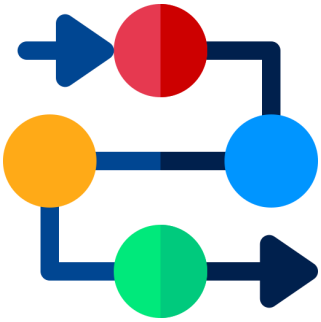
QUICK START GUIDE
Web GUI for Soft Codecs

Overview

The AMX Web GUI is license free and behaves like a traditional touch panel complete with BUTTON, CHANNEL, and LEVEL events received from the GUI virtual device (ex. 41001). The GUI is 2-way and can be viewed from multiple devices at the same time—all observing the same state feedback. One AMX controller can support multiple GUI instances to provide flexibility in control architecture. Options range from a single instance on an AMX controller to multiple-rooms using unique GUI designs or the same design when assigned to a single controller, or even multiple GUI designs for a single space (i.e. user console and tech page console).



1 Firmware

Minimum controller firmware is 1.6.201—hotfix firmware is located @ help.harmanpro.com

2 Netlinx Programming

Use traditional BUTTON, CHANNEL, and LEVEL events from the GUI virtual device number.

3 Configure the GUI

The AMX Web GUI is not designed within the TPDesign application. A JSON configuration file is modified to enable needed widgets to create control objects. The JSON configuration also dictates color, text, and icon for a control object. Sample layouts and a full UI guide are included in the demo workspace for developers to explore.

4 Files

Beyond the module jar files, additional files are required to be transferred to the controller as demonstrated in the example workspace. Be sure to transfer:

- UI configuration JSON
- UI resource .zip

5 Access Control

This module implements a stand-alone webserver and leverages existing user credentials set within the AMX controller. The module requires user authentication prior to accessing the UI and offers two methods intended to be one-time configuration items completed during the commissioning process — 1) user credentials (default and preferred method) or 2) preauthorized access list (must be enabled via Netlinx code). Upon successful authentication, the AMX controller will transfer a cookie to the endpoint. NOTE—endpoint appliances behave differently and may not allow the use of persistent cookies. Installers should test their configuration under multiple scenarios to include power loss to ensure end users are not confronted with a user login dialog. In cases where endpoint hardware does not allow persistent cookies or clears cookies daily or after reboot, the preauthorized access list will need to be implemented to ensure users are not confronted with an authentication request. The preauthorized list can be uploaded via the webserver configuration web page, built programmatically, or via FTP transfer (requires module REINIT).

6 SSL Certificate

Some soft codec applications will require a HTTPS url and a certificate signed by a certificate authority. The certificate will be issued with an expiration date and will require management to ensure customers are not disrupted following an expired certificate. End customer IT policy will dictate certificate specifics and this item cannot be purchased through Harman.