Konfigurieren des automatisierten Workflows für die Endpunktisolierung mit Cisco XDR

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Automatisierungs-Workflow erstellen, um einen Endpunkt für einen neuen Vorfall zu isolieren.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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.

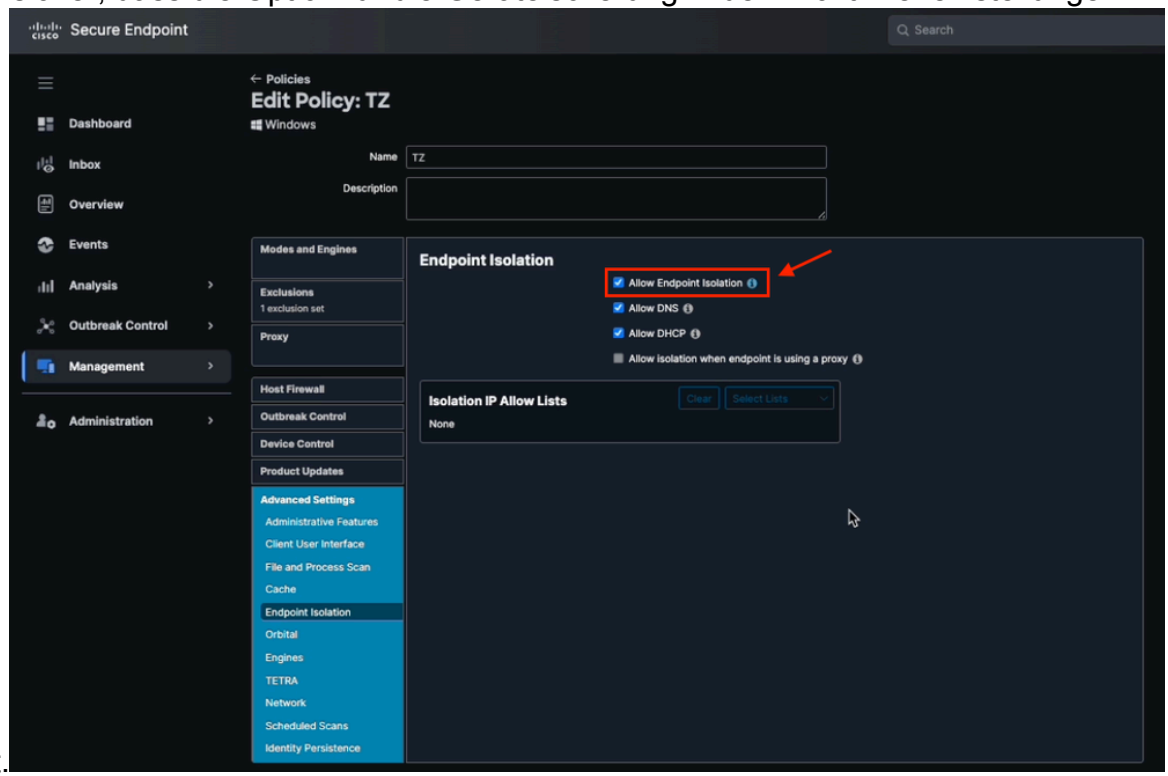
Konfigurieren

In diesem Leitfaden werden die erforderlichen Schritte zum Konfigurieren und Aktivieren eines Workflows beschrieben, mit dem ein Endpunkt bei einem Vorfall automatisch isoliert wird. Die Integration erfolgt mit Cisco Secure Endpoint und der Workflow-Automatisierungsfunktion. Die Schritte sind wie folgt skizziert.

Erstkonfiguration in Cisco Secure Endpoint

Phase 1.1: Aktivieren der Isolationsfunktion in der Richtlinie

1. Melden Sie sich beim Cisco Secure Endpoint-Portal an.
2. Navigieren Sie zum Abschnitt Verwaltung > Richtlinien.
3. Wählen Sie die Richtlinie aus, die auf den zu isolierenden Endpunkt angewendet wird.
4. Stellen Sie sicher, dass die Option für die Geräteisolierung in den Richtlinieneinstellungen aktiviert ist.



