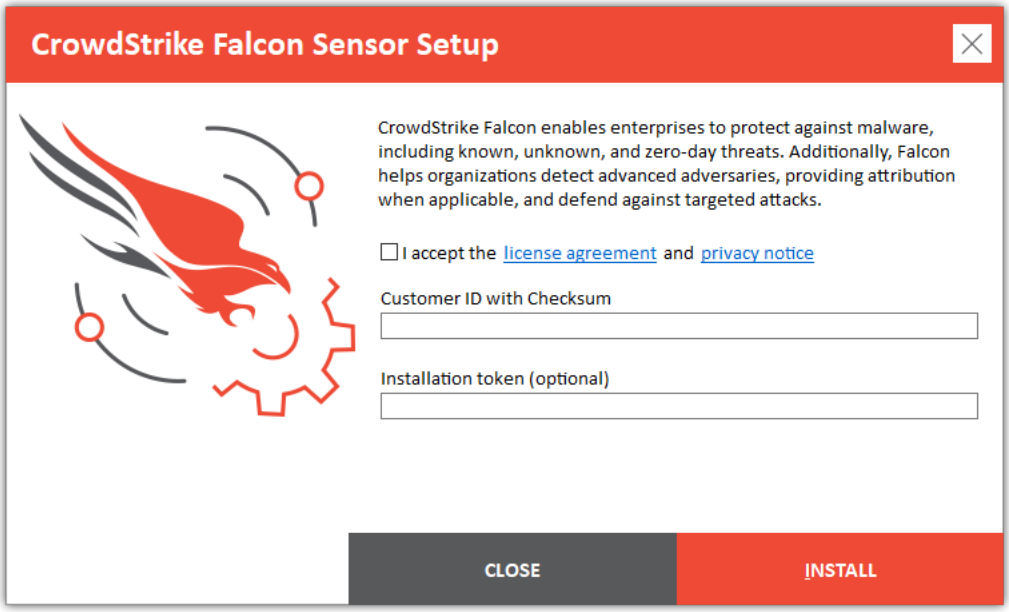
Installing to a CID that requires installation tokens

Installation tokens [/documentation/page/f8a0f751/host-and-host-group-management#r5bd2729] prevent unauthorized hosts from being accidentally or maliciously added to your customer ID (CID). Installation tokens are an optional security measure for your CID. To use installation tokens, you create one or more tokens in the Falcon console or through the API, enable the token requirement, and then provide the tokens to sensors at installation time.

When you install a sensor after enabling **Require tokens**, the installation command must include an additional parameter and an active token, such as:

```
<installer_filename> /install /quiet /norestart CID=<CCID> ProvToken=ABCD1234
```

This argument is supported with any other Windows installer argument, as well as the installation wizard:



Assigning sensor grouping tags during installation

Sensor grouping tags are optional, user-defined identifiers you can use to group and filter hosts.

You can assign one or more tags to a host using the `GROUPING_TAGS` parameter during installation. Assigning tags at this point makes them immediately available when the sensor first connects to the CrowdStrike cloud.

> Note: This section is about sensor grouping tags, which you can use with sensor images and templates. For more information about these tags and how they compare to Falcon grouping tags, see Using grouping tags [/documentation/page/f8a0f751/host-and-host-group-management#eed98281].

Tags are case-sensitive.

Tags can include these characters	Tags can't include these characters
Letters (a-z,A-Z)	Spaces ()
Numbers (0-9)	Commas (,)
Hyphens (-)	
Underscores (_)	
Forward slashes (/)	

To use multiple tags, separate tags with commas. The combined length of all tags for a host, including comma separators, cannot exceed 256 characters.

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

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

Replace `<installer_filename>` with the name of the install file you downloaded, and `<CCID>` with the CCID from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].

Viewing a host's sensor grouping tags

Use Host Management [/hosts/hosts] to search for the host. The **Grouping Tags** information for the host includes Falcon grouping tags and sensor grouping tags.

Adding or changing tags after installation

After sensor installation, the way you add or remove tags depends on your sensor version.

- For version 6.42 and later, see Managing sensor grouping tags [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#m451d2e5].

- For version 6.40 and earlier, see
  How to add or modify Falcon sensor for Windows tags locally [https://supportportal.crowdstrike.com/s/article/ka16T000000wx5tQAA].

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.

```
<installer_filename> /install /norestart CID=<CCID> ProvNoWait=1
```

Replacing `<installer_filename>` with the name of the install file you downloaded, and `<CCID>` with the CCID from
Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].

Installing in a virtual environment

You have 2 options when you install the sensor on a VM. Use the correct installation method to ensure that each host receives a unique agent ID (AID). If the same AID is inadvertently assigned to more than one VM, events and detections from your various VMs would appear to be from a single host.

