Fehlerbehebung bei SSO in Cisco Unified Communications Manager

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration der einmaligen Anmeldung (Single Sign-On, SSO) in Cisco Unified Communications Manager (CUCM).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der folgenden Themen zu verfügen:

- CUCM
- Active Directory Federation Services (ADFS)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Weitere Informationen finden Sie unter Konfiguration der einmaligen Anmeldung 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 Deployment Guide for Cisco Unified Communications Applications, 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.

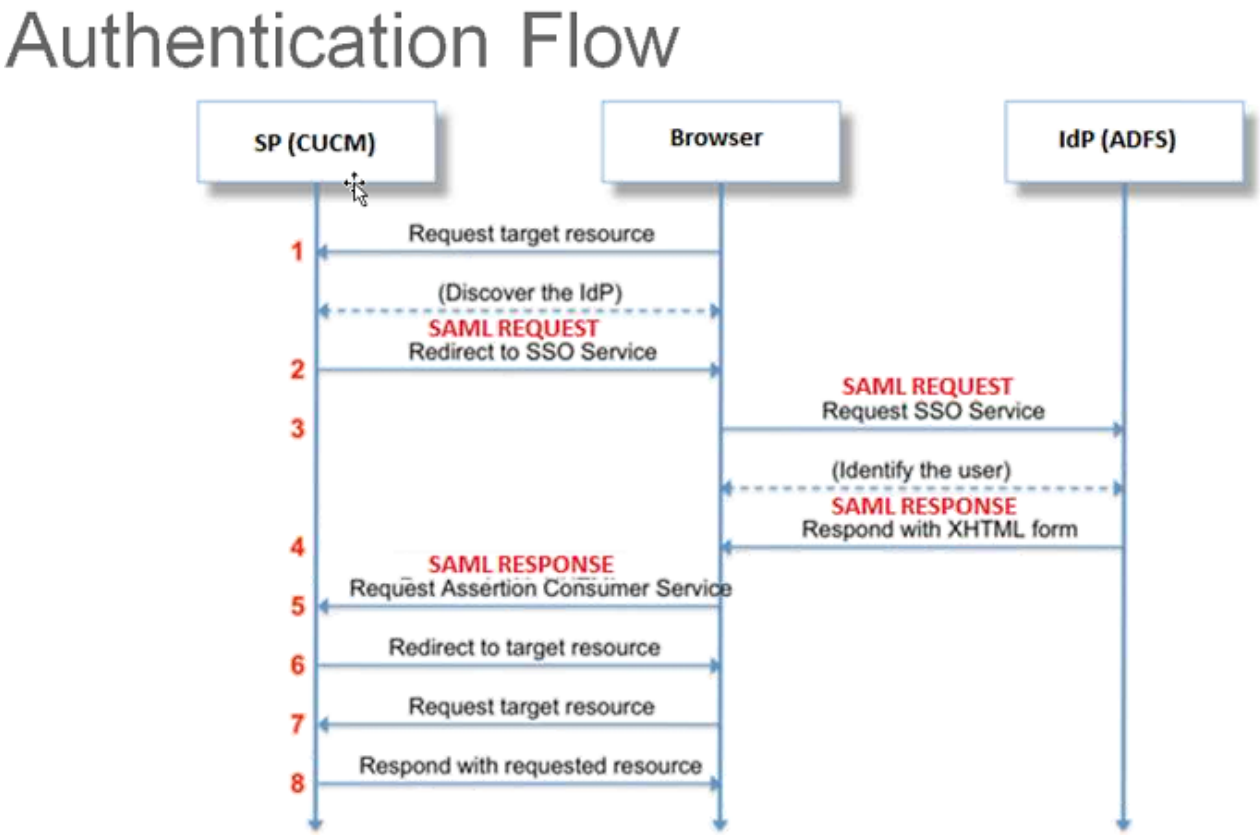
- https://tools.ietf.org/html/rfc6595

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Anmeldungsablauf in SSO



Dekodieren der SAML-Antwort

Verwenden von Plugins in Editor++

Installieren Sie diese Plugins:

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

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

In SSO-Protokollen suchen Sie nach der Zeichenfolge "authentication.SAMLAuthenticator - SAML Response is ::", die die codierte Antwort enthält.

Verwenden Sie dieses Plugin oder online SAML Decode, um die XML-Antwort zu erhalten. Die Antwort kann in einem lesbaren Format mit dem installierten Pretty Print Plugin angepasst werden.

In der neueren Version der CUCM-SAML-Antwort ist das XML-Format vorhanden. Suchen Sie hierzu nach "SPACSUtils.getResponse: got response=<samlp:

Antwort xmlns:samlp="und dann mit Pretty Print Plugin drucken.

Fiddler verwenden:

Mit diesem Dienstprogramm kann der Echtzeitdatenverkehr abgerufen und decodiert werden. Hier ist der Leitfaden für dasselbe: https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/.

SAML-Anforderung:

```
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-Antwort (unverschlüsselt):

```
<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
```

Falls die SAML-Antwort verschlüsselt ist, können Sie die vollständigen Informationen nicht sehen und müssen die Verschlüsselung für Intrusion Detection & Prevention (IDP) deaktivieren, um die vollständige Antwort anzuzeigen. Die für die Verschlüsselung verwendete Zertifikatsdetails finden Sie unter "ds:X509IssuerSerial" der SAML-Antwort.

Protokolle und CLI-Befehle

CLI-Befehle:

utils so deaktivieren

Dieser Befehl deaktiviert die auf OpenAM SSO oder SAML SSO basierende Authentifizierung. Dieser Befehl listet die Webanwendungen auf, für die SSO aktiviert ist. Geben Sie **Yes** ein, wenn Sie dazu aufgefordert werden, SSO für die angegebene Anwendung zu deaktivieren. Sie müssen diesen Befehl auf beiden Knoten ausführen, wenn Sie sich in einem Cluster befinden. SSO kann auch über die grafische Benutzeroberfläche (GUI) deaktiviert werden, und wählen Sie die Schaltfläche **Disable** (**Deaktivieren**) in der Cisco Unity Connection-Verwaltung unter bestimmten SSO aus.

Befehlssyntax
utils so deaktivieren

utils so status

Dieser Befehl zeigt den Status und die Konfigurationsparameter der SAML SSO an. Es hilft, den SSO-Status (aktiviert oder deaktiviert) für jeden Knoten einzeln zu überprüfen.

Befehlssyntax
utils so status

utils aktivieren

Dieser Befehl gibt eine informative Textmeldung zurück, in der der Administrator aufgefordert wird, die SSO-Funktion nur über die Benutzeroberfläche zu aktivieren. Mit diesem Befehl können sowohl OpenAM-basierte SSO als auch SAML-basierte SSO nicht aktiviert werden.

Befehlssyntax
utils aktivieren

utils sso restore url enable

Dieser Befehl aktiviert den Wiederherstellungs-URL-SSO-Modus. Außerdem wird überprüft, ob diese URL erfolgreich funktioniert. Sie müssen diesen Befehl auf beiden Knoten ausführen, wenn Sie sich in einem Cluster befinden.

Befehlssyntax
utils sso restore url enable

utils sso restore-url disable

Dieser Befehl deaktiviert den Wiederherstellungs-URL-SSO-Modus auf diesem Knoten. Sie müssen diesen Befehl auf beiden Knoten ausführen, wenn Sie sich in einem Cluster befinden.

Befehlssyntax
utils sso restore-url disable

Festlegen der Ablaufverfolgungsebene <Ablaufverfolgungsebene>

Dieser Befehl aktiviert die spezifischen Ablaufverfolgungen und Ablaufverfolgungsebenen, die Fehler, Debuggen, Informationen, Warnungen oder schwerwiegende Fehler lokalisieren können. Sie müssen diesen Befehl auf beiden Knoten ausführen, wenn Sie sich in einem Cluster befinden.

Befehlssyntax
Festlegen der Ablaufverfolgungsebene <Ablaufverfolgungsebene>

Beispiel Trace-Ebene anzeigen

Mit diesem Befehl wird die Protokollstufe für SAML SSO angezeigt. Sie müssen diesen Befehl auf beiden Knoten ausführen, wenn Sie sich in einem Cluster befinden.

Befehlssyntax
Beispiel Trace-Ebene anzeigen

Ablaufverfolgungen zum Zeitpunkt der Fehlerbehebung:

SSO-Protokolle sind standardmäßig nicht auf die Detailstufe festgelegt.

Führen Sie zuerst den Befehl **Set samltrace level debug aus**, um die Protokollstufen zum Debuggen, zur Reproduktion des Problems und zum Erfassen dieser Protokollsätze festzulegen.

Aus RTMT:

Cisco Tomcat

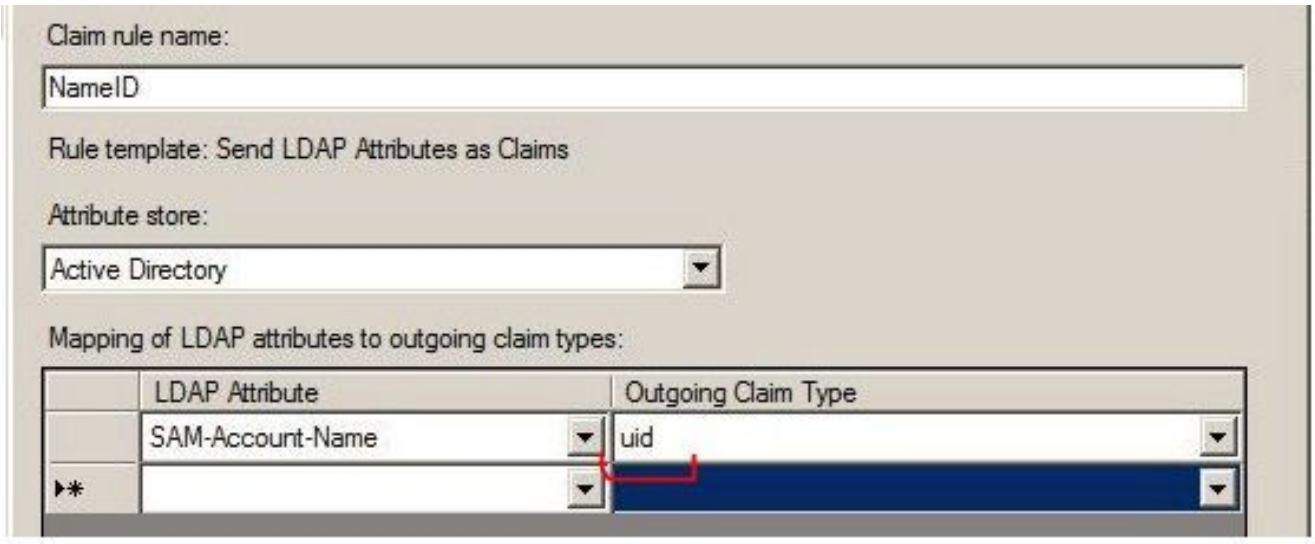
Cisco Tomcat Security

Cisco SSO

Häufige Probleme

Falscher Wert für Unique Indentifier (UID):

Es sollte sich genau um eine UID handeln, und wenn dies nicht der Fall ist, kann der CUCM dies nicht verstehen.



Falsche Anspruchsregel oder Falsche Name-ID-Richtlinie:

In diesem Szenario wird höchstwahrscheinlich kein Benutzername und kein Kennwort angezeigt.

In der SAML-Antwort gibt es keine gültige Assertion, und der Statuscode lautet wie folgt:

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

Überprüfen Sie, ob die Anspruchsregel auf der IDP-Seite richtig definiert ist.

Unterschied in Fall/Name definiert in Anspruchsregel:

Der CUCM-FQDN in der Anspruchsregel sollte genau mit dem auf dem eigentlichen Server angegebenen übereinstimmen.

Sie können den Eintrag in der XML-Metadatendatei von IDP mit dem Eintrag in CUCM vergleichen, indem Sie den Befehl **show network cluster/show network etho details** command in CLI von CUCM ausführen.

Falsche Uhrzeit:

Das NTP zwischen CUCM und IDP hat einen Unterschied von mehr als 3 Sekunden, der im Bereitstellungsleitfaden erlaubt ist.

Assertion Signer Not Trusted:

Zum Zeitpunkt des Austauschs der Metadaten zwischen IDP und CUCM (Service Provider).

Zertifikate werden ausgetauscht, und falls ein Widerruf des Zertifikats erfolgt, sollten die Metadaten erneut ausgetauscht werden.

DNS-Fehlkonfiguration/Keine Konfiguration

DNS ist die Hauptanforderung für die SSO-Funktion. Führen Sie **show network etho detail aus**, **utils diagnose test** auf der CLI aus, um zu überprüfen, ob DNS/Domain korrekt konfiguriert ist.

Bekannte Fehler

CSCuj66703

Das ADFS-Signaturzertifikat verlängert das IDP-Zertifikat und fügt es zwei Signaturzertifikate hinzu, sodass Sie auf Fehler stoßen. Sie müssen das nicht erforderliche Signaturzertifikat löschen.

CSCvf63462

Wenn Sie von CCM Admin zur Seite "SAML SSO" navigieren, wird Ihnen die Meldung "Die folgenden Server sind beim Versuch, den SSO-Status zu erhalten, fehlgeschlagen" angezeigt, gefolgt vom Knotennamen.

CSCvf96778

CTI-basierte SSO schlägt fehl, wenn der CUCM-Server in CCMAdmin//System/Server als IP-Adresse definiert wird.