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:

- アバストビジネスクラウドケア

全体的な機能性と、ウイルス対策クライアントの認証/更新を有効にするには、エンドポイント上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

- TCP 80 - インターネットの脆弱性チェックと機能更新
- TCP 443 - ポータルとインストールされたクライアント間の基本的な通信
- UDP 123 - コンテンツフィルタリングスケジュール設定の改ざんを防ぐためにパブリックタイムサーバーにアクセスする
- TCP/UDP 135 - リモート展開
- TCP/UDP 5222 - XMPP通信

URL

- *.avast.com
- *.avg.com

- *.avcdn.net
- *.m.in-app.io
- islonline.net (プレミアム リモート コントロールを使用している場合)
- *.sosonlinebackup.com (クラウド バックアップを使用している場合)
- *.managedoffsitebackup.net (クラウド バックアップを使用している場合)
- アプリケーション ベンダーが必要とする URL (パッチ管理を使用している場合、必要なパッチはベンダーから直接ダウンロードされるため、サービスが正しく動作するには接続を許可する必要があります)

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:

CloudCare システム要件

関連記事：

CloudCare へのデバイスの追加

デバイスのクローン作成

現在のページ: *CloudCare* >デバイス管理>要件>ファイアウォールの要件