

# Fehlerbehebung bei Geräteeinblicken und Intune-Integration

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Fehlerbehebung](#)

[Konnektivitätstest mit Device Insights und Intune](#)

[Zugriffstoken ist leer. Überprüfen Sie das Intune-Konfigurationsmodul.](#)

[Wert für geheime ID](#)

[Überprüfung](#)

## Einleitung

In diesem Dokument werden die Schritte zur Konfiguration der Integration und zur Fehlerbehebung bei Device Insights- und Intune-Integration beschrieben.

## Voraussetzungen

### Anforderungen

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

- SecureX
- Intune
- Grundkenntnisse der APIs
- Postman-API-Tool

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen.

- SecureX 1.103

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 verstehen.

## Hintergrundinformationen

SecureX Device Insights bietet eine einheitliche Ansicht der Geräte in Ihrem Unternehmen und konsolidiert Bestände aus integrierten Datenquellen.

Microsoft Intune ist ein Enterprise Mobility Manager (EMM), auch bekannt als Mobile Device Manager (MDM) oder Unified Endpoint Manager (UEM). Wenn Sie Microsoft Intune mit SecureX integrieren, werden die Endpunktdetails in SecureX Device Insights und die Endpunktdaten, die bei der Untersuchung von Vorfällen verfügbar sind, erweitert. Wenn Sie die Microsoft Intune-Integration konfigurieren, müssen Sie einige Informationen aus dem Azure-Portal abrufen und dann das Microsoft Intune-Integrationsmodul in SecureX hinzufügen.

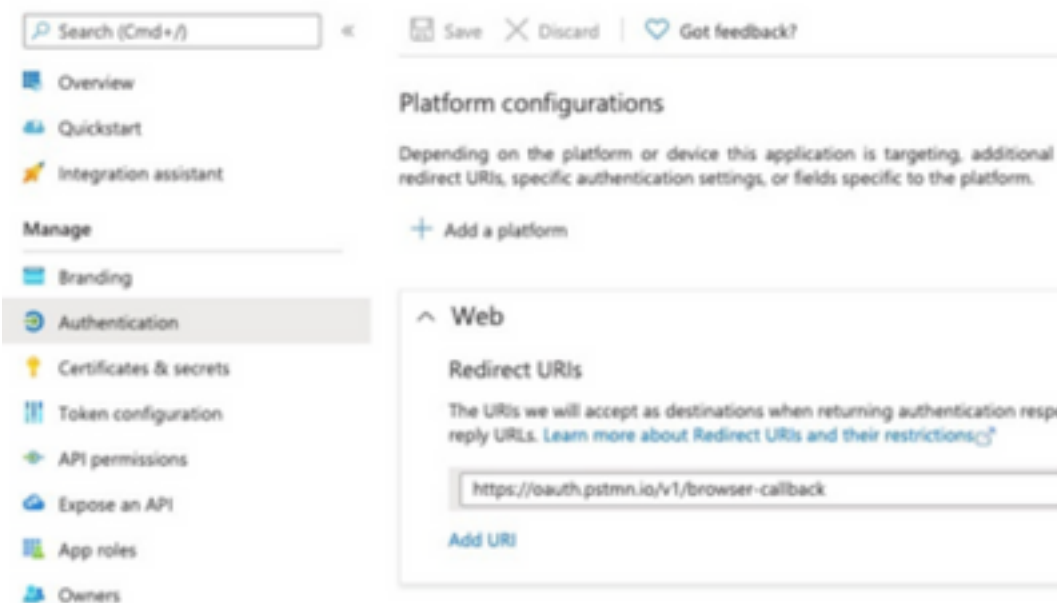
Wenn Sie mehr über die Konfiguration erfahren möchten, lesen Sie bitte die Details zum Integrationsmodul.

## Fehlerbehebung

Um häufige Probleme mit der SecureX- und InTune-Integration zu beheben, können Sie die Verbindung und Leistung der API überprüfen.

### Konnektivitätstest mit Device Insights und InTune

- Postman Azure App-Konfiguration für Graph API [hier](#) dokumentiert
- Auf höchster Ebene muss der Administrator beispielsweise Umleitungs-URIs definieren.



- API-Berechtigungen können wie in der Device Insights-App beibehalten werden.
- Fork for Graph API Sammlung kann [hier](#) erstellt werden

API / Permissions name	Type	Description
▼ Microsoft Graph (2)		
DeviceManagementManagedDevices.Read	Application	Read Microsoft Intune devices
User.Read	Delegated	Sign in and read user profile

- In der Umgebung, die mit dieser Gabel ausgeliefert wird, müssen diese Werte pro

Anwendung/Tenant angepasst werden.

