Configuring Nginx 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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 Nginx 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 Nginx, 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 *(already enabled in Nginx by default.)*
5. If required, configure your proxy software to trust the new SSL certificate provided by Command Centre *(Nginx will already trust the backend server 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 *(Requires the proxy_set_header Host $host:$server_port; directive in nginx.)*
    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 Linux server with Nginx installed that you wish to use as the Reverse Proxy.
   Tested against nginx/1.10.3 on Ubuntu 16.04 Xenial

2. An SSL certificate to install on both the Nginx 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 two separate files. The certificate should be in a PEM formatted file (usually with extension **.cer** or **.pem**) and the private key should be in a PEM formatted file (usually with extension **.key**, **.pem** or no extension.)
   If you have a single .pfx or .p12 file, you can extract the certificate and private key as follows:

```
openssl pkcs12 -in filename.pfx -nocerts -nodes -out commandcentre-server.key

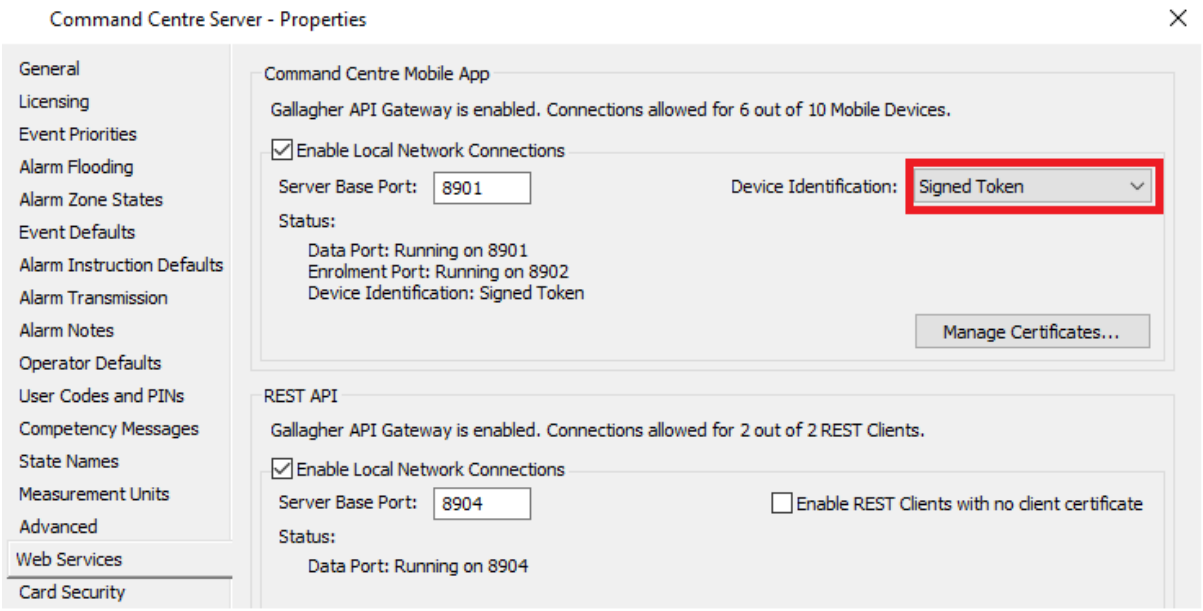
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out commandcentre-server.cer
```

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 Nginx 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. Copy the certificate and key files to:

```
/usr/local/nginx/conf/commandcentre-server.cer
/usr/local/nginx/conf/commandcentre-server.key
```

2. Set permissions on the key files so only root can read them (assuming that Nginx is running as root. If not alter these for the correct account)

```
sudo chown root:root /usr/local/nginx/conf/commandcentre-server.cer
sudo chown root:root /usr/local/nginx/conf/commandcentre-server.key
sudo chmod 600 /usr/local/nginx/conf/commandcentre-server.key
sudo chmod 600 /usr/local/nginx/conf/commandcentre-server.cer
```

3. Create a new file **/etc/nginx/sites-enabled/commandcentre-proxy.conf** with the following contents, replacing **your.server.dns.name** and **commandcentre-ip-or-dns-name** with the appropriate values

```
server {
        listen 8901 ssl http2 default_server;
        listen [::]:8901 ssl http2 default_server;
        server_name your.server.dns.name;

        ssl_certificate /usr/local/nginx/conf/commandcentre-server.cer;
        ssl_certificate_key /usr/local/nginx/conf/commandcentre-server.key;
        ssl_session_cache shared:SSL:10m;

        location / {
                proxy_pass https://commandcentre-ip-or-dns-name:8901;
                proxy_set_header Host $host:$server_port;
        }
}

server {
        listen 8902 ssl http2 default_server;
        listen [::]:8902 ssl http2 default_server;
        server_name your.server.dns.name;

        ssl_certificate /usr/local/nginx/conf/commandcentre-server.cer;
        ssl_certificate_key /usr/local/nginx/conf/commandcentre-server.key;
        ssl_session_cache shared:SSL:10m;

        location / {
                proxy_pass https://commandcentre-ip-or-dns-name:8902;
                proxy_set_header Host $host:$server_port;
        }
}
```

4. Restart Nginx

Copyright © Gallagher Group Limited