Dépannage de XDR Device Insights et de Microsoft Intune Integration

Table des matières

Introduction

Ce document décrit les étapes pour configurer l'intégration et dépanner l'intégration de Device Insights et Intune.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes .

- XDR
- Microsoft Intune
- Connaissances de base des API
- Outil API Postman

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- XDR

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Informations générales

XDR Device Insights fournit une vue unifiée des périphériques de votre entreprise et consolide les inventaires à partir de sources de données intégrées.

Microsoft Intune est un Enterprise Mobility Manager (EMM), également appelé Mobile Device Manager (MDM) ou Unified Endpoint Manager (UEM). Lorsque vous intégrez Microsoft Intune à XDR, il enrichit les détails des points de terminaison disponibles dans XDR Device Insights et les données des points de terminaison disponibles lorsque vous enquêtez sur des incidents. Lorsque vous configurez l'intégration Microsoft Intune, vous devez collecter des informations à partir de votre portail Azure, puis ajouter le module d'intégration Microsoft Intune dans XDR.

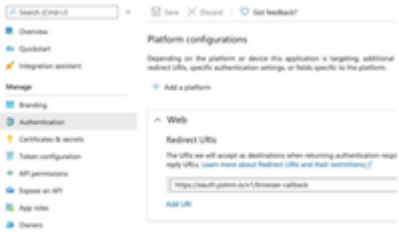
Si vous souhaitez en savoir plus sur la configuration, consultez les détails du module d'intégration.

Dépannage

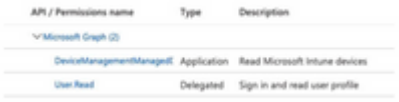
Afin de dépanner les problèmes courants avec l'intégration XDR et Intune, vous pouvez vérifier la connectivité et les performances de l'API.

Test de connectivité avec XDR Device Insights et Intune

- La configuration de Postman Azure App pour l'API Graph est documentée ici
- Au niveau supérieur, l'administrateur doit définir des URI de redirection, par exemple



- Les autorisations API peuvent rester identiques à celles de l'application Device Insights
- La collection d'API Fork pour Graph peut être créée ici

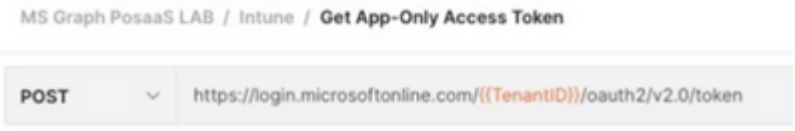


- L'environnement fourni avec la fourchette doit avoir ces valeurs ajustées par application/locataire

- Vous pouvez utiliser l'outil Postman pour avoir une sortie plus visuelle pendant que vous testez la connectivité.

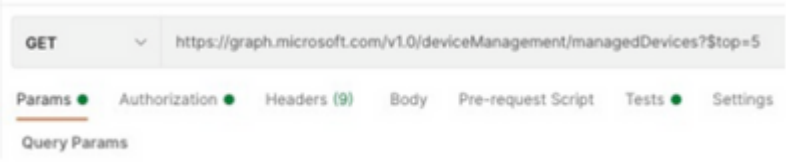
Remarque : Postman n'est pas un outil développé par Cisco. Si vous avez une question sur la fonctionnalité de l'outil Postman, veuillez contacter le support de Postman.

- Le premier appel à être exécuté est **Get App-Only Access Token**. Si les **informations d'identification** de l'**application** et l'**ID de locataire** corrects ont été utilisés, cet appel remplit l'environnement avec le jeton d'accès à l'application. Une fois l'opération terminée, les appels d'API réels peuvent être exécutés comme indiqué dans l'image



- Vous pouvez utiliser cet appel d'API pour obtenir les terminaux Intune, comme indiqué dans l'image (si nécessaire, consultez ce document de pagination de l'API Graph)

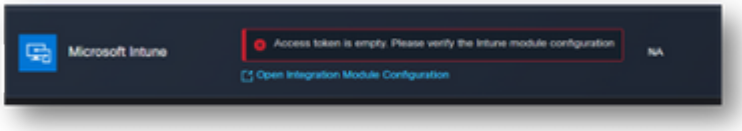
```
https://graph.microsoft.com/v1.0/deviceManagement/managedDevices
```



Le jeton d'accès est vide. Vérifiez le module de configuration Intune

Le jeton d'accès est vide est une erreur OAuth, comme indiqué dans l'image.

- Généralement causé par un bogue de l'interface utilisateur Azure
- Il doit s'agir du point de terminaison du jeton pour l'organisation



- Vous pouvez essayer les deux emplacements pour voir les terminaux, l'**application intégrée** et la racine des **enregistrements d'applications > Terminaux**

- Vous pouvez afficher les terminaux de votre application intégrée Azure sous forme d'URL génériques et non spécifiques pour les terminaux OAuth, comme illustré dans l'image

Valeur d'ID secret

Vérifiez que vous avez copié l'**ID secret**, et non la **valeur secrète** (la valeur est la clé API et l'ID secret lui-même est un index interne pour Azure lui-même et cela n'aide pas). Vous devez utiliser la valeur dans XDR Device Insights, et cette valeur n'est affichée que temporairement.

Vérifier

Une fois Intune ajouté en tant que source à XDR Device Insights, vous pouvez voir un état de connexion

REST API réussi.

- Vous pouvez voir la connexion de l'**API REST** avec un état vert.
- Appuyez sur **SYNC NOW** pour déclencher la synchronisation complète initiale, comme illustré dans l'image.

Si le problème persiste avec l'intégration XDR Device Insights et Intune, collectez les journaux HAR à partir du navigateur et contactez le support TAC afin d'effectuer une analyse plus approfondie.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.