iOS Introduction

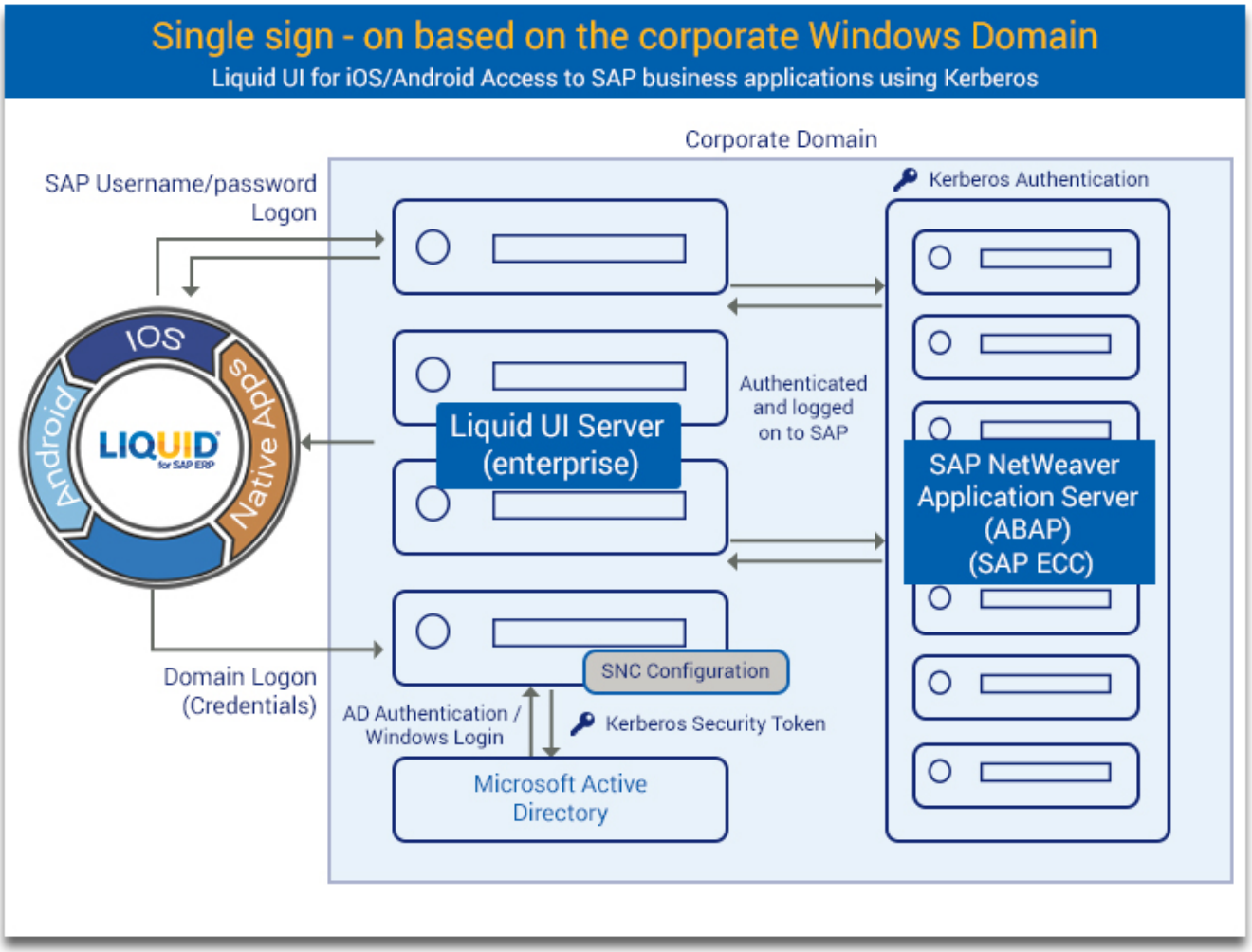
2.3.06 Single Sign-On

Purpose

Usually, organizations manage multiple usernames and passwords across various applications to access SAP systems. To simplify this process, many companies have adopted Windows Active Directory with Kerberos for centralized authentication. While setting up Single Sign-On (SSO) on SAP GUI for desktops within the domain is straightforward, the challenge arises with iOS devices outside the Active Directory domain.

Liquid UI offers robust support for Single Sign-On (SSO) authentication on iOS, eliminating the need for IT teams to handle countless username and password combinations. With the SSO feature, Liquid UI users can conveniently authenticate using their domain username and password, simplifying the login process and reducing the burden of remembering multiple credentials. Now, users only need to manage one set of login credentials to access SAP, enhancing efficiency and user experience securely.

Architecture



iOS Introduction

Mechanism

- Enter Domain credentials on Liquid UI for iOS native SAP logon screen.
- These credentials are securely transmitted to the Liquid UI Server and subsequently forwarded to the Microsoft Active Directory.
- Upon receiving the request, the Active Directory generates a Kerberos token, which is then sent back to the Liquid UI Server.
- The Liquid UI Server forwards this Kerberos token to the SAP Application Server (ABAP), where it undergoes validation.
- Once validated, the user is authenticated and granted access to SAP ECC, ensuring a seamless and secure login process.

Liquid UI supports Single Sign-On to allow users to log in to SAP ERP systems using any of the following four methods:

1. **Domain credentials**

   Configurations:

   - Valid Windows Domain Login Credentials
   - Kerberos Configuration on SAP ECC (Transaction: RZ10)
   - Liquid UI Server v3.5.549.0 and above
     - The Liquid UI Server should be on the same domain
     - Kerberos DLL is distributed as part of the Liquid UI Server installation. Older Version: Make sure that you have kerberos library (32bit:gsskrb5.dll, 64bit:gx64krb5.dll) files under Liquid UI Server (or GuXTWSServer) folder.
   - Configure Liquid UI Server with sapproxy.ini file
   - Configure Secure Network Communication in SAP GUI (if doesn't exist)
   - Login to Liquid UI for iOS using Windows Domain Credentials

2. **Portal**

   Configurations:

   - Configure Liquid UI Server with sapproxy.ini file

3. **Key-certificate pair**

   Configurations:

   - Valid Windows Domain Login Credentials
   - Liquid UI Server v3.5.561.0 and above
     - The Liquid UI Server should be on the same domain
   - Obtaining Certificate
   - Import the certificate into Liquid UI Server and SAP System
   - Import the key-certificate pair into SAP Server

- Import Synssl.dll, version 2.0.0.0 and later
- Configure Liquid UI Server with sapproxy.ini file
- Login to Liquid UI for iOS using Windows Domain Credentials

4. **Key-certificate pair with Cyber safe**

Configurations:

- Valid Windows Domain Login Credentials
- Liquid UI Server v3.5.584.0 and above
  - The Liquid UI Server should be on the same domain
- Generating certificate using openssl.exe
- Import the certificate into the Liquid UI Server and SAP System
- Import the key certificate pair into the SAP Server
- Install and configure Cyber Safe on the Liquid UI Server
- Configure Liquid UI Server with sapproxy.ini file
- Check SSO running successfully
- Login to Liquid UI for iOS using Windows Domain Credentials

Users have the option to create a domain name within the 'Secure Network Communications' (SNC) framework, which can be utilized for multiple logins. Liquid UI Server facilitates user authentication via Windows Active Directory for Liquid UI for iOS, streamlining the process. This means users only need to remember one set of credentials, and administrators have just one username database to manage.

Unique solution ID: #1988
Author: Poojitha Reddy
Last update: 2024-06-11 11:27