Finesse Thirdparty Client Integration con SSO

Contenido

Introducción

Este documento describe cómo integrar el cliente de escritorio personalizado con el inicio de sesión único (SSO) en Unified Contact Center Enterprise (UCCE) o Unified Contact Center Express (UCCX).

SSO está disponible de forma nativa con Finesse. Se trata de una de las funciones cruciales de Cisco Unified Contact Center. SSO es un proceso de autenticación que permite a los usuarios iniciar sesión en una aplicación y luego acceder de forma segura a otras aplicaciones autorizadas sin necesidad de volver a suministrar las credenciales del usuario. SSO permite a los supervisores y agentes de Cisco iniciar sesión una sola vez con un nombre de usuario y una contraseña para obtener acceso a todas sus aplicaciones y servicios de Cisco basados en navegador en una única instancia del navegador.

Prerequisites

Requirements

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Como cliente personalizado, para enviar solicitudes API al servidor Finesse, sus solicitudes deben estar autorizadas. En el contexto de SSO, esta autorización se proporciona utilizando tokens para comprender primero tokens.

Hay dos tipos de tokens:

- Access Token: accede a los recursos protegidos. Los clientes reciben un token de acceso que contiene información de identidad para el usuario. La información de identidad se cifra de forma predeterminada.
- Refresh Token- Obtiene un nuevo token de acceso antes de que caduque el token de acceso actual. El IdS genera el token de actualización.

Los tokens de actualización y acceso se generan como un par de tokens. Al actualizar el token de acceso, el par de tokens proporciona una capa adicional de seguridad.

Puede configurar la hora de vencimiento del token de actualización y del token de acceso en la administración de IdS. Cuando caduque el token de actualización, no podrá actualizar el token de acceso.

Obtener el token de acceso

Con las nuevas implementaciones de la API Finesse, puede utilizar dos parámetros de consulta **cc_username** y **return_refresh_toekn** en la URL Finesse para obtener el token de acceso.

(Disponible con 11.6.1(1)ES10, 12.0(1)ES3,12.5(1)ES1 y versiones posteriores).

(En versiones anteriores, solíamos almacenar el cc_username y los tokens en las cookies de sesión y sigue siendo el mismo con el escritorio Finesse nativo)

Ejemplo:

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

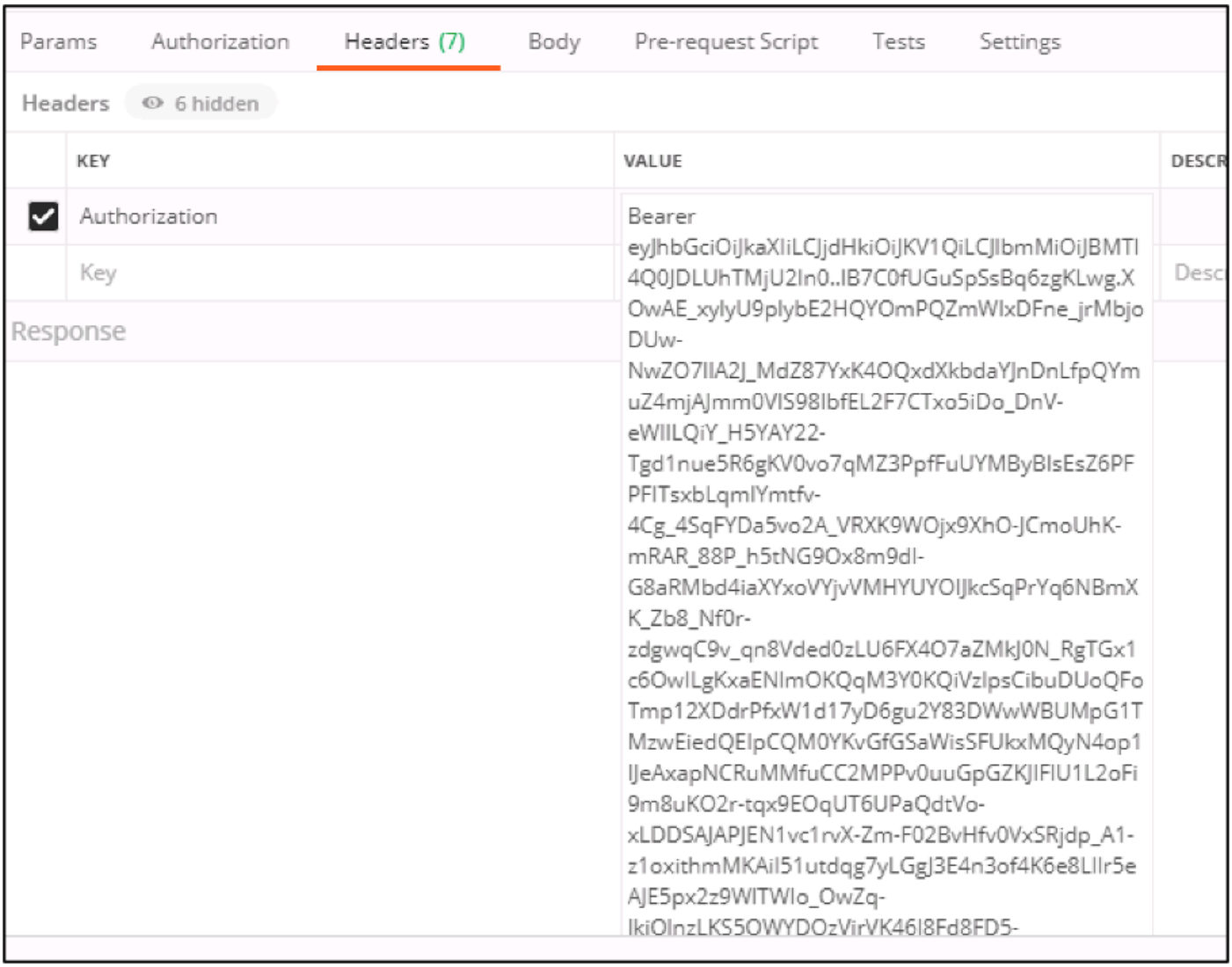
Esto le redirige a la página AD FS (IdP)

Después de una autenticación exitosa de ADFS, se le redirige directamente al token.

