Cisco Secure Endpoint Connector für Mac-Diagnosedatensammlung

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Erstellen einer Diagnosedatei mit dem Support-Tool](#)
[Starten des Support-Tools mit macOS Finder](#)
[Starten des Support-Tools mit macOS Terminal](#)
[Fehlerbehebung](#)
[Debug-Modus aktivieren](#)
[Single-Heartbeat-Debug-Modus aktivieren](#)
[Debug-Modus deaktivieren](#)

Einleitung

In diesem Dokument wird der Prozess beschrieben, der zum Generieren einer Diagnosedatei über die Support Tool-Anwendung verwendet wird, die auf dem Cisco Secure Endpoint Mac-Connector verfügbar ist. Außerdem wird beschrieben, wie Leistungsprobleme behoben werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Secure Endpoint Mac-Anschluss
- MacOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Secure Endpoint Mac-Connector.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Der Secure Endpoint Mac-Connector verpackt eine Anwendung namens Support Tool, die verwendet wird, um Diagnoseinformationen über den Connector zu generieren, der auf Ihrem Mac installiert ist. Zu den Diagnosedaten gehören Informationen über Ihren Mac wie:

- Ressourcennutzung (Festplatte, CPU und Arbeitsspeicher)
- verbindungsspezifische Protokolle
- Anschlusskonfigurationsinformationen

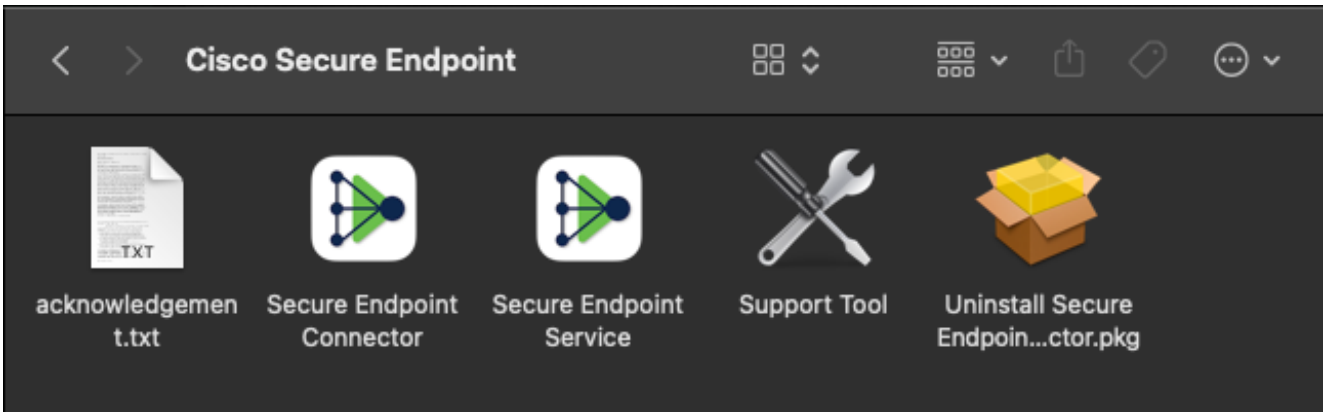
Erstellen einer Diagnosedatei mit dem Support-Tool

In diesem Abschnitt wird beschrieben, wie Sie das Support Tool über die GUI oder die CLI starten, um eine Diagnosedatei zu erstellen.

