

# HTTP Security

The **HTTP Security Policy** allows to set security-related HTTP headers such as HSTS, CSP and XSS protections.

Policy Type

HTTP Security Policy

HTTP Security Policy Configuration

HTTP Security Headers Configuration

HTTP Strict Transport Security

Enforce transport security when using HTTP to mitigate a range of common web vulnerabilities.

Enable HTTP Strict Transport (HSTS)

false

Include Subdomains

false

Maximum Age

0

Delta seconds user agents should cache HSTS status for.

Enable HSTS Preload Flag

false

[Goto Mozilla Dev: HTTP Strict-Transport-Security Guide](#)

[Goto Chromium: HSTS Preload Submission Guidelines](#)

Flag to verify HSTS preload status. Popular browsers contain a hard-coded (pinned) list of domains and certificates, which they always connect securely with. This mitigates a wide range of identity and MITM attacks, and is particularly useful for high-profile domains. Users must submit a request for their domain to be included in the scheme.

Content Security Policy

A mechanism to precisely define the types and sources of content that may be loaded, with violation reporting and the ability to restrict the availability and scope of many security-sensitive features.

CSP Mode

DISABLED

Content Security Policy Definition

[Goto Mozilla Dev: Content-Security-Policy \(CSP\) Guide](#)

Valid CSP definition must be provided.

Frame Options

DISABLED

[Goto Mozilla Dev: X-Frame-Options Guide](#)

Defines if, or how, a resource should be displayed in a frame, iframe or object.

XSS Protection

DISABLED

[Goto MSDN: X-XSS-Protection Guide](#)

Enable or disable XSS filtering in the UA.

Content Type Options

false

[Goto MSDN: X-Content-Type-Options Guide](#)

X-Content-Type-Options: Prevent MIME-sniffing to any type other than the declared content type.

Add Policy

Cancel

Use the provided links underneath the fields to open further information on the subject in the Mozilla or Microsoft developer documentation.

## On this Page:

- [Configuration Options](#)
  - [HTTP Strict Transport Security](#)
  - [Content Security Policy](#)

## Related Pages:

- [Policies](#)
  - [Assigning Policies](#)
  - [Policy Configuration](#)


## Related Documentation:

- [Official Mozilla Online Documentation](#)





## Configuration Options

### HTTP Strict Transport Security

Option	Type	Description	Possible Values	Default
Enable HTTP Strict Transport (HSTS)	Boolean	Set to true if you want to enable HTTP Strict Transport.	true / false	false
Include Subdomains	Boolean	Set to true if you want to include subdomains.	true / false	false
Maximum Age	Integer	Delta seconds user agents should cache HSTS status for.	-	0

<b>Enable HSTS Preload Flag</b>	Boolean	<p>Flag to verify HSTS preload status. Popular browsers contain a hard-coded (pinned) list of domains and certificates, which they always connect securely with. Users must submit a request for their domain to be included in the scheme.</p> <div>  For more detailed information about <b>Strict-Transport-Security</b> go to the <a href="#">official Mozilla online documentation</a>. For further details about <b>Chromium's HSTS preload list</b>, go to <a href="https://hstspreload.org">hstspreload.org</a>. </div>	true / false	false
---------------------------------	---------	--	--------------	-------

## Content Security Policy

Option	Type	Description	Possible Values	Default
<b>CSP Mode</b>	Enum	Defines the content security policy mode to use.	ENABLED REPORT_ONLY DISABLED	DISABLED
<b>Content Security Policy Definition</b>	String	<p>A valid CSP definition must be provided.</p> <div>  For further details about the <b>Content Security Policy</b> go to the <a href="#">official Mozilla online documentation</a>. </div>	-	-
<b>Frame Options</b>	Enum	<p>Defines if, or how, a resource should be displayed in a frame, iframe or object.</p> <div>  For further details about the <b>Frame Options</b> go to the <a href="#">official Mozilla online documentation</a>. </div>	DENY SAMEORIGIN  DISABLED	DISABLED
<b>XSS Protection</b>	Enum	<p>Enable or disable XSS filtering in the UA.</p> <div>  For further details about <b>X-XSS-Protection</b> go to the <a href="#">official Mozilla online documentation</a>. </div>	OFF ON BLOCK DISABLED	DISABLED
<b>Content Type Options</b>	Boolean	<p>X-Content-Type-Options: Prevent MIME-sniffing to any type other than the declared content type.</p> <div>  For further details about the <b>X-Content-Type-Options</b> go to the <a href="#">official Mozilla online documentation</a>. </div>	true / false	false