Securing ACTAtek Terminal Access over HTTPS for Third-Party Integration

Document Purpose

This document provides guidance for resellers, IT teams, and integration partners who need to publish ACTAtek terminals securely over HTTPS for third-party systems such as payroll platforms, time attendance systems, or middleware applications.

It explains why certificate warnings may appear when accessing ACTAtek terminals internally, why installing a public SSL certificate directly on each terminal is not normally recommended, and how to configure a secure firewall, reverse proxy, VPN, or DDNS-based access method.

1. Typical Integration Requirement

A third-party system may request secure HTTPS access to ACTAtek terminals, for example using TCP port 443.

Example internal terminal URL: https://10.1.30.11:8093

Example external public URL: https://actatek01.customer-domain.com

or DDNS example:https://actatek-hko.no-ip.org/cgi-bin/login.cgi?command=0

The goal is to allow the third-party system to connect securely from outside the customer network while keeping ACTAtek terminals protected inside the private LAN.

2. Understanding HTTPS, TLS, and Certificate Warnings

ACTAtek terminals support HTTPS/TLS communication, for example TLS 1.3 on the latest firmware version.

However, when accessing the terminal internally using a private IP address, such as:

https://10.1.30.11:8093

the browser may display a certificate warning.

This is expected in many deployments.

The warning does not necessarily mean that TLS encryption is not working. It means the certificate presented by the terminal is not trusted by the browser or firewall as a public CA-issued certificate.

This usually happens because:

- The terminal is using **an internal/private IP address**, such as 10.x.x.x, 172.16.x.x, or 192.168.x.x.
- Public Certificate Authorities normally validate public domain names, not private LAN IP addresses.
- The device certificate is not issued by a public trusted Certificate Authority.
- The certificate identity does not match a public DNS name.

Therefore, HTTPS may be encrypted, but the certificate is not publicly trusted.

3. Can a CSR Be Generated Directly from the ACTAtek Terminal?

For standard ACTAtek terminal deployments, there is no normal user-facing function to generate a CSR directly from the terminal and install a public third-party SSL certificate in the same way as a web server such as IIS, Apache, or Nginx.

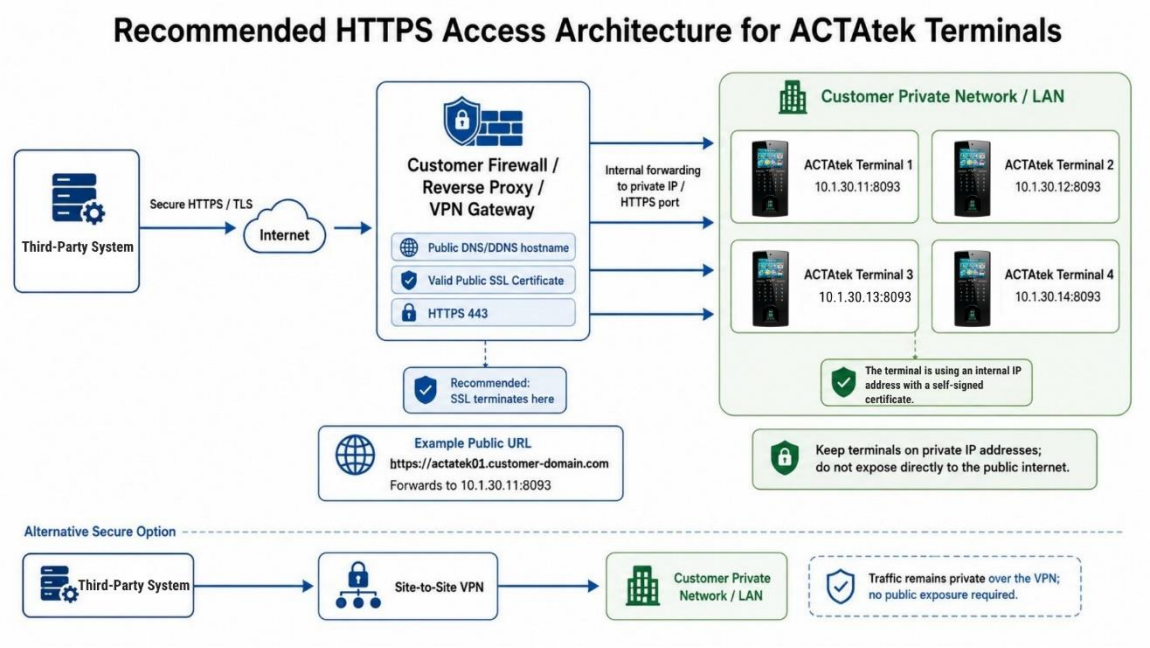
For this reason, installing a public SSL certificate directly on each ACTAtek terminal is not the recommended approach.

Instead, the recommended approach is to install the public SSL certificate on one of the following network components:

- Firewall
- Reverse proxy
- VPN gateway
- Load balancer
- Secure web gateway
- AMS IIS server, if the third-party integration is with AMS rather than directly with terminals

4. Recommended Architecture

Recommended Option: SSL Termination on Firewall or Reverse Proxy



In this design, the firewall or reverse proxy presents a valid public SSL certificate to the third-party system.

Example: https://actatek01.customer-domain.com

The firewall or reverse proxy then forwards the traffic internally to the ACTAtek terminal:

https://10.1.30.11:8093

Typical traffic flow:

Third-party system → HTTPS 443 → Public DNS/DDNS hostname → Firewall/Reverse Proxy → Internal ACTAtek terminal IP/HTTPS port

Example:

Emplive → HTTPS 443 → actatek01.customer-domain.com → Firewall → 10.1.30.11:8093

In this design:

- The third-party system sees a trusted public SSL certificate.
- The public SSL certificate is installed on the firewall or reverse proxy.
- The ACTAtek terminal remains on a private/internal IP address.
- The internal connection remains protected inside the customer's trusted network.

5. Example Using Public DDNS URL

Example demo URL:

https://actatek-hko.no-ip.org/cgi-bin/login.cgi?command=0

This URL can be understood as follows:

- https:// means the external access is using HTTPS.
- actatek-hko.no-ip.org is the public DNS/DDNS hostname pointing to the firewall/router public IP address.
- No port is shown in the URL, so the external connection is using standard HTTPS port 443.
- /cgi-bin/login.cgi?command=0 is the ACTAtek terminal web login path.
- The firewall/router forwards the external HTTPS request to the internal ACTAtek terminal private IP address.

Example mapping:

External URL: https://actatek01.customer-domain.com

Internal terminal:https://10.1.30.11:8093

Firewall NAT/reverse proxy rule:

External TCP 443 → Internal 10.1.30.11 TCP 8093

---

6. Configuration Steps

Step 1: Configure a Fixed Internal IP Address on the Terminal

Each ACTAtek terminal should use a static private IP address.

Example: 10.1.30.11

Confirm the following settings on each terminal:

- IP address
- Subnet mask
- Default gateway
- DNS server
- Correct HTTPS port, for example 8093
- The latest Firmware version supports the TLS 1.3 version

Step 2: Confirm Internal HTTPS Access

Before publishing the terminal externally, confirm that the terminal can be accessed internally.

Example:

https://10.1.30.11:8093

A browser certificate warning may appear. This is expected if the terminal is using an internal/self-signed certificate.This confirms that HTTPS is available, but the certificate is not publicly trusted.

Step 3: Create a Public DNS or DDNS Hostname

Create a public hostname that points to the customer firewall/router public IP address.

Examples:

actatek01.customer-domain.com

or

actatek01.no-ip.org

Using a public hostname is required because public SSL certificates are normally issued for domain names, not internal private IP addresses.

Step 4: Install the Public SSL Certificate on the Firewall or Reverse Proxy

Install the public SSL certificate on the firewall, reverse proxy, VPN gateway, or equivalent network device.

The certificate should match the public hostname.

Example:

Certificate for:actatek01.customer-domain.com

Public access URL:

https://actatek01.customer-domain.com

The ACTAtek terminal itself does not need to host the public certificate in this design.

Step 5: Configure Firewall NAT or Reverse Proxy Rule

Create a firewall or reverse proxy rule to forward the external HTTPS request to the internal terminal.

Example external access:

https://actatek01.customer-domain.com:443

Internal terminal destination:

10.1.30.11:8093

Example rule:

- Source: Approved third-party public IP addresses only
- Destination: Customer public IP / hostname
- External port: TCP 443
- Internal destination: 10.1.30.11
- Internal port: TCP 8093, or the terminal's configured HTTPS port
- Action: Allow

For security, do not allow access from the entire internet unless absolutely required.

Step 6: Publishing Multiple Terminals

If multiple ACTAtek terminals need to be accessed externally, use separate DNS hostnames or reverse proxy rules.

Example:

https://actatek01.customer-domain.com → 10.1.30.11:8093
https://actatek02.customer-domain.com → 10.1.30.12:8093
https://actatek03.customer-domain.com → 10.1.30.13:8093
https://actatek04.customer-domain.com → 10.1.30.14:8093

This is cleaner than using different public port numbers, especially when the third-party system requires standard HTTPS port 443.

7. Important Certificate Clarification

If the firewall is configured for simple HTTPS pass-through or SSL bridging, the third-party system or firewall may still see the ACTAtek terminal's internal certificate.

In that case, the certificate warning may remain.

To avoid this, the preferred design is SSL termination at the firewall or reverse proxy.

This means:

Third-party system → Trusted public SSL certificate → Firewall/Reverse Proxy

Then internally:

Firewall/Reverse Proxy → ACTAtek terminal

If the firewall requires the backend device to present a public CA-trusted certificate, the same issue may occur. The firewall policy should then be adjusted to either:

- Terminate SSL at the firewall/reverse proxy; or
- Trust the internal ACTAtek terminal certificate for the backend connection; or
- Use a VPN-based design instead.

The correct option depends on the firewall model, customer security policy, and integration requirements.

8. Alternative Secure Option: Site-to-Site VPN

A site-to-site VPN is also a secure option.

In this design:

- ACTAtek terminals remain on private IP addresses.
- The terminals are not published directly to the public internet.
- The third-party system connects through an encrypted VPN tunnel.
- Access can be restricted to only the required terminal IP addresses and ports.

Typical traffic flow:

Third-party system → VPN tunnel → Customer network → ACTAtek terminal

This is often more secure than publishing each terminal externally.

9. Security Best Practices

For production deployments, follow these best practices:

- Do not expose ACTAtek terminals directly to the public internet without firewall protection.
- Use a firewall, reverse proxy, VPN gateway, or AMS server as the secure access point.
- Use a valid public SSL certificate on the public-facing endpoint.
- Use public DNS or DDNS hostnames rather than private IP addresses.
- Restrict access to the third-party system's approved public IP addresses.
- Publish only the required ports.
- Use static IP addresses for all ACTAtek terminals.
- Use strong administrator passwords on all terminals.
- Keep terminal firmware updated.
- Enable firewall logging for audit and troubleshooting.
- Use VPN where possible for long-term production integrations.
- Avoid broad inbound rules such as "Any source to terminal".

---

10. Troubleshooting Checklist

Issue: Browser shows certificate warning internally

Expected when accessing the terminal by private IP address.

Example:https://10.1.30.11:8093

Cause:

The terminal certificate is not issued by a public trusted CA or does not match a public DNS hostname.

Recommended action:

Use SSL termination at firewall/reverse proxy or access through VPN.

Issue: Firewall refuses HTTPS publishing because backend certificate is not trusted

Cause:

The firewall may be using SSL bridging or backend certificate validation.

Recommended action:

Configure the firewall to terminate SSL on the public side, or configure it to trust the internal terminal certificate according to the customer's security policy.

Issue: Third-party system requires port 443 only

Recommended action:

Use public DNS hostname and map external TCP 443 to the terminal's internal HTTPS port.

Example:

External TCP 443 → Internal 10.1.30.11 TCP 8093

Issue: Multiple terminals need to be published

Recommended action: Use separate public hostnames or reverse proxy rules.

Example:

actatek01.customer-domain.com
actatek02.customer-domain.com
actatek03.customer-domain.com

Each hostname can forward to a different internal terminal.

11. Summary

ACTAtek terminals can support HTTPS/TLS communication, but the certificate presented by the terminal may not be publicly trusted when accessed by internal private IP address.

For this reason, installing a public SSL certificate directly on each ACTAtek terminal is not normally recommended.

The recommended production design is to use one of the following:

- SSL termination on firewall or reverse proxy
- Site-to-site VPN
- Secure AMS server integration over HTTPS
- Public DNS/DDNS hostname with firewall-controlled access

For third-party integrations such as TA system, the preferred setup is:

Third-party system → HTTPS 443 → Public DNS/DDNS hostname → Firewall/Reverse Proxy with valid SSL certificate → Internal ACTAtek terminal

This allows secure external HTTPS access while keeping ACTAtek terminals protected inside the customer's private network.