Debuggen auf Endgeräten von AMP für Endgeräte-Konsole aus aktivieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Debuggen auf dem Endgerät über die Cisco Secure Endpoint Console aktivieren.

Voraussetzungen

Anforderungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

- Administrator-Zugriff auf die Konsole von Cisco Secure Endpoint für Endgeräte
- Der Endpunkt, den Sie debuggen möchten, ist bereits in Cisco Secure Endpoint registriert.

Verwendete Komponenten

Die in diesem Dokument verwendeten Informationen basieren auf den folgenden Softwareversionen:

- Cisco Secure Endpoint Console Version 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 und höher
- Microsoft Windows-Betriebssystem

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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die generierten Diagnosedaten können dem Cisco Technical Assistance Center (TAC) zur weiteren Analyse zur Verfügung gestellt werden.

Die Diagnosedaten enthalten Informationen wie:

- Ressourcennutzung (Festplatte, CPU und Arbeitsspeicher)
- Connector-spezifische Protokolle
- Konfigurationsinformationen für den Connector

Problem

In einem dieser Szenarien ist die Aktivierung von Debug auf Endgeräten über die Cisco Secure Endpoint Console erforderlich.

Szenario 1: Wenn Sie das Gerät neu starten, aktivieren Sie den Debug-Modus von der IP Tray-Schnittstelle aus, oder es übersteht den Neustart nicht. Falls Bootdebugprotokolle erforderlich sind, können Sie den Debug-Modus über die Richtlinienkonfiguration in der Secure Endpoint-Konsole aktivieren.

Szenario 2: Wenn beim Cisco Secure Endpoint Connector Leistungsprobleme auf einem Gerät auftreten, kann die Aktivierung des Debug-Modus dazu beitragen, detaillierte Protokolle zur Analyse zu sammeln.

Szenario 3: Bei der Fehlerbehebung in Verbindung mit Secure Endpoint Connector können detaillierte Protokolle Einblicke in die Ursache des Problems liefern.

Konfigurieren

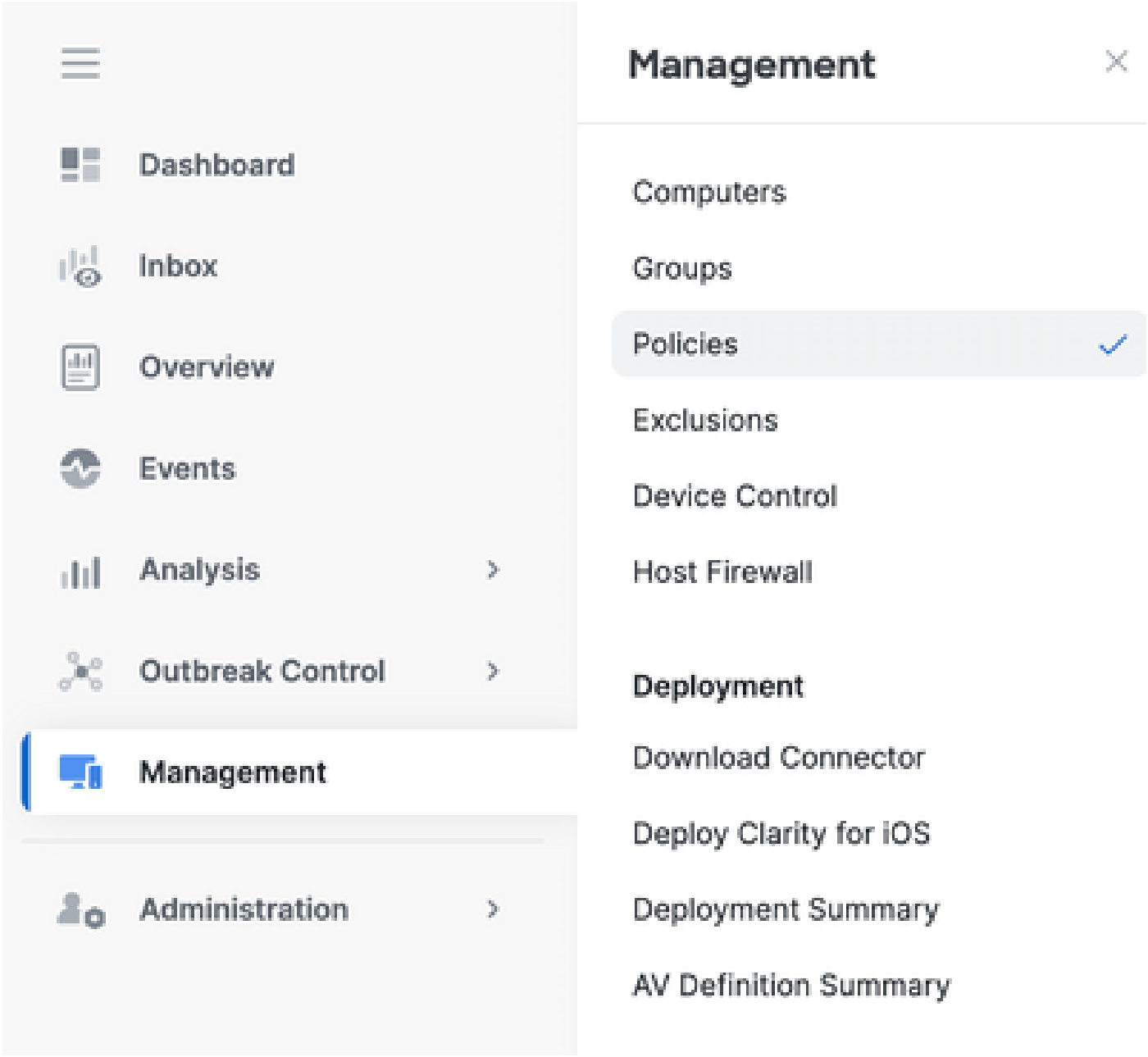
Führen Sie diese Schritte aus, um den Debugmodus auf dem angegebenen Endpunkt über die Konsole für sichere Endpunkte erfolgreich zu aktivieren.

