ERR_SSL_PROTOCOL_ERROR

- Rule out common causes first
- Test HTTP/3 (QUIC) compatibility
  - When to suspect HTTP/3 issues
  - How to test
- Test TLS 1.3 compatibility
  - When to suspect TLS 1.3 issues
  - How to test
- ISP and network interference
  - How to identify network interference
  - If network interference is confirmed
- Collect diagnostic information

import { DashButton } from "~/components";

If visitors to your site experience SSL protocol errors such as:

- `ERR_SSL_PROTOCOL_ERROR` (Chrome)
- `Secure Connection Failed` or `PR_END_OF_FILE_ERROR` (Firefox)
- `Safari can't open the page because it couldn't establish a secure connection to the server` (Safari)

These errors indicate that the SSL/TLS handshake failed. This can happen for many reasons, including certificate issues, protocol incompatibilities, or network interference.

Rule out common causes first

Before investigating protocol-specific issues, verify that the error is not caused by:

- **Certificate not yet active** - If you recently added your domain, wait for your Universal SSL certificate to activate.

- **Multi-level subdomain not covered** - Universal SSL only covers one level of subdomains. Refer to ERR_SSL_VERSION_OR_CIPHER_MISMATCH for solutions.
- **Cipher suite mismatch** - Older clients may not support modern cipher suites. Refer to cipher suites for configuration options.

Test HTTP/3 (QUIC) compatibility

HTTP/3 uses the QUIC protocol over UDP, which some networks, firewalls, or devices do not fully support. If visitors experience intermittent SSL protocol errors, HTTP/3 may be the cause.

When to suspect HTTP/3 issues

- Errors occur intermittently, not on every request
- The issue affects only some visitors (often those on corporate networks or certain ISPs)
- Visitors report the site works after refreshing multiple times
- The issue does not occur when using a VPN

How to test

Temporarily disable HTTP/3 to determine if it is the cause:

1. In the Cloudflare dashboard, go to the **Protocol Optimization** page.
2. Turn off **HTTP/3 (with QUIC)**.
3. Ask the affected visitor to test again.

If disabling HTTP/3 resolves the issue, the visitor's network likely blocks or mishandles UDP traffic on port 443. **Re-enable HTTP/3 after testing** and work with the visitor to identify the specific network issue.

Test TLS 1.3 compatibility

TLS 1.3 is the latest version of the TLS protocol and provides improved security and performance. However, some network security devices that perform SSL/TLS inspection may not fully support TLS 1.3.

When to suspect TLS 1.3 issues

- Visitors using corporate networks with SSL inspection report connection issues
- Antivirus software with HTTPS scanning is installed on the visitor's device
- The error occurs consistently for specific visitors but not others

How to test

:::caution Disabling TLS 1.3 reduces security for all visitors. Only disable it temporarily for diagnostic purposes. :::

Temporarily disable TLS 1.3 to determine if it is the cause:

1. In the Cloudflare dashboard, go to the **Edge Certificates** page.
2. Find **TLS 1.3** and turn it off.
3. Ask the affected visitor to test again.

If disabling TLS 1.3 resolves the issue, the visitor's network has a middlebox (firewall, proxy, or antivirus) that does not support TLS 1.3. **Re-enable TLS 1.3 after testing** and ask the visitor to:

- Update their security software to a version that supports TLS 1.3
- Contact their IT department to update network security devices
- Temporarily disable HTTPS scanning in their antivirus software

If you cannot identify the root cause, contact Cloudflare Support with packet captures from the affected visitor showing the failed TLS handshake.

ISP and network interference

Some Internet Service Providers (ISPs) and corporate networks deploy security features that can interfere with HTTPS connections:

- **Deep packet inspection (DPI)** - Inspects encrypted traffic and may interfere with connections it cannot analyze
- **SSL/TLS interception proxies** - Intercept and re-encrypt traffic, which can fail with newer protocols
- **Parental controls or content filters** - May block or interfere with connections to certain sites
- **Carrier-grade NAT (CGNAT)** - Can cause connection issues, especially with UDP-based protocols like QUIC

How to identify network interference

Ask the affected visitor to:

1. **Try a different network** - Use mobile data instead of Wi-Fi, or try a different ISP
2. **Use a VPN** - If the site works through a VPN, the ISP or local network is likely interfering
3. **Disable local security software** - Temporarily disable antivirus or firewall software to test
4. **Check with their ISP** - Some ISPs have security features that can be disabled upon request

If network interference is confirmed

If the issue is caused by the visitor's ISP or network:

- The visitor may need to contact their ISP to add the domain to an allowlist or disable specific security features
- For corporate networks, the IT department may need to update firewall or proxy rules
- As a site owner, you have limited options since the interference occurs outside of Cloudflare

---

Collect diagnostic information

If the above steps do not resolve the issue, collect the following information from affected visitors:

1. **Cloudflare diagnostic data** - Ask the visitor to access `https://your-domain.com/cdn-cgi/trace` and share the output
2. **Exact error message** - The full error text and error code from the browser
3. **Browser and OS version** - Including any security software installed
4. **Network information** - Whether they are on a corporate network, using a VPN, or have any proxy configured

Check Cloudflare Status to verify there are no ongoing incidents affecting SSL/TLS.

If the issue persists and affects many visitors, contact Cloudflare Support with the diagnostic information collected.

□□□ #2
□ □□□ □□□ 2026-11-01 04:31:02 UTC
□ □□□ □□□ 2026-11-01 04:31:03 UTC