

Description: Instructions for setting up the CFSWorX server to receive mobile device updates including location, and for configuring the app on the mobile devices.

General Requirements:

- Familiarity with CFSWorX (see *CFSWorX – Getting Started*).
- Familiarity with Workbench and ICONICS security
- Familiarity with IIS and security certificates.

Introduction

One of the key features of CFSWorX is the ability to send notifications to workers based upon their location. To make this feature possible, each field worker must download the MobileHMI app on their mobile device and enable the CFSWorX Worker Access feature. This will enable each mobile device to send data to the server. You must also set up the server to receive these messages. The following steps will guide you through this process.

Internet Information Services (IIS) Setup

Follow the steps in the link below to set up IIS to use SSL.

<https://docs.microsoft.com/en-us/iis/manage/configuring-security/configuring-ssl-in-iis-manager>

Security Provider Setup

1. Open **Workbench**.
2. Expand **Security**.
3. Edit **Global Settings**.
4. Go to the **Web Login** tab.
5. Make sure **Enabled** is checked under **General Settings**.
6. In the **OIDC Provider / OAuth Authorization Server Settings** section, set **Signing credentials type** to **From the windows certificate store**.
7. For **Certificate Identifier**, choose a certificate that will be used to sign the tokens provided by security.
8. Apply the changes.
9. Make sure you have at least one user created in the **Users** folder. We will use a user to log into the MobileHMI application.

FrameWorX Server Setup

Change Platform Services setting

1. In **Workbench**, go to **Tools > Platform Services Configuration**.
2. On the **Basic** tab, set **Public origin** to match the address configured in IIS. For example:
`https://servername.website.com`
3. Select **OK**.

Change FrameWorX Server Location

1. In **Workbench**, go to **Tools > FrameWorX Server Location**.
2. Go to the **Mobile Clients** tab.
3. In the Transport section, select **HTTPS**.
4. Select **Save**.

MobileHMI Application Setup

Universal Windows Platform (UWP) App

1. Launch the **MobileHMI** application for Windows.
2. Add a new server connection.
3. Choose **HTTPS** for the first dropdown.
4. In the text box to the left of the Connect button, enter the server name. This should match the address configured in the public origin of the Platform Services Configuration and within IIS.
5. Enable **I have credentials for this server**.
6. Fill in the **user name** and **password** of an ICONICS security user.
7. Select **Connect**.
8. After the client is connected to the server, go to **Settings**.
9. Under **Worker Access**, select **Enable**.
10. Log in again with your ICONICS security user.
11. Select **Grant Access**.
12. Observe that the **Worker Access** button now says "disable" instead of "enable".

The MobileHMI app should now be sending its health and location information to CFSWorX.

Android or iOS App

1. Launch the **MobileHMI** app.
2. Select your server to connect to, but do not connect.

3. Select the **settings** gear icon in the upper left corner.
4. In the **Worker Access** section, select **User**.
5. Select **Login**.
6. Sign in with your ICONICS username and password.
7. Select **Grant access**.
8. Select **Back** to return to settings.
9. Enable the toggle in the **Worker Access** section.
10. Select **Back** to return to the connection screen.

The MobileHMI app should now be sending its health and location information to CFSWorX.