# Salesforce Shield Platform Encryption Implementation Guide

@salesforcedocs

Last updated: January 15, 2019

# CONTENTS

# STRENGTHEN YOUR DATA'S SECURITY WITH SHIELD PLATFORM ENCRYPTION

Shield Platform Encryption gives your data a whole new layer of security while preserving critical platform functionality. It enables you to encrypt sensitive data at rest, and not just when transmitted over a network, so your company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

Shield Platform Encryption builds on the data encryption options that Salesforce offers out of the box. Data stored in many standard and custom fields and in files and attachments is encrypted using an advanced HSM-based key derivation system, so it is protected even when other lines of defense have been compromised.

Your data encryption key is never saved or shared across organizations. Instead, it is derived on demand from a master secret and your organization-specific tenant secret, and cached on an application server.

You can try out Shield Platform Encryption at no charge in Developer Edition orgs. It is available in sandboxes after it has been provisioned for your production org.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Encrypt Fields, Files, and Other Data Elements With Encryption Policy

You have a lot of flexibility in how to implement your encryption policy. Encrypt individual fields and apply different encryption schemes to those fields. Or choose to encrypt other data elements such as files and attachments, data in Chatter, or search indexes. Remember that encryption is not the same thing as field-level security or object-level security. Put those controls in place before you implement your encryption strategy.

Filter Encrypted Data with Deterministic Encryption

You can filter data that you have protected with Salesforce Shield Platform Encryption using deterministic encryption. Your users can filter records in reports and list views, even when the underlying fields are encrypted. Deterministic encryption supports WHERE clauses in SOQL queries and is compatible with unique and external ID fields. It also supports single-column indexes and single-column case-sensitive unique indexes. Shield Platform Encryption uses the Advanced Encryption Standard (AES) with 256-bit keys with CBC mode, and a static initialization vector (IV).

Cache-Only Key Service (Beta)

Shield Platform Encryption's Cache-Only Key Service addresses a unique need for non-persisted key material. You can store your key material outside of Salesforce and have the Cache-Only Key Service fetch your key on demand from a key service that you control. Your key service transmits your key over a secure channel that you configure, and the Cache-Only Key Service uses your key for immediate encrypt and decrypt operations. Salesforce doesn't retain or persist your cache-only keys in any system of record or backups. You can revoke key material at any time.

Manage Shield Platform Encryption

To provide Shield Platform Encryption for your organization, contact your Salesforce account executive. They'll help you provision the correct license so you can get started on creating your own unique tenant secret.

# Encrypt Fields, Files, and Other Data Elements With Encryption Policy

You have a lot of flexibility in how to implement your encryption policy. Encrypt individual fields and apply different encryption schemes to those fields. Or choose to encrypt other data elements such as files and attachments, data in Chatter, or search indexes. Remember that encryption is not the same thing as field-level security or object-level security. Put those controls in place before you implement your encryption strategy.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Encrypt New Data in Standard Fields

You can encrypt standard fields on standard objects from the Encryption policy page. For best results, encrypt the least amount of fields possible.

Encrypt Fields on Custom Objects and Custom Fields

You can encrypt standard fields on custom objects, and custom fields on both standard and custom objects, from the management settings for each object. For best results, encrypt the least amount of fields possible. When you add encryption to a field, all new data in that field is encrypted.

Encrypt New Files and Attachments

For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it's uploaded.

Get Statistics About Your Encryption Coverage

The Encryption Statistics page provides an overview of all your encrypted data. This information helps you to stay on top of your key rotation and management tasks. You can also use encryption statistics to identify which objects and fields you may want to update after you rotate your key material.

Synchronize Your Data Encryption with the Background Encryption Service

Periodically, you change your encryption policy. Or you rotate your keys. To get the most protection out of your encryption strategy, it's important to synchronize new and existing encrypted data under your most recent encryption policy and keys.

Fix Compatibility Problems

When you select fields or files to encrypt, Salesforce automatically checks for potential side effects and warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

Use Encrypted Data in Formulas

Use custom formula fields to quickly find encrypted data. You can write formulas with several operators and functions, render encrypted data in text, date, and date/time formats, and reference quick actions.

Apply Encryption to Fields Used in Matching Rules

Matching rules used in duplicate management help you maintain clean and accurate data. Apply deterministic encryption to the fields to make them compatible with standard and custom matching rules.

