

# Securing CAREWare Internet-Facing Servers

|                                        |                                                                                                                                                        |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                         | Explain the CAREWare security features used to help protect internet-facing installations.                                                             |
| <b>Who should do this</b>              | Program administrators and IT staff responsible for CAREWare installations accessed over the internet.                                                 |
| <b>Use this guide when you need to</b> | You need an overview of TLS, certificates, internal CAREWare access, and CAREWare two-factor authentication (2FA).                                     |
| <b>Main warning</b>                    | Use a valid TLS certificate and enable 2FA for internet-facing CAREWare installations. Security configuration should be handled by qualified IT staff. |

**Important:** TLS protects communications in transit, while 2FA adds protection when a username and password are compromised. These features address different risks and should be used together when appropriate.

## Overview

CAREWare includes Transport Layer Security (TLS) and two-factor authentication security features. This document is written for program administrators who have oversight responsibility for CAREWare installations that are accessed over the internet. Its purpose is to help familiarize you with these features.

[View a diagram](#) of the CAREWare 6 architecture.

## What is TLS?

When your browser shows a lock symbol after connecting to a website using https:// in the URL, your browser and the server are using TLS. This aspect of web security is achieved by obtaining an X.509 certificate from an official Certificate Authority (CA). The CA implements measures to ensure that your organization controls the URL users connect to and that your organization is the valid website owner.

Every time a user connects to a server through TLS, the protocol ensures that the server holds a secret key that is unique to that server. TLS is now required by HIPAA for internet-facing applications and replaces the older SSL protocol, which can be compromised in certain situations.

### Is TLS just for internet browsers?

No. While internet browsers such as Chrome, Edge, Opera, and Firefox are the best-known clients that use TLS, any client and server can use the TLS protocol. You can get instructions for configuring CAREWare with TLS [here](#).

### Can TLS be used if CAREWare is not internet-facing?

Yes. You will need to register the domain name, get a certificate that includes that domain name, and make sure the server is internally available under that name.

### Since CAREWare 6 uses a browser, does the server have to be internet-facing?

No. CAREWare 6 will work on an internal network or even on a single computer.

## What is CAREWare Two-Factor Authentication (2FA)?

In addition to a username and password, CAREWare's [Two-Factor Authentication](#) (2FA) prompts for a six-digit code generated on a device that only the user controls. 2FA is a built-in feature that can be turned on at the server level by a CAREWare administrator. CAREWare 2FA is compatible with the Google Authenticator smartphone app and desktop apps such as WinAuth.

Without 2FA, someone who finds or guesses a username and password can gain access to client data available to that user. With 2FA turned on, someone who gains password information would still need access to that user's device to sign in.

## Related References

| Document                                            | Use it for                                                      |
|-----------------------------------------------------|-----------------------------------------------------------------|
| <a href="#">CAREWare 6 Application Architecture</a> | Review the CAREWare 6 component layout and communication paths. |
| <a href="#">CAREWare 6 HTTP Server Setup</a>        | Configure the CAREWare HTTP server and TLS communication.       |
| <a href="#">Two-Factor Authentication Setup</a>     | Configure Two-Factor Authentication in CAREWare.                |