

# 在思科安全終端中建立高級自定義檢測清單

## 目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[建立高級自定義檢測清單](#)

[相關資訊](#)

## 簡介

本檔案介紹在思科安全終端中建立進階自訂偵測(ACD)的步驟。

## 背景資訊

TALOS Intelligence於2020年1月14日發佈部落格，以響應Microsoft Patch Tuesday漏洞披露。

1月15日更新：為AMP新增了一個ACD簽名，該簽名可用於通過偽裝為Microsoft ECC代碼簽名證書頒發機構的偽裝證書來檢測對CVE-2020-0601的利用

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

在TALOS部落格中找到的要用於ACD的檔案的簽名：

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

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

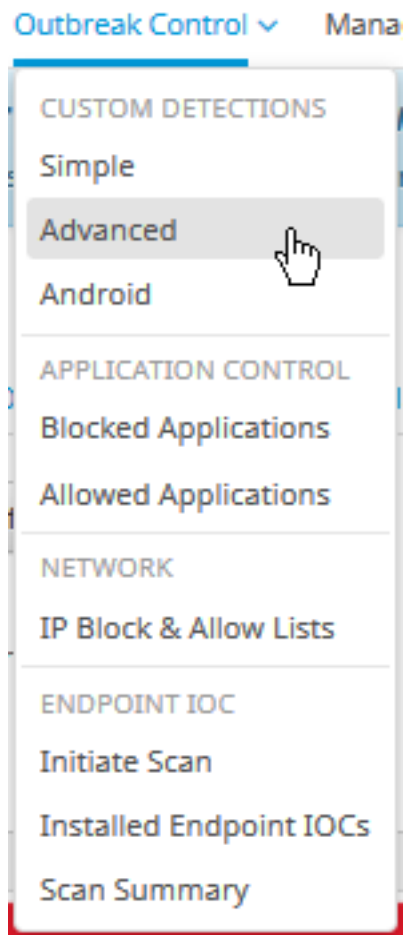
- 思科安全終端雲端入口網站
- ACD
- TALOS部落格

本文中的資訊是根據特定實驗室環境內的裝置所建立。所有使用的裝置都以已清除（預設）的配置啟動。如果您的網路處於活動狀態，請確保您瞭解任何命令可能產生的影響。

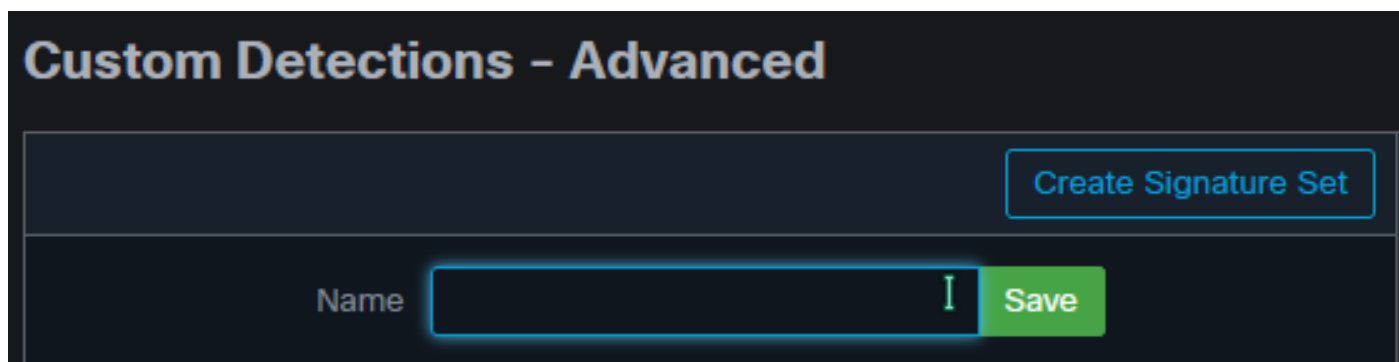
## 建立高級自定義檢測清單

現在，讓我們建立要匹配的ACD。

步驟1。導覽至安全終端入口網站>爆發控制>進階自訂偵測，如下圖所示。



步驟2.以特徵碼集CVE-2020-0601的名稱開始，如下圖所示。



步驟3.下一步編輯該新簽名集和新增簽名。

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

