Troubleshoot Debug Log Collection in Secure Endpoint for Windows Devices

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Collect Debug Log Files in Cisco Secure Endpoint for Windows

- Version 7.5.5 and earlier
- Version 8.0.1 and later (Cisco Secure Client)

Related Content

Introduction

This document describes how to generate a Debug Bundle file from Cisco Secure Endpoint Connector on Windows.

Prerequisites

Requirements

Required knowledge: Cisco Secure Endpoint Connector.

Components Used

The information in this document applies to:

- Microsoft Windows
- Cisco Secure Endpoint Connector for Windows:
  - Version 7.x.x and later (procedure in **Version 7.5.5 and later**)
  - Version 8.x.x and later (Cisco Secure Client; procedure in **Version 8.0.1 and later (Cisco Secure Client)**)

Note: Versions 7.5.6 through 8.0.0 are not covered in this document. If these versions are in use, confirm the correct workflow in the product documentation or with Cisco TAC.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

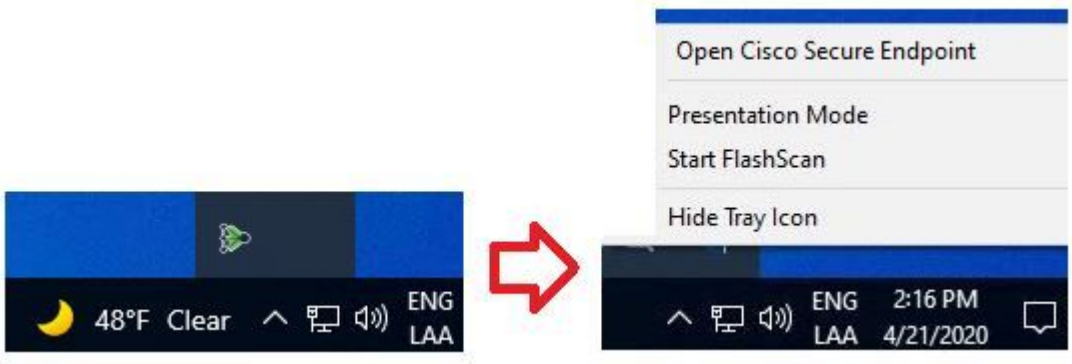
For performance issues with Cisco Secure Endpoint Connector on the Microsoft Windows operating system, contact the Cisco Technical Assistance Center (TAC). A Cisco Technical Support Engineer analyzes the logs available in the Debug Bundle file in order to identify the root cause.

Note: If Debug mode is enabled from the tray icon menu, Debug mode does not persist after a reboot. To preserve the setting across a reboot, enable Debug mode from the policy configuration in the Secure Endpoint console.

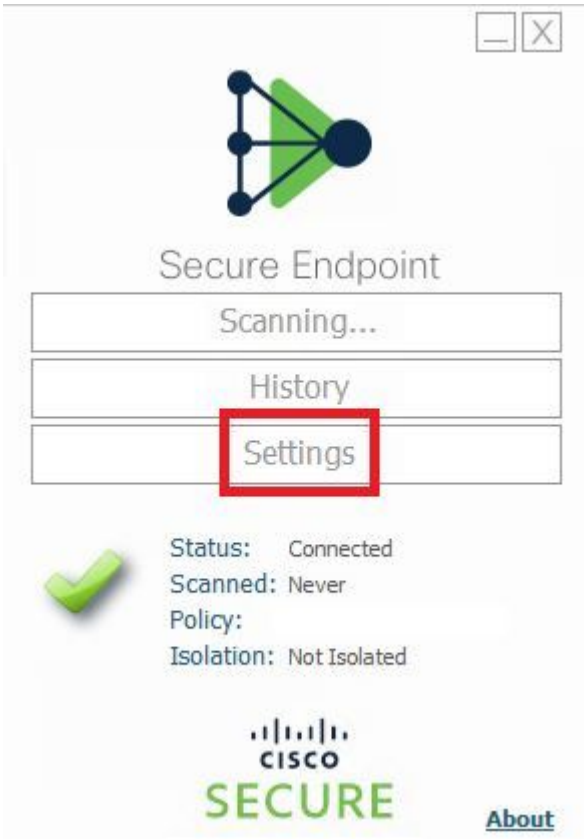
Collect Debug Log Files in Cisco Secure Endpoint for Windows

Version 7.5.5 and earlier

Step 1. Click the **Cisco Secure Endpoint tray icon** on the taskbar, and then click **Open Cisco Secure Endpoint**, as shown in the image.



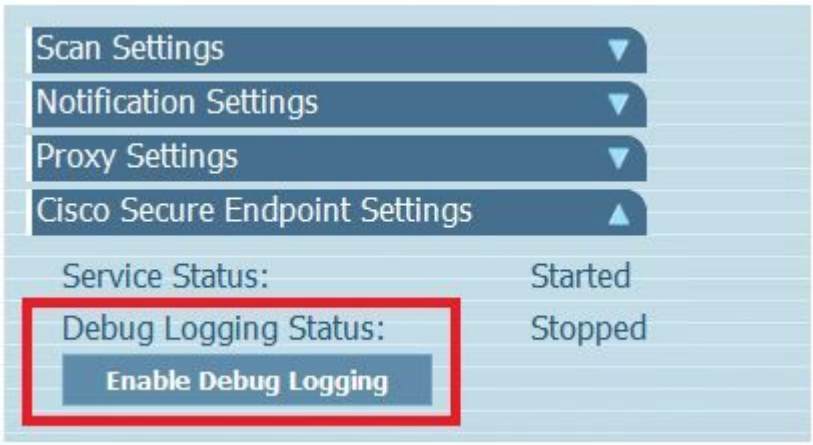
Step 2. Click **Settings** in Secure Endpoint Connector, as shown in the image.



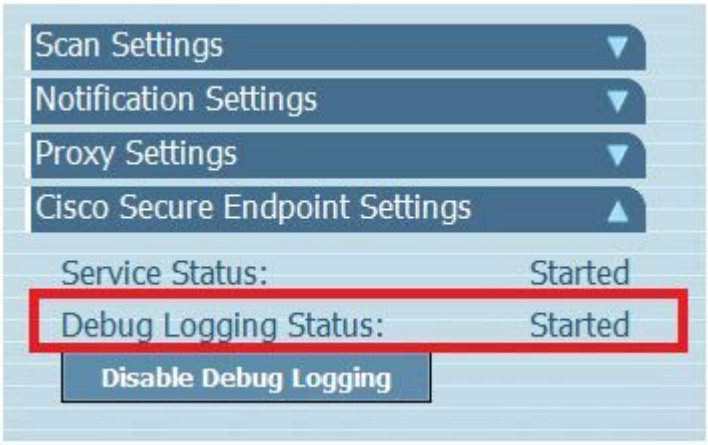
Step 3. Choose **Settings** > **Cisco Secure Endpoint Connector Settings**, as shown in the image.



Step 4. Click **Enable Debug Logging**, as shown in the image.

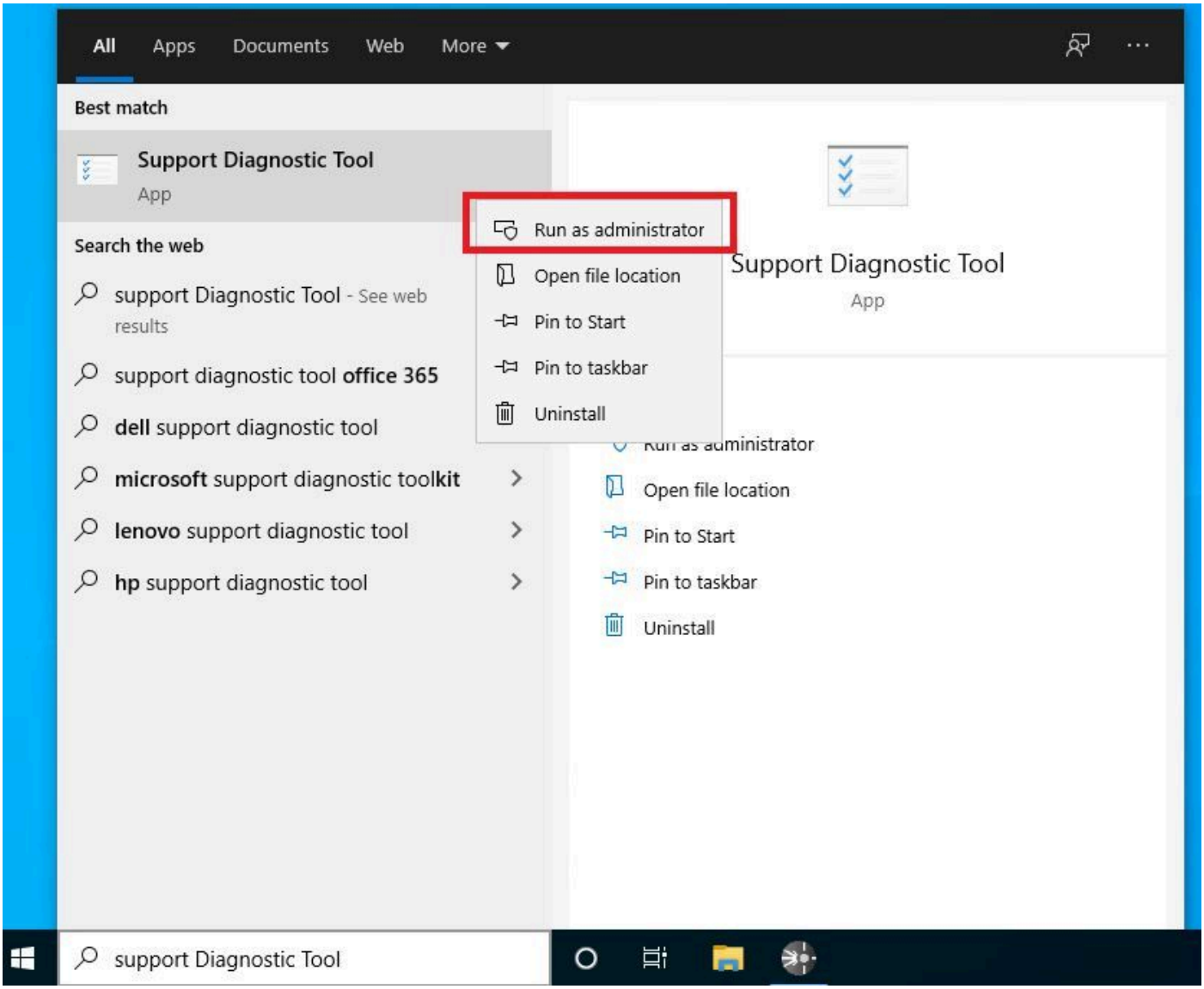


Step 5. The button name changes to **Disable Debug Logging**. Debug mode is now enabled, as shown in the image.



Step 6. Recreate the issue and let the device run for at least 30 minutes.

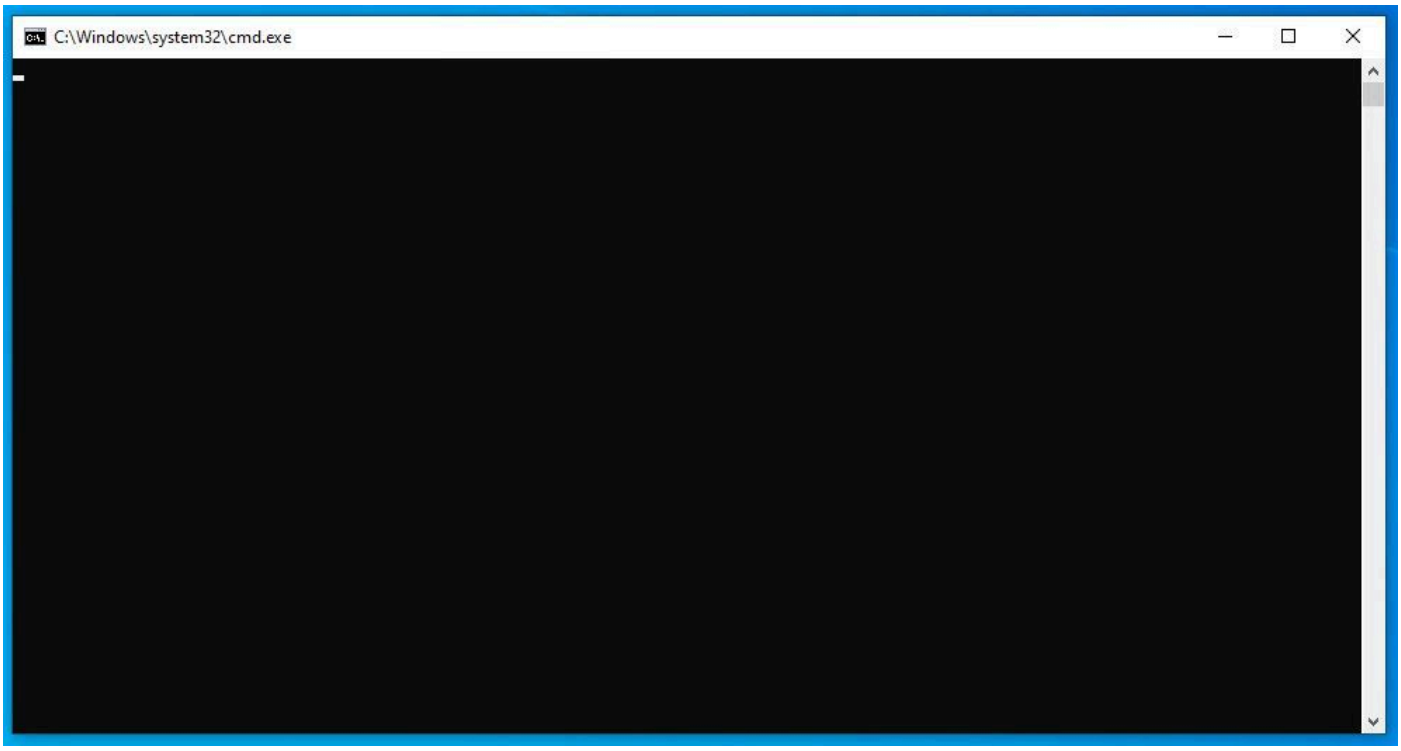
Step 7. After 30 minutes, open Windows Search and type **Support Diagnostic Tool**. Run the tool with **Administrator** privileges, as shown in the image.



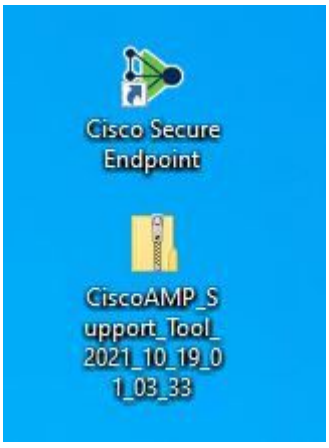
Note: Starting with Secure Endpoint Connector version 7.5.5, a Windows account with administrator privileges is not required to open the Support Diagnostic Tool in order to collect the debug logs. Release Notes: "Updated support diagnostic tool so that it does not require elevated privileges".

Step 8. A temporary Windows black screen appears, as shown in the image.

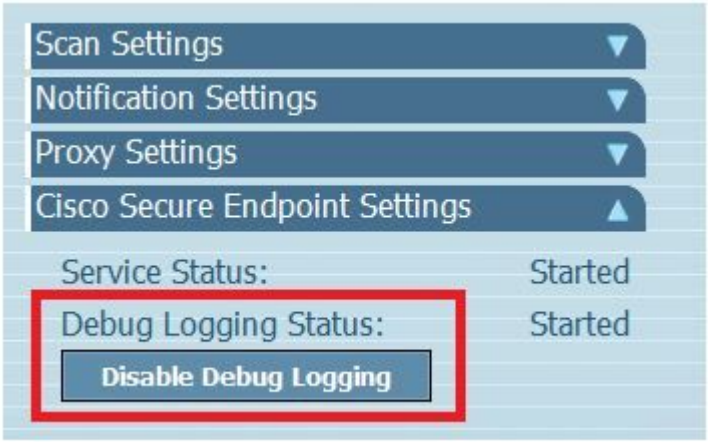
Note: Wait a few seconds for the black window to close automatically.



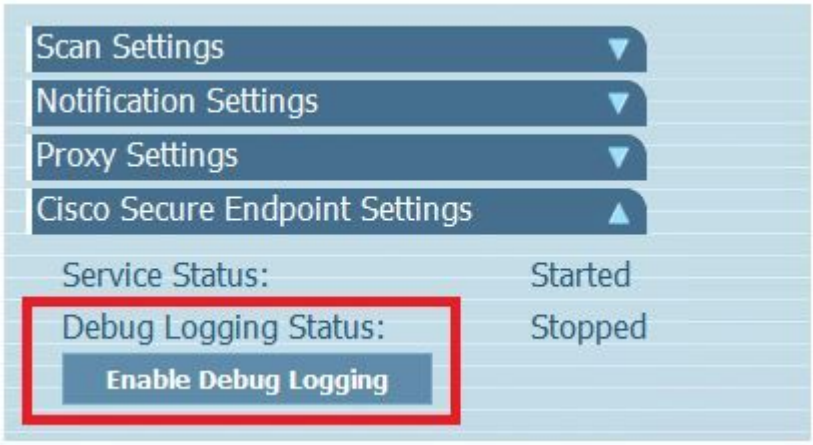
Step 9. After a few minutes, the Debug Bundle file appears on the desktop, as shown in the image.



Step 10. Once the Debug Bundle file is generated, Debug mode can be disabled. Select the **Disable Debug Logging** button, as shown in the image.



Step 11. The button name changes to **Enable Debug Logging**, as shown in the image.



Note: Debug mode must be enabled only to collect the Debug Bundle file. Enabling Debug mode for a longer time can fill up the disk space.

Step 12. Once the Debug Bundle file is collected, upload it to My Case in Cloud Apps.

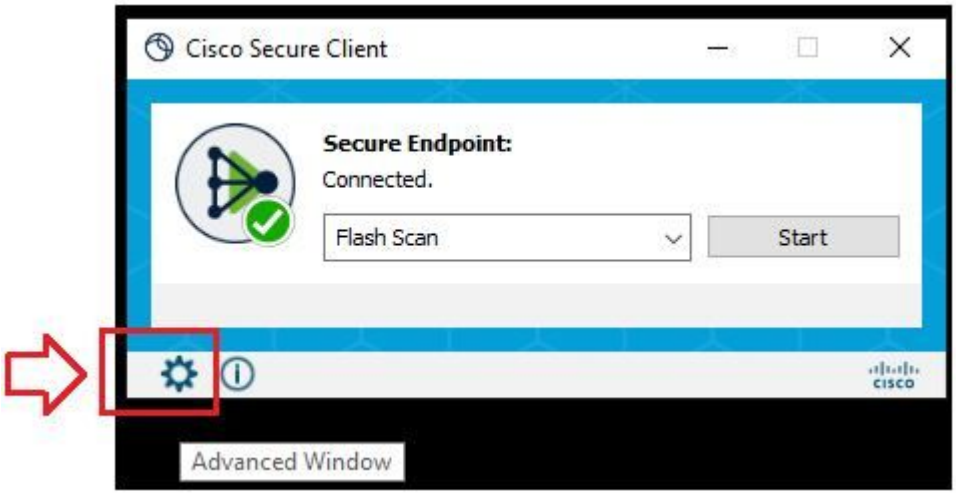
Note: Ensure that you reference the Service Request number.

Version 8.0.1 and later (Cisco Secure Client)

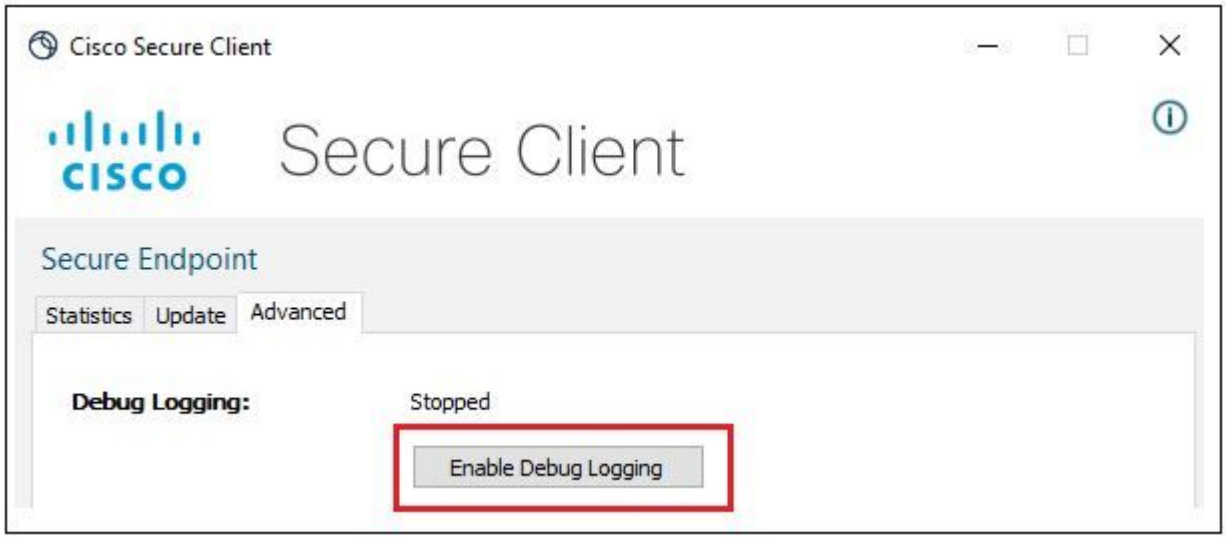
Step 1. Click the **Cisco Secure Endpoint tray icon** on the taskbar, as shown in the image.



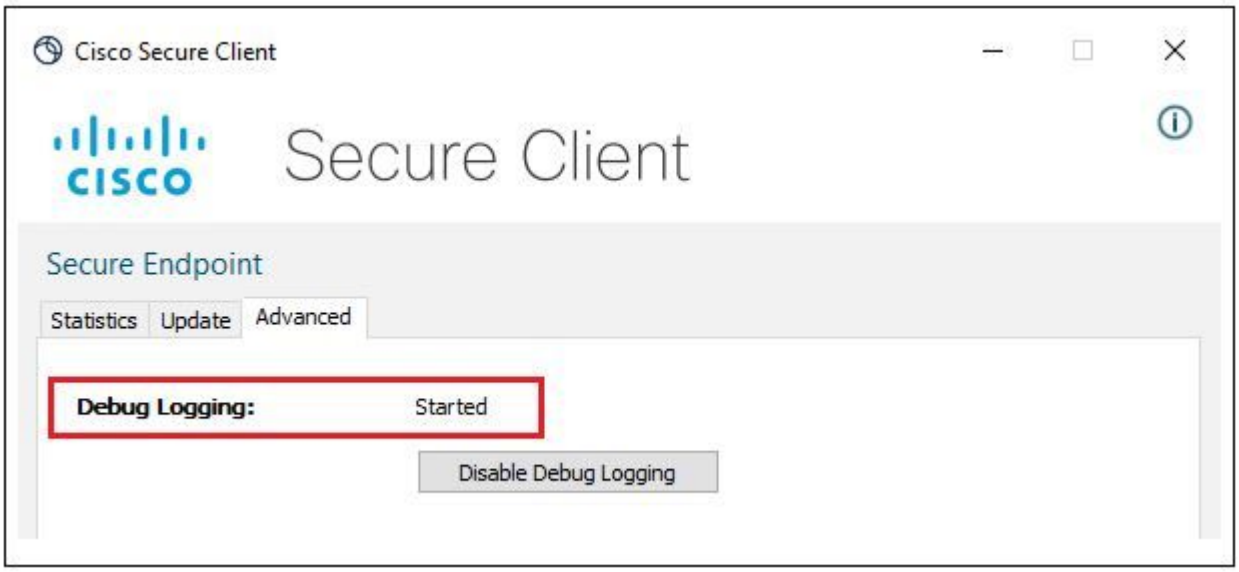
Step 2. Click **Advanced Window** from the tray icon menu in Secure Endpoint Connector, as shown in the image.



Step 3. Click the **Advanced** tab, and then click **Enable Debug Logging**, as shown in the image.



Step 4. The debug logging button name changes to **Started**. Debug mode is now enabled, as shown in the image.

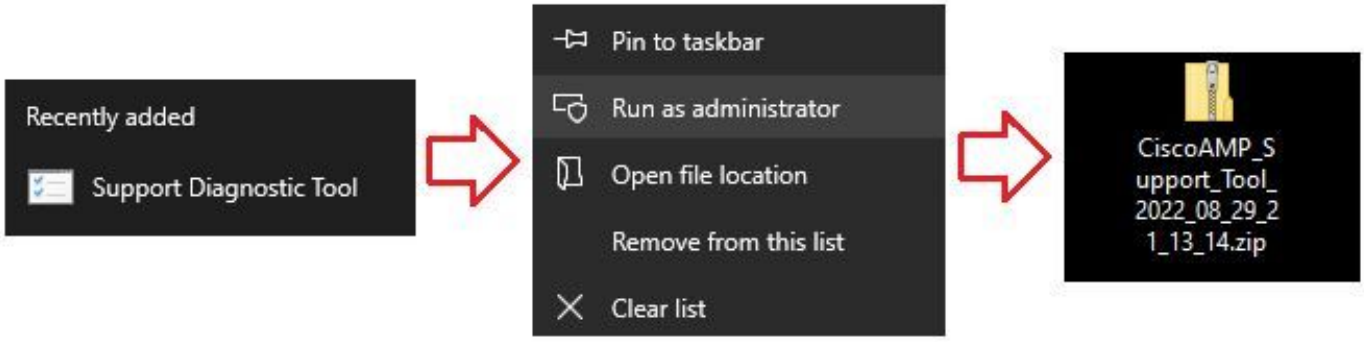


Step 5. Recreate the issue and let the device run for at least 30 minutes.

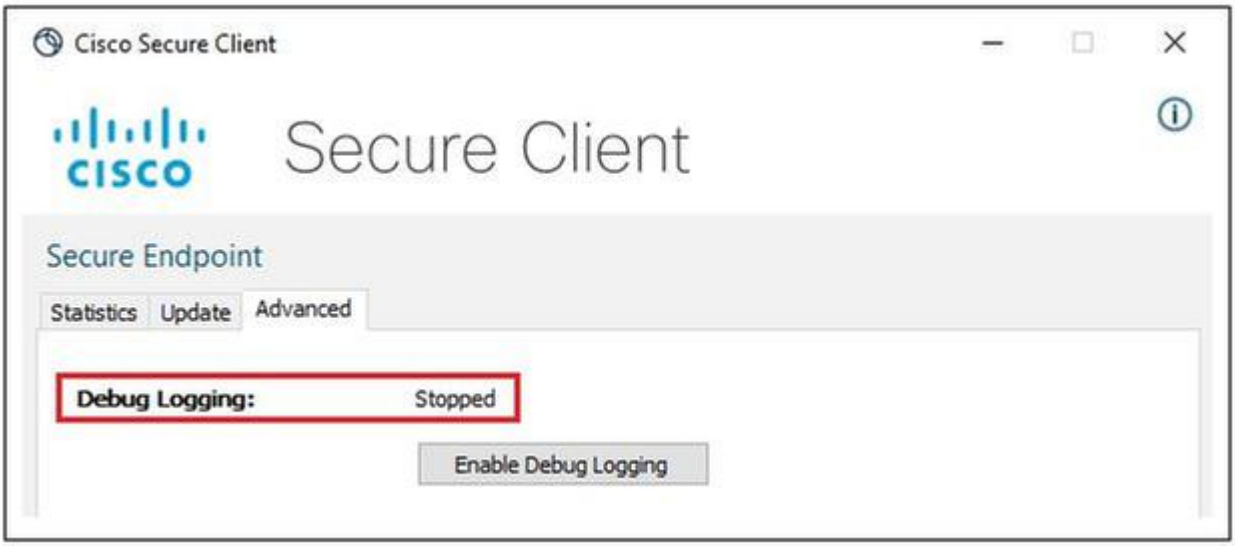
Step 6. Open Windows Search and enter **Support Diagnostic Tool**.

Step 7. Click **Support Diagnostic Tool**, and then run it with **Administrator** privileges.

Step 8. After a few minutes, confirm that the **Debug Bundle** file appears on the desktop, as shown in the image.



Step 9. Once the Debug Bundle file is generated, Debug mode can be disabled. Click **Disable Debug Logging**.



Note: Debug mode must be enabled only to collect the Debug Bundle file. Enabling Debug mode for a longer time can fill up the disk space.

Step 10. Once the Debug Bundle file is collected, upload it to My Case in Cloud Apps.

Note: Ensure that you reference the Service Request number.

Related Content

- Cisco Secure Endpoint Connector Release Notes
- Cisco Secure Endpoint Documentation
- My Case in Cloud Apps (upload files to a TAC service request)