AMP for Endpointsポータルでの簡易カスタム検出リストの設定

内容

概要

このドキュメントでは、Advanced Malware Protection(AMP)for Endpointsコネクタをインストールしたデバイスで許可されるファイルを防止するために、特定のファイルを検出、ブロック、および検疫するための簡易カスタム検出リストを作成する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AMPポータルへのアクセス
- 管理者権限を持つアカウント
- ファイルサイズは20 MB以下

使用するコンポーネント

このドキュメントの情報は、Cisco AMP for Endpointsコンソールバージョン5.4.20190709に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ワークフロー

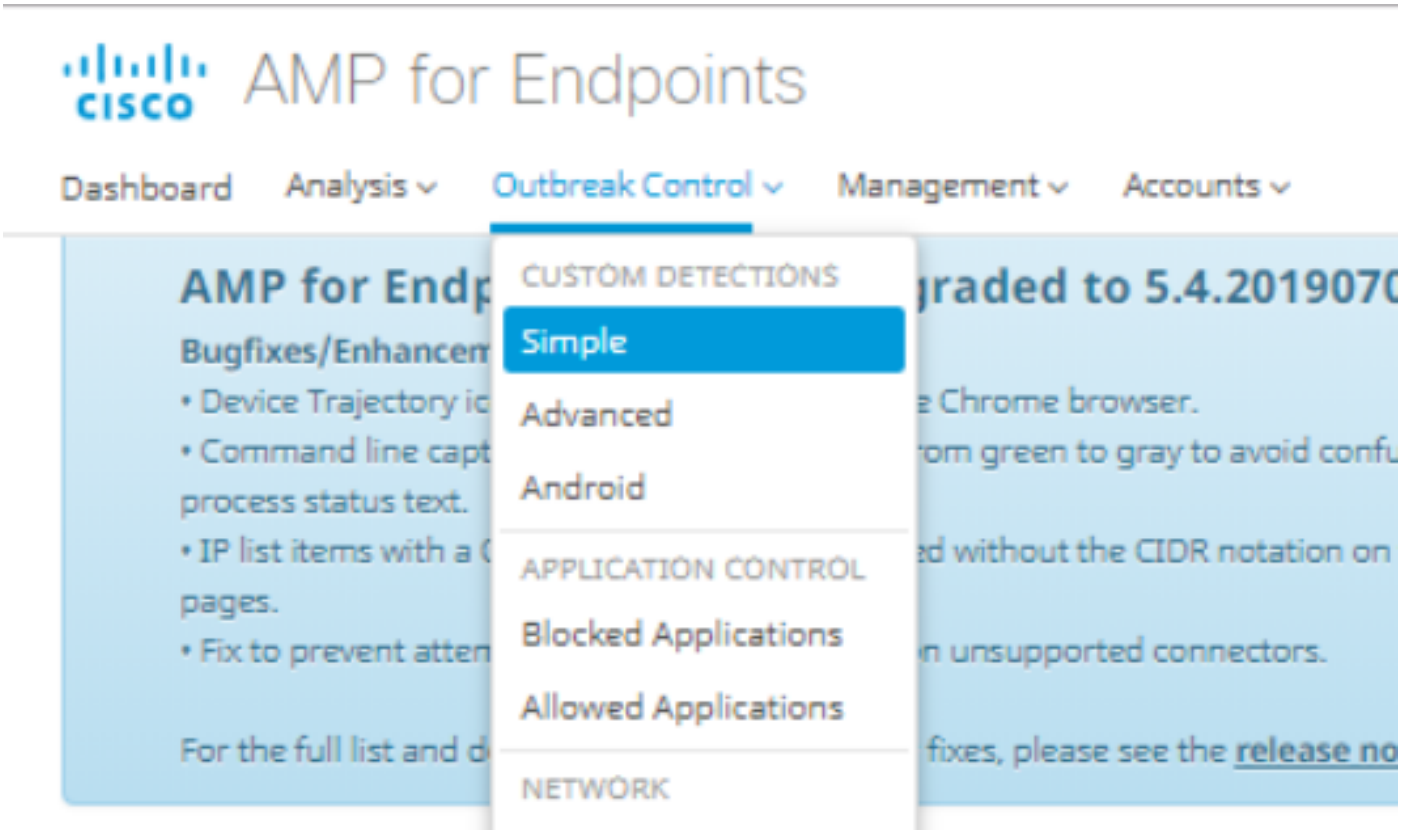
[Simple Custom Detection]リストオプションでは、次のワークフローを使用します。

