Troubleshooting Cloudflare 1XXX errors

Overview

The errors described in this document might occur when visiting a website proxied by Cloudflare. For Cloudflare API or dashboard errors, review our Cloudflare API documentation. HTTP 409, 530, 403, and 429 errors are the HTTP error codes returned in the HTTP status header for a response. 1XXX errors appear in the HTML body of the response.

> Cloudflare **Custom Error Pages** allows customers to change the appearance of the default error pages discussed in this article.

If the resolutions within each error description below do not resolve the error, contact Cloudflare Support.

> Only the site owner may contact Cloudflare for technical support. Lookup contact information for a domain via the Whois database.

> Dedicated email support is available for all Pro, Business, and Enterprise Plan users. Business and Enterprise plan users also have access to chat support. If you require additional support, explore our plans.

Error 1000: DNS points to prohibited IP

Common causes

Cloudflare halted the request for one of the following reasons:

- An A record within your Cloudflare DNS app points to a Cloudflare IP address, or a Load Balancer Origin points to a proxied record.
- Your Cloudflare DNS A or CNAME record references another reverse proxy (such as an nginx web server that uses the proxy_pass function) that then proxies the request to Cloudflare a second time.
- The request X-Forwarded-For header is longer than 100 characters.
- The request includes two X-Forwarded-For headers.
- The request includes a CF-Connecting-IP header.
- A Server Name Indication (SNI) issue or mismatch at the origin.

Resolution

- If an A record within your Cloudflare DNS app points to a Cloudflare IP address, update the IP address to your origin web server IP address. Reach out to your hosting provider if you need help obtaining the origin IP address.
- There is a reverse-proxy at your origin that sends the request back through the Cloudflare proxy. Instead of using a reverse-proxy, contact your hosting provider or site administrator to configure an HTTP redirect at your origin.

Error 1001: DNS resolution error

Common causes

- A web request was sent to a Cloudflare IP address for a non-existent Cloudflare domain.
- An external domain that is not on using Cloudflare has a CNAME record to a domain active on Cloudflare
- The target of the DNS CNAME record does not resolve.
- A CNAME record in your Cloudflare DNS app requires resolution via a DNS provider that is currently offline.
- Always Online is enabled for a Custom Hostname (Cloudflare for SaaS) domain.

Resolution

A non-Cloudflare domain cannot CNAME to a Cloudflare domain unless the non-Cloudflare domain is added to a Cloudflare account.

Attempting to directly access DNS records used for Cloudflare CNAME setups also causes error 1001 (For example: *www.example.com.cdn.cloudflare.net*).

Disable Always Online if using Custom Hostname (Cloudflare for SaaS) domain.

Error 1002: DNS points to Prohibited IP

Common causes

- A DNS record in your Cloudflare DNS app points to one of Cloudflare's IP addresses.
- An incorrect target is specified for a CNAME record in your Cloudflare DNS app.
- Your domain is not on Cloudflare but has a CNAME that refers to a Cloudflare domain.

Resolution

Update your Cloudflare *A* or *CNAME record* to point to your origin IP address instead of a Cloudflare IP address:

1. Contact your hosting provider to confirm your origin IP address or CNAME record target.
2. Log in to your Cloudflare account.
3. Select the domain that generates error 1002.
4. Select the **DNS** app.
5. Click **Value** for the *A* record to update.
6. Update the *A* record.

To ensure your origin web server doesn't proxy its own requests through Cloudflare, configure your origin webserver to resolve your Cloudflare domain to:

- The internal NAT'd IP address, or
- The public IP address of the origin web server.

Error 1002: Restricted

Common cause

The Cloudflare domain resolves to a local or disallowed IP address or an IP address not associated with the domain.

Resolution

If you own the website:

1. Confirm your origin web server IP addresses with your hosting provider,
2. Log in to your Cloudflare account, and
3. Update the A records in the Cloudflare DNS app to the IP address confirmed by your hosting provider.

Error 1003 Access Denied: Direct IP Access Not Allowed

Common cause

A client or browser directly accesses a Cloudflare IP address.

Resolution

Browse to the website domain name in your URL instead of the Cloudflare IP address.

Error 1004: Host Not Configured to Serve Web Traffic

Common causes

- Cloudflare staff disabled proxying for the domain due to abuse or terms of service violations.
- DNS changes have not yet propagated or the site owner's DNS *A records* point to Cloudflare IP addresses.

Resolution

If the issue persists beyond 5 minutes, contact Cloudflare Support.

Errors 1005 Access Denied: Autonomous System Number (ASN) banned

Common causes

The owner of the website (e.g. example.com) has banned the autonomous system number (ASN) from accessing the website.

Resolution

If you are not the website owner, provide the website owner with a screenshot of the 1005 error message you received.

If you are the website owner:

1. Retrieve a screenshot of the 1005 error from your customer
2. Search the **Security Events log** (available at **Security** > **Events**) for the **RayID**, or client IP Address from the visitor's 1005 error message.

> Convert the UTC timestamp of the 1005 error to your local timezone when searching in the **Security Events log**.

3. Assess the cause of the block and ensure the ASN is allowed under the IP Access Rules security feature.

Errors 1006, 1007, 1008 or 1106 Access Denied: Your IP address has been banned

Common causes

A Cloudflare customer blocked traffic from your client or browser.

> Error 1006 also occurs in the Cloudflare **Workers** app under the **Preview** tab when a customer uses Zone Lockdown or any other Cloudflare security feature to block the Google Cloud Platform IPs that the **Preview** tab relies upon.

Resolution

Request the website owner to investigate their Cloudflare security settings or allow your client IP address. Since the website owner blocked your request, Cloudflare support cannot override a customer's security settings.

Errors 1009 Access Denied: Country or region banned

Common causes

The owner of the website (e.g. example.com) has banned the country or region your IP address from accessing the website.

Resolution

Ensure your IP address is allowed under the IP Access Rules security feature.

Error 1010: The owner of this website has banned your access based on your browser's signature

Common cause

A website owner blocked your request based on your client's web browser.

Resolution

Notify the website owner of the blocking. If you cannot determine how to contact the website owner, lookup contact information for the domain via the Whois database. Site owners disable **Browser Integrity Check** via the **Settings** tab of the **Security** app.

> Since the website owner performed the blocking, Cloudflare support cannot override a customer's security settings.

Error 1011: Access Denied (Hotlinking Denied)

Common cause

A request is made for a resource that uses Cloudflare hotlink protection.

Resolution

Notify the website owner of the blocking. If you cannot determine how to contact the website owner, lookup contact information for the domain via the Whois database. **Hotlink Protection** is managed via the Cloudflare **Scrape Shield** app.

> Since the website owner performed the blocking, Cloudflare support cannot override a customer's security settings.

Error 1012: Access Denied

Common cause

A website owner forbids access based on malicious activity detected from the visitor's computer or network (ip_address). The most likely cause is a virus or malware infection on the visitor's computer.

Resolution

Update your antivirus software and run a full system scan. Cloudflare can not override the security settings the site owner has set for the domain. To request website access, contact the site owner to allow your IP address. If you cannot determine how to contact the website owner, lookup contact information for the domain via the Whois database.

> Since the website owner performed the blocking, Cloudflare support cannot override a customer's security settings.

Error 1013: HTTP hostname and TLS SNI hostname mismatch

Common cause

The hostname sent by the client or browser via Server Name Indication (SNI) does not match the request host header.

Resolution

Error 1013 is commonly caused by the following:

- your local browser setting the incorrect SNI host header, or
- a network proxying SSL traffic caused a mismatch between SNI and the Host header of the request.

Test for an SNI mismatch via an online tool such as: SSL Shopper.

Provide Cloudflare Support the following information:

1. A HAR file captured while duplicating the error.

Error 1014: CNAME Cross-User Banned

Common cause

By default, Cloudflare prohibits a DNS *CNAME record* between domains in different Cloudflare accounts. *CNAME records* are permitted within a domain (*www.example.com* CNAME to *api.example.com*) and across zones within the same user account (*www.example.com* CNAME to *www.example.net*) or using our Cloudflare for SaaS solution.

Another common cause is connecting a custom domain to an R2 bucket, where the domain is an active zone with the zone hold feature enabled.

> Cloudflare Apps are not currently supported by Cloudflare for SaaS, therefore any app using a domain configured on our SaaS solution may produce 1014 errors.

Resolution

- To allow CNAME record resolution to a domain in a different Cloudflare account, the domain owner of the CNAME target must use Cloudflare for SaaS.
- To allow connecting to a R2 bucket with a custom domain, disable the zone hold feature on the custom domain target zone to resovle the 1014 error.

Error 1015: You are being rate limited

Common cause

The site owner implemented Rate Limiting that affects your visitor traffic.

> *Unable to purge* is another 1015 error code relating to Cloudflare cache purge. Retry the cache purge and contact Cloudflare support if errors persist.

Resolution

- If you are a site visitor, contact the site owner to request exclusion of your IP from rate limiting.
- If you are the site owner, review Cloudflare Rate Limiting thresholds and adjust your Rate Limiting configuration.
- If your Rate Limiting blocks requests in a short time period (i.e. 1 second) try increasing the time period to 10 seconds.

> If you expect a new Cloudflare Worker to exceed rate limits, refer to the Workers documentation for guidance.

Error 1016: Origin DNS error

Common cause

Cloudflare cannot resolve the origin web server's IP address.

Common causes for Error 1016 are:

- A missing DNS *A record* that mentions origin IP address.
- A *CNAME record* in the Cloudflare DNS points to an unresolvable external domain.
- The origin hostnames (CNAMEs) in your Cloudflare Load Balancer default, region, and fallback pools are unresolvable. Use a fallback pool configured with an origin IP as a backup in case all other pools are unavailable.
- When creating a Spectrum app with a CNAME origin, you need first to create a CNAME on the Cloudflare DNS side that points to the origin. Please see Spectrum CNAME origins for more details
- There is no DNS record for the hostname in the Cloudflare for SaaS target zone

Resolution

To resolve error 1016:

1. Verify your Cloudflare DNS settings include an *A record* that points to a valid IP address that resolves via a DNS lookup tool.
2. For a CNAME record pointing to a different domain, ensure that the target domain resolves via a DNS lookup tool.

Error 1018: Could not find host

Common causes

- The Cloudflare domain was recently activated and there is a delay propagating the domain's settings to the Cloudflare edge network.
- The Cloudflare domain was created via a Cloudflare partner (e.g., a hosting provider) and the provider's DNS failed.

> Error 1018 is returned via a HTTP 409 response code.

Resolution

Contact Cloudflare Support with the following details:

1. Your domain name
2. A screenshot of the 1018 error including the **RayID** mentioned in the error message
3. A HAR file captured while duplicating the error

Error 1019: Compute server error

Common cause

A Cloudflare Worker script recursively references itself.

Resolution

Ensure your Cloudflare Worker does not access a URL that calls the same Workers script.

Error 1020: Access denied

Common cause

A client or browser is blocked by a Cloudflare customer's Firewall Rules (deprecated).

Resolution

If you are not the website owner, provide the website owner with a screenshot of the 1020 error message you received.

If you are the website owner:

1. Retrieve a screenshot of the 1020 error from your customer
2. Search the **Security Events log** (available at **Security** > **Events**) for the **RayID** or client IP Address from the visitor's 1020 error message.

> Convert the UTC timestamp of the 1020 error to your local timezone when searching in the **Security Events log**.

3. Assess the cause of the block and either update the **Firewall Rule** or allow the visitor's IP address in **IP Access Rules**.

Error 1023: Could not find host

Common causes

- If the owner just signed up for Cloudflare it can take a few minutes for the website's information to be distributed to our global network. Something is wrong with the site's configuration.
- Usually, this happens when accounts have been signed up with a partner organization (e.g., hosting provider) and the provider's DNS fails.

> Error 1023 is returned via a HTTP 409 response code.

Resolution

Contact Cloudflare Support with the following details:

1. Your domain name
2. A screenshot of the 1023 error including the **RayID** mentioned in the error message
3. A HAR file captured while duplicating the error
4.

Error 1025: Please check back later

Common cause

A request is not serviced because the domain has reached plan limits for Cloudflare Workers.

Resolution:

Purchase the Unlimited Workers plan via the Plans page on the Workers dashboard.

Error 1033: Argo Tunnel error

Common cause

You've requested a page on a website (`tunnel.example.com`) that is on the Cloudflare network. The host (`tunnel.example.com`) is configured as an Argo Tunnel, and Cloudflare is currently unable to resolve it.

Resolution

- **If you are a visitor of this website**: Please try again in a few minutes.
- **If you are the owner of this website**: Ensure that *cloudflared* is running and can reach the network. You may wish to enable load balancing for your tunnel.

Error 1034: Edge IP Restricted

Common cause

Customers who previously pointed their domains to `1.1.1.1` will now encounter **1034 error**. This is due to a new edge validation check in Cloudflare's systems to prevent misconfiguration and/or potential abuse.

Resolution

Ensure DNS records are pointed to IP addresses you control, and in the case a placeholder IP address is needed for "originless" setups, use the IPv6 reserved address `100::` or the IPv4 reserved address `192.0.2.0` .

Error 1035: Invalid request rewrite (invalid URI path)

Common cause

The value or expression of your rewritten URI path is not valid.

This error also occurs when the destination of the URL rewrite is a path under `/cdn-cgi/` .

Resolution

Make sure that the rewritten URI path is not empty and it starts with a `/` (slash) character.

For example, the following URI path rewrite expression is not valid:

```
concat(lower(ip.geoip.country), http.request.uri.path)
```

To fix the expression above, add a `/` prefix:

```
concat("/", lower(ip.geoip.country), http.request.uri.path)
```

Error 1036: Invalid request rewrite (maximum length exceeded)

Common cause

The value or expression of your rewritten URI path or query string is too long.

Resolution

Use a shorter value or expression for the new URI path/query string value.

Error 1037: Invalid rewrite rule (failed to evaluate expression)

Common cause

The expression of the rewrite rule could not be evaluated. There are several causes for this error, but it can mean that one expression element contained an undefined value when it was evaluated.

For example, you get a 1037 error when using the following URL rewrite dynamic expression and the `X-Source` header is not included in the request:

```
http.request.headers["x-source"][0]
```

Resolution

Make sure that all the elements of your rewrite expression are defined. For example, if you are referring to a header value, ensure the header is set.

Error 1040: Invalid request rewrite (header modification not allowed)

Common cause

You are trying to modify an HTTP header that HTTP Request Header Modification Rules cannot change.

Resolution

Make sure you are not trying to modify one of the reserved HTTP request headers.

Error 1041: Invalid request rewrite (invalid header value)

Common causes

The added/modified header value is too long or it contains characters that are not allowed.

Resolution

- Use a shorter value or expression to define the header value.
- Remove the characters that are not allowed. See Format of HTTP request header names and values in Developer Docs for more information on the allowed characters.

Error 1101: Rendering error

Common cause

A Cloudflare Worker throws a runtime JavaScript exception.

Resolution:

Provide appropriate issues details to Cloudflare Support.

Error 1102: Rendering error

Common cause

A Cloudflare Worker exceeds a CPU time limit. CPU time is the time spent executing code (for example, loops, parsing JSON, etc). Time spent on network requests (fetching, responding) does not count towards CPU time.

Resolution

Contact the developer of your Workers code to optimize code for a reduction in CPU usage in the active Workers scripts.

Error 1104: A variation of this email address is already taken in our system. Only one variation is allowed.

Common cause

This error can occur if an email has been added with some variation of the email you're trying to add. For example, *my+user@example.com* and *my.user@example.com* will be treated the same in our system.

Resolution

Log in as the old user and change email to a "throwaway" address, which will free up the new email.

Error 1200: Cache connection limit

Common cause

There are too many requests queued on Cloudflare's edge that are awaiting process by your origin web server. This limit protects Cloudflare's systems.

Resolution

Tune your origin webserver to accept incoming connections faster. Adjust your caching settings to improve cache-hit rates so that fewer requests reach your origin web server. Reach out to your hosting provider or web administrator for assistance.

Related resources

- Customizing Cloudflare error pages
- Contacting Cloudflare Support

Edit on GitHub · Updated 23 days ago