



Troubleshooting SAML SSO Access in Cisco Unity Connection 10.x

See the following sections:

- [Redirection to IdP fails, page 29-1](#)
- [IdP authentication fails, page 29-1](#)
- [Redirection to Unity Connection fails, page 29-2](#)
- [Run Test Fails, page 29-2](#)
- [Mismatch in SAML Status on Publisher and Subscriber servers, page 29-2](#)
- [Incorrect status of the SAML SSO feature on the two servers in a Unity Connection cluster, page 29-3](#)
- [Diagnostics Traces for Problems with SAML SSO Access, page 29-3](#)

Redirection to IdP fails

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

Solution

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 Cisco Unity Connection.
- Verify if the server and the IdP are part of the same circle of trust.

IdP authentication fails

The end user is not getting authenticated by the IdP.

Solution

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, the user is not redirected to SAML SSO enabled web applications.

Solution

- The clocks of the Unity Connection and the IdP are synchronized. See the NTP Settings section in *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection* for information on synchronizing clocks.
- 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.

Solution

Refer the corrective actions that are outlined in [Redirection to IdP fails, page 29-1](#), [IdP authentication fails, page 29-1](#) and [Redirection to Unity Connection fails, page 29-2](#).

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.

Solution

- 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.

Incorrect status of the SAML SSO feature on the 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.

Solution:

- 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.

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 will 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
