Introduction

The Security Assertion Markup Language (SAML) interaction between Cisco Identity Service (IdS) and Active Directory Federation Services (AD FS) via a browser is the core of Single-Sign on (SSO) log in flow. This document will help you in debugging issues related to configurations in Cisco IdS and AD FS, along with the recommended action to resolve them.

Cisco IdS Deployment Models

Product Deployment
UCCX   Co-resident
PCCE Co-resident with CUIC (Cisco Unified Intelligence Center) and LD (Live Data)
UCCE Co-resident with CUIC and LD for 2k deployments.
Standalone for 4k and 12k deployments.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Contact Center Express (UCCX) Release 11.5 or Cisco Unified Contact Center Enterprise Release 11.5 or Packaged Contact Center Enterprise (PCCE) Release 11.5 as applicable.
- Microsoft Active Directory - AD installed on Windows Server
- IdP (Identity Provider) - Active Directory Federation Service (AD FS) Version 2.0/3.0

Components Used

This document is not restricted to specific software and hardware versions.

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, make sure that you understand the potential impact of any command.

Background Information

After the trust relationship is established between Cisco IdS and AD FS (see here for details, common for UCCX and UCCE), the administrator is expected to run Test SSO Set up in the Settings page of Identity Service Management to ensure that the configuration between Cisco IdS and AD FS works fine. If the test fails, use the appropriate applications and suggestions given in this guide to resolve the issue.

Applications and logs that can be handy in debugging

Application/Log Details

<table>
<thead>
<tr>
<th>Application/Log Details</th>
<th>Where to find the tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IdS log</td>
<td>Use RTMT to get Cisco IdS logs. For information on how to use RTMT see Guide to Use RTMT</td>
</tr>
<tr>
<td>Fedlet Logs</td>
<td>Use RTMT to get Fedlet logs. The location for Fedlet log is same as the Cisco IdS logs. The fedlet logs start with the prefix fedlet-</td>
</tr>
<tr>
<td>Cisco IdS API metrics</td>
<td>Use RTMT to get API metrics. Please note that the RTMT name is Cisco Identity Service.</td>
</tr>
</tbody>
</table>

Cisco IdS logger will log any error that happened in Cisco IdS.
Fedlet logs will give more details about any SAML errors that happens in Cisco IdS
API metrics can be used to look into and validate any errors that Cisco IdS APIs may have returned
This will appear under a separate folder **metrics**. Please note that **saml_metrics.csv** and **authorize_metrics.csv** are the relevant metrics for this document.

In AD FS machine, navigate to **Event Viewer >Applications and Service Logs >AdFS 2.0 > Admin**

**Flow Diagram with Debugging options**

The various steps for SSO authentication is shown in the image along with and debugging artifacts at each step in case of a failure in that step.

This table gives the details on how to identify failures at each step of SSO in the browser. The different tools and how can they help in debugging is specified as well.

<table>
<thead>
<tr>
<th>Step</th>
<th>How to identify the failure in the Browser</th>
<th>Tools/Log</th>
<th>Configurations to look at</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthCode Request Processing by Cisco IdS</td>
<td>In case of failure, the browser is not redirected to SAML endpoint or AD FS, a JSON error is shown by Cisco IdS, which indicates that the Client Id or Redirect URL is invalid.</td>
<td>Cisco IdS logs- Indicates the errors which occur while the authcode request is validated and processed. Cisco IdS API metrics - Indicates the number of requests processed and failed.</td>
<td>Client Registration</td>
</tr>
<tr>
<td>SAML Request Initiation by Cisco IdS</td>
<td>During failure, the browser is not redirected to AD FS, and an error page/message will be shown by Cisco IdS.</td>
<td>Cisco IdS logs- Indicates whether there is an exception or not while the request is initiated. Cisco IdS API metrics - Indicates the number of requests processed and failed.</td>
<td>Cisco IdS in NOT_CONFIGURED state.</td>
</tr>
<tr>
<td>SAML Request Processing</td>
<td>Any failure to process this request will result in an error page being displayed by AD FS server instead</td>
<td>Event Viewer in AD FS- Indicates the errors which occur while the request is processed.</td>
<td>Relying Party Trust Configuration in IdP</td>
</tr>
</tbody>
</table>
by AD FS: of the login page.

Sending SAML Response by AD FS: Any failure to send the response results in an error page being displayed by AD FS server after the valid credentials are submitted.

Event Viewer in AD FS: Indicates the errors which occur while the request is processed.

SAML Browser Plugin - Helps to see the SAML request which is sent to the AD FS.

Relying Party Trust Configuration in IdP

Form Authentication setting in AD FS.

Event Viewer in AD FS: Indicates the error if AD FS sends a SAML response without a successful status code.

