Integrazione client di terze parti Finesse con SSO

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Recupera token di accesso](#)
[Aggiorna token di accesso](#)

Introduzione

In questo documento viene descritto come integrare il client desktop personalizzato con Single Sign-On (SSO) in Unified Contact Center Enterprise (UCCE) o Unified Contact Center Express (UCCX).

SSO è disponibile in modo nativo con Finesse. Si tratta di una delle funzionalità fondamentali di Cisco Unified Contact Center. SSO è un processo di autenticazione che consente agli utenti di accedere a un'applicazione e quindi accedere in modo sicuro ad altre applicazioni autorizzate senza dover fornire nuovamente le credenziali dell'utente. L'SSO consente ai supervisori e agli agenti Cisco di accedere una sola volta con un nome utente e una password per accedere a tutte le applicazioni e i servizi Cisco basati su browser all'interno di una singola istanza del browser.

Prerequisiti

Requisiti

Il documento può essere consultato per tutte le versioni software o hardware.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Come client personalizzato, per inviare richieste API al server Finesse è necessario che le richieste siano autorizzate. Nel contesto di SSO, questa autorizzazione viene fornita utilizzando i token in modo da comprendere prima i token.

Esistono due tipi di token:

- Token di accesso: consente di accedere alle risorse protette. Ai client viene rilasciato un token di accesso che contiene informazioni sull'identità dell'utente. Le informazioni sull'identità vengono crittografate per impostazione predefinita.
- Token di aggiornamento: ottiene un nuovo token di accesso prima della scadenza del token di accesso corrente. IdS genera il token di aggiornamento.

I token di aggiornamento e accesso vengono generati come una coppia di token. Quando si aggiorna il token di accesso, la coppia di token fornisce un ulteriore livello di sicurezza.

Èpossibile configurare l'ora di scadenza del token di aggiornamento e del token di accesso nell'amministrazione IdS. Alla scadenza del token di aggiornamento, non è possibile aggiornare il token di accesso.

Recupera token di accesso

Con le nuove implementazioni API Finesse, è possibile utilizzare due parametri di query **cc_username** e **return_refresh_token** nell'URL Finesse per ottenere il token di accesso.

(disponibile con le versioni 11.6(1)ES10, 12.0(1)ES3, 12.5(1)ES1 e successive).

(Nelle versioni precedenti, il nome utente cc_username e i token venivano memorizzati nei cookie della sessione ed è ancora lo stesso con Finesse Desktop nativo)

Esempio:

