Debug op endpoint inschakelen vanuit AMP voor endpointconsole

Inhoud

Inleiding

Dit document beschrijft hoe u debug op het endpoint kunt inschakelen vanuit Cisco Secure Endpoint Console.

Voorwaarden

Vereisten

Zorg er voordat u begint voor dat u:

- Administratieve toegang tot de Cisco Secure Endpoint voor Endpoints-console.
- Het eindpunt dat u wilt nemen, wordt al geregistreerd in Cisco Secure Endpoint

Gebruikte componenten

De in het document gebruikte informatie is gebaseerd op deze softwareversies:

- Cisco Secure Endpoint Console versie 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 en hoger
- Microsoft Windows-besturingssysteem

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De gegenereerde diagnostische gegevens kunnen aan het Cisco Technical Assistance Center (TAC) worden geleverd voor verdere analyse.

De diagnostische gegevens omvatten informatie zoals:

- Resourcegebruik (schijf, CPU en geheugen)
- Connectorspecifieke logbestanden
- Informatie over configuratie van connector

Probleem

Schakel Debug on Endpoint uit vanaf Cisco Secure Endpoint console is vereist tijdens een van deze scenario's.

Scenario 1: Als u het apparaat herstart, schakel Debug modus in vanaf de interface van het IP-tray of het overleeft de herstart niet. In het geval dat bootup debug logboeken worden vereist, kunt u Debug modus inschakelen vanuit de beleidsconfiguratie in de Secure Endpoint console.

Scenario 2: Als u prestatieproblemen ondervindt met de Cisco Secure Endpoint Connector op een apparaat, kan het inschakelen van de Debug-modus u helpen gedetailleerde logbestanden voor analyse te verzamelen.

Scenario 3: Wanneer u specifieke problemen met de Secure Endpoint Connector oplost, kunnen gedetailleerde logbestanden inzicht geven in de oorzaak van het probleem.

Configureren

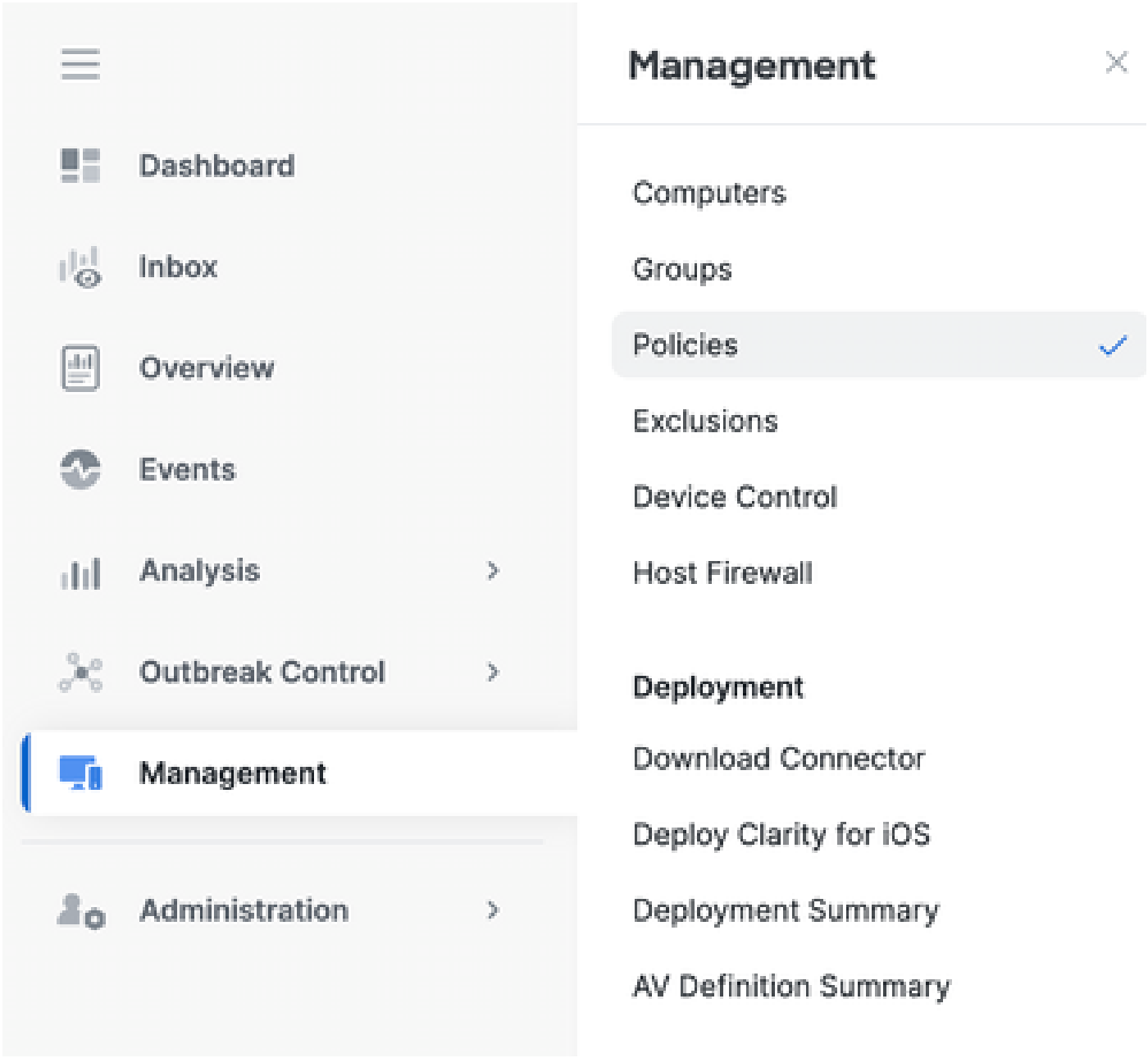
Voltooi deze stappen om de debugmodus op het opgegeven eindpunt met succes in te schakelen via de Secure Endpoint Console.

