Falcon Sensor for Windows

Version 6.23 - Last updated: October 16, 2019

Contents:

- System Requirements
  - Operating Systems
  - Services
- Networking Requirements
  - Maintain Internet Access During Installation
  - Avoid Interference with Certificate Pinning
  - Whitelist URLs
- Standard Installation
  - Manual install
  - Automatic Sensor Installation
- Advanced Installation Types
  - Uninstall Protection for the Falcon Sensor
  - Assigning Sensor Tags During Installation
  - Installing the Sensor with IE Proxy Detection
  - Installing the Falcon Sensor on a Virtual Machine Template
  - Installing the Falcon Sensor in a Virtual Desktop Infrastructure (VDI) Environment
- Uninstalling the Falcon Sensor for Windows
  - Uninstall from Control Panel
  - Uninstall from the Command Line
  - Validate the Uninstallation
- Troubleshooting Sensor Installation
  - Issue: Installation Fails
  - Verify that the Sensor is Running
- Troubleshooting General Sensor Issues
  - Issue: Sensor Installed, but Doesn't Run
  - Verify the Host's Connection to the CrowdStrike Cloud
  - Issue: Host Can't Connect to the CrowdStrike Cloud
  - Issue: Host Can't Establish Proxy Connection
- Logs
  - Sensor Operational Logs
  - Normal Log Contents
- Appendix A - Installer Parameters
  - Installation Parameters
  - Sensor Startup Parameters
  - Proxy Parameters
  - Troubleshooting Parameters
- Revision History
System Requirements

Operating Systems

Falcon on GovCloud is supported on Falcon sensor for Windows 4.5 and later.

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

- 64-bit server OSes:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1
  - Windows Server Core 2019
  - Windows Server Core 2016
  - Windows Storage Server 2012 R2

- 64-bit desktop OSes:
  - Windows 10 November 2019 Update, also named v1909, or 19H2
  - Windows 10 May 2019 Update, also named Redstone 6, v1903, or 19H1
  - Windows 10 October 2018 Update, also named Redstone 5 or v1809
  - Windows 10 April 2018 Update, also named Redstone 4 or v1803
  - Windows 10 Fall Creators Update, also named Redstone 3 or v1709
  - Windows 10 Creators Update, also named Redstone 2 or v1703
  - Windows 10 Anniversary Update, also named Redstone 1 or v1607
  - Windows 10
  - Windows 8.1
  - Windows 7 SP1
  - Windows 7 Embedded

- 32-bit desktop OSes:
  - Windows 7 SP1
  - Windows 7 Embedded POSReady
All other operating systems are unsupported, such as Windows Server 2008 (non-R2), versions of Windows Server Core released before version 2016, Windows 8, and 32-bit versions of Windows 10 or Windows 8.1.

We do not support hosts running in containers, or the installation of the Falcon sensor in containers (such as Docker).

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 on commercial cloud
  - TLS 1.0 or later
- Falcon on GovCloud
  - 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.

```
WindowsSensor.exe /install /norestart CID=<your CID> ProvWaitTime=3600000
```

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," "TLS interception," or "SSL inspection") or similar network configurations. Common sources of interference with certificate pinning include antivirus systems, firewalls, or proxies.

Whitelist URLs

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

**Commercial Cloud (most customers):**
- ts01-b.cloudsink.net
- Ifodown01-b.cloudsink.net

**Falcon for GovCloud:**
- ts01-laggar-gcw.cloudsink.net
- Ifodown01-laggar-gcw.cloudsink.net

**Falcon EU Cloud:**
- ts01-lanner-lion.cloudsink.net
- Ifodown01-lanner-lion.cloudsink.net

If your network requires whitelisting by IP address instead of FQDN, see [Cloud IP Addresses](https://falcon.crowdstrike.com/support/documentation/23/falcon-sensor-for-windows) 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
(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 `<your executable file name>` with the name of the
install file you downloaded, and `<CCID>` with the CCID from step 2:

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

For information on these parameters and their functions, see Appendix B.
Advanced Installation Types

Uninstall Protection for the Falcon Sensor

*Sensor version 5.10.9105 and later*

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](https://falcon.crowdstrike.com/support/documentation/23/falcon-sensor-for-windows) 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](https://falcon.crowdstrike.com/support/documentation/23/falcon-sensor-for-windows). 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 `<your executable file name>` with the name of the install file you downloaded:

   `<your executable file name>.exe 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.

*Sensor version 3.6.5703–4.26.8904*

You can set a password on a host to protect its sensor from unauthorized tampering. Once you set the password, it must be provided whenever someone attempts to unload, uninstall, repair, or manually upgrade the sensor.

**Selecting a password:**

- Your password can’t contain the quotation mark character, because the command used to set the password is enclosed in quotation marks.

- Your password can contain other common ASCII characters, including `a - z`, `A - Z`, `0 - 9`, common symbol characters like `!@#$%`, and spaces.

**SETTING A PASSWORD**

- During installation:

  - Install the sensor from the command line. In addition to the parameters used in a basic installation, include this parameter: `PW="examplepassword"`
After installation:

1. On a host with the Falcon sensor installed, open the folder %ProgramFiles%\CrowdStrike.

2. Run CSInstallGuard.exe with the PW parameter:

   CSInstallGuard.exe PW="examplepassword"

CHANGE OR REMOVE AN EXISTING PASSWORD

You can't directly change or remove an existing password. You must uninstall and reinstall the sensor.

1. Uninstall the sensor using its existing password.

2. Reinstall the sensor with either the new password or no password.

RESET A LOST PASSWORD

If you lose a host's password, contact Support for password reset. A user with the Falcon Admin role (or equivalent) must send the host's AID or hostname to our support team.

