Encrypted Forms in Central

As of version 0.6, ODK Central supports the encryption of submitted data, similar to ODK Aggregate.

> For Aggregate users already using encryption
>
> If you already use encryption with ODK Aggregate, you can use the same encrypted forms with ODK Central without any change, and decrypt data using Briefcase with the same steps you already use today. However, you may still wish to read the rest of this document to understand what Central does and the easier to use encryption available to you in Central.

Encryption with Central

First, here is what enabling encryption on a project or form will do:

- Collect will encrypt finalized data on the mobile device.
- Submission data is sent encrypted, even if Central is not configured with HTTPS.
- Data (filled forms and their attachments) at rest on the Central server is encrypted, and can only be decrypted by using the appropriate secret key information.

However, here are some things that encryption will **not** do:

- Increase the security of user passwords or Collect QR codes.
- Encrypt the blank form contents or attachments.
- Prevent a hijacker from replacing forms or redirecting submissions to a malicious server.
- Prevent the creation of phony submissions.
- Substitute for HTTPS security on the web administration panel.

And, here are some limitations that will appear when encryption is enabled on a project or form:

- Encrypted submissions will appear only as metadata records over OData. Metadata like the submitter and the submission date will be available, but none of the actual data from the form will appear.
- The same restriction applies to the submission preview table on the Central administration panel.
- As of version 0.6, enabling encryption will not encrypt already-submitted submissions.
- As of version 0.6, it is not possible to disable *project managed* encryption (explained below) once enabled.
- As of version 0.6, submissions using *self-supplied key* encryption (Aggregate-style encryption) can be retrieved and decrypted only through Briefcase or direct API access.

Central Encryption Modes

We offer two methods of form encryption in ODK Central:

- **Self-supplied key encryption** is our term for the encryption process already supported by Aggregate and other ODK ecosystem servers. To use self-supplied key encryption, you must generate and securely store your own cryptographic keys which are used to perform the encryption and decryption of the data. The public key (which cannot decrypt the data) is embedded into the XForm itself and this is how it is distributed with the form to Collect and other mobile clients. Decryption is possible only with the private key, and only through Briefcase.
- **Project managed encryption** is new to ODK Central. It uses the same existing ODK encryption standard under the covers, and so it is compatible with existing mobile clients like Collect. However, Central will generate and securely store the cryptographic keys *for* you. The keys are themselves protected by a passphrase that you provide. You do not need to use Briefcase: if you can supply the correct passphrase, the Central administration panel will decrypt the data on the fly and provide you with exported data as usual. Without the passphrase, the data cannot be decrypted, and as Central does not store the passphrase, it cannot decrypt the data without your input.

For most cases, **we recommend using project managed encryption**. It is easier to use, as you do not have to learn how to generate a cryptographic key, you do not have to manually configure each form with the correct key, and you do not need to use Briefcase to decrypt the data. It can also be more secure in many cases, because cryptographic keys are files that must be stored digitally and can be difficult to secure properly. Conversely, a passphrase can be memorized, saved in a password manager, or written down and physically secured.

If you already have familiarity with the encryption in Aggregate, or you cannot at all trust the security of Central itself due to where it has been installed, you may prefer to use self-supplied key encryption.

Using Self-Supplied Key Encryption

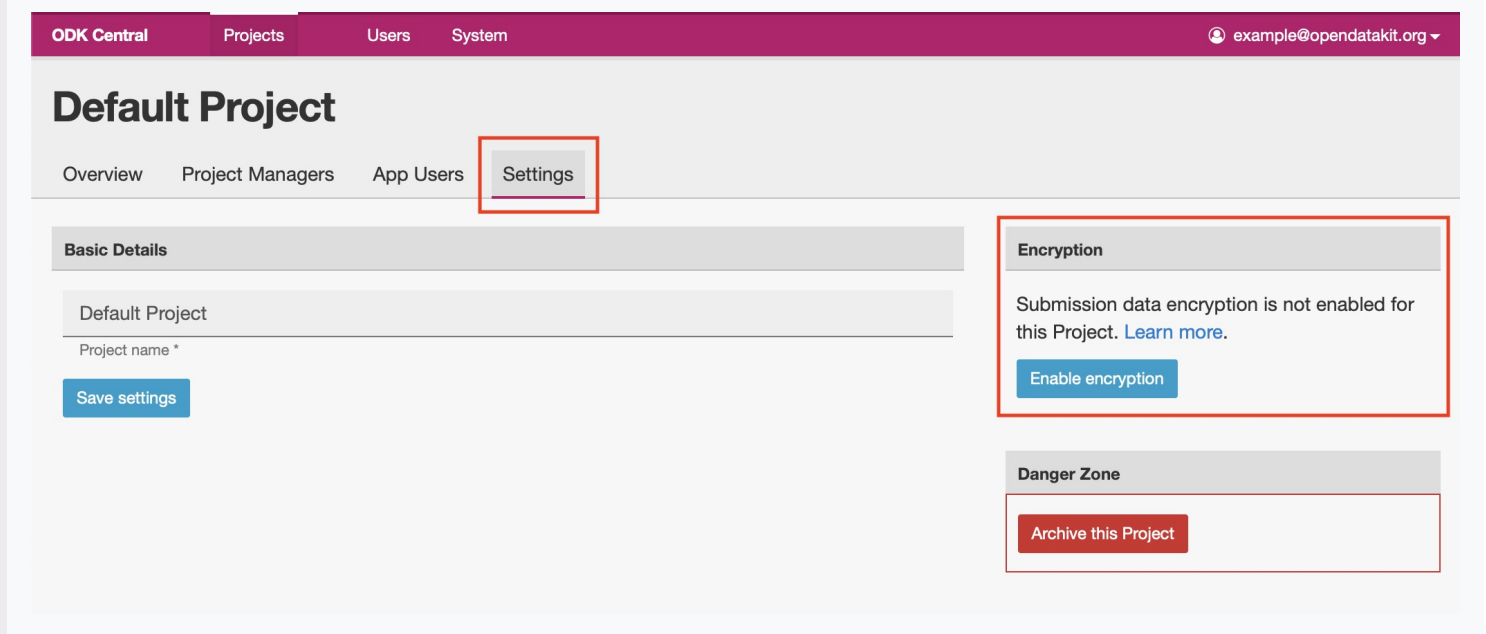
To use self-supplied key encryption, please see the Encrypted Forms document.

When using a self-supplied key with Central, you may and must apply encryption to each form in a project individually. The encrypted data will not be available over OData or for download as a ZIP file. You will need to use Briefcase to retrieve and decrypt encrypted submissions.

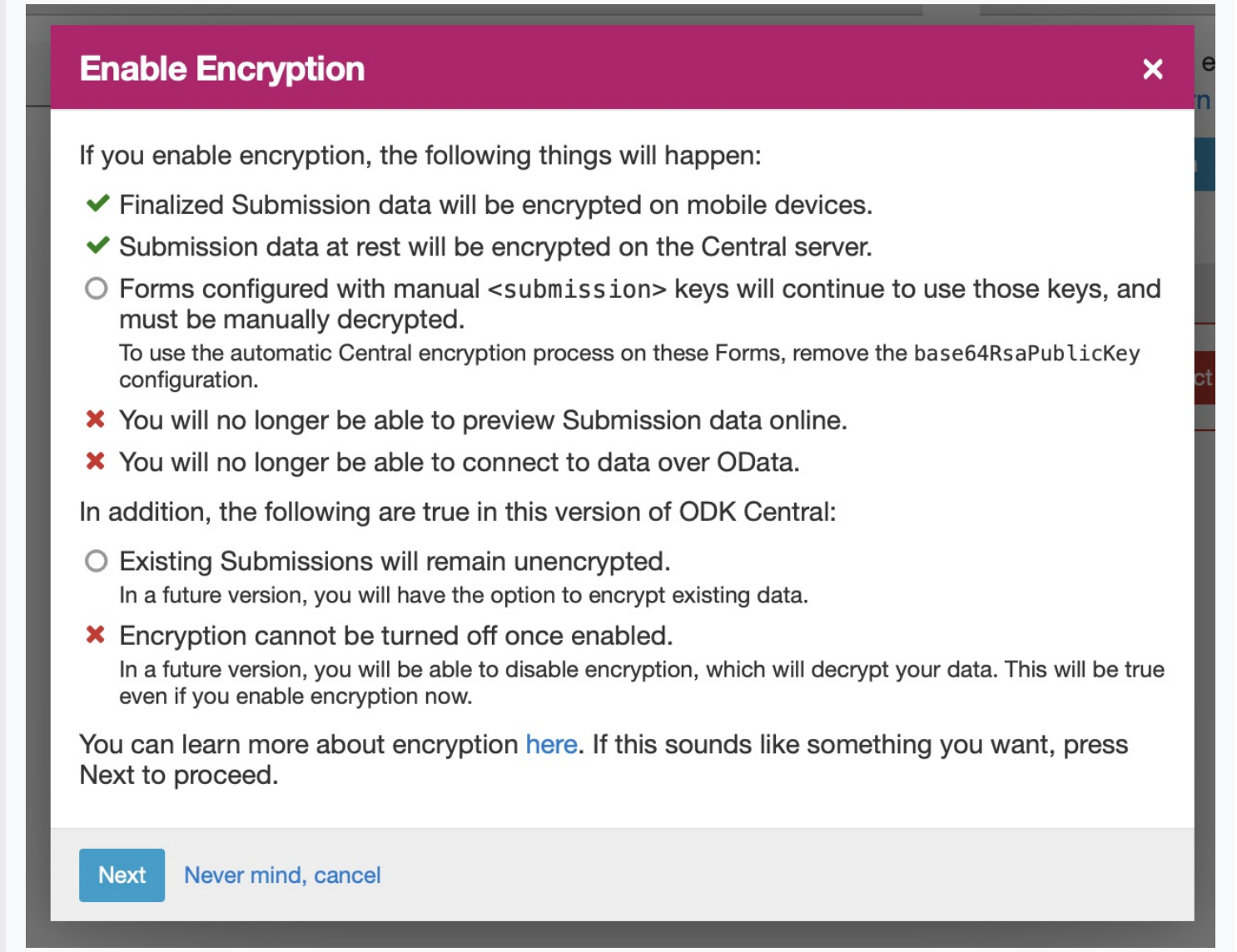
Using Project Managed Encryption

> For Aggregate users already using encryption
>
> Central will always respect any encryption settings already present in your Forms. This means that if you have already put `<submission base64RsaPublicKey="…"/>` configuration in your Forms, Central managed encryption will ignore those Forms and you will not be able to decrypt Submissions uploaded to those Forms using your managed encryption passphrase. Perhaps this is something you want to have happen, but if not you should remove encryption configuration from your Forms before turning managed encryption on.

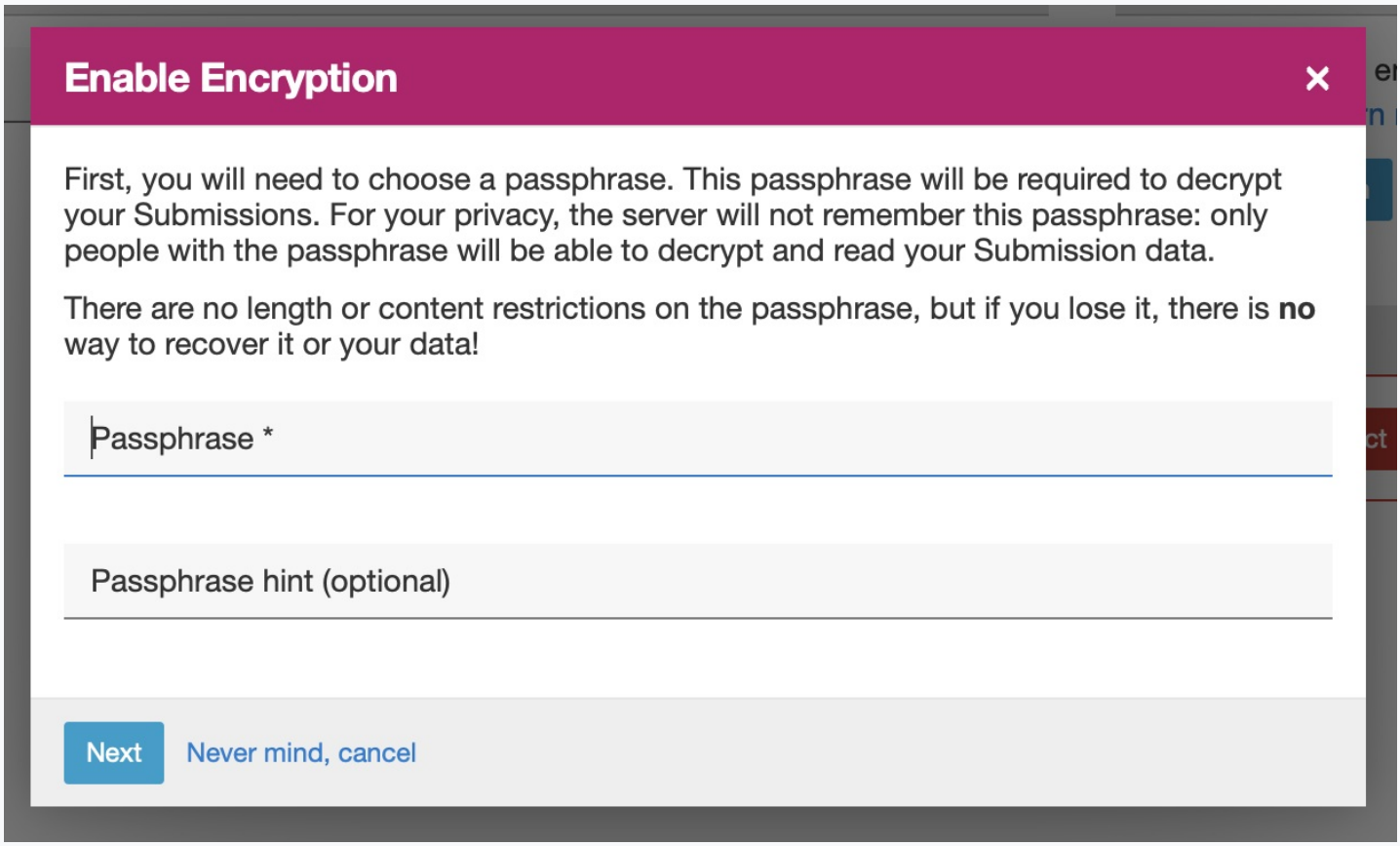
Managed encryption can be enabled only at the Project level. To enable managed encryption, first navigate to the Project, then to the `Settings` tab underneath the Project name. On the right side, you will find the section managing your encryption settings.



To enable managed encryption for the whole project, first click on the `Enable Encryption` button. You will be presented with some warnings, which we have also described above in this document:



Once you review those warnings and press `Next` to proceed, you will be asked for your passphrase, and an optional passphrase hint:

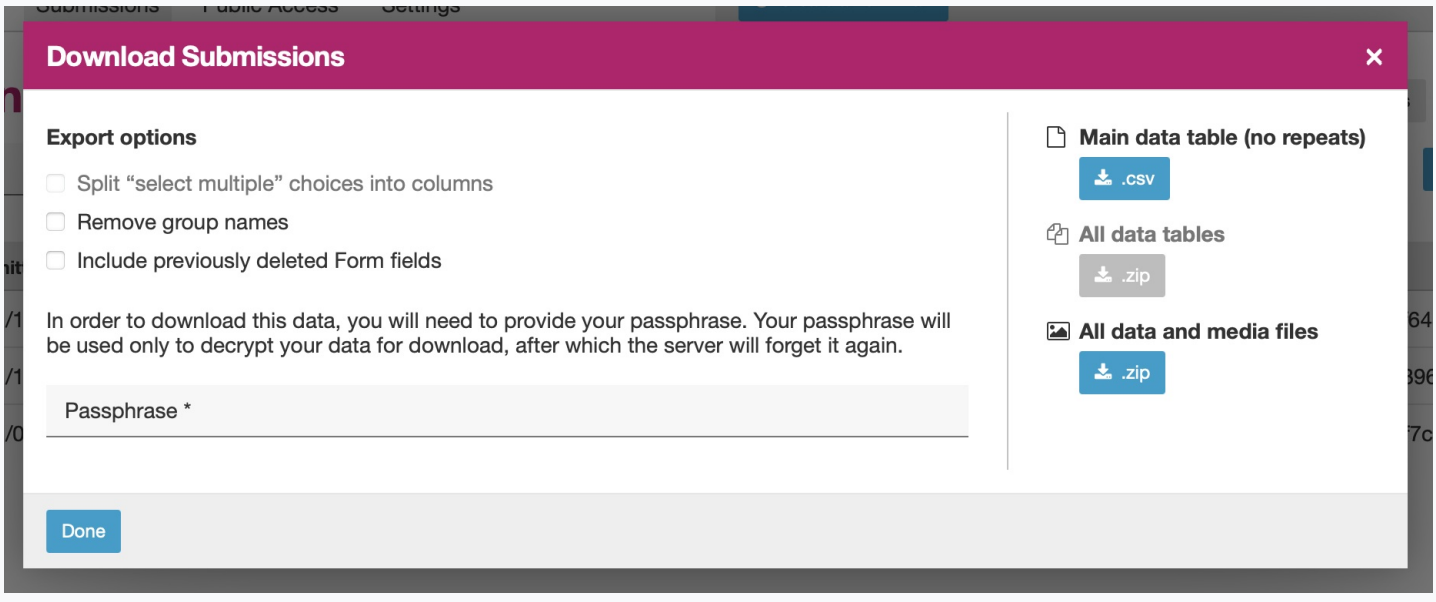


The passphrase you provide is the encryption secret that will be used to secure your data. Anybody who has it will be able to decrypt your submission data. If you lose it, there is no way to recover it, and no way to decrypt your data. Central does not store your passphrase in any way.

The passphrase hint will be displayed whenever the passphrase is needed to decrypt data. It can be a useful way to store information like where in a shared password manager to look for the passphrase. It is optional.

Once you have provided a passphrase and ensured that it is correct, press `Next` to proceed. At this time, managed encryption will be turned on for the Project. All Forms within the Project will be updated to include encryption information, and mobile devices will have to fetch these new versions in order to submit successfully to Central.

Once encrypted data has been submitted, you will be asked for your encryption passphrase when you try to download your data:



Enter your passphrase and press `Download` to download the data. If the passphrase you provide is incorrect, an error message will be displayed after a moment.