SAML Browser Plugin - Helps to see the SAML response sent by AD FS to identify what is wrong.

Cisco IdS log - Indicates the error/exception occurred during the processing.

Cisco IdS API metrics - Indicates the number of requests processed and failed.

Claim Rules Configuration

Message and Assertion Signing

Authcode Request Processing by Cisco IdS

The starting point of SSO login, as far as the Cisco IdS is concerned, is the request for an authorization code from an SSO enabled application. The API request validation is done to check if it is a request from a registered client. A successful validation results in the browser being redirected to the SAML endpoint of Cisco IdS. Any failure in the request validation results in an error page/JSON (JavaScript Object Notation) being sent back from Cisco IdS.

Common Errors Encountered during this Process

1. Client Registration Not Done

   Problem Summary: Login request fails with 401 error on the browser.
   **Browser:**
   401 error with this message: {"error":"invalid_client","error_description":"Invalid ClientId."
   **Cisco IdS Log:**
   2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] WARN com.cisco.ccbu.ids IdSConfigImpl.java:121 - Client Id: fb308a80050b2021f974f48a72ef9518a5e7ca69 does not exist 2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] ERROR com.cisco.ccbu.ids IdSOAuthEndPoint.java:45 - Exception processing auth request. org.apache.oltu.oauth2.common.exception.OAuthProblemException: invalid_client, InvalidClientId. at org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemException.java:59) at com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthorizeValidator.java:55) at com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSAuthorizeValidator.java:70) at org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.java:63)
   **Possible Cause:**
   The client registration with Cisco IdS is not complete.
   **Recommended Action:** Navigate to Cisco IdS Management console and confirm if the client is registered successfully before proceeding with SSO.

2. User Accesses Application using IP Address/ Alternate Host Name

   Problem: Login request fails with 401 error on the browser.
Summary

Error Message
401 error with this message: {"error":"invalid_redirectUri","error_description":"invalid Redirect Uri"}

Possible Cause
User accesses application using IP Address/ Alternate Host Name.

Recommended Action
Navigate to Cisco IdS Management console and confirm if the client is registered with the correct redirect URL and the same is used to access the application.

SAML Request Initiation by Cisco IdS

SAML Endpoint of Cisco IdS is the starting point of the SAML flow in SSO based login. The initiation of the interaction between Cisco IdS and AD FS is triggered in this step. The prerequisite here is that the Cisco IdS should know the AD FS to connect to as the corresponding IdP metadata should be uploaded to Cisco IdS for this step to succeed.

Common Errors Encountered during this Process

1. AD FS Metadata not added to Cisco IdS

Problem Summary
Login request fails with 503 error on the browser.

Error Message
503 error with this message: {"error":"service_unavailable","error_description":"SAML Metadata is not initialized"}

Possible Cause
Idp Metadata is not available in Cisco IdS. Trust establishment between Cisco IdS and AD FS is not complete.

Recommended Action
Navigate to Cisco IdS Management console and see if the IdS is in Not Configured state. Confirm if IdP metadata is uploaded or not. If not, upload the IdP metadata downloaded from AD FS. For more details see here.

SAML Request Processing by AD FS

SAML Request Processing is the first step in the AD FS in the SSO flow. The SAML request sent by the Cisco IdS is read, validated and deciphered by AD FS in this step. Successful processing of this request results in two scenarios:

1. If it is a fresh log in in a browser, AD FS shows the login form. If it is a relogin of an already authenticated user from an existing browser session, AD FS attempts to send the SAML response back directly.

Note: The main prerequisite for this step is for the AD FS to have the replying party trust configured.

Common Errors Encountered during this Process

1. AD FS not having the latest Cisco IdS’ SAML certificate.
AD FS not showing the login page, instead shows an error page.

Browser
AD FS shows an error page similar to this:
There was a problem accessing the site. Try to browse to the site again.
If the problem persists, contact the administrator of this site and provide the reference number.
Reference number: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e

AD FS Event Viewer
The Federation Service encountered an error while processing the SAML authentication request.

Additional Data
Exception details: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException:
MSIS0038: SAML Message has wrong signature. Issuer: 'myuccx.cisco.com'.

Possible Cause
Relying party trust is not established or Cisco IdS certificate has changed, but the same is not uploaded to the AD FS.

Recommended Action
Establish trust between AD FS and Cisco IdS with the latest Cisco IdS certificate.
Please ensure that the Cisco IdS Certificate is not expired. You can see the status dashboard in Cisco Identity Service Management. If so, regenerate the certificate in the Settings page.
For more details on how to establish metadata trust across ADFS & Cisco IdS see, here

SAML Response Sending by AD FS

The ADFS sends the SAML response back to the Cisco IdS via the browser after the user is successfully authenticated. ADFS can send a SAML response back with a status code which indicates Success or Failure. If form authentication is not enabled in AD FS then this will indicate a Failure response.

