## imagicle<sup>•</sup>

# 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 â Default Web Site
- Double-click on HTTP Response Headers icon
- On top-right panel, click Add

iew Help				
I LA133 (LA133\Administrator)	With the set of the se			Actions Add Set Common Head
				Help
Application Pools Sites Painagick.com Default for site Default Web Site J-G appert.client 	Group by: No Grouping Name Content-Security-Policy X-Frame-Options	Value frame-ancetons 'self' * example.com https://myfriend.site.com ALLOW-FROM http://www.example.com	Entry Type Local Local	
	Entran View Michael	Mau		

#### Couple of example:

- 1. If you need to embed the Imagicle <u>App for MS-Teams</u>, then you need to add the following string: Content-Security-Policy: frame-ancestors teams.microsoft.com \*.teams.microsoft.com
- 2. If you need to embed Imagicle <u>Gadgets for Cisco Finesse</u>, 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.