Stap 1: Identificeer het te verplaatsen eindpunt om te debuggen

1. Log in op Cisco Secure Endpoint console. Ga van het hoofddashboard naar de sectie Beheer.
2. Navigeren naar Beheer > Computers.
3. Identificeer en noteer het eindpunt dat debug modus vereist.

Stap 2: Het bestaande beleid dupliceren

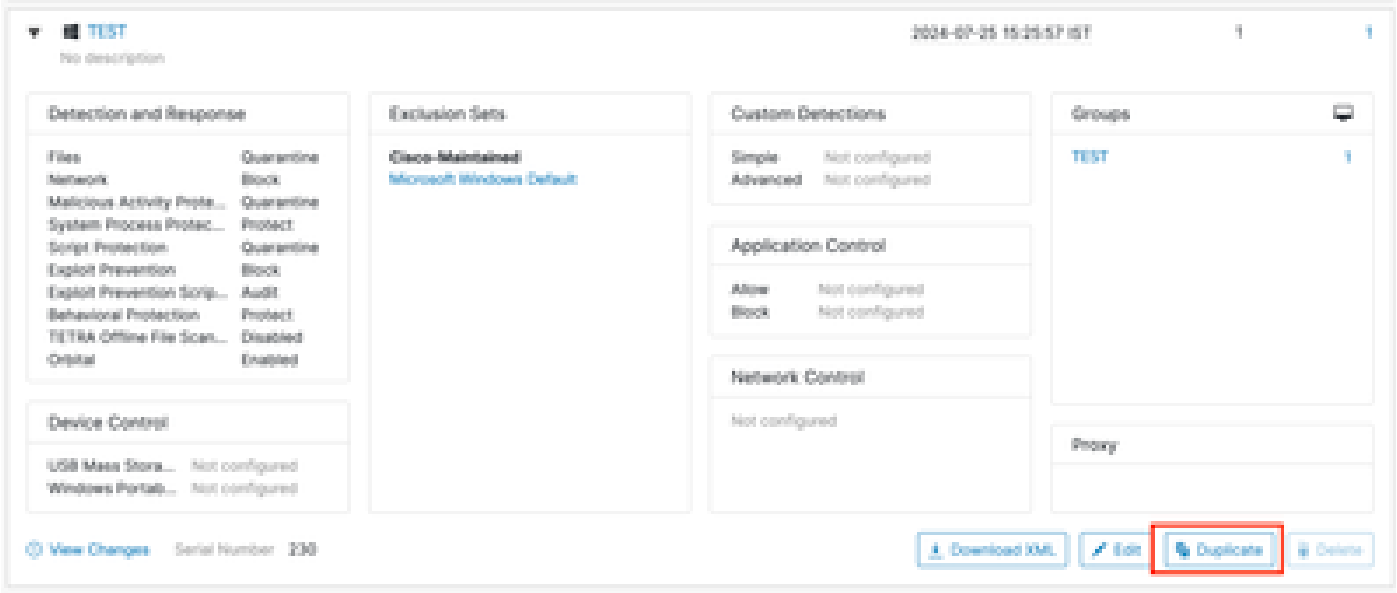
1. Navigeren naar Beheer > Beleid.



