

Cisco Secure Endpoint Connector per la raccolta dei dati di diagnostica per Mac

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Generare un file di diagnostica con lo strumento di supporto](#)

[Avvia lo strumento di supporto utilizzando il Finder di macOS](#)

[Avvia lo strumento di supporto utilizzando il terminale macOS](#)

[Risoluzione dei problemi](#)

[Abilita modalità debug](#)

[Abilita modalità di debug heartbeat singolo](#)

[Disabilita modalità di debug](#)

Introduzione

Questo documento descrive il processo utilizzato per generare un file diagnostico tramite l'applicazione Support Tool disponibile sul connettore Cisco Secure Endpoint Mac e come risolvere i problemi di prestazioni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Connettore per Mac Secure Endpoint
- macOS

Componenti usati

Le informazioni fornite in questo documento si basano sul connettore Secure Endpoint Mac.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il connettore Secure Endpoint Mac comprende un'applicazione chiamata Strumento di supporto, che viene utilizzata per generare informazioni diagnostiche sul connettore installato sul Mac. I dati di diagnostica includono informazioni sul Mac quali:

- Utilizzo delle risorse (disco, CPU e memoria)
- registri specifici del connettore
- informazioni sulla configurazione del connettore

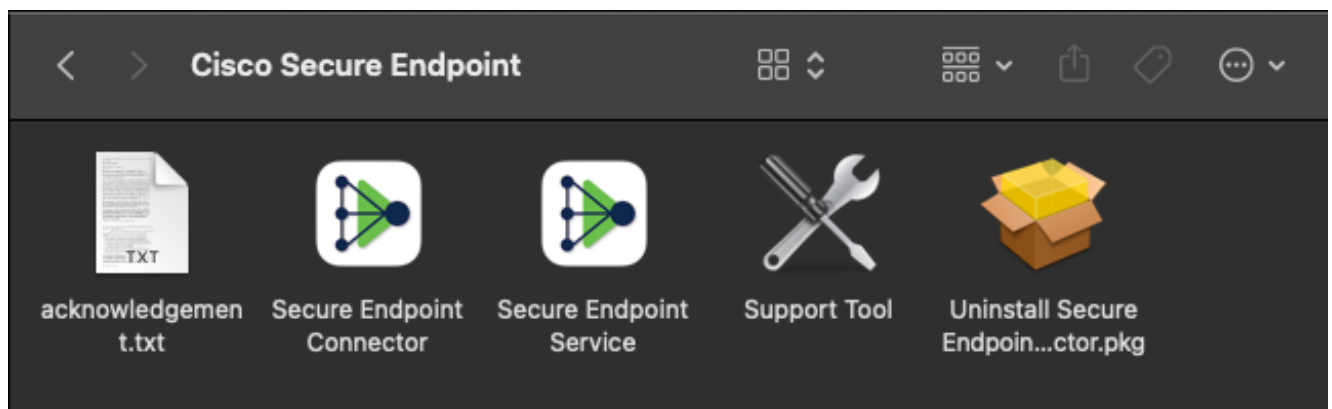
Generare un file di diagnostica con lo strumento di supporto

Questa sezione descrive come avviare l'applicazione Support Tool dalla GUI o dalla CLI per generare un file diagnostico.

