Een eenvoudige aangepaste detectielijst instellen op het Advanced Malware Protection voor endpoints

Inhoud

Inleiding

Dit document beschrijft de stappen om een Eenvoudige Aangepaste Detectielijst te maken om specifieke bestanden te detecteren, te blokkeren en in quarantaine te zetten om te voorkomen dat bestanden worden toegestaan op apparaten die de Advanced Malware Protection (AMP) voor endpoints hebben geïnstalleerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot het AMP-portaal
- Account met administratorrechten
- Bestandsgrootte maximaal 20 MB

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Advanced Malware Protection voor endpoints, versie 5.4.2019.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Werkstroom

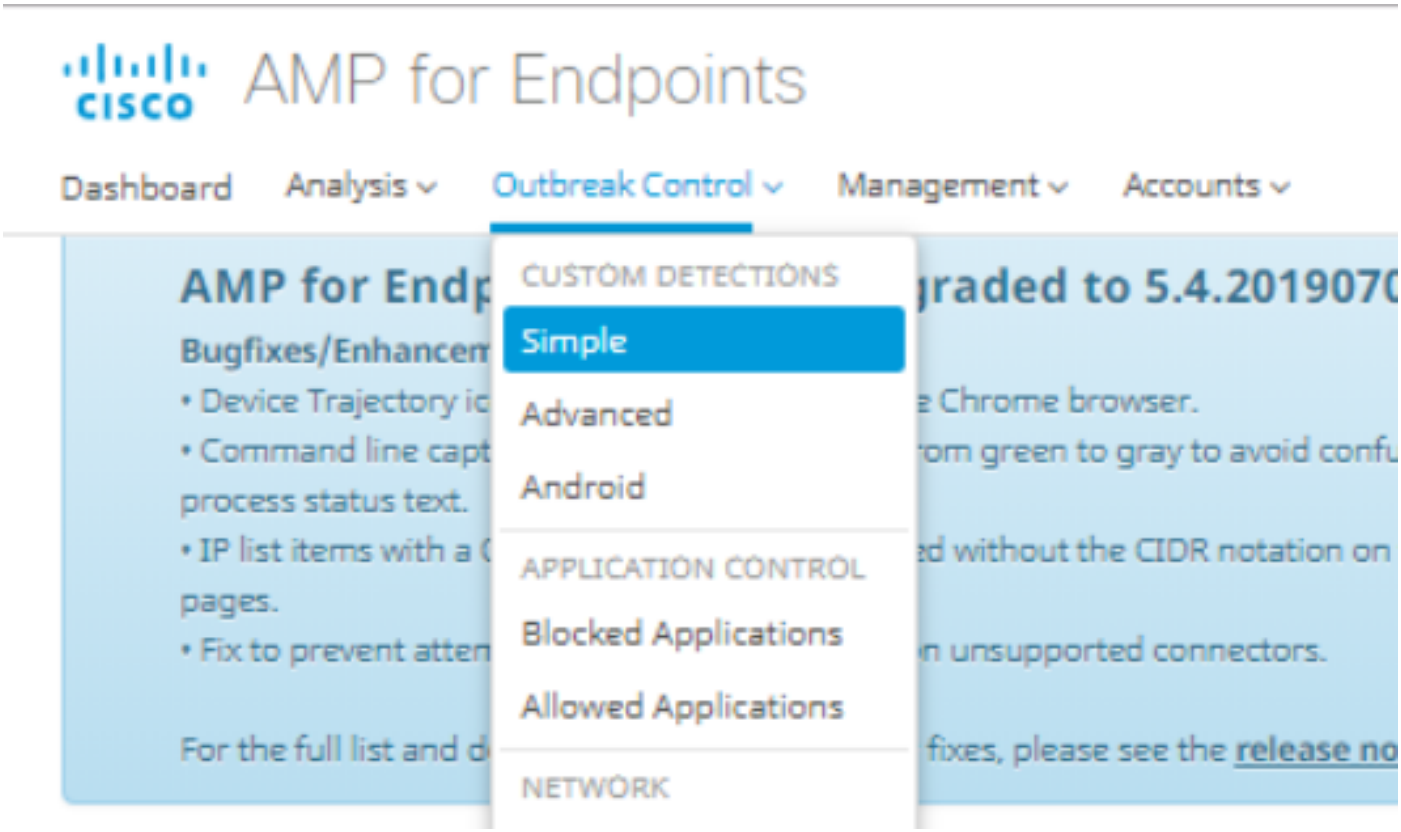
De optie Eenvoudige Aangepaste Detectie gebruikt deze werkstroom:

- De Eenvoudige Aangepaste Detectielijst die uit het AMP-portaal is gemaakt.
- Een eenvoudige lijst met aangepaste detectie die in een eerder gemaakt beleid is toegepast.
- De AMP-connector is op het apparaat geïnstalleerd en wordt in het beleid toegepast.

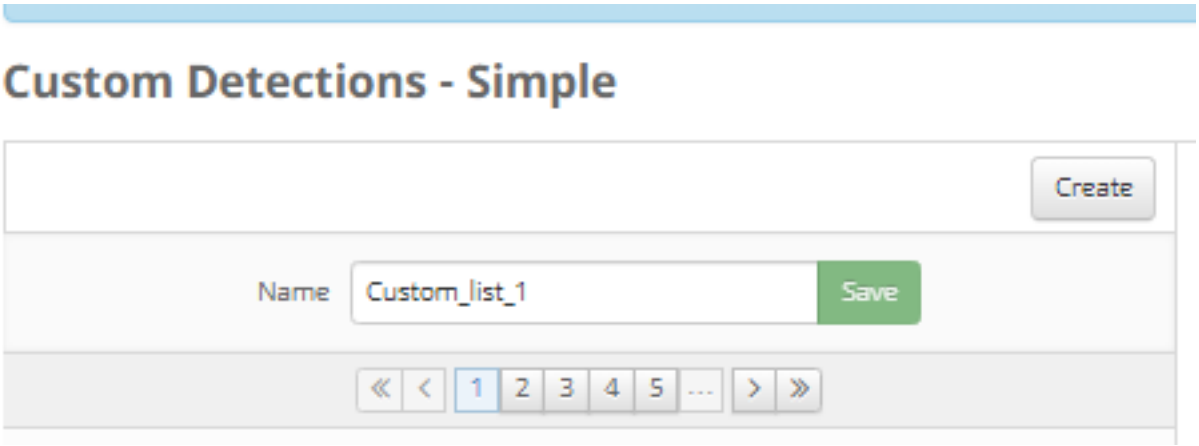
Configuratie

Om een eenvoudige lijst met aangepaste detectie te maken, volgt u deze stappen:

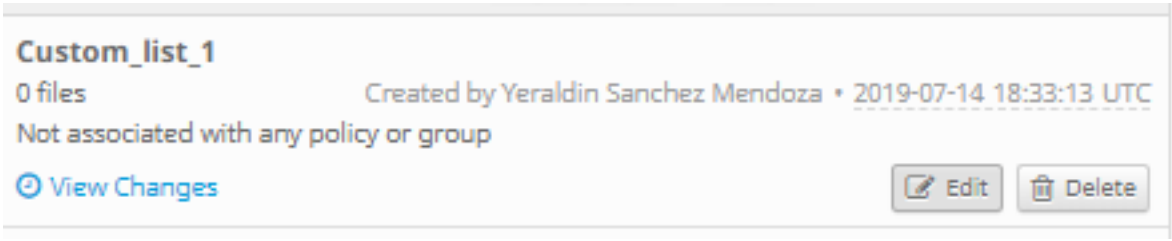
Stap 1. Ga op het AMP-portal naar **Outdoorkleding, Control > Eenvoudige** optie, zoals in de afbeelding.



