TRUSTED CERTIFICATE

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

Trusted Certificate

Certificate TLS SSL Certificate Custom SSL Certificate

1. How to Use my Own Trusted Certificate in WebADM

During installation, WebADM generates its own certificate authority certificate and server SSL certificates. Yet, you can use your own SSL certificates instead of the pre-generated ones. Using a trusted certificate may be required when you use the RCDevs OpenID IDP, and to avoid user browser warnings when accessing the WebApps.

Just create the SSL certificate and key files in `/opt/webadm/pki/custom.crt` and `/opt/webadm/pki/custom.key`. WebADM will continue using its own CA certificate for issuing and validating user certificates (for PKI-based logins) and SOAPd services but will use your trusted certificate for the SSL on the HTTPd.

The certificate and key files must be in PEM format. If an intermediate certificate chain is required, then just concatenate your certificate file with the chained certificates in the same file.

Please set the file permission of `custom.key` to `400` and `custom.crt` to `444` because it must be readable by WebADM.

```
[root@rcvm8 ~]# chmod 400 /opt/webadm/pki/custom.key
[root@rcvm8 ~]# chmod 444 /opt/webadm/pki/custom.crt
[root@rcvm8 ~]# ls -lha /opt/webadm/pki/
total 20K
drwxr-xr-x.  4 root root  136 Oct 11 11:11 .
drwxr-xr-x. 12 root root  245 Oct  8 15:23 ..
-rw-r--r--.  1 root root    0 Oct  8 16:56 .master
drwx------.  2 root root   48 Oct  8 16:56 ca
-r--r--r--.  1 root root 1.1K Oct 11 11:11 custom.crt
-r--------.  1 root root 1.7K Oct 11 11:11 custom.key
drwxr-xr-x.  2 root root   54 Oct  8 16:56 trusted
-rw-r--r--.  1 root root 1.1K Oct  8 16:56 webadm.crt
-rw-r--r--.  1 root root  936 Oct  8 16:56 webadm.csr
-rw-------.  1 root root 1.7K Oct  8 16:56 webadm.key
```

After the creation of the two custom certificate files, please restart webadm with:

```
[root@webadm ~]# /opt/webadm/bin/webadm restart
```

2. How to Use my Own Trusted Certificate in WebADM Publishing Proxy

The process is the same for WebADM Publishing Proxy (waproxy). Place the trusted SSL certificate and key files in `/opt/waproxy/conf/custom.crt` and `/opt/waproxy/conf/custom.key`.

3. How to use Let's Encrypt certificate with WebADM

Once webadm is installed and running, you can install certbot (you need EPEL repository on Centos)

```
[root@webadm ~]# yum install certbot
```

The port 80 should be reachable to the web and used by WebADM, then you can request a new certificate. Here the server name is *webadm.test.com*, and the webroot is `/opt/webadm/lib/htdocs/htroot/`:

```
[root@webadm ~]# certbot certonly --webroot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator webroot, Installer None
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org
Please enter in your domain name(s) (comma and/or space separated)  (Enter 'c'
to cancel): webadm.test.com
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for webadm.test.com
Input the webroot for webadm.test.com: (Enter 'c' to cancel): /opt/webadm/lib/htdocs/htroot/
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/webadm.test.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/webadm.test.com/privkey.pem
   Your cert will expire on 2020-05-10. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

Now you can install certificates, don't forget to replace *webadm.test.com* with your server name:

```
[root@webadm ~]# ln -s /etc/letsencrypt/live/webadm.test.com/fullchain.pem
/opt/webadm/pki/custom.crt
[root@webadm ~]# ln -s /etc/letsencrypt/live/webadm.test.com/privkey.pem /opt/webadm/pki/custom.key
[root@webadm ~]# /opt/webadm/bin/webadm restart
```

You can automate the certificate renew with crontab (webadm restart not included):

```
[root@webadm ~]# crontab -e
0 0,12 * * * root python -c 'import random; import time; time.sleep(random.random() * 3600)' && certbot renew
```