



Exchange 2019 IIS HSTS Header einrichten

HTTP Strict Transport Security (HSTS) ist ein Mechanismus „Webseitensicherheitsrichtlinien“, der es Webseiten ermöglicht, sich nur über sichere Verbindungen zugänglich zu erklären. Dies trägt dazu bei, User und Webseiten vor Protokoll-Downgrades und Cookie-Hijacking-Angriffen zu schützen.

Anforderungen:

Die Anforderungen für die Umsetzung des [HSTS-Headers](#) sind folgende:

- Ein gültiges Zertifikat
- Umleitung aller http-Links mithilfe einer 301 Umleitung auf https
- Subdomains sollten über ein Wildcard-Zertifikat oder über SAN abgedeckt sein
- HSTS-Header in der Main-Domain konfigurieren
- Aktivierung der Preload-Funktion

Umsetzung IIS:

Die Umsetzung ist recht simpel, gezeigt mithilfe der GUI und der Powershell:

Dazu klicken wir den Baum Exchange Backend an und navigieren dann auf die Rechte Seite hin zur Option HSTS.

Aktivieren die Option und setzen die Parameter wie gezeigt. Preload ist nicht zwingend erforderlich.



The screenshot shows the Internet Information Services (IIS) Manager interface. The left pane shows the site structure with 'Exchange Back End' selected. The main pane displays the 'Exchange Back End Home' site with various configuration options. A dialog box titled 'Edit Website HSTS' is open, showing the following settings:

- Enable
- Max-Age: 31536000
- IncludeSubDomains
- Preload
- Redirect Http to Https

The 'HSTS...' option is highlighted in the right pane under the 'Manage Website' section.



Exchange 2019 IIS HSTS Header einrichten

Umsetzung Powershell:

```
Reset-IISServerManager -Confirm:$false
```

```
Start-IISCommitDelay
```

```
$sitesCollection = Get-IISConfigSection -SectionPath "system.applicationHost/sites" |  
Get-IISConfigCollection
```

```
$siteElement = Get-IISConfigCollectionElement -ConfigCollection $sitesCollection -  
ConfigAttribute @{"name"="Exchange Back End"}
```

```
$hstsElement = Get-IISConfigElement -ConfigElement $siteElement -ChildElementName  
"hsts"
```

```
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "enabled" -  
AttributeValue $true
```

```
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "max-age" -  
AttributeValue 31536000
```

```
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName  
"redirectHttpToHttps" -AttributeValue $true
```

```
Stop-IISCommitDelay
```

Screenshot der Powershelleingabe

```
PS C:\Windows\system32> Start-IISCommitDelay  
  
PS C:\Windows\system32> $sitesCollection = Get-IISConfigSection -SectionPath "system.applicationHost/sites" | Get-IISConfigCollection  
$siteElement = Get-IISConfigCollectionElement -ConfigCollection $sitesCollection -ConfigAttribute @{"name"="Exchange Back End"}  
$hstsElement = Get-IISConfigElement -ConfigElement $siteElement -ChildElementName "hsts"  
  
PS C:\Windows\system32> Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "enabled" -AttributeValue $true  
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "max-age" -AttributeValue 31536000  
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "includeSubDomains" -AttributeValue $true  
  
PS C:\Windows\system32> Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "redirectHttpToHttps" -AttributeValue $true  
  
PS C:\Windows\system32> Stop-IISCommitDelay  
  
PS C:\Windows\system32> |
```




Exchange 2019 IIS HSTS Header einrichten

Überprüfung:

Der Test zeigt, dass der Header ordentlich implementiert wurde. Exchange dient an dieser Stelle nur als Beispielapplikation, hatte gerade keinen anderen IIS zur Verfügung, weil ich meine DMZ gerade neu aufsetze.

Domsignal Toolbox Compiler Log in Sign Up FREE Products

Results



Great! HSTS header was found in the HTTP response headers as highlight below.

Header	Value
cache-control	no-cache, no-store
pragma	no-cache
content-type	text/html; charset=utf-8
expires	-1
server	
request-id	9989cddf-30bf-4b78-8059-df6c0bc48b19
x-frame-options	SAMEORIGIN
x-aspnet-version	
x-powered-by	
strict-transport-security	max-age=0; includeSubDomains
date	Thu, 24 Aug 2023 09:45:42 GMT
connection	close
content-length	27983



Exchange 2019 IIS HSTS Header einrichten

Der interne sowie der externe Stream zeigen ebenfalls, dass der HSTS-Header erkannt wurde:

The screenshot displays the developer tools interface for a web request. The top section shows the **Request Headers** for a GET request to /ecp/HTTP/1.1. The **Cache** header is Cache-Control: max-age=0. The **Client** section lists various headers including Accept, Accept-Encoding, Accept-Language, and User-Agent. The **Cookies** section is currently empty. Below the request headers, a yellow bar indicates that the response body is encoded. The bottom section shows the **Response Headers** for an HTTP/1.1 200 OK response. The **Cache** header is Cache-Control: no-cache, no-store. The **Cookies / Login** section contains several Set-Cookie headers, including ASP.NET_SessionId, msExchEcpCanary, X-BackendCookie, and X-BEResource. The **Entity** section shows Content-Encoding: gzip, Content-Length: 9485, and Content-Type: text/html; charset=utf-8. The **Miscellaneous** section includes request-id, Server, X-AspNet-Version, X-CalculatedBETarget, X-FEServer, X-Powered-By, and X-UA-Compatible. The **Security** section shows Strict-Transport-Security: max-age=0; includeSubDomains, X-Content-Type-Options: nosniff, and X-Frame-Options: SameOrigin.

```
Request Headers [Raw] [Header Definitions]
GET /ecp/HTTP/1.1
Cache
  Cache-Control: max-age=0
Client
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
  Accept-Encoding: gzip, deflate, br
  Accept-Language: de,de-DE;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Edg/116.0.1938.5
Cookies
<
Response body is encoded. Click to decode.
Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON
XML
Response Headers [Raw] [Header Definitions]
HTTP/1.1 200 OK
Cache
  Cache-Control: no-cache, no-store
  Date: Thu, 24 Aug 2023 09:53:49 GMT
  Expires: -1
  Pragma: no-cache
  Vary: Accept-Encoding
Cookies / Login
  Set-Cookie: ASP.NET_SessionId=5682c503-4514-4f88-86b1-77a07ea21547; path=/; secure; HttpOnly
  Set-Cookie: msExchEcpCanary=ZvlOp-dJR0O8WEi8esteDYB-wACIpNsIVLHVUG04F44fjKhUY7IsGACtEB_cE7jSCPIyKYrUsFA.; path=/ecp; SameSite=None;
  Set-Cookie: X-BackendCookie=S-1-5-21-3990916814-2290254576-2840917798-1104=u56Lnp2ejJqBnMzMzprIyJnSns+cz9LLysub0sfNzZ75mc/IyJ3Onsion
  Set-Cookie: X-BEResource=EX1.windowspapst.de~1942127850; path=/ecp/15.2.1258.25; secure; HttpOnly
Entity
  Content-Encoding: gzip
  Content-Length: 9485
  Content-Type: text/html; charset=utf-8
Miscellaneous
  request-id: 39a4b2f1-4cb4-4c21-8167-281e5fa653a7
  Server:
  X-AspNet-Version:
  X-CalculatedBETarget: ex1.windowspapst.de
  X-FEServer: EX1
  X-Powered-By:
  X-UA-Compatible: IE=10
Security
  Strict-Transport-Security: max-age=0; includeSubDomains
  X-Content-Type-Options: nosniff
  X-Frame-Options: SameOrigin
```



Exchange 2019 IIS HSTS Header einrichten

Request Headers [\[Raw \]](#) [\[Header Definitions\]](#)

GET /ecp HTTP/1.1

Client

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: de,de-DE;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Edg/116.0.

Security

sec-ch-ua: "Chromium";v="116", "Not)A;Brand";v="24", "Microsoft Edge";v="116"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1

Transport

Connection: keep-alive
Host: mail.windowspapst.de

Transformer | **Headers** | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw

JSON | XML

Response Headers [\[Raw \]](#) [\[Header Definitions\]](#)

HTTP/1.1 302 Found

Cache

Cache-Control: private
Date: Thu, 24 Aug 2023 10:03:17 GMT

Entity

Content-Length: 223
Content-Type: text/html; charset=utf-8

Miscellaneous

request-id: f004f356-f3eb-4b8d-82a6-9910d0f28245
Server:
X-AspNet-Version:
X-FEServer: EX1
X-OWA-Version: 15.2.1258.25
X-Powered-By:

Security

Strict-Transport-Security: max-age=0; includeSubDomains

Transport

Location: <https://mail.windowspapst.de/owa/auth/logon.aspx?url=https%3a%2f%2fmail.windowspapst.de%2fecp&reason=0>