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

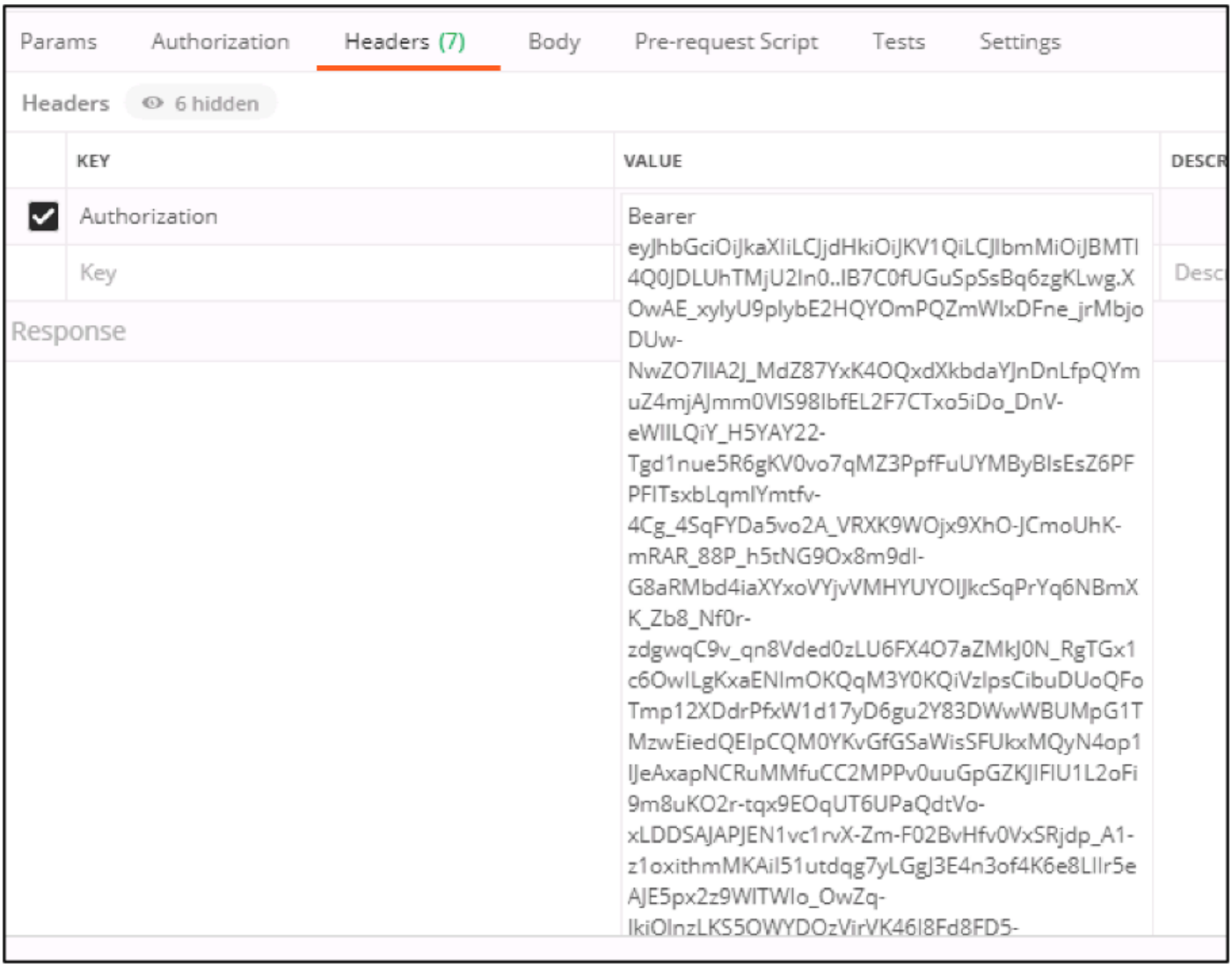
Verrà visualizzata la pagina ADFS (IdP)

Una volta completata l'autenticazione da ADFS, l'utente viene reindirizzato direttamente al token.

Èpossibile utilizzare questo token per inviare richieste a Finesse per l'utente come token di connessione.

