Tiers intégration de client de finesse avec SSO

Contenu

Introduction

Ce document décrit comment vous pouvez intégrer le client de bureau fait sur commande avec l'ouverture de session simple (SSO) dans Unified Contact Center Enterprise (UCCE) ou Unified Contact Center Express (UCCX).

SSO est à la façon des indigènes disponible avec la finesse. Il est l'une des caractéristiques cruciales de Cisco Unified Contact Center. SSO est une procédure d'authentification qui permet à des utilisateurs pour se connecter à une application et puis pour accéder à sécurisé autre des applications autorisées sans nécessité de réapprovisionner des identifiants utilisateurs. SSO permet à des superviseurs et à des agents de Cisco pour se connecter seulement une fois avec un nom d'utilisateur et mot de passe pour accéder à tous leurs applications basées sur navigateur et services de Cisco dans un exemple simple de navigateur.

Conditions préalables

Exigences

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

Composants utilisés

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

- Serveur d'identité de Cisco (id) 12.5
- Finesse 12.5(1)ES1
- ADFS 2012
- UCCE 12.5

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

En tant que client fait sur commande, envoyer à des demandes API au serveur de finesse vos demandes doit être autorisé. Dans le cadre de SSO, cette autorisation est fournie utilisant des jetons ainsi comprenez les jetons d'abord.

Il y a deux types de jetons :

- Jeton d'Access il accède aux ressources protégées. Des clients sont émis un jeton d'accès qui contient les informations d'identité pour l'utilisateur. Les informations d'identité sont chiffrées par défaut.
- Régénérez le jeton qu'il obtient un nouveau jeton d'accès avant que le jeton en cours d'accès expire. Les id génère le jeton de régénération.

Les jetons de régénération et d'accès sont générés comme paire de jetons. En régénérant le jeton d'accès, les paires de jetons fournissent une couche supplémentaire de Sécurité.

Vous pouvez configurer l'échéance temps du jeton de régénération et du jeton d'accès dans la gestion d'id. Quand le jeton de régénération expire, vous ne pouvez pas régénérer le jeton d'accès.

Jeton d'Access d'effort

Avec les nouvelles réalisations de la finesse API, vous pouvez employer le **cc_username** et le **return_refresh_toekn de** deux paramètres de requête dans l'URL de finesse pour obtenir l'Access-jeton.

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

(Dans des releases plus anciennes que nous enregistrions le cc_username et les jetons dans les Témoins et lui de session est toujours identiques avec l'appareil de bureau indigène de finesse)

Exemple :

