Does Blancco LUN (UNIX) require a valid certificate when using HTTPS

Created Date	Updated Date	Affects version	Fix Version
18 Feb 2020			

Description

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

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

The verification of the certificate can be enabled in the LUN Eraser configuration file using the option "**VerifyMCCert**"**.** Changing the value to 1 enables the verification and 0 disables it (default).

Enable certificate verification

```
VerifyMCCert = "1"
```

In some cases, the 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.

The custom certificate location can be defined using the "**MCCertPath"** option within the configuration file. In the following example, the certificates will also be checked using the path /tmp/mc_certificate.

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