Abilita debug su endpoint da AMP for Endpoint Console

Sommario

Introduzione

In questo documento viene descritto come abilitare il debug sull'endpoint da Cisco Secure Endpoint Console.

Prerequisiti

Requisiti

Prima di iniziare, assicurati di avere:

- Accesso amministrativo alla console Cisco Secure Endpoint for Endpoints.
- L'endpoint di cui eseguire il debug è già registrato in Cisco Secure Endpoint

Componenti usati

Le informazioni contenute nel documento si basano sulle seguenti versioni software:

- Cisco Secure Endpoint Console versione 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 e versioni successive
- Sistema operativo Microsoft Windows

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

I dati diagnostici generati possono essere forniti al Cisco Technical Assistance Center (TAC) per ulteriori analisi.

I dati diagnostici includono informazioni quali:

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

Problema

in uno di questi scenari è necessario abilitare il debug sull'endpoint da Cisco Secure Endpoint Console.

Scenario 1: se si riavvia il dispositivo, abilitare la modalità di debug dall'interfaccia della barra delle applicazioni IP altrimenti il riavvio non verrà completato. Se sono necessari log di debug di avvio, è possibile abilitare la modalità di debug dalla configurazione dei criteri nella console dell'endpoint sicuro.

Scenario 2: se si verificano problemi di prestazioni con Cisco Secure Endpoint Connector su un dispositivo, l'abilitazione della modalità di debug può aiutare a raccogliere i log dettagliati per l'analisi.

Scenario 3: quando si risolvono problemi specifici con Secure Endpoint Connector, i registri dettagliati possono fornire informazioni dettagliate sulla causa principale del problema.

Configurazione

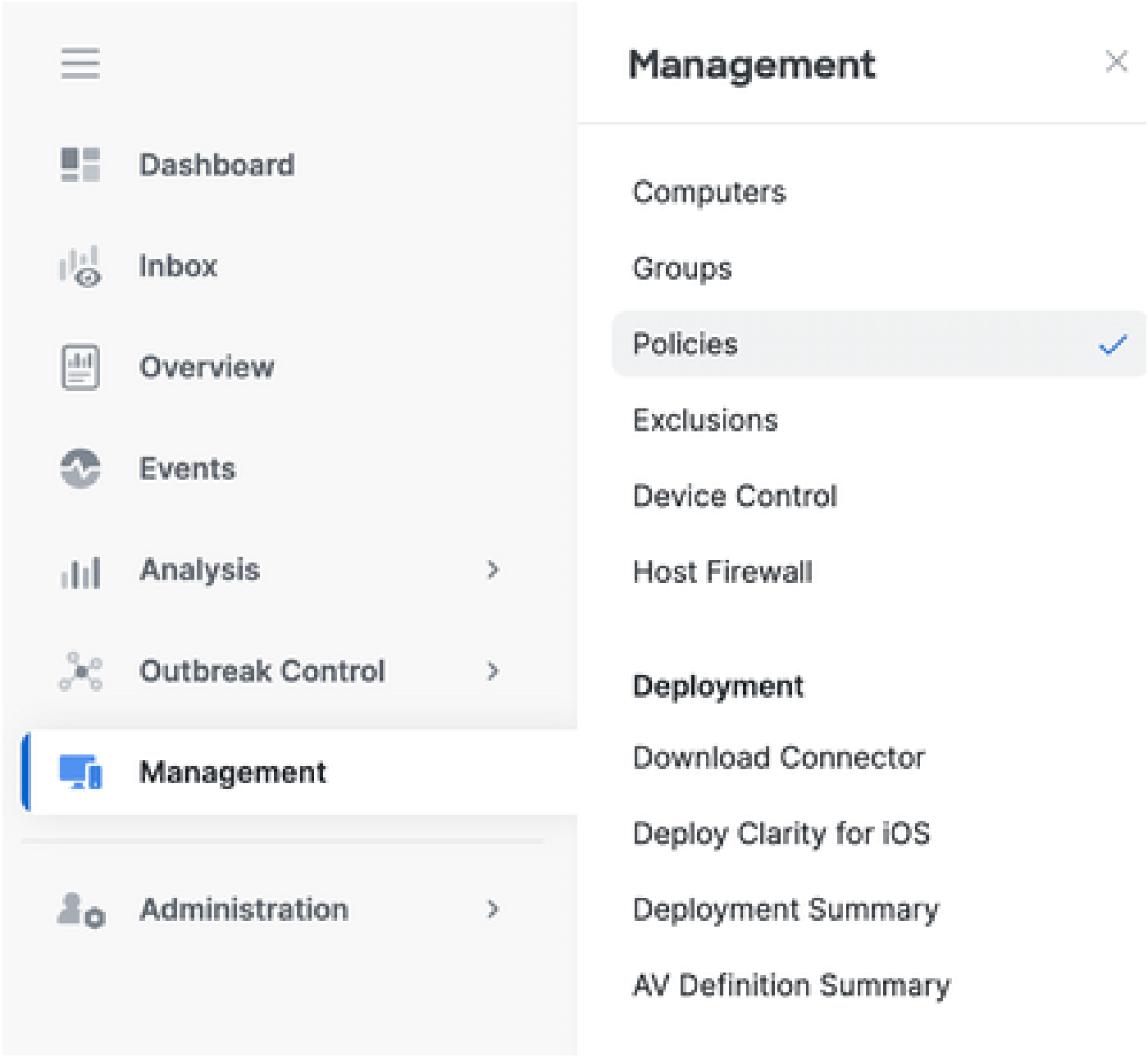
Completare la procedura seguente per abilitare correttamente la modalità di debug sull'endpoint specificato tramite la console dell'endpoint sicuro.

