Finesse Thirdparty Client Integration con SSO

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Obtener el token de acceso Actualizar token de acceso

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 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)

🕲 Sign In	× +		8	ĸ	
$\ \ \leftarrow \ \ \rightarrow \ \ G$	Not secure fs.stooges.icm/adfs/ls/7SAMLRequest=tVRNj9owEL3vr4h8BychLIIFkCioKtK2TYHtoTfjTHYtJXbqcZbtv68d6JZqUQ5IPXo8efM%28xpkjb%28qW	LTv7rLbwswO0QfDa1ApZf5OTziimOUpkijeAz	☆	Θ	:
	STC	DOGES ADFS			
	Sign in	n with your organizational account			
	1001005@steoges.icm				
		•			
	Sig	n in			
	Sign in	n using your operating system account			

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

\sim						- 0	
(+) → ୯ ଜ	A https://finesse70a.stooges.icm:8445/desktop/sso/authcode?state=aHR0cHM6Ly9maW5lc3NINzBiLnN0b29nZXMuaWNtOjg0NDUvZGVza3RvcC9zc28vdG9rZW4%2	ŝ	$\overline{\mathbf{A}}$	lin 🗉)	Ē	
UCCE-Administr	ation 🛅 Agent Desktop						
JSON Raw Data Headers							
Save Copy Collapse All Expand All 🛛 Filter JSON							
▼ token:	*ey3hb6ci013kxT1LC35#ki013xV1qLC31bmH013BHT4q03DUUhThjU2Tn0x8#Ab4Y35PUK8yYBpVLShq.qvmkTgbT6BF2aQCC+_hSHAy4HnDPShYck1DVLw1k4tsbj005TR9HLb5Ocr42qLVK_BQfmG3wC2NLkaeL6ePvxs17k0FamUMAeCqUC RSSfytVmahmkvjfPULAwA-NrfHYD9pS15H6d588kv- UX385jjVVM3Ypk01xFHLCTHV016g5g5C8ADUSKT71HHL61gV127VcK3MecKT7F5K4E12b40F8_aTP12fgCHeKXvj1n5Efd8IAL1kwcZFM8xghbshqLLn1jvC08C030Cq5S19T1yN25SmExL19dA3nzthd8W/26pbq25dkWtjqPG9FUp1s6cy2thK7wg Ta1ss4H0111bWjj5ekb4XKF2Ub4ZCdnzLs-3FfyRzC1djeHLxjmT128VBCS1BUH2gKKNu1jVUc3Vx6FqVYTL8L5VxMfgC86pee3t4V5n55PRyTB378ze1VH2_0F3FL03-NrTHXRVsNU1QnUmkruke-DoFi-G2bd-Q&wgN890-ia5kmhbdfs2	kw∂5is wraxca ≋pAfeH	Af9tv IeXinn PTyDT	iANKPIt isreU2Rb _SKeprr2	SENEXX9t _XNFguOY 7-UOgaet	1tBN/F btmrna xg46dL	
▼ refresh_token:	"eyohdocioliXxXIILC3jdHkloiDXVQLLC3bmkloiDXVIQLC3bmkloiD8VII4Q800LUhTMjuZIM».eZBKXdWpVWgSd0-6d9hx_A.rHxYD04gvzTlu3Fh3FeHWWlSdy02somW64Hkr3VCAd0LDR14Sg6FWyhoK3NLN3ClSztzZkLoqbeyYjpAz2KcF8ss5T4QWr_LsYgm r4sz1q05y2qefGgghzivyvSklxr1Az389F4531vf1hoptvdTvS8sgjewzy8Kr0xLcaiajtiz3Sxv2vQ00THKDCMXXPCyc2NvUhuzdozEpx3Lpj7H8VL7Rv189KmBeQ2BUyHzn11takimzIdW0ApExrTqQ55cv8Ubr1Efh146FETY_sux leH1448Hlgf=_QS51a80kcos8ankSU_BbuZP8dcsju5Ev28m8PqdAxYhp38a0ErUkmpkZejWQ8VETRdh_QPTVS7et8x0-msfpjmpHR-8f_a-Tajf8WaULsPGW4px0JUkmPL4Rv8MLMgHgMV9GzcZdP3RofmivIF.wb36nfmFn11vdssg5y8sXQ"	NN9UMn NYfk4yC	eQ9Pj pziFB	JUBEDXD3 3Y4A_wOq	Lyly9EMM Ty3WC_FC	V 3WFOC XXgv_7	
expires_in:	3600						

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.

