Probleemoplossing in Cisco Unified Communications Manager

Inhoud

Inleiding

Dit document beschrijft hoe u Single aanmelding (SSO) kunt configureren in Cisco Unified Communications Manager (CUCM).

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben over de onderwerpen:

- CUCM
- Active Directory Federation Services (ADFS)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Raadpleeg de configuratie van één teken in 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 SSO-implementatiegids voor Cisco Unified Communications-toepassingen, release 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.

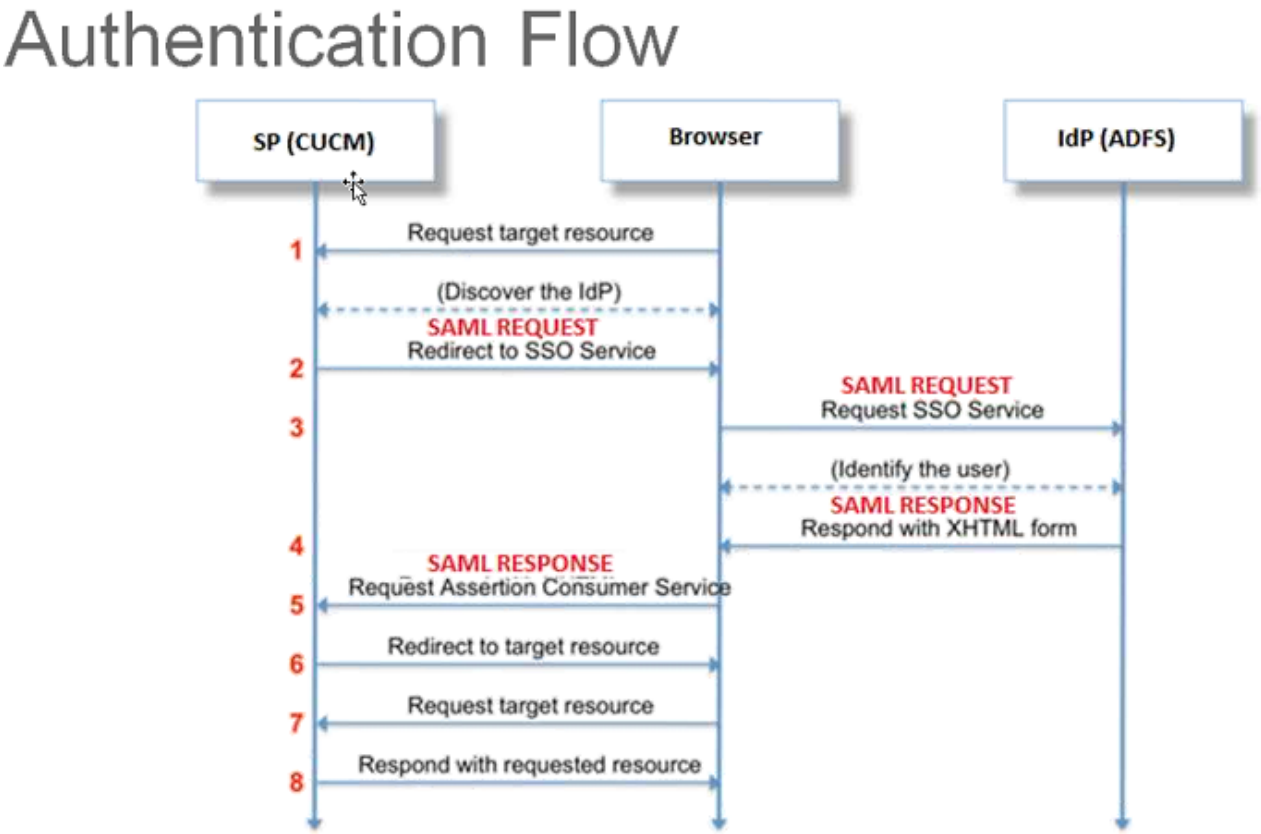
- https://tools.ietf.org/html/rfc6595

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Login Flow in SSO



decoderen van SAML-respons

Pluizen in Kladblok+ gebruiken

Installeer deze stekkers:

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

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

In SSO logs zoekt u naar de string "Authentication.SAMLAutheter - SAML Response is:" die de gecodeerde respons bevat.

Gebruik deze plug-in of online SAML-decode om de XML-respons te krijgen. De respons kan in een leesbare indeling worden aangepast met de ingebouwde Best Print Plug.

In de nieuwere versie van CUCM SAML is de respons in XML-formaat te vinden, die kan worden gevonden door te zoeken naar "SPACSUtils.getResponse: kreeg respons=<samlp:

Response xmlns:samlp="en print vervolgens af met de N.B.-stekker.

Gebruik Fiddler:

Deze voorziening kan worden gebruikt om het real-time verkeer te krijgen en het te decoderen. Hier is de handleiding voor hetzelfde: https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/.

SAML-aanvraag:

```
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-respons (niet versleuteld):

```
<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>
```

</min:respons>

```
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
```

Als de SAML-respons is versleuteld, kunt u de volledige informatie niet zien en moet u encryptie bij Inbraakdetectie en -preventie (IDP) uitschakelen om de volledige respons te zien. De certificaathoudelijkheid die gebruikt wordt voor encryptie is onder "ds:X509IssuerSerial" van de SAML-respons.

Logs en CLI-opdrachten

CLI-opdrachten:

utist sao

Deze opdracht schakelt beide (OpenAM SSO of SAML SSO) gebaseerde verificatie uit. Deze opdracht maakt een lijst van de webtoepassingen waarvoor SSO is ingeschakeld. Voer **Ja in** als dit wordt gevraagd om de SSO voor de gespecificeerde toepassing uit te schakelen. U moet deze opdracht op beide knooppunten uitvoeren indien in een cluster. SSO kan ook worden uitgeschakeld vanuit Graphical User Interface (GUI) en de knop **Uitschakelen** selecteren onder specifieke SSO in Cisco Unity Connection-beheer.

Complexe
utist sao

utils sso-status

Deze opdracht geeft de status- en configuratieparameters van SAML in de SSO weer. Het helpt de SSO status voor elk knooppunt afzonderlijk te controleren, ingeschakeld of uitgeschakeld.

Complexe
utils sso-status

utisten die

Deze opdracht geeft een informatief tekstbericht terug dat ertoe leidt dat de beheerder de SSO-functie alleen vanuit GUI kan inschakelen. Zowel op OpenAM gebaseerde SSO als op SAML gebaseerde SSO kan niet met deze opdracht worden ingeschakeld.

Complexe
utisten die

utisten die geschikt zijn voor nuttige toepassing

Met deze opdracht kunt u de URL SSO-modus herstellen. Tevens wordt geverifieerd dat deze URL met succes werkt. U moet deze opdracht op beide knooppunten uitvoeren indien in een cluster.

Complexe
utisten die geschikt zijn voor nuttige toepassing

utils herstel-url-uitschakelen

Deze opdracht schakelt de URL SSO-modus van herstel in dat knooppunt uit. U moet deze opdracht op beide knooppunten uitvoeren indien in een cluster.

syntax van commando's
utils herstel-url-uitschakelen

niveau samentrekken <spoorniveau> instellen

Deze opdracht stelt de specifieke sporen en spoorniveaus in die elke fout, debug, informatie, waarschuwing of fataal kunnen opsporen. U moet deze opdracht op beide knooppunten uitvoeren indien in een cluster.

syntax van commando's
niveau samentrekken <spoorniveau> instellen

voorbeeldniveau tonen

Deze opdracht geeft het logniveau weer dat voor SAML SLB is ingesteld. U moet deze opdracht op beide knooppunten uitvoeren indien in een cluster.

syntax van commando's
voorbeeldniveau tonen

Traces om te kijken op het tijdstip van probleemoplossing:

SSO-logbestanden zijn standaard niet ingesteld op gedetailleerd niveau.

Start eerst de opdracht **samlspoorniveau debug** om de logniveaus in te stellen om de kwestie te debug, reproduceren en deze verzameling logbestanden te verzamelen.

Vanaf RTMT:

Cisco Tomcat

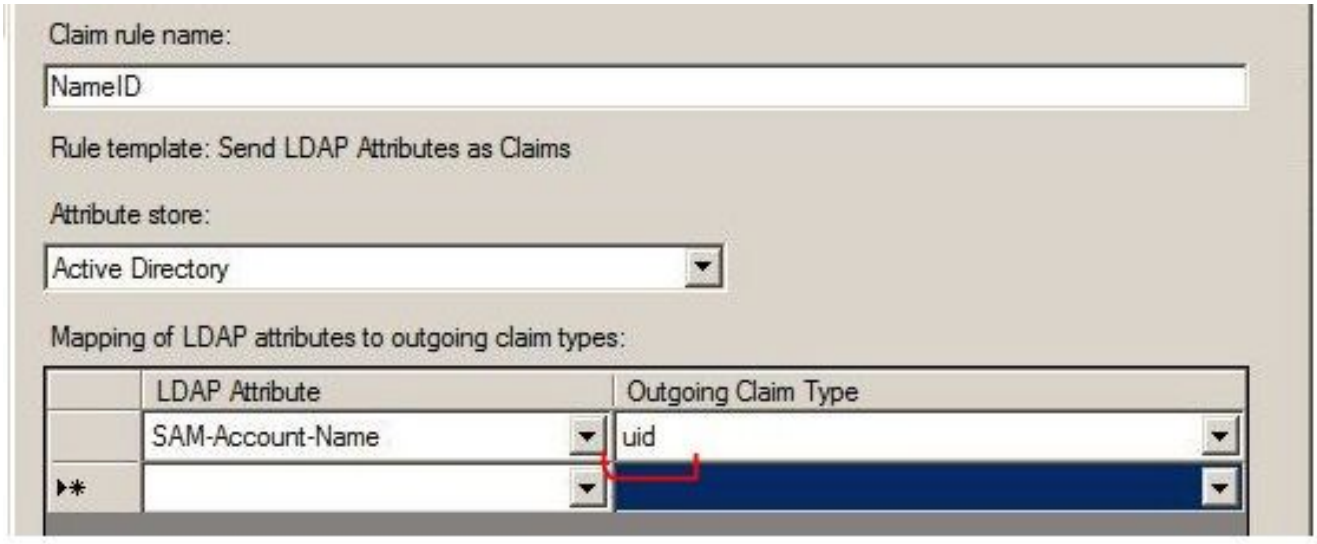
Cisco ScanSafe-beveiliging

Cisco SSO

Gemeenschappelijke kwesties

Onjuiste waarde voor unieke identificatiecode (UID):

Het moet precies UID zijn en als dat niet het geval is, kan CUCM dat niet begrijpen.



Onjuiste Claimregel of onjuist NaamID-beleid:

Waarschijnlijk worden geen gebruikersnaam en wachtwoord in dit scenario gevraagd.

Er zal geen geldige bewering zijn in de SAML respons en de Status Code zal zijn zoals:

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

Controleer dat de claimregel correct aan de kant van het IDP is gedefinieerd.

Verschil in geval/naam gedefinieerd in vorderingsregel:

CUCM FQDN zou op claimregel precies moeten overeenkomen met degene die op de eigenlijke server gespecificeerd is.

U kunt de ingang in meta-xml dossier van IDP met de ingang op CUCM vergelijken door **netwerkcluster/de** opdracht van de **netwerkdetails** op CLI van CUCM uit te voeren.

Onjuiste tijd:

NTP tussen CUCM en IDP heeft een verschil dat groter is dan de 3 seconden die in de implementatiegids zijn toegestaan.

Asseringssignaal niet betrouwbaar:

Ten tijde van de uitwisseling van de metagegevens tussen IDP en CUCM (dienstverlener).

Certificaten worden uitgewisseld en indien er sprake is van intrekking van certificaten, dienen metagegevens opnieuw te worden uitgewisseld.

DNS-wanconfiguratie/geen configuratie

DNS is de primaire eis voor een SSO om te werken. Start **eto-details voor netwerken**, **utils diagnosticeert test** op de CLI om te controleren of DNS/Domain correct is ingesteld.

bekende gebreken

CSCuj6703

ADFS-signaalcertificaat vernieuwt en voegt twee gebarenteksten toe aan IDP-reacties op CUCM (SP), waardoor u in een defect terechtkomt. U moet het ondertekeningscertificaat verwijderen dat niet vereist is

CSCvf63462

Wanneer u vanuit CCM Admin naar de SAML SSO-pagina navigeert, wordt u gevraagd "De volgende servers zijn mislukt tijdens een poging om SSO-status te krijgen", gevolgd door de naam van het knooppunt.

CSCvf9678

Op CTI gebaseerde SSO faalt bij het definiëren van CUCM server als IP adres in CCMAdmin/System/Server.