Troubleshooting SSO en el administrador de las Comunicaciones unificadas de Cisco

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Configurar](#)
[Verificación](#)
[Troubleshooting](#)
[Flujo del login en el SSO](#)
[Decodificar SAML la respuesta](#)
[Registros y comandos CLI](#)
[Problemas comunes](#)
[Defectos conocidos](#)

Introducción

Este documento describe cómo configurar solo Muestra-en (SSO) en el administrador de las Comunicaciones unificadas de Cisco (CUCM).

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de los temas:

- CUCM
- Servicios de la federación del Active Directory (ADFS)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM 11.5.1.13900-52 (11.5.1SU2)
- ADFS 2.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Refiera a la configuración de la sola muestra encendido en CUCM.

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-version-105/118770-configure-cucm-00.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html

SAML Guía de despliegue SSO para las aplicaciones de Comunicaciones unificadas de Cisco, versión 11.5(1).

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/11_5_1/CUCM_BK_S12EF288_00_saml-sso-deployment-guide--1151.html

SAML RFC 6596.

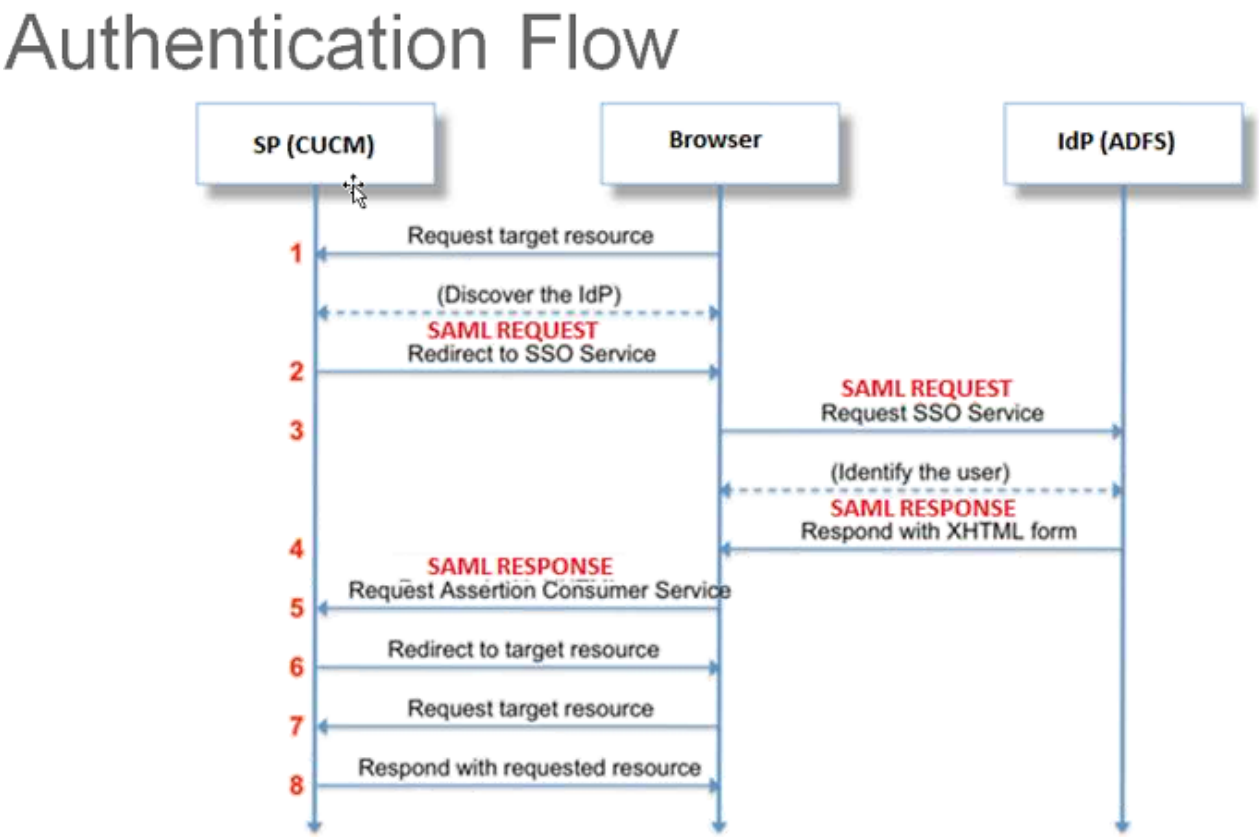
- https://tools.ietf.org/html/rfc6595

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Flujo del login en el SSO



Decodificar SAML la respuesta

Usando los plug-in en Notepad++

Instale estos plug-in:

```
Notepad++ Plugin -> MIME Tools--SAML DECODE

Notepad++ Plugin -> XML Tools -> Pretty Print(XML only - with line breaks)
```

En los registros SSO busque para la cadena “authentication.SAMLAuthenticator - SAML la respuesta está:: ” que contiene la respuesta codificada.

