NetIQ Communities (/communities/)

Cool Solutions

NetIQ Cool Solutions › (/communities/cool-solutions/)
(https://forums.netiq.com)

NetIQ Views › (/communities/cool-solutions/netiq-views/)

NetIQ Support Forums ›

Products & Solutions   Support   About   Partners   Communities/company/contact/)   Contact Us (/company/contact/)

Enabling HTTP Strict Transport Security (HSTS) for Tomcat 8

By: kdziekonski
(https://www.netiq.com/
communities/cool-
solutions/author/kdzieko
nski/)

How to add HTTP Strict Transport Security (HSTS) to Tomcat 8

For Regular HSTS within Tomcat 8

Edit the web.xml file in a text editor.

Uncomment the httpHeaderSecurity filter definition and the <filter-mapping> section, and then add the hstsMaxAgeSeconds parameter, as shown below.

```
<filter>
 <filter-name>httpHeaderSecurity</filter-name>
 <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
 <init-param>
  <param-name>hstsEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>maxAgeSeconds</param-name>
  <param-value>31536000</param-value>
 </init-param>
 <init-param>
  <param-name>includeSubDomains</param-name>
  <param-value>true</param-value>
 </init-param>
 <async-supported>true</async-supported>
</filter>

<filter-mapping>
<filter-name>httpHeaderSecurity</filter-name>
<url-pattern>/*</url-pattern>
<url-pattern>*</url-pattern>
<dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

If you are going to add preload (Site is on the Internet and not internal only)

If a site sends the `preload` directive in an HSTS header, it is considered to be requesting inclusion in the preload list and may be submitted via the form on this site.

In order to be accepted to the HSTS preload list through this form, your site must satisfy the following set of requirements:

1. Serve a valid **certificate**.
2. **Redirect** from HTTP to HTTPS on the same host, if you are listening on port 80.
3. Serve all **subdomains** over HTTPS.

    - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists.
4. Serve an **HSTS header** on the base domain for HTTPS requests:

- The `max-age` must be at least eighteen weeks (`10886400` seconds).
- The `includeSubDomains` directive must be specified.
- The `preload` directive must be specified.
- If you are serving an additional redirect from your HTTPS site, that redirect must still have the HSTS header (rather than the page it redirects to).

Please go to **https://hstspreload.org/** to include your site and then add the following after the last init-param and before the async statement in the above statement add the following:

```
<init-param>
  <param-name>preload</param-name>
  <param-value>true</param-value>
</init-param>
```

For Jira add this to the filter section of the Web.xml to enable HSTS.

```xml
<filter>
<filter-name>HstsFilter</filter-name>
<filter-class>org.apache.catalina.filters.HstsFilter</filter-class>
<init-param>
<param-name>maxAgeSeconds</param-name>
<param-value>31536000</param-value>
</init-param>
<init-param>
<param-name>includeSubDomains</param-name>
<param-value>true</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>HstsFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

```java
package org.apache.catalina.filters;

import java.io.IOException;

import javax.servlet.FilterChain;
import javax.servlet.FilterConfig;
import javax.servlet.ServletException;
import javax.servlet.ServletRequest;
import javax.servlet.ServletResponse;
import javax.servlet.http.HttpServletResponse;

import org.apache.juli.logging.Log;
import org.apache.juli.logging.LogFactory;

public class HstsFilter extends FilterBase {
private static final String HEADER_NAME = "Strict-Transport-Security";
private static final String MAX_AGE_DIRECTIVE = "max-age=%s";
private static final String INCLUDE_SUB_DOMAINS_DIRECTIVE = "includeSubDomains";

private static final Log log = LogFactory.getLog(HstsFilter.class);

// The default is "0" like recommended in section 11.2 of RFC 6797
private int maxAgeSeconds = 0;
private boolean includeSubDomains = false;

private String directives;

public void setMaxAgeSeconds(int maxAgeSeconds) {
this.maxAgeSeconds = maxAgeSeconds;
}

public void setIncludeSubDomains(boolean includeSubDomains) {
this.includeSubDomains = includeSubDomains;
}

@Override
public void doFilter(ServletRequest request, ServletResponse response,
FilterChain chain) throws IOException, ServletException {
chain.doFilter(request, response);

// Note that the HSTS header must not be included in HTTP responses
// conveyed over non-secure transport
if (request.isSecure() && response instanceof HttpServletResponse) {
HttpServletResponse res = (HttpServletResponse) response;
res.addHeader(HEADER_NAME, this.directives);
}
}

@SuppressWarnings("boxing")
@Override
public void init(FilterConfig filterConfig) throws ServletException {
super.init(filterConfig);
if (this.maxAgeSeconds < 0) {
throw new ServletException(sm.getString(
"hsts.invalidParameterValue", this.maxAgeSeconds,
"maxAgeSeconds"));
}
this.directives = String.format(MAX_AGE_DIRECTIVE, this.maxAgeSeconds);
if (this.includeSubDomains) {
this.directives += (" ; " + INCLUDE_SUB_DOMAINS_DIRECTIVE);
}
}

@Override
```

```
protected Log getLogger() {
return log;
}
}
```

