

View if deploy with Terraform provider:

Security » Application Security : URLs : Allowed URLs : Allowed HTTP URLs » Allowed HTTP URL Properties

URL Properties | URL Parameters | Flows to URL | Advanced Extractions | Dynamic Flows from URL

Allowed URL Properties **Advanced**

URL	/test (Explicit)
Perform Staging	<input type="checkbox"/> Enabled
Check Flows to this URL	<input type="checkbox"/> Enabled
Clickjacking Protection	<input type="checkbox"/> Enabled
Disallow File Upload of Executables	<input checked="" type="checkbox"/> Enabled
Body is Mandatory	<input type="checkbox"/> Enabled
URL Description	

Attack Signatures | Header-Based Content Profiles | **HTML5 Cross-Domain Request Enforcement** | Methods Enforcement

Enforcement Mode: **Enforce on ASM**
Note: Since no allowed origins are configured then only requests from the application's origins will be allowed.

Allowed Origins

Protocol	Any
Origin Name	<input type="text"/> (wildcard supported, case insensitive)
Port	* All Ports
Include Sub-Domains	<input type="checkbox"/> Enabled

<input type="checkbox"/>	Protocol	Origin Name
No records to display.		

View if we deploy manually with choosing the Disabled value:

Security » Application Security : URLs : Allowed URLs : Allowed HTTP URLs » Allowed HTTP URL Properties

URL Properties | URL Parameters | Flows to URL | Advanced Extractions | Dynamic Flows from URL

Allowed URL Properties **Advanced** ▾

URL	/test (<i>Explicit</i>)
Perform Staging	<input type="checkbox"/> Enabled
Check Flows to this URL	<input type="checkbox"/> Enabled
Clickjacking Protection	<input type="checkbox"/> Enabled
Disallow File Upload of Executables	<input checked="" type="checkbox"/> Enabled
Body is Mandatory	<input type="checkbox"/> Enabled
URL Description	<input type="text"/>

Attack Signatures | Header-Based Content Profiles | **HTML5 Cross-Domain Request Enforcement** | Methods Enforcement

Enforcement Mode: ▾

Cancel | Update