Puede utilizar este token para enviar solicitudes a Finesse para el usuario como token portador.

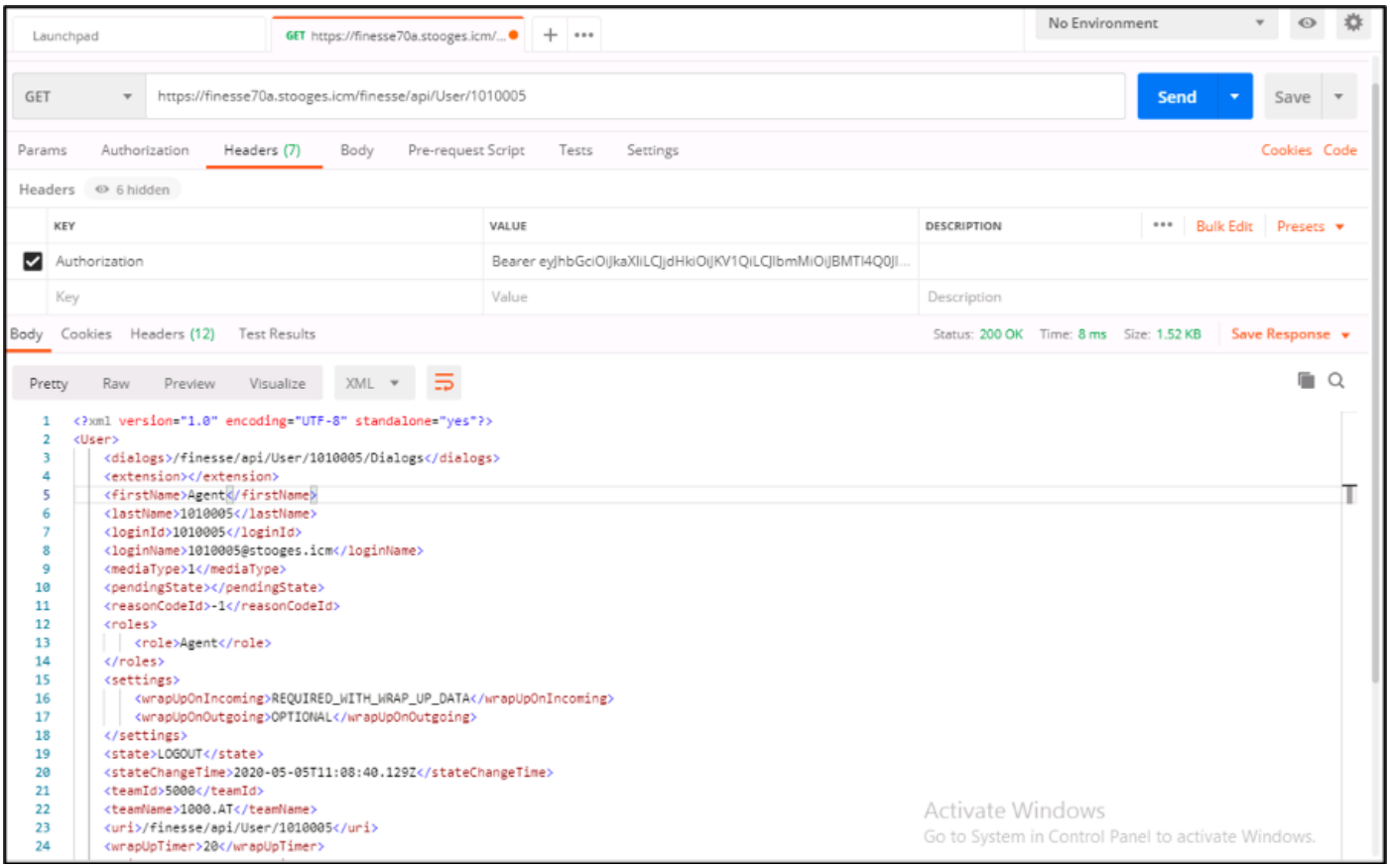
Utilice el encabezado de autorización como **portador <token de acceso>** en su código personalizado.

Este ejemplo utiliza el cliente Postman.



Cuando la solicitud se envía con el token de acceso, obtiene la respuesta con 200OK y el

resultado correspondiente. Esta imagen muestra que se obtiene el estado actual.



Del mismo modo, el token se puede utilizar para que las API de cambio de estado preparen Agente, No preparado, Cierre de sesión, etc., y para las API de cuadro de diálogo para contestar, Realizar llamada, etc. en el cliente personalizado.

Actualizar token de acceso

Un token de acceso tiene una hora de vencimiento. Debe actualizar este token antes de que caduque.

Según la recomendación:

- Las aplicaciones de terceros deben actualizar el token de acceso después de que transcurra el 75% del tiempo de vencimiento del token.
- La invocación de esta API podría implicar la redirección del navegador a Cisco Identity Server y Cisco Identity Provider.

PARA actualizar el token de acceso, utilice esta URL:
https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&refresh-token=<update-token-value>

Recibirá el nuevo token de acceso como se muestra en la imagen.

Una vez más, puede utilizar este nuevo token como símbolo de acceso para enviar una solicitud al servidor Finesse.