Utilice este plug-in o SAML en línea decodifica para conseguir la respuesta XML. La respuesta se puede ajustar en un formato legible con la impresión bonita instalada uso plug-in.

En la versión más reciente de la respuesta CUCM SAML está en el formato XML que puede ser encontrado buscando “SPACSUtils.getResponse: response=<samlp conseguido:

Xmlns de la respuesta: el samlp= “y entonces imprime con el uso de la impresión bonita plug-in.

Fiddler del uso:

Esta utilidad se puede utilizar para conseguir el tráfico en tiempo real y para decodificarlo. Aquí está la guía para lo mismo; https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/.

SAML petición:

```
ID="s24c2d07a125028bfffa7757ea85ab39462ae7751f" Version="2.0" IssueInstant="2017-07-
15T11:48:26Z" Destination="https://win-91uhcn8tt3l.emeacucm.com/adfs/ls/" ForceAuthn="false"
IsPassive="false" AssertionConsumerServiceIndex="0">
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">cucmsso.emeacucm.com</saml:Issuer>
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
SPNameQualifier="cucmsso.emeacucm.com" AllowCreate="true"/>
</samlp:AuthnRequest>
```

SAML respuesta (unencrypted):

```
<samlp:Response ID="_53c5877a-0fff-4420-a929-1e94ce33120a" Version="2.0" IssueInstant="2017-07-
01T16:50:59.105Z"
Destination="https://cucmsso.emeacucm.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacucm.com"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://win-
91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
```

```
</samlp:Status>
<Assertion ID="_0523022c-1e9e-473d-9914-6a93133ccfc7" IssueInstant="2017-07-01T16:50:59.104Z"
Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
<Issuer>http://win-91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#_0523022c-1e9e-473d-9914-6a93133ccfc7">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<ds:DigestValue>9OvwrpJVeOQsDBNghwvkLIdnf3bc7aW82qmo7Zdm/Z4=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>VbWcKUwvwiNDhUg5AkdqSzQOmP0qs5OT2VT+u1LivWx7h9U8/plyhK3kJMUuxoG/HXPQJgVQaMOwN
q/Paz7Vg2uGNFigA2AFQsKgGo9hAA4etfucIQlMmkeVg+ocvGY+8IzaNVfaUXSU5laN6zriTArxXwxCK0+thgRgQ8/46vm91
Skq2Fa5Wt5uRPJ3F4eZPOEPdtKxOmUuHi3Q2pXTw4ywZ/y89xPfSixNQEmr10hpPAdyfPsIFGdNJJwWJV4WjNmfcAqClzaG8
pB74e5EawLmwrfV3/i8QfR1DyU5yCCpxj02rgE6Wi/Ew/X/l6qSCzOZEpl7D8LwAn74KijO+Q==</ds:SignatureValue>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC5DCCAcygAwIBAgIQZLLskb6vppxCiYP8xOahQDANBgkqhkiG9w0BAQsFADAuMSwwKgYDVQQD
EyNBREZTIFNpZ25pbmcgLSBXSU4ySzEyLnJrb3R1bGFrLmxhYjAeFw0xNTA2MjIxOTE2NDRaFw0xNjA2MjExOTE2NDRaMC4x
LDAqBgNVBAMTI0FERlMgU2lnbmluZyAtIFdJTjJLMTIucmtvdHVsYWsubGFiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApEe09jnZXEcEC7s1VJ7fMXAHPXj7jgOOcs9/Lzxrx4c68tePGItrEYnzW9vLe0Dj8OJET/Rd6LsKvuMQHfcGYqA+
XugZyHBrpc18wlhSmMfvfa0jN0Qc0lf+a3j72xfI9+hLtsqSPSnMp9qby3qSiQutP3/ZyXRN/TnzYDEmzur2MA+GP7vdeVOF
XlpENrRfaINzc8INqGRJ+1jZrm+vLFvX7YwIL6aOpmjaxcPoxDcjgEGMYO/TaoP3eXutX4FuJV5R9oAvbqD2F+73XrvP4e/w
Hi5aNrHrgiCnuBJTIxHwRGSoichdpZlvSB15v8DFaQSVAiEMPj1vP/4rMkacNQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA5
uJZI0K1Xa40H3s5MAo1SG00bnn6+sG14eGIBe7BugZMw/FTgKd3VRsmlVuUWCabO9EgyfgdI1nYZCciyFhts4W9Y4BgTH0j4
+VnEWiQg7dMqp2M5lykZWPS6vV2uD010sX5V0avyYi3Qr88vISCtniIZpl24c3TqTn/5j+H7LLRVI/ZU38Oa17wuSNPyed6/
N4BfWhhCRZAdJgijapRG+JIBeoA1vNqN7bgFQMe3wJzSlLkTIoERWYgJGBciMPS3H9nkQlP2tGvmn0uwacWPglWR/LJG3VYo
isFm/oliNUF1DONK7QYiDzIE+Ym+vzYgIDS7MT+ZQ3XwHg0Jxtr8</ds:X509Certificate>
</ds:X509Data>
</KeyInfo>
</ds:Signature>
<Subject>
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http:///win-
91uhcn8tt3l.emeacucm.com/com/adfs/services/trust"
SPNameQualifier="cucmsso.emeacucm.com">CHANDMIS\chandmis</NameID>
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<SubjectConfirmationData InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f"
NotOnOrAfter="2017-07-01T16:55:59.105Z"
Recipient="https://cucmsso.emeacucm.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacucm.com" />
</SubjectConfirmation>
</Subject>
<Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z">
<AudienceRestriction>
<Audience>ccucmsso.emeacucm.com</Audience>
</AudienceRestriction>
</Conditions>
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>chandmis</AttributeValue>
</Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2017-07-01T16:50:59.052Z" SessionIndex="_0523022c-1e9e-473d-9914-
6a93133ccfc7">
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnCo
ntextClassRef>
</AuthnContext>
</AuthnStatement>
```

```
</Assertion>
```

</samlp: Response>

```
Version="2.0"  :- The version of SAML being used.

InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f" :- The id for SAML Request to which
this reponse corresponds to

samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success :- Status Code of SAML
reponse. In this case it is Success.

<Issuer>http://win-91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer> :- IdP FQDN

SPNameQualifier="cucmsso.emeacucm.com" :- Service Provider(CUCM) FQDN

Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z :- Time
range for which the session will be valid.

<AttributeValue>chandmis</AttributeValue> :- UserID entered during the login
```

En caso de que la respuesta de SAML entonces se cifre usted no podrá ver la Información completa y tuvo que inhabilitar el cifrado en la detección de intrusos y la prevención (IDP) para ver la respuesta completa. Los detalles del certificado usados para el cifrado están bajo "ds:X509IssuerSerial" de la respuesta de SAML.

Registros y comandos CLI

Comandos CLI:

neutralización del sso del utils

Este comando inhabilita ambo (OpenAM SSO o SAML SSO) la autenticación basada. Este listas de comandos las aplicaciones de Web para las cuales se habilita el SSO. Ingrese **sí** cuando está indicado para inhabilitar el SSO para la aplicación especificada. Usted debe funcionar con este comando en ambos los Nodos si en un cluster. El SSO puede también ser inhabilitado del Interfaz gráfica del usuario (GUI) y seleccionar el botón de la **neutralización**, bajo el SSO específico en la administración del Cisco Unity Connection.

Sintaxis del comando
neutralización del sso del utils

estatus del sso del utils

Este comando visualiza el estatus y los parámetros de la configuración de SAML SSO. Ayuda a verificar el estatus SSO, habilitado o inhabilitado, en cada nodo individualmente.

Sintaxis del comando
estatus del sso del utils

permiso del sso del utils

Este comando devuelve un mensaje de texto informativo que indique que el administrador pueda habilitar la característica SSO solamente del GUI. OpenAM basó el SSO y el SSO SAML basado no se puede habilitar con este comando.

Sintaxis del comando
permiso del sso del utils

permiso del sso recuperación-URL del utils

Este comando habilita el modo de la recuperación URL SSO. También verifica que este URL trabaje con éxito. Usted debe funcionar con este comando en ambos los Nodos si en un cluster.

Sintaxis del comando
permiso del sso recuperación-URL del utils

neutralización del sso recuperación-URL del utils

Este comando inhabilita el modo de la recuperación URL SSO en ese nodo. Usted debe funcionar con este comando en ambos los Nodos si en un cluster.

Sintaxis de los comandos
neutralización del sso recuperación-URL del utils

fije el <trace-level> llano del samltrace

Este comando habilita las trazas y los niveles de traza específicos que pueden localizar cualquier error, debug, información, advertencia o fatal. Usted debe funcionar con este comando en ambos los Nodos si en un cluster.

Sintaxis de los comandos
fije el <trace-level> llano del samltrace

muestre el samltrace llano

Este comando visualiza el nivel del registro fijado para SAML SSO. Usted debe funcionar con este comando en ambos los Nodos si en un cluster.

Sintaxis de los comandos
muestre el samltrace llano

Trazas a mirar a la hora del Troubleshooting:

Los registros SSO no se fijan al nivel detallado por abandono.

