CAREWare 6 HTTP Server Setup

Overview

The CAREWare 6 (CW6) HTTP server installs as a Windows Service. By default it listens and responds to unencrypted HTTP requests on port 8080. If you plan on opening up CAREWare to the internet, you will want to configure the CW6 HTTP server to use TLS with a X.509 Certificate obtained from an official Certificate Authority (CA). There are many CAs who offer different levels of services with varying costs. Support for choosing a CA that fits your needs is outside the scope of this document.

The rest of this document outlines each step you should take for installing and configuring the CW6 HTTP server.

Install the CW6 Business Tier

The CW6 HTTP service acts as a broker between browsers and the Business Tier, so make sure the Business Tier is up and running first. See the Business Tier Upgrade document **here** for those instructions.

Run CwHttpSetup.exe

CwHttpSetup runs a simple installer that puts the necessary files in a designated directory and starts the *CAREWare HTTP Service*. The default install directory is *C:\Program Files\CAREWare HTTP Server*. After you have run this setup program, open the Windows Services application and make sure *CAREWare HTTP Service* is on the list and has a status of *Running*.

Run CW6 from a browser on the installation computer

Open up an HTML 5-compatible browser (Chrome, Edge or FireFox) on the computer where you just installed the service. In the address bar of the browser enter *http://localhost:8080/rs/index.htm*, and the CAREWare 6 login screen should appear. If you get errors, check the HTTP Server log file in *C:\Program Files\CAREWare HTTP Server\cwhttp\logs* or the Business Tier log files. If you can't figure out the problem, contact the CAREWare Help Desk by following the instructions **here**.

TLS Setup Steps

Overview

HIPAA requires HTTP applications that communicate across the internet to encrypt their communications with TLS 1.2. The TLS protocol uses X.509 Certificates; see the Overview at the beginning of this document for more information.

Get your X.509 certificate

X.509 certificates come in a few different forms, and there are various tools provided by different companies and organizations that can convert these certificates to different file formats. The CAREWare HTTP Server uses *Apache style* certificate files where the certificate is in one file and the private key is in another, typically with .crt and .key extensions. If your certificate and private key are already in the Windows Certificate Store, you can export the certificate and the private key, which will give you the two files you need.

Configure your DNS, Router, and Server

X.509/TLS Certificates are linked to a domain name that you control. That domain name will need to be registered in the public DNS system so that it forwards TCP traffic to your router. The default port for HTTPS/TLS is 443. Your router will need to be configured to forward incoming traffic for port 443 from the IP linked to your URL to the CAREWare HTTP server. The Windows Firewall on the CAREWare HTTP Server will need to be configured to allow incoming traffic on port 443 as well.

Configure the CAREWare HTTP Server to use TLS

Open the HttpSettingsTool

The CAREWare HTTP Server comes with HttpSettingsTool.exe to help you with configuration options. If you installed the CAREWare HTTP Server in the default directory, you can find the tool in the *C:\Program Files\CAREWare HTTP Server* folder. Because the HttpSettingsTool makes changes to configuration files and restarts the HTTP Server, you will need to run it with administrator-level privileges by right clicking on it and clicking *Run as Administrator*. The HttpSettingsTool configures the CAREWare HTTP Server by making changes to the res_admin_settings.txt file located in the *cwhttp\res_admin* subfolder of your install directory. When the CAREWare HTTP Server is started, it retrieves its configuration information from res_admin_settings.txt.

Once you have opened HttpSettingsTool in administrative mode:

1. For Security Choice, select *Encrypt HTTP Traffic using TLS with x509 certificate*.
2. Either leave Port blank or enter: *443*. If Port is blank, then *443* will be used.
3. For Security type and location select *Apache style crt and key file located in file system*.
4. For Certificate File Path and Name click the ellipses and navigate to the certificate file.
5. For Key File Path and Name click the ellipses and navigate to the private key file.
6. Leave Business Tier URL set to *http://localhost:8000/getDocument*.
7. Uncheck *Write* debug info to log file.
8. Click *Save*.
9. Restart the *HTTP Service*.

Check today’s log file in the *cwhttp\logs* directory and make sure there is a log entry that reads *HTTP: communication with browsers are encrypted with TLS 1.2*.

Test the URL

Open up a browser and enter *https://yourURL/rs/index.htm* and make sure the browser reports the connection as secure.