Finesse Integração de cliente terceirizado com SSO

Contents

Introduction

Este documento descreve como você pode integrar o cliente de desktop personalizado com o Logon Único (SSO) no Unified Contact Center Enterprise (UCCE) ou no Unified Contact Center Express (UCCX).

O SSO está nativamente disponível com o Finesse. É um dos recursos cruciais do Cisco Unified Contact Center. SSO é um processo de autenticação que permite que os usuários entrem em um aplicativo e acessem com segurança outros aplicativos autorizados sem a necessidade de refornecer credenciais de usuário. O SSO permite que os supervisores e agentes da Cisco iniciem sessão apenas uma vez com um nome de usuário e senha para obter acesso a todos os aplicativos e serviços da Cisco baseados em navegador em uma única instância do navegador.

Prerequisites

Requirements

Este documento não se restringe a versões de software e hardware específicas.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Como cliente personalizado, para enviar solicitações de API ao servidor Finesse, suas solicitações devem ser autorizadas. No contexto do SSO, essa autorização é fornecida usando tokens para entender os tokens primeiro.

Há dois tipos de tokens:

- Token de acesso- Ele acessa recursos protegidos. Os clientes recebem um token de acesso que contém informações de identidade para o usuário. As informações de identidade são criptografadas por padrão.
- Atualizar token- Obtém um novo token de acesso antes de o token de acesso atual expirar. O IdS gera o token de atualização.

Os tokens de atualização e acesso são gerados como um par de tokens. Ao atualizar o token de acesso, o par de tokens fornece uma camada extra de segurança.

Você pode configurar o tempo de expiração do token de atualização e do token de acesso na administração de IdS. Quando o token de atualização expira, não é possível atualizar o token de acesso.

Buscar token de acesso

Com as novas implementações da API Finesse, você pode usar dois parâmetros de consulta **cc_username** e **return_refresh_toekn** na URL do Finesse para obter o access-token.

(Disponível com 11.6(1)ES10, 12.0(1)ES3,12.5(1)ES1 e versões posteriores).

(Em versões mais antigas, costumávamos armazenar o cc_username e os tokens em cookies de sessão e ainda é o mesmo com o Finesse Desktop nativo)

Exemplo:

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

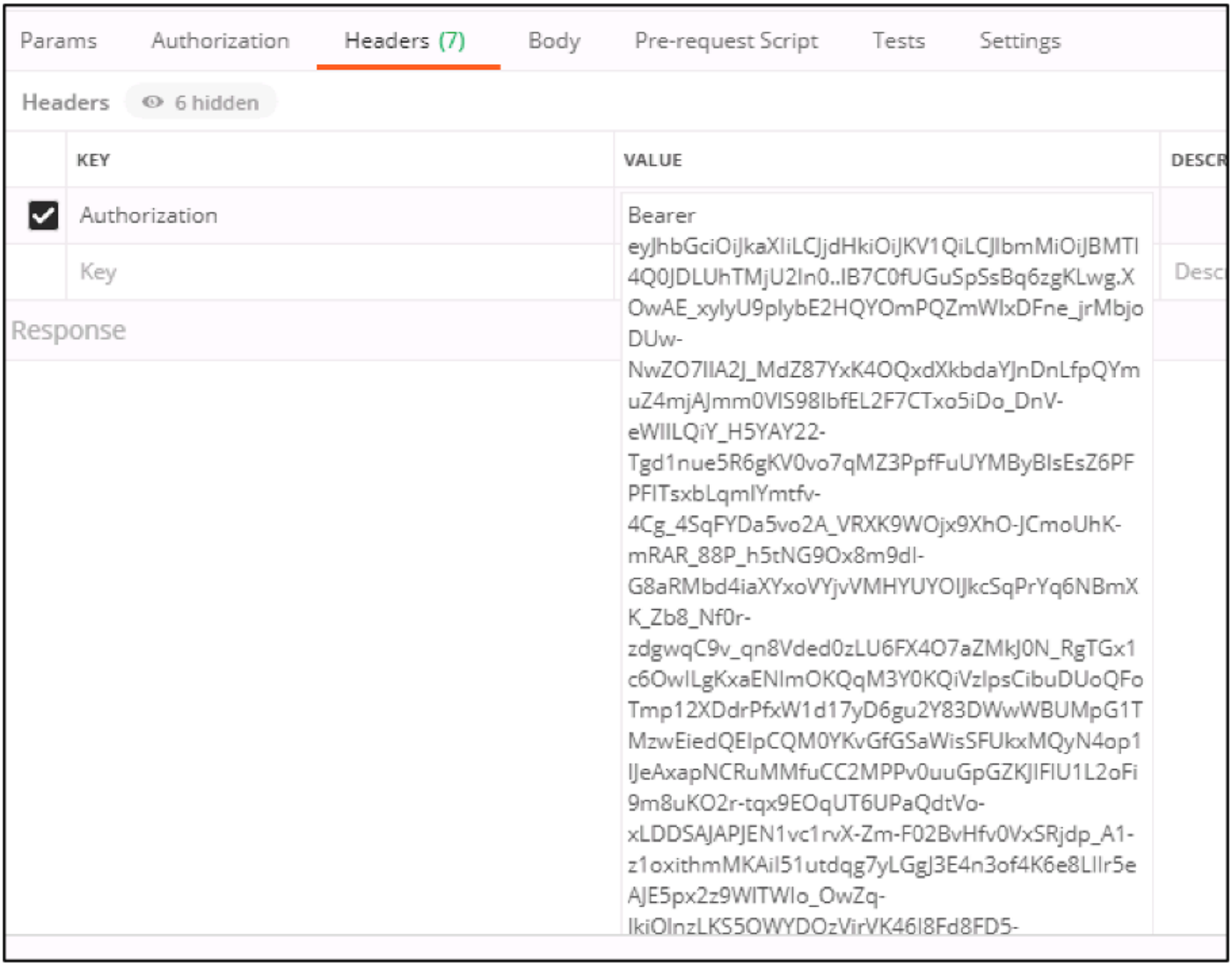
Isso o redireciona para a página do AD FS (IdP)

Após a autenticação bem-sucedida do ADFS, você é redirecionado para o token diretamente.

