Security in Confirmit Software - Survey Settings

Revised: 2019-10-15

1 Protecting Your Confirmit Horizons Surveys Against Fraud And Unauthorized Access

Detecting and preventing fraudulent responses to a survey are vitally important for maintaining the integrity and reliability of the survey results and thereby any decisions based on those results. It is also of great importance to prevent intruders from accessing or sniffing your respondents' answers over the internet.

Confirmit Horizons has many built-in features that allow Survey Designers to protect their surveys. Listed below are some of the key features for securing your Confirmit Horizons Surveys:

- **Encrypt System Request Parameters** - This prevents attempts to reverse-engineer URL state values within a survey. These state values can for example be used to identify individual survey pages and create fraudulent survey records automatically, something which could be done in order to generate large number of incentives. The Confirmit Horizons SaaS Environment default value, and our recommended setting, for this property for new surveys is 'checked'.
- **Enforce HTTPS** – This enables encryption between the browser and the Confirmit Horizons Servers to secure the data while it is transmitted over a public internet connection, and will protect your respondents answers from being "sniffed". This also prevents firewalls/proxy servers from inspecting http packets and causing issues when they are not handled properly for respondents. This is enforced for all companies on the SaaS site and this setting cannot be modified.
- **Use Limited Surveys** - This restricts survey access to a defined list of respondents, and prevents respondents from submitting more than one response to the survey.
- **Login Page** – When the survey project manager does not want to send out long Limited Survey links, a login page can be enforced with username and password on a Limited Survey.
- **Continue links** – Use Continue Links to allow respondents to continue their survey in the event of a network issue.
- **Allow Respondents To Change Their Original Answers** – Uncheck this option to prevent Respondents changing their answers.
- **Allow respondents to re-enter a completed interview and change their answers** – Uncheck this option to prevent Respondents from accessing their survey record after they have completed the survey.
- **Geolocation Flex Extension** - Allows you to identify possibly fraudulent responses based on the geographical location of the respondent or whether or not a respondent is using an anonymous proxy or a satellite provider. You can then for example flag those responses such that they can be identified in the database, allowing you to investigate them further, or you can block them immediately, thereby preventing the data from those respondents being added to the database.
- **Prevents survey page being displayed within a frame** – Check this option to prevent framing of surveys in the browser. Surveys that are not meant to be embedded, such as inline surveys and Digital Feedback programs, can enable this setting.

Revised: 2019-10-15