このサイトはAvast Business製品専用です。AVG Business製品に関する記事については、AVG Business ヘルプを参照してください。適切な場所にいても探している情報が見つからない場合は、 Avast Businessサポートに連絡してさらにサポートを受けてください。

ウイルス対策除外の設定

この記事は以下に適用されます:

- アバストビジネスハブ

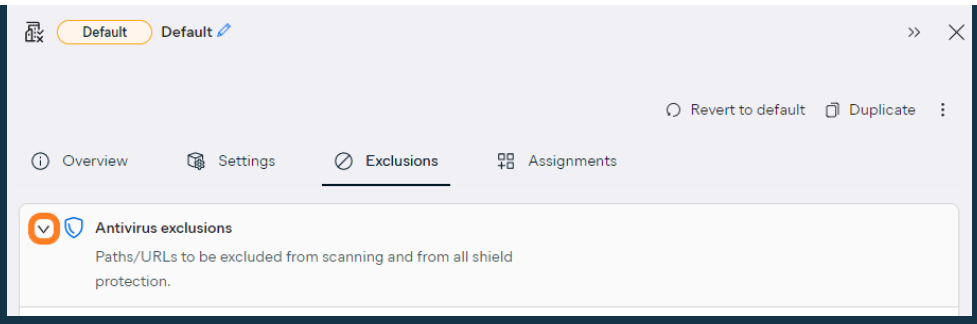
あなたのビジネスハブ ポリシーを使用すると、必要に応じて、指定したファイル、フォルダー、または Web サイトをウイルス対策によるスキャンから除外できます。標準およびコンポーネント固有の除外を構成すると、スキャンが高速化され、誤検出を防ぐことができます。

除外は、標準 (すべてのスキャンとシールド) とコンポーネント固有の (ファイル シールド、Web シールドなど) 除外の両方で約 8000 文字に制限されています。したがって、セキュリティ上の欠陥やシステム パフォーマンスへの影響を防ぐために、可能な限り除外を最小限に抑えることをお勧めします。

除外を設定する際にワイルドカードを使用できます。ただし、サンドボックス、行動シールド、および Web シールドでは、ワイルドカードの使用に関して一定の制限があります。詳細については、以下の各セクションを参照してください。

ウイルス対策除外の設定にアクセスするには:

1. ポリシーページを開く
2. 希望するポリシーをクリックして詳細ドロワーを開きます
3. **除外**タブをクリックします
4. **ウイルス対策除外**セクションを展開する



標準除外の設定

選択したポリシー内で、コンソールの*[除外]*タブにあるさまざまなウイルス対策シールドとコンポーネント全体に伝播する除外 (ローカル UI では例外と呼ばれます) を構成できます。

