e-OSCAR™ User Group

March 31, 2026

Attendance:

Please send the Host a CHAT message (in Zoom) with the name of your company to be counted as attending today's meeting.

*If you cannot send a message to the host in Zoom, please send an email to confirm your attendance.

Joel Strickland:
jstrickland@newmgtservices.com

User Group Antitrust Guidelines

As a user of the e-OSCAR Application and participant in User Group meetings and discussions regarding the e-OSCAR Application, you should acquaint yourself with these Antitrust Guidelines of OLDE (Online Data Exchange LLC).

It is appropriate for OLDE and its users to engage in these discussions to generate and facilitate feedback for potential modifications or enhancements to the e-OSCAR Application and its users' e-OSCAR experience. However, in participating in the User Group meetings and discussions, it is important that representatives of participating users remember that their actions are subject to antitrust and competition laws. Antitrust concerns are heightened when, as in this case, participants may be competitors of one another. Accordingly, all participants must be careful to avoid even the appearance of engaging in any inappropriate conduct, both during the formal meetings and in any informal discussions.

In this regard, participants should bear in mind several important principles. First of all, the antitrust laws prohibit conduct that unreasonably restrains trade. In most cases, an "agreement" must be shown to establish a violation; however, agreements can be explicit or can be inferred.

Secondly, some types of agreements or understandings – with respect to certain topics – are considered so harmful that they are automatically unlawful and no justification may be offered to defend them under most antitrust laws. Participants should exercise extreme caution, and refrain from any discussion of or action in connection with the following topics:

1. Current or future prices/rates or price/rate components, price/rate adjustments, or discounts;
2. Costs or profit levels sought or attained;
3. Dividing or allocating customers, markets, product lines, or territories;
4. Any refusal to deal with or boycott a customer, potential customer, supplier or potential supplier;
5. Activities which would lessen the ability of others to compete or potentially compete with other users;
6. Restrictions or limits upon output or production or capacity levels;
7. Any limits upon transactions with specific customers or categories/classes of customers; and/or
8. Negotiated terms with customers, suppliers, or other third parties.

To facilitate compliance with antitrust and competition laws, participants in the User Group meetings should (i) adhere to the prepared agenda and (ii) refrain from discussing competitive issues or exchanging competitively sensitive information that is not necessary to the topics on the prepared agenda and the legitimate goal of enhancing the e-OSCAR Application and users' e-OSCAR experience. Each participant should consult its legal counsel should it have questions concerning the permissibility of any topic. All topics are subject to approval by OLDE legal counsel.

Discussions and submissions during or in connection with the User Group meetings are subject to the confidentiality provisions of the e-OSCAR Terms of Use. OLDE may, but is not obligated to, incorporate any suggestions made in connection with the User Group meetings into the e-OSCAR Application.

The foregoing Antitrust Guidelines, and the User Group meetings and discussions to which they relate, have been developed for the mutual benefit and protection of OLDE and the e-OSCAR users. By signing below, each participant acknowledges and agrees to abide by such Guidelines.

Agenda topics for today's call

Topic	Facilitator	Intent / Description
Welcome & Opening Comments	Joel Strickland	
Services by e-OSCAR	Christy Macdonald	Overview of upcoming changes
New Approach to Backward Compatibility	Christy Macdonald	Discussion regarding how to use current and newest versions of schema for API Services
Updates to Authentication Token Endpoint	Christy Macdonald	Upcoming changes to the /auth/v2/authRequest endpoint
Updates to Notification (Block/DR) Service	Christy Macdonald	Upcoming changes to /notification/v1/getList endpoint
Updates to ACDV Response Service	Christy Macdonald	Upcoming changes to /acdvresp/v2/submit, /acdvresp/v2/validate, /acdvresp/v2/get/{acdvCtrlNum} and /acdvresp/v2/getList endpoints
Updates to Payload Encryption	Christy Macdonald	Upcoming changes to all endpoints when using Payload Encryption

New Approach to Backward Compatibility

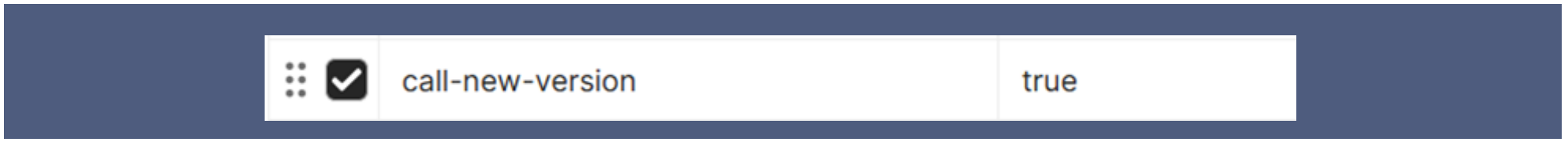
New Approach to Backward Compatibility

What's Changing:

In the past, whenever e-OSCAR updated an API schema, we released a new endpoint version (for example, when the ACDV Request FIND call was updated, we introduced /acdvreq/v3/find to replace /acdvreq/v2/find). Users could continue using the older version for six months before switching to the new one.

With e-OSCAR 4.0, you'll no longer need to switch endpoint versions. Instead, you'll use a **backward compatibility request header** that gives you control over which version of the schema to use — all under the same endpoint.

The new header is:



New Approach to Backward Compatibility

Here's how it works:

- When a schema update is released, the **endpoint name will stay the same**.

- To continue using the **prior version** of the schema simply continue making the call as you do today (no additional header needed).

- To move to the **newest version**, for up to six months, include the **backward compatibility header** in your API call.

New Approach to Backward Compatibility

What happens after the 6 months of Backward Compatibility is over?

- The backward compatibility header will no longer be required.
- The newest version of the endpoint will be the default, and the prior version will be deprecated.

NOTE:

- Communications will be sent out periodically to remind you that the 6 months of backwards compatibility is approaching.
- The API calls **WILL NOT** fail if you include the backward compatibility header **AFTER** the 6 months has passed.

Updates to /auth/v2/authRequest

Updates to /auth/v2/authRequest

To improve the **performance and efficiency** of the Auth token process, e-OSCAR will require Data Furnishers to include the **most recent Auth token** in the header of each new Auth token request via the **auth/v2/authRequest** endpoint.