Does your VM meet all of the following requirements:

- It is non-persistent (the VM reverts to the original setup after a user logs out)
- It is domain-joined
- It uses a fully qualified domain name (FQDN)

If your VM meets all of the requirements, follow the steps in
Installing the Falcon sensor in a VDI environment [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#g821cff2].

For VMs that don't meet all of those requirements, follow the steps in
Installing the Falcon sensor on a virtual machine template [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#p8997ec6].

Installing the Falcon sensor in a VDI environment

When you install the sensor in a Virtual Desktop Infrastructure (VDI) environment, the sensor runs from a shared, read-only OS image. The CrowdStrike cloud assigns a unique 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. Put your image template system into read/write mode.
2. Install the Falcon sensor using the `VDI=1` parameter.
   - `<installer_filename> /install CID=<CCID> VDI=1`
   - Replacing `<installer_filename>` with the name of the install file you downloaded, and `<CCID>` with the CCID from
     Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].
   - After the installation is complete, the sensor communicates with the cloud and updates to the sensor version defined in the host's assigned
     Sensor Update [/configuration/sensor-update/policies] policy. You can check the update status by finding the host in
     Host Management [/hosts/hosts].
3. After the sensor is on the proper version, switch your template system back to read-only mode and save the image.

Installing the Falcon sensor on a virtual machine template

Use a virtual machine template when your virtual hosts are built off of an image, or a template is being cloned.

> Do not use a standard installation on a virtual machine. If you perform a standard install on a template, all VMs created from that template will be assigned the same Agent ID (AID). If the same AID is inadvertently assigned to more than one VM, events and detections from your various VMs would appear to be from a single host.

Installing the sensor on a VM template

1. Complete all steps required to generalize the VM template, such as sysprep or installing Windows and software updates.

2. Install the Falcon sensor using the NO_START=1 parameter:

```
WindowsSensor.exe /install CID=<YOUR CID> NO_START=1
```

   - After installation, the sensor does not attempt to communicate with the CrowdStrike cloud.
   - Don't reboot the host, or it will attempt to communicate with the CrowdStrike cloud on reboot.

3. Confirm that the installation is complete.
4. Shut down the VM and convert it to a template image.

Troubleshooting VM templates

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

After the sensor has been installed using the NO_START=1 parameter, if you inadvertently restart the VM template before you convert the VM to a template image, hosts created with that template will all share an AID. If the same AID is inadvertently assigned to more than one VM, events and detections from your various VMs would appear to be from a single host. You can resolve this by removing the following registry keys:

- 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

> Note: Having sensor tampering protection enabled will prevent you from removing these registry keys. To work around this, disable sensor tampering protection, remove the registry keys, and then re-enable sensor tampering protection.

Modifying a VM template

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

1. Prepare your VM template.
2. If sensor tampering protection is enabled, disable sensor tampering protection:
   a. On the Prevention Policies [/configuration/prevention/policies] page, locate the sensor's policy and click **Edit Policy**.
   b. In the **Sensor Capabilities** area, disable **Sensor Tampering Protection**.
   c. Click **Save**.
3. Delete these registry values:
   - 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
4. If needed, re-enable sensor tampering protection in the sensor's prevention policy and click **Save**. The AID is removed from the VM template.
5. Shut down the VM.
6. Convert the VM to a template image using your virtualization software.

Installing the Falcon sensor with Pay-As-You-Go billing

See Falcon for Cloud Workloads [/documentation/page/d5d5ebd6/falcon-for-cloud-workloads-pay-as-you-go] for full information about Pay-As-You-Go billing.

To create a new master image template with no agent ID and Pay-As-You-Go billing enabled:

1. Prepare your master image instance, including any software configuration or updates.
2. Download the Falcon sensor installer from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads] or by using sensor download APIs [/documentation/page/c1f0f0b8/sensor-download-apis].
3. Install the Falcon sensor using the case-sensitive BILLINGTYPE=Metered and NO_START=1 parameters:

```
WindowsSensor.exe /install /quiet /norestart CID=<your CID> BILLINGTYPE=Metered NO_START=1
```

   - After installation, the sensor does not attempt to communicate with the CrowdStrike cloud.
   - Don't reboot the host, or it will attempt to communicate with the CrowdStrike cloud on reboot.

4. Confirm that the installation is complete.
5. Configure your cloud workloads to create ephemeral images based on this master image.
6. According to your organization's update policies, plan to regularly re-create this master image using an up-to-date Falcon sensor installer.

> To automate this more effectively, consider using sensor download APIs [/documentation/page/c1f0f0b8/sensor-download-apis] to automatically retrieve new versions of the Falcon sensor. Then, use your organization's existing automation tools to install the newer version on your master image without an agent ID.

