

# Certificate for Mobile App

## Contents

- [1 Introduction](#)
- [2 Requirements](#)
- [3 Updating the Certificate](#)
- [4 Installing the Keystore](#)

## Introduction

Some versions of Swivel Secure's mobile apps will not connect to the Sentry appliance unless the entire certificate chain is in the keystore as a single entry. This document describes how to achieve that.

## Requirements

You will need:

- The keystore from your Sentry appliance, including the signed certificate
- A copy of [Keystore Explorer](#).
- The intermediate certificate(s) and root certificate from your certificate authority. You should be able to get these from their website.

If you have not yet installed your certificate in the keystore, Keystore Explorer can do that for you as well, but this document assumes the certificate is installed but without any chain.

You can access your current keystore from your appliance in the following location:

```
/home/swivel/.keystore
```

Use WinSCP or Filezilla to download this file to a local Windows machine.



## Updating the Certificate

Open Keystore Explorer, then open the copy of the keystore using File, Open. Note that you will need to know the password for your keystore.

swiveladfs.com-single.jks - KeyStore Explorer 5.5.1

File Edit View Tools Examine Help

swiveladfs.com-single.jks


	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
 	*.swiveladfs.com	RSA	2048	21/11/2022 23:59:59 GMT	08/03/2022 14:47:09 ...

KeyStore Type: JKS, Size: 1 entry , Selected: 1 entry, Path: 'D:\Work\Certs\swiveladfs.com-single.jks'


There may be other entries shown, if you have imported the intermediate certificates as separate entries (trusted certificates). The server certificate is the one with the double-key icon next to it.


To confirm that the certificate doesn't already have a chain, double-click on the certificate:

Certificate Details for Entry '\*.swiveladfs.com'

Certificate Hierarchy:  \*.swiveladfs.com

Version: 3

Subject: CN=\*.swiveladfs.com 


Issuer: CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com 

Serial Number (hex.): 0xA6C8627AB0A763B131BEBE2B72BCA0A



Serial Number (dec.): 13855769004290731759691324766989044234

Valid From: 22/11/2021 00:00:00 GMT

Valid Until: 21/11/2022 23:59:59 GMT

Public Key: RSA 2048 bits 

Signature Algorithm: SHA-256 with RSA

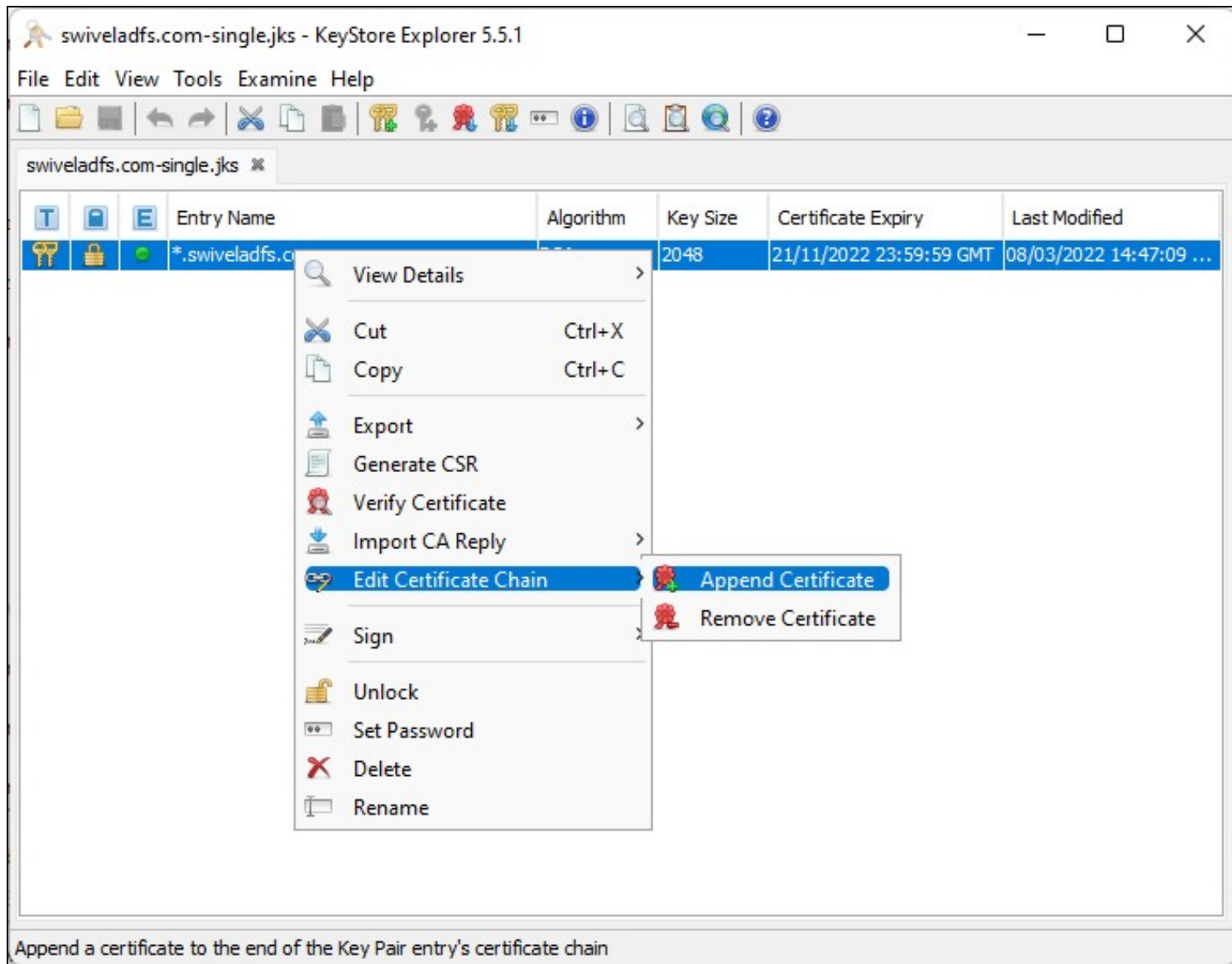
Fingerprint: SHA-256  C9:EB:40:30:56:4A:3B:D3:E5:7E:3B:0D:EC:6C:6E 

Export Extensions PEM Verify ASN.1

OK

Now you need to append the intermediate certificate(s) and root certificate. This must be done in the correct order, starting with the immediate signing certificate and ending with the root. If you select the wrong certificate, the operation will fail.

Right-click on the certificate, then click "Edit Certificate Chain", then "Append Certificate"






You will need to enter the password again (only once, no matter how many intermediate certificates there are).


Select the intermediate certificate from the file dialog. Assuming you selected the right intermediate certificate, you will see the message "Append Certificate Successful".


Once you have added all the certificates, double-click on the certificate entry again to confirm that there is a chain of certificates:

Certificate Details for Entry '\*.swiveladfs.com'

Certificate Hierarchy:  DigiCert Global Root CA  
 Encryption Everywhere DV TLS CA - G1  
 \*.swiveladfs.com

Version: 3

Subject: CN=\*.swiveladfs.com 


Issuer: CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com 

Serial Number (hex.): 0xA6C8627AB0A763B131BEBE2B72BCA0A



Serial Number (dec.): 13855769004290731759691324766989044234

Valid From: 22/11/2021 00:00:00 GMT

Valid Until: 21/11/2022 23:59:59 GMT

Public Key: RSA 2048 bits 

Signature Algorithm: SHA-256 with RSA

Fingerprint: SHA-256  C9:EB:40:30:56:4A:3B:D3:E5:7E:3B:0D:EC:6C:6E 

Export Extensions PEM Verify ASN.1

OK

Save this modified keystore.

## Installing the Keystore

To install the modified keystore, you will need to upload it to the folder /backups/upload on the appliance.

On the appliance console, go to the Tomcat menu, then Certificates:

```
Swivel Maintenance (c) 2019                                Certificate Menu

PrivateKeyEntry      : *.swiveladfs.com
Keystore Password    : lockbox

1) Create Local Certificate
2) Generate CSR
3) Import to New / Existing Alias
4) View Keystore
5) Delete Certificate from Keystore
6) Generate Self-Signed Certificate
7) Clone Certificate
8) Import / Roll Back to Previous Keystore
9) Change Keystore Password
0) Back

Select: _
```

Now select "Import / Roll Back to Previous Keystore":

```
Swivel Maintenance (c) 2019                                Replace Keystore Menu

1) Import Keystore
2) Roll Back Keystore
0) Back

Select: _
```

Select your modified keystore from the menu, then enter Y to confirm you want to overwrite the keystore.

In order to activate the new keystore, you will need to restart Tomcat. If you want to check the certificate before restarting Tomcat, enter N not to restart Tomcat, then choose the option "View Keystore" then the appropriate certificate to check the certificate. You should see the Certificate chain length of 3, assuming there is just one intermediate certificate. If the length is 1, then you have not added the intermediates correctly.

When you are satisfied, restart Tomcat to activate the new certificate.