Schritt 1: Identifizieren des zu debuggenden Endpunkts

1. Melden Sie sich bei der Cisco Secure Endpoint-Konsole an. Navigieren Sie vom Haupt-Dashboard zum Abschnitt Management.
2. Navigieren Sie zu Verwaltung > Computer.
3. Identifizieren und notieren Sie den Endpunkt, der den Debugmodus erfordert.

Schritt 2: Duplizieren der vorhandenen Richtlinie

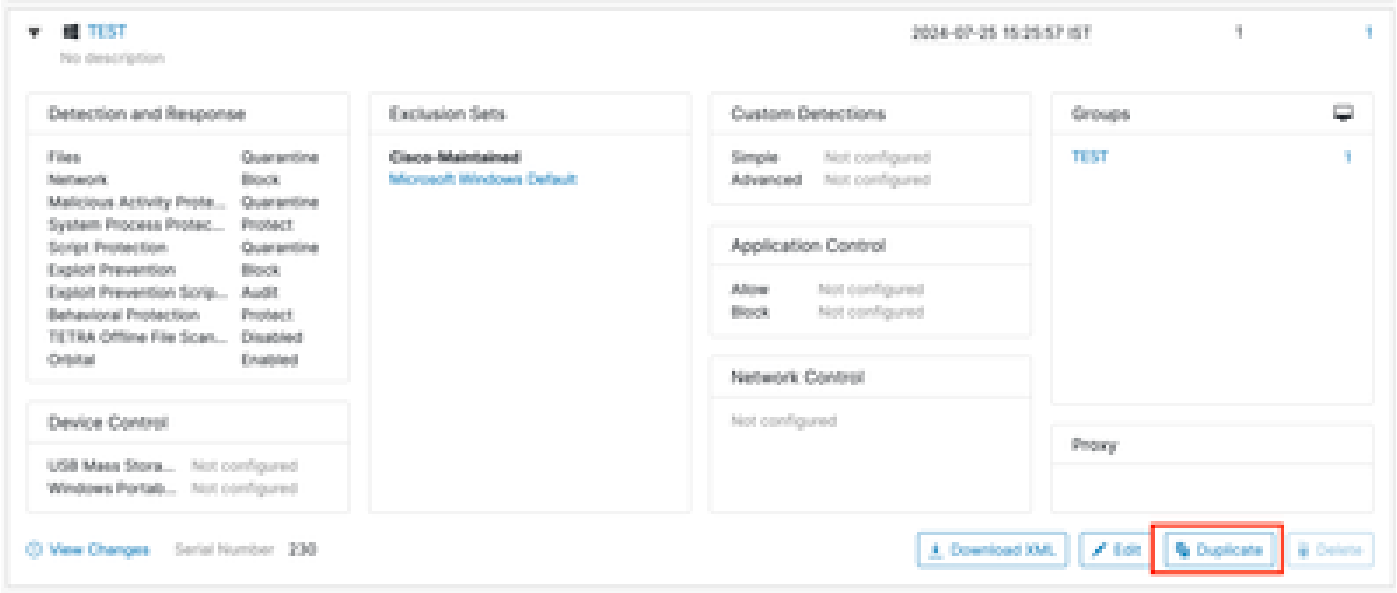
1. Navigieren Sie zu Verwaltung > Richtlinien.



2. Suchen Sie nach der Richtlinie, die derzeit auf den identifizierten Endpunkt angewendet wird.

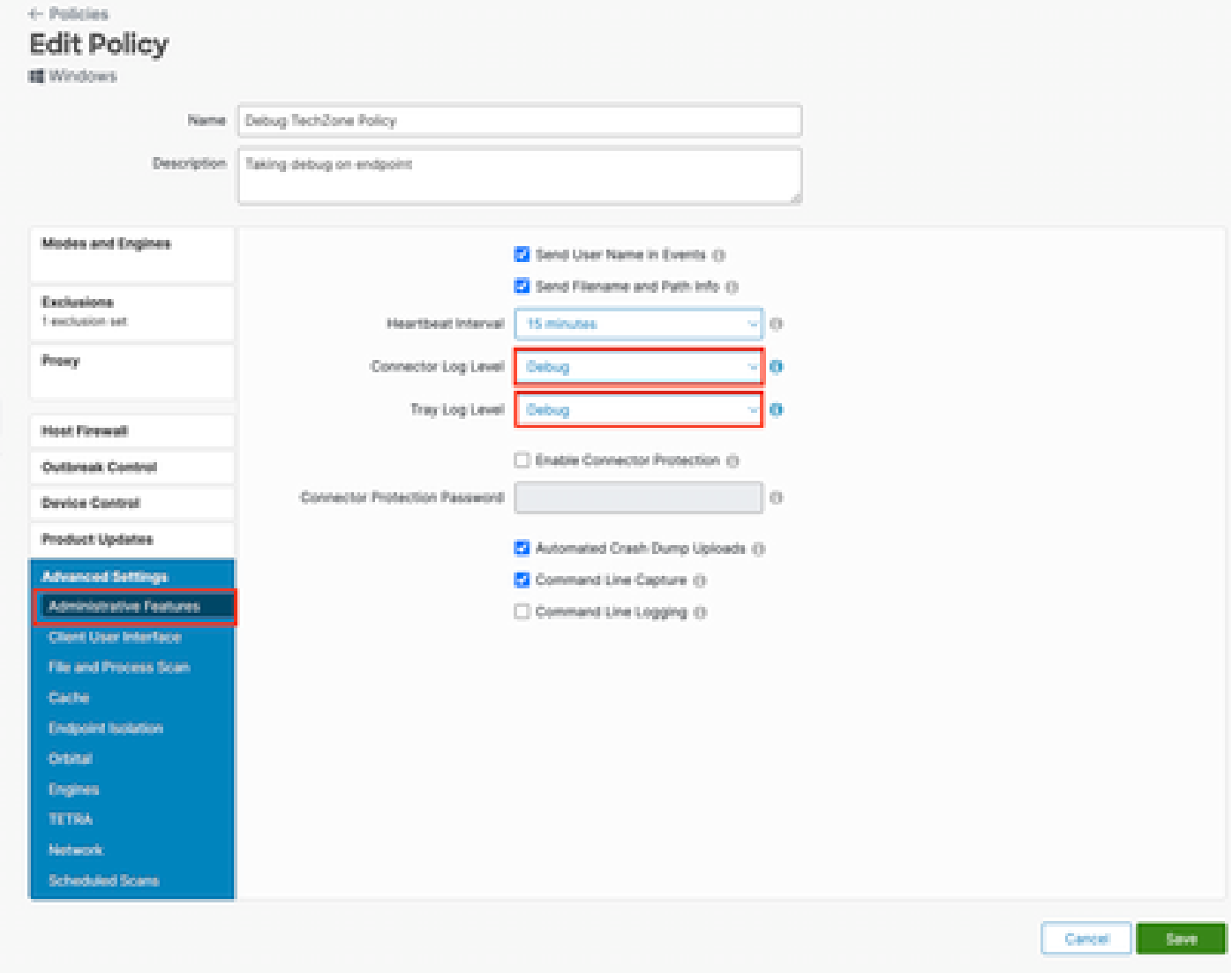
3. Klicken Sie auf die Richtlinie, um das Richtlinienfenster zu erweitern.

4. Klicken Sie auf Duplizieren, um eine Kopie der vorhandenen Richtlinie zu erstellen.



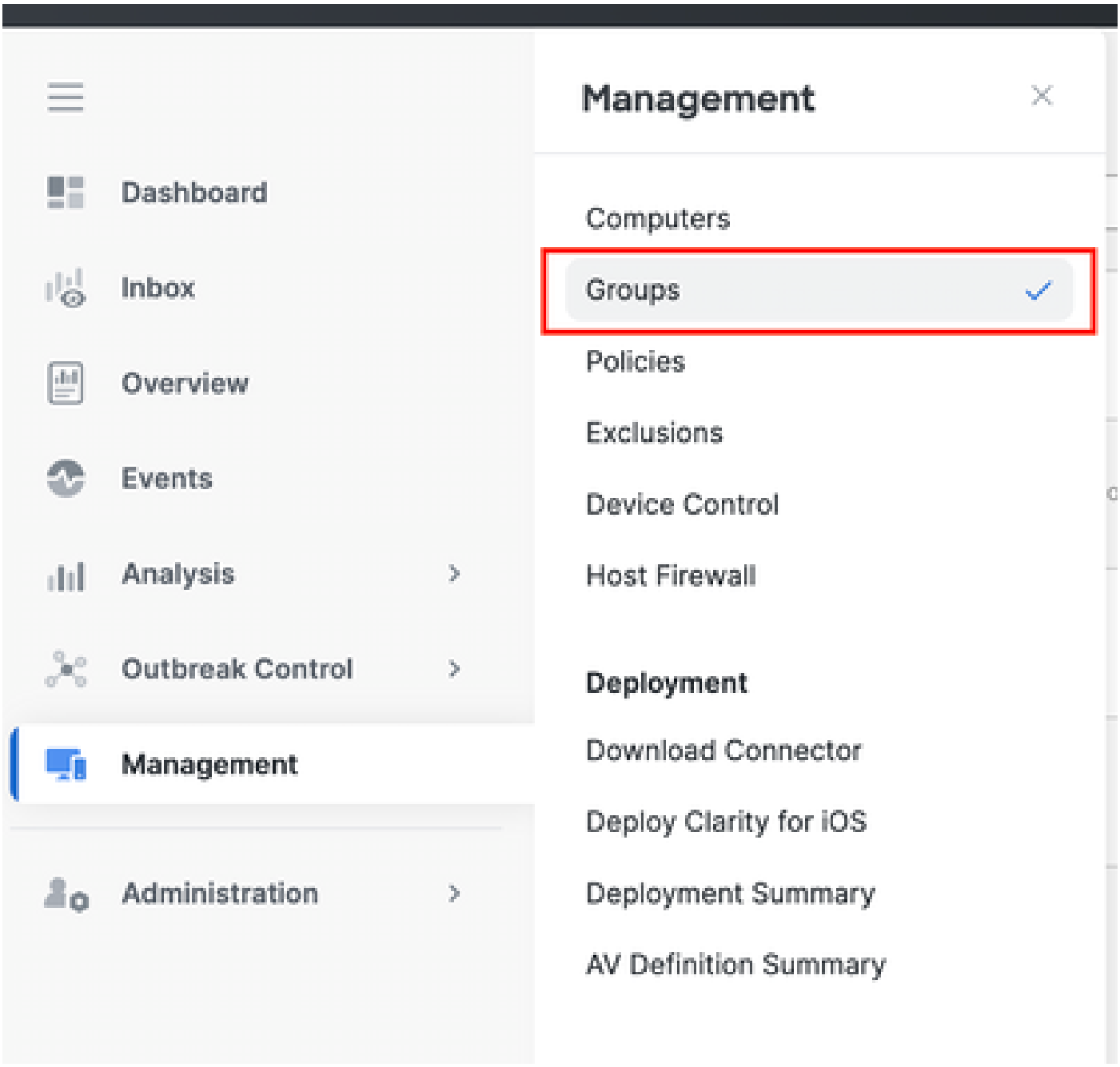
Schritt 3: Konfigurieren der Protokollstufe zum Debuggen dieser Richtlinie

1. Wählen Sie das Fenster für duplizierte Richtlinien aus, und erweitern Sie es.
2. Klicken Sie auf Bearbeiten, und benennen Sie die Richtlinie um (z. B. TechZone-Richtlinie debuggen).
3. Klicken Sie auf Erweiterte Einstellungen.
4. Wählen Sie in der Seitenleiste Administrative Features aus.
5. Legen Sie die Connector-Protokollstufe und die Tray-Protokollstufe auf Debug fest.
6. Klicken Sie auf Speichern, um die Änderungen zu speichern.



Schritt 4: Neue Gruppe erstellen und neue Richtlinie verknüpfen

1. Navigieren Sie zu Verwaltung > Gruppen.

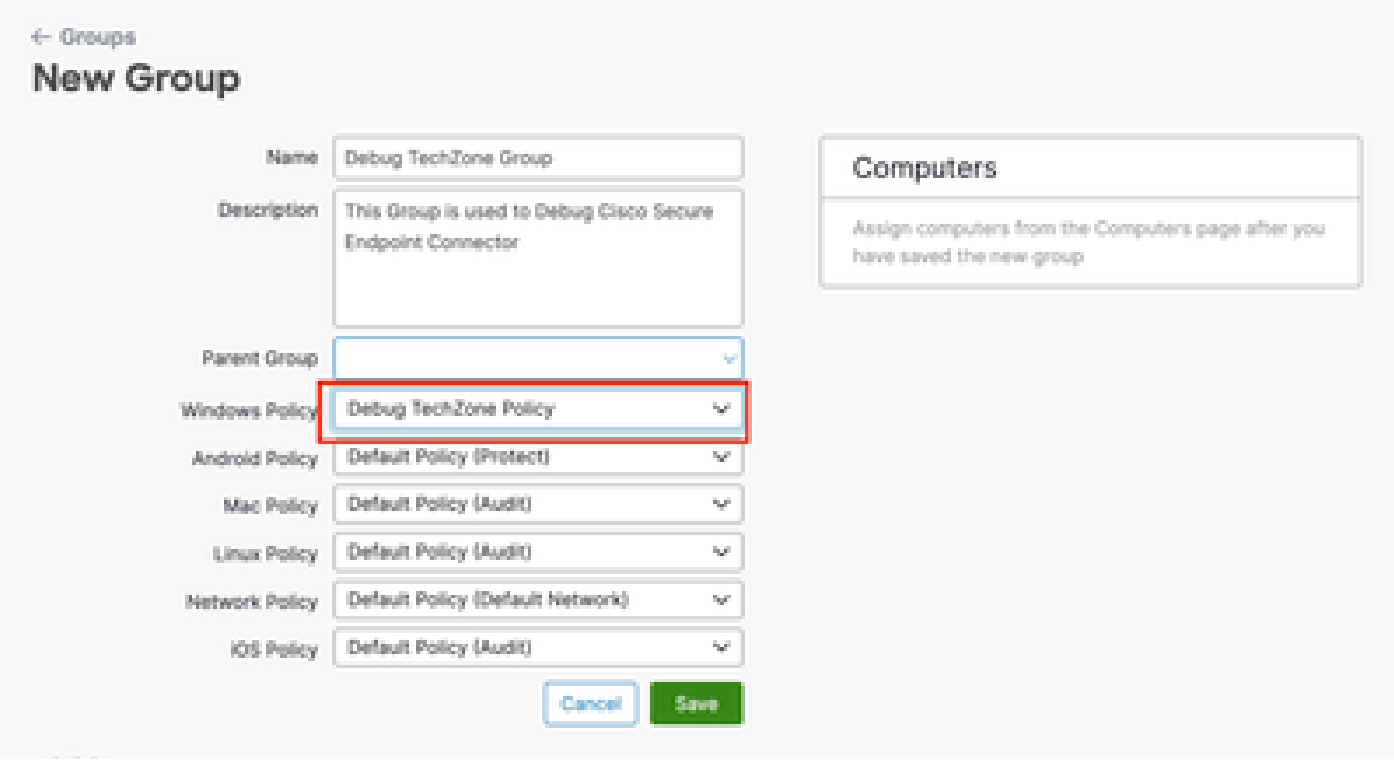


2. Klicken Sie oben rechts auf Ihrem Bildschirm auf Gruppe erstellen.

3. Geben Sie einen Namen für die Gruppe ein (z. B. Debug TechZone Group.)

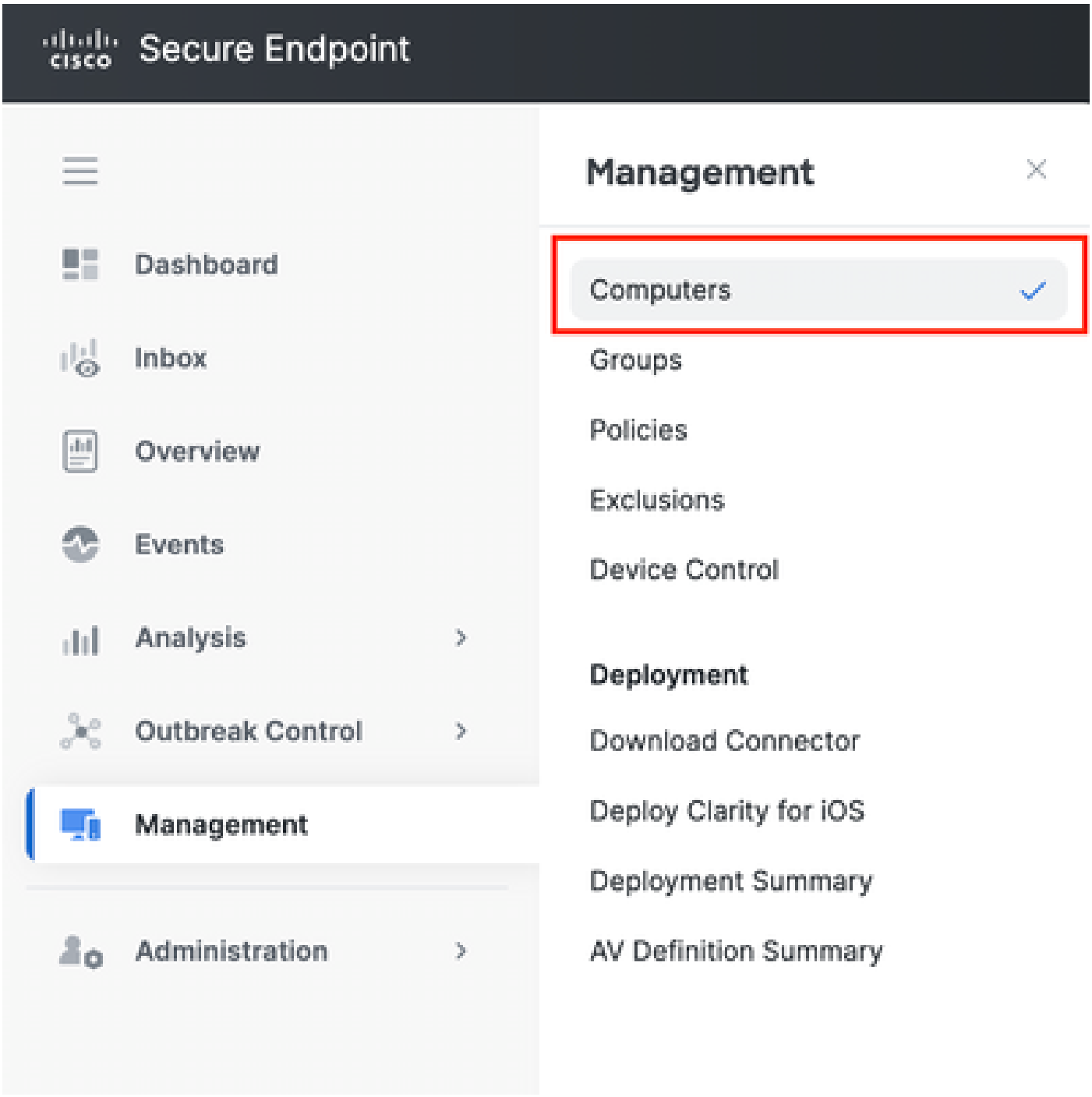
4. Ändern Sie die Richtlinie von der Standardeinstellung in die neu erstellte Debugrichtlinie.

5. Klicken Sie auf Speichern.



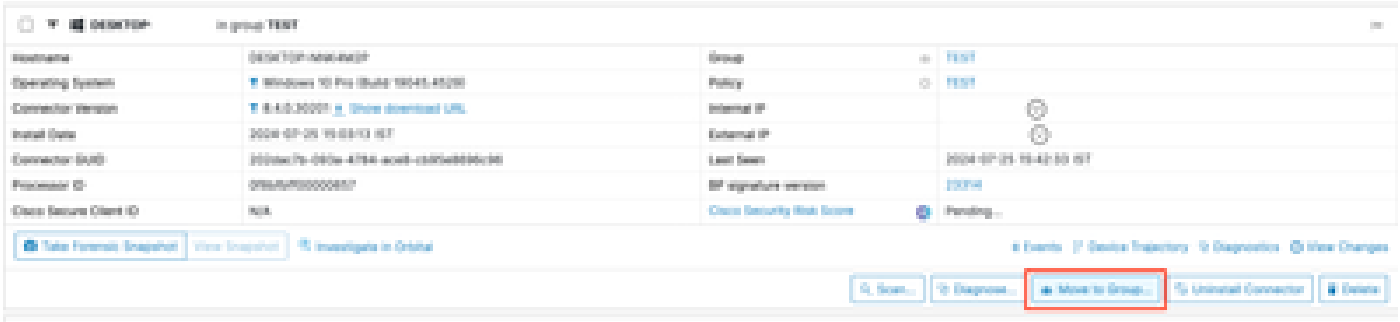
Schritt 5: Verschieben des identifizierten Endpunkts in diese neue Gruppe

1. Navigieren Sie zurück zu Verwaltung > Computer.



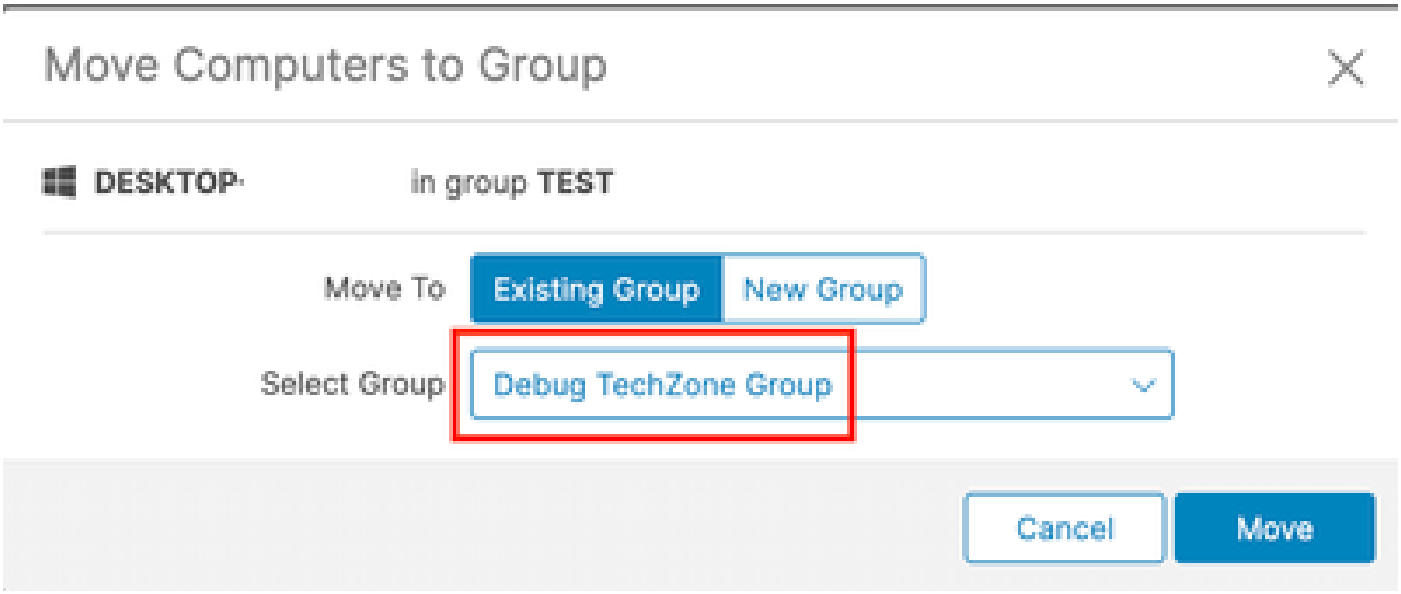
2. Wählen Sie den identifizierten Endpunkt aus der Liste aus.

3. Klicken Sie auf In Gruppe verschieben.



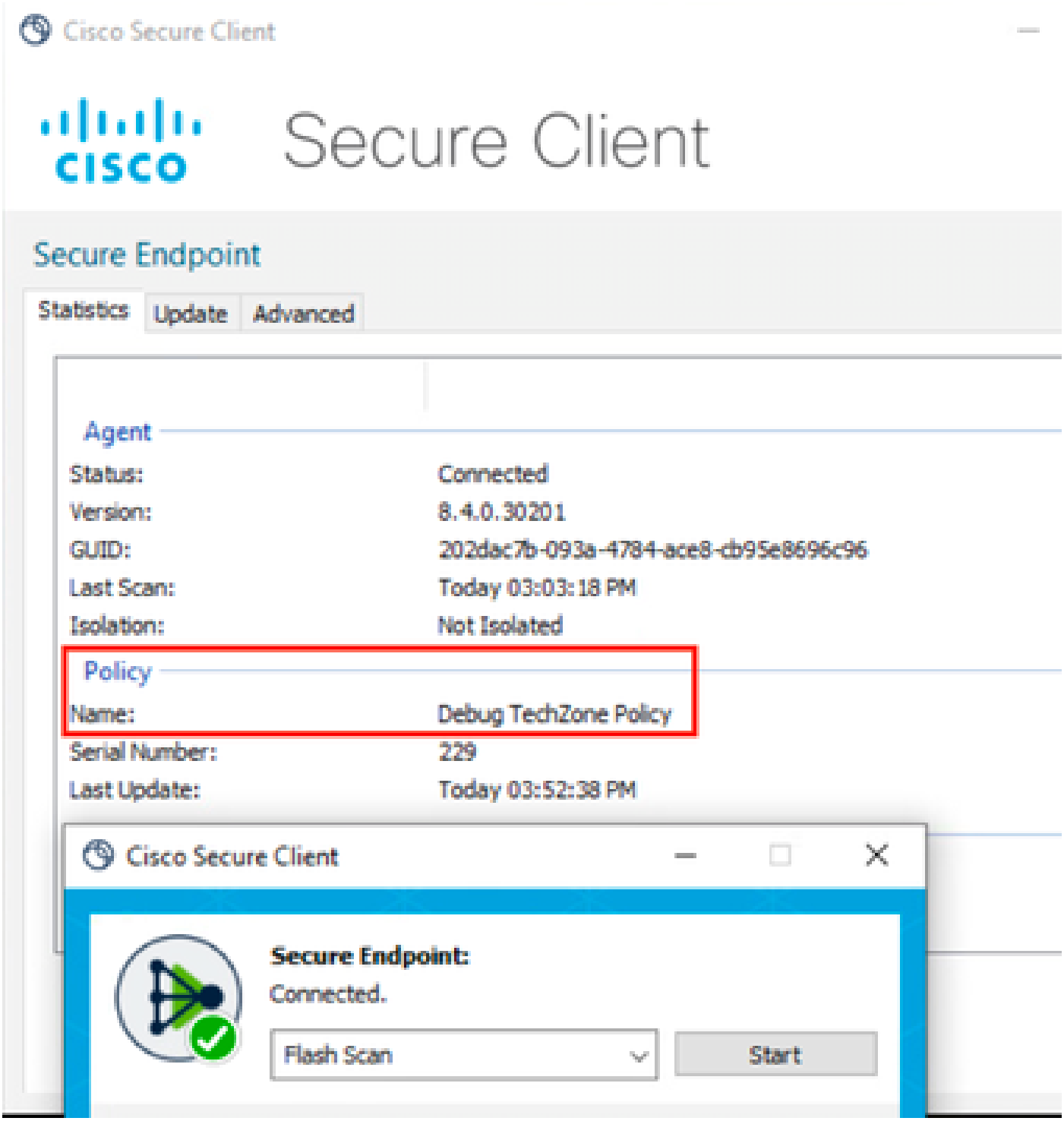
4. Wählen Sie die neu erstellte Gruppe aus dem Dropdown-Menü Gruppe auswählen.

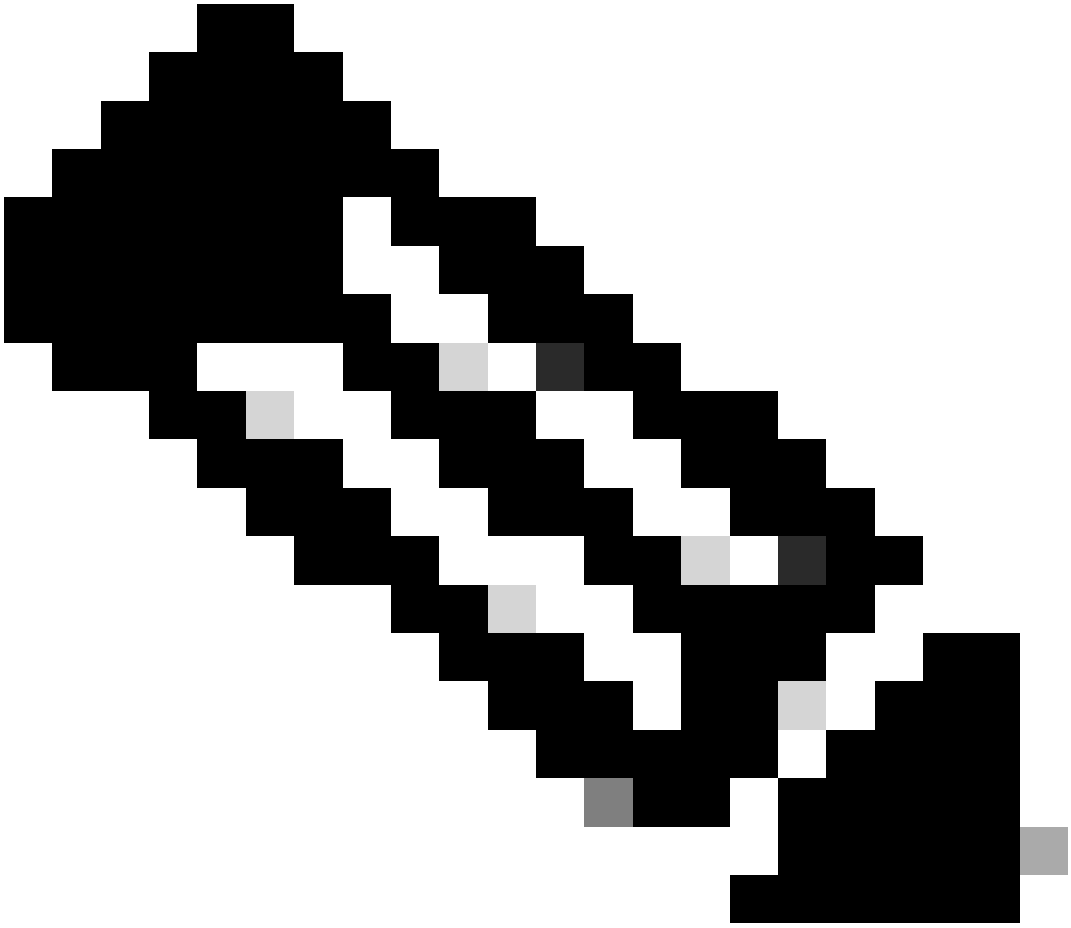
5. Klicken Sie auf Verschieben, um den ausgewählten Endpunkt in die neue Gruppe zu verschieben.



Schritt 6: Überprüfen des Endpunkts auf der Seite "Computer" und in der Connector-Benutzeroberfläche

1. Stellen Sie sicher, dass der Endpunkt auf der Seite Computer unter der neuen Gruppe aufgeführt ist.
2. Öffnen Sie auf dem Endgerät die Benutzeroberfläche des sicheren Endgerätekonnektors.
3. Überprüfen Sie, ob die neue Debugrichtlinie angewendet wird, indem Sie das Symbol Sicherer Endpunkt in der Menüleiste aktivieren.


Cisco Secure Client
Secure Client
Secure Endpoint
Statistics
Update
Advanced
Agent
Status: Connected
Version: 8.4.0.30201
GUID: 202dac7b-093a-4784-ace8-cb95e8696c96
Last Scan: Today 03:03:18 PM
Isolation: Not Isolated
Policy
Name: Debug TechZone Policy
Serial Number: 229
Last Update: Today 03:52:38 PM
Cisco Secure Client
Secure Endpoint:
Connected.
Flash Scan
Start



Hinweis: Der Debug-Modus kann nur aktiviert werden, wenn ein Techniker des technischen Supports von Cisco diese Daten anfordert. Wenn der Debug-Modus für einen längeren Zeitraum aktiviert bleibt, kann schnell Speicherplatz belegt werden, und es kann verhindert werden, dass die Protokoll- und Tray-Protokoll-Daten des Connectors in der Support-Diagnosedatei aufgrund einer zu großen Dateigröße erfasst werden.

Wenden Sie sich für weitere Unterstützung an den Cisco Support.

Weltweiter Kontakt zum Cisco Support

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.