Day-to-day Administration: How do I replace the user portal self-signed certificate?

How do I replace the user portal self-signed certificate?

NOTE: This article only applies to versions of Bright prior to 7.0. For Bright 7.0 onward, please refer to the article titled "How can I set up a reverse proxy for the user portal from 7.1 onward?"

For a portal that is accessible via the internet, some administrators may regard it as more secure to ask users to trust the self-signed certificate rather than external certificate authorities. The external certifcate authority security model has some issues inherent in its design, as the DigiNotar compromise (http://www.bbc.co.uk/news/technology-14789763) showed.

Alternatively the administrator can replace the self-signed certificate with one obtained by a standard CA, if that is preferred. This is simply a standard Linux administration task, and can be done as follows:

You will need to edit the ssl.conf file in

```
/etc/httpd/conf.d
```

and change the following directives:

```
SSLCertificateFile /cm/local/apps/cmd/etc/cert.pem
SSLCertificateKeyFile /cm/local/apps/cmd/etc/cert.key
```

Replace the key and pem files with the ones you obtained after submitting a signing request to your CA. The files must be stored in a path outside the Apache's root directory.

You will also need to obtain the intermediate certificate from your CA and add the following directive to ssl.conf:

```
SSLCertificateChainFile /etc/ssl/certs/intermediatecert.crt
```

Then restart Apache2:

```
service httpd restart
```

If the administrator would like to use port 443 instead of the default 8081, then the reverse-proxy procedure in
http://kb.brightcomputing.com/faq/index.php?action=artikel&id=291
can be followed.

Unique solution ID: #1151

Day-to-day Administration: How do I replace the user portal self-signed certificate?

Author: Frank Furter
Last update: 2017-08-30 19:50