Passaggio 1: Identificare l'endpoint da spostare nel debug

1. Accedere alla console Cisco Secure Endpoint. Dal dashboard principale, passare alla sezione Gestione.
2. Selezionare Gestione > Computer.
3. Identificare e annotare l'endpoint che richiede la modalità di debug.

Passaggio 2: Duplicare il criterio esistente

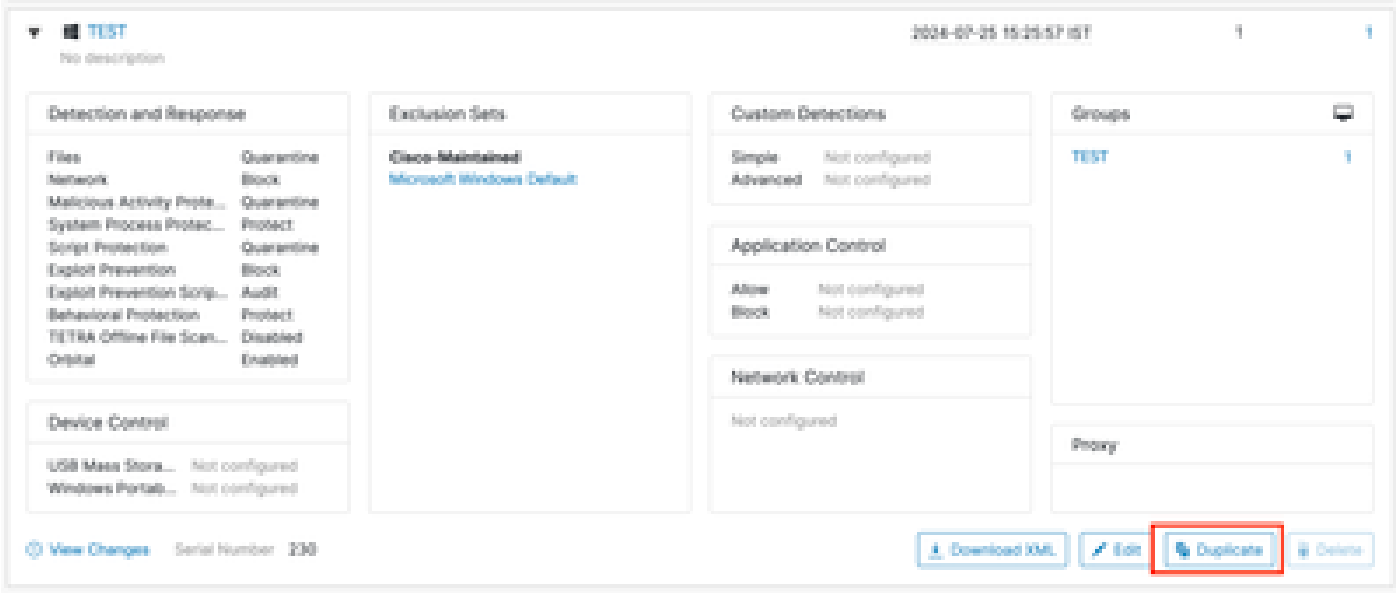
1. Passare a Gestione > Criteri.