2. Bepaal de plaats van het beleid dat momenteel op het geïdentificeerde eindpunt wordt toegepast.

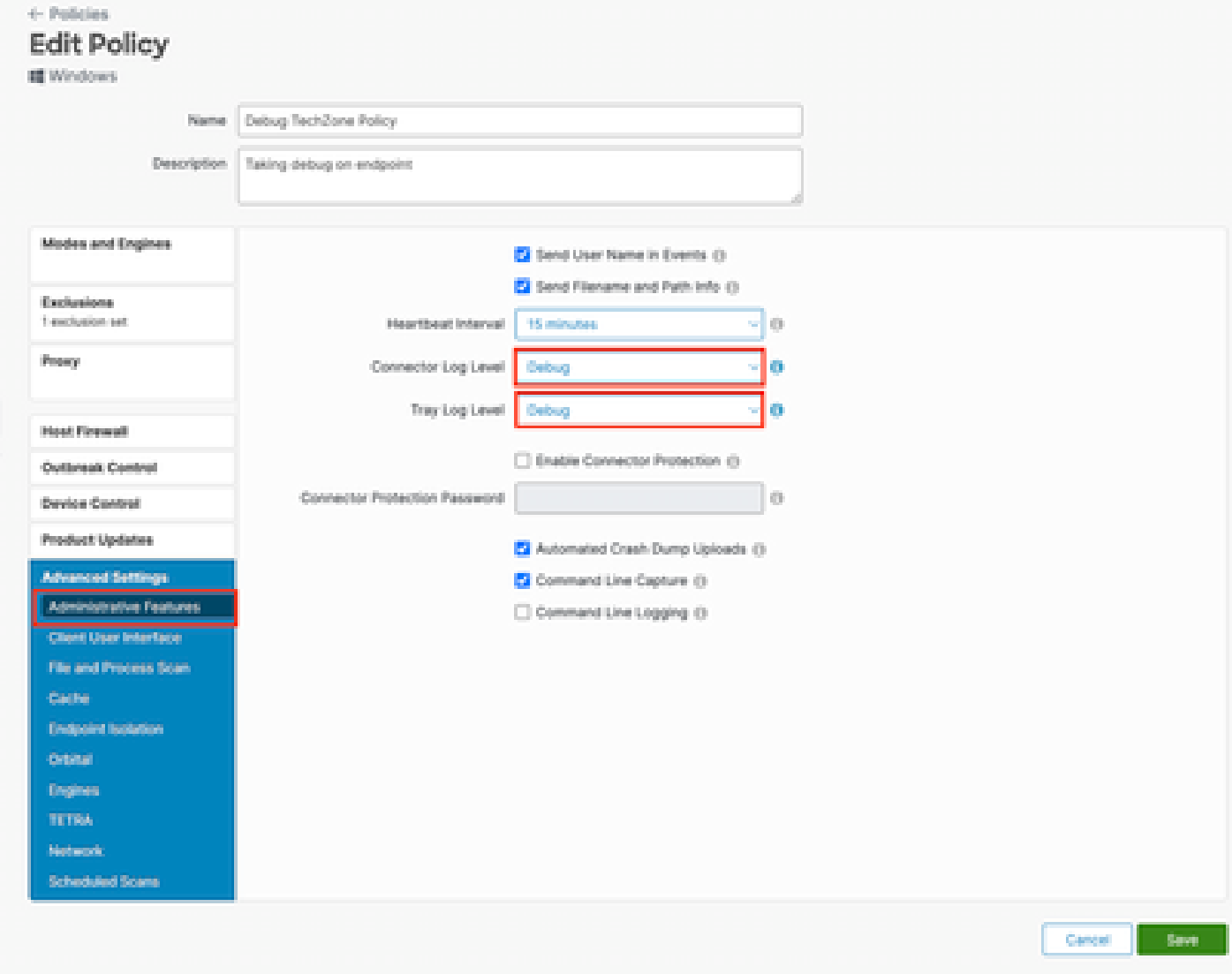
3. Klik op het beleid om het beleidsvenster uit te vouwen.

