Konfigurieren der automatischen Einfügefunktion auf der AD FS-Anmeldeseite für UCCE SSO

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Endbenutzererfahrung bei der Anmeldung bei Unified Contact Center Enterprise (UCCE) Single Sign-On (SSO) verbessert werden kann. Dies kann verbessert werden, wenn der Benutzer nicht gezwungen ist, seine Anmelde-ID ein zweites Mal auf der Anmeldeseite des Identitätsanbieters (IdP) einzugeben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- UCCE SSO-Login-Flow und AD-FS
- Hyper-Text Transfer Protocol (HTTP)
- Markup-Sprache für Hyper-Text (HTML)
- Security Assertion Markup Language 2.0 (SAMLv2)
- Open Authorization 2.0 (OAuthv2)
- Vertrautheit mit Windows PowerShell (PS)
- Vertrautheit mit JavaScript (JS)

Verwendete Komponenten

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

- UCCE 11.5(1) und höher
- Finesse 11.5(1) und höher
- Cisco Unified Intelligence Center (CUIC) 11.5(1) und höher
- Microsoft Active Directory (AD) - AD installiert auf Windows Server

- AD FS 2.0/3.0
- Windows Server 2012 R2

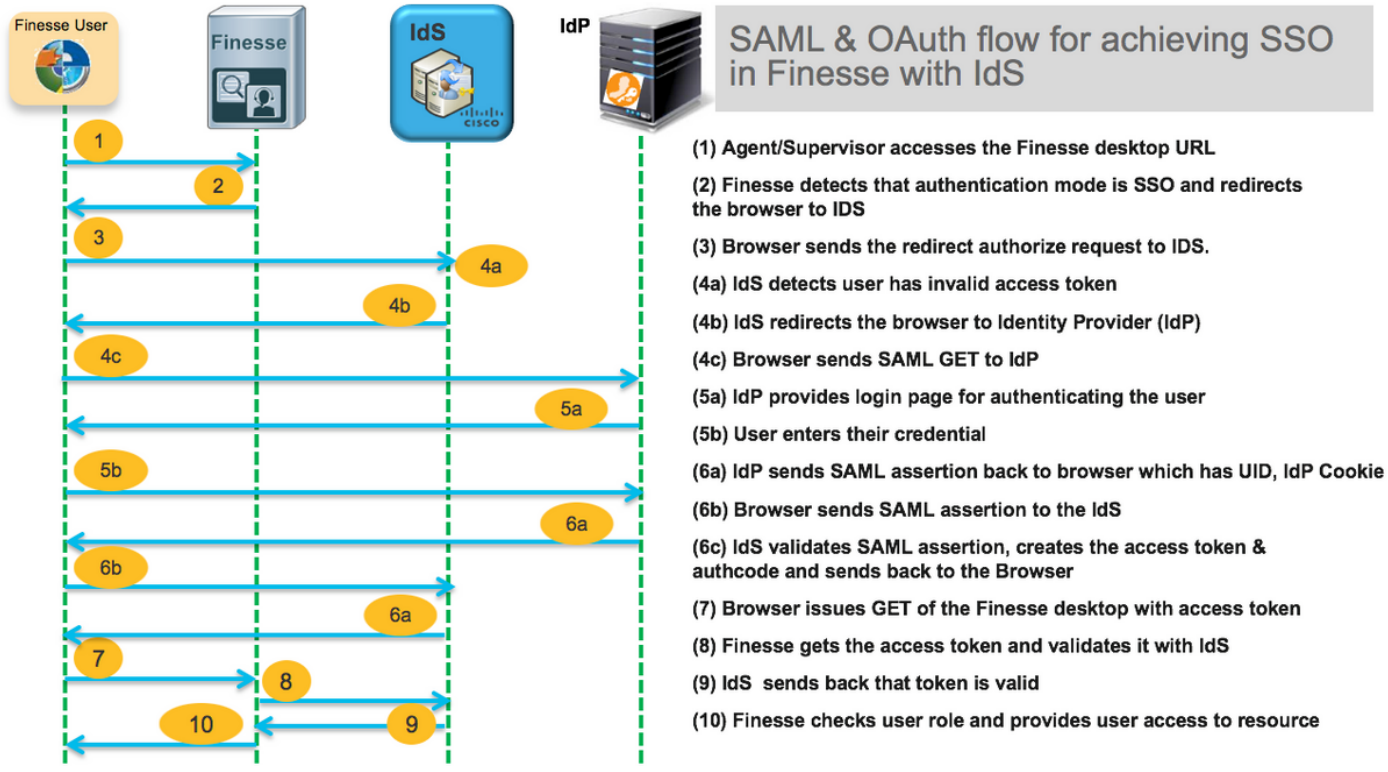
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

Hintergrundinformationen

Bei einer UCCE-SSO-Anmeldung muss der Benutzer seine Anmelde-ID zweimal eingeben: zuerst auf der Anmeldeseite der UCCE-Anwendung (Finesse, CUIC, z. B.) und zweitens auf der Anmeldeseite des IDP (wenn eine Formularauthentifizierungsmethode verwendet wird). Im Beispiel in diesem Dokument wird Active Directory Federation Service (AD FS) als IdP verwendet.

Wenn in UCCE SSO aktiviert ist, wird nach Eingabe der Anmelde-ID und Betätigung der Schaltfläche Submit/Login auf CUIC/Finesse die eingegebene Anmelde-ID im Cookie **cc_username** gespeichert und für die Umleitung zum Identitätsserver (IdS) und dann zum IDP beibehalten. Es ist möglich, dieses Cookie auf der IDP-Anmeldeseite zu verwenden, um automatisch die Anmelde-ID einzugeben.

Im folgenden Beispiel wird ein HTTP/SAML-Flussdiagramm dargestellt, in dem der Endbenutzer ein Finesse-Agent und die UCCE-Anwendung ein Finesse-Server ist.



Dies ist ein Beispiel für die **Schritt 4c**-HTTP-Anforderungs-Header, die vom Webbrowser des Endbenutzers an AD FS (die IDP) gesendet werden.

```
Request URL: https://dc01.omozol.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.lab
Host: dc01.omozol.lab
Pragma: no-cache
Referer: https://fns01p.omozol.lab/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
```

Konfigurieren

Mit AD FS 3.0 als IdP wird die Konfiguration durch die Änderung der **onload.js**-Datei erreicht, die AD FS in die HTML-Seite einfügt, die dem Benutzer als Antwort auf die Anforderung an **https://<AD FS FQDN>/adfs/ls/**zurückgegeben wird.

Schritt 1: Um die Datei **onload.js** zu verändern, exportieren Sie die Datei über den PowerShell c→ in das Dateisystem:

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

Die Datei **onload.js** wird in diesem Verzeichnis gespeichert:

C:\temp\adfs\script

Schritt 2: Fügen Sie je nach Anmeldungsformat den richtigen JS-Codeausschnitt an einem beliebigen Ort in der Datei außerhalb der bereits vorhandenen Codestrukturen/Logik hinzu. Fügen Sie es einfach zum unteren Teil der Datei hinzu.

Standardmäßig erfordert die Anmeldeseite, die SSO-Benutzern von AD FS in Windows Server 2012 R2 präsentiert wird, einen Benutzernamen, der ein UserPrincipleName (UPN)-Formular ist. Dies ist ein E-Mail-ähnliches Format, z. B. **user@cisco.com**. In einem einzigen Domain Contact Center kann die AD FS-Anmeldeseite so geändert werden, dass eine einfache sAMAccountNameUser ID (UID) zugelassen wird, die keinen Domänennamen als Teil des Benutzernamens enthält.

Wenn ein UPN-Benutzername auf der AD FS-Anmeldeseite eingegeben werden muss, verwenden Sie diesen Codeausschnitt:

```
// 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 delimitor 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 dieser Zeile muss **domain.com** so geändert werden, dass sie der Domäne der UCCE-Agenten entspricht, wenn als Anmelde-UID ein UPN verwendet wird.

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

> **Hinweis**: AD FS verwendet standardmäßig eine UPN-Anmeldung. Im UCCE-Funktionsleitfaden, **Einmalanmeldung, optionales Anpassen der AD FS-Anmeldeseite in Windows Server 2012 R2 an Zulassen der Benutzer-ID** Abschnitt finden Sie Informationen zur Konfiguration der AD FS-Anmeldeseite für die Anmeldung bei sAMAccountName.

Wenn auf der AD FS-Anmeldeseite ein sAMAccountName (UID ohne Domäne)-Benutzername eingegeben werden soll, verwenden Sie diesen Codeausschnitt:

```
// 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 delimitor 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(); } } } }
```

> **Hinweis**: Die //Symbole im Code geben Kommentare an. Diese Posten können bei Bedarf entfernt werden. Ihr Zweck ist es, das Verständnis des Javascript-Codes zu unterstützen.

Schritt 3: Speichern Sie **onload.js** und laden Sie es mit den folgenden PowerShell-Befehlen in ein neues AD FS-Webdesign:

Erstellen Sie ein benutzerdefiniertes AD FS-Design mit der Vorlage aus dem Standarddesign:

PS C:\> New-AdfsWebTheme -Name custom -SourceName default

Legen Sie das benutzerdefinierte AD FS-Design als aktiv fest:

PS C:\> Set-AdfsWebConfig -ActiveThemeName benutzerdefiniert

Laden Sie die geänderte Datei **onload.js** in das benutzerdefinierte Design:

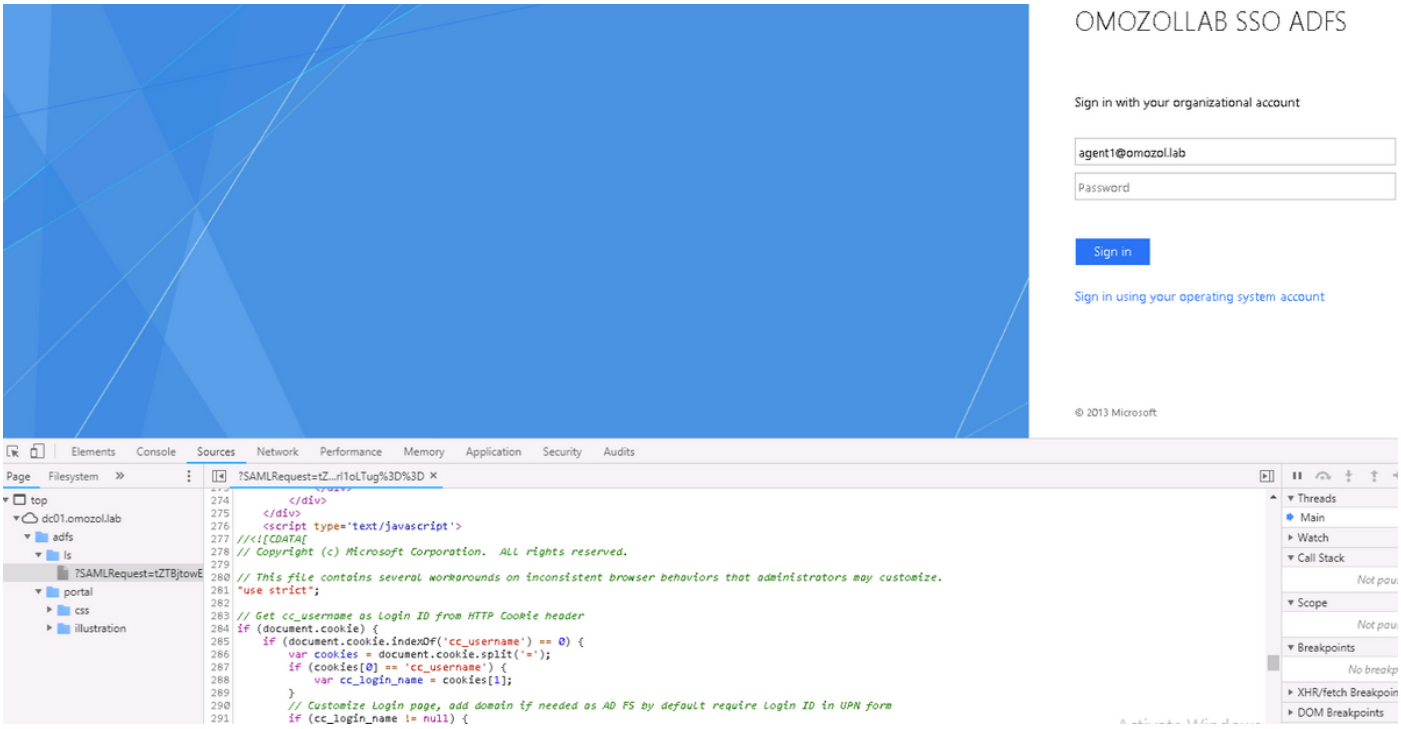
PS C:\> Set-AdfsWebTheme -TargetName custom -AdditionalFileResource @{Uri='/adfs/portal/script/onload.js';path="c:\temp\adfs\script\onload.js"}

> **Hinweis**: AD FS muss nicht neu gestartet werden. Das aktive Design wird automatisch geändert.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Melden Sie sich bei Finesse oder CUIC mit einem SSO-aktivierten Konto mit sAMAccountName oder UPN als Anmelde-ID an (abhängig von der AD FS-Konfiguration), und stellen Sie fest, dass die Benutzer-ID auf der Anmeldeseite von AD FS automatisch mit dem Fokus auf das Feld für die Kennwortaufforderung versehen wird. Nur das Passwort muss eingegeben werden, damit die Anmeldung fortgeführt werden kann.



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Bei Problemen werden die Webbrowser-Entwicklertools verwendet, um zu überprüfen, ob die Änderungen von **onload.js** in die zurückgegebene HTML-Seite eingespeist werden und ob Fehler in der Webbrowser-**Konsole** beobachtet werden.

Zugehörige Informationen

- Firefox-Entwicklertools
- Chrome Developer-Tools
- Internet Explorer (F12) Entwicklertools
- SAM-Kontoname
- userPrincipleName
- UID
- Cisco Unified Contact Center Enterprise - Funktionsleitfäden
- Technischer Support und Dokumentation - Cisco Systems