U.S. Department of Transportation
Federal Motor Carrier Safety Administration

DRUG & ALCOHOL CLEARINGHOUSE

Web Services Development Handbook For State Driver Licensing Agencies

Version 1.7

Prepared By:

Federal Motor Carrier Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

May 2024

Revision History

Revision Number	Version	Description of Change	Revision Date
1	Draft 1.0	Initial Draft	March 2022
2	Draft 1.1	• Addition of a certificate-based option for self-generation of JWTs. • Updates to driver element. • Details on elements to be included in push notifications.	April 2022
3	1.2	• Updates to the driver element. • Updates to push attributes. • Addition of new REST actions.	June 2022
4	1.3	• Minor corrections based on AAMVA feedback. • Inclusion of Rescinds element in REST request responses to bring it into alignment with push notification. • Addition of an error reporting service. • Update to the pull by date service to target notification dates rather than creation dates.	March 2023
5	1.4	• Example test cases and test endpoints added. • Portal authentication endpoint marked deprecated.	February 2024
6	1.5	• Clarification of ISO 8601 Format.	March 2024
7	1.6	• Addition of “ping” example CDLs for TEST and PROD service. • Demo access request using Postman. • Cleanup of document formatting. • Descriptions of common errors responses and how to debug them, including an explanation of the 404 response for a driver lookup.	May 2024
8	1.7	• Highlighting of a typo in one of the attributes available for notifications delivered to a POST endpoint. • Addition of information on default POST notification retry policies and flow limits.	May 2024

List of Definitions

Term	Definition
JSON	A data interchange format used to store object data as a string.
JSON Web Token (JWT)	A token composed as a JSON object for providing user authentication.
Public Key Certificate	A file containing the public key component of the public/private key pair along with expiration and issuance data.
Public/Private Key Pairs	Also known as asymmetric keys, public/private key pairs are used for encrypting and decrypting data, as well as signing and verifying electronic signatures. Public keys can be distributed to anyone who requests them, while private keys must be kept private and secure.
State(s)	All of the States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, American Samoa, Guam, and the Virgin Islands.

List of Abbreviations

Acronym	Definition
AAMVA	American Association of Motor Vehicle Administrators
CDL	Commercial driver's license
Clearinghouse	FMCSA CDL Drug and Alcohol Clearinghouse
CLP	Commercial learner's permit
CMV	Commercial motor vehicle
DOT	Department of Transportation
FMCSA	Federal Motor Carrier Safety Administration
ICD	Interface Control Document
JSON	JavaScript Object Notation
JWT	JSON Web Token
REST	Representational state transfer
RTD	Return-to-duty
SDLA	State Driver Licensing Agency
SOR	State of Record
SNS	Amazon Simple Notification Service
UTC	Coordinated Universal Time

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose and Scope

This Web Services Development Handbook has been prepared by the Volpe National Transportation Systems Center (Volpe Center) for the Federal Motor Carrier Safety Administration (FMCSA) to guide and support States with the development of systems that will receive and retrieve driver status in the Drug and Alcohol Clearinghouse.

This handbook is for use by States who intend to set up a direct connection between their State IT systems and the Clearinghouse.

This handbook covers the following steps that States, or their third-party vendors, will need to take:

- Request an SDLA portal account.
- Interface with the Clearinghouse web service, which requires you to:
    - Authenticate with the service.
    - Submit requests for information.
    - Interpret service responses.
- Register for push notifications from the Clearinghouse push service.
- Receive and decode messages from the Clearinghouse push service.

1.2 About the Clearinghouse

FMCSA's Commercial Driver's License (CDL) Drug and Alcohol Clearinghouse (Clearinghouse) is a secure online database that gives employers, FMCSA, and State Driver Licensing Agencies (SDLAs) real-time information about CDL/CLP holder drug and alcohol program violations. The Clearinghouse improves safety on our Nation's roadways by making it more difficult for drivers to conceal their drug and alcohol program violations from current or prospective employers.

1.3 Background

The Moving Ahead for Progress in the 21st Century Act (MAP–21) mandated that the U.S. Department of Transportation establish, operate, and maintain a national clearinghouse for records relating to alcohol and controlled substances testing of commercial motor vehicle (CMV) operators. MAP-21 also required that States request information pertaining to the individual from the Clearinghouse before completing certain licensing transactions.

The first Clearinghouse final rule entitled Commercial Driver's License Drug and Alcohol Clearinghouse, was published on December 5, 2016. This rule established the requirements for the Clearinghouse, including the requirements for reporting CDL/CLP holder drug and alcohol program violations, and requirements for employers to query the Clearinghouse to determine if a driver they hire or are considering hiring is prohibited from operating a CMV due to an unresolved drug and alcohol program violation. This rule was implemented on January 6, 2020, when the Clearinghouse became fully operational.

On October 7, 2021, the second Clearinghouse (Clearinghouse-II) final rule, entitled Controlled Substances and Alcohol Testing: State Driver's Licensing Agency Non-Issuance/Downgrade of Commercial Driver's License, was published. This rule established the Clearinghouse requirements for SDLAs. Beginning November 18, 2024, SDLAs must query the Clearinghouse before issuing, renewing, upgrading, or transferring CDLs and CLPs, and to review a driver's information when notified by the Clearinghouse of a status change. SDLAs will be required to remove the CLP or CDL privilege from the driver's license of an individual subject to the CMV driving prohibition, which would result in a downgrade of the license until the driver complies with the return-to-duty (RTD) requirements.

1.4 Roles and Responsibilities

FMCSA, employers, drivers, service agents, and States all play important roles in the implementation of the second Clearinghouse final rule. See the table below for a brief overview of these roles and responsibilities.

Table 1-1. Roles and Responsibilities

FMCSA	• Develop and maintain the Clearinghouse. • Support state agencies adoption of Clearinghouse-II technical requirements.
Employers, MROs	• Register and create a Clearinghouse user account. • Submit violation information, as required. • Report negative RTD tests. • Employers only: Query Clearinghouse to determine if a CDL/CLP holder is prohibited from operating a CMV when hiring, and at least once annually.
SAPs	• Record CDL/CLP holder RTD information, including the date when a driver is eligible for RTD testing
SDLAs	• Query Clearinghouse data to verify a driver is not in a prohibited status before issuing, renewing, upgrading, or transferring CDLs and CLPs. • Query Clearinghouse data when notified by the Clearinghouse of a status change. • Remove CLP or CDL privilege from the driver's license after receiving notification of prohibited status; record downgrade on the CDLIS driver record within 60 days of receiving notification. • Reinstate commercial driving privilege to the driver's license and expunge the driving record accordingly when notified that an erroneous violation has been removed from the Clearinghouse. • Reinstate commercial driving privilege to the driver's license when notified that the driver is no longer in the prohibited status (obtained negative RTD test result).

AAMVA	• Update CDLIS state procedures manual. • Define CDLIS updates to support States requesting and receiving Clearinghouse data via CDLIS.
Drivers	• Register and create a user account and respond to electronic consent requests from employers (consent not required for SDLA queries).

2 Accessing the Clearinghouse

Authorized employees of SDLAs must use their FMCSA Portal accounts to access the Clearinghouse. Portal accounts are user-specific, which means that anyone logging in to the Portal should have their own unique user ID and password; an SDLA may not allow multiple users to log in using the same Portal account. Review the information below to learn about the FMCSA Portal and how to register for an account, if needed.

If you already have an FMCSA Portal account but have not yet requested the Portal Clearinghouse user role, download the Portal Clearinghouse User Role job aid.

You may log in to the Clearinghouse once you have an SDLA Portal account with the Clearinghouse Portal user role.

2.1 Authenticating Web Service Requests

All requests to the Clearinghouse's representational state transfer (REST) service will be secured using a JSON web token (JWT) and bearer authentication. The JWT will be generated by submitting valid Portal credentials to a REST endpoint or using a client certificate issued to an organization by the Clearinghouse.

2.1.1 *Deprecated: Generating a JWT with Portal Credentials*

As part of the migration to enforce MFA for all systems utilizing usernames and passwords, the ability to generate a JWT using FMCSA Portal credentials has been deprecated.

> ***If you had been planning to make use of this method of obtaining a JWT, you should instead use the method outlined in 2.1.2 Generating a JWT Using a Client Certificate.***

2.1.2 *Generating a JWT Using a Client Certificate*

SDLAs that wish to use this option will log in to the Clearinghouse web interface and generate access credentials. These credentials will consist of three parts:

1. A unique identifier for the issued credentials.
2. A certificate that will be used by FMCSA to verify that messages submitted by your service are coming from you.
3. A private key that pairs with this certificate.

Be sure to save your private key and keep it protected as you would an account password. FMCSA will not maintain a copy of your private key. If you lose it, you will need to generate new credentials.

2.1.2.1 Creating the JWT

When composing a request to the REST service, the client will need to generate a JWT with the following characteristics:

- Header must include the following claims:
    - "alg" (Algorithm) – must use the RS256, RS384 or RS513 signing algorithm

    - “typ” (Type) – must be set to JWT
- Payload must contain the following claims:
    - “nbf” (Not Before) – must be the current time or later with a 5 minute skew for clocks out of sync. The value must be provided as a Unix timestamp.
    - “exp” (Expiration) – must be no greater than 20 minutes after the “nbf” value and must not be in the past, plus a 5-minute skew for clocks out of sync. The value must be provided as a Unix timestamp.
    - “iss” (Issuer) – identifier for the credentials used to sign the token that has been issued by FMCSA in the generation process described in section 2.1.2.
- Must be signed using the private key generated in the process described in section 2.1.2 of this document.
- Payload may contain the following optional claim:
    - “sub” (Subject) – for tracking purposes, the client may pass a local identifier, which will be used to further identify actions performed by the service call. This value must be a URL encoded ASCII string with a maximum of 250 characters.

3 Retrieving Driver Status Date from FMCSA

FMCSA will provide a REST service to allow States to search for and retrieve driver status data from the Clearinghouse. The REST service will provide the ability to search for a driver or drivers by State and license number, prohibited status, and date of status change. Request and response bodies will use JavaScript Object Notation (JSON) formatting.

States will access the service using the credentials issued by FMCSA to generate a JWT and include this token in the request.

3.1 Endpoints

States may use the same or separate certificates to connect to the production and test endpoints. Both endpoints are accessible via the public internet and do not require any whitelisting for access.

- Production: https://clearinghouse.fmcsa.dot.gov/api
- Test: https://clearinghouse.fmcsa.dot.gov/api/test (see 5)

3.2 JWT Inclusion

The JWT defined in 2.1 should be included in all service requests using the bearer authentication header. Specifically, a header should be included in the request with the key “Authorization” and value “Bearer <JWT Token>”.

3.2.1 *Responses*

The Clearinghouse web service will notify the client of success or error using the HTTP response codes as defined in Table 3 1. Request Response Codes.

Table 3-1. Request Response Codes

Code	Description
200	Request was processed successfully.
400	The format of the request was invalid. Details of the issue will be provided in a RFC 7807 compliant JSON response body.
401	Bearer JWT token was not found or was rejected. Details will be returned in the x-amzn-Remapped-WWW-Authenticate header.
403	User was authenticated but tried to access a resource to which they did not have permission.
404	Requested resource was not found. In the case detail action, this would indicate that no driver information was found for the supplied ID.
405	Incorrect verb was used when calling the action.

Code	Description
415	Content type header was excluded or not set to “application/json”.
500	Internal server error. Details of the issue will be provided in a RFC 7807 compliant JSON response body.

3.2.2 *Health Check*

The current health of the Clearinghouse service can be queried by performing a GET request on the path “/api/Health". A response with a status code of 200 that begins with the text “healthy” indicates the service is healthy with network and database connectivity.

3.2.3 *Access Checks*

In addition to a basic health check, which can confirm that the service is up and running, consumers can validate their service connection in both TEST and PROD by submitting a status check on a fake CDL number loaded into each environment.

3.2.3.1 Test

> ***/Driver/ByNumber/US-XX/XXZZTESTZZXX***


```
[
    {
        "State": "US-XX",
        "Number": "XXZZTESTZZXX",
        "FirstName": "XXZZTESTZZXX",
        "LastName": "XXZZTESTZZXX",
        "DateOfBirth": "2000-01-01",
        "DriverId": "2f7eda50-2fb0-4276-8680-9a6a57470b32",
        "Id": "f1a17136-679b-4274-b59d-998ec2288aa6",
        "IsProhibited": false,
        "Current": true,
        "StatusDate": "2024-03-27T19:56:04.133184Z",
        "NotificationSentOn": "2024-11-18T00:00:00Z",
        "Rescinds": []
    }
]
```


Figure 3-1. Expected Test Service Response

3.2.3.2 Production

> ***/Driver/ByNumber/US-XX/XXZZPRODZZXX***

```
[
    {
        "State": "US-XX",
        "Number": "XXZZPRODZZXX",
        "FirstName": "XXZZPRODZZXX",
        "LastName": "XXZZPRODZZXX",
        "DateOfBirth": "2000-01-01",
        "DriverId": "a15239e0-26be-4d22-b990-606d7547578f",
        "Id": "88e99ca1-886d-4e34-9db5-97034d76f603",
        "IsProhibited": false,
        "Current": true,
        "StatusDate": "2024-11-18T00:00:00Z",
        "NotificationSentOn": "2024-11-18T00:00:00Z",
        "Rescinds": []
    }
]
```


Figure 3-2. Expected Production Service Response

3.3 Driver Element

All successful requests to the Clearinghouse web service will return one or more (up to 100 at a time) driver elements.

Table 3-2. Driver Status Element

Attribute Name	Description	Requirements
DriverId	Unique identifier for the driver in the Clearinghouse	GUID in the format 00000000-0000-0000-0000-000000000000.
Number	Number used to identify CDL or CLP issued by the SDLA.	Up to 25 characters in length.
State	Country and subdivision code as defined in ISO 3166-2.	Up to 6 characters using a 2-character country code, a dash, and a locality code of up to 3 characters.
FirstName	Given name of the driver.	Up to 100 characters in length.
LastName	Surname of the driver.	Up to 100 characters in length.

Attribute Name	Description	Requirements
DateOfBirth	Date in the ISO 8601 format, including dashes to separate the components.	YYYY-MM-DD
IsProhibited	Driver status within the Clearinghouse. 'true' if the driver is prohibited from driving due to an unresolved drug and alcohol program violation, otherwise 'false.'	true/false
StatusDate	Date and time the driver status went into effect in ISO 8601 format. Date/time will be expressed in coordinated universal time (UTC).	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision
Current	'true' if the returned record represents the driver's most recent status. 'False' indicates that the status has changed one or more times since the change represented by this event.	true/false
MarkedErroneousOn	Optional: If supplied, this is the date/time it was determined that the status change entry was based on an erroneous violation entry. In ISO 8601 format. Date/time will be expressed in coordinated universal time (UTC).	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision
NotificationSentOn	If supplied, this is the date/time when the Clearinghouse sent a push notification to the State indicating the status change had occurred. In ISO 8601 format. Date/time will be expressed in coordinated universal time (UTC).	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision
Rescinds	Optional: This element will contain the id values (see id attribute in this table) of previously-entered status changes that have been determined to be the result of erroneous data entry. A notification containing rescinded ids indicates that the State may need to reinstate a driver's commercial driving privilege or purge data from State systems. In	An array of GUID values in the format 00000000-0000-0000-0000-000000000000.

Attribute Name	Description	Requirements
	these scenarios, we recommend that the State review the driver's full status history to determine the correct course of action. Note: The attribute that is excluded, the attribute present with an empty value assigned, and the attribute assigned an empty array should all be treated equivalently.	

3.3.1 *Driver Information Source*

When data is entered into the Clearinghouse, the driver's license information will be checked against the State of Record using the Commercial Driver's License Information System (CDLIS). Alias information returned by the state of record (SOR) will be used to merge new and old license values into a single internal driver record. The license number, name, and date of birth values returned will represent the CDL/CLP information associated with the driver that was most recently validated successfully.

3.3.2 *Notification Dates*

Historical driver status tracking is a new Clearinghouse feature being added to support the Clearinghouse-II final rule implementation. As a result, all notification values in the system will have an epoch of <TBD> and any driver with a notification date of <TBD> can be presumed to have received that status some time prior to that date.

If a state query is conducted against a CDL/CLP which is not yet recorded in the system, the Clearinghouse will conduct a new query and assign the driver status data with the current date and time.

3.4 Driver Status Requests

FMCSA is currently supporting the query of driver status using 4 search functions:

- Driver ID
- Country/subdivision and license number
- Country/subdivision and prohibited status
- Country/subdivision and status date

All 4 functions will return an array of driver elements as defined in Table 3 2. Driver Element. For searches by prohibited status and date, results will be returned 100 elements at a time. A search by country/subdivision and license number or driver ID will offer the option of retrieving either the driver's current status or status history, depending on action used.

3.4.1 *Search by Driver ID*

A search by driver ID can be used to complement an email-based push notification or to quickly re-query a driver's status once an ID has previously been obtained. A driver ID will never be re-used but may become inactive if the system identifies a second license number or set of license numbers which need to be merged into a single driver record. When this happens one of the driver records remains and the other is removed. A search by driver ID is guaranteed to return results for a single driver.

Table 3-3. Search by Driver ID Request Parameters

Parameter Name	Description	Requirements
DriverID	Unique identifier for the driver in the Clearinghouse	GUID in the format 00000000-0000-0000-0000-000000000000.

3.4.1.1 Paths

Driver search by Id can return the driver's current status as well as their status history.

> ***Current Value: Driver/ById/{DriverID}***
>
> ***History: Driver/History/ById/{DriverID}***

3.4.2 *Search by Country/Subdivision and License Number*

A search by country/subdivision and license number is expected to return only a single driver record, as license number and State uniqueness are internally enforced.

Table 3-4. Search by Country/Subdivision and License Number Request Parameters

Parameter Name	Description	Requirements
Number	Number used to identify a CDL or CLP issued by the SDLA.	Up to 50 characters in length.
State	Country and subdivision code as defined in ISO 3166-2.	Up to 6 characters using a 2-character country code, a dash, and a locality code of up to 3 characters. Any code defined in ISO 3166-2:US, ISO 3166-2:CA, and ISO 3166-2:MX

3.4.2.1 Paths

Driver search by country/subdivision and number can return the driver's current status, as well as their status history.

Current Value: Driver/ByNumber/{State}/{Number}

History: Driver/History/ByNumber/{State}/{Number}

3.4.3 *Search by Country/Subdivision and Prohibited Status*

A search by country/subdivision and prohibited status is expected to return a listing of all drivers currently in a prohibited status. The results will be returned in a paged result set ordered by the date the driver status was changed to prohibited and then by driver ID.

Table 3-5. Search by State and Prohibited Status Request Parameters

Parameter Name	Description	Requirements
State	Country and subdivision code as defined in ISO 3166-2. Implementation will restrict access to only country subdivisions to which an organization has been granted access.	Up to 6 characters using a 2-character country code, a dash, and a locality code of up to 3 characters. ISO 3166-2:US code representing one of the 50 states or DC.
Page	Page number for the returned results were 1 is the number of the first page.	An integer value of 1 or more

3.4.3.1 Path

Driver/Prohibited/{State}/{Page}

3.4.4 *Search by Country/Subdivision and Status Date*

A search to return a listing of all driver status changes in a country/subdivision over a given period. The results will be returned in a paged result set ordered by the date the driver status was changed and then by driver id.

Table 3-6. Search by Country/Subdivision and Notification Date Request Parameters

Parameter Name	Description	Requirements
State	Country and subdivision code as defined in ISO 3166-2. Implementation will restrict access to only country subdivisions to which an organization has been granted access.	Up to 6 characters using a 2-character country code, a dash, and a locality code of up to 3 characters. ISO 3166-2:US code representing one of the 50 states or DC.

Parameter Name	Description	Requirements
NotificationDateFrom	Date and time of the driver status notification was created in ISO 8601 format. Date/time must be sent in UTC.	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision
NotificationDateTo	Date and time of the driver status notification was created in ISO 8601 format. Date/time will be expressed in UTC.	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision
Page	Page number for the returned results where 1 is the number of the first page.	An integer value of 1 or more

3.4.4.1 Endpoint

Driver/ByDate/{State}/{StatusDateFrom}/{StatusDateTo}/{Page}

3.5 Error Reporting

A function to allow an SDLA to submit an error report indicating they are not able to process a particular status change. Status changes which have errors will be flagged for manual follow-up.

Table 3-7. Error Submission Request Body

Attribute Name	Description	Requirements
StatusChangeId	Unique identifier for this status change event that could not be processed.	GUID in the format 00000000-0000-0000-0000-000000000000.
Type	High level category for the error event.	One of: • InvalidFormat • NotCurrentSOR • InvalidDriver • NotCDLCLPHolder • Deceased • Other
Description	Optional: Text description of the error.	String up to 1000 characters in length

3.5.1 *Path*

> ***Driver/Status/Error***

4 Receiving Data From FMCSA

The Clearinghouse will provide States with the ability to receive push notifications on driver status change. Notifications will be delivered using the Amazon Simple Notification Service (SNS). States will be able to register to receive notifications via email (JSON or text) or POST endpoints. All push mechanisms will require a confirmation step for use. This will involve accessing a link delivered via email or POST, depending on the push mechanism selected.

> ***Note: push notifications will only be used to send status change notifications for drivers licensed in one of the 50 States or DC. Driver status may be queried for drivers in US territories, Mexico or Canada, but no status change push notifications will be sent for these drivers.***

4.1 POST Endpoint

To receive machine-to-machine push notifications to a POST endpoint, States will need to supply a publicly accessible endpoint that is accessed over HTTPS. In addition, States may choose to implement basic or digest access authentication to secure the endpoint.

Once configured, there may be a required confirmation step before the endpoint can be activated.

4.1.1 *Confirmation*

To begin receiving push notifications, you must be able to respond to subscription confirmation messages by accessing the link from the attribute “SubscribeURL”. This may be done either within the application or via a manual mechanism and will be required for each State topic.

4.1.1.1 Example


```
{
  "Type": "SubscriptionConfirmation",
  "MessageId": "769129a2-539d-4565-8455-f0587f03eed6",
  "Token":
"2336412f37fb687f5d51e6e2425dacbba931e5f40e20eb015ee444dc9207cda1135670b4c720fa896ba92
e55b95b19446517134e24c0d4cd6472f93d2d75d2b2a0880ceafeac21e13bb70ac0b7fac9432670777317f
6bc492cc0cd56c5680bf0419fca83d8c09a676582329ccbdf6c441f04610096c598fab133fb5c63080eed"
,
  "TopicArn": "arn:aws:sns:us-east-1:423271844905:DACH-Dev-US-MA",
  "Message": "You have chosen to subscribe to the topic arn:aws:sns:us-east-
1:423271844905:DACH-Dev-US-MA.\nTo confirm the subscription, visit the SubscribeURL
included in this message.",
  "SubscribeURL": "https://sns.us-east-
1.amazonaws.com/?Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-east-
1:423271844905:DACH-Dev-US-
MA&Token=2336412f37fb687f5d51e6e2425dacbba931e5f40e20eb015ee444dc9207cda1135670b4c720f
a896ba92e55b95b19446517134e24c0d4cd6472f93d2d75d2b2a0880ceafeac21e13bb70ac0b7fac943267
0777317f6bc492cc0cd56c5680bf0419fca83d8c09a676582329ccbdf6c441f04610096c598fab133fb5c6
3080eed",
  "Timestamp": "2022-06-27T16:19:30.559Z",
  "SignatureVersion": "1",
  "Signature":
"ULFBcX7ljIPgwMWpiK/QDoAQAEZFyNPkRxlgYXC30sXvmA1fd7Ggabq+7pSDJOZt8afKaS/CFipypARLQLn/I
GrcJHLb9whYiF8wFMWRXluKnEk2DV7NmyeaWEYpQyZfAAEn7yvsbmYfnYVr7JfPzTQ9yhsibfZuzvdiyBi7H2/
XPIN1w/Y5GqE1Ia4WR3T4XvAAk2KTJEhX+TqQuxEzN5KjvDer1HLE2uPeZH/xYKh0jTt0nKkT7CVcjbf2pg09H
KRiZg3/yuPrboA5d6Ork24lNPSRsOGBuEKFWATXhQe0N9MAUAWb3NGZ12QPjHuPj37d/HXpcTnUB4v5GCTumg=
=",
  "SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
7ff5318490ec183fbaddaa2a969abfda.pem"
}
```


Figure 4-1. Example subscription confirmation body

4.1.2 *POST Body*

A driver status change message will be delivered to a subscribed POST endpoint as the message body in JSON format. The message will consist of the attributes described in Tables 4-1 and 4-2.

Table 4-1. POST Endpoint Notification (more information)

Attribute Name	Description	Requirements
Message	An encoded JSON string containing the attributes defined in Table 4-2.	String (JSON)
MessageId	A Universally Unique Identifier, unique for each message published. For a notification that Amazon SNS resends during a retry, the message ID	GUID in the format 00000000-0000-0000-0000-000000000000.

Attribute Name	Description	Requirements
	of the original message is used.	
Signature	Base64-encoded SHA1withRSA signature of the Message, MessageId, Subject (if present), Type, Timestamp, and TopicArn values. Details on how to verify the signature can be found in the SNS Developer's Guide	String
SignatureVersion	Version of the Amazon SNS signature used.	String
SigningCertURL	The URL to the certificate that was used to sign the message.	Url
Timestamp	The time (GMT) when the notification was published.	YYYY-MM-DDTHH:mm:SS.sssZ
TopicArn	The Amazon Resource Name (ARN) for the topic that this message was published to.	String in the format arn:aws:sns:<Region>:<AWS Account ID>:<Topic Name>:<Subscription ID> Region: typically be us-east-1 but could change in the event of catastrophic AWS failure Account ID: 423271844905 Topic Name: will take the form DACH-Prod-<ISO 3166-2 State Code> Subscription ID: unique id which identifies the specific user for this specific topic
Type	The type of message. For a notification, the type is Notification.	Notification
UnsubscribeUrl	A URL that you can use to unsubscribe the endpoint from this topic. If you visit this	Url

Attribute Name	Description	Requirements
	URL, Amazon SNS unsubscribes the endpoint and stops sending notifications to this endpoint.	
MessageAttributes	List of message attributes containing the structured detailed data of the event.	Object as defined in Table 4-3

Table 4-2. POST Endpoint Message Body

Attribute Name	Description	Requirements
Id	Unique identifier for this particular status change in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.
DriverId	Unique identifier for the driver in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.
Number	Number used to identify CDL or CLP issued by the SDLA.	Up to 25 characters in length.
StateCode	Country and subdivision code as defined in ISO 3166-2. Note: the initial releases version of the push service contains only the 2-character State code. This will be corrected in a future release.	Up to 6 characters using a 2-character country code, a dash, and a locality code of up to 3 characters.
FirstName	Given name of the driver.	Up to 100 characters in length.
LastName	Surname of the driver.	Up to 100 characters in length.
DateOfBirth	Date in the ISO 8601 format, including dashes to separate the components.	YYYY-MM-DD
IsProhibited	Driver status within the clearinghouse. 'True' if the driver is prohibited from	true/false

Attribute Name	Description	Requirements
	driving due to an unresolved drug and alcohol program violation, otherwise 'false.'	
StatusDate	Date and time the driver status went into effect in ISO 8601 format. Date/time will be expressed in coordinated universal time (UTC).	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision
Rescinds	Optional: This element will contain the id values (see id attribute in this table) of previously-entered status changes that have been determined to be the result of erroneous data entry. A notification containing rescinded ids indicates that the State may need to reinstate a driver's commercial driving privilege or purge data from State systems. In these scenarios, we recommend that the State review the driver's full status history to determine the correct course of action. Note: The attribute that is excluded, the attribute present with an empty value assigned, and the attribute assigned an empty array should all be treated equivalently.	An array of GUID values in the format 00000000-0000-0000-0000-000000000000.

Table 4-3. POST Endpoint Message Attributes

Attribute Name	Description	Requirements
Id	Unique identifier for this particular status change in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.

Attribute Name	Description	Requirements
DriverId	Unique identifier for the driver in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.
IsProhibied	Driver status within the clearinghouse. 'True' if the driver is prohibited from driving due to an unresolved drug and alcohol program violation, otherwise 'false.' Note: FMCSA is aware that this attribute name is incorrectly spelled and plans to add a new attribute with the correct spelling ('IsProhibited') in a future update. The incorrectly spelled attribute ('IsProhibied') will be removed at a later date, after FMCSA has confirmed that any consumer using it has migrated to the correctly spelled attribute.	true/false
StatusDate	Date and time the driver status went into effect in ISO 8601 format. Date/time will be expressed in coordinated universal time (UTC).	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision

4.1.2.1 Example


```
{
  "Type": "Notification",
  "MessageId": "c09e706b-ad61-56f6-9fd8-2b58761b830a",
  "TopicArn": "arn:aws:sns:us-east-1:423271844905:DACH-Dev-US-MA",
  "Message": "{\"Id\":\"fdf1c846-1690-4658-b446-
80a2d5567b0b\",\"DriverId\":\"65ce3946-f3de-45c0-bf67-
24516d176f62\",\"StatusDate\":\"2022-06-
27T16:22:18.3604713Z\",\"IsProhibited\":true,\"Rescinds\":[],\"StateCode\":\"MA\",\"Nu
mber\":\"TEST123456789\",\"FirstName\":\"Test\",\"LastName\":\"User\",\"DateOfBirth\":
\"1900-01-01\"}",
  "Timestamp": "2022-06-27T16:22:18.418Z",
  "SignatureVersion": "1",
  "Signature":
"l4BtYrE06J7chZ3LyHOtW4sewQuBoa+2aIs+p5q4fQrkQcmTA1/jpUfuhgsh2rhQqht1cyGSRlTsSjhT4Ecxo
c8+vKYdX4/Q4s+9V5vaCzAnsbjWxX5gFpwYD0vCuU4fVGmy5CQeE2IuT+L/QlTedRyTAIVs8DqufuKo4yIbuhm
A6yEsof60O7bCnRU1/PtEhdnCpfIqgMrNWKWuy2rEmK9nSxt/PZ6XMYCcKmGfyy5tIjjF1qcdLjCWsM2YZIjcp
2UkhWzCIWHokqRuz4Z1l9ABiZqb9puSjxFTqFTBkJ9J1Obwgw39/dE7nWxueEXPMZn6skJLuCfUHSsZfmd2zw=
=",
  "SigningCertURL": "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-
7ff5318490ec183fbaddaa2a969abfda.pem",
  "UnsubscribeURL": "https://sns.us-east-
1.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-
1:423271844905:DACH-Dev-US-MA:4c287588-4165-4e5c-b266-62619e89378e",
  "MessageAttributes": {
    "DriverId": {
      "Type": "String",
      "Value": "65ce3946-f3de-45c0-bf67-24516d176f62"
    },
    "StatusDate": {
      "Type": "String",
      "Value": "2022-06-27T16:22:18.3604713Z"
    },
    "IsProhibied": {
      "Type": "String",
      "Value": "True"
    },
    "Id": {
      "Type": "String",
      "Value": "fdf1c846-1690-4658-b446-80a2d5567b0b"
    }
  }
}
```


Figure 4-2. Example POST endpoint notification body

4.1.3 *Retry Policy*

When delivering notifications to your endpoint, the system will consider any response with a code between 200 and 499 to be a successful delivery. Any code outside this range or a connection failure will be considered a message delivery failure. When a delivery failure occurs, the system will attempt to deliver the message using the following default back-off procedure:

- Two redelivery attempts will be made immediately, without any system-enforced delay.

- 18 redelivery attempts will be made, starting with 20 seconds between each attempt, and then linearly increasing up to 60 seconds.
- 30 redelivery attempts will be made, with 60 seconds between each attempt.

If the message cannot be delivered in this timeframe, it will be marked as "failed" and will require manual review.

If needed for your implementation, this retry policy can be overridden with a custom policy. The policy must fit within the outlines defined in the SNS documentation.

4.1.4 *Flow Limit*

By default, the system is configured to throttle requests to your endpoint to a maximum of 10 notifications per second. If required, this limit can be configured down to a minimum of one notification per second.

> ***Note: In practice, the system rarely exceeds two notifications per second (this has only occurred 31 times in the last two years). Please review the "Driver Status Change Report" available to SDLA users in the Clearinghouse to understand what type of load to expect for your State.***

4.2 JSON Formatted Email

To receive machine-to-machine push notifications via email, States will need to supply an email address to FMCSA for subscription. Once configured, there may be a required confirmation step before the endpoint can be activated.

4.2.1 *Confirmation*

To begin receiving push notifications, you must be able to respond to subscription confirmation messages by accessing the link from the attribute "SubscribeURL". This may be done either within the application or via a manual mechanism and will be required for each State topic.

```
{
  "Type": "SubscriptionConfirmation",
  "MessageId": "64a4f9c1-1027-4662-a273-895aaf681f86",
  "Token":
"2336412f37fb687f5d51e6e2425dacbba931e5f40e20eb015eed004b14ef836fe119cfdf427118ed8d4c
e70903c3501cb61b43769484a3419eb8acad8e68595cb65978a366429e9885c229f206b17194f3f2f1fee
e40a536b2b793528c4dd45548cf8fb955aed90c877fb99f779231972fc5e8b22b81274bb2409568f6b6f8
,
  "TopicArn": "arn:aws:sns:us-east-1:423271844905:DACH-Dev-US-MA",
  "Message": "You have chosen to subscribe to the topic arn:aws:sns:us-east-
1:423271844905:DACH-Dev-US-MA.\nTo confirm the subscription, visit the SubscribeURL
included in this message.",
  "SubscribeURL":
"https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsns.us-east-
1.amazonaws.com%2F%3FAction%3DConfirmSubscription%26TopicArn%3Darn%3Aaws%3Asns%3Aus-
east-1%3A423271844905%3ADACH-Dev-US-
MA%26Token%3D2336412f37fb687f5d51e6e2425dacbba931e5f40e20eb015eed004b14ef836fe119cfdf
27118ed8d4c5e70903c3501cb61b43769484a3419eb8acad8e68595cb65978a366429e9885c229f206b17
94f3f2f1feece40a536b2b793528c4dd45548cf8fb955aed90c877fb99f779231972fc5e8b22b81274bb2
09568f6b6f8&amp;data=05%7C01%7Candrew.nagel%40dot.gov%7Cfe58b5be3bbd4052a3bc08da58578
e9%7Cc4cd245b44f04395a1aa3848d258f78b%7C0%7C0%7C637919430252739423%7CUnknown%7CTWFpbG
sb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%
C&amp;sdata=0K2VzCEP1%2B1cehtSTggSgkk7Nbl3wXQH2PEtflRbnfA%3D&amp;reserved=0",
  "Timestamp": "2022-06-27T16:10:19.247Z",
  "SignatureVersion": "1",
  "Signature":
"QuJMiSgLxXPnf4umsYL0vO9030IXK9Be9m/HGSbHmoadysUmi2ZCW2apjwJc6i+n+fKN82Ro14kKMLsU2W7G
ds3iFaTJu+/e0X2/sqv2x3hV9iniD5J1NGr0dsQ5K+p+4duC8tJ8triYGlFc1U+Iuxx1lrf/qjm9wFhG8qfY/
g0kGPLwZgMqpuqujmVk91Jix7E0YhmNhqyjLACICcFCbazAX56WN5n9ytwpH0T1T3nFVbVf9QndKanYCMcS3R
LKtkNuF0ps105rjAHmP/n3MERO6c5MfnxQW2HxUNIsd20bmYvAvur29sG9ydYQHVApY8tkdkDzPUC4C3eVtxA
=",
  "SigningCertURL":
"https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsns.us-east-
1.amazonaws.com%2FSimpleNotificationService-
7ff5318490ec183fbaddaa2a969abfda.pem&amp;data=05%7C01%7Candrew.nagel%40dot.gov%7Cfe58
5be3bbd4052a3bc08da585789e9%7Cc4cd245b44f04395a1aa3848d258f78b%7C0%7C0%7C637919430252
39423%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJ
VCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=oxB2f%2FpYOpTn9vw5oN1G%2B19Jva6Yram3bDAWJZriI1I%
D&amp;reserved=0"
}
```


Figure 4-3. Example JSON email subscription confirmation

4.2.2 *Message Body*

A driver status change message will be delivered to this email with the message body in JSON format. The message will consist of the attributes described in Tables 4-3 and 4-4. Due to the inherently insecure nature of email communication, no PII will be delivered via this mechanism. States wishing to use email for push notifications will need to pair the push receipt with a call to the driver detail REST service.

Table 4-4. JSON Email Notification (more information)

Attribute Name	Description	Requirements
Message	An encoded JSON string containing the attributes defined in Table 4-4.	String (JSON)
MessageId	A Universally Unique Identifier, unique for each message published. For a notification that Amazon SNS resends during a retry, the message ID of the original message is used.	GUID in the format 00000000-0000-0000-0000-000000000000.
Signature	Base64-encoded SHA1withRSA signature of the Message, MessageId, Subject (if present), Type, Timestamp, and TopicArn values. Details on how to verify the signature can be found in the SNS Developer's Guide	String
SignatureVersion	Version of the Amazon SNS signature used.	String
SigningCertURL	The URL to the certificate that was used to sign the message.	Url
Timestamp	The time (GMT) when the notification was published.	YYYY-MM-DDTHH:mm:SS.sssZ

Attribute Name	Description	Requirements
TopicArn	The Amazon Resource Name (ARN) for the topic that this message was published to.	String
Type	The type of message. For a notification, the type is Notification.	Notification
UnsubscribeUrl	A URL that you can use to unsubscribe the endpoint from this topic. If you visit this URL, Amazon SNS unsubscribes the endpoint and stops sending notifications to this endpoint.	Url
MessageAttributes	List of message attributes containing the structured detailed data of the event.	Object as defined in Table 4-5

Table 4-5. JSON Email Message Body

Attribute Name	Description	Requirements
Id	Unique identifier for this status change in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.
DriverId	Unique identifier for the driver in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.
IsProhibited	Driver status within the Clearinghouse. 'True' if the driver is prohibited from driving due to an unresolved	true/false

Attribute Name	Description	Requirements
	drug and alcohol program violation, otherwise 'false.'	
StatusDate	Date and time the driver status went into effect in ISO 8601 format. Date/time will be expressed in coordinated universal time (UTC).	YYYY-MM-DDTHH:mm:SSZ
Rescinds	Optional: This element will contain the id values (see id attribute in this table) of previously-entered status changes that have been determined to be the result of erroneous data entry. A notification containing rescinded ids indicates that the State may need to reinstate a driver's commercial driving privilege or purge data from State systems. In these scenarios, we recommend that the State review the driver's full status history to determine the correct course of action. Note: The attribute that is excluded, the attribute present with an empty value assigned, and the attribute assigned an empty array should all be treated equivalently.	An array of GUID values in the format 00000000-0000-0000-0000-000000000000.

Table 4-6. JSON Email Message Attributes

Attribute Name	Description	Requirements
Id	Unique identifier for this status change in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.
DriverId	Unique identifier for the driver in the Clearinghouse.	GUID in the format 00000000-0000-0000-0000-000000000000.

Attribute Name	Description	Requirements
IsProhibited	Driver status within the clearinghouse. 'True' if the driver is prohibited from driving due to an unresolved drug and alcohol program violation, otherwise 'false.'	true/false
StatusDate	Date and time the driver status went into effect in ISO 8601 format. Date/time will be expressed in coordinated universal time (UTC).	YYYY-MM-DDTHH:mm:SSZ Optional: between 0 and 6 digits of sub-second precision

4.2.2.1 Example


```
{
  "Type": "Notification",
  "MessageId": "c09e706b-ad61-56f6-9fd8-2b58761b830a",
  "TopicArn": "arn:aws:sns:us-east-1:423271844905:DACH-Dev-US-MA",
  "Message": "{\"Id\":\"fdf1c846-1690-4658-b446-
80a2d5567b0b\",\"DriverId\":\"65ce3946-f3de-45c0-bf67-
24516d176f62\",\"StatusDate\":\"2022-06-
27T16:22:18.3604713Z\",\"IsProhibited\":true,\"Rescinds\":[]}",
  "Timestamp": "2022-06-27T16:22:18.418Z",
  "SignatureVersion": "1",
  "Signature":
"SVgrDb3eeG5vcWKhTrztfPpXaDr/Tf6PXKUCn/tKapZzinE7eocwazQhHV4KsFWUn2v26NCZaIzuMytwJNUQ
5WzvwN3R1RWt6ZhoJX2kCEsmXdPntyzmNpZwmTplI1BEbQn+ba4EttcggJMU9Xjyl2WV/LRkiZlYrDZZwpfRv
z+uZXhJy+D1GpYcJ0KjWlvF5xR/Rw1pQGwZ/C5WS3pt0V7ugQvEkLi6gfRA1trklBJnjPS+ylo0DygaIxrPGN
jPxxeJn/uXE/bROLp5E0v/glP1RCGOWPXbYTdWf5ml/0K0szYHPlnS5VhZ37+0G19CqKnGPR0jth5CU9auoQg
=",
  "SigningCertURL":
"https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsns.us-east-
1.amazonaws.com%2FSimpleNotificationService-
7ff5318490ec183fbaddaa2a969abfda.pem&amp;data=05%7C01%7Candrew.nagel%40dot.gov%7C9db2
696ea734ac45f3808da58593659%7Cc4cd245b44f04395a1aa3848d258f78b%7C0%7C0%7C637919437424
09292%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJ
VCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=s0OK70ws0ZUnr5x0jYqh9Dfv3C1f%2BZ1Iou9TirE5J58%3D
amp;reserved=0",
  "UnsubscribeURL":
"https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsns.us-east-
1.amazonaws.com%2F%3FAction%3DUnsubscribe%26SubscriptionArn%3Darn%3Aaws%3Asns%3Aus-
east-1%3A423271844905%3ADACH-Dev-US-MA%3Ae5d6adba-a6ea-4642-8fb3-
e55eebe2de29&amp;data=05%7C01%7Candrew.nagel%40dot.gov%7C9db21696ea734ac45f3808da5859
659%7Cc4cd245b44f04395a1aa3848d258f78b%7C0%7C0%7C637919437424909292%7CUnknown%7CTWFpb
Zsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C
7C&amp;sdata=HPCn%2BkjI3uljy8bSCQOaGlSOnp7XLcu3hsr17v%2Bz4iI%3D&amp;reserved=0",
  "MessageAttributes": {
    "DriverId": {
      "Type": "String",
      "Value": "65ce3946-f3de-45c0-bf67-24516d176f62"
    },
    "StatusDate": {
      "Type": "String",
      "Value": "2022-06-27T16:22:18.3604713Z"
    },
    "IsProhibied": {
      "Type": "String",
      "Value": "True"
    },
    "Id": {
      "Type": "String",
      "Value": "fdf1c846-1690-4658-b446-80a2d5567b0b"
    }
  }
}
```


Figure 4-4. Example JSON email notification body

4.3 Text Email

To receive machine-to-person push notifications via email, States will need to supply an email address to FMCSA for subscription. Once configured, there may be a required confirmation step before the endpoint can be activated.

4.3.1 *Confirmation*

To begin receiving push notifications, you must be able to respond to subscription confirmation messages by accessing the link labeled “Confirm Subscription”. This will be required for each State topic.

> You have chosen to subscribe to the topic:
> **arn:aws:sns:us-east-1:423271844905:DACH-Dev-US-DC**
>
> To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
> Confirm subscription

Figure 4-5. Example text email confirmation

4.3.2 *Message Body*

When a driver’s status changes, an email will be sent to confirmed addresses indicating the change has occurred. The email will include the date of the change, the ID of the driver, and a link State users can click to retrieve details of the driver record.

> ***Note: The email body below is intended only as an example. The exact message sent with these notifications is intended for a human recipient and may change over time for improved clarity. If you wish to process these emails programmatically, please make use of the JSON formatted email, which will have a consistent format and content.***

> A driver's status has been changed in FMCSA's Drug and Alcohol Clearinghouse. This may require you to update their commercial driver's license (CDL) or commercial learner's permit (CLP) privileges.
>
> Clearinghouse ID: 65ce3946-f3de-45c0-bf67-24516d176f62
> Status changed on 06/27/2022 16:22:18 (UTC).
>
> View the details of the driver's status at
> https://clearingouse.fmcsa.dot.gov/SDLA/Driver/65ce3946-f3de-45c0-bf67-24516d176f62.

Figure 4-6. Example test email notification body

5 Testing Your Connection

For States that will be connecting directly to the Clearinghouse, FMCSA provides different testing mechanisms depending on your connection method:

REST Service—a base set of test data has been pre-loaded to the test service endpoint for each State. These test cases are static and can be used at any time, without needing direct coordination with FMCSA. If States need additional specific test scenarios, they can send a request to the Clearinghouse SDLA inbox (SDLAClearinghouse@dot.gov).

Machine push services (POST endpoint, JSON email)—because these services require an action to be initiated within the Clearinghouse, testing must be coordinated with FMCSA. FMCSA can stage complimentary test data in the test REST service, but the act of pushing emails and POST messages must be initiated by the Clearinghouse team. States looking to utilize these services can reach out to FMCSA using the SDLA inbox (SDLAClearinghouse@dot.gov) to coordinate this testing.

Non-IT solutions (web portal and/or email notifications)—because these are process and not IT changes, the Clearinghouse does not offer a test version of these interfaces.

5.1 Example Test Data

To facilitate the testing process, FMCSA is providing a set of example test data, which will be pre-loaded for each State into the Clearinghouse test endpoint. These example test cases (noted by the assigned CDL number) cover the following scenarios:

- PROHIBITED – driver has a violation recorded in the Clearinghouse and has not completed the RTD process.
- NOTPROHOBITED – driver has not had any violations recorded in the Clearinghouse.
- REPROHIBITED – driver has completed their RTD test on a past violation, after which a new violation was entered into the Clearinghouse.
- RTDCOMPLETE7DAY – driver has a violation recorded in the Clearinghouse and completed their RTD test 7 days after the violation was entered.
- RTDCOMPLETE30DAY – driver has a violation recorded in the Clearinghouse and completed their RTD test 30 days after the violation was entered.
- RTDCOMPLETE90DAY – driver has a violation recorded in the Clearinghouse and completed their RTD test 90 days after the violation was entered.
- PROHIBITEDRESCINDED – driver had a violation entered into the Clearinghouse, which was deemed to be incorrectly entered and was subsequently removed by FMCSA.
- RESCINDEDSTILLPROHIBITED – driver has two violations entered into the Clearinghouse and the oldest of the two was deemed to be incorrectly entered and removed by FMCSA.
- TWORTDS – driver has a violation entered into the Clearinghouse, completed their RTD test, has a second violation entered into the Clearinghouse, and then completes a second RTD test.

See Appendix A for details.

5.2 Base Test Cases

At a minimum, FMCSA expects that States will test each of the following scenarios. Depending on how a State implements their solution, they will very likely need many more test scenarios, but these cover the broad use cases of the rule.

Table 5-1. FMCSA Test Cases

Scenario	Expected Result
Status check on a prohibited driver	State would not issue credential or endorsement.
Status check on a not prohibited driver	State would not be prohibited by the Clearinghouse from issuing the credential or endorsement.
State receives a message indicating a driver has received a new prohibition	Driver CDL must be downgraded within 60 days.
State receives a message indicating a previously prohibited driver is no longer prohibited (due to completing the RTD process)	Driver is now eligible to receive their previous credential.
State receives a message indicating a previous prohibition on a driver was based on erroneously reported data and the driver is no longer prohibited.	Driver should immediately have their previous credential restored.
State receives a message indicating a previous prohibition on a driver was based on erroneously reported data, but the driver is still prohibited due to other existing violations.	If the downgrade process for the driver was already complete, then no action is required. If the downgrade process was not yet complete States may elect to continue the existing process or to restart the process using the receipt date of the new message as the start date of the downgrade process.

Appendix A: Example Test Data

Example Driver Data

Number	First Name	Last Name	Date of Birth
RTDCOMPLETE7DAY	RTD	COMPLETE7DA	1995-03-13
TWORTDS	TWO	RTDS	2000-08-09
REPROHIBITED	RE	PROHIBITED	1989-04-23
PROHIBITTEDRESCINDED	PROHIBITED	REESCINDED	1999-06-30
NOTPROHIBITED	NOT	PROHIBITED	1999-01-10
RTDCOMPLETE30DAY	RTD	COMPLETE30DAY	1990-05-12
PROHIBITED	IS	PROHIBITED	1997-01-10
RTDCOMPLETE90DAY	RTD	COMPLETE90DAY	1997-01-23
RESCINDEDSTILLPROHIBITED	RESCINDED	STILLPROHIBITED	1994-07-25

Example Status Change Data

Number	Prohibited	Status Date	Notification Date	Marked Erroneous On
TWORTDS	Yes	2023-09-12 16:02:50	2023-09-12 16:02:50	
REPROHIBITED	Yes	2023-10-12 16:01:35	2023-10-12 16:01:35	
TWORTDS	No	2023-11-12 16:02:50	2023-11-12 16:02:50	

Number	Prohibited	Status Date	Notification Date	Marked Erroneous On
RTDCOMPLETE90DAY	Yes	2023-11-14 15:49:50	2023-11-14 15:49:50	
REPROHIBITED	No	2023-12-12 16:01:35	2023-12-12 16:01:35	
NOTPROHIBITED	No	2024-01-01 15:48:19	2024-01-01 15:48:19	
PROHIBITED	Yes	2024-01-01 15:48:59	2024-01-01 15:48:59	
PROHIBITTEDRESCINDED	Yes	2024-01-01 15:53:31	2024-01-01 15:53:31	2024-02-12 15:54:13
RESCINDEDSTILLPROHIBITED	Yes	2024-01-01 15:54:43	2024-01-01 15:54:43	2024-02-12 15:55:20
REPROHIBITED	Yes	2024-01-12 16:01:35	2024-01-12 16:01:35	
TWORTDS	Yes	2024-01-12 16:02:50	2024-01-12 16:02:50	
RTDCOMPLETE30DAY	Yes	2024-01-13 15:51:22	2024-01-13 15:51:22	
RTDCOMPLETE7DAY	Yes	2024-02-05 15:52:17	2024-02-05 15:52:17	
RTDCOMPLETE90DAY	No	2024-02-12 15:49:50	2024-02-12 15:49:50	
RTDCOMPLETE30DAY	No	2024-02-12 15:51:22	2024-02-12 15:51:22	
RTDCOMPLETE7DAY	No	2024-02-12 15:52:17	2024-02-12 15:52:17	
PROHIBITTEDRESCINDED	No	2024-02-12 15:54:13	2024-02-12 15:54:13	
RESCINDEDSTILLPROHIBITED	Yes	2024-01-03 15:55:20	2024-02-12 15:55:20	
RESCINDEDSTILLPROHIBITED	Yes	2024-02-12 15:55:20	2024-02-12 15:55:20	

Number	Prohibited	Status Date	Notification Date	Marked Erroneous On
TWORTDS	No	2024-02-12 16:02:50	2024-02-12 16:02:50	

Appendix B: Additional Resources

This section provides some of the resources and documents that are related to or referenced within this document, such as the Clearinghouse final rules.

- FMCSA Portal
- Drug and Alcohol Clearinghouse
- Clearinghouse final rule
- Clearinghouse-II final rule
- Guidance on developing JSON Web Tokens can be found at JWT.io
- Postman is a tool for testing REST service connections prior to full build out
- Contact information for submitting questions and comments to the Clearinghouse Development Team: https://clearinghouse.fmcsa.dot.gov/Contact
- Amazon Simple Notification Service Developer's Guide
    - Details on configuring an HTTPS endpoint

Appendix C: Examples

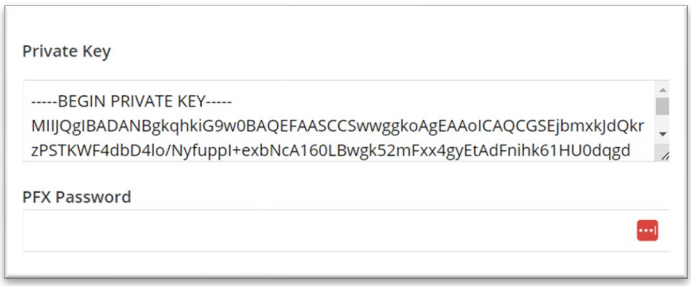
Configuring Postman to Test Connection

Postman is a useful tool for configuring and testing a REST service connection to see how it responds before going through the process of coding access to the service.

