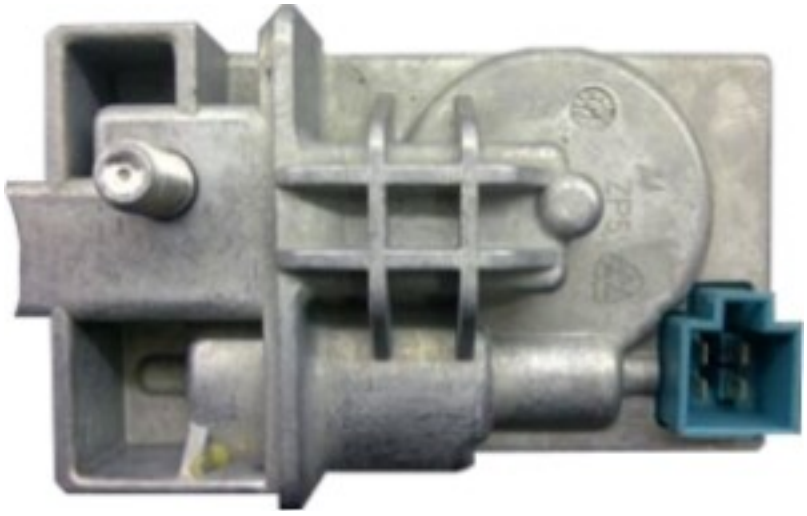
ESL Doctor



User Manual

Overview

This software and accompanied drivers are intended for strictly personal educational purposes only and it's use is sole liability of customer. All further consequences of any other possible device commercial or illegal use is subject of user's choice and responsibility.

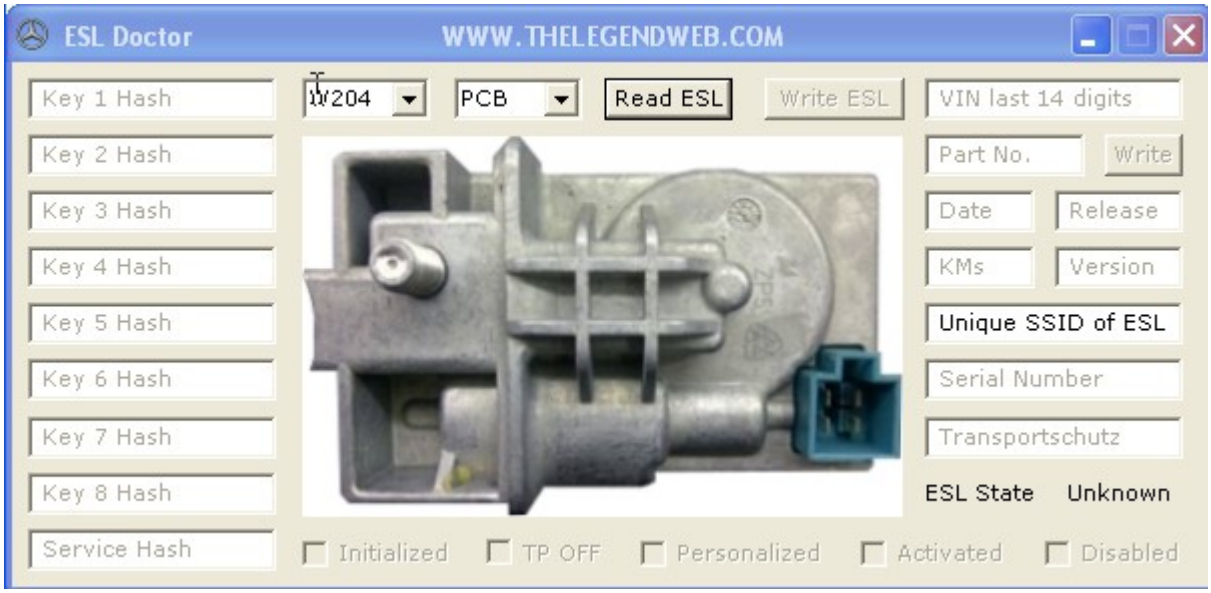
The drivers, provided are original FTDI® files – both self-installing executable and zip archive, containing files for manual install. Choose the one suitable for You or download latest version from FTDI® website. Any further questions of misbehaved FTDI® drivers to be forwarded to their support center.

