Introduction to SSL

- How SSL work
- Authentication and trust: SSL
- The strongest SSL-encryption: 128-bit

Secure Sockets Layer (SSL): How It Works

What Happens When a Browser Encounters SSL?

1. A browser attempts to connect to CLIQ Web Manager secured with SSL.
2. The **browser** requests that the web server identify itself.
3. The **server** sends the browser a copy of its SSL Certificate.
4. The **browser** checks whether it trusts the SSL Certificate. If so, it sends a message to the CLIQ Remote server.
5. The **server** sends back a digitally signed acknowledgement to start an SSL encrypted session.
6. **Encrypted data is shared between the browser and the CLIQ Remote server**.

Encryption Protects Data During Transmission

Web servers and web browsers rely on the Secure Sockets Layer (SSL) protocol to help users protect their data during transfer by create a uniquely **encrypted** channel for private communications over the public Internet. Each SSL Certificate consists of a **key pair as well as verified identification information**. When a web browser (or client) points to a secured website, the server shares the public key with the client to establish an encryption method and a unique session key. CLIQ Web Manager confirms that it recognizes and trusts the issuer of the SSL Certificate. This process is known as the "SSL handshake" and it begins a secure session that protects message privacy and message integrity.

Strong encryption, at 128 bits, can calculate 288 times as many combinations as 40-bit encryption. **That's over a trillion times stronger.** At current computing speeds, a hacker with the time, tools, and motivation to attack using brute force would require a trillion years to break into a session protected by an SGC-enabled certificate. To enable strong encryption for the most site visitors, choose an SSL Certificate that enables 128-bit minimum encryption for 99.9 percent of website visitors.

Credentials Establish Identity Online

Credentials for establishing identity are common: a driver's license, a passport, a company badge. SSL Certificates are credentials for the online world, uniquely issued to a specific domain and web server and authenticated by the SSL Certificate provider. When a browser connects to a server, the server sends the identification information to the browser.

To view a websites' credentials:

- Click the closed padlock in a browser window
- Click “show certificate information”