SALESFORCE PLATFORM ENCRYPTION

Summary

Platform Encryption provides an extra layer of Salesforce security while enabling users to enjoy business-critical platform features, such as search, workflow, and validation rules.

Encrypt Your Data and Keep Core Functionality

Now you can encrypt data stored throughout Salesforce, whether in the Sales Cloud, Service Cloud, or even custom apps. Encrypt sensitive, confidential, and private data at rest on the Salesforce App Cloud to help meet privacy policies, regulatory requirements, and contractual obligations for handling private data. Salesforce Platform Encryption sets up in minutes, with no additional hardware or software, and uses native strong, standards-based encryption.

Shield Platform Encryption Terminology

Encryption has its own specialized vocabulary. To get the most out of your Shield Platform Encryption features, it's a good idea to familiarize yourself with the key terms, such as hardware security module, key rotation, and master secret.

Data Encryption
: The process of applying a cryptographic function to data that results in ciphertext. The platform encryption process uses symmetric key encryption and a 256-bit Advanced Encryption Standard (AES) algorithm using CBC mode, PKCS5 padding, and a randomized, 128-bit initialization vector (IV) to encrypt field-level data and files stored on the Salesforce platform. Both data encryption and decryption occur on the application servers.

Data Encryption Keys
: Shield Platform Encryption uses data encryption keys to encrypt and decrypt data. Data encryption keys are derived on a key derivation server using keying material split between a per-release master secret and an organization-specific tenant secret stored encrypted in the database as a part of your organization. The 256-bit derived keys exist in memory until evicted from the cache.

Encrypted Data at Rest
: Data that is encrypted when stored on disk. Salesforce supports encryption for fields stored in the database, documents stored in Files, Content Libraries, and Attachments, and archived data.

Encryption Key Management
: Refers to all aspects of key management, such as key creation, processes, and storage. Tenant secret management is performed by administrators or users who have the "Manage Encryption Keys" permission.

Hardware Security Module (HSM)
: Used to provide cryptography processing as well as key management for authentication. Shield Platform Encryption uses HSMs to generate and store secret material and run the function that derives data encryption keys used by the encryption service to encrypt and decrypt data.

Initialization Vector (IV)
: A random sequence used with a key to encrypt data.

Last updated: December 9, 2016

Key Derivation Function (KDF)
Uses a pseudorandom number generator and input such as a password to derive keys. Shield Platform Encryption uses PBKDF2 (Password-based Key Derivation Function 2) with HMAC-SHA-256.

Key (Tenant Secret) Rotation
The process of generating a new tenant secret and archiving the previously active one. Active tenant secrets are used for both encryption and decryption. Archived ones are used only for decryption until all data has been re-encrypted using the new, active tenant secret.

Master HSM
The master HSM consists of a USB device used to generate secure, random secrets each Salesforce release. The master HSM is "air-gapped" from Salesforce's production network and stored securely in a bank safety deposit box.

Master Secret
Used in conjunction with the tenant secret and key derivation function to generate a derived data encryption key. The master secret is updated each release by Salesforce and encrypted using the per-release master wrapping key, which is in turn encrypted with the Key Derivation Servers' public key so it can be stored encrypted on the file system. Only HSMs can decrypt it. *No Salesforce employees have access to these keys in cleartext.*

Master Wrapping Key
A symmetric key is derived and used as a master wrapping key, also known as a key wrapping key, encrypting all the per-release keys and secrets bundle.

Tenant Secret
An organization-specific secret used in conjunction with the master secret and key derivation function to generate a derived data encryption key. When an organization administrator rotates a key, a new tenant secret is generated. To access the tenant secret via the API, refer to the TenantSecret object. *No Salesforce employees have access to these keys in cleartext.*

Platform Encryption Q&A

What are the hardware and software requirements for using Platform Encryption?
None. The crypto functions run natively on the Salesforce platform. No custom code is required to encrypt or decrypt data.

Why can some users edit fields encrypted with Platform Encryption while others can't?
Encrypted fields are editable regardless of whether the user has the "View Encrypted Data" permission. Use validation rules, field-level security settings, or page layout settings to prevent users from editing encrypted fields, according to your company policy and business solution requirements.

Must I encrypt all of my data when using Platform Encryption?
No. Not all data is sensitive and therefore encryption is not always required. Additionally, unnecessarily encrypting data can affect performance and functionality.

When I enable Platform Encryption, how are my existing encrypted fields affected?
The Platform Encryption process does not affect fields encrypted using Classic Encryption.

Why do I see masked field values?
When using Platform Encryption, you must have the "View Encrypted Data" permission to view field values in plaintext.

Why can I read an encrypted file when I don't have the View Encrypted Data permission?

An encrypted file is visible to all users who have access to that file, regardless of the "View Encrypted Data" permission.

What encryption algorithm is used with Platform Encryption?

The Platform Encryption uses symmetric key encryption and a 256-bit Advanced Encryption Standard (AES) algorithm to encrypt field-level data and files stored on the Salesforce platform. Both data encryption and decryption occur on the application servers. Encryption is integrated into the Salesforce application so the application knows when data needs to be encrypted or decrypted. Whether you're accessing data through the user interface or the API, encryption and decryption is handled the same way.

Can I access tenant secrets using the API?

Yes. For example, you can use the API to define an automatic process to rotate the Platform Encryption key regularly. For detailed information, search for "TenantSecret" in the *Object Reference for Salesforce and Force.com*.

Will data encryption keys that are held in memory rotate automatically when Salesforce rotates the master secret?

No. While Salesforce rotates the master secret on a per-release basis, customers' data encryption keys are not impacted. No new data encryption key is derived automatically.

I use Platform Encryption, and the Encrypted checkbox is not visible when I create or edit an existing custom field. Why?

Only Email, Phone, Text, Text Area, Text Area (Long), and URL custom field types are available for encryption.

What happens to existing data if I rotate a tenant secret?

When you generate a new tenant secret, existing encrypted data remains encrypted and accessible, as long as the old tenant secret is not destroyed. New and existing data is encrypted using the new tenant secret. There is no functional difference to the user.

How finely can I control what data is encrypted with Platform Encryption?

For field data, you control exactly which supported standard and custom fields to encrypt. For files and attachments, you control whether or not encryption is enabled in your organization.

If I enable Platform Encryption, is the format for custom phone, email, and URL fields preserved?

Yes, formats for custom phone, email, and URL fields are preserved when they are encrypted.

Are the Hardware Security Module (HSM)s shared by multiple tenants?

Yes, the Hardware Security Modules (HSM)s are shared across multiple tenants.

Do third-party vendors have access to the Hardware Security Module (HSM)s?

No. Salesforce controls access to the HSMs exclusively.

How long are the tenant secret, master secret, and data encryption keys?

256 bits in length.

Where is my data encryption key stored?

The keys are stored only in memory and never persisted on disk.

Can I change the masking type?

No, the mask types cannot be changed.

What is the limit for how many keys we can have?

There is only a single active key for encrypting data at any time. There is no limit for the number of keys used for decryption.

How is my organization-specific key generated?

The data encryption keys are derived by a key derivation function (KDF) that combines a master secret with an organization-specific tenant secret.

Why are only some fields masked when I view an object?

Only Email, Phone, Text, Text Area, Text Area (Long), and URL custom field types are available for encryption. You must have the "View Encrypted Data" permission to view field values in plaintext.

Where are encryption policies defined?

Your organization defines its own policies.

Can I re-encrypt encrypted data?

Yes. While this process is not automated, you can export and mass update the record IDs for records that include encrypted fields using an ETL tool, such as Data Loader. The existing data is then decrypted with the relevant old keys and re-encrypted with the new, active one. However, this process isn't available for files and attachments.

Can a Platform Encryption key be shared across more than one organization?

No. Encryption keys are specific to an organization and can't be shared with other organizations.

Does encrypting fields, files, and attachments with Platform Encryption count against my organization's storage limits?

No. Encryption and decryption do count against your organization's per-transaction Apex limits, but they are not counted as separate transactions.

Can administrators see the unmasked value of a Platform Encryption encrypted field?

Not by default. When using Platform Encryption, standard profiles do not have the "View Encrypted Data" permission selected. To give this permission to users, create a permission set and assign it to the relevant profiles. You can also create a custom profile with the "View Encrypted Data" permission selected and assign it to users who must view the data unmasked.

If I can see unmasked values when using Platform Encryption, can Salesforce Support representatives see the data, too?

Yes. If you have the "View Encrypted Data" permission and grant login access to other users, they can see encrypted field values in plaintext. To avoid exposing sensitive data, clone your profile and remove the "View Encrypted Data" permission from the cloned profile. Then, assign yourself to the cloned profile before granting login access to the other user.

More Information About Platform Encryption

You don't have to be a security expert to administer a Salesforce organization with Shield Platform Encryption, but you should be an experienced admin with a working knowledge of data security. The Salesforce Platform Encryption white paper (http://sfdc.co/encrypt) is a good starting point. For even more information, try these resources:

- For a comprehensive view of how Shield Platform Encryption fits into an overall Salesforce security policy, search for "security guide" at developer.salesforce.com.
- For detailed instructions and background information on setting up Shield Platform Encryption, search for "platform encryption" at success.salesforce.com.
- For troubleshooting help while working with Shield Platform Encryption, search for "platform encryption" at help.salesforce.com.
- For a view of the features other customers have requested, and what's coming in future releases, search for "encryption" at https://success.salesforce.com/ideaSearch.