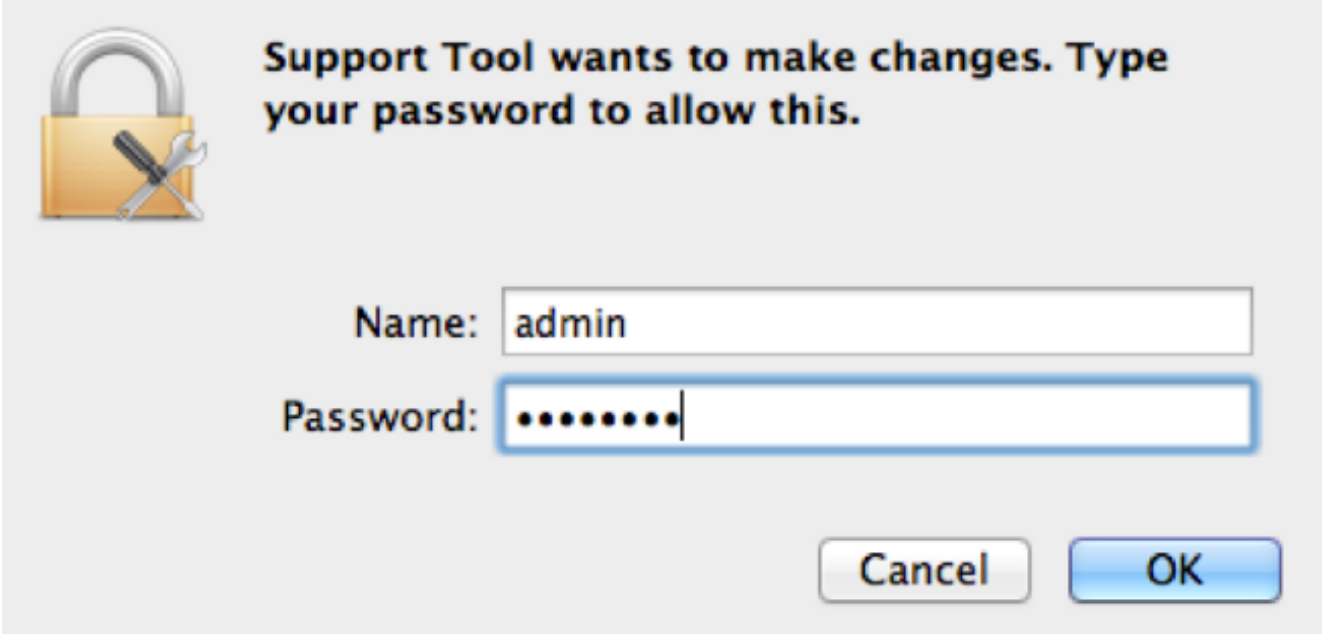
Starten des Support-Tools mit macOS Finder

Führen Sie die folgenden Schritte aus, um das Secure Endpoint Mac Connector Support Tool mit dem macOS Finder zu starten:

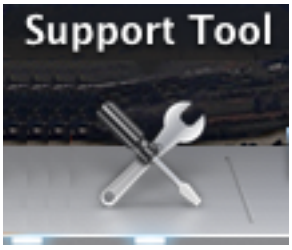
1. Navigieren Sie zum Verzeichnis Cisco Secure Endpoint im Ordner Applications (Anwendungen), und suchen Sie nach dem Launcher für das Support Tool:



2. Doppelklicken Sie auf den Launcher des Support Tools, und Sie werden zur Eingabe der administrativen Anmeldeinformationen aufgefordert:

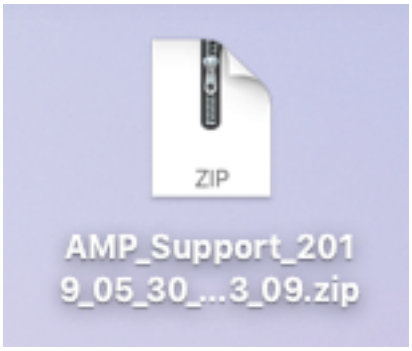


3. Nachdem Sie Ihre Anmeldeinformationen eingegeben haben, sollte in Ihrem Dock das Symbol für das Support-Tool angezeigt werden:

