**Electronic Logging Devices and Hours of Service -Training**

1. **ELD Provider Training**

Welcome to ELD provider training. This training is intended to aid manufacturers and providers of electronic logging devices, or ELDs, in providing devices to motor carriers that are fully functional and in compliance with the ELD Rule. It is meant to supplement the technical specifications in the ELD rule. ELD providers are responsible for ensuring that their devices meet all the minimum requirements.

# Data Transfer Methods

## *What are ELDs?*

FMCSA aims to make highways safer for all drivers. One danger on the road is fatigued driving, which leads to hundreds of crashes and deaths each year.

The ELD rule requires the adoption of electronic logging devices, or ELDs, by the vast majority of commercial truck and bus drivers.

This is the Agency’s latest step to address fatigued driving among drivers of large trucks and buses-and we are relying on you to make sure these drivers and their employers are equipped with fully functional and compliant devices.

First, what is an ELD, and what does it do? An ELD synchronizes with a vehicle’s engine to automatically record a driver’s off-duty and on-duty time, and securely transfers this “hours of service” data to a safety official for review.

## *Telematics vs Local Transfer*

There are four possible methods by which an ELD may transfer data to a safety official. In this section, we will walk through each method and steps your ELD will need to take to implement them. A factsheet with this information is also available. This factsheet will also cover testing procedures for each method.

The four data transfer methods are broken down into two categories: Telematics, which includes web services and email and Local Transfer, which includes Bluetooth and USB. To be considered compliant, ELDs must support either *both methods* of the telematics transfer option, or *both methods* of the local transfer option. FMCSA’s preferred method of data transfer is web services.

## *Web Services*

Because it is the fastest and most efficient method, web services is FMCSA’s preferred method of data transfer.

In the web services transfer method, the ELD connects to an FMCSA Web Service using its own internet connection and submits: the client certificate, the ELD data file, and an output file comment. This is received by the ELD Web Service. FMCSA then cross-references the list of registered, self-certified ELDs and validates the ELD certification status. If the ELD is found on the list, the ELD data file will then be validated.

If no serious errors are found in the ELD file, the file will be retrieved and read by the safety official using their enforcement software. If errors are found, they will be indicated in the Web Service response. For more information regarding warnings and errors, please consult the ELD Interface Control Document and Web Services Development Handbook, which can be found in FMCSA’s ELD Provider portal online, or in the resources in the top right corner of your screen.

## *Email*

If you choose to support the telematics option, you will also need to support email transfer. It’s important to note that the email data transfer method does not allow for sending the ELD output file directly to the safety official. Like web services, the output file is transferred to the ELD Web Service where it can be retrieved by the safety official.

To transfer via email, the ELD will generate an email message that is automatically addressed to a specific FMCSA ELD email address. Using the S/MIME standard, the email must be encrypted using at the minimum the AES-256 algorithm and FMCSA’s ELD public key. The message must be signed using the manufacturer’s private key. The email will be composed as seen on the screen.

The FMCSA email address and public key are provided once you have registered as a provider with FMCSA. We will cover this a little later on.

Once the email is transmitted to FMCSA, the email will be decrypted, the signature will be validated using the manufacturer’s private key, and the ELD file will be validated. A reply is sent to the “From” address indicating success, or providing a list of errors.

## *Bluetooth*

If you choose to support local transfer, the ELD will need to support the Bluetooth data transfer method.

In a Bluetooth transfer, the ELD borrows the Internet connection from a safety official’s Bluetooth device. Therefore, the first step is to establish the Bluetooth connection between the ELD and the safety official’s Bluetooth device. Note that the Bluetooth method does not allow for direct transfer to the safety official. This is another method for transferring the output file to the ELD Web Service where it can be retrieved by the safety official.

Once the ELD and safety official’s Bluetooth device are paired, the ELD connects to an FMCSA Web Service and submits the following: the client certificate, the ELD output file, and the output file comment. As with the web services transfer method, FMCSA then cross-references the list of registered, self-certified ELDs and validates the ELD certification status. If the ELD is found on the list, the ELD data file will then be validated. If no serious errors are found in the ELD file, the file will be readable by the safety official. If errors are found, they will be indicated in the Web Service response.

## *USB 2.0*

If you choose to support the local transfer option, you will also need to support the USB transfer method. This is the only “offline” transfer method, in that it does not require internet connectivity.

To transfer via USB, the safety official would first unlock the hardware-encrypted USB device, and hand it to the driver. The driver will then connect the USB to the ELD and initiate data transfer. The ELD will check the USB device to ensure the configuration file is downloaded prior to transferring data. Once the data has transferred to the USB drive, the safety official can insert the USB drive into their computer and use the eRODS software, which you’ll learn more about in a bit, to open the file.

# Information for ELD Providers

## *Provider Landing Page*

To assist you in providing motor carriers with devices that are fully functional and meet the minimum requirements in the technical specifications of the ELD rule, FMCSA has made a number of resources available. You can access these on the ELD website by navigating to the ELD Providers landing page. This page includes information you need to develop and test your ELD. You can also use the links provided on this page to request a provider account with FMCSA. Once that account is approved, you can use it to access the ELD Provider Portal.

## *Request an Account*

We accessed the “Request an Account” page from the ELD provider page on the ELD website, but you can also access this page from anywhere on the ELD website using the “ELD Providers” dropdown in the top navigation.

Once you have filled out the required information, click “Create.” You will receive a confirmation email once your account has been approved. Once approved, you can also invite other users from your company, as we’ll see in a moment.

## *Log in to ELD Provider Portal*

Once you have your approved ELD Provider Account, you will be able to log into the ELD Provider Portal. To log in, you’ll click the “Log In” button in the top right corner of the site, or below the title on the ELD Providers page.

Enter the credentials you used to create the account in the ELD Provider Portal Login area, which is on the left-hand side of the screen.

##

## *Inside the ELD Provider Portal*

Once you are logged in, you can also invite other users from your company to register by selecting “Invite User.”

## *Invite New User*

Inviting new users will allow multiple employees from your company to access or edit your device listings. To invite a user, you will enter the email address of the user, and then click “Send Invite.” This will generate an email inviting the user to create their ELD provider account, which will automatically be associated with your company. This will also set you up as the “admin” for your company. As the admin, you can click on “Manage Company Accounts” to view and edit accounts associated with your company.

# Public Keys

## *Referencing the Handbook*

Provider certificates, which must include a public key, are vital to completing both the telematics and local transfer options for submitting ELD data. The following information is excerpted from the ELD Interface Control Document and Web Services Development Handbook, which is available on the “Develop and Test Your Device” page in the logged-in section of the ELD Provider Portal.

## *ELDs and Public Keys*

### Compliance

All providers will need a public/private key pair for their ELDs. The Public/Private Key pair must be compliant with the NIST SP800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure.

### Pairs Per Provider

Key pairs do not have to be unique for individual devices-the same public/private key pair can be used by a provider for all ELD devices. However, each provider must have their own public/private key pair, as they may not be shared by providers.

### Registration

Providers must register the public key portion of the public/private key pair registered

with their ELD. This is done by submitting a vendor certificate containing the public key during the device registration process. We’ll see this later in the training.

## *Vendor Certificates*

### Compliance

Submitting a vendor certificate containing the public key is a required step in the ELD registration process per Section 5.2.2.

### Obtaining Certificate

Providers may purchase a certificate from a certificate authority, or may use a self- signed certificate. When requesting a certificate from a CA or generating a self-signed certificate, providers must make certain the certificate adheres to best practices as detailed in Section 2.2.1 of the ELD Interface Control Document and Web Services Development Handbook.

### When to Use

You will use your certificate in a few cases. First, when connecting to the FMCSA ELD Web Service to submit ELD data. Next, when electronically signing emails when submitting ELD data to FMCSA using the email data transfer method. And finally, when calculating ELD Authentication Values while generating ELD files for all data transfer methods.

### Expiration

FMCSA will honor the expiration date listed in providers’ certificates. Should an ELD device submit data using an expired certificate, FMCSA will consider the device to be out of compliance with the ELD rule. You will submit your certificate when you register your ELD with FMCSA, as we will see in a few minutes.

# Testing Your ELD

## *Testing Your ELD Files*

Before registering your device, you must ensure that it is fully compliant. One step in this process is to make sure the ELD output file conforms to the technical specifications in the ELD rule. To assist with this, FMCSA offers a File Validator.

Using the File Validator is not a mandatory step of the self-certification process. ELD providers are encouraged to use this tool to help the self-certification process go as smoothly as possible.

You can access the File Validator regardless of whether you are logged in or not, however logging in will help you view your test files later on, as we’ll see in a bit.

In this example, we’ll navigate to the ELD website and log in. You can access the file validator a few ways from this page. There’s a link in the ELD providers dropdown menu. There is also a quick link on the right side of the page. And finally, you can scroll down and click the File Validator button.

## *Using the FMCSA File Validator*

On this page, you’ll find a short description of the file validator and its purpose, as well as step- by-step instructions for using it.

Before we test a file, let’s review the tips shown here. First, remember to start small. Use a simple output file with two or three events. This will help identify any basic issues that need resolving before more complex problems can be identified.

Next, check files often as you resolve issues. A second check may detect issues that were not detectable during an initial check.

When using this tool, remember that the File Validator will only validate the technical specifications of an ELD file, not the file’s content. The File Validator does not check for violations of FMCSA’s Hours-of-Service regulations, as these will be determined by enforcement personnel’s interpretation of the data after it has successfully transferred through FMCSA’s systems.

## *Uploading Files and Getting Results*

To begin using the File Validator, locate the file upload area on this page and click “Browse” to find the file you want to test. Select the ELD file from your computer and click “Open” to upload it. Click “Check” to run the uploaded file through the File Validator.

The results summary will appear at the bottom of the page. Use the Validation Key to understand the results. Similar errors are grouped together, click the plus signs to see more details. Use the information provided to resolve the issues in the file. If you have questions about the File Validator results, contact ELDTech@dot.gov.

Now that we’ve reviewed how to use the File Validator, let’s learn more about testing your device’s ability to transfer ELD data.

## *Testing Data Transfer*

Before you can self-certify that your device is a compliant ELD, you must ensure that it is capable of transferring the output file to the ELD Web Service. This is required to support both the Telematics and Local Transfer options.

FMCSA’s “ELD Data Transfer Requirements” job aid includes step-by-step instructions on how to test each of the four data transfer methods. You can download this job aid from the ELD Providers page of the ELD website.

## *Flagging Test Files*

FMCSA has enabled the ability to set a “test” flag when submitting test ELD files to the Web Service. Set this to ensure that these test submissions will not be treated by FMCSA as true ELD files, which would fail the file validation process as a result of the device not yet being on FMCSA’s list of registered, self-certified ELDs.

## *Enforcement View of Test Files*

Once you have successfully submitted ELD Output Files to FMCSA, you will be able to see how safety officials will view these files. It is important to ensure that your device is accurately recording and transferring hours of service data, and properly presenting that data to a safety official upon request. You can access the enforcement view of your test ELD files in two ways.

### From File Validator Archive

Files you have submitted to the FMCSA File Validator while logged into your ELD Provider account will be accessible in your File Validator Archive. Here, you can access the enforcement view of these files.

### From ELD Successful Test Submission

You can access the enforcement view of files that have been successfully submitted to the FMCSA Web Services test environment in your ELD Test Output Files. To access the enforcement view, these test files must be tagged with the ELD Identifier and ELD Registration ID your company has on file with FMCSA.

# Register and Manage Your ELD Listing

## *FMCSA's ELD List*

The FMCSA ELD website hosts the official list of registered devices that have been self-certified by providers as meeting the technical specifications in the ELD rule.

Motor carriers are required to select a device from this list when purchasing ELDs. By ensuring your device listing is complete and up-to-date, you can offer potential customers details to help determine if your device will meet their needs. Safety officials may also use this list to determine if a driver or motor carrier is using a compliant device.

For your device to be listed, you will need to register it with FMCSA on the ELD website.

## *Register and Self-Certify Your ELD*

To register your device, log in to the ELD Provider Portal and select “Register Your ELD” from the bottom of page or on the side navigation.

Section 5.2.1 of the technical specifications in the ELD rule lists the information that all ELD providers are required to provide to FMCSA when registering devices. This includes:

* Product name
* Model number
* Software version
* ELD Identifier (see Section 7.15 for details on this)
* Picture or screen shot of device
* User’s manual describing how to operate the ELD
* Description of the supported and certified data transfer mechanisms, along with step- by-step instructions for a driver to produce and transfer ELD records to a safety official
* Summary description of ELD malfunctions
* Procedure to validate an ELD authentication value (see Section 7.14 for more details)
* A Certifying statement describing how the product was tested to comply with FMCSA regulations

This is also where you will provide the required Public Key Certificate.

## *Manage Your Device Listing*

The information we just outlined is required for “each ELD model and version.” This means that this information must be updated anytime you update your device or your device’s software.

Maintaining this information ensures that those viewing your ELD listing will have access to the most up-to-date information about your device.

To view and edit your device listings, log in to the ELD Provider Portal and select “Manage Your Device Listing” from the page or “Manage Your Devices” on the left side navigation. You’ll find more details for each listing in the “Actions” column.

To edit a device listing, Select “Edit” for the appropriate device. Select “Replace” to upload any updated files, then click “Agree and Submit” to save changes.

# Is Your Device Compliant?

## *What is the Data Transfer Summary Report*

FMCSA tracks the success and failure rates of all attempted data transfers from ELDs to the Web Service. To help you better detect and diagnose any issues with your ELD output files, FMCSA gives ELD providers access to this information for the devices they have registered with FMCSA.

By logging into the ELD Provider Portal, you will be able to access a history of the successful and unsuccessful data transfers from your device, organized by data transfer method and by motor carrier or customer.

You can also view a list of any issues in your ELD output files which have generated either an “Error” or “Warning” message for the safety official attempting to open and review the file. These are issues you will need to resolve to ensure that your device is compliant with the technical specifications in the ELD rule, which is a requirement for remaining on FMCSA’s list of registered, self-certified devices.

## *Access Data Transfer Summary Report*

To view your Data Transfer Summary Report, first into the ELD Provider Portal. Click “Manage Your Devices” in the left side navigation. Select a device by clicking on the device name or the “Detail” button. This will bring up the device detail page. At the top of the page, click on the “Data Transfer Summary” hyperlink to view the summary report for that device.

## *Web eRODS*

eRODS, or Electronic Records of Duty Status, software is used by safety officials to view data transferred from an ELD to determine if hours-of-service violations are present. A web-based version of the eRODS software is also available on the FMCSA ELD website. You can use this web-based version to see the enforcement view of your registered ELD’s output files. To access Web eRODS click the Web eRODS button in the top navigation. Here, you will be able to upload and view your saved ELD files.

## *ELD Files in Web eRODS*

Opening this file allows you to see what a safety official will see upon opening the transferred ELD file.

Using Web eRODS is recommended to ensure that there are no issues with your ELD output file that is preventing the proper display of the recorded data. Resolving these issues could help your customers avoid violations, which could result in fines or drivers being placed out-of- service.

## *How FMCSA Responds to Reported Issues*

When FMCSA receives notice of a registered ELD that does not meet the minimum requirements in the ELD rule, this begins the following process:

* First, the ELD Technical Team reviews the issue and does any necessary background research.
* Once the Technical Team has determined the root cause of the issue, they will reach out to the provider via email to make them aware of the issue(s) with their device(s), list some recommended and required next steps, and request a response. If the provider does not respond, the technical team will also follow up via a phone call.
* The Technical Team will provide guidance to the provider, but it is ultimately the provider’s responsibility to resolve their device issues in a timely manner.
* The issue will be closed when the provider successfully resolves their device’s issues.

At any time during this process, the issue may be escalated to FMCSA to initiate the process delineated in Section 5.4 of the technical specifications of the ELD final rule, which details the five-step process for removing a device from the list of registered, self-certified devices. To avoid this process, providers must demonstrate to FMCSA their progress toward resolving any device issues.

# Help and Resources

## *Resources from FMCSA*

If you have issues you encounter in developing and testing your device, FMCSA is here to help. First, be sure to consult the resources listed here.

1. Read and understand the technical specifications in the ELD rule.
2. Run your ELD output files through FMCSA’s File Validator.
3. If your device supports telematics, use the web services and email test procedures provided by FMCSA to ensure your device is able to successfully transfer files to the Web Service. Full details are in the ICD/Web Development Handbook in the ELD Provider Portal.
4. Check the safety official view of test files you have successfully submitted via the test procedures, or successfully run through the file validator, and compare them to your ELD display. Log into the ELD Provider Portal for more details.
5. For issues with registered ELDs, check your Data Transfer Summary Report.
6. Consult the ELD Technical Specification Frequently Asked Questions.
7. If you still have questions, contact ELDTech@dot.gov for assistance on resolving your technical issues.

## *Tech Spec FAQs*

As you develop and test your device, remember to visit the ELD Provider Website for plenty of helpful information.

In particular, you’ll be able to access frequently asked questions regarding technical specifications, which are intended to aid you in providing devices to motor carriers that are fully functional and in compliance with the ELD rule. Below that, you’ll also find the latest News for ELD providers. And of course, you’ll be able to access the ELD Provider Portal when you’re logged in and find important resources in the “Develop and Test Your Device” section.

If you have consulted all these resources and still have questions, you can also contact the ELD Technical Team at ELDTech@dot.gov.