Configurare un elenco di rilevamento personalizzato semplice nel portale AMP for Endpoints

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Flusso di lavoro](#)
[Configurazione](#)
[Verifica](#)
[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come creare un elenco di rilevamento personalizzato semplice per rilevare, bloccare e mettere in quarantena file specifici al fine di impedire che i file vengano autorizzati sui dispositivi che hanno installato i connettori Advanced Malware Protection (AMP) for Endpoints.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso al portale AMP
- Account con privilegi di amministratore
- Dimensioni del file non superiori a 20 MB

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la console Cisco AMP for Endpoints versione 5.4.20190709.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Flusso di lavoro

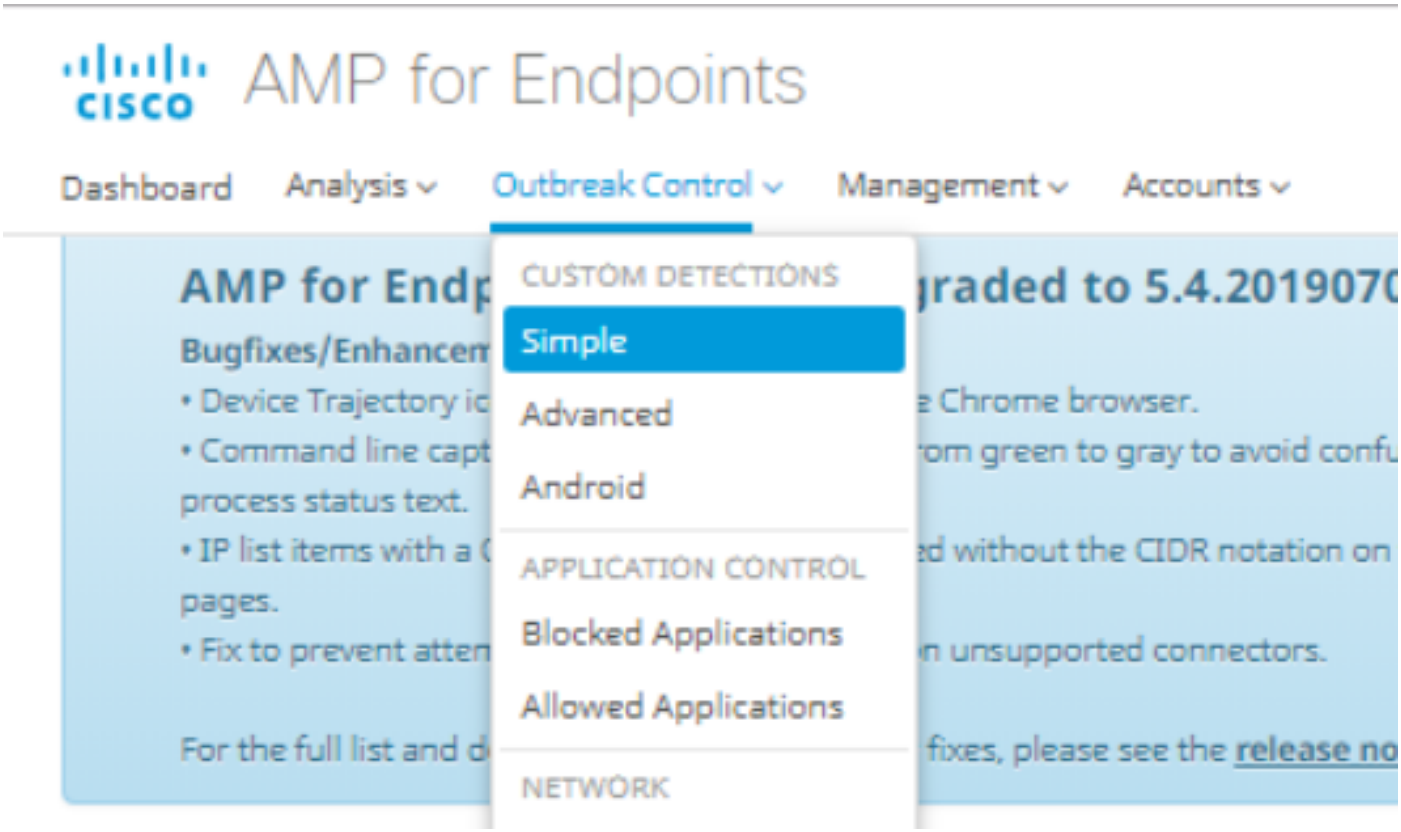
L'opzione Elenco rilevamento personalizzato semplice utilizza il flusso di lavoro seguente:

- Elenco di rilevamento personalizzato semplice creato dal portale AMP.
- Elenco di rilevamento personalizzato semplice applicato in un criterio creato in precedenza.
- Il connettore AMP installato nel dispositivo e applicato nel criterio.

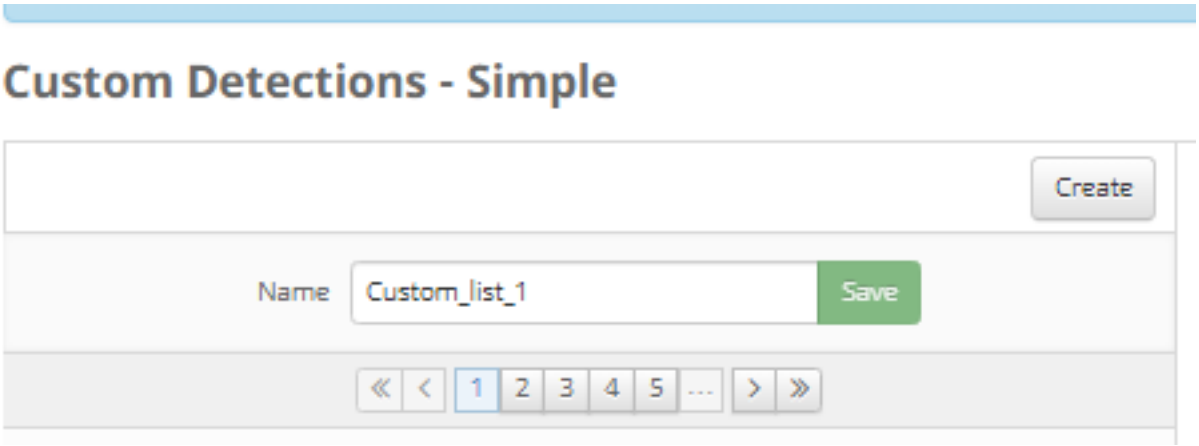
Configurazione

Per creare un elenco di rilevamento personalizzato semplice, eseguire la procedura seguente:

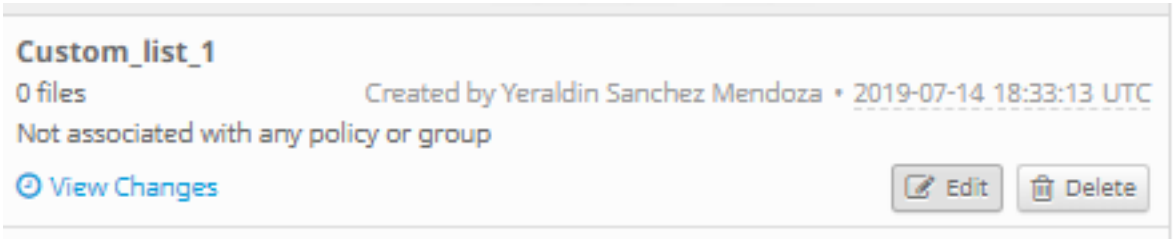
Passaggio 1. Sul portale AMP, selezionare **Controllo epidemie > Semplice**, come mostrato nell'immagine.



