

Solucionar problemas de SSO no Cisco Unified Communications Manager

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

[Fluxo de login no SSO](#)

[Decodificação da resposta SAML](#)

[Logs e comandos CLI](#)

[Problemas comuns](#)

[Defeitos conhecidos](#)

Introduction

Este documento descreve como configurar o SSO (Single Sign-On, login único) no Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

A Cisco recomenda que você conheça os tópicos:

- CUCM
- Serviços de Federação do Ative Directory (ADFS)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e 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 Configuração de Login Único no 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>

Guia de implantação do SSO SAML para aplicativos de comunicação unificada da Cisco, versão 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

SAML RFC 6596.

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

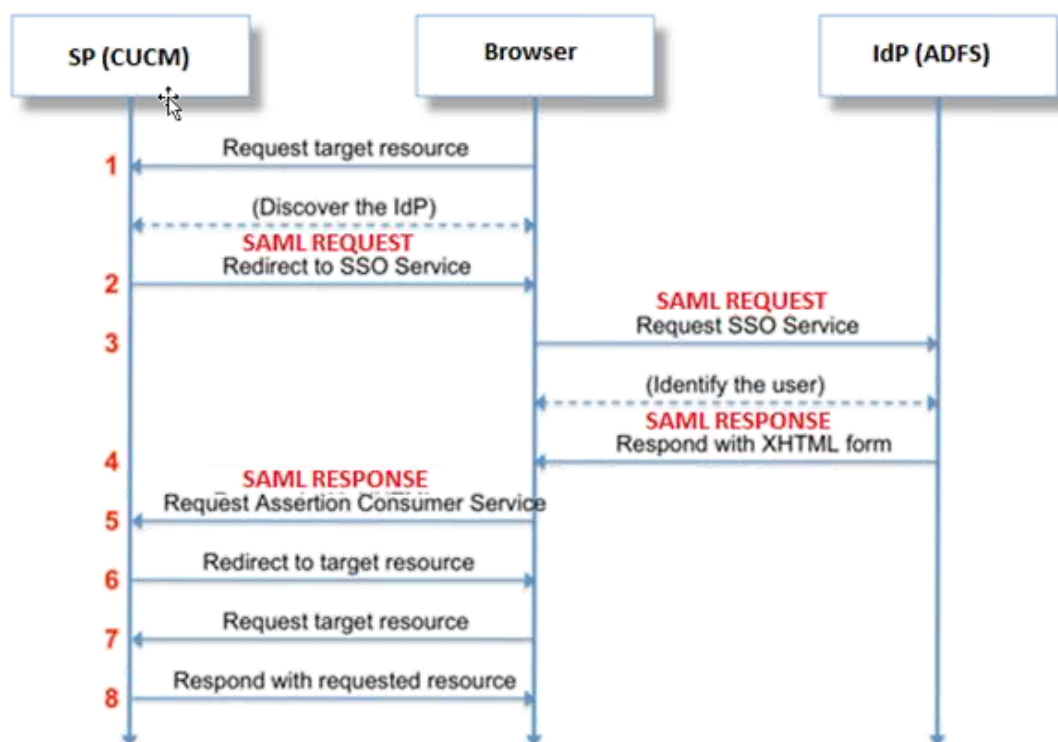
Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Fluxo de login no SSO

Authentication Flow



Decodificação da resposta SAML

Usando plugins no Bloco de Notas++

Instalar estes plugins:

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

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

Nos registros SSO, procure a string "authentication.SAMLAuthenticator - SAML Response is ::" que contém a resposta codificada.

Use este plugin ou decodificação SAML on-line para obter a resposta XML. A resposta pode ser ajustada em um formato legível com o uso do plugin Pretty Print instalado.

Na versão mais recente da resposta SAML do CUCM está no formato XML que pode ser encontrado pesquisando "SPACSUtills.getResponse: got response=<samlp:

Resposta xmlns:samlp="e, em seguida, imprima com o uso do plug-in Impressão Pretty.

Use o conversor:

Esse utilitário pode ser usado para obter o tráfego em tempo real e decodificá-lo. Aqui está o guia para o mesmo; <https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/>.

Solicitação SAML:

```
ID="s24c2d07a125028bffffa7757ea85ab39462ae7751f" 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>
```

Resposta SAML (não criptografada):

```
<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-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-9luhcn8tt31.emeacum.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>9OvwrpJVeOQsDBNghvkwLIIdnf3bc7aW82qmo7Zdm/Z4=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>VbWcKUwwiNDhUg5AkdqSzQOmP0qs5OT2VT+uLiVWx7h9U8/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
EyNBREZTIFNpZ25pbmcgLSBXSU4yS3ZyLnJrb3R1bGFrcmVhYyAeFw0xNTA2MjIxOTE2NDRAfW0xNjA2MjExOTE2NDRAmC4x
LDAqBgNVBAMTI0FERlMgU2lnbmluZyAtIFdJTjJLMTIucmtdvHVvYwsubGF1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApEe09jnzXEcEc7s1VJ7fMXAHPXj7jg00cs9/Lzxr4c68tePGItrEYnzW9vLe0Dj8OJET/Rd6LsKvuMQHfcGYqA+
XugZyHBrpc18wlhSmMfvfa0jN0Qc0lf+a3j72xfI9+hLtsqSPSnMp9qby3qSiQutP3/ZyXRN/TnzYDEmzur2MA+GP7vdeVOF
XlpENrRfaINzc8INqGRJ+1jZrm+vLfvX7YwIL6aOpmjxaxcPoxDcJgEGMYO/TaoP3eXutX4FuJV5R9oAvbqD2F+73XrvP4e/w
Hi5aNRHrgiCnuBJTIXHwRGSoichdpZlvSB15v8DFaQSVAiEMPjlvP/4rMkacNQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA5
uJZIOk1Xa40H3s5MAo1SG00bnn6+sG14eGIBe7BugZMw/FTgKd3VRsmlVuUWCab09EgyfgdIlnYZCciyFhts4W9Y4BgTH0j4
+VnEWiQg7dMqP2M5lykZWP6vV2u010sX5V0avyYi3Qr88vISctniIZpl24c3TqTn/5j+H7LLRVI/ZU38Oa17wuSNPyed6/
N4BfWhhCRZAdJgijapRG+JIBeoAlvNqN7bgFQMe3wJzSlLkTioERWYgJGBciMPS3H9nkQ1P2tGvmn0uwacWPglWR/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-
9luhcn8tt31.emeacum.com/com/adfs/services/trust"
SPNameQualifier="cucmsso.emeacum.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.emeacum.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacum.com" />
</SubjectConfirmation>
</Subject>
<Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z">
<AudienceRestriction>
<Audience>ccucmsso.emeacum.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="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.emeacum.com/adfs/services/trust</Issuer> :- IdP FQDN

SPNameQualifier="cucmsso.emeacum.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

Caso a resposta SAML seja criptografada, você não poderá ver as informações completas e terá que desabilitar a criptografia na Detecção e Prevenção de Intrusão (IDP) para ver a resposta completa. O detalhe do certificado usado para criptografia está em "ds:X509IssuerSerial" da resposta SAML.

Logs e comandos CLI

Comandos CLI:

utils sso disable

Este comando desativa a autenticação baseada em ambos (SSO OpenAM ou SSO SAML). Esse comando lista os aplicativos da Web para os quais o SSO está ativado. Insira **Sim** quando solicitado para desabilitar SSO para o aplicativo especificado. Você deve executar esse comando em ambos os nós se estiver em um cluster. O SSO também pode ser desabilitado na Interface Gráfica do Usuário (GUI) e selecione o botão **Desabilitar**, em SSO específico na Administração do Cisco Unity Connection.

Sintaxe do comando

utils sso disable

status do utils sso

Esse comando exibe os parâmetros de status e configuração do SSO SAML. Ele ajuda a verificar o status do SSO, ativado ou desativado, em cada nó individualmente.

Sintaxe do comando

status do utils sso

utils sso enable

Esse comando retorna uma mensagem de texto informativa que solicita que o administrador possa ativar o recurso SSO somente da GUI. SSO baseado em OpenAM e SSO baseado em SAML não podem ser habilitados com este comando.

Sintaxe do comando
utils sso enable

utils sso recovery-url enable

Esse comando ativa o modo SSO de URL de recuperação. Também verifica se este URL funciona com êxito. Você deve executar esse comando em ambos os nós se estiver em um cluster.

Sintaxe do comando
utils sso recovery-url enable

utils sso recovery-url disable

Este comando desativa o modo SSO de URL de recuperação nesse nó. Você deve executar esse comando em ambos os nós se estiver em um cluster.

Sintaxe do comando
utils sso recovery-url disable

set samltrace level <trace-level>

Esse comando permite rastreamentos específicos e níveis de rastreamento que podem localizar qualquer erro, depuração, informação, aviso ou fatal. Você deve executar esse comando em ambos os nós se estiver em um cluster.

Sintaxe do comando
set samltrace level <trace-level>

show samltrace level

Esse comando exibe o nível de log definido para SAML SSO. Você deve executar esse comando em ambos os nós se estiver em um cluster.

Sintaxe do comando
show samltrace level

Rastreios para observar o momento da solução de problemas:

Por padrão, os logs SSO não são definidos para o nível detalhado.

Primeiro execute o comando **set samltrace level debug** para definir os níveis de log como debug, reproduzir o problema e coletar esses conjuntos de logs.

De RTMT:

Cisco Tomcat

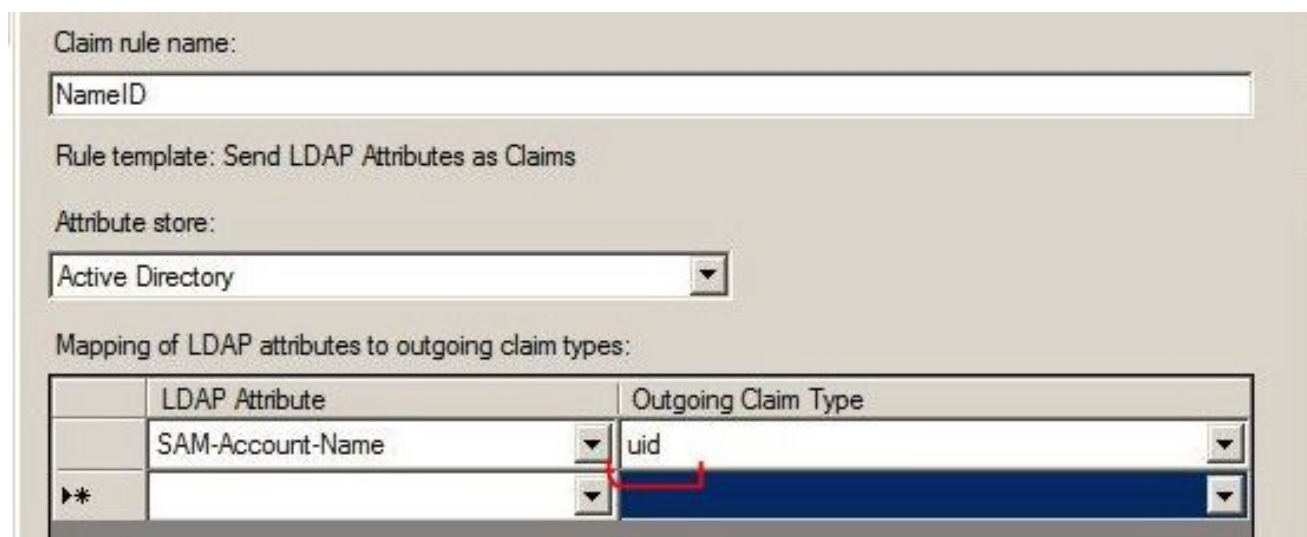
Cisco Tomcat Security

SSO da Cisco

Problemas comuns

Valor incorreto para identificador exclusivo (UID):

Deve ser exatamente UID e, se não for o caso, o CUCM não consegue entender isso.



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
▶*		

Regra de reivindicação incorreta ou política de ID de nome errada:

Provavelmente, nenhum nome de usuário e senha é solicitado nesse cenário.

Não haverá nenhuma asserção válida na resposta SAML e o Código de status será como:

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

Verifique se a regra de reivindicação está definida corretamente no lado IDP.

Diferença de caso/nome definida na regra de reivindicação:

O CUCM FQDN na regra de reivindicação deve corresponder exatamente ao especificado no servidor real.

Você pode comparar a entrada no arquivo xml de metadados do IDP com a entrada no CUCM executando o comando **show network cluster/show network etho details** na CLI do CUCM.

Hora incorreta:

O NTP entre o CUCM e o IDP tem uma diferença maior que os [3 segundos permitidos no Guia de implantação](#).

Assinante da Asserção Não Confiável:

No momento da troca de metadados entre o IDP e o CUCM (provedor de serviços).

Os certificados são trocados e, em caso de revogação do certificado, os metadados devem ser novamente trocados.

Configuração incorreta/Sem configuração de DNS

O DNS é o requisito principal para que o SSO funcione. Execute **show network etho detail, utils diagnose test** na CLI para verificar se o DNS/Domínio está configurado corretamente.

Defeitos conhecidos

[CSCuj66703](#)

O certificado de assinatura do ADFS renova e adiciona dois certificados de assinatura às respostas do IDP ao CUCM (SP), fazendo com que você fique com defeito. Você deve excluir o certificado de assinatura que não é obrigatório

[CSCvf63462](#)

Quando você navega para a página SSO SAML do CCM Admin, é solicitado que você informe "Os seguintes servidores falharam durante a tentativa de obter o status SSO" seguido do nome do nó.

[CSCvf96778](#)

O SSO baseado em CTI falha ao definir o servidor CUCM como endereço IP no CCMAdmin//System/Server.