Sage 300c

Digital Certificate Configuration Guide

June 2017

This is a publication of Sage Software, Inc.

© 2017 The Sage Group plc or its licensors. All rights reserved. Sage, Sage logos, and Sage product and service names mentioned herein are the trademarks of The Sage Group plc or its licensors. All other trademarks are the property of their respective owners.

Last updated: June 22, 2017

Contents

Overview **4**
Digital Certificates 4
Certificate Requirements for OAuth and SIRC Services 4

Prerequisites **5**

Configuring Your System **6**
Step 1: Configure SIRC 6
Step 2: Configure Sage 300c 8
Step 3: Configure OAuth 8
Step 4: Update Application Pool Identity 9

Overview

This guide provides instructions for configuring Sage 300c, OAuth, and Sage Intelligence Reporting Cloud (SIRC) services to run in a secured environment using digital certificates.

Digital Certificates

A Digital Certificate is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject.

In a typical public-key infrastructure (PKI) scheme, the certificate issuer is a certificate authority (CA), usually a company that charges customers to issue certificates for them. By contrast, in a web of trust scheme, individuals sign each other's keys directly, in a format that performs a similar function to a public key certificate.

Examples of certificate authorities:

- https://www.digicert.com
- https://www.globalsign.com
- https://www.entrust.com/ssl-certificates/
- https://www.godaddy.com/web-security/ssl-certificate

After a certificate is acquired, it needs to be imported into the certificate store of the machine where Sage300 is installed.

Instructions for installing a certificate are available here:
https://www.godaddy.com/help/iis-7-install-a-certificate-4801

Certificate Requirements for OAuth and SIRC Services

OAuth and SIRC services both need to run under a secure protocol, so a digital certificate(s) must be installed and assigned to each of these services.

The default digital certificate that comes with Sage 300c is for development purposes only. If you use this certificate, users may receive warning messages from their browser about accessing “insecure” websites. To ensure that such messages do not appear, a digital certificate must be purchased to replace the one that comes with Sage 300c.

Prerequisites

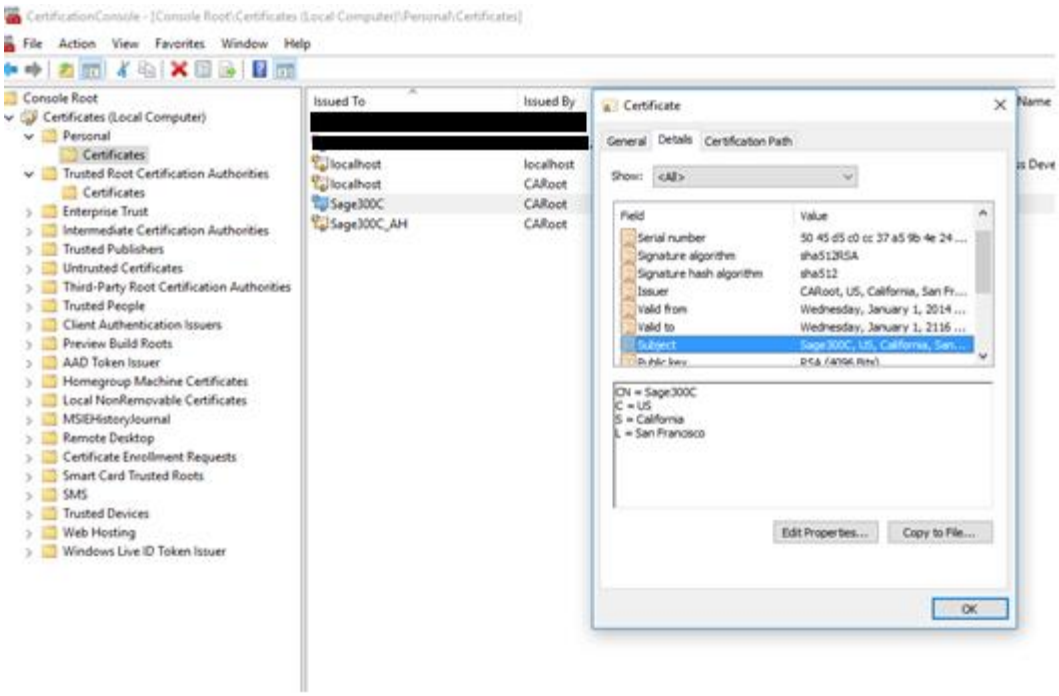
Before performing the tasks in this guide, ensure that:

- The new digital certificate is installed, and it is:
  - A server authentication certificate.
  - Trusted by a Trusted Root Certification Authority.
- Sage 300c is installed.
- The OAuth website is using the new certificate.
- IIS is updated to use the new certificate for both SIRC and OAuth.

Configuring Your System

Step 1: Configure SIRC

1. In the Certificate Store, double-click the digital certificate.
2. On the Details tab, select **Subject**.

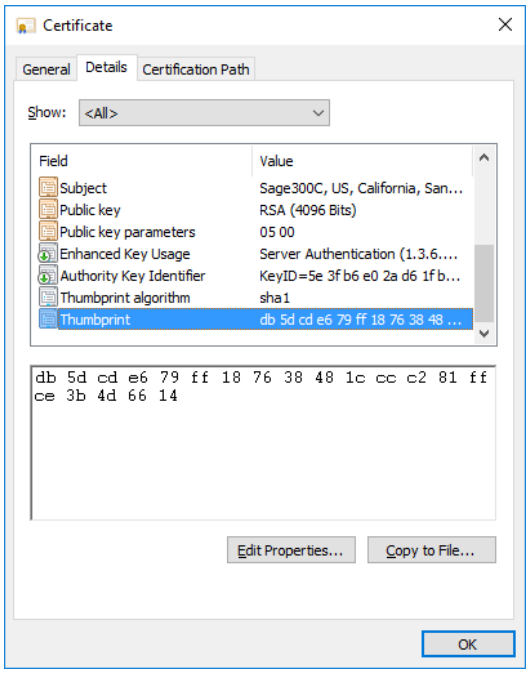


3. Copy the Subject value to a text editor, and convert it to the following format:

   CN=Sage300C, C=US, S=California, L=San Francisco

   > **Important!** Ensure that there are no spaces on either side of the '=' characters. If there are multiple subjects, ensure that entries are separated by ", " (a comma followed by a space).

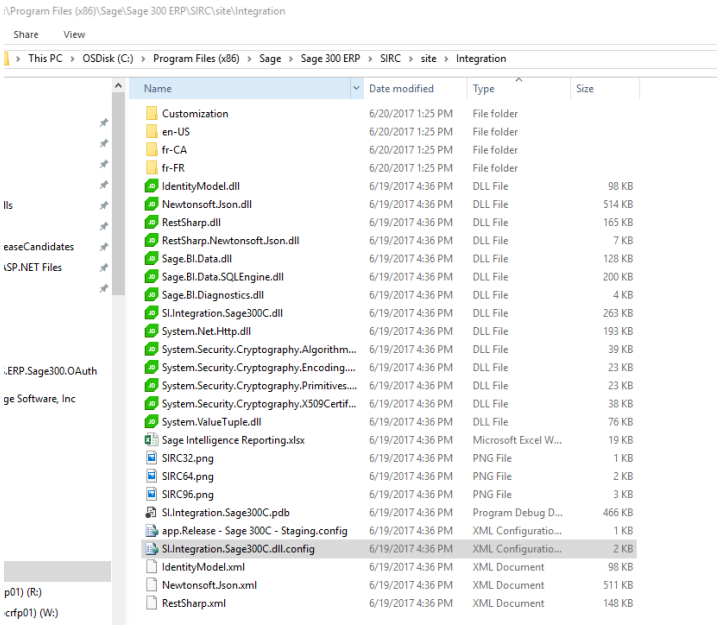
4. Select **Thumbprint**.



5. Copy the Thumbprint value to a text editor, and convert it into capital letters with no spaces. The example shown above would look like this after being converted:

   DB5DCDE679FF187638481CCCC281FFCE3B4D6614

6. In a text editor, open the SI.Integration.Sage300C.dll.config file, which is in the *{Sage 300 Installation}*\SIRC\site\Integration folder.

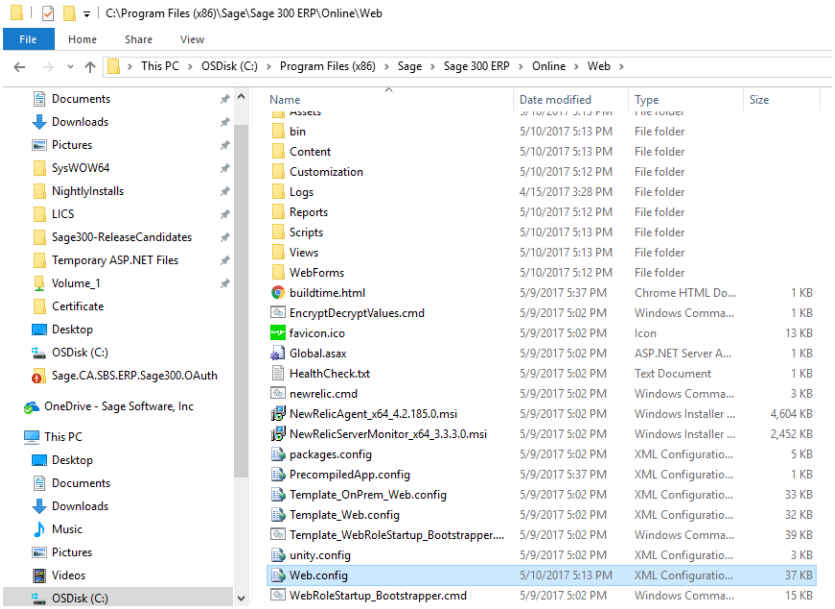


7. Search for “ValidCertSubject”, and replace the value with the one previously defined:

   <add key="ValidCertSubject" value="CN=Sage300C, C=US, S=California, L=San Francisco"/>

Step 2: Configure Sage 300c

1. In a text editor, open the Web.config file for Sage 300c, which is in the *{Sage 300 Installation}*\Online\Web folder.

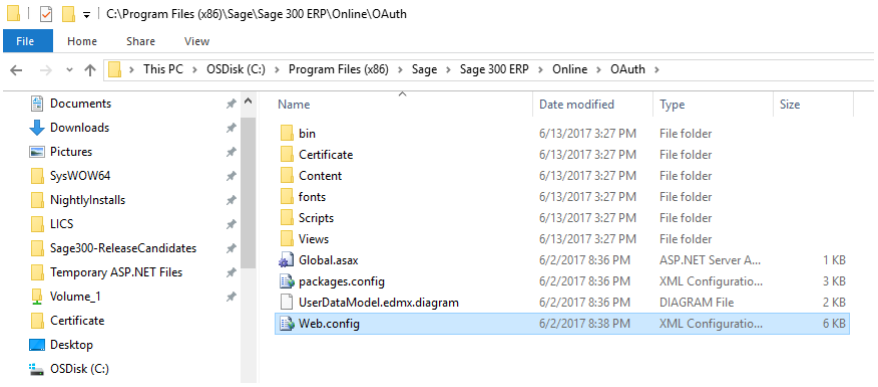


2. Search for “ValidCertSubject”, and replace the value with the one previously defined:

   <add key="ValidCertSubject" value="CN=Sage300C, C=US, S=California, L=San Francisco"/>

Step 3: Configure OAuth

1. In a text editor, open the Web.config file for OAuth, which is in the *{Sage 300 Installation}*\Online\OAuth folder.



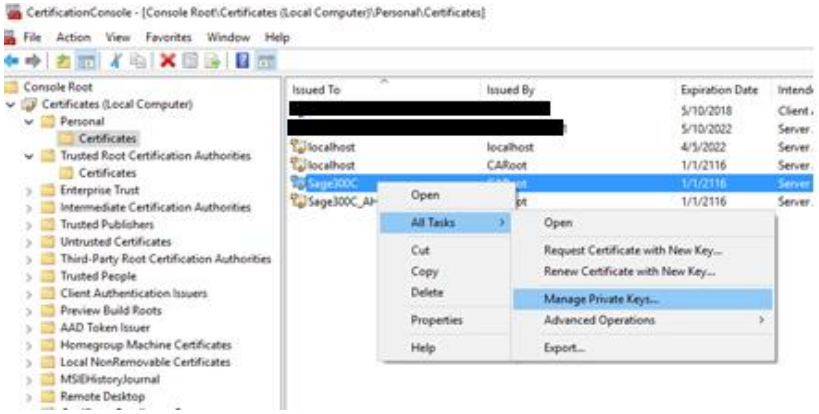
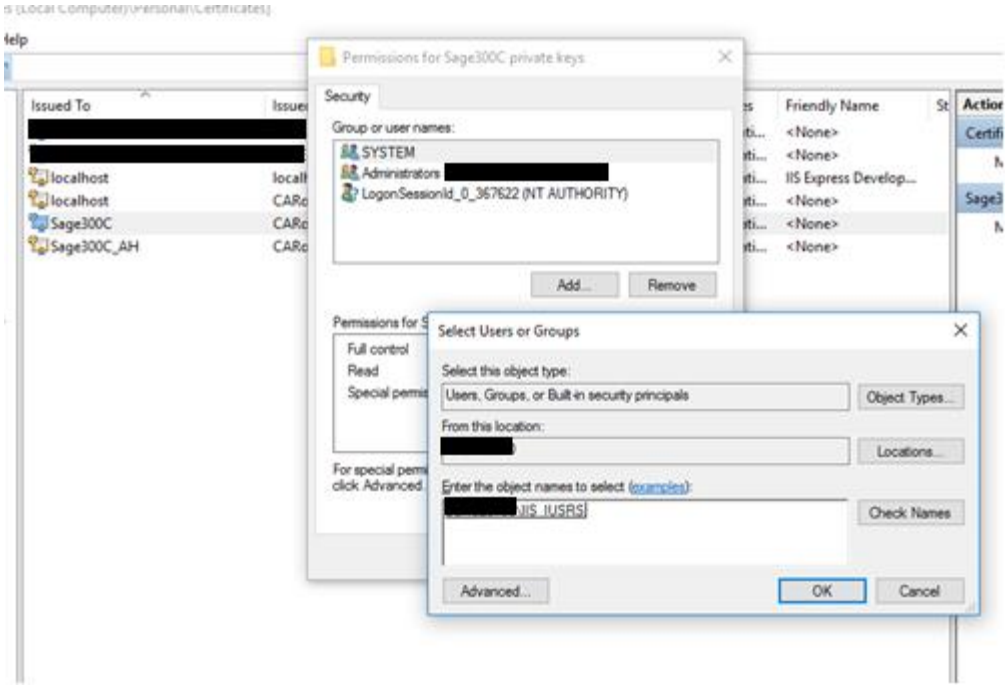
2. Search for “CertificateThumbprint”, and replace the value with the one previously defined:

   <add key="CertificateThumbprint" value="DB5DCDE679FF187638481CCCC281FFCE3B4D6614"/>

Step 4: Update Application Pool Identity

The OAuth server needs access to the private key of the digital certificate for signing the tokens.

1. In the Certificate Store, right-click the digital certificate and select **All Tasks** > **Manage Private Key**.



- On the Permissions for Sage300C private keys screen, click **Add**.
- In the **From this location** field, enter your local machine name.
- In the **Enter the object names to select** field, enter **IIS_IUSRS**.
- Click **Check Names**.
- Click **OK** and then **OK** to close the screens.