Falcon Sensor for Legacy Systems Deployment

Last updated: May 23, 2025

Overview

Falcon sensor for legacy systems provides anti-malware capabilities that leverage cloud-based machine learning to secure vulnerable legacy Windows endpoints found in your environment.

System requirements

Review specifications required to successfully install and run the Falcon sensor on legacy Windows systems.

Subscriptions

Deploying Falcon for Legacy Systems requires specific product subscriptions.

- Falcon for Legacy Systems and one or more of these subscriptions:
  - Falcon Insight XDR
  - Falcon Prevent

Supported operating systems

Verify which legacy Windows operating systems are compatible with the Falcon sensor before beginning your installation.

Only these operating systems are supported for use with the Falcon sensor for legacy systems. Any attempts to install the sensor on unsupported operating systems will fail.

This table provides info about requirements for the supported legacy Windows operating systems.

Windows OSes	OS Architecture	Service Pack	Knowledge Base	Notes
Windows XP	32-bit	Service Pack 3	SHA-2 code sign support is not required.	The WMI service is required for XP 32-bit only, and the legacy sensor service will start the WMI service if it is not already running, as long as the WMI service is not disabled.
Windows XP	64-bit	Service Pack 2	Requires KB3072630. For more info, see the Microsoft Update Catalog [https://www.catalog.update.microsoft.com/Search.aspx?q=KB3072630] .	There is no SP3 of 64-bit
Windows Server 2003	32-bit and 64-bit	Service Pack 2	Requires KB3072630. For more info, see the Microsoft Update Catalog [https://www.catalog.update.microsoft.com/Search.aspx?q=KB3072630] .	
Windows Server 2003 R2	32-bit and 64-bit	Service Pack 2	Requires KB3072630. For more info, see the Microsoft Update Catalog [https://www.catalog.update.microsoft.com/Search.aspx?q=KB3072630] .	
Windows Vista	32-bit and 64-bit	Service Pack 2	Requires KB4474419. For more info, see the Microsoft Update Catalog [https://www.catalog.update.microsoft.com/Search.aspx?q=KB4474419] .	
Windows Server 2008	32-bit and 64-bit	Service Pack 2	Requires KB4474419. For more info, see the Microsoft Update Catalog [https://www.catalog.update.microsoft.com/Search.aspx?q=KB4474419] .	
Windows Embedded POSReady 2009			SHA-2 code sign support is not required.	
Windows 8	32-bit and 64-bit		SHA-2 code sign support is not required.	

Windows 8.1	32-bit and 64-bit		SHA-2 code sign support is not required.	

Services

Verify if these services are enabled and running on your hosts.

Some older operating systems might not have these services, so disregard any that don't apply:

- **LMHosts**
  - 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**

Network protocols

The Falcon sensor requires TLS 1.2 to communicate with the CrowdStrike cloud. The Falcon sensor for legacy systems automatically contains support for TLS 1.2 on supported operating systems to ensure secure cloud communication. No additional action is required. For more info, see Supported operating systems [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#nf45be6e].

Additional services for hosts using proxies

Configure these additional Windows services required when your legacy hosts connect to the Falcon cloud through proxy servers.

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

Certificates

The Falcon sensor requires certain certificates.

For more information, see Verify that your host trusts CrowdStrike's certificate authority [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#f4905002].

Networking requirements

Ensure your legacy systems can communicate with the Falcon cloud by configuring required ports, protocols, and network access rules.

Internet access

Internet connectivity requirements ensure legacy systems can communicate with the cloud.

Hosts must connect to the CrowdStrike cloud on port 443 outbound 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].

The sensor discovers a CID's cloud during provisioning. For optimal discovery, allowlist all the IP addresses for the US-1, US-2, and EU-1 clouds.

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

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].