To change an existing Falcon sensor to use Pay-As-You-Go billing, you must uninstall the sensor and reinstall it with the `BILLINGTYPE=Metered` parameter.

Uninstalling the Falcon sensor for Windows

To uninstall a sensor, you can use the Control Panel or the command line.

If uninstall protection is enabled, you must complete additional steps. See
Uninstall protection on sensor version 5.10.9105 and later [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#j46f2a25].

Uninstalling using the Control Panel

1. Open the Windows Control Panel running it as administrator.
2. Click **Uninstall a Program**.
3. Choose **CrowdStrike Windows Sensor** and uninstall it, providing the maintenance token through the installer if necessary.

Uninstalling using the command line

1. Download `CSUninstallTool` from Tool Downloads [/support/tool-downloads]
2. Open a command prompt with administrative privileges and run this command:
   ```
   CsUninstallTool.exe /quiet
   ```

Uninstall protection on sensor version 5.10.9105 and later

Case: Sensor is online

Move the host into a sensor update policy with **Uninstall and maintenance protection** disabled, then uninstall using one of the two uninstall methods.

Case: Sensor is offline and "Uninstall and maintenance protection" is enabled

Open the host's summary panel in Hosts > Host Management [/hosts/hosts] page and click **Reveal Maintenance Token** to get the single-use maintenance token needed to uninstall the sensor. Use this token in this command line script to uninstall the sensor:

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

Case: Sensor is offline and bulk maintenance mode is enabled

Go to the host's sensor update policy and click **Reveal Token** to get the bulk maintenance token needed to uninstall the sensor. Use the token in this command line script to uninstall the sensor:

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

Validating the uninstallation

When the sensor has been uninstalled:

- The sensor does not appear in your programs list

- The directory `C:\Windows\System32\drivers\CrowdStrike` is not present
- The registry key `HKLM\System\Crowdstrike` does not appear in the registry

Troubleshooting an installation

Installation process

The sensor goes through several phases: the "installing" phase, the "provisioning" phase, and ongoing operation.

Installing phase

1. The sensor installer uses standard Windows installer mechanisms to set up the Falcon sensor's files and registry keys.
2. If you're using installation tokens, the CrowdStrike cloud checks the installer's token.
3. The sensor contacts the CrowdStrike cloud, which assigns an agent ID for the host.

If any part of the installing phase fails, the installer attempts to roll back the installation and exit cleanly.

> Don't shut down or reboot a host during installation. If a host is shut down or rebooted during installation, the installer can't exit cleanly, and the host might be left in an unusable or unknown state.

Provisioning phase

The sensor downloads supplementary data called "channel files." Channel files are additional sensor instructions that provide updated settings for policies, allowlists and blocklists, detection exclusions, support for new OS patches, and more.

Provisioning might take minutes or much longer, depending on your network configuration and channel file throttling settings [/documentation/page/d2d629cf/sensor-update-policies#zd8423e5]. When a channel file is downloaded and more channel files remain, the sensor tries for 20 minutes to download them.

Make sure your hosts stay online through the provisioning phase so they can download all channel files. The sensor operates normally during provisioning. Even if a sensor can't yet download all channel files, it operates on its previous known configuration.

When a host has downloaded all available channel files, the CrowdStrike cloud notes that the host is fully provisioned. You can check the provisioning status of your hosts on the Sensor Health dashboard [/investigate/events/en-US/app/eam2/sensor_health].

Ongoing operation

The sensor periodically checks for new channel files from the CrowdStrike cloud during normal operations. New channel files are available when you make changes in Falcon, such as prevention policies or host group assignments. CrowdStrike also sends channel files to hosts to improve sensor compatibility and performance (after Microsoft's regular Patch Tuesday releases, for example).

Sensors automatically check for new channel files at regular, staggered intervals to minimize simultaneous traffic on your network. However, you can choose to throttle channel file downloading [/documentation/page/d2d629cf/sensor-update-policies#zd8423e5] if channel files affect your network's performance.

Installer errors

Windows sensor version 6.22 and later

Error message	Exit code (logs, command-line installation)	Recommended solution
Falcon was unable to communicate with the CrowdStrike cloud. Check your network configuration and try again.	Decimal: 1232 Hex: 0x4d0	Use the troubleshooting steps below: Host Can't Connect to the CrowdStrike Cloud [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#v1db7d62]
Falcon was unable to communicate with the CrowdStrike cloud. Check your	Decimal: 1244	Check the CID you provided to the installer.

Error message	Exit code (logs, command-line installation)	Recommended solution
installation token and try again.	Hex: 0x4dc	If you're using installation tokens [/documentation/page/f8a0f751/host-and-host-group-management#r5bd2729], confirm that your installation token was entered correctly and is active in Falcon.