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

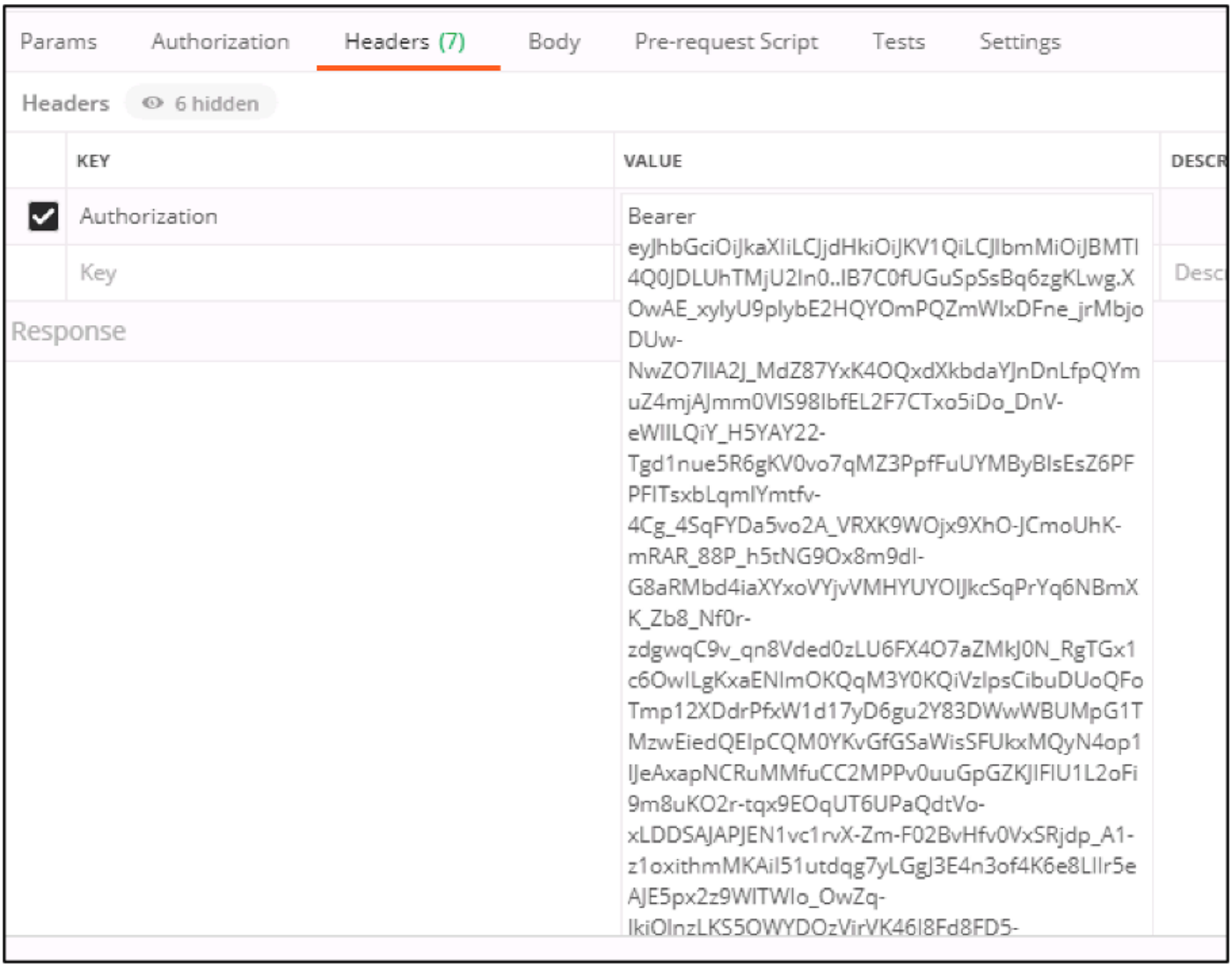
Ceci vous réoriente à la page FS d'AD (IDP)

Après l'authentification réussie d'ADFS, vous êtes réorienté au jeton directement.

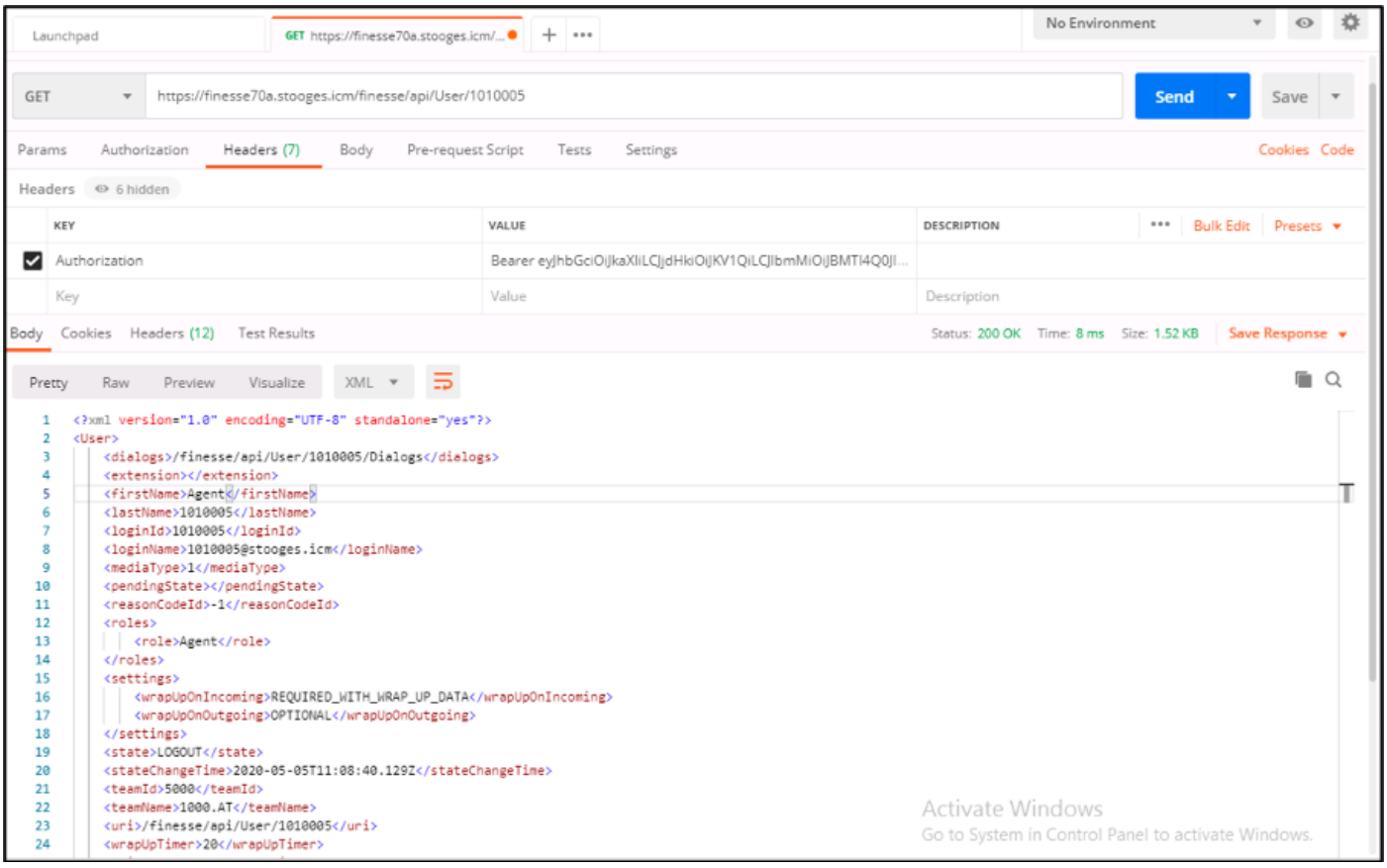
Vous pouvez employer ce jeton pour envoyer des demandes à la finesse pour l'utilisateur comme jeton de support.

Utilisez l'en-tête d'autorisation en tant que **token> de <access de support** en votre code personnalisé.

Cet échantillon utilise le client de facteur.



Quand la demande est envoyée avec le jeton d'Access, vous obtenez la réponse avec 200OK et la sortie correspondante. Cette image prouve que l'état actuel est cherché.



De même, le jeton peut être utilisé pour la modification d'état API pour préparer l'agent prêts, la déconnexion, etc., et pour le dialogue API pour répondre, font l'appel, etc. dans le client fait sur commande.

Régénérez le jeton d'Access

Un jeton d'accès a une échéance temps. Vous devez régénérer ce jeton avant qu'il expire.

Selon la recommandation :

- Les applications tierces doivent régénérer le jeton d'accès après que 75% de l'échéance symbolique temps soit écoulé.
- L'invocation de cet API pourrait faire participer le serveur d'identité de Cisco de redirect to de navigateur et le fournisseur d'identité de Cisco.

Afin de régénérer l'utilisation d'Access-jeton cet URL : **https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&refresh-token=<refresh-token-value>**

Vous recevez le nouveau jeton d'accès suivant les indications de l'image.

Maintenant de nouveau vous pouvez employer ce nouveau jeton comme jeton d'accès pour envoyer une demande au serveur de finesse.