

FAQ's for Encryptik

-Encryption solution for salesforce

Q.1 Why should I set the key for the Encryptik app?

The key is the important aspect of the application. This is the first thing the administrator needs to setup as part of the application setup. The key is a vital component as it's used for the encryption as well as the decryption of data.

Q.2 The key is used for what purpose?

Encryption and Decryption require this key, without which the data can't be encrypted or decrypted.

Q.3 Do I have the option to change the key?

No, currently the application does not support changing or re-generating the key. The key once generated for a particular org will be there for its lifetime.

Q.4 What are the security issues if I reveal the key to others?

None, as the application after encryption of data with the generated key also masks the encrypted data because of which anyone having only the key would be unable to decrypt any

information as there is an additional security of masking added to the encrypted data.

Q.5 What will happen if I forgot the key or misplaced the key?

As said earlier, key is generated only once and kept in a protected custom settings which can't be updated or deleted nor retrieved. You need to keep the key information securely as it can't be regenerated or viewed later.

Once the key is generated and set, the application only understands to interact with the key and within the same org, it does not ask again to revalidate at any point of time.

Q.6 What is the chance of key hacking from the salesforce database?

The key is saved in a protected custom settings wherein any administrator or salesforce support are restricted to query this object. So technically it can't be viewed by anyone. In addition to that, application encrypts the key twice before storing which leaves out any room of key been hacked.

Q.7 What is the difference between an auto generated key and manual key?

When the key is generated auto, using the AES 256 protocol a highly secured key is generated. In addition to that one more internal key is generated which combines together to form a secure key for encryption and decryption.

Similarly for the manual key generation option, likewise one more internal key using the same AES 256 protocol is generated which combines together to form a secure key for encryption and decryption.

So to summarize, both the keys are secured and doesn't matter if you choose manual key generation or auto key generation.

Q.8 Can I store the key in my own database?

Yes, you can do that. But you need to ensure that the application has access to this database and also it should be available all times for the smooth functioning of the encryption and decryption.

Q.9 Does Encryptik supports all data types?

Except Geolocation and Multi-picklist, Encryptik supports all other salesforce data types.

Q.10 Does Encryptik supports any third party data loader ?

Encryptik supports third party data loader like Dataloader.io.

Q.11 What happens to the data when I wish to uninstall the application?

Before uninstalling the application, all the data needs to be decrypted back else the data would be in encrypted format and you cannot get your data back after the application is uninstalled.

Encryptik provides various options for decryption wherein the data can be decrypted and you get your original data back.

The various options are Encryptik Data Export, Encryptik query explorer and also via disabling the configuration settings.

Q.12 Why string tokenisation needs additional 4 characters?

The additional 4 characters are generated for any data that uses string tokenisation as they store some information that is required during decryption of data.

Q.13 For 255 text area if some records have 252 characters stored in it, will the encryption work? If not, Why?

Encrypted data is always longer than the actual data. So, for a 255 text area the actual data of 170 characters only can be stored.

Q.14 What is the highest level of encryption within the encryption schemes? ?

Text Type-1 encryption scheme is the highest level of encryption available.

Q.15 Does "Is Searchable option" in the configuration should be always selected for encryption to work?

No, Is searchable is a feature which we are providing if you want that field data to be searchable after its encrypted.

Q.16 If the administrator deactivates the trigger, what will happen to the data inserted after the deactivation?

If the trigger is deactivated then the records inserted after that will be in plain text format. To encrypt these data, all those records needs to passed to the ENCServices which will return the records with encrypted text.

So we recommend that the Encryptik trigger is not touched after the setup. If the trigger is deleted or made inactive the application won't be able to automatically sync the object.

Q.17 Can I change the earlier configured schemes for a field to a different one? What will be the impact on the records?

Yes you can change the scheme for already configured field. Records will be automatically updated according to the new configuration.

Q.18 We have some major implementation happening involving some data

migration into salesforce from other systems? How can I temporarily DISABLE encryption?

You can temporarily disable the Encryptik app when you turn off "Is Active" checkbox which is provided in the setup page.

Once you are ready to activate again, just turn on "Is Active" checkbox and the existing data would be automatically reconciled as well.

Q.19 Can I keep some data encrypted and some data decrypted in the same object as some records are created by specific sales rep who deals with high profile clients?

Yes, you can. There is an additional condition that needs to be added to the triggers and the VF pages but it can be achieved using the Encryptik application.

The only limitation is, only encryption schemes should be used. No tokenisation schemes should be used.

Q.20 There are production support profiles and I want these profiles to see only encrypted data as they are vendors who provide support to the system? They need not see the production data? Does Encryptik supports this scenario?

The key is saved in a protected custom settings wherein any administrator or salesforce support are restricted to query this object. So technically it can't be viewed by anyone. In addition to that, application encrypts the key twice before storing which leaves out any room of key been hacked.

Q.21 What is the chance of key hacking from the salesforce database?

Yes, Encryptik application very much support this. You just need to add the Read Only Or Production Support profile to the Custom Setting and set the field "View Encrypted Data" to TRUE.

Q.22 What will happen to data that are imported to the salesforce database via Dataloader or any other ETL tool? Will those data be encrypted or need some manual process to encrypt this?

For importing data using any of the ETL tools or Dataloader a make sure the object where the data is getting imported the trigger should be active which will automatically encrypt and save it in database.

Q.23 There is requirement form the compliance to get some information for some specific data that are stored in encrypted format within the database? Need to run some adhoc query to view and analyse this data ? Is it possible to

run custom queries on the encrypted data?

Encryptik Query Explorer can be used to run any custom queries to access the actual data.

Q.24 I wanted to do generic search on the encrypted data ? Is it possible?

Yes, Encryptik application provides a VF page (similar to the Salesforce Search page) where you can search any text. The text will be searching in both Encryptik configured objects as well as non-configured objects. The search page can be placed in the home page sidebar. Search operation exposes as web services as well, where user can write their own custom search page.

Q.25 Is sort supported for the encrypted data ?

Sorting is not currently available .This is in roadmap where the data shows in a JS/HTML table where you can apply the sorting, filtering and many other features.

Q.26 Our organization uses some managed packages from the AppExchange? These packages have VF pages which pulls information form the database. Can we integrate Encryptik within these pages to view the decrypted data ?

Managed packages Components (VF Pages, Components, Classes, Triggers) can not be overridden. Encryption can happen as it happens in the database level (as new trigger can be created for a managed custom object). But to see the decrypt data the app provides a component called <csenc:Encryptik /> which needs to be injected to the VF pages. The alternative solution to support the managed package to see the clear original data is to use of home page component or browser extension.

Q.27 Can I create or schedule reports that access encrypted data ? Reports generated should be in decrypted format as this reports are MIS reports to be sent to the management?

The app provides "Query Explorer" utility which facilitates to build query on the fly and then provides the clear data on the screen (just like reports). The same query can be scheduled for future run and can be notified to user(s).

Q.28 Can I do periodic backup of the objects (data is kept encrypted) as these are sensitive data and we need to archive these data periodically?

The application provides "Data Export" utility, where you can export the data immediately. It can be scheduled for future export as well. Data export happens in the background, all data will be exported

to a csv file and stored in Document inside the salesforce org. The user will receive an email as soon as the data export job is completed.

Q.29 I need to Export the objects which are currently marked as critical and have data stored in encryptik format?

The application provides "Data Export" utility, where you can export the data immediately. It can be scheduled for future export as well. Data export happens in the background, all data will be exported to a csv file and stored in a document inside the salesforce org. The user will receive an email as soon as the data export job is completed. Apart from this, the app provides "Query Explorer" which provides data on the screen and can be exported into CSV file. But it is recommended to use if you have a small data set (less than 10K records).

Q.30 I need to encrypt an entire object as Compliance wants the entire object to be kept encrypted? So rather than choose each fields, do you just an option to select the Object?

We are not providing this now, if this is needed then we can put an option while selecting fields to configure we can provide select all option so that all fields are configured(Which is similar to entire object encryption). The reason of not providing "Select All" option is to make sure the admin is configuring the fields, schemes carefully by looking into the data type and size restriction. Also, "Select All" will impact the performance of the application.

Q.31 Can I manually run sync on any particular object ?

App does not provide any direct/manual sync. But there is an alternative way to sync the data for one object. Admin can go to config page, deactivate all the fields (which converts all the encrypted data to clear original data). Then activate fields again will sync the data for that object(converts all the clear data to encrypted data).

Q.32 Our organization have customised our salesforce enterprise and have many custom application built via our team. Does Encryptik application supports our custom application?

Yes, Encryptik application supports all custom application built using VF page and Apex class. For more information, check the "How to integrate and implement custom application" document.

Q.33 For integrating Encryptik with custom application do we need a major implementation

Yes and No, as it depends on how the data comes in /goes out of salesforce database. If your custom application does not depend on any encrypted fields, then you no need to do any changes. If it uses any encrypted fields, then you need to change your code.

For VF page changes, the app provides a utility which will add one component <CSENC:encryptik /> after <apex:page>

automatically. Even you can add this component manually to any VF pages. For apex class, you can use global service methods like encrypt, decrypt & query to do any operation. Also, the app comes up with robust APIs (both Rest/Soap) where you can integrate. Check the API integration document for more examples & other information.