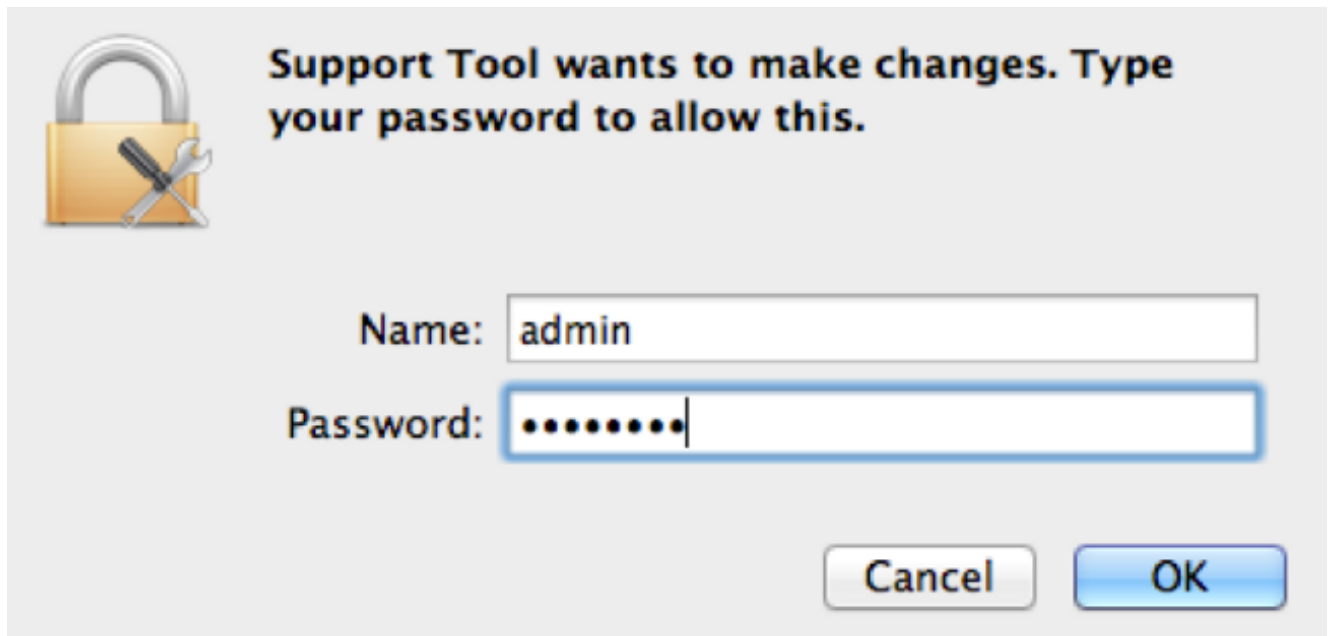
Avvia lo strumento di supporto utilizzando il Finder di macOS

Completare questi passaggi per avviare lo strumento di supporto del connettore Secure Endpoint Mac utilizzando il Finder macOS:

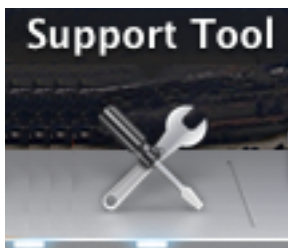
1. Passare alla directory Cisco Secure Endpoint nella cartella Applications e individuare l'utilità di avvio dello strumento di supporto:



2. Fare doppio clic sull'utilità di avvio dello strumento di supporto e vengono richieste le credenziali amministrative:

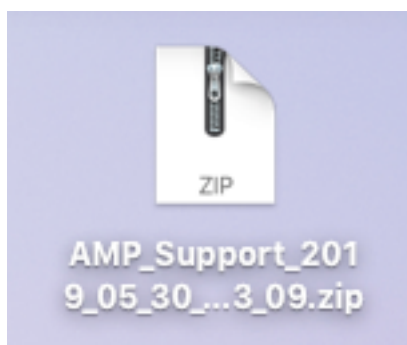


3. Dopo aver immesso le credenziali, l'icona dello strumento di supporto dovrebbe essere visualizzata nell'alloggiamento di espansione:

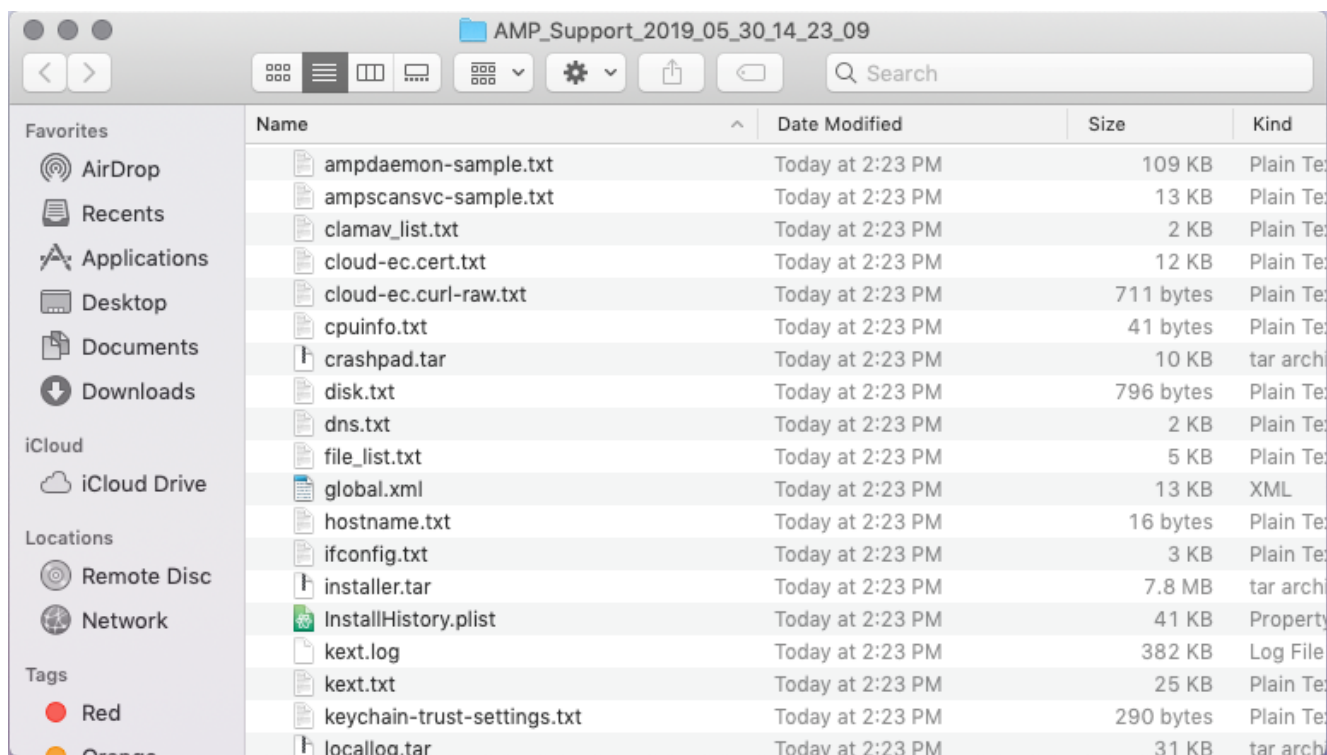


Nota: L'applicazione Support Tool viene eseguita in background e richiede del tempo (circa 20-30 minuti).

4. Al termine dell'applicazione dello strumento di supporto, viene generato un file che viene quindi posizionato sul desktop:



Di seguito è riportato un esempio di output non compresso:



5. Per analizzare i dati, fornire questo file al team di supporto tecnico Cisco.

Avvia lo strumento di supporto utilizzando il terminale macOS

Il pulsante di avvio dello strumento di supporto si trova nella seguente directory:

```
/Library/Application Support/Cisco/AMP for Endpoints Connector/
```

Per avviare lo strumento di supporto, immettere il seguente comando:

Nota: È necessario eseguire questo comando come root, quindi accertarsi di passare alla root o di anteporre il comando a **sudo**.

```
root@mac# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector root@mac#  
./SupportTool
```

Nota: Questo comando viene eseguito in modo dettagliato. Al termine, viene generato un file di diagnostica che viene quindi posizionato sul desktop.

Risoluzione dei problemi

In questa sezione viene descritto come abilitare e disabilitare la modalità di debug sul connettore Secure Endpoint Mac per risolvere i problemi di prestazioni.

