Redact sensitive data in Alchemer Survey

Overview

The Alchemer 'Redact sensitive data' integration uses Google's 'Sensitive Data Protection' capabilities to automatically detect and redact sensitive information from survey data. This integration allows organizations to protect personal and confidential data by identifying sensitive content and applying de-identification rules before data is stored, routed, or passed to downstream system.

Common uses for the Alchemer Redact sensitive data integration

- Detect and redact personally identifiable information (PII) from survey data
- Protect sensitive survey responses before routing or storage
- Apply consistent de-identification rules across workflows
- Prepare sanitized data for downstream integrations and analytics
- Reduce compliance risk when handling sensitive information

What can the Redact sensitive data integration do?

- Inspect survey data for sensitive content
- Redact or transform detected sensitive values
- Return sanitized outputs for use in survey

You will need

- An inspectConfig object defining what sensitive data to detect — or one of the built-in configuration levels described below
- A deifentifyConfig object defining how detected data should be redacted or transformed — or one of the built-in configuration levels described below
- An Alchemer plan that includes integrations and the Integration Manager permission enabled.
    - Contact us if you are unsure if your plan includes integrations.

Setup Redact sensitive data integration in workflow

Tools & Utilities | Redact sensitive data

Your browser does not support HTML5 video.

You will need:

- A valid inspectConfig object, or one of the built-in configuration levels (Basic, Intermediate, or Advanced)
- A valid deifentifyConfig object, or one of the built-in configuration levels (Basic, Intermediate, or Advanced)
- Survey fields containing data to inspect and redact

Configure the action

1. Open your survey in **Survey builder**.
2. Select **Add New: Action**.
3. In the Add Action modal, scroll to the **Integrations** section.
4. Select **Tools & Utilities.**
5. Select **Tools & Utilities | Redact sensitive data.**
6. **Tools | Select default configuration:** Choose a configuration level from the dropdown— **Basic**, **Intermediate**, **Advanced**, or **Custom**. Each level pre-populates the Inspect Config and Deidentify Config fields below with a different set of sensitive info types and redaction approach. See Default configuration levels below for what each level detects and how it redacts matches. Select **Custom** to start from an empty configuration and build your own.
7. **Tools | Deidentify configuration:** Review the `inspectConfig` and `deidentifyConfig` objects in the respective textbox. These are pre-filled based on the configuration level you selected above. Edit either object directly if you need to adjust the info types detected, the likelihood threshold, or the redaction method.
   a. **Note**: The **Basic** level pre-fills the deidentify configuration with an empty `redactConfig` object, which does not remove or mask matched values on its own. If you select Basic, you must still configure how matches are handled (for example, by populating `redactConfig` or replacing it with a masking configuration) before matched values will actually be redacted.
8. **Tools | Select question to redact:** Select the field in this survey that you want to redact. Only one field can be redacted per action. Add additional actions as needed.
9. Save the action.

Status codes

- 200: Successfully redacted sensitive data
- 400: The external integration returned an error

Default configuration levels

Each configuration level sets a starting point for what's detected and how it's redacted. You can edit the generated `inspectConfig` and `deidentifyConfig` objects after selecting a level, or start from scratch with Custom.

Note: Selecting a level only pre-fills the configuration objects—it doesn't guarantee that matched values will be removed or masked. In particular, the **Basic** level generates an empty `redactConfig` placeholder in the deidentify configuration. Until you configure that object (or switch to a level like Intermediate or Advanced that includes a populated masking configuration), matched values will pass through unredacted even though they were successfully detected.

Level	Info types detected	Likelihood threshold	Redaction method
Basic	Person name, email address, phone number, SSN, credit card number	Very likely (flags only high-confidence matches)	None set by default. The generated `deidentifyConfig` includes an empty `redactConfig` object as a placeholder, but matched values are **not** removed or masked until you configure the redaction behavior yourself.
Intermediate	Everything in Basic, plus street address, date of birth, IP address, passport number	Likely	Character masking — matched values are replaced with asterisks
Advanced	Everything in Intermediate, plus financial account number, medical record number, generic ID, auth token, password	Possible (flags more potential matches, which can increase false positives)	Character masking — matched values are replaced with asterisks
Custom	None by default — you define your own `infoTypes`	Possible (editable)	None by default — you define your own transformation

Testing & Support

Testing and Validation

How to test

- Submit a survey response that triggers the integration action.
- Confirm the expected field has been redacted in the results.

- Use metadata for verification and debugging

How to verify results

- Inspect returned metadata values for redacted content.
- Use sanitized outputs in routing, conditions, or merge codes.

Monitoring Integration Activity

Where to find logs

- Go to **Results → Individual Responses**.
- Select the Redact sensitive data integration step.

What logs display

- Inspection inputs and redacted outputs

Troubleshooting

Configuration issues

- Invalid or improperly formatted `inspectConfig` object
- Invalid or improperly formatted `deidentifyConfig` object

Redaction issues

- Sensitive data types not included in the inspection configuration
- Unexpected redaction behavior due to de-identification rules
- Values are detected but not redacted or masked—this is expected with the **Basic** configuration level unless the `redactConfig` object has been configured

---

FAQs

What permissions do I need?

Integration Manager permission in Alchemer.

When does the integration run?

When the workflow reaches the Redact sensitive data integration step.

Can I use multiple Redact sensitive data actions in one workflow?

Yes. Each action runs independently and can be chained as needed.

Why isn't my data being redacted?

Check that your `inspectConfig` includes the correct infoTypes and your `deidentifyConfig` defines valid transformation rules. If you selected the **Basic** configuration level, note that its default `deidentifyConfig` includes an empty `redactConfig` object—matched values are detected but not removed or masked until you configure that object yourself.

What if I need additional functionality?

Contact Alchemer Support for enhancement requests.

Related Articles