Configuring IIS as a Reverse Proxy for Mobile Client Web Services

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

1 Reverse Proxy Configuration Overview 3
2 Pre-requisites 4
3 Configure the Command Centre Server 4
4 Configure IIS to Act as a Reverse Proxy Server 5
4.1 Reference Configuration Instructions 5

1 Reverse Proxy Configuration Overview

In order to configure a reverse proxy server to be used for Command Centre Mobile Client Web Services, the following general steps must be taken. This document details specific instructions for Microsoft IIS, however the following steps should be generalizable for a reverse proxy solution regardless of vendor.

1. Obtain or create an SSL certificate, to be installed on both Command Centre and the reverse proxy.
2. Install the SSL certificate into and configure the Command Centre server.
3. Install the SSL certificate into the reverse proxy server and give it appropriate permissions.
4. If required, enable the reverse proxy functionality of your proxy software *(This is not installed or enabled in IIS by default.)*
5. If required, configure your proxy software to trust the new SSL certificate provided by Command Centre *(IIS will not trust the certificate by default.)*
6. Configure reverse proxy entries for port 8901 and 8902, ensuring:
    a. The TCP ports on the reverse proxy server match the ones used by Command Centre.
    If different ports are required, it is recommended that you configure both Command Centre and the reverse proxy to both use those different ports, rather than attempting to rewrite URL's in responses on the proxy.
    b. The just-installed SSL certificate is used.
    c. The reverse proxy server passes the HTTP Host header from the mobile device through to Command Centre without rewriting it *(IIS will rewrite it by default.)*
    d. The proxy does not attempt "SSL Offloading". It should communicate with the backend Command Centre server using HTTPS.
    e. The reverse proxy does not otherwise attempt to rewrite or manipulate the requests or responses.
7. Secure the proxy server, including deploying strong TLS configuration.
    For example, refer to https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility

Copyright © Gallagher Group Limited

2 Pre-requisites

1. A Windows Server with IIS installed that you wish to use as the reverse proxy appliance.
   These instructions have been tested on Windows Server 2012 R2 and Windows Server 2016.

2. An SSL certificate to install on both the IIS proxy server and the Command Centre server.
   This can either be a certificate purchased from a legitimate online certificate authority (such as Digitrust, Comodo, Entrust, etc.), or a self-signed certificate.

   You must have both the certificate and the private key, contained in a single PKCS12 file (.p12 or .pfx). If you have the certificate and private key in two separate files (.cer and .key), you can use openssl to load them into a pfx file as follows:

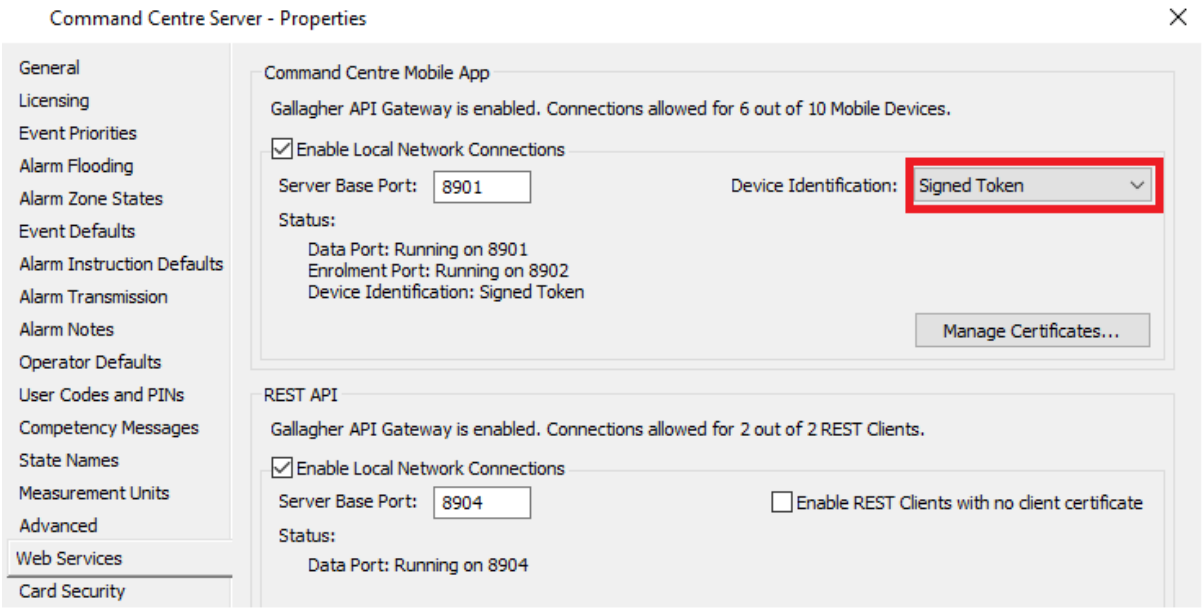
```
openssl pkcs12 -export -out cert.pfx -inkey filename.key -in filename.cer
```

3 Configure the Command Centre Server

1. Install the SSL certificate into the Command Centre server according to the instructions in the *Replacing the web service certificate with an alternative certificate* section of the *Changing the Mobile Client Web Service* document.

2. In Configuration Client, open **Server Properties** then open the **Web Services** tab.

3. Set the **Device Identification** mode to **Signed Token**.



Copyright © Gallagher Group Limited

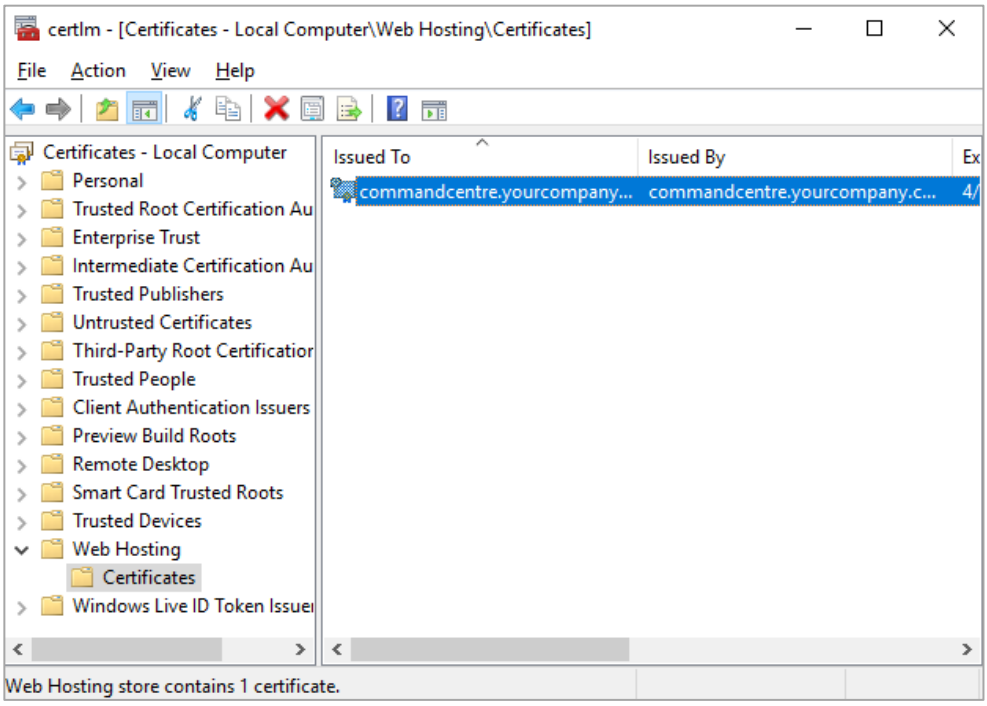
4 Configure IIS to Act as a Reverse Proxy Server

The following configuration instructions are designed to provide a **basic reference configuration only**. Gallagher provides no guarantee as to the correctness, security or functionality of the following configuration information.

A reverse proxy installation for a production system should be configured by a knowledgeable system administrator according to the specific security and functionality needs of the site.

4.1 Reference Configuration Instructions

1. Locate the SSL certificate .pfx or .p12 file that you loaded into Command Centre in Step 1 of the previous procedure. Import it into the **Local Machine** \ **Web Hosting** certificate store on the IIS server.



2. **<u>For self-signed certificates only.</u>**
   You will need to copy the certificate into the **Trusted Root Certification Authorities** certificate store.

   You will also need to disable windows **Automatic Root Certificates Update**. If you do not do this, windows may periodically delete your self-signed certificate from Trusted Root Certification Authorities and cause the proxy to stop functioning.

   a. Launch **gpedit.msc**

   b. Navigate to the folder **Computer Configuration** \ **Administrative Templates** \ **System** \ **Internet Communication Management** \ **Internet Communication settings**

   c. Double-click **Turn off Automatic Root Certificates Update**

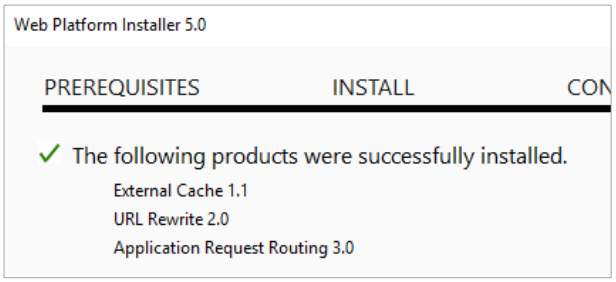
   d. Select **Enabled**, then click **OK**

3. Install the **Application Request Routing** IIS module.
   Note: This is not built in to windows. You must download and install it by following the instructions

Copyright © Gallagher Group Limited

at the following link: http://www.iis.net/expand/ApplicationRequestRouting

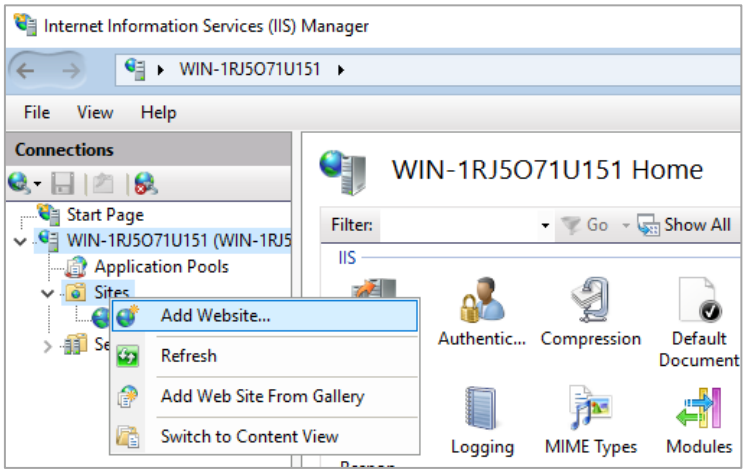
When successful, you should see an indicator such as this:



4. Enable the **preserveHostHeader** setting for Application Request routing by executing the following from an Administrator privileged command prompt:

```
%windir%\system32\inetsrv\appcmd.exe set config -
section:system.webServer/proxy -preserveHostHeader:true /commit:apphost
```

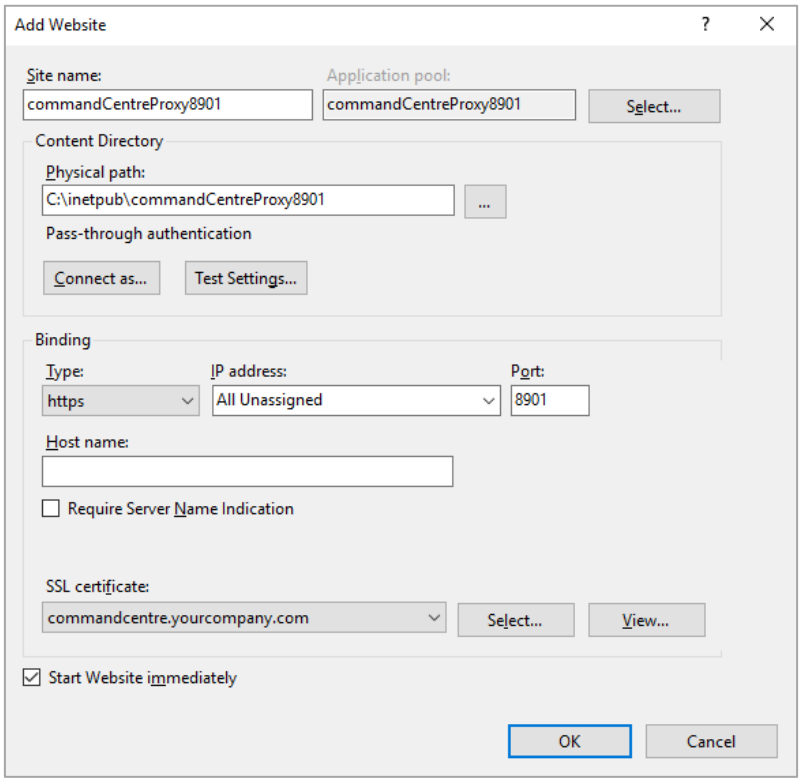
5. Open Internet Information Services (IIS) Manager, right-click **Sites**, then click **Add Website…**.



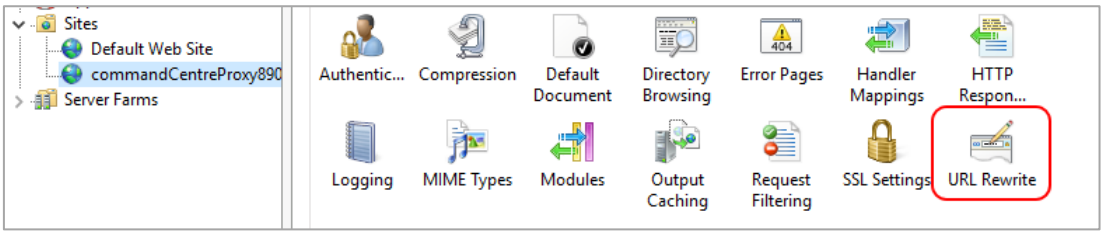
6. Enter the following information:

   - Site name: A name of your choice
   - Physical path: A directory of your choice. **This must reference a new, empty directory**
   - Binding Type: **https**
   - Port: **8901**
   - SSL Certificate: The certificate you imported in Step 1 of this procedure

Copyright © Gallagher Group Limited

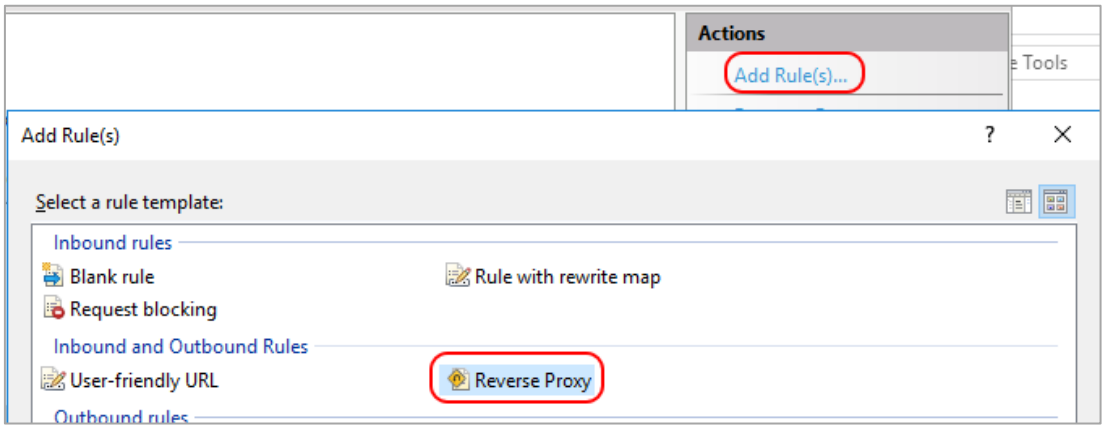


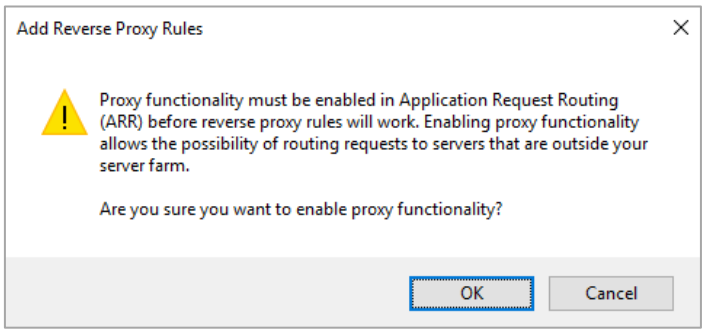
7. Select the site, and double-click **URL Rewrite**



8. From the **Actions** toolbar on the far right, select **Add Rule(s)…**, then select **Reverse Proxy.** When prompted, confirm that you want to enable proxy functionality

Copyright © Gallagher Group Limited

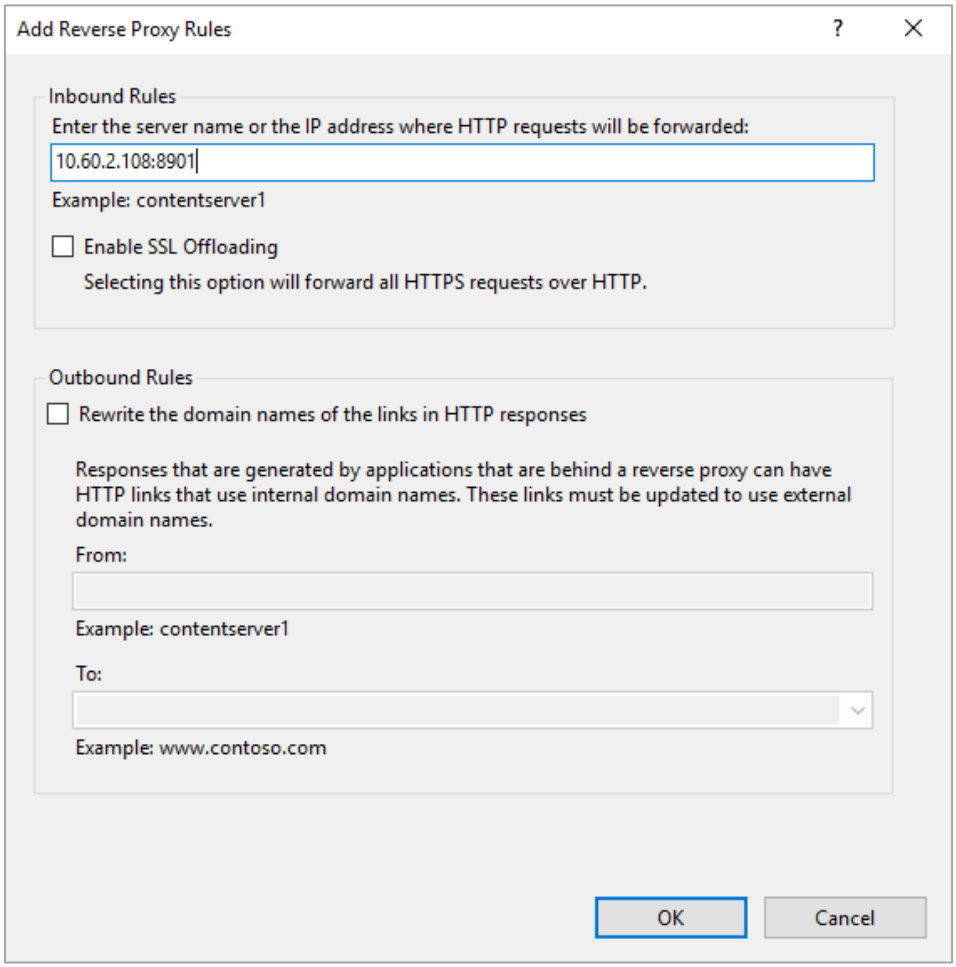




Copyright © Gallagher Group Limited

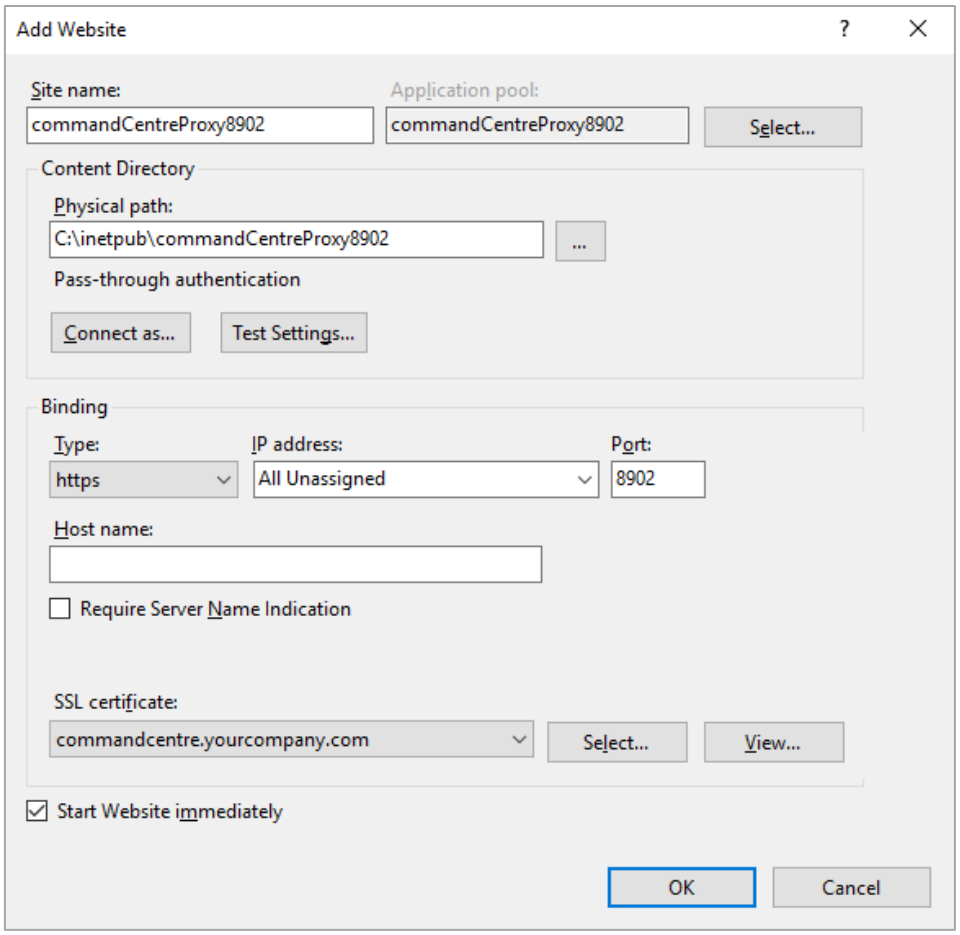
9. Enter the hostname or IP address of the internal Command Centre server, as well as the port number.

10. Make sure the **Enable SSL Offloading** and **Rewrite the domain names of the links in HTTP responses** checkboxes are **not** ticked.



Copyright © Gallagher Group Limited

11. Repeat steps 5 through 9 to add a second site on port 8902.



12. Ensure that the Windows Firewall (or any other firewalls) are allowing the proxy to listen on ports 8901 and 8902

13. You should now be able to enrol your mobile devices against the IP or DNS name of the proxy server, and log in.

Copyright © Gallagher Group Limited