步驟4.選擇Build Database From Signature Set，此時已生成資料庫。

步驟5.將新的特徵碼集應用於策略，按一下Edit> Outbreak Control > Custom Detections > Advanced，如下圖所示。

**Modes and Engines**

**Exclusions**  
3 exclusion sets

**Proxy**

**Outbreak Control**

**Product Updates**

**Advanced Settings**

Custom Detections - Simple

Custom Detections - Advanced

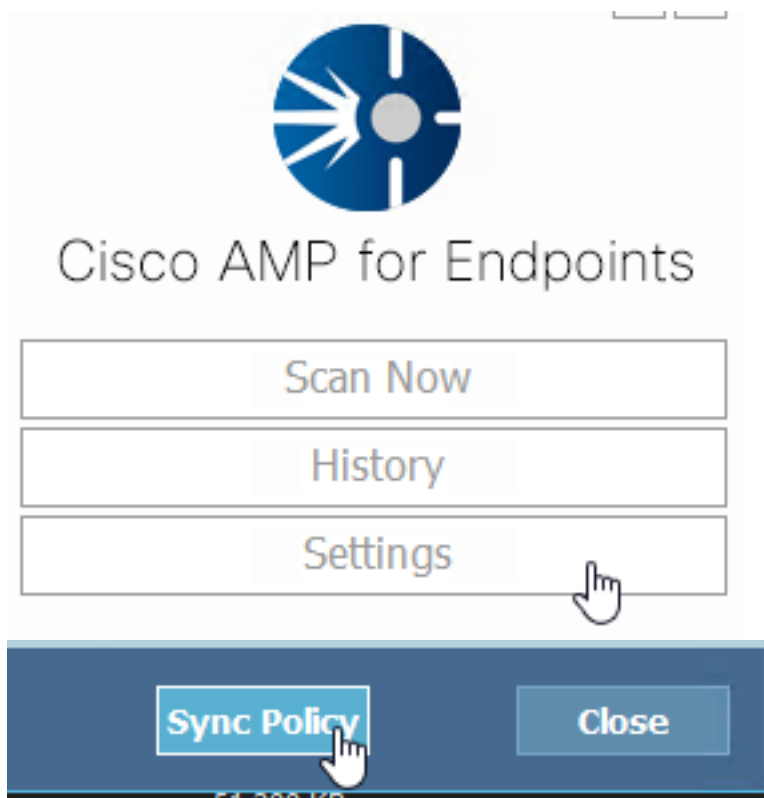
Application Control - Allowed

Application Control - Blocked

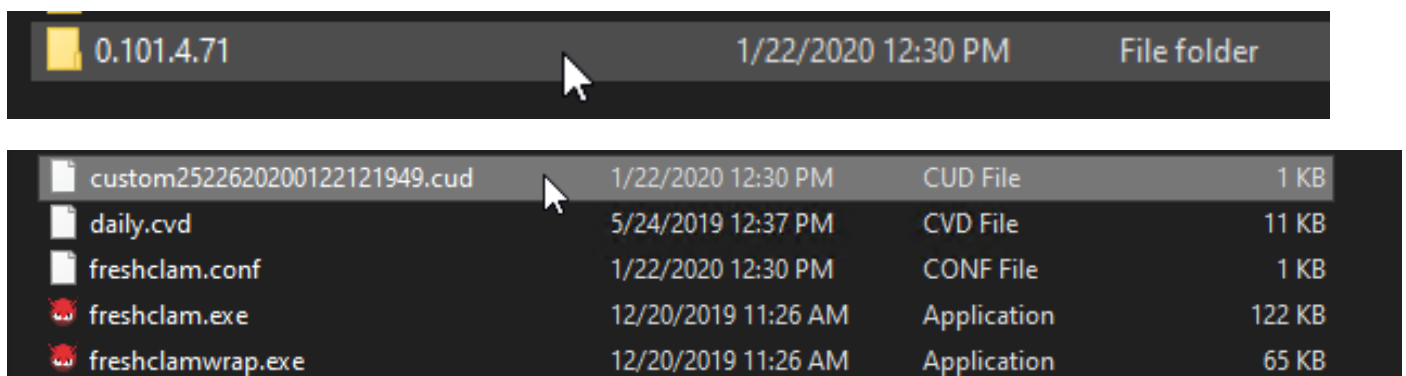
Network - IP Block & Allow Lists  [Clear](#)

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

步驟6.將「Policy (策略)」和「Sync (同步)」儲存在連結器UI中，如下圖所示。



步驟7. 在C:\Program Files\Cisco\AMP\ClamAV目錄中搜尋當天建立的新簽名資料夾，如下圖所示。



## 相關資訊

- 用於測試的版本是Windows 10 1909，它不受MSKB漏洞的影響  
； <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>
- 適用於：Windows 10、版本1809、Windows Server版本1809、Windows Server 2019，所有版本
- [技術支援與文件 - Cisco Systems](#)