Troubleshoot UCCE SSO Integration with Azure IdP

Contents

Introduction

This document describes how to troubleshoot some common issues faced while performing UCCE SSO integration with Microsoft Azure IdP.

Contributed by Anurag Atul Agarwal, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Security Assertion Markup Language (SAML) 2.0
- Cisco Unified/Packaged Contact Center Enterprise UCCE/PCCE
- Single Sign On (SSO)
- Cisco Identity Service (IdS)
- Identity Provider (IdP)

Components Used

The information in this document is based on these software and hardware versions:

- Azure IdP
- UCCE 12.0.1
- Cisco IdS 12.0.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes some of the common issues faced during integration of Cisco Identity Service (IdS) and Identity Provider (IdP) for Azure based SSO and their potential fixes. It is always recommended to gather these logs to troubleshoot issues with SSO integration:

- Cisco IdS logs: Link to collection: IDS logs
- Browser console logs
- Any logs from IdP

Problem: Certificate Does Not Match

Test SSO fails with message 'IdS was unable to process the SAML response even though, the authentication was successful' and IdS logs print the error message: "SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: The signing certificate does not match what's defined in the entity metadata'"

Solution

Verify the certificate and setting **Signing Algorithm** in Azure. Ensure it matches with the supported hash algorithm based on the IdS version. Refer to Chapter 'Single Sign-On' in Features Guide and verify the supported **secure hash algorithm**. Download the latest IdP metadata file and upload it to Cisco IdS via the Identity Service Management user interface.

Problem: AADSTS900235 - Authentication Context Issue

Test SSO redirects to Microsoft page and fails with message: "Sorry, but we’re having trouble signing you in."
AADSTS900235: SAML authentication request's RequestedAuthenticationContext Comparison value must be **Exact**. Received value: **Minimum**

Solution

AuthContext might need to be tuned as described in bug CSCvm69290 . Please contact Cisco TAC to perform the workaround in IdS.

Problem: SAML Response Is Not Signed

Test SSO fails with message, IdS was unable to process the SAML response even though, the authentication was successful' and IdS logs print the error message: "SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: Response is not **signed**."

Solution

Azure IdP needs to send signed assertion to IdS. Modify Azure setting to have signing option: **Sign SAML response and assertion**

Problem: Issue with Claim Rules

Test SSO fails with message 'IdP configuration error : SAML processing failed. Could not retreive user principal from SAML response.' and IdS logs print the error message: "SAML response processing failed with exception com.sun.identity.saml.common.SAMLException: Could not retreive **user principal** from SAML response."

Solution

This error points to wrong 'Claim names' configured in Azure. This could happen with other attributes like UID,NameID etc. and similar errors with different attribute names is generated. To fix this, locate any attribute in Azure in this format, 'schemas.xmlsoap.org/ws/2005/05/identity/claims/<attribute_name>'. Remove everything before the actual attribute name.

This section provides the example configuration for ADFS in the Features guide and that needs to be replicated in Azure.

ADFS Example Configuration

Problem: AADSTS50011 - Reply URL Does Not Match

Test SSO redirects to Microsoft page and fails with message: "Sorry, but we're having trouble signing you in.
AADSTS50011: The reply URL specified in the request does not match the reply URL's configured for the application"

Solution

Please contact Cisco TAC. '**Assertion Consumer Service**' parameter needs to be checked in root on the IdS node where this fails. If the parameter is correct, Microsoft Azure has to troubleshoot this.