

Sensor Deployment and Maintenance

06/08/2026

Copyright © CrowdStrike

1. Falcon Sensor for Windows Deployment

1.1. Introduction

1.2. System requirements

1.2.1. Supported operating systems

1.2.1.1. Supported 64-bit server OSes

1.2.1.2. Supported desktop OSes

1.2.1.3. Unsupported features on ARM64-based hosts

1.2.1.4. Unsupported Windows versions

1.2.2. Services

1.2.2.1. Network protocols

1.2.2.2. Additional services for hosts using proxies

1.2.2.3. Local audit policy setting

1.2.3. Certificates

1.2.4. Supported sensor languages

1.3. Networking requirements

1.3.1. Internet access

1.3.2. Allow additional network access from domain controllers

1.3.3. Validate certificates for MFA

1.3.4. Avoid interference with certificate pinning

1.3.5. Allow TLS traffic

1.4. Best practices for sensor deployment

1.5. Standard installation

1.5.1. Manual installation

1.5.2. Automatic installation

1.6. Post-installation steps

1.6.1. Verifying sensor installation

1.6.1.1. Falcon console

1.6.1.2. Host

1.6.2. Enabling Identity Protection configuration policies

1.6.2.1. Enabling Identity Protection Active Directory auditing

1.6.2.2. Enabling Identity Protection traffic inspection

1.7. Advanced installation options

1.7.1. Enabling uninstall protection for the Falcon sensor

1.7.1.1. Sensor upgrades with uninstall protection enabled and cloud updates disabled

1.7.2. Enable visibility for WSL 2

1.7.2.1. Requirements

1.7.2.2. WSL 2 workflow overview

1.7.2.3. Step 1: Install the Falcon sensor for Windows on your Windows host

1.7.2.4. Step 2: Enable the prevention policy setting

1.7.2.5. Step 3: Restart WSL 2 and deploy the plug-in

1.7.2.6. Architecture

1.7.2.7. Limitations

1.7.3. Installing to a CID that requires installation tokens

1.7.4. Assigning sensor grouping tags during installation

1.7.4.1. Viewing a host's sensor grouping tags

1.7.4.2. Adding or changing tags after installation

1.7.5. Installing the sensor with IE proxy detection

1.7.6. Specifying the cloud where an endpoint's CID resides

1.7.7. Installing in a virtual environment

1.7.7.1. Installing the Falcon sensor in a non-persistent VDI environment

1.7.7.2. Installing the Falcon sensor on a virtual machine template

1.7.7.2.1. Installing the sensor on a VM template

1.7.7.2.2. Troubleshooting VM templates

1.7.7.2.3. Modifying a VM template

1.7.7.3. Installing the Falcon Sensor on linked or instant clones

1.8. Uninstall the Falcon sensor for Windows

1.8.1. Uninstall using the Control Panel

1.8.2. Uninstall using the command line

1.8.3. Validating the uninstallation

1.9. Troubleshooting an installation

1.9.1. Installation process

1.9.1.1. Installing phase

1.9.1.2. Provisioning phase

1.9.1.3. Ongoing operation

1.9.2. Installer errors

1.9.3. Installation fails

1.10. Troubleshooting general sensor issues

1.10.1. Verifying that the sensor is running

1.10.2. Issue: Sensor installed but doesn't run

1.10.3. Verifying the sensor is connected to the CrowdStrike cloud

1.10.3.1. Falcon console

1.10.3.2. Host

1.10.4. Issue: Host can't connect to the CrowdStrike cloud

1.10.4.1. Endpoint firewalls

1.10.4.2. Allow the installer more provisioning time with the ProvNoWait parameter

1.10.4.3. Verify that your host trusts CrowdStrike's certificate authority

1.10.5. Issue: Host can't establish proxy connection

1.11. Providing troubleshooting info to Support

1.12. Logs

1.12.1. Sensor operational logs

1.12.1.1. Enable logging

1.12.1.2. Disable logging

1.12.2. Normal log contents

1.13. Installer parameters

1.13.1. Installation parameters

1.13.2. Sensor startup parameters

1.13.3. Proxy parameters

1.13.4. Troubleshooting parameters

1.14. CsSensorSettings commands

1.14.1. Managing sensor grouping tags

1.14.2. Managing Real Time Response (RTR)

1.14.3. General CsSensorSettings commands

1.15. Reduced functionality mode: Windows hosts

1.15.1. What is OSFM?

1.15.2. What is RFM?

1.15.2.1. What happens to domain controllers (DCs) in RFM?

1.15.2.2. What happens to sensors in RFM?

1.15.2.3. What causes RFM?

1.15.2.4. How can I tell if my system is in RFM?

1.15.2.5. Returning a sensor in RFM to full functionality

1.15.2.6. Need additional support?

1.16. Sensor safe mode: Windows hosts

1.16.1. What is sensor safe mode?

1.16.2. What happens to sensors in safe mode?

1.16.3. What causes safe mode?

1.16.4. How can I tell if my system is in sensor safe mode?

1.16.5. Returning a sensor in safe mode to full functionality

1.16.6. Need additional support?

Falcon Sensor for Windows Deployment

Install, uninstall, and troubleshoot issues with the Falcon sensor for Windows.

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 and later.

