

https://microsoft.com

Scan

☐ Hide results ☒ Follow redirects

F

Site:

https://www.microsoft.com/

IP Address:

23.217.74.103

Report Time:

15 Aug 2025 09:05:48 UTC

Headers:

✖ Strict-Transport-Security

✖ Content-Security-Policy

✖ X-Frame-Options

✖ X-Content-Type-Options

✖ Referrer-Policy

✖ Permissions-Policy

Advanced:

Ouch, you should work on your security posture immediately:

Start Now

Missing Headers

Strict-Transport-Security

HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".

Content-Security-Policy

Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.

X-Frame-Options

X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".

X-Content-Type-Options

X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".

Referrer-Policy

Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

Permissions-Policy

Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Raw Headers

HTTP/2

200

accept-ranges

bytes

content-type

text/html

etag

"85de642e1467807f647e10807df3869:1711562737.176211"

last-modified

Tue, 26 Mar 2024 18:16:43 GMT

server

AkamaiNetStorage

vary

Accept-Encoding

content-encoding

gzip

date

Fri, 15 Aug 2025 09:05:48 GMT

content-length

12623

Upcoming Headers

Cross-Origin-Embedder-Policy

Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.

Cross-Origin-Opener-Policy

Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.

Cross-Origin-Resource-Policy

Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.





Additional Information

server


Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".

TEST RESULTS

Test Information

	Tested URL	https://microsoft.com
	Test completed	Fri, Aug 15, 2025 6:21 AM Eastern Time (GMT -5)
	Results URL	<a href="https://www.whynopadlock.com/results/4bc5df37-a12b-455c-8983-0d5de16coef5">https://www.whynopadlock.com/results/4bc5df37-a12b-455c-8983-0d5de16coef5</a> 

SSL Connection - Pass



SSL Certificate Info

Certificate Issuer


Microsoft Corporation

Certificate Type

Microsoft Azure RSA TLS Issuing CA o8


Issued On

2025-06-26



Force HTTPS

Your webserver is forcing the use of SSL.



Valid Certificate

Your SSL Certificate is installed correctly.

Your SSL certificate matches your domain name!

Protected Domains:

microsoft.com

s.microsoft.com

ga.microsoft.com

aep.microsoft.com

aer.microsoft.com

grv.microsoft.com

hup.microsoft.com

mac.microsoft.com

mkb.microsoft.com

pme.microsoft.com

pmi.microsoft.com

rss.microsoft.com

sar.microsoft.com

tco.microsoft.com

fuse.microsoft.com

ieak.microsoft.com

mac2.microsoft.com

jpn.delve.office.com  
aus.delve.office.com  
ind.delve.office.com  
kor.delve.office.com  
cobra.me.microsoft.com  
www.businesscentral.com  
businesscentral.com  
msaidatastudio.officeppe.net  
ideas.fabric.microsoft.com  
www.cpt.link  
cpt.link  
yarp.dot.net  
microsoftstream.com  
www.microsoftstream.com  
web.microsoftstream.com  
discover.copilot.ai  
copilot.com  
www.copilot.com  
discover.copilot.com  
researchforum.microsoft.com

Signature

Your SSL certificate is using a sha384WithRSAEncryption signature!

Expiration Date

Your SSL certificate is current. Your SSL certificate expires in 129 days. (2025-12-23)

Mixed Content - Pass

You have no mixed content.

https://apple.com using securityheaders.com

https://apple.com

Scan

☐ Hide results ☒ Follow redirects

Security Report Summary

Site:  
IP Address:  
Report Time:  
Headers:  
Warning:  
Advanced:

https://www.apple.com/  
2.19.60.204  
15 Aug 2025 12:29:07 UTC  

X-Frame-Options

Content-Security-Policy

Referrer-Policy

Strict-Transport-Security

X-Content-Type-Options

Permissions-Policy

Grade capped at A, please see warnings below.

Great grade! Perform a deeper security analysis of your website and APIs:

Try Now

Missing Headers

Permissions-Policy

Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Warnings

Content-Security-Policy

This policy contains 'unsafe-inline' which is dangerous in the script-src directive. This policy contains 'unsafe-eval' which is dangerous in the script-src directive.

## Raw Headers

HTTP/2	200
server	Apple
content-type	text/html; charset=utf-8
set-cookie	ac_ss=a2926c1:1770812947; expires=Wed, 11-Feb-2026 12:29:07 GMT; path=/; secure; HttpOnly
set-cookie	geo=IE; path=/; domain=.apple.com
x-frame-options	SAMEORIGIN
vary	X-MVT-Story-Data, Accept-Encoding
x-mvt-analytics-data	[{"experimentId":"a2926c","variationId":"B"}]
x-mvt-story-data	us-7-2025-homepage-ipad-family-content:B
content-security-policy	default-src 'self' blob: data: *.akamaized.net *.apple.com *.apple-mapkit.com *.cdn-apple.com *.organicfruitapps.com; child-src blob: mailto: embed.music.apple.com embed.podcasts.apple.com https://recyclingprogram.apple.com https://smb.apple.com https://nova.apple.com swdlp.apple.com www.apple.com www.instagram.com platform.twitter.com www.youtube-nocookie.com; img-src 'unsafe-inline' blob: data: *.apple.com *.apple-mapkit.com *.cdn-apple.com *.mzstatic.com; script-src 'unsafe-inline' 'unsafe-eval' blob: *.apple.com *.apple-mapkit.com www.instagram.com platform.twitter.com; style-src 'unsafe-inline' *.apple.com
referrer-policy	no-referrer-when-downgrade
strict-transport-security	max-age=31536000; includeSubdomains; preload
x-content-type-options	nosniff
x-xss-protection	1; mode=block
content-encoding	gzip
cache-control	max-age=290
expires	Fri, 15 Aug 2025 12:33:57 GMT
date	Fri, 15 Aug 2025 12:29:07 GMT

## Upcoming Headers







Cross-Origin-Embedder-Policy	<a href="#">Cross-Origin Embedder Policy</a> allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	<a href="#">Cross-Origin Opener Policy</a> allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	<a href="#">Cross-Origin Resource Policy</a> allows a resource owner to specify who can load the resource.

## Additional Information

server	<a href="#">Server</a> value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".
x-frame-options	<a href="#">X-Frame-Options</a> tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
content-security-policy	<a href="#">Content Security Policy</a> is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. <a href="#">Analyze</a> this policy in more detail. You can sign up for a free account on <a href="#">Report URI</a> to collect reports about problems on your site.
referrer-policy	<a href="#">Referrer Policy</a> is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
strict-transport-security	<a href="#">HTTP Strict Transport Security</a> is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.
x-content-type-options	<a href="#">X-Content-Type-Options</a> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
x-xss-protection	<a href="#">X-XSS-Protection</a> sets the configuration for the XSS Auditor built into older browsers. The recommended value was "X-XSS-Protection: 1; mode=block" but you should now look at <a href="#">Content Security Policy</a> instead.

<https://apple.com> using [whynopadlock.com](https://whynopadlock.com)

### SSL Connection - Pass

	SSL Certificate Info	Certificate Issuer Apple Inc. Certificate Type Apple Public EV Server ECC CA 1 - G1 Issued On 2025-08-11
	Force HTTPS	Your webserver is forcing the use of SSL.
	Valid Certificate	Your SSL Certificate is installed correctly.
	Domain Matching	Your SSL certificate matches your domain name! Protected Domains: apple.com
	Signature	Your SSL certificate is using a ecdsa-with-SHA256 signature!
	Expiration Date	Your SSL certificate is current. Your SSL certificate expires in 81 days. (2025-11-04)

### Mixed Content - Pass

	You have no mixed content.
---	----------------------------