Securing CAREWare 5 and 6 Internet-Facing Servers

Overview

CW5 and CW6 (alpha version) both include the Transport Level 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.

What is TLS?

When your browser shows a green lock symbol to the left after connecting to a banking application (for example) using https:// in the URL, your browser and the server are using TLS. IT staff running the bank's website will have obtained something called an X.509 Certificate from an official Certificate Authority (CA). The CA will have taken steps to ensure that the bank controls the URL that you connected to and that the bank is who it says it is.

Every time a client connects to a server via TLS, the protocol ensures that the server holds a secret key that only they should have. TLS is now required by HIPAA for internet-facing applications and replaces the older SSL protocol that can be hacked in certain situations.

Is TLS just for Internet Browsers?

No. While Internet Browsers like Chrome, Edge, Opera, and Firefox are the best known clients that use TLS, any client and server can use TLS if they use the protocol. CW5 and CW6 can both be configured to use TLS. You can get instructions for configuring CW5 here. You can get information on configuring CW6 here

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

Yes, although 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 the CW6 uses a browser, does the server have to be internet-facing?

No. CW6 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 2FA prompts for the entry of a six-digit code, which is generated on a device that only the user controls. Both CW5 and CW6 now have 2FA as 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 smart phone app and desktop apps like WinAuth.

Without 2FA, if someone finds out or guesses a username and password, he or she can gain access to client data to which that user has access. With 2FA turned on, if someone gains password information, he or she would still need to have access to that user's device to get in.