CROWDSTRIKE ENDPOINT SECURITY DEPLOYMENT GUIDE

02 November 2022

PREPARED FOR:

Table of Contents

EMAIL COMMUNICATION

The automated emails sent by our cloud instance are sent using the domain ***amazonses.com** . These emails are sent in the beginning to initiate the onboarding process and whenever a password reset is requested. Therefore, please whitelist the email address **falcon@crowdstrike.com** and sending address ***amazonses.com** in your email gateway

NETWORK REQUIREMENTS – WHITELISTED URLS

In preparation of our POV kick off, I'd like to make you aware of some networking prerequisites which are required in order to allow the Falcon agent to communicate with the CrowdStrike cloud.

1. Firewall Connectivity

a. **Open the following for outbound TCP 443 with SSL BYPASS** Sensor Built-In IPs

- 100.20.76.137
- 35.162.239.174
- 35.162.224.228
- 34.209.79.111
- 52.10.219.156
- 34.210.186.129
- 54.218.244.79
- 54.200.109.111
- 100.20.109.43
- 44.225.216.237
- 44.227.134.78
- 44.224.200.221

Full IP Range : https://falcon.us-2.crowdstrike.com/documentation/65/cloud-ip-addresses#us2-cloud-ips

2. **Whitelist/Allow the two domains below through your proxy and/or firewall on port 443 (outbound direction from all the endpoints).**

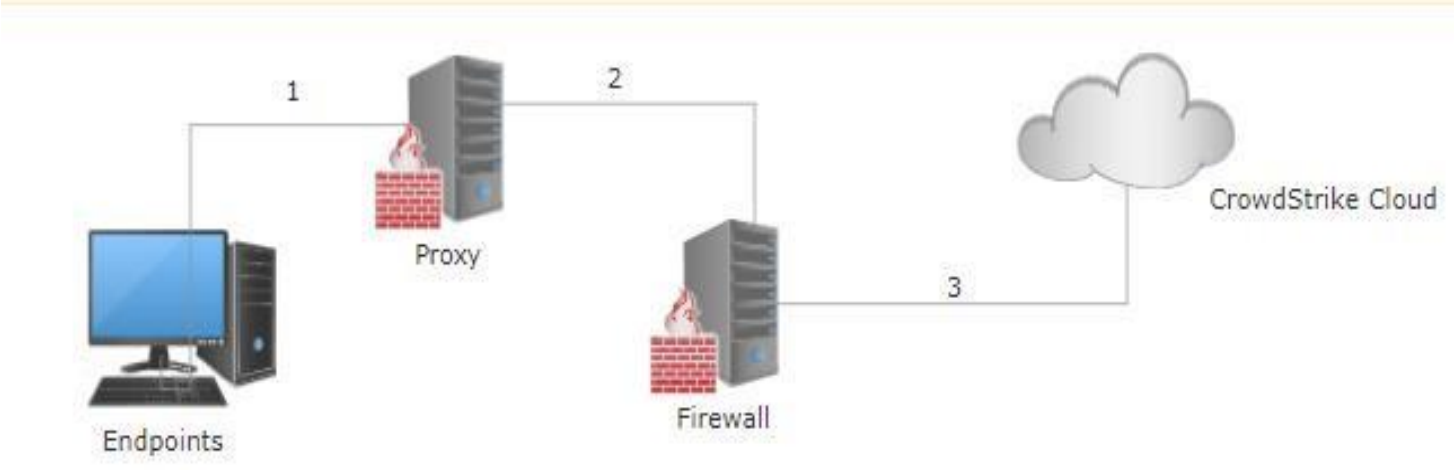
US-2:

- ffc.us-2.crowdstrike.com
- ts01-gyr-maverick.cloudsink.net
- lfodown01-gyr-maverick.cloudsink.net
- https://falconapi.us-2.crowdstrike.com
- https://firehose.us-2.crowdstrike.com

3. **Disable SSL inspection on your proxy and firewall for these URLs.**

US-2:

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



IMPORTANT: If the CrowdStrike agent is unable to communicate with the CrowdStrike cloud check your network configuration and try again.

TROUBLESHOOTING

If the CrowdStrike agent is having difficulty connecting to the falcon cloud, follow the below troubleshooting steps to identify the potential root cause.

Some steps to troubleshoot:

1. Please ensure that the three links specified are allowed through firewall/proxy/web gateway/any intermediate device towards internet on port 443

   Quick test: You can test connectivity to the domains by using telnet

   For example Command: telnet ts01-gyr-maverick.cloudsink.net 443

1. Verify SSL inspection is disabled for the domains

- ffc.us-2.crowdstrike.com
- ts01-gyr-maverick.cloudsink.net
- lfodown01-gyr-maverick.cloudsink.net
- https://falconapi.us-2.crowdstrike.com
- https://firehose.us-2.crowdstrike.com

   Quick test: Open a web browser and browse to either of the two CrowdStrike domains. Check the SSL certificate that is being used. It should be issued by DigiCert and not the one from your local proxy or gateway.

