Troubleshooting Authorization Code Grant Flow

This section explains various problems that may occur while using Authorization Code Grant Flow along with the resolution. For Authorization Code Grant Flow, Unity Connection uses an Authz server that provides the authorization keys to validate the Jabber user.

Troubleshooting Authorization Code Grant Flow

This section explains various problems that may occur while using Authorization Code Grant Flow along with the resolution. For Authorization Code Grant Flow, Unity Connection uses an Authz server that provides the authorization keys to validate the Jabber user.

Unable to Configure an Authz Server

While configuring an Authz server in Unity Connection or synchronizing the keys between Authz server and Unity connection, you may receive any of the following error message on the New Authz Server page, Edit Authz Server page or Search Authz Server page of Cisco Unity Connection Administration:

- "Failed to connect to Authz Server. Check network connectivity with Authz Server. For more details, check error log" or
- "Failed to connect to Authz Server"

If you receive the "Failed to connect to Authz Server. Check network connectivity with Authz Server. For more details, check error log" or "Failed to connect to Authz Server" error message, verify the following:

- The Cisco Unified CM must be up and running
- The version of Cisco Unified CM must be 11.5(1) SU3 or later
- You entered a valid port number.
- You entered a valid Hostname, IP address or Fully-Qualified Domain Name (FQDN) for the Authz server

- "Not authorized - Invalid Username or Password"

If you receive the "Not authorized - Invalid Username or Password" error message, make sure that the username or password entered for the Authz server are correct.

- "Failed to validate certificates. Make sure proper tomcat certificates are uploaded for the Authz Server" or
- "Failed to validate certificates. Tomcat certificates uploaded for the Authz Server are not yet valid" or

- "Failed to validate certificates. Tomcat certificates uploaded for the Authz Server have expired"

If you receive any of the above error message, make sure proper tomcat certificates are uploaded for the Authz server or check the **Ignore Certificate Errors** check box to ignore the certificate validation errors.

To upload the certificate, log in to the Cisco Unified OS Administration, go to Security > Certificate Management. On the Find and List Certificates page, select Upload Certificate\Certificate Chain. On the Upload Certificate\Certificate Chain page upload a valid certificate for the Cisco Unified CM to the Cisco Unity Connection tomcat-trust.

Jabber User is Unable to Login

If Jabber user is not able to login, verify the following:

- Jabber user must enter a valid username and password.
- The Tomcat services of Cisco Unified CM are up and running.
- The Authz server is properly configured in Unity Connection.
- OAuth Authorization Code Grant Flow feature is enabled on both Cisco Unified CM and Cisco Unity Connection

You can also collect Cisco Syslogs for RTMT, which help in analyzing the alerts for Authz server. The path to access Cisco Syslogs is /var/log/active/syslog/CiscoSyslog.

Occurrence of "EvtAuthzKeyRotation" alert in Cisco SysLog indicates that the authorization keys are changed on Cisco Unified CM. Due to which Unity Connection is not able to validate the token of a Jabber user. Hence Jabber user is not able to login.

To resolve the issue, you must synchronize the authorization keys between Authz server and Unity Connection. To synchronize the keys, in Cisco Unity Connection Administration, navigate to System Settings > Authz Servers. On the Search Authz Servers page, select Sync Keys.

To synchronize the authorization keys through REST API, see "TBD".

To troubleshoot more problems related to Authz server, you can collect diagnostic traces for the Authz server. For detail instructions on enabling and collecting diagnostic traces, see the "Traces in Cisco Unity Connection Serviceability" section.