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。

ファイアウォールの要件

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

全体的な機能とウイルス対策クライアントを有効にするにはおよび/または管理コンソール認証/更新を行うには、エンドポイントのファイアウォールまたはプロキシ サーバーを介して特定のポートと URL アドレスを許可する必要があります。

ポート

- UDP 53 DoH 有効 – セキュア DNS サービス (リアルサイトを使用している場合)
- TCP 80 – インターネットの脆弱性チェックと機能更新
- TCP/UDP 443 * – 暗号化通信
- TCP 8080 *、8090 * –オンプレミス コンソールとローカル ネットワーク内のクライアント間の通信
- TCP 4158 – ミラー、ローカルネットワーク内のローカル更新用
- TCP 7074 – ローカルネットワーク内のリモート展開
- TCP 7500 - プッシュ通知サービス用

***これらのデフォルト ポートは、必要に応じてオンプレミス コンソールのセットアップ中またはセットアップ後に変更できます。変更はファイアウォール構成に反映される必要があることに注意してください。**

URL

- *.avast.com
- *.avcdn.net

ジオブロッキング

Avastウェブ サービスは世界中の多くの国でホストされています。そのため、ファイアウォール設定でジオブロックすることはお勧めしません。ジオブロックが必要な場合は、ジオブロックよりも優先される URL許可ルールを設定し、Avast トラフィックを許可することをお勧めします。

このセクションの他の記事:

システム要求

リムーバブルウイルス対策製品

関連記事：

オンプレミスコンソールへのデバイスの追加

マネージドアンチウイルスのインストール

現在の場所: オンプレミス コンソール>デバイス管理>一般情報>ファイアウォールの要件