Installation & Help Guide

SigWeb Browser SDK

Version 1.6.4
April 23, 2020

Table of Contents

Installation

Release Notes and Requirements

Version 1.6.0.2

- Added certificate checker and updater
- Added TLS 1.2 support
- Implemented additional Autokey Option (for developer use)
- Microsoft .NET Framework Version 4.7.1 or later required.

First-Time Install Steps

Follow Steps 1-4 here if you have never installed SigWeb before:

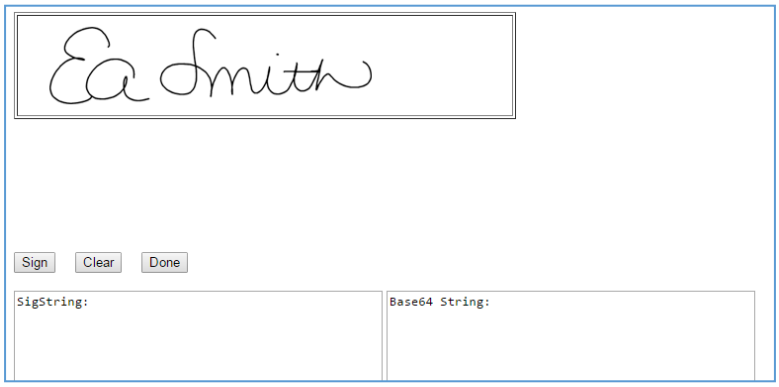
1. Download the SigWeb installer at: **www.topazsystems.com/software/sigweb.exe**.

2. Before installing, be sure to close all open browsers (i.e. Chrome, Firefox, Internet Explorer, etc).

3. Run the SigWeb installer.

   Note: Do not connect your signature pad until installation is complete.

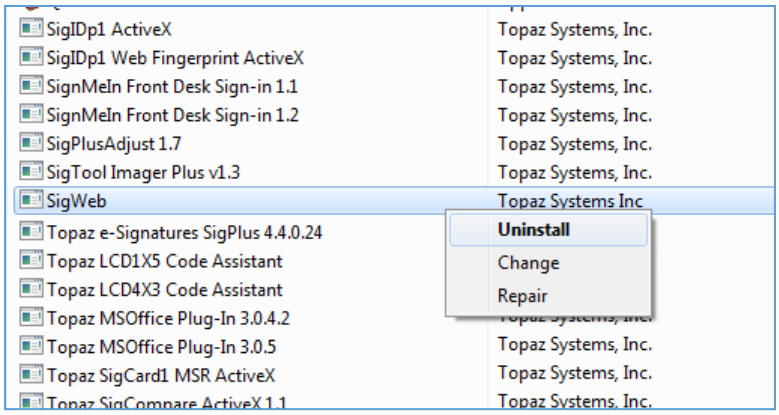
4. Once complete, test SigWeb with the SigWeb Demo at this page: **www.sigplusweb.com/sigwebtablet_demo.htm**. Click “Sign” and sign on your signature pad; your signature will appear in the signature box.



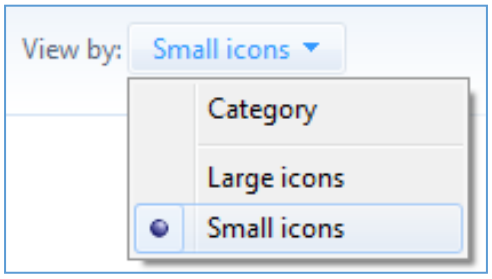
Re-Installation Steps

Follow Steps 1-2 here if SigWeb has already been installed and you are performing a re-install:

1. Under “Start” → “Control Panel” → “Programs and Features”, right-click on “SigWeb”, and choose “Uninstall”. Allow the “Uninstall” to complete.



Note: If you do not see the “Programs and Features” option under the “Control Panel”, click “View by:” in the top right of your window, and select “Small icons”.



2. Follow the steps in the first section of this guide called “**First-Time Install Steps**” in order to install SigWeb properly.

SigWeb Cert Checker Software Package

Background

SigWeb requires an SSL certificate be installed to allow communication between Topaz signature pads and a webpage within a secure context (https). If Topaz's SSL certificate is not installed on the client machine, then SigWeb will not work within secure web contexts (https). The SSL certificate also expires after a few years for security reasons. Thus, the SSL certificate must be checked and updated after a few years. Topaz developed the SigWeb Cert Checker Software Package to automate this process.

Overview

SigWeb installs the SigWeb Certificate Checker software package. The SigWeb Certificate Checker software package provides the ability to check the SigWeb certificate's status and notify users and/or update the SigWeb certificate. The SigWeb Certificate checker software package contains two applications for performing the checking, notifying, and updating: SigWebCertUpdater and SigWebCertStatusNotifier. Both applications check if the SigWeb certificate is expiring or expired and notify specified users if an updated certificate is available and the certificate is expiring or expired. SigWebCertUpdater also updates the SigWeb certificate with a new certificate if available. Each application is run automatically before the certificate expires through a task in Windows Task Scheduler. These applications can be configured by modifying the sigWebCertCheckerConfigs.xml file and other files referenced within this xml file.

Applications

There are two applications that provide the ability to check the SigWeb certificate status. Each application provides separate functionality for checking and/or updating the certificate.

SigWebCertUpdater

Description: Updates the SigWeb certificate if there is a new certificate available to install. Notifies the user if there is an update available, if there are any issues with the update, and if the update succeeded. After a successful install, the sigWebCertCheckerConfgs.xml file is updated with the new certificate data and PFXConfigs.xml data. This application requires Administrative permissions. This application is run by the "SigWeb Cert Updater Task".

Arguments:

manuallyInstall – Set as true or false.

true - The application checks if a new certificate is available for installation. If a new certificate is available, then the application prompts a user to install the new certificate.

false - The application checks if a new certificate is available and there are at least 60 days before the certificate expires. If a new certificate is available and there are at least 60 days before the certificate expires, then the application prompts a user to install the new certificate. Otherwise, no users are notified.

Default Value - true.

enableLogging – Set as true or false. This log file is located in the “C:\ProgramData\Topaz Systems\SigWeb\Logs” directory.

true - Logging will be enabled.

false - Logging will not be enabled.

Default Value - false.

SigWebCertStatusNotifier

Description: Notifies a user if the certificate is expiring or expired. Only notifies a user if a new certificate is available and there are at least 60 days before the certificate expires. This application is run by the “SigWeb Cert User Notifier Task”.

Arguments:

enableLogging – Set as true or false. This log file is located in the “C:\ProgramData\Topaz Systems\SigWeb\Logs” directory.

true - Logging will be enabled.

false - Logging will not be enabled.

Default Value - false.

Task Scheduler

There is a task for each SigWebCertChecker application. Each task is triggered on a weekday 60 days before the expiration of the SigWeb certificate. The tasks run with different permissions, for different user groups, and with different arguments. Each task runs as soon as possible for a user once a trigger date is missed. The following are the tasks and their attributes:

SigWebCertChecker Task:

Task Name: "SigWeb Cert Updater Task"

Weekday Triggered: Monday

Permissions: Highest

User Group: BUILTIN/Administrators

Arguments: "manuallyInstall=false"

SigWebCertCheckerNotifyUsers Task:

Task Name: "SigWeb Cert User Notifier Task"

Weekday Triggered: Friday

Permissions: Standard

User Group: BUILTIN/Users

Arguments: ---

Configurations

Each SigWebCertChecker application uses the sigWebCertCheckerConfigs.xml file for configuring its operations. These configurations help orchestrate the application's checking and updating process.

sigWebCertCheckerConfigs.xml:

Description: This file is the base configuration file that configures the information to use for checking the SigWeb certificate, notifying users, and retrieving the updated certificate.

Configurations:

certificate: Defines the thumbprint and subjectName to use for finding the SigWeb certificate. This information is automatically updated when a new SigWeb certificate is installed. DO NOT MODIFY.

thumbprint: The thumbprint used for finding the SigWeb certificate. If cannot find the certificate by the thumbprint, then search by the subjectName.

subjectName: The subjectName used for finding the SigWeb certificate. Each element within the subjectName must match the certificate's subjectName's elements exactly.

notification: Defines when to show notifications in the SigWebCertUpdater and SigWebCertStatusNotifier applications.

showPopupNotifications: If set to true, show notifications. If set to false, then do not show notifications.

pfx: Defines the location and update status of the PFXConfigs.xml file.

pfxConfigsURL: Address to the PFXconfigs.xml file that configures the pfx location and data.

URI Schema must be: 'file:///', 'http://', or 'https://'.

-For local or network files, use 'file:///'.

-For HTTP, use 'http://' or 'https://'

utcDateUpdated: UTC Date that is compared with the PFXConfigs.xml file to detect whether there is an update to the pfx file that needs to be installed. Determines if a new certificate is available. DO NOT MODIFY.

PFXConfigs.xml:

Description: This file is the base configuration file used for determining the location of the new certificate (PFX file), decryption information, and date this file was updated.

Configurations:

pfxURL: Link to the pfx file that is used to install the SigWeb certificate.

pfxDataURL: Link to data used for installing the SigWeb certificate

iv: IV used for decrypting information

utcDateUpdated: UTC Date that is compared with the sigWebCertCheckerConfigs.xml file to determine whether there is an update to the PFXConfigs.xml file. Determines if a new certificate is available.

pfxConfigsURL: Link to this PFXConfigs.xml file. Used to allow the SigWebCertUpdater application to change the location of the PFXConfigs.xml within the sigWebCertCheckerConfigs.xml file. If not set, then the sigWebCertCheckerConfigs.xml file will not be modified.

Support Help

For troubleshooting help or assistance, view the SigWeb Software FAQs on the Topaz Software FAQ page at **www.topazsystems.com/softwarefaq-endusers.html**, or contact Topaz Dev Software Support at **devsupport@topazsystems.com**.

Silent installers are available upon request. Visit the Topaz SigWeb webpage at **www.topazsystems.com/sigweb.html** for details.

Topaz recommends that you keep your SigWeb SSL certificate up-to-date. To do so, download and run the SigWeb Certificate Update Program from **www.topazsystems.com/sigweb.html**.