

Workflow

The recommended user experience is as follows:

1. Promote exclusive benefits
2. Present the user with the ability to [verify their eligibility](#), if successful move directly to the final step
3. If unable to verify successfully, present the user with an opportunity to correct their information and [resubmit](#) (one or two times)
4. If still unable to verify, present the user with the option to [upload documentation](#) proving their eligibility
5. Upon successful receipt of documents, notify the user that they will receive an update when verification is complete, let them continue with their action
6. If eligibility cannot be confirmed with document review, notify the user with a reason why and invite them to upload a valid document (Using a [SheerID email notifier](#))
7. Upon successful document review, notify the user and provide a link to proceed to the final step below
8. Present the user with a message indicating they have been verified and proceed to next steps which are exclusive to eligible users

Note that the above workflow may be asynchronous - a manual review of documents will result in a short delay (generally about 5 minutes, could take up to 20 minutes). It's important to consider this potential when deciding where in the process to place the eligibility verification. For best results, eligibility verification should occur at an early enough time in the conversion funnel to allow for some time to elapse between the initial verification attempt and a final document review response if necessary. Our customers have found success performing this check on a targeted landing page, at the time of account signup or when adding an item or a promo code to a shopping cart. It should not be performed during order finalization (like a credit card transaction), since you won't want to hold up the processing of the order.

Design Considerations

Persistence

It's preferable to maintain a relationship between the SheerID verification request performed and some object in your system, whether it be a registered user, a quote (shopping cart), or an order. This can be done in one of two ways:

Storing SheerID Attributes

Add additional fields in your database to store the following data points that are returned with a VerificationResponse:

- Verification Request ID - the unique identifier for the SheerID verification request
- Person ID - the unique identifier for the individual that was verified, can be used to track an

individual's verification activity

- Request Timestamp - when the verification occurred - for some affiliation types (students, employees) it is advantageous to periodically re-verify
- Verified Affiliations - if your integration is handling multiple types of affiliations, this is helpful in presenting verified users with the appropriate benefits

Using Request Metadata

Additional attributes (such as your site's customer ID, order ID, etc.) can be included with the verification request that is submitted to SheerID. This information is stored by SheerID with the verification request and can be obtained at any time by using the [Inquire](#) API method to fetch the verification response. These request metadata can also be included in bulk reports of verification activity. Even when using this technique to link SheerID activity with your system, it's recommended that your system store the Verification Request ID so that the additional attributes can be retrieved from SheerID.

Preventing Fraud and Abuse

Same Person Limit

The samePersonLimit request configuration can be supplied to restrict the number of successful verifications performed by a single end-user. For example, by specifying the following additional request parameters when invoking the Verify method, a user would only be able to verify successfully once per 90 days:

```
_samePersonLimit=1&_samePersonLimitExpiration=90
```

If the same person limit policy has been exceeded, the request will not be completed and the Verify REST API resource method will return a 409 Conflict HTTP status code rather than a VerificationResponse JSON object.

Links in Email Notifiers

Caution should be exercised when emailing your end-user a link back to the success step as described in the "Email Notifier" section below. For user experience reasons, it's important that the link takes the user back to a personalized destination which continues where they left off; however, it's important to take steps to prevent this user from being able to share that link and its associated restricted benefits (for example, a 25% discount) with other users.

The best way to handle this for applications that have user accounts is to store the in-progress verification request ID in the session or with the user account so that they can return to the verification workflow on a subsequent visit or session. If this strategy is used, the URL does not need to contain any state. If user accounts are not supported or desired in this workflow, a single-use token or key should be generated and stored using one of the techniques described in the "Persistence" section above. URLs may then use the single-use token to allow the user to recover the state of their workflow in progress. Make sure to invalidate or destroy this token once the verification workflow has been completed.

Coding Considerations

Access Token Security

The SheerID API access token(s) used to authenticate requests should be protected like a sensitive password. It should go without saying that this token should never be exposed on the client side or in any page's HTML source. Provisions should be made to store this value external to the source code so that it can be rotated periodically.

Verification Data

Consult the [verification field requirements](#) documentation for a list of required and optional data for each type of verification that you may wish to perform.

If the type of verification you wish to perform requires an organizationId, it is recommended that you use the [Organization Combobox JSAPI component](#) or otherwise obtain the [list of SheerID Organizations from the REST API](#) so that you can help your users to select the SheerID Organization ID matching their organization (school, etc.). While it is possible to specify an organization by name, you will experience a decreased rate of instantly-verified requests due to name ambiguity/matching issues.

Unified VerificationResponse Handling

The VerificationResponse object (JSON) returned by the [Verify](#) method is identical to that returned by the [Inquire](#) method. It's suggested that you use the same subroutine to process the VerificationResponse (attributing a customer record, granting a discount) whether it is the direct, synchronous result of a call to Verify, or if it's the result of performing an Inquire after receiving a HTTP notification that the response is complete.

Document Upload

Document upload is a necessity in order to ensure a high-quality user experience for your integration. Submitting a document for review has three steps:

1. [Perform a verification request](#) to try and instantly verify
2. [Issue an asset upload token](#) associated with the unsatisfied request
3. [Upload one or more documents](#), authorized by the asset upload token

Our recommendation for step 3 is to use the [JSAPI Asset Upload component](#) to allow your user to submit their documents directly to SheerID. This simplifies the coding for you and improves the performance and security of the document transfer for your end-user. Once you have obtained an asset token, this module can be used to easily place and customize a SheerID document upload form on any HTML page.

Service Settings

The following one-time provisioning steps may be performed via the REST API but are more easily performed via the SheerID Control Center.

Managed Document Reviews

By default, SheerID API customers are responsible for reviewing their end-users' submitted documents using the Asset Review utility. It's generally preferable to have this handled by SheerID's team of document review specialists. This can be done using the following steps:

- Log in to the [SheerID Control Center](#)
- From the SheerID Account Home page, select "Document Review Settings" from the "Settings" section
- Set the Managed Reviews switch to Enabled and click Update Settings.

Notifiers

Due to the asynchronous nature of some of the SheerID verification scenarios, Notifiers are a critical component of any successful SheerID API integration. There are two varieties that will be of use to you, described below.

Email Notifier

An event handler which sends the end-user an email (with content customized by you) as a result of the following actions:

- Failed document review - conveys the reason the document was not approved and optionally includes a link back to your site so that they may upload an alternate document.
- Successful document review - notifies the end-user of a completed document review, with a direct, personalized link back to the final ("success") step in your verification workflow.

To set up an email notifier, follow these steps:

- Log in to the [SheerID Control Center](#)
- From the SheerID Account Home page, select "Verification Email Management" from the "Tools" section
- Fill out the form to create an Email Notifier
- After creating, find the Email Notifier under "Emails" tab and click "Edit" if further content customizations are necessary. Email content is specified as HTML.

Note that emails will be sent for all relevant Verification Request activity initiated by your SheerID account from this point forward. This is a one-time setup step.

HTTP Notifier

An event handler which sends a HTTP request (a "webhook") to a specified URL on your site for each state change that occurs for Verification Requests in your account. Your callback URL should be provisioned to accept the `requestId` parameter from the request (either GET or POST method depending on your choice), and then use the [Inquire](#) REST API method to obtain the corresponding `VerificationResponse`.

To set up a HTTP notifier, follow these steps:

- Log in to the [SheerID Control Center](#)
- From the SheerID Account Home page, select "Configure Notifiers" from the "Tools" section

- Enter a URL and HTTP verb, then submit the form create your HTTP Notifier

Note that HTTP requests will be sent for all Verification Request state changes related to your SheerID account from this point forward. It's possible for one verification request to send more than one notification - for example as it moves through the status transitions from NEW (created) to OPEN (submitted but not verified) to PENDING (docs uploaded, awaiting decision) to COMPLETE (finished). You should be prepared to handle more than one notification for a given requestId and may choose to ignore the activity based on the status and the result properties of the returned [VerificationResponse object](#). A common action taken in response to receiving a notification of a VerificationResponse in COMPLETE status is adding attributes to a customer or order record to indicate the result of the verification and allowing the user to subsequently access some protected resource (discount, offer, etc.).