4. Klik op Dupliceren om een kopie van het bestaande beleid te maken.



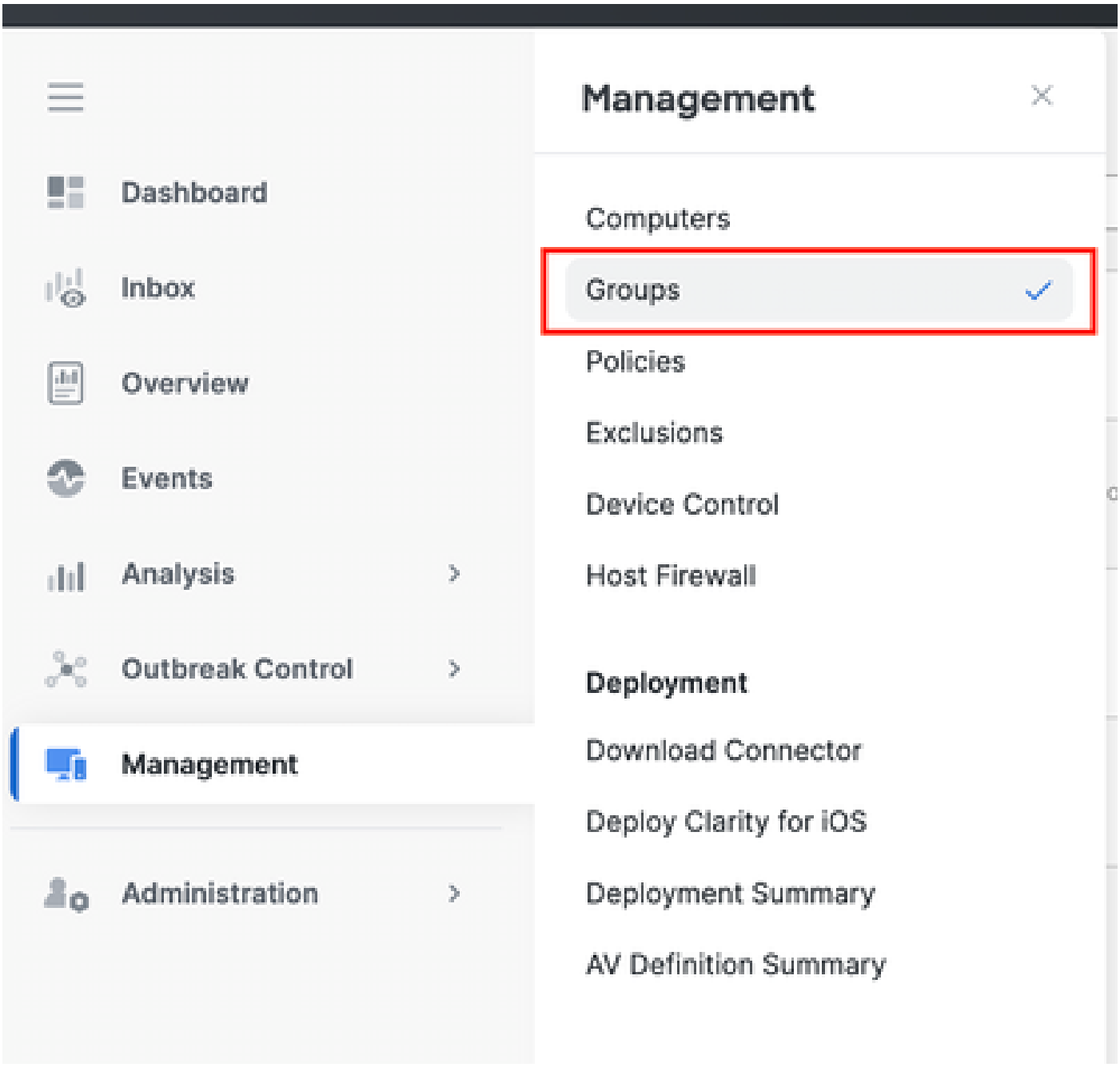
Stap 3: Configureer het logniveau om dit beleid te debuggen

1. Selecteer en vouw het gedupliceerde beleidsvenster uit.
2. Klik op Bewerken en hernoemen van het beleid (bijvoorbeeld Debug TechZone Policy).
3. Klik op Geavanceerde instellingen.
4. Selecteer Administratieve functies in de knoppenbalk.
5. Stel zowel het Connector Log Level als het Tray Log Level in op Debug.
6. Klik op Opslaan om de wijzigingen op te slaan.



