

NAME

CURLOPT_SSH_HOST_PUBLIC_KEY_MD5 – MD5 checksum of SSH server public key

SYNOPSIS

```
#include <curl/curl.h>
```

```
CURLcode curl_easy_setopt(CURL *handle, CURLOPT_SSH_HOST_PUBLIC_KEY_MD5,
                           char *md5);
```

DESCRIPTION

Pass a char pointer pointing to a string containing 32 hexadecimal digits. The string should be the 128-bit MD5 checksum of the remote host's public key, and libcurl aborts the connection to the host unless the MD5 checksum match.

MD5 is a weak algorithm. We strongly recommend using *CURLOPT_SSH_HOST_PUBLIC_KEY_SHA256(3)* instead.

The application does not have to keep the string around after setting this option.

Using this option multiple times makes the last set string override the previous ones. Set it to NULL to disable its use again.

This option is only applied when libcurl creates a new SSH connection. Once a connection has been created and successfully verified with this MD5 check, it is deemed vetted and may be reused by libcurl without performing the MD5 verification again, even if you later change or disable this option or switch to other verification mechanisms such as *CURLOPT_SSH_KNOWNHOSTS(3)* or *CURLOPT_SSH_HOST_PUBLIC_KEY_SHA256(3)*. Any such changes only affect future new connections, not already established ones.

When MD5 verification is enabled for a connection via this option, libcurl uses that MD5-based check instead of the known hosts/host key callback verification path for that connection, so you must not assume that both the MD5 check and the known hosts/host key callback verification are performed for the same connection.

DEFAULT

NULL

PROTOCOLS

This functionality affects scp and sftp

EXAMPLE

```
int main(void)
{
    CURL *curl = curl_easy_init();
    if(curl) {
        CURLcode result;
        curl_easy_setopt(curl, CURLOPT_URL, "sftp://example.com/file");
        curl_easy_setopt(curl, CURLOPT_SSH_HOST_PUBLIC_KEY_MD5,
                        "afe17cd62a0f3b61f1ab9cb22ba269a7");
        result = curl_easy_perform(curl);
        curl_easy_cleanup(curl);
    }
}
```

AVAILABILITY

Added in curl 7.17.1

RETURN VALUE

curl_easy_setopt(3) returns a CURLcode indicating success or error.

CURLE_OK (0) means everything was OK, non-zero means an error occurred, see *libcurl-errors(3)*.

SEE ALSO

CURLOPT_SSH_AUTH_TYPES(3), CURLOPT_SSH_HOST_PUBLIC_KEY_SHA256(3), CURLOPT_SSH_KNOWNHOSTS(3), CURLOPT_SSH_PUBLIC_KEYFILE(3)