Changing the Mobile Client Web Service

Technical Document

Copyright © Gallagher Group Limited

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2024. All rights reserved.

Contents

Disclaimer 2

Introduction 3

1 Changing the TCP Ports that the Web Service Listens on 3

2 Replacing the Web Service Certificate with an Alternative Certificate 4

2.1 Explanation: Certificate Modes 4

2.2 Using a Custom External Certificate 5

Introduction

This document references version 9.00 of the Command Centre server. It also contains correct information for versions 8.00 through 8.90.

Important: If you are working with a version of Command Centre earlier than 8.00, the procedures in this document will not work for you. Please obtain an older version of this document to match your server version.

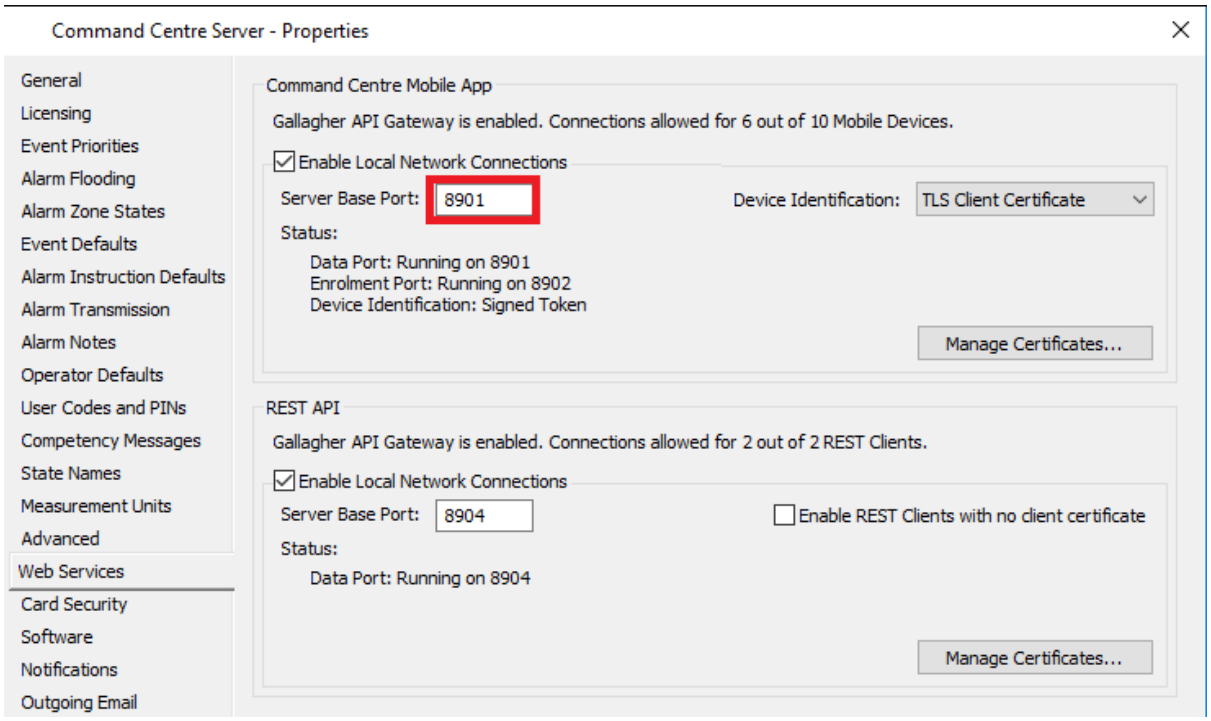
If you are working with a newer version of command centre, please confirm with your Gallagher representative that you are following the correct process for your version.

This document describes how you can change or replace the default Mobile Client and/or REST API web service TLS certificate with an alternative certificate. **These procedures are optional**.

- Replacing the web service certificate does not increase the security of the solution. Typically, this is done to satisfy corporate policy or to support a reverse proxy.
- Altering the ports is only required to avoid collisions with other third-party software, or to satisfy corporate policy.

1 Changing the TCP Ports that the Web Service Listens on

1. Launch the Command Centre Configuration client and log in as an operator with Edit Site or Advanced User privileges in the Root division
2. Open the **Web Services** tab of the **Server Properties** within the Configuration Client and enter the new data port number in the **Server Base Port** field.



Note: The mobile web service data port is the one you specify here. The mobile device enrolment port is always that port plus one.

