Procédure de désinstallation du connecteur AMP si le mot de passe est oublié

Contenu

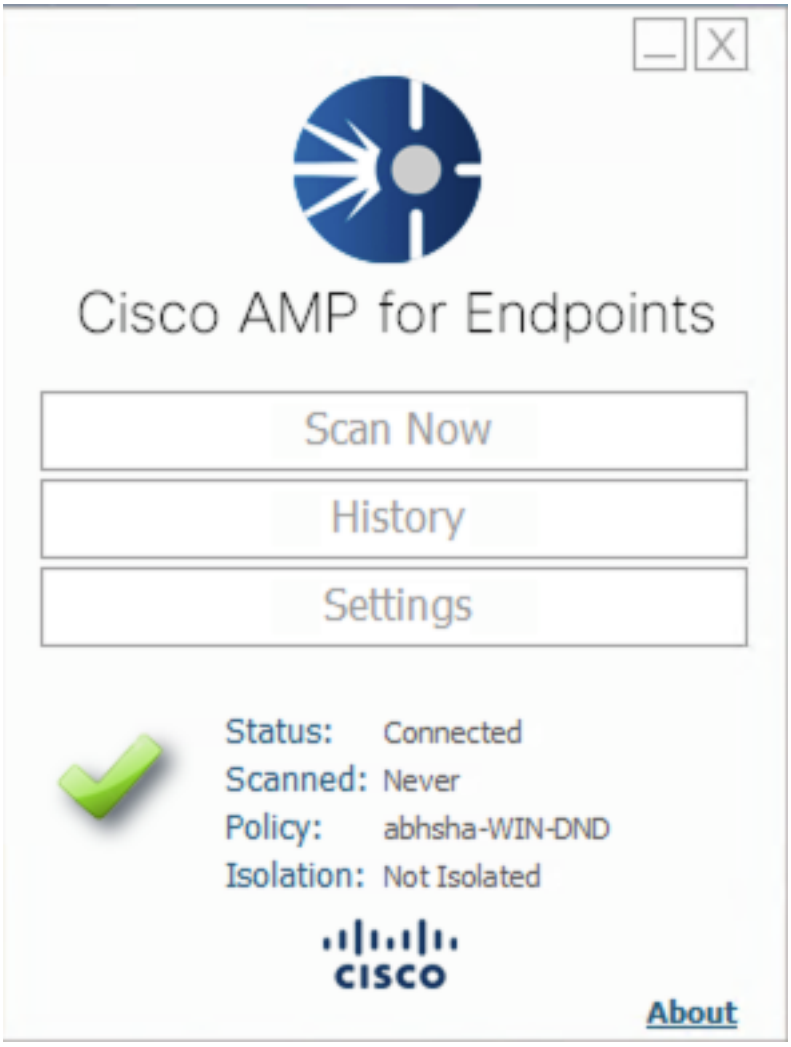
Introduction

Ce document décrit la procédure de désinstallation du connecteur Advanced Malware Protection (AMP) de Cisco au cas où la désinstallation serait bloquée par la fonction de protection du connecteur qui nécessite un mot de passe pour être fourni et que ce mot de passe est oublié. Il y a 2 scénarios dans ce cas, et cela dépend de si le connecteur indique « Connecté » au cloud AMP. Il s'applique uniquement au système d'exploitation Windows, car Connector Protection est une fonctionnalité disponible uniquement sur le système d'exploitation Windows.

Connecteur connecté

Étape 1. Cliquez sur l'icône de la barre d'état et ouvrez le connecteur Cisco AMP for Endpoints.

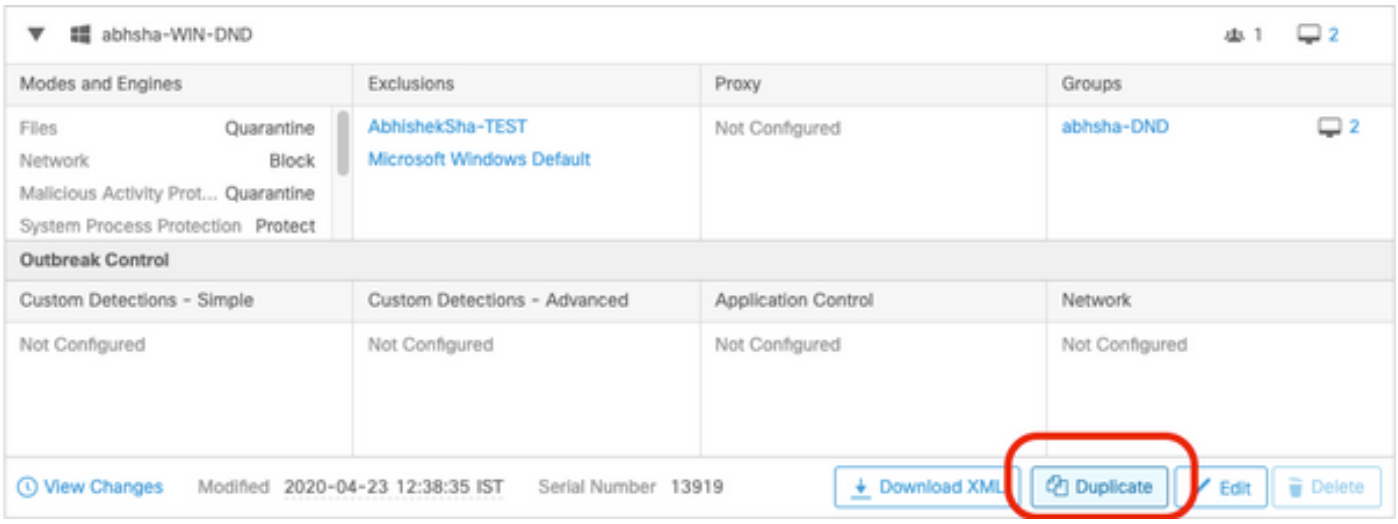
Étape 2. Assurez-vous que le connecteur est indiqué comme étant connecté.



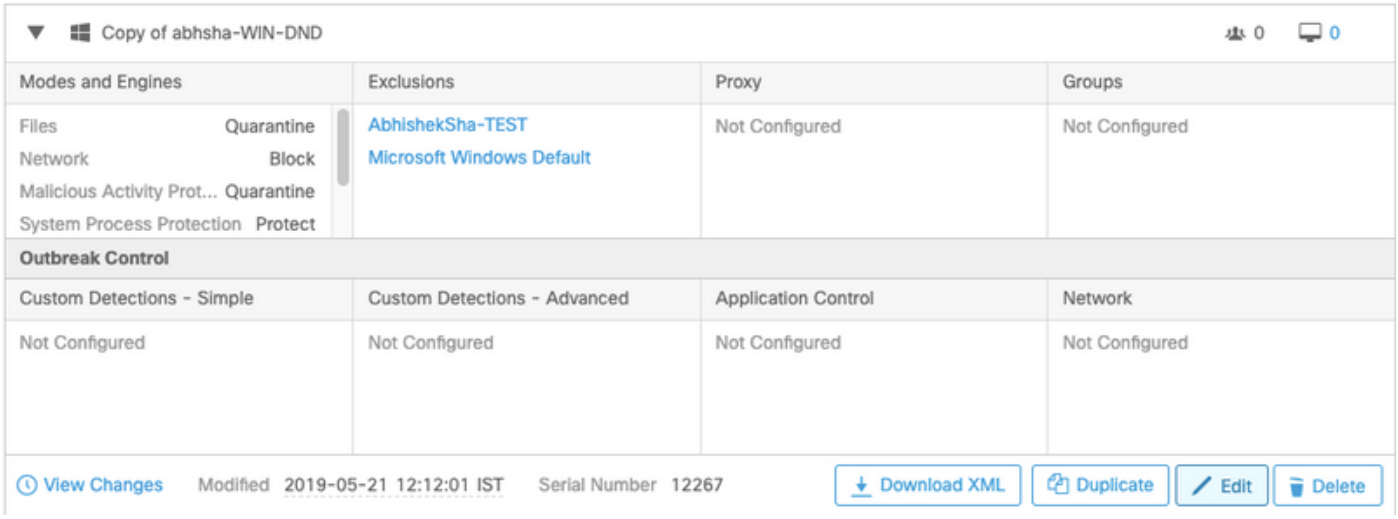
Étape 3. Notez que la stratégie a été affectée à ce connecteur.

Étape 4. Accédez à la console AMP for Endpoints et recherchez la stratégie précédemment notée.

Étape 5. Développez la stratégie et cliquez sur **Dupliquer** comme indiqué dans l'image.

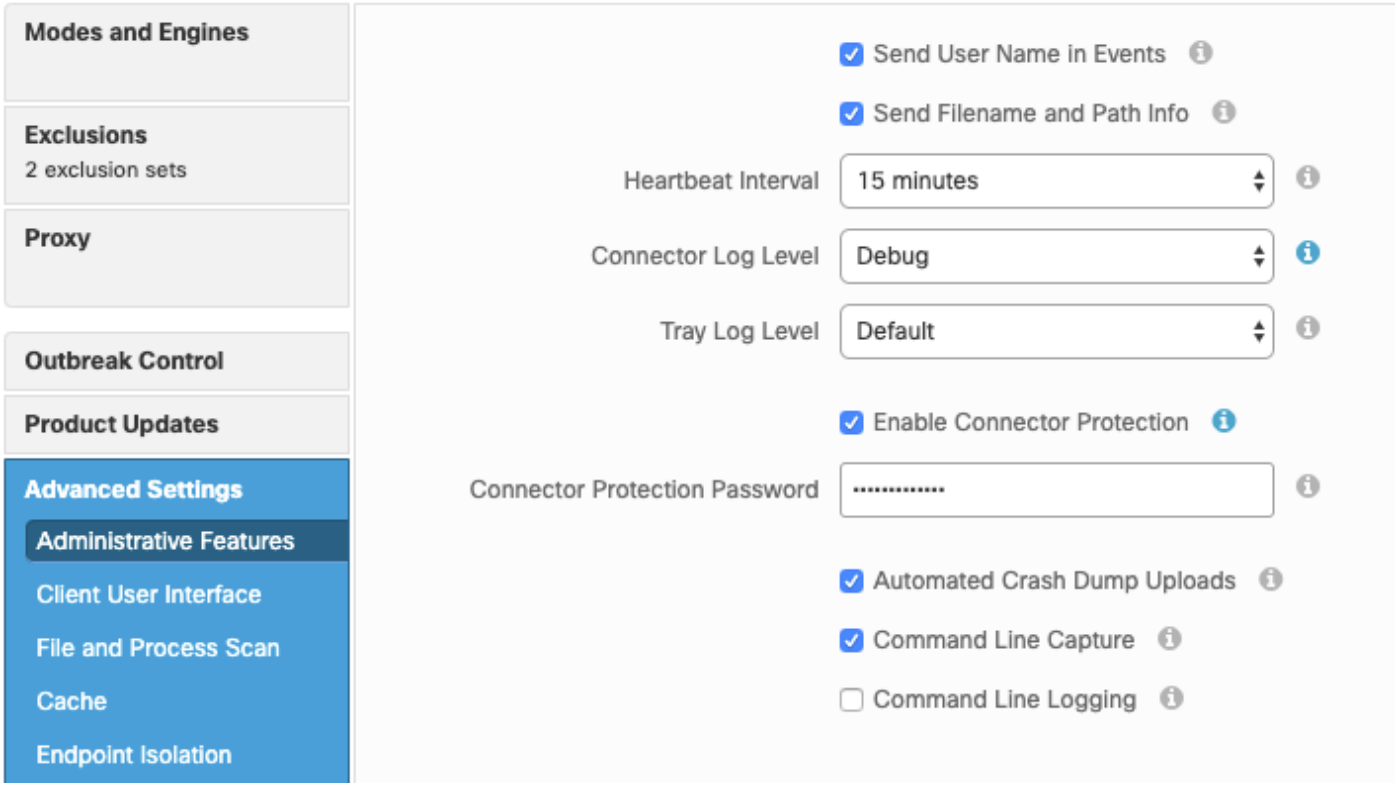


Étape 6. Une nouvelle stratégie appelée « Copie de... » sera créé. Cliquez sur **Modifier** afin de modifier cette stratégie comme indiqué dans l'image.



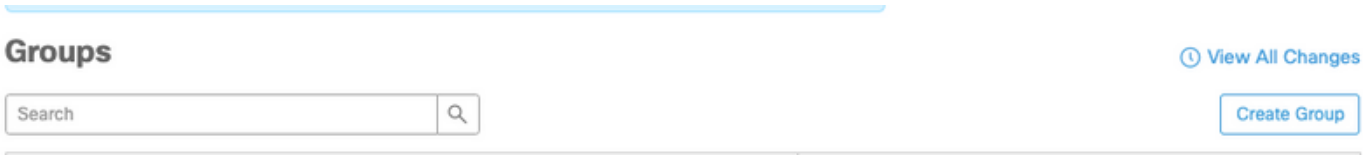
Étape 7. À la page **Modifier la stratégie**, accédez à **Paramètres avancés > Fonctions administratives.**

Étape 8. Dans le champ **Protection par mot de passe du connecteur**, remplacez le mot de passe par un nouveau mot de passe qui peut être rappelé comme indiqué dans l'image.

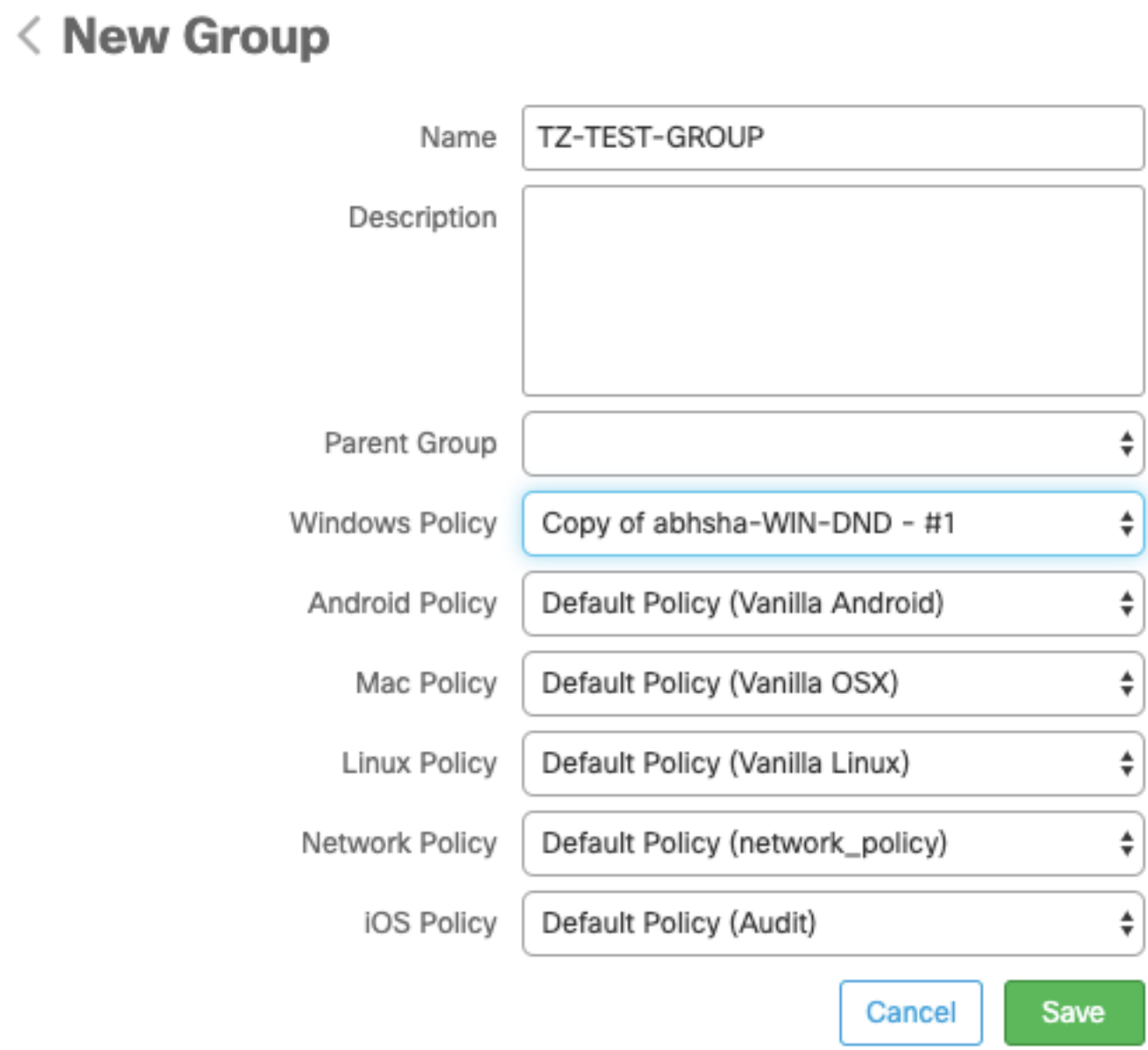


Étape 9. Cliquez sur le bouton **Enregistrer** afin d'enregistrer cette stratégie.

Étape 10. Accédez à **Management > Groups** et créez un nouveau groupe.

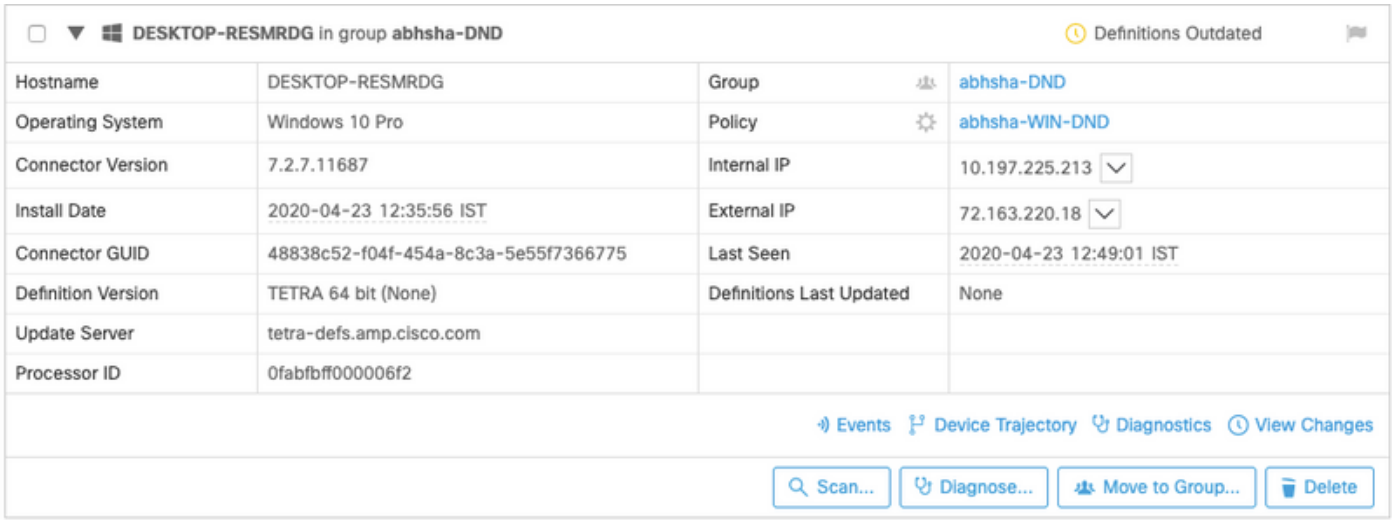


Étape 11. Entrez un nom de groupe et sélectionnez la **stratégie Windows** comme stratégie précédemment modifiée. Cliquez sur le bouton **Enregistrer** comme indiqué dans l'image.



Étape 12. Accédez à **Management > Computers** et recherchez l'ordinateur sur lequel vous essayez de désinstaller le connecteur AMP.

Étape 13. Développez l'ordinateur et cliquez sur **Déplacer vers le groupe**. Dans la boîte de dialogue qui s'affiche, sélectionnez le groupe précédemment créé.



Étape 14. Attendez que la stratégie soit mise à jour sur le point de terminaison. Cela prend généralement entre 30 minutes et 1 heure et dépend de l'intervalle configuré.

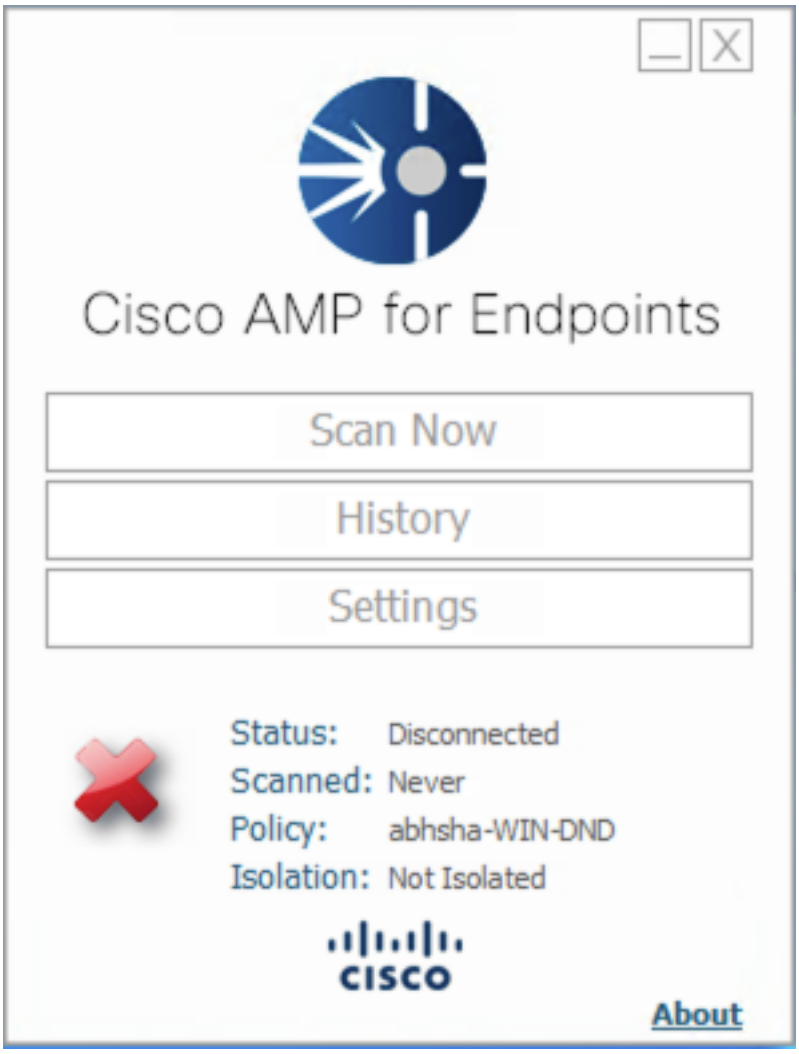
Étape 15. Une fois la stratégie mise à jour sur le point d'extrémité, vous pourrez désinstaller le connecteur à l'aide du mot de passe que vous venez de configurer.

Le connecteur est déconnecté

Si le connecteur est déconnecté du cloud AMP, il est important de pouvoir démarrer l'ordinateur en mode sans échec.

Étape 1. Cliquez sur l'icône de la barre d'état et ouvrez le connecteur Cisco AMP for Endpoints.

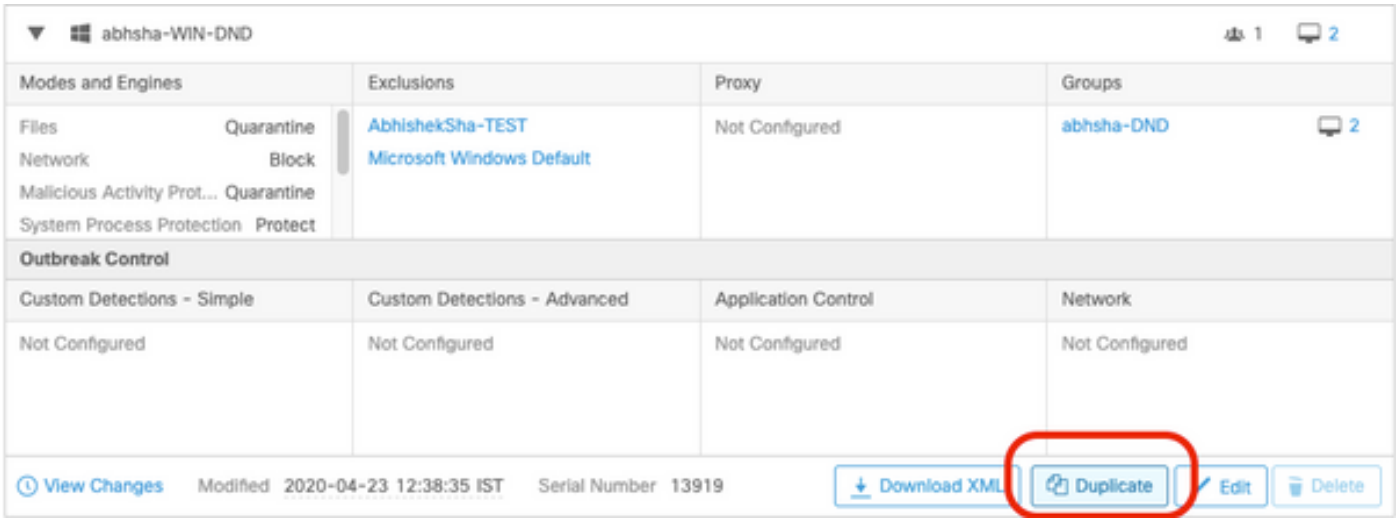
Étape 2. Vérifiez que le connecteur est déconnecté.



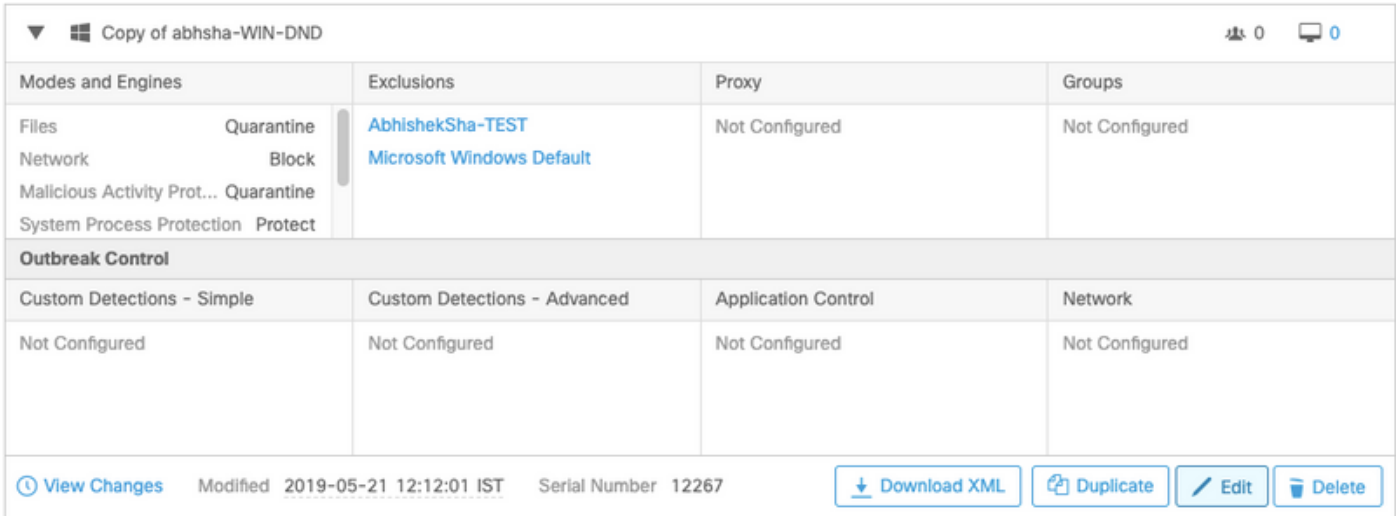
Étape 3. Notez la stratégie affectée à ce connecteur.

Étape 4. Accédez à la console AMP for Endpoints et recherchez la stratégie précédemment notée.

Étape 5. Développez la stratégie et cliquez sur **Dupliquer** comme indiqué dans l'image.

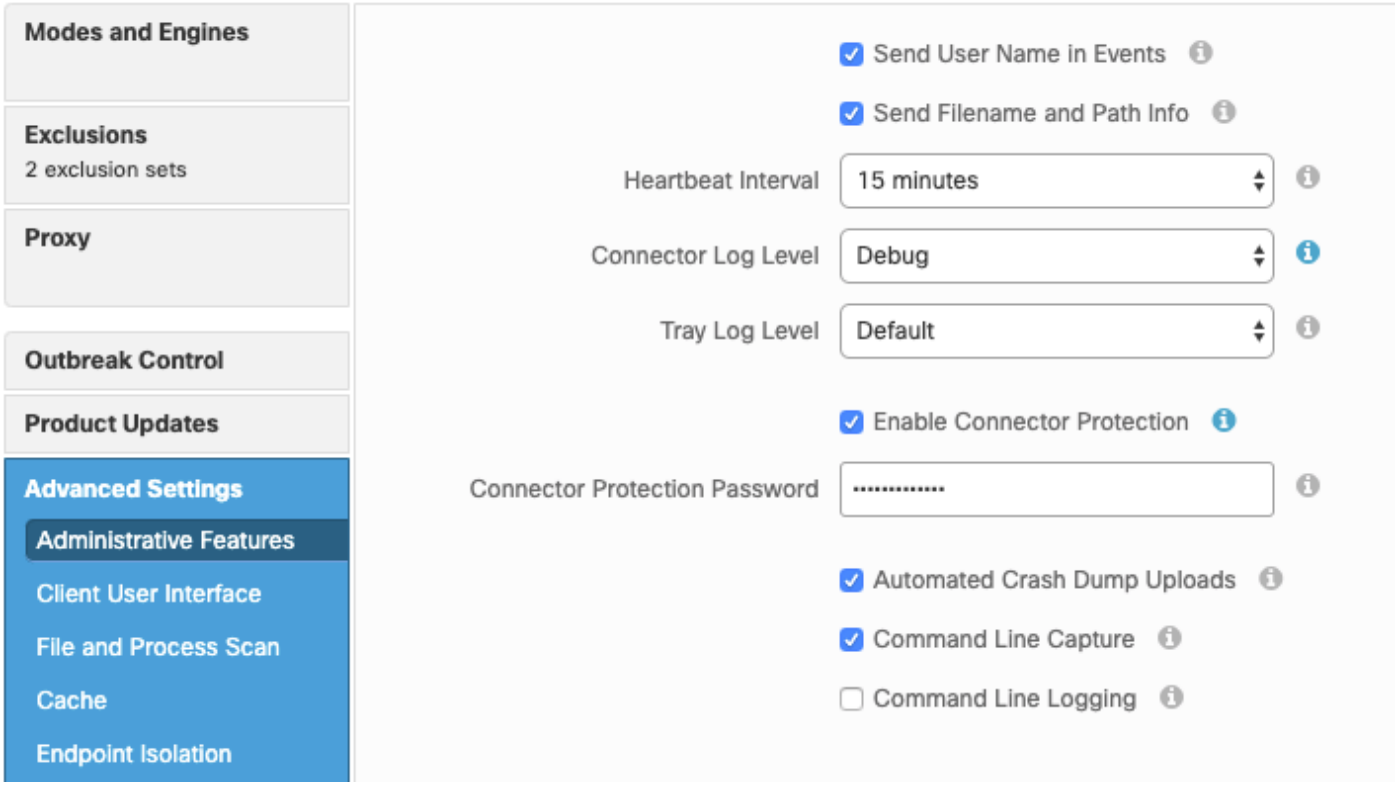


Étape 6. Une nouvelle stratégie appelée « Copie de... » sera créé. Cliquez sur **Modifier** pour modifier cette stratégie.



Étape 7. À la page Modifier la stratégie, accédez à **Paramètres avancés > Fonctions administratives**.

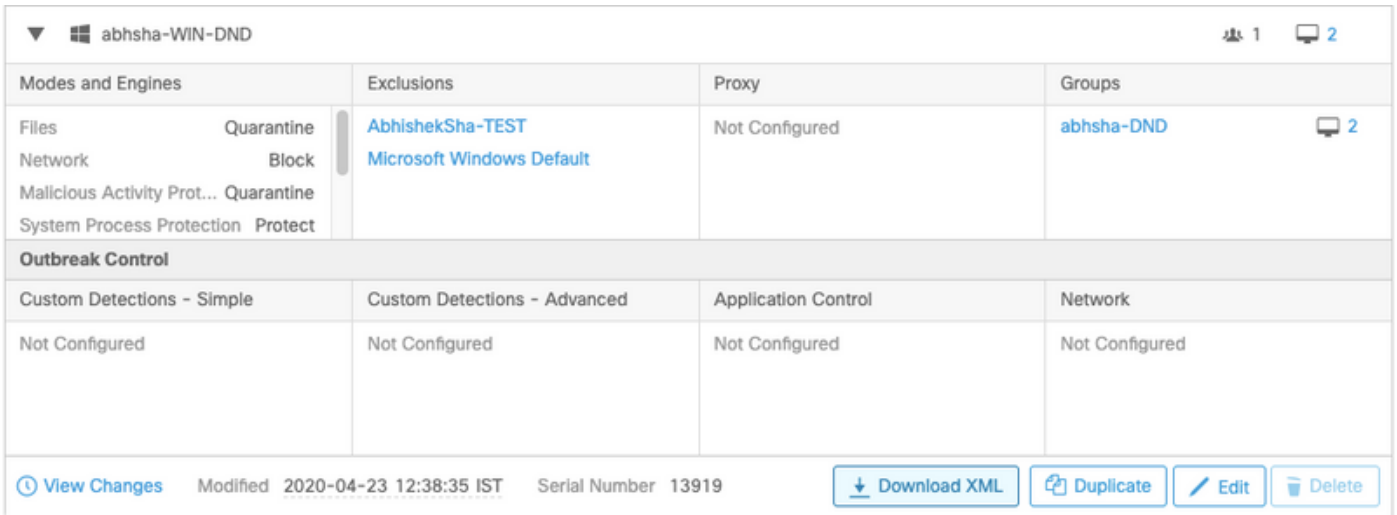
Étape 8. Dans le champ **Connector Password Protection**, remplacez le mot de passe par un nouveau mot de passe qui peut être rappelé.



Étape 9. Cliquez sur le bouton **Enregistrer** afin d'enregistrer cette stratégie.

Étape 10. Accédez à **Management > Policies** et recherchez la stratégie qui a été dupliquée.

Étape 11. Développez la stratégie et cliquez sur **Télécharger le fichier XML.** Un fichier nommé **policy.xml** sera enregistré sur votre ordinateur.

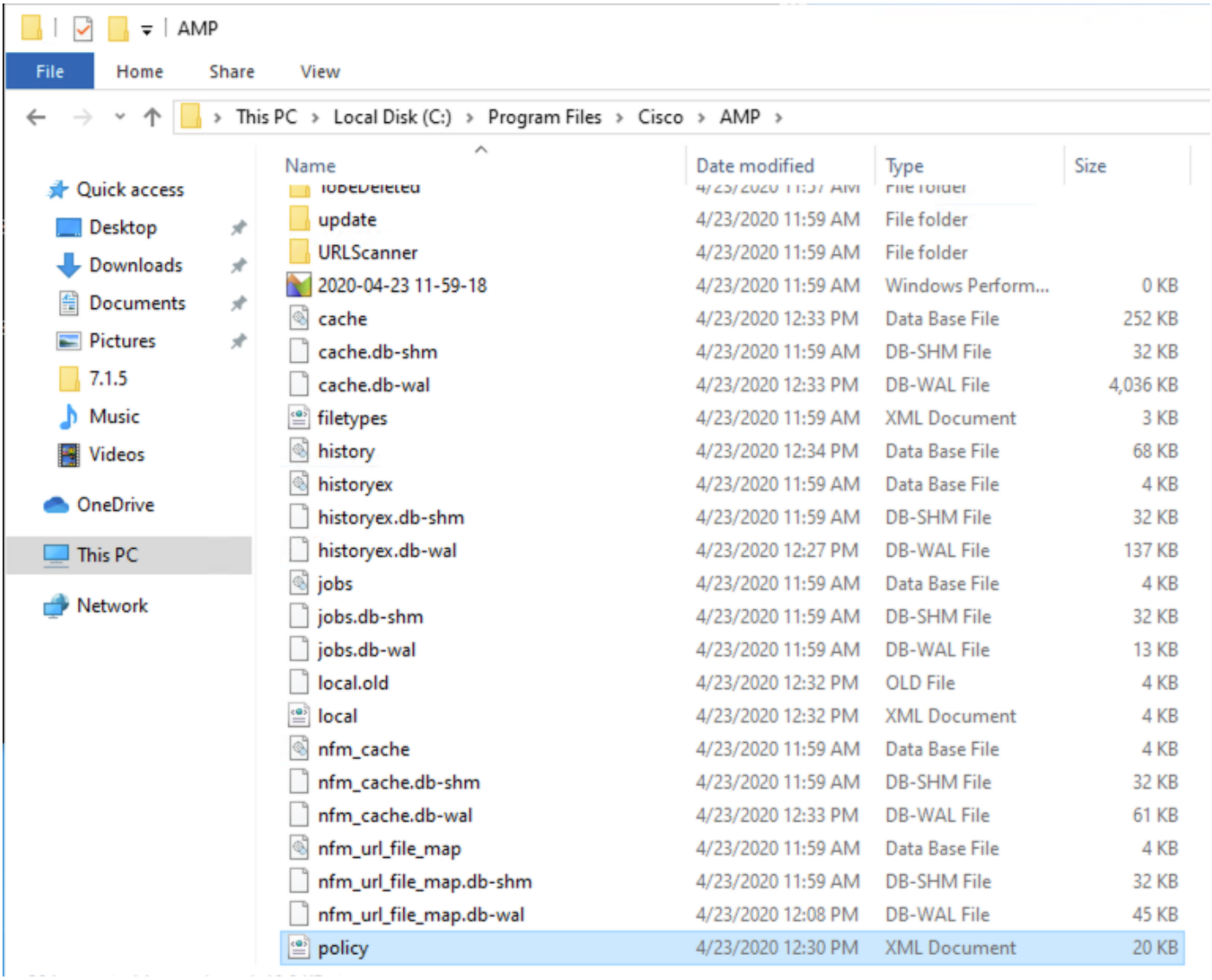


Étape 12. Copiez ce **policy.xml** sur le point de terminaison affecté.

Étape 13. Redémarrez le point de terminaison affecté en **mode sans échec**.

Étape 14. Une fois le point de terminaison affecté en **mode sans échec**, accédez à **C:\Program Files\Cisco\AMP**.

Étape 15. Dans ce dossier, recherchez un fichier nommé **policy.xml** et renommez-le **policy_old.xml**.



Étape 16. Maintenant, collez le fichier **policy.xml** précédemment copié dans ce dossier.

Étape 17. Une fois le fichier copié, la désinstallation peut être effectuée normalement et à l'invite du mot de passe, le mot de passe nouvellement configuré doit être entré.

Étape 18. Il s'agit d'une étape facultative. Comme le connecteur a été désinstallé lors de la déconnexion de la machine, l'entrée de l'ordinateur reste sur la console. Par conséquent, vous pouvez accéder à **Management > Computers** et développer le point de terminaison affecté. Cliquez sur **Supprimer** afin de supprimer le point de terminaison.