Supported 64-bit server OSes

64-bit Windows Server OSes	Version	Build	LTSC Release?	Minimum Sensor Version	Falcon EOS Date
Server Core 2025	24H2	26100	Yes	7.22.19405	April 8, 2035
Server 2025	24H2	26100	Yes	7.19.18909	April 8, 2035
Server 2022 Annual Channel (AC) release	23H2	25398	—	7.21.19205	April 22, 2026
Server 2022	21H2	20348	Yes	All supported sensor versions	April 13, 2032
Server Core 2022	21H2	20348	Yes	All supported sensor versions	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 12, 2028
Server Core 2016	1607	14393	Yes	All supported sensor versions	July 12, 2028
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 through 7.16 (last supported version)	December 31, 2027

For hosts running the Server 2008 R2 SP1 operating system, CrowdStrike will use commercially reasonable efforts to continue offering machine learning updates and critical bug fixes through the end of support (EOS) date shown in the table. Due to limitations in the operating system and/or given the prior expiration of support from Microsoft, it might not be possible to provide these updates and bug fixes. In that situation, the only recourse would be to upgrade affected hosts to a supported Windows operating system.

Supported desktop OSes

Windows Desktop OSes	Version	Codename	Marketing Name	Build	LTSC Release?	64-bit Enterprise Support?	64-bit IoT Enterprise Support?	32-bit Support?	ARM
Windows 11	25H2	—	2025 Update	26200	No	Yes	No	—	Yes
Windows 11	24H2	Hudson Valley	2024 Update	26100	Yes	Yes	Yes	—	Yes

Windows Desktop OSes	Version	Codename	Marketing Name	Build	LTSC Release?	64-bit Enterprise Support?	64-bit IoT Enterprise Support?	32-bit Support?	ARM
Windows 11	23H2	Sun Valley 3	2023 Update	22631	—	Yes	—	—	Yes
Windows 11	22H2	Sun Valley 2	2022 Update	22621	—	Yes	—	—	Yes
Windows 10	22H2	22H2	2022 Update	19045	—	Yes	Yes	Yes	Yes
Windows 10	21H2	21H2	November 2021 Update	19044	Yes	Yes	Yes	Yes	Yes
Windows 10	1809	Redstone 5 ("RS5")	October 2018 Update	17763	Yes	Yes	Yes	Yes	—
Windows 10	1607	Redstone 1 ("RS1")	Anniversary Update	14393	Yes	Yes	—	—	—
Windows 10	1507	Threshold 1	N/A	10240	Yes	Yes	—	—	—
Windows 7 SP1	—	—	—	7601	—	Yes	—	Yes	—
Windows 7 Embedded POS Ready	—	—	—	7601	—	Yes	—	Yes	—

For hosts running the Windows 7 SP1 or Windows 7 Embedded POS Ready operating systems, CrowdStrike will use commercially reasonable efforts to continue offering machine learning updates and critical bug fixes through the end of support (EOS) dates shown in the table. Due to limitations in the operating systems and/or given the prior expiration of support from Microsoft, it might not be possible to provide these updates and bug fixes. In that situation, the only recourse would be to upgrade affected hosts to a supported Windows operating system. For more info, see Tech Alert | Update Regarding Falcon Support for Windows 7 SP1, Windows 7 Embedded POS Ready, and Windows Server 2008 R2 SP1.

For Windows 10 32-bit operating systems, Additional User Mode Data (AUMD) and Script Control are not supported.

Windows ARM64-based hosts:

- Windows ARM64-based hosts require an ARMv8.1-compatible CPU. For Qualcomm-based hosts, Snapdragon 845 and later CPUs are supported.
- Some features and prevention policy settings aren't supported on Windows ARM64-based hosts. For more info, see Unsupported features on ARM64-based hosts.

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
- 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, and so on – unless specifically stated in a Release Note.
- Windows Storage Server 2019/2016, which are OEM versions for third-party storage solutions
- 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
- Windows 10 v20H2
- Windows 11 21H2
- All 32-bit versions of Windows 10 not in this list
- All versions of Windows 8.1
- All versions of Windows 8
- Container-based Windows OS solutions, including but not limited to Docker, are not 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. For US-GOV-1 and US-GOV-2 customers, see Windows 10 & 11 running in S mode

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)
- For Falcon sensor for Windows versions up to and including 7.27:

  Windows Power Service, sometimes labeled Power

On Windows Server 2016, 2019, and 2022, 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
```

If you prefer, you can uninstall Defender by using this Powershell command:

```
Uninstall-WindowsFeature -Name Windows-Defender
```

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. If these certificates are not present, you may see network requests on port 80 to locations other than the CrowdStrike cloud. These network requests result from the Falcon sensor installer attempting to create a certificate chain and download the missing certificates from Digicert.

For more information, see Verify that your host trusts CrowdStrike's certificate authority.

Supported sensor languages

For Falcon sensor text shown to users, such as sensor connection status, context menu, and notifications, the Falcon sensor provides localized text. To see localized text, set the language of the host's operating system to a supported language. For all other operating system languages, the Falcon sensor displays English text. Supported languages:

- English
- Chinese (Traditional)
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Spanish

Networking requirements

Internet access

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. You must allow the cloud that has the CID that the installer should connect to. For optimal discovery, allow all the IP addresses for the US-1, US-2, EU-1, US-GOV-1, and US-GOV-2 clouds. For more info, see Cloud IP Addresses and FQDNs.

The sensor can discover a CID's cloud, or you can specify the cloud as shown in Specifying the cloud where an endpoint's CID resides.

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

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, 139, 389, 445, 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.

Validate certificates for MFA

To ensure the certificates that Identity Protection multi-factor authentication uses to display the MFA prompt are not blocked by your firewall settings, click the following links:

- fe2.update.microsoft.com
- ocsp.digicert.com
- crl3.digicert.com
- crl4.digicert.com

If you receive an error message, update your firewall settings.

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.

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
lfoup01-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
lfoup01-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
```

Best practices for sensor deployment

The primary purpose of change control is to maintain stability in the production environment by thoroughly testing all changes in a pre-production (QA) setting.