2. Individuare il criterio attualmente applicato all'endpoint identificato.

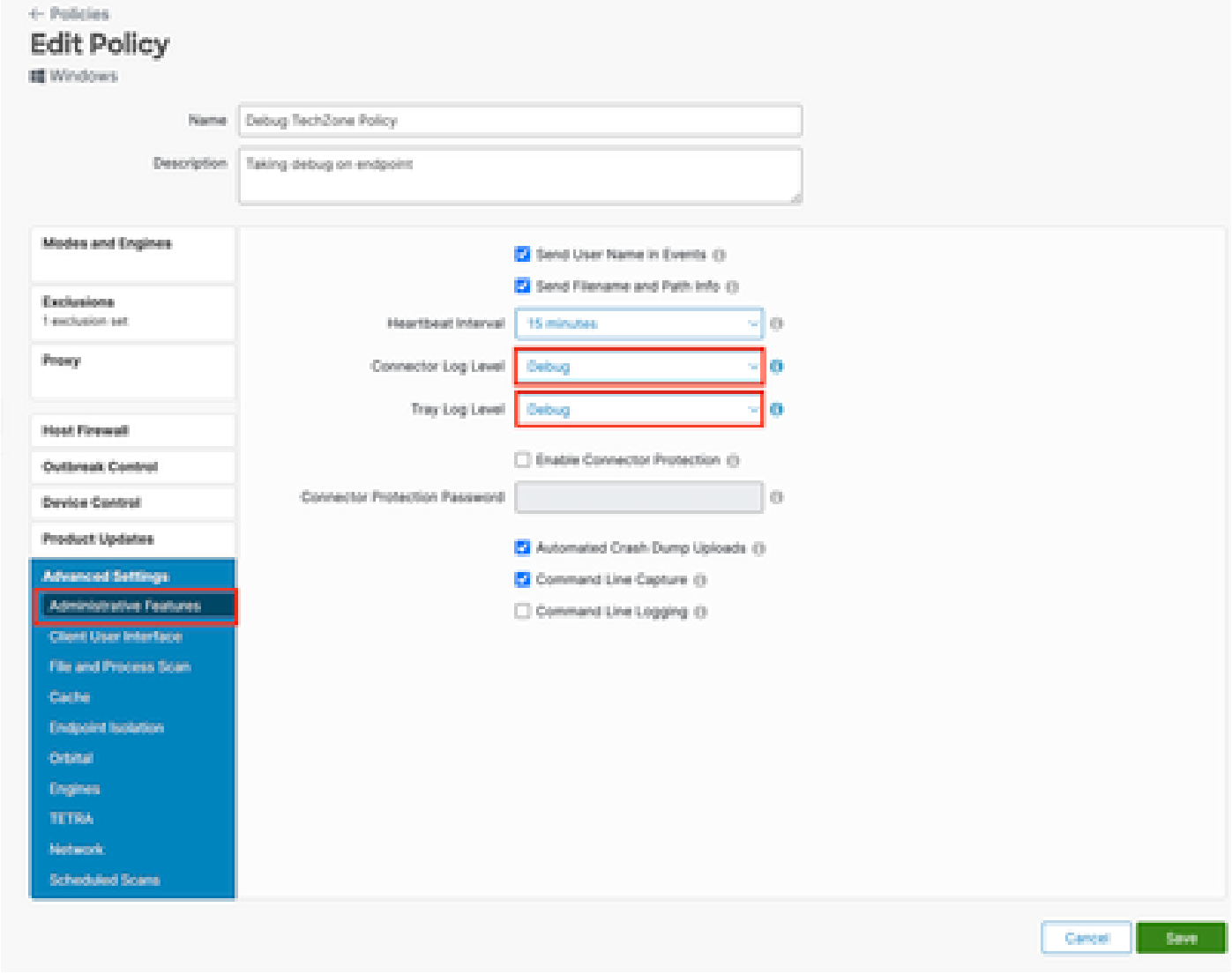
3. Fare clic sul criterio per espandere la relativa finestra.

