Fehlerbehebung: Geräteerkennung und Umbrella-Integration

Inhalt

Einleitung

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

Voraussetzungen

Anforderungen

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

- SecureX
- Umbrella
- 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.

Umbrella erkennt automatisch die Infrastruktur von Angreifern, die auf aktuelle Bedrohungen ausgerichtet ist, und blockiert proaktiv böswillige Anfragen, bevor diese das Netzwerk oder die Endpunkte eines Unternehmens erreichen. Durch die Integration können Sie Malware-Infektionen früher stoppen, bereits infizierte Geräte schneller identifizieren und Datendiebstahl verhindern. Durch die Integration erhalten Sie einen vollständigen Überblick über die Internetaktivitäten aller Standorte und Benutzer und können mit nur zwei Klicks Maßnahmen ergreifen, um Domänen schnell zu blockieren. Mehrere Umbrella-Funktionen werden unterstützt und über API-Schlüssel verknüpft, die in der Umbrella Platform generiert wurden.

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

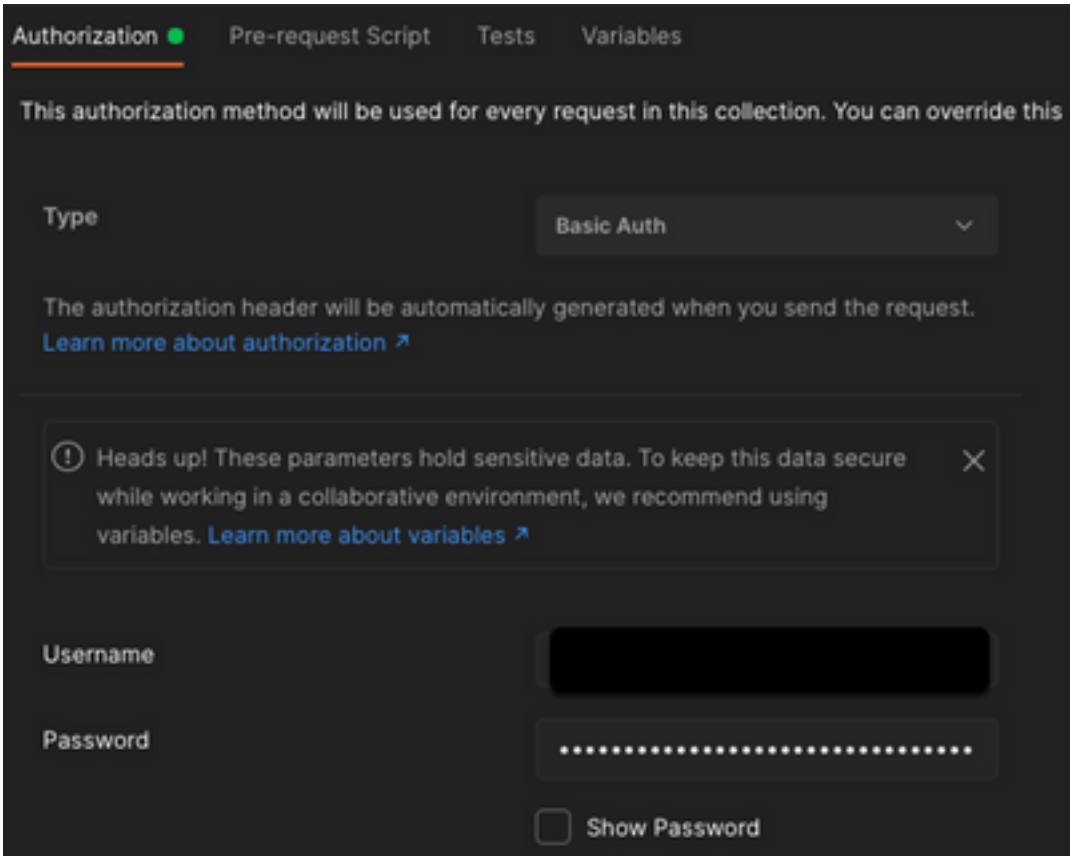
Fehlerbehebung

Um häufige Probleme bei der Integration von SecureX und Umbrella zu beheben, können Sie die Konnektivität und Leistung der API überprüfen.

Konnektivitätstest mit Device Insights und Umbrella

Schritt 1: Sie können **Basic** Authas als Autorisierungsmethode auswählen, da MobileIron diese verwendet, wie im Bild gezeigt.

> **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.



Schritt 2. Sie können **die Roaming-Computer** mit diesem API-Aufruf (die Standardseitenbeschränkung ist 100 Einträge).

```
https://management.api.umbrella.com/v1/organizations/
```

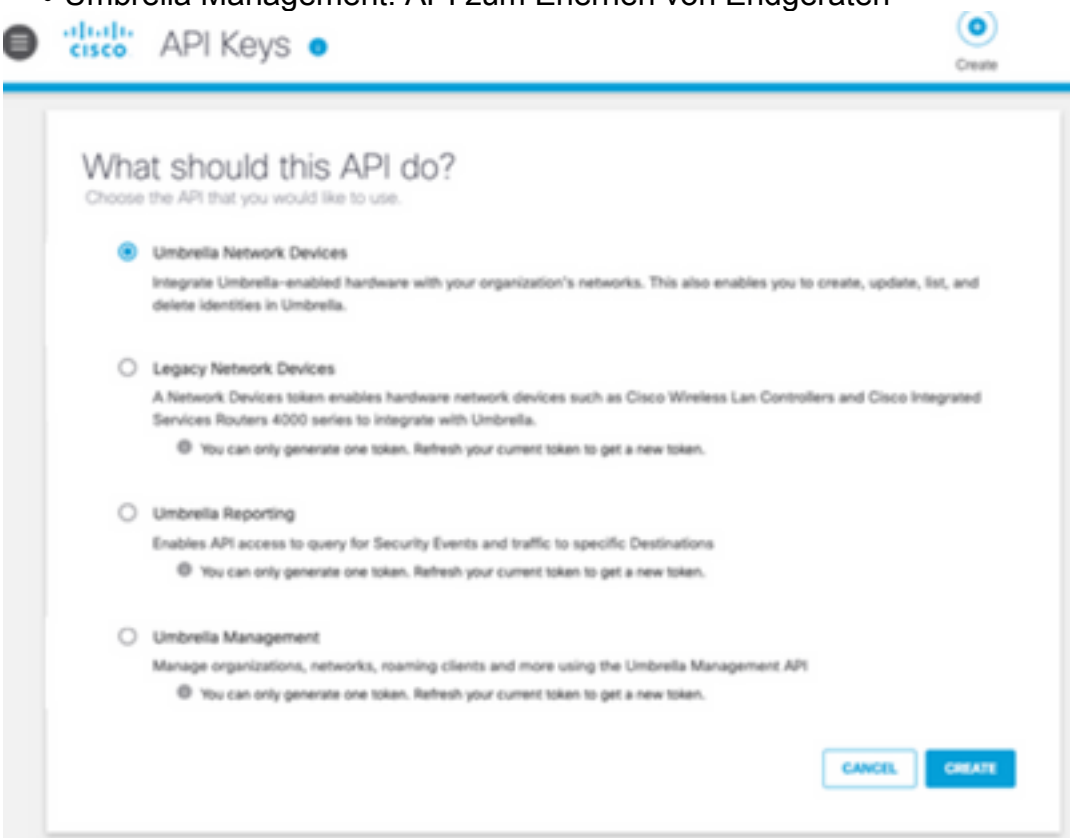
Schritt 3: Als Reaktion auf den ersten Aufruf wird die Gesamtzahl der Objekte zurückgegeben. Sie können die Limit- und Seitenparameter verwenden, um die nächsten Seiten abzurufen.

```
https://management.api.umbrella.com/v1/organizations/
```

Falscher Schlüssel

Device Insights verwendet nicht die gleichen Schlüssel wie SecureX. Sie müssen dann überprüfen und bestätigen, dass die als Umbrella API-Schlüssel konfigurierten Schlüssel korrekt sind, wie im Bild gezeigt.

- Umbrella-Netzwerkgeräte: API zur Ermittlung der DNS-Richtlinien
- Umbrella Management: API zum Erlernen von Endgeräten



Überprüfung

Sobald Umbrella Device Insights als Quelle hinzugefügt wurde, wird ein erfolgreicher **REST API-** Verbindungsstatus angezeigt.

- Sie sehen **den** Status **der REST**-APIverbindung
- Klicken Sie **auf** Jetzt synchronisieren, um die erste vollständige Synchronisierung auszuführen, wie im Bild gezeigt.

Sollte das Problem weiterhin mit den Geräteinformationen und der Umbrella-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.