Endpunktisolierung von der Richtlinie für sichere Endpunkte zulassen

5. Speichern Sie die Änderungen, und verteilen Sie ggf. die Richtlinie.

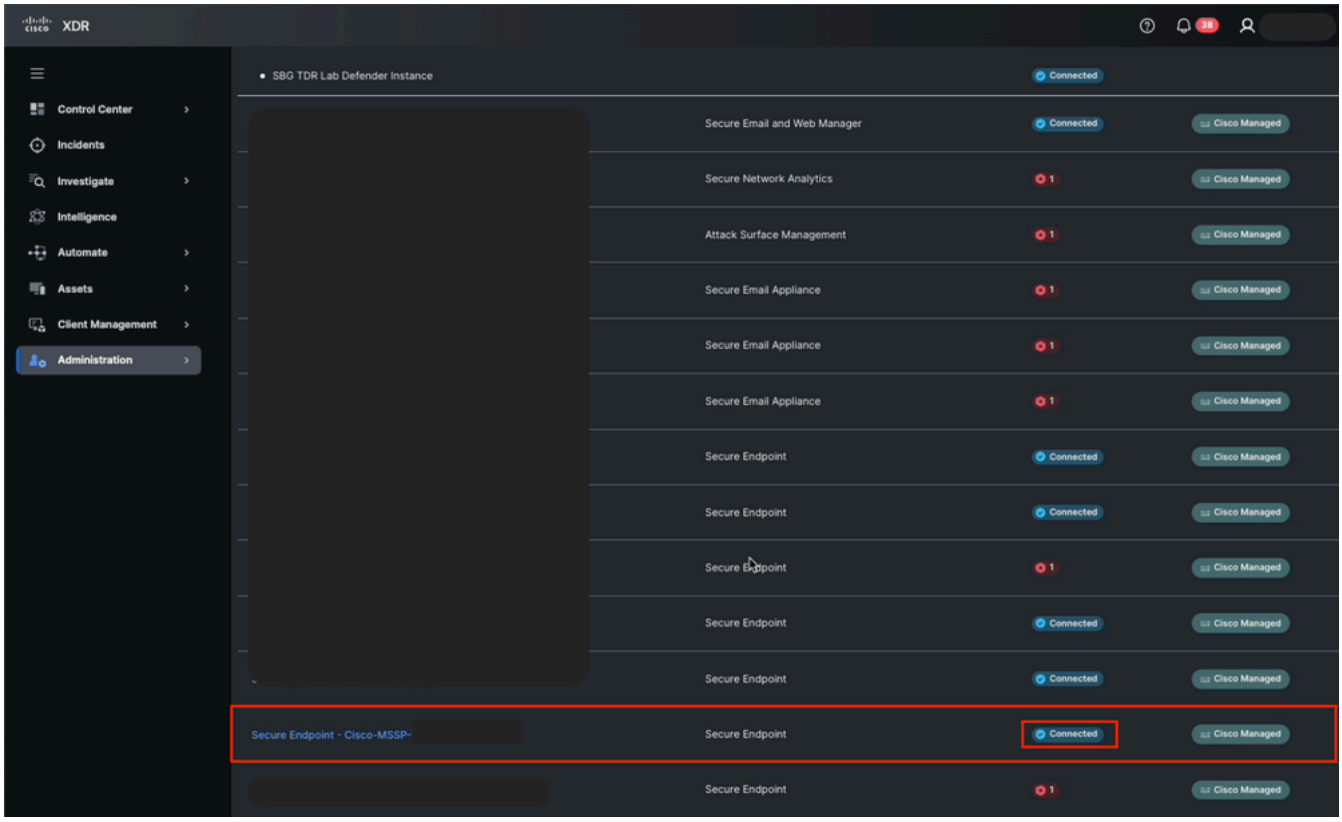
Validierung der Integration mit Cisco Secure Endpoint

Phase 2.1: Überprüfen der Integration

1. Bei Cisco XDR anmelden

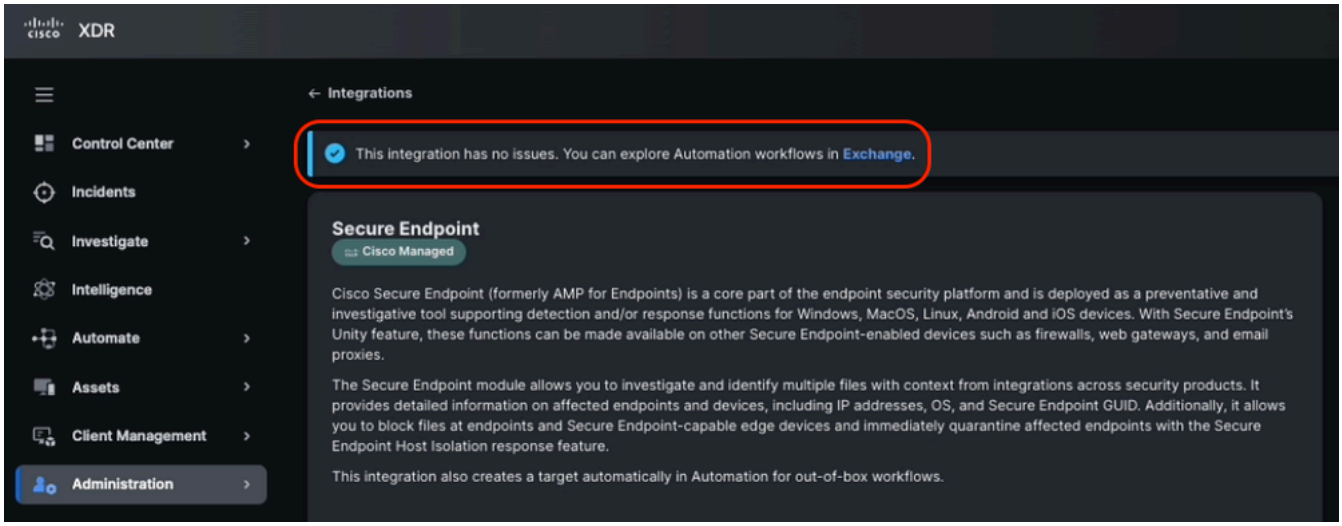
2. Navigieren Sie zu Administration > Integrations > My Integrations (Verwaltung > Integrationen > Meine Integrationen).
3. Stellen Sie sicher, dass die Integration mit Cisco Secure Endpoint ordnungsgemäß konfiguriert ist:

Überprüfen Sie den Integrationsstatus unter Verbunden.



Status der sicheren Endpunkt-Integration von Cisco XDR

Bestätigen Sie, dass keine Fehler in der API-Konfiguration vorliegen.

