Configurer la mise en service de certificat Umbrella avec MS Intune

Table des matières

Introduction

Ce document décrit la configuration de la mise en service du certificat Umbrella avec MS Intune.

Aperçu

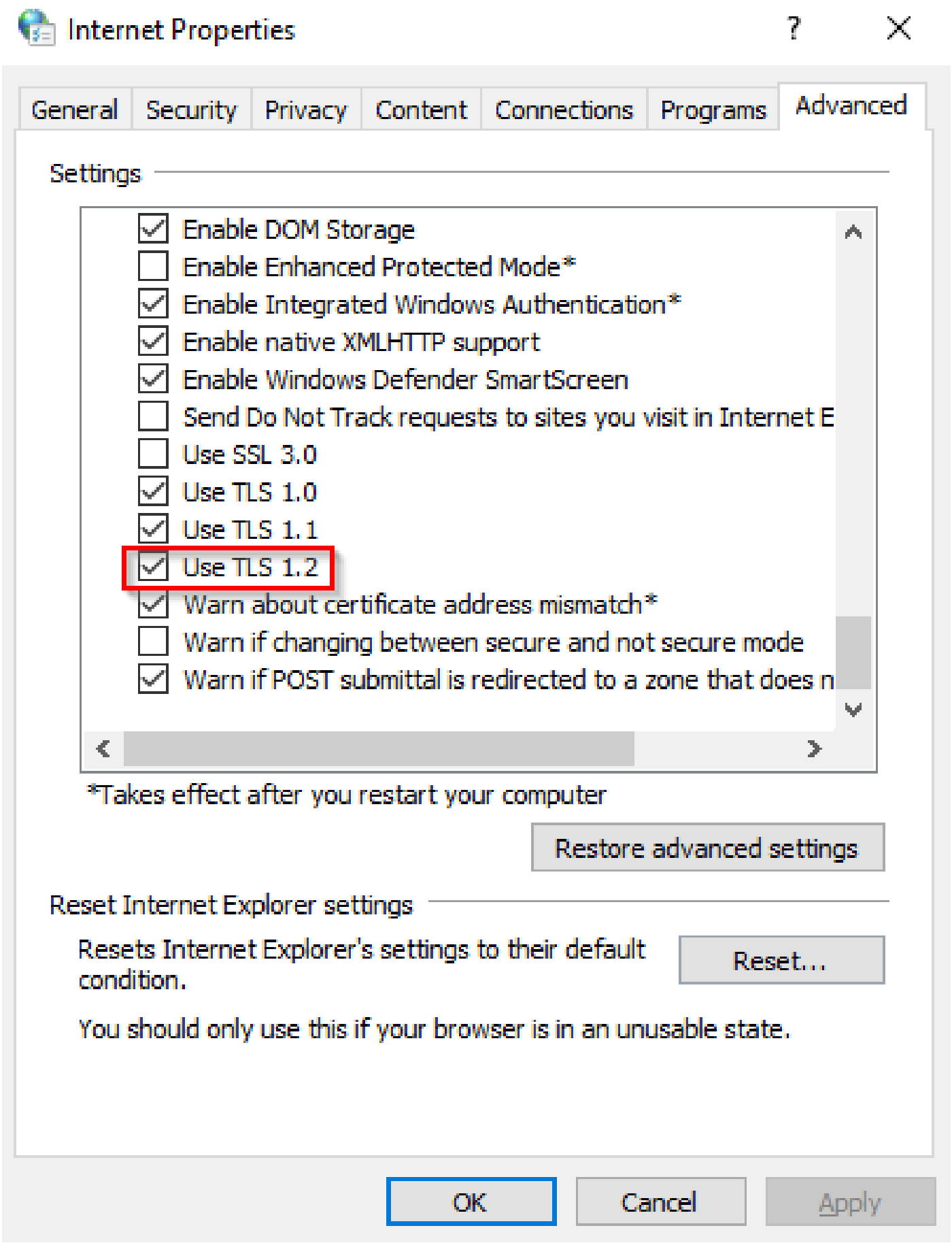
Ce guide de configuration couvre les éléments requis pour provisionner l'AC racine Umbrella via MS Intune.

Conditions préalables

- Accès au tableau de bord Umbrella
- CA racine de parapluie
- Accès à la console MS Intune

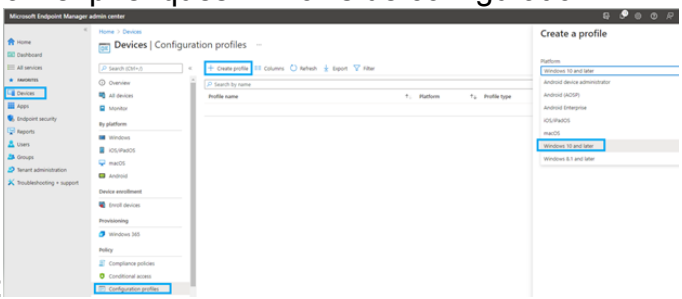
Tableau de bord Umbrella

1. Accédez à votre tableau de bord Umbrella sous Déploiements > Configuration > Root Certificate et téléchargez l'autorité de certification Umbrella Root :

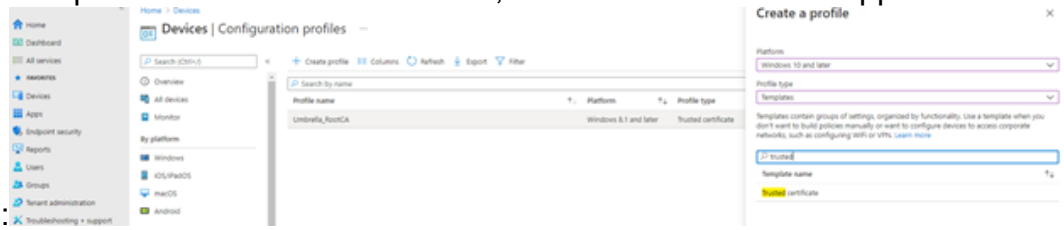

Internet Properties
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Enable DOM Storage
Enable Enhanced Protected Mode*
Enable Integrated Windows Authentication*
Enable native XMLHTTP support
Enable Windows Defender SmartScreen
Send Do Not Track requests to sites you visit in Internet E
Use SSL 3.0
Use TLS 1.0
Use TLS 1.1
Use TLS 1.2
Warn about certificate address mismatch*
Warn if changing between secure and not secure mode
Warn if POST submittal is redirected to a zone that does n
*Takes effect after you restart your computer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

blobid0.png

Console MS Intune

1. Accédez à votre MS Intune MDM et accédez à Périphériques > Profils de configuration > Créer un profil > Sélectionner la plate-forme : 

86b492a7fb03fb72fa2c255ed5f34309fc7427aee918937b6990a66f956dc9ac.png

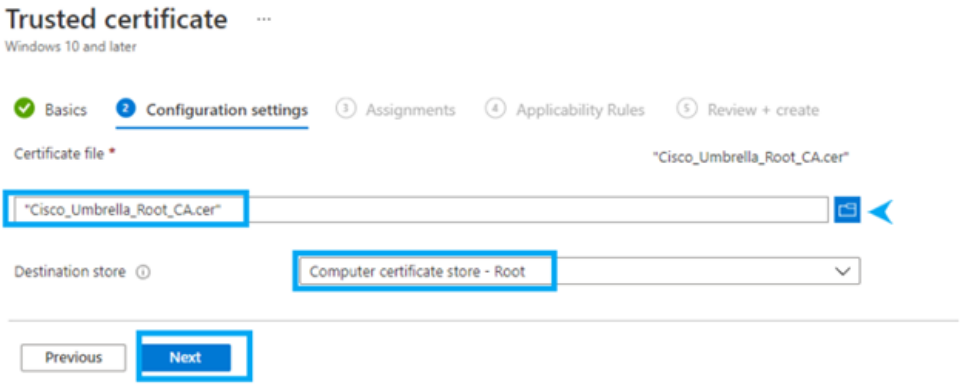
2. Spécifiez le « Type de profil » et utilisez « Modèles », recherchez « Certificat approuvé » et cliquez sur Créer : 

ca00d2c34ecac4f6fe2584d61b9c8a9832c458d7c083e0aabb532b8c8ebcd7aa.png

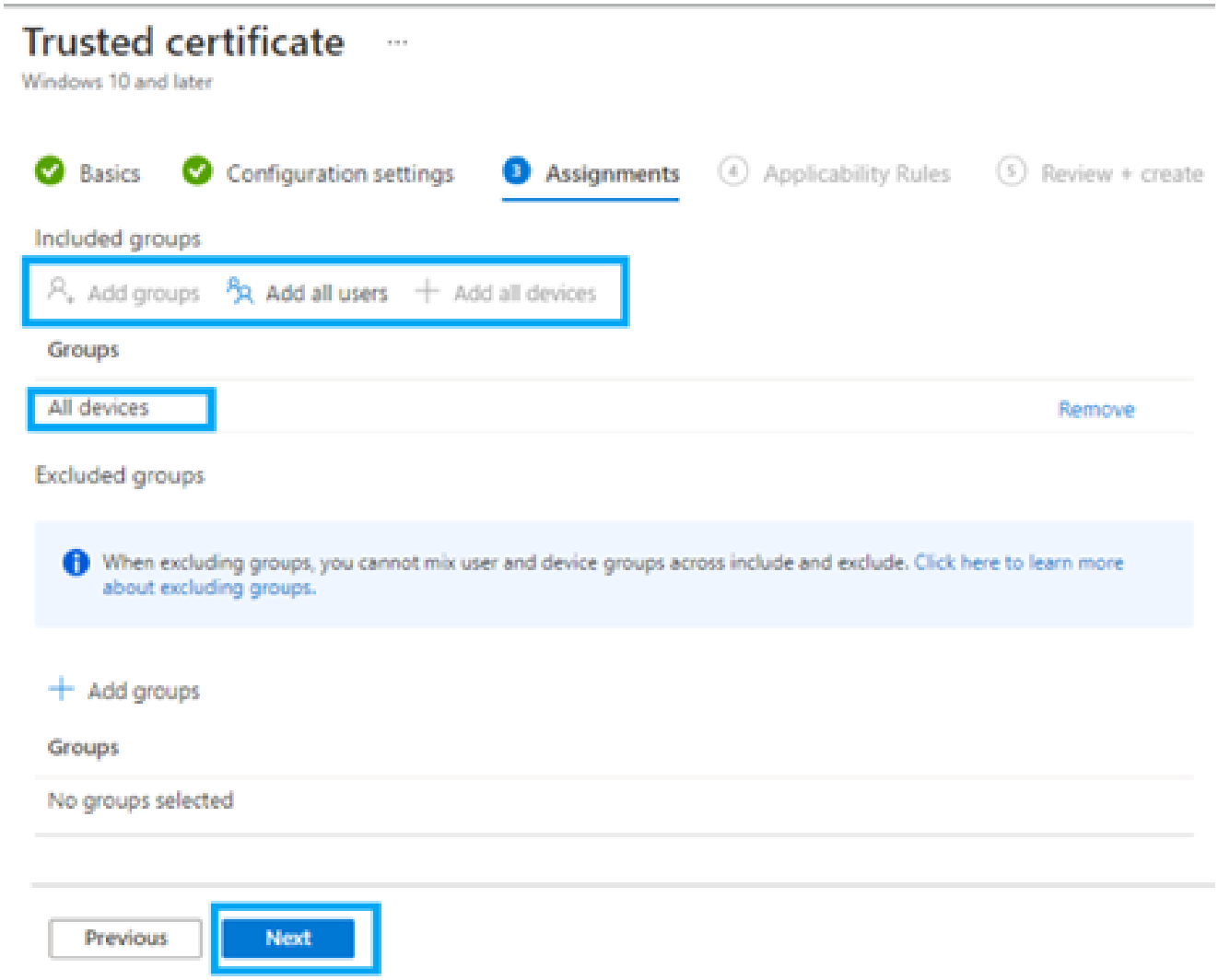
3. Entrez un nom significatif pour le profil de certificat approuvé et cliquez sur Suivant. 

dfd78f03070787c9ffc4c6c968929d7a12be36429590740ed27641144cf143cf.png

4. Téléchargez l'autorité de certification racine Umbrella et spécifiez le magasin de destination, puis cliquez sur Suivant :

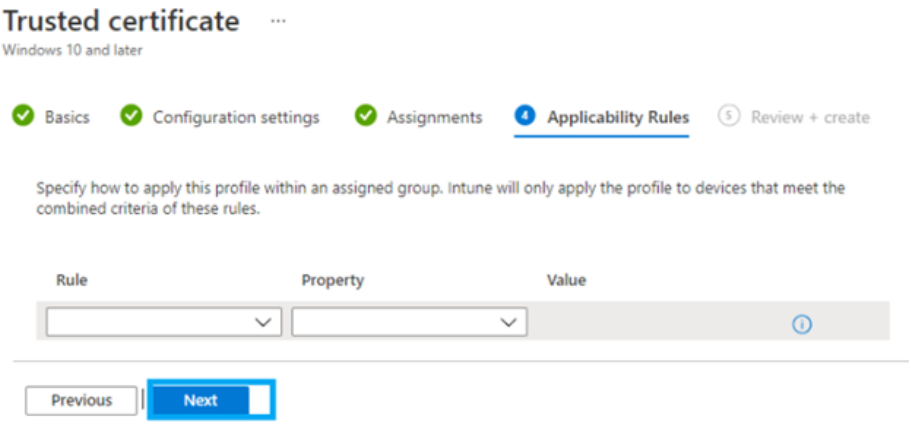


a318563a22a600910b206f01cdfeb483ccc04cb0e15a1757c48e663cfe234ec0.png



93effe94c92c3b063c406e89c4b6d0f759cb8c5d606302e3701b702b1a8cb213.png

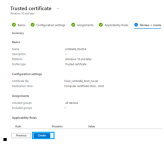
5. Spécifiez le groupe d'utilisateurs/périphériques que vous souhaitez attribuer à l'autorité de certification racine Umbrella.



c436635d3e0dce29ec76802ffb26e604964abe08862c00ec25866dbf4a9d5b95.png

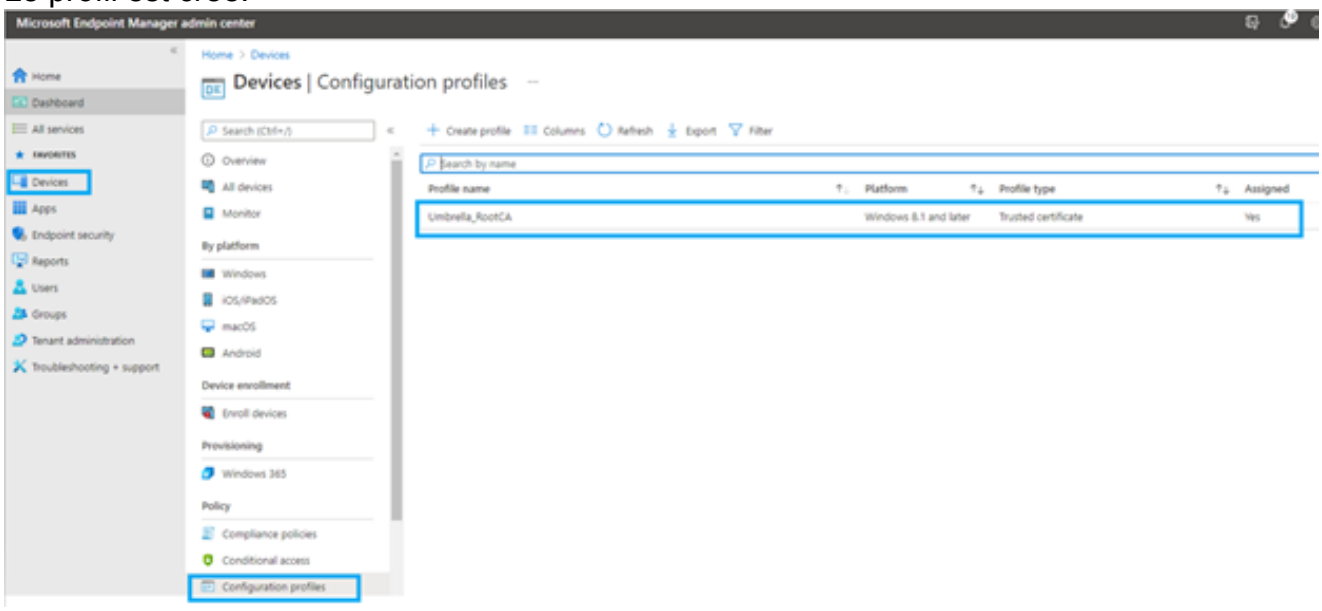
6. Vous pouvez également spécifier « Règles d'applicabilité » et cliquer sur Suivant.

7. Vérifiez que la configuration a été correctement effectuée, puis cliquez sur Create.



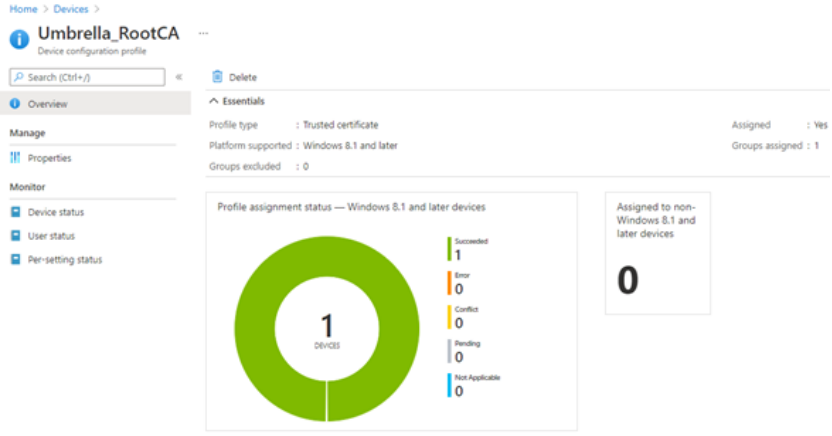
6329621f732c63ec97b6ef656b78dc1c392fe976105a0c3dbb7a779b945ba7e8.png

8. Le profil est créé.



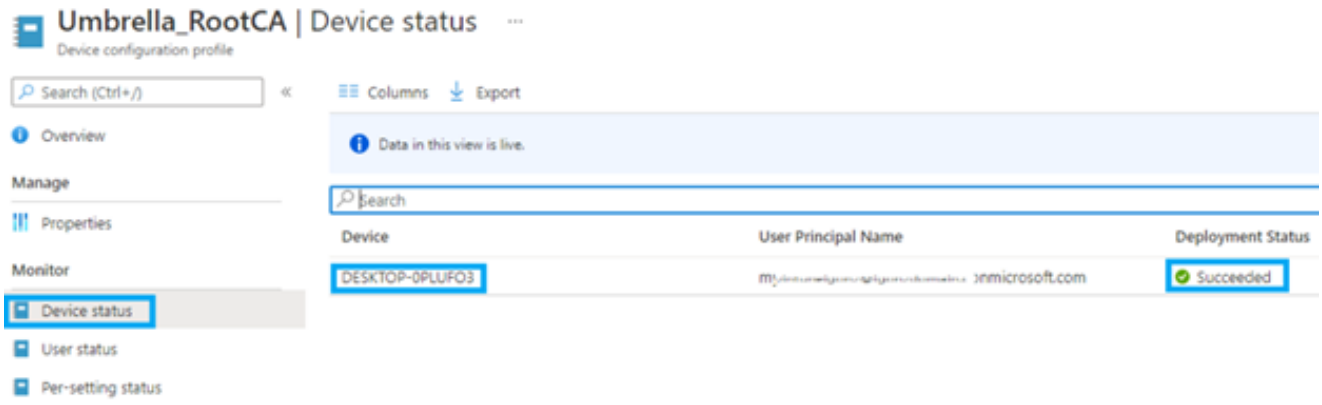
40c213cc1de22637d88e671a7074d58426573aed1f2fb7ebfda4bc338a691d84.png

9. Cliquez sur le profil pour accéder à la page Vue d'ensemble, où vous pouvez vérifier l'état de l'affectation et le nombre de périphériques pour lesquels une autorité de certification Umbrella Root a été implémentée.



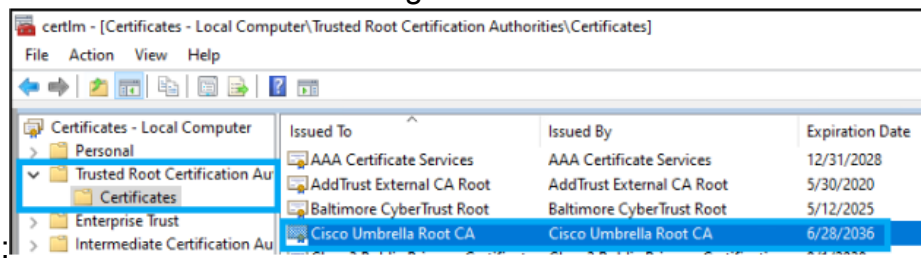
24b011d4b760c8245d7a4363e885857dea9881cb4ef0a683b83024e618ac9c.png

10. Vous pouvez également cliquer sur la section « Device Status » (Etat du périphérique) pour confirmer que les périphériques ont été correctement déployés.



cadac2eb3017c37d68f0f8aa8230508ea33777afb93250291384962555a4de2b.png

11. Vous pouvez également confirmer l'installation sur le magasin d'autorité de certification racine du périphérique final :



a9e8eaebad6df501ad7627dbc87f5ea6cf9488b273925c5277fbf8a396ae1a49.png

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.