# Security and Developers' Tools FAQ

Last Modified on 09/09/2019 3:18 pm EDT |

SurveyGizmo offers a number of features that can simplify keeping data safe in your account while using the API and other advanced features available to developers.

This article is an overview of security from a developers point of view.

**Who has access to SurveyGizmo data through the API?**

By default, all users are able to make API requests using their user name and password or using their user name and MD5 as covered in the authentication section.

Each user will be able to work with surveys and data in a manner that is consistent with their access as a User, to certain Teams, per the Role they have on that team – see our User, Teams, and Roles Tutorialfor more information.

**Can access via the API be restricted?**

API access can be restricted at two levels:

1. Account wide restriction of access methods and accepted authentication

2. Individual User Access - restrict all API access for a set of credentials, irrespective of the Account settings. Click **Account > User Management > Users**, then click on the**User Name** you wish to restrict access for and then the **"Permissions" Tab**. Then check the box that says "Do not allow user to access the API".

**How do I ensure HTTPs?**

All API calls require HTTPs.

**My organization requires that users' credentials are not used in API calls. What authentication methods can we use?**

Use the O-Auth method outlined in our Authentication Section.

**Can project encryption be detected, enabled, or confirmed through the API?**

No. Project encryption is about the data being encrypted at rest, meaning on our servers. When encryption is selected (using the User Interface) for a project, data that is collected after encryption is enabled is encrypted using anAdvanced Encryption Standard (AES) 256 bit encryption cypher. Aside from access restrictions outlined above, an API request leads to the data being decrypted on our servers to retrieve the data for your request, with that data being returned to your servers using HTTPs.

**How does at-rest encryption work?**

At-rest encryption means that at any point in our data collection process when data is stored on any of our servers - from staging to permanent storage - the unique key that we generate for you when encryption is enabled is used in an AES 256 bit encryptionmechanism prior to storage, and that the key is stored separately from your data.

**My colleagues / compliance team / business development folks need more details. Where can I find them?**

Please point them to the following resources:Privacy Policy and Security & Reliability Overview