

Introduktion till SSL

- Hur SSL fungerar
- Autentisering och förtroende: SSL
- Starkaste SSL-krypteringen: 128-bit



Secure Sockets Layer (SSL): Så här fungerar det

Vad händer när CLIQ Web Manager använder SSL?

1. En administratör ansluter till CLIQ Web Manager som skyddas med SSL.
2. **Webbläsaren** kräver identifikation från webbservern.
3. En kopia av SSL-certifikatet skickas från **servern** till webbläsaren.
4. I **webbläsaren** kontrolleras om SSL-certifikatet är tillförlitligt.
Om det godkänns skickas ett meddelande till CLIQ Remote servern.
5. **Servern** returnerar en digitalt signerad bekräftelse på att en krypterad SSL-session kan startas.
6. **Krypterade data delas mellan webbläsaren och CLIQ Remote servern.**

Kryptering skyddar data under överföring

Webbserverar och webbläsare använder Secure Sockets Layer (SSL)-protokollet för att hjälpa användare att skydda data vid överföring. En unik, **krypterad** kanal för privat kommunikation skapas på det annars offentliga Internet. Varje SSL-certifikat består av ett **nyckelpar samt verifierade identifikationsdata**. När en CLIQ Remote (eller klient) pekar på en säker hemsida, delar servern den offentliga nyckeln med klienten i syfte att skapa en krypteringsmetod och en unik sessionsnyckel. CLIQ Web Manager bekräftar att den erkänner och litar på utfärdaren av SSL-certifikatet. Den här processen kallas "SSL-handskakning" och den inleder en säker session som upprätthåller meddelandese sekretess och meddelandeintegritet.

Certifikat visar identitet på internet

Det är vanligt med referenser för att visa sin identitet: ett körkort, pass eller företags-ID. SSL-certifikat är referenser som används på Internet, unikt utfärdade för en specifik domän och webbserver och som autentiseras av SSL-certifikatets leverantör. När en webbläsare ansluter till en server skickar servern identifieringsinformation till webbläsaren.

Ett sätt att veta att en webbplats använder SSL är att titta på webbadressen. Webbadresser som kräver en SSL-anslutning börjar med `https://` i stället för `http://`

Så här visar du en webbplats certifikat:

- Klicka på det stängda hänglåset i ett webbläsarfönster
- Klicka på "visa certifikatinformation"