4. Fare clic su Duplica per creare una copia del criterio esistente.



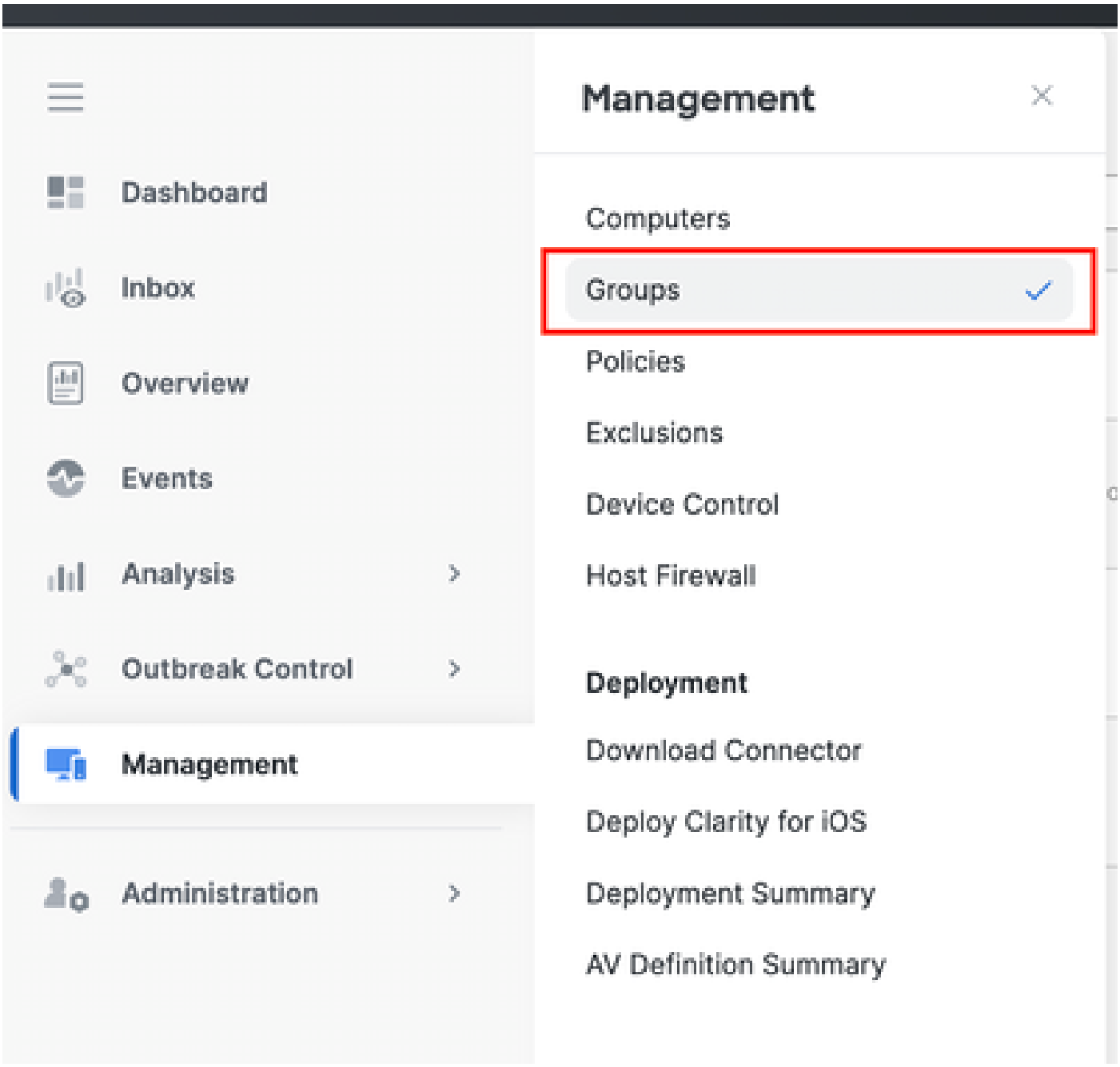
Passaggio 3: Configurare il livello di log per eseguire il debug del criterio

1. Selezionare ed espandere la finestra dei criteri duplicati.
2. Fare clic su Modifica e rinominare il criterio (ad esempio, Debug criterio TechZone).
3. Fare clic su Impostazioni avanzate.
4. Selezionare Funzioni amministrative dalla barra laterale.
5. Impostare Connector Log Level (Livello log connettore) e Tray Log Level (Livello log cassetto) su Debug.
6. Fare clic su Salva per salvare le modifiche.