Please ensure you're using a domain admin or local admin to install the agent. It should be installed via an administrator account.

AUTOMATIC SENSOR INSTALLATION

Use the following installation path if you want to automate silent installations on host endpoints. This includes installations via a deployment tool such as Windows System Center Configuration Manager (SCCM) and JAMF (for MacBooks)

Download the sensor installer from Hosts > Sensor Downloads. (*Use the Chrome browser*).

Run or configure your deployment tool to use this command, replacing <your executable/package file name> with the name of the install file you downloaded:

Windows For each Active Directory OU:

WindowsSensor.exe /install /quiet /norestart PROXYDISABLE=1 ProvNoWait=1 CID=******REPLACE THIS WITH CUSTOMER CID****** GROUPING_TAGS="**DEV**"

Mac

sudo installer -verboseR -package <installer_filename> -target / sleep
5
sudo /Applications/Falcon.app/Contents/Resources/falconctl license ********

Redhat/CentOS

1. **Prerequisites** - How to to fix (all redhat 7 upgrade systemd service to 7.7+) https://access.redhat.com/errata/RHBA-2019:2356 basically perform: yum update yum
   yum upgrade systemd

2. Usually already installed: Upgrade OpenSSL to 1.1.1+

3. Install Agent Commands (download agent from the Web UI/Console at https://falcon.crowdstrike.com/hosts/sensor-downloads) sudo yum install <sensorfile name> sudo /opt/CrowdStrike/falconctl -s --cid=<CID> service falcon-sensor start systemctl start falcon-sensor systemctl enable falcon-sensor

   ps -e | grep falcon-sensor
   sudo netstat -tapn | grep falcon

Debian/Ubuntu

sudo apt-get update sudo
apt --fix-broken install
sudo apt-get -y install libnl*
sudo dpkg -i /root/falcon-sensor_5.29.0-9403_amd64.deb
sudo /opt/CrowdStrike/falconctl -s -f --cid="******REPLACE THIS WITH CUSTOMER CID******"
sudo /opt/CrowdStrike/falconctl -s --tags=israel,ubuntu1416prod sudo service falcon-sensor start
sudo systemctl start falcon-sensor

Check Agent is NOT in Reduced Functionality Mode (RFM) status to verify kernel is fully supported (should return False) sudo /opt/CrowdStrike/falconctl -g --rfm-state

*** For VDI AND proxy deployment please contact us.

Windows Falcon Documentation
Mac Falcon Documentation
Linux Redhat Documentation

MANUAL SENSOR INSTALLATION

Windows

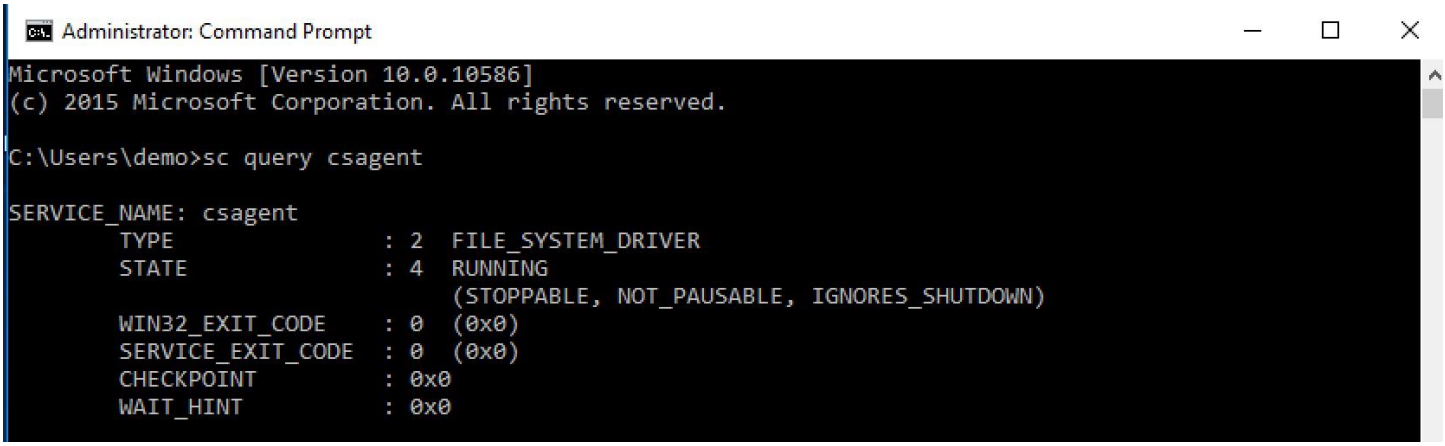
The following highlights how to manually install the CrowdStrike Falcon Agent for Windows hosts.

1. Download the Falcon sensor installer from **Hosts > Sensor Downloads** within the Falcon Cloud platform.
2. Copy your customer ID checksum (CID) from **Hosts > Sensor Downloads**.
3. Run the sensor installer *as an administrator* on your device.
4. Enter your customer ID checksum and accept the EULA.
5. If your OS prompts to allow the installation, click **Yes**.

6. After the installation has completed, 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:



Mac

The following highlights how to manually install the CrowdStrike Falcon Agent for Mac hosts.

1. Download the sensor installer from **Hosts > Sensor Downloads**. Use the Chrome browser.
2. Copy your customer ID checksum (CID) from **Hosts > Sensor Downloads**.
3. Double-click the .pkg file.
4. When prompted, enter administrative credentials for the installer.
5. Run falconctl, installed with the Falcon sensor, to provide your customer ID checksum (CCID). **sudo /Applications/Falcon.app/Contents/Resources/falconctl license <Your CID>**
6. Approve the Kernel Extension:
7. Grant Full Disk Access (Catalina/Mojave Only):

Linux

The following highlights how to manually install the CrowdStrike Falcon Agent for Linux hosts.

1. Download the Falcon sensor installer from **Hosts > Sensor Downloads.**
2. Copy your Customer ID Checksum (CID), displayed on Sensor Downloads.
3. Run the installer, substituting <installer_package> with your installer's file name.
    a. **Ubuntu:** sudo dpkg -i <installer_package>
    b. **RHEL**, **CentOS, Amazon Linux**: sudo yum install <installer_package>
    c. **SLES**: sudo zypper install <installer_package>
4. Set your CID on the sensor, substituting <CID> with <**your CID**> (found under Sendor Downloads). This step is not required for versions 4.0 and earlier.
    a. All OSes: **sudo /opt/CrowdStrike/falconctl -s --cid=<your CID>**

5. Start the sensor manually. This step is not required for versions 4.0 and earlier.
    a. Hosts with SysVinit: **service falcon-sensor start**
    b. Hosts with Systemd: **systemctl start falcon-sensor**
6. Confirm the sensor is running.
    a. **All OSes: ps -e | grep falcon-sensor**
7. You'll see output similar to this:

```
[root@centos6-installtest ~]# sudo ps -e | grep falcon-sensor   905 ?        00:00:02 falcon-sensor
```

UNINSTALLING THE CROWDSTRIKE SENSOR

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.

Uninstall from the Command Line

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

You can include `/quiet` (for silent uninstallation) parameters: `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

Uninstalling the Falcon Sensor for Mac

Sensor version 5.10.9003 and later

Move the host to a sensor update policy with Uninstall and maintenance protection turned off, then uninstall the sensor. For more info, read our Groups and Policies Guide.

Run this command at a command line:

- With Uninstall and maintenance protection disabled
  Sudo /Applications/Falcon.app/Contents/Resources/falconctl uninstall
  - With Uninstall and maintenance protection enabled:
  sudo /Applications/Falcon.app/Contents/Resources/falconctl uninstall --maintenance-token

- ○ If the sensor is offline and Uninstall and maintenance protection is enabled, use the Reveal Maintenance Token button on the Host Management page to get the single-use token required to uninstall the sensor. Enter this token when prompted by falconctl. ○ If the sensor is offline and Bulk Maintenance Mode is enabled, reveal the bulk maintenance token within the policy. Enter this token when prompted by falconctl.

Uninstalling the Falcon Sensor for Linux

Run these commands to uninstall the Falcon sensor from your Linux host:

1. **Ubuntu**: sudo apt-get purge falcon-sensor
2. **RHEL, CentOS, Amazon Linux**: sudo yum remove falcon-sensor
3. **SLES**: sudo zypper remove falcon-sensor

SUPPORTED OS VERSIONS

Please find an attachment with all the supported Operating systems.

For up-to-date list of supported Operating Systems and other FAQs, please visit:
https://www.crowdstrike.com/endpoint-security-products/crowdstrike-falcon-faq/

OTHER AV EXCLUSIONS

In every security agent you have installed (Windows Defender / other Anti-Virus, other EDR, CyberArk, Minerva, Ant-Exploit, Deception, DLP, Web Filtering, CASB agent etc.)

Whitelist/exclude these directories:

%ProgramFiles%\CrowdStrike*.*

%windir%\system32\windows\Crowdstrike

%windir%\system32\drivers\Crowdstrike

Exclusion Scan on Real time the services:

%ProgramFiles%\CrowdStrike\CSCOMUtils.exe

%ProgramFiles%\CrowdStrike\CSDeviceControlSupportTool.exe

%ProgramFiles%\CrowdStrike\CSFalconContainer.exe

%ProgramFiles%\CrowdStrike\CSFalconController.exe

%ProgramFiles%\CrowdStrike\CSFalconService.exe

%ProgramFiles%\CrowdStrike\CSFirmwareAnalysisSupportTool.exe

%ProgramFiles%\CrowdStrike*.*

%windir%\System32\drivers\CrowdStrike*.*

%windir%\System32\Drivers\CrowdStrike\Quarantine*.*

%windir%\System32\Drivers\CrowdStrike\Downloads*.*