

BULLETIN #: AN201229AS

Title: HTML5 Web Client – Best Practices

Date: December 29th, 2020

Description:

This best practice only applies to users who do not want to use the Salient hosted web client and instead want to rely on the internally hosted HTML5 web client included with CompleteView 5.3 Recording Server and newer.

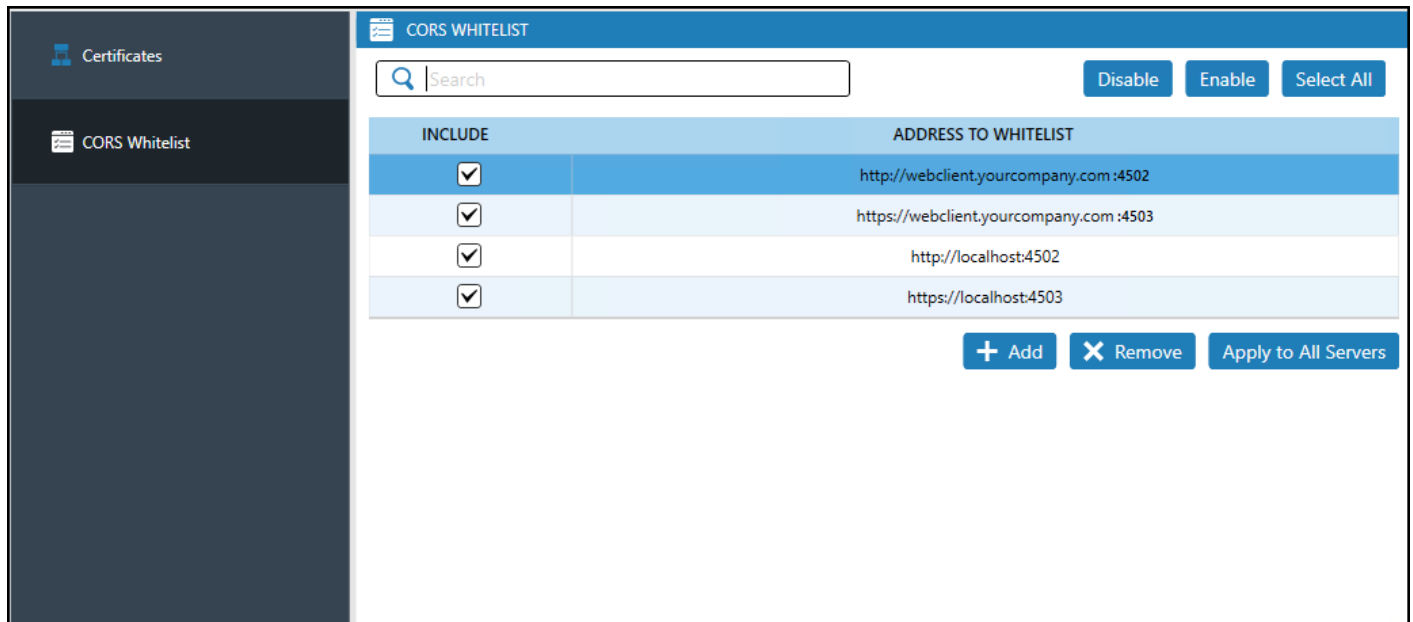
Best Practice Recommendation:

Background: As a part of the 5.3.0 release, **the HTML5 web client is available on any Recording Server that is installed with / running v5.3.0.** However, administrators and users will quickly run into Cross-Origin Resource Sharing (CORS) troubles if they acquire the web client from multiple Recording Servers. Doing so would require adding every Recording Server in the deployment to the CORS whitelist, which can create issues for IT and/or support.

In order to have a more secure, scalable, and manageable experience, **we strongly recommend that the Operating System of one Recording Server is configured** to designate it as the Recording Server from which the web client should be accessed. This can be co-located with the Management Server, but is not necessary. The name or address of the Windows server must be resolvable on the network on which the CompleteView deployment resides. For servers on a domain, the Fully Qualified Domain Name (FQDN) may be configured on the machine and used. Otherwise, a static IP address will suffice. Once configured, **we recommend that the friendly hostname or IP address is entered into the CORS Whitelist setting** – and applied to all Recording Servers (this configuration allows users to pull from any Recording Server from that friendly hostname/IP address without any CORS challenges).

For example, edit the designated web client hosting Recording Server's OS Computer Name to "webclient.yourcompany.com", save the changes, and restart the machine. Alternately, verify and record the static IP address.

Add the new FQDN or IP address to the CORS Whitelist on the Management Server. It is highly recommended adding both the non-secured (http – port 4502 by default) and secured (https – port 4503 by default) port entries to the list. In the example, both "http://webclient.yourcompany.com:4502", and "https://webclient.yourcompany.com:4503" are added. Select Apply to All Servers when completed.



| INCLUDE | ADDRESS TO WHITELIST |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | http://webclient.yourcompany.com:4502 |
| <input checked="" type="checkbox"/> | https://webclient.yourcompany.com:4503 |
| <input checked="" type="checkbox"/> | http://localhost:4502 |
| <input checked="" type="checkbox"/> | https://localhost:4503 |

Finally, direct personnel who request the web client to the newly added address:

http://[address]:port or https://[address]:port

After successfully connecting to the address above, the user will enter in the Management Server's information and valid credentials at the prompts.

The Salient-hosted web client may be accessed from the sites below:

Secured HTML5 download available here: <https://webclient.salientsys.com/>

No SSL certificate and/or don't want to use TLS, can access the web client here: <http://webclient.salientsys.com/>