Passaggio 4: Creare un nuovo gruppo e collegare il nuovo criterio

1. Selezionare Gestione > Gruppi.

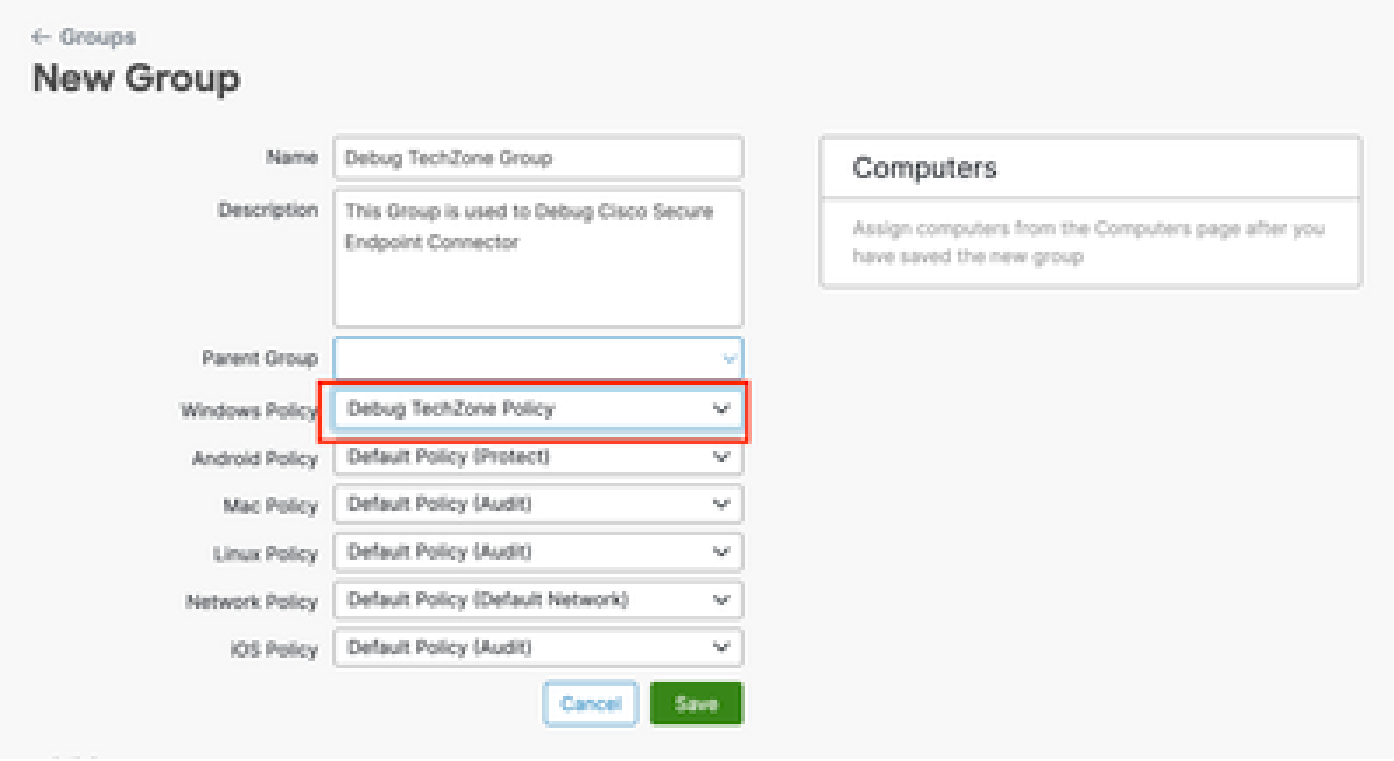


2. Fare clic su Create Group (Crea gruppo) nella parte superiore destra dello schermo.

3. Inserire un nome per il gruppo (ad esempio, Debug TechZone Group).

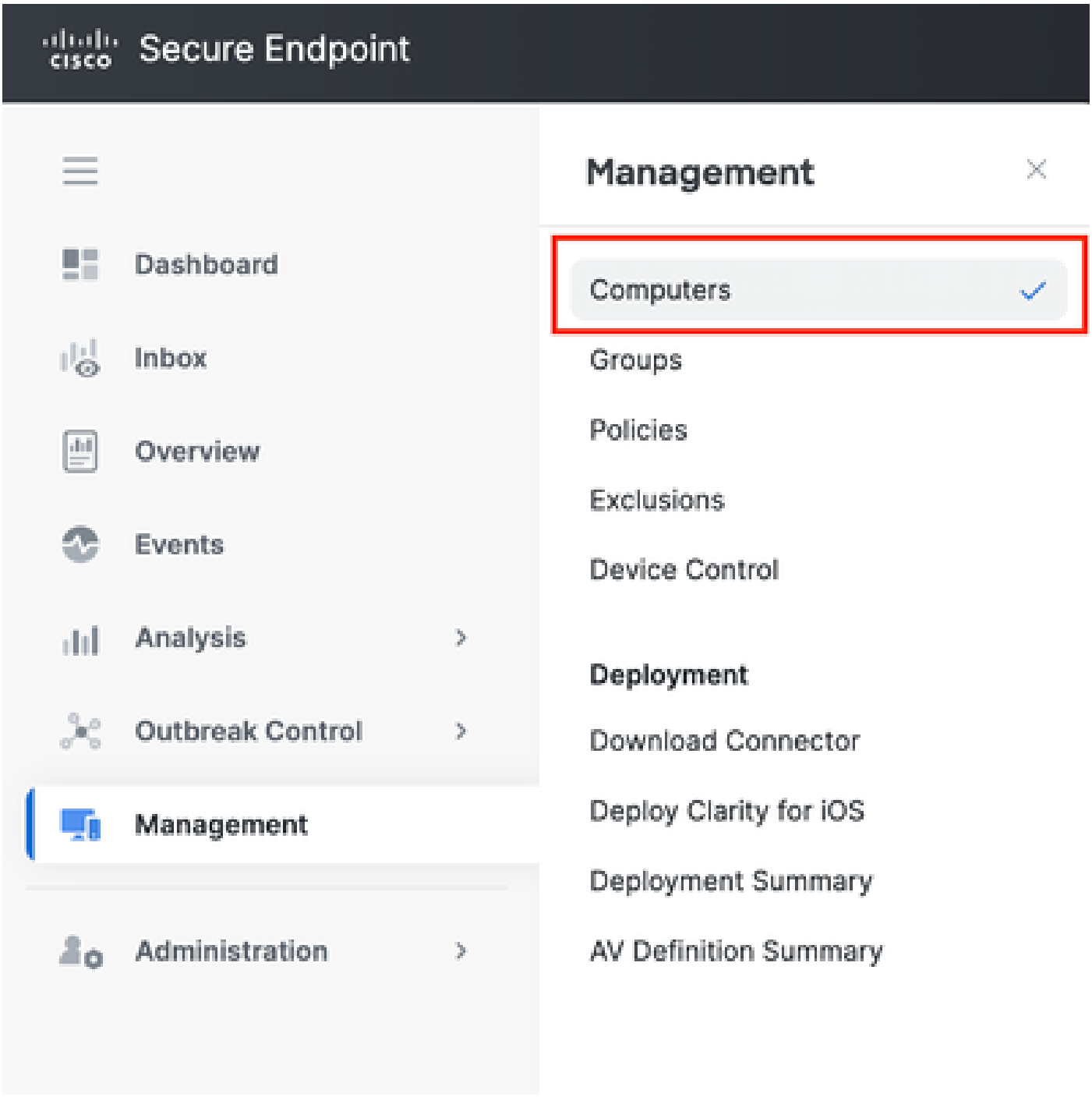
4. Modificare il criterio da quello predefinito a quello appena creato.

5. Fare clic su Salva.



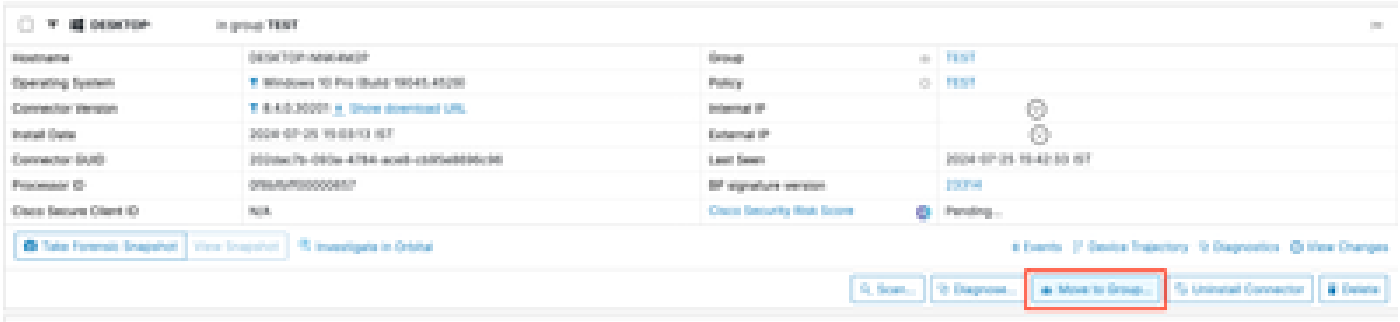
Passaggio 5: Spostare l'endpoint identificato in questo nuovo gruppo

1. Tornare a Gestione > Computer.



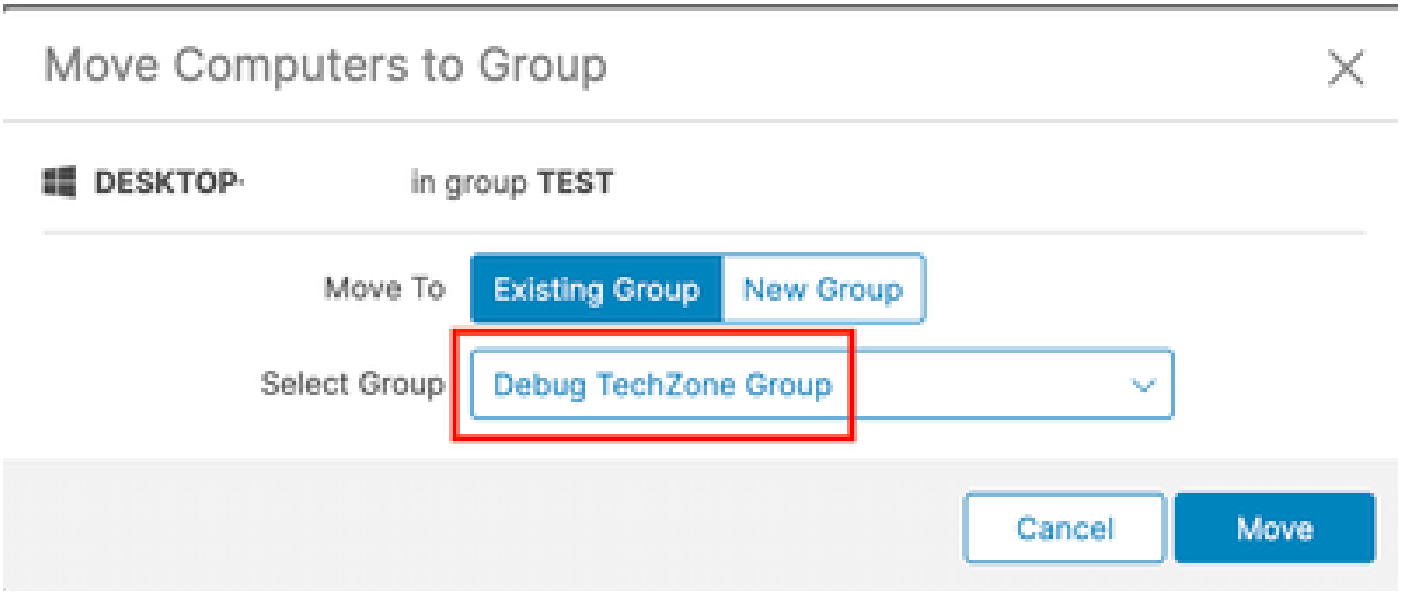
2. Selezionare l'endpoint identificato dall'elenco.