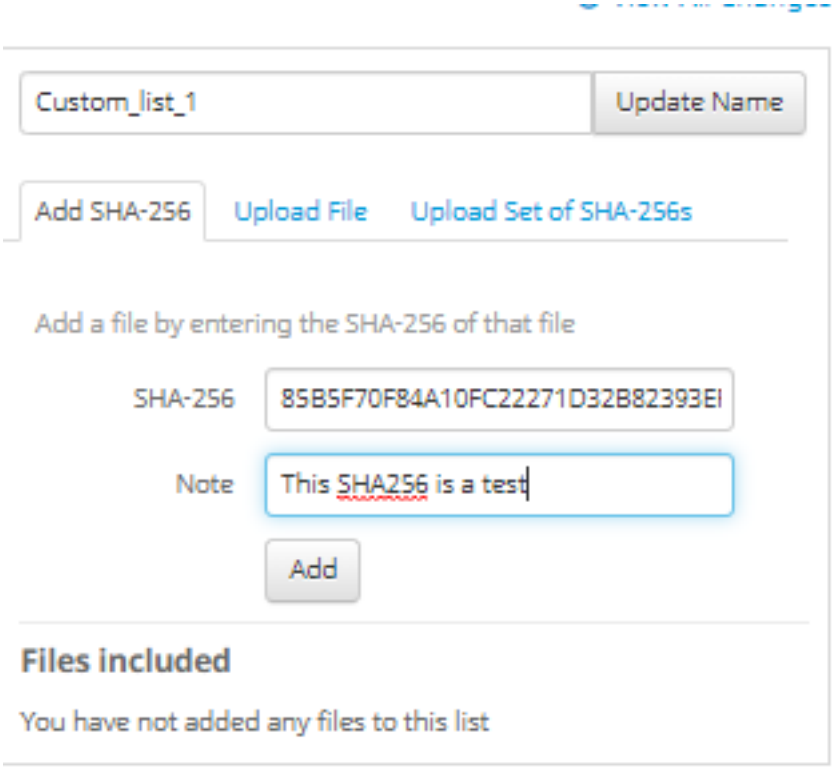
Passaggio 2. Nell'opzione Rilevamenti personalizzati - Semplici, fare clic su **Crea** pulsante per aggiungere un nuovo elenco, scegliere un nome per identificare l'elenco Rilevamento personalizzato semplice e salvarlo, come mostrato nell'immagine.



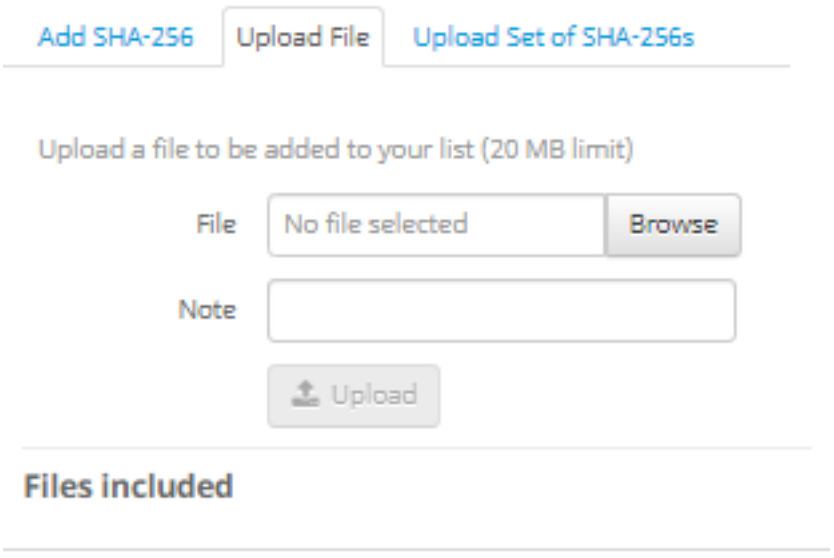
Passaggio 3. Una volta creato l'elenco, fare clic sul pulsante **Edit** (Modifica) per aggiungere l'elenco dei file che si desidera bloccare, come mostrato nell'immagine.