CrowdStrike cloud US-1 domains

```
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
```

Supported features

Falcon sensor for legacy systems supports these Falcon features:

- Performs lookups to Cloud-based machine learning (ML) when processes are created to determine file maliciousness.
  - The cloud-based ML confidence thresholds are set to **High**.
  - ML predictions with lower confidence thresholds do not trigger detection or prevention actions.
- Processes are blocked when they are determined to be malicious.
- Prevention policy settings allow you to enable or disable detection and prevention features. An additional toggle allows you to disable the sensor for troubleshooting purposes.
- ProcessRollup2 (PR2) event visibility for all process creations are available to customers with Falcon Insight XDR.

Review these considerations:

- Support for cloud-based ML requires a network connection to the Falcon cloud.
- No self-service allowlisting or exclusion tools are available in the Falcon console for this sensor. If there are detections that cause concern, create a Support ticket for CrowdStrike to investigate.
- No other features, functionality, or modules are supported beyond what is listed in this section.

Standard installation

In most cases, you can install the Falcon sensor for Legacy Systems 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, boot in safe mode to fix the Windows registry.

For information about other installation considerations, see Advanced installation options [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#sd4cbeaf].

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

Manual installation

The Falcon sensor for legacy systems requires manual installation using the following steps:

1. Download the sensor installer from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].
   The installer works for only one of the CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, or US-GOV-2. The downloaded file has a name that varies by the

The installer works for only one of the CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, or US-GOV-2. The downloaded file has a name that varies by the cloud: `WindowsLegacySensor.exe` or `WindowsLegacySensor.<cloud>.exe`.

2. Copy your customer ID checksum (CCID) from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].

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 your OS prompts you 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 [/hosts/sensor-downloads].
   The installer works for only one of the CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, or US-GOV-2. The downloaded file has a name that varies by the cloud: `WindowsLegacySensor.exe` or `WindowsLegacySensor.<cloud>.exe`.

2. Copy your CCID from Host setup and management > Deploy > Sensor downloads [/hosts/sensor-downloads].

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>`

Post-installation steps

Verifying sensor installation

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 [/investigate/dashboards/sensor-report].

Host

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

```
sc.exe query csagent
```

This output appears 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/j86ac82d/falcon-sensor-for-legacy-systems-deployment#h684a8e3].

Advanced installation options

Specifying the cloud where an endpoint's CID resides

CrowdStrike provides a unified installer to deploy sensors in the US-1, US-2, and EU-1 clouds.

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

The sensor automatically discovers and connects to the appropriate CrowdStrike cloud based on the CID. Unlike other sensors, you cannot manually specify the cloud connection for this sensor.

Installing in a virtual environment

Unlike other CrowdStrike sensors, this sensor only supports the persistent method of VM installation. If the same AID is assigned to more than one VM, events and detections from your various VMs appear to be from a single host.

In the persistent method of VM installation, the VM retains user profile settings, data, or configuration changes after a user logs off or reboots. The VM resumes in the same state it was when shut down. For detailed instructions, see
Installing the Falcon sensor on a virtual machine template [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#z679cd34].

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 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 appear to be from a single host.

Installing the sensor on a VM template

Follow these steps to install 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. If the Falcon sensor is already installed on the template, follow the instructions to remove it. For more info, see Uninstalling the Falcon sensor for legacy systems [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#ef9e808d].
3. Install the Falcon sensor using the `NO_START=1` parameter:
   `<installer_filename> /install CID=<CCID> NO_START=1`
   - After installation, the sensor does not attempt to communicate with the CrowdStrike cloud.
   - Don't reboot the host, or it attempts to communicate with the CrowdStrike cloud on reboot.
4. Confirm that the installation is complete.
5. 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 appear to be from a single host.

