Breaking Change: 4.10 Content-Security-Policy Support

Video

Feeds from video cameras, such as Axis and Milestone, may make use of WebSockets to transfer video. WebSocket connections are governed by the connect-src directive of the Content-Security-Policy header, and the secure default value only allows connections to your local station, not to remote cameras. Here are some options for setting connect-src, in order of decreasing security. Note that 'self' refers to your local station and usually must be present. Contact your local IT personnel to verify the optimal settings.

- 'self' workbench https://myMileStoneServer:8084 wss://%hostname%:%port% wss://%hostname%:%port% wss://myCameraServer:myCameraPort - allow local BajaScript connections, HTTPS requests to a Milestone server, and individually specify each camera you need to connect to. You may need "ws:" instead of "wss:" if your camera is not configured with HTTPS. Note that the use of HTTPS for video feeds is strongly recommended.
- 'self' workbench ws://%hostname%:%port% wss://%hostname%:%port% wss://*.myCameraDomain.com - allow local BajaScript connections, and secure connections to any camera server on a known domain
- 'self' workbench wss: - allow a WebSocket to any server, as long as it is secure
- 'self' workbench ws: wss: - allow a WebSocket anywhere, secure, or not
- * - allow any connection, anywhere. This will raise a warning on Security Dashboard.

In addition, some cameras may make use of <video> tags or similar, which are governed by the media-src directive. For Axis cameras, media-src may be set to 'self' blob: which allows the camera to send individual video frames down in blob format.
Other camera implementations may require the use of iframes, as configured in the next section.

Embedded WebBrowsers in Px

When adding a WebBrowser widget to a Px page, when viewed in the browser, the widget will be implemented as an iframe. Iframes are governed by the frame-src directive of Content-Security-Policy, and the secure default behavior only allows pages served by your local station to be embedded in iframes. Here are some options for setting frame-src, in order of decreasing security. Note that 'self' refers to your local station and usually must be present. Contact your local IT personnel to verify the optimal settings.

- 'self' workbench https://myembeddedwebsite.com - specify the individual domains you wish to embed.
- 'self' workbench https: - allow an iframe to anywhere, as long as it is secure
- * - allow any iframe, anywhere. This will raise a warning on Security Dashboard.