CROWDSTRIKE CONFIDENTIAL

Falcon Sensor for Windows

Last updated: Jul 24, 2020

Contents:

System Requirements

Operating Systems

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

- 64-bit Server OSes:
  - Windows Server 2019 – requires WIN sensor 4.18.8104+
  - Windows Server Core 2019 - requires WIN sensor 5.13.9404+
  - Windows Server 2016
  - Windows Server Core 2016 - requires WIN sensor 5.12.9302+
  - Windows Server 2012 R2
  - Windows Storage Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1
- 64-bit Desktop OSes:
  - Windows 10 May 2020 Update v2004 aka 20H1 – requires WIN sensor 5.34.11603
  - Windows 10 November 2019 Update v1909 aka 19H2 – requires WIN sensor 5.19.10102+
  - Windows 10 May 2019 Update v1903 aka 19H1 – requires WIN sensor 5.12.9302+
  - Windows 10 October 2018 Update v1809 aka RS5 – requires WIN sensor 4.17.8003+
  - Windows 10 April 2018 Update v1803 aka RS4 - requires WIN sensor 4.4.6711+
  - Windows 10 Fall Creators Update v1709 aka RS3 - requires WIN sensor 3.8.5906+
  - Windows 10 Anniversary Update v1607 aka RS1
  - Windows 10 v1507 aka Threshold 1
  - Windows 10 IOT Enterprise v2004 (20H1) - requires WIN sensor 5.34.11603
  - Windows 10 IOT Enterprise v1909 (19H2)- requires WIN sensor 5.26.10806+
  - Windows 10 IOT Enterprise v1903 (19H1) - requires WIN sensor 5.26.10806+
  - Windows 10 IOT Enterprise v1809 (RS5) - requires WIN sensor 5.26.10806+
  - Windows 8.1
  - Windows 7 SP1
  - Windows 7 Embedded
- 32-bit Desktop OSes:
  - Windows 10 May 2020 Update v2004 aka 20H1* – requires WIN sensor 5.34.11603
  - Windows 10 November 2019 Update v1909 aka 19H2* – requires WIN sensor 5.26.10806+
  - Windows 10 May 2019 Update v1903 aka 19H1* – requires WIN sensor 5.26.10806+
  - Windows 10 October 2018 Update v1809 aka RS5* – requires WIN sensor 5.26.10806+
  - Windows 7 SP1

- Windows 7 Embedded POSReady

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

UNSUPPORTED WINDOWS VERSIONS

All other Windows OSes are ***unsupported***, including:

- Windows Server 2008 (non-R2), which is based on the Vista kernel
- Windows Server Core, all versions other than 2016 and 2019
- Windows 10 64-bit v1511 (aka Threshold 2) and v1703 (aka RS 2)
- 32-bit Windows 10 October 2018 Update v1809 aka RS5* (EOS as of Oct 1, 2020)
- 32-bit versions of Windows 10 prior to RS5
- All 32-bit versions of Windows 8.1 (EOS as of 06/08/18)
- Windows 8 all versions (EOS as of 06/08/18)

> Container-based Windows OS solutions – including but not limited to Docker – are not currently supported.

Services

These services must be installed and running:

- **LMHosts**
- **Network Store Interface (NSI)**
- **Windows Base Filtering Engine (BFE)**
- **Windows Power Service** (sometimes labeled **Power**)

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

Additionally, the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Dnscache\Type` must be set to `0x00000020`, the Microsoft default value.

NETWORK PROTOCOLS

Falcon uses TLS 1.2 on Windows 7 and Windows Server 2008 R2 to communicate with the CrowdStrike cloud. If TLS 1.2 has been disabled by the system administrator, Falcon negotiates TLS 1.1 or TLS 1.0, depending on the cloud.

- US-1 and US-2
  - TLS 1.0 or later
- US-GOV-1
  - TLS 1.1 or later

> The CrowdStrike cloud doesn't support connecting via SSL.

ADDITIONAL SERVICES FOR HOSTS USING PROXIES

- **WinHTTP AutoProxy**

- **DHCP Client**, if you use Web Proxy Automatic Discovery (WPAD) via DHCP

To use Falcon's Next-Gen Antivirus policy settings on Windows Server 2016 or 2019, manually disable Windows Defender.