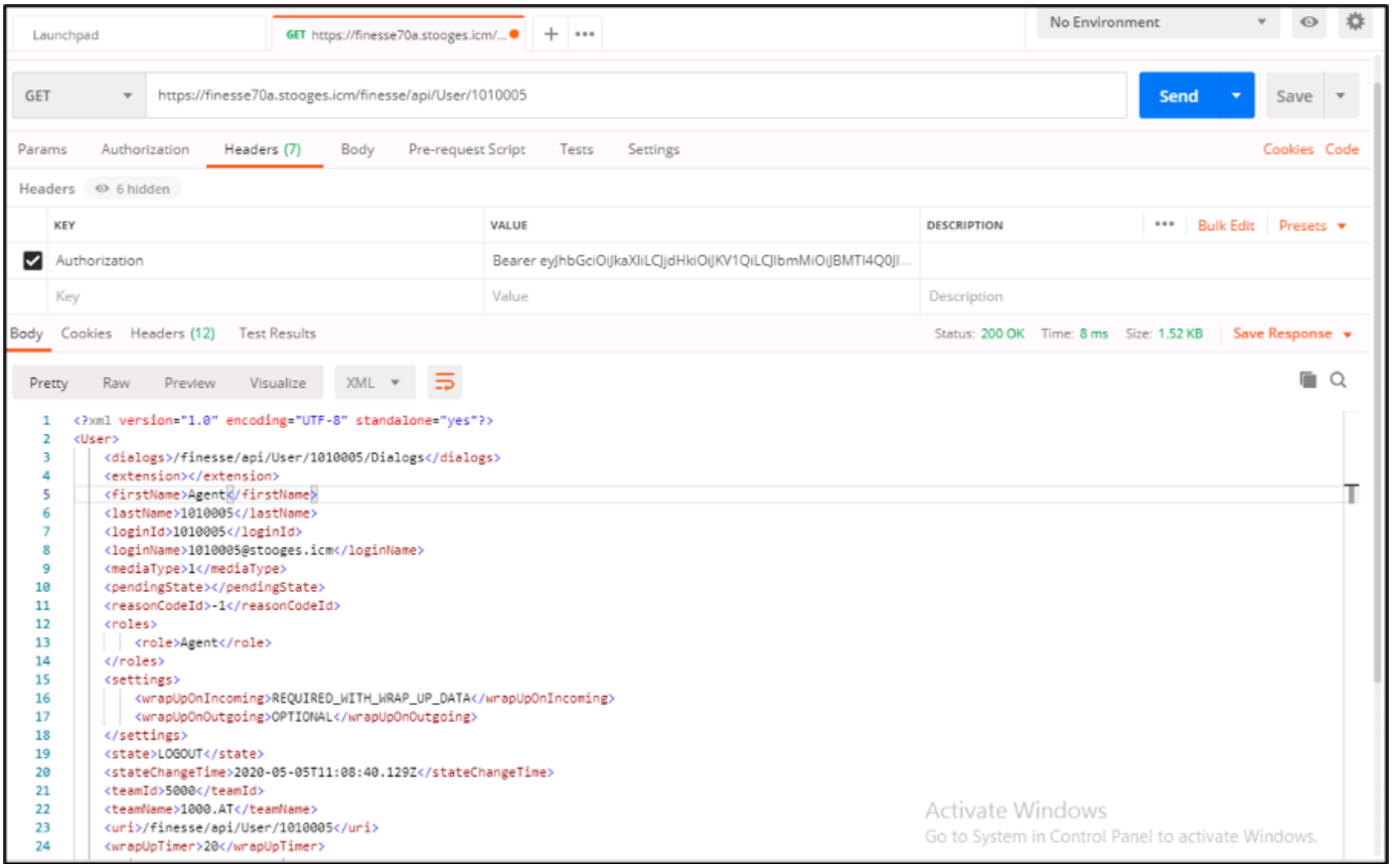
Você pode usar esse token para enviar solicitações ao Finesse para o usuário como token do Portador.

Use o cabeçalho de autorização como **portador <access token>** em seu código personalizado.

Esta amostra usa o cliente Postman.



Quando a solicitação é enviada com o Access Token, você obtém a resposta com 200OK e a saída correspondente. Esta imagem mostra que o estado atual é buscado.



Da mesma forma, o token pode ser usado para APIs de alteração de estado para tornar o Agent Ready, Not Ready, Logout, etc., e para APIs de diálogo para Answering, Make Call, etc. no cliente personalizado.

Atualizar token de acesso

Um token de acesso tem um tempo de expiração. Você deve atualizar este token antes que ele expire.

De acordo com a recomendação:

- Os aplicativos de terceiros precisam atualizar o token de acesso depois que 75% do tempo de expiração do token tiver expirado.
- Invocar esta API pode envolver o redirecionamento do navegador para o Cisco Identity Server e o Cisco Identity Provider.

Para atualizar o access-token, use este URL:
https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&refresh-token=<refresh-token-value>

Você recebe o novo token de acesso como mostrado na imagem.

Agora, novamente, você pode usar esse novo token como o token de acesso para enviar uma solicitação ao servidor Finesse.