Finesseサードパーティクライアントと SSOの統合

内容

概要

このドキュメントでは、Unified Contact Center Enterprise(UCCE)またはUnified Contact Center Express(UCCX)でカスタムデスクトップクライアントをシングルサインオン(SSO)と統合する方法について説明します。

SSOはFinesseでネイティブに利用できます。これは、Cisco Unified Contact Centerの重要な機能の1つです。SSOは、ユーザが1つのアプリケーションにサインインし、ユーザのクレデンシャルを再入力することなく、他の許可されたアプリケーションに安全にアクセスできるようにする認証プロセスです。SSOを使用すると、Ciscoスーパーバイザとエージェントは、ユーザ名とパスワードを使用して1回だけサインインし、1つのブラウザインスタンス内のすべてのブラウザベースのシスコアプリケーションとサービスにアクセスできます。

前提条件

要件

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Server(IdS)12.5
- Finesse 12.5(1)ES1
- ADFS 2012
- UCCE 12.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

カスタムクライアントとして、API要求をFinesseサーバに送信するには、要求を承認する必要があります。SSOのコンテキストでは、この認可はトークンを使用して提供されるため、まずトークンを理解します。

トークンには次の 2 種類があります。

- アクセストークン：保護されたリソースにアクセスします。クライアントには、ユーザのID情報を含むアクセストークンが発行されます。ID情報はデフォルトで暗号化されます。
- [Refresh Token]：現在のアクセストークンが期限切れになる前に、新しいアクセストークンを取得します。IdSが更新トークンを生成します。

リフレッシュおよびアクセストークンは、トークンのペアとして生成されます。アクセストークンを更新すると、トークンのペアによってセキュリティの追加レイヤが提供されます。

IdS管理では、更新トークンとアクセストークンの有効期限を設定できます。更新トークンの有効期限が切れると、アクセストークンを更新できません。

フェッチアクセストークン

新しいFinesse APIの実装では、Finesse URLで2つのクエリパラメータ**cc_username**と**return_refresh_toeknを使用**して、アクセストークンを取得できます。

(11.6.(1)ES10、12.0(1)ES3、12.5(1)ES1以降のリリースで利用可能)。

（以前のリリースでは、以前はセッションcookieにcc_usernameとトークンを保存していましたが、ネイティブのFinesseデスクトップでも同じです）

以下に例を挙げます。

https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&return_refresh_token=true

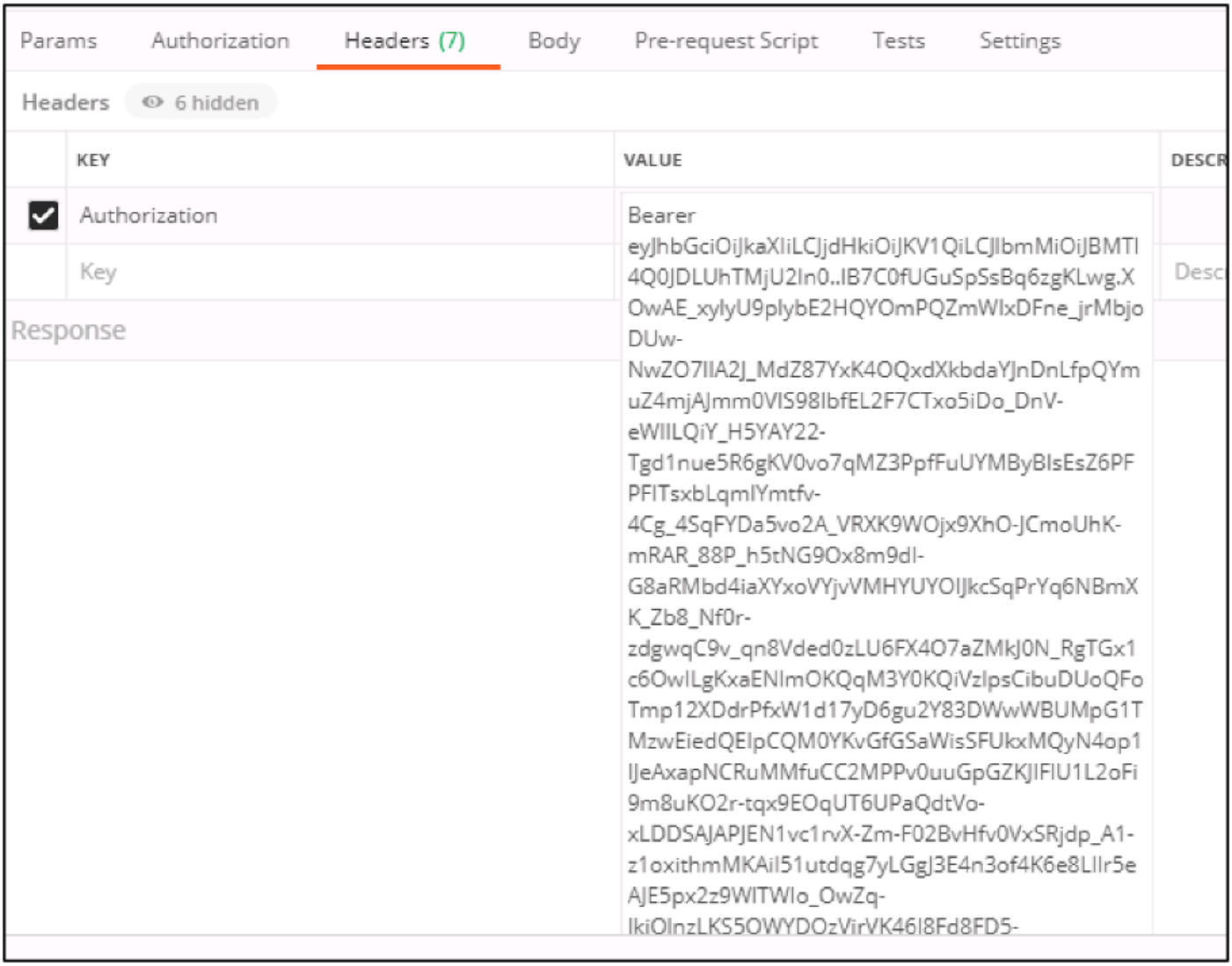
これにより、[AD FS (IdP)]ページにリダイレクトされます

ADFSからの認証に成功すると、トークンに直接リダイレクトされます。

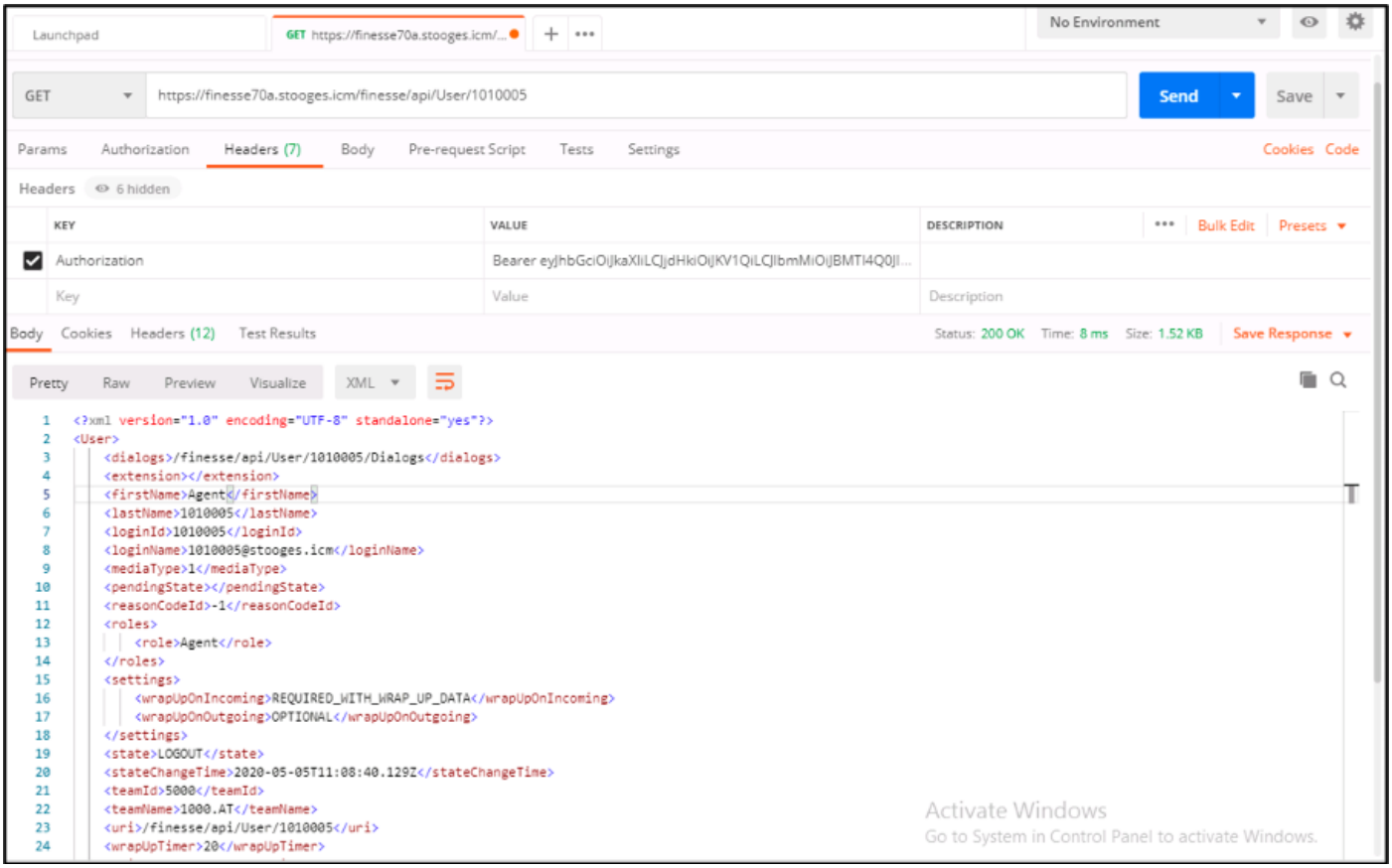
このトークンを使用して、ユーザに対する要求をベアラートークンとしてFinesseに送信できます。

承認ヘッダーをカスタムコードのBearer <access token>として使用します。

この例では、Postman Clientを使用します。



要求がアクセストークンで送信されると、200OKと対応する出力で応答が得られます。次の図は、現在の状態がフェッチされたことを示しています。



同様に、トークンを状態変更APIで使用して、エージェントの準備、受信不可、ログアウトなどを行ったり、カスタムクライアントの応答、コールの発信などを行うダイアログAPIで使用できます。

アクセストークンの更新

アクセストークンに有効期限があります。このトークンは、有効期限が切れる前に更新する必要があります。

推奨事項：

- サードパーティアプリケーションは、トークンの有効期限の75 %が経過した後で、アクセストークンを更新する必要があります。
- このAPIを起動すると、Cisco Identity ServerおよびCisco Identity Providerへのブラウザリダイレクトが含まれる場合があります。

アクセストークンを更新するには、次のURLを使用します。
https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&refresh-token=<refresh-token-value>

次の図に示すように、新しいアクセストークンを受信します。

ここでも、この新しいトークンをアクセストークンとして使用して、Finesseサーバに要求を送信できます。