Networking Requirements

Maintain Internet Access During Installation

Hosts must remain connected to the CrowdStrike cloud throughout installation, which is generally 10 minutes. A host unable to reach and retain a connection to the cloud within 10 minutes will not successfully install the sensor.

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

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

Replacing `<installer_filename>` with the name of the install file you downloaded, and `<CCID>` with the CCID from Hosts > Sensor Downloads.

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

Depending on your network environment, you may need to allow ("whitelist") TLS traffic between your network and our cloud's network addresses:

US-1 (most customers):

- ts01-b.cloudsink.net
- lfodown01-b.cloudsink.net

US-GOV-1:

- ts01-laggar-gcw.cloudsink.net
- lfodown01-laggar-gcw.cloudsink.net

EU-1:

- ts01-lanner-lion.cloudsink.net
- lfodown01-lanner-lion.cloudsink.net

US-2:

- ts01-gyr-maverick.cloudsink.net
- lfodown01-gyr-maverick.cloudsink.net

If your network requires allowing by IP address instead of FQDN, see Cloud IP Addresses for a list of IP addresses we use.

> We use AWS for some communications between hosts and the CrowdStrike cloud.

Standard Installation

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

Manual install

Use this installation path if you want to point and click on an installer file.

1. Download the sensor installer from Hosts > Sensor Downloads. Use the Chrome browser.
2. Copy your customer ID checksum from Hosts > Sensor Downloads.

   If you're a trial user, skip this step.
3. Run the sensor installer on your device.
4. Enter your customer ID checksum and accept the EULA.

   If you're a trial user, skip this step.
5. If your OS prompts to allow the installation, click **Yes**.

After installation, the sensor will run silently and will be invisible to the user. To validate that the sensor is running on the host, run this command at a command prompt:

```
sc 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.

Automatic Sensor Installation

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

1. Download the sensor installer from Hosts > Sensor Downloads. Use the Chrome browser.
2. Copy your customer ID checksum (CCID) from Hosts > Sensor Downloads.
3. Run or configure your deployment tool to use this command, replacing `<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 on these parameters and their functions, see Appendix A.

Uninstall Protection for the Falcon Sensor

Protect sensors from unauthorized uninstallation by enabling **Uninstall and maintenance protection** in sensor update policies to protect hosts. For more info, read our Sensor Update Policies guide.

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 via a deployment tool like Windows System Center Configuration Manager (SCCM).

1. Download the sensor installer from **Hosts** > **Sensor Downloads**. Use the Chrome browser.
2. In the sensor update policy you want to update, turn on **Bulk maintenance mode**. Make sure the **Sensor version updates off** build version is selected and **Uninstall and maintenance protection** is turned on.
3. Retrieve the bulk maintenance token to include in the deployment package. This token doesn't change, so you don't need to modify your deployment package each time you enter bulk maintenance mode.
4. Run or configure your deployment tool to use this command, replacing`<installer_filename>` with the name of the install file you downloaded:

   ```
   <installer_filename> MAINTENANCE_TOKEN=<bulk maintenance token>  /install /quiet /norestart
   ```

5. For increased security, turn off bulk maintenance mode after completing your upgrades. This restores the per-sensor maintenance token and disables the bulk maintenance token.

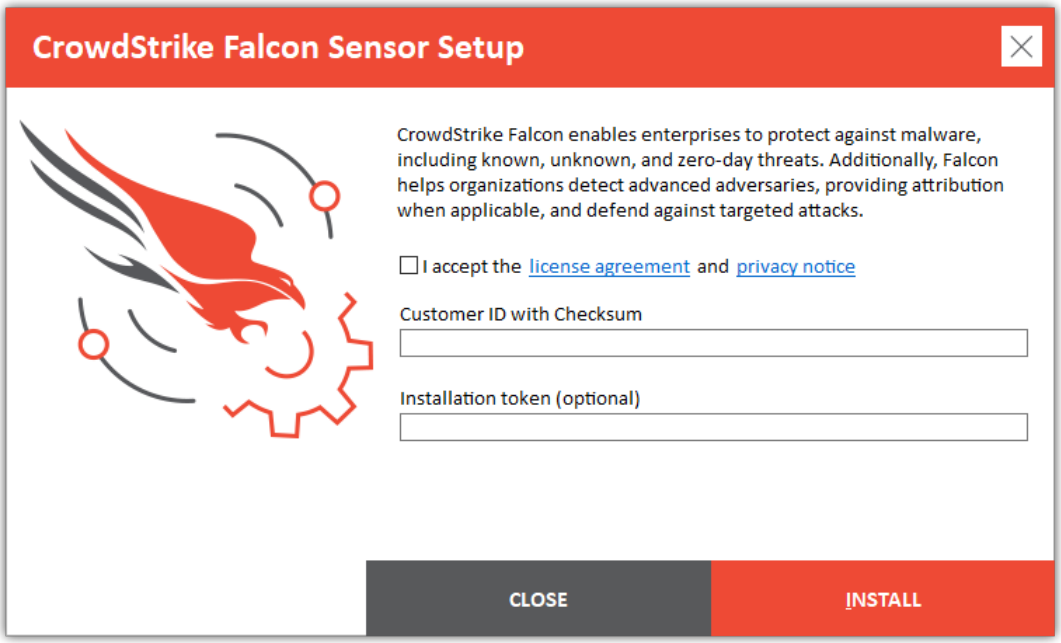
Installing to a CID that requires installation tokens

Installation tokens 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 via the API, enable the token requirement, and then provide the tokens to sensors at installation time.

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

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

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



Assigning Sensor Tags During Installation

Sensor tags are user-selected identifiers you can use to group and filter hosts. You can assign one or more tags to a host using the `GROUPING_TAGS` parameter. This parameter is case sensitive.

Tags can include these characters:

1. alphanumeric characters
2. hyphens (-)
3. underscores (_)
4. forward slashes (/)

Tags can't include spaces ( ) or commas (,).

To use multiple tags, separate each tag with commas. All tags for a host, including comma separators, cannot exceed 256 characters.

```
<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 Hosts > Sensor Downloads.

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

Assign tags during installation to make them immediately available when the sensor first connects to the CrowdStrike cloud. Tags can be added or changed after sensor installation by editing a registry key, but the host needs to be restarted for the changes to take effect.

For information see Manually adding or modifying Falcon Sensor tags on Windows.

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 Hosts > Sensor Downloads.

Choosing the best virtual installation method

When you install the sensor on a VM, use the correct installation method to ensure that each host ends up with 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.

Use the `VDI=1` parameter during installation if your VM meets all of the following criteria:

- It is non-persistent
- It is domain-joined
- It uses a fully qualified domain name (FQDN)

For VMs that don't meet all of those criteria, use the Virtual Machine Template installation.

Installing the Falcon Sensor in a VDI Environment

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

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

1. Put your image template system into read/write mode.
2. Install the Falcon sensor using the `VDI=1` parameter.
   - `<installer_filename> /install CID=<CCID> VDI=1`
   - Replacing `<installer_filename>` with the name of the install file you downloaded, and `<CCID>` with the CCID from Hosts > Sensor Downloads.
   - After the installation is complete, the sensor communicates with the cloud and updates to the sensor version defined in the host's assigned Sensor Update policy. You can check the update status by finding the host in Host Management.
3. After the sensor is on the proper version, switch your template system back to read-only mode and save the image.

Installing the Falcon Sensor on a Virtual Machine Template

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

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

INSTALLING THE SENSOR ON A VM TEMPLATE

1. Complete all steps required to generalize the VM template, such as sysprep or installing Windows and software updates.
2. Install the Falcon sensor using the `NO_START=1` parameter:

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

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

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

TROUBLESHOOTING VM TEMPLATES

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

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

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

MODIFYING A VM TEMPLATE

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

1. Prepare your VM template.
2. Delete these registry values:
   - HKEY_LOCAL_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default\AG
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSAgent\Sim\AG

The AID is removed from the VM template.

1. Shut down the VM.
2. Convert the VM to a template image using your virtualization software.

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

See Falcon for Cloud Workloads for full information about Pay-As-You-Go billing.

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

1. Prepare your master image instance, including any software configuration or updates.
2. Download the Falcon sensor installer from Hosts > Sensor Downloads or via sensor download APIs.
3. Install the Falcon sensor using the `NO_START=1` and `BILLINGTYPE=Metered` parameters (case-sensitive):

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

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

4. Confirm that the installation is complete.

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

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

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

Uninstalling the Falcon Sensor for Windows

Uninstall from Control Panel

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

Uninstall from the Command Line

1. Download `CSUninstallTool` from Tool Downloads
2. Run `CSUninstallTool` from the command line with this command:

```
CsUninstallTool.exe /quiet
```

UNINSTALL PROTECTION ON SENSOR VERSION 5.10.9105 AND LATER

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

If the sensor is offline and **Uninstall and maintenance protection** is enabled, open the host's summary panel in **Hosts > Host Management** page and click **Reveal Maintenance Token** to get the single-use maintenance token needed to uninstall the sensor. Use this token in this command line script to uninstall the sensor:

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

If the sensor is offline and bulk maintenance mode is enabled, go to the host's sensor update policy and click **Reveal Token** to get the bulk maintenance token needed to uninstall the sensor. Use the token in this command line script to uninstall the sensor:

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

Validate 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 Sensor Installation

Issue: 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 may 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.

Verify that the Sensor is Running

To verify that the sensor is running on your host:

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

The following output is displayed if the sensor is running:

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

Troubleshooting General Sensor Issues

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 may 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 can install, but not run, if any of these services are disabled or stopped:

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

The sensor can install, but not run, if the **WinHTTP AutoProxy** service is disabled.

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

See Logs for more information.

Verify the Host's Connection to the CrowdStrike Cloud

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

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

```
netstat -f
```

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

```
Active Connections

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

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

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

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 may 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

ATTEMPT A COMMAND LINE INSTALLATION

Hosts must remain connected to the CrowdStrike cloud throughout installation. A host unable to reach the cloud within 10 minutes will not successfully install the sensor.

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

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

Replacing `<installer_filename>` with the name of the install file you downloaded, and `<CCID>` with the CCID from Hosts > Sensor Downloads.

VERIFY THAT YOUR HOST TRUSTS CROWDSTRIKE'S CERTIFICATE AUTHORITY

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

1. Download the certificates from Digicert: DigiCertHighAssuranceRootCA and DigiCertAssuredIDRootCA
2. Follow Microsoft's documentation for the Microsoft Management Console (MMC) to:
    1. Enable the Certificates snap-in.
    2. Add the certificate.

Issue: Host Can't Establish Proxy Connection

The following use cases are currently supported:

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

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

1. Try to use the CS Sensor application-specific proxy which is specified via 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 via 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 (via connection methods 1-6, excluding 5), 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.

This will put the proxy settings in the registry under the `CsProxyHostname` and `CsProxyPort` keys located here:

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

Logs

Providing logs to our support team can help diagnose sensor issues.

Export your logs in their native directory structure and format (such as `.evtx` for sensor operations logs). This helps our support team diagnose sensor issues accurately and efficiently.

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 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 myfile.reg
```

Normal Log Contents

A normal startup log includes messages similar to these:

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

Appendix A - Installer Parameters

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

> Enter the parameters exactly as shown.

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

Installation Parameters

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

Sensor Startup Parameters

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

Proxy Parameters

Parameter	Description	Usage
`APP_PROXYNAME=<proxy FQDN or IP> APP_PROXYPORT=<Proxy server port>`	Configure a proxy connection using both a proxy address (by FQDN or IP) and a proxy port.	Cannot be used with the `PACURL` parameter.
`PACURL=<PAC file URL>`	Configure a proxy connection using a PAC file.	Cannot be used with the `APP_PROXYNAME` and `APP_PROXYPORT` parameters.

`PROXYDISABLE=1`	By default, the Falcon sensor for Windows automatically attempts to use any available proxy connections when it connects to the CrowdStrike cloud. This parameter forces the sensor to skip those attempts and ignore any proxy configuration, including Windows Proxy Auto Detection.	
`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 will retry the connection for 10 minutes. After that, the host will automatically uninstall its sensor.)	Use this parameter when upgrading to version 3.5 or later if you use IE proxy detection for Falcon, because proxy data will not be available until another user logs into the machine.
`ProvWaitTime=3600000`	The sensor will be allowed 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.

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.