Android Introduction

2.3.05 Data Encryption using TLS

Prerequisite

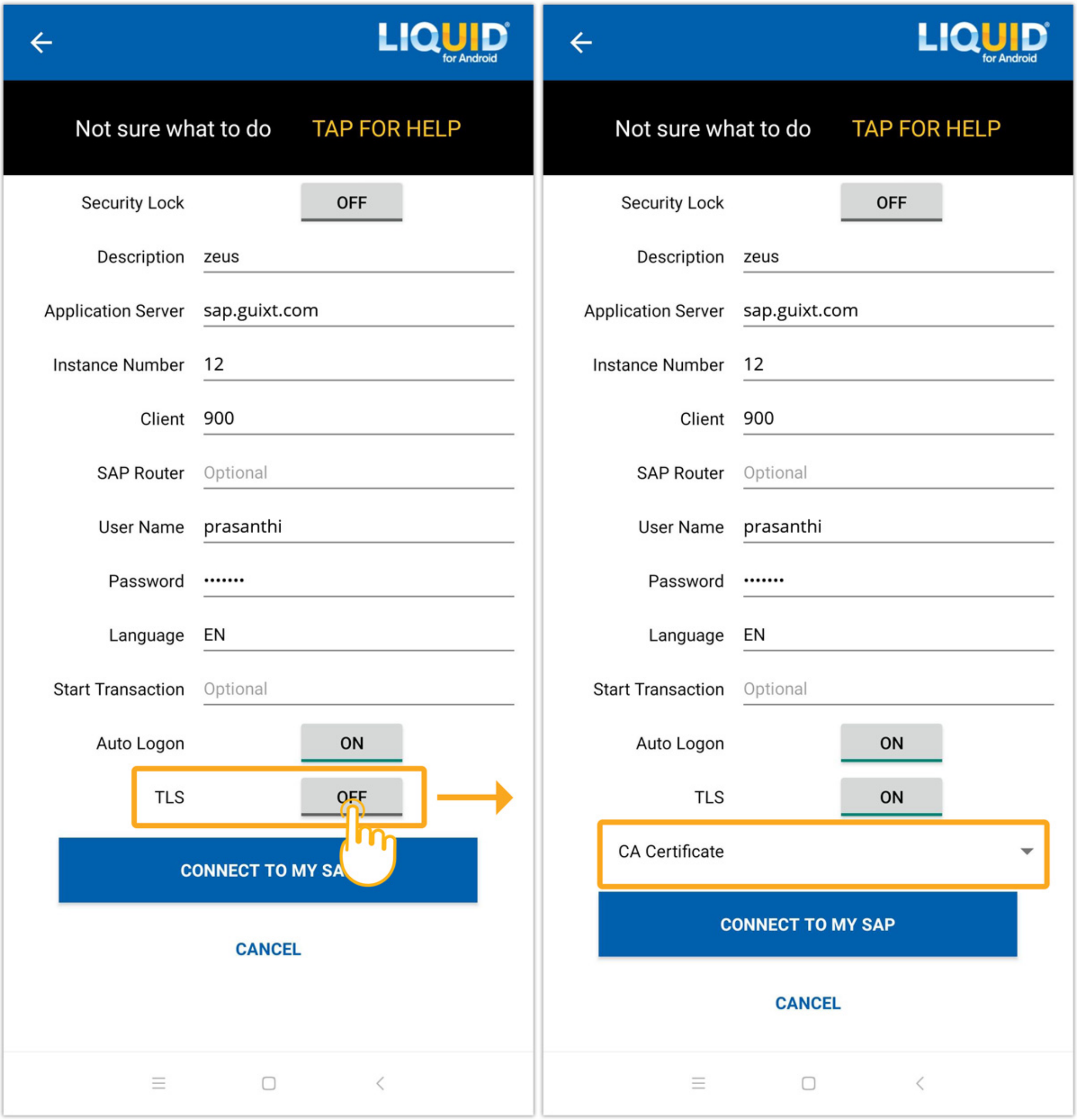
- Configure Liquid UI Server
- Configure Liquid UI Client
- A valid X.509 certificate to support directory access control

Liquid UI provides a completely secure communication channel between your SAP Server and the Liquid UI for Android on your device. The Liquid UI for Android uses TLS 1.3 encryption to ensure the security of the communication channel.

Liquid UI has designed a function in its library to verify whether the encryption key is associated with the function while receiving the data package from the server, which also ensures the security of your data. For an identified encryption key, we will establish a secure connection flag and initialize the TLS state. In addition, TLS 1.3 handles socket communication.

Please follow step-by-step guidelines to enable TLS on the Android device: enable TLS on Android, please do the following:

1. Launch the Liquid UI for Android App on your device.
2. Select the Liquid UI Connection setting screen and select the Edit connection option.
3. Scroll down to the TLS option and tap on the control to **ON** position.

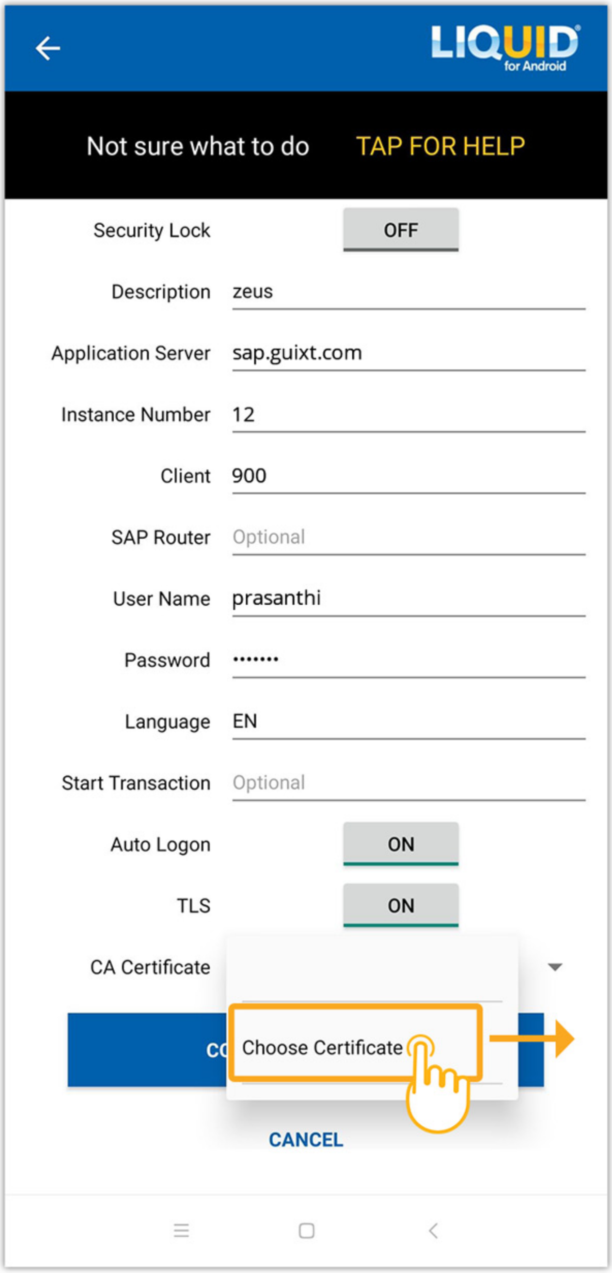


Security Lock: OFF
Description: zeus
Application Server: sap.guixt.com
Instance Number: 12
Client: 900
SAP Router: Optional
User Name: prasanthi
Password: •••••••
Language: EN
Start Transaction: Optional
Auto Logon: ON
TLS: OFF

Security Lock: OFF
Description: zeus
Application Server: sap.guixt.com
Instance Number: 12
Client: 900
SAP Router: Optional
User Name: prasanthi
Password: •••••••
Language: EN
Start Transaction: Optional
Auto Logon: ON
TLS: ON
CA Certificate

4. When you enable the TLS option, the CA certificate option is displayed. Click on the drop-down to choose a certificate. A click on choose certificate option displays a message dialogue box to upload the certificate. From the available CA certificate options, select the certificate and click on select, as shown in the image below.

Android Introduction



Not sure what to do TAP FOR HELP

Security Lock: OFF

Description: zeus

Application Server: sap.guixt.com

Instance Number: 12

Client: 900

SAP Router: Optional

User Name: prasanthi

Password: •••••••

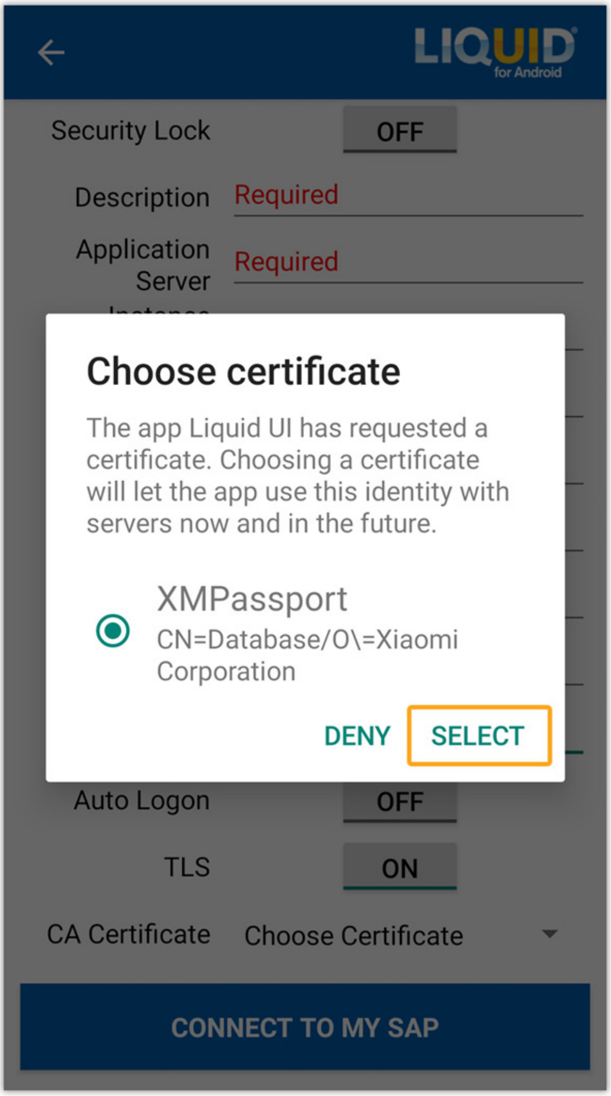
Language: EN

Start Transaction: Optional

Auto Logon: ON

TLS: ON

CA Certificate: Choose Certificate



Security Lock: OFF

Description: Required

Application Server: Required

Choose certificate

The app Liquid UI has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.

● XMPassport
CN=Database/O\=Xiaomi Corporation

DENY SELECT

Auto Logon: OFF

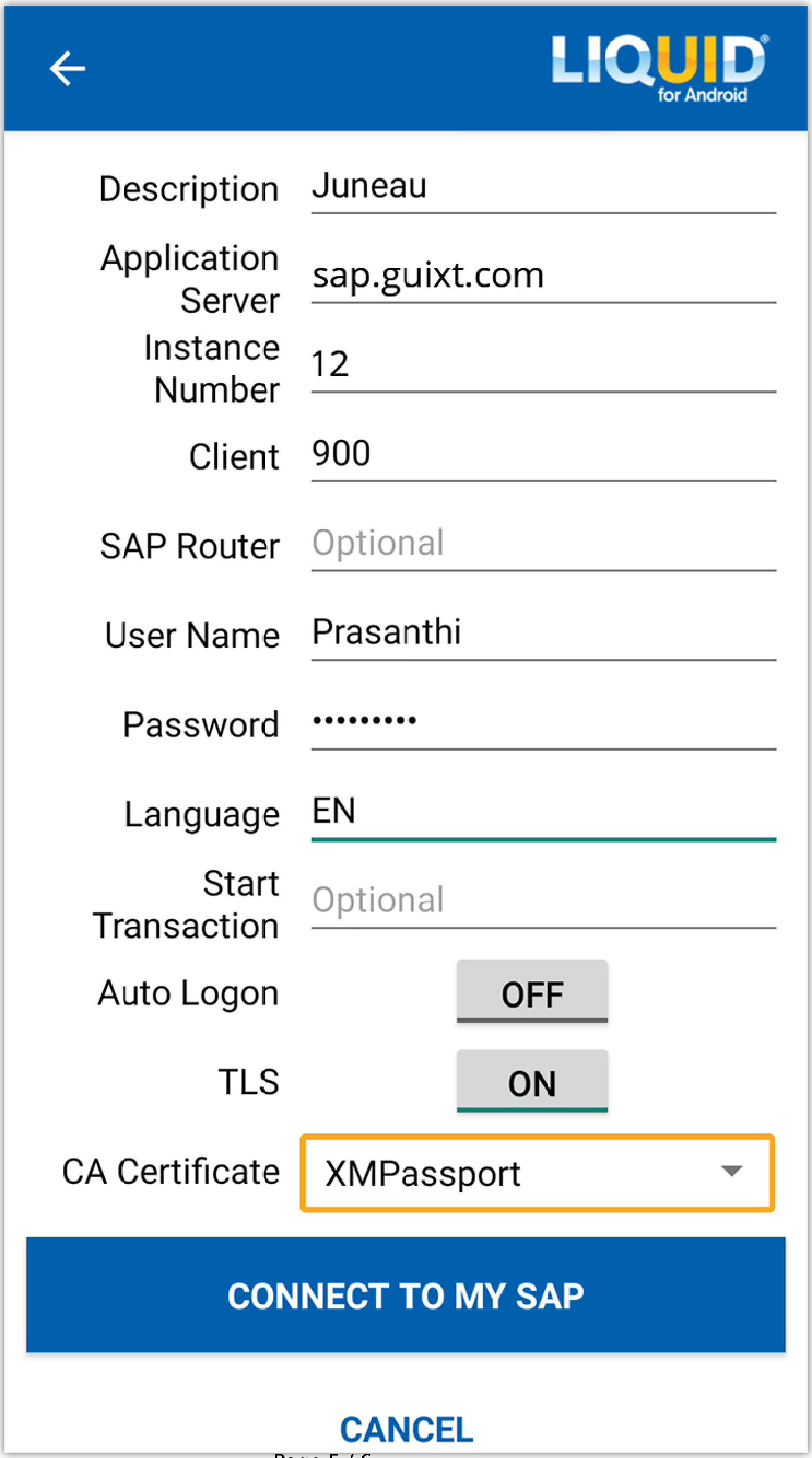
TLS: ON

CA Certificate: Choose Certificate

Note: Upon selecting the certificate, information gets saved into a file from the Server. This helps to connect a server with TLS.

5. After selecting the certificate, the CA certificate option in the setting displays the certificate applied, as shown below:

Android Introduction



Description: Juneau

Application Server: sap.guixt.com

Instance Number: 12

Client: 900

SAP Router: Optional

User Name: Prasanthi

Password: •••••••••

Language: EN

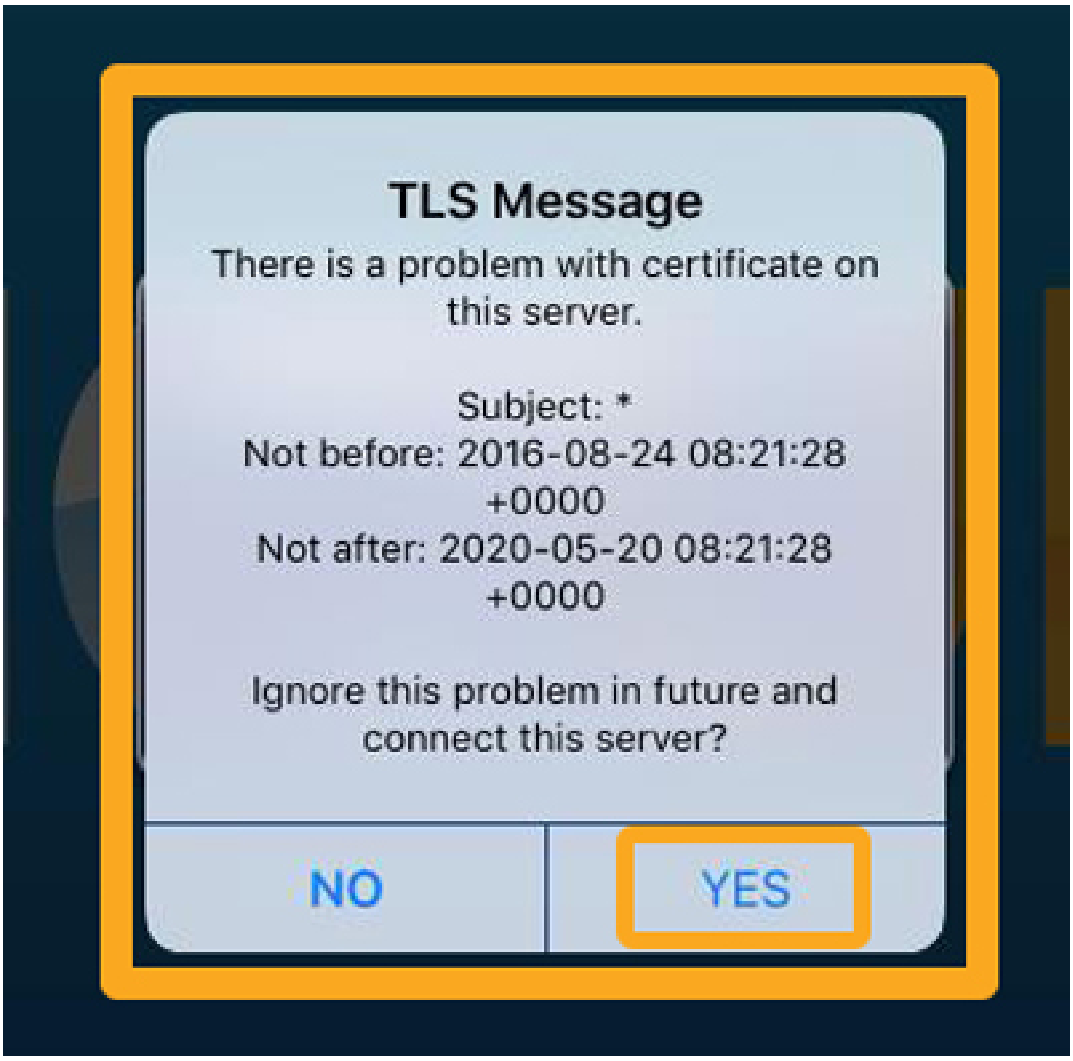
Start Transaction: Optional

Auto Logon: OFF

TLS: ON

CA Certificate: XMPassport

6. In case of any trouble with certificate information, an error message pops up, as shown below. Click **Yes** to connect the certificate to the Server and resolve the certificate validation issue. This also updates the local certification lists.



TLS Message

There is a problem with certificate on this server.

Subject: *
Not before: 2016-08-24 08:21:28 +0000
Not after: 2020-05-20 08:21:28 +0000

Ignore this problem in future and connect this server?

To know more about end-to-end security for your SAP using TLS, click here.

Unique solution ID: #1984
Author: Sarvani Kusuri
Last update: 2022-11-14 10:19