

# Set Up Duplicate Protection

If you would like to prevent duplicate responses to your survey, you can select either Cookie-Based or IP-Based duplicate protection. Before you choose an option it's best to review how each of these options work so you can make an informed decision!

## How Does Duplicate Protection Work?

The first thing to know about both duplicate protection methods is that they only take effect if the initial response proceeds past the first page. For IP-Based Duplicate Protection, the second and later attempts need to submit the first page before they receive the duplicate protection message.

Second, it is important to note that both duplicate protection methods will prevent survey respondents who only recorded a partial response (as well as those that are disqualified) from returning to complete the survey. If you wish to allow survey respondents to return to partially completed responses, we recommend enabling [Save and Continue](#) as this will return the respondent to the same session thus trumping the duplicate protection settings.

Third, each method works a little differently and thus has its strengths and weaknesses. Read on to learn more!

## How Does Cookie-Based Duplicate Protection Work?

Cookie-based Duplicate Protection works by storing a small piece of data on the respondent's web browser. In this way, one response per browser per device is allowed.

### What Is a Cookie?

A cookie or an HTTP cookie <sup>[1]</sup> (also called **web cookie**, **Internet cookie**, **browser cookie** or simply **cookie**), is a small piece of data sent from a website and stored in the user's web browser. Every time the user loads the website, the browser sends the cookie back to the server to notify of the user's previous activity. Cookies were designed to be a reliable mechanism for websites to remember information (such as items added to the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). Cookies can also store passwords and other previously entered form content such as an address.

### Cookies Are Not a Fail-Proof Duplicate Protection Method

Because cookies are set on a specific browser on a specific device, if a respondent accesses the survey from more than one device or browser, they would be permitted to enter more than one response.

In addition, tech-savvy respondents can use their browser's option to clear their cookies if they are really set on recording more than one response.

### Does the Alchemer's Duplicate Protection Cookie Expire?

Yes, the duplicate-protection cookie expires after 90 days.

### Using User Agent to Determine if a Respondent Used Another Browser/Device

The [User Agent](#) field which includes information, found on the Details tab of an Individual Response, can be used to see if two responses were recorded on different devices. The User Agent field indicates the device and browser used.

## How Does IP-Based Duplicate Protection Work?

IP-based Duplicate Protection allows one response per IP address.

### IP-Based Duplicate Protection Isn't Always An Option

Because some environments share a single IP address, e.g. corporations, universities, hospitals, this option is not ideal if distributing your survey to multiple recipients in an organization that might be sharing an IP.

### Review Respondents' IP Addresses In Individual Responses

IP address is stored by default (unless your survey is set to [anonymous](#)). You can review IP addresses for each response on the Details tab of [Individual Responses](#).

## Setup

To set up duplicate protection:

1. Click **Tools > Response Settings**.
2. Choose between Cookie or IP based Protection
3. Customize your duplicate messaging and **Save Settings**.

## Alternative Options For Preventing Duplicate Responses

- [Email Campaigns](#) - If you know who your contacts are, using an email campaign to send out your survey will automatically prevent duplicate responses.
- [Login/Password Action](#) - If you know who your contacts are you can also set up your survey so that respondents have to log in thus preventing multiple responses per contact.

### Duplicate Protection for SSO-Authenticated Respondents

To help ensure the integrity of your survey data, Alchemer includes a **Duplicate Protection setting for Single Sign-On (SSO)** authentication. This feature works similarly to IP-based Duplicate Protection: once a respondent has accessed the survey using their SSO credentials, they won't be able to re-enter through the Primary Link again.

If a respondent attempts to authenticate a second time using the same SSO credentials, they'll encounter a Duplicate Protection message, letting them know that their response has already been recorded.

This setting is especially helpful for preventing duplicate entries in environments where SSO is

used to control access to surveys, such as internal employee feedback or secure customer evaluations.

**Note:** This feature is specific to the Primary Link and applies only when SSO authentication is enabled for the survey.

## References

1. HTTP cookie. In Wikipedia. Retrieved February 1, 2016 from [http://en.wikipedia.org/wiki/HTTP\\_cookie](http://en.wikipedia.org/wiki/HTTP_cookie)

## Related Articles