Configure Process Crash Dump Collection for sfc.exe on Windows

Contents

Introduction

Prerequisites

Issue

- Download and prepare environment
- Automatic collection
- Uninstall the Automatic Debugger
- Manual collection

Crash dump folder compression

- Use CLI (Command Line Interface)
- Use GUI (Graphical User Interface)

Introduction

This document describes how to collect crash dumps on Windows for the sfc.exe process.

Environment

Platform: Windows endpoint

Product: Cisco Secure Endpoint connector

Tools: Windows Command Prompt; Microsoft Sysinternals ProcDump (procdump64.exe)

Assumed knowledge:

- Cisco Secure Endpoint connector
- Windows Command Prompt

This document is not restricted to software and hardware versions. The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Review the potential impact of any command before use on a live network.

Cause

- sfc.exe crashes can leave the Cisco Secure Endpoint application in a disabled or disconnected state.
- Windows can invoke a postmortem debugger configured through the AeDebug registry values; ProcDump can be registered as that debugger to capture crash dumps.

Issue

- Cisco Secure Endpoint can enter a disabled or disconnected state if sfc.exe crashes. This can occur after an unexpected Windows shutdown or other Windows activity.
- Windows activates a debugging tool configured in the AeDebug (Application Error Debug) registry values. In this scenario, a program can be pre-selected as the tool to use, which is referred to as the postmortem debugger.

Resolution

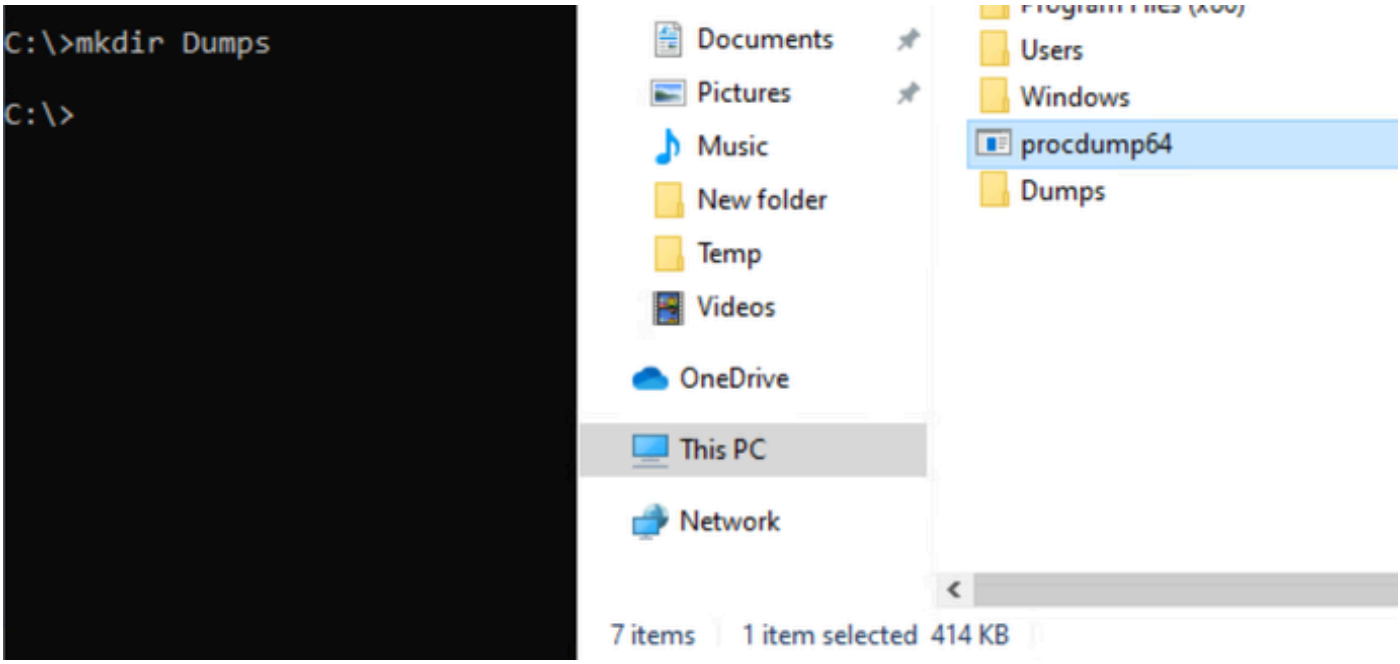
Before you begin

1. Confirm administrative access on the Windows endpoint.
2. Confirm **C:\Dumps** exists (or can be created) and that the account running ProcDump has write access to the folder.
3. Decide whether automatic collection (postmortem debugger registration) or manual collection (on-demand dump) is required.