Encrypt Data in Chatter

Enabling Shield Platform Encryption for Chatter adds an extra layer of security to information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

Encrypt Search Index Files

Sometimes you need to search for personally identifiable information (PII) or data that's encrypted in the database. When you search your org, the results are stored in search index files. You can encrypt these search index files, adding another layer of security to your data.

Encrypt Einstein Analytics Data

To get started with Einstein Analytics Encryption, generate a tenant secret with Shield Platform Encryption. Once you generate an Analytics tenant secret, Einstein Analytics Encryption uses the Shield Platform Encryption key management architecture to encrypt your Einstein Analytics data.

## Encrypt New Data in Standard Fields

You can encrypt standard fields on standard objects from the Encryption policy page. For best results, encrypt the least amount of fields possible.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

Depending on the size of your org, enabling a standard field for encryption can take a few minutes.

1. Make sure that your org has an active encryption key. If you're not sure, check with your administrator.
2. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Policy**.
3. Click **Encrypt Fields**.
4. Click **Edit**.
5. Select the fields you want to encrypt.
   All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select **Deterministic** from the Encryption Scheme list. For more information, see "How Deterministic Encryption Supports Filtering" in Salesforce Help.
6. Click **Save**.

The automatic Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Contact Salesforce to update existing records so that their field values are encrypted.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To encrypt fields:
- Customize Application

Note: To encrypt standard fields on custom objects, such as Custom Object Name, see Customize Standard Fields.

SEE ALSO:

Which Standard Fields and Data Elements Can I Encrypt?

Which Custom Fields Can I Encrypt?

Field Limits with Shield Platform Encryption

Data Loader

Fix Compatibility Problems

Encrypt New Files and Attachments

# Encrypt Fields on Custom Objects and Custom Fields

You can encrypt standard fields on custom objects, and custom fields on both standard and custom objects, from the management settings for each object. For best results, encrypt the least amount of fields possible. When you add encryption to a field, all new data in that field is encrypted.

IN THIS SECTION:

Encrypt New Data in Custom Fields in Salesforce Classic

Add encryption when you create a field in Salesforce Classic, or add encryption to new data entered in an existing custom field.

Encrypt New Data in Custom Fields in Lightning Experience

Add encryption when you create a new field in Lightning Experience, or add encryption to new data entered in an existing custom field.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

## Encrypt New Data in Custom Fields in Salesforce Classic

Add encryption when you create a field in Salesforce Classic, or add encryption to new data entered in an existing custom field.

To apply deterministic encryption to custom fields, first enable deterministic encryption from the Platform Encryption Advanced Settings page in Setup.

1. From the management settings for the object, go to **Fields**.
2. In the Custom Fields & Relationships section, create a field or edit an existing one.
3. Select **Encrypted**.
   All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select a deterministic option listed under Encrypted.
4. Click **Save**.

The automatic Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Contact Salesforce to encrypt existing data.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To encrypt fields:
- Customize Application

## Encrypt New Data in Custom Fields in Lightning Experience

Add encryption when you create a new field in Lightning Experience, or add encryption to new data entered in an existing custom field.

To apply deterministic encryption to custom fields, first enable deterministic encryption from the Platform Encryption Advanced Settings page in Setup.

1. From Setup, select **Object Manager**, and then select your object.
2. Click **Fields & Relationships**.
3. When you create or edit a custom field, select **Encrypted**.
   All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select a deterministic option listed under Encrypted.
4. Click **Save**.

The automatic Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Contact Salesforce to encrypt existing data.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To encrypt fields:
- Customize Application

# Encrypt New Files and Attachments

For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it's uploaded.

Note: Before you begin, make sure that your organization has an active encryption key; if you're not sure, check with your administrator.

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Policy**.
2. Select **Encrypt Files and Attachments**.
3. Click **Save**.

Important: Users with access to the file can work normally with it regardless of their encryption-specific permissions. Users who are logged in to your org and have read access can search and view the body content.

Users can continue to upload files and attachments per the usual file size limits. Expansion of file sizes caused by encryption doesn't count against these limits.

Turning on file and attachment encryption affects new files and attachments. It doesn't automatically encrypt files and attachments that were already in Salesforce. To encrypt existing files, contact Salesforce.

To check whether a file or attachment is encrypted, look for the encryption indicator on the detail page of the file or attachment. You can also query the `isEncrypted` field on the ContentVersion object (for files) or on the Attachment object (for attachments).

## EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

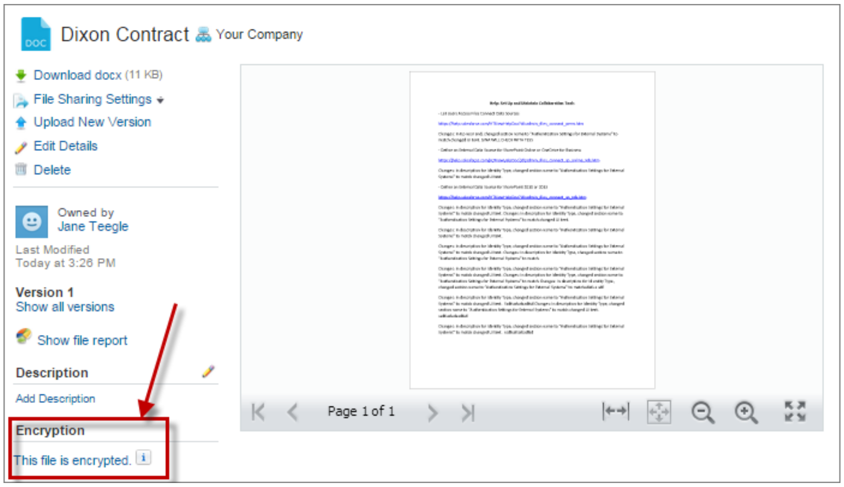
Available in both Salesforce Classic and Lightning Experience.

## USER PERMISSIONS

To view setup:
- View Setup and Configuration

To encrypt files:
- Customize Application

**Here's What It Looks Like When a File Is Encrypted.**



Dixon Contract Your Company

Owned by Jane Teegle

Last Modified Today at 3:26 PM

Version 1

Description

Encryption

This file is encrypted.

SEE ALSO:

Encrypt New Data in Standard Fields

# Get Statistics About Your Encryption Coverage

The Encryption Statistics page provides an overview of all your encrypted data. This information helps you to stay on top of your key rotation and management tasks. You can also use encryption statistics to identify which objects and fields you may want to update after you rotate your key material.

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Gather Encryption Statistics

The Encryption Statistics page shows you how much of your data is encrypted by Shield Platform Encryption, and how much of that data is encrypted by an active tenant secret. Use this information to inform your key rotation actions and timelines. You can also use the Encryption Statistics page to collect information about the fields and objects you want to synchronize with the background encryption service.

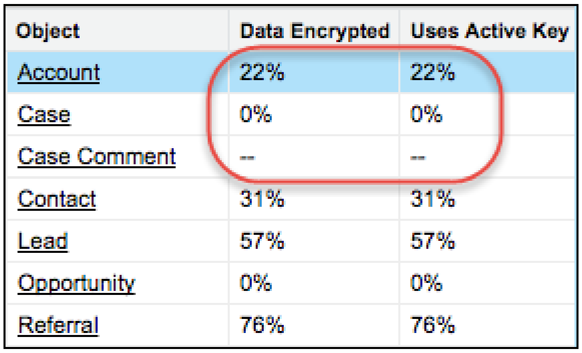
Interpret and Use Encryption Statistics

The Encryption Statistics page offers a snapshot of your encrypted data. You can use the information on this page to help make informed decisions about managing your encrypted data.

## Gather Encryption Statistics

The Encryption Statistics page shows you how much of your data is encrypted by Shield Platform Encryption, and how much of that data is encrypted by an active tenant secret. Use this information to inform your key rotation actions and timelines. You can also use the Encryption Statistics page to collect information about the fields and objects you want to synchronize with the background encryption service.

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Statistics**.
2. Select an object type or custom object from the left pane. If you see a "--" in the Data Encrypted or Uses Active Key columns, you haven't gathered statistics for that object yet.



| Object | Data Encrypted | Uses Active Key |
|---|---|---|
| Account | 22% | 22% |
| Case | 0% | 0% |
| Case Comment | -- | -- |
| Contact | 31% | 31% |
| Lead | 57% | 57% |
| Opportunity | 0% | 0% |
| Referral | 76% | 76% |

3. Click **Gather Statistics**.
4. Refresh the page.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view Setup

- View Setup and Configuration

The statistics show all available information about data for each object.

Note:

- The gathering process time varies depending on how much data you have in your object. You're notified by email when the gathering process is finished. You can gather statistics once every 24 hours.
- Feed Item doesn't display statistics because it's derived from Feed Post. Gathering statistics for Feed Post is sufficient to confirm the encryption status of both Feed Post and Feed Item.

## Interpret and Use Encryption Statistics

The Encryption Statistics page offers a snapshot of your encrypted data. You can use the information on this page to help make informed decisions about managing your encrypted data.

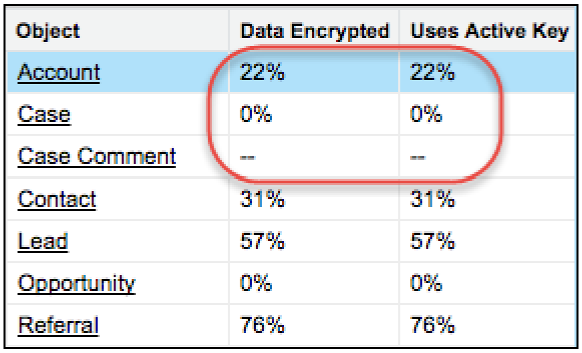
Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

The page offers two views of your encrypted data: a summary view and a detail view.

**Encryption Summary View**

The summary shows all your objects and statistics about the data in those objects.



| Object | Data Encrypted | Uses Active Key |
|---|---|---|
| Account | 22% | 22% |
| Case | 0% | 0% |
| Case Comment | -- | -- |
| Contact | 31% | 31% |
| Lead | 57% | 57% |
| Opportunity | 0% | 0% |
| Referral | 76% | 76% |

- Object—Lists your standard and custom objects. Data about standard objects are aggregated for all standard objects of a given type. Data about custom objects are listed for each custom object.
- Data Encrypted—The total percentage of data in an object that's encrypted. In the example above, 22% of all data in Account objects in encrypted. The Case object shows 0%, meaning none of the data in any Case is encrypted.
- Uses Active Key—The percentage of your encrypted data in that object or object type that is encrypted with the active tenant secret.

When the numbers in both Data Encrypted and Uses Active Key columns are the same, all your encrypted data uses your active tenant secret. A double dash (--) means that statistics haven't been gathered for that object or object type yet.

**Encryption Detail View**

When you select an object, you see detailed statistics about the data stored in that object.

- Field—All encryptable standard and custom fields in that object that contain data.

Note: Chatter data is stored in the Feed Attachment, Feed Comment, Feed Poll Choice, Feed Post, and Feed Revision objects. The Encryption Statistics page lists these objects and all fields that hold encrypted Chatter data in the database. Some fields listed on the Encryption Statistics page aren't visible in the UI by the same name, but they store all encrypted data that's visible in the UI. See Which Standard Fields and Data Elements Can I Encrypt? on page 52 in Salesforce Help for a list of the encrypted Chatter fields.

- API Name—The API name for fields that contain data.
- Encrypted Records—The number of encrypted values stored in a field type across all objects of given type. For example, you select the Account object and see "9" in the Encrypted Records column next to Account Name. That means there are nine encrypted records across all Account Name fields.
- Unencrypted Records—The number of plaintext values stored in a field type.
- Mixed Tenant Secret Status—Indicates whether a mixture of active and archived tenant secrets apply to encrypted data in a field type.
- Mixed Schemes— Indicates whether a mixture of deterministic and probabilistic encryption schemes apply to encrypted data in a field type.

Note: The following applies to both encrypted and unencrypted records:

- The records count for a field doesn't include NULL or BLANK values. A field with NULL or BLANK values may show a different (smaller) records count than the actual number of records.
- The records count for compound fields such as Contact.Name or Contact.Address may show a different (larger) records count than the actual number of records. The count includes the two or more fields that are counted for every record.

**Usage Best Practices**

Use these statistics to make informed decisions about your key management tasks.

- Update encryption policies—The encryption statistics detail view shows you which fields in an object contain encrypted data. Use this information to periodically evaluate whether your encryption policies match your organization's encryption strategy.
- Rotate keys—You may want to encrypt all your data with your active tenant secret. Review the encryption summary pane on the left side of the page. If the percentage in the Uses Active Key column is lower than the percentage in the Data Encrypted column, some of your data uses an archived tenant secret. To synchronize your data, Contact Salesforce Customer Support.
- Synchronize data—Key rotation is an important part of any encryption strategy. When you rotate your key material, you may want to apply the active key material to existing data. Review the Uses Active Key and Mixed Tenant Secret Status columns to identify any fields that include data encrypted with an archived key. Make a note of these objects and fields, then contact Salesforce Customer Support to request the background encryption job. Salesforce Customer Support can focus just on those objects and fields you need to synchronize, keeping the background encryption job as short as possible.

# Synchronize Your Data Encryption with the Background Encryption Service

Periodically, you change your encryption policy. Or you rotate your keys. To get the most protection out of your encryption strategy, it's