3. Fare clic su Sposta nel gruppo.



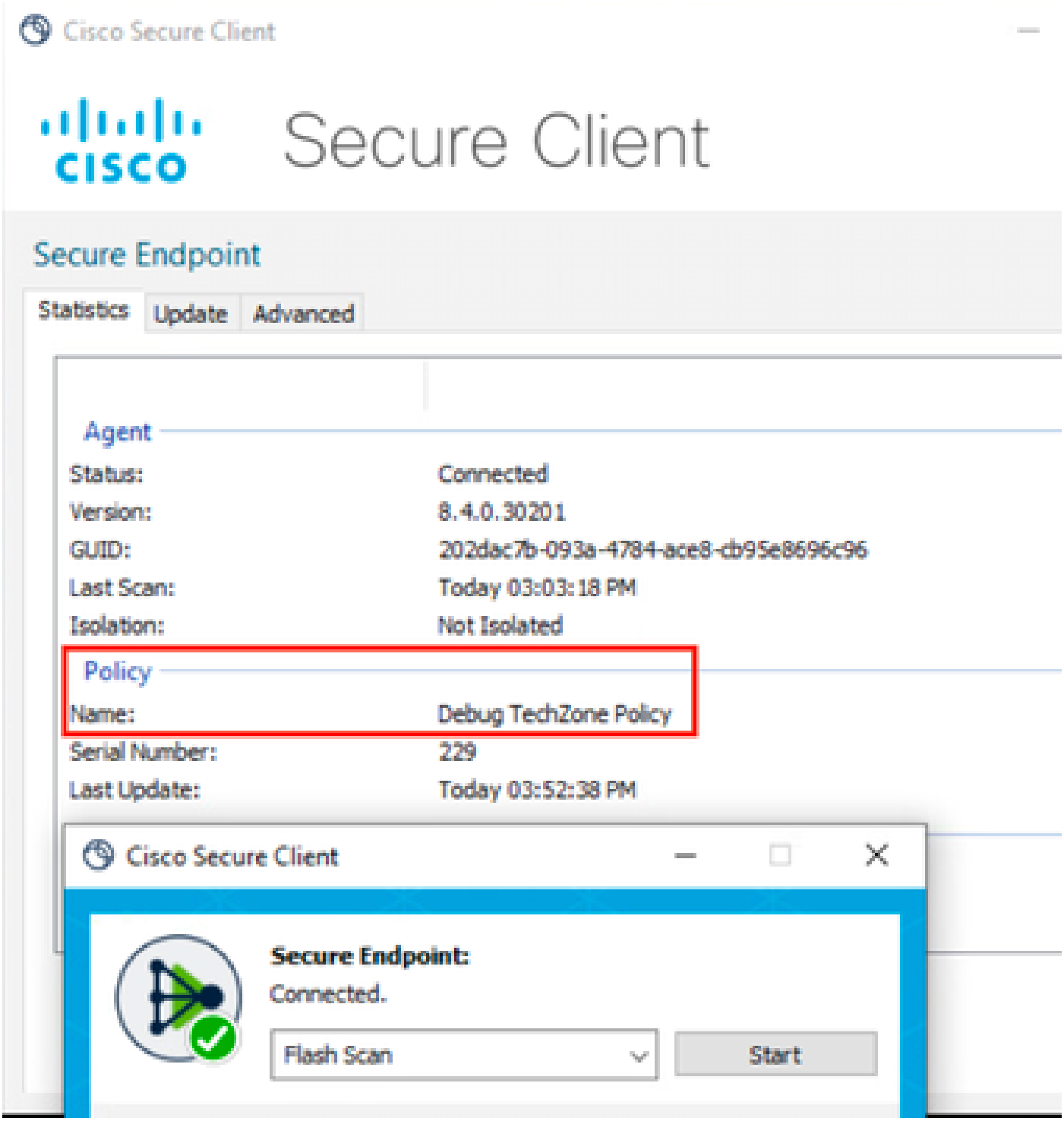
4. Selezionare il gruppo appena creato dal menu a discesa Seleziona gruppo.