To ensure successful testing, your pre-production test systems should accurately mirror their production counterparts.

Testing must verify application compatibility, performance, interoperability, and user permissions, among other factors.

In addition to typical user workstations, your test groups should include samples of your critical infrastructure, such as Domain Controllers, Exchange servers, critical database and application servers (including SQL and Web), encompassing both internal and customer-facing examples.

Most organizations already have a process for software distribution, which can be adapted as a working change control model. This model typically involves a time-phased, systematic deployment progression:

- Canary/QA Hosts: Initial deployment to a small group for early testing.
- Staging/Pre-Production Hosts: Deployment to a larger test group, which may be divided into sub-groups for staggered changes.
- Production Hosts: Final deployment to the live environment, which should also be broken into sub-groups for a phased rollout.

Whenever possible, deployment to production systems should occur during off-hours, strictly following the phased progression defined in your change control methodology.

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.

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. Download the sensor installer from Host setup and management > Deploy > Sensor downloads .

   The downloaded file has this name: `FalconSensor_Windows.exe`

2. Copy your customer ID checksum (CCID) from Host setup and management > Deploy > Sensor downloads .

   If you're a trial user, skip this step.

3. Copy the sensor installer to the endpoint and double-click the 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. Download the sensor installer from Host setup and management > Deploy > Sensor downloads .

   The downloaded file has this name: `FalconSensor_Windows.exe`

2. Copy your customer ID checksum (CCID) from Host setup and management > Deploy > 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, see Installer parameters.

Post-installation steps

Verifying sensor installation

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

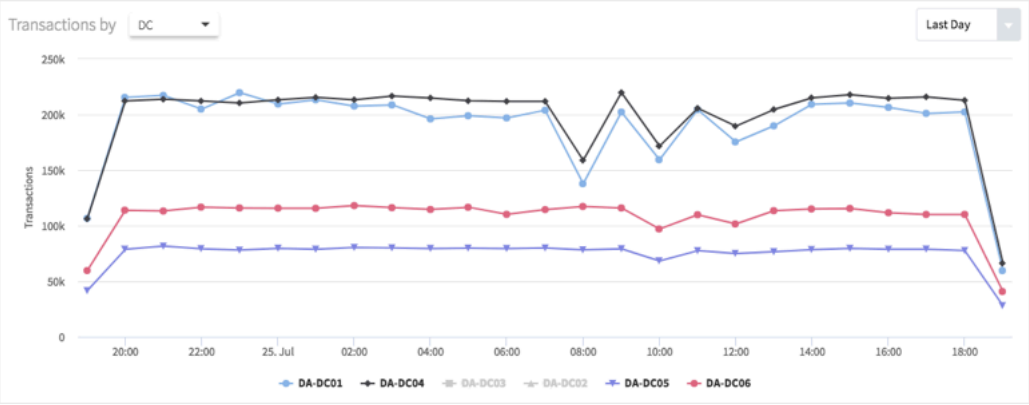
Falcon console

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 Dashboards and reports > Reports > Sensor report .

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

1. In the Falcon console, go to Identity Protection > Configure > 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.

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.

Enabling Identity Protection configuration policies

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

Important: Identity Protection will not work on a domain if it is disabled. To check the status of your domains, go to Identity protection > Configure > Domains.
Note: You can prevent Identity Protection from being automatically enabled on new domains using the Domain Management toggle. For more info, see Domain management.

Enabling Identity Protection Active Directory auditing

Required subscriptions:

- Identity Threat Detection or Identity Threat Protection
- Falcon XDR Insight

Sensor support: Supported on Falcon Windows sensor version 7.14 and later

To start tracking management actions performed within Active Directory, you must enable Active Directory auditing. This allows the sensor to gather additional events on the domain controller. Data is available in Investigate.
Note: To avoid performance issues, ensure all domain controllers have a minimum of 2 CPU and 8 GB RAM before enabling Active Directory auditing.
Follow these steps to enable Active Directory auditing on domain controllers:

1. In the Falcon Console, go to Identity Protection > Configure > Identity configuration policies.
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 Active Directory auditing to On.
4. Optional. If you want to collect group policy changes, set Group Policy Object (GPO) auditing to On.
   Note: When Group Policy Object (GPO) auditing is enabled, GPO events are displayed on Windows Event Viewer.
5. When you're done configuring the policy, click Save.
6. To finish setup and apply the policy, click Enable policy.

Enabling Identity Protection traffic inspection

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 2 CPU and 8 GB RAM before enabling Identity Protection traffic inspection.

