# Using TLS Application-Layer Protocol Settings (ALPS) in HTTP

## Abstract

This document describes the use of TLS Application-Level Protocol
Settings (ALPS) in HTTP/2 and HTTP/3. Additionally, it defines a set
of additional HTTP SETTINGS parameters that would normally be
impractical without ALPS.

## Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the HTTPBIS Working Group
mailing list (httpbis@ietf.org), which is archived at https://
mailarchive.ietf.org/arch/browse/httpbis/.

Source for this draft and an issue tracker can be found at https://
github.com/vasilvv/httpbis-alps.

## Status of This Memo

## Copyright Notice

## Table of Contents

## 1. Introduction

HTTP/2 defines a mechanism for exchanging the protocol settings
using a SETTINGS frame ([RFC7540], Section 6.5). HTTP/3 uses a
similar mechanism ([HTTP3], Section 7.2.4). One of the properties of
the mechanism as defined by both of those protocols is that the
parties start out without having access to the entirety of the
peer's settings. This means that they have to initially operate
using the default settings, and after receiving the SETTINGS frame,
they have to find a way to transition from the default to the
exchanged settings.

HTTP is commonly used in conjunction with TLS. TLS performs its own
handshake that precedes any data being exchanged by the HTTP layer
itself. The TLS Application-Level Protocol Settings extension [ALPS]
allows settings negotiation to be performed within the TLS
handshake, thus making the result immediately available to the HTTP
layer as soon as the handshake completes. This removes the need for
synchronizing settings, and makes them available earlier than they
would be otherwise.

This document defines how ALPS is used with HTTP/2 and HTTP/3, and
introduces certain new settings that would not be practical without
ALPS.

## 2.  Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3.  Use of ALPS in HTTP

If ALPS is successfully negotiated during the TLS handshake for an HTTP/2 connection, the ALPS payload for both peers SHALL be a sequence of HTTP/2 frames. Frames SHALL NOT be present in ALPS unless they are explicitly allowed to be there; this document only allows the SETTINGS frame ([RFC7540], Section 6.5.1). Sending a SETTINGS frame in ALPS supersedes the requirement to send a SETTINGS frame at the beginning of the connection. All settings exchanged via ALPS SHALL be automatically treated as acknowledged.

If ALPS is successfully negotiated during TLS handshake for an HTTP/3 connection, the ALPS payload for both peers SHALL be a sequence of HTTP/3 frames. Frames SHALL NOT be present in ALPS unless they are explicitly allowed to be there; this document only allows the SETTINGS frame ([HTTP3], Section 7.2.4). Sending a SETTINGS frame in ALPS supersedes the requirement to send a SETTINGS frame at the beginning of the control stream.

Since settings exchanged through ALPS are always available at the beginning of the connection, some HTTP extensions may opt to require those to be sent through ALPS. Such extensions are exempt from the initialization requirements of the Section 7.2.4.2 of [HTTP3].

## 4.  New Settings

In addition to specifying the use of ALPS, this document introduces a way for an endpoint to use HTTP/2 and HTTP/3 without any form of header compression. Previously, using SETTINGS to opt into the use of header compression would result in the first flight of requests being sent fully uncompressed; ALPS provides settings before any of the requests are sent, thus removing that concern.

The following new HTTP/2 setting is introduced:

**SETTINGS_HPACK_ENABLE_STATIC_TABLES (0x??):**  May be "0" or "1". If set to "0", the only allowed HPACK instructions are "Literal Header Field without Indexing" and "Literal Header Field Never Indexed" (Sections 6.2.2 and 6.2.3 of [RFC7541]), with index set to "0", and the "H" bit set to zero for both string literals. The default value is "1".

The following new HTTP/3 setting is introduced:

**SETTINGS_QPACK_ENABLE_STATIC_TABLES (0x??):**  May be "0" or "1". If
   set to "0", the only allowed QPACK instruction is "Literal Field
   Line Without Name Reference", with the "H" bit set to zero for
   both string literals. The default value is "1".

Those settings MUST be supported by any endpoint that uses ALPS in
conjunction with HTTP/2 or HTTP/3. Both of those settings MUST NOT
be sent outside of the ALPS.

## 5.  Security Considerations

In ALPS, both client and server settings are sent encrypted.
Settings communicated through ALPS are presented to all clients
before they are authenticated; thus, if a server relies on TLS
client authentication and considers its settings private, it MUST
NOT use the mechanism defined in this document.

## 6.  IANA Considerations

IANA will add an "Allowed in ALPS" column to the "HTTP/2 Frames"
section of the "Hypertext Transfer Protocol version 2 (HTTP/2)
Parameters" registry, with a value set to "Yes" for SETTINGS (0x4),
and to "No" for all other previously defined settings.

IANA will add the following entry into the "HTTP/2 Settings" table:

**Code**  0x??

**Name**  HPACK_ENABLE_STATIC_TABLES

**Initial Value**  1

**ALPS Only**  Yes

**Reference**  This document

TODO: Add HTTP/3 once IANA has an HTTP/3 registry.

## 7.  Normative References

[ALPS]     Vasiliev, V., "TLS Application-Layer Protocol Settings
           Extension", Work in Progress, Internet-Draft, draft-vvv-
           tls-alps-latest, , <https://tools.ietf.org/html/draft-
           vvv-tls-alps-latest>.

[HTTP3]    Bishop, M., Ed., "Hypertext Transfer Protocol Version 3
           (HTTP/3)", Work in Progress, Internet-Draft, draft-ietf-

quic-http-latest, , <https://tools.ietf.org/html/draft-ietf-quic-http-latest>.

[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
           RFC2119, March 1997, <https://www.rfc-editor.org/info/
           rfc2119>.

[RFC7540]  Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext
           Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI
           10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/
           info/rfc7540>.

[RFC7541]  Peon, R. and H. Ruellan, "HPACK: Header Compression for
           HTTP/2", RFC 7541, DOI 10.17487/RFC7541, May 2015,
           <https://www.rfc-editor.org/info/rfc7541>.

[RFC8174]  Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/info/rfc8174>.

## Acknowledgments

## Author's Address

Victor Vasiliev
Google

Email: vasilvv@google.com