Intégration client tiers Finesse avec SSO

Contenu

Introduction

Ce document décrit comment vous pouvez intégrer le client de bureau personnalisé avec l'authentification unique (SSO) dans Unified Contact Center Enterprise (UCCE) ou Unified Contact Center Express (UCCX).

SSO est nativement disponible avec Finesse. Il s'agit d'une des fonctionnalités essentielles de Cisco Unified Contact Center. SSO est un processus d'authentification qui permet aux utilisateurs de se connecter à une application, puis d'accéder en toute sécurité à d'autres applications autorisées sans avoir à réapprovisionner les informations d'identification des utilisateurs. SSO permet aux superviseurs et agents Cisco de se connecter une seule fois avec un nom d'utilisateur et un mot de passe pour accéder à toutes leurs applications et services Cisco basés sur navigateur dans une instance de navigateur unique.

Conditions préalables

Conditions requises

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

En tant que client personnalisé, pour envoyer des demandes d'API au serveur Finesse, vos demandes doivent être autorisées. Dans le contexte de SSO, cette autorisation est fournie à l'aide de jetons afin de comprendre d'abord les jetons.

Il existe deux types de jetons :

- Jeton d'accès : il accède aux ressources protégées. Un jeton d'accès qui contient des informations d'identité pour l'utilisateur est attribué aux clients. Les informations d'identité sont chiffrées par défaut.
- Actualiser le jeton : il obtient un nouveau jeton d'accès avant l'expiration du jeton d'accès actuel. L'IDS génère le jeton d'actualisation.

Les jetons d'actualisation et d'accès sont générés sous la forme d'une paire de jetons. Lors de l'actualisation du jeton d'accès, la paire de jetons fournit une couche supplémentaire de sécurité.

Vous pouvez configurer le délai d'expiration du jeton d'actualisation et du jeton d'accès dans l'administration d'IDS. Lorsque le jeton d'actualisation expire, vous ne pouvez pas actualiser le jeton d'accès.

Récupérer le jeton d'accès

Avec les nouvelles implémentations de l'API Finesse, vous pouvez utiliser deux paramètres de requête **cc_username** et **return_fresh_toekn** dans l'URL Finesse pour obtenir le jeton d'accès.

(Disponible avec les versions 11.6.(1)ES10, 12.0(1)ES3, 12.5(1)ES1 et ultérieures).

(Dans les versions précédentes, nous avons utilisé pour stocker le nom d'utilisateur cc et les jetons dans les cookies de session et c'est toujours la même chose avec Finesse Desktop natif)

Exemple :