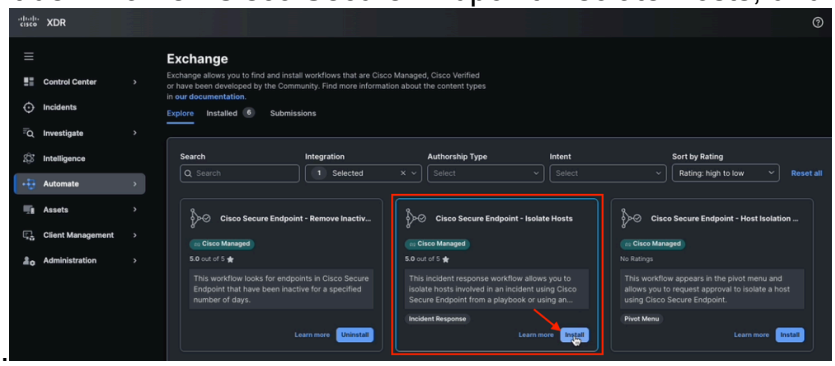


Integritätsprüfung der sicheren Endgeräteintegration

Workflow aus Cisco XDR Exchange installieren

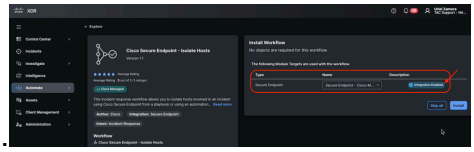
Phase 3.1: Installieren des Endpunktisolations-Workflows

1. Melden Sie sich bei Cisco XDR an, und navigieren Sie zu Automate > Exchange.
2. Suchen Sie nach dem Workflow mit dem Namen Cisco Secure Endpoint - Isolate Hosts, und klicken Sie auf Install (Installieren).



Host-Workflow von Exchange isolieren

3. Überprüfen Sie vor der Installation, ob das Ziel verfügbar ist.



Modulziel aus Workflow aktiviert

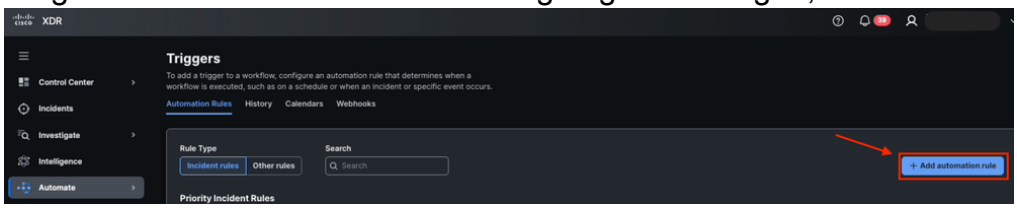
4. Installieren Sie den Workflow in Ihrem Automatisierungssystem.

Erstellen einer Automatisierungsregel

Eine Automatisierungsregel ist eine Konfiguration, die definiert, wann ein Workflow basierend auf bestimmten Ereignissen oder einem vordefinierten Zeitplan ausgeführt werden soll. Diese Regeln können optionale Bedingungen enthalten, und wenn diese Bedingungen erfüllt sind, werden die zugehörigen Workflows automatisch ausgelöst.

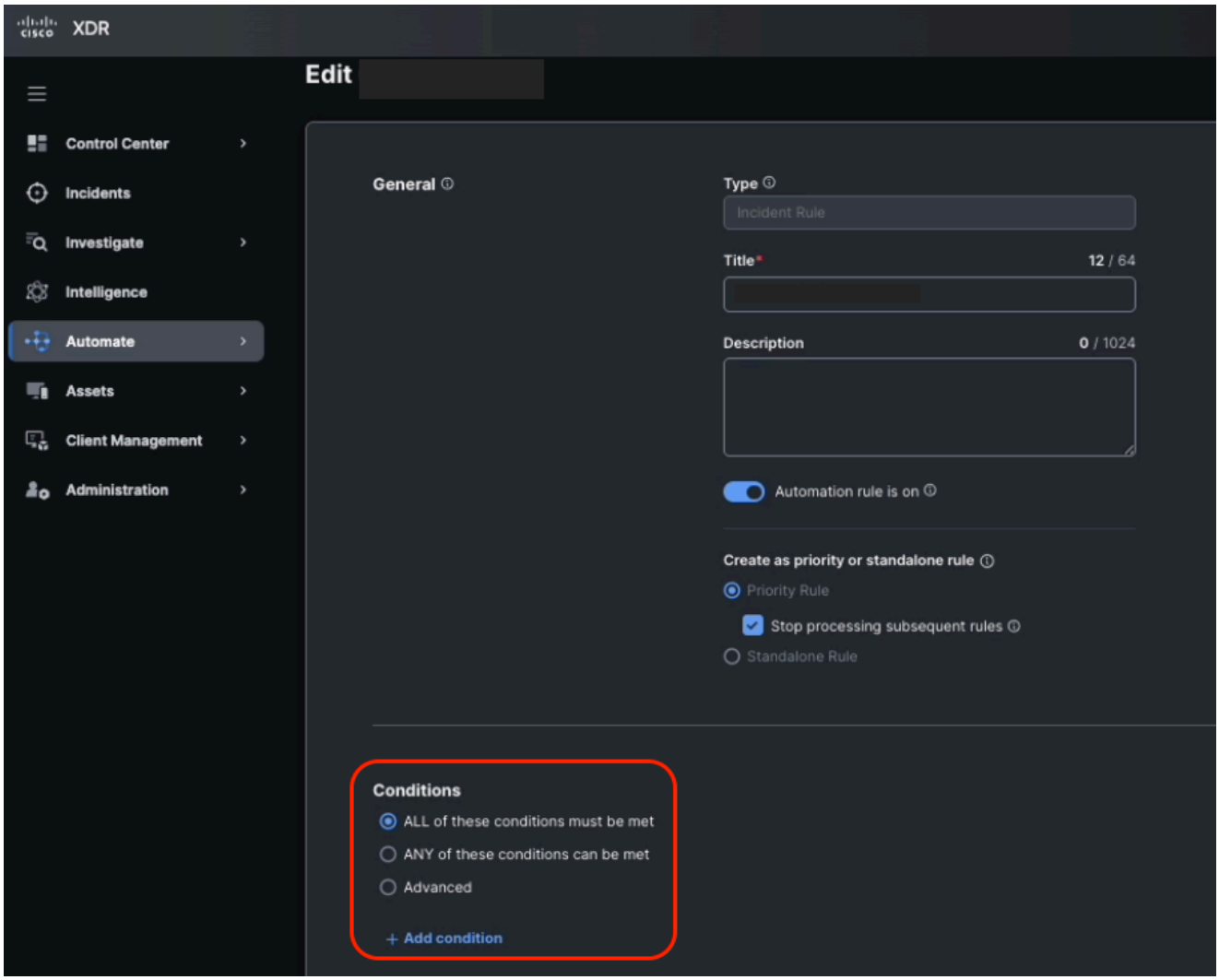
Phase 4.1: Konfigurieren einer Automatisierungsregel

1. Navigieren Sie zum Abschnitt Automatisierung > Trigger.
2. Erstellen einer neuen Regel Klicken Sie auf Automatisierungsregel hinzufügen, und weisen Sie einen Namen zu.



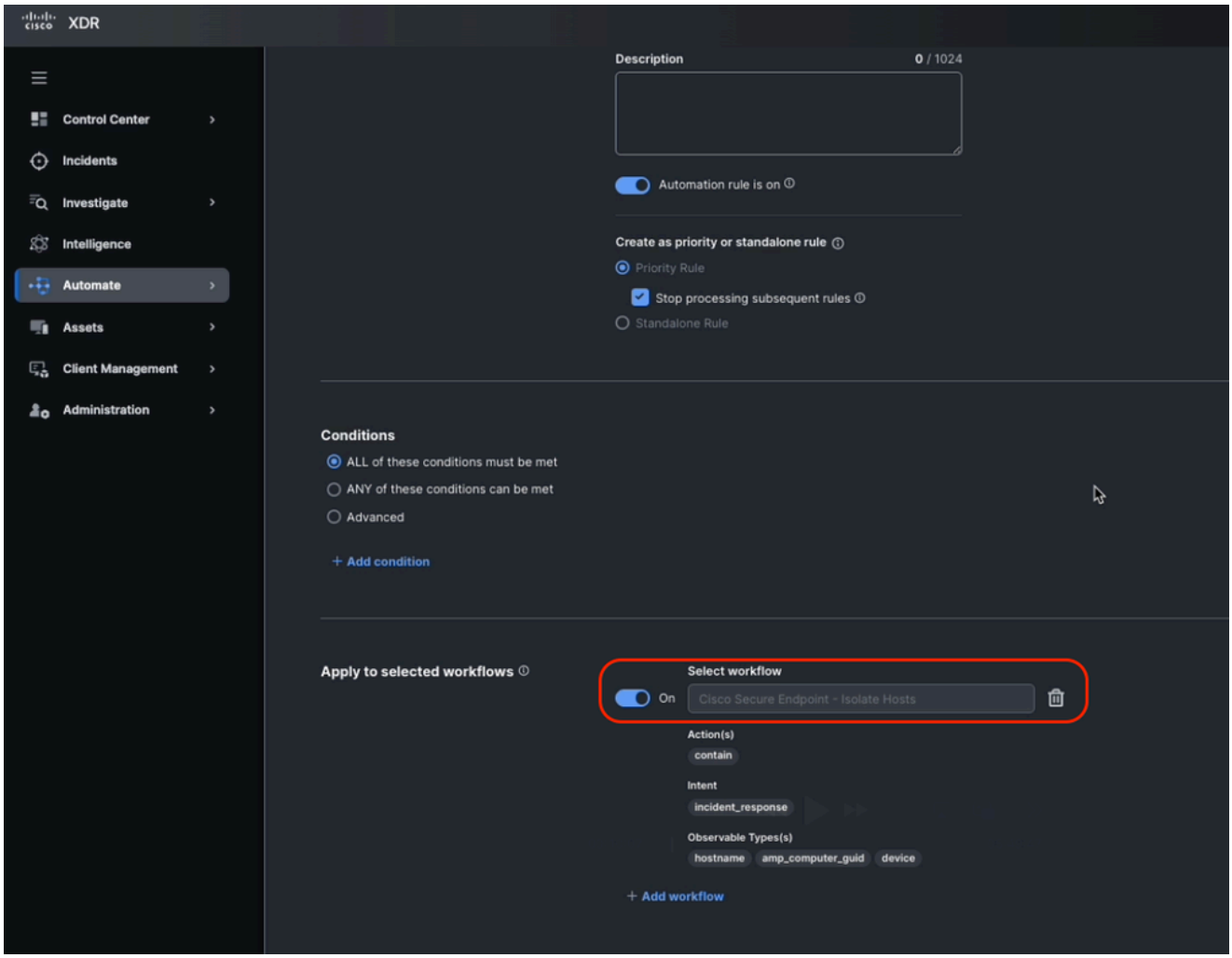
Automatisierungsregel aus Triggern hinzufügen

3. Stellen Sie die Auslösebedingungen ein. Sie können die Bedingungen leer lassen. Dadurch wird sichergestellt, dass jeder Vorfall diese Regel aktiviert. Passen Sie ggf. die Bedingung an.



