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:

- Avast Business オンプレミス コンソール

オンプレミス コンソール 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。

標準除外の設定

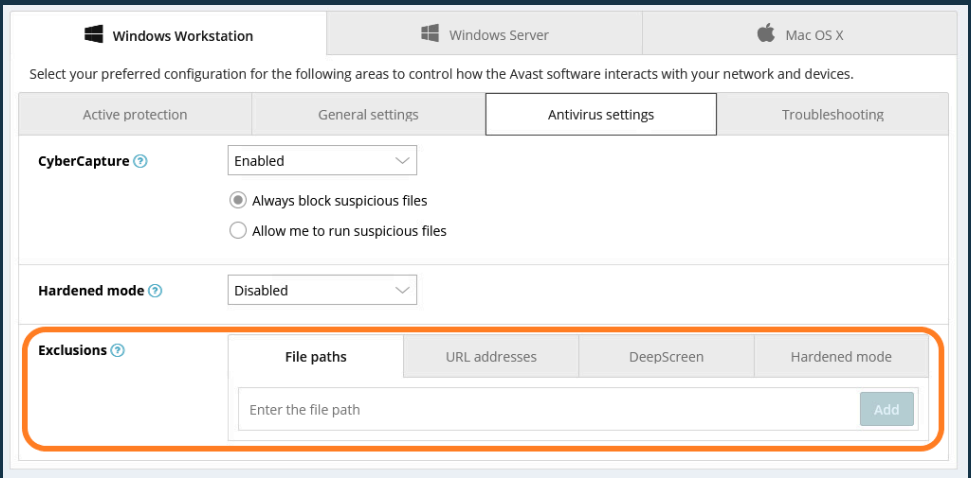
コンソールの*[*ウイルス対策設定*]*タブで、選択したポリシー内で、さまざまなウイルス対策シールドとコンポーネント全体に伝播する除外 (ローカル UI では例外と呼ばれます) を構成できます。

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:

1. ポリシーページに移動
2. 希望するポリシーを開く
3. **Windowsワークステーション**または**Windowsサーバー**を選択
4. **ウイルス対策設定**タブに移動します
5. *[*除外*]*セクションで、正しいタブが選択されていることを確認しながら、必要な除外を入力します。
   - **ファイルパス**: 指定したファイルパスをウイルススキャンとシールド保護から除外します
   - **URLアドレス**: 指定したURLをウイルススキャンとシールド保護から除外します
   - **DeepScreen** : 指定された実行ファイルを DeepScreen チェックから除外する
   - **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
6. エントリーの横にある**「追加」**をクリックします



追加されたすべての除外はここに表示され、必要に応じて編集または削除できます。

コンポーネント固有の除外の設定

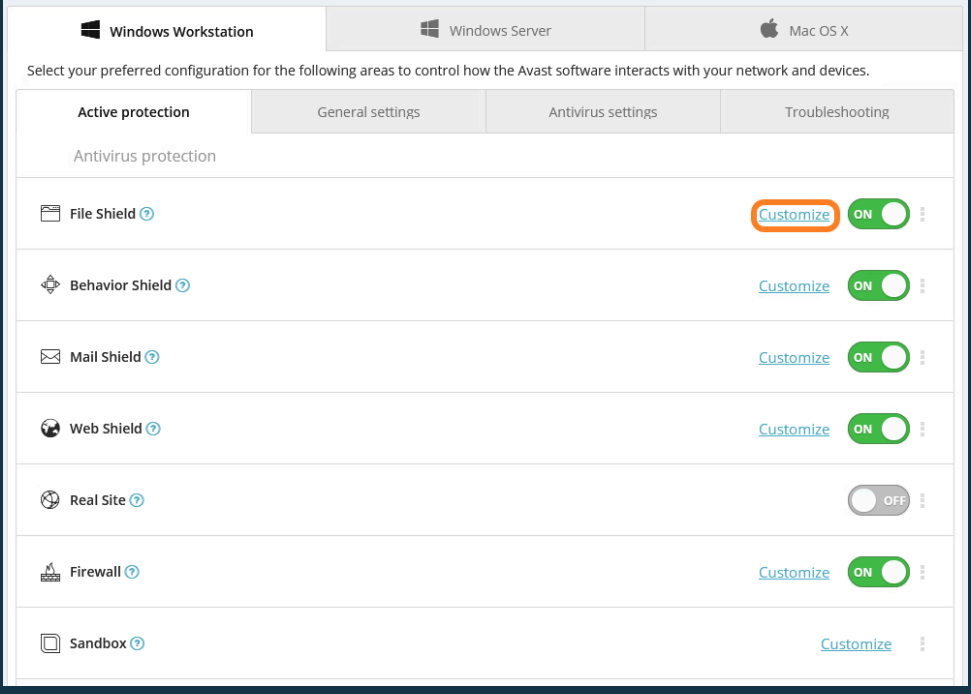
カスタマイズ可能なウイルス対策コンポーネントの多くには、特定のコンポーネントにのみ影響する除外を設定するための専用タブがあります。特定の除外を作成するプロセスは、ほとんどのシールドとコンポーネントで同様です。

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:

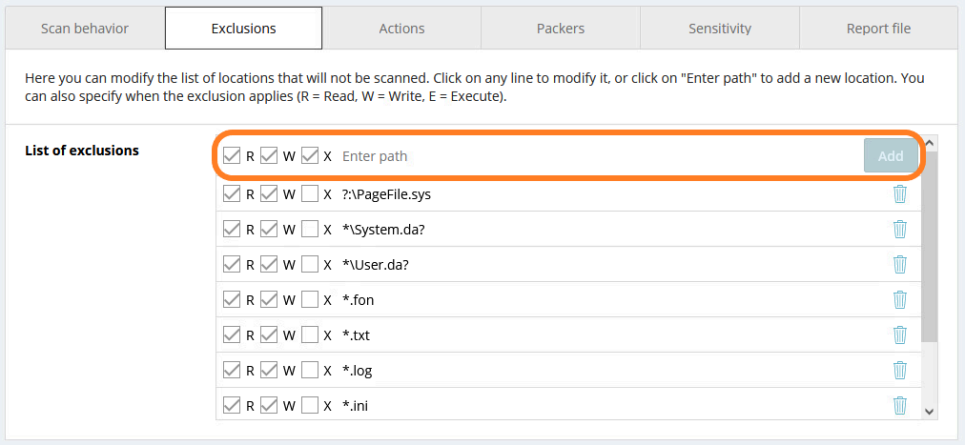
1. ポリシーページに移動
2. 希望するポリシーを開く
3. OSを選択
4. **アクティブ保護**タブに移動します
5. ファイルシールドの横にある**カスタマイズ**リンクをクリックします



6. **除外**タブを選択します
7. パスを入力フィールドで、除外したいファイルパスを指定します
8. 左側のチェックボックスを使用して、除外を適用するタイミング（ファイルが**読み取り**、**書き込み**、**実行されたとき**）を

指定します。

9. エントリーの横にある**「追加」**をクリックします



追加されたすべての除外はここに表示され、必要に応じて編集または削除できます。

行動シールドの除外

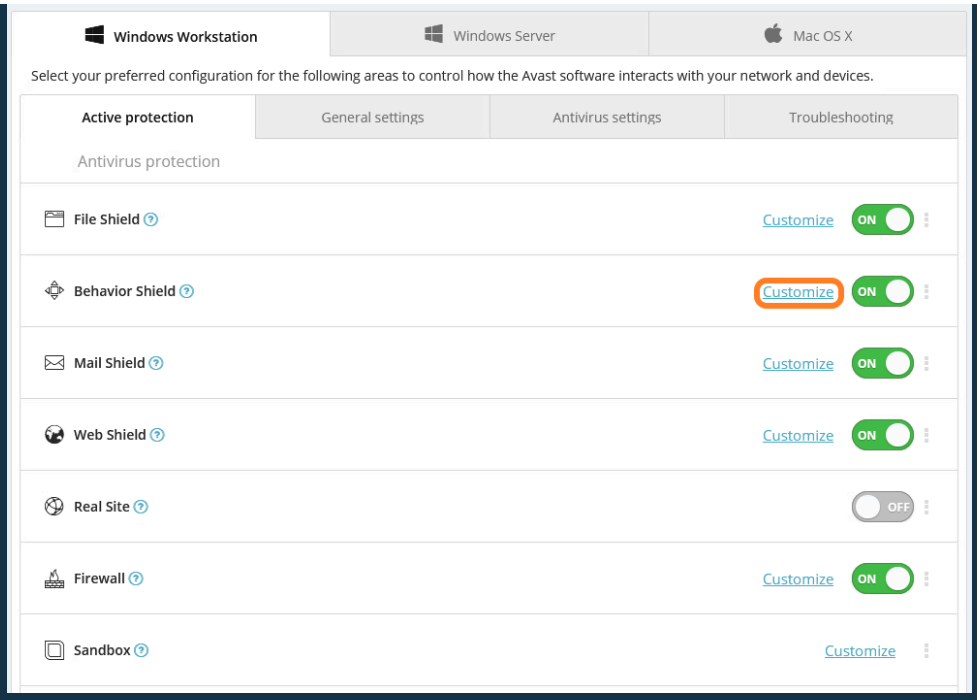
ここで指定された除外は、デバイスがプログラムやプロセスを実行しているときに、Behavior Shield によってスキャンされません。フォルダー/ファイルへの絶対パスを使用している限り、ネットワーク共有はサポートされます。

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¥*`**)。**

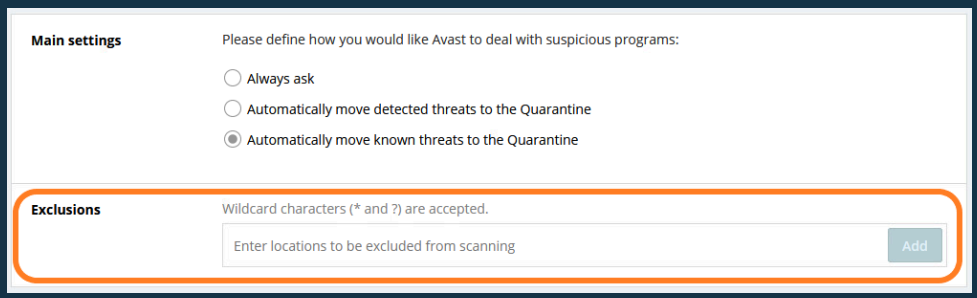
Behavior Shield の除外は Windows ワークステーションにのみ適用されます。

動作シールド スキャンに除外を追加するには:

1. ポリシーページに移動
2. 希望するポリシーを開く
3. **Windowsワークステーション**を選択
4. **アクティブ保護**タブに移動します
5. 行動シールドの横にある**カスタマイズ**リンクをクリックします



6. 除外セクションで除外したい場所を入力します
7. エントリーの横にある**「追加」**をクリックします



追加されたすべての除外はここに表示され、必要に応じて編集または削除できます。

メールシールドの除外

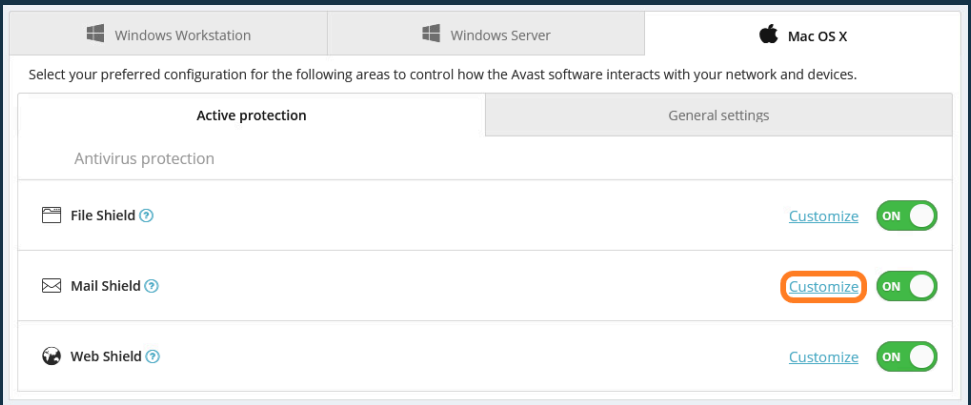
ここで指定されたメール サーバーは、デバイスのスキャン中に Mail Shield によってスキャンされません。

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。

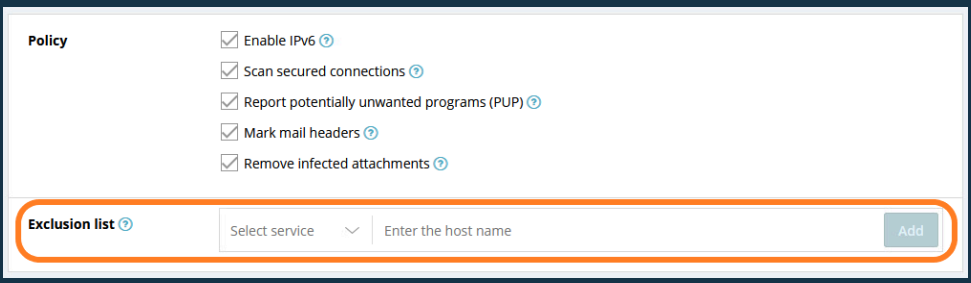
メール シールド スキャンに除外を追加するには:

1. ポリシーページに移動
2. 希望するポリシーを開く
3. **Mac OS X**を選択
4. **アクティブ保護**タブに移動します

5. メールシールドの横にある**カスタマイズ**リンクをクリックします



6. 除外リストセクションの上部にあるサービスの選択ドロップダウンメニューから、**imap**、**imaps**、**pop3**、**pop3s**プロトコルを選択します。
7. ホスト名を入力フィールドに除外するドメインを指定します
8. エントリーの横にある**「追加」**をクリックします



追加されたすべての除外はここに表示され、必要に応じて編集または削除できます。

ウェブシールドの除外

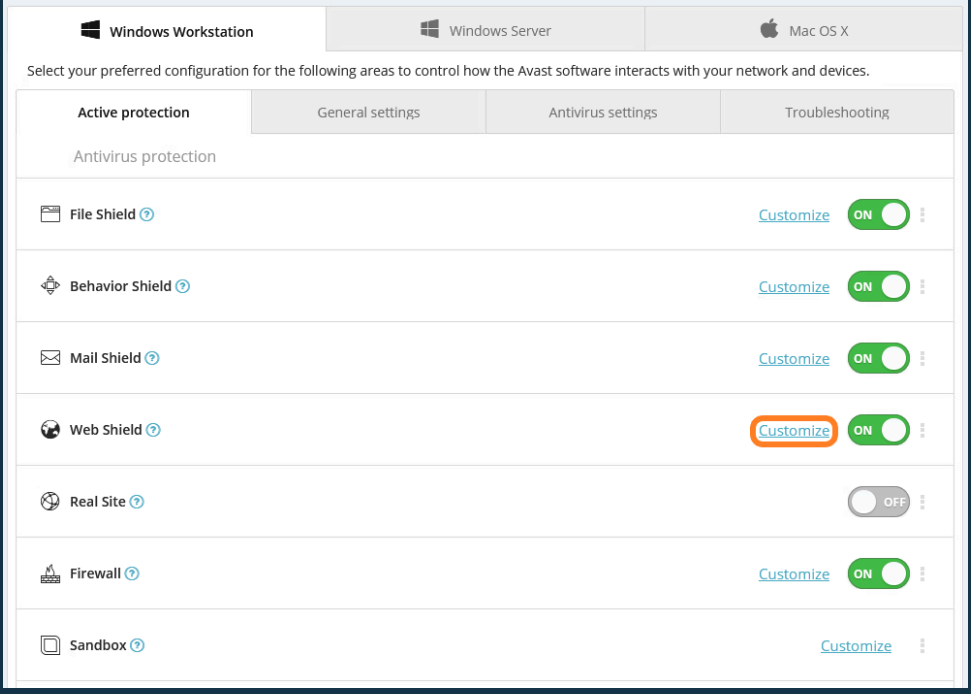
ここで指定された除外は、デバイスがインターネットにアクセスしているときに Web シールドによってスキャンされません。これは誤検知を防ぐために使用できます。

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。

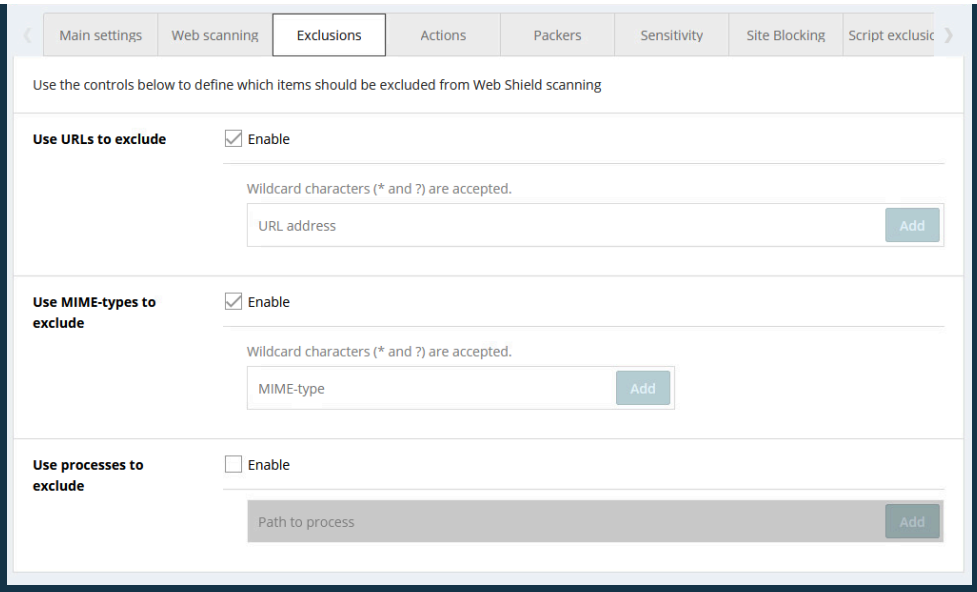
ウィンドウズ

Webシールドスキャンに除外を追加するにはWindowsデバイスで実行:

1. ポリシーページに移動
2. 希望するポリシーを開く
3. **Windowsワークステーション**または**Windowsサーバー**を選択
4. **アクティブ保護**タブに移動します
5. Webシールドの横にある**カスタマイズ**リンクをクリックします



6. **除外**タブを選択します
7. 作成する除外の種類に応じて、次のいずれかを実行します。
   - URLの場合は、**[有効]**チェックボックスがオンになっていることを確認し、除外するURLを*URL*アドレスフィールドに入力します。
   - MIMEタイプについては、**「有効」**チェックボックスがオンになっていることを確認し、除外するMIMEタイプを*MIME*タイプフィールドに入力します。
   - プロセスの場合は、**[有効]チェックボックスがオンになっていることを確認し、** *[プロセスへのパス]*フィールドにプロセス パスを入力します(ワイルドカードは使用できません)。
8. エントリーの横にある**「追加」**をクリックします

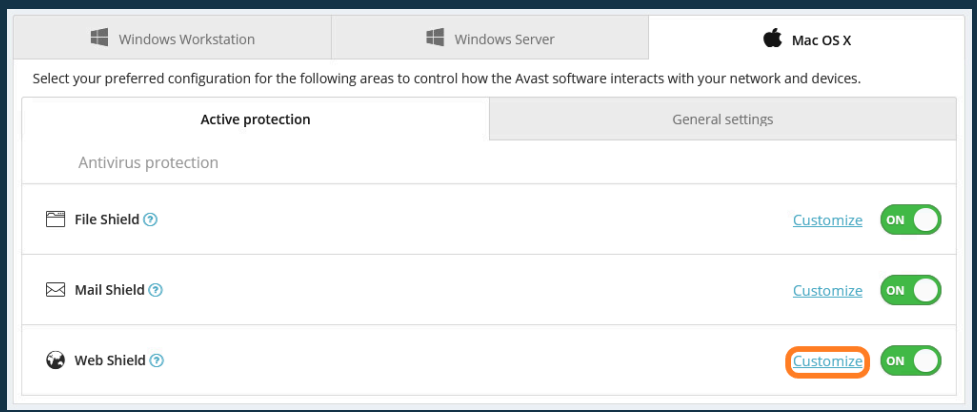


追加されたすべての除外はここに表示され、必要に応じて編集または削除できます。

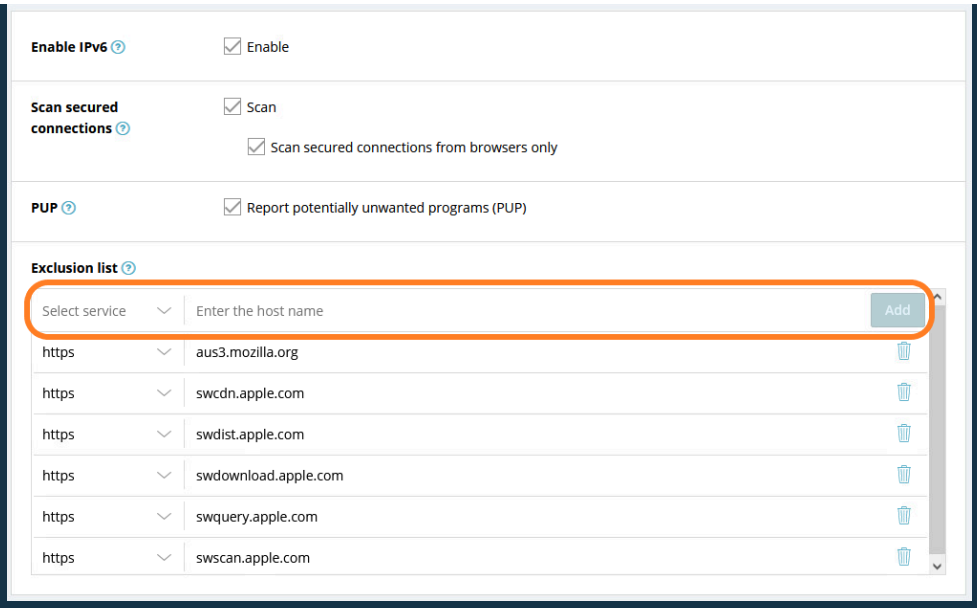
マックOS

macOS デバイスで実行される Web シールド スキャンに除外を追加するには:

1. ポリシーページに移動
2. 希望するポリシーを開く
3. **Mac OS X**を選択
4. **アクティブ保護**タブに移動します
5. Webシールドの横にある**カスタマイズ**リンクをクリックします



6. 除外リストセクションの上部にあるサービスの選択ドロップダウンメニューから、**http**と**https**プロトコルを選択します。
7. ホスト名を入力フィールドに除外するドメインを指定します
8. エントリーの横にある**「追加」**をクリックします



追加されたすべての除外はここに表示され、必要に応じて編集または削除できます。

サンドボックスの除外

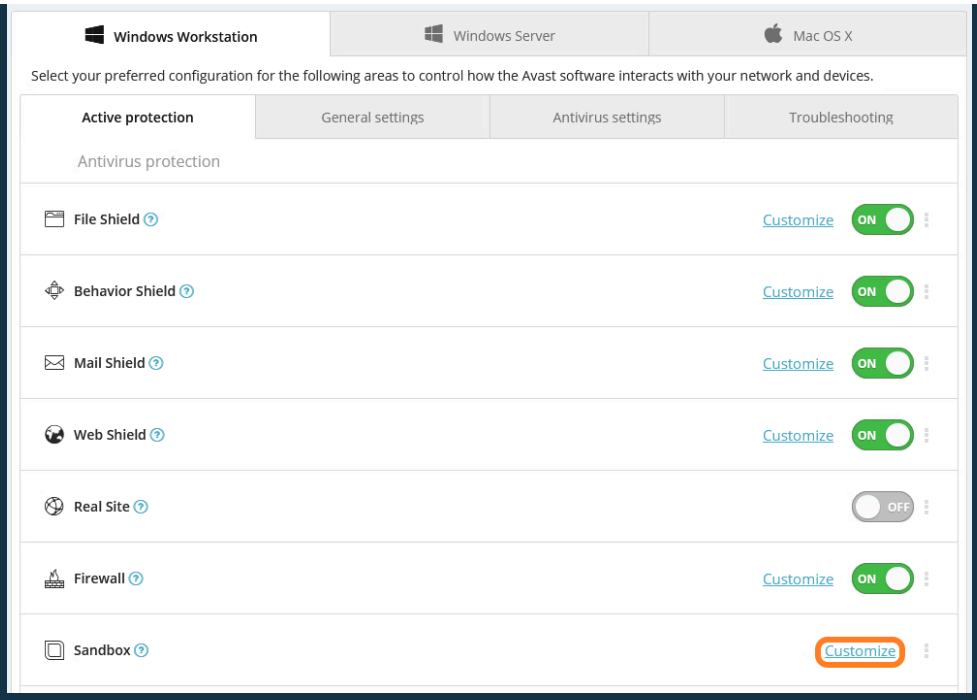
これらの除外は、サンドボックスを使用して感染の可能性があるファイルを仮想化する場合にのみ適用され、指定された場所が仮想化環境に持ち込まれないようにします。たとえば、仮想化環境のブラウザーからダウンロードしたファイルがブラウザーを閉じても削除されないように、ダウンロード フォルダーを除外できます。

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。

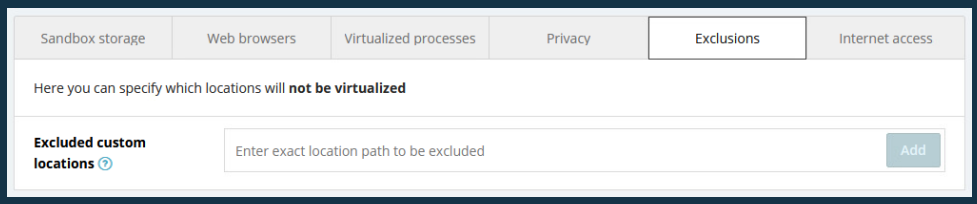
サンドボックスの除外は、Windows ワークステーションとサーバーにのみ適用されます。

サンドボックス除外を追加するには:

1. ポリシーページに移動
2. 希望するポリシーを開く
3. **Windowsワークステーション**または**Windowsサーバー**を選択
4. **アクティブ保護**タブに移動します
5. サンドボックスの横にある**カスタマイズ**リンクをクリックします。



6. **除外**タブを選択します
7. 除外する正確な場所のパスを入力フィールドに、除外したい場所を入力します。
8. エントリーの横にある**「追加」**をクリックします



追加されたすべての除外はここに表示され、必要に応じて編集または削除できます。

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: オンプレミス コンソール>設定とポリシーの構成>除外>ウイルス対策除外の構成