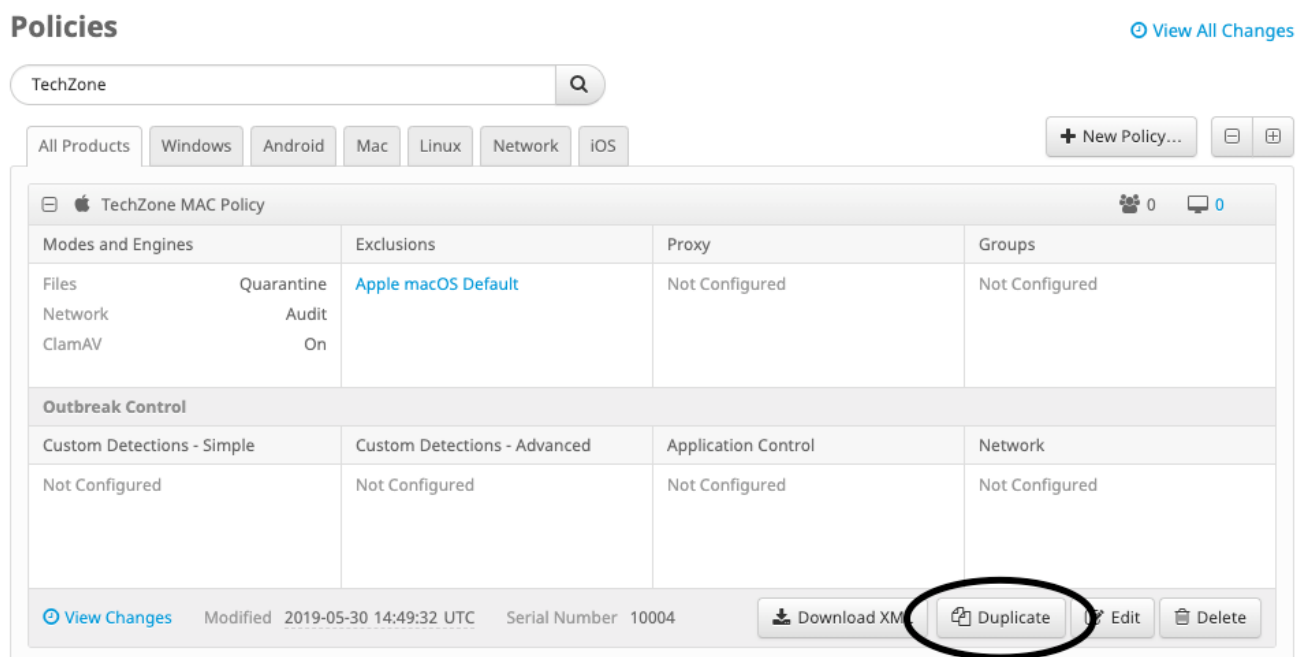
Abilita modalità debug

Avviso: la modalità di debug deve essere abilitata solo se un tecnico del supporto Cisco richiede i dati. Se si mantiene attiva la modalità di debug per un periodo di tempo prolungato,

lo spazio su disco potrebbe esaurirsi molto rapidamente e i dati del log del connettore e del log della barra delle applicazioni potrebbero non essere raccolti nel file di diagnostica del supporto a causa di dimensioni eccessive del file.

La modalità debug è utile quando si tenta di risolvere i problemi di prestazioni su un connettore di endpoint sicuro. Completare questa procedura per abilitare la modalità di debug e raccogliere i dati diagnostici;

1. Accedere a Secure Endpoint Console.
2. Passare a **Gestione > Criteri**.
3. Individuare un criterio applicato a un computer, fare clic sul criterio per espandere la finestra del criterio e quindi fare clic su **Duplica**. Secure Endpoint Console si aggiorna con il criterio duplicato:



The screenshot shows the 'Policies' page in the Secure Endpoint Console. At the top, there is a search bar containing 'TechZone' and a 'View All Changes' link. Below the search bar are tabs for 'All Products', 'Windows', 'Android', 'Mac', 'Linux', 'Network', and 'iOS'. A '+ New Policy...' button is visible on the right. The main content area displays a policy card for 'TechZone MAC Policy'. The card has a table with columns: Modes and Engines, Exclusions, Proxy, and Groups. The 'Exclusions' column contains 'Apple macOS Default'. Below the table is an 'Outbreak Control' section with columns for Custom Detections - Simple, Custom Detections - Advanced, Application Control, and Network. At the bottom of the card, there is a metadata bar with 'View Changes', 'Modified 2019-05-30 14:49:32 UTC', and 'Serial Number 10004'. A row of action buttons includes 'Download XML', 'Duplicate', 'Edit', and 'Delete'. The 'Duplicate' button is circled in red.

