Qumulex Insights

HTTPS ENCRYPTION

HTTPS Enables QxControl to Provide a Secure Browser-Based Experience

Qumulex understands the importance of security and delivers QxControl as secure browser-based experience. QxControl leverages HTTPS (Hypertext Transfer Protocol Secure) encryption, which is a protocol used by web browsers to secure the communication between a user's browser and a website's server.

Simply put, HTTPS adds a layer of encryption to ensure the confidentiality and integrity of the data exchanged when using a browser interface. This process allows QxControl to be secure both when connected to the cloud, and also protects you in offline mode. Our Web based solution contacts the gateway allowing you to log into QxControl securely on your local network when the internet connection has been interrupted.

Certificates & Authentication

HTTPS involves the use of digital certificates issued by trusted Certificate Authorities (CAs). These certificates validate the identity of the website's server, ensuring that users are connecting to the intended, legitimate site and not a malicious one attempting to impersonate it.

This helps defend against problems like man-in-the-middle attacks where an attacker intercepts and manipulates the communication between the user and the server, because HTTPS encryption makes it significantly harder for attackers to eavesdrop on or modify the data. Or data interception, where attackers may attempt to capture sensitive information.

Qumulex Has Your Certificate Updates Covered

SSL/TLS security certificates are crucial for encrypting data transmitted between users and the QxControl platform. Regular updates ensure that the latest security protocols and algorithms are in place, strengthening the overall security posture and protecting your sensitive information.

Qumulex provides all necessary certificate updates as a part of your QxControl subscription. This makes QxControl both secure, AND worry free, as you will never need to address the certificate updates yourself!

HTTPS ENCRYPTION

How does HTTPS work?

As we have discussed, HTTPS encryption is a protocol used by web browsers to secure the communication between a user's browser and a website's server. So, how does this work?

Initiating a Connection:

When a user enters a website's URL in the browser's address bar and hits Enter, the browser initiates a request to the server hosting the website.The server responds by sending its public key and a digital certificate to the browser.

Digital Certificates:

The digital certificate is issued by a trusted Certificate Authority (CA). It contains the server's public key and information about the website.The certificate is signed by the CA, validating the authenticity of the server's public key.

Verifying the Certificate:

The browser checks the digital certificate to ensure it is valid and has been signed by a trusted Certificate Authority.If the certificate is valid, the browser proceeds with the connection. If not, the browser may display a warning to the user.

Generating a Session Key:

The browser generates a symmetric session key. This key will be used for encrypting and decrypting the data exchanged between the browser and the server during the current session.

Key Exchange using Public Key Encryption:

The browser encrypts the session key with the server's public key obtained from the digital certificate. This encrypted session key is sent back to the server.

Server Decrypts the Session Key:

The server, using its private key, decrypts the session key sent by the browser. Now both the browser and the server have the shared session key.

Secure Data Transfer:

With the shared session key, the browser and server can now encrypt and decrypt data using symmetric encryption algorithms. All data transferred between the browser and the server, including user inputs, login credentials, and other sensitive information, is encrypted using the session key.

Continuous Communication:

Throughout the secure session, the browser and server continue to use the shared session key for encrypting and decrypting data.

Session Termination:

When the user closes the browser or navigates away from the secure site, the session key is discarded. This ensures that subsequent sessions will use a new session key.

In summary, HTTPS encryption uses a combination of asymmetric (public-key) and symmetric (session key) encryption to secure the communication between a web browser and a server. It provides confidentiality, integrity, and authentication, ensuring that data remains private and secure during transit.

QxControl Provides Value

QxControl is a cloud-based solution that is able to keep your security updated in real-time. When new security enhancements are available they can be pushed out to customers immediately. And in just the same fashion, Qumulex also monitors your certificate status and automatically updates your certificates prior to expiration.

This keeps your data fully secure at all times, and saves your organization time and money, allowing your resources to focus on other tasks.

Additional Resources

Knowledge Base

User Manual

QXI-02: Offline Functionality