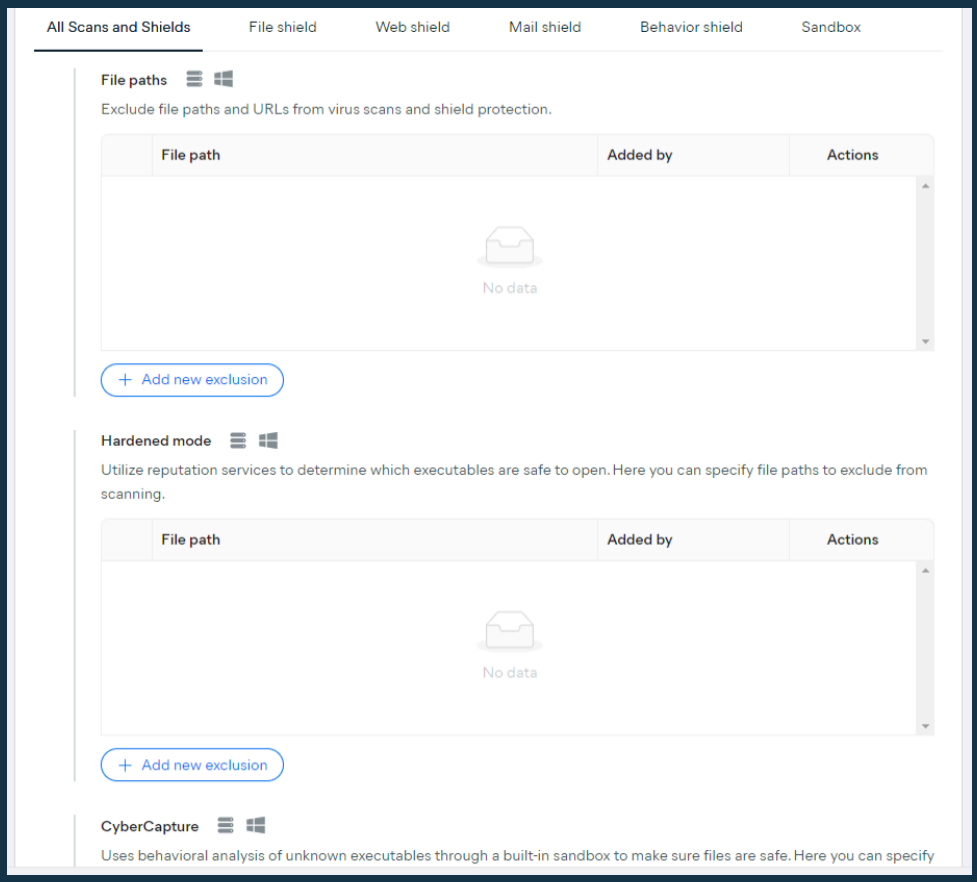
ポリシー内の除外に対する変更は、5 ～ 10 分ごとにネットワーク全体に伝播されます。

標準の除外は Windows ワークステーションとサーバーにのみ適用されます。

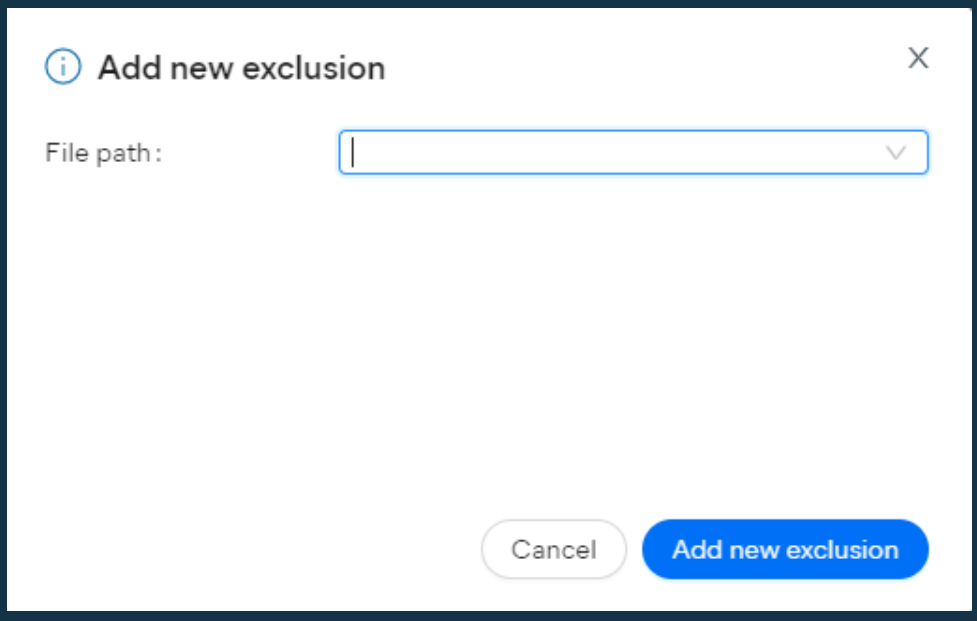
標準の除外、つまりすべてのスキャンとシールドに適用される除外を追加するには:

5. ポリシーの**除外**設定のウイルス対策除外セクションから、**すべてのスキャンとシールド**タブを選択します。
6. 目的のセクションで**「+ 新しい除外を追加」を**クリックします。
    - **ファイルパス**: 指定したファイルパスまたは URL をウイルススキャンおよびシールド保護から除外します
        - **完全なアプリケーション パスを含む除外は、Anti-Rootkit コンポーネントにも適用されます。**
    - **強化モード**: 指定された実行ファイルを強化モードのチェックから除外します
    - **CyberCapture** : 指定した実行ファイルを CyberCapture チェックから除外する
    - **URLアドレス**: 指定したURLアドレスをスキャンから除外します
        - **リアルサイトの除外 (Windows のみ)の場合は、*dns://domain.com/**形式を使用します。**
    - **オンデマンドスキャン**: エンドユーザーが開始したウイルススキャンから指定されたファイルパスを除外します

- **プログラム:**ウイルス対策チェックからプログラムまたはスクリプトへの指定されたパス (およびオプションのパラメータ) を除外します。



3. ポップアップダイアログで、除外するファイル/プログラムパスまたはURLを指定します。
4. **新しい除外を追加を**クリック



5. 除外の追加が完了したら変更を**保存します**

コンポーネント固有の除外の設定

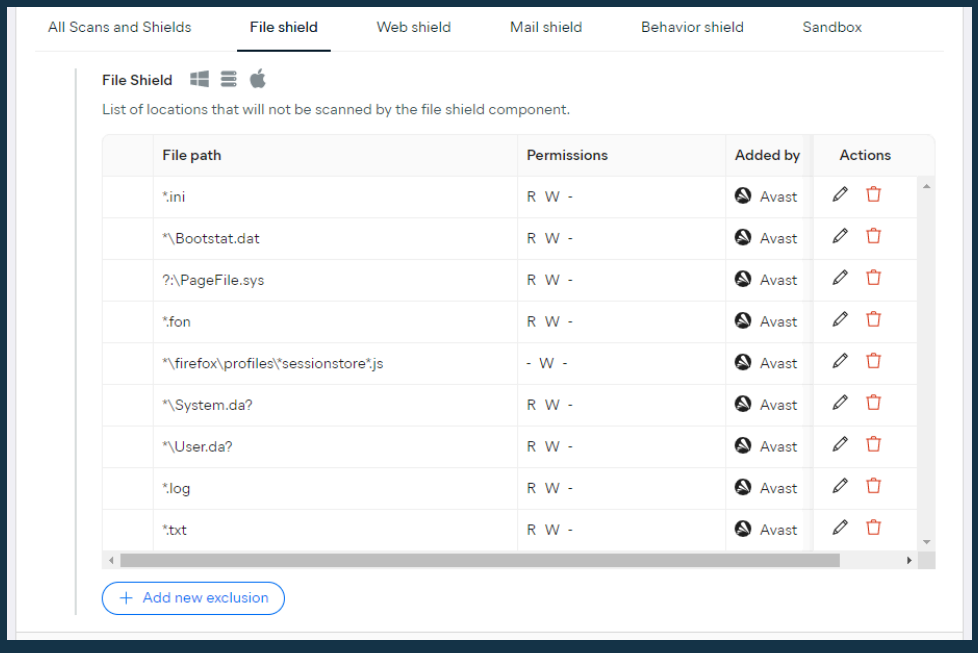
カスタマイズ可能なウイルス対策コンポーネントの多くには、特定のコンポーネントにのみ影響する除外を設定するための専用タブがあります。特定の除外を作成するプロセスは、ほとんどのシールドとコンポーネントで同様です。

ファイルシールドの除外

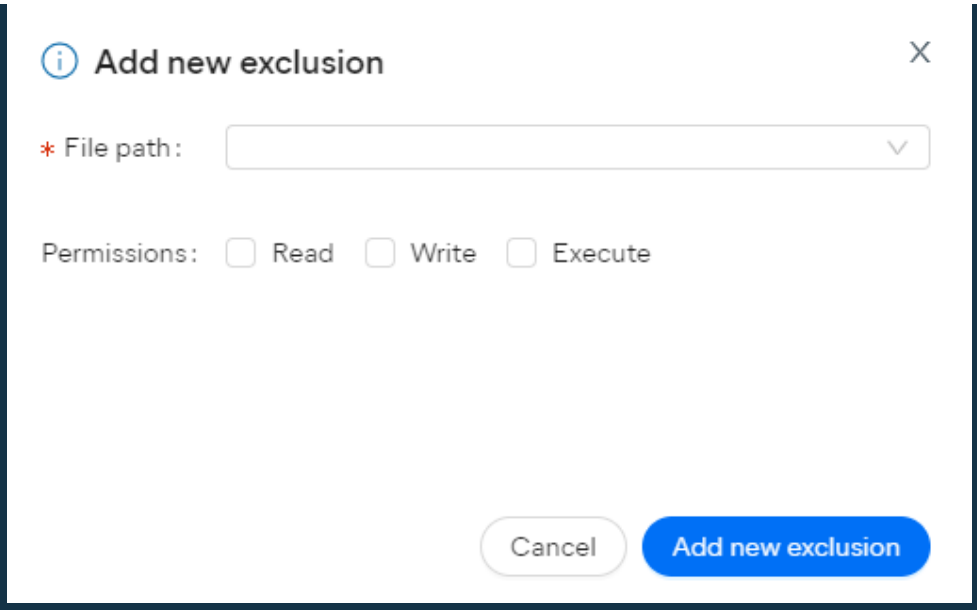
ここで指定された除外は、デバイス スキャン中にファイル シールドによってスキャンされません。これを使用すると、安全であることがわかっている場所のスキャンを高速化したり、誤検知を防止したりできます。

ファイル シールド スキャンに除外を追加するには:

1. ポリシーの**除外**設定のウイルス対策除外セクションから、**ファイルシールド**タブを選択します。



2. **+ 新しい除外を追加を**クリック
3. ポップアップダイアログで除外したいファイルパスを入力します
4. チェックボックスを使用して、除外が適用されるアクション（ファイルの読み取り、書き込み、実行）を指定します。
5. **新しい除外を追加を**クリック



6. 除外の追加が完了したら変更を**保存します**

ウェブシールドの除外

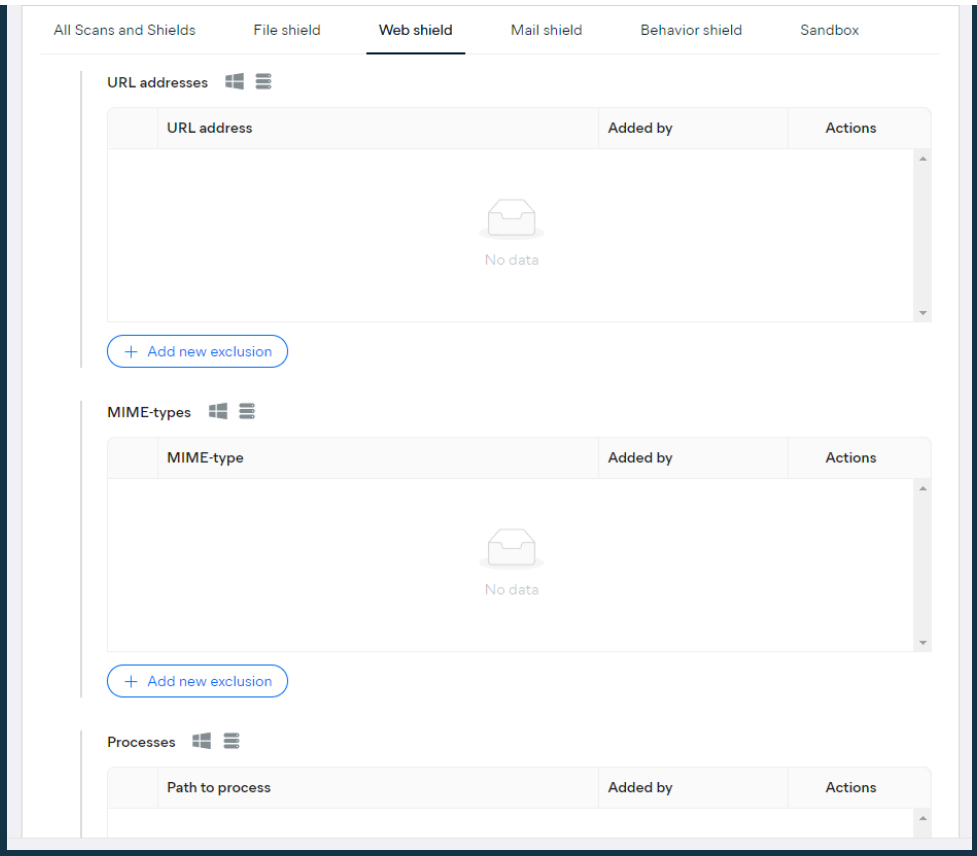
ここで指定された除外は、デバイスがインターネットにアクセスしているときに Web シールドによってスキャンされません。これは誤検知を防ぐために使用できます。

Web Shield のプロセス除外ではワイルドカード文字は使用できません。

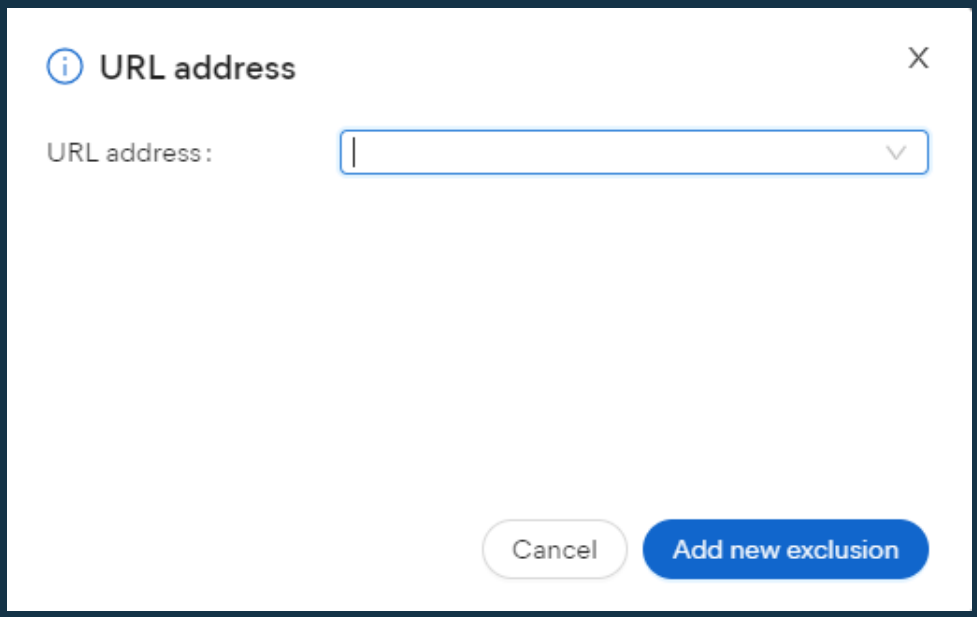
Web シールドの除外は、Windows ワークステーションとサーバーにのみ適用されます。

Web シールド スキャンに除外を追加するには:

1. ポリシーの**除外**設定のウイルス対策除外セクションから、**Webシールド**タブを選択します。
2. 目的のセクションで**「+ 新しい除外を追加」を**クリックします。
   - **URLアドレス**
   - **MIME タイプ**
   - **プロセス**（ワイルドカードは使用できません）
   - **スクリプト**
   - **Mac 除外リスト**



3. ポップアップダイアログで、除外の詳細（URLアドレス、MIMEタイプ、プロセスへのパス、またはホスト名、選択したセクションによって異なります）
4. **新しい除外を追加を**クリック



5. 除外の追加が完了したら変更を**保存します**

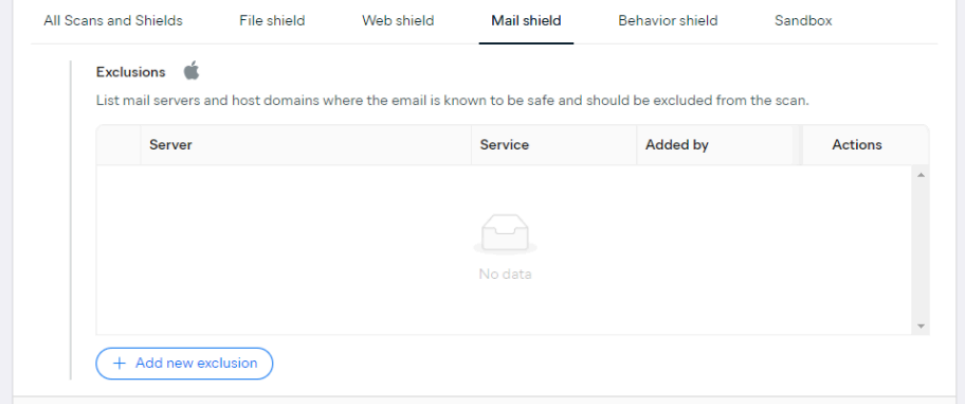
メールシールドの除外

ここで指定されたメール サーバーは、デバイスのスキャン中に Mail Shield によってスキャンされません。

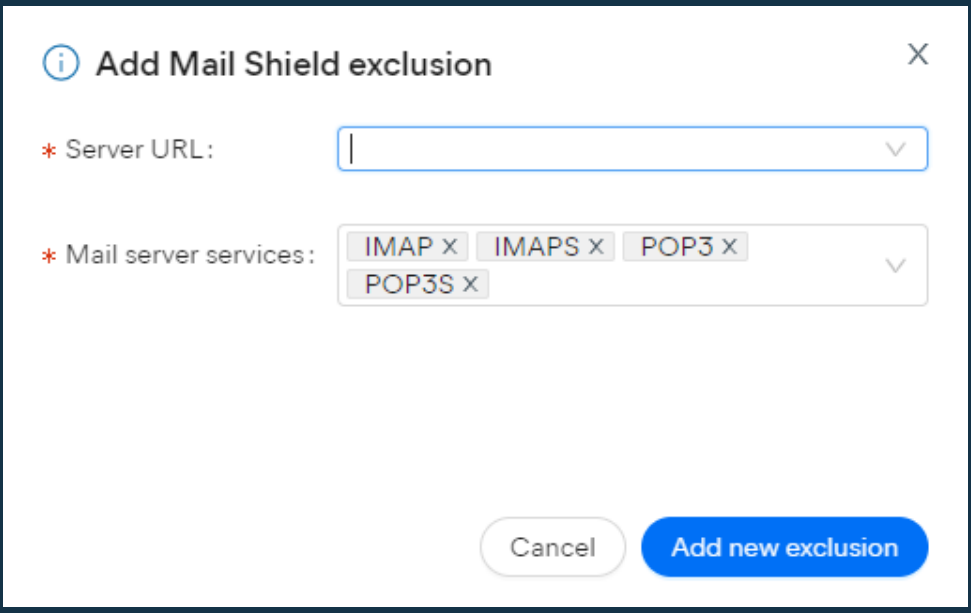
メール シールドの除外は macOS デバイスにのみ適用されます。

メール シールド スキャンに除外を追加するには:

1. ポリシーの**除外**設定のウイルス対策除外セクションから、**メールシールド**タブを選択します。
2. **+ 新しい除外を追加を**クリック



3. ポップアップダイアログで、除外するサーバーのURLとメールサーバーサービスを入力します。
4. **新しい除外を追加を**クリック



5. 除外の追加が完了したら変更を**保存します**

行動シールドの除外

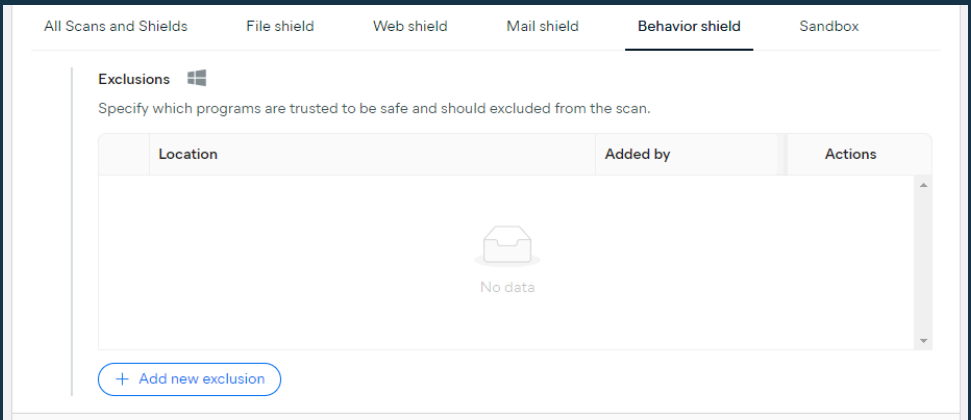
ここで指定された除外は、デバイスがプログラムやプロセスを実行しているときに、Behavior Shield によってスキャンされません。フォルダー/ファイルへの絶対パスを使用している限り、ネットワーク共有はサポートされます。

Behavior Shield では、ファイル パスの先頭または途中にワイルドカードを挿入することはできません (例: `C:¥users¥*¥application.exe`**)。ただし、パスの末尾にワイルドカードを使用することはできます (例:** `C:¥users¥username¥*`**)。**

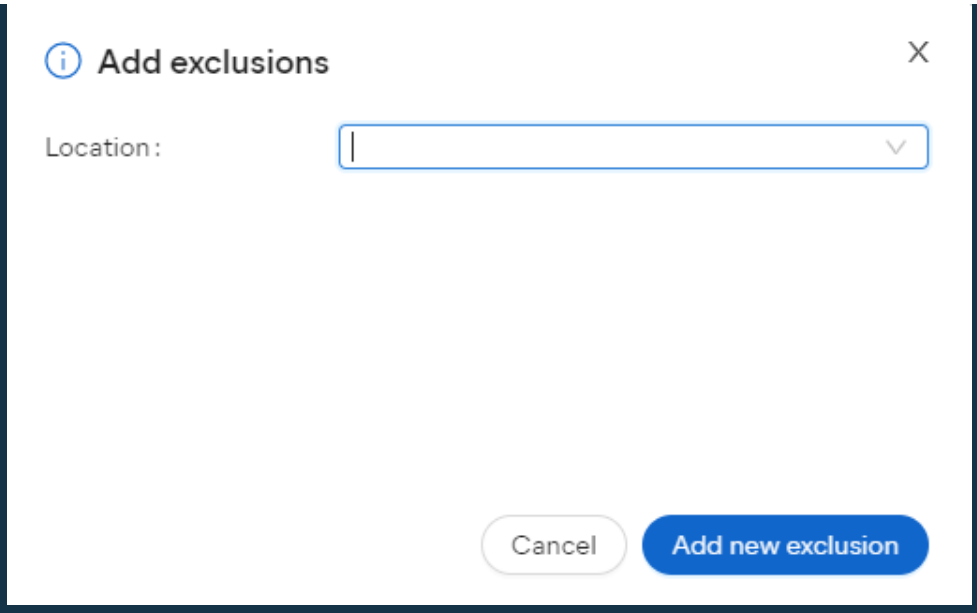
Behavior Shield の除外は Windows ワークステーションにのみ適用されます。

Behavior Shield スキャンに除外を追加するには:

1. ポリシーの**除外**設定のウイルス対策除外セクションから、**Behavior Shield**タブを選択します。
2. **+ 新しい除外を追加を**クリック



3. ポップアップダイアログで、除外したいプログラムの場所を入力します。
4. **新しい除外を追加を**クリック



5. 除外の追加が完了したら変更を**保存します**

サンドボックスの除外

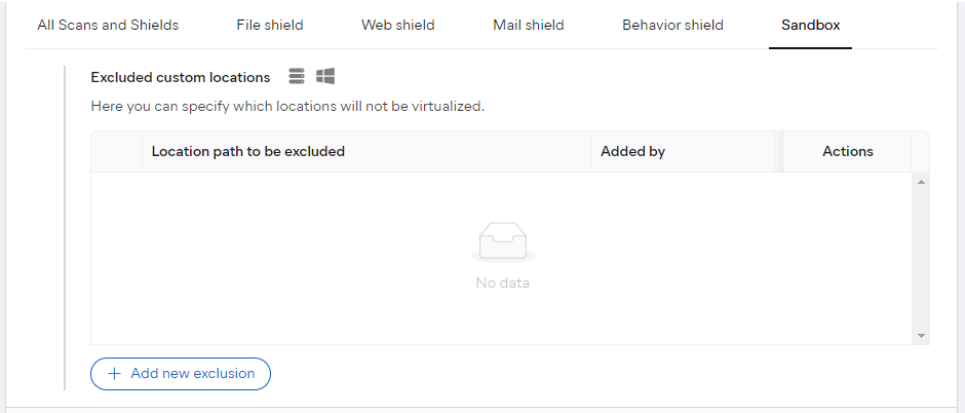
これらの除外は、サンドボックスを使用して感染の可能性があるファイルを仮想化する場合にのみ適用され、指定された場所が仮想化環境に持ち込まれないようにします。たとえば、仮想化環境のブラウザーからダウンロードしたファイルがブラウザーを閉じても削除されないように、ダウンロード フォルダーを除外できます。

サンドボックス除外パスではワイルドカード文字は受け入れられません。

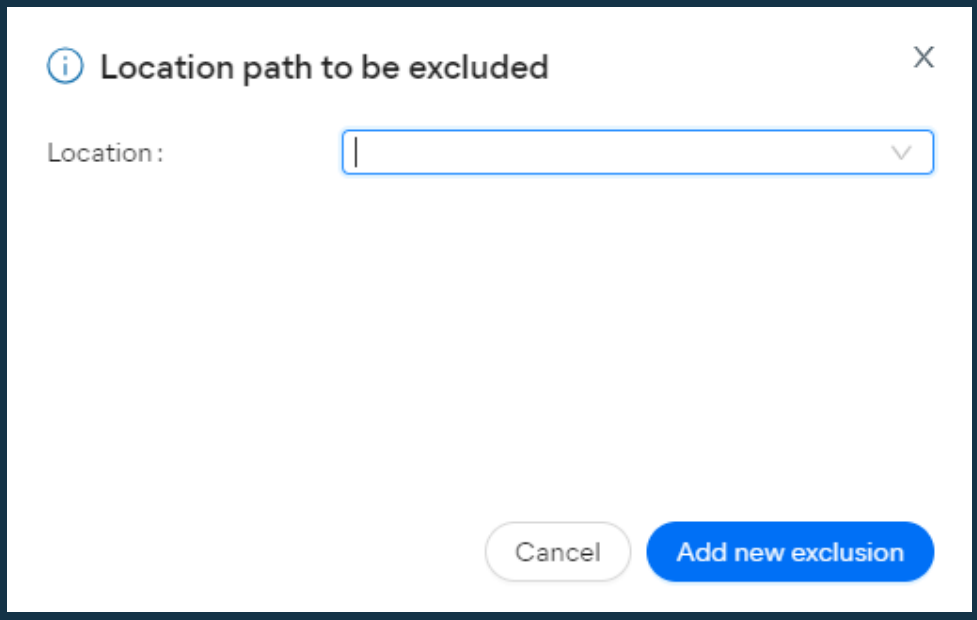
サンドボックスの除外は、Windows ワークステーションとサーバーにのみ適用されます。

標準の除外、つまりすべてのスキャンとシールドに適用される除外を追加するには:

1. ポリシーの**除外**設定のウイルス対策除外セクションから、**Sanbox**タブを選択します。
2. **+ 新しい除外を追加を**クリック



3. ポップアップダイアログで、仮想化から除外する場所を入力します。
4. **新しい除外を追加を**クリック



5. 除外の追加が完了したら変更を**保存します**

このセクションの他の記事:

- パッチ管理除外の設定
- クラウド バックアップの除外の設定
- USB保護除外の設定

関連記事：

- ワイルドカード
- ブロックされたパケットを記録して除外を作成する

現在の場所: ビジネス ハブ>設定とポリシーの構成>除外>ウイルス対策除外の構成