Set Up Response Data Encryption

All Alchemer data is encrypted "at rest" at *disk level*. If you are looking for a further layer of security, the **Response Data Encryption** feature allows you to encrypt data at the *application level*. We recommend using this encryption feature if you are collecting sensitive information such as PHI (personal health information).

Don't confuse Response Data Encryption with secure (SSL) share links. Using SSL share links will ensure your link is *encrypted and will secure data while being transferred to our servers**.

*All data in transit to the Alchemer survey tier (https://www.alchemer.com) via ssl, is sha256 With RSA Encryption.

Enabling and Disabling Data Encryption

Data Encryption *cannot be turned on or off* once a survey has collected data. If data has previously been collected in a particular survey, the option to turn this feature on is not available.

Please be sure you want to encrypt your data before clicking this option. The Response Data Encryption option will be available per survey for Account Administrators *only.* To enable encryption, within your survey:

1. Click on **Tools > Survey Settings**.

2. Scroll to find the **Encrypt Response Data** section.

3. Click **Yes, Encrypt my response data**. To disable encryption, select **No, don't Encrypt response data**. *Keep in mind that once your survey has collected data, this feature will be locked down.*

4. Remember to **Save Settings** when you're finished.

Voila! Response Data Encryption is now turned on. Now, make sure to Customize your link to use secure SSL so that response data is encrypted when transmitted.

Surveys with Data Encryption that have collected data cannot have encryption turned off. If you were just testing the setting out and collected data, you can make a copy of your survey and then you can disable encryption.

Incompatible Features

The below features do not work when data encryption is turned on in your survey:

- **Public Shared Standard Reports** - The only privacy settings available for shared Standard Reports on encrypted surveys are Password Protected and Only Logged-in Alchemer Users. Learn more about these settings.
- Data Cleaning Tool
- Segmented Quotas
- Using the 'contains' operator in CSV/Export filter conditions
- Searching in Individual Responses tab for specific Open Text answers
- Response Tagging
- Show Checkboxes Single Column in CSV/Excel Export

FAQ

What level of encryption does Alchemer use?
We provide 256-bit encryption for your data. This is extremely secure and is used by health care companies and even the military to secure their data. All backups in our system will be 256-bit encrypted as well.

What in my survey will be affected when data encryption is turned on?
When you have encryption turned on, the application will be noticeably slower. This is a side effect of encrypting and decrypting your data. We cannot speed up the application if encryption is turned on. Additionally, secure encryption prevents some features from working (because the encryption makes it impossible to decrypt).

Can I turn project encryption on for all surveys in my account?
Project Data Encryption must be enabled on a survey-by-survey basis. Once you have collected data in an encrypted survey, encryption cannot be enabled/disabled.

Related Articles