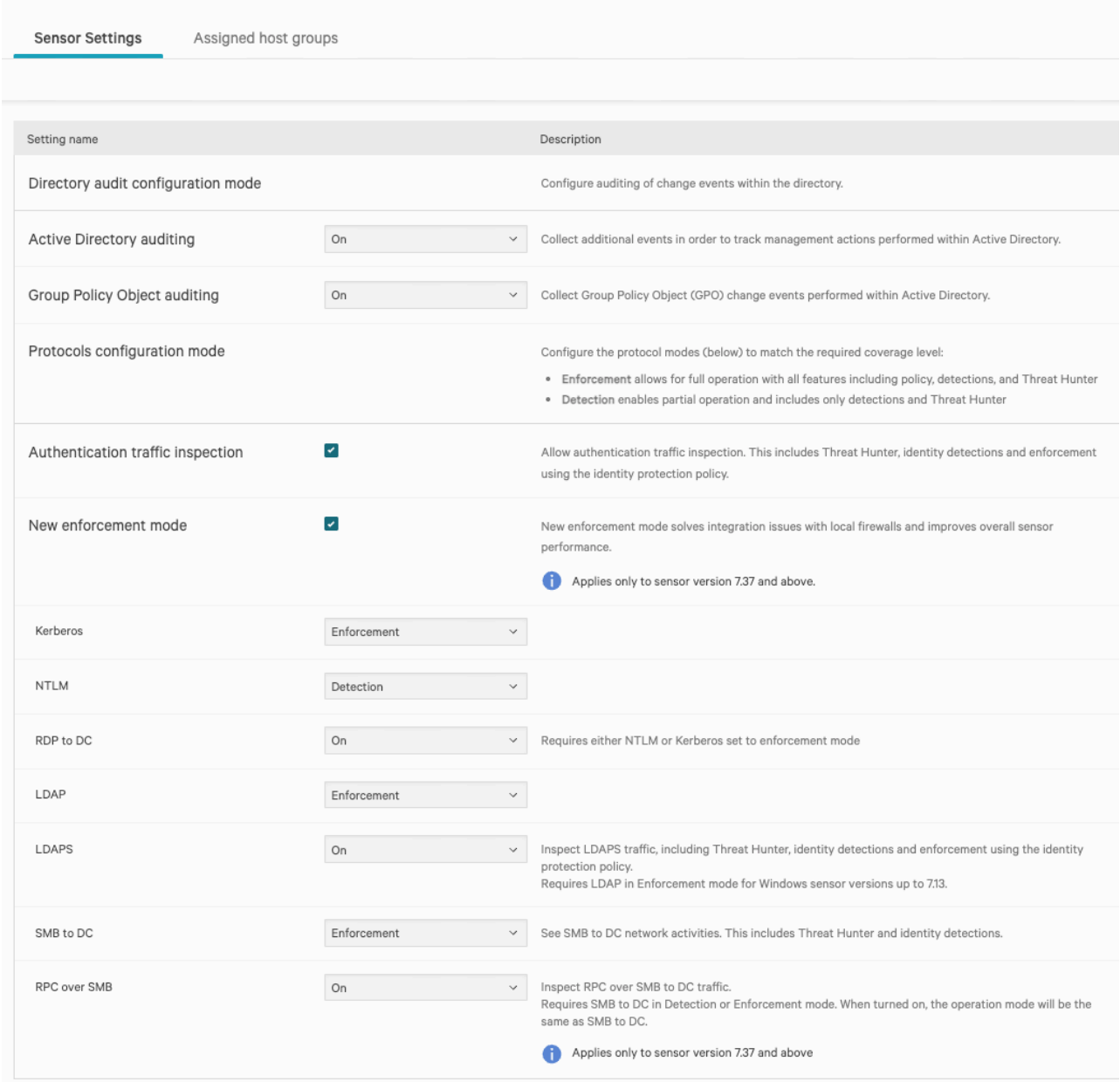
Inspecting authentication traffic on domain controllers enables Identity Protection to populate Threat Hunter, create identity-based detections, and the enforcement of identity-based policy rules.

Follow these steps to enable inspection of authentication traffic on domain controllers, and optionally enable AD auditing and new enforcement mode:

1. In the Falcon Console, go to Identity Protection > Configure > Identity configuration policies.
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. Optional. On the Sensor Settings tab, set Active Directory auditing to On.
   Tip: Active Directory auditing collects additional events in order to track management actions performed within Active Directory.
4. Optional. If you want to collect group policy changes, set Group Policy Object (GPO) auditing to On.
   Note: When Active Directory auditing and Group Policy Object (GPO) auditing are both enabled, AD and GPO events are still monitored even if Authentication traffic inspection is disabled.
5. Optional. On the Sensor Settings tab, set New enforcement mode to On.
   Note: New enforcement mode solves integration issues with local firewalls, improves overall sensor performance, and provides compatibility with VMware NSX driver.
6. On the Sensor Settings tab, set Authentication traffic inspection to On.
7. 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 using 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 RPC over SMB dropdown menu selection appears dimmed, the protocol is actually set to Off, even though On might be displayed in the dropdown.



8. On the Assigned host groups tab, assign host groups that contain your domain controllers.

   For information on creating host groups, see Managing host groups.
9. When you're done configuring the policy, click Save.
10. 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 Sensor Update Policies.

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 .
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.

Enable visibility for WSL 2

Deploy the Falcon sensor WSL plug-in library to gain high-level visibility into Windows Subsystem for Linux 2 (WSL 2) Linux instances.

Requirements

- Subscription: Falcon Prevent or Falcon Insight XDR
- Sensor: Falcon sensor for Windows 7.26 or later
- Default roles:
  - Can configure prevention policies:
    - Falcon Administrator
    - Prevention Policy Manager
- CrowdStrike clouds: Available in all clouds
- Additional system requirements: 64-bit x86-64 versions of Windows that support WSL 2 and are supported for use with the Falcon sensor for Windows. For more info, see Supported operating systems.

WSL 2 workflow overview

Follow these general steps to enable visibility for WSL 2:

1. Install the Falcon sensor on a Windows host.
2. Enable the prevention policy setting.
3. Restart WSL 2 and deploy the plug-in.

Step 1: Install the Falcon sensor for Windows on your Windows host

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

Step 2: Enable the prevention policy setting

Follow these steps to enable the WSL 2 visibility setting and apply it to your host groups:

1. In the Falcon console, go to Endpoint security > Configure > Prevention policies . Select Windows from the Platform dropdown menu.
2. Click the prevention policy Name that you want to enable WSL 2 visibility for.
3. Under Sensor visibility > Enhanced visibility, select WSL 2 visibility.
4. Click Save.

