# Azure IdPとのUCCE SSO統合のトラブルシューティング

## 内容



## はじめに

このドキュメントでは、Microsoft Azure IdPとのUCCE SSO統合の実行中に発生する一般的な問題のトラブルシューティング方法について説明します。


著者：Cisco TACエンジニア、Anurag Atul Agarwal


## 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。

- Security Assertion Markup Language(SAML)2.0
- Cisco Unified/Packaged Contact Center Enterprise UCCE/PCCE
- シングル サインオン（SSO）
- シスコアイデンティティサービス(Id)
- アイデンティティプロバイダー(IdP)

### 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。

- Azure IdP
- UCCE 12.0.1
- Cisco IdS 12.0.1

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、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

このドキュメントでは、AzureベースのSSO向けのCisco Identity Service(IdS)とIdentity Provider(IdP)の統合中に発生する一般的な問題のいくつかと、その潜在的な修正について説明します。 SSO統合の問題をトラブルシューティングするには、次のログを収集することが常に推奨されます。

- Cisco IdSログ：コレクションへのリンク：IDSログ
- ブラウザのコンソールログ
- IdPからのログ

## 問題：証明書が一致しない

テストSSOが失敗し、「認証は成功しましたがSAML応答を処理できませんでした」というメッセージが表示され、IdSログに「例外com.sun.identity.saml2.common.SAML2Exception：署名証明書がエンティティメタデータで定義されている内容と一致しません」というエラーメッセージが表示されます。

## 解決方法

Azureで証明書を確認し、署名アルゴリズムを設定します。IdSバージョンに基づいてサポートされているハッシュアルゴリズムと一致していることを確認します。『機能ガイド』の「シングルサインオン」の章を参照して、サポートされているセキュアハッシュアルゴリズムを確認してください。最新のIdPメタデータファイルをダウンロードし、Identity Service Managementユーザインターフェイスを介してCisco IdSにアップロードします。

## 問題：AADSTS900235 – 認証コンテキストの問題

テストSSOがMicrosoftページにリダイレクトされ、失敗して「申し訳ありませんが、サインインできません」というメッセージが表示されます。
AADSTS900235: SAML認証要求のRequestedAuthenticationContext Comparisonの値はExactである必要があります。受信した値：最小

## 解決方法

AuthContextは、バグCSCvm69290で説明されているように調整する必要がある場合があります を参照。IdSで回避策を実行するには、Cisco TACにお問い合わせください。

## 問題：SAML応答が署名されていない

テストSSOは次のメッセージで失敗します。「IdS was unable to process the SAML response even though the authentication was successful」というメッセージが表示され、IdSログに「SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: Response is not signed」というエラーメッセージが出力されます。

## 解決方法

Azure IdPはIdSに署名されたアサーションを送信する必要があります。 署名オプションを含むようにAzureの設定を変更します： SAML応答とアサーションに署名します

## 問題：クレームルールの問題

テストSSOが失敗し、メッセージ「IdP configuration error: SAML processing failed.Could not retreive user principal from SAML response.」というエラーメッセージが出力され、IdSログに「SAML response processing failed with exception com.sun.identity.saml.common.SAMLException: Could not retreive user principal from SAML response.」というエラーメッセージが出力されます。

## 解決方法

このエラーは、Azureで構成されている'Claim names'が正しくないことを示しています。これは、UID、NameIDなどの他の属性で発生する可能性があり、異なる属性名を持つ同様のエラーが生成されます。これを修正するには、Azure内の任意の属性を'schemas.xmlsoap.org/ws/2005/05/identity/claims/<attribute_name>'の形式で見つけます。実際の属性名より前の部分をすべて削除します。

このセクションでは、機能ガイドのADFSの構成例を示します。これは、Azureでレプリケートする必要があります。

ADFSの設定例

## 問題： AADSTS50011 – 応答URLが一致しない

テストSSOがMicrosoftページにリダイレクトされ、失敗して次のメッセージが表示されます：「申し訳ありませんが、サインインできません。
AADSTS50011：要求で指定された応答URLが、アプリケーションに対して構成された応答URLと一致しません"

# 解決方法

Cisco TACにお問い合わせください。これが失敗したIdSノードのルートで「Assertion Consumer Service」パラメータをチェックする必要があります。パラメータが正しい場合、Microsoft Azureはこれをトラブルシューティングする必要があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。