Contents

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	Where to find the tool
Cisco IdS log	Cisco IdS logger will log any error that happened in Cisco IdS.	Use RTMT to get Cisco IdS logs. F information on how to use RTMT se Guide to Use RTMT Please note that the RTMT name is **Cisco Identity Service**. In order to the logs, navigate to **Cisco Identity** **Service > log**
Fedlet Logs	Fedlet logs will give more details about any SAML errors that happens in Cisco IdS	Use RTMT to get Fedlet logs. The location for Fedlet log is same the Cisco IdS logs. The fedlet logs start with the prefix **fedlet-**
Cisco IdS API metrics	API metrics can be used to look into and validate any errors that Cisco IdS APIs may have returned	Use RTMT to get API metrics. Please note that the RTMT name is

	and number of requests that are processed by Cisco idS	**Cisco Identity Service** 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.
Event Viewer in AD FS	Allows users to view the event logs in the system. Any error in AD FS while processing the SAML request/sending the SAML response will be logged here.	In AD FS machine, navigate to **Eve Viewer >Applications** and **Service Logs >AdDFS 2.0 > Admin** In Windows 2008, launch Event Vie from **Control Panel > Performanc and Maintenance > Administrativ Tools** In Windows 2012, launch it from Control Panel\System and Security\Administrative Tools. Please look at your windows documentation to see where to find Event Viewer.
SAML Viewer	A SAML Viewer will help in looking at the SAML Request and Response that are sent from/to Cisco IdS. This browser application is very useful for the analysis of SAML Request/Response.	These are some suggested SAML viewers that you can use for looking the SAML request and response 1. Fiddler How to use fiddler wit AD FSFiddler Chrome Plugin 2. SAML Tracer - Firefox 3. SAML Chrome Panel

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.

Step	**How to identify the failure in the Browser**	**Tools/Log**	**Configurations to look at**
AuthCode Request Processing by Cisco IdS	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.	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.	Client Registration
SAML Request Initiation by Cisco IdS	During failure, the browser is not redirected to AD FS, and an error page/message will be shown by Cisco IdS.	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.	Cisco IdS in NOT_CONFIGURED state.
SAML Request Processing	Any failure to process this request will result in an error page being displayed by AD FS server instead	Event Viewer in AD FS- Indicates the errors which occur while the request is processed.	Relying Party Trust Configuration in IdP

by AD FS	of the login page.	SAML Browser Plugin - Helps to see the SAML request which is sent to the AD FS.	
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.	• Relying Party Trust Configuration in IdP • Form Authentication setting in AD FS.
SAML Response processing by Cisco IdS	Cisco IdS will show a 500 error with the error reason and a quick check page.	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.

Error Message	**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 IdSConfigI`
	`fb308a80050b2021f974f48a72ef9518a5e7ca69 does not exist 2016-09-02 00:16:58.604 IST(+05`
	`ERROR com.cisco.ccbu.ids IdSOAuthEndPoint.java:45 - Exception processing auth request.`
	`org.apache.oltu.oauth2.common.exception.OAuthProblemException: invalid_client, Invalid`
	`org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemExcepti`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthor`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSA`
	`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 succes the clients 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	**Browser:** 401 error with this message: {"error":"invalid_redirectUri","error_description":"Invlalid Redirect Uri"}
Possible Cause	User accesses application using IP Address/ Alternate Host Name. In SSO mode, if the application is accessed using IP, it does not work. Applications shou be accessed by the hostname by which they are registered in Cisco IdS. This issue can happen if user accessed an alternate host name that is not registered with Cisco IdS.
Recommended Action	Navigate to Cisco IdS Management console and confirm if the client is registered with th correct redirect URLand 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	**Browser:** 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 an FS is not complete.
Recommended Action	Navigate to Cisco IdS Management console and see if the IdS is in **Not Configured** s 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.

Problem Summary	AD FS not showing the login page, instead shows an error page.
Error Message	**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 nu problem. Reference number: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e **AD FS Event Viewer** The Federation Service encountered an error while processing the SAML authentication **Additional Data** `Exception details: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificatior MSIS0038: SAML Message has wrong signature. Issuer: 'myuccx.cisco.com'. at Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage message) at Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage(Cr createErrorMessageRequest) at Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest(Messag`
Possible Cause	Relying party trust is not established or Cisco IdS certificate has changed, but the same 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 dashl 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

Problem Summary	Browser shows NTLM login, and then fails without successfully redirecting to Cisco
Step of Failure	Sending SAML Response
Error Message	**Browser:** Browser shows NTLM login, but after successful log in, it fails with many redirects.
Possible Cause	Cisco IdS supports only form based authentication, Form authentication is not enal in AD FS.
Recommended Action	For more details on how to enable Form authentication see: ADFS 2.0 Form Authentication Setting ADFS 3.0 Form Authentication Setting

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.

Problem Summary	Login request fails with 500 error on the browser with Error Code as invalidSignature.
Step of Failure	SAML Response processing

Error Message	**Browser:**
	500 error with this message in the browser:
	Error Code: invalidSignature
	Message: The signing certificate does not match what's defined in the entity metadata.
	AD FS Event Viewer:
	No error
	Cisco IdS Log:
	`2016-04-13 12:42:15.896 IST(+0530) default ERROR [IdSEndPoints-0] com.cisco.ccbu.ids`
	`IdSEndPoint.java:102 - Exception processing request com.sun.identity.saml2.common.SAML2`
	`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(StatusResponse`
	`at com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985) a`
	`com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)`

Possible Cause	SAML Response processing failed as IdP certificate is different from what is available in
Recommended Action	Download the latest AD FS metadata from: **https://<ADFSServer>/federationmetadat** **06/federationmetadata.xml** And upload it to Cisco IdS via the Identity Service Managament user interface. For details , see Configure Cisco IdS and AD FS

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

Problem Summary	Login request fails with 500 error on the browser with the status code: urn:oasis:names:tc:SAML:2.0:status:Success
Step of Failure	SAML Response processing

Error Message	**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:Su
	configuration and try again.
	Cisco IdS Log
	`2016-08-24 18:46:56.780 IST(+0530) [IdSEndPoints-SAML-22] ERROR com.cisco.ccbu.ids`
	`IdSSAMLAsyncServlet.java:298 - SAML response processing failed with exception`
	`com.sun.identity.saml2.common.SAML2Exception: The time in SubjectConfirmationData is in`
	`com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:76`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609) at`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAM`
	`at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsync`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncS`
	`com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269) at`

```
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145) at
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615) at
java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread-
```

SAML Viewer:

Look for the NotBefore and NotOnOrAfter fields

<Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45

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 sy 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 SHA

Step of Failure

SAML Response processing

Error Message

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:R configuration and try again.

AD FS Event Viewer:

SAML request is not signed with expected signature algorithm. SAML request is signed 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 faile
com.sun.identity.saml2.common.SAML2Exception: Invalid Status code in Response. at
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) at
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:203
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSA
```

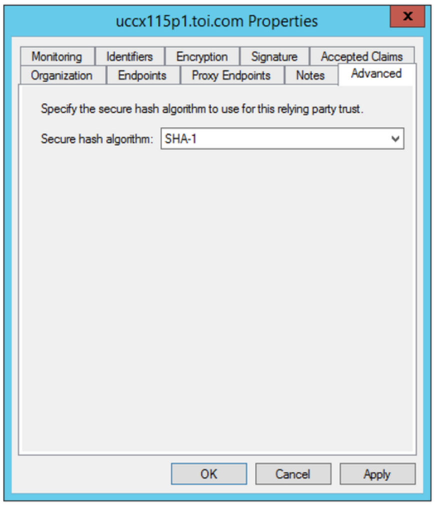
Possible Cause

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.


uccx115p1.toi.com Properties

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

4. Outgoing Claim Rule not Configured Correctly

Problem Summary

Login request fails with 500 error on the browser with message "Could not retrieve user i
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 f

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 retreive user identifier from SAM
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServ
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSer
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncS
```

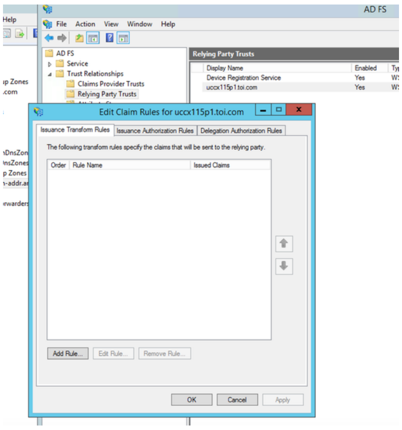
Possible Cause

Mandatory outgoing claims (uid and user_principal) are not configured correctly in the Cl
If you have not configured the NameID claim rule or either uid or user_principal is not co
If NameID rule is not configured or user_principal is not mapped correctly, Cisco IdS ind
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.

Recommended Action

Under AD FS claim rules, ensure that attributes mapping for "user_principal" and "uid" a
Configuration guide(which guide?).

1. RDP to AD FS system.
2. Edit the Claim Rules for the relying party trust.



Relying Party Trusts

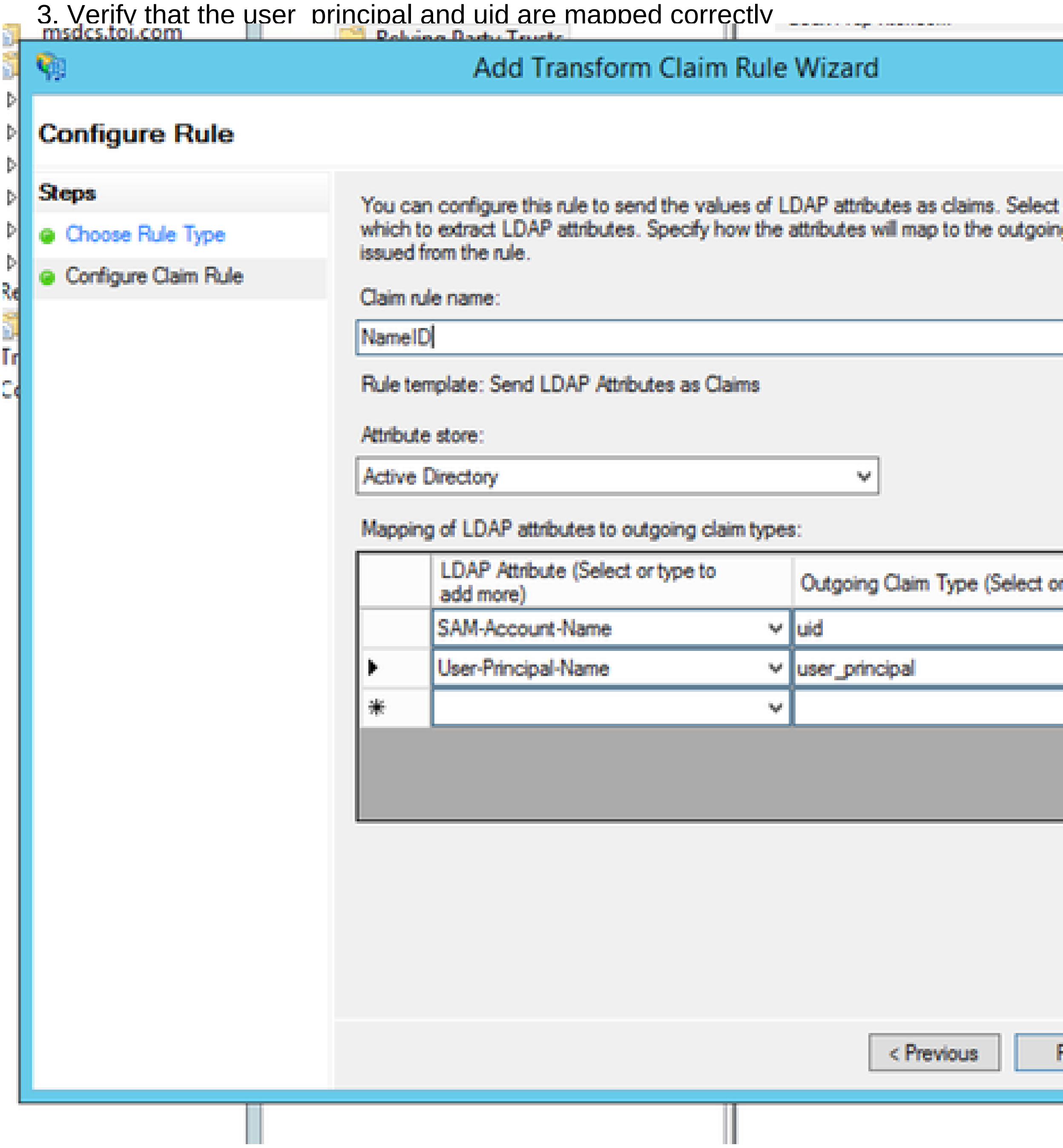
Display Name	Enabled	Ty
Device Registration Service	Yes	W:
uccx115p1.toi.com	Yes	W:

Edit Claim Rules for uccx115p1.toi.com

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

3. Verify that the user principal and uid are mapped correctly



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select which to extract LDAP attributes. Specify how the attributes will map to the outgoin issued from the rule.

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 (Select or type to add more)	Outgoing Claim Type (Select o
	SAM-Account-Name	uid
▶	User-Principal-Name	user_principal
✱		

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 i SAML response. or Could not retrieve user principal from SAML response." when the AD Federated AD FS.
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 response.
	AD FS Event Viewer:
	No error
	Cisco IdS Log:
	`ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAML response processing faile`
	`com.sun.identity.saml.common.SAMLException: Could not retreive user identifier from SAN`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServ`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSe`
	`at`

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncS
```

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 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 i 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:
SAML assertion failed from IdP with status code:
urn:oasis:names:tc:**SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:statu**
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:
MSIS1000: The SAML request contained a NameIDPolicy that was not satisfied by the is
NameIDPolicy: AllowCreate: True Format: urn:oasis:names:tc:SAML:2.0:nameid-format:
SPNameQualifier: myids.cisco.com. Actual NameID properties: null.
This request failed.
User Action
Use the AD FS 2.0 Management snap-in to configure the configuration that emits the rec
Cisco IdS Log:

```
2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAML2
failed with code: 1. Response status: <samlp:Status> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Requester"> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp:StatusCode> </s
</samlp:Status> for AuthnRequest: n/a 2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:299 - SAML response processing failed with
com.sun.identity.saml2.common.SAML2Exception: Invalid Status code in Response. at
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) at
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038
```

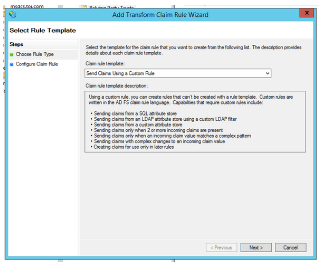
Possible Cause

Custom claim rule is not configured correctly.

Recommended Action

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

1. RDP to AD FS system.
2. Edit the Claim Rules for custom claim rules.



Add Transform Claim Rule Wizard

Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

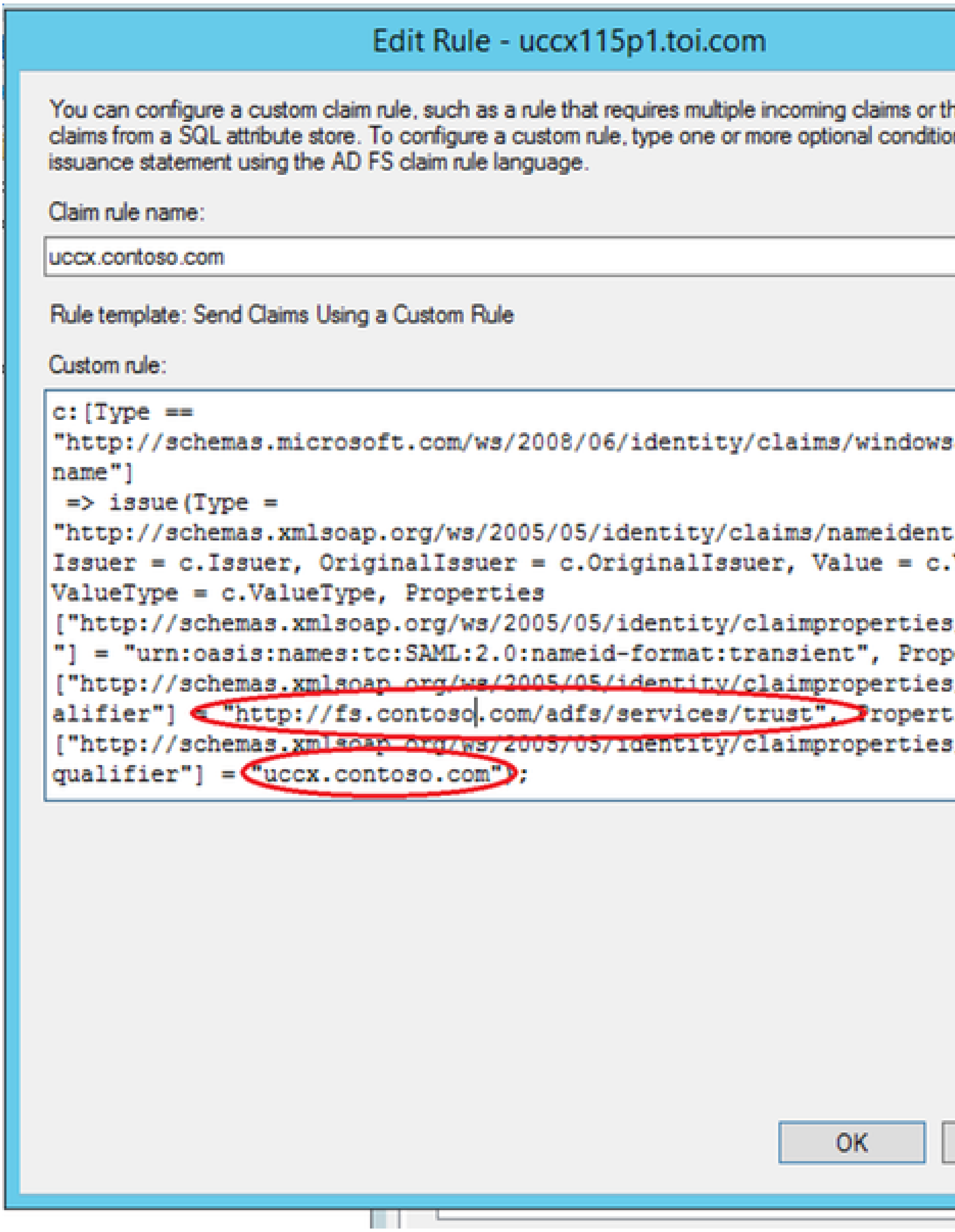
Claim rule template:
Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

3. Verify that the AD FS and Cisco IdS fully qualified domain names are given.



Edit Rule - uccx115p1.toi.com

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or th
claims from a SQL attribute store. To configure a custom rule, type one or more optional conditio
issuance statement using the AD FS claim rule language.

Claim rule name:

uccx.contoso.com

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windows
name"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameident
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.
ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties
"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Prop
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties
alifier"] = "http://fs.contoso.com/adfs/services/trust", Propert
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties
qualifier"] = "uccx.contoso.com");
```

7. Too Many Requests to 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 indicates there are too many requests to AD F
Step of Failure	SAML Response processing
Error Message	**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:R
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.**
  at Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectio
  at
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(M
response)

```
Event Xml: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Syste
FS 2.0" Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}" /> <EventID>364</EventID> <Versic
<Level>2</Level> <Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8000000000000001</Keywor
SystemTime="2016-04-19T12:14:58.474662600Z" /> <EventRecordID>29385</EventRecordID> <Co
ActivityID="{98778DB0-869A-4DD5-B3B6-0565AC17BFFE}"/> <Execution ProcessID="2264" Threa
<Channel>AD FS 2.0/Admin</Channel> <Computer>myadfs.cisco.com</Computer> <Security User
1680627477-1295527365-1502263146-1105"/> </System> <UserData> <Event xmlns:auto-
ns2="http://schemas.microsoft.com/win/2004/08/events"
xmlns="http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events"> <Eve
<Data>Microsoft.IdentityServer.Web.InvalidRequestException: MSIS7042: The same client b
'6' requests in the last '16' seconds. Contact your administrator for details. at
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(MSISSig
</Data> </EventData> </Event> </UserData> </Event>
```

Cisco IdS Log

```
2016-04-15 16:19:01.220 EDT(-0400) default ERROR [IdSEndPoints-1] com.cisco.ccbu.ids Id
Exception processing request com.sun.identity.saml2.common.SAML2Exception: Invalid Stat
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) at
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAM
```

Possible Cause

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

Recommended Action

This should typically not happen in production. But if you encounter this, you can:

1. Check AD FS Windows Event Viewer.
2. Recheck the Relying Party Trust Settings. For more details, *see* Configure Cisco Id
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

Error Message

Browser

500 error with this message:
Error Code:invalidSignature
Message:Invalid signature in ArtifactResponse.

Cisco IdS Log:

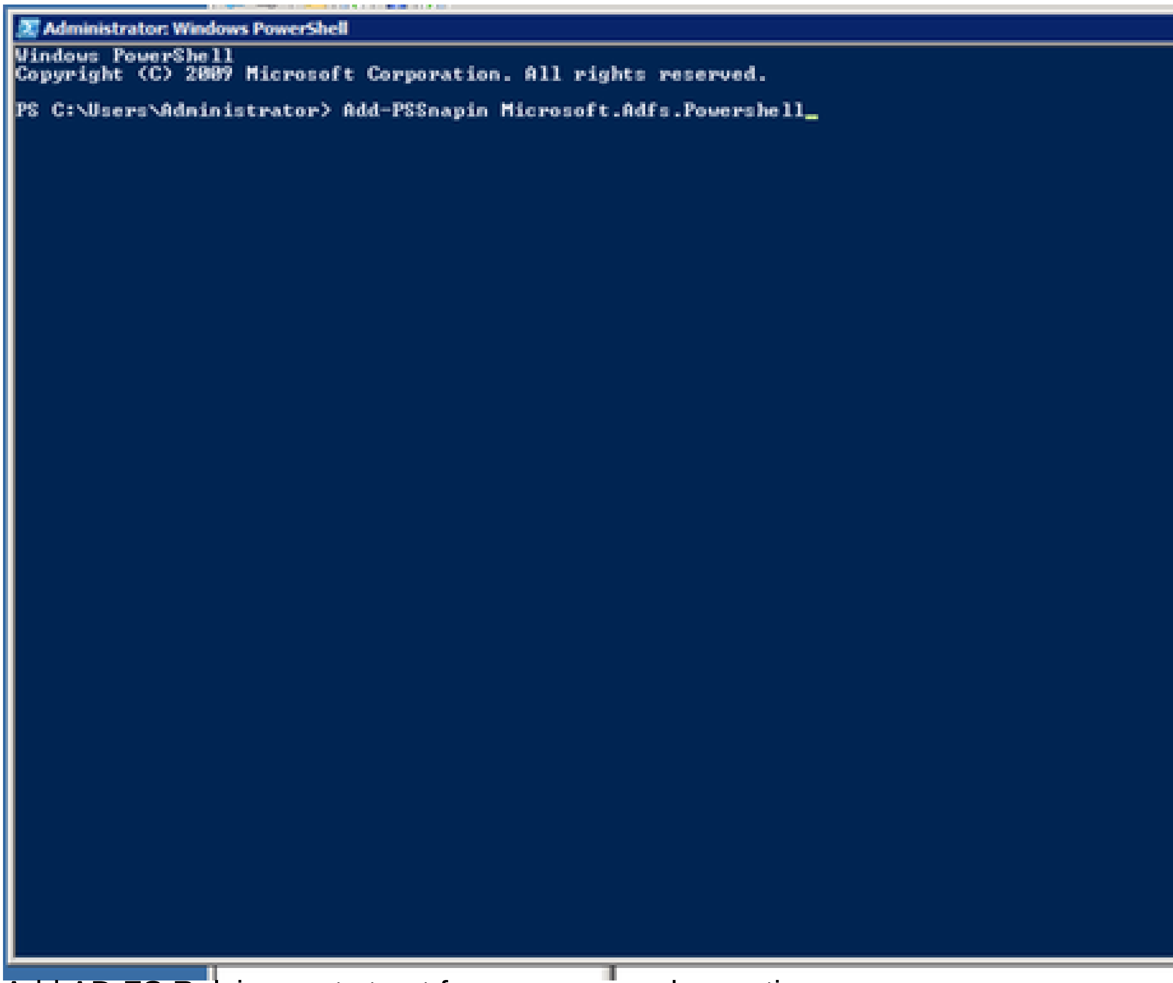
```
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] INFO saml2error.jsp saml2err
response processing failed with code: invalidSignature; message: Invalid signature in A
08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] ERROR com.cisco.ccbu.ids IdSSAML
SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Excep
in Response. at com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUti
com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2028
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAM
```

Possible Cause

AD FS is not configured to sign both Assertion and Message.

Recommended Action

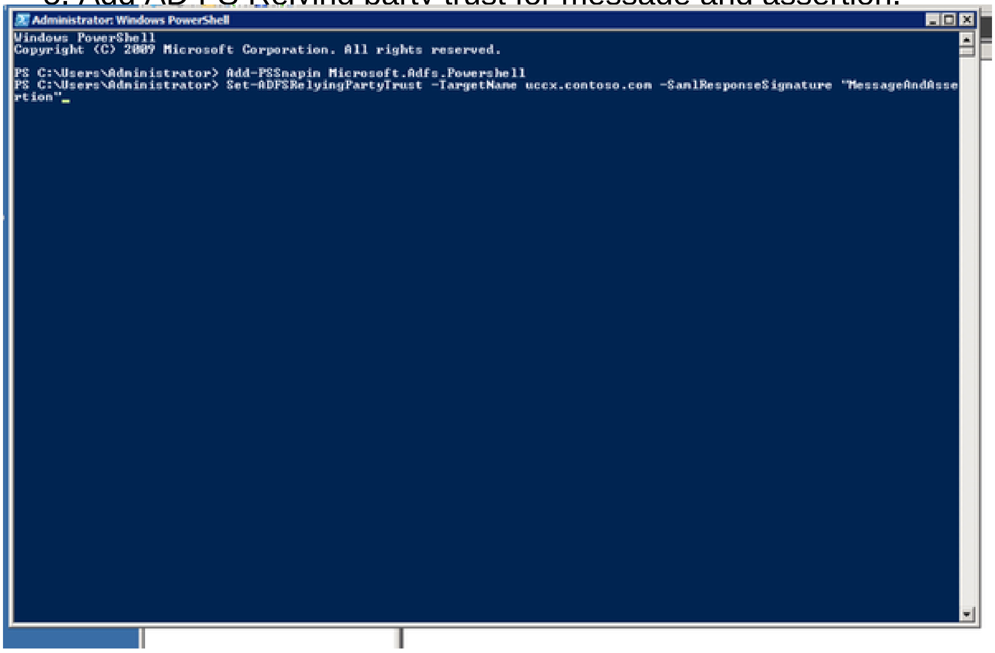
1. Run the AD FS powershell command: **Set-ADFSRelyingPartyTrust -TargetName Identifier> -SamlResponseSignature "MessageAndAssertion"**
2. RDP to AD system.
3. Open **Powershell**.
4. Add Windows PowerShell snap-ins to the current session. This step may not be re ADFS 3.0 since the CmdLet is already installed as a part of adding the roles and fe



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-PSSnapin Microsoft.Adfs.Powershell_
```

5. Add AD FS Relying party trust for message and assertion.



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-PSSnapin Microsoft.Adfs.Powershell
PS C:\Users\Administrator> Set-ADFSRelyingPartyTrust -TargetName uccx.contoso.com -SamlResponseSignature "MessageAndAsse
rtion"_
```

Related Information

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

- **https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html**
- **Technical Support & Documentation - Cisco Systems**