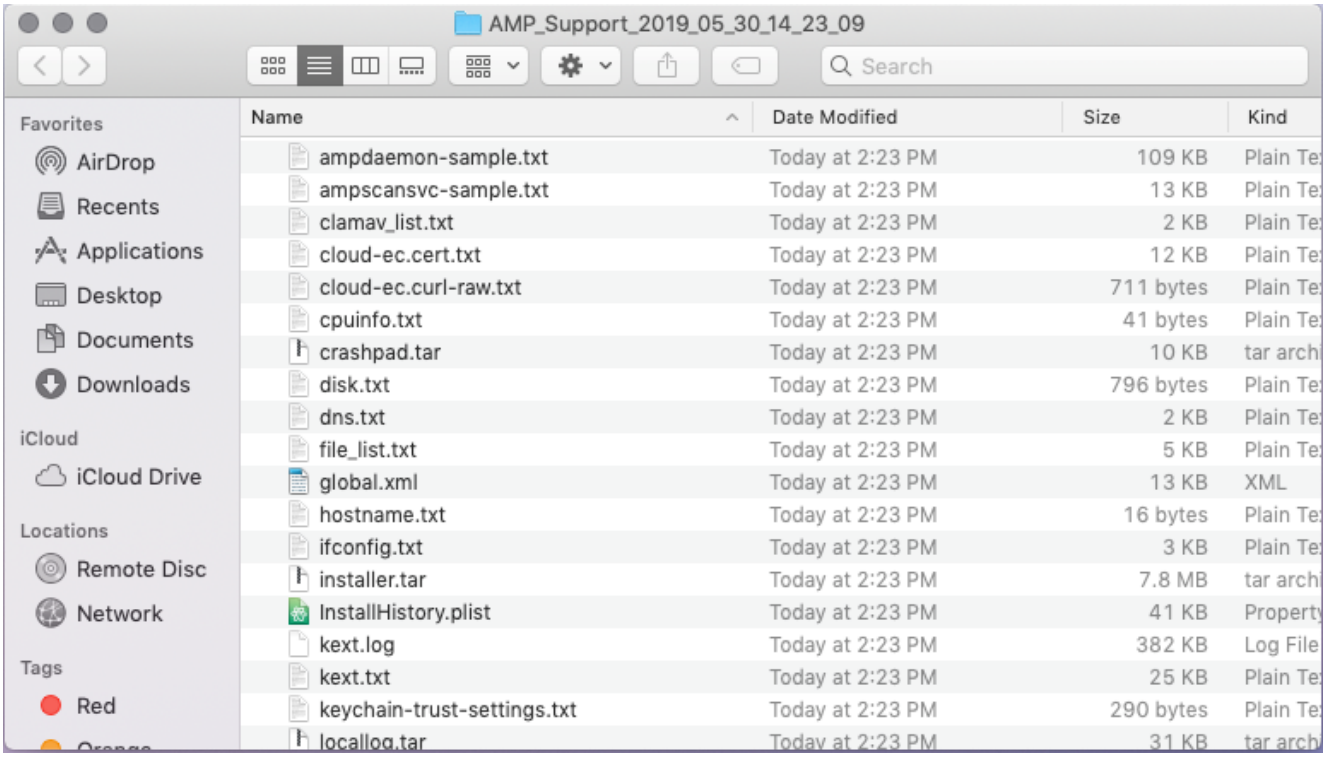


Anmerkung: Die Anwendung des Support Tools wird im Hintergrund ausgeführt und nimmt einige Zeit in Anspruch (ca. 20-30 Minuten).

4. Wenn die Support Tool-Anwendung abgeschlossen ist, wird eine Datei generiert und auf Ihrem Desktop gespeichert:



Hier ist ein Beispiel für die unkomprimierte Ausgabe:



5. Stellen Sie diese Datei dem technischen Support von Cisco zur Verfügung, um die Daten zu analysieren.

Starten des Support-Tools mit macOS Terminal

Der Launcher des Support Tools befindet sich in folgendem Verzeichnis:

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

Geben Sie den folgenden Befehl ein, um das Support Tool zu starten:

> **Anmerkung:** Sie müssen diesen Befehl als root ausführen, also stellen Sie sicher, dass Sie zu root wechseln oder den Befehl mit **sudo** voranstellen.

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

> **Anmerkung: Dieser Befehl wird ausführlich ausgeführt. Nach Abschluss des Vorgangs wird eine Diagnosedatei generiert und auf Ihrem Desktop gespeichert.**

Fehlerbehebung

In diesem Abschnitt wird beschrieben, wie Sie den Debugmodus auf dem Mac-Connector für sichere Endgeräte aktivieren und deaktivieren, um Leistungsprobleme zu beheben.

