

# Solución de problemas de SSO en Cisco Unified Communications Manager

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Flujo de inicio de sesión en SSO](#)

[Decodificación de la respuesta SAML](#)

[Registros y comandos CLI](#)

[Problemas comunes](#)

[Defectos conocidos](#)

## Introducción

Este documento describe cómo configurar el inicio de sesión único (SSO) en Cisco Unified Communications Manager (CUCM).

## Prerequisites

### Requirements

Cisco recomienda que conozca los temas siguientes:

- CUCM
- Servicios de federación de 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.

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. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

Consulte Configuración del inicio de sesión único 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>

Guía de implementación de SAML SSO para aplicaciones de Cisco Unified Communications, 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-ss0-deployment-guide--1151.html](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-ss0-deployment-guide--1151.html)

SAML RFC 6596.

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

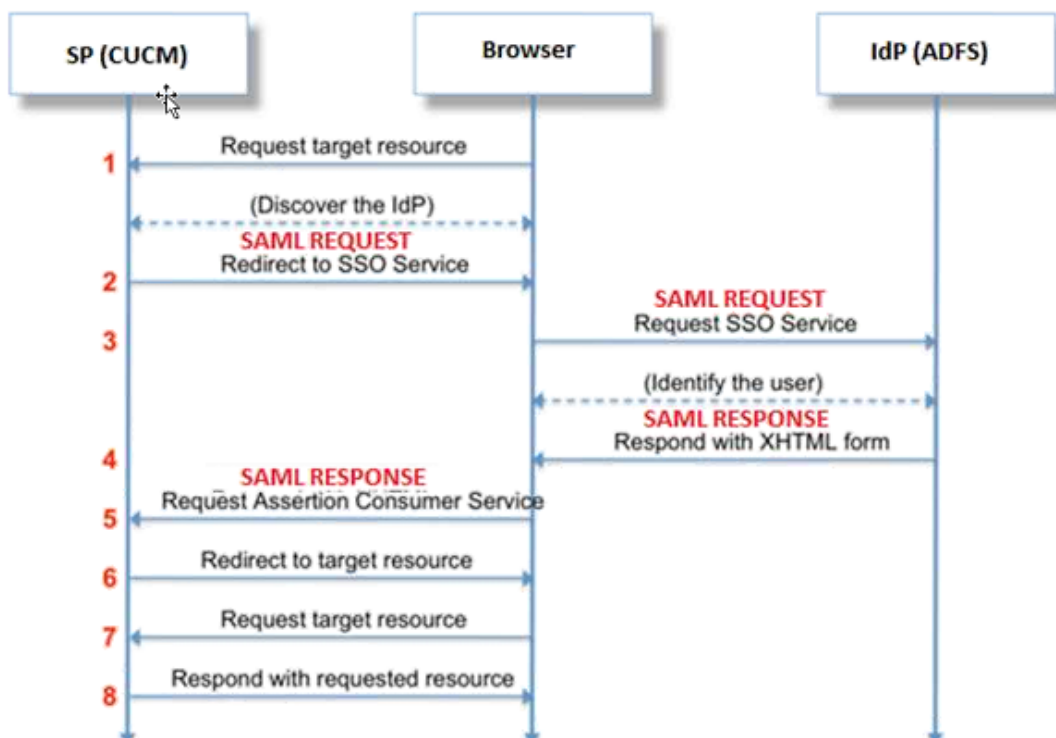
## Verificación

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

## Troubleshoot

Flujo de inicio de sesión en SSO

# Authentication Flow



## Decodificación de la respuesta SAML

Uso de complementos en el Bloc de notas++

## Instale estos complementos:

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

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

En los registros de SSO, busque la cadena "authentication.SAMLAuthenticator - SAML Response is ::" que contiene la respuesta codificada.

Utilice este plugin o SAML Decode en línea para obtener la respuesta XML. La respuesta se puede ajustar en un formato legible con el complemento Pretty Print instalado.

En la versión más reciente de CUCM SAML, la respuesta está en formato XML, que se puede encontrar buscando "SPACSUtills.getResponse: got response=<samlp:

Response xmlns:samlp="y luego imprima con el uso del complemento de impresión bonita.

## Usar Fiddler:

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

## Solicitud de SAML:

```
ID="s24c2d07a125028bffffa7757ea85ab39462ae7751f" Version="2.0" IssueInstant="2017-07-15T11:48:26Z" Destination="https://win-91uhcn8tt31.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>
```

