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:

- アバストビジネスクラウドケア

重要: CloudCareコンソールは、同じブラウザ セッションで複数のタブを開くことをサポートしていません。代わりに、複数のブラウザまたはシークレット モードを使用してください。

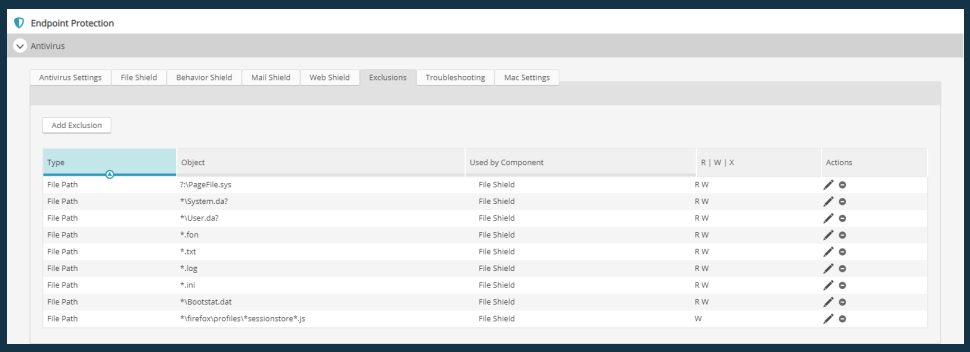
あなたのクラウドケアコンソール ポリシーを使用すると、必要に応じて、指定したファイル、フォルダー、または Web サイトをウイルス対策によるスキャンから除外できます。標準およびコンポーネント固有の除外を構成すると、スキャンが高速化され、誤検出を防ぐことができます。

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。

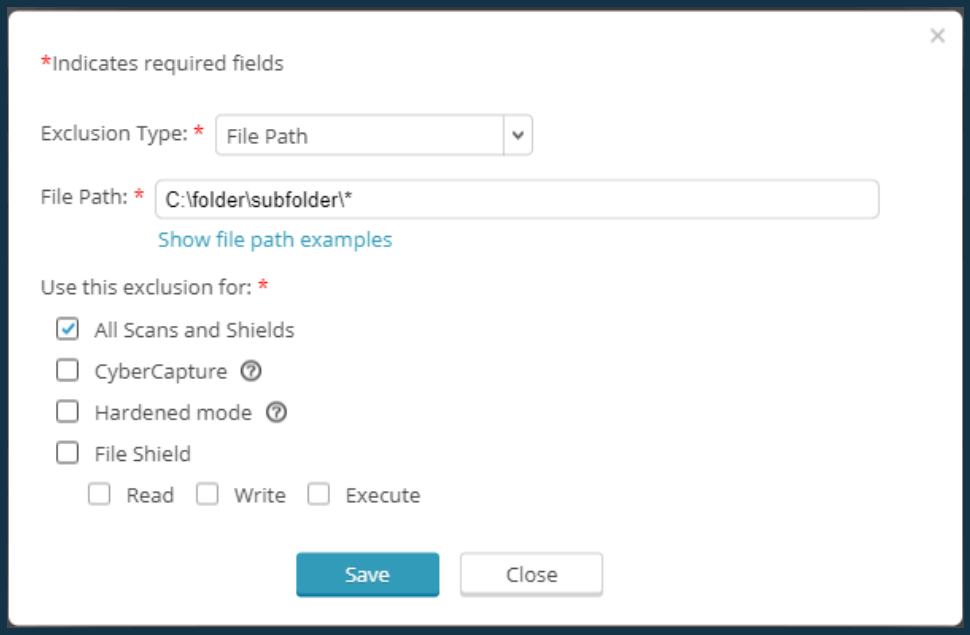
除外を設定する際にワイルドカードを使用できます。ただし、サンドボックス、行動シールド、および Web シールドでは、ワイルドカードの使用に関して一定の制限があります。詳細については、以下の各セクションを参照してください。