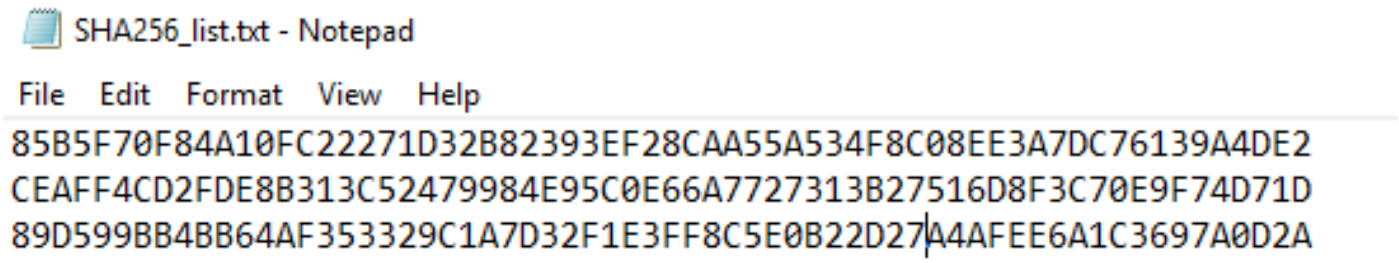
Passaggio 4. Nell'opzione Add SHA-256, incollare il codice SHA-256 precedentemente raccolto dal file specifico che si desidera bloccare, come mostrato nell'immagine.

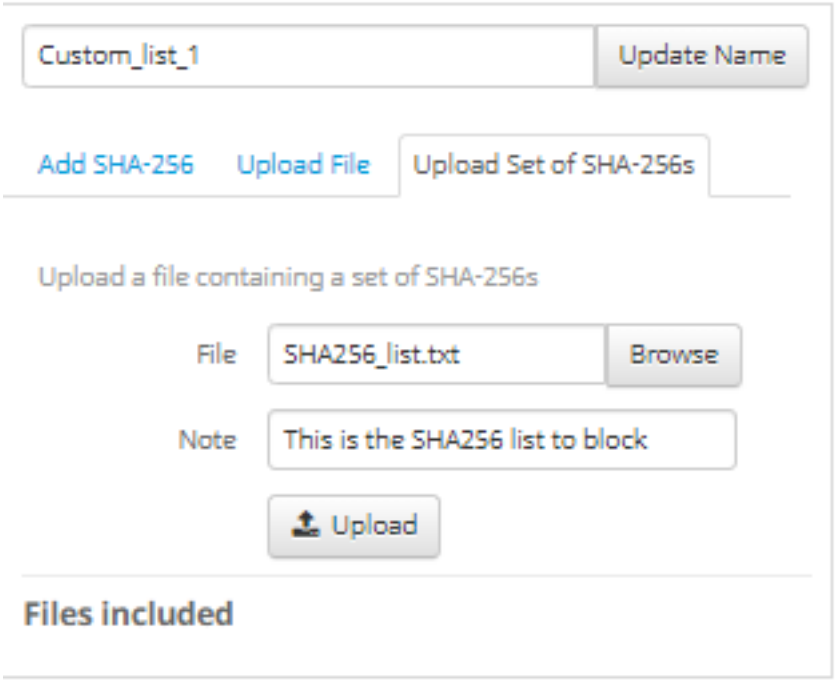


Passaggio 5. Nell'opzione Carica file, individuare il file specifico che si desidera bloccare, una volta caricato il file, l'SHA-256 di questo file viene aggiunto all'elenco, come mostrato nell'immagine.

