How to change my 4PSA DNS Manager HTTP server SSL certificate

This article describes how to change the digital certificate used by your 4PSA DNS Manager 3 (or later version) HTTP server.

Requirements

Before you start, make sure that the following requirements are met:

- You have a 4PSA DNS Manager version higher than 3.0.0 (e.g. 4.0.0)
- You have access and basic knowledge for using a SSH client (e.g. `Putty`)

Changing the Server's SSL certificate

To change the digital certificate used by your HTTP server, you have to create a signing request, send the request to your CA authority and then install the new certificate on your server:

STEP 1: Log in to your 4PSA DNS Manager server using your favorite SSH console (e.g. `Putty`).

STEP 2: Create the signing request for the certificate by executing the command:

```
openssl req -new -key /usr/local/dnsmanager/admin/conf/httpd.pem -out certrequest.csr
```

STEP 3: Send the `certrequest.csr` file to the CA authority of your choice (there are many vendors like GeoTrust, RapidSSL, Verisign, etc.).

STEP 4: After you receive the certificate, copy it on the server (in this example, the certificate will be temporarily stored in `/root/newcert.pem`).

STEP 5: Open the `/usr/local/dnsmanager/admin/conf/httpd.pem` file with your favorite text editor (e.g. NotePad++, jEdit) and remove the lines starting with:

-----BEGIN CERTIFICATE-----

and ending with:

-----END CERTIFICATE-----

STEP 6: Copy the new certificate by executing the command:

```
cat /root/newcert.pem >> /usr/local/dnsmanager/admin/conf/httpd.pem
```

STEP 7: Restart 4PSA DNS Manager HTTP server using:

```
/etc/init.d/dnsmanager restart
```

Related articles

- How to install a LetsEncrypt SSL certificate in VoipNow
- How to avoid the SSL Poodle attack
- How to change the SSL certificate in VoipNow
- Where can I find the VoipNow certificates
- How to change my 4PSA DNS Manager HTTP server SSL certificate