Gallagher Command Centre

Enable OPC UA over HTTPS for Visitor Management Kiosk

Technical Information Paper

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 2023. All rights reserved.

Table of Contents

1 Introduction 3
2 Affected services 3
3 Implications 3
4 Configure Command Centre Service 3
5 VM Kiosk Client Configuration Files 4
6 Command Centre server Certificate Port Binding 5
7 Export Certificate from Command Centre server to VM Kiosk PC 5

1 Introduction

This document outlines a method on how to configure Command Centre and the Visitor Management Kiosk client application to communicate using OPC UA over HTTPS. This document only demonstrates how to implement the HTTPS connection using the Command Centre generated and self-signed certificates. It is possible to use alternative certificates; the application of these certificates is outside the scope of this document.

OPC UA over HTTPS communication for the Visitor Management Kiosk client is normally used when a reverse proxy is setup to segregate the Visitor Management Kiosk from the rest of the network.

2 Affected services

The following services and applications will be affected by changes recommended in this document:

- FT Command Centre Service (CCNTSAD.exe)
- Visitor Management Kiosk Application (VMKiosk.exe)

3 Implications

The modifications to your Command Centre installation as specified in this document will have the following implications:

- You will need to restart the FT Command Centre Service for your changes to take effect.
- The changes recommended in this document involve editing the Command Centre configuration files. If these become corrupted, the service or application will fail to start or will run incorrectly.

Note: This process will also need to be followed if the Command Centre version is upgraded.

4 Configuring Command Centre Service

An 'OpcUaHttpsPort' entry needs to be added to the Command Centre Server 'CCNTSad.exe.config' file. This is required for the Visitor Management Kiosk communication to the server using OPC UA over HTTPS.

1. Navigate to the Gallagher Command Centre Bin folder. By default, this is located in:

   ```
   For 32-bit systems:  C:\Program Files (x86)\Gallagher\Command Centre\Bin
   ```

   ```
   For 32-bit systems:  C:\Program Files (x86)\Gallagher\Command Centre\Bin
   ```

2. Make a backup copy of the file **CCNTSad.exe.config**.
3. Edit **CCNTSad.exe.config** using Windows Notepad, as follows:
   a. Click the Windows taskbar **Search** button and type in notepad to find the "Notepad" application.
   b. Right-click the result and select **Run as administrator**.
   c. Click **File** > **Open**, then navigate to the Command Centre Bin folder and open **CCNTSad.exe.config**.

Copyright © Gallagher Group Limited

4. Add the following line to the configuration/commandcentre/serverSettings (<serverSettings>) section, where “4840” is any available port number:

   ```
   <opcuasetting name="OpcUaHttpsPort" value="4841" />
   ```

   a. Locate the tag <serverSettings>.

   b. Create a new line after the last entry in that section but prior the closing tag</serverSettings>.

   c. Place the new entry on a new line ensuring you enter the text exactly as shown, with the exception that you may place your own allocated port number in place of “4841”.

Example:

```
<serversettings>
      <opcuasetting name="Port" value="4840" />
      <opcuasetting name="OpcUaHttpsPort" value="4841" />
```

5. Once the entry has been completed, save the changes made to the **CCNTSad.exe.config**.
6. Restart the Command Centre Services.

5 VM Kiosk Client Configuration Files

1. On the server, navigate to VMKioskSetup\VMKiosk. By default, this is located in:

   ```
   C:\Program Files (x86)\Gallagher\Command Centre\VMKioskSetup\VMKiosk
   ```

2. Make a backup copy of the file **VMKiosk.exe.config**.
3. Edit **VMKiosk.exe.config** using Windows Notepad, as follows:

   a. Click the Windows taskbar **Search** button and type in notepad to find the “Notepad” application.

   b. Right-click the result and select **Run as administrator**.

   c. Click **File** > **Open**, then navigate to the Command Centre Bin folder and open **VMKiosk.exe.config**.

4. Change the “ServerUri” configuration setting from:

   opc.tcp://<server>:4840/UA/CommandCentre

   to the following, with your allocated port number in place of “4840”:

   https://<server>:4841/UA/CommandCentre/

Example:

```
<appSettings>
 <add key="ServerUri" value="opc.tcp://CCFTServerName:4840/UA/CommandCentre/"/>
```

Replaced with:

```
<add key="ServerUri" value="https:// CCFTServerName:4841/UA/CommandCentre/"/>
```


Copyright © Gallagher Group Limited

5. Run the **ClickOnceBuilder.exe** for the Kiosk to prepare it for deployment.
   By default, this is located in:

   C:\Program Files (x86)\Gallagher\Command Centre\VMKioskSetup\

6. Export the certificate to the Kiosk PC by following the steps in section 7 Export Certificate from Command Centre server to Kiosk PC.
7. Complete the procedure detailed in the "Visitor Management Kiosk Installation Instructions" topic in v8.00 of the *Gallagher Command Centre Configuration Client User Guide* (on page 52-3).

6 Command Centre server Certificate Port Binding

If the server port 4841 does not already have a TLS certificate bound, you will need to set that up using PowerShell.

a. Click the Windows taskbar **Search** button and type in powershell to find the "PowerShell ISE" application.

b. Right-click the result and select **Run as administrator**.

c. Paste the following script into PowerShell and press <**Enter**>.

```
$dataport = 4841

$thumbprint = (Get-ChildItem Cert:"LocalMachine\Gallagher Applications" | Where FriendlyName -eq "Gallagher Command Centre Server").Thumbprint

netsh http add sslcert ipport=0.0.0.0:$dataPort certhash=$thumbprint appid="{3be37061-a4d8-11d2-8b31-006097a452a8}" certstorename="Gallagher Applications" clientcertnegotiation=enable
```

This will return a message: *"SSL Certificate successfully added"*

d. To view the SSL Certificate port 4841, paste the following script into PowerShell and press <**Enter**>.

```
netsh http show sslcert ipport=0.0.0.0:4841
```

7 Export Certificate from Command Centre server to VM Kiosk PC

1. On the Command Centre Server system, run **mmc.exe**.
2. Click **File** > **Add/Remove Snap-in** > **Certificates** > **Computer account** > **Local computer** > **OK**.
3. Click **Certificates (Local Computer)** > **Gallagher Applications** > **Certificates** from the tree.
4. Select **All Tasks** > **Export** from the Gallagher Command Centre Server context menu. Click **Next** on the following three screens.
5. Specify a file name and location to export the certificate to.
6. On the Visitor Management Kiosk system, log in with the user account that the Kiosk application will run as and run **mmc.exe**.

Copyright © Gallagher Group Limited

7. Choose **File** > **Add/Remove Snap-in** > **Certificates** > **My user account**.
8. Right-click **Certificates (Current User)** then click **Trusted Root Certification Authorities** > **Certificates** in the tree.
9. Select **All Tasks** > **Import** from the context menu.
10. Select the file you exported in step 5 and then **Next** > **Next** > **Finish** to import it.

Copyright © Gallagher Group Limited