Step-by-Step ACTAtek device HTTPS Access and Verification Guide

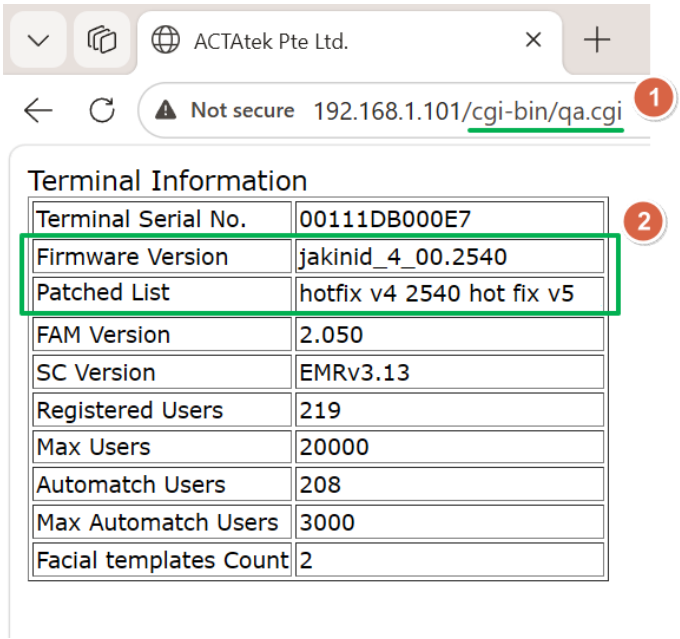
To switch from a standard HTTP connection to a secure HTTPS one,follow these steps to verify your device status and establish a secure HTTPS connection.

Phase 1: Firmware and Patch Verification

Before proceeding to secure access, verify that your ACTAtek terminal is up to date.

1. **Access the QA Page:** Navigate to the device's QA page using the following example URL:
   http://192.168.1.101/cgi-bin/qa.cgi
   Note: Replace the IP address with the actual IP of your device.
2. **Verify Updates:** Check the **Terminal Information** table to confirm that the device is running the latest firmware version and hotfix patch file, ensuring it is ready for secure communication and equipped with the latest feature sets and cybersecurity fixes.

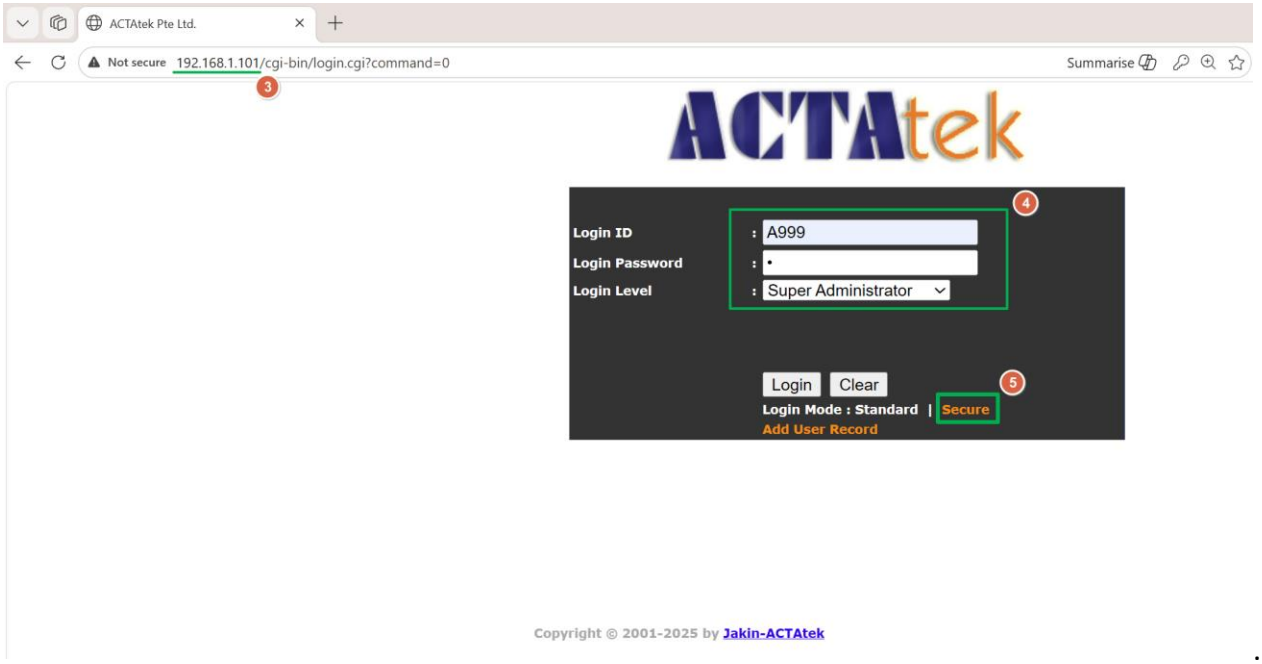
   - **Firmware Version:** Confirm it shows jakinid_4_00.2540.
   - **Patched List:** Ensure hotfix v4 2540 hot fix v5 is listed.



Terminal Serial No.	00111DB000E7
Firmware Version	jakinid_4_00.2540
Patched List	hotfix v4 2540 hot fix v5
FAM Version	2.050
SC Version	EMRv3.13
Registered Users	219
Max Users	20000
Automatch Users	208
Max Automatch Users	3000
Facial templates Count	2

Phase 2: Switching to Secure Mode (HTTPS)

3. **Initiate Secure Login:** Go to the ACTAtek device login webpage . At the bottom of the login interface, click the **Secure** link

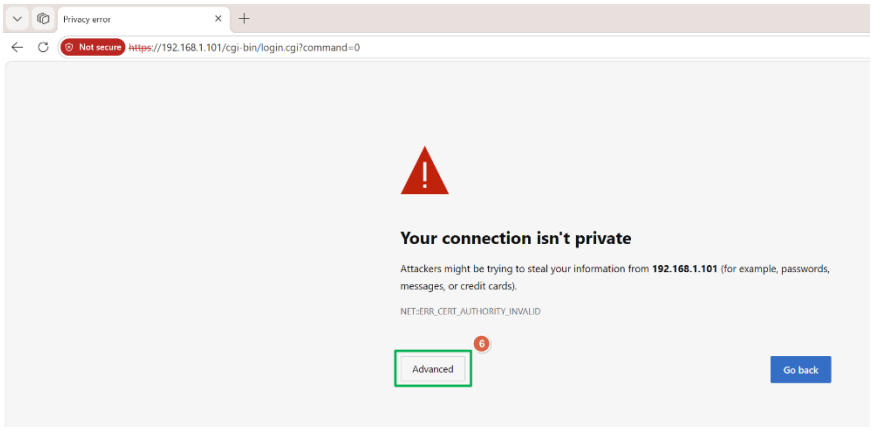


This actions the switch from http:// to https://.

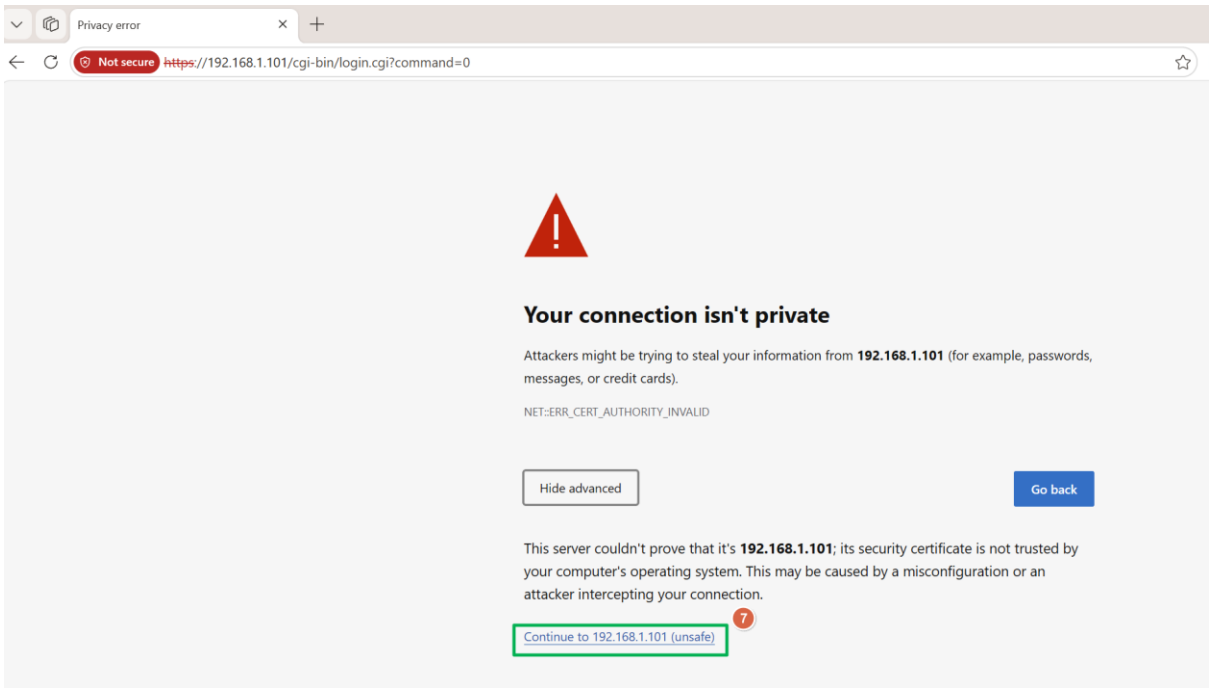
Phase 3: Bypassing the Browser Security Warning

Since the device uses a **self-signed certificate** for internal IP encryption, you can accept the connection:

4. **Enter Advanced Menu:** When the "Your connection isn't private" page appears, click the **Advanced** button .



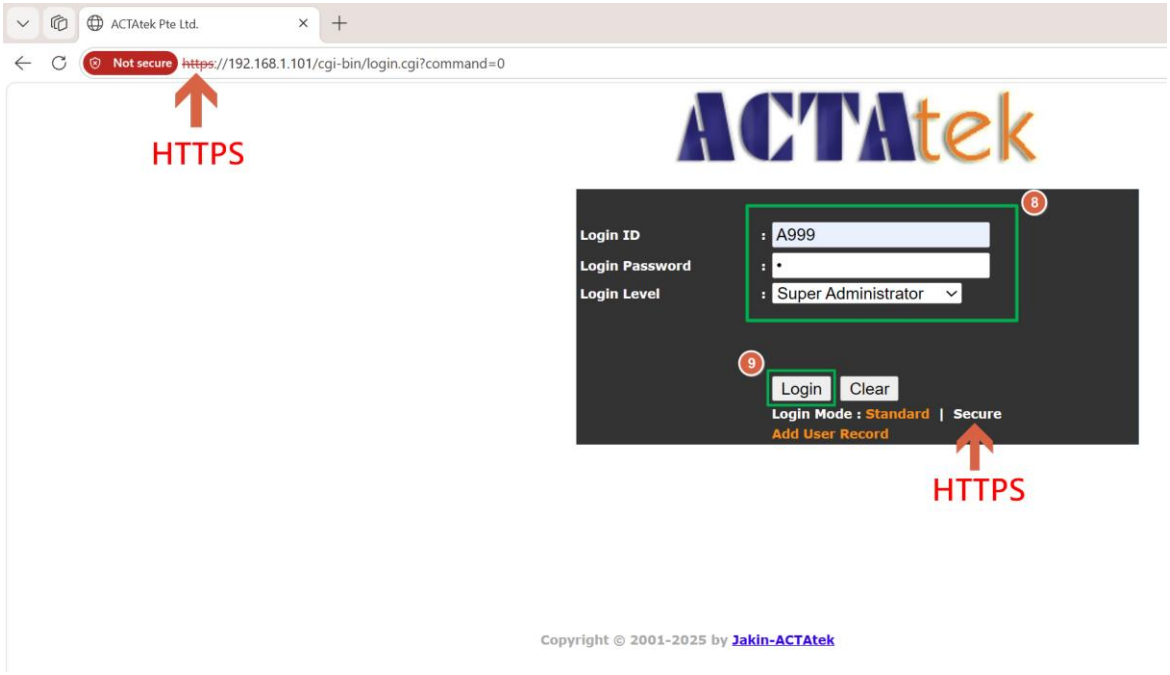
5. **Confirm Exception:** Click the link at the bottom: **Continue to 192.168.1.101 (unsafe)**
    - *Note: Your connection is now encrypted via TLS 1.3.*

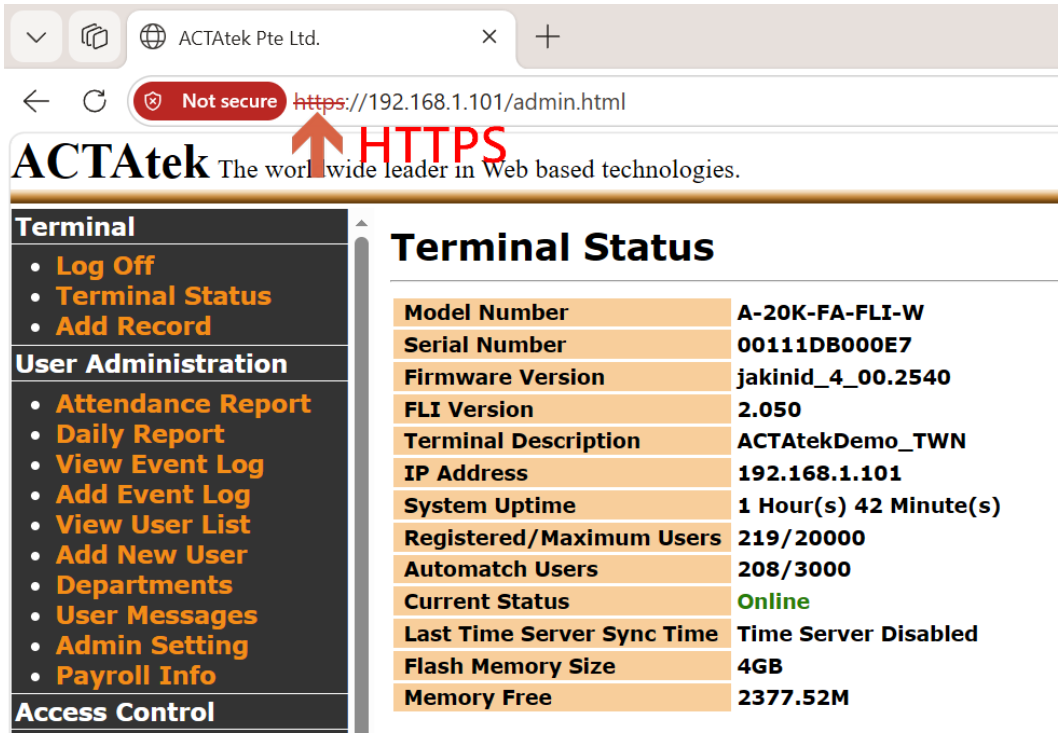


Phase 4: Secure Authentication

6. **Verify SSL Status:** Confirm the address bar now displays **https://** .
7. **Enter Credentials:** Fill in your **Login ID**, **Password**, and **Login Level** (e.g., Super Administrator)

   Execute Login: Click the **Login** button to enter the secure admin dashboard.





Understanding the Self-Signed Certificate of the device

It is common to see a **"Not Secure"** or red strike-through on the HTTPS text in your browser. Here is why this happens and why the device is still secure:

- **Encryption vs. Trust:** The **TLS 1.3 encryption** is fully active, meaning the data traveling between your computer and the ACTAtek device is scrambled and safe from hackers.

- **The "Not Secure" Label:** Browsers like Chrome or Edge show this label simply because they don't recognize the "signer" of the certificate.

  Since the device uses an internal private IP address (e.g., 192.168.1.X), it cannot be "verified" by global authorities who only verify public domain names (like google.com).

- **No Extra Cost:** You do **not** need to purchase or install a third-party SSL certificate.

  The preloaded self-signed certificate is sufficient for secure professional use, including integration with Azure cloud services or IIS servers.

Summary of Device Status

Feature	Status
Encryption Protocol	TLS 1.3 (Current Industry Standard)
Certificate Type	Self-Signed (Pre-installed)
Connection Security	Encrypted & Secure
Action Required	None (Simply bypass the browser warning)