La primera ejecución el **debug del nivel del samltrace del** comando set para fijar el registro nivela para hacer el debug de, reproduce el problema y la recogida este conjunto de los registros.

De RTMT:

Cisco Tomcat

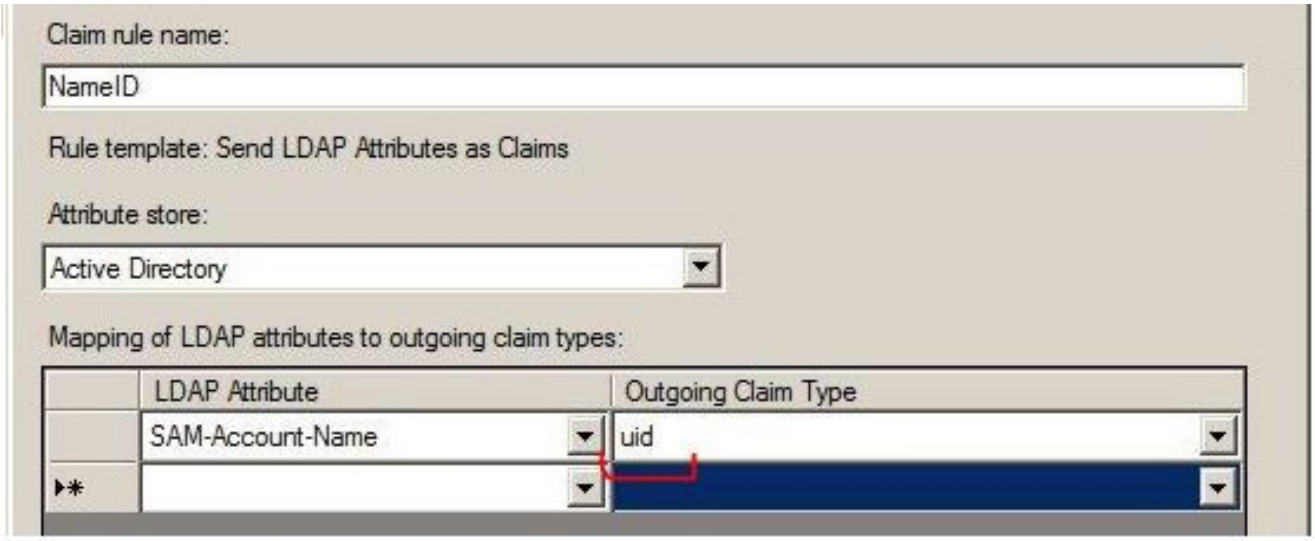
Seguridad de Cisco Tomcat

Cisco SSO

Problemas comunes

Valor incorrecto para Indentifier único (UID):

Debe exactamente ser UID y si no es el caso, CUCM no puede entender eso.



Regla incorrecta de la demanda o directiva incorrecta de NameID:

No hay nombre de usuario y contraseña muy probablemente pronto para arriba en este escenario.

No habrá ninguna aserción válida en la respuesta de SAML y el código de estado estará como:

```
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"/>
```

Verifique que la regla de la demanda esté definida correctamente en el lado IDP.

Diferencia en caso de que/nombre definido en la regla de la demanda:

CUCM FQDN en la regla de la demanda debe hacer juego exactamente con la especificada en el servidor real.

Usted puede comparar la entrada en el archivo del xml de los meta datos de IDP con el que está en CUCM funcionando con los **detalles del etho de la red del cluster**/de la **demostración de la red**

de la demostración ordena en el CLI de CUCM.

Hora incorrecta:

El NTP entre CUCM e IDP tiene una diferencia mayor que los 3 segundos dados un plazo en el Guía de despliegue.

Firmante de la aserción no confiado en:

A la hora del intercambio de los meta datos entre IDP y CUCM (proveedor de servicio).

Se intercambian los Certificados y si hay cualquier revocación del certificado hecha, los meta datos se deben intercambiar otra vez.

Configuración DNS Misconfiguration/No

El DNS es el requisito principal para que el SSO trabaje. Funcione con el **detalle del etho de la red de la demostración**, **utils diagnostican la prueba** en el CLI para verificar DNS/Domain se configura correctamente.

Defectos conocidos

CSCuj66703

El certificado de firma ADFS renueva y agrega dos certs de firma a las respuestas IDP de nuevo a CUCM (SP) le hace así ejecutarse en el defecto. Usted tiene que borrar el certificado de firma que no se requiere

CSCvf63462

Cuando usted navega a la página de SAML SSO de CCM Admin le indican con “los servidores siguientes fallados durante la tentativa de conseguir el estatus SSO” seguido por el Nombre del nodo.

CSCvf96778

El SSO basado CTI falla al definir el servidor CUCM como dirección IP en CCMAdmin//System/Sever.