Pesquise defeitos o SSO no gerente das comunicações unificadas de Cisco

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Configurar](#)
[Verificar](#)
[Troubleshooting](#)
[Entre o fluxo no SSO](#)
[Resposta da descodificação SAML](#)
[Logs e comandos CLI](#)
[Problemas comuns](#)
[Defeitos conhecidos](#)

Introdução

Este documento descreve como configurar único Sinal-em (SSO) no gerente das comunicações unificadas de Cisco (CUCM).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento dos assuntos:

- CUCM
- Serviços da federação do diretório ativo (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.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Refira a configuração do único sinal sobre em 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 distribuição de SAML SSO para aplicativos de comunicações unificadas de Cisco, liberação 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

RFC 6596 DE SAML.

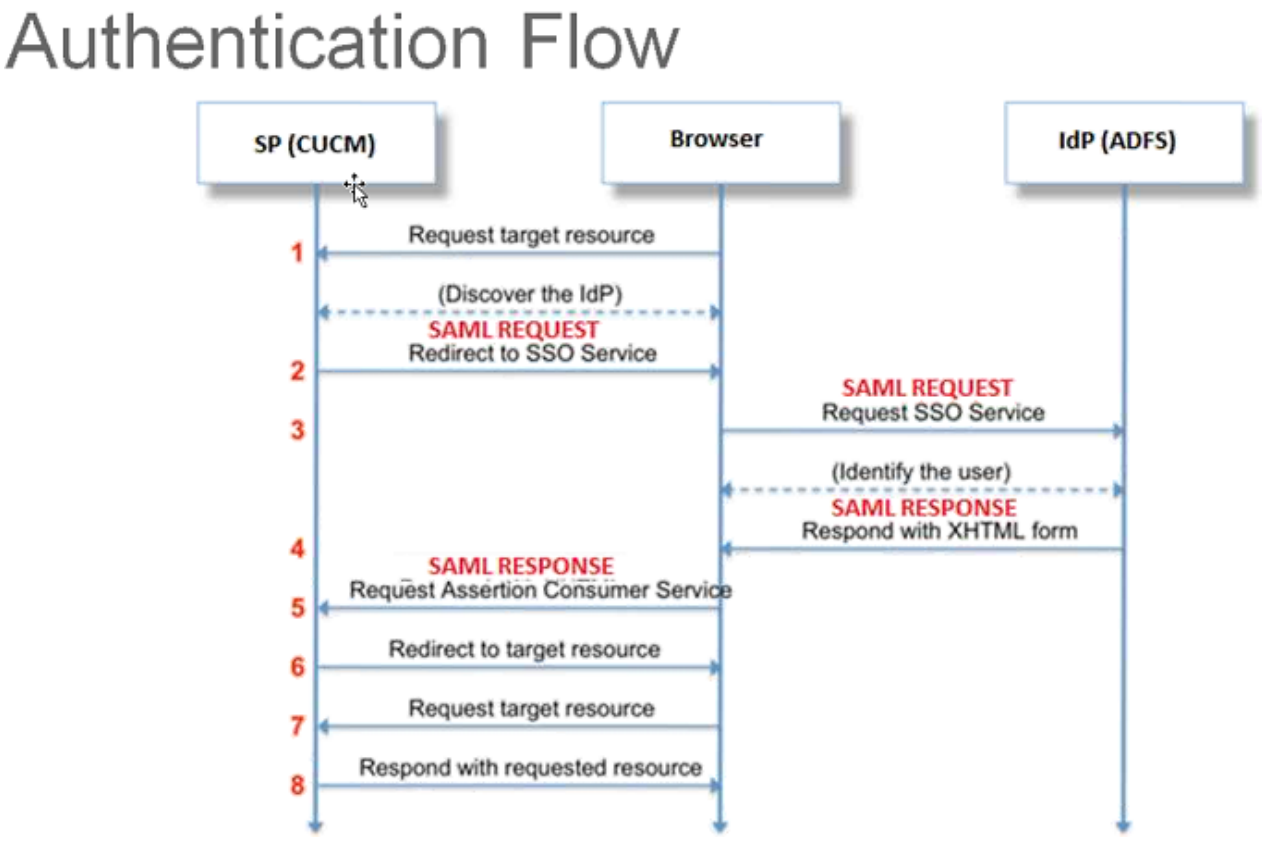
- https://tools.ietf.org/html/rfc6595

Verificar

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

Troubleshooting

Entre o fluxo no SSO



Resposta da descodificação SAML

Usando encaixes em Notepad++

Instale estes encaixes:

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

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

Em logs SSO procure pela corda “authentication.SAMLAuthenticator - resposta de SAML é:: ” que contém a resposta codificada.

Use este de encaixe ou SAML em linha descodifica a fim obter a resposta XML. A resposta pode ser ajustada em um formato legível com a cópia bonita instalada uso de encaixe.

Na versão mais nova da resposta CUCM SAML está no formato XML que pode ser encontrado procurando “SPACSUtils.getResponse: response=<samlp obtido:

Xmlns da resposta: o samlp= “e imprime então com o uso da cópia bonita de encaixe.

Violinista do uso:

Esta utilidade pode ser usada para obter o tráfego de tempo real e para descodificá-lo. Está aqui o guia para o mesmos; https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/.

Pedido de SAML:

```
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>
```

Resposta de SAML (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
```

Caso que a resposta de SAML é cifrada então você não poderá ver a informação completa e tem que desabilitar a criptografia na intrusion detection & na prevenção (IDP) para ver a resposta completa. O detalhe certificado usado para a criptografia está sob "ds:X509IssuerSerial" da resposta de SAML.

Logs e comandos CLI

Comandos CLI:

desabilitação do sso dos utils

Este comando desabilita ambo (OpenAM SSO ou SAML SSO) a autenticação baseada. Lista deste comando os aplicativos de web para que o SSO é permitido. Entre **sim** quando alertado a fim desabilitar o SSO para o aplicativo especificado. Você deve executar este comando em ambos os Nós se em um conjunto. O SSO pode igualmente ser desabilitado da interface gráfica de usuário (GUI) e selecionar o botão do **desabilitação**, sob o SSO específico na administração do Cisco Unity Connection.

Sintaxe do comando
desabilitação do sso dos utils

estado do sso dos utils

Este comando indica o estado e os parâmetros de configuração de SAML SSO. Ajuda a verificar o estado SSO, permitido ou desabilitado, em cada nó individualmente.

Sintaxe do comando
estado do sso dos utils

o sso dos utils permite

Este comando retorna um mensagem de texto informativo esse alertas que o administrador pode permitir a característica SSO somente do GUI. OpenAM baseou o SSO e o SSO baseado SAML não pode ser permitido com este comando.

Sintaxe do comando
o sso dos utils permite

o sso recuperação-URL dos utils permite

Este comando permite o modo da recuperação URL SSO. Igualmente verifica que esta URL trabalha com sucesso. Você deve executar este comando em ambos os Nós se em um conjunto.

Sintaxe do comando
o sso recuperação-URL dos utils permite

desabilitação do sso recuperação-URL dos utils

Este comando desabilita o modo da recuperação URL SSO nesse nó. Você deve executar este comando em ambos os Nós se em um conjunto.

Sintaxe de comando
desabilitação do sso recuperação-URL dos utils

ajuste o <trace-level> nivelado do samltrace

Este comando permite os traços específicos e os níveis de rastreamento que podem encontrar todo o erro, debugam, informação, aviso ou fatal. Você deve executar este comando em ambos os Nós se em um conjunto.

Sintaxe de comando
ajuste o <trace-level> nivelado do samltrace

mostre o samltrace em nível

Este comando indica o nível do log ajustado para SAML SSO. Você deve executar este comando em ambos os Nós se em um conjunto.

Sintaxe de comando
mostre o samltrace em nível

Os traços a olhar na altura de pesquisam defeitos:

Os logs SSO não são ajustados a nível detalhado à revelia.

Primeiro lote que o **nível do samltrace do** comando set **debuga** a fim ajustar os níveis do log para debugar, reproduz a edição e a coleta estas grupo de logs.

De RTMT:

Cisco Tomcat

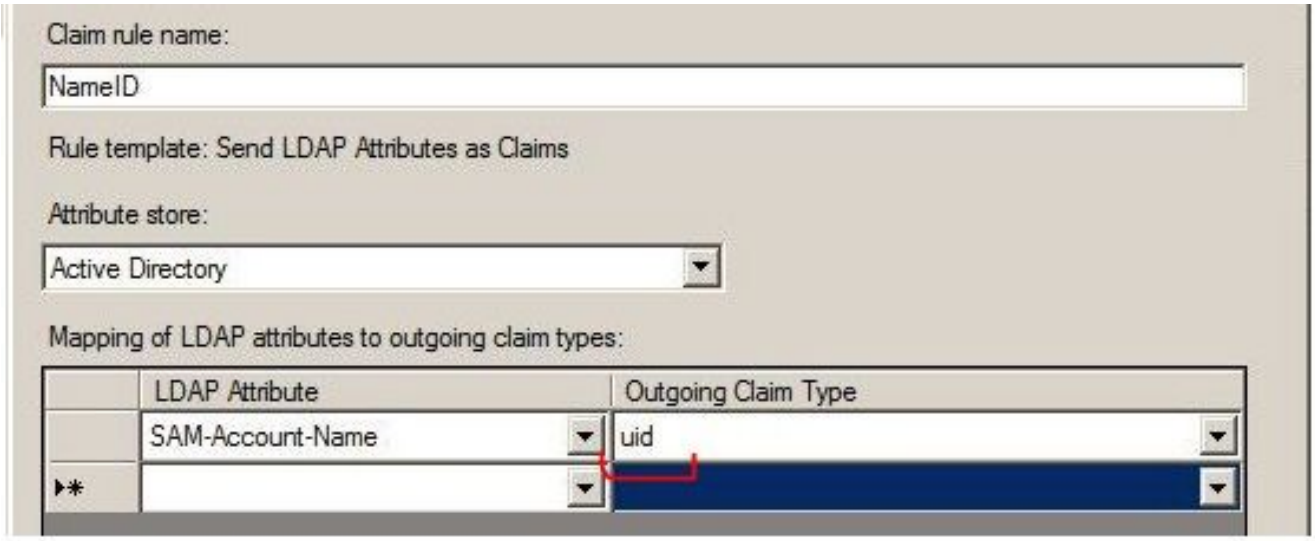
Segurança de Cisco Tomcat

Cisco SSO

Problemas comuns

Valor incorreto para Indentifier original (UID):

Deve exatamente ser UID e se não é o caso, CUCM é incapaz de compreender isso.



Regra incorreta da reivindicação ou política errada de NameID:

Muito provavelmente nenhum nome de usuário e senha é alerta acima nesta encenação.

Não haverá nenhuma afirmação válida na resposta de SAML e o código de status estará como:

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

Verifique que a regra da reivindicação está definida corretamente no lado IDP.

Diferença caso que/nome definido na regra da reivindicação:

O FQDN CUCM na regra da reivindicação deve exatamente combinar com essa especificada no servidor real.

Você pode comparar a entrada no arquivo do xml dos metadata de IDP com esse em CUCM executando **detalhes do etho da rede do conjunto/mostra da rede da mostra** comanda no CLI de

CUCM.

Horas incorreta:

O NTP entre CUCM e IDP tem uma diferença maior do que os 3 segundos reservados no guia de distribuição.

Signatário da afirmação não confiado:

Na altura da troca dos metadata entre IDP e CUCM (provedor de serviços).

Os Certificados são trocados e se há qualquer revogação do certificado feita, os metadata devem ser trocados outra vez.

Configuração DNS Misconfiguration/No

O DNS é o requisito principal para que o SSO trabalhe. Execute o **detalhe do etho da rede da mostra**, **utils diagnosticam o teste no** CLI a fim verificar que DNS/Domain está configurado corretamente.

Defeitos conhecidos

CSCuj66703

O certificado de assinatura ADFS renova e adiciona dois certs de assinatura às respostas IDP de volta a CUCM (SP) faz com assim que você seja executado no defeito. Você tem que suprimir do certificado de assinatura que não é exigido

CSCvf63462

Quando você navega à página de SAML SSO de CCM Admin você está alertado com “os seguintes server falhados durante a tentativa de obter o estado SSO” seguido pelo nome de nó.

CSCvf96778

O SSO baseado CTI falha ao definir o server CUCM como o endereço IP de Um ou Mais Servidores Cisco ICM NT em CCMAdmin//System/Sever.