Datacap Navigator application returns a pop up message, "To scan, download and run the DynamsoftServiceSetup.msi program. You need to do this only one time," when attempting to launch Datacap Navigator application in a browser.

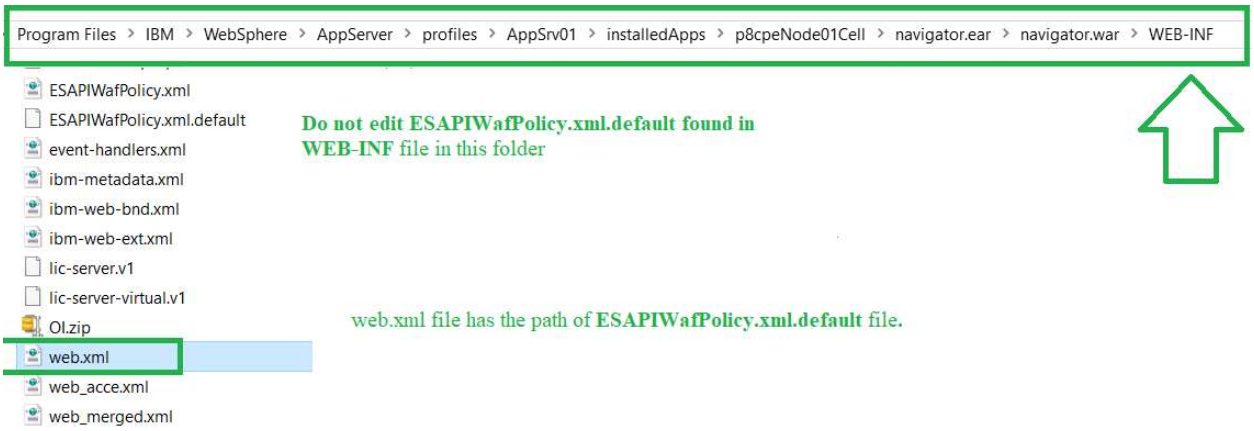
Resolution: Users need to configure the Content Security Policy header in Datacap Navigator application.

Steps

1. Stop the WAS server.

2. Navigate to \Program Files\IBM\WebSphere\AppServer\profiles\>AppSrv01\installedApps\<**FindYourNode**>\navigator.ear\navigator.war\WEB-INF folder.

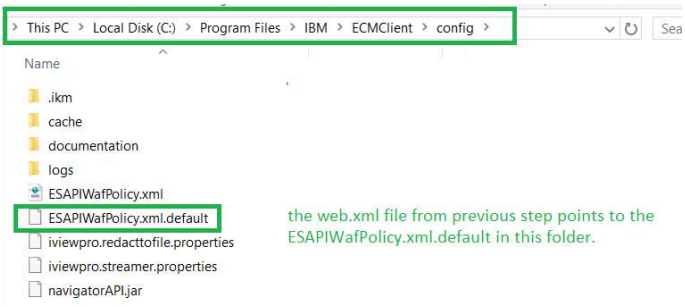
3. In WEB-INF folder, make a copy of WEB.xml file to a temporary location.



4. Edit Web.xml file and locate the path of **ESAPIWafPolicy.xml.default** file in <param-value> tag.

```
<filter>
<filter-name>ESAPIWebApplicationFirewallFilter</filter-name>
<filter-class>com.ibm.ecm.filters.ESAPIWafFilter</filter-class>
    <init-param>
        <param-name>configuration</param-name>
    <param-value> c:\\Program Files\\IBM\\ECMClient\\config\\ESAPIWafPolicy.xml.default</param-value>
    </init-param>
    <init-param>
        <param-name>filterUploads</param-name>
        <param-value>false</param-value>
    </init-param>
</filter>
```

5. Navigate to path of ESAPIWafPolicy.xml.default file listed in the web.xml file.
Example, in previous step, the path listed in web.xml file was:\\Program Files\\IBM\\ECMClient\\config folder.
(** Do not edit the **ESAPIWafPolicy.xml.default** file found in WEB-INF folder.)



6. Make a copy of **ESAPIWafPolicy.xml.default** file found in previous step, (example, \Config folder) to a temp folder.
7. Edit **ESAPIWafPolicy.xml.default** file and delete all its contents.

8. Manually add the following contents to **ESAPIWafPolicy.xml.default** file found in the **\config folder** as seen in the example.

```
<?xml version="1.0" encoding="UTF-8"?>
<policy>
	<aliases/>
	<settings>
		<mode>block</mode>
		<error-handling>
			<default-redirect-page>/error.jsp</default-redirect-page>
			<block-status>500</block-status>
		</error-handling>
	</settings>

	<virtual-patches>
	<!-- Uncomment and update to add return host validation when enableOAuthProxy is set to true in web.xml
		<virtual-patch id="oauth2-return" path=".*/jaxrs/oauth2/.*"
			variable="request.parameters.state"
			pattern="^(localhost|localhost:http)$"
			message="Detected invalid OAuth2 return host.">
		</virtual-patch>
		-->
	</virtual-patches>

	<outbound-rules>
		<add-header name="Cache-Control" value="no-cache, no-store"
path=".*/|.*\.jsp|.*/jaxrs/.*|.*/api/.*"/>

<add-header name="Content-Security-Policy"
value="default-src 'self' blob: https:;
connect-src 'self' blob: https http://127.0.0.1:* wss://127.0.0.1:*;
font-src 'self' data: blob: https:;
img-src 'self' data: blob: https:;
script-src 'self' 'unsafe-inline' 'unsafe-eval' https:;
worker-src 'self' blob: https:;
style-src 'self' 'unsafe-inline' https:;
frame-ancestors 'self'"
path="/.*"/>

		<!-- <add-header name="Content-Security-Policy"
value="default-src 'self' blob: https:; font-src 'self' data: blob: https:; img-src
'self' data: blob: https:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https:; worker-src 'self' blob: https:; style-src 'self'
'unsafe-inline' https:; frame-ancestors 'self'"
path="/.*"/> -->
		<add-header name="Referrer-Policy" value="same-origin" path="/.*"/>
```

```
                <add-header name="Strict-Transport-Security" value="max-age=7776000; includeSubdomains"
path="/.*"/>
                <add-header name="X-Content-Type-Options" value="nosniff" path="/.*"/>
                <add-header name="X-Frame-Options" value="sameorigin" path="/.*"/>
                <add-header name="X-Permitted-Cross-Domain-Policies" value="none" path="/.*"/>
                <add-header name="X-XSS-Protection" value="1; mode=block" path="/.*"/>
        </outbound-rules>

        <url-rules>
                <!-- Deny HTTP methods other than GET, POST, PUT, DELETE, HEAD, and OPTIONS, and only
allow POST for logon requests -->
                <restrict-method deny="^((?!GET|POST|PUT|DELETE|HEAD|OPTIONS).)*$"/>
                <restrict-method deny="^(GET|PUT|DELETE|HEAD|OPTIONS)$" path=".*/jaxrs(/|/.+/)logon$"/>
        </url-rules>
</policy>
```

9. Restart WAS server.

Troubleshooting to confirm Content Security Policy was correctly configured.

Collect browser console logs and confirm if in the logs you see the following entry:

13:16:23.859 Content Security Policy: The page's settings blocked the loading of a resource at http://127.0.0.1:18622/f/VersionInfo?ts=1603192583826 ("default-src").
dynamsoft.webtwain.initiate.js:13:34379

This means the setup to enable Content Security Policy for Datacap Navigator for windows server was not properly executed. Please follow the directions again to configure it.