Download and prepare environment

1. Download Procdump (to be used as the AeDebug postmortem debugger) from Sysinternals Suite.

2. Extract **procdump64.exe** to the **C:** drive and create the **Dumps** folder for crash dump collection.

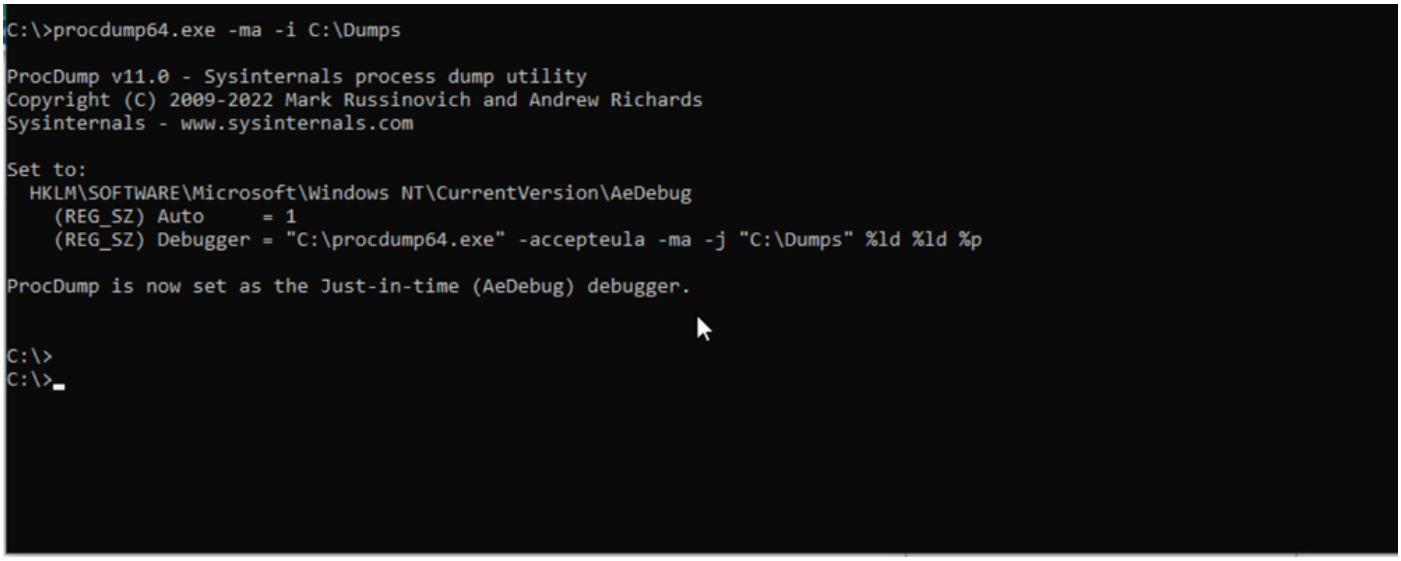


Note: ProcDump (procdump64.exe) supports two dump-collection methods: automatic collection (register ProcDump as the postmortem debugger and specify an output folder) and manual collection (trigger a dump for a specific process ID or process name).

