Controller Authorization

Cindy Myers

Controller Authorization

First published
12 September 2016

Revised
13 September 2017

Contents

Prerequisites

Intended Audience

This document is intended to assist EFILive customers with managing controller authorization codes to facilitate reading and flashing of GM controllers where access permissions are no longer automatically handled by EFILive. Most 2017+ GM vehicles use the process outlined in this document.

Computer Knowledge

It is expected that readers have a basic understanding of:

- The Windows operating system;
- Starting and using Windows applications;
- Navigating folders using Windows Explorer.

Introduction

What is Controller Authorization

Prior to reading or flashing any controller, the EFILive software performs a security negotiation with the controller for permission to access the controller. In the past, the security negotiations were implemented using a simple challenge-response process. The controller challenged the EFILive software with a unique code called a seed and if the EFILive software replied with the correct response called a key then the controller would grant the EFILive software permission to read or flash its contents. That challenge response process was designed using decades old technology and was trivial to implement within the EFILive software which made the entire process relatively automatic and largely transparent to the end user.

In 2017 GM began modernizing and hardening their controllers' security negotiations which is now far more complex and virtually impossible to automate within the EFILive software. That means the end user must now concern themselves with the security negotiations prior to reading or flashing one of these new controllers. Specifically the end user must provide the response (the key) to the controller's challenge (the seed).

It takes on average about five days to find the correct security code on a controller that use GM's previous security system.

It would take on average about 174,000 years to find the correct security code on a controller that use GM's new, hardened security system.

Over 1 trillion possible security codes exist and guessing the correct code used on a particular vehicle is virtually impossible.

To make that task a little easier, the EFILive software now has a controller-authorization module that helps you manage the seed/key data required to gain access to your controller.

The basic process requires users to:

1. Attempt to read or flash the controller to obtain the controller's seed. Because the correct key is not yet known the read or flash will fail with the error message: $0552 Reading and flashing are not yet authorized for this controller.
2. Place an order using the seed in the EFILive store to obtain the correct key. Automated controller auth-code processing occurs within approximately 20 minutes of correct order placement.
3. Enter the key into the EFILive software.
4. Continue to read or flash the controller using the normal EFILive process.

The seed and key are managed by EFILive software inside controller authorization codes or controller auth-codes. A controller auth-code is a 24 character code split into 6 x 4-character sections. It exists in one of two states:

- ***Unauthorized***, which means the controller auth-code only contains the controller's seed. A controller auth-code containing only the seed cannot be used to gain access to the controller.
- ***Authorized***, which means the controller auth-code contains both the seed and the key. A controller auth-code containing both the seed and the correct key can be used to gain access to the controller.

A controller auth-code that contains a seed and an incorrect key will always appear in the EFILive software as if it were correctly authorized because the EFILive software can't know if a key is correct or not, it can only know if a key is present or not.

Additional Support Resources

If, after reviewing this guide, further assistance is required please contact the EFILive Authorised Reseller from whom you purchased your product. They are your first point of contact for EFILive support related inquiries.

If your question is in relation to the actual tuning of your vehicle (i.e. how to gain performance, economy etc.) then please ask these questions on the EFILive Forum (http://forum.efilive.com). EFILive does not provide support or assistance for the actual tuning of any supported vehicles.

Software

Overview

EFILive presently has two major software versions (V7 and V8) that implement different parts of the tuning and scanning process. The V8 software is undergoing significant development and will eventually supersede V7 entirely for FlashScan V2 customers. For the moment however, you must install both versions.

Feature	V7	V8
Scanning	✔	✔
OBDII Diagnostics	✔	✔
Bidirectional Controls	✔	✘
Reading	✔	✔
Flashing	✔	✔
Tune Editing	✔	✘
VIN License Management	✘	✔
Controller Auth-Code Management	✘	✔
Firmware Management	✘	✔

Note: V7 does not support reading and flashing of many late model controllers. Because V7 does not support controller auth-codes, any controller that requires controller authorization can only be read or flashed using the V8 software.

Requirements

The EFILive V8 Scan and Tune software automatically manages controller auth-codes for end users and low volume tuners.

For tuners who are managing controller auth-codes on behalf of multiple customers EFILive can provide a standalone utility to manage your controller auth-code database. The utility is called EFILive_CtrlAuth.exe and which is installed as part of the EFILive V8 software.

After installing V8 Scan and Tune, the EFILive _CtrlAuth.exe can found in the C:\Program Files (x86)\EFILive\V8 folder. Users may choose to create a desktop shortcut for this utility.

The controller authorization software enhancements are available in the following product versions:

- EFILive V8.2.2.305 or later.
- FlashScan V2 / AutoCal Firmware - V2.07.104 or later.

The latest software is available for download from the EFILive website here: http://www.efilive.com/latest/cat/download-efilive

Supported Controllers

Controller Authorization is required on the following controllers:

Controller	
E39/E39A	2017 and later
E78	2017 and later
E80	2017 and later
E81	All
E82	All
E84	All
E92	2017 and later
E98	2017 and later

NOTE: Where the controller type has been in use prior to model year 2017, Controller Authorization is not required.

Licensing Requirements

FlashScan V2 licensing requirements MUST be met in order to flash a tune into a controller. The GM Tuning Option must be enabled, and a VIN license for the target controller must be available on the FlashScan or AutoCal device. If the ECM has already been licensed then the EFILive licensing requirements are already met.

- Tuning Options can be managed by opening the EFILive V8 Scan and Tune software with your device connected and selecting [F7: Licenses]->[F2: Hardware].
- VIN licenses can be managed by opening the EFILive V8 Scan and Tune software with your device connected and selecting [F7: Licenses]->[F3: VIN's].

AutoCal end users DO NOT have access to create, edit or modify tunes. AutoCal end users MUST contact the Tuner who's FlashScan V2 their AutoCal is licensed to.

Controller Authorization

The EFILive Tune Tool [F3: Tune] -> [F8: Authorization] menu manages controller authorization codes for both pass-thru reading and flashing and standalone (BBX) reading and flashing via FlashScan and/or AutoCal.

Display

Controller shows the controller type, and Authorization status icon

 for un-authorized records, containing only the challenge data and

 for authorized records, containing both challenge and response data.

Authorization Code (aka controller auth-code) contains the seed or seed and key that provides security access to the target controller. The controller auth-code will change when the key is added to it.

Authorization Date shows the date and time the response data was added to the controller auth-code effectively authorizing it. No date/time will be displayed until the controller auth-code has been authorized.

VIN shows the VIN obtained from the controller that generated the controller auth-code.

Controller Serial shows the serial number obtained from the controller that generated the controller auth-code.

BB shows the boot block number obtained from the controller that generated the controller auth-code.

OS shows the operating system number obtained from the controller that generated the controller auth-code.

Comments may be used to store information about the controller, the controller auth-code or the authorization process for the target controller.

The VIN, serial, BB, OS and comment fields are all descriptive only and are not required for correct operation of controller auth-codes. However, it is recommended that some form of identification is included in one or more of those fields so that later you can determine which controller auth-code belongs to which vehicle/controller.

Options

Status allows records to be filtered based on authorization status – Authorized Only, Un-Authorized Only or All.

Search For enter text to search for matching controller authorization data.

Clear removes text in the Search For text dialog box and resets Status filters.

Re-Open re-loads controller authorization details from the Local.ska file.

Synchronize synchronizes controller auth-codes between the PC and the attached FlashScan/AutoCal device. Synchronizing is only necessary if/when you are using stand-alone black box reading or flashing. During synchronization, for each unauthorized controller auth-code on FlashScan/AutoCal one of the following two options is performed:

- If the controller auth-code does not already exist on the PC then it is copied from FlashScan/AutoCal to the PC. The controller auth-code can then be used to place an order for the key.
- If the controller auth code already exists on the PC ***and*** has had it's status updated to authorized after purchasing the key then the controller auth-code on FlashScan/AutoCal is updated with the authorized version from the PC.

Sync Selected Items synchronizes all selected controller auth-codes regardless of whether they already exist on FlashScan/AutoCal. This option is useful for tuners who need to copy pre-authorized controller auth-codes to FlashScan/AutoCal prior to shipping the FlashScan/AutoCal to a customer.

Paste (Ctrl+V) pastes controller auth-codes from the clipboard. You may paste just controller auth-codes or entire records.

Copy (Ctrl+C) copy selected records to the clipboard.

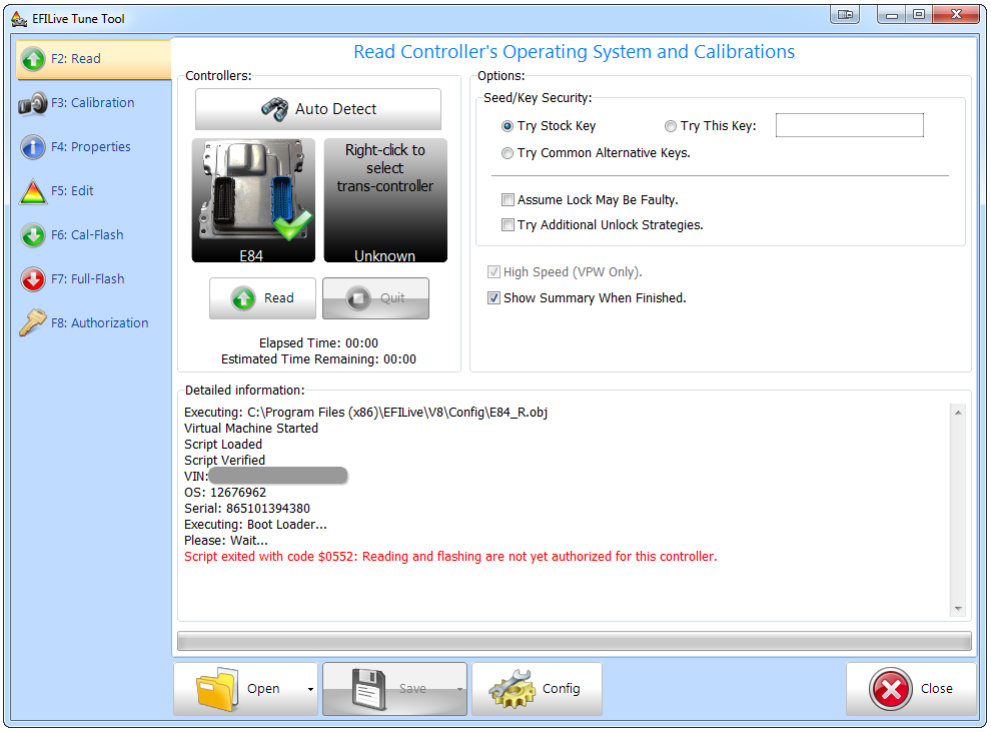
Copy Code (Alt+C) copy controller auth-code only to clipboard.

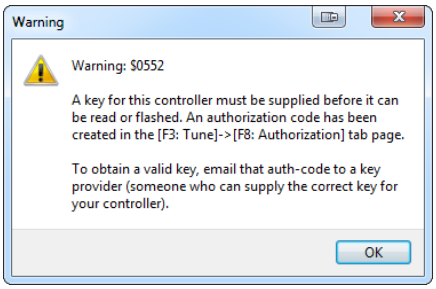
Help opens the Authorization Quick Reference window.

End User Process

Obtain the controller's seed

Attempt to read the controller using either pass-thru or stand-alone black box reading. If the controller is using the latest generation of GM's security and the authorized controller auth-code has not yet been obtained, you will see the following error: "$0552: Reading and flashing not yet authorized for this controller".





The controller's seed will be stored either in the Local.ska file if you are using pass-thru or in the Remote.ska file on the FlashScan/AutoCal if you are using stand-alone black box reading.

Manage Controller Authorization Codes

Generate Unauthorized Controller Auth-Code

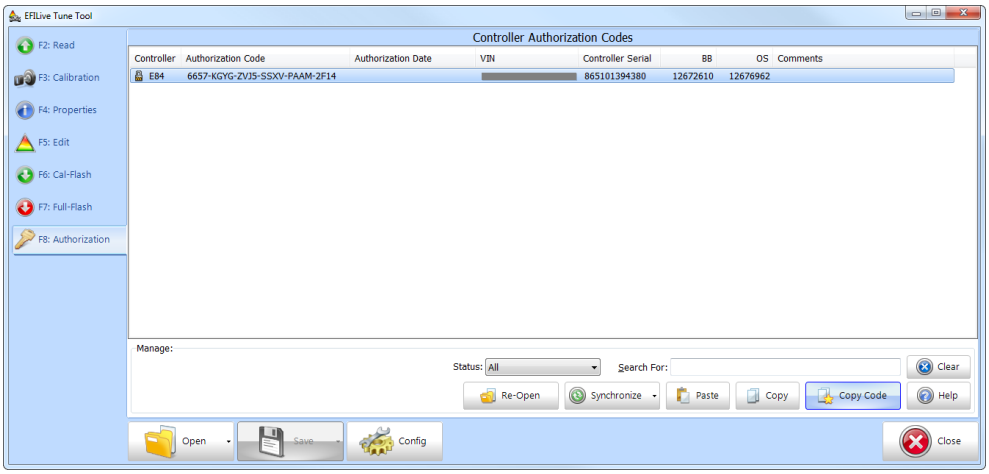
Attempt to read the controller to obtain the unauthorized controller auth-code. Because the authorized controller auth-code has not yet been obtained, reading will fail with the error message: $0552 Reading and flashing are not yet authorized for this controller.

1. Navigate to the [F3: Tune] -> [F8: Authorization] menu in the V8 Scan and Tune software.

a. If you attempted the failed read using FlashScan or AutoCal in pass-thru mode, your unauthorized controller auth-code will be automatically available in the [F8: Authorization] tab page.

b. If your attempt to read the controller was performed using FlashScan/AutoCal via BBR, click [Synchronize] to copy the controller auth-code from FlashScan/AutoCal to the [F8: Authorization] tab page.

2. Highlight the entry you wish to have authorized and click [Copy] or [Copy Code].



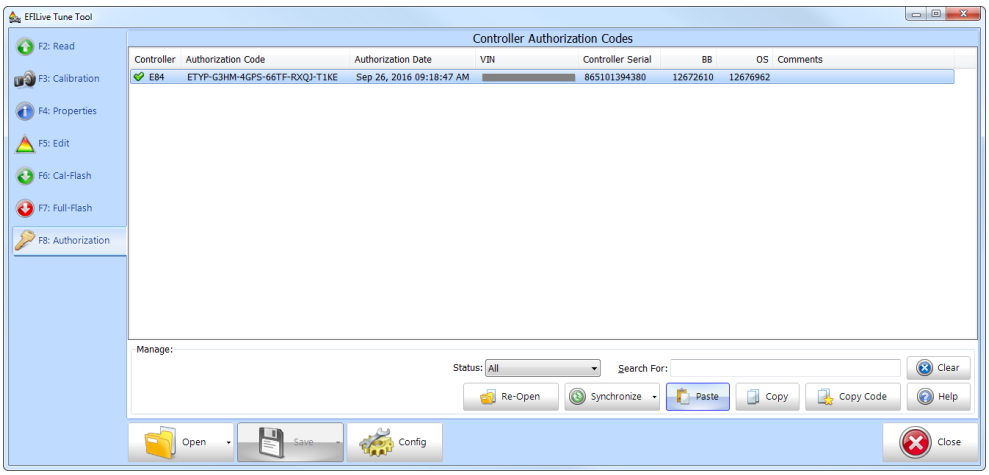
3. Place an order in the EFILive store or contact your tuner if your tuner is managing this process for you.

DO NOT send FlashScan or AutoCal serial number or Authentication Code in lieu of the Controller Auth-Code. Controller Authorization can only be generated by providing a Controller Auth-Code.

Update Authorized Controller Auth-Code

When your controller auth-code provider or tuner contacts you with your authorized controller auth-code, you will need to:

1. Copy the controller auth-code provided.
2. Navigate to the [F3: Tune] -> [F8: Authorization] menu in the V8 Scan and Tune software.
3. Click the [Paste] button to update the authorization details. When the controller auth-code is pasted the icon should change from the locked padlock to a green tick.



4. Click the [Synchronize] button to copy the updated details to your FlashScan or AutoCal device. If a different FlashScan/AutoCal is being used for BBR, the user will need to highlight the correct record and click [Sync Selected Items].

Read Tune with Authorization

Once the controller auth-code has been pasted into the [F8: Authorization] screen, and synchronized (if using stand-alone black box reading/flashing), the controller can be read or flashed using the standard EFILive read/flash processes.

If the controller auth-code was not correctly authorized after receiving the key the controller will reject the controller auth-code with error $0322: “A request was made by FlashScan or AutoCal and the controller was not able or ready to handle the request.” In that case you should contact the authorization code provider for assistance.

Controller Auth-Code Providers

Controller Authorization can be obtained from:

EFILive Limited - Customers can log into their existing EFILive store account and purchase a Controller Authorization code. Automated controller auth-code processing occurs within approximately 20 minutes of correct order placement. For assistance on correct order placement, refer to the License Purchase & Activation Codes FAQ.

Wait4Me Performance gmecmkeys@gmail.com can manually process controller auth-code requests. Contact Wait4Me for pricing.

EFILive Controller Authorization Manager

The EFILive_CtrlAuth.exe program is a utility that manages the local controller auth-code database. The EFILive_CtrlAuth.exe program is an optional utility for advanced users, or tuners who need to manage a large number of controller authorization codes.

In addition to mirroring many of the display features and functions of the tune tool Controller Authorization option, EFILive_CtrlAuth.exe allows users to modify the VIN, serial number, boot block number, operating system number and comment fields. It can also be used to manage controller auth-codes in one or more controller auth-code database (*.ska) files.

Buttons

Open

Open (Ctrl+O) will open a *.ska controller authorization file.

New (Ctrl+N) will create a new *.ska file.

Import (Ctrl+I) will import all records from another *.ska file into the current *.ska file.

Save

Save (Ctrl+S) will save the *.ska file with its current name.

Save As (Alt+S) will save the *.ska file with a new name.

Export (Ctrl+E) will export all selected records in the current *.ska file to another *.ska file.

Delete

Delete (Shift+Delete) will delete all selected records.

Copy

Copy (Ctrl+C) will copy all selected records to the clipboard.

Paste

Paste (Ctrl+V) will paste records or controller auth-codes from the clipboard.

Info

Info (Ctrl+Enter) can be used to paste controller auth-codes from the clipboard so you can view them before deciding to paste them into the controller auth-code database.

Edit

Edit (Alt+Enter) will allow VIN, Serial, Boot Block, Operating System and Comments to be amended.

Set Key will allow a key to be entered to generate the EFILive authorization code. This option should only be used where the actual key for the controller is known.

About

About will display the EFILive software version number.

Close

Close (Alt+F4) will close the EFILive_CtrlAuth.exe program.

Display

See the “Display” section in Controller Authorization for a description of the various display columns.

File Formats

Controller authorization files are saved in EFILive *.ska format. EFILive manages two default *.ska files;

1. Local.ska for all records viewed in [F3: Tune] -> [F8: Authorization], and;
2. Remote.ska for records managed on FlashScan/AutoCal.

Users can create multiple *.ska files which may assist tuners in managing authorization records over multiple customers.

Remote.ska is normally managed by the [Synchronize] option in the V8 software. If you are trouble shooting a problem and wish to view/modify the contents of the Remote.ska file, you can use the EFILive_Explorer.exe program to copy the Remote.ska file from FlashScan/AutoCal’s [Config] file system to the PC where it can be viewed using this software.

File Management

EFILive Ctrl_Auth.exe allows users to edit and delete records. The controller auth-codes in the *.ska files are ***required*** each time you read or flash controllers that are secured via those controller auth-codes.

Deleting or editing records makes permanent changes to that record. Saving a *.ska file after editing or deleting records will make permanent changes to the file.

You should regularly backup all *.ska files. The *.ska files reside in the folder: \Documents\EFILive\V8\Config.

In fact EFILive highly recommends regularly backing up your entire \Documents\EFILive folder tree.

Controller Authorization FAQ

How long will it take to obtain a Controller Authorization?

Automated controller auth-code processing occurs within approximately 20 minutes of correct order placement.

Customers will receive an automated email response with the authorized controller auth-code, and these details will also be appended the online order for future reference.

How will Controller Authorization work with existing BBX and Quick Setup options?

The controller auth-code synchronization process is NOT part of the BBX options or BBX Quick Setup. Users must use the synchronization options in the [F3: Tune] -> [F8: Authorization] tab page to move controller auth-codes to and from FlashScan/AutoCal.

What happens if I Format the Config file system on FlashScan/AutoCal?

Formatting the Config file system will remove the Remote.ska file that contains the controller auth-codes required for BBR and BBF operations. Users can [Sync Selected Items] option to copy selected controller auth-codes back onto the device.

What happens if I delete a record using EFILive Ctrl_Auth.exe program?

- Restore a backup of your *.ska file.
- If the controller auth-code exists on a FlashScan or AutoCal device then you can use the Synchronize option to copy the controller auth-code from the device to your PC again.
- Copy/Paste the controller auth-code from your Controller Auth-Code email or your online order.
- Perform the controller authorization process again. (This may incur additional charges from the Controller Authorization Provider.)