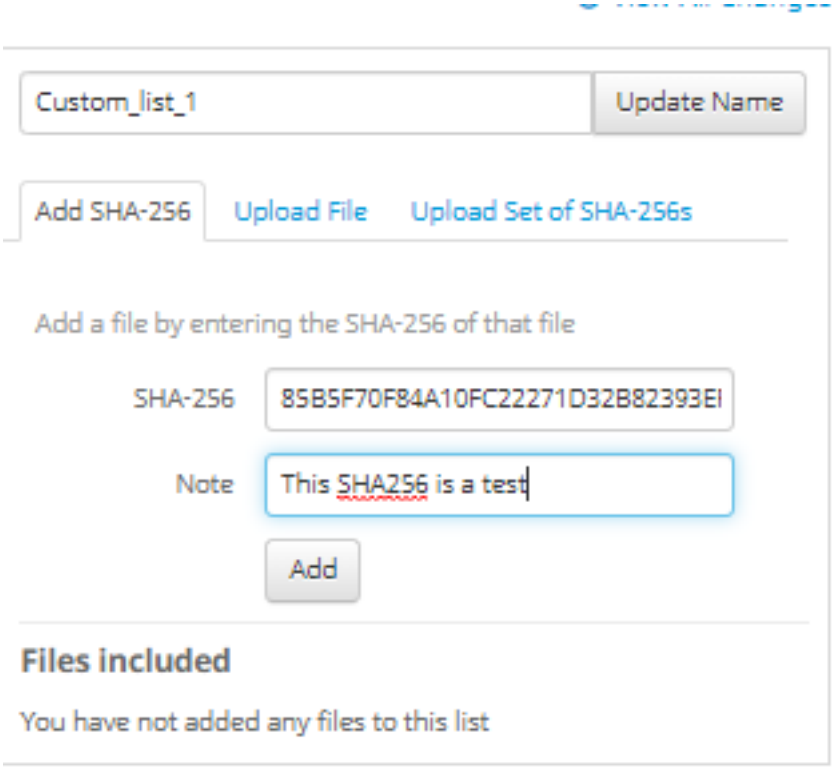
Stap 2. Klik op de optie Aangepaste detectie - Eenvoudige optie, klik op knop **maken** om een nieuwe lijst toe te voegen, kies een naam om de lijst Eenvoudige aangepaste detectie te identificeren en op te slaan, zoals in de afbeelding.



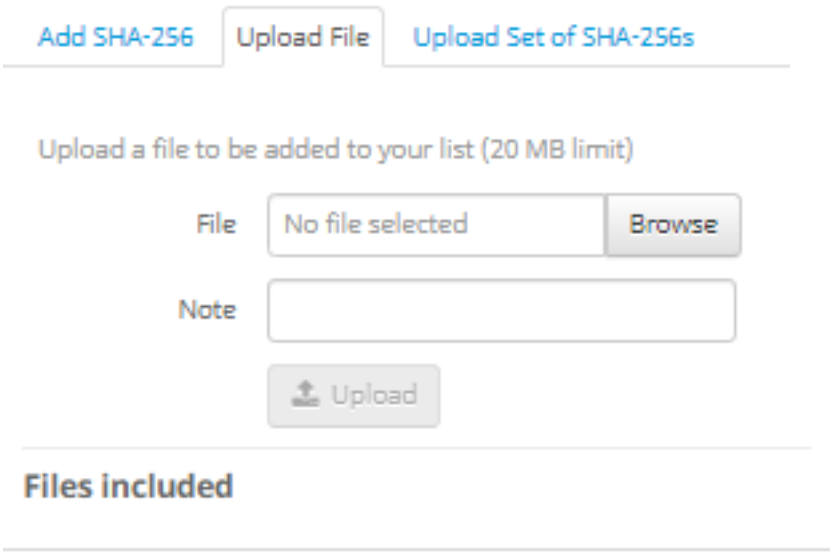
Stap 3. Klik op de knop **Bewerken** om de lijst met bestanden toe te voegen die u wilt blokkeren, zoals in de afbeelding.



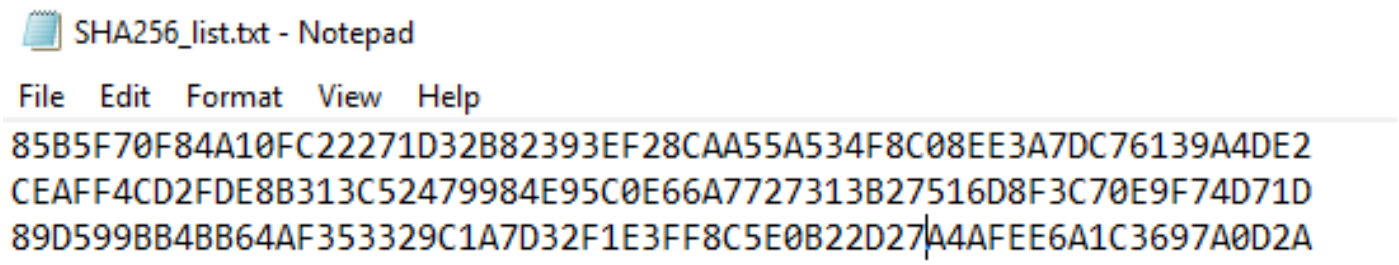
Stap 4. Voor de optie SHA-256 toevoegen, plakt u de SHA-256-code die eerder is verzameld uit het specifieke bestand dat u wilt blokkeren, zoals in de afbeelding.

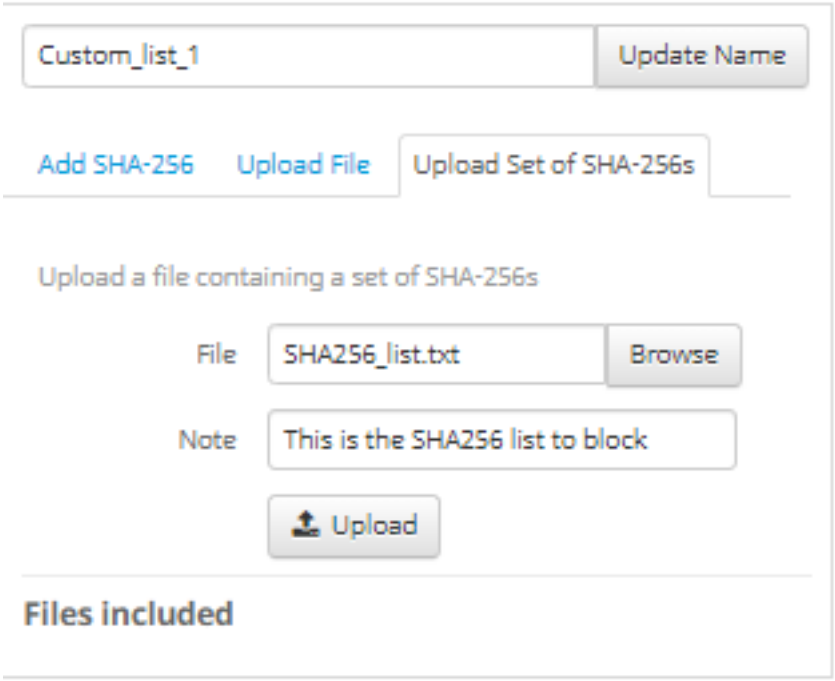


Stap 5. Blader in de optie Upload File voor het specifieke bestand dat u wilt blokkeren wanneer het bestand is geüpload, de SHA-256 van dit bestand wordt toegevoegd aan de lijst, zoals in de afbeelding.

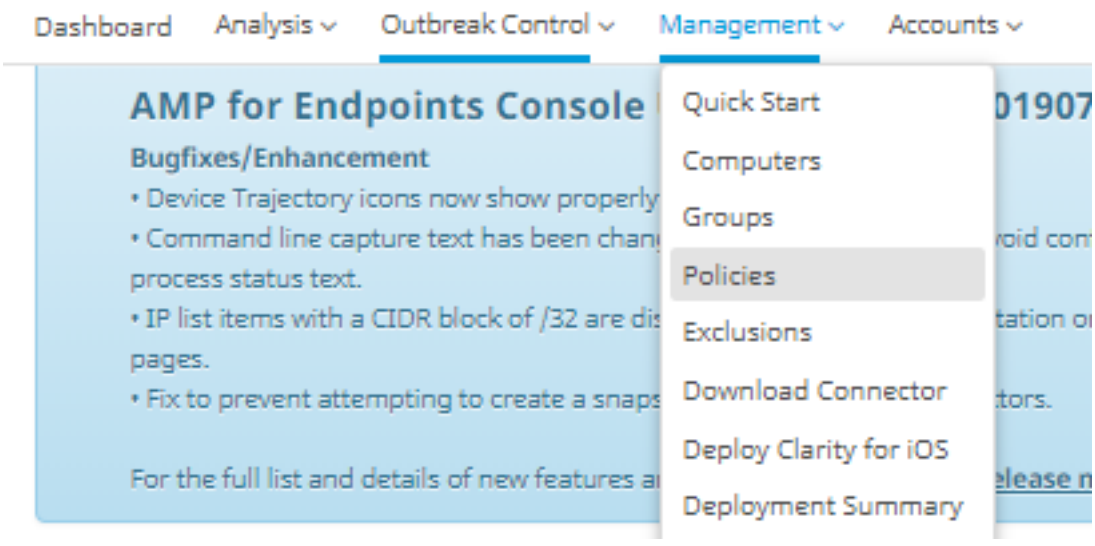


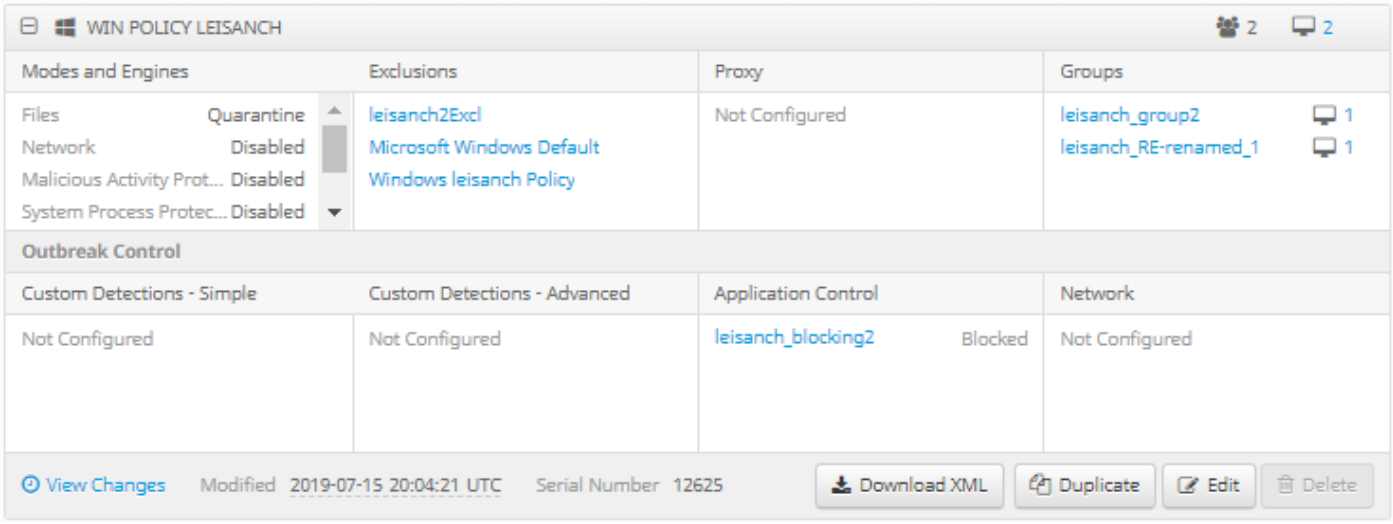
Stap 6. Met de optie Upload Set van SHA-256s kunt u een bestand toevoegen met een lijst met meerdere SHA-256-codes die u eerder hebt aangeschaft, zoals in de afbeeldingen.



