Integration von Drittanbieter-Clients in SSO

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie den benutzerdefinierten Desktop-Client mit Single Sign-On (SSO) in Unified Contact Center Enterprise (UCCE) oder Unified Contact Center Express (UCCX) integrieren können.

SSO ist nativ bei Finesse erhältlich. Es ist eine der wichtigsten Funktionen von Cisco Unified Contact Center. Bei SSO handelt es sich um einen Authentifizierungsprozess, bei dem sich Benutzer bei einer Anwendung anmelden und dann sicher auf andere autorisierte Anwendungen zugreifen können, ohne dass Benutzeranmeldeinformationen erneut eingegeben werden müssen. Mit SSO können sich Cisco Supervisoren und Agenten nur einmal mit einem Benutzernamen und einem Kennwort anmelden, um innerhalb einer Browser-Instanz Zugriff auf alle browserbasierten Anwendungen und Services von Cisco zu erhalten.

Voraussetzungen

Anforderungen

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Server (IDs) 12.5
- Finesse 12.5(1)ES1
- ADFS 2012
- UCCE 12,5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Als benutzerdefinierter Client müssen Ihre Anfragen autorisiert werden, um API-Anfragen an den Finesse-Server zu senden. Im Zusammenhang mit der SSO wird diese Autorisierung mit Token bereitgestellt. Verwenden Sie daher zunächst Token.

Es gibt zwei Arten von Token:

- Zugriffs-Token - Es greift auf geschützte Ressourcen zu. Clients wird ein Zugriffstoken ausgegeben, das Identitätsinformationen für den Benutzer enthält. Die Identitätsinformationen werden standardmäßig verschlüsselt.
- Aktualisierungstoken - Es erhält ein neues Zugriffstoken, bevor das aktuelle Zugriffstoken abläuft. Die IDs generieren das Aktualisierungstoken.

Die Aktualisierungs- und Zugriffstoken werden als ein Paar Token generiert. Beim Aktualisieren des Zugriffstokens bieten die Token eine zusätzliche Sicherheitsebene.

Sie können die Ablaufzeit des Aktualisierungstokens und des Zugriffstoken in der IDs-Verwaltung konfigurieren. Wenn das Aktualisierungstoken abläuft, können Sie das Zugriffstoken nicht aktualisieren.

Access-Token abrufen

Mit den neuen Finesse API-Implementierungen können Sie zwei Abfrageparameter **cc_username** und **return_fresh_toekn** in der Finesse-URL verwenden, um das Zugriffstoken abzurufen.

(Verfügbar ab Versionen 11.6.(1)ES10, 12.0(1)ES3,12.5(1)ES1).

(In älteren Versionen haben wir den cc_username und die Token in Session-Cookies gespeichert, und das ist bei nativem Finesse Desktop immer noch dasselbe.)

Beispiel:

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

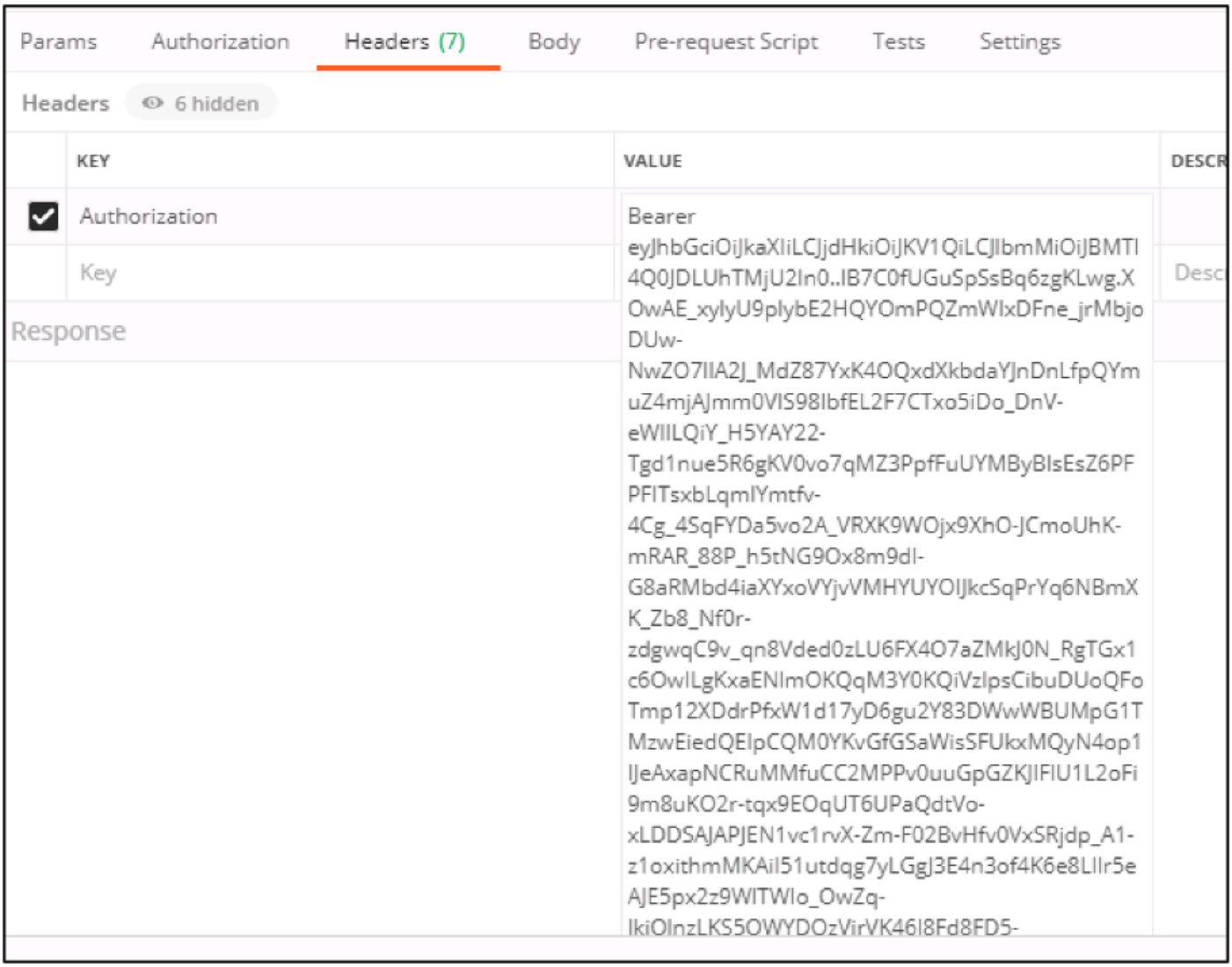
Dadurch werden Sie zur AD-FS-Seite (IdP) weitergeleitet.

Nach erfolgreicher Authentifizierung durch ADFS werden Sie direkt zum Token umgeleitet.

Sie können dieses Token verwenden, um Anfragen als Träger-Token an Finesse zu senden.