Params Authorization	Headers (7) Body	Pre-request Script Tests Settings	
Headers © 6 hidden			
KEY		VALUE	DESCR
Authorization		Bearer	
Key		4Q0JDLUhTMjU2In0IB7C0fUGuSpSsBq6zgKLwg.X	Desc
Response		OwAE_xylyU9plybE2HQYOmPQZmWlxDFne_jrMbjo DUw-	
		NwZO7IIA2J_MdZ87YxK4OQxdXkbdaYJnDnLfpQYm uZ4mjAJmm0VIS98IbfEL2F7CTxo5iDo_DnV- eWIILQiY_H5YAY22- Tgd1nue5R6gKV0vo7qMZ3PpfFuUYMByBIsEsZ6PF PFITsxbLqmIYmtfv- 4Cg_4SqFYDa5vo2A_VRXK9WOjx9XhO-JCmoUhK- mRAR_88P_h5tNG9Ox8m9dI- G8aRMbd4iaXYxoVYjvVMHYUYOIJkcSqPrYq6NBmX K_Zb8_Nf0r- zdgwqC9v_qn8Vded0zLU6FX4O7aZMkJ0N_RgTGx1 c6OwlLgKxaENImOKQqM3Y0KQiVzIpsCibuDUoQFo Tmp12XDdrPfxW1d17yD6gu2Y83DWwWBUMpG1T MzwEiedQEIpCQM0YKvGfGSaWisSFUkxMQyN4op1 IJeAxapNCRuMMfuCC2MPPv0uuGpGZKJIFIU1L2oFi 9m8uKO2r-tqx9EOqUT6UPaQdtVo- xLDDSAJAPJEN1vc1rvX-Zm-F02BvHfv0VxSRjdp_A1- z1oxithmMKAiI51utdqg7yLGgJ3E4n3of4K6e8LIIr5e AJE5px2z9WITWIo_OwZq- IkiOInzLKS5OWYDOzVirVK46I8Fd8FD5-	

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

Launchpad GET https://finesse70a.stooges.ic	m/• + •••	No Environment 🔻 💿 🔅					
GET • https://finesse70a.stooges.icm/finesse/api/User/10	010005	Send v Save v					
Params Authorization Headers (7) Body Pre-request	Params Authorization Headers (7) Body Pre-request Script Tests Settings Cookies Code						
Headers 🐵 6 hidden							
KEY	VALUE	DESCRIPTION *** Bulk Edit Presets •					
Authorization	Bearer eyJhbGciOiJkaXliLCJjdHkiOiJKV1QiLCJlbmMiOiJBMTI4Q0JI						
Key	Value	Description					
Body Cookies Headers (12) Test Results		Status: 200 OK Time: 8 ms Size: 1.52 KB Save Response 👻					
Pretty Raw Preview Visualize XML * 1 xml version="1.0" encoding="UTF-8" standalone="yes";</td 2 <user> 3 <ddalogs>/finesse/api/User/1010005/Dialogs 4 <extension></extension> 5 <firstnome>Agent[/firstNome] 6 <lastname>1010005c/lastName> 7 <loginid>1010005c/lastName> 8 <loginid>1010005c/lastName> 9 <mediatype>1 10 <cpre>cpendingState> 11 <crele>Agent 12 <crele> 13 14 </crele> 15 <settings> 16 17 <uraphponincoming>REQUIRED_WITH_WRAP_UP_DATA 18 19 <state>LOGUV 19 <state>LOGUV</state></state></uraphponincoming></settings></crele></cpre></mediatype></loginid></loginid></lastname></firstnome></ddalogs></user>	<pre>>> gs> /wrapUpOnIncoming> pageTime></pre>	■ Q					
<pre>21</pre>		Activate Windows Go to System in Control Panel to activate Windows.					

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: <u>https://<fqdn>:8445/desktop/sso/token?cc_username=<agentid>&refresh-token=<update-token-value></u>

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.