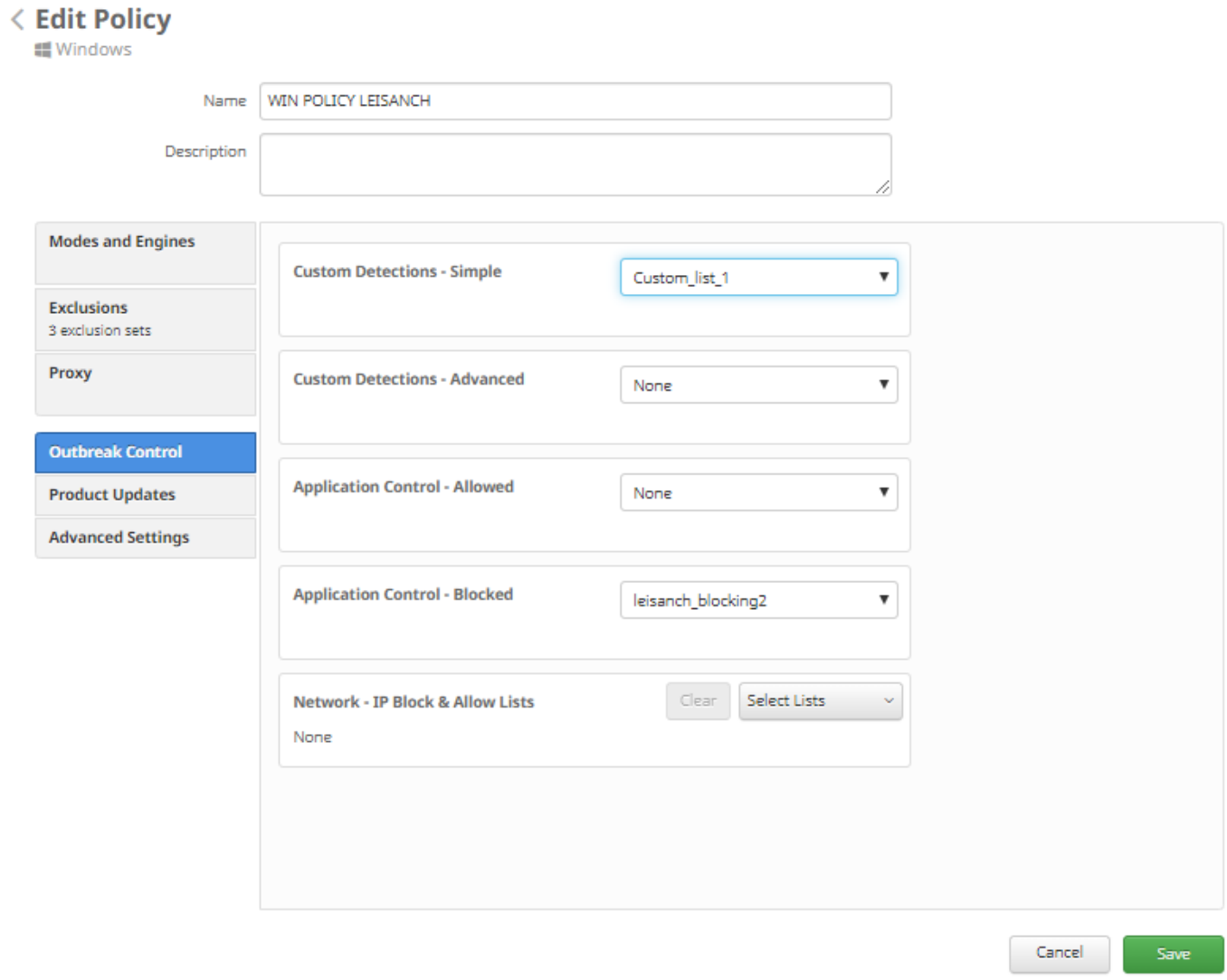


Stap 7. Zodra de lijst Eenvoudige Eigen detectie is gegenereerd, navigeer dan naar **Beheer > Beleid** en kies het beleid waar u de eerder gemaakte lijst wilt toepassen, zoals in de afbeeldingen.





Stap 8. Klik op de knop **Bewerken** en navigeer naar **Outdoorkleding > Aangepaste Detectie - Eenvoudig,** selecteer de lijst die eerder gegenereerd is in het vervolgkeuzemenu en bewaar de wijzigingen, zoals in de afbeelding.



Zodra alle stappen zijn uitgevoerd en de connectors zijn gesynchroniseerd voor de laatste beleidswijzigingen, wordt de Eenvoudige Aangepaste Detectie van kracht.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

> **Waarschuwing**: Als een bestand wordt toegevoegd aan een Eenvoudige Eigen Detectielijst, moet de cache tijd verlopen voordat de detectie effect heeft.

> Opmerking: Wanneer u een eenvoudige aangepaste detectie toevoegt, is deze onderworpen aan cached. Hoe lang een bestand gecached is, is mede afhankelijk van de beschikbaarheid, zoals in deze lijst wordt weergegeven:
> - Bestanden reinigen: 7 dagen
> - Onbekende bestanden: 1 uur
> - Kwaadaardige bestanden: 1 uur