⭐⭐⭐⭐⭐ (*1 votes, average: *5.00* out of 5)*
You need to be a registered member to rate this post.

Tags: Access Review (https://www.netiq.com/communities/cool-solutions/tag/access-review-2/), HSTS (https://www.netiq.com/communities/cool-solutions/tag/hsts/), Tomcat (https://www.netiq.com/communities/cool-solutions/tag/tomcat/)
Categories: Access Governance Suite (https://www.netiq.com/communities/cool-solutions/category/access-governance-suite/), Access Manager (https://www.netiq.com/communities/cool-solutions/category/access-manager/), Cool Tools (https://www.netiq.com/communities/cool-solutions/category/cool-tools/), Identity & Access Management (https://www.netiq.com/communities/cool-solutions/category/identity-access-management-2/), Identity Governance & Administration (https://www.netiq.com/communities/cool-solutions/category/identity-governance-administration/), Identity Manager (https://www.netiq.com/communities/cool-solutions/category/identity-manager/), IDM Designer (https://www.netiq.com/communities/cool-solutions/category/idm-designer/), iManager (https://www.netiq.com/communities/cool-solutions/category/imanager/), Security (https://www.netiq.com/communities/cool-solutions/category/security/), Security Web (https://www.netiq.com/communities/cool-solutions/category/security-web/), Technical Solutions (https://www.netiq.com/communities/cool-solutions/category/technical-solutions/)

⬤-⬤-⬤-⬤-⬤-💬s://www.netiq.com/communities/cool-solutions/hsts-for-tomcat/#comments)

Disclaimer: As with everything else at NetIQ Cool Solutions, this content is definitely not supported by NetIQ, so Customer Support will not be able to help you if it has any adverse effect on your environment. It just worked for at least one person, and perhaps it will be useful for you too. Be sure to test in a non-production environment.

Leave a Reply

You must be logged in (https://www.netiq.com/communities/cool-solutions/wp-login.php?redirect_to=https%3A%2F%2Fwww.netiq.com%2Fcommunities%2Fcool-solutions%2Fhsts-for-tomcat%2F) to post a comment.

2 Comments

lhaeger (http://www.is4it.de/en/solutions/identity-access-management/) says (https://www.netiq.com/communities/cool-solutions/hsts-for-tomcat/#comment-24873)

Would it have been too much to write out the acronym used at least once so reader can decide if this is interesting at all without googling HSTS first?

Log in to Reply (https://www.netiq.com/communities/cool-solutions/wp-login.php?redirect_to=https%3A%2F%2Fwww.netiq.com%2Fcommunities%2Fcool-solutions%2Fhsts-for-tomcat%2F)

kdwarloksteps.com (https://www.netiq.com/communities/cool-solutions/hsts-for-tomcat/#comment-24875)

Hi lhaeger,

Sorry for not adding it earlier. Thought since it has been out since 2009, figured most tech folks would know that it is HTTP Strict Transport Security. Updated the article to include HSTS for Tomcat 8 and use of Jira as well for your reference. I have added preload for internet based sites as well.
What did you search for that landed you on this page?

Have a great day,
Kevin

Log in to Reply (https://www.netiq.com/communities/cool-solutions/wp-login.php?redirect_to=https%3A%2F%2Fwww.netiq.com%2Fcommunities%2Fcool-solutions%2Fhsts-for-tomcat%2F)
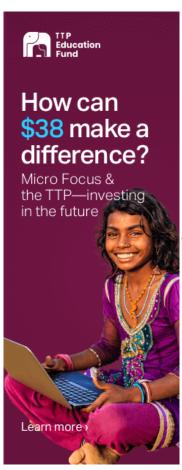
Search for...

Recent Comments

Recent Posts

Categories

Active Directory (https://www.netiq.com/communities/cool-solutions/tag/active_directory/) Authentication (https://www.netiq.com/communities/cool-solutions/tag/authentication/) Automation (https://www.netiq.com/communities/cool-solutions/tag/automation/) Cloud Computing (https://www.netiq.com/communities/cool-solutions/tag/cloud-computing/) Cloud Security (https://www.netiq.com/communities/cool-solutions/tag/cloud-security/) Configuration (https://www.netiq.com/communities/cool-solutions/tag/configuration/) Customizing (https://www.netiq.com/communities/cool-solutions/tag/customizing/) Data Breach (https://www.netiq.com/communities/cool-solutions/tag/data-breach/) DirXML (https://www.netiq.com/communities/cool-solutions/tag/dirxml/) Drivers (https://www.netiq.com/communities/cool-solutions/tag/drivers/) End User Management (https://www.netiq.com/communities/cool-solutions/tag/end-user-management/) Identity Manager (https://www.netiq.com/communities/cool-solutions/tag/identity-manager/) Importing-Exporting / ICE/ LDIF (https://www.netiq.com/communities/cool-solutions/tag/importing-exporting_ice_ldif/) Intelligent Workload Management (https://www.netiq.com/communities/cool-solutions/tag/intelligent-workload-management/) IT Security (https://www.netiq.com/communities/cool-solutions/tag/it-security/) Knowledge Depot (https://www.netiq.com/communities/cool-solutions/tag/knowledge-depot/) LDAP (https://www.netiq.com/communities/cool-solutions/tag/ldap/) Monitoring (https://www.netiq.com/communities/cool-solutions/tag/monitoring/) Open Enterprise Server (https://www.netiq.com/communities/cool-solutions/tag/open_enterprise_server/) Passwords (https://www.netiq.com/communities/cool-solutions/tag/passwords/) Reporting (https://www.netiq.com/communities/cool-solutions/tag/reporting/) Secure Access (https://www.netiq.com/communities/cool-solutions/tag/secure_access/) Supported (https://www.netiq.com/communities/cool-solutions/tag/supported/) Troubleshooting (https://www.netiq.com/communities/cool-solutions/tag/troubleshooting/) Workflow (https://www.netiq.com/communities/cool-solutions/tag/workflow/)

Top Contributors

*geoffc (93700)
(/communities/cool-
solutions/author/geoffc)*

*martincotter (19051)
(/communities/cool-
solutions/author/martincotter)*

*ab (12960) (/communities/cool-
solutions/author/ab)*

*tisenberg (7795)
(/communities/cool-
solutions/author/tisenberg)*

*cstumula (7085)
(/communities/cool-
solutions/author/cstumula)*

*rrawson (4020)
(/communities/cool-
solutions/author/rrawson)*

*alexmchugh (3900)
(/communities/cool-
solutions/author/alexmchugh)*

*TSureshkumar (3740)
(/communities/cool-
solutions/author/TSureshkumar)*

*lhaeger (3690)
(/communities/cool-
solutions/author/lhaeger)*

*ScorpionSting (2705)
(/communities/cool-
solutions/author/ScorpionSting)*

Join the conversation on social media:

Subscribe to our technical newsletter:

Enter Email Address