Microsoft Graph environment	
VARIABLE	INITIAL VALUE
ClientID	
ClientSecret	
TenantID	

- Sie können Postman Tool verwenden, um eine visuellere Ausgabe zu erhalten, während Sie die Konnektivität testen.

**Anmerkung:** Postman ist kein von Cisco entwickeltes Tool. Wenn Sie Fragen zur Funktionalität des Postman-Tools haben, wenden Sie sich bitte an den Postman-Support.

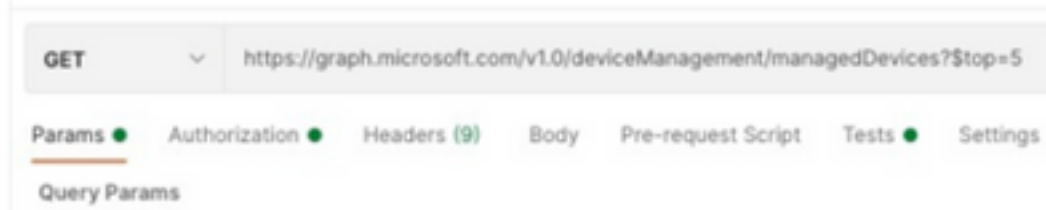
- Der erste Aufruf, der ausgeführt werden soll, ist **Get App-Only Access Token**. Wenn die richtigen **App-Anmeldeinformationen** und die **Tenant-ID** verwendet wurden, wird die Umgebung mit dem App-Zugriffstoken aufgefüllt. Anschließend können tatsächliche API-Aufrufe wie im Image dargestellt ausgeführt werden.

MS Graph PosaaS LAB / Intune / **Get App-Only Access Token**



- Sie können diesen API-Aufruf verwenden, um Intune-Endpunkte abzurufen, wie im Bild dargestellt (falls erforderlich, lesen Sie dieses Graph API Pagination-[Dokument](#))

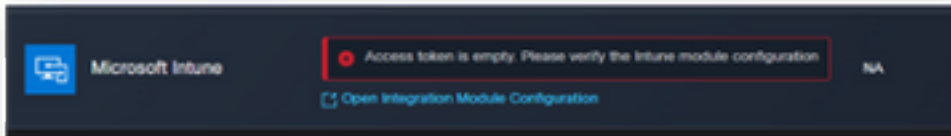
`https://graph.microsoft.com/v1.0/deviceManagement/managedDevices`



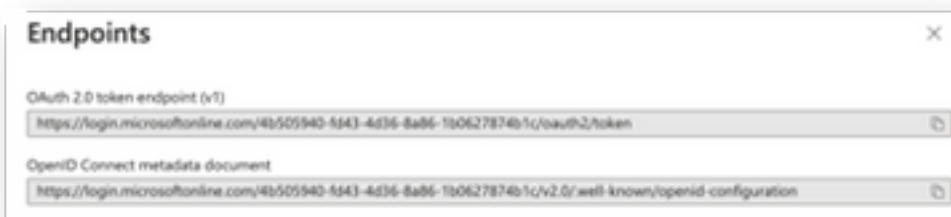
**Zugriffstoken ist leer. Überprüfen Sie das Intune-Konfigurationsmodul.**

Das Zugriffstoken ist leer. Dies ist ein OAuth-Fehler, wie im Bild gezeigt.

- In der Regel verursacht durch einen Azure UI-Fehler
- Es muss der Token-Endpunkt für die Organisation sein.



- Sie können an beiden Standorten versuchen, die Endpunkte, die **integrierte App** und den Stamm von **App-Registrierungen > Endpunkte** anzuzeigen.
- Sie können Endpunkte aus Ihrer integrierten Azure-App anzeigen, die als generische, nicht spezifische URLs für die OAuth-Endpunkte angezeigt werden, wie im Bild gezeigt



## Wert für geheime ID

Vergewissern Sie sich, dass Sie die **geheime ID** kopiert haben, nicht den **geheimen Wert** (der Wert ist der API-Schlüssel, und die geheime ID selbst ist ein interner Index für Azure selbst, was nicht hilfreich ist). Sie müssen den Wert in SecureX Device Insights verwenden. Dieser Wert wird nur vorübergehend angezeigt.

## Überprüfung

Sobald Intune als Quelle zu Device Insights hinzugefügt wurde, wird der Verbindungsstatus der erfolgreichen REST-API angezeigt.

- Die Verbindung der REST-API wird grün angezeigt.
- Drücken Sie auf Jetzt synchronisieren, um die erste vollständige Synchronisierung auszulösen, wie im Bild gezeigt.



Sollte das Problem weiterhin mit den Geräteinformationen und der Intune-Integration bestehen,

lesen Sie diesen [Artikel](#), um HAR-Protokolle vom Browser zu erfassen, und wenden Sie sich an den TAC-Support, um eine tiefere Analyse durchzuführen.

## 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.