Debug-Modus aktivieren

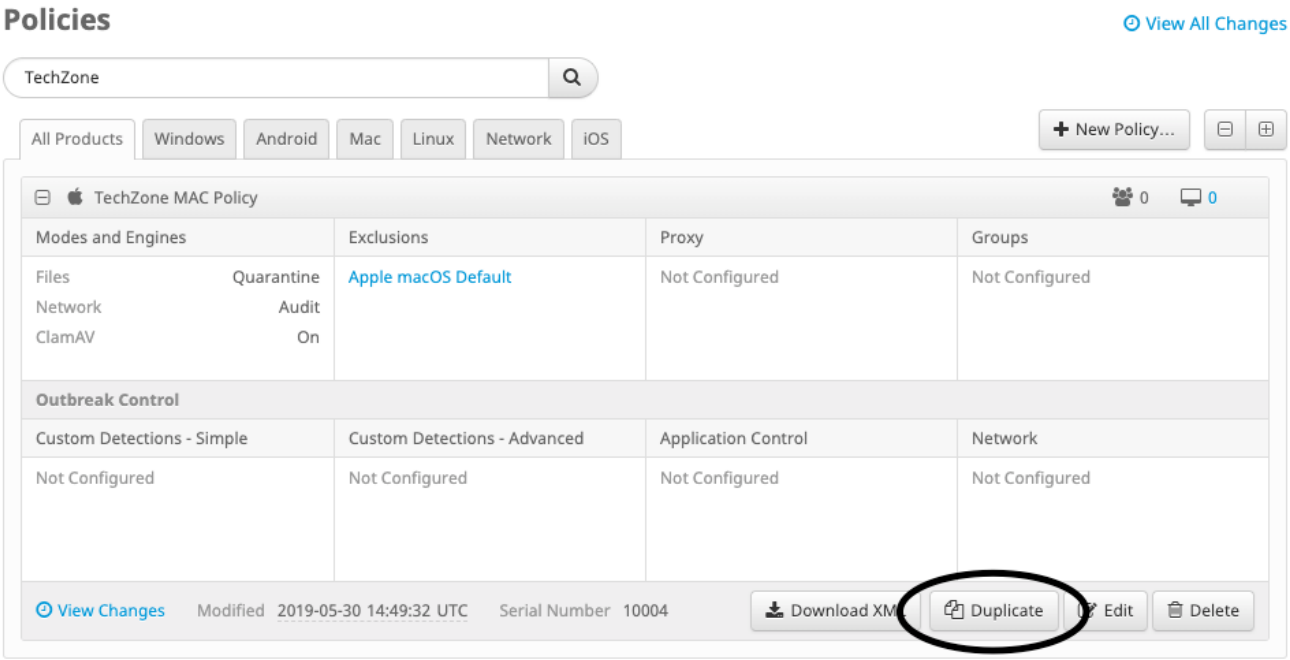
> **Warnung**: Der Debug-Modus sollte nur aktiviert werden, wenn ein Techniker des

technischen Supports von Cisco eine Anfrage für diese Daten stellt. Wenn Sie den Debug-Modus für einen längeren Zeitraum aktiviert lassen, kann er sehr schnell den Speicherplatz belegen und möglicherweise verhindern, dass die Protokoll- und Tray-Protokoll-Daten des Connectors in der Diagnosedatei des Supports aufgrund einer zu großen Dateigröße erfasst werden.

Der Debug-Modus ist nützlich, wenn versucht wird, Leistungsprobleme an einem Secure Endpoint Connector zu beheben. Führen Sie diese Schritte aus, um den Debugmodus zu aktivieren und Diagnosedaten zu sammeln.

