

Secure Access RAVPN認証がDuo SAML統合で失敗した

内容

お問い合わせ内容

Active Directoryがバックグラウンドで統合されたIDプロバイダー(IDP)としてDuoを使用して、Cisco Secure Access Remote Access VPN(RAVPN)への接続を試みると、Duoポータルレベルで認証に成功したにもかかわらず、ユーザに認証エラーが発生します。

具体的な症状は次のとおりです。

- Duoポータルに、認証の成功メッセージが表示されます。
- Cisco SecureClientは、Duoが成功した直後に「Authentication failed」エラーメッセージを表示します。
- Duoログに「access granted」ステータスが表示されます。
- Cisco Secure Accessポータルログに「AAA failure」のステータスが表示されます。

これにより、外部IDプロバイダーは認証の成功を確認するが、Secure Accessインフラストラクチャ内での認証の検証エラーが原因でVPNクライアントが接続を確立できないという接続解除が発生します。

環境

- Cisco Secure Access RAVPNの導入
- SAML IDプロバイダーとしてのDuo Security
- DuoとのActive Directory統合
- VPN接続用Cisco SecureClient

- SAMLベースの認証フロー

解決策

認証の失敗は、DuoとCisco Secure Access間のユーザ属性マッピングを修正することで解決されました。次のセクションで説明する手順は、問題を特定して解決するために実行されました。

ステップ1：アクティビティ検索の確認

- 1.- Cisco Secure Access Dashboardにログインします。Monitor> Remote Access Logsの順にクリックします。
- 2.- authorization check failureメッセージのusernameフィールドをチェックします。
- 3.- Connect > User and Groupsの下にUPN値と照合します。

Cisco Secure Accessは、ユーザプリンシパル名(UPN)の値を検証して認証をチェックします。

Duoから渡されたユーザプリンシパル名(UPN)が、ユーザとグループの下にあるそのユーザのユーザプリンシパル名(UPN)の値と一致していませんでした。

調査の結果：

- ユーザの電子メールアドレス：user@gmail.com
- ユーザープリンシパル名(UPNユーザー名

ステップ2:Duo構成の調整

この問題を解決するには、Duo SAML構成を変更して、ユーザ属性のマッピングが適切であることを確認する必要がありました。

- Duo Admin Panelにアクセスします。

- Cisco Secure AccessのSAMLアプリケーション設定に移動します。
- ユーザ属性マッピングを変更して、電子メールアドレスを送信します。電子メールアドレスは、[ユーザとグループ]のそのユーザの[ユーザプリンシパル名]の値と一致する必要があります。
- 設定の変更を保存します。

ステップ4：検証

Duo設定を調整した後、認証フローがテストされ、正常に検証されました。ユーザはリモートアクセスVPNを使用して、認証に失敗することなく接続できました。

原因

認証失敗の根本原因は、Duo SAMLアサーションとCisco Secure Accessの期待との間でユーザ属性マッピングが一致していなかったことにあります。Duoは、SAMLアサーションでユーザプリンシパル名(UPN)でユーザ名を送信するように設定されていますが、Cisco Secure Accessはユーザの電子メールアドレスを想定するように設定されています。この不一致により、Duo IDPレベルでの認証が成功したにもかかわらず、Secure Accessレベルで認証が失敗し、Duoログには「access granted」と表示される一方、Secure Accessに「AAA failure」が記録されました。

関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。