Installation fails

If the sensor installation fails, confirm that the host meets our system requirements [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#vd9352c6], including required Windows services. If required services are not installed or running, you might see an error message: **A required Windows service is disabled, stopped, or missing. Please see the installation log for details.**

See Logs [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#da4aa575] for more information.

Troubleshooting general sensor issues

Verifying 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.exe 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
```

Issue: Sensor installed but doesn't run

If the sensor doesn't run, confirm that the host meets our system requirements [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#vd9352c6], including required Windows services. If required services are not installed or running, you might see an error message in the sensor's logs: **A required Windows service is disabled, stopped, or missing. Please see the installation log for details.**

The sensor might require these services in certain environments:

- **LMHosts***
- **Windows Base Filtering Engine (BFE)**
- **DHCP Client**, if you use Web Proxy Automatic Discovery (WPAD) through DHCP
- **DNS Client**

The sensor might require the **WinHTTP AutoProxy** service in certain environments using proxies.

* - LMHosts might be disabled on your host if the **TCP/IP NetBIOS Helper** service is disabled.

See Logs [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#da4aa575] for more information.

Verifying the sensor is connected to the CrowdStrike cloud

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

Falcon console

Use the Sensor Report [/investigate/events/en-US/app/eam2/sensor_app] to search for the host.

Host

Run this command from a command line with administrative privileges:

```
netstat.exe -f
```

If the sensor can connect to the CrowdStrike cloud, the command output is similar to the following output:

```
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`. A full list of CrowdStrike cloud IPs is available. For more info, see Cloud IP Addresses and FQDNs [/documentation/page/e87d1418/cloud-ip-addresses].

> **Note:** If your host uses a proxy, the **Foreign Address** shows the proxy address, such as `proxy.example.com`, instead of the CrowdStrike cloud address.

Issue: Host can't connect to the CrowdStrike cloud

If your host can't connect to the CrowdStrike Cloud, check these network configuration items:

1. Verify that your host can connect to the internet.
2. If your host uses a proxy, verify your proxy configuration.
3. If your host uses an endpoint firewall, configure it to permit traffic to and from the Falcon sensor.
4. Verify that your host's **LMHost** service is enabled. LMHosts might be disabled if you've disabled the **TCP/IP NetBIOS Helper** on your host.
5. Verify that your host trusts CrowdStrike's certificate authority.

Endpoint firewalls

If you're using an endpoint firewall on your host, it must be configured to allow access to the CrowdStrike domains. Customers have reported that these products require additional configuration when used with the Falcon sensor:

- Ad-Aware Pro Security
- Avast Internet Security
- AVG Internet Security
- BITDEFENDER Total Security
- Bullguard Internet Security
- Chili Internet Security
- Dr. Web Security Space
- ESET NOD32 Smart Security
- MyInternetSecurity Preventon A/V + Firewall
- Trustport Internet Security
- UnThreat Internet Security
- VIPRE Internet Security

- ZoneAlarm Internet Security Suite

Allow the installer more provisioning time with the ProvNoWait parameter

Hosts must remain connected to the CrowdStrike cloud throughout installation. A host unable to reach the cloud within 20 minutes (10 minutes, in Falcon sensor version 6.21 and earlier) will not successfully install the sensor.

If your host requires more time to connect, you can override this by using the `ProvNoWait` parameter in the command line. This also provides additional time to perform additional troubleshooting measures.

```
<installer_filename> /install /quiet /norestart CID=<CCID> ProvNoWait=1
```

Replacing `<installer_filename>`with the name of the install file you downloaded, and `<CCID>` with the CCID from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].

Verify that your host trusts CrowdStrike's certificate authority

The Falcon sensor requires your host to have the **DigiCertHighAssuranceEVRootCA** and **DigiCertAssuredIDRootCA** certs in your Trusted Root CA store.

> Note: Starting with Falcon sensor for Windows version 6.18, the sensor installer checks whether these certs are present. If they are not present, the installer checks the **Turn off Automatic Root Certificate Update** Windows setting. If the setting is disabled, the installer continues and attempts to build the required certificate chain that would cause Windows to install the missing root CA. If sensor installs are failing and **Turn off Automatic Root Certificate Update** is enabled, set **Turn off Automatic Root Certificate Update** to disabled to have the sensor installer address missing certs.

Check whether the certs are already present. Download and import them if needed.

1. Follow the Microsoft documentation for the Microsoft Management Console (MMC) to enable the Certificates snap-in per How to: View certificates with the MMC snap-in [https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-view-certificates-with-the-mmc-snap-in]
   .
2. In the MMC, click **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
3. Verify that both of the required certs are present.
   If either certificate is not present, complete these steps.
   a. Download the missing certificate from Digicert:
   DigiCertHighAssuranceEVRootCA [https://www.digicert.com/CACerts/DigiCertHighAssuranceEVRootCA.crt] and
   DigiCertAssuredIDRootCA [https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt].
   b. Import a certificate by right-clicking **Certificates** and then **All Tasks > Import**. Choose your local machine, click **Next**, and browse to the downloaded cert. Complete the import.
   c. Import the other certificate if needed.
   d. Confirm that both certs are now present in **Trusted Root Certification Authorities > Certificates**.

Issue: Host can't establish proxy connection

The following use cases are currently supported:

- Manually specifying a global proxy URL through Group Policy or manual input
- Manually specifying a PAC file through Group Policy or manual input
- WPAD configured to auto-detect a PAC file through DHCP or DNS

Connection happens in two phases: (1) proxy discovery and (2) connection. The order is as follows:

1. Try to use the CS Sensor application-specific proxy which is specified through the installer (`APP_PROXYNAME=<Proxy server hostname or IP address>` and `APP_PROXYPORT=<Proxy server port>`)
2. Use proxy settings from the Local Area Network (LAN) Settings under **"Proxy Servers" (also called IE Proxy Settings)**, if available.
3. Use PAC file URL provided through the installer (`PACURL=<PAC file URL>`).
4. Use PAC file URLs from Local Area Network **(LAN) Settings > "Use automatic configuration script"**. Use if you want to use Windows AutoProxy with a PAC File.

5. Use persisted proxy settings (of any type). Any time the sensor successfully connects to a proxy, the sensor will cache the host name and port.
6. Use Windows Proxy Auto-Discovery (WPAD).
7. Direct TCP/IP connection.
8. DnsLookup Fallback. This tries to use config-driven DNS lookup table to connect.

When `PROXYDISABLE=1` is passed to the installer, the installer will skip 1-6 and proceed directly to 7 (Direct Connection) and then proceed to step 8 above.

CrowdStrike does not support Proxy Authentication. If connection to the CrowdStrike cloud through the specified proxy server fails, or no proxy server is specified, the sensor will attempt to connect directly. For more assistance on proxy configurations, contact your proxy vendor or CrowdStrike Support [https://supportportal.crowdstrike.com/].

This puts the proxy settings into values of `CsProxyHostname` (as REG_SZ) and `CsProxyPort` (as REG_DWORD) at the registry key located here:

```
HKEY_LOCAL_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default
```

Providing troubleshooting info to Support

Providing `CSWinDiag` output to our Support [https://supportportal.crowdstrike.com/] team can help troubleshoot sensor issues.

To run a `CSWinDiag` collection, complete these steps.

Note: If you have access to Real Time Response (RTR), you can use the `cswindiag` RTR command instead of downloading the tool. For more info, see Real Time Response and Network Containment [/documentation/page/b8c1738c/real-time-response-and-network-containment].

1. Download the tool.
   In the Falcon console, go to Support and resources > Resources and tools > Tool downloads [/support/tool-downloads] and download the latest `CSWinDiag` available.
2. Unzip the file to a folder in `%PROGRAMFILES%`.
3. Go to that folder and run the tool.
   Options to run the tool:
   - Double-click the `cswindiag.exe` file.
     If prompted, enter local administrator credentials.
   - Using the command prompt, type `cswindiag` and press **Enter**.
4. If prompted to allow the program to make changes to the computer, click **Yes**.
   The program does not install or make any system changes. It only collects host information.
5. Wait about 4 minutes for the collection to complete.
   When done, the tool indicates the location of the collection file, such as `\Windows\Temp\CSWinDiag-<hostname>-mRRfqs8F.zip`.

For more info, including how to securely send the collection file to Support, see Using CSWinDiag for Falcon Sensor for Windows Diagnostics [https://supportportal.crowdstrike.com/s/article/Using-CSWinDiag-for-Falcon-Sensor-for-Windows-Diagnostics]

.

Logs

You can export your logs in their native directory structure and format (such as `.evtx` for sensor operations logs).

Log type	Enabled by default?	Location	Log size	Log retention
Sensor operations	No	In Windows Event Viewer under Windows Log > System. Look for the label CSAgent.	Based on OS or group policy settings	Based on OS or group policy settings

Log type	Enabled by default?	Location	Log size	Log retention
Sensor installation (installation, uninstallation, upgrades, or downgrades)	Yes	If initiated by a user: %LOCALAPPDATA%\Temp If initiated by the CrowdStrike cloud: %SYSTEMROOT%\Temp	Based on OS or group policy settings	Based on OS or group policy settings

Sensor operational logs

The sensor's operational logs are disabled by default. To enable or disable logging on a host, you must update specific Windows registry entries.

Enable logging

1. Create a file with the extension `.reg`, such as `myfile.reg`.
2. Copy and paste the following into your file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default]
"AFLAGS"=hex:03,00,00,00
```

3. Open a command prompt and run the following command to enable logging:
   `regedit.exe myfile.reg`

Disable logging

1. Create a file with the extension `.reg`, such as `myfile.reg`.
2. Copy and paste the following into your file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default]
"AFLAGS"=hex:00,00,00,00
```

3. Open a command prompt and run the following command to disable logging:
   `regedit.exe myfile.reg`

Normal log contents

A normal startup log includes messages similar to these:

- The sensor is starting.
- The sensor is locating and initializing the config.
- The sensor is checking communications (whether to use proxy or not and on which host/port).
- The sensor is connecting and setting up SSL.
- The sensor connected and is sending its first message to CrowdStrike cloud.
- The sensor received a response from cloud. All startup tasks are complete.

Appendix A: Installer parameters

This is a complete index of all parameters that the Falcon sensor installer accepts.

> Enter the parameters exactly as shown.

- All installer parameters are case-sensitive.

- Some parameters require a leading slash, and some require no leading slash.

Installation parameters

Parameter	Description
`CID=0123456789ABCDEFGHIJKLMNOPQRSTUV-WX`	Your Customer ID Checksum [/hosts/sensor-downloads/], which is required when installing.
`/install`	Installs the sensor (default).
`/passive`	Shows a minimal UI with no prompts.
`/quiet`	Shows no UI and no prompts.
`/norestart`	Prevents the host from restarting at the end of the sensor installation.
`GROUPING_TAGS=`	Assigns user-selected identifiers you can use to group and filter hosts.
`ProvToken=`	Optional security measure to prevent unauthorized hosts from being accidentally or maliciously added to your customer ID (CID).
`BILLINGTYPE=`	Sets the sensor to use standard billing or Pay-As-You-Go billing [/documentation/page/d5d5ebd6/falcon-for-cloud-workloads-pay-as-you-go]. • BILLINGTYPE=Default: standard billing per sensor • BILLINGTYPE=Metered: Pay-As-You-Go billing

Sensor startup parameters

Parameter	Description
`NO_START=1`	Prevents the sensor from starting up after installation. The next time the host boots, the sensor will start and be assigned a new agent ID (AID). This parameter is usually used when preparing master images for cloning.
`VDI=1`	Enable virtual desktop infrastructure mode.

Proxy parameters

Parameter	Description	Usage
`APP_PROXYNAME=<Proxy FQDN or IP> APP_PROXYPORT=<Proxy server port>`	Configure a proxy connection using both a proxy address (by FQDN or IP) and a proxy port.	Cannot be used with the PACURL parameter.
`PACURL=<PAC file URL>`	Configure a proxy connection using a PAC file.	Cannot be used with the `APP_PROXYNAME` and `APP_PROXYPORT`parameters.
`PROXYDISABLE=1`	By default, the Falcon sensor for Windows automatically attempts to use any available proxy connections when it connects to the CrowdStrike cloud. This parameter forces the sensor to skip those attempts and ignore any proxy configuration, including Windows Proxy Auto Detection.	

Parameter	Description	Usage
`ProvNoWait=1`	The sensor does not abort installation if it can't connect to the CrowdStrike cloud within 20 minutes (10 minutes, in Falcon sensor version 6.21 and earlier). (By default, if the host can't contact our cloud, it will retry the connection for 20 minutes. After that, the host will automatically uninstall its sensor.)	Use this parameter when upgrading to version 3.5 or later if you use IE proxy detection for Falcon, because proxy data will not be available until another user logs into the host.
`ProvWaitTime=3600000`	The sensor waits for 1 hour to connect to the CrowdStrike cloud when installing (the default is 20 minutes).	Use this to install the sensor on hosts that require more time to connect to the CrowdStrike cloud. In Windows sensor version 6.22 and later, this parameter is usually only used by request from our Support team. It's typically not needed because the sensor can complete installation even if all channel files can't be downloaded.

Troubleshooting parameters

Troubleshooting parameters	Description
`/?`	Show help information for the installer.
`/repair`	Repair the sensor installation.
`/log log.txt`	Change the log directory [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#da4aa575] to the specified file.
`MAINTENANCE_TOKEN`	An optional single-use security token used when uninstalling or installing sensors.

Appendix B: CsSensorSettings commands

`CsSensorSettings` is a command-line tool that's automatically installed with Windows sensor version 6.42 and later. Use this tool after sensor installation to modify the sensor grouping tags on a host.

To run `CsSensorSettings` commands, use a Windows `cmd` shell as an administrator.

`CsSensorSettings` is located in: `C:\Program Files\CrowdStrike`

Managing sensor grouping tags

Sensor grouping tags are optional, user-defined identifiers you can use to group and filter hosts. If you didn't assign sensor grouping tags at installation, or if you want to change the tags after installation, add or remove tags using `CsSensorSettings` for sensors version 6.42 and later.

For info on allowed characters in sensor grouping tags, see
Assigning sensor grouping tags during installation [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#w685001d].

To modify sensor grouping tags for sensors version 6.40 and earlier, see
How to add or modify Falcon sensor for Windows tags locally [https://supportportal.crowdstrike.com/s/article/ka16T000000wx5tQAA].

Command	Description
`set`	Modify the assigned sensor grouping tags.This command replaces the existing set of assigned tags. For example, even if you're adding only one tag, you must specify the new tag in addition to all existing sensor grouping tags on the host. You can view current tags in the host summary panel in Host setup and management > Manage endpoints > Host management [/hosts/hosts] . Example: `CsSensorSettings set --grouping-tags "tag1,tag2,tag3"`

Command	Description
`clear`	Remove all assigned sensor grouping tags. Example: `CsSensorSettings clear --grouping-tags`

Note: If hosts belong to a sensor update policy that has **Uninstall and maintenance protection** enabled, entering the `set` or `clear` commands prompts you to enter a valid maintenance token. This prevents unauthorized users from changing tags assigned to the host, which could place them in a less restrictive policy. For more info about maintenance protection, including how to reveal maintenance tokens for use with these commands, see Sensor Update Policies - Managing sensor maintenance and uninstallation [/documentation/page/d2d629cf/sensor-update-policies#o075803c].

General CsSensorSettings commands

Command	Description
`version`	Displays the `CsSensorSettings` version. Example: `CsSensorSettings --version`
`help`	Displays the help for `CsSensorSettings`. Example: `CsSensorSettings --help`

Reduced functionality mode: Windows hosts

What is OSFM?

OS Feature Manager (OSFM) monitors changes in the Windows kernel so the sensor can adapt accordingly. This includes allowing the sensor to certify new kernels without updating the sensor version, and placing the sensor in reduced functionality mode (RFM) if the current host kernel is uncertified.

What is RFM?

Reduced functionality mode (RFM) is a safe mode for the sensor that prevents compatibility issues if the host's kernel is uncertified. RFM is most common during Windows updates. Without full kernel support, your sensor could experience severe compatibility issues, potentially resulting in system crashes and other performance issues.

> **Note:** Hosts on other platforms can also enter RFM, but RFM for the Falcon sensor behaves differently on each platform. See Reduced functionality mode: Mac hosts [/documentation/page/e261a9b7/falcon-sensor-for-mac-deployment#pb0ee694] and Reduced functionality mode: Linux hosts [/documentation/page/ea6bf997/falcon-sensor-for-linux-modes#r1167a77].

What happens to domain controllers (DCs) in RFM?

For customers with Falcon Identity Protection, the following protection measures help to avoid disturbance of the normal activities of a domain controller:

- The sensor monitors different counters and measurements and can modify its behavior to keep the footprint low.
- If the sensor measurements exceed a set of thresholds, the sensor might disable the Identity Protection policy rules or disable traffic inspection to reduce disturbance.

  > **Note:** If the sensor disables an Identity Protection policy rule or traffic inspection, a system notification is created.

- The sensor returns to normal functionality once the measurements stay below a second set of thresholds.

To view the **Status** and **Status details** of each DC, go to **Identity protection > Configure > Domain controller hosts [/identity-protection/hosts]**.

What happens to sensors in RFM?

When a Windows sensor enters RFM, it still actively monitors your system, reports events, and trigger detections, but at a reduced capacity. Sensors in RFM temporarily unhook from some kernel elements [https://supportportal.crowdstrike.com/s/article/OS-Feature-Manager-and-Reduced-Functionality-Mode#RFM]. Without these elements, some detection patterns and a small number of preventions will not be triggered.

What causes RFM?

The most likely reason your Windows hosts are in RFM is due to Microsoft updates. Not all Windows updates alter the kernel, but when they do, there is a brief delay while we certify the kernel to work with the sensor.

How can I tell if my system is in RFM?

From the Host management page

On the **Host management** page (**Host setup and management** > **Manage endpoints** > **Host management**), you can filter your list of hosts to show devices currently in RFM. You can also see the RFM status of a specific host from the host's summary panel [/documentation/page/f8a0f751/host-and-host-group-management] **.** If a host is in RFM or has an unknown RFM status, a warning banner alerts you at the top of the panel.

From the Executive Summary dashboard

The Executive Summary [/dashboards/dashboard/en-US/app/eam2/dashboards__executive_summary] dashboard (**Dashboards > Executive Summary)** lists a count of sensors in RFM by operating system. You can click an RFM widget in the dashboard to open more details in Investigate.

From Investigate

In Investigate [/investigate/], you can see `SensorHeartBeat` events generated by the sensor that contain the value `SensorStateBitMap_decimal`. Use this value to see if the sensor is in RFM.

- If `SensorStateBitMap_decimal` is 2, the sensor is in RFM.
- If `SensorStateBitMap_decimal` is 0, the sensor isn't in RFM.

You can use a query to report a list of hosts in RFM.

> **Note:** The Raptor release, which includes the CrowdStrike Query Language (CQL), is being rolled out in waves. When your wave begins, you'll gain access to CQL. Until then, use the legacy query language syntax. For more info, see Raptor Release Resource Center [/documentation/page/de2919a2/raptor-release-resource-center].

- CrowdStrike Query Language syntax
  Go to **Investigate > Search > Advanced event search** and run this query:

  ```
  #event_simpleName=SensorHeartbeat event_platform=Win SensorStateBitMap=2 ConfigIDBuild>=17206
  | groupBy([aid], function=(selectFromMax(field="@timestamp", include=[@timestamp, ComputerName, aid,
  ConfigBuild])))
  | rename([[ComputerName, Hostname], [aid, "Sensor ID"], [FileName, "OSFM Filename"], [ConfigBuild,
  "Agent Build"]])
  ```

  With CQL, you search for `SensorStateBitMap` instead of `SensorStateBitMap_decimal`.

- Legacy query language syntax
  Go to **Investigate > Events** and run this query:

  ```
  event_simpleName=SensorHeartbeat event_platform=Win SensorStateBitMap_decimal=2
  ConfigIDBuild_decimal>=5906 earliest=-1d latest=now| table timestamp ComputerName aid
  ConfigIDBuild_decimal| dedup aid| sort -timestamp| eval timestamp=timestamp/1000| convert
  ctime(timestamp)| rename timestamp as "Timestamp (UTC)", ComputerName as "Hostname", aid as "Sensor
  ID", ConfigIDBuild_decimal as "Agent Build"
  ```

You can modify the query reporting period, however we recommend searching no more than 2 days back. If a host was previously in RFM but has since been fixed, you will still see the events that predate its repair.

From the API

RFM status information is also available through the CrowdStrike Host management API [/documentation/page/c0b16f1b/host-and-host-group-management-apis].

Returning a sensor in RFM to full functionality

If you apply Windows updates that alter the Windows kernel before CrowdStrike certifies the kernel, your sensor receives an OSFM certification file from the CrowdStrike cloud when the file becomes available. That file allows your sensor to resume full functionality.

Subscribe to the Release Notes mailing list in the CrowdStrike Customer Center [https://supportportal.crowdstrike.com/s/topic-subscription] to get emails when new patches are certified.

Verify that your sensors have the current certification in one of these ways:

- Use a query to verify your sensors have the current OSFM certification file. Replace `OSFM-*.bin` with the current certification file provided by the email.

  > **Note:** The Raptor release, which includes the CrowdStrike Query Language (CQL), is being rolled out in waves. When your wave begins, you'll gain access to CQL. Until then, use the legacy query language syntax. For more info, see Raptor Release Resource Center [/documentation/page/de2919a2/raptor-release-resource-center].

  - CrowdStrike Query Language syntax

    Go to **Investigate > Search > Advanced event search** and run this query:

    ```
    #event_simpleName=LFODownloadConfirmation CompletionEventId=Event_OsfmDownloadCompleteV1
    FileName=Osfm-*.bin
    | groupBy([aid], function=(selectFromMax(field="@timestamp", include=[@timestamp, ComputerName,
    aid, FileName, ConfigBuild])))
    | rename([[ComputerName, Hostname], [aid, "Sensor ID"], [FileName, "OSFM Filename"],
    [ConfigBuild, "Agent Build"]])
    ```

  - Legacy query language syntax

    Go to **Investigate > Events** and run this query:

    ```
    event_simpleName=LFODownloadConfirmation CompletionEventId=Event_OsfmDownloadCompleteV1
    FileName=Osfm-*.bin earliest=-1d latest=now
    | table timestamp ComputerName aid FileName ConfigBuild
    | dedup aid
    | sort -timestamp
    | eval timestamp=timestamp/1000
    | convert ctime(timestamp)
    | rename timestamp as "Timestamp (UTC)", ComputerName as "Hostname", aid as "Sensor ID",
    FileName as "OSFM Filename", ConfigBuild as "Agent Build"
    ```

- If you'd prefer to verify the file version on your host, OSFM certification files are located in the CrowdStrike directory:

  - `%SYSTEMROOT%\system32\drivers\CrowdStrike\`

If your hosts are on an unsupported Windows build, upgrade them to a supported build [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#nf425a87] to resume full functionality.

Need additional support?

For additional troubleshooting information or to open a support case, visit the CrowdStrike Customer Center [https://supportportal.crowdstrike.com/].

Falcon Icon for Windows [/documentation/page/cd135e5a/falcon-icon-for-windows]