

How to Enable and Disable Opportunistic Encryption ?

Opportunistic encryption is a method of encrypting data transmission that occurs automatically whenever two systems communicate with each other over a network. It is used to secure data transmitted between systems without requiring any additional configuration or setup by the user.

Tutorial :

You can watch the Video or Continue reading the post.

<https://www.youtube.com/embed/BRibGaLHZa8>

Follow the steps to Enable and Disable Opportunistic Encryption.

Navigate to the SSL/TLS of Cloudflare ([Use this link to view How to Navigate](#)).

Disable Opportunistic Encryption :

Click on the Switch button.

Host	Type	status	Expires on
▼ *.testaccount.live,testaccount.live	universal	active	in 6 months(Managed)

Rows per page: 10 1-1 of 1 < >

TLS 1.3
Enable the latest version of the TLS protocol for improved security and performance.
☐

Opportunistic Encryption
Opportunistic Encryption allows browsers to benefit from the improved performance of HTTP/2 by letting them know that your site is available over an encrypted connection. Browsers will continue to show "http" in the address bar, not "https".
This setting was last changed 4 days ago
☒

Minimum TLS Version
Only allow HTTPS connections from visitors that support the selected TLS protocol version or newer.
TLS 1.2 ▼

Here, you can see Opportunistic Encryption is disabled successfully.

Host	Type	status	Expires on
▼ *.testaccount.live,testaccount.live	universal	active	in 6 months(Managed)

Rows per page: 10 1-1 of 1 < >

TLS 1.3
Enable the latest version of the TLS protocol for improved security and performance.
☐

Opportunistic Encryption
Opportunistic Encryption allows browsers to benefit from the improved performance of HTTP/2 by letting them know that your site is available over an encrypted connection. Browsers will continue to show "http" in the address bar, not "https".
☐

Minimum TLS Version
Only allow HTTPS connections from visitors that support the selected TLS protocol version or newer.
TLS 1.2 ▼

HTTP Strict Transport Security (HSTS)
Enforce web security policy for your website
☐

Enable Opportunistic Encryption :

Click on the **Switch** button.

Host	Type	status	Expires on
▼ *.testaccount.live,testaccount.live	universal	active	in 6 months(Managed)

Rows per page: 10 1-1 of 1 < >

TLS 1.3
Enable the latest version of the TLS protocol for improved security and performance.

☐

Opportunistic Encryption
Opportunistic Encryption allows browsers to benefit from the improved performance of HTTP/2 by letting them know that your site is available over an encrypted connection. Browsers will continue to show "http" in the address bar, not "https".

☐

Minimum TLS Version
Only allow HTTPS connections from visitors that support the selected TLS protocol version or newer.

TLS 1.2 ▼

HTTP Strict Transport Security (HSTS)
Enforce web security policy for your website

Here, you can see Opportunistic Encryption is enabled successfully.

Host	Type	status	Expires on
▼ *.testaccount.live,testaccount.live	universal	active	in 6 months(Managed)

Rows per page: 10 1-1 of 1 < >

TLS 1.3
Enable the latest version of the TLS protocol for improved security and performance.

☐

Opportunistic Encryption
Opportunistic Encryption allows browsers to benefit from the improved performance of HTTP/2 by letting them know that your site is available over an encrypted connection. Browsers will continue to show "http" in the address bar, not "https".

This setting was last changed 6 hours ago

☒

Minimum TLS Version
Only allow HTTPS connections from visitors that support the selected TLS protocol version or newer.

TLS 1.2 ▼

Looking for mobile app Instructions?

Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-enable-and-disable-opportunistic-encryption>

Revision #7

Created 27 December 2022 06:55:00 by Admin

Updated 2 September 2023 07:14:28 by Admin