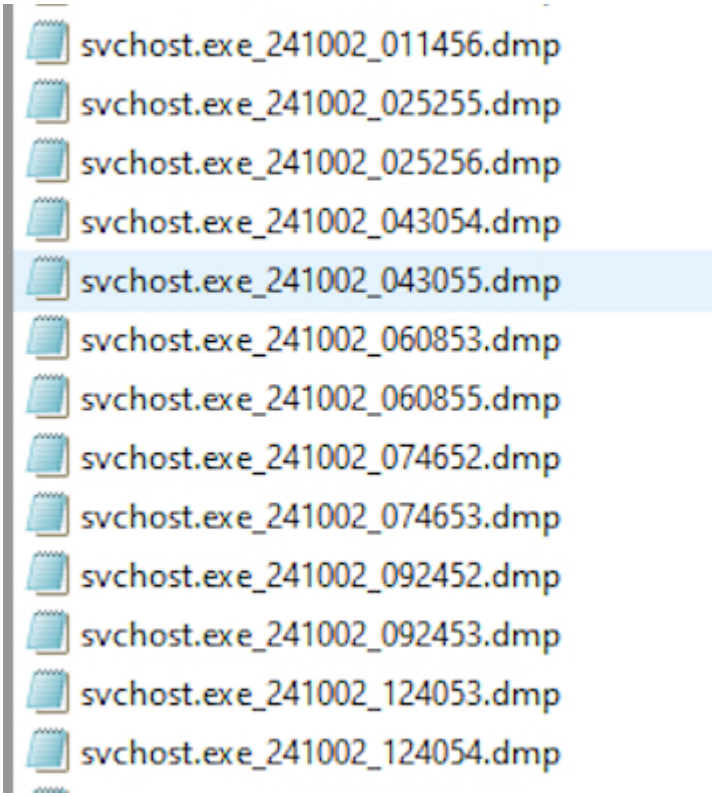
Automatic collection

1. Set **procdump64.exe** as the automatic debugger in the Windows postmortem debugging registry configuration (AeDebug) with this command. When a program crashes, ProcDump saves the crash dump in the specified folder.

```
procdump64.exe -ma -i C:\Dumps
```



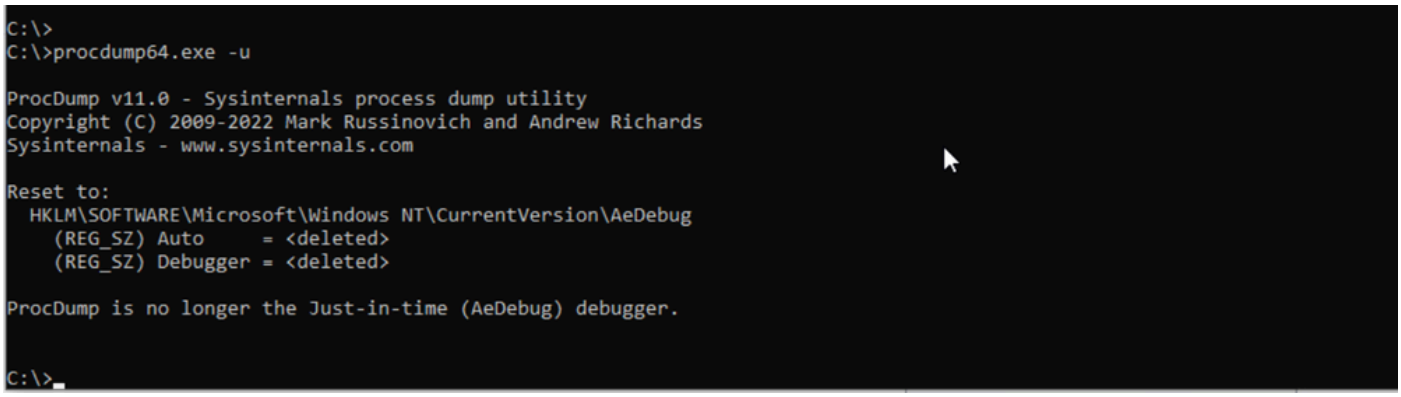
2. Navigate to the **C:\Dumps** folder. Zip it and share it for analysis.



Uninstall the Automatic Debugger

1. To uninstall **procdump64.exe**, use this command.

```
procdump64.exe -u
```



Manual collection

1. Use this command to create a dump on demand.

```
procdump64.exe -accepteula -ma -e -x c:\Dumps <PID | Process Name>
```

Example for sfc.exe.

```
procdump64.exe -accepteula -ma -e -x c:\Dumps "%ProgramFiles%\Cisco\AMP\8.6.1.30582\sfc.exe"
```

2. Navigate to the **C:\Dumps** folder. Zip it and share it for analysis.

Crash dump folder compression

Crash dumps can occupy a significant amount of disk space, so it is important to stop procdump once the collection is complete. You can also use the workaround to compress the size of the folder.

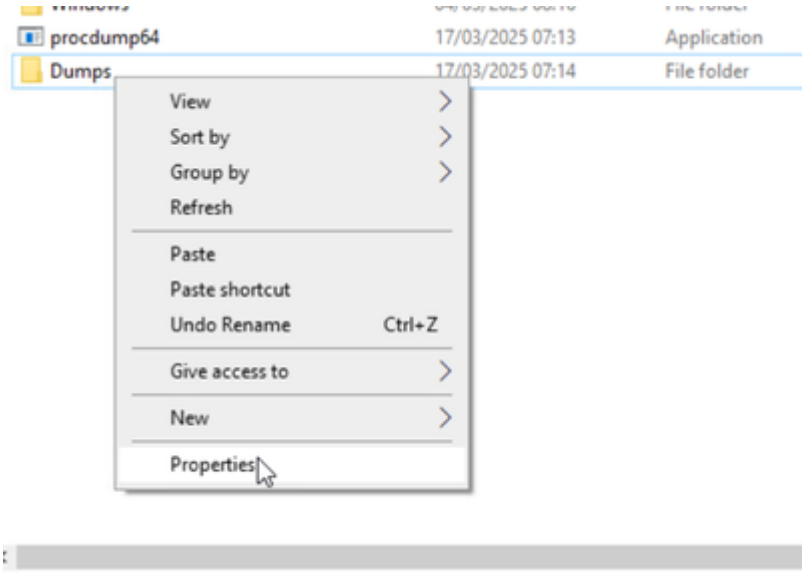
Use CLI (Command Line Interface)

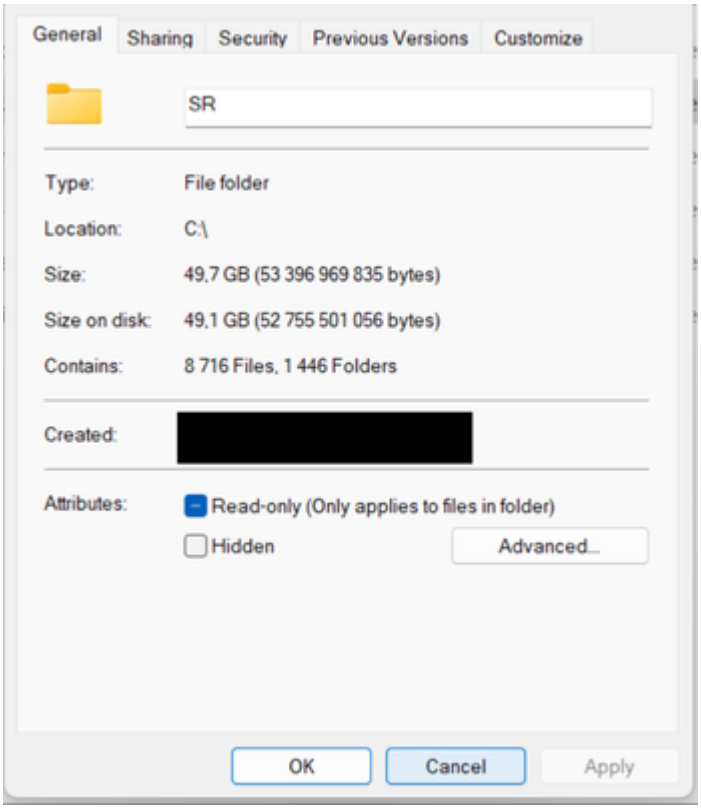
Use this command in the command prompt to enable compression.

```
compact /c /s:c:\Dumps
```

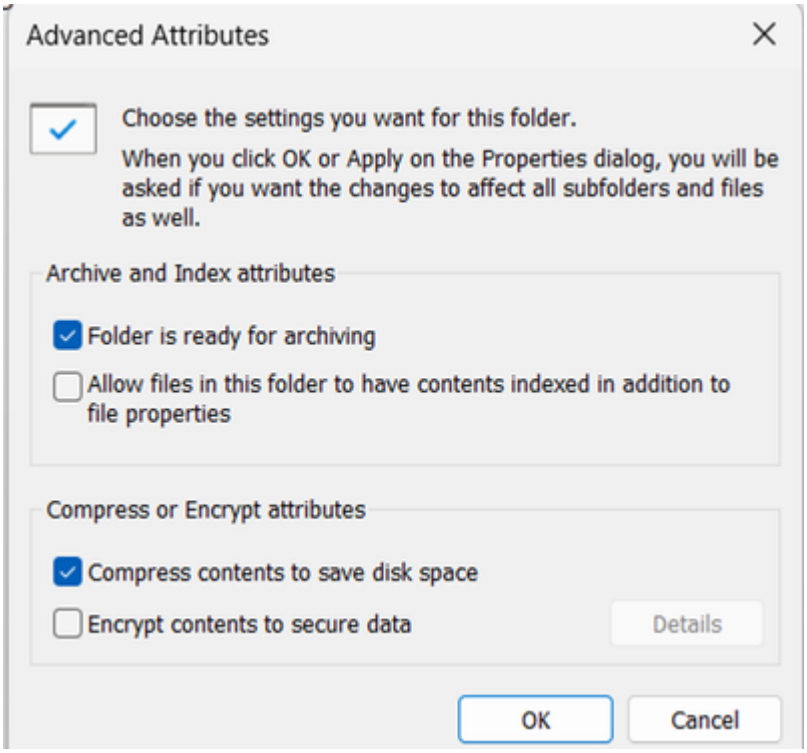
Use GUI (Graphical User Interface)

1. Navigate to **Properties** for the **Dumps** folder and check the **original size** of the folder on disk.

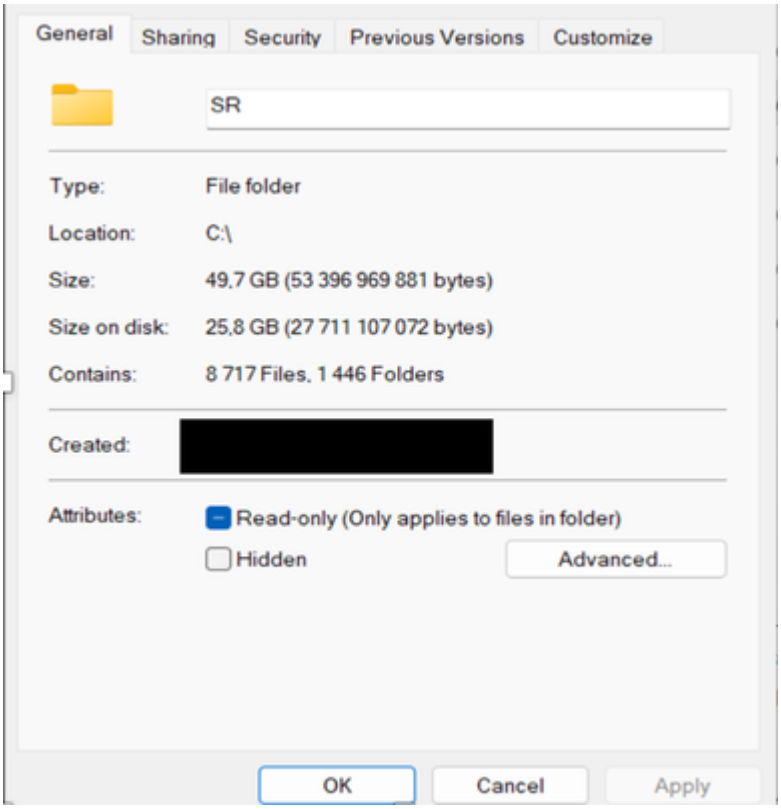




2. In **Properties**, click **Advanced**, select **Compress contents to save disk space**, and click **OK** to apply the change. This process can take several minutes.



3. In the end, you can observe that the folder size has significantly reduced, almost reaching half of its original size.


General
Sharing
Security
Previous Versions
Customize
SR
Type:
File folder
Location:
C:\
Size:
49,7 GB (53 396 969 881 bytes)
Size on disk:
25,8 GB (27 711 107 072 bytes)
Contains:
8 717 Files, 1 446 Folders
Created:
Attributes:
Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply