

# Créer une liste de détection personnalisée avancée dans Cisco Secure Endpoint

## Contenu

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Créer une liste de détection personnalisée avancée](#)

[Informations connexes](#)

## Introduction

Ce document décrit les étapes à suivre pour créer une détection personnalisée avancée (ACD) dans Cisco Secure Endpoint.

## Informations générales

TALOS Intelligence a publié un BLOG le 14 janvier 2020 en réponse aux révélations de vulnérabilité de Microsoft Patch Mardi.

Mise à jour le 15 janvier : Ajout d'une signature ACD pour AMP qui peut être utilisée pour détecter l'exploitation de CVE-2020-0601 en usurpant les certificats se faisant passer pour une autorité de certification de signature de code ECC Microsoft :

<https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html>.

Signature du fichier trouvé dans le BLOG TALOS à utiliser dans l'ACD :

- Win.Exploit.CVE\_2020\_0601:1:\*:06072A8648CE3D020106\*06072A8648CE3D020130
- <https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt>

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

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

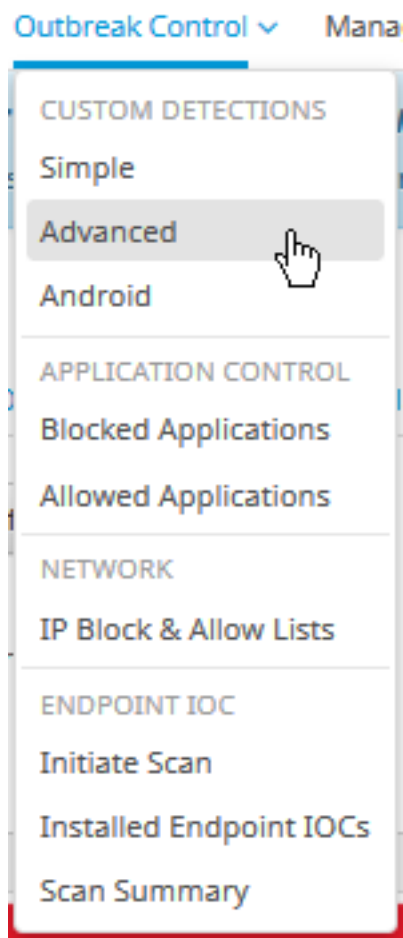
- Portail cloud Cisco Secure Endpoint
- ACD
- Blog TALOS

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Créer une liste de détection personnalisée avancée

Maintenant, créons l'ACD pour qu'il corresponde.

Étape 1. Accédez à **Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection** comme indiqué dans l'image.



Étape 2. Commencez par un nom pour le jeu de signatures **CVE-2020-0601** comme indiqué dans l'image.

# Custom Detections - Advanced

Create Signature Set

Name

Save

Étape 3. Ensuite, **modifiez** ce nouveau jeu de signatures et **ajoutez une signature**.  
Win.Exploit.CVE\_2020\_0601:1:\*:06072A8648CE3D020106\*06072A8648CE3D020130.

## Custom Detections - Advanced

[View All Changes](#)

Create Signature Set

**CVE-2020-0601**  
Created by Mustafa Shukur · 2020-01-22 12:19:38 CST

Used in policies:   
Used in groups:

[View Changes](#) [Download](#) [Edit](#) [Delete](#)

CVE-2020-0601 [Update Name](#)

Created by Mustafa Shukur · 2020-01-22 12:19:38 CST

[Add Signature](#) [Build Database From Signature Set](#)

ndb: Win.Exploit.CVE\_2020\_0601.UNOFFICIAL

Étape 4. Sélectionnez **Créer une base de données à partir d'un jeu de signatures** et la base de données a été créée.

Étape 5. Appliquer le nouveau jeu de signatures à une stratégie, cliquez sur **Modifier** > **Contrôle des attaques** > **Détections personnalisées** > **Avancé** comme indiqué dans l'image.

**Modes and Engines**

**Exclusions**  
3 exclusion sets

**Proxy**

**Outbreak Control**

**Product Updates**

**Advanced Settings**

Custom Detections - Simple

Custom Detections - Advanced

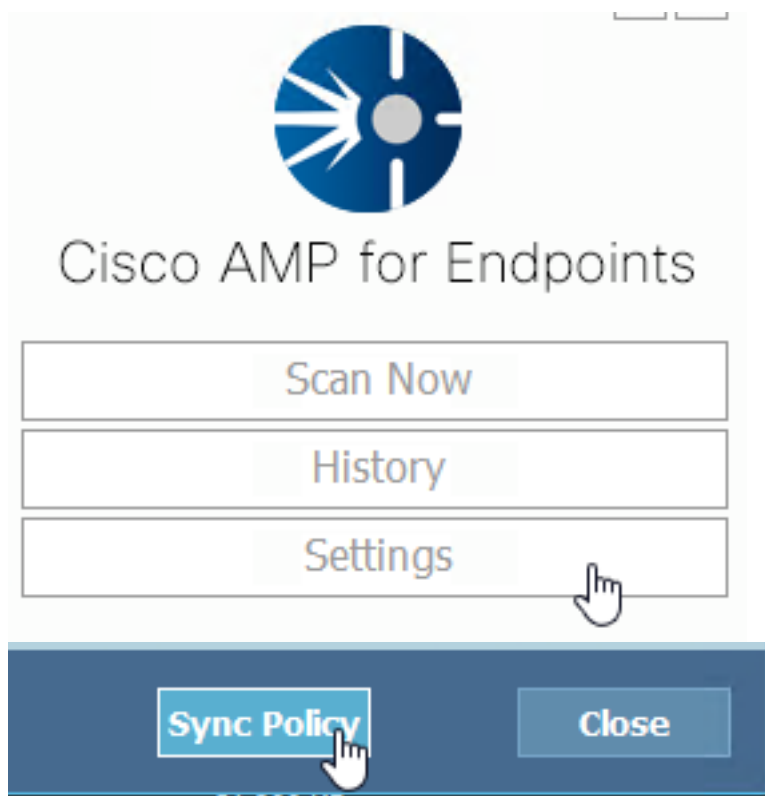
Application Control - Allowed

Application Control - Blocked

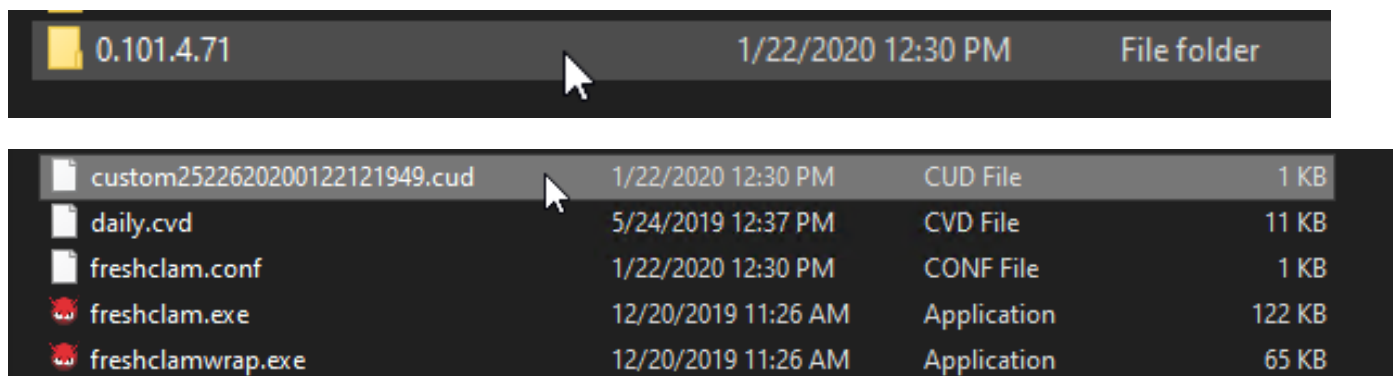
Network - IP Block & Allow Lists  [Clear](#) [Select Lists](#)

[Cancel](#) [Save](#)

Étape 6. Enregistrez la stratégie et la synchronisation au niveau de l'interface utilisateur du connecteur, comme indiqué dans l'image.



Étape 7. Recherchez dans le répertoire C:\Program Files\Cisco\AMP\ClamAV un nouveau dossier Signature créé ce jour-là, comme illustré dans l'image.



## Informations connexes

- La build utilisée pour le test est Windows 10 1909 qui n'est pas affecté par la vulnérabilité par le MSKB ; <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601>
- <https://support.microsoft.com/en-us/help/4534273/windows-10-update-kb4534273>
- S'applique à : Windows 10, version 1809, Windows Server version 1809, Windows Server 2019, toutes versions
- [Support et documentation techniques - Cisco Systems](#)