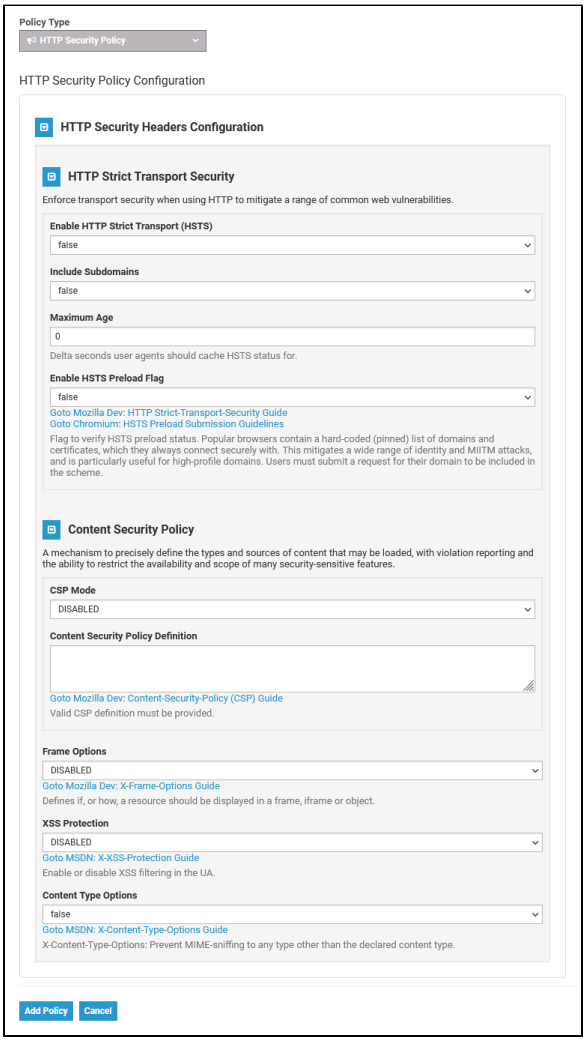
HTTP Security

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



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

Enable HSTS Preload Flag	Boolean	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. For more detailed information about **Strict-Transport-Security** go to the official Mozilla online documentation. For further details about **Chromium's HSTS preload list**, go to hstspreload.org.	true / false	false

Content Security Policy

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