Assigning Sensor Tags During Installation

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

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

WindowsSensor.exe /install /norestart CID=<your cid> GROUPING_TAGS="Washington/DC_USA,Production"

This sets two tags: Washington/DC_USA and Production.

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

Installing the Sensor with IE Proxy Detection

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

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

Installing the Falcon Sensor on a Virtual Machine Template
Follow these steps to set up a virtual machine template with a Falcon sensor.

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

INSTALLING ON A VM TEMPLATE

To install on a virtual machine (VM) template:

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

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

3. Shut down the VM.
4. Use your virtualization software to convert the VM to a template image.

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

MODIFYING A VM TEMPLATE

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

1. Prepare your VM template.
2. Remove these registry values to remove the AID from the VM template:

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

3. Shut down the VM.
4. Use your virtualization software to convert the VM to a template image.

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

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

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

1. Prepare your VDI master image.
2. Install the sensor with the \texttt{VDI=1} parameter:

\texttt{WindowsSensor.exe /install CID=<your CID> VDI=1}

**Update your VDI master's sensor:** We recommend regularly updating your VDI master image to use the latest Falcon sensor version. This minimizes the risk of new VDI instances running outdated Falcon sensors, as well as network traffic caused by sensor updates.
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.
WindowsSensor.exe /install /norestart CID=<your CID> ProvNoWait=1

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-7858-48c9-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.

<table>
<thead>
<tr>
<th>Log type</th>
<th>Enabled by default?</th>
<th>Location</th>
<th>Log size</th>
<th>Log retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor operations</td>
<td>No</td>
<td>In Windows Event Viewer under Windows Log &gt; System. Look for the label CSAgent.</td>
<td>Based on OS or group policy settings</td>
<td>Based on OS or group policy settings</td>
</tr>
<tr>
<td>Sensor installation (installation, uninstallation, upgrades, or downgrades)</td>
<td>Yes</td>
<td>If initiated by a user: %LOCALAPPDATA%\Temp If initiated by the CrowdStrike cloud: %SYSTEMROOT%\Temp</td>
<td>Based on OS or group policy settings</td>
<td>Based on OS or group policy settings</td>
</tr>
</tbody>
</table>

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:
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CID=0123456789ABCDEFGHIJKLMNOPQRSTUV-WX</td>
<td>Your <strong>Customer ID Checksum</strong>, which is required when installing.</td>
<td></td>
</tr>
<tr>
<td>/install</td>
<td>Install the sensor (default).</td>
<td></td>
</tr>
<tr>
<td>/passive</td>
<td>The installer shows a minimal UI with no prompts.</td>
<td></td>
</tr>
<tr>
<td>/quiet</td>
<td>The installer shows no UI and no prompts.</td>
<td></td>
</tr>
<tr>
<td>/norestart</td>
<td>Prevents the host from restarting at the end of the sensor installation.</td>
<td></td>
</tr>
</tbody>
</table>

Sensor Startup Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PW=&quot;examplepassword&quot;</td>
<td>Sets a protection password, which must be provided in order to stop or uninstall the sensor. The protection password must be enclosed in quotation marks (&quot;).</td>
<td>If used, this parameter must be the first parameter. The password cannot include the quotation mark character (&quot;), Requires sensor version 3.6.5703 or later.</td>
</tr>
<tr>
<td>NO_START=1</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>VDI=1</td>
<td>Enable virtual desktop infrastructure mode.</td>
<td></td>
</tr>
</tbody>
</table>

Proxy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Usage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>APP_PROXYNAME=&lt;proxy FQDN or IP&gt;</td>
<td>Configure a proxy connection using both a proxy address (by FQDN or IP) and a proxy port.</td>
<td>Cannot be used with the <strong>PACURL</strong> parameter.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PACURL=&lt;PAC file URL&gt;</td>
<td>Configure a proxy connection using a PAC file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROXYDISABLE=1</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProvNoWait=1</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProvWaitTime=3600000</td>
<td>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. ##################################################################################################################################################################################################</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Parameters**

<table>
<thead>
<tr>
<th>Troubleshooting parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/?</td>
<td>Show help information for the installer.</td>
</tr>
<tr>
<td>/repair</td>
<td>Repair the sensor installation.</td>
</tr>
<tr>
<td>/log log.txt</td>
<td>Change the log directory to the specified file.</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision date</th>
<th>Revision details</th>
<th>Completed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>02/2016</td>
<td>Initial release.</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>2.0</td>
<td>03/23/2016</td>
<td>Added certificate troubleshooting content.</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>2.1</td>
<td>05/25/2016</td>
<td>Added second registry key to list of keys that must always be removed to avoid duplicate VMs with same Agent ID (aid).</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>2.2</td>
<td>05/16/2016</td>
<td>Added in NETBIOS prerequisite. Added list of supported protocols. Added uninstall confirmation steps. Rebranding as Sensor Deployment Guide.</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>2.3</td>
<td>06/13/2016</td>
<td>Updating styles.</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>2.4</td>
<td>06/28/2016</td>
<td>Added instructions for logging.</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>2.5</td>
<td>08/08/2016</td>
<td>Added additional sensor dependencies.</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>3.0</td>
<td>10/24/2016</td>
<td>GA for new UI.</td>
<td>Nick Cangie</td>
</tr>
<tr>
<td>4.0</td>
<td>01/13/2017</td>
<td>Updating install guide for new Windows Sensor.</td>
<td>Nick Cangie</td>
</tr>
</tbody>
</table>