

Configura popolamento automatico dell'ID utente nella pagina Accesso AD FS per UCCE SSO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come migliorare l'esperienza dell'utente finale con l'accesso Single Sign-On (SSO) UCCE (Unified Contact Center Enterprise). Questa impostazione può essere migliorata se l'utente non è obbligato a immettere il proprio ID di accesso per la seconda volta nella pagina di accesso del provider di identità (IdP).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Flusso di accesso UCCE SSO e AD FS
- HTTP (Hyper-Text Transfer Protocol)
- HTML (Hyper-Text Markup Language)
- Security Assertion Markup Language 2.0 (SAMLv2)
- Autorizzazione apertura 2.0 (OAuthv2)
- Familiarità con Windows PowerShell (PS)
- Familiarità con JavaScript (JS)

Componenti usati

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

- UCCE versione 11.5(1) e successive
- Finesse 11.5(1) e versioni successive
- Cisco Unified Intelligence Center (CUIC) versione 11.5(1) e successive.
- Microsoft Active Directory (AD) - AD installato in Windows Server

- AD FS 2.0/3.0
- Windows Server 2012 R2

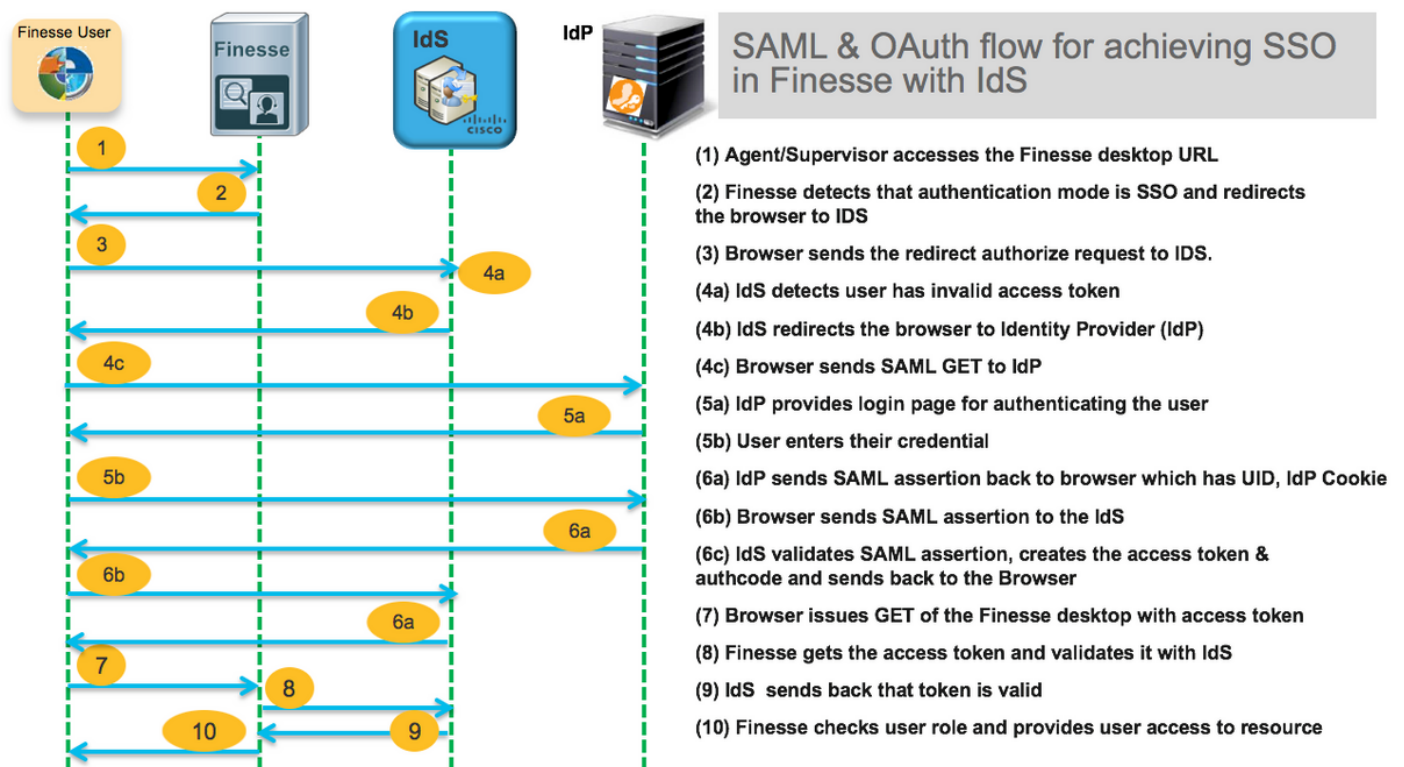
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Premesse

In un accesso UCCE SSO, l'utente deve immettere il proprio ID di accesso due volte: prima nella pagina di accesso dell'applicazione UCCE (Finesse, CUIC, ad esempio) e seconda nella pagina di accesso IdP (se viene utilizzato un metodo di autenticazione Forms). Nell'esempio di questo documento, come provider di identità viene utilizzato Active Directory Federation Service (ADFS).