Step 3: Restart WSL 2 and deploy the plug-in

The WSL 2 plug-in doesn't deploy until the WSL 2 service is restarted.

To manually restart the WSL 2 service, in Powershell, run this command:

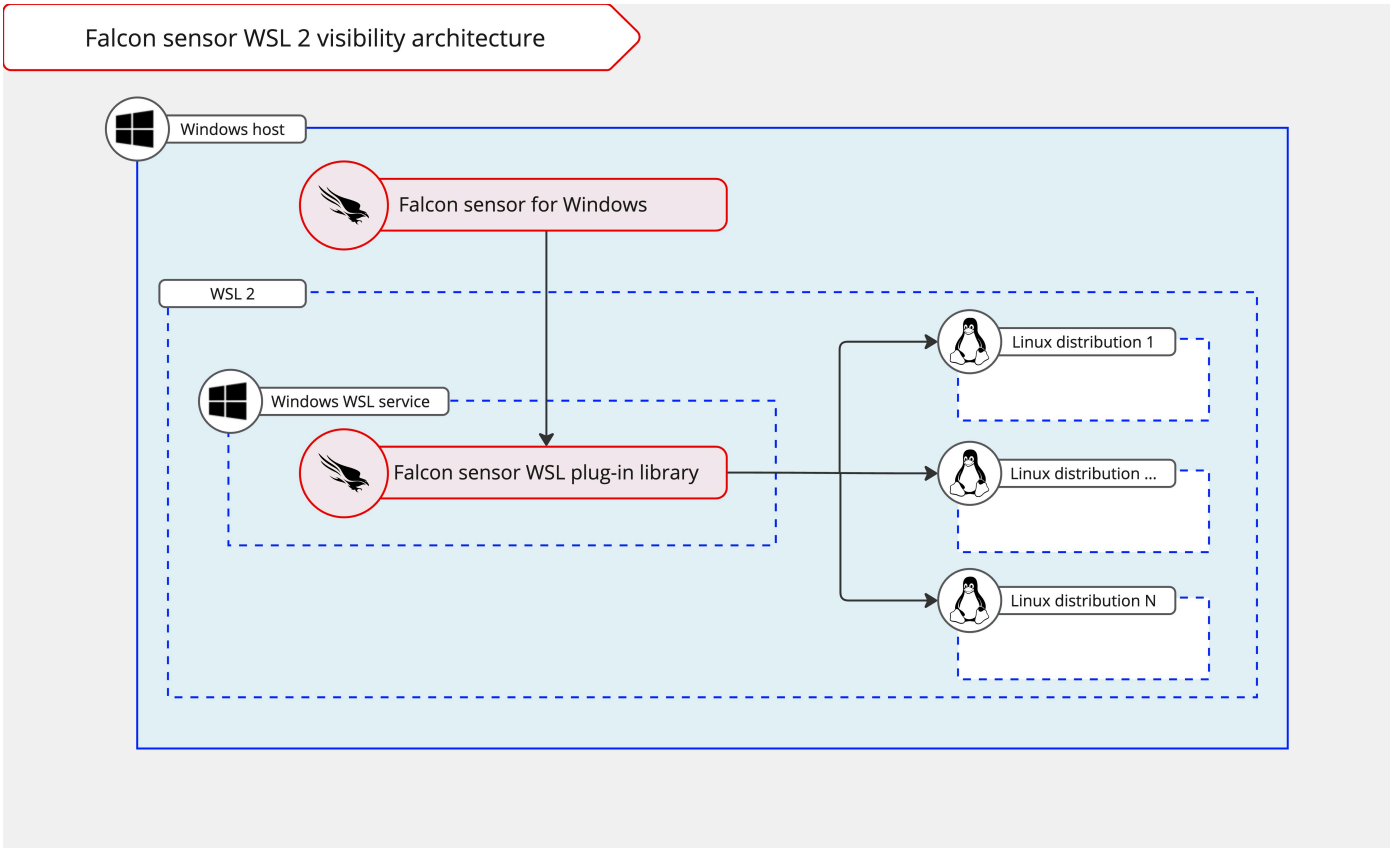
```
wsl --shutdown
```

For more information, see the Microsoft article Basic commands for WSL.

After the WSL 2 visibility policy setting is enabled and WSL 2 is restarted, the plug-in automatically loads.

Architecture

This architecture diagram gives you insight into how sensor support for WSL 2 visibility is implemented.



Visibility into WSL 2 includes monitoring of these events:

- `WSLVMStarted`
  - The Linux Virtual Machine Root Namespace starts
- `WSLDistributionStarted`
  - The Linux distribution starts
- `WSLDistributionStopping`
  - The Linux distribution is stopping
- `WSLVMStopping`
  - The Linux Virtual Machine Root Namespace is stopping
- `WSLDistributionRegistered`
  - A user registers a Linux distribution but hasn't started it yet
- `WSLDistributionUnregistered`
  - A user unregisters a Linux distribution

Limitations

- In some older versions of WSL 2, if you run `wsl --import-in-place` to register a Linux distribution, visibility of it being registered is blocked. However, there is still visibility of the distribution starting and stopping.

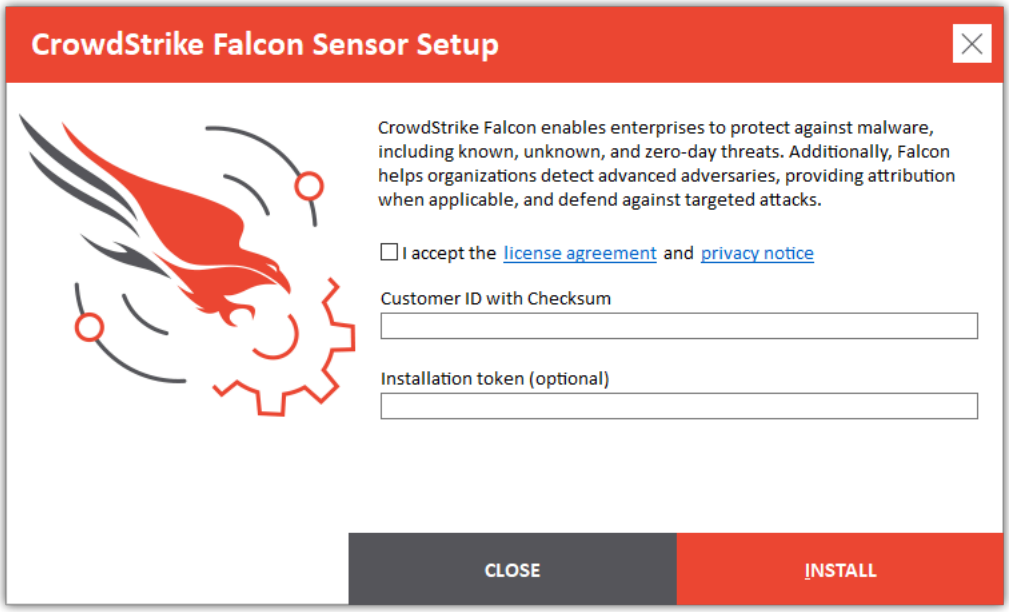
Installing to a CID that requires installation tokens

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. For more info, see Protecting your CID with installation tokens.

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.

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 (/)	
Periods (`.`)	
At symbol (@)	

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 .

Viewing a host's sensor grouping tags

Use Host Management 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.
- For version 6.40 and earlier, see How to add or modify Falcon sensor for Windows tags locally. For US-GOV-1 and US-GOV-2 customers, see How to add or modify Falcon sensor for Windows tags locally.

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 .

Specifying the cloud where an endpoint's CID resides

After installation, the sensor must connect to the CrowdStrike cloud where the endpoint's CID resides.

You can let the sensor discover the CID's cloud automatically, or you can specify the cloud where the CID resides.

Using the installer, you specify the CrowdStrike cloud to connect to by running this command, choosing exactly one value for `CLOUD_NAME`:

```
FalconSensor_Windows.exe CID=<CCID> CLOUD_NAME={"us-1"|"us-2"|"eu-1"|"us-gov-1"|"us-gov-2"}
```

Installing in a virtual environment

You have 3 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.

- Non-persistent: The VM does not retain any user profile settings, data, or configuration changes on a machine after a user logs off or reboots. It's rebuilt and brought back up to replicate the VDI image with every next user login or reboot. Follow the steps in Installing the Falcon sensor in a non-persistent VDI environment.
- Persistent: The VM retains user profile settings, data, or configuration changes after a user logs off or reboots. The VM is brought back up in the same state it was shut down. Follow the steps in Installing the Falcon sensor on a virtual machine template.
- Linked or instant clones: A linked clone is a copy of a VM that shares virtual disks with the parent VM in an ongoing manner. A snapshot of the VDI image is taken and then used to used to create the VDI parent for the VDI pooled machines. Follow the steps in Installing the Falcon Sensor on linked or instant clones.

Installing the Falcon sensor in a non-persistent 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.

The host machines must meet all of the following criteria:

- Are non-persistent
- Are domain-joined
- Uses an FQDN that does not change

In a VDI environment, we recommend that you install the desired sensor version on the master image and lock your sensor update policy to that version. When the VDI comes online it queries the cloud and attempts to upgrade to the latest sensor, but when the host reboots, it goes back to the version that's installed within your master image.

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

1. Put your image template system into read/write mode.
2. If the Falcon sensor is already installed on the template, follow the instructions to remove it in Uninstall the Falcon sensor for Windows.
3. 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 .
    - 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 policy. You can check the update status by finding the host in Host Management.
4. 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.

Note: 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 installing Windows and software updates.
2. If the Falcon sensor is already installed on the template, follow the instructions to remove it in Uninstall the Falcon sensor for Windows.
3. Install the Falcon sensor using the `NO_START=1` parameter and possibly the `ProvToken` parameter:

- `NO_START=1`

  With the `NO_START=1` parameter, the sensor does not attempt to communicate with the CrowdStrike cloud after installation. Don't reboot the host, or it will attempt to communicate with the CrowdStrike cloud.

- `ProvToken`

  If you enabled the Require tokens option at Host setup and management > Deploy > Installation tokens , the installation command must include the `ProvToken` parameter and an active token.

For example, the installation command with only the `NO_START` parameter:

```
<installer_filename> /install CID=<CCID> NO_START=1
```

For another example, the installation command with both the `NO_START` parameter and the `ProvToken` parameter:

```
<installer_filename> /install CID=<CCID> NO_START=1 ProvToken=ABCD1234
```

4. Confirm that the installation is complete.
5. Prepare the VM.

   To remove unique identifiers (SID), clean up logs, and reset activation so that the VM can be safely cloned or converted into a template:

   a. Run the `sysprep.exe` tool from `C:\Windows\System32\Sysprep`.

   b. For System Cleanup Action, select Enter System Out-of-Box Experience (OOBE).

   c. Select Generalize.

   d. For Shutdown Options, select Shutdown.

   e. Click OK.

6. Shut down the VM and convert it to a template image.

Troubleshooting VM templates

Here are some issues you might see.

- Events and detections from various VMs appear to be from a single host.

  When a VM created from this template first starts, 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.

- Installation token used unexpectedly

  If you installed the sensor using an Installation token and the VM template was rebooted, the provided Installation token would have been consumed to generate the AID upon connection to the CrowdStrike cloud.

To address these issues, uninstall the sensor from the template and then reinstall it. For more info, see Uninstall the Falcon sensor for Windows and Installing the Falcon sensor on a virtual machine template.

Modifying a VM template

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

1. Prepare your VM template.
2. Uninstall the sensor from the template. For more info, see Uninstall the Falcon sensor for Windows.
3. Reinstall the sensor. For more info, see Installing the Falcon sensor on a virtual machine template.
4. Prepare the VM.

   To remove unique identifiers (SID), clean up logs, and reset activation so that the VM can be safely cloned or converted into a template:

   a. Run the `sysprep.exe` tool from `C:\Windows\System32\Sysprep`.

   b. For System Cleanup Action, select Enter System Out-of-Box Experience (OOBE).

   c. Select Generalize.

   d. For Shutdown Options, select Shutdown.

   e. Click OK.

5. Shut down the VM.
6. Convert the VM to a template image using your virtualization software.

Installing the Falcon Sensor on linked or instant clones

There can be multiple parent VDI machines created from an image, and each parent can host multiple VDI non-persistent desktops, which are also referred to as the VDI pools. This is useful if you have multiple domains. A parent can be created for each domain, and have its own group of VDI pooled machines or desktops for each individual domain.

Important: When installing the sensor with linked or instant clones, install the sensor at the top-level image.

To install the Falcon sensor for Windows on your VDI top-level image:

1. Set your image template system into read/write mode.
2. Install the Falcon sensor on the VDI image using both the `VDI=1` and `NO_START=1` parameters:

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

   Note: After installation, the sensor does not attempt to communicate with the CrowdStrike cloud.
3. Shut down the image.
4. Take a snapshot of the image to use as a template.
5. Create the VDI template from the snapshot in step #2.
6. Create the VDI parent from the VDI template.
7. Create the VDI pools from the VDI parent.

Uninstall the Falcon sensor for Windows

Important: Uninstalling the sensor requires admin privileges.
Uninstall the Falcon sensor for Windows using one of these methods:

- Uninstall using the Control Panel
- Uninstall using the command line

Note: If the Uninstall and maintenance protection setting in your sensor update policy is enabled, you must retrieve a maintenance token to authorize uninstallation. For more info, see Managing sensor maintenance and uninstallation.

Uninstall using the Control Panel

Note: If Uninstall and maintenance protection is enabled, follow the steps in Making changes to a single host to retrieve the maintenance token for your host.

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.

   Tip: If Bulk maintenance mode is enabled for your hosts, follow the steps in Making changes to multiple hosts to retrieve the bulk maintenance token for your hosts.

Uninstall using the command line

Note: If Uninstall and maintenance protection is enabled, follow the steps in Making changes to a single host to retrieve the maintenance token for your host.

1. Download Falcon Windows Sensor, Uninstall Tool from Tool Downloads
2. Open a command prompt with administrative privileges and run this command:

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

   Tip: If Bulk maintenance mode is enabled for your hosts, follow the steps in Making changes to multiple hosts to retrieve the bulk maintenance token for your hosts.

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.

Note: 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 update throttling. 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.

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 if channel files affect your network's performance. These download settings are applied to all hosts. For more info, see Channel file update throttling.

You can also configure content update policies, which specify when to deploy CrowdStrike-initiated channel files after the files are made available. These policies are applied on a host-level basis. For more info, see Content Update Policies.

Installer errors

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
Falcon was unable to communicate with the CrowdStrike cloud. Check your installation token and try again.	Decimal: 1244 Hex: 0x4dc	Check the CID you provided to the installer. If you're using installation tokens, 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, 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 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, 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 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

To search for the host, use Dashboards and reports > Reports > Sensor report .

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.

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 does 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 .

Verify that your host trusts CrowdStrike's certificate authority

The Falcon sensor requires each host to have specific security certificates in its Trusted Root CA store. If the certificates are not present, the host may be unable to communicate with the CrowdStrike cloud and may display unexpected behavior.

Most sensors need only the certificate DigiCert TLS RSA4096 Root G5. Other security certificates can also be used in the event CrowdStrike discovers an operational or security issue with the main certificate.

- Main certificate: DigiCert TLS RSA4096 Root G5
- Fallback certificates:
  - DigiCert Global Root G2
  - GlobalSign Root R6
  - Sectigo Public Server Authentication Root R46
  - IdenTrust Commercial Root CA 1

Note: The sensor installer checks whether these certificates 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 certificates 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.
2. In the MMC, click Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.
3. Verify that the required certificates are present.

   If the certificates are not present, complete these steps.

   a. Download the missing certificates.

   b. For each certificate:

      i. Import a certificate by right-clicking Certificates and then All Tasks > Import.

      ii. Choose your local machine, click Next, and browse to the downloaded cert.

      iii. Complete the import.

   c. Confirm that the certs are now present in Trusted Root Certification Authorities > Certificates.

Issue: Host can't establish proxy connection

The following use cases are 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. For US-GOV-1 and US-GOV-2 customers, contact CrowdStrike Support.

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. For US-GOV-1 and US-GOV-2 customers, go to the Support 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.

1. Download the tool.

   In the Falcon console, go to Support and resources > Resources and tools > 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. For US-GOV-1 and US-GOV-2 customers, see 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
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.

Installer parameters

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

Note: 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, which is required when installing.
`CLOUD_NAME`	Specifies the cloud that the installer should connect to. Valid values: • `us-1` • `us-2` • `eu-1` • `us-gov-1` • `us-gov-2` Example: `CLOUD_NAME=us-1`
`/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).