Bedingungen für Automatisierungsregeln

4. Wählen Sie in der Aktion der Regel den zuvor installierten Workflow Cisco Secure Endpoint - Isolate Hosts aus.



Zuweisen der Automatisierungsregel zum Workflow

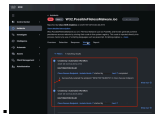
5. Klicken Sie auf Speichern.

Workflow-Funktionalität überprüfen

Phase 5.1: Workflow-Ausführung überprüfen

1. Generieren oder warten Sie auf einen Vorfall, der die Bedingungen der Regel erfüllt. 

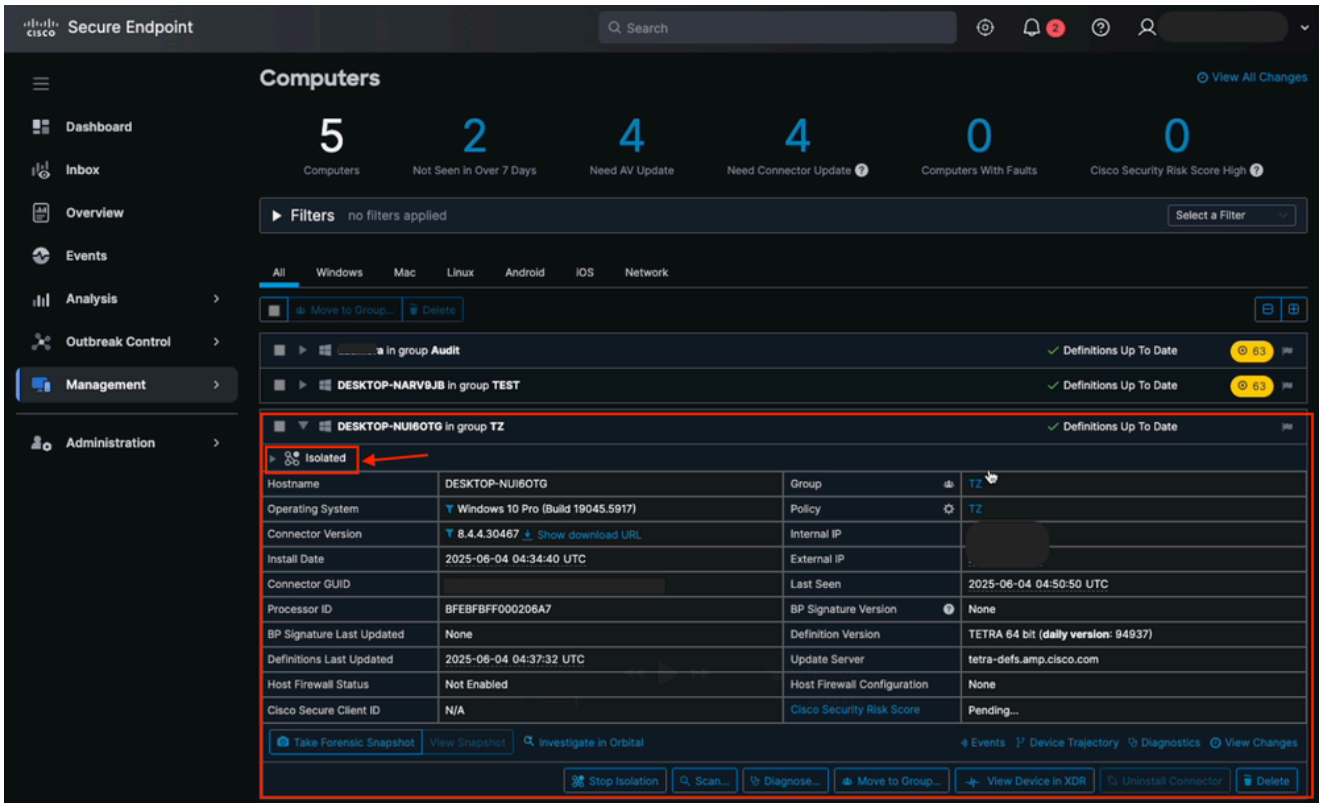
   Neuer Vorfall in Cisco XDR erkannt

2. Nachdem der Incident erstellt wurde, überprüfen Sie die Registerkarte Worklog (innerhalb des Incident), um sicherzustellen, dass der Workflow erfolgreich ausgeführt wurde. 

   Informationen auf der Registerkarte "Incident Worklog"

Phase 5.2: Endpunktisolierung bestätigen

1. Melden Sie sich beim Cisco Secure Endpoint-Portal an.
2. Navigieren Sie zum Abschnitt Verwaltung > Computer, und suchen Sie den Zielendpunkt.
3. Bestätigen Sie, dass der Gerätestatus "Isolated" lautet.



Isolationsstatus von sicheren Endpunktcomputern

4. Wenn der Endpunkt nicht isoliert ist, überprüfen Sie die Workflow-Protokolle und die Konfiguration, um mögliche Probleme zu identifizieren.

Häufiges Problem

Die Isolationsfunktion von Cisco Secure Endpoint ist nicht aktiviert.