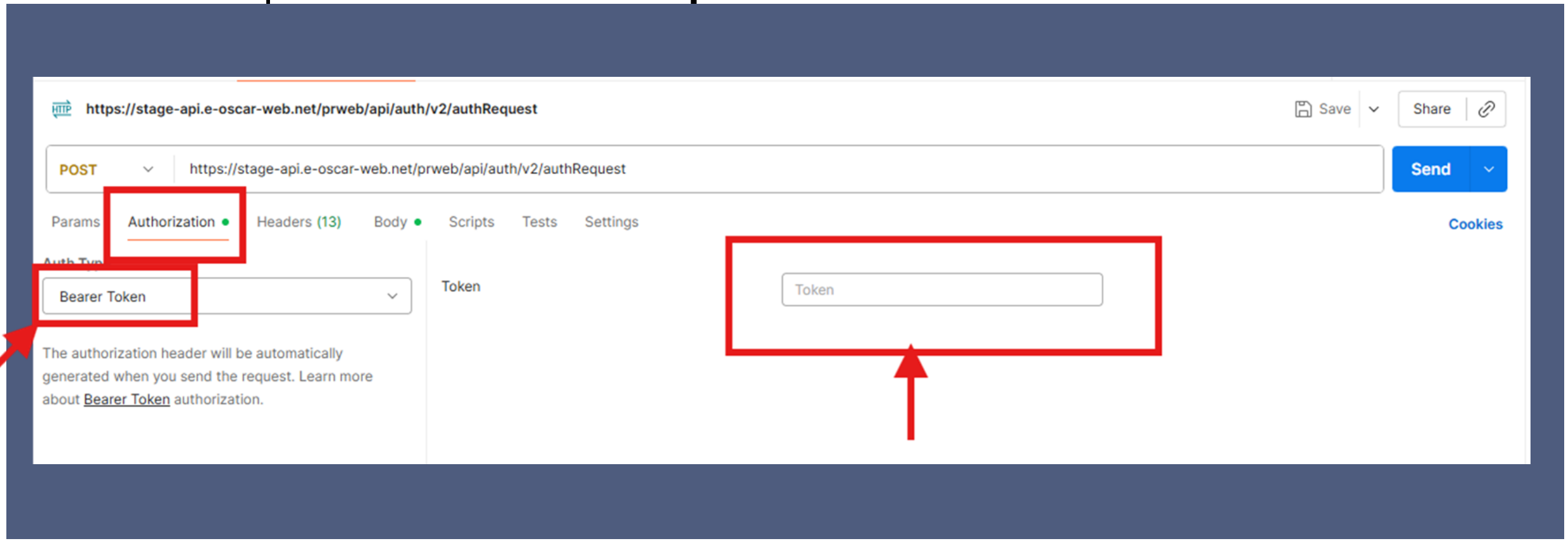
By including the previous token in your request header for the **auth/v2/authRequest** API call, e-OSCAR can determine if the token is still valid:

- If the token **is still valid**, the system will return the **same token** without reaching out to Okta, improving response time.
- If the token **has expired**, the system will automatically request and return a **new token** from Okta.

This enhancement will help reduce unnecessary calls to our Okta instance and improve overall system performance.

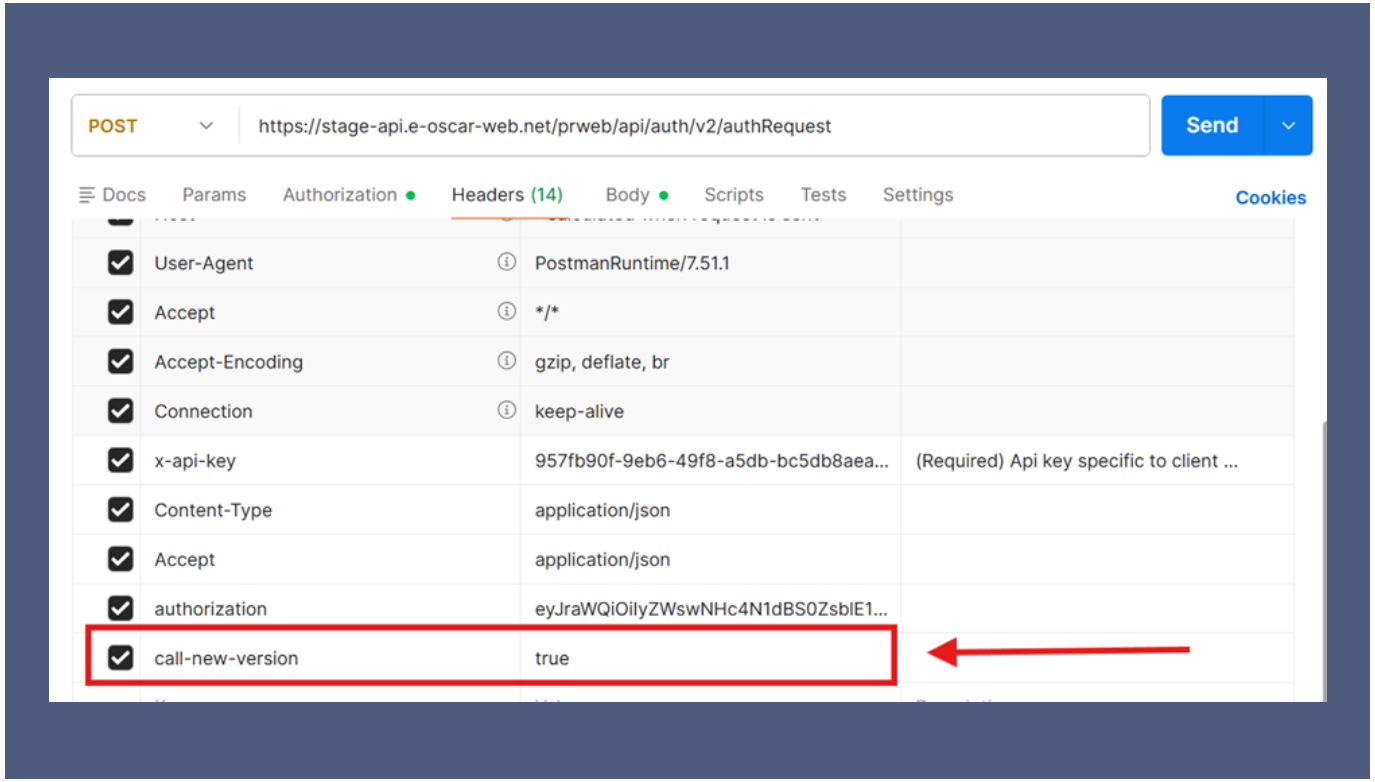
Updates to /auth/v2/authRequest

The previous Authorization Token received will be entered as the Bearer Token in all subsequent **auth/v2/authRequest** API calls as shown below:



Updates to /auth/v2/authRequest Backward Compatibility

Example of backward compatibility to call the newest version of the **auth/v2/authRequest** endpoint post release:

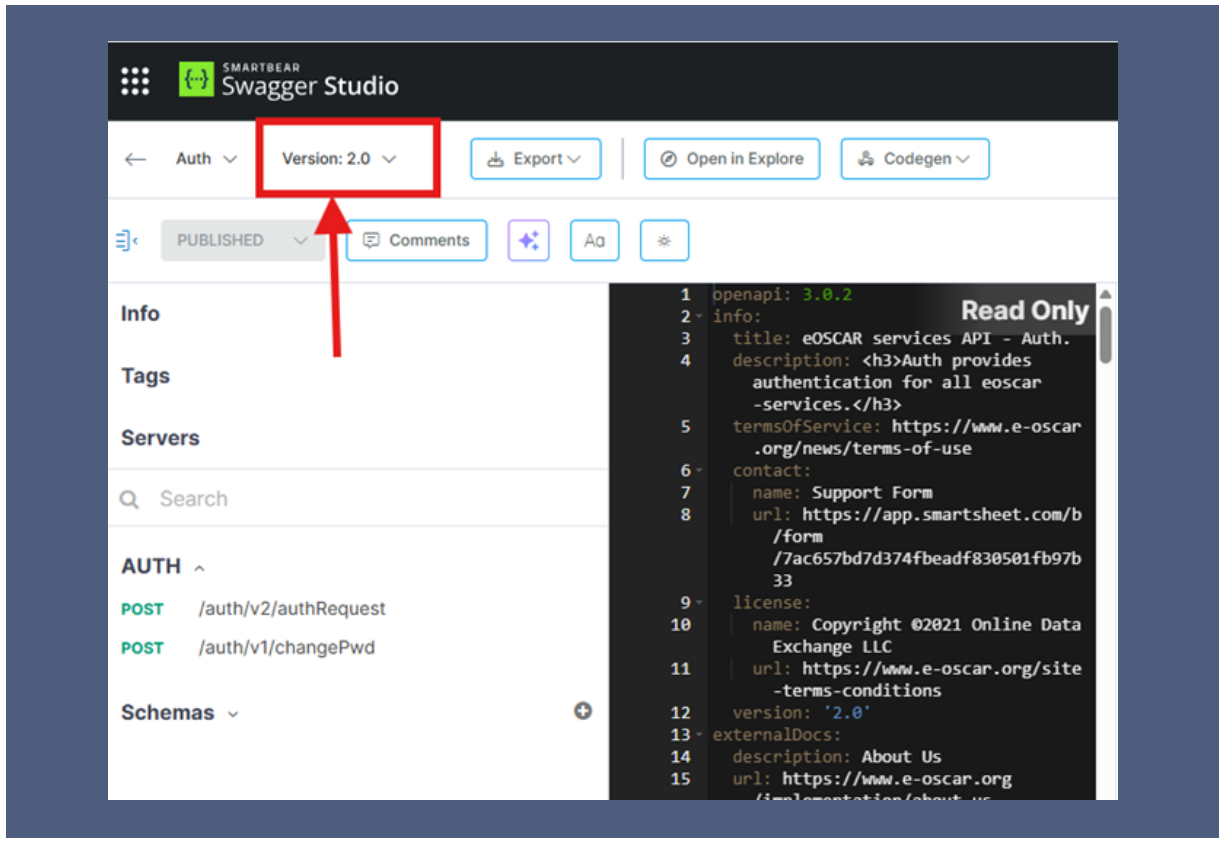


To maintain backward compatibility for 6 months post release, you may continue making the calls as you do today. No change to the header is required.

To utilize the newest version, **you must include the backward compatibility header** in your API calls if you will be utilizing **auth/v2/authRequest** in its new configuration during the 6-month transition period.

Updates to /auth/v2/authRequest Swaggerhub Updates

Auth Services are currently in version 2.0:



The newest version (version 2.1) will appear (when released) upon selecting the dropdown for the version:

Updates to /notification/v1/getList

Updates to notification/v1/getList

Currently, when Data Furnishers call the **Block/DR Notification Service**, multiple notifications can sometimes be returned for the same control number, which can cause confusion.

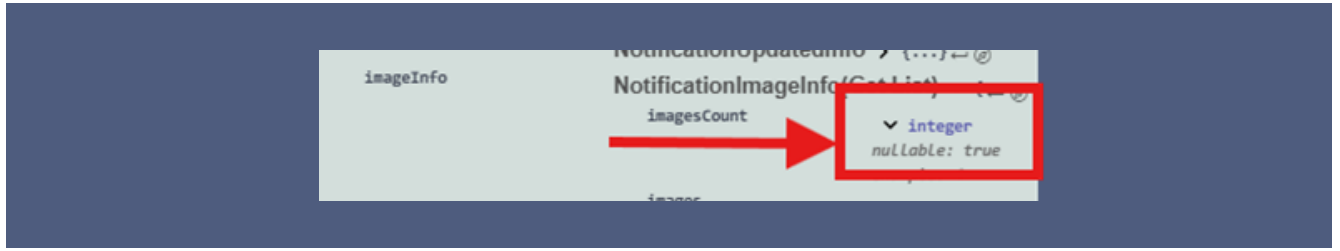
To improve clarity, the **/notification/v1/getList** endpoint will be updated to include a new field: **notificationId**.

This field will assign a **unique identifier** to each Block and DR notification, helping you easily distinguish between individual notifications.