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.	
`ProvNoWait=1`	The sensor does not abort installation if it can't connect to the CrowdStrike cloud within 20 minutes. By default, if the host can't contact our cloud, it retries the connection for 20 minutes. After that, the host automatically uninstalls 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 3600000 milliseconds, or 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. 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 to the specified file.
`MAINTENANCE_TOKEN`	An optional single-use security token used when uninstalling or installing sensors.

CsSensorSettings commands

`CsSensorSettings` is a command-line tool that's automatically installed with the Windows sensor. Use this tool after sensor installation to modify the sensor grouping tags or manage Real Time Response (RTR) 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 info about allowed characters in sensor grouping tags, see Assigning sensor grouping tags during installation.

Command	Description
`set --grouping-tags "<tag_list>"`	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.

Command	Description
	To view the current tags, go to Host setup and management > Manage endpoints > Host management. Example: `CsSensorSettings set --grouping-tags "tag1,tag2,tag3"`
`clear --grouping-tags`	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 requirement 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.

Managing Real Time Response (RTR)

Real Time Response (RTR) allows administrators to remotely connect to endpoints for investigation and remediation. For more info, see Real Time Response.

The `--no-rtr` option controls whether Real Time Response (RTR) functionality is enabled or disabled on the sensor. Disabling RTR prevents any remote interactive sessions from being established to the host.

Note: Entering the `set` or `clear` commands prompts you to enter a valid maintenance token. For more info about maintenance protection, including how to reveal maintenance tokens for use with these commands, see Managing sensor maintenance and uninstallation.

Command	Description
`set --no-rtr`	Disable RTR functionality on this sensor. With RTR disabled, remote interactive sessions cannot be established to this host. Disabling RTR is useful for sensitive systems where remote shell access should be prevented regardless of Falcon console policy. Example: `CsSensorSettings.exe set --no-rtr`
`clear --no-rtr`	Remove the NoRTR override, re-enabling RTR. After you clear the NoRTR override, RTR functionality is governed by the cloud-side policy, if any, that is configured in the Falcon console. Example: `CsSensorSettings.exe clear --no-rtr`

General CsSensorSettings commands

Command	Description
`version`	Display the `CsSensorSettings` version. Example: `CsSensorSettings –-version`
`help`	Display 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 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 and Reduced functionality mode: Linux hosts.

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 when 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.

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. For US-GOV-1 and US-GOV-2 customers, see some kernel elements. 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 . 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 Dashboards and reports > Reports > Executive summary dashboard 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 > Search > Advanced event search , you can see `SensorHeartBeat` events generated by the sensor that contain the value `SensorStateBitMap`. Use this value to see if the sensor is in RFM.

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

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

```
#event_simpleName=SensorHeartbeat event_platform=Win ConfigIDBuild>=17206
| bitfield:extractFlags(field="SensorStateBitMap", output=[[1, RFM]])
| RFM=true
| groupBy([aid], function=(selectFromMax(field="@timestamp", include=[@timestamp, ComputerName, aid, ConfigBuild])))
| rename([[ComputerName, Hostname], [aid, "Sensor ID"], [FileName, "OSFM Filename"], [ConfigBuild, "Agent Build"]])
```

From the API

RFM status information is also available through the CrowdStrike Host management API.

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.

Content update release notes are published to notify you when the OSFM certification file will be released. The content update category is Sensor Operations Content. See Content Updates. Additionally, you can subscribe to receive content update release notes notifications automatically. See Notifications for Content Update Release Notes.

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.

  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"]])
  ```

- 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 to resume full functionality. See Supported operating systems.

Need additional support?

For additional troubleshooting information or to open a support case, visit the CrowdStrike Customer Center.

Sensor safe mode: Windows hosts

What is sensor safe mode?

Starting with Falcon sensor for Windows 7.26, the sensor provides safe mode to detect when a system has entered into sensor-related boot loops or repeated system crashes and then take corrective action.

What happens to sensors in safe mode?

The sensor detects system crash loops and switches to safe mode.

This mode provides no functional capabilities other than ensuring that the sensor gracefully comes back online and connects to the CrowdStrike cloud. The sensor can then receive remediation updates from the CrowdStrike cloud to return to a healthy state.

What causes safe mode?

Repeated boots or system crashes can result in a sensor switching to safe mode.

How can I tell if my system is in sensor safe mode?

To check which hosts have sensors that are in safe mode, you have these options:

- Check the Host Management table

  Go to Host setup and management > Manage endpoints > Host management and check the table's Safe mode column. If the column is not present, add it by using Configure table columns .

  Possible values:

  - Yes
  - No
  - Unknown

    Indicates a supported platform with either a state that cannot be determined or a sensor with a version earlier than 7.26. Safe mode requires version 7.26 or later.
  - N/A

    Indicates an unsupported platform.

- Run a query

  Go to Investigate > Search > Advanced event search , set the time interval to Last 5m, and run this query:

```
#event_simpleName=SensorHeartbeat event_platform=Win ConfigIDBuild>=19813
| bitfield:extractFlags(field="SensorStateBitMap", output=[[3, Safemode]])
| Safemode=true
| groupBy([aid], function=(selectFromMax(field="@timestamp", include=[@timestamp, ComputerName, aid, ConfigBuild])))
| rename([[ComputerName, Hostname], [aid, "Sensor ID"], [ConfigBuild, "Agent Build"]])
```

Returning a sensor in safe mode to full functionality

A sensor in safe mode periodically attempts to return to a healthy state.

However, if you encounter a host in safe mode, visit the CrowdStrike Customer Center and open a support case.

Need additional support?

For additional troubleshooting information or to open a support case, visit the CrowdStrike Customer Center.