Copyright (C) 2019 Gaman SP z o.o

<https://gaman-gt.com>

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

UCCE, PCCE, UCCX SSO

Tips & Tricks

# Table of Contents

[Table of Contents 2](#_Toc12620547)

[Configuration 3](#_Toc12620548)

[Troubleshoot approach 4](#_Toc12620549)

[Cisco RTMT 4](#_Toc12620550)

[AD Event Viewer 5](#_Toc12620551)

[SSO Time synchronization problems 6](#_Toc12620552)

[The time in the Assertion's Condition is invalid 7](#_Toc12620553)

[The time in SubjectConfirmationData is invalid 9](#_Toc12620554)

[How to resolve SSO Time synchronization problems 11](#_Toc12620555)

[IdP side SSO errors 12](#_Toc12620556)

[Response is not signed 12](#_Toc12620557)

# Configuration

Configuration of the SSO should not be a problem as if you look at it from the UCCE side. Most of the work is performed on the IdP side. There are multiple ways to get it done but at Gaman we are using two Cisco documents available online:

1. **Cisco Unified Contact Center Enterprise Features Guide, Release 11.5(1)** – section: **Single Sign-On**:

<https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf>

1. **Unified Contact Center Enterprise (UCCE) Single Sign On (SSO) Certificates and Configuration**

<https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise/211307-Unified-Contact-Center-Enterprise-UCCE.html>

# Troubleshoot approach

SSO troubleshooting can be quite tricky when you try to set it up for the first time. At Gaman we use two approaches:

1. Validation of the IdS server-side logs
2. Validation of the AD FS-side logs

We use those approaches in the top-down order, which means if the logs form IdS don’t give the straightforward answer what is the problem then we move to AD FS system to check what is happening. In most cases IdS logs are enough to determinate the root cause of the problem.

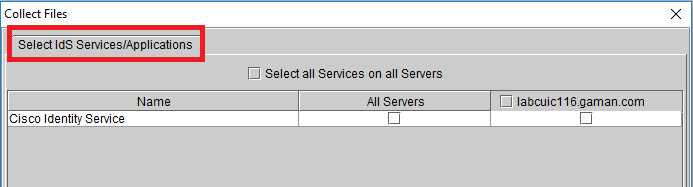
## Cisco RTMT

To get the logs from Cisco IdS server you will need to use RTMT tool – dedicated for CUIC appliance.

The log gathering procedure is identical to the one used for other platforms that support RTMT. Here is a quick guide how to do it:

1. Open RTMT tool
2. Provide login details
3. In the application view select **Trace & Log Central**
4. Choose **Collect Logs**
5. If you have IdS in a coresident deployment with CUIC, skip and don’t check any options available at CUIC Services/Applications and LiveData Service/Applications tab.

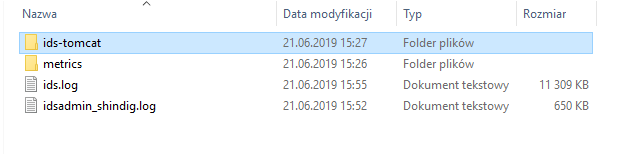
When you see the IdS Services/Applications tab, select all logs from all servers for the Cisco Identity Service.



1. Procced and download logs from specified time-range.
2. Once files are on your workstation, go to folder:

**<download\_folder>/<ids\_server\_name>/<date>/ids/log**

For troubleshooting use ids.log files. Here is a screen shot with the sample file structure:

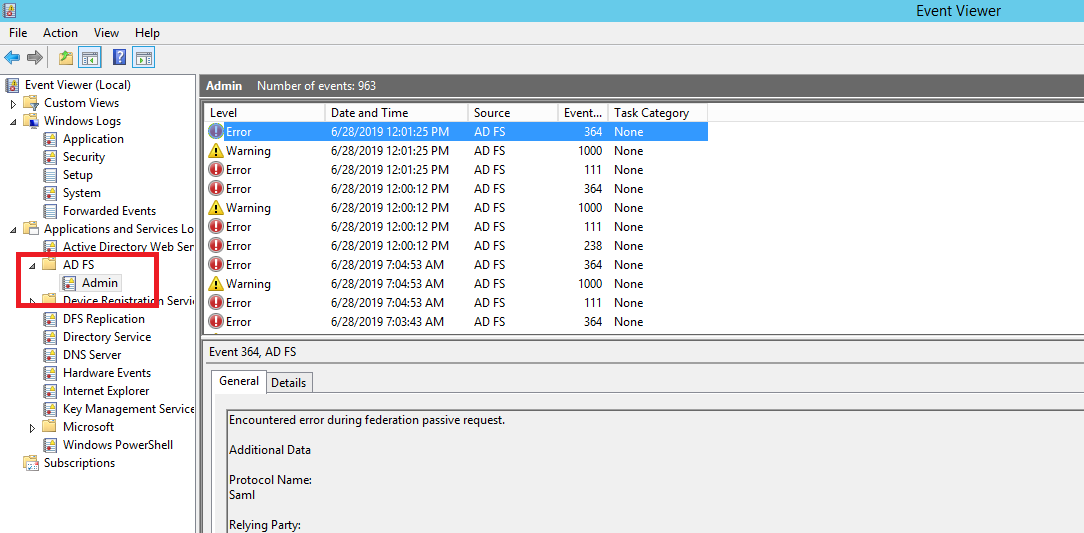


## AD Event Viewer

To check what is happening on the AD FS Server you can use Windows Event Viewer application. Instead of checking basic Windows logs navigate to:

**Event Viewer (Local) > Applications and Services Logs**

Select and expand **AD FS** folder and select **Admin** leaf. Presented view will show all server errors and warnings related to the AD FS service.



# SSO Time synchronization problems

One of the most common problems with SSO is the problem related to time synchronization between IdS and IdP servers. From the end user perspective this error pops-up as a generic error (once user provides valid SSO login credentials in the login form). The question is – how to identify and resolve those this error?

Below are some errors from real life that may appear during SSO configuration.

## The time in the Assertion's Condition is invalid

Let’s look at the below set of logs that show the time assertion error: “The time in the Assertion's Condition is invalid”.

2019-05-29 22:15:39.959 BST(+0100) [IdSEndPoints-SAML-29] INFO com.cisco.ccbu.ids SAML2SPAdapter.java:82 - SSO Failure response from fedlet **<samlp:Response ID="\_9e55d8b9-529e-4001-93c8-3b746dec3740"…………………………………………………………….**

2019-05-29 22:15:39.959 BST(+0100) [IdSEndPoints-SAML-29] ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:302 - SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: **The time in the Assertion's Condition is invalid.**

at com.sun.identity.saml2.common.SAML2Utils.checkConditions(SAML2Utils.java:905)

at com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:600)

at com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1013)

at com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:1990)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:477)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:262)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)

at 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)

2019-05-29 22:15:39.960 BST(+0100) [http-apr-8553-exec-13] DEBUG com.cisco.ccbu.ids IdSEndPointAsyncListener.java:53 - onComplete https://labcuic116.gaman.com:8553/ids/saml/response

If you look at the SSO response context – starts with “<samlp:Response” -you will see some sections with dates. All dates mandatory for problem resolution are highlighted in red in the sample context presented below. Please look at:

1. Log line entry time (generated by the IdS server) – in our example - 2019-05-29 22:15:39.959 BST(+0100)
2. Dates in the assertion condition (generated by IdP server):
   1. NotBefore - 2019-05-29T21:00:37.862Z
   2. NotOnOrAfter - 2019-05-29T22:00:37.862Z

Here is a more detailed view of the output form Ids server. **Condition** section has been highlighted in red:

**2019-05-29 22:15:39.959 BST(+0100)** [IdSEndPoints-SAML-29] INFO com.cisco.ccbu.ids SAML2SPAdapter.java:82 - SSO Failure response from fedlet <samlp:Response ID="\_560051fc-a3d5-46e3-82f4-6535e7e42779" InResponseTo="s27950f2aeef6773ee3d6ab2255f926f59bc31bc2d" Version="2.0" IssueInstant="2019-05-29T21:00:37Z" Destination="https://LabCUIC116.gaman.com:8553/ids/saml/response" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"><saml:Issuer>http://WIN-OMA048UUEP5.gaman.com/adfs/services/trust</saml:Issuer><samlp:Status>

<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">

</samlp:StatusCode>

</samlp:Status><Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="\_91a7c3ac-2f7a-4809-b55d-1eac5ce086f8" IssueInstant="2019-05-29T21:00:37.909Z" Version="2.0"><Issuer>http://WIN-OMA048UUEP5.gaman.com/adfs/services/trust</Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><ds:Reference URI="#\_91a7c3ac-2f7a-4809-b55d-1eac5ce086f8"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>ndduPDTdQZGizee9cjw0UZDQfOw=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>XKr3el0UzrswoyvbBLG+dPRVCaJy3mpPtl07hh276zTNmHQCTC8ZVljKRG2uisiwDjqGfLAh1yULKBisCwUpP8JNHH2h2sr/n46LF5dMh5wum1Qhe5xKSKlQWfmKVsWh5hCMRJSyo+/AnvzA4xsc8mu8SlaGk1+FyOZdvazUcXYie1Xmm9QmMcbxn1wiuTu+9osjJHtYRHUr2beuIn0kaBPQo1nZgti51vW3akhLZEn/12VQz5LzbAFMOpeCMVnGdiXopwcmIjpsyL9HjxPbauf7kQmneY1UPzVkWHSthhkylG1PoqKIPCktK9sk0b5AObkRi7PfpPDX4PRmkd5eyA==</ds:SignatureValue><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate>**Certificate data has been removed**</ds:X509Certificate></ds:X509Data></KeyInfo></ds:Signature><Subject><NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://WIN-OMA048UUEP5.gaman.com/adfs/services/trust" SPNameQualifier="LabCUIC116.gaman.com">GAMAN\Administrator</NameID><SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData InResponseTo="s27950f2aeef6773ee3d6ab2255f926f59bc31bc2d" NotOnOrAfter="2019-05-29T21:05:37.910Z" Recipient="https://LabCUIC116.gaman.com:8553/ids/saml/response"/></SubjectConfirmation></Subject>**<Conditions NotBefore="2019-05-29T21:00:37.862Z" NotOnOrAfter="2019-05-29T22:00:37.862Z"><AudienceRestriction><Audience>LabCUIC116.gaman.com</Audience></AudienceRestriction></Conditions><**AttributeStatement><Attribute Name="uid"><AttributeValue>Administrator</AttributeValue></Attribute><Attribute Name="user\_principal"><AttributeValue>Administrator@gaman.com</AttributeValue></Attribute></AttributeStatement><AuthnStatement AuthnInstant="2019-05-29T19:41:49.092Z" SessionIndex="\_91a7c3ac-2f7a-4809-b55d-1eac5ce086f8"><AuthnContext><AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextClassRef></AuthnContext></AuthnStatement></Assertion></samlp:Response>

If you calculate the time difference between dates/times you will see that it’s around 15 min in the presented example. This is not acceptable by IdS server and this is the root cause that the SSO fails.

## The time in SubjectConfirmationData is invalid

Let’s look at the set of logs that show the time assertion error: “The time in the Assertion's Condition is invalid”.

**2019-05-29 21:15:36.989 BST(+0100)** [IdSEndPoints-SAML-60] INFO com.cisco.ccbu.ids SAML2SPAdapter.java:82 - SSO Failure response from fedlet **<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ………………………**

2019-05-29 21:15:36.989 BST(+0100) [IdSEndPoints-SAML-60] INFO com.cisco.ccbu.ids SAML2SPAdapter.java:97 - SSO failed with code: 0. Response status: <samlp:Status>

<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">

</samlp:StatusCode>

</samlp:Status> for AuthnRequest: n/a

2019-05-29 21:15:36.990 BST(+0100) [IdSEndPoints-SAML-60] ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:302 - SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: **The time in SubjectConfirmationData is invalid.**

at com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:721)

at com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:566)

at com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1013)

at com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:1990)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:477)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:262)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)

at 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)

2019-05-29 21:15:38.406 BST(+0100) [http-apr-8553-exec-5] INFO com.cisco.ccbu.ids IdSClusterMonitor.java:145 - Current cluster nodes in cache - [LabCUIC116.gaman.com]

If you look at the SSO response context – starts with “<samlp:Response” – you will see some sections with dates. All dates mandatory for problem resolution are highlighted in red in the sample context presented below. Please look at:

1. Log line entry time – in our example - 2019-05-29 22:15:39.959 BST(+0100)
2. Dates in the SubjectConfirmationData XML element. Please look at the date inserted in the NotOnOrAfter attribute. In our case the value is: 2019-05-29T19:26:20.0072Z

Here is a more detailed view of the output form Ids server. **Log date** and **SubjectConfirmationData** section has been highlighted in red:

**2019-05-29 21:15:36.989 BST(+0100)** [IdSEndPoints-SAML-60] INFO com.cisco.ccbu.ids SAML2SPAdapter.java:82 - SSO Failure response from fedlet <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" Destination="https://LabCUIC116.gaman.com:8553/ids/saml/response" ID="\_532bab47-4c35-4280-b4d1-9c8e0b7156cf" InResponseTo="s2b9ea43075fcd60f8328ee2652aae255eb99ba82d" IssueInstant="2019-05-29T19:26:22.012Z" Version="2.0"><Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://WIN-OMA048UUEP5.gaman.com/adfs/services/trust</Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><ds:Reference URI="#\_532bab47-4c35-4280-b4d1-9c8e0b7156cf"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>+oGEmxWTknSRcNKkNrp7mGyIGBk=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>aGCT3JJ99eWbFtHsFZ0aHGQP/1euox/iiNQ1gau1rSHEAxxwksCO0AsiaeV4E2fKqv2pMZN/kYfeu/RhV4V02W7E3KHVXHVnlP7Y7AV/B+We1sNMerGA/M0LfIVuTqMjMbvbwqmxNShM3xCSewo26izRUOEJW9+LwjZrwOhtgsWlu0FVbm00ZVrsYiDJ1tN/6otRlGOJVjJWWAL2jS1umImG+I1NPgtssXXVG4U3h8YDXUvRJwp+KpT8nLOMuzvWPm5Dds/c2KKPRrzNuWnJveki72UVtmqSNR/NQPjqsUrzyuniLZMcXNnW+/f5crcigUx7BcggfANtcIkBDrTiUg==</ds:SignatureValue><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate> **Certificate data has been removed** </ds:X509Certificate></ds:X509Data></KeyInfo></ds:Signature><samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="\_dd03bbf0-24f7-4e17-94e5-219019e44b6d" IssueInstant="2019-05-29T19:26:21.895Z" Version="2.0"><Issuer>http://WIN-OMA048UUEP5.gaman.com/adfs/services/trust</Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><ds:Reference URI="#\_dd03bbf0-24f7-4e17-94e5-219019e44b6d"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>pLEgB5/3rFfL0sjKabAZe10Cs2E=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>DXuwUsUU8CMtgUQuIm1n8aCVyXJriYms1NSeGc0GQY1Izks+Gk6UM8rIURgsL1Fl5UdxQonIWVKGWP6aiV2V/jEr8Z0BT2weG3ApxqPnMI0AlI0sSEXthb5mMvWwMgmuGNWHVNEuj/jfWzaAnEWUJVNVpmG8Iwq3bfv9wCM7AWJAvFgGU+DJBw+rHim2H/2FdhsaVg679rVckjL0o8+ZF83yIGNH7vo8jvQvkiguCD+fXtP5RR9AdBQv+Fw2UPvb9vJ7e9RzTRgOvwNnJKTR2lVfWSNRSTZgCo7WyNigYEiHnji046z4yBoBfZXmJcDKm0bcDEYz+YU0iHVygBaixg==</ds:SignatureValue><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate> **Certificate data has been removed** </ds:X509Certificate></ds:X509Data></KeyInfo></ds:Signature><Subject><NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://WIN-OMA048UUEP5.gaman.com/adfs/services/trust" SPNameQualifier="LabCUIC116.gaman.com">GAMAN\Administrator</NameID**><SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData InResponseTo="s2b9ea43075fcd60f8328ee2652aae255eb99ba82d" NotOnOrAfter="2019-05-29T19:31:22.014Z" Recipient="https://LabCUIC116.gaman.com:8553/ids/saml/response"/></SubjectConfirmation>**</Subject><Conditions NotBefore="2019-05-29T19:26:20.072Z" NotOnOrAfter="2019-05-29T20:26:20.072Z"><AudienceRestriction><Audience>LabCUIC116.gaman.com</Audience></AudienceRestriction></Conditions><AttributeStatement><Attribute Name="uid"><AttributeValue>Administrator</AttributeValue></Attribute><Attribute Name="user\_principal"><AttributeValue>Administrator@gaman.com</AttributeValue></Attribute></AttributeStatement><AuthnStatement AuthnInstant="2019-05-29T19:21:09.411Z" SessionIndex="\_dd03bbf0-24f7-4e17-94e5-219019e44b6d"><AuthnContext><AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextClassRef></AuthnContext></AuthnStatement></Assertion></samlp:Response>

If you calculate the time difference between dates/times you will see that it’s around 2h and 10 min in the presented example. This is not acceptable by IdS server and this is the root cause that the SSO fails.

## How to resolve SSO Time synchronization problems

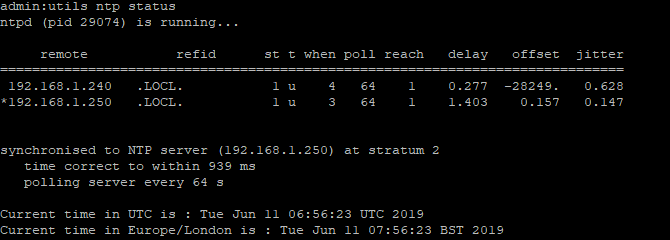
Here is a simple procedure that shows how to deal with time synchronization problem in scenario where Cisco IdS is connected to Microsoft AD FS (starting from Windows Server 2008). Please go through below steps:

1. Log into the IdP server and check if it’s synchronizing with NTP server.

If you are using Windows as IdS server, here are useful commands to verify status of the Windows Time service (commands issued on command line, available starting from Windows Server 2008):

* w32tm /query /configuration – shows Windows Time service configuration.
* w32tm /query /status – shows Windows Time service status (stratum, leap indicator, precision, last sync, NTP server, poll interval).
* time /T – outputs the current system time.

1. Log into the Cisco IdS server using CLI – use OS administrator login credentials
2. Issue a command: show ntp status and check results. Please look at the below screenshot:



If the system is in sync with NTP, then system should show NTP IP/Hostname/FQDN of server that is a time source for IdS.

1. Compare date from IdP and IdS servers. If there is a difference, then one of the servers is out of sync with NTP.

# IdP side SSO errors

## Response is not signed

Let’s look at the set of logs that show the time assertion error: “Response is not signed”.

2019-05-29 22:22:44.543 BST(+0100) [IdSEndPoints-SAML-31] INFO com.cisco.ccbu.ids SAML2SPAdapter.java:82 - SSO Failure response from fedlet <samlp:Response ID="\_c7641394-cefc-4a42-b208-df09810dbe65" ……………

**2019-05-29 22:22:44.544 BST(+0100) [IdSEndPoints-SAML-31] ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:302 - SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: Response is not signed.**

at com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:643)

at com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1013)

at com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:1990)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:477)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:262)

at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)

at 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)

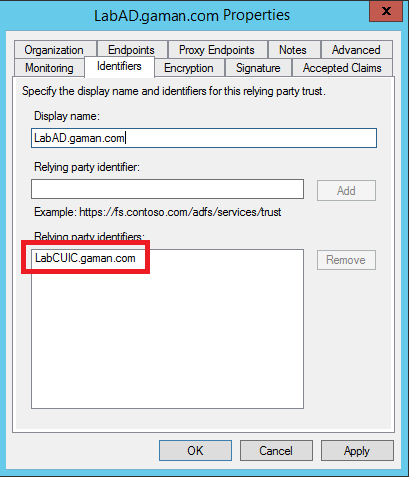
2019-05-29 22:22:44.545 BST(+0100) [http-apr-8553-exec-5] DEBUG com.cisco.ccbu.ids IdSEndPointAsyncListener.java:53 - onComplete <https://labcuic116.gaman.com:8553/ids/saml/response>

This error occurs when the administrator that configures AD FS services skips/omits the steps to establish the Signed SAML Assertions for the Relying Party Trust for the IdS server. To resolve the issue, execute the following command in PowerShell on AD FS server:

**Set-ADFSRelyingPartyTrust -TargetName LabCUIC.gaman.com -SamlResponseSignature "MessageAndAssertion"**

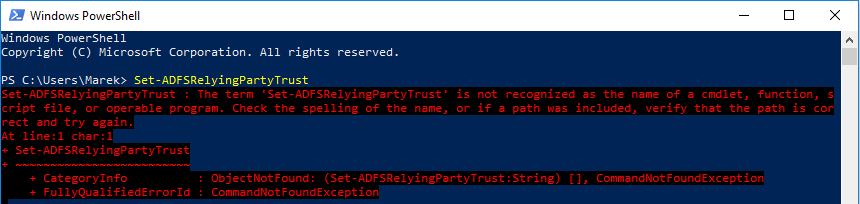
Where:

**LabCUIC.gaman.com** is the name of the cisco IdS server. Please also remember that the name has to exactly match the Identifier tab of the RelyingPartyTrust properties on the AD FS configuration screen.



**Please note:**

If you get the following error during the execution of the above PS command: “**The term 'Set-ADFSRelyingPartyTrust' is not recognized as the name of a cmdlet**”



This means that the ADFS command set is not added to PowerShell command list. To add it, please run the following command in PS:

**Add-PSSnapin Microsoft.Adfs.PowerShell**