- AMPポータルから作成された簡易カスタム検出リスト。
- 以前に作成したポリシーに適用された簡易カスタム検出リスト。
- デバイスにインストールされ、ポリシーに適用されたAMPコネクタ。

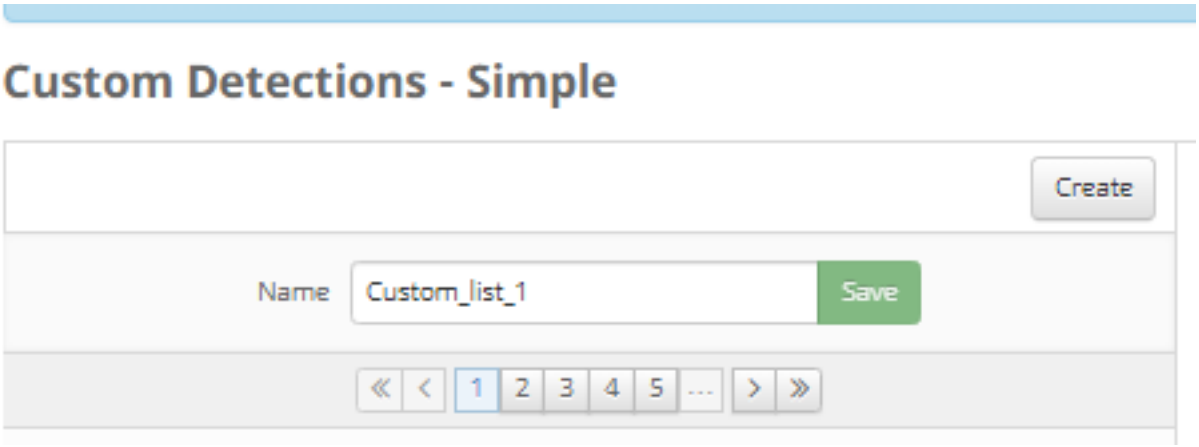
コンフィギュレーション

簡易カスタム検出リストを作成するには、次の手順を実行します。

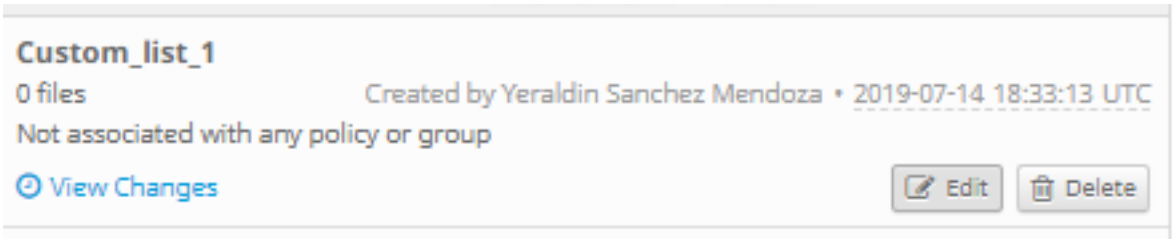
ステップ1：図に示すように、AMPポータルで[**Outbreak Control**] > [**Simple**]オプションに移動します。



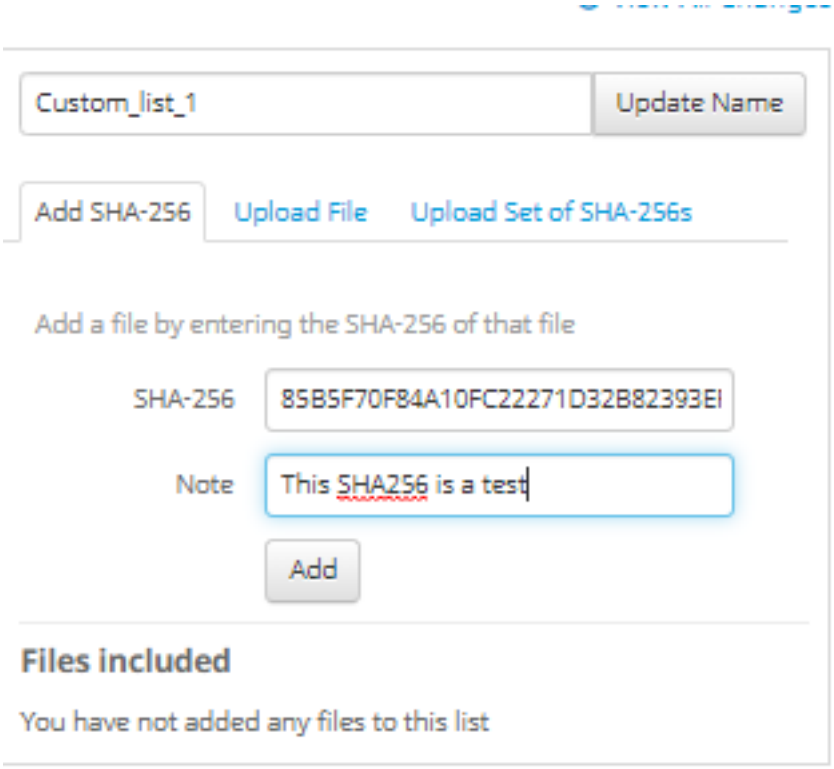
ステップ2:[Custom Detections - Simple]オプションで、[**Create**]ボタンをクリックして新しいリストを追加し、名前を選択して[Simple Custom Detection]リストを識別し、図に示すように保存します。



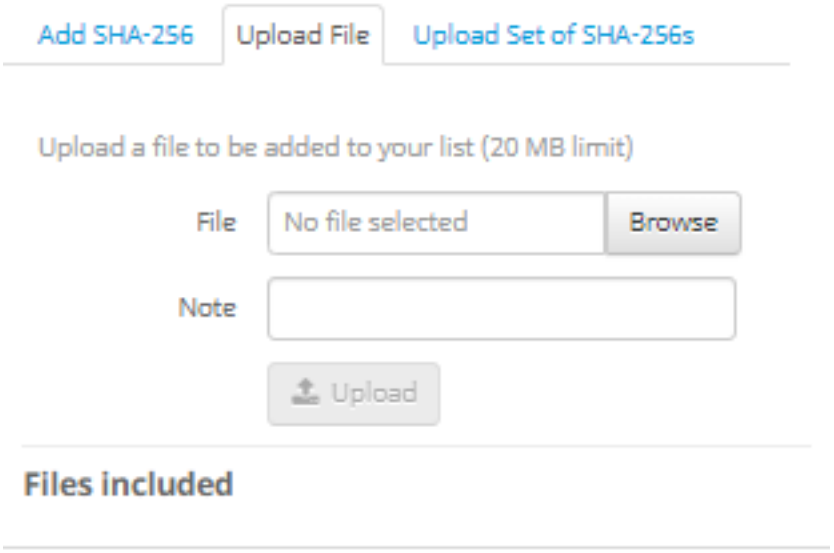
ステップ3：リストが作成されたら、[**Edit**]ボタンをクリックして、ブロックするファイルのリストを追加します（図を参照）。



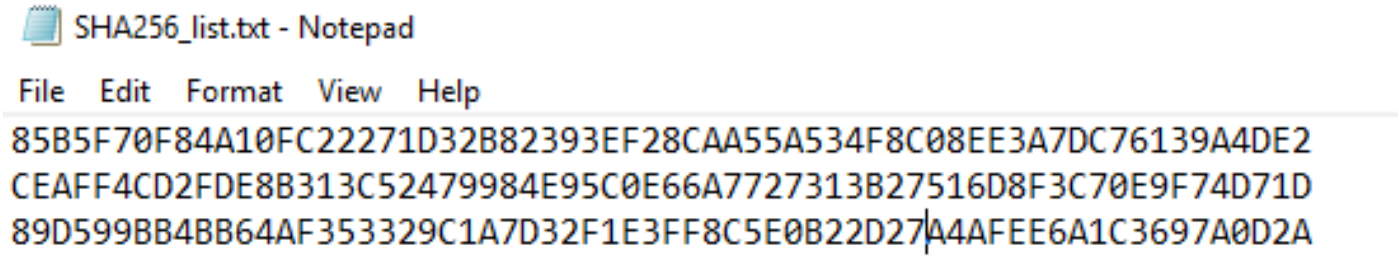
ステップ4:[Add SHA-256]オプションで、ブロックする特定のファイルから以前に収集したSHA-256コードを貼り付けます（図を参照）。

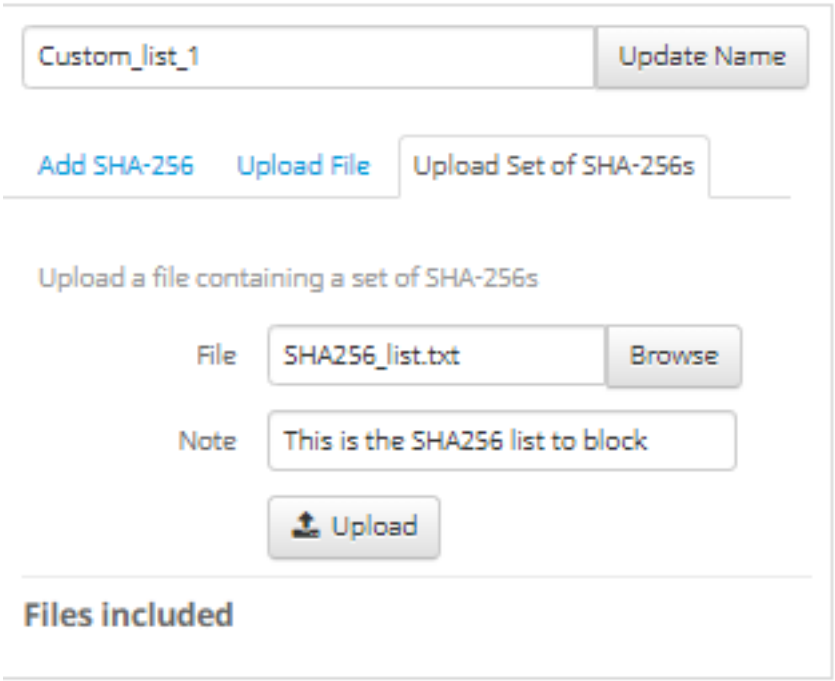


ステップ5:[Upload File]オプションで、ブロックする特定のファイルを参照します。ファイルがアップロードされると、このファイルのSHA-256がリストに追加されます（図を参照）。

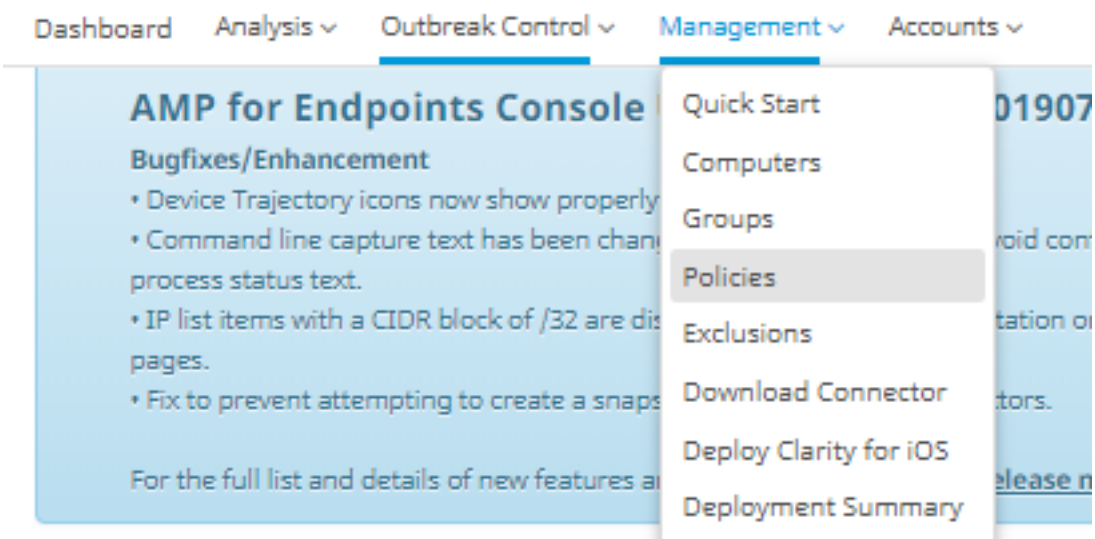


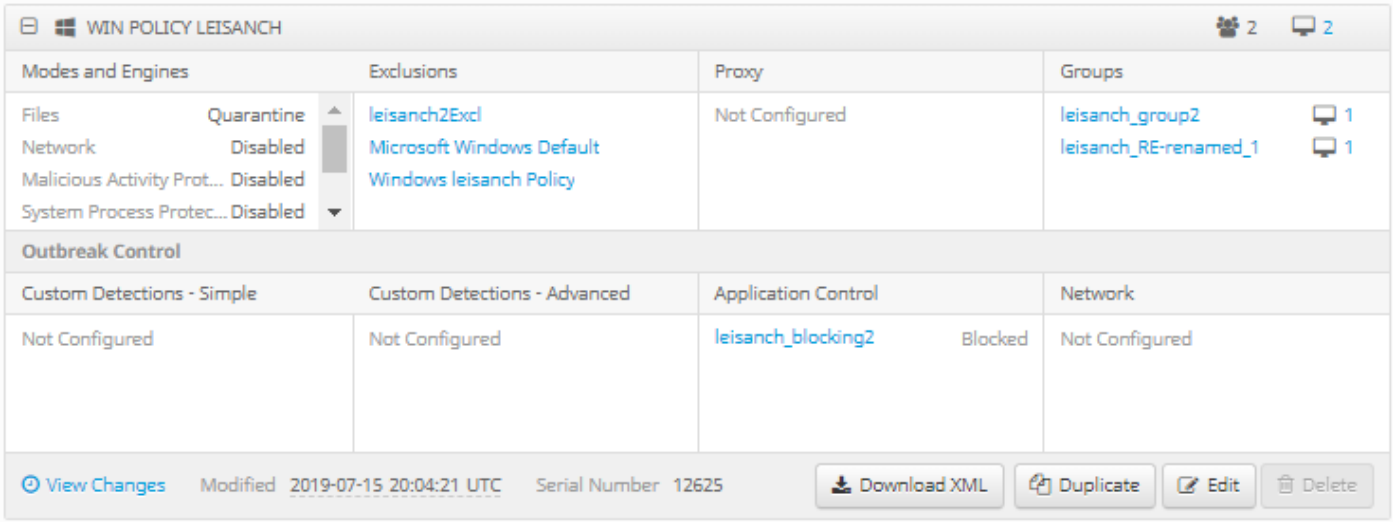
ステップ6:[Upload Set of SHA-256]オプションを使用すると、図に示すように、以前に取得した複数のSHA-256コードのリストを含むファイルを追加できます。



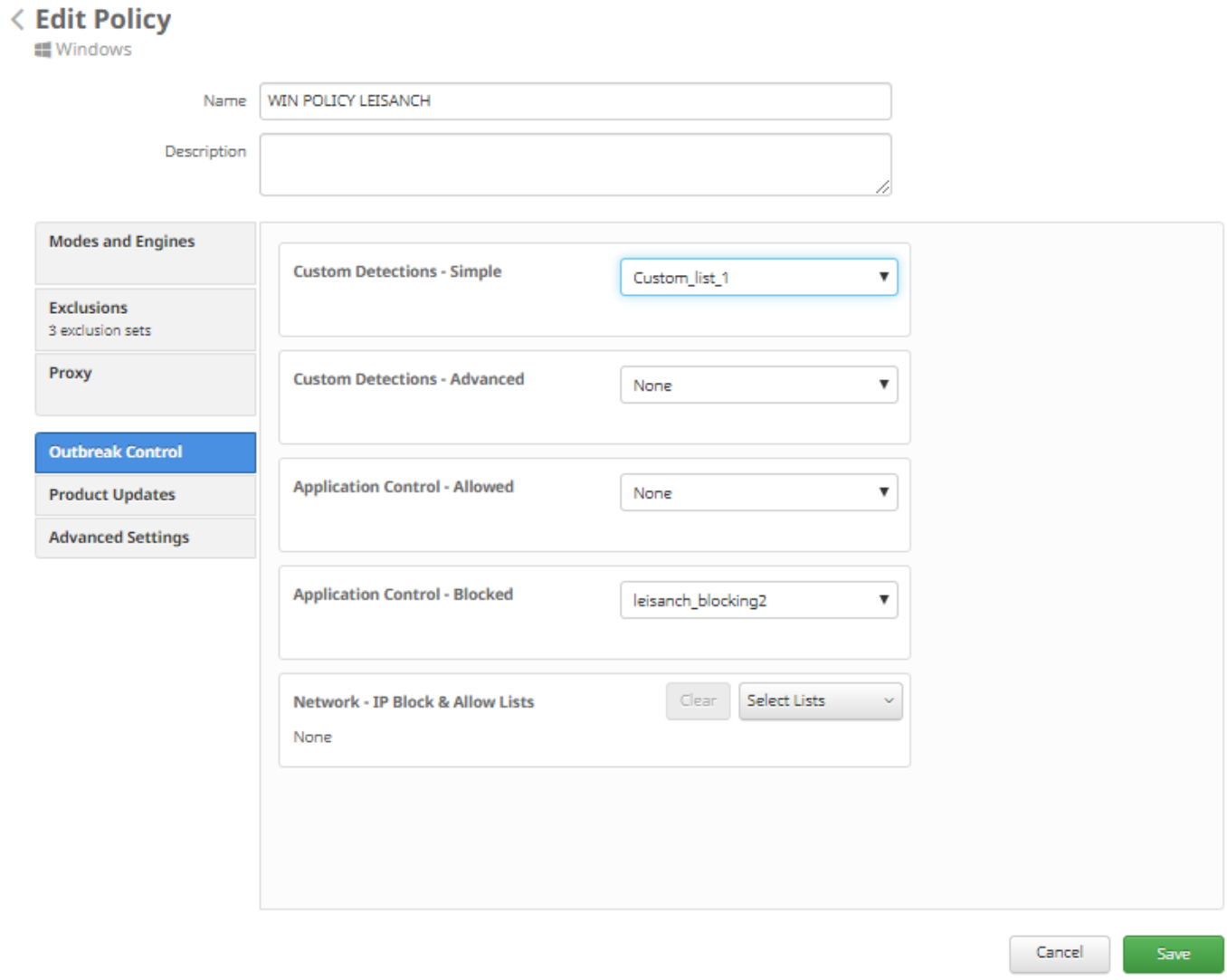


ステップ7:[Simple Custom Detection]リストが生成されたら、**[Management] > [Policies]に移動**し、図に示すように、以前に作成したリストを適用するポリシーを選択します。





ステップ8:[Edit]ボタンをクリックし、[Outbreak Control] > [Custom Detections - Simple]に移動し、ドロップダウンメニューで以前に生成したリストを選択して、変更を保存します（図を参照）。



すべての手順が実行され、コネクタが最後のポリシー変更に同期されると、簡易カスタム検出が有効になります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

警告：ファイルが簡易カスタム検出リストに追加された場合、検出が有効になるまでにキャッシュ時間が経過する必要があります。

注：簡易カスタム検出を追加すると、キャッシュされます。ファイルがキャッシュされる時間は、次のリストに示すように、その性質によって異なります。
- ファイルのクリーニング：7 日
- 不明なファイル：1 時間
- 悪意のあるファイル：1 時間