

Configuration de la notification contextuelle dans Cisco Secure Endpoint

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer des notifications contextuelles lorsque Cisco Secure Endpoint détecte un fichier malveillant.

Contribution de Javier Martinez, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur ces sujets :

- Tableau de bord de la console Cisco Secure Endpoint
- Un compte avec des privilèges d'administrateur

Components Used

Les informations de ce document sont basées sur Cisco Secure Endpoint version 6.3.7 et ultérieures.

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. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Cisco Secure Endpoint peut envoyer une alerte contextuelle sur les principaux terminaux sécurisés au niveau du point de terminaison lorsqu'il détecte, bloque ou met en quarantaine un fichier/processus.

Étape 1. Connectez-vous à AMP Console ; <https://console.amp.cisco.com/> comme indiqué dans

l'image.



Dashboard

Analysis ▾

Outbreak Control ▾

Management ▾

Accounts ▾

Étape 2. Accédez à **Management > Politiques** (sélectionnez la stratégie) **>Advance settings > Client User Interface**.

Les notifications du moteur sont désactivées par défaut, comme le montre l'image.

A screenshot of the Secure Endpoint management interface. On the left is a navigation sidebar with categories: Modes and Engines, Exclusions (2 exclusion sets), Proxy, Outbreak Control, Product Updates, and Advanced Settings. Under Advanced Settings, the following options are listed: Administrative Features, Client User Interface (highlighted in dark blue), File and Process Scan, Cache, Endpoint Isolation, Orbital, Engines, TETRA, Network, Scheduled Scans, and Identity Persistence. The main content area shows four settings: 'Start Client User Interface' (checked), 'Cloud Notifications' (checked), 'Engine Notifications' (unchecked and highlighted with a red box), and 'Hide Exclusions' (unchecked). Each setting has an information icon to its right.

Étape 3. Cochez la case **Notifications du moteur** comme indiqué dans l'image.