Hardware serial number is visible in Windows in “My Computer” /“Properties” / “Hardware” / “Device Manager” - selecting the device - “Properties” / “Details” / “Device Instance id” and Serial Number (8 digits and / or characters) is shown after VID (Vendor Identifier) and PID (Product Identifier) of the interface hardware. The method, described above may vary, depending on exact operation system You are using, but in general is the same. This unique serial number eases identification of Your hardware in manufacturer database, providing You corresponding initial software and further updates.

Hardware contains Lithium battery for backing up the critical data for supporting it's functionality. Do not use / store the device in extreme temperatures or inappropriate humidity or another operational conditions, as this could lead to big leakage currents, shortening battery life. Consult Lithium-battery specifications for proper storage, transportation and usage. In any case it is good idea to have device connected and powered by USB port or another external compatible +5V DC source for prolonging battery lifespan.

How to use

When software starts, if hardware is properly connected, You will see the following (if button “Read ESL” if not active, this means You did something wrong):



Always mind the exact order of connecting and disconnecting the ESL / interface / PC ! Not following it might seriously harm any / all components:

1. Plug ESL Doctor hardware to available USB port.
2. Connect ESL wiring to ESL Doctor hardware using it's fast installing 2-pin green connector.
3. Power-on ESL from steady +12V DC power supply – it is a must!!!

Upon completion of Your work with ESL disconnect in the reverse order:

1. Power-off ESL by removing +12V DC power supply.
2. Disconnect ESL wiring from ESL Doctor hardware by removing 2-pin green connector.
3. Unplug ESL Doctor hardware from USB port of PC.

You could use ESL Doctor for ESL units, which are not dismounted from car. Just be sure You have connected them properly to “GND” and “K-line” of ESL Doctor hardware. Powering such ESL units is a matter of choice – either use existing car +12V power supply or by external power unit. Power supply is very important for proper locking/unlocking of ESL – it might lead to undesirable effects if You can't guarantee proper power to the ESL. Consult vehicle's technical documentation for available power supply connection point with enough current throughput.

Above described sequence of connecting / disconnecting ESL Doctor concerns “K-line” operation for reading / writing assembled ESL units or bare ESL PCBs. Except that mode of operation, ESL Doctor provides a lot of features (Initialize, Viriginize, etc…), which are possible only if MCU is removed from ESL PCB and placed to adapter board provided. Below are given required steps for proper connections of MCU to ESL Doctor:

1. Solder Motorola or NEC MCU to adapter board or put into ZIF-socket of adapter board. Both options could be available, depending on ESL Doctor configuration, so You choose which one to use. Mind pin 1 orientation of MCU – exact placement on adapter board is a must!!! If MCU is placed wrong it could harm as itself and ESL Doctor hardware. Please, look at photo below for adapter boards pin 1 location and always check correct MCU placement before proceeding to next step!!!
2. Plug adapter board to ESL Doctor hardware in proper direction. DO NOT reverse adapter board !!! The orientation of adapter board should be facing up to the label of ESL Doctor – look at picture given below, showing proper orientation of adapter board. Also Motorola or NEC MCU soldered to adapter board should be free of dirt, soldering paste and any other flux, which might interfere with electrical signals. Have the adapter well cleared after soldering, using Isopropyl alcohol or another suitable cleaning solution. When connecting adapter board, ESL Doctor should be disconnected from USB – always mind that !!!
3. Connect hardware to available USB port of PC.

Upon completion of Your work with ESL Doctor disconnect in the reverse order:

1. Unplug ESL Doctor hardware from USB port of PC.
2. Disconnect adapter board from ESL Doctor hardware.
3. Unsolder Motorola or NEC MCU from adapter board (or remove from ZIF-socket if using it).

After connecting hardware as described above and starting software, proceed with selecting desired model and mode of operation. Here is brief description of available options:
“W204” - newest generation ESL with NEC MCU, installed in 204, 207, 212, etc… models of MB cars.
“W203” - older generation ESL with NEC MCU, installed in 203, 211, Sprinter, etc.. models of MB cars.
“W210” - all generations ESL with Motorola MCU, installed in many models of MB cars.
“K-line” - selects that mode of operation, using fast installing 2-pin green connector.
“PCB” - selects that mode of operation, using adapter board.

Note: “K-line” or “PCB” mode of operation, selected by software should correspond exactly to hardware connected to ESL Doctor!!! Do not use hardware and software with inappropriate selection! Do not use hardware with simultaneously connected adapter board and 2-pin green connector!!! ONLY one mode of operation is possible! Avoiding this might seriously harm any / all components!!!

If You know the unique SSID of the car ESL belongs to, enter it in the corresponding field. If SSID is provided for W204-type of ESL it is possible to read odometer, which will be displayed in “KMs” field. Press “Read ESL” button and You will get the data:

After Hash data is read and shown on screen, be sure that You see all Keys Hashes, numbered from 1 to 8, and also so called “Service Hash” (also called “Dealer Password” or different, depending on people's habit to name it) and also data about the software version of ESL should be present in “Version” window. All these records (Hashes and SSID) are needed for further comparison to data in EIS or Key or other modules – Electronic Control Unit (ECU) for the engine or transmission modules - “7G-Tronic” (ETC), ISM, etc… modules, which are related to FBS® (immobilizer) system.

The exact order of Hashes is very important and should be properly aligned to corresponding data in Electronic Ignition Switch (EIS). If misaligned, the ESL unit will not unlock and not permit the EIS to turn into “Ignition ON” state or/and issue “Starter ON” signal. There are vast number of ESL stopped to operate due to corrupted Hashes. It is possible to operate (Lock / Unlock) the ESL with software, simulating presence of EIS, so misbehaving reason could be identified – EIS or ESL.

Except Hash data of ESL, ESL Doctor reads also status of ESL itself and Key Hashes (if enabled will have green background / if disabled the background will be red).

Depends on the model selected, additional data could be available. Software reads data and fills corresponding windows or shades them depending on data ESL provides to requests sent. Most of data is provided by 204-family of ESL. Part number and unique Serial number are available for this ESL and also release dates of production and software version. “Transportschutz” a.k.a Transport Protection Key (TP Key) is present and if correct is highlighted in green. If it's value is not correct it is highlighted in red and ESL should be “Virginized” to correct this issue. Read further for “Virgin” function description…

Always look the ESL State information, provided by software – if “Unlocked” / ”Locked” / ”Moving” or “Fault”! If internal position switches of ESL are faulty or got stuck by dirt or other reason, then ESL unit will not be able to follow properly it's movement and will not respond to EIS requests. It is very common for W204 ESL units. The unit could be in unlocked state with steering wheel free, while ESL reports “Moving” state. Dismantle the ESL and align it's moving parts to position switches, so correct information to be present. W204 motor's problems often cause it to stuck in the middle of it's movement, just before reaching end position, but enough to confuse position keys. Also after repairing / dismantling ESL it is important to put it in car with correct position – check it first with software, that it's properly assembled and not showing “Moving” before You connect it to car wiring. Further in this document You will find hardware repair hints.

Those hardware issues with motor/switches/gears, described above, could lead to “Disabled” status of ESL. In that situation, ESL is not making any attempts to operate relays for motor – no “clicking” sound is heard from relays. Also ESL is not authorizing the EIS, so car becomes useless. No reset / renew procedure could be performed to such ESL units with “Dealer Password” !!! Until ESL Doctor software all these ESL were also useless! Now You have opportunity to bring such ESL back to life and use it over and over again! Read further for “Enable” button function…

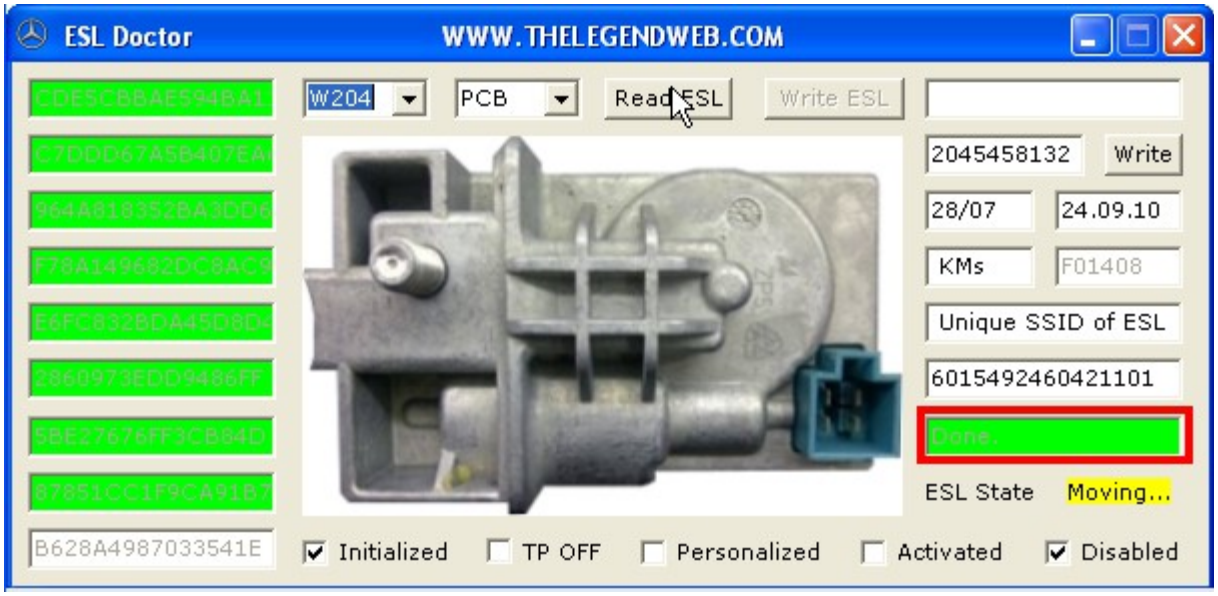
If for some reason ESL unit is being repaired or You put new ESL unit or ESL Emulator then You should adapt it to the car, using information, provided by us. Press “Write ESL” button and select the file for the car, You are working on. The SSID, contained in file will be displayed in corresponding window and adaptation process will start.

If You leave VIN field and KMs field with their default values “ VIN last 14 digits” and “KMs” then ESL will be programmed with “zero” values and will have odometer “0” kilometers and VIN will be 14 “zeroes” - “0 000 000 000 0000” - this is valid for 204-family. For all other types of ESL these data is not needed. It is not required to have correct data filled to these fields, but is good practice to adapt new ESL with expected data for any specific car.

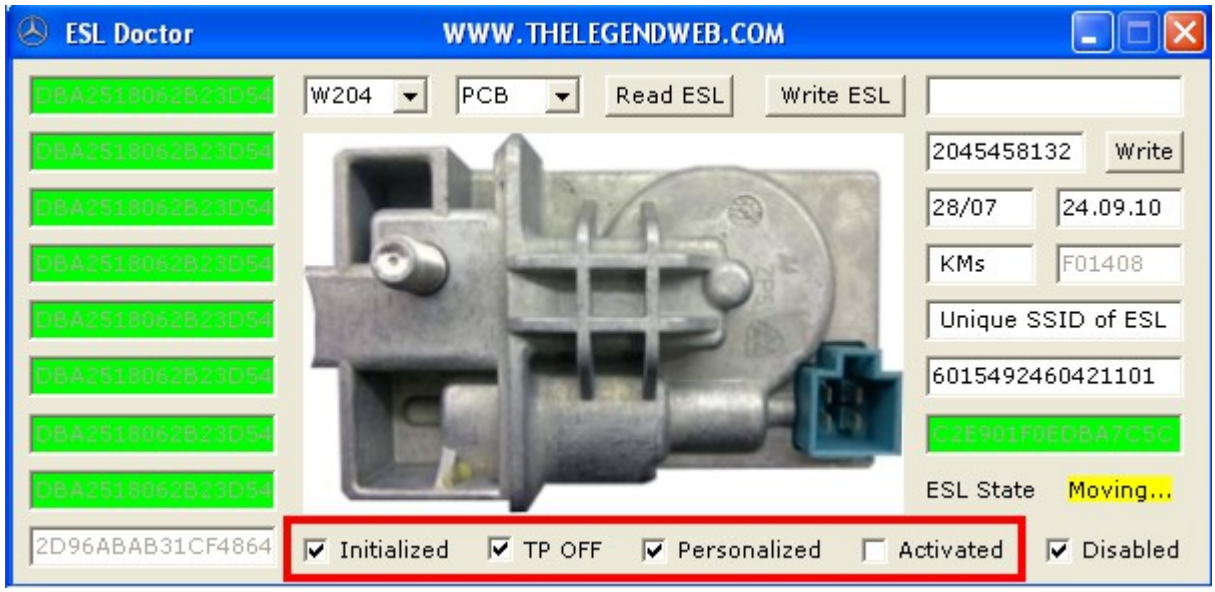
Just have in mind, that You should provide VIN and KM values to corresponding fields BEFORE You click “Write ESL”. Note that You can't decrease the odometer of ESL – it is synchronized to EIS value and could only be incremented. Also You should know that VIN , Part number, release dates and several more values could be changed at any moment. At the initial stage only SSID and KMs are being programmed with the values provided.

Note that “Write ESL” is activated after reading ESL status only if it allows writing new data to MCU. This button remains shaded if writing is prohibited by MCU. Also button is being shaded until write operation is in process. Adaptation steps are indicated in corresponding field as shown. Software takes care of current ESL status and performs needed commands according to ESL if “Initialized”, “TP OFF”, “Personalized”, etc… Here is how it looks for the specific example:

When it is ready software will inform You and will put the ESL in “Locked” position if 204-family ESL is operated in “K-line” mode. If it is in “PCB” mode this command is not issued to MCU and it remains non-”Activated”. The only way to complete adaptation process of that 204-family ESL is to perform it via “K-line”, not while NEC MCU is being placed on adapter board.



You could check the success of adaptation process by clicking “Read ESL”:



As already noted, when operated in “PCB”-mode for 204-family ESL, it is not possible to issue final “Lock”-command to MCU and it remains non-”Activated”, which leaves the option to program it further when soldered back to original PCB. While ESL is only “Personalized” it is in kind of Test-mode and re-writing with same/another data is possible.

If above described adaptation procedure is not possible, because “Write ESL” is shaded, due to already “Activated” ESL (i.e. 2nd hand unit, taken from scrap-yard) then You could put that ESL back to “Initialized” state WITHOUT using “Service Hash” a.k.a “Dealer Password”!!!

Double-Click on the ESL picture in the center of software and new window will appear:

Click “Initialize” button and process starts. Caption is changed to “Stop” making possible to interrupt process at nay desired moment and also progress is indicated:

In few seconds (time is relative and not fixed! It depends on many factors – MCU status, version, etc.. In general previous versions of 204-family ESL, E0.XX.XX are faster to initialize than later one F0.XX.XX. The F0-versions have slightly different behavior, but up-to-date of writing this document any version of 204-family is able to Initialize, Enable, Virginze) confirmation appears:

Now, You could close that window and return to previous one for reading ESL if You want to check success of operation or proceed with writing as described in previous pages. Always pay attention to “Disabled” status of ESL and observe it BEFORE proceeding with “Write ESL” button.

"Disabled" status doesn't prevent ESL from re-writing it with new data, but prevents normal ESL operation. It is the biggest pain-in-the-*** for a years, leaving a lot of ESL units in the garbage, because "Dealer Password" renewal doesn't affects this flag. ONLY ESL Doctor solves this problem, which is indicated in two ways – either observe "Disabled" check-box on initial screen of software or "Flag" window on secondary screen:

"Disabled" is equal to 0xAA value. Enabled (normal operating) state equals to value 0x00.

To fix that issue and "resurrect" ESL, click "Enable" button. Caption is changed to "Stop" as per "Initialize" button and progress of operation is indicated in same manner:

Execution times are longer than "Initialize" operation. Just be patient and give the software time to execute. If You need to do something else with that computer, do not worry to interrupt the process and continue it at any convenient for You moment. Press "Stop", exit the software, disconnect hardware as mentioned in the beginning of this manual and use Your computer as You need it. When You decide to continue with "Enable" operation, just start everything from beginning. Do not worry for tracking progress of previous attempts. Information is stored inside the MCU, so You do not loose anything if stop it and continue it at another computer or at later moment. Just follow the right sequence of actions, keeping MCU and hardware intact.

Same precautions as per “Enable” button are valid for “Virginize” function. You should provide enough time for that operation to be performed as it requires relatively much more time than previous ones - “Initialize“ and ”Enable”, due to the fact that a lot more data in MCU should be processed to factory values. But turning MCU back to factory default (virgin) state is needed in rare cases, so it is not so inconvenient the required time to perform it. Virgin state is required when Transport Protection Key is corrupted or when You need to change unique Serial Number of ESL. Those two parameters are initialized in factory and then ESL units are being delivered to dealers. In fact it is unique Serial Number which is important data, being programmed by factory and after that ESL unit is being “locked” for transportation, so no commands could be performed on it until valid Transport Protection Key has been sent to unlock the ESL unit. For this reason those are the two values, which determines success of following adaptation process. And if TP Key is corrupt, this adaptation process couldn't be performed. And in this situation button “Virginize” comes at help! Use it only if You are sure that ESL MCU couldn't be programmed due to corrupted data of MCU, preventing it from accepting adaptation commands. Random use of “Virginize” button is just a waste of resources, because You do not need to put every NEC MCU in virgin state – if it could be programmed with “W204_Factory.bin” provided by us, it means MCU has intact internal data. Always use “W20X_Factory.bin” files provided by us to test NEC MCU if ready for programming. Those factory files comes with Dealer Password implemented in ESL Doctor software, so You could renew those MCU at any moment. Also if You are programming NEC MCU while placed on adapter board, it doesn't get into “Activated” status and many further programming attempts are possible. That was already noted, so after any “Initialize”, “Enable” or “Virginize” operation being performed successfully, write the NEC MCU with file “W20X_Factory.bin”. With it is possible to test locking / unlocking operation when ESL unit is assembled and as mentioned above, after all test, You could renew ESL with factory Dealer Password, so ESL unit will become again in “Initialized” status and looks shiny new!!!

The operation described above is exactly how ESL manufacturing process happens and how post-production tests are being performed. And of course at the end ESL unit is being reset with factory Dealer Password (same, which You see on ESL Doctor secondary window).

Note that “Renew” button for resetting ESL with Dealer Password is enabled only when ESL allows such action. In example for 204-family ESL it is possible only if working by “K-line” and if ESL has “Activated” and not “Disabled” status!

Of course any 204-family ESL could be renewed with Dealer Password if above cited two conditions are satisfied – status is “Activated” and not “Disabled”! Older ESL families could be renewed without those prerequisites. Just place in above marked window Your 8-bytes Dealer Password and click “Renew” button. In few seconds confirmation message will be present or if there is an error You will be notified. Default value here is for “W20X_Factory.bin” file !!!

Above described adaptation / renewing processes were concerning security features of ESL. Alongside with security data, ESL units contain and information data, identifying module. Most of this data could be altered. Here is an example for 204-family ESL, but for any other model selected, ESL Doctor software will enable or disable for writing specific fields, according to available options.

Here, VIN is missing and Part Number and release/software dates values are random. You could enter any desired values, but is advisable to stick to MB-common values, so DAS diagnostics software do not get confused if read this identification information from ESL. Here is an example:

Click “Write” button when all data is entered correct and the button shades for a while until all data is being written. If You click “Read” You will see the success of operation:

Also on secondary screen of software You have options to edit values: