Secure Container Release

How to migrate from an ID wallet in the Cloud to an ID wallet on Premise?

Introduction

In this guide, we will provide you with a 3 step approach to install the ID wallet on Premise for Secure Container Release (SCR).

Step 1: Prepare your hardware infrastructure;
Step 2: Make sure you have a valid SSL certificate;
Step 3: Plan a call with our support team to install the ID wallet on Premise.

Step 1: Prepare your hardware infrastructure

For Windows, you need:

1. a Windows server (tested on 2012 R2, 2016 and 2019), with minimal specs: 1vCPU, 8GB ram, 80GB SSD;
2. an administrator account or an account that can install services on this server;
3. the internal IP address or machine name of the server;
4. an open port 3002 between the server and the clients that need access to the wallet (can be adjusted);
5. an open port 443 between the server and the blockchain nodes: 37.252.121.190; 84.22.107.112; 37.252.127.71 & 84.22.115.76.
6. the NTP service should be enabled;
7. In case an ID wallet on Premise was installed on the server before, first stop the wallet services and then uninstall the wallet first using the uninstall.exe in the c:/program files/tmining-directory.

For Linux, you need:

1. a Linux server with Ubuntu or CentOS (tested on Ubuntu 18.04 LTS or later and CentOS 8.1 or later), with minimal specs: 1vCPU, 8GB ram, 80GB SSD;
2. an administrator account or an account with sudo-privileges that enables you to install software on your computer;
3. the internal IP address or machine name of the server;
4. an open port 3002 between the server and the clients that need access to the wallet (can be adjusted);
5. an open port 443 between the server and the blockchain nodes: 37.252.121.190; 84.22.107.112; 37.252.127.71 & 84.22.115.76.
6. the NTP service should be enabled;
7. In case an ID wallet on Premise was installed on the server before, first stop the wallet services and then uninstall the wallet first

Step 2: Make sure you have a valid SSL certificate

SSL-certificates for ID wallets on Premise

An ID wallet on Premise runs on your own server but users that access the SCR web app will initiate (in the background) a connection to this wallet. This connection is used for authentication and for decrypting the pins.

Modern browsers require that this kind of cross-site access is secured using valid SSL-certificates. Therefore, this should also be the case when you use an ID wallet on Premise.

We do not support the use of self-signed certificates for this purpose. Therefore, when installing an ID wallet on Premise, you are expected to provide a valid SSL-certificate for this server, including the files and passphrase and:

- obtained from a valid, trusted CA (= NOT self-signed)
- contains the FQD-name of the server in the CN-field
- in case of a multi-domain certificate: contains the FQD-names of the server in the SAN-field
- obtained from the certificate authority as e.g. pfx / cer / crt / cert / pem-file, and to be installed on your server
- for specific browsers like Safari the validity of the certificate should be less than one year.

If you do not have a valid SSL-certificate, you can buy this from a trusted CA.

Other issues

My external and internal domain do not match

If your external and internal domain do not match, for instance you use company.local internally and Company.com externally, buying an SSL-certificate from an external CA is not that easy. From 2015, local names are not accepted for SSL certificates anymore (see for instance https://cabforum.org/internal-names/).

However, there are some solutions documented in this white paper: https://www.globalsign.com/en/resources/white-paper-internal-server-names-ip-address-requirements.pdf

It is also still possible to buy intranet SSL certificate from certain CA's, e.g. . https://www.globalsign.com/en/ssl/intranet ssl

However, we do not support these solutions out of the box, so we advise to use a server for which you can obtain a publicly trusted certificate. This is because modern browsers tend to update their policies on SSL/TLS-certificates regularly, and the requirements tend to get stronger over time.

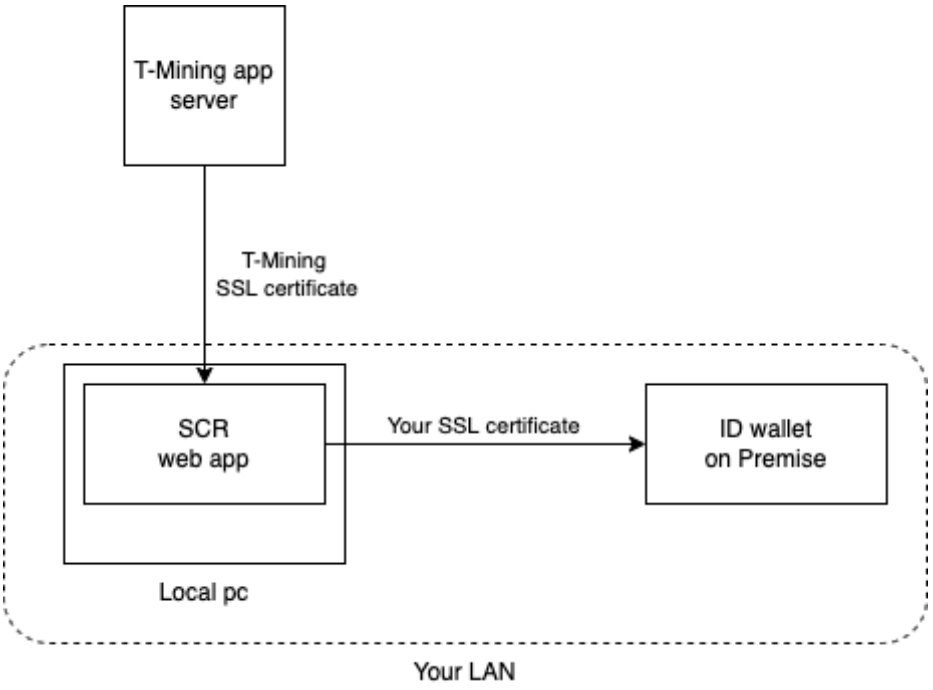
A common solution is to buy a certificate with the external domain name and put the IP-address of the server in the public DNS. Then clients can resolve the IP-address and the certificate is validated.

Why are these certificates necessary?

When a user opens the SCR web or governance app, the application will be loaded from the T-Mining application server. This connection is secured with an SSL-certificate of T-Mining.

However, when a user logs in into the application or executes transactions on the decentralised network, the web app connects to your ID wallet on Premise (in your LAN) to do this. This connection stays within your LAN, but should also be secured by a SSL/TLS-certificate. Modern browsers require this, to allow for cross-domain calls from the web app.

This is also illustrated below:



Step 3: Plan a call with our support team to install the ID wallet on Premise

Our support team will assist you with the installation of an ID wallet on Premise on your server. This will take approximately 1 hour. Please contact us via support@securecontainerrelease.com.