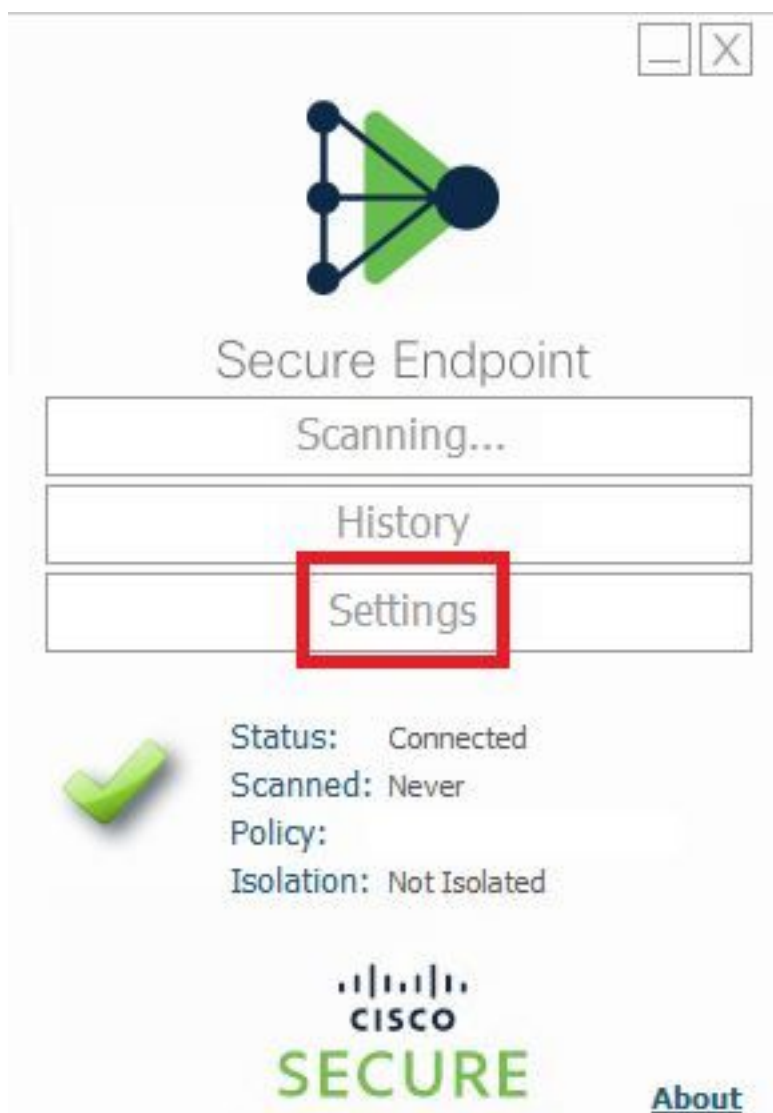
Start Client User Interface 

Cloud Notifications 

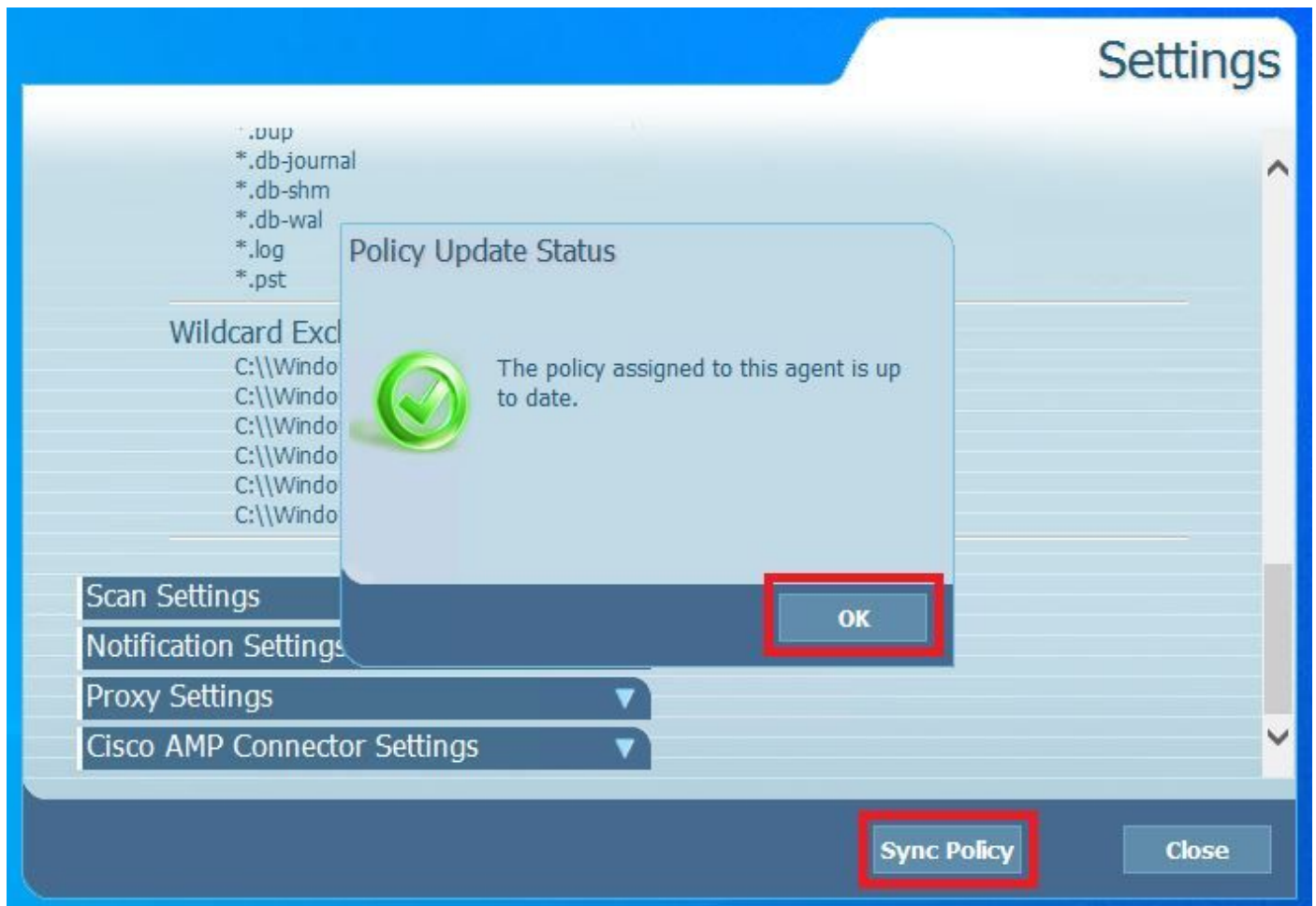
Engine Notifications 

Hide Exclusions 

Étape 4. Pour appliquer les nouvelles modifications, accédez à Desktop > OpenCisco Secure Endpoint et sélectionnez **Settings**, comme illustré dans l'image.



Étape 5. Cliquez sur **Stratégie de synchronisation** et sélectionnez **OK**, comme illustré dans l'image.



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Lorsque le moteur de point de terminaison sécurisé met en quarantaine un fichier/processus, une notification contextuelle s'affiche sur le bureau, comme l'illustre l'image.



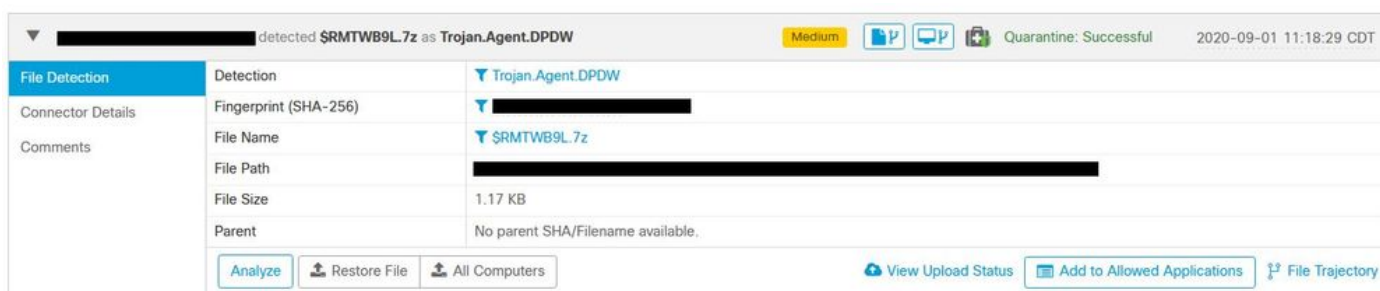
Note: Cette configuration s'applique à tous les périphériques appartenant à la stratégie.

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Si le point de terminaison sécurisé ne déclenche pas de notification contextuelle, un événement d'alerte s'affiche sur la console de point de terminaison sécurisé.

Accédez à **Cisco Secure Endpoint Console > Dashboard > Events**, comme illustré dans l'image.



S'il n'y a pas de notification contextuelle dans l'événement de point de terminaison ou d'alerte dans la console de point de terminaison sécurisé, contactez le support technique de Cisco.

Assistance Cisco : Visitez le portail en ligne à l'adresse <http://cisco.com/tac/caseopen> ou par téléphone : Numéros de téléphone régionaux gratuits :

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html