Before you start you will need:

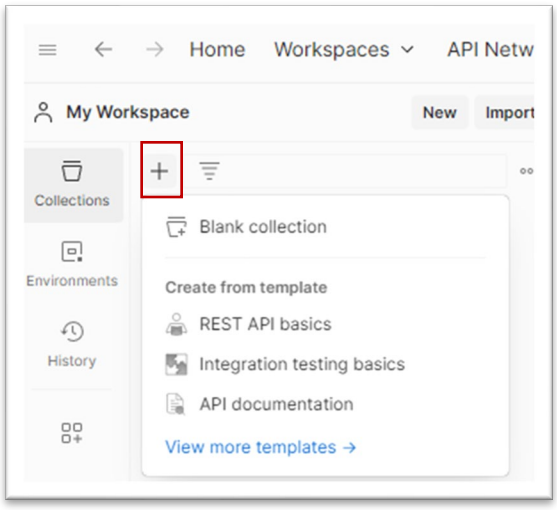
- An installed copy of the postman client.
- The credential identifier displayed when you create your API credential

- A private key generated in the Clearinghouse web interface in PEM format.



The procedure below will allow you to set up and test your connection to the Clearinghouse REST service.

1. Create a new blank collection to configure authorization for each test submission by clicking on the plus icon in the upper left-hand corner of the screen.



2. Give the collection a name and then click on the “Pre-request Script” tab.
3. Enter the code snippet below into the “Pre-request Script” tab.

```
var moment = require("moment")
pm.environment.set('exp', moment().add(20, 'minutes').unix())
```

This creates a variable that stores a Unix timestamp for 20 minutes from the current time, which can be used as a compliant JWT expiration date.

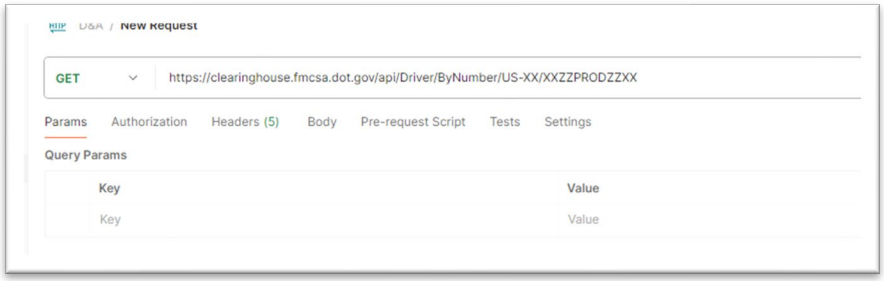
4. Click on the “Authorization” tab and update the following values:
    a. Type: JWT Bearer
    b. Algorithm: RS256 (or RS384 or RS512)
    c. Private key: Key generated in the Clearinghouse web interface in PEM format (see pre-requisites)
    d. Payload:

```
{
    "nbf": {{$timestamp}},
    "exp": {{exp}},
    "iss": "<<Credential ID for your private key>>"
}
```

    e. JWT headers (Postman will include the “alg” value to match your previously selected algorithm value):

```
{
    "typ": "JWT"
}
```

5. Right-click on the tab for your collection and select “New Request”.
6. Configure the request you would like to test. For all except the error submission request, this means simply entering a URL in the “Enter URL” field, as shown in the example test PROD status check, below:



7. Click “Send”

Generate a JWT (.Net Core, C#)

This example requires two packages in addition to the framework:

- Microsoft.IdentityModel.Tokens
- System.IdentityModel.Tokens.Jwt

```
using Microsoft.IdentityModel.Tokens;
using System.IdentityModel.Tokens.Jwt;
using System.Security.Claims;
using System.Security.Cryptography.X509Certificates;

X509Certificate2 cert = new X509Certificate2("Test.pfx", "password");

Console.WriteLine(GetJwt(cert, new Guid("8df92a9d-fdc0-4f47-9412-58a057796515")));

static string GetJwt(X509Certificate2 cert, Guid issuer, string? sub = null)
{
    X509SigningCredentials cred = new X509SigningCredentials(cert, "RS256");

    var token = new JwtSecurityToken(
        issuer: issuer.ToString(),
        expires: DateTime.Now.AddMinutes(20),
        notBefore: DateTime.Now,
        signingCredentials: cred,
        claims: string.IsNullOrWhiteSpace(sub) ? new List<Claim>() : new[] { new
Claim("sub", sub) }
    );

    return new JwtSecurityTokenHandler().WriteToken(token);
}
```

Example JWT Generation Code

Debugging Common Issues

The following are common issues and tips for resolving them.

400 Bad Request

This error indicates an issue with the parameters that are sent with the request. Typically, this will be an issue of encoding formats. More details can be found in the body of the response in the "errors" object.

401 Unauthorized Response

This error indicates an issue with the JWT token you are using to access the service. Details about what went wrong can be found in the "x-amzn-remapped-www-authenticate" response header.

Some common values and their meaning:

- Bearer—no token was received.
- Bearer error= "invalid_token"—the token could not be parsed, check to be sure you are not truncating part of the token's text.
- Bearer error="invalid_token", error_description="MESSAGE"—the message will contain a description of the issue with the token.

403 Forbidden

This error typically indicates that you are trying to query status change or prohibited driver data for a State to which you have not been granted access. If you believe this is in error, please submit a request to SDLAClearinghouse@dot.gov and FMCSA will grant access, as appropriate.

404 Not Found

This code will only be returned from the Driver "ById" (see 3.4.1) or "ByNumber" (see 3.4.2) actions, and it indicates a successful completion of the action in which no driver record was found. The response body will include a problem details object, as defined in the Open API specification.

In the case of "ById," this means that there was no valid driver record found in the Clearinghouse database with the specified id value.

In the case of "ByNumber," this means that there was no valid CDL record in the Clearinghouse with the specified number and state/province code; and that a CD03 check of the number by the Clearinghouse did not return a valid record.

> ***Even if you have already conducted a CD03 check and confirmed the number cannot be retrieved, the number must still be checked in the Clearinghouse, as it is possible that past records associated with the specific CDL number exist in the Clearinghouse.***

Appendix D: References

Organization	Standard	Purpose
International Standards Organization (ISO)	ISO 3166-2	Used to define State codes in driver searches and search results.
	ISO 3166-2:US	List of subdivision codes used for US states and other subdivisions.
	ISO 3166-2:CA	List of subdivision codes used for Canadian provinces and other subdivisions.
	ISO 3166-2:MX	List of subdivision codes used for Mexican states and other subdivisions.
	ISO 8601	Format used for encoding dates
Internet Engineering Task Force	RFC 7797	Definition of the JSON Web Token used to authenticate requests.
	RFC 7807	Define standard error responses for REST API
	RFC 6750	Define details of bearer authentication process and error handling
	RFC 2617	Basic and Digest Authentication
	RFC 2616	HTTP verb and response code definitions

Federal Motor Carrier Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590
855-368-4200
www.fmcsa.dot.gov

Drug and Alcohol Clearinghouse Technical Support
844-955-0207
https://clearinghouse.fmcsa.dot.gov/contact

John A. Volpe National Transportation Systems Center
220 Binney Street, Kendall Square
Cambridge, MA 02142-1093
617-494-2000
www.volpe.dot.gov

U.S. Department of Transportation
Federal Motor Carrier Safety Administration