4. Selezionare ed espandere la finestra del criterio duplicato, quindi fare clic su **Modifica** e modificare il nome del criterio. Ad esempio, è possibile utilizzare *Debug criteri MAC TechZone*.
5. Clic **Impostazioni avanzate**, selezionare **Funzioni amministrative** dalla barra laterale e selezionare **Debug** per entrambi i menu a discesa Connector Log Level e Tray Log Level:

Name

Description

Modes and Engines

Exclusions
1 exclusion set

Proxy

Outbreak Control

Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

ClamAV

Network

Scheduled Scans

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval ⓘ

Connector Log Level ⓘ

Tray Log Level ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

6. Fare clic sul pulsante **Salva** per salvare le modifiche.
7. Passa a **Gestione > Gruppi** e fare clic su **Crea gruppo** nella parte superiore destra dello schermo.
8. Immettere un nome per il gruppo. Ad esempio, è possibile *utilizzare Debug TechZone Mac Group*.

< **New Group** ?

Name

Description

Parent Group

Windows Policy

Android Policy

Mac Policy

Linux Policy

Network Policy

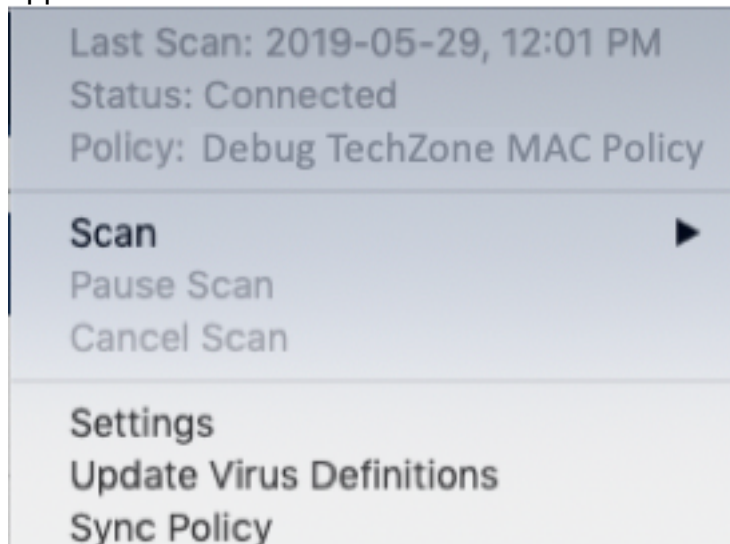
iOS Policy

Computers

Assign computers from the Computers page after you have saved the new group

9. Cambia criteri Mac da *Criteri Mac Predefiniti* alla nuova regola appena creata, ovvero **Debug criteri Mac TechZone** in questo esempio. Clic **Salva**.

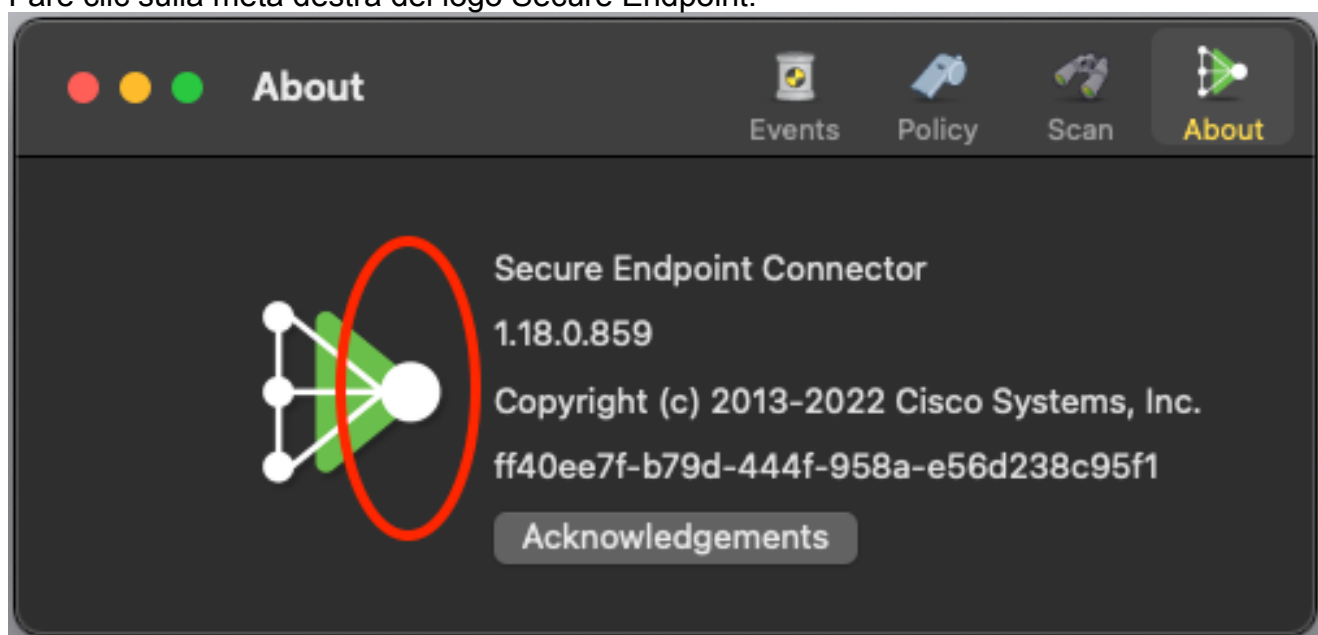
10. Passa a **Gestione > Computer** e identificare il computer nell'elenco. Selezionarlo e fare clic su **Sposta nel gruppo...**
11. Selezionare il gruppo appena creato dall'elenco **Seleziona gruppo** menu a discesa. Clic **Sposta** per spostare il computer selezionato nel nuovo gruppo. A questo punto il Mac dovrebbe avere un criterio di debug funzionale. È possibile selezionare l'icona Endpoint protetto che viene visualizzata sulla barra dei menu e verificare che il nuovo criterio sia applicato:



Abilita modalità di debug heartbeat singolo

Questa procedura è disponibile solo per il connettore 1.0.4 e versioni successive. In questo modo, un singolo connettore può essere messo in modalità debug fino al successivo heartbeat. A seconda della situazione, questo potrebbe fornire informazioni sufficienti per i nostri sviluppatori ma a seconda della lunghezza dell'heartbeat, rischia di non catturare tutti i processi necessari per fare un'analisi diagnostica completa. Di seguito sono riportati i passaggi per abilitare il debug per un singolo heartbeat:

1. Accedere alla barra dei menu del connettore e passare a **Impostazioni**.
2. Fare clic su **Informazioni su**.
3. Fare clic sulla metà destra del logo Secure Endpoint.



4. se è stato fatto correttamente, sul lato destro dello schermo apparirà il seguente avviso:



Il debug verrà disabilitato automaticamente dopo il prossimo heartbeat.

Disabilita modalità di debug

Dopo aver ottenuto i dati diagnostici in modalità di debug, è necessario ripristinare la modalità normale del connettore Secure Endpoint. Per disabilitare la modalità di debug, completare la procedura seguente:

1. Accedere alla Secure Endpoint Console.
2. Passare a **Gestione > Gruppi**.
3. Individuare il nuovo gruppo, *Debug TechZone Mac Group*, creato in modalità di debug.
4. Fare clic su **Modifica**.
5. Nella finestra Computer posizionata nella parte superiore destra dello schermo individuare il computer nell'elenco. Selezionarlo per passare alla pagina Computer. Selezionare nuovamente il computer dall'elenco e **fare clic su Sposta nel gruppo...**
6. Selezionare il gruppo precedente dal menu a discesa **Seleziona** gruppo. Fare clic su **Sposta** per spostare il computer selezionato nel gruppo precedente.
7. Fare clic sull'icona Secure Endpoint nella barra dei menu. **Selezionare Sincronizza** criterio dal menu.
8. Verificare che venga ripristinato il valore predefinito precedente del criterio. Controllare sulla barra dei menu. Il criterio dovrebbe essere stato ripristinato al criterio originale utilizzato prima di essere modificato in *Debug TechZone Mac Group*:

