

How to embed Imagicle web pages into 3rd party apps

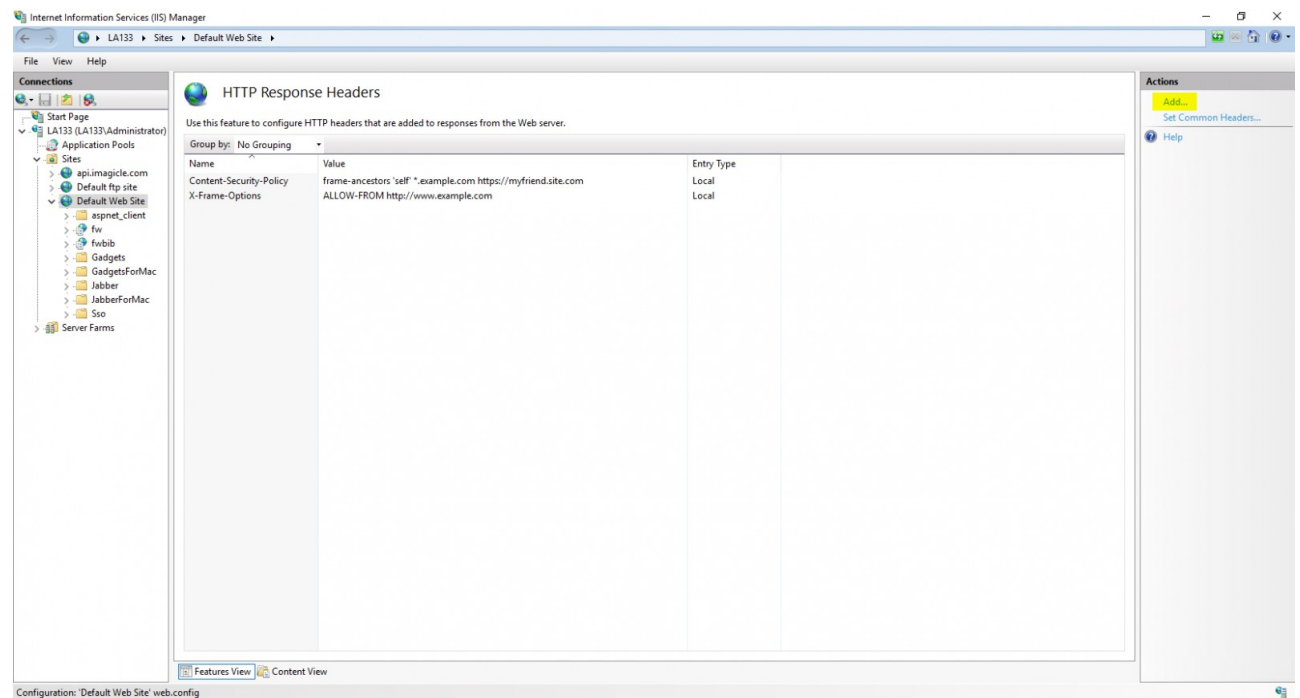
When leveraging Imagicle gadgets in Cisco Finesse or the Imagicle App for MS-teams, the UCX Suite can verify and allow the originating domain of each http/https request coming into own web server (IIS-based). This is accomplished by amending the default http/https Response Header, to make sure that source applications are recognized as safe.

It is required for accessing Imagicle web pages embedded in any third party application leveraging iframe wrapping.

Solution

The external web domains or URLs to be trusted by Imagicle should be whitelisted in Imagicle web server by adding a Content-Security-Policy header from Windows IIS. Here is the procedure:

- Access to Imagicle UCX Suite via RDP session
- Launch Windows IIS Manager
- Select Sites → Default Web Site
- Double-click on HTTP Response Headers icon
- On top-right panel, click Add



Couple of example:

1. If you need to embed the Imagicle [App for MS-Teams](#), then you need to add the following string: `Content-Security-Policy: frame-ancestors teams.microsoft.com *.teams.microsoft.com *.skype.com`
2. If you need to embed Imagicle [Gadgets for Cisco Finesse](#), you need to add the following string, replacing "company.com" with your own actual domain: `Content-Security-Policy: frame-ancestors *.company.com myuccx.company.com:8445`

Imagicle UCX Cloud Suite customers

Please contact Imagicle Support to let them know what are the web domains or URLs to be trusted.