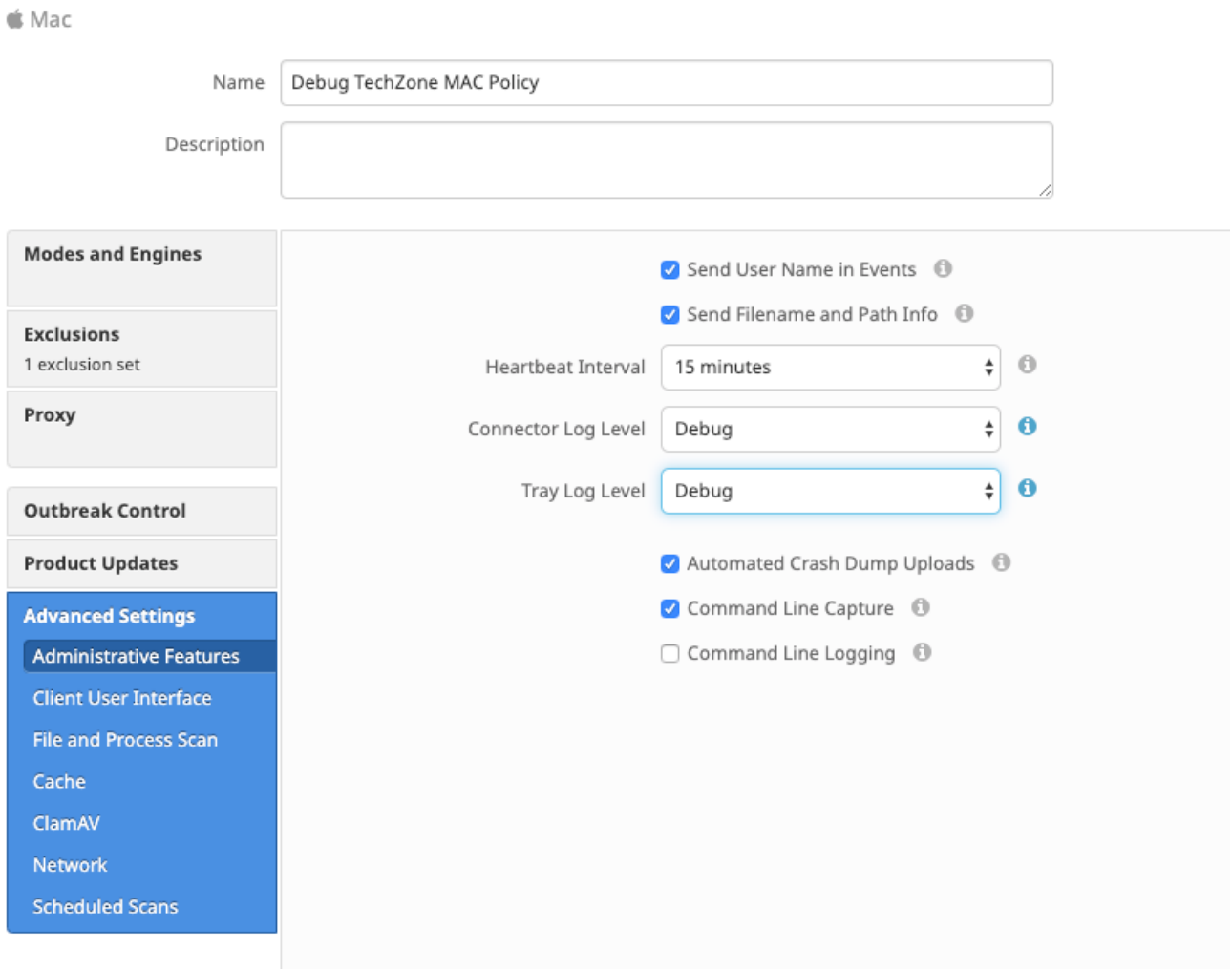
1. Melden Sie sich bei der Konsole für sichere Endgeräte an.
2. Navigieren Sie zu **Verwaltung > Richtlinien**.

3. Suchen Sie eine Richtlinie, die auf einen Computer angewendet wird, klicken Sie auf die Richtlinie, die das Richtlinienfenster erweitert, und klicken Sie auf **Duplizieren**. Die Konsole für sichere Endgeräte wird mit der duplizierten Richtlinie aktualisiert:

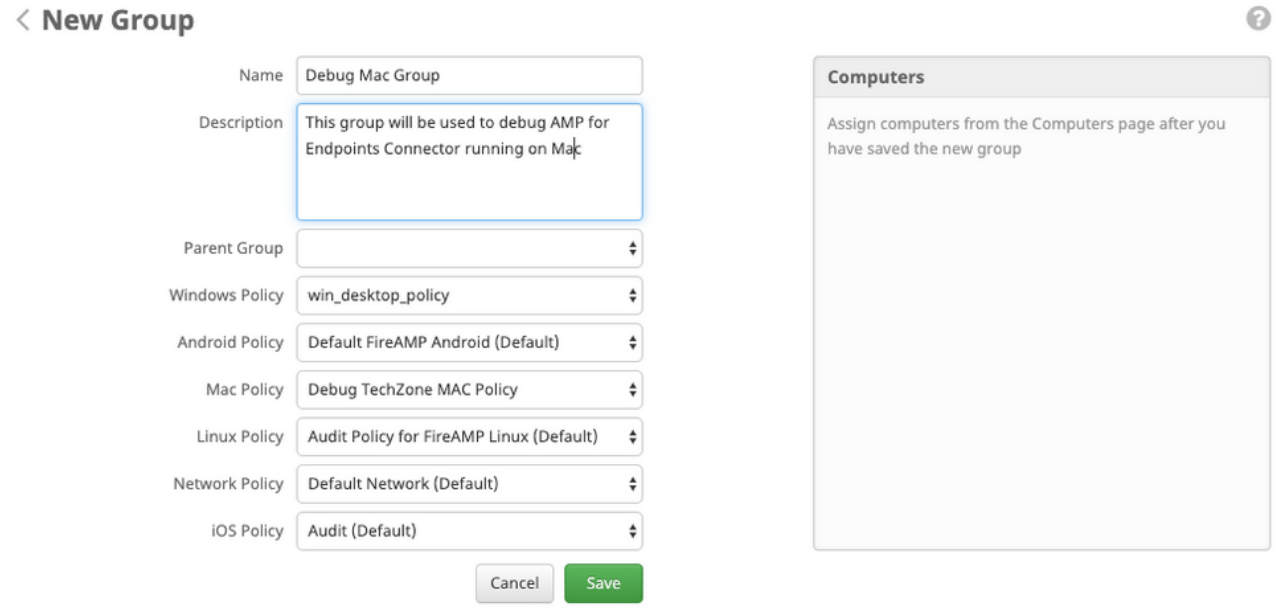


4. Wählen Sie das doppelte Richtlinienfenster aus, und erweitern Sie es. Klicken Sie auf **Bearbeiten** und den Namen der Richtlinie ändern. Sie können z. B. *Debuggen der TechZone MAC-Richtlinie*.

5. Klicken Sie auf **Erweiterte Einstellungen**, wählen **Verwaltungsfunktionen** und wählen Sie **Fehlersuche** für die Dropdown-Menüs "Log Level" (Protokollstufe) und "Tray Log Level" (Protokollstufe):



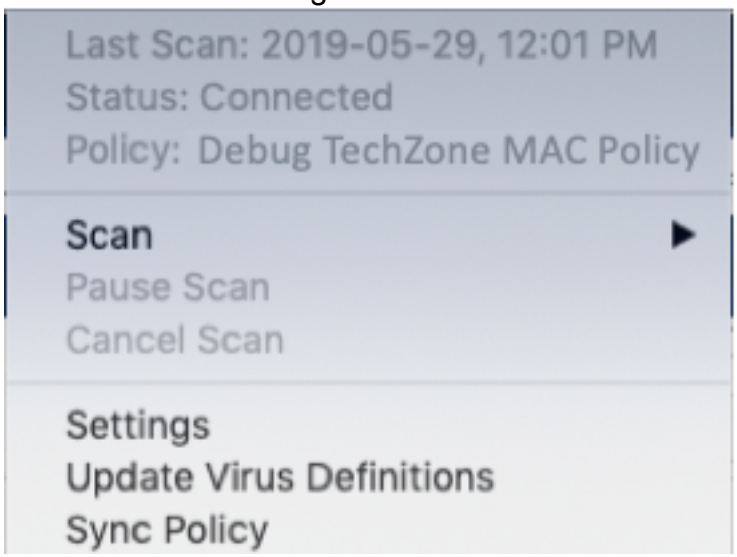
6. Klicken Sie auf **Speichern** um die Änderungen zu speichern.
7. Navigieren Sie zu **Verwaltung > Gruppen** und klicke auf **Gruppe erstellen** oben rechts auf dem Bildschirm angezeigt.
8. Geben Sie einen Namen für die Gruppe ein. Sie können beispielsweise *Debug TechZone Mac Group verwenden*.



9. Ändern Sie die Mac-Richtlinie von *Standard-MAC-Richtlinie* auf die duplizierte, neue Richtlinie anwenden, die Sie gerade erstellt haben. **TechZone Mac-Richtlinie debuggen** in

diesem Beispiel. Klicken Sie auf **Speichern**.

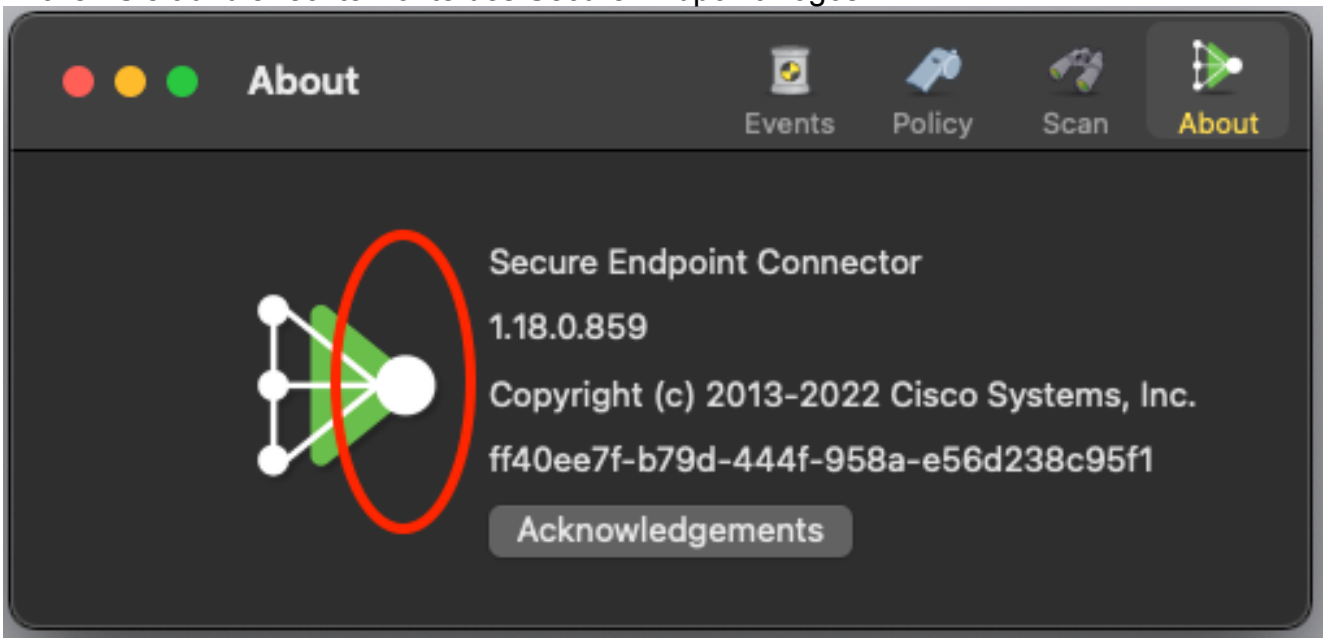
10. Navigieren Sie zu **Verwaltung > Computer** und identifizieren Sie Ihren Computer in der Liste. Wählen Sie es aus, und klicken Sie auf **In Gruppe verschieben...**.
11. Wählen Sie Ihre neu erstellte Gruppe aus dem **Gruppe auswählen** Dropdown-Menü. Klicken Sie auf **Verschieben** um den ausgewählten Computer in die neue Gruppe zu verschieben. Ihr Mac sollte nun über eine funktionierende Debug-Richtlinie verfügen. Sie können das in der Menüleiste angezeigte Symbol für sichere Endgeräte auswählen und sicherstellen, dass die neue Richtlinie angewendet wird:



Single-Heartbeat-Debug-Modus aktivieren

Dieses Verfahren steht nur für den 1.0.4-Anschluss und höher zur Verfügung. Dadurch kann ein einzelner Connector bis zum nächsten Heartbeat in den Debug-Modus versetzt werden. Abhängig von der Situation, kann dies genügend Informationen für unsere Entwickler, aber abhängig von der Länge des Herzschlages, Risiken nicht alle Prozesse erforderlich, um eine vollständige diagnostische Analyse. So aktivieren Sie Debug für einen einzelnen Heartbeat:

1. Öffnen Sie die Menüleiste des Anschlusses, und gehen Sie zu **Einstellungen.**
2. Klicken Sie auf **Info.**
3. Klicken Sie auf die rechte Hälfte des Secure Endpoint-Logos.



4. Wenn sie richtig ausgeführt wurde, wird rechts auf dem Bildschirm folgender Hinweis eingeblendet:

Debug wird nach dem nächsten Heartbeat automatisch deaktiviert.

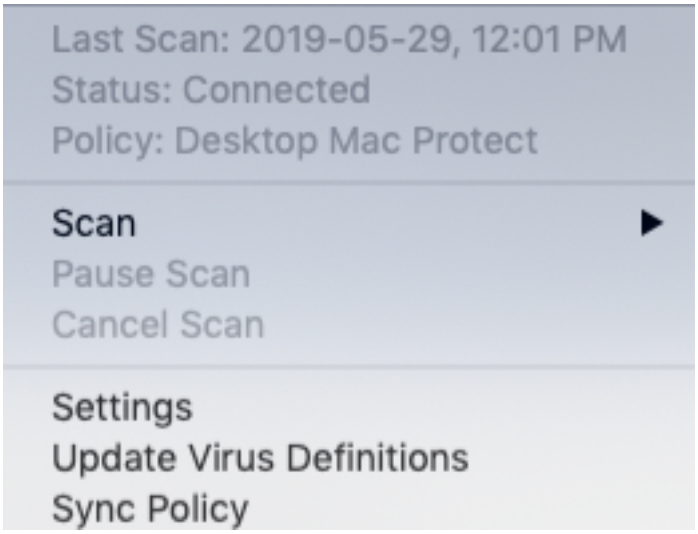
Debug-Modus deaktivieren

Nachdem die Diagnosedaten im Debugmodus abgerufen wurden, müssen Sie den Secure Endpoint Connector in den normalen Modus zurücksetzen. Führen Sie die folgenden Schritte aus, um den Debugmodus zu deaktivieren:

1. Melden Sie sich bei der Secure Endpoint Console an.
2. Navigieren Sie zu **Verwaltung > Gruppen**.

3. Suchen Sie die neue Gruppe*, Debug TechZone Mac Group*, die Sie im Debugmodus erstellt haben.
4. Klicken Sie auf **Bearbeiten**.

5. Suchen Sie im Fenster Computer oben rechts auf dem Bildschirm Ihren Computer in der Liste. Wählen Sie es, die Sie auf die Computerseite führen. Wählen Sie Ihren Computer erneut aus der Liste aus, und **klicken Sie auf In Gruppe verschieben...**.
6. Wählen Sie Ihre vorherige Gruppe aus **dem** Dropdown-Menü Gruppe **auswählen**. Klicken Sie auf Verschieben, um den ausgewählten Computer in die vorherige Gruppe zu verschieben.
7. Klicken Sie in der Menüleiste auf das Symbol Secure Endpoint (Sicheres Endgerät). **Wählen Sie** im Menü die OptionSync Policy.
8. Überprüfen Sie, ob die Richtlinie jetzt auf den vorherigen Standardwert zurückgesetzt wird. Überprüfen Sie dies in der Menüleiste. Die Richtlinie sollte jetzt auf die ursprüngliche Richtlinie zurückgesetzt haben, die verwendet wurde, bevor Sie sie in *dieDebug TechZone Mac Group* geändert haben:


Last Scan: 2019-05-29, 12:01 PM
Status: Connected
Policy: Desktop Mac Protect
Scan
Pause Scan
Cancel Scan
Settings
Update Virus Definitions
Sync Policy

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.