Blancco LUN (UNIX) Require valid certificate for HTTPS

Created Date	Updated Date	Affects version	Fix Version
18 Feb 2020			

Description

By default Blancco LUN Eraser does not check Blancco Management Console's certificate validity when connecting with HTTPS. If additional security is needed then certificate verification can be enabled.

When certificate validity is checked then Blancco Management Console hostname must match that in certificate and certificate's signer must be trusted. If either of those conditions are not met you get following error code. In this case the Blancco Management Console is in address 192.168.1.1.

```
Could not initiate secure connection to 192.168.1.1

Verify that your operating systems security certificates are up to date.

Refer to manual or support.blancco.com for setting custom certificate location.
```

Step-by-step guide

Certificate check can be toggled in LUN Eraser configuration file with option **VerifyMCCert.** Value 1 enables the verification and value 0 disables it (default).

Enable certificate verification

```
VerifyMCCert = "1"
```

In some cases certificate's signer is not trusted. This can happen for example if the environment running Blancco LUN Eraser is not updated or the Blancco Management Console certificate is self signed. In this case you need to add the certificate signer to a list of trusted signers. This can be done by either placing the certificate file to one of the default locations **/etc/ssl/certs** and **/etc/pki/tls/certs/ca-bundle.crt** or to a custom location.

Custom certificate location can be dedfined with option **MCCertPath**. In following example certificates are searched also from path /tmp/mc_certificate.

```
MCCertPath = "/tmp/mc_certificate"
```