Quando l'SSO è abilitato in UCCE, dopo aver immesso l'ID di accesso e aver premuto il pulsante Invia/Accedi in CUIC/Finesse, l'ID di accesso immesso viene memorizzato nel cookie `cc_username` e conservato per i reindirizzamenti a Identity Server (IdS) e quindi all'IdP. È possibile utilizzare questo cookie nella pagina di accesso IdP per popolare automaticamente l'ID di accesso.

Di seguito è riportato un esempio di diagramma di flusso HTTP/SAML in cui l'utente finale è un agente Finesse e l'applicazione UCCE è un server Finesse.



Questo è un esempio delle intestazioni di richiesta HTTP del **passaggio 4c** inviate dal browser Web dell'utente finale ad AD FS (IdP).

```
Request URL: https://dc01.omezol.lab/adfs/ls/?SAMLRequest=tZTBjtowEIbv%2BxSR...
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
```

Connection: keep-alive
Cookie: cc_username=agent1%40omozol.1ab
Host: dc01.omozol.1ab
Pragma: no-cache
Referer: https://fns01p.omozol.1ab/desktop/container/landing.jsp?locale=en_US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36

Configurazione

Se l'IdP è AD FS 3.0, la configurazione viene ottenuta modificando il file **onload.js**, inserito da AD FS nella pagina HTML restituita all'utente in risposta alla richiesta di **https://<FQDN di AD FS>/adfs/ls/**.

Passaggio 1. Per modificare il file **onload.js**, esportare il file nel file system tramite il cmdlet di PowerShell:

```
PS C:\> Export-AdfsWebTheme -Name default -DirectoryPath c:\temp\adfs\
```

Il file **onload.js** viene posizionato nella seguente directory:

```
C:\temp\adfs\script
```

Passaggio 2. A seconda del formato di accesso, aggiungere il frammento di codice JS appropriato in qualsiasi punto del file al di fuori della logica o delle strutture di codice già presenti. Per facilitare l'operazione, aggiungerlo alla fine del file.

Per impostazione predefinita, la pagina di accesso presentata agli utenti SSO da ADFS in Windows Server 2012 R2 richiede un nome utente che sia un modulo [userPrincipalName](#) (UPN). Si tratta di un formato simile alla posta elettronica, ad esempio **user@cisco.com**. In un singolo contact center di dominio è possibile modificare la pagina di accesso di AD FS in modo da consentire un semplice sAMAccountNameUser ID ([UID](#)) che non include un nome di dominio come parte del nome utente.

Se è necessario immettere un nome utente UPN nella pagina di accesso di AD FS, utilizzare questo frammento di codice:

```
// Get cc_username as login ID from HTTP Cookie header
if (document.cookie) {
// If the position of cc_username in the cookie is the first position, 0... if
(document.cookie.indexOf('cc_username') == 0) {
// Split the cookie into an array with the delimiter being '=' var cookies =
document.cookie.split('=');
// If the first element of the array is cc_username then...
if (cookies[0] == 'cc_username') {
// ...the second element will be the actual username and we should save that. var cc_login_name
= cookies[1]; } // Customize Login page: add domain if needed as AD FS by default require login
ID in UPN form
// If the parsed login is not null, do the following logic if (cc_login_name != null) {
// If %40 (encoded '=') does not exist in the login name... if (cc_login_name.indexOf('%40') ==
-1) {
// ...then add '@domain.com' to ensure a UPN format is input var userNameValue = cc_login_name +
'@' + 'domain.com';
// Populate the UPN into the userNameInput of the page, and put the focus
// on the password. document.getElementById("userNameInput").value = userNameValue;
```

```
document.getElementById("passwordInput").focus(); } else {
// Otherwise, if %40 does exist in the username, replace it with the @ sign
// and populate the UPN into the userNameInput of the page, and put the
// focus on the password. var userNameValue = cc_login_name.replace('%40', '@');
document.getElementById("userNameInput").value = userNameValue;
document.getElementById("passwordInput").focus(); } } }
```

In questa riga, **domain.com** deve essere modificato in modo da corrispondere al dominio degli agenti UCCE se viene utilizzato un UPN come UID di accesso.

```
var userNameValue = cc_login_name + '@' + 'domain.com';
```

Nota: ADFS utilizza un account di accesso UPN per impostazione predefinita. Fare riferimento alla [guida alle funzionalità UCCE](#), capitolo **Single Sign-On, Personalizzare facoltativamente la pagina di accesso ad AD FS in Windows Server 2012 R2 per consentire l'ID utente** nella sezione relativa alla configurazione della pagina di accesso ad AD FS per consentire l'accesso a sAMAccountName.

Se nella pagina di accesso di ADFS è necessario immettere un nome utente sAMAccountName (UID senza dominio), utilizzare questo frammento di codice:

```
// Get cc_username as login ID from HTTP Cookie header
if (document.cookie) {
// If the position of cc_username in the cookie is the first position, 0... if
(document.cookie.indexOf('cc_username') == 0) {
// Split the cookie into an array with the delimiter being '=' var cookies =
document.cookie.split('=');
// If the first element of the array is cc_username then...
if (cookies[0] == 'cc_username') {
// ...the second element will be the actual username and we should save that. var cc_login_name
= cookies[1]; } // Customize Login page: remove domain if needed to use login ID in sAMAccount
form
// If the parsed login is not null, do the following logic if (cc_login_name != null) {
// If %40 (encoded '=') DOES exist in the login name... if (cc_login_name.indexOf('%40') != -1)
{
// ...then split the login into an array about the @ sign and only keep the username.
var domainLogin = cc_login_name.replace('%40', '@')
var noDomainLogin = domainLogin.split('@'); var userNameValue = noDomainLogin[0];
// Populate the sAMAccountName into the userNameInput of the page, and put the focus
// on the password. document.getElementById("userNameInput").value = userNameValue;
document.getElementById("passwordInput").focus(); } else {
// Otherwise, if %40 does not exist in the username, there is no "@domain",
// so populate the sAMAccountName into the userNameInput of the page,
// and put the focus on the password. document.getElementById("userNameInput").value =
cc_login_name; document.getElementById("passwordInput").focus(); } } }
```

Nota: i simboli // nel codice indicano i commenti. Se lo si desidera, è possibile rimuovere tali linee. Il loro scopo è quello di aiutare a comprendere il codice Javascript.

Passaggio 3. Salvare **onload.js** e ricaricarlo in un nuovo tema Web ADFS con i seguenti comandi di PowerShell:

Creare un tema ADFS personalizzato con il modello dal tema predefinito:

```
PS C:\> Impostazione predefinita di New-AdfsWebTheme -Name personalizzato -SourceName
```

Impostare il tema ADFS personalizzato come attivo:

PS C:\> Impostazione-AdfsWebConfig -ActiveThemeName personalizzato

Caricare il file `onload.js` modificato nel tema personalizzato:

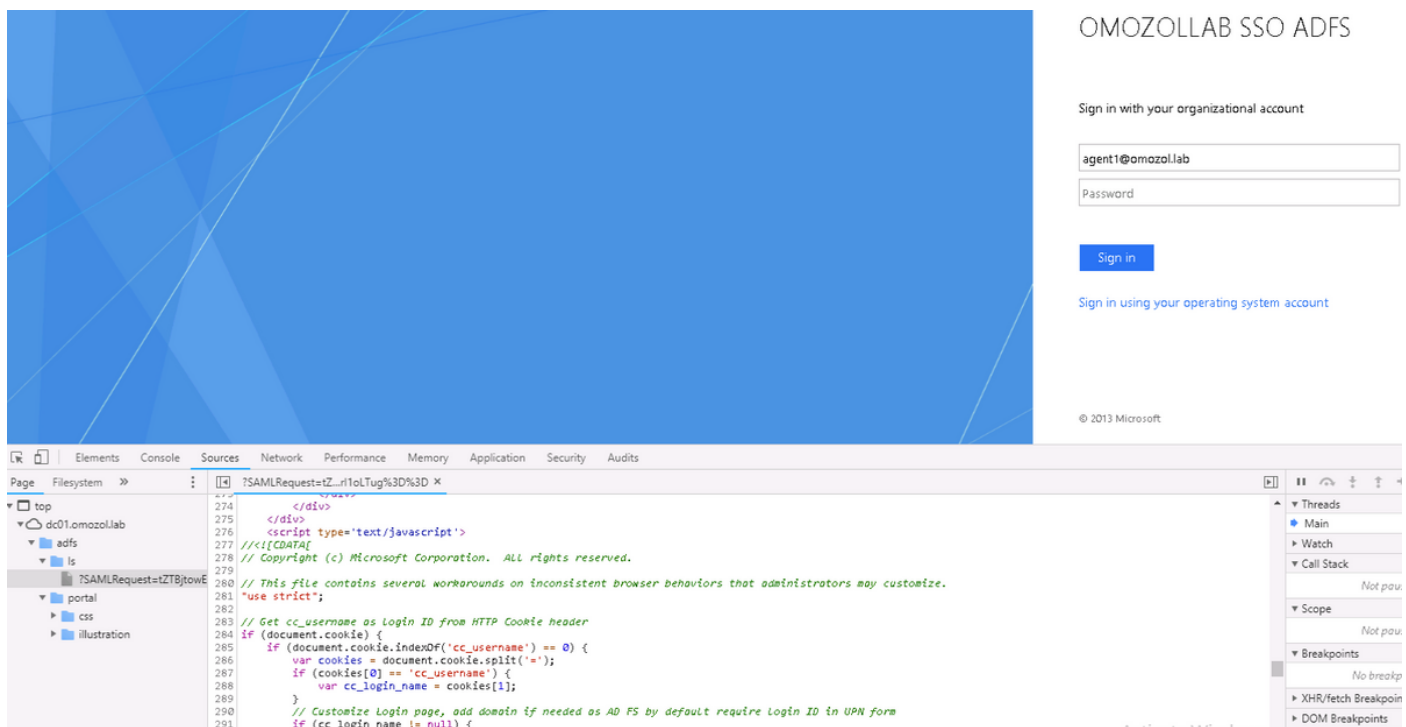
PS C:\> Set-AdfsWebTheme -TargetName personalizzato -AdditionalFileResource
@{Uri='/adfs/portal/script/onload.js';path="c:\temp\adfs\script\onload.js"}

Nota: Non è necessario riavviare ADFS. Il tema attivo viene modificato automaticamente.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Accedere a Finesse o CUIC con un account abilitato a SSO con `sAMAccountName` o UPN come ID di accesso (dipende dalla configurazione di AD FS) e osservare che nella pagina di accesso di AD FS l'ID utente viene automaticamente compilato con lo stato attivo nel campo della richiesta della password. Per continuare l'accesso è necessario immettere solo la password.



The image shows a screenshot of a web browser displaying the OMOZOLLAB SSO ADFS login page. The page has a blue background with a geometric pattern. On the right side, there is a login form with the title "OMOZOLLAB SSO ADFS". Below the title, it says "Sign in with your organizational account". There are two input fields: one for the username, containing "agent1@omozol.lab", and one for the password. A blue "Sign in" button is below the fields. Below the button, it says "Sign in using your operating system account". At the bottom right, there is a copyright notice: "© 2013 Microsoft".

The bottom part of the image shows the browser's developer tools, specifically the "Sources" panel. The file `?SAMLRequest=tZr1toLTug%3D%3D` is selected. The code in the `onload.js` file is visible, showing a JavaScript function that checks for a cookie named `cc_username` and sets the `cc_login_name` property of the `document.cookie` object. The code is as follows:

```
274 </div>
275 </div>
276 <script type="text/javascript">
277 //
278 // Copyright (c) Microsoft Corporation. All rights reserved.
279 // This file contains several workarounds on inconsistent browser behaviors that administrators may customize.
280 "use strict";
281
282 // Get cc_username as Login ID from HTTP Cookie header
283 if (document.cookie) {
284   if (document.cookie.indexOf('cc_username') == 0) {
285     var cookies = document.cookie.split('=');
286     if (cookies[0] == 'cc_username') {
287       var cc_login_name = cookies[1];
288     }
289     // Customize Login page, add domain if needed as AD FS by default require Login ID in UPN form
290     if (cc_login_name != null) {</pre></div><div data-bbox="57 727 392 752" data-label="Section-Header"><h2>Risoluzione dei problemi</h2></div><div data-bbox="57 772 863 808" data-label="Text"><p>Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.</p></div><div data-bbox="57 823 949 875" data-label="Text"><p>In caso di problemi, gli strumenti di sviluppo del browser Web vengono utilizzati per verificare se le modifiche del file <code>onload.js</code> vengono inserite nella pagina HTML restituita e se vengono rilevati errori nella console del browser Web.</p></div><div data-bbox="57 897 353 921" data-label="Section-Header"><h2>Informazioni correlate</h2></div>
```

- [Strumenti di sviluppo di Firefox](#)
- [Strumenti Chrome Developer](#)
- [Strumenti di sviluppo di Internet Explorer \(F12\)](#)
- [Nome-Account-SAM](#)
- [NomePrincipioUtente](#)
- [UID](#)
- [Guide alle funzioni di Cisco Unified Contact Center Enterprise](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)