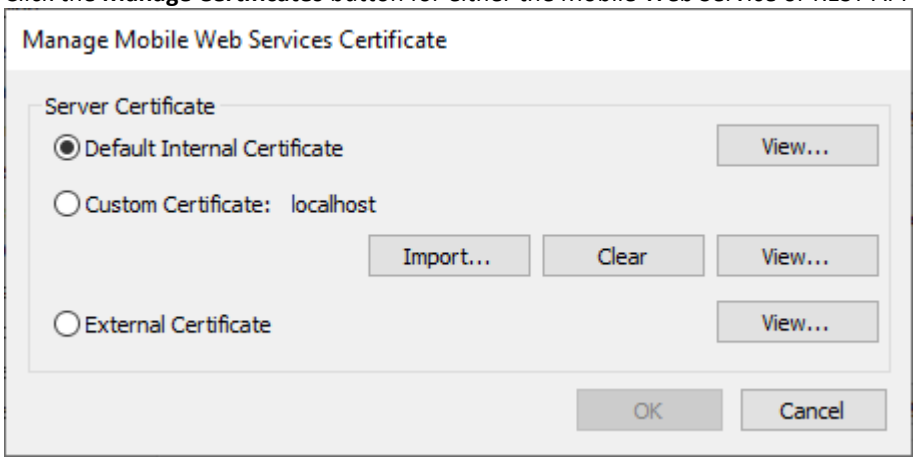
3. Click **Apply**. You should see the status update to reflect the port change. No further steps should be required in Command Centre, although it is likely you will need to reconfigure Windows Firewall, or any other third-party Firewall software to allow the new ports.

Copyright © Gallagher Group Limited

The same procedure can be followed to change the REST API port.

2 Replacing the Web Service Certificate with an Alternative Certificate

1. Login to the Command Centre configuration client and open the **Web Services** tab as above.
2. Click the **Manage Certificates** button for either the Mobile Web Service or REST API



3. Select **Custom Certificate** and click **Import…**
4. Use the file browser to find your PFX or P12 file containing the certificate and its associated private key, and then when prompted enter the password

   Note: If you do not have a certificate in a PFX/P12 file, and instead have two separate files for the certificate and private key, you will need to convert them to a PFX/P12 file first. This can be easily done using OpenSSL or other tooling.
5. Click **OK** to close the Manage Certificates dialog.
   Note that the new certificate will not be saved to the database and will not take effect until you click **Apply** on the main **Web Services** tab, so it is likely you will wish to do this too.

Note: If you have existing devices running the Command Centre Mobile App, they will see the certificate change as a potential malicious attack and block connections to the server. You must re-enrol them. This does not affect the Mobile Connect App or Mobile Credentials.

2.1 Explanation: Certificate Modes

In the **Manage Certificates** dialog, there are three modes you can select.

Default Internal Certificate:
The Default Internal Certificate is a self-signed certificate which is generated by Command Centre and stored in the database. It exists to provide a standard option for sites that don't need a custom certificate. The private key is protected by Command Centre's Database Encryption.

Custom Certificate:
This lets you import your own certificate as per the instructions above.
The private key will be protected by Command Centre's Database Encryption.

External Certificate:
An "External" certificate is loaded from the Windows certificate store rather than Command Centre's database.

Copyright © Gallagher Group Limited

This option exists for sites with IT policy that mandates use of the Windows Certificate Store, or for upgrade compatibility. Older versions of Command Centre *only* supported external certificates, so if you configured any mobile devices on an older Command Centre, and then upgrade to 8.30, those mobile devices will still be locked to the external certificate in the Windows Store. Upgrading servers will default to the External option to avoid breaking existing connections.

Unless required to use external certificates by policy, we recommend that you use either the Default Internal or a Custom certificate. These are easier to manage, and because they are stored in the database, they are included in Command Centre database backups and will survive a restore onto a new server in the case of server upgrade/migration or disaster recovery.

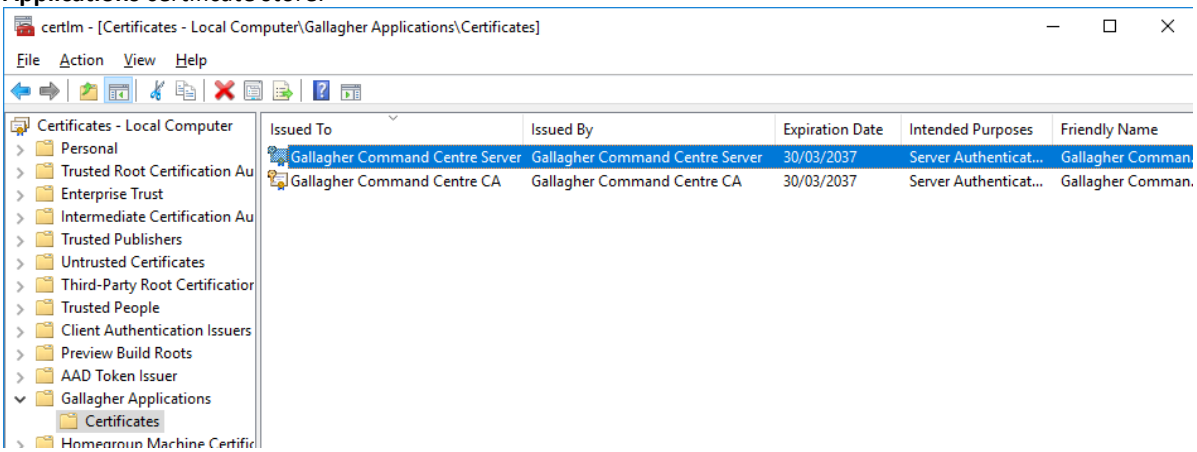
2.2 Using a Custom External Certificate

These instructions should also be correct for Command Centre versions 8.00 through 8.20, which only support external certificates.

The default external certificate is automatically generated by the Command Centre installer.

If you have an IT policy which requires that you store certificates in the Windows Certificate Store, ***and*** you wish to change the certificate used by the Mobile Web Service, you must replace the default external certificate using these instructions.

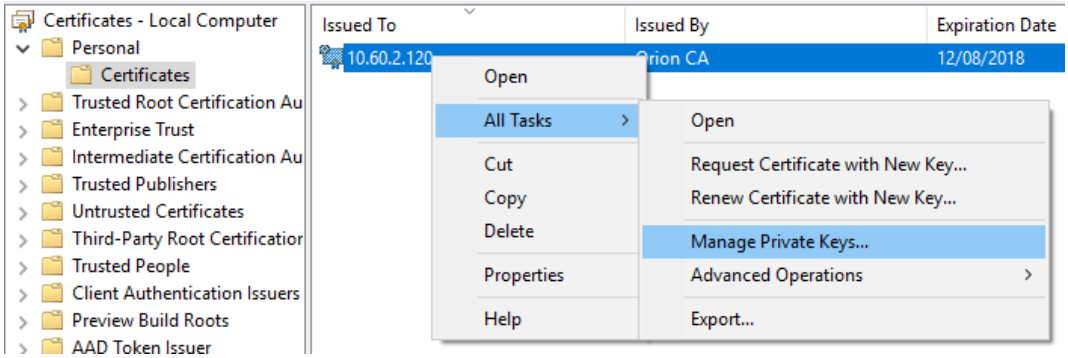
1. Launch the windows certificate manager for Local Computer certificates
   *Shortcut: run **certlm.msc***
2. Locate the default self-signed **Gallagher Command Centre Server** certificate from the **Gallagher Applications** certificate store.



   Change its Friendly Name to **Gallagher Command Centre Server Backup** or **Original** or similar to reflect that it will no longer be in use.
   It is also recommended that you move it to another folder, such as the Personal folder, until you have confirmed that the new certificate is in place and all services are working correctly, at which point you may delete the old certificate if you wish.
3. Right-click on the **Personal** folder under **Certificates - Local Computer** and from the context menu select **All Tasks** > **Import…**
4. Browse to find the PFX or P12 file which contains the certificate and private key you wish to import, then follow the rest of the Certificate Import Wizard to import it, placing the certificate in the **Personal** store

Copyright © Gallagher Group Limited

5. Expand and select **Personal** / **Certificates** in the tree view, then right click on the newly-imported certificate and select **All Tasks** > **Manage Private Keys**.



6. Add the user account which the Command Centre service is running under, and give that account **Read** permissions. The default account for new installations of Command Centre 7.70 is **Network Service**, however this may be different depending on customer requirements.

7. Right-click on the certificate, select **Properties**, then set the certificate's **Friendly Name** to "Gallagher Command Centre Server".

8. Move the certificate out of the **Personal** folder and into the **Gallagher Applications** / **Certificates** folder, by dragging and dropping the certificate entry.

9. Restart the mobile client web services, as follows:
   Change **Device Identification Mode** to the opposite mode of whatever it is.
   Click the **Apply** button.
   Change **Device Identification Mode** back to the original mode.
   Click the **Apply** button.

Note: If you have existing devices running the Command Centre Mobile App, they will see the certificate change as a potential malicious attack and block connections to the server. You must re-enrol them. This does not affect the Mobile Connect App or Mobile Credentials.

Copyright © Gallagher Group Limited