Using CSWinDiag (v1.8) for Falcon Sensor for Windows Diagnostics
How to grab a CSWinDiag collection (used to help diagnose common issues).
Release Date: July 2022
Name: cswindiag.exe
SHA256: d8d1dc4096b969a770e19ebeeecb70f44656bb2ab7f4daa5f4377d1143937791

Details
CrowdStrike Support will often ask for a CSWinDiag collection on your Windows host when having an issue with the Falcon sensor. CSWinDiag gathers information about the state of the Windows host as well as log files and packages them up into an archive file which you can send to Support.

What CSWinDiag Gathers
- Troubleshooting Windows Sensors - Installation Issues:
  - Sensor installation logs from %TEMP% (aka %LOCALAPPDATA%\temp)
  - Sensor cloud update logs from %SYSTEMROOT%\temp
  - Sensor crash dump files if present in %SYSTEMROOT%\system32\drivers\crowdstrike\support\crashdumps
  - Log files from %SYSTEMROOT%\INF\setupapi*.log
  - Windows installer configuration, registration data, and installer cached files list
  - Firewall events, firewall rules, filter, and Device Control troubleshooting data
  - CrowdStrike registry keys
- Microsoft system, NIC, and hot fix details
- Currently installed programs and registered AV programs
- DigiCert certificates checks
- DNS Cache Type check
- .NET Framework version and registry data
- BitLocker encryption status
- Windows ELAM (Early Launch Anti-Malware) backup directory check
- Windows Installer directory check
- Core service dependencies status
- Basic network details
- Connectivity checks/configuration data (Commercial, Gov, and EU Clouds):
  - Basic cloud connectivity check
  - TLS connection tests
  - Certificate chain check
  - Supported ciphers check
  - User's proxy settings
  - Falcon Sensor proxy configuration

    - SCHANNEL registry configuration
- CID and AID details
- Falcon sensor and related services start configuration and status
- CS program and driver files list
- CS policy/system registry tags
- Currently running processes, AUMD and ScriptControl loaded modules data
- Installed Microsoft patches
- Running services details
- Windows Event logs errors: Application and System
- Falcon Sensor Event logs (if logging is enabled)
- MSInfo32 data export

Using CSWinDiag to Create a Collection

- Triggering a CSWinDiag collection by Double-Clicking:
    - Download the attached ZIP file and unzip it. Unzip to a directory located in in %PROGRAMFILES% (i.e. C:\Program Files\AdminTools or similar).
    - Change to the directory where the unzipped EXE was placed.
    - Double-click the cswindiag.exe executable.
      Note: CSWinDiag must be run from a folder located in %PROGRAMFILES%.
    - If prompted, enter local administrator credentials.
    - If prompted to allow the program to make changes to the computer, click YES.
      (Note: The program does not install or make any system changes. It only collects host information).

    Wait 3-4 minutes (average) for collection to complete.

- Triggering a CSWinDiag collection from Command Line:
    - Download the attached ZIP file and unzip it. Unzip to a directory located in in %PROGRAMFILES% (i.e. C:\Program Files\AdminTools or similar).
    - Open a command line prompt as administrator.
    - Change to the directory where the unzipped EXE was placed
    - Type cswindiag, then press <Enter>
      Note: CSWinDiag must be run from a folder located in %PROGRAMFILES%.
    - If prompted to allow the program to make changes to the computer, click YES.
      (Note: The program does not install or make any system changes. It only collects host information).
    - Wait 3-4 minutes (average) for collection to complete.

- Either way you choose to trigger the CSWinDiag collection, the process averages 3-4 minutes to complete. Once finished, the program will display output similar to the following:

```
C:\Program Files\AdminTools>cswindiag

CSWinDiag v1.8 collection progress (avg. 3-4 minutes):
 - basic host details.....(done)
 - network connectivity tests.....(done)
 - additional host details.....(done)
 - Windows errors/warnings.....(done)
 - msinfo32 data.....(done)
 - sensor and windows logs.....(done)
 - finalizing collection.....(done)

Falcon sensor diagnostics are complete.

Please review and/or send this file to CrowdStrike Support: C:\Program
Files\AdminTools\CSWinDiag-<hostname>-mRRfqs8F.zip

C:\Program Files\AdminTools>
```

Using CSWinDiag via RTR to Create a Collection

Once connected to a host running a supported 6.x sensor, Falcon Administrators may issue the built-in RTR command "cswindiag". Detailed instructions and video demonstration are available on the Support Portal.

Securely Sending the CSWinDiag Collection File to Support

For your security and privacy, **we strongly advise you to never e-mail these collections to Support** (by either opening a case via email-to-case, or by email-replying to a case with email attachment). We do recommend attaching directly to your case as outlined below, or using another secure file sending method outlined in the last bullet-point if necessary.

Here are the steps and methods we *do* endorse for securely delivering these files to us:

- If you already have an open case, find your open case under **CASES** here in the Support Portal.
- If you have not opened a Support case yet, open a Support case by clicking the Create New Case button in the Support Portal.
- Attach the file to your case there, and update the case to notify your assigned agent that you have completed the collection gathering.
- For more information on getting files to Support, please see the KB article, "Sending Large File Attachments to Support".

Contacting Support

If you have any questions about this topic beyond what is covered here, or this article (and others) do not resolve your issue, you may open a Support case by clicking the Create New Case button in the Support Portal, or by emailing support@crowdstrike.com.

Alternatively, you may also seek help from other Customers by participating in the **Discussion Board**, and you can learn more about this in the Discussions Board Guide.