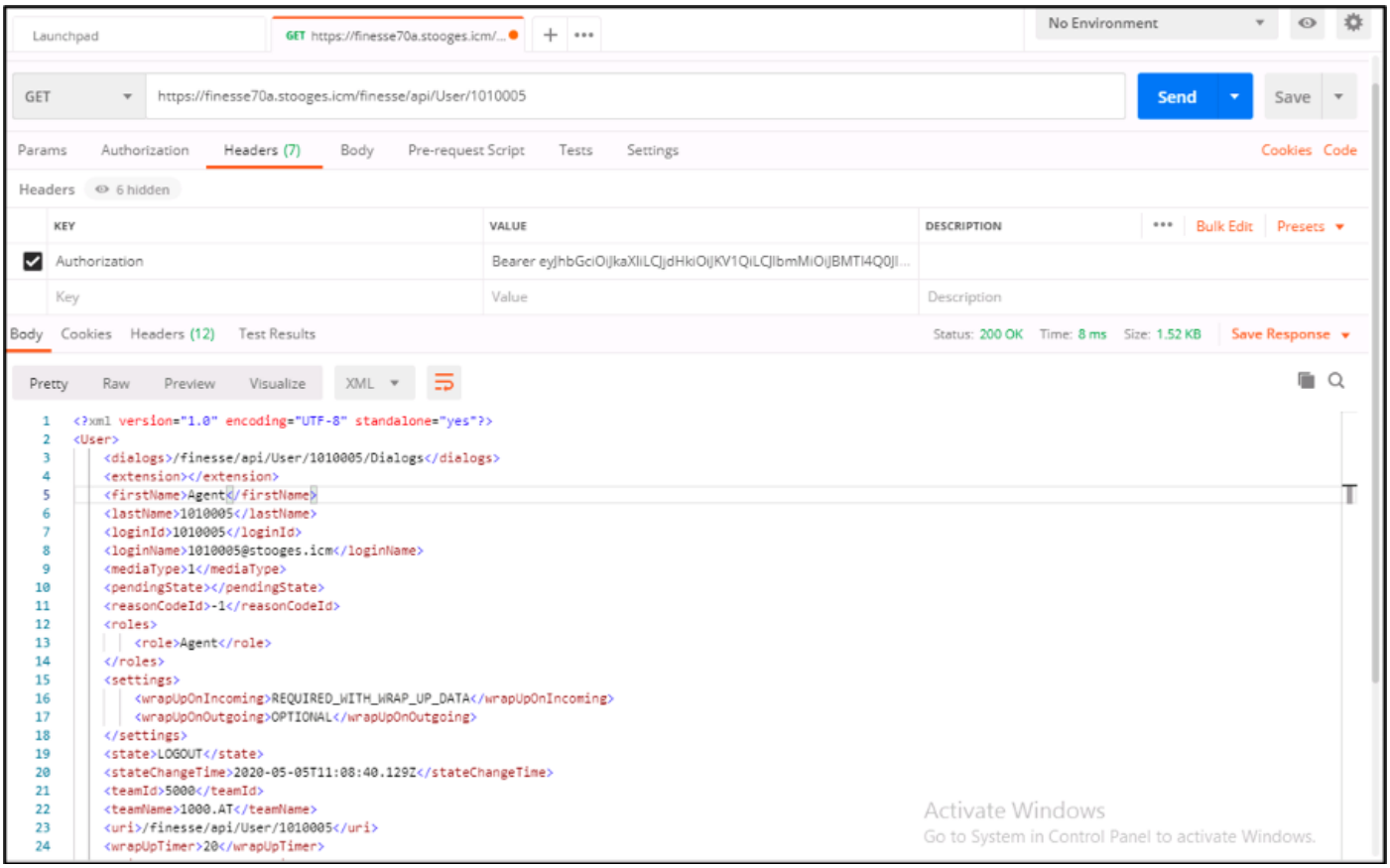
Utilizzare l'intestazione Authorization come **Bearer <access token>** nel codice personalizzato.

In questo esempio si utilizza il client Postman.



Quando la richiesta viene inviata con il token di accesso, si riceve la risposta con 200OK e l'output

corrispondente. In questa immagine viene mostrato come recuperare lo stato corrente.



Analogamente, il token può essere utilizzato per le API di modifica dello stato per rendere l'agente pronto, non pronto, disconnessione e così via, e per le API di dialogo per rispondere, effettuare una chiamata e così via nel client personalizzato.

Aggiorna token di accesso

Un token di accesso ha un'ora di scadenza. È necessario aggiornare il token prima della scadenza.

Secondo la raccomandazione:

- Le applicazioni di terze parti devono aggiornare il token di accesso dopo che è trascorso il 75% del tempo di scadenza del token.
- La chiamata di questa API potrebbe comportare il reindirizzamento del browser a Cisco Identity Server e Cisco Identity Provider.

Per aggiornare il token di accesso, utilizzare il seguente URL:
https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&refresh-token=<refresh-token-value>

Si riceve il nuovo token di accesso come mostrato nell'immagine.

Èora possibile utilizzare questo nuovo token come token di accesso per inviare una richiesta al server Finesse.