Updates to notification/v1/getList, continued

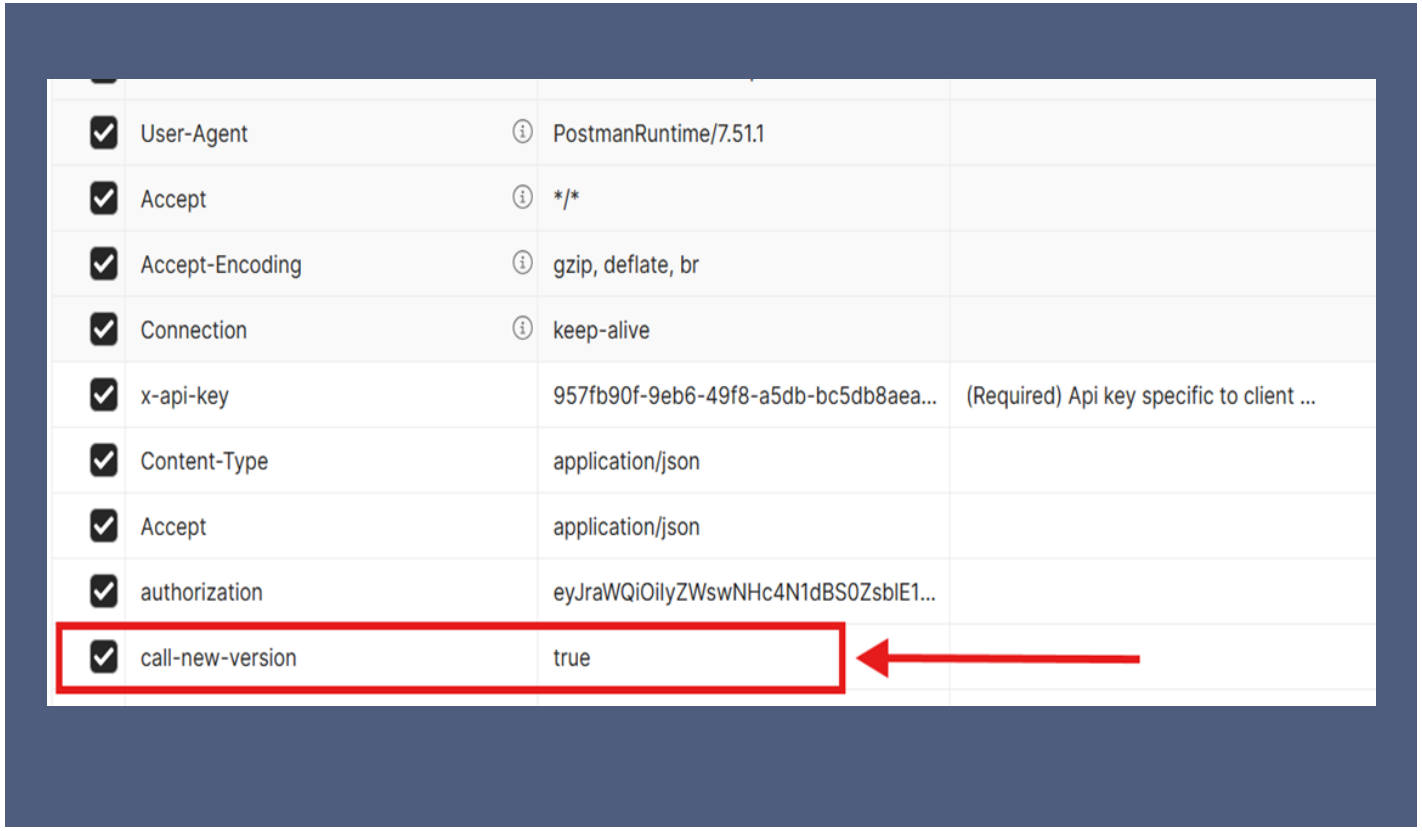
Currently, when Data Furnishers call the **/notification/v1/getList** endpoint, the schema states that an integer may be returned, but sometime a value of null is returned, which can cause confusion.

To improve clarity, the **/notification/v1/getList** endpoint will be updated to include text stating that this field may be nullable.



Updates to /notification/v1/getList Backward Compatibility

Example of backward compatibility to call the newest version of the **/notification/v1/getList** endpoint post release:

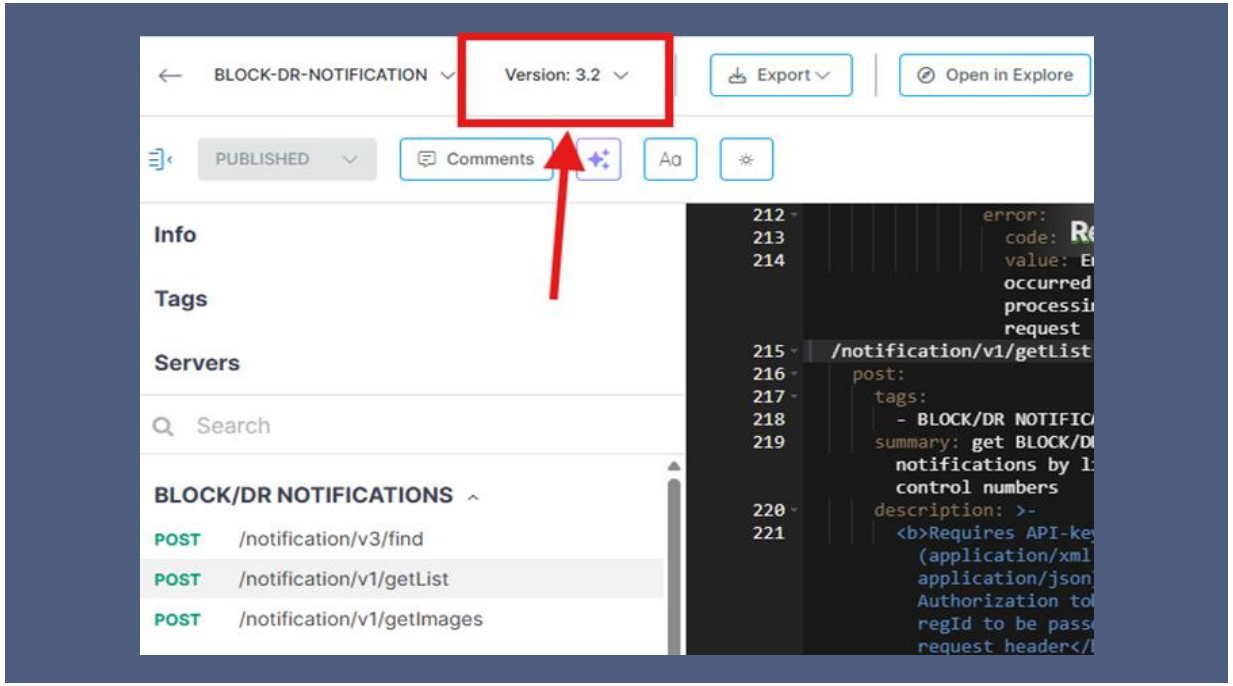


To maintain backward compatibility for 6 months post release, you may continue making the calls as you do today. No change to the header is required.

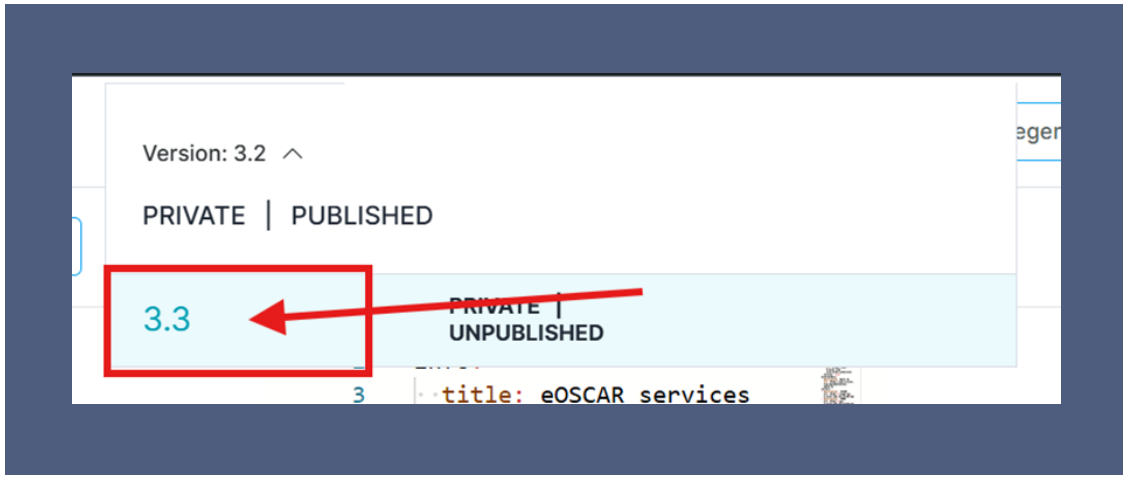
To utilize the newest version, **you must include the backwards compatibility header** in your API calls if you will be utilizing **/notification/v1/getList** in its new configuration during the 6-month transition period.

Updates to /notification/v1/getList Swaggerhub Updates

Notification Block/DR Services are currently in version 3.2 (unencrypted) 3.0 (encrypted):



The newest version (version 3.3 unencrypted and 3.1 encrypted) will appear (when released) upon selecting the dropdown for the version:



Updates to ACDV Response Services

Updates to ACDV Response Services

Currently, when Data Furnishers utilize the **/acdvresp/v2/submit** or **/acdvresp/v2/validate** endpoints, the following fields are optional:

- **dfAuthorizedName**
- **dfContactNumber**

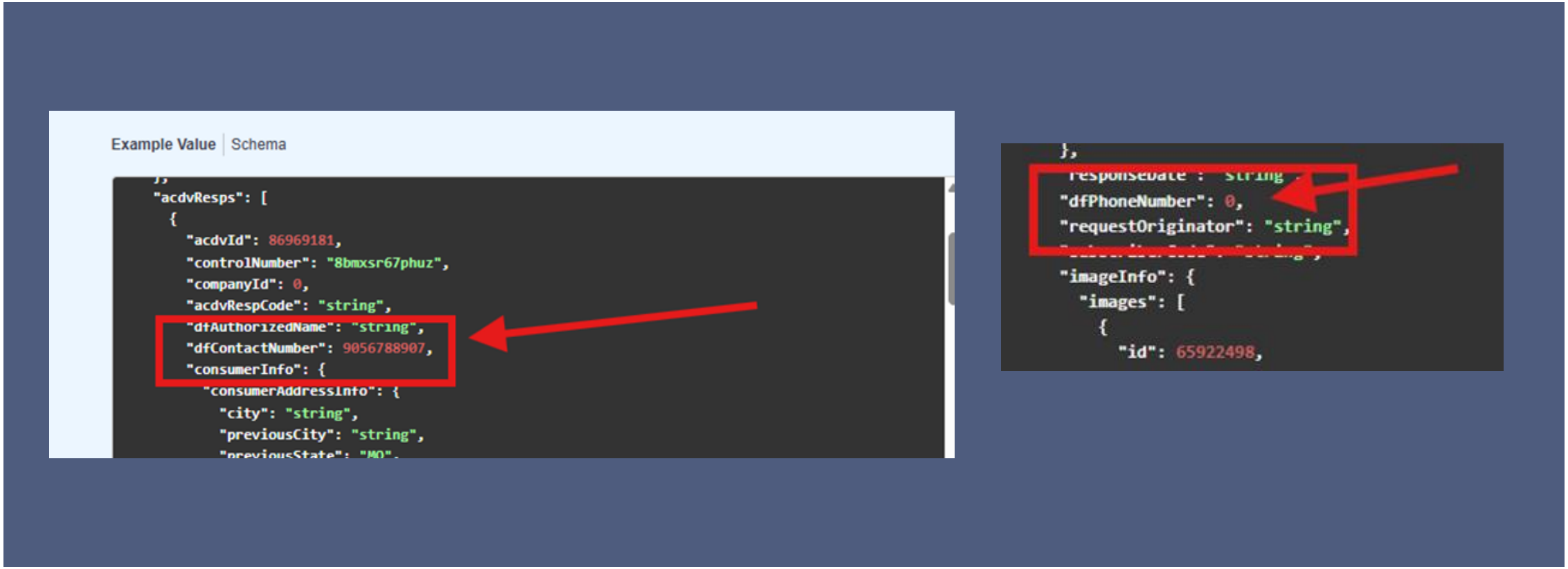
When the updated version of our API Service is released, these fields will become mandatory.