## Respuesta SAML (no cifrada):

```
<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="s24c2d07a125028bffffa7757ea85ab39462ae7751f"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://win-91uhcn8tt31.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-91uhcn8tt31.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>90vwrpJVeOQsDBNGhwkLIIdnf3bc7aW82qmo7Zdm/Z4=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>VbWcKUwwwiNDhUg5AkdqSzQOmP0qs5OT2VT+u1LivWx7h9U8/plyhK3kJMUuxoG/HXPQJgVQaMOWN
q/Paz7Vg2uGNFigA2AFQsKgGo9hAA4etfucIQlMmkeVg+ocvGY+8IzaNVfaUXSU5laN6zriTArxXwxCK0+thgRgQ8/46vm91
Skq2Fa5Wt5uRPUJ3F4eZPOEPdtKxOmUuHi3Q2pXtw4yWz/y89xPfsixNQEmr10hpPadyfPsIFGdNJJwWJV4WjNmfcAqClzaG8
pB74e5EawLmwrFv3/i8QFr1DyU5yCCpxj02rgE6Wi/Ew/X/16qSczOZEpl7D8LwAn74Kij0+Q==</ds:SignatureValue>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC5DCCAcygAwIBAgIQZLLskb6vppxciYP8xOahQDANBgkqhkiG9w0BAQsFADAuMSwwKgYDVQQD
EYNBREZTIFNpZ25pbmcgLSBXSU4ySzEyLnJrb3R1bGFrcmRlLmXhYjAeFw0xNTA2MjIxOTE2NDRAfW0xNjA2MjExOTE2NDRA
MC4xLDAqBgNVBAMTI0FERlMgU2lnbmluZyAtIFdJTjJLMTIucmVudHVzYWsubGFiMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApEe09jnzXEcEC7s1VJ7fMXAHPXj7jg00cs9/Lzxr4c68tePGItrEYnzW9vLe0Dj8OJET/Rd6LsKvuMQHfcGYqA+
XugZyHBrpc18w1hSmMfvfa0jN0Qc0lf+a3j72xfI9+hLtsqSPSnMp9qby3qSiQutP3/ZyXRN/TnzYDEmzur2MA+GP7vdeVOF
XlpENrRfaINzc8INqGRJ+1jZrm+vLFvX7YwIL6aOpmjxpcPoxDcjgEGMYO/TaoP3eXutX4FuJV5R9oAvbqD2F+73XrvP4e/w
Hi5aNRHrgiCnuBJTIxHwRGSoiChdpZlvSB15v8DFaQSVAiEMPj1vP/4rMkacNQIDAQABMA0GCsGSIb3DQEBCwUAA4IBAQA5
uJZI0K1Xa40H3s5MAo1SG00bnn6+sG14eGIBe7BugZMw/FTgKd3VRsmlVuUWCab09EgyfgdI1nYZCciyFhts4W9Y4BqTH0j4
+VnEWiQg7dMqp2M5lykZWPS6vV2uD010sX5V0avyYi3Qr88vISctniIZpl24c3TqTn/5j+h7LLRVI/ZU380a17wuSNPyed6/
N4BfWhhCRZAdJgijapRG+JIBeoAlvNqN7bgFQMe3wJzS1LkTioERWYgJGBciMPS3H9nkQ1P2tGvmn0uwacWPglWR/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-
91uhcn8tt31.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="s24c2d07a125028bffffa7757ea85ab39462ae7751f"
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>cucmsso.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</AuthnC
ontextClassRef>
</AuthnContext>
</AuthnStatement>
</Assertion>
```

</samlp:Response>

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

InResponseTo="s24c2d07a125028bffffa7757ea85ab39462ae7751f" :- The id for SAML Request to which this response corresponds to

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

<Issuer>http://win-91uhcn8tt31.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 SAML esté cifrada, no podrá ver la información completa y tendrá que desactivar el cifrado en Detección y prevención de intrusiones (IDP) para ver la respuesta completa. El detalle del certificado utilizado para el cifrado se encuentra en "ds:X509EmierSerial" de la respuesta SAML.

## Registros y comandos CLI

Comandos CLI:

### utils sso disable

Este comando inhabilita la autenticación basada en OpenAM SSO o SAML SSO. Este comando enumera las aplicaciones web para las que se habilita SSO. Ingrese **Yes** cuando se le solicite para inhabilitar SSO para la aplicación especificada. Debe ejecutar este comando en ambos nodos si está en un clúster. SSO también se puede inhabilitar desde la interfaz gráfica de usuario (GUI) y seleccionar el botón **Desactivar**, en SSO específico en Administración de Cisco Unity Connection.

Sintaxis del comando

utils sso disable

### utils sso status

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

Sintaxis del comando

utils sso status

## **utils sso enable**

Este comando devuelve un mensaje de texto informativo que solicita que el administrador pueda habilitar la función SSO solamente desde la GUI. Con este comando no se puede habilitar tanto el SSO basado en OpenAM como el SSO basado en SAML.

Sintaxis del comando

```
utils sso enable
```

## **utils sso recovery-url enable**

Este comando habilita el modo de recuperación URL SSO. También verifica que esta URL funcione correctamente. Debe ejecutar este comando en ambos nodos si está en un clúster.

Sintaxis del comando

```
utils sso recovery-url enable
```

## **utils sso recovery-url disable**

Este comando inhabilita el modo de recuperación URL SSO en ese nodo. Debe ejecutar este comando en ambos nodos si está en un clúster.

Sintaxis del comando

```
utils sso recovery-url disable
```

## **set samltrace level <trace-level>**

Este comando habilita los seguimientos y niveles de seguimiento específicos que pueden localizar cualquier error, depuración, información, advertencia o fatal. Debe ejecutar este comando en ambos nodos si está en un clúster.

Sintaxis del comando

```
set samltrace level <trace-level>
```

## **show samltrace level**

Este comando muestra el nivel de registro establecido para SAML SSO. Debe ejecutar este comando en ambos nodos si está en un clúster.

Sintaxis del comando

```
show samltrace level
```

Rastrea para ver el momento de la resolución de problemas:

Los registros de SSO no se establecen en el nivel detallado de forma predeterminada.

Primero ejecute el comando **set samltrace level debug** para establecer los niveles de registro para depurar, reproducir el problema y recopilar estos registros.

Desde RTMT:

Tomcat de Cisco

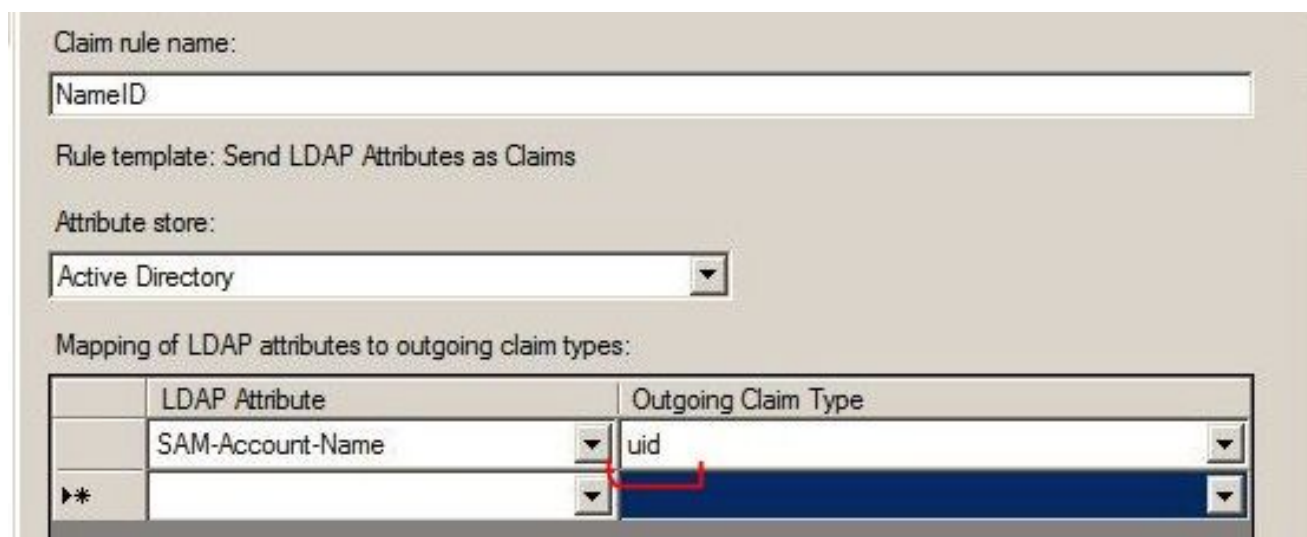
Seguridad Tomcat De Cisco

SSO de Cisco

## Problemas comunes

Valor incorrecto para identificador único (UID):

Debe ser exactamente UID y, si no es así, CUCM no puede entenderlo.



Claim rule name:  
NameID

Rule template: Send LDAP Attributes as Claims

Attribute store:  
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
	SAM-Account-Name	uid
▶*		

Regla de reclamación incorrecta o política de ID de nombre incorrecta:

Lo más probable es que en esta situación no se pida ningún nombre de usuario ni contraseña.

No habrá ninguna afirmación válida en la respuesta de SAML y el código de estado será como:

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

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

Diferencia en el caso/nombre definido en la regla de reclamación:

El FQDN de CUCM en la regla de reclamación debe coincidir exactamente con el especificado en el servidor real.

Puede comparar la entrada en el archivo xml de metadatos de IDP con la de CUCM ejecutando el comando **show network cluster/show network etho details** en la CLI de CUCM.

Hora incorrecta:

El NTP entre CUCM y IDP tiene una diferencia mayor que los [3 segundos permitidos en la Guía de Implementación](#).

Firmante de afirmación no fiable:

En el momento del intercambio de los metadatos entre los desplazados internos y CUCM (proveedor de servicios).

Los certificados se intercambian y, si se produce alguna revocación del certificado, los metadatos deben intercambiarse de nuevo.

Configuración incorrecta de DNS/Sin configuración

DNS es el requisito principal para que SSO funcione. Ejecute **show network etho detail, utils diagnose test** en la CLI para verificar que DNS/Domain esté configurado correctamente.

## Defectos conocidos

### [CSCuj66703](#)

El certificado de firma ADFS se renueva y agrega dos certificados de firma a las respuestas IDP de vuelta a CUCM (SP), por lo que se produce un defecto. Debe eliminar el certificado de firma que no es obligatorio

### [CSCvf63462](#)

Cuando se desplaza a la página SAML SSO desde el Administrador de CCM, se le pregunta "Los siguientes servidores han fallado al intentar obtener el estado de SSO" seguido del nombre del nodo.

### [CSCvf96778](#)

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