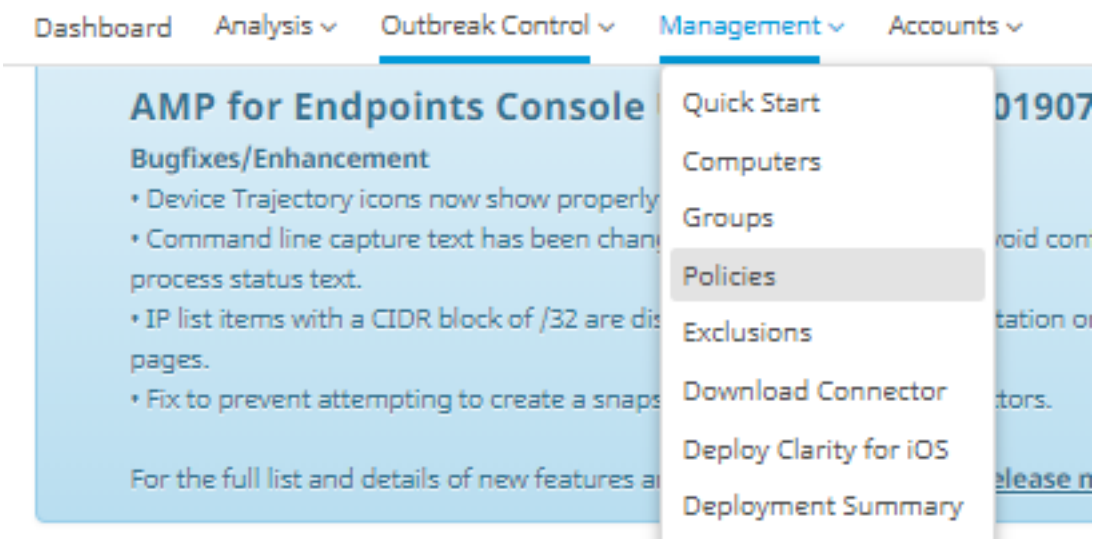


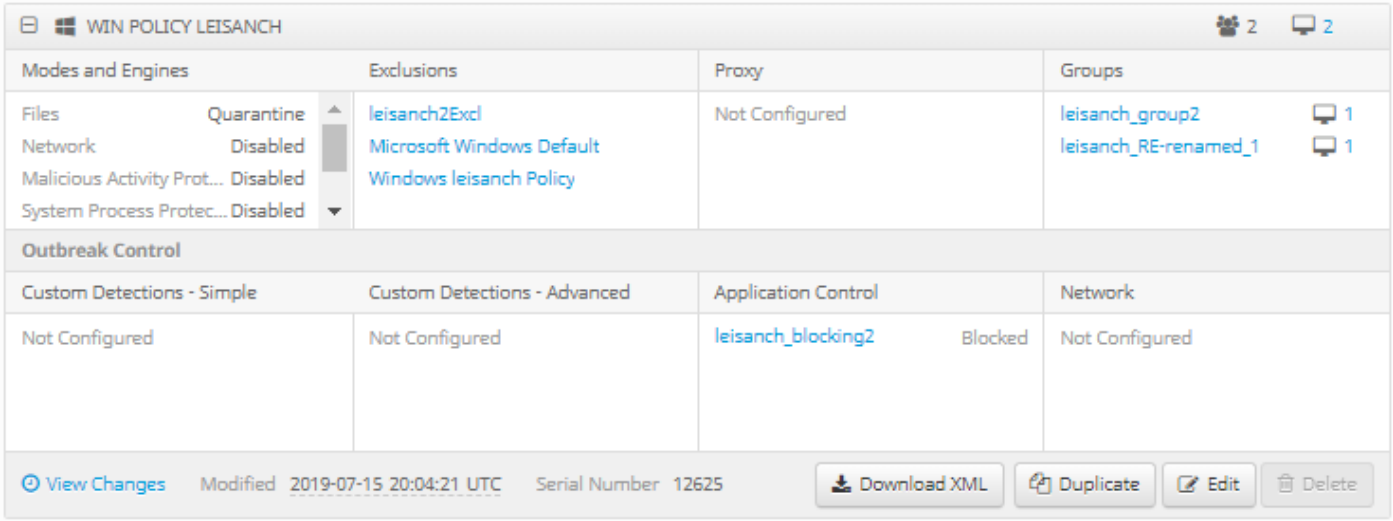
Passaggio 6. L'opzione Upload Set of SHA-256s consente di aggiungere un file con un elenco di più codici SHA-256 precedentemente acquisiti, come mostrato nelle immagini.



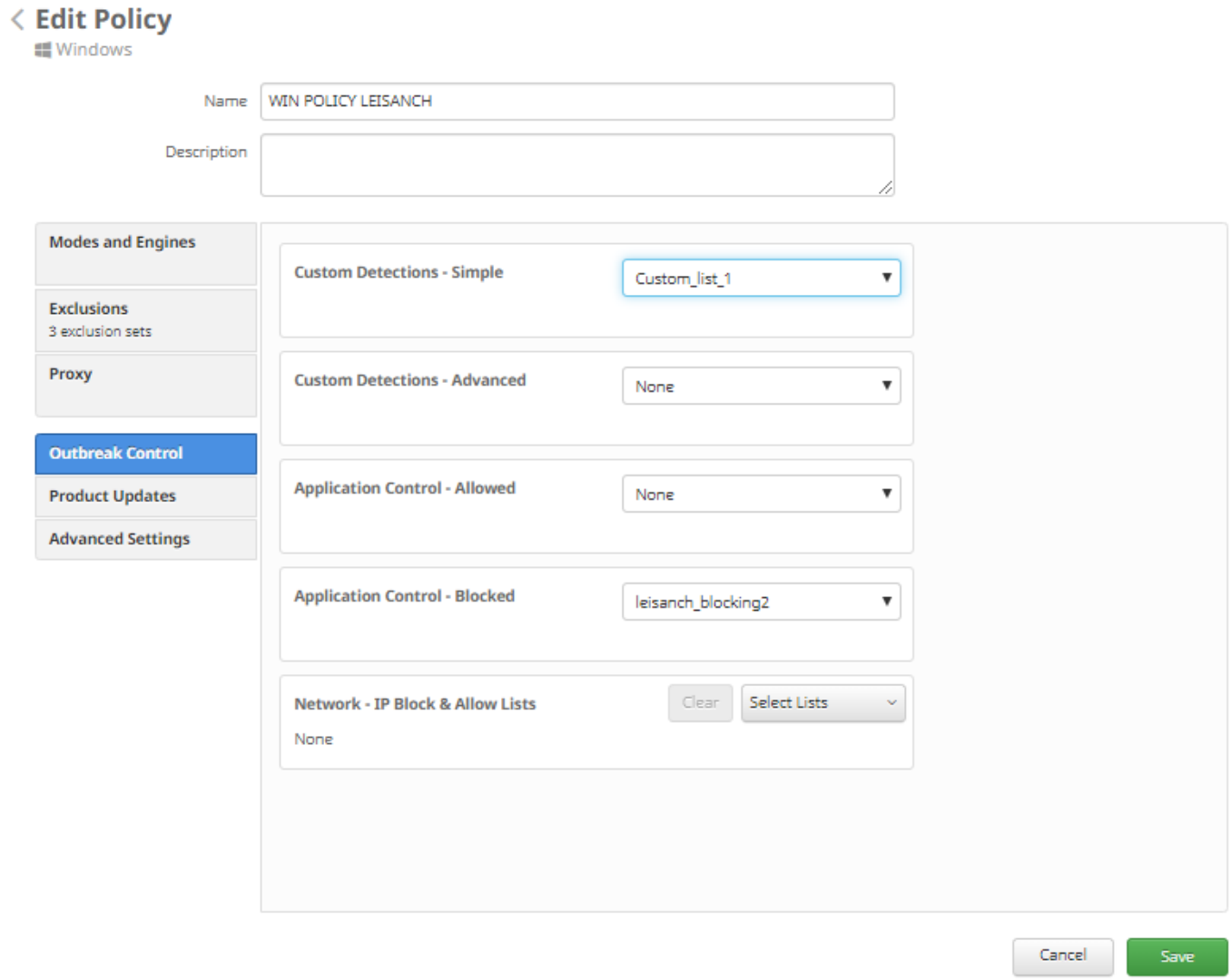


Passaggio 7. Una volta generato l'elenco Rilevamento custom semplice, passare a **Gestione > Criteri** e scegliere il criterio a cui applicare l'elenco creato in precedenza, come mostrato nelle immagini.





Passaggio 8. Fare clic sul pulsante **Modifica** e selezionare **Controllo epidemie > Rilevamenti personalizzati - Semplice,** selezionare l'elenco generato in precedenza dal menu a discesa e salvare le modifiche, come mostrato nell'immagine.



Dopo aver eseguito tutte le operazioni e aver sincronizzato i connettori con le ultime modifiche apportate ai criteri, viene attivato il rilevamento personalizzato semplice.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

> **Avviso:** Se un file viene aggiunto a un elenco di rilevamento personalizzato semplice, il tempo di memorizzazione nella cache deve scadere prima che il rilevamento abbia effetto.

> **Nota:** Quando si aggiunge un rilevamento personalizzato semplice, questo viene memorizzato nella cache. La durata della memorizzazione di un file nella cache dipende dalla relativa disposizione, come illustrato nell'elenco seguente:
> ·Pulizia dei file: 7 giorni

·File sconosciuti: 1 ora
·File dannosi: 1 ora