1. Navigieren Sie von Cisco XDR zu Incidents (Vorfälle), suchen Sie den letzten Vorfall, und navigieren Sie zu Worklog.

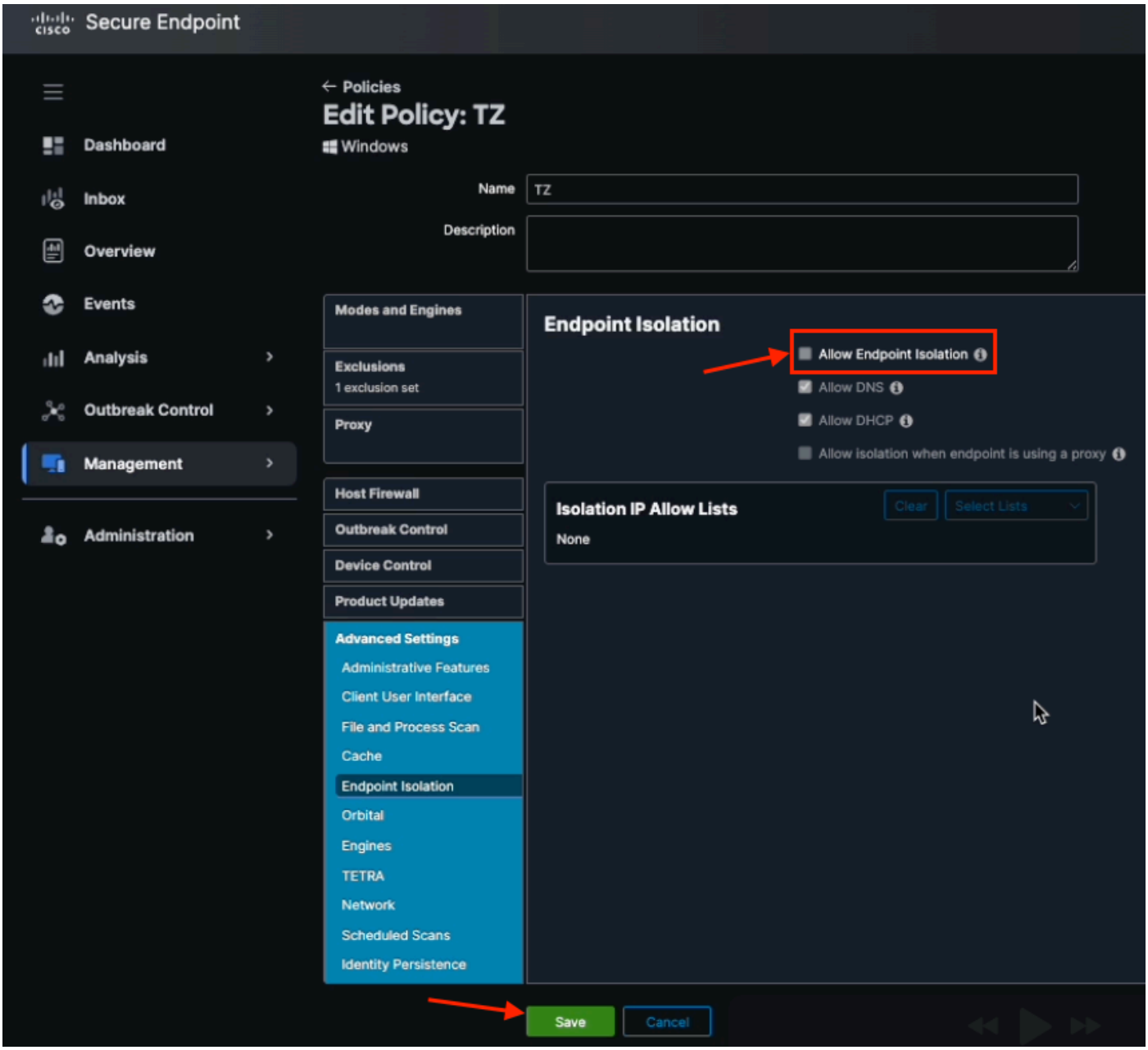
2. Überprüfen Sie nach dem Ausführen des Automatisierungs-Workflows, ob ein damit zusammenhängender Fehler vorliegt.

Die Endpunktisolierung ermöglichte es beispielsweise nicht, den Host zu isolieren, da die Endpunktisolierung in der Richtlinie für sichere Endpunkte nicht aktiviert war.

Ergebnisse des Automatisierungs-Workflows aus dem Incident-Worklog

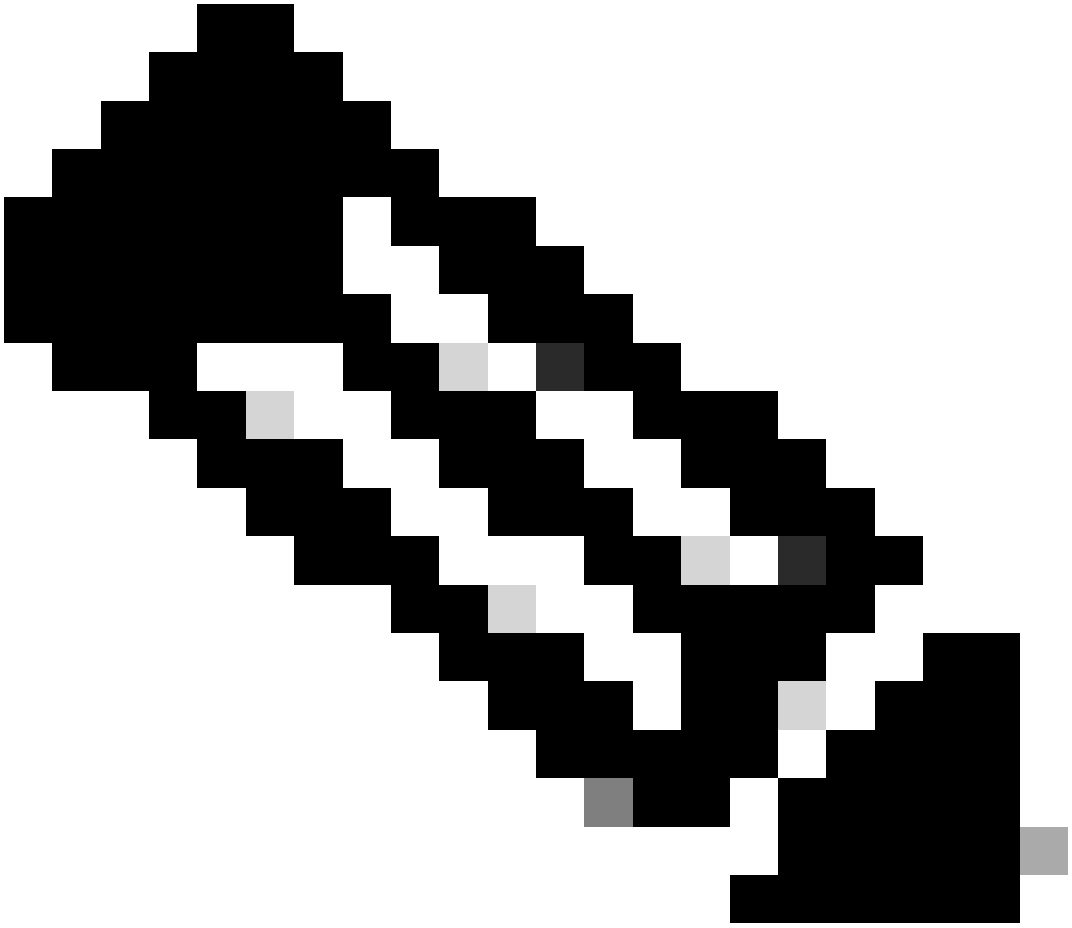
3. Navigieren Sie von einem sicheren Endpunkt aus zu Management > Policies (Verwaltung > Richtlinien), und wählen Sie die betreffende Richtlinie aus.

4. Navigieren Sie in der Richtlinie zu Erweiterte Einstellungen > Endpunktisolierung, und aktivieren Sie das Kontrollkästchen Endpunktisolierung zulassen.

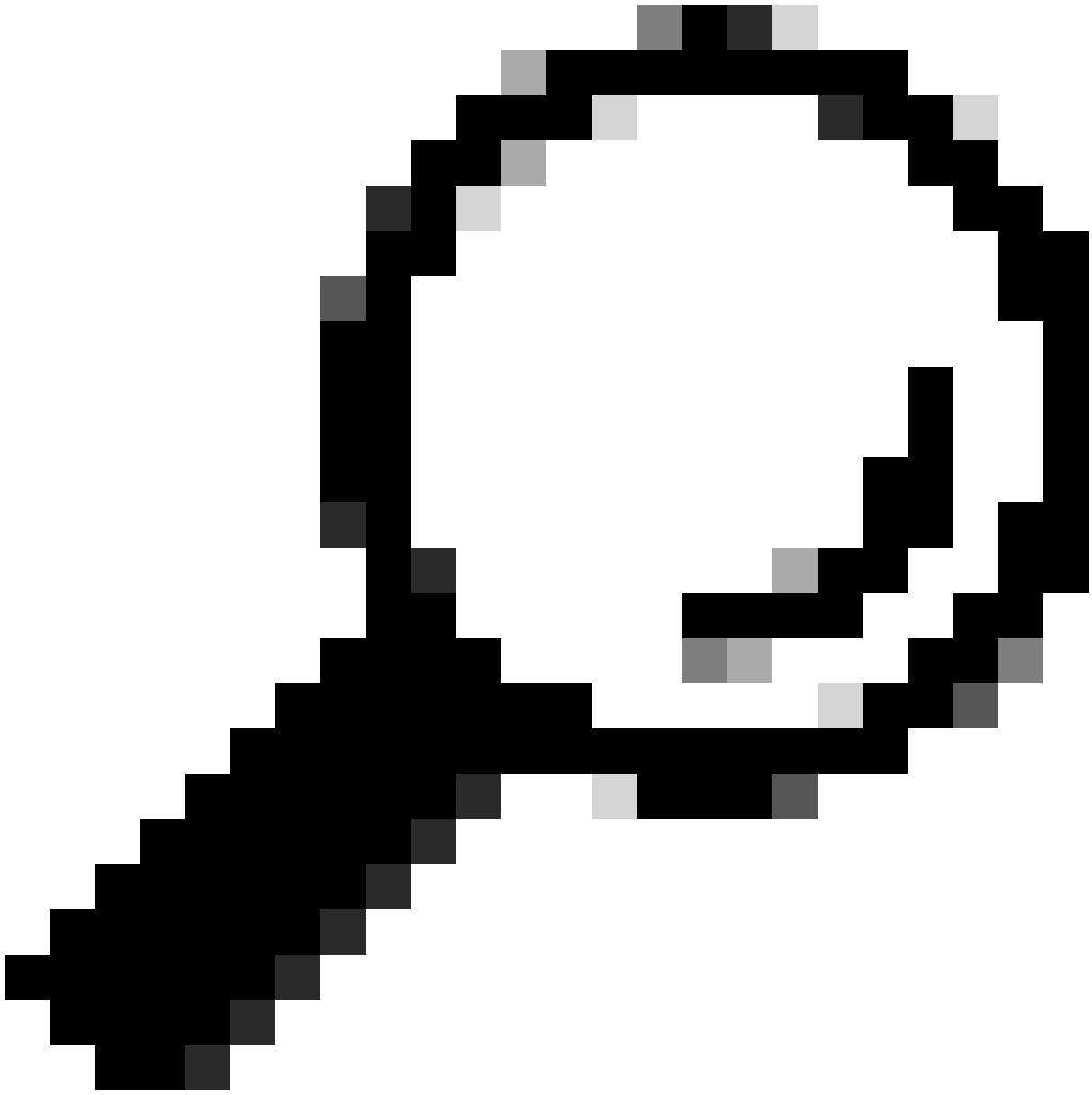


Kontrollkästchen Endpunktisolierung in Richtlinie für sichere Endpunkte zulassen

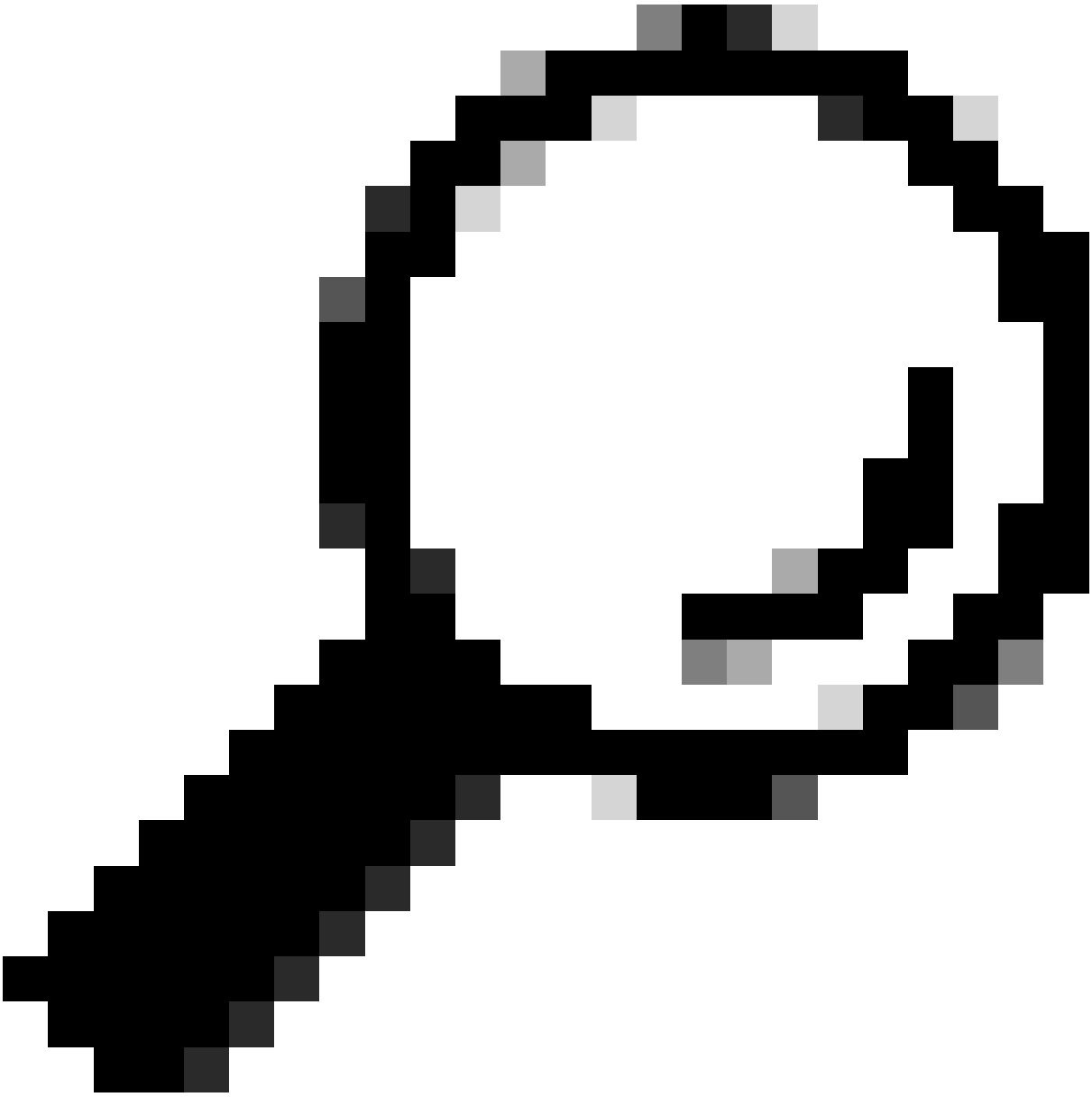
5. Klicken Sie auf Speichern.



Hinweis: Stellen Sie sicher, dass Sie über die erforderlichen Administratorberechtigungen zum Konfigurieren der Integration und des Workflows verfügen.



Tipp: Testen Sie die Einrichtung in einer kontrollierten Umgebung, bevor Sie die Automatisierung in der Produktion bereitstellen.



Tipp: Dokumentieren Sie alle benutzerdefinierten Anpassungen am Workflow oder an der Automatisierungsregel.

Nach Abschluss dieser Schritte können Sie einen Workflow erfolgreich konfigurieren und aktivieren, der ein Endgerät automatisch isoliert, nachdem ein Vorfall aufgetreten ist, und so eine schnelle und effektive Reaktion auf Sicherheitsbedrohungen sicherstellen.

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.