Stap 4: Maak een nieuwe groep en koppel dat nieuwe beleid

1. Navigeren naar Beheer > Groepen.

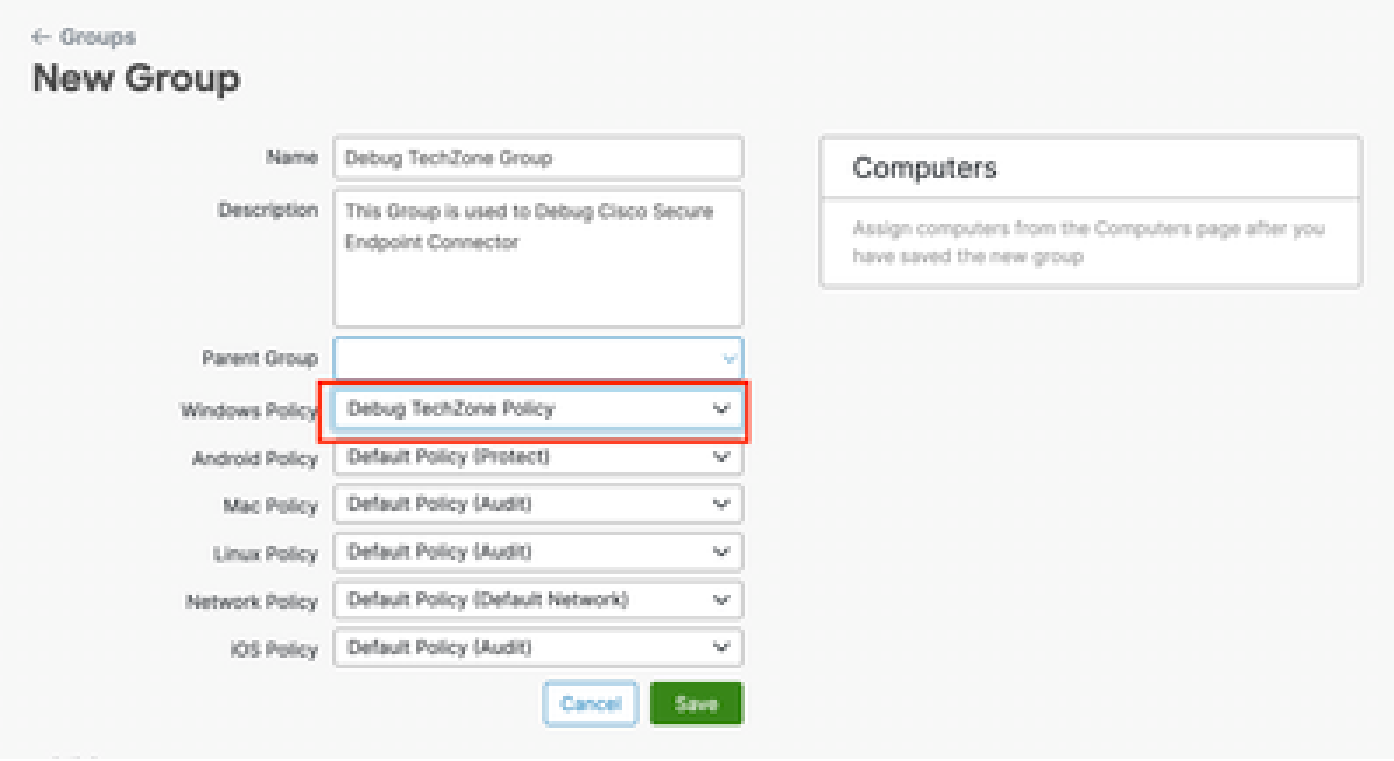


2. Klik op Create Group rechtsboven op het scherm.

3. Voer een naam in voor de groep (bijvoorbeeld Debug TechZone Group.)

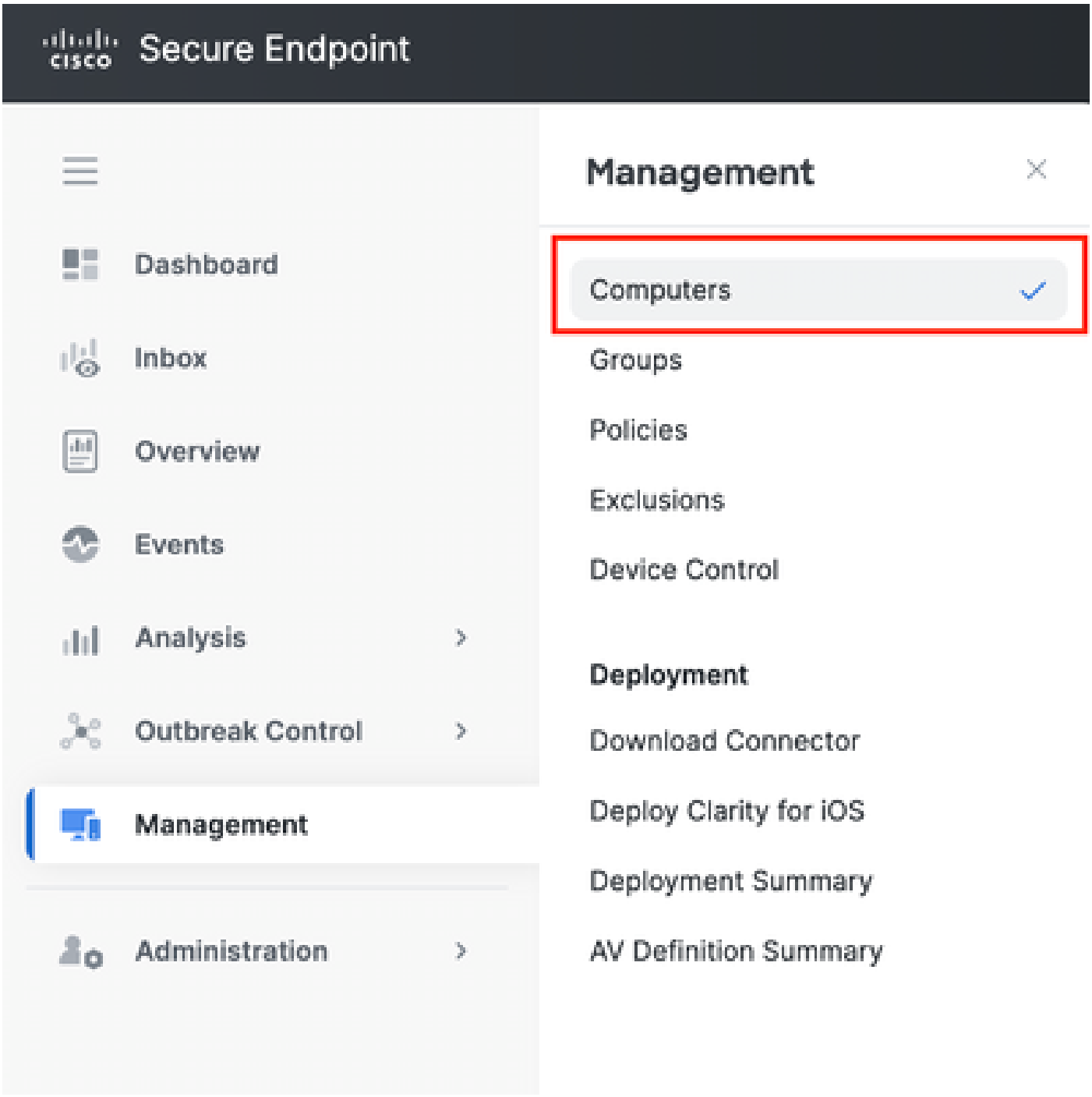
4. Verander het beleid van de standaardinstelling naar het nieuwe debug-beleid.

5. Klik op Opslaan.



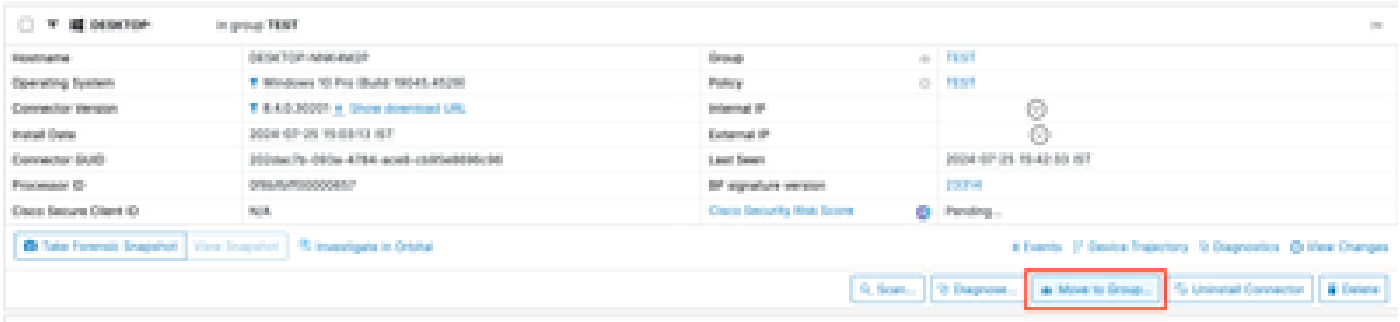
Stap 5: Verplaats het geïdentificeerde eindpunt naar deze nieuwe groep

1. Ga terug naar Beheer > Computers.



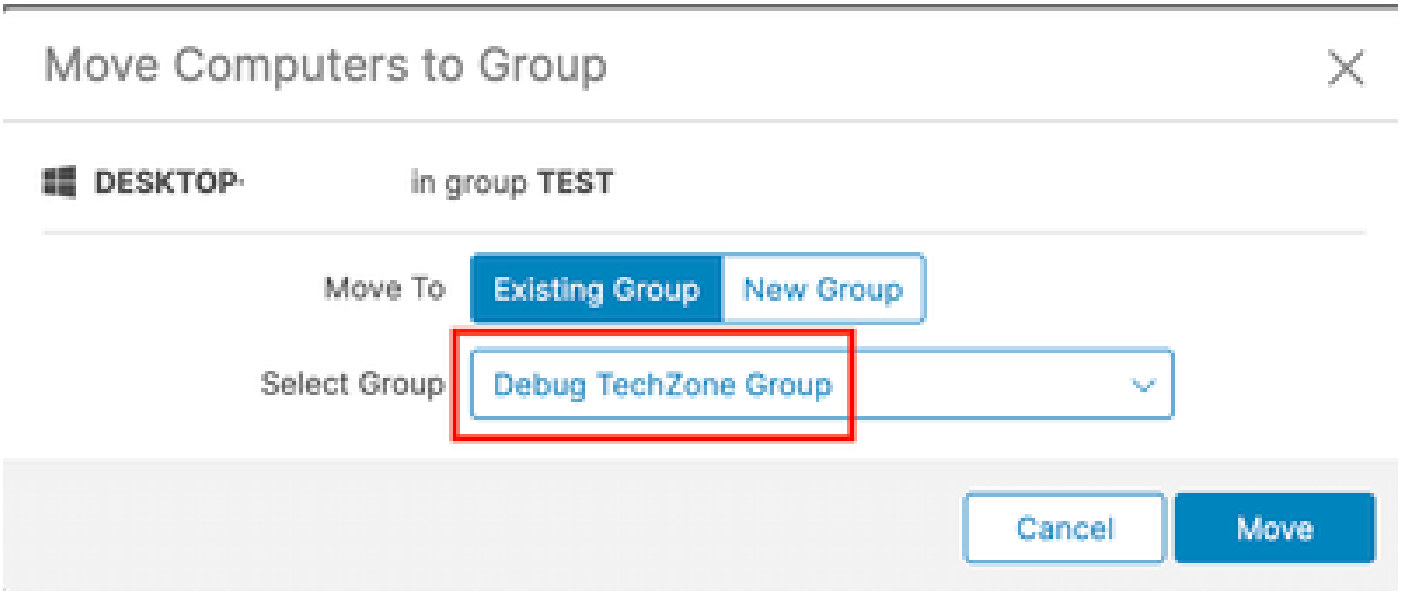
2. Selecteer het geïdentificeerde eindpunt in de lijst.

3. Klik op Verplaatsen naar groep.



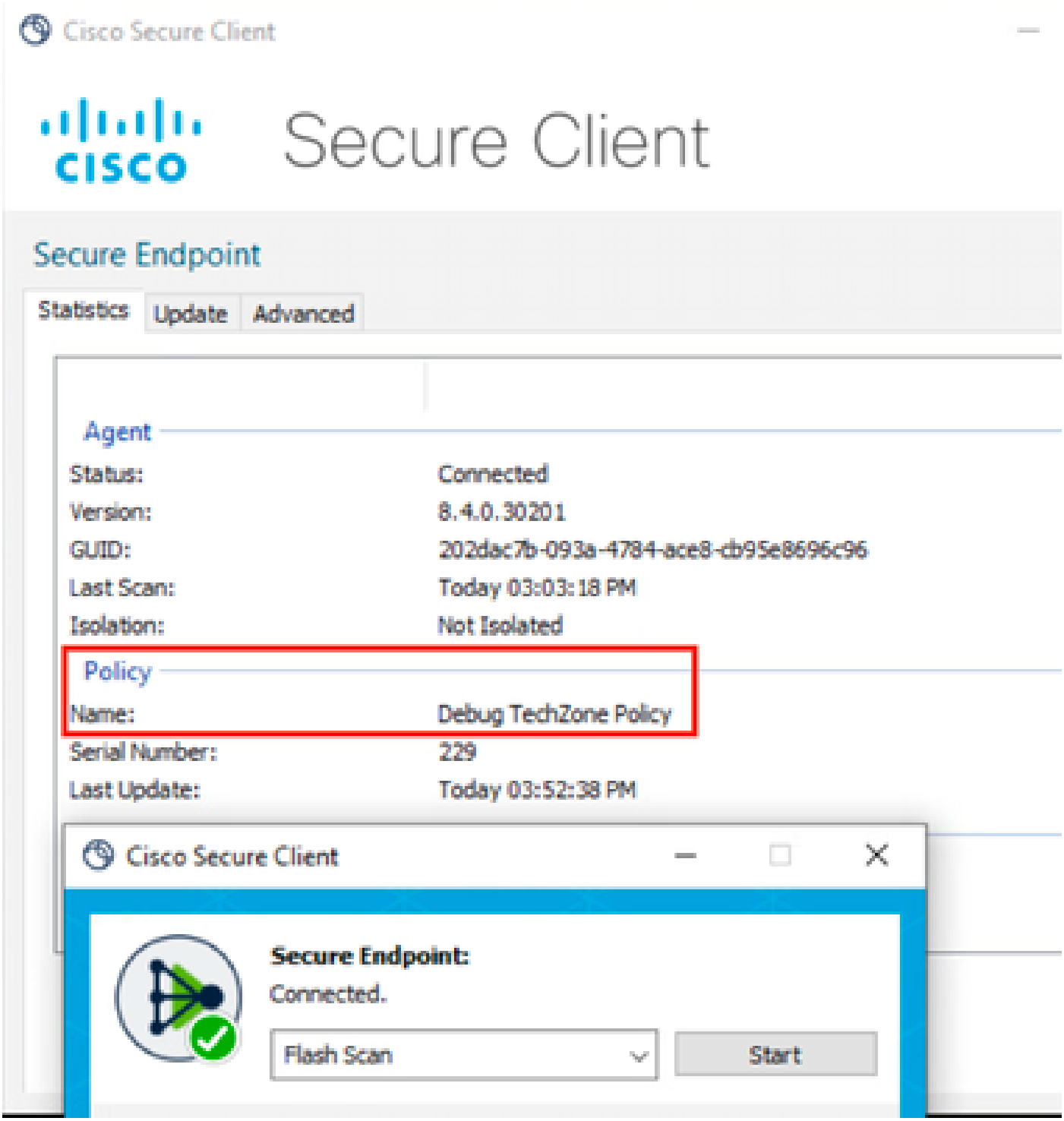
4. Selecteer de nieuwe groep in het vervolgkeuzemenu Groep selecteren.

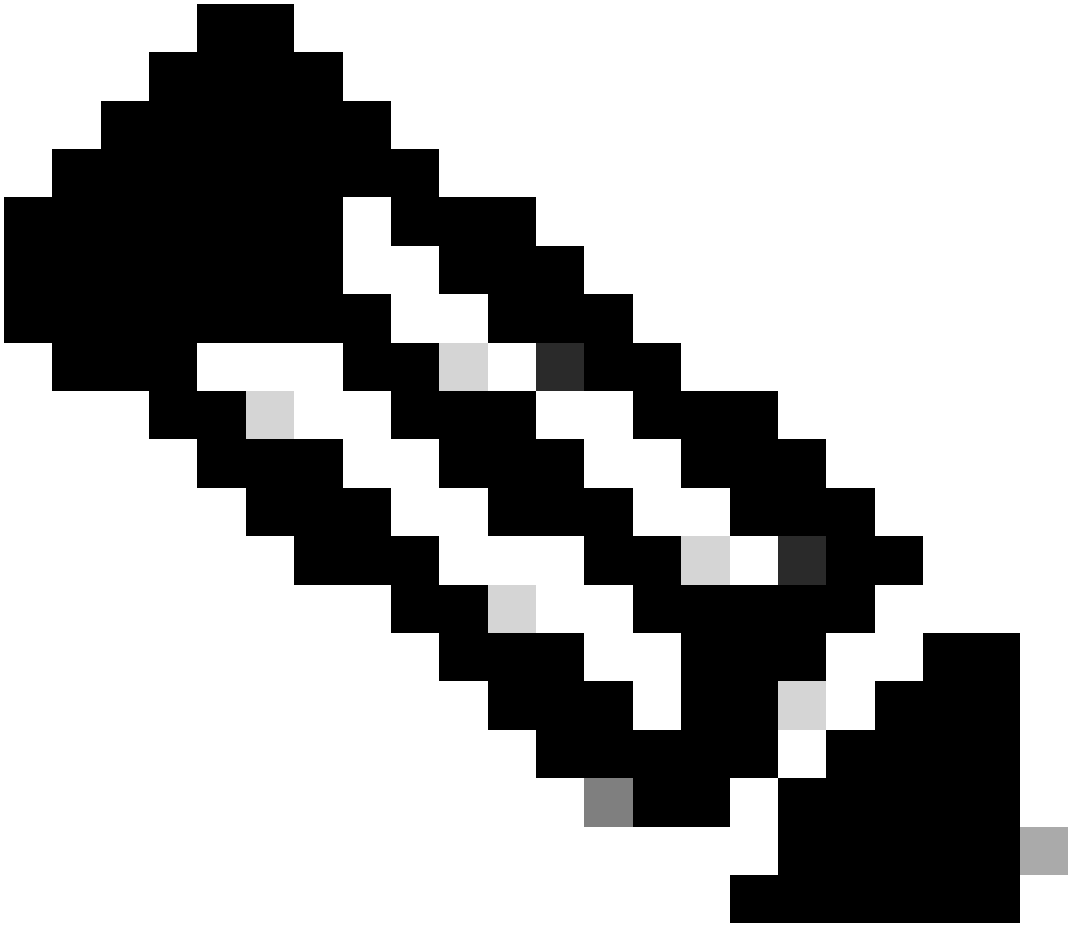
5. Klik op Verplaatsen om het geselecteerde eindpunt naar de nieuwe groep te verplaatsen.



Stap 6: Controleer het eindpunt op de pagina van de computer en in de connector-gebruikersinterface

1. Zorg ervoor dat het eindpunt in de nieuwe groep op de pagina Computers wordt vermeld.
2. Open in het eindpunt de Secure Endpoint-connector UI.
3. Controleer dat het nieuwe debug-beleid wordt toegepast door het pictogram Secure Endpoint op de menubalk te controleren.


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



Opmerking: de debug-modus kan alleen worden ingeschakeld als een Cisco Technical Support Engineer om deze gegevens verzoekt. Door de debug-modus voor een langere periode ingeschakeld te houden, kan de schijfruimte snel worden gevuld en kan worden voorkomen dat de loggegevens van de connector-log en -tray worden verzameld in het diagnostische bestand voor ondersteuning als gevolg van buitensporige bestandsgrootte.

Neem contact op met Cisco ondersteuning voor verdere assistentie.

Cisco's wereldwijde contactgegevens voor ondersteuning

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.