Troubleshooting SAML SSO Access

Troubleshooting SAML SSO Access

Redirection to IdP fails

When the end users attempt to log into a SAML-enabled web application using a Cisco Unity Connection supported web browser, they are not redirected to their configured Identity Provider (IdP) to enter the authentication details. Check if the following conditions are met:

- The Identity Provider (IdP) is up and running.
- The correct IdP metadata file (idp.xml) is uploaded to Unity Connection.
- Verify if the server and the IdP are part of the same circle of trust.

IdP authentication fails

If the end user is not getting authenticated by the IdP, check if the following conditions are met:

- The LDAP directory is mapped to the IdP.
- The user is added to the LDAP directory.If the problem still exists, then check the NTP servers associated with Unity Connection and Identity Provider. Make sure that the time on NTP servers associated to both these servers are in synchronization.
- The LDAP account is active.
- The User Id and password are correct.

Redirection to Unity Connection fails

Even after getting authenticated by the IdP, if the user is not redirected to SAML SSO enabled web applications, check the following:

- The clocks of the Unity Connection and the IdP are synchronized. See the "NTP Servers" section of "Settings" chapter in *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html
- The mandatory attribute uid is configured on the IdP.
- The correct Unity Connection server metadata file is uploaded to the IdP.
- The user has the required privileges.

Run Test Fails

When the Run Test fails on Unity Connection, refer the corrective actions that are outlined in Redirection to IdP fails, IdP authentication fails and Redirection to Unity Connection fails.

Mismatch in SAML Status on Publisher and Subscriber Servers

When there is a mismatch of SAML status on publisher and subscriber servers in Unity Connection, do the following:

- Check if IdP metadata is correct on Subscriber server, if not then select the option Re-import Meta Data from SAML Single Sign-On web page.
- If problem still exists, then select the option Fix All Disabled Servers.

Note There is no option to re-import meta data for Publisher server in case of Unity Connection cluster.

Problem in Accessing Web Application on Unity Connection

When a user is not able to access the web applications on Unity Connection using SAML SSO feature and encounters the given error:

Error

<ADFS server>

There was a problem accessing the site. Try to browse to the site again. If the problem persists, contact the administrator of this stie and provide the reference number to identify the problem.

Use the following task list to determine the source of the problem and correct it:

1. Confirm that the Service Provider metadata (SPMetadata<hostname of Unity Connection>.xml) is not missing on Identity Provider. Try uploading the Service Provider metadata of the Unity Connection via Import or URL option.
2. After importing the sp.xml successfully, add the following two claim rules:
   - Send LDAP Attributes as Claims: Select LDAP attribute as SAM-Account-Name and add Outgoing Claim type corresponding to this as uid.
   - Send Claims using a Custom Rule: Under the Custom Rule description, write the following claim:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 = "http://<ADFS_FQDN>/adfs/com/adfs/service/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 = "<UC_Node_FQDN>");
```

Save these two claim rules successfully to ensure that Identity Provider used in SAML SSO feature is configured well. (In the above problem description, we have considered ADFS as Identity Provider for

SAML SSO. You may choose any of the supported Identity Provider instead.)

1. The Unity Connection server entry on Identity Provider server must not be disabled.
2. There should be any errors upon accessing the Service Provider metadata (SPMetadata<hostname of Unity Connection>.xml) as a corrupted SP metadata file never allows a user to gain single sign-on access to web applications.

Encryption Error Upon User Login to Unity Connection

When a user tries to login to a web application on Unity Connection and encounters the following

exception error:

Error 500 with Exception

Unable to decrypt secret key

Use the following task list to determine the source of the problem and correct it:

1. Confirm that the SAML SSO feature is enabled on Unity Connection.
2. Under the Identity Provider server Relying party trust page, select Edit Claim Rule and then select

Encryption tab. Remove the encryption from that location and the issue gets fixed.

Unable to Upload Subscriber SP Metadata on ADFS in Cluster

When a user tries to upload the subscriber' SP metadata on ADFS server in a cluster and it fails, the user must try the following steps:

1. Update roll 3 on ADFS 2.0 with hotfix. (http://support.microsoft.com/kb/2790338).
2. Start Windows powershell and run the command:

cd "$env:programfiles\active directory federation services 2.0\sql"

Add-PSSnapin microsoft.adfs.powershell

.\PostReleaseSchemaChanges.ps1

Note: If you get following error at powershell

script cannot be loaded because the execution of scripts is disabled on this system

execute: Set-ExecutionPolicy RemoteSigned with yes on Windows powershell.

SAML Exception Time Synchronization Error

When a user tries to configure SAML SSO feature on Unity Connection and encounters the following error related to time mismatch:

SAML Exception issue: SAML2Exception

The time in SubjectConfirationData is invalid

Use the following task list to determine the source of the problem and correct it:

1. Make sure that the clocks of Identity Provider (like ADFS) and Unity Connection are in synchronization with each other.
2. If the problem still exists, then check the NTP servers associated with Unity Connection and Identity Provider. Make sure that the time on NTP servers associated to both these servers are in synchronization.

SAML Exception Invalid Status Code

Whenever user tries to configure SAML SSO feature on Cisco Unity Connection, in **FIPS mode** with signing algorithm as **SHA1** then below problems will appear:

Error: Invalid status code in response.

SAML Exception issue: ServletException.

Configuration Error in IdP. Please check IdP logs and configuration.

Use the following task list to correct this problem:

1. Change the signing algorithm from SHA1 to SHA256 by executing Unity Connection admin cli command: utils sso set signing-algorithm sha256
2. Configure the SMAL SSO feature on Unity Connection.

Incorrect status of SAML SSO on Two Servers in a Unity Connection Cluster

When the status of SAML SSO feature is different on the two servers in a Unity Connection cluster, do the following:

- If SAML SSO status is disabled on subscriber server and enabled on publisher server, login to Cisco Unity Connection Administration on subscriber server, and select the option “Fix All disabled servers”.
- If we disable the SAML SSO feature on subscriber server when the publisher server is not reachable, a user needs to explicitly disable the SAML SSO feature from publisher server and vice versa. You may also be required to reboot the server if the issue still persists.
- In case of publisher rebuild, administrator needs to explicitly update the IdP metadata file on the publisher server of cluster.

Troubleshooting Cross Origin Resource Sharing

When a third party browser application makes CORS request from a different origin to get the status of SAML Single Sign On by calling the http://<hostname>/ssosp/ws/public/singleSignOn API, the user may get the “Domain not Allowed” error message. To resolve this issue:

- Verify if the domain name is configured properly into the trace file.
- Check if the API method type is configured correctly.
- Verify if the <Hostname> is mentioned correctly in the API.

Diagnostics Traces for Problems with SAML SSO Access

You can enable the Unity Connection trace levels to detect and study any issues related to SAML SSO feature. The traces are turned on from command line access(CLI) to the system server.

The given command turn on the traces for SAML SSO:

admin: set samltrace level <trace-level>

The traces defined are:

- Debug
- Info
- Warning
- Error
- Fatal

The traces are collected in the following location on Unity Connection :

/var/log/active/tomcat/logs/ssosp