

Cisco Unified Communications ManagerでのSSOのトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシュート](#)

[SSOのログインフロー](#)

[SAML応答のデコード](#)

[ログおよびCLIコマンド](#)

[一般的な問題](#)

[既知の障害](#)

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)でシングルサインオン(SSO)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CUCM
- Active Directoryフェデレーションサービス(ADFS)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

「CUCMでのシングルサインオンの設定」を参照してください。

- <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-ss0-deployment-guide--1151.html

SAML RFC 6596

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

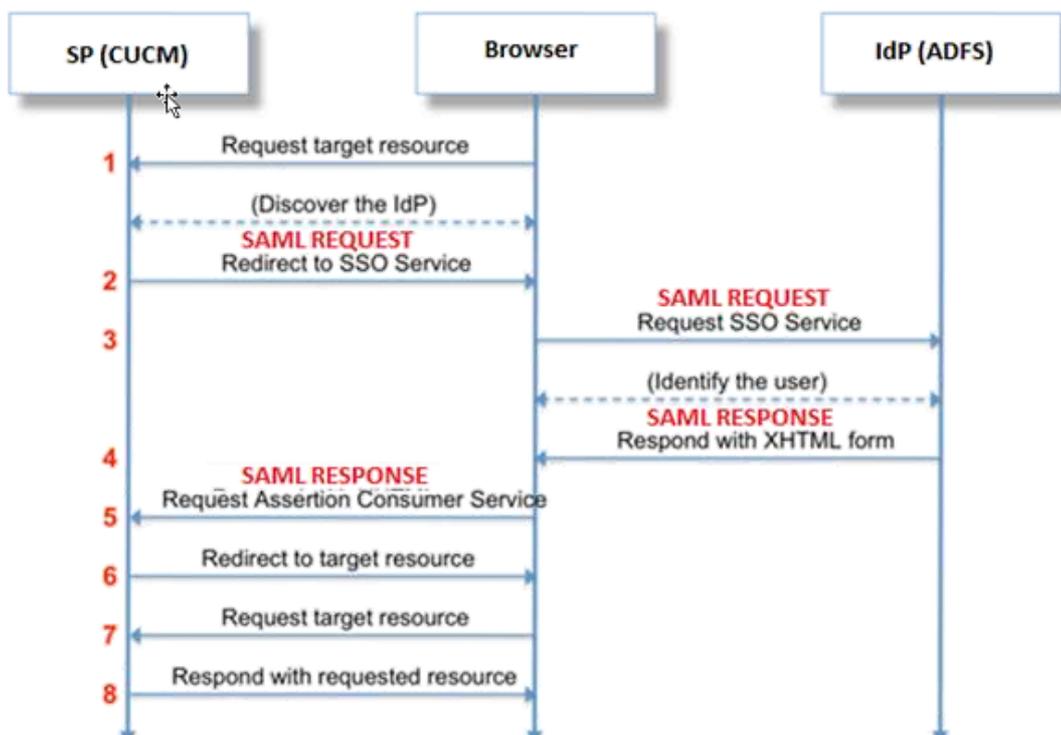
確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

SSOのログインフロー

Authentication Flow



SAML応答のデコード

メモ帳でのプラグインの使用++

次のプラグインをインストールします。

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

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

SSOログで、エンコードされた応答を含む文字列「authentication.SAMLAuthenticator - SAML Response is ::」を検索します。

このプラグインまたはオンラインSAMLデコードを使用して、XML応答を取得します。応答は、Pretty Printプラグインを使用して読み取り可能な形式で調整できます。

CUCM SAML応答の新しいバージョンでは、XML形式で「SPACSUtills.getResponse:response=<samlp:

応答xmlns:samlp="と入力し、Pretty Printプラグインを使用して印刷します。

Fiddlerを使用 :

このユーティリティは、リアルタイムトラフィックを取得してデコードするために使用できます。このガイドは同じです。<https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/>。

SAML要求 :

```
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>
```

SAML応答 (非暗号化) :

```
<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"
```


</samlp : 応答>

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

SAML応答が暗号化されている場合は、完全な情報が表示されず、完全な応答を表示するために Intrusion Detection & Prevention(IDP)の暗号化を無効にする必要があります。暗号化に使用される証明書の詳細は、SAML応答の「ds:X509IssuerSerial」の下にあります。

ログおよびCLIコマンド

CLI コマンド:

utils sso disable

このコマンドは、両方 (OpenAM SSOまたはSAML SSO) ベースの認証を無効にします。このコマンドは、SSOが有効になっているWebアプリケーションをリストします。指定したアプリケーションのSSOを無効にするよう求められたら、**Yes**と入力します。クラスタ内の場合は、両方のノードでこのコマンドを実行する必要があります。SSOは、グラフィカルユーザインターフェイス(GUI)から無効にし、Cisco Unity Connection Administrationの特定のSSOの下にある[Disable]ボタンを選択することもできます。

コマンド構文

utils sso disable

utils sso status

このコマンドは、SAML SSOのステータスと設定パラメータを表示します。各ノードのSSOステータスを個別に確認できます (有効または無効)。

コマンド構文

utils sso status

utils sso enable

このコマンドは、管理者がGUIからのみSSO機能を有効にすることを求める情報テキストメッセージを返します。このコマンドでは、OpenAMベースのSSOとSAMLベースのSSOの両方を有効にできません。

コマンド構文

```
utils sso enable
```

utils sso recovery-url enable

このコマンドは、リカバリURL SSOモードを有効にします。また、このURLが正常に動作していることを確認します。クラスタ内の場合は、両方のノードでこのコマンドを実行する必要があります。

コマンド構文

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

utils sso recovery-url disable

このコマンドは、そのノードのリカバリURL SSOモードを無効にします。クラスタ内の場合は、両方のノードでこのコマンドを実行する必要があります。

コマンド構文

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

set samltrace level <trace-level>

このコマンドは、エラー、デバッグ、情報、警告、または致命的なエラーを検出できる特定のトレースとトレースレベルを有効にします。クラスタ内の場合は、両方のノードでこのコマンドを実行する必要があります。

コマンド構文

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

show samltrace level

このコマンドは、SAML SSOのログレベル設定を表示します。クラスタ内の場合は、両方のノードでこのコマンドを実行する必要があります。

コマンド構文

```
show samltrace level
```

トラブルシューティング時に確認するトレース：

SSOログは、デフォルトでは詳細レベルに設定されません。

最初に**set samltrace level debug**コマンドを実行して、ログレベルをデバッグに設定し、問題を再現し、これらのログを収集します。

RTMTから：

Cisco Tomcat

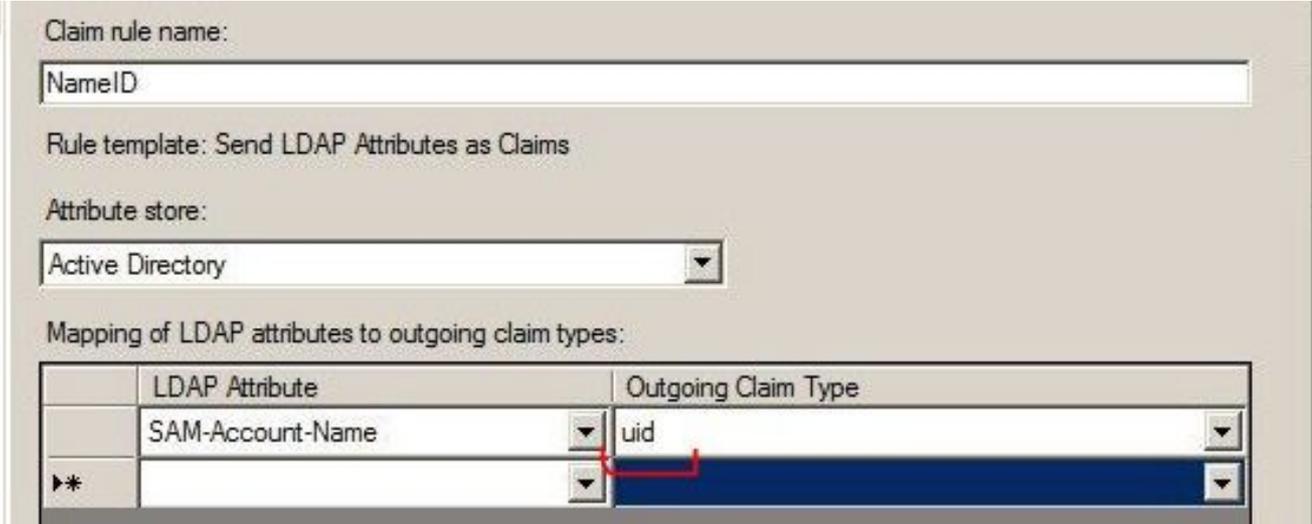
Cisco Tomcatセキュリティ

Cisco SSO

一般的な問題

一意の識別子(UID)の値が正しくありません：

これは正確にUIDである必要があり、CUCMではUIDを理解できません。



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
▶*		

クレームルールまたは誤ったNameIDポリシー：

このシナリオでは、ユーザ名とパスワードのプロンプトが表示されない可能性が高いです。

SAML応答に有効なアサーションがないため、ステータスコードは次のようになります。

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

クレームルールがIDP側で正しく定義されていることを確認します。

クレームルールで定義されたケース/名前の違い：

要求ルールのCUCM FQDNは、実際のサーバで指定されたFQDNと完全に一致している必要があります。

CUCMのCLIで**show network cluster/show network ethoo details**コマンドを実行すると、IDPのメタデータxmlファイルのエントリとCUCMのエントリを比較できます。

不正確な時間：

CUCMとIDPの間のNTPの違いは、導入ガイドで[許可されている3秒を超えています。](#)

Assertion Signer Not Trusted:

IDP (サービスプロバイダー) とCUCM (サービスプロバイダー) 間のメタデータの交換時。

証明書が交換され、証明書の失効が行われた場合は、メタデータを再度交換する必要があります。

DNSの設定ミス/設定なし

DNSは、SSOが動作するための主な要件です。CLIで**show network ethoo detail**、**utils diagnose test**を実行し、DNS/ドメインが正しく設定されていることを確認します。

既知の障害

[CSCuj66703](#)

ADFS署名証明書が更新され、CUCM(SP)へのIDP応答に2つの署名証明書が追加されるため、不具合が発生します。必要のない署名証明書を削除する必要があります

[CSCvf63462](#)

CCM AdminからSAML SSOページに移動すると、「The following servers failed during get SSO Status」というメッセージが表示され、ノード名が表示されます。

[CSCvf96778](#)

CCMAdmin//System/SeverでCUCMサーバをIPアドレスとして定義すると、CTIベースのSSOが失敗します。