標準除外の設定

ポリシーのウイルス対策セクションで、CloudCare ウイルス対策のさまざまなシールドとコンポーネント全体に伝播する除外を設定できます。



ポリシー内の除外に対する変更は、およそ 5 ～ 10 分ごとにネットワーク全体に伝播されます。コンソールポリシーはローカル設定を上書きします。



1. パートナーの場合、1人の顧客のみを除外設定したい場合は、顧客ドロップダウンメニューで顧客を選択します。
2. ポリシータブに移動します
3. 除外を追加したいポリシーをクリックします
4. ウイルス対策セクションを展開し、**除外**タブをクリックします。
5. **[除外を追加] を**クリックし、除外タイプを選択します。
    - **ファイルパス:**除外したいファイルパスを入力してください

- **URL:**除外したいURLを入力してください

6. すべてのスキャンとシールドをチェックし、**「保存」をクリックします**
7. 完了したら**「保存してデバイスに適用」を**クリックします。
    - **マスターポリシーを編集している場合、このオプションは「保存して顧客に適用」と表示されます。**

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。

1. パートナーの場合、1人の顧客のみを除外設定したい場合は、顧客ドロップダウンメニューで顧客を選択します。
2. ポリシータブに移動します
3. 除外を追加したいポリシーをクリックします
4. ウイルス対策セクションを展開し、**除外**タブをクリックします。
5. **除外の追加を**クリックし、**ファイルパスを選択します。**
6. 除外したいファイルパスを入力してください
7. ファイルシールドをチェックし、**保存をクリックします**
    - **ファイルシールドの下にあるチェックボックスを使用して、ファイルの読み取り、書き込み、または実行時に除外を適用するかどうかを選択することもできます。**

8. 完了したら**「保存してデバイスに適用」を**クリックします。
    - **マスターポリシーを編集している場合、このオプションは「保存して顧客に適用」と表示されます。**

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。特定の URL をブロックする場合は、*[サイト ブロック]*タブで入力する必要があることに注意してください。

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

1. パートナーの場合、1人の顧客のみを除外設定したい場合は、顧客ドロップダウンメニューで顧客を選択します。
2. ポリシータブに移動します
3. 除外を追加したいポリシーをクリックします
4. ウイルス対策セクションを展開し、**除外**タブをクリックします。
5. **[除外を追加] を**クリックし、次のいずれかを選択します。
    - **URL:**除外したいURLを入力してください
    - **MIMEタイプ:**除外したいMIMEタイプを入力してください
    - **プロセス:**除外するプロセス パスを入力します (ワイルドカードは使用できません)
6. *Web*シールドをチェックし、**「保存」をクリックします**
7. 完了したら**「保存してデバイスに適用」を**クリックします。
    - **マスターポリシーを編集している場合、このオプションは「保存して顧客に適用」と表示されます。**

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。

Behavior Shield 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をサポートしていません (例: `C:¥users¥*¥application.exe`)。ただし、ファイル 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¥*`)。

1. パートナーの場合、1人の顧客のみを除外設定したい場合は、顧客ドロップダウンメニューで顧客を選択します。
2. ポリシータブに移動します
3. 除外を追加したいポリシーをクリックします
4. ウイルス対策セクションを展開し、**Behavior Shield**タブをクリックします。
5. スキャンから除外したい場所を入力してください
6. **追加を**クリック
7. 完了したら**「保存してデバイスに適用」を**クリックします。
    - **マスターポリシーを編集している場合、このオプションは「保存して顧客に適用」と表示されます。**

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。

1. パートナーの場合、1人の顧客のみを除外設定したい場合は、顧客ドロップダウンメニューで顧客を選択します。
2. ポリシータブに移動します
3. 除外を追加したいポリシーをクリックします
4. ファイアウォールとウイルス対策アドオンセクションを展開し、**サンドボックス**タブをクリックします。
5. **除外**タブをクリックします

6. 仮想化から除外したい場所を入力してください
7. **追加を**クリック
8. 完了したら**「保存してデバイスに適用」を**クリックします。
    - **マスターポリシーを編集している場合、このオプションは「保存して顧客に適用」と表示されます。**

関連記事：

- スキャンのスケジュール設定
- ファイルシールド
- ウイルスチェスト
- ワイルドカード

現在の場所: *CloudCare* >ポリシーの設定>除外>ウイルス対策除外の設定