You can resolve this by removing the following registry key:

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

Modifying a VM template

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

1. Prepare your VM template.
2. Delete this registry value:
   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default\AG
   ```
3. Shut down the VM.
4. Convert the VM to a template image using your virtualization software.

Uninstalling the Falcon sensor for legacy systems

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

Uninstalling using the Control Panel

Follow these steps to uninstall the Falcon sensor using the Control Panel:

1. Open the **Windows Control Panel** running it as administrator.
2. Click **Uninstall a Program**.
3. Select **CrowdStrike Windows Legacy Sensor** and uninstall the sensor.

Uninstalling using the command line

To uninstall the sensor, open a command prompt with administrative privileges and run the installer with the `/uninstall` parameter.

Validating the uninstallation

After the sensor is 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. The sensor contacts the CrowdStrike cloud, which assigns an agent ID to 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 shuts down or reboots during installation, the installer can't exit cleanly, and the host might be left in an unusable or unknown state.

Provisioning phase

Provisioning might take minutes or much longer, depending on your network configuration.

Make sure your hosts stay online through the provisioning phase. The sensor operates normally during provisioning using its previously known configuration.

When a host has finished provisionings, 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/dashboards/sensor-health].

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	For info on how to troubleshoot, see Issue: Host can't connect to the CrowdStrike cloud [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#b5da4b1a] .

Installation fails

If the sensor installation fails, confirm that the host meets our system requirements, including required Windows services. For more info, see System requirements [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#nc6578ff].

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.

For more info, see Logs [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#n18cb8a3].

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 is installed but doesn't run

If the sensor doesn't run, confirm that the host meets our system requirements, including required Windows services. For more info, see System requirements [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#nc6578ff].

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.

For more info, see Logs [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#n18cb8a3].

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 [/investigate/dashboards/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 [/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.

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.

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**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 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: The first phase is proxy discovery and the second phase is connection. This occurs in the following order:

1. Try to use the CS Sensor application-specific proxy, which is specified through the installers `APP_PROXYNAME=<Proxy server hostname or IP address>` and `APP_PROXYPORT=<Proxy server port>`.
2. If available, apply proxy settings from the Local Area Network (LAN) Settings. This setting is found under **Proxy Servers**, also called **IE Proxy Settings**.
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"**. Select this if you want to use Windows AutoProxy with a PAC File.
5. Use any type of persisted proxy settings. 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 a config-driven DNS lookup table to connect.

When `PROXYDISABLE=1` is passed to the installer, the installer will skip steps 1-6 and proceed directly to step 7 and connect directly, and then to step 8.

When PROXYDISABLE=1 is passed to the installer, the installer will skip steps 1-6 and proceed directly to step 7 and connect directly, and then to step 8.

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

Run a `CSLegacyWinDiag` collection:

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 `CSLegacyWinDiag` available.
2. Unzip the file to `\Windows\Temp`
3. Go to that folder and run the tool.
   Options to run the tool:
   - Open a command prompt with local administrator privileges. If prompted, enter local administrator credentials.
   - Using the command prompt, type `CSLegacyWinDiag` and press **Enter**.
4. Wait about 4 minutes for the collection to complete.
   When done, the tool indicates the location of the collection file, such as `\Windows\Temp\CSLegacyWinDiag-<hostname>-mRRfqs8F.cab`.

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 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

Appendix A: Installer parameters

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

- All installer parameters are case-sensitive.
- Some parameters require a leading slash, and some require no leading slash.

Note: Enter the parameters exactly as shown.

Installation parameters

Parameter	Description
`CID=0123456789ABCDEFGHIJKLMNOPQRSTUV-WX`	Your Customer ID Checksum, which is required when installing. For more info, see Customer ID Checksum [/hosts/sensor-downloads/].
`/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.

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.

	This parameter is usually used when preparing master images for cloning.

Proxy parameters

Parameter	Description	Usage
`APP_PROXYNAME=` `APP_PROXYPORT=`	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=`	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 Legacy Systems 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 10 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 the host is offline during installation and won't be provisioned until it is back online.
`ProvWaitTime=3600000`	The sensor waits 3600000 milliseconds, or 1 hour, to connect to the CrowdStrike cloud when installing. The default is 10 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 within 5 minutes.

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. For more info, see Logs [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment#n18cb8a3].

Falcon for Legacy Systems - Prevention Policy Settings > [/documentation/page/vbb2ddab/falcon-for-legacy-systems-prevention-policy-settings]