Additionally, the field for **dfContactNumber** will be renamed to **dfPhoneNumber** for the following endpoints:

- **/acdvresp/v2/submit**
- **/acdvresp/v2/validate**
- **/acdvresp/v2/get/{acdvCtrlNum},** and
- **/acdvresp/v2/getList**

Updates to ACDV Response Services, continued

Currently the **/acdvresp/v2/get/{acdvCtrlNum},** and **/acdvresp/v2/getList** endpoints have a field for **dfContactNumber** and **dfPhoneNumber** as indicated here:



Updates to ACDV Response Services, continued

Because the field name for **dfContactNumber** is being updated to **dfPhoneNumber,** the following changes are being made to the **/acdvresp/v2/get/{acdvCtrlNum},** and **/acdvresp/v2/getList** endpoints**:**

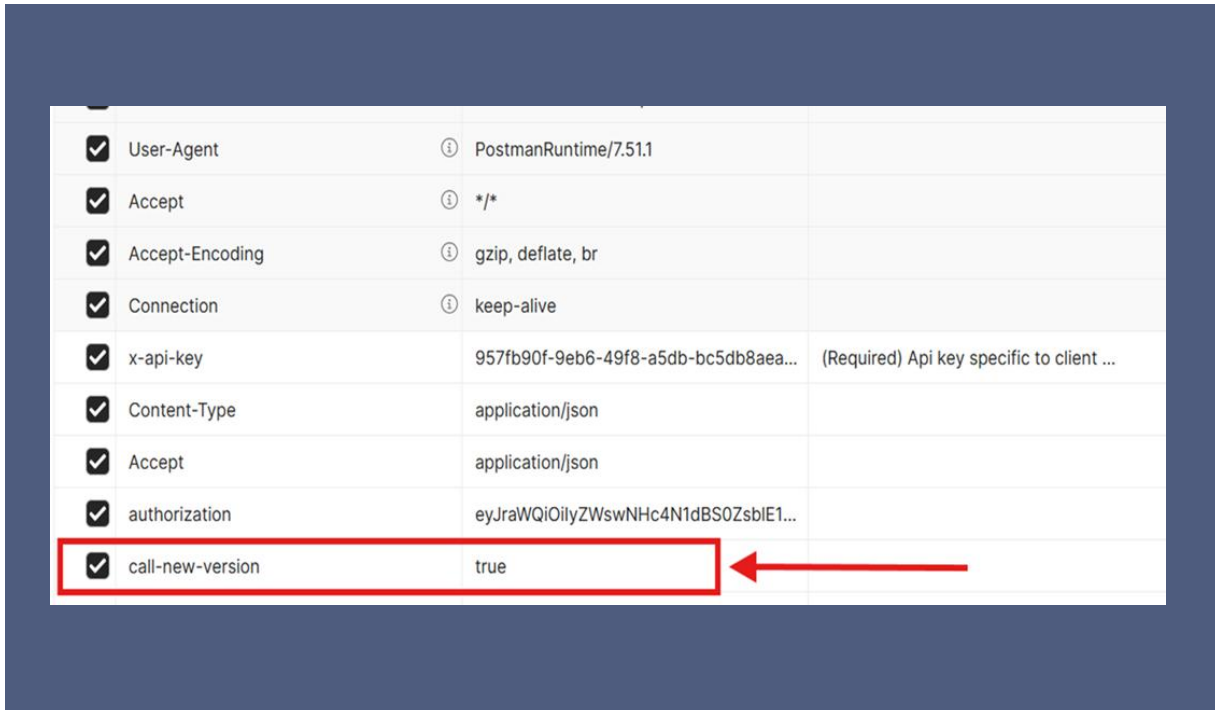
- The existing field for **dfContactNumber** will be changed to reflect **dfPhoneNumber.**

- The field that is currently shown as **dfPhoneNumber** will be removed from the schema.

Updates to ACDV Response Service Backward Compatibility

Example of backward compatibility to call the newest version of the following endpoints post release:

- **/acdvresp/v2/submit**
- **/acdvresp/v2/validate**
- **/acdvresp/v2/get/{acdvCtrlNum},** and
- **/acdvresp/v2/getList**

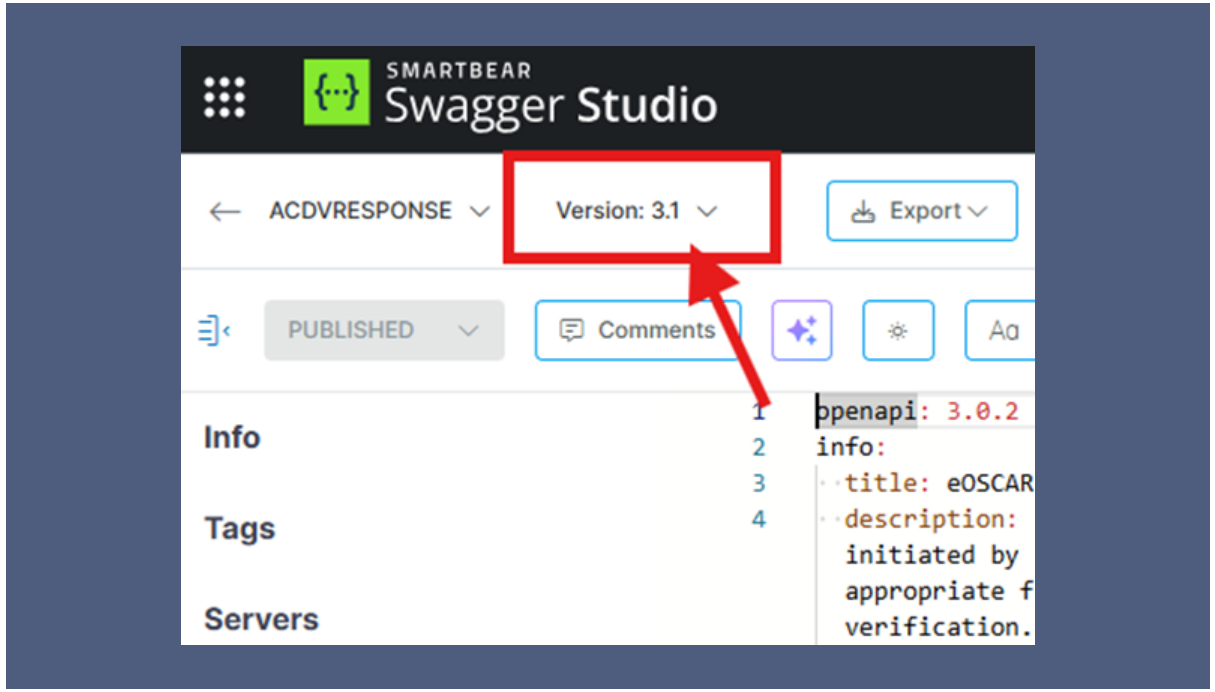


To maintain backward compatibility for 6 months post release, you may continue making the calls as you do today. No change to the header is required.