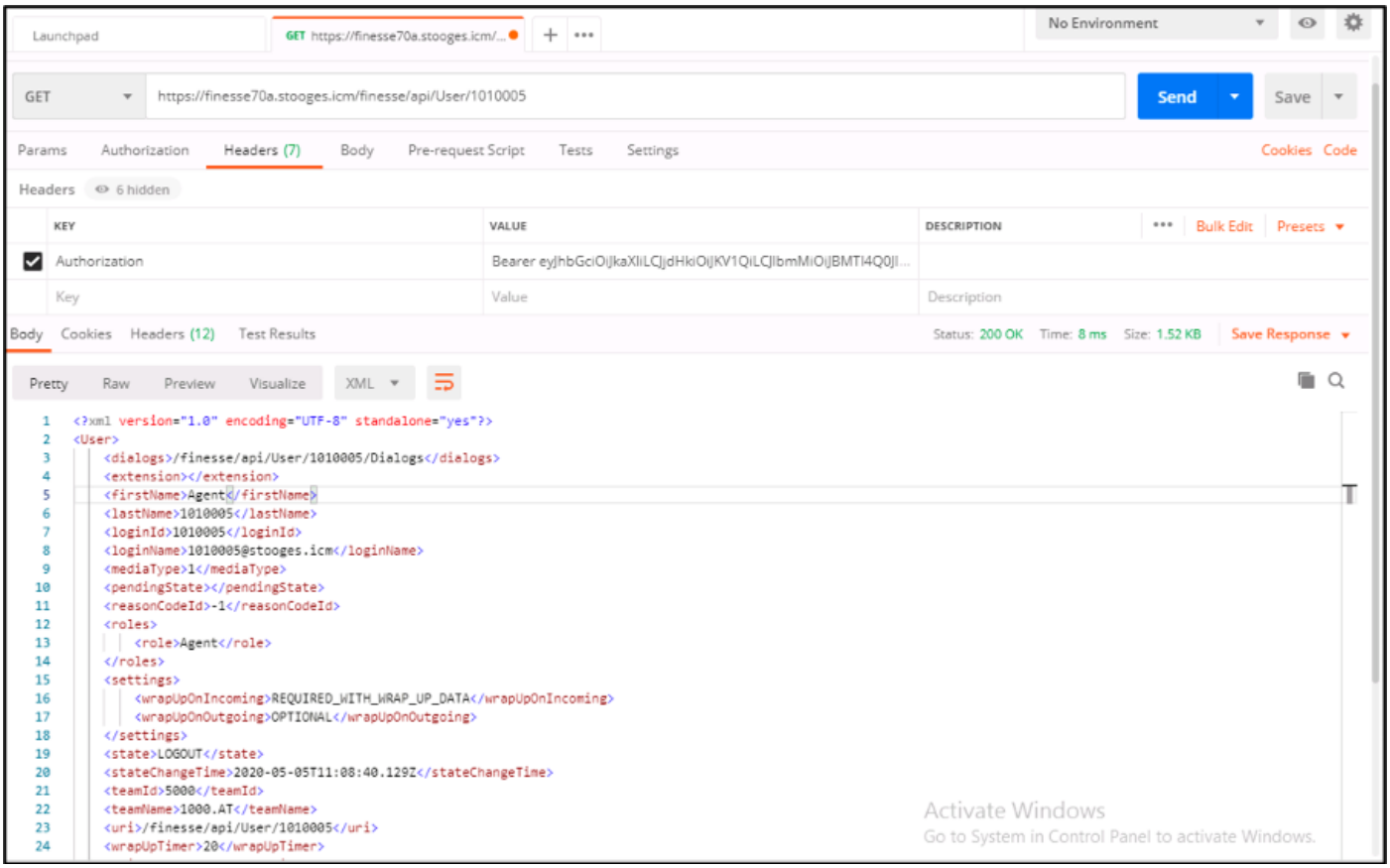
Verwenden Sie den Autorisierungs-Header als **Träger <Zugriffstoken>** in Ihrem benutzerdefinierten Code.

In diesem Beispiel wird der Postman-Client verwendet.



Wenn die Anfrage mit Access Token gesendet wird, erhalten Sie die Antwort mit 200OK und die

entsprechende Ausgabe. Dieses Bild zeigt, dass der aktuelle Status abgerufen wird.



Ebenso kann das Token für APIs für Statusänderungen verwendet werden, um Agent Ready, Not Ready, Logout usw. sowie für Dialog-APIs für Answering, Make Call usw. im benutzerdefinierten Client bereitzustellen.

Zugriffstoken aktualisieren

Ein Zugriffstoken hat eine Ablaufzeit. Sie müssen dieses Token aktualisieren, bevor es abläuft.

Entsprechend der Empfehlung:

- Drittanbieteranwendungen müssen das Zugriffstoken nach Ablauf von 75 % der Ablaufzeit für das Token aktualisieren.
- Für den Aufruf dieser API kann ein Browser erforderlich sein, der an Cisco Identity Server und Cisco Identity Provider umgeleitet wird.

Um das Zugriffstoken zu aktualisieren, verwenden Sie die folgende URL:
https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&fresh-token=<update-token-value>

Sie erhalten das neue Zugriffstoken, wie im Bild gezeigt.

Nun können Sie dieses neue Token wieder als Zugriffstoken verwenden, um eine Anfrage an den Finesse-Server zu senden.