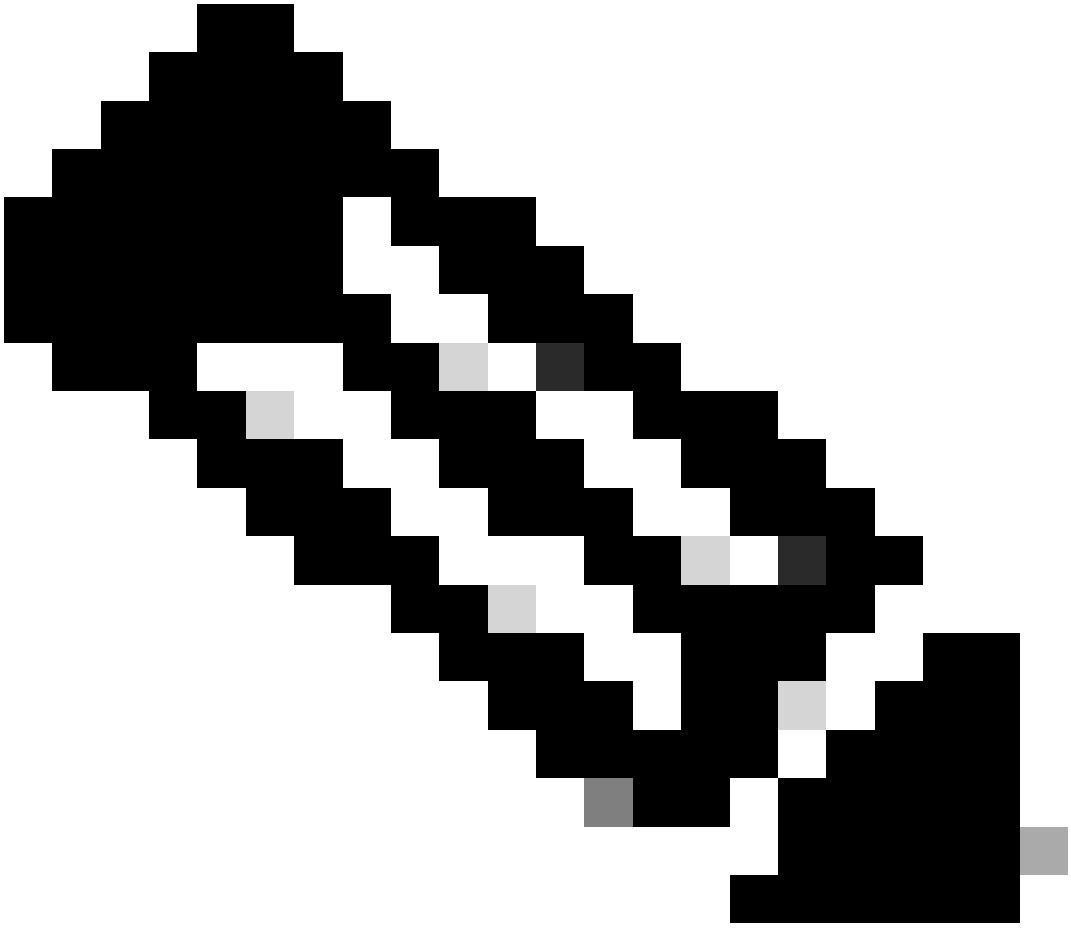
5. Fare clic su Sposta per spostare l'estremità selezionata nel nuovo gruppo.



Passaggio 6: Verificare l'endpoint nella pagina del computer e nell'interfaccia utente del connettore

1. Verificare che l'endpoint sia elencato sotto il nuovo gruppo nella pagina Computer.
2. Sull'endpoint, aprire l'interfaccia utente del connettore Secure Endpoint.
3. Verificare che il nuovo criterio di debug sia applicato selezionando l'icona Secure Endpoint nella barra dei menu.


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



Nota: la modalità di debug può essere abilitata solo se un tecnico del supporto Cisco richiede questi dati. Mantenere attiva la modalità di debug per un periodo di tempo prolungato può occupare spazio su disco rapidamente e impedire la raccolta dei dati del registro e del registro dell'area di notifica del connettore nel file di diagnostica del supporto a causa delle dimensioni eccessive del file.

Contatta il supporto Cisco per ulteriore assistenza.

Contatti del supporto Cisco internazionali

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).