To utilize the newest version, **you must include the backward compatibility header** in your API calls if you will be utilizing the listed endpoints in their new configuration during the 6-month transition period.

Updates to ACDV Response Service Swaggerhub Updates

ACDV Response Services are currently in version 3.1 (unencrypted) 3.0 (encrypted):



The newest version (version 3.2 unencrypted and 3.1 encrypted) will appear (when released) upon selecting the dropdown for the version:

Updates to Payload Encryption

Updates to Payload Encryption

The following change affects **Data Furnishers who use payload encryption services**. If you are not currently utilizing our Payload Encryption service, this will **NOT** impact you.

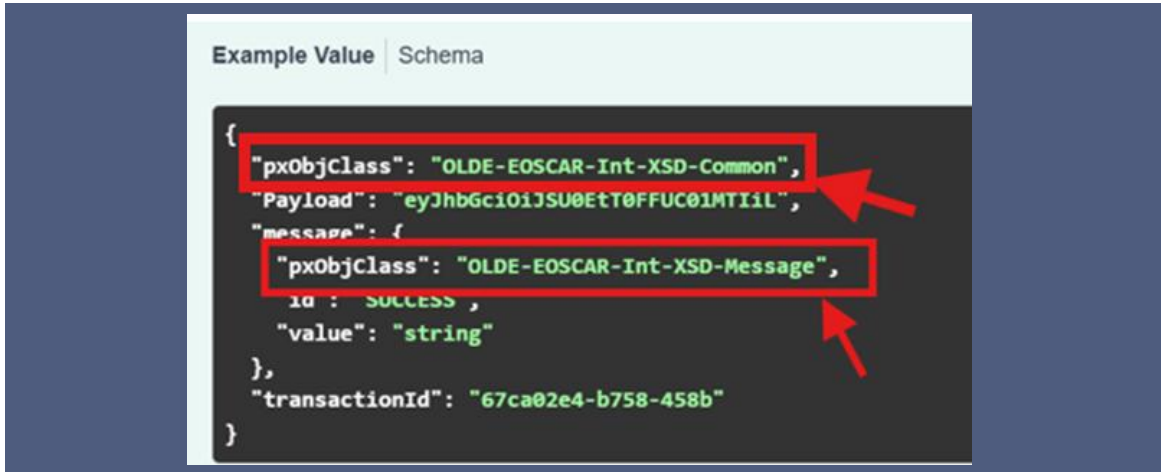
Currently, the field **pxObjClass** appears in the response payload for all encrypted API calls (if leveraging JSON; XML did not include this field). With this update, **pxObjClass will be removed** from response payloads for **all endpoints** when payload encryption is used.

To maintain backward compatibility for 6 months post release, you may continue making the calls as you do today. No change to the header is required if you need to continue receiving the pxObjClass field during the 6-month transition period.

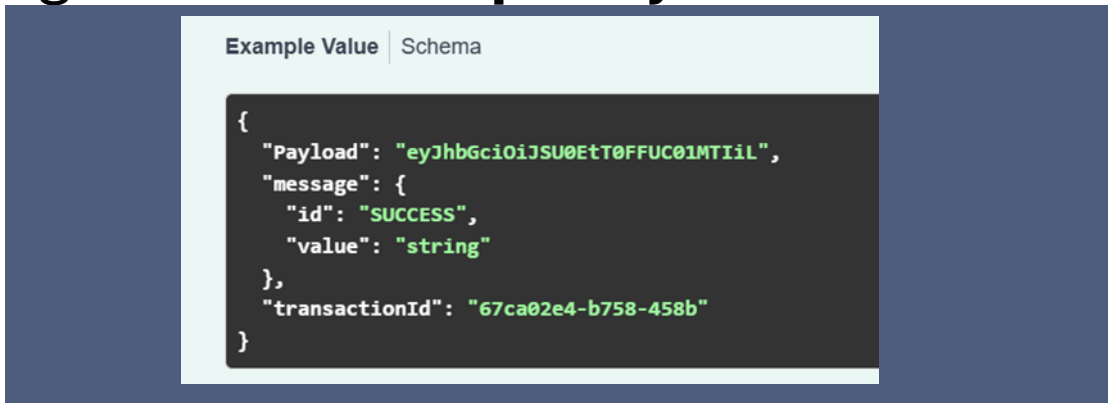
To utilize the newest version, **you must include the backward compatibility header** in your API calls if you will be utilizing the listed endpoints in their new configuration during the 6-month transition period.

Updates to Payload Encryption, continued

Currently, all responses from e-OSCAR in our Payload Encryption include the following:

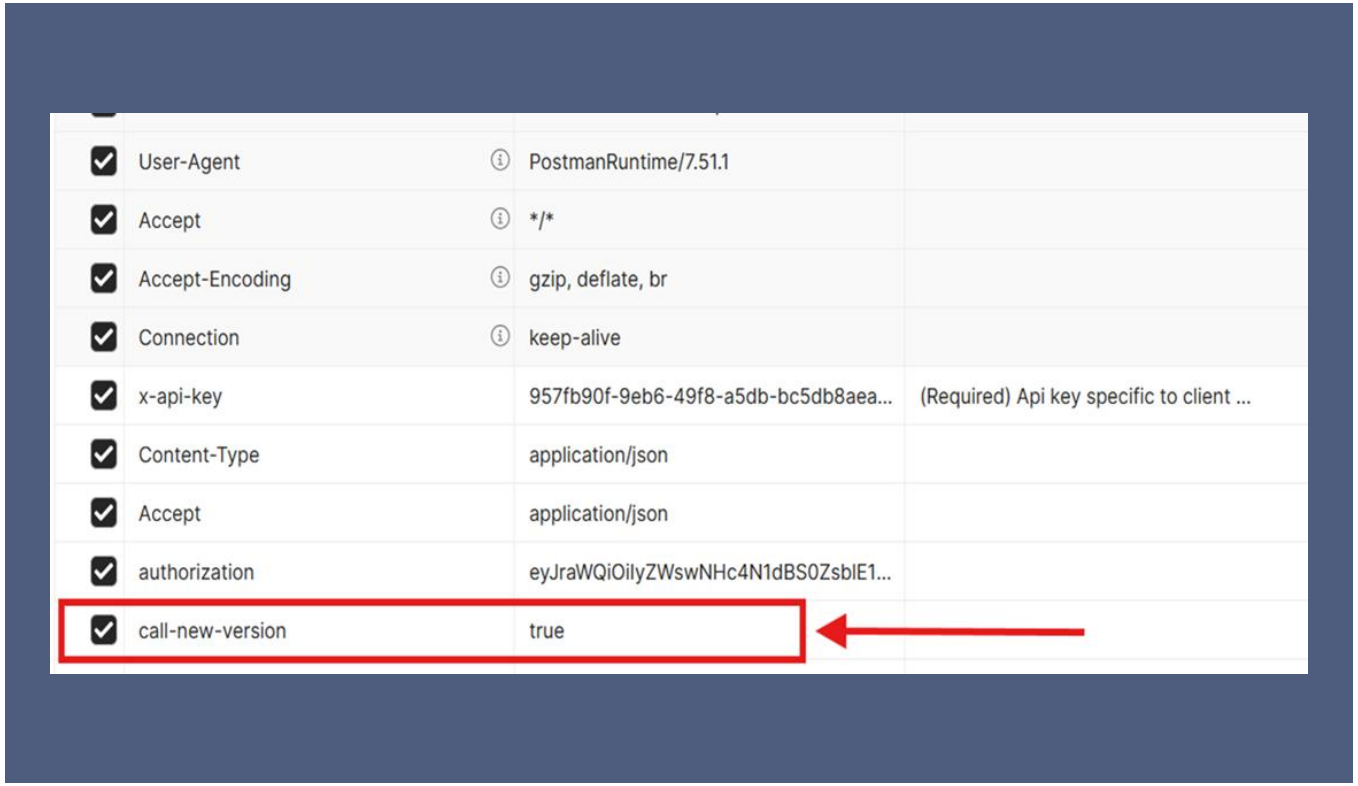


The update will no longer include the **pxObjClass** as shown here**:**



Updates to Payload Encryption Backward Compatibility

Example of backward compatibility to call the new version all endpoints using Payload Encryption post release:

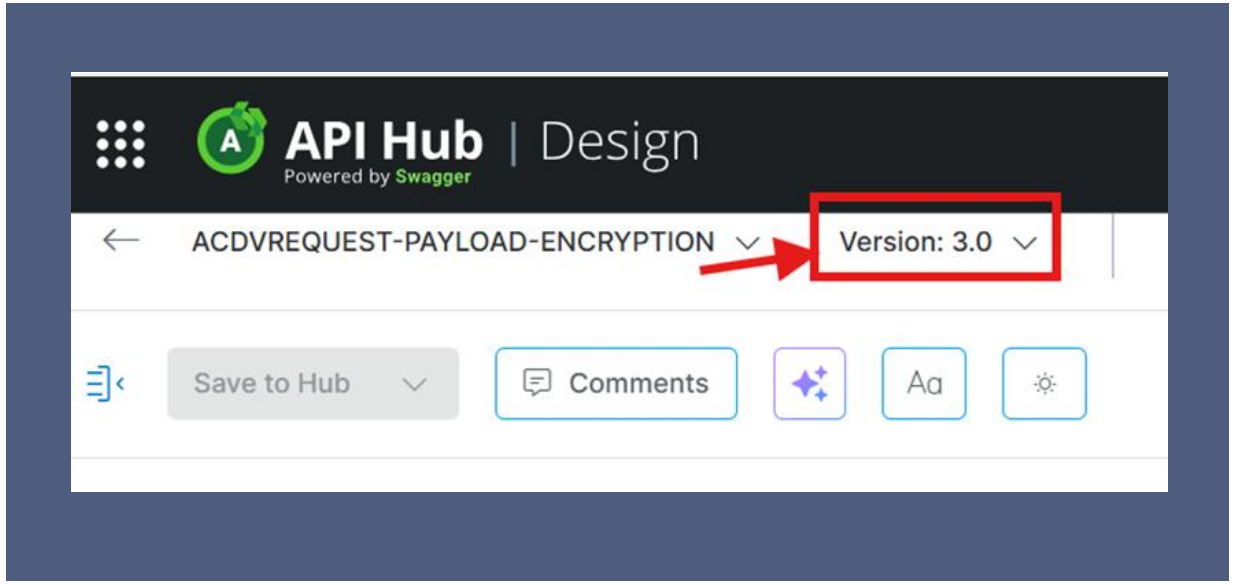


To maintain backward compatibility for 6 months post release, you may continue making the calls as you do today. No change to the header is required if you need to continue receiving the pxObjClass field during the 6-month transition period.

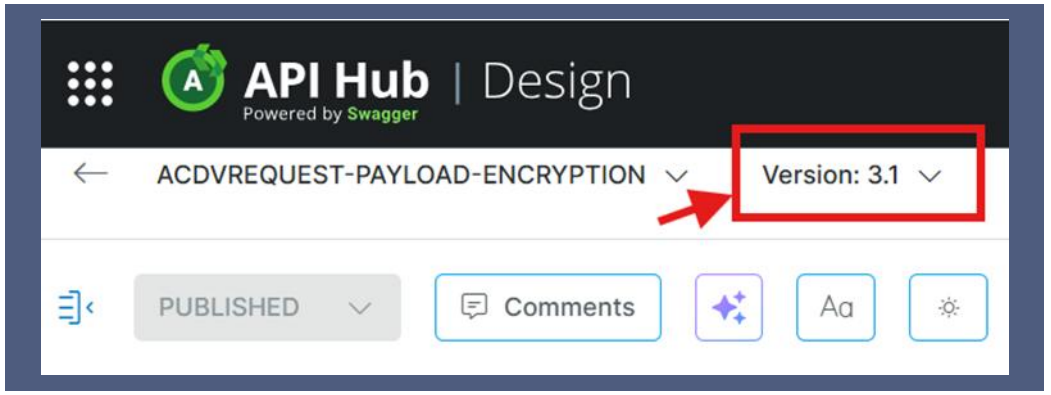
To utilize the newest version, **you must include the backward compatibility header** in your API calls if you will be utilizing the listed endpoints in their new configuration during the 6-month transition period.

Updates to Payload Encryption Swaggerhub Updates

Payload Encryption Services are currently in version 3.0:



The newest version (Version 3.1) will appear (when released) upon selecting the dropdown for the version:



Note: This change impacts **EVERY** Service and Endpoint for Payload Encryption for JSON specifically. After the 6 months backward compatibility period expires, all endpoints in Payload encryption will default to the newest version and will no longer return the **pxObjClass** field.