Common Errors Encountered during this Process

1. Form Authentication is not enabled in AD FS

Browser shows NTLM login, and then fails without successfully redirecting to Cisco IdS after sending SAML Response

SAML Response Processing by Cisco IdS

In this stage, Cisco IdS gets a SAML response from AD FS. This response could contain a status code that indicates Success or Failure. An error response from AD FS results into an error page and the same has to be debugged.
During a successful SAML response, the processing of the request can fail for these reasons:

- Incorrect IdP (AD FS) metadata.
- Failure to retrieve expected outgoing claims from AD FS.
- Cisco IdS and AD FS clocks are not synchronized.

### Common Errors Encountered during this Process

#### 1. AD FS Certificate in Cisco IdS is not the latest.

<table>
<thead>
<tr>
<th>Problem Summary</th>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login request fails with 500 error on the browser with Error Code as invalidSignature.</td>
<td>2016-04-13 12:42:15.896 IST(+0530) default ERROR [IdSEndPoints-0] com.cisco.ccbu.idsIdSEndPoint.java:102 - Exception processing request com.sun.identity.saml2.common.SAML2Exception: The signing certificate does not match what's defined in the entity metadata. at com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) at com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseImpl.java:985) at com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985) at com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)</td>
</tr>
<tr>
<td>SAML Response processing</td>
<td>No error</td>
</tr>
<tr>
<td>Browser: 500 error with this message in the browser: Error Code: invalidSignature</td>
<td>SAML Response processing failed as IdP certificate is different from what is available in Cisco IdS.</td>
</tr>
<tr>
<td>Message: The signing certificate does not match what's defined in the entity metadata.</td>
<td>Download the latest AD FS metadata from: https://&lt;ADFSServer&gt;/federationmetadata/2007-06/federationmetadata.xml and upload it to Cisco IdS via the Identity Service Management user interface. For details, see Configure Cisco IdS and AD FS</td>
</tr>
</tbody>
</table>

#### 2. Cisco IdS and AD FS clocks are not Synchronized.

<table>
<thead>
<tr>
<th>Problem Summary</th>
<th>Error Message</th>
</tr>
</thead>
</table>
SAML Viewer:
Look for the NotBefore and NotOnOrAfter fields
<Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45:03.325Z">

Possible Cause
Time in Cisco IdS and IdP system is out of sync.

Recommended Action
Synchronize the Time in Cisco IdS and AD FS system. It is recommended that AD FS system and Cisco IdS are time synchronized using NTP Server.

3. Wrong Signature Algorithm (SHA256 vs SHA1) in AD FS

Problem Summary
Login request fails with 500 error on the browser with status code:urn:oasis:names:tc:SAML:2.0:status:Responder
Error Message in AD FS Event View Log – Wrong Signature Algorithm(SHA256 vs SHA1)
(data) SAML Response processing
Browser
500 error with this message:
IdP configuration error : SAML processing failed
SAML assertion failed from IdP with status code: urn:oasis:names:tc:SAML:2.0:status:Responder. Verify IdP configuration and try again.

AD FS Event Viewer:
SAML request is not signed with expected signature algorithm. SAML request is signed with signature algorithm http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 .
Expected signature algorithm is http://www.w3.org/2000/09/xmldsig#rsa-sha1

Cisco IdS Log:
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAML response processing failed

Possible Cause
AD FS is configured to use SHA-256.

Recommended Action
Update AD FS to use SHA-1 for signing and encryption.
1. RDP to the AD FS system.
2. Open AD FS console.
3. Select the Relying Party Trust and click Properties
4. Select the Advanced tab.
5. Select SHA-1 from the drop-down list.
4. Outgoing Claim Rule not Configured Correctly

Problem Summary
Login request fails with 500 error on the browser with message "Could not retrieve user identifier from SAML response./Could not retrieve user principal from SAML response." uid and/or user_principal not set in the outgoing claims.

Step of Failure
SAML Response processing

Error Message

**Browser:**
500 error with this message:
IdP configuration error : SAML processing failed.
Could not retrieve user identifier from SAML response./Could not retrieve user principal from SAML response.

**AD FS Event Viewer:**
No error

**Cisco IdS Log:**
ERROR com.cisco.ccbu.ids.IdSSAMLAsyncServlet.java:294 - SAML response processing failed
com.sun.identity.saml.common.SAMLException: Could not retrieve user identifier from SAML response.

Possible Cause
Mandatory outgoing claims (uid and user_principal) are not configured correctly in the Claim Rules. If you have not configured the NameID claim rule or either uid or user_principal is not configured correctly, Cisco IdS indicates that user_principal is not retrieved since this is the property that Cisco IdS looks for. If uid is not mapped correctly, Cisco IdS indicates that uid is not retrieved.

Under AD FS claim rules, ensure that attributes mapping for "user_principal" and "uid" are defined as in the IdP Configuration guide.

Recommended Action
Under AD FS claim rules, ensure that attributes mapping for "user_principal" and "uid" are defined as in the IdP Configuration guide.

1. RDP to AD FS system.
2. Edit the Claim Rules for the relying party trust.
3. Verify that the user principal and uid are mapped correctly

5. Outgoing Claim Rule is not configured correctly in a Federated AD FS

**Problem Summary**
Login request fails with 500 error on the browser with message "Could not retrieve user id from SAML response. or Could not retrieve user principal from SAML response." when the AD FS is a Federated AD FS.

**Step of Failure**
SAML Response processing

**Browser**
500 error with this message:
IdP configuration error : SAML processing failed
Could not retrieve user identifier from SAML response./ Could not retrieve user principal from SAML response.

**Error Message**

**AD FS Event Viewer:**
No error

**Cisco IdS Log:**

ERROR com.cisco.ccbu.ids.IdSSAMLAsyncServlet.java:294 - SAML response processing failed
com.sun.identity.saml.common.SAMLException: Could not retrieve user identifier from SAML response.
at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServlet.java:231)
at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:263)
Possible Cause

In a Federated AD FS there are more configurations required that could be missing.

Recommended Action

Check if the AD FS configuration in Federated AD is done as per the section For a Multi-domain Configuration for Federated AD FS in Configure Cisco IdS and AD FS

6. Custom Claim Rules not Configured Correctly

Problem Summary

Login request fails with 500 error on the browser with message "Could not retrieve user identifier from SAML response. Could not retrieve user principal from SAML response." uid and/or user_principal not set in the outgoing claims.

Step of Failure

SAML Response processing

Browser

500 error with this message:
SAML assertion failed from IdP with status code:
Verify IdP configuration and try again.

AD FS Event Viewer:

The SAML authentication request had a NameID Policy that could not be satisfied.
Requestor: myids.cisco.com
Name identifier format: urn:oasis:names:tc:SAML:2.0:nameid-format:transient
SPNameQualifier: myids.cisco.com
Exception details:
This request failed.
User Action
Use the AD FS 2.0 Management snap-in to configure the configuration that emits the required name identifier.

Cisco IdS Log:

Possible Cause

Custom claim rule is not configured correctly.

Recommended Action

Under AD FS claim rules, ensure that attributes mapping for "user_principal" and "uid" are defined as in configuration guide (which guide?).

1. RDP to AD FS system.
2. Edit the Claim Rules for custom claim rules.
Verify that the AD FS and Cisco IdS fully qualified domain names are given.

3. Too Many Requests to AD FS.

<table>
<thead>
<tr>
<th>Problem Summary</th>
<th>Login request fails with 500 error on the browser with status code:urn:oasis:names:tc:SAML:2.0:status:Responder. Error Message in AD FS Event View Log indicates there are too many requests to AD FS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step of Failure</td>
<td>SAML Response processing</td>
</tr>
<tr>
<td>Browser Error Message</td>
<td>500 error with this message: IdP configuration error : SAML processing failed</td>
</tr>
</tbody>
</table>
SAML assertion failed from IdP with status code: urn:oasis:names:tc:SAML:2.0:status:Responder. Verify IdP configuration and try again.

AD FS Event Viewer:
Microsoft.IdentityServer.Web.InvalidRequestException:
MSIS7042: The same client browser session has made '6' requests in the last '16' seconds. Contact your administrator for details.

EventXml:

Cisco IdS Log

Possible Cause
There are too many requests coming to AD FS from the same browser session.

Recommended Action
1. Check AD FS Windows Event Viewer.
2. Recheck the Relying Party Trust Settings. For more details, see Configure Cisco IdS and AD FS.
3. Relogin.

8. AD FS is not Configured to Sign both Assertion and Message.

Problem Summary
Login request fails with 500 error on the browser with Error Code:invalidSignature

Step of Failure
SAML Response processing
Browser
500 error with this message:
Error Code:invalidSignature
Message:Invalid signature in ArtifactResponse.

Cisco IdS Log:
AD FS is not configured to sign both Assertion and Message.

1. Run the AD FS powershell command: `Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Identifier> -SamlResponseSignature "MessageAndAssertion"
2. RDP to AD system.
3. Open **Powershell**.
4. Add Windows PowerShell snap-ins to the current session. This step may not be required in ADFS 3.0 since the CmdLet is already installed as a part of adding the roles and features.
5. Add AD FS Relying party trust for message and assertion.
Related Information

This is related to the configuration of Identity Provider described in the article: