Secure Endpoint Mac Connector Loses Full Disk Access Permission after macOS 13 Ventura Upgrade on non-MDM Managed Macs

Contents

Introduction

This document describes guidance to regain Full Disk Access (FDA) for a Secure Endpoint Mac connector that is not MDM managed on macOS Ventura 13.0.

Issue Description

On non-MDM-managed systems, Secure Endpoint Mac connector runs in degraded mode after an upgrade to macOS 13 Ventura 13.0.

Even though previously granted, Full Disk Access permission does not persist; in fact, the permission appears to be enabled in the Privacy and Security System Settings UI, but the system extension does not actually have the granted permission.

Affected Secure Endpoint Mac Connector version

Secure Endpoint Mac connector 1.14 or newer

Affected macOS version:

macOS 13.0 - Ventura

Note: this issue is fixed in macOS Ventura 13.1.

MDM Profiles

The issue does not affect MDM managed computers where Full Disk Access for Secure Endpoint connector is granted through MDM.

Resolution

Option 1: Upgrade to macOS Ventura 13.1

This problem is resolved in macOS Ventura 13.1. If the Secure Endpoint Mac connector is in a degraded mode on macOS Ventura 13.0, an upgrade to macOS Ventura 13.1 resolves the issue without any further action.
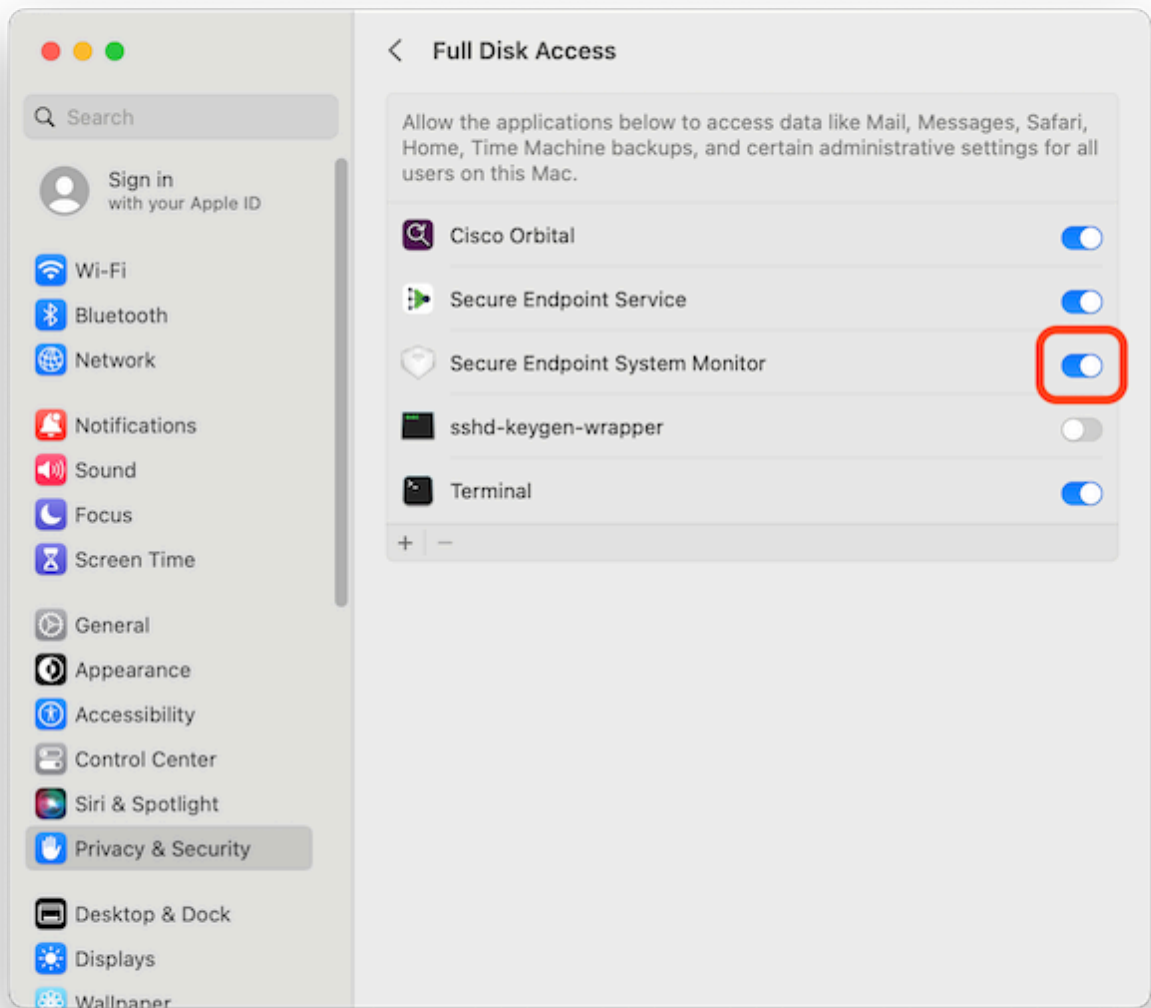
Option 2: Manually remove FDA for Secure Endpoint System Monitor
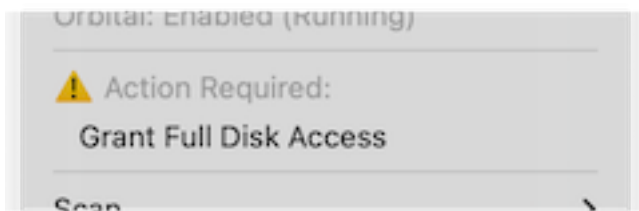
1. In the Secure Endpoint menu, click the **Grant Full Disk Access** warning to open the Full Disk Access page in System Settings. Alternatively, navigate to the Full Disk Access page manually in System Settings under Privacy & Security.
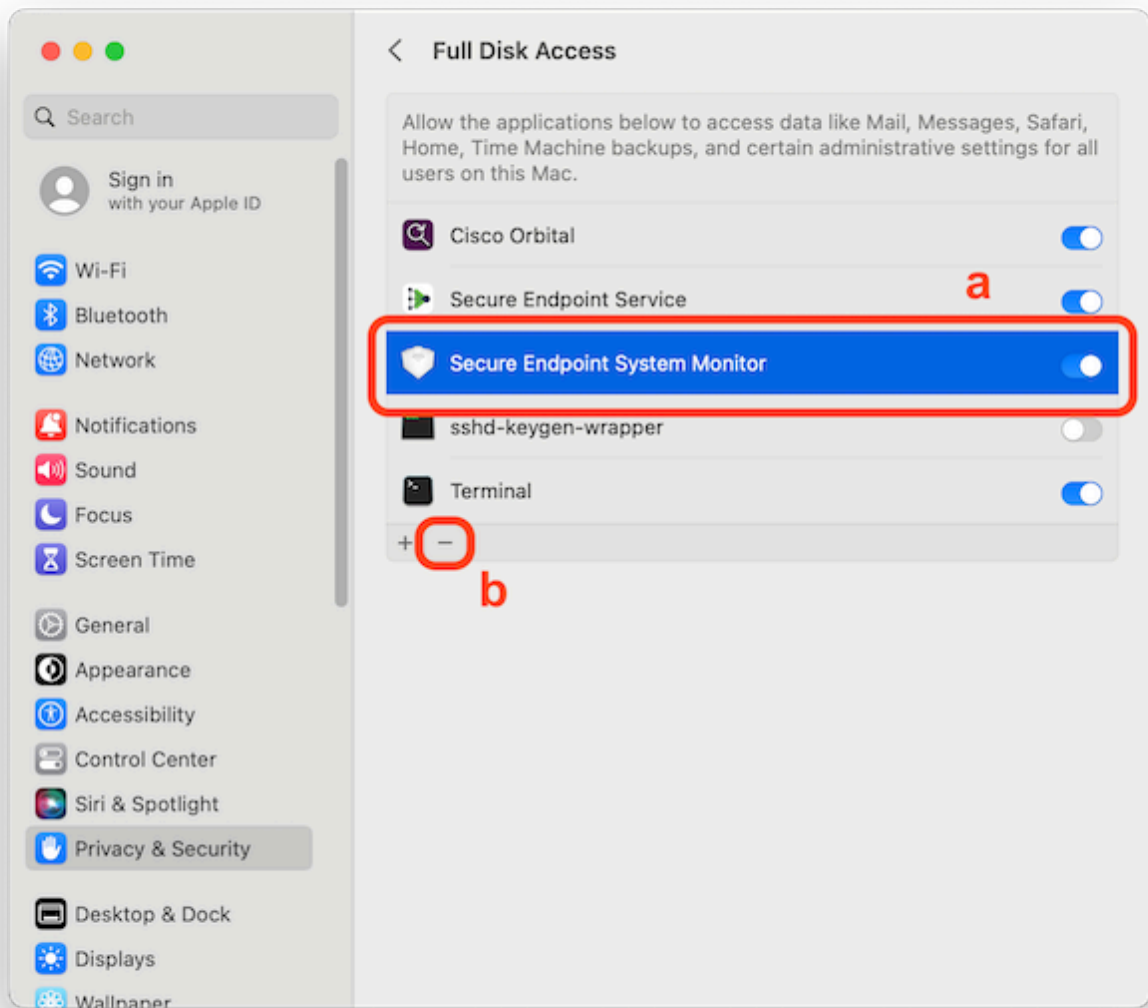
2. Remove the Secure Endpoint System Monitor bundle. To do so: a) Click on Secure Endpoint System Monitor to highlight it   b) Click the minus sign and enter the admin password if prompted   **Only remove the Secure Endpoint System Monitor bundle. Do not remove the Secure Endpoint Service bundle.**

3. Wait for the connector to automatically add the Secure Endpoint System Monitor back to the Full Disk Access page (this can take up to 30 seconds).
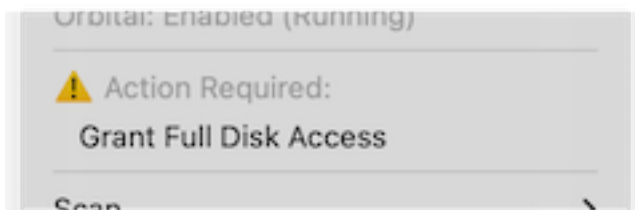
4. Click the toggle to enable Full Disk Access for the Secure Endpoint System Monitor.
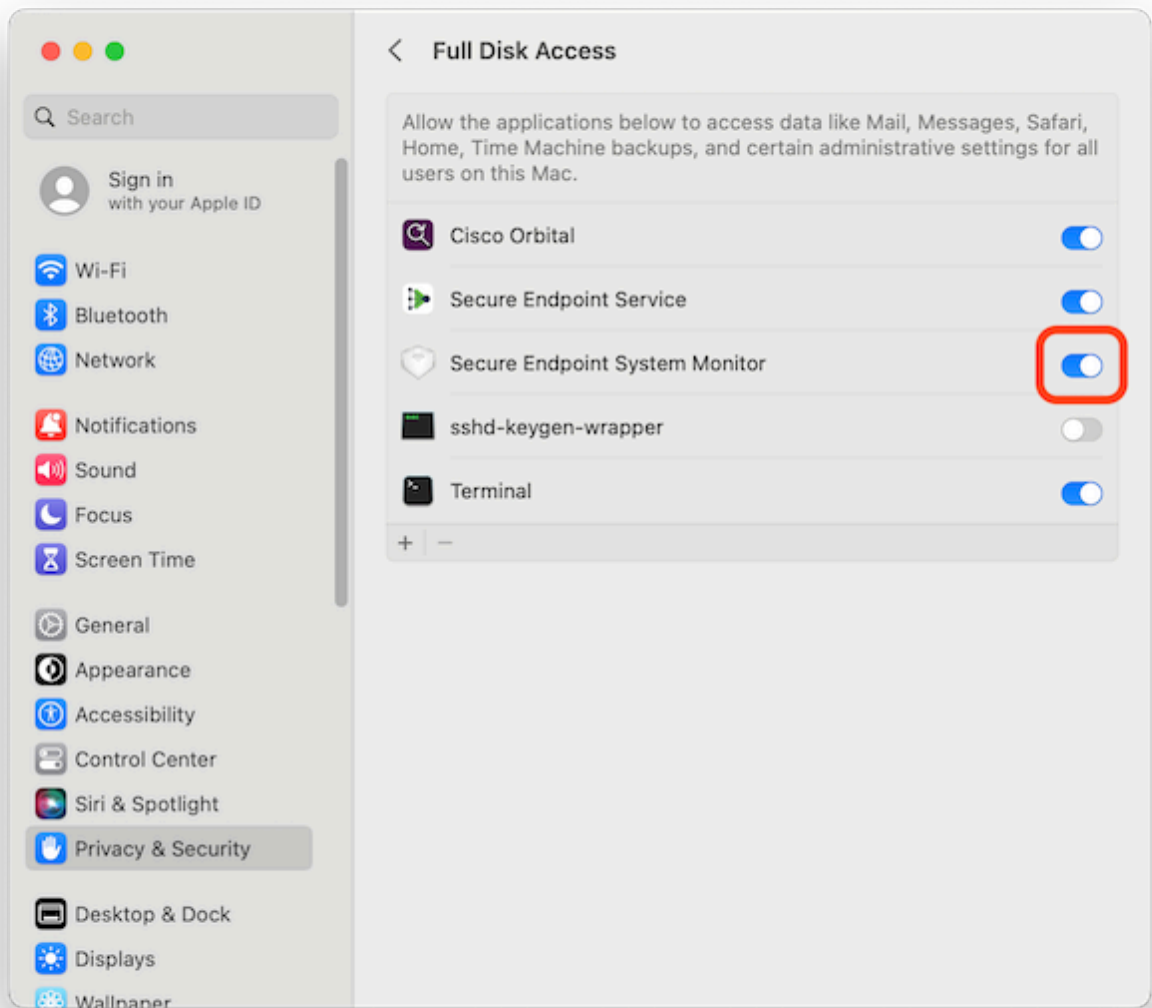
Option 3: Disable FDA for the Secure Endpoint System Monitor with the tccutil command

1. Open a terminal and enter this command and the admin password when prompted:
   ```
   sudo tccutil reset SystemPolicyAllFiles com.cisco.endpoint.svc.securityextension
   ```


2. In the Secure Endpoint menu, click the **Grant Full Disk Access** warning to open the Full Disk Access page in System Settings. Alternatively, navigate to the Full Disk Access page manually in System Settings under Privacy & Security.

3. Click the toggle to enable Full Disk Access for the Secure Endpoint System Monitor.