## NAME

**fido_dev_enable_entattest**, **fido_dev_toggle_always_uv**, **fido_dev_force_pin_change**, **fido_dev_set_pin_minlen**, **fido_dev_set_pin_minlen_rpid** - CTAP 2.1 configuration authenticator API

## SYNOPSIS

**#include <fido.h>**
**#include <fido/config.h>**

*int*
**fido_dev_enable_entattest**(*fido_dev_t *dev*, *const char *pin*);

*int*
**fido_dev_toggle_always_uv**(*fido_dev_t *dev*, *const char *pin*);

*int*
**fido_dev_force_pin_change**(*fido_dev_t *dev*, *const char *pin*);

*int*
**fido_dev_set_pin_minlen**(*fido_dev_t *dev*, *size_t len*, *const char *pin*);

*int*
**fido_dev_set_pin_minlen_rpid**(*fido_dev_t *dev*, *const char * const *rpid*, *size_t n*, *const char *pin*);

## DESCRIPTION

The functions described in this page allow configuration of a CTAP 2.1 authenticator.

The **fido_dev_enable_entattest**() function enables the *Enterprise Attestation* feature on *dev*. *Enterprise Attestation* instructs the authenticator to include uniquely identifying information in subsequent attestation statements. The *pin* parameter may be NULL if *dev* does not have a PIN set.

The **fido_dev_toggle_always_uv**() function toggles the "user verification always" feature on *dev*. When set, this toggle enforces user verification at the authenticator level for all known credentials. If *dev* supports U2F (CTAP1) and the user verification methods supported by the authenticator do not allow protection of U2F credentials, the U2F subsystem will be disabled by the authenticator. The *pin* parameter may be NULL if *dev* does not have a PIN set.

The **fido_dev_force_pin_change**() function instructs *dev* to require a PIN change. Subsequent PIN authentication attempts against *dev* will fail until its PIN is changed.

The **fido_dev_set_pin_minlen**() function sets the minimum PIN length of *dev* to *len*. Minimum PIN

lengths may only be increased.

The **fido_dev_set_pin_minlen_rpid**() function sets the list of relying party identifiers (RP IDs) that are allowed to obtain the minimum PIN length of *dev* through the CTAP 2.1 FIDO_EXT_MINPINLEN extension. The list of RP identifiers is denoted by *rpid*, a vector of *n* NUL-terminated UTF-8 strings. A copy of *rpid* is made, and no reference to it or its contents is kept. The maximum value of *n* supported by the authenticator can be obtained using fido_cbor_info_maxrpid_minpinlen(3).

Configuration settings are reflected in the payload returned by the authenticator in response to a fido_dev_get_cbor_info(3) call.

## RETURN VALUES

The error codes returned by **fido_dev_enable_entattest**(), **fido_dev_toggle_always_uv**(), **fido_dev_force_pin_change**(), **fido_dev_set_pin_minlen**(), and **fido_dev_set_pin_minlen_rpid**() are defined in <*fido/err.h*>. On success, FIDO_OK is returned.

## SEE ALSO

fido_cbor_info_maxrpid_minpinlen(3), fido_cred_pin_minlen(3), fido_dev_get_cbor_info(3), fido_dev_reset(3)