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

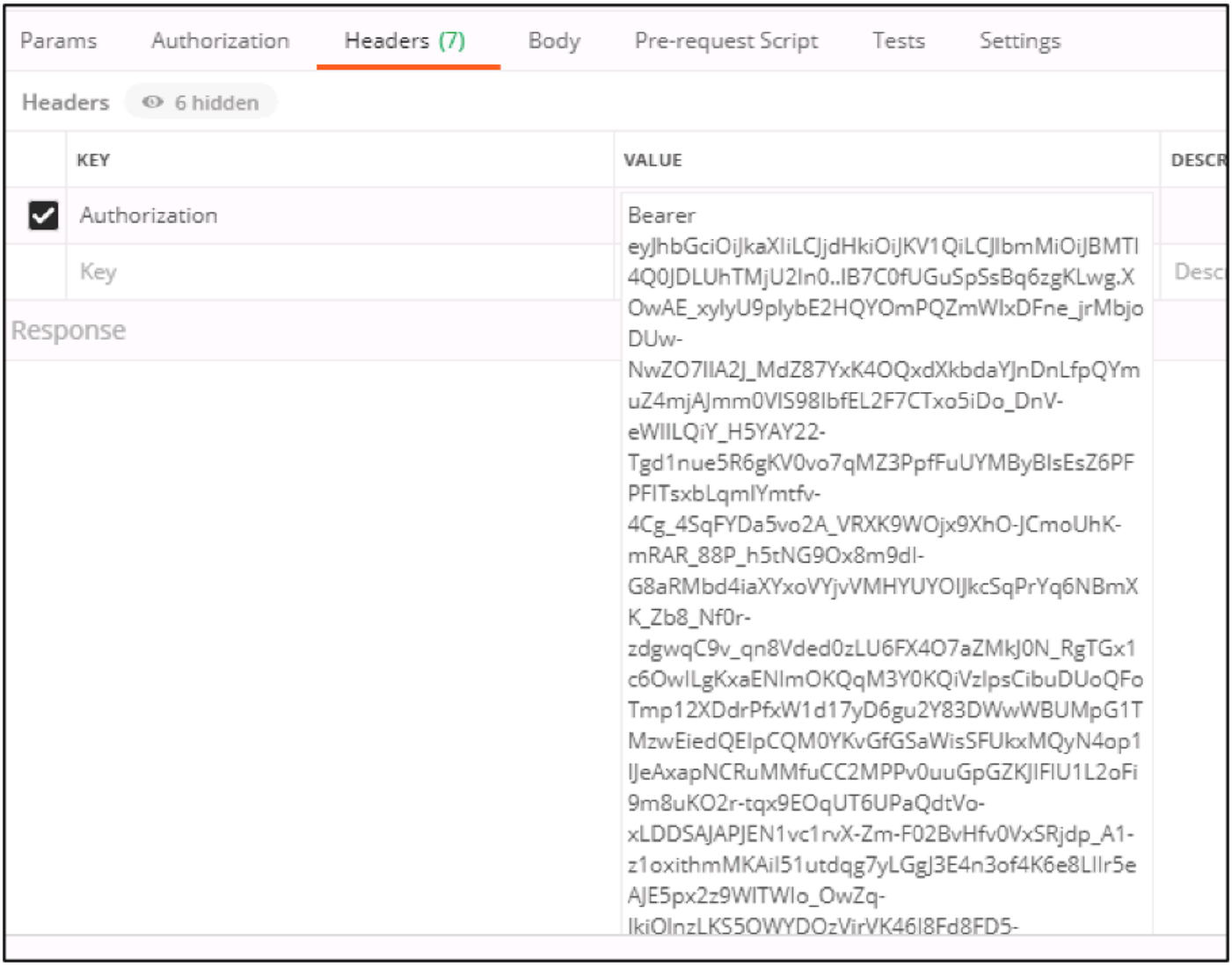
Vous êtes redirigé vers la page AD FS (IdP)

Après une authentification réussie à partir d'ADFS, vous êtes redirigé vers le jeton directement.

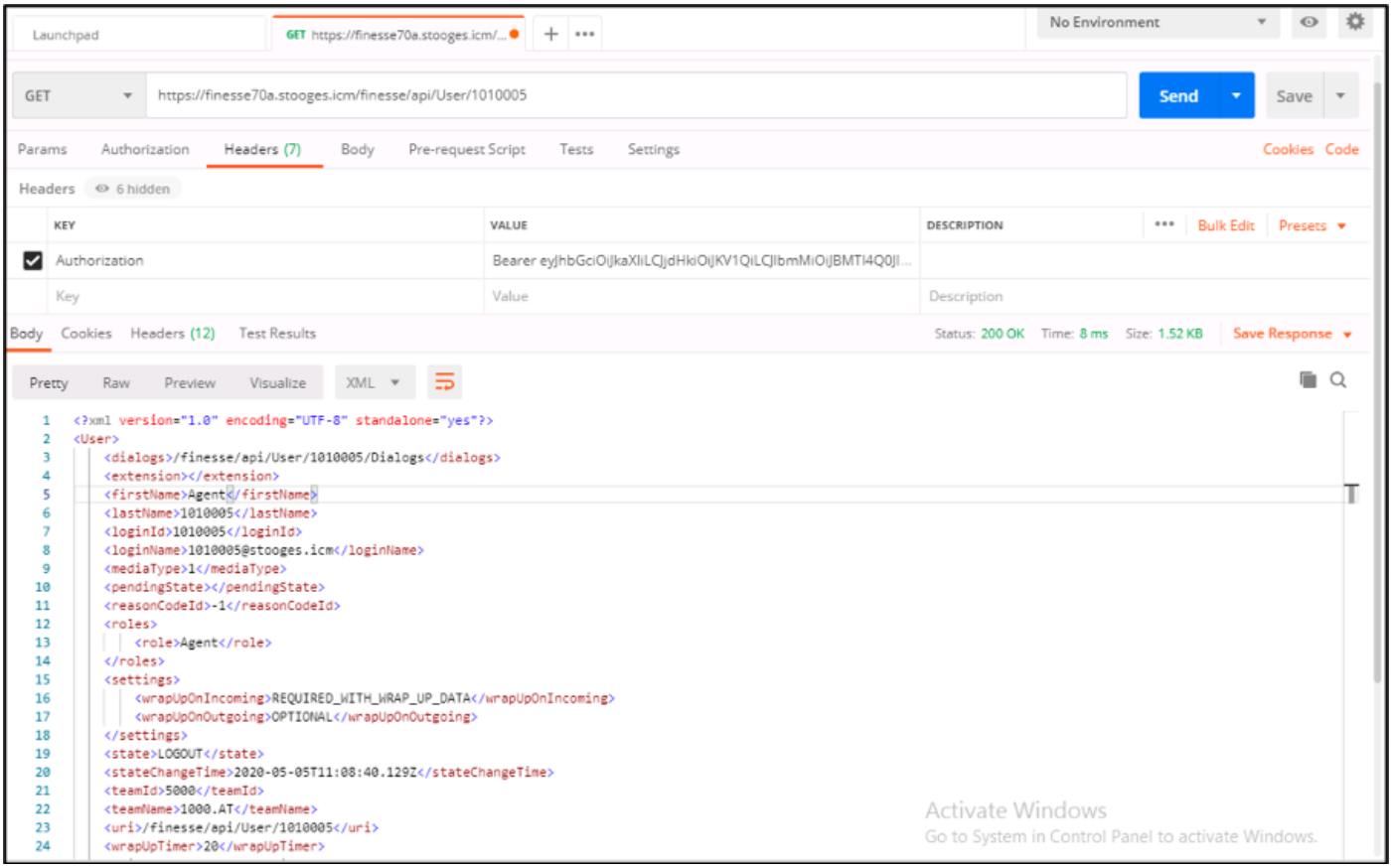
Vous pouvez utiliser ce jeton pour envoyer des requêtes à Finesse pour l'utilisateur en tant que jeton porteur.

Utilisez l'en-tête d'autorisation en tant que **support <jeton d'accès>** dans votre code personnalisé.

Cet exemple utilise le client Postman.



Lorsque la demande est envoyée avec un jeton d'accès, vous obtenez la réponse avec 200OK et la sortie correspondante. Cette image montre que l'état actuel est récupéré.



De même, le jeton peut être utilisé pour les API de changement d'état pour rendre Agent Ready, Not Ready, Logout, etc, et pour les API de dialogue pour Répondre, Passer un appel, etc dans le client personnalisé.

Actualiser le jeton d'accès

Un jeton d'accès a un délai d'expiration. Vous devez actualiser ce jeton avant qu'il expire.

Selon la recommandation :

- Les applications tierces doivent actualiser le jeton d'accès après l'expiration de 75 % du délai d'expiration du jeton.
- L'appel de cette API peut impliquer une redirection du navigateur vers Cisco Identity Server et Cisco Identity Provider.

Afin d'actualiser le jeton d'accès, utilisez cette URL : **https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&fresh-token=<actuh-token-value>**

Vous recevez le nouveau jeton d'accès comme indiqué dans l'image.

Vous pouvez à nouveau utiliser ce nouveau jeton comme jeton d'accès pour envoyer une requête au serveur Finesse.