Security Certificates in Gen6 Devices

Technical Bulletin (TB240912A)

ISSUE

KMC Conquest Gen6 Ethernet/IP-capable devices (such as the BAC-5051**AE** router and BAC-5901**A**CE general purpose controller**)** use self-signed certificates for security when accessing their served web pages. Current web browsers will display a warning message when attempting to access a KMC Gen6 device's served web pages if there is no security certificate present. Device web pages will be slower than usual to open due to security. Monitor the progress activity indicator on the browser tab.

SOLUTIONS

To access a Gen6 "-E" device's served web pages without the warning pop-up message from the browser, choose one of the following methods.

Proceed by Initial Log In

Note: The following steps use Google Chrome as an example. Follow equivalent steps in other browsers.

1. Enter the IP address in the browser. A message stating that the connection is not private will appear. The browser will also show "Not Secure" in the URL field until a signed certificate is installed on the PC and in the device.
2. Click **Advanced** or similar to proceed.
3. Click P**roceed to 192.168.1.251 (unsafe)** or the configured IP address of the device.
4. In the Log In dialog box, type the user name and password. The web served pages will be accessible with no browser warning from now on until one of the following occurs:
    - The browser cache is cleared.
    - The security cetificate is updated.
    - The firmware is updated.
    - The IP address of the device is changed from what is in the certificate.

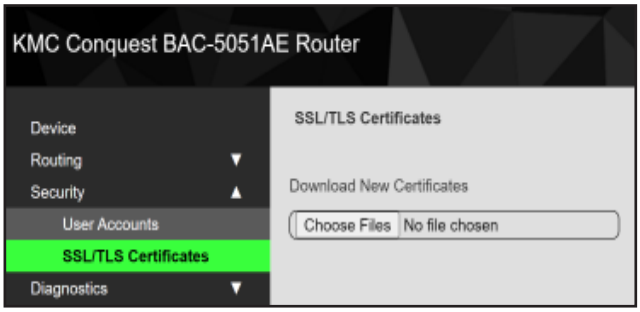
Follow steps 1-4 during each initial log in after performing one of the above procedures.

Proceed by Downloading a Customer's Certificate

The customer's certificate can be downloaded to the device via the SSL/TLS Certificates web option on the device's served web pages by doing the following.

1. Log in to the device's served web pages as in steps 1-4 above.
2. In the navigation column on the left side of the served web pages' Home screen, click **Security**.

3. From the drop-down menu, click **SSL/TLS Certificates**.



Note: Certificate and key files must meet the following criteria.

- No chained certificates
- No encrypted keys
- RSA length must be 1,024 bits or less.
- Certificate total file size must be 4,096 bytes or less.
- Key total file size must be 4,096 bytes or less.

Note: Contact **KMC Technical Support** if you have questions regarding certificate generation.

4. In the Download New Certificates box, click **Choose Files**.
5. Browse to the location of the certificate file and click **Open** to select it.
6. In the Certificate found... dialog box, click **OK**.
7. In the Download New Certificates dialog box, click **Choose Files**.
8. Browse to the location of the key file and click **Open** to select it.
9. In the Commit Download? dialog box, click **Commit**.
10. In the Change Requires a Restart dialog box, click **OK**.

SUPPORT

Additional resources for installation, configuration, application, operation, programming, upgrading, and more are available on the web at **www.kmccontrols.com**. To see all available files, log-in to the KMC Partners site.