

# 認証を有効にすると、トランスペアレント モードの WSA 経由で TeamViewer が動作しない

## 目次

[質問](#)

[環境](#)

[症状](#)

[ステップ 1: カスタム URL カテゴリの作成](#)

[ステップ 2: 新しいアイデンティティの追加](#)

[ステップ 3: アクセス ポリシーへの新しいアイデンティティの追加](#)

[既存のアクセス ポリシーの使用に関する回避策](#)

[新しいアクセス ポリシーの使用に関する回避策](#)

## 質問

Cisco Web セキュリティ アプライアンス ( WSA ) で認証が有効な場合に TeamViewer Agent が機能しないのはなぜですか

## 環境

Cisco Web セキュリティ アプライアンス ( WSA ) 、すべての AsyncOS バージョン。

## 症状

TeamViewer Agent がタイムアウトし、「Proxy Authentication Required」を示す 401 または 407 エラーを含むエントリがアクセス ログに示されます。

TeamViewer Agent が認証を処理しません。つまり、WSA が TeamViewer アプリケーションからの認証を要求すると、このアプリケーションはドメイン クレデンシャルを提供しません。したがって、認証からこれを除外する必要があります。

WSA がアイデンティティでサロゲートとして Cookie を使用するよう設定されている場合 ( [GUI] > [Web Security Manager] > [Identities] ) 、認証免除が必要です。

アイデンティティが IP アドレス サロゲートに設定されている場合、次に示す手順は不要です。これは、ブラウザを使用して Web サイトにアクセスすると、クライアントのクレデンシャルが [Surrogate Timeout] と同等の期間 ( デフォルトでは 1 時間 ) にわたってキャッシュされるためです。

- 注: 明示的モード ( PAC ファイルまたはブラウザのプロキシ設定を使用 ) では、[Apply same

surrogate settings to explicit forward requests] オプションがオンになっていることを確認します。

- それでもまだ、TeamViewer へのアクセス中にアクセス ログに 401 と 407 が断続的に出力される場合は、次の手順を使用して認証をバイパスできます。

TeamViewer の認証免除を設定するには、次の手順に従います。

## ステップ 1：カスタム URL カテゴリの作成

TeamViewer Agent は異なる IP アドレスの異なるサーバに接続するため、いくつかの正規表現を設定しておく必要があります。

1. [Web GUI ] >[Web Security Manager] > [Custom URL Categories] に移動します。
2. [Add Custom Category...] ボタンをクリックします。
3. カテゴリ名を選択します。
4. [Sites] フィールドに、次のように入力します。 `..teamviewer.com, dyngate.com.`
5. [Advanced] をクリックし、[Regular Expressions] フィールドで次を追加します。  
`din\.aspx`  
`dout\.aspx`
6. 変更を送信し、保存します。

## ステップ 2：新しいアイデンティティの追加

1. [Web GUI ] >[Web Security Manager] > [Identities] に移動します。
2. [Add Identity...] ボタンをクリックします。
3. **認証なし**のアイデンティティを作成します。
4. [Advanced] ドロップダウン メニューをクリックし、[URL Categories] の右側にある [None Selected] リンクをクリックします。
5. 正しい行を選択し、新たに作成したカスタム URL カテゴリ ( 上記を参照 ) をアイデンティティに追加します。
6. 変更を送信し、保存します。

## ステップ3：アクセス ポリシーへの新しいアイデンティティの追加

この操作を行うには、既存のアクセス ポリシーを使用するか、または新しいアクセス ポリシー

を使用するという 2 通りの方法があります。

## 既存のアクセス ポリシーの使用に関する回避策

1. [Web GUI ] > [Web Security Manager] > [Access Policies] に移動します。
2. カスタム URL を許可する必要があるアクセス ポリシー名の場合、[URL Categories] 列にあるリンクをクリックします。
3. 新たに作成されたカスタム カテゴリで [include] リンクをクリックし、アクションを [Allow] または [Monitor] に設定します。
4. 変更を送信し、保存します。

## 新しいアクセス ポリシーの使用に関する回避策

1. [Web GUI ] > [Web Security Manager] > [Access Policies] に移動します。
2. [Add Policy...] ボタンをクリックします。
3. **<Policy Name>** を選択します。
4. [Identities and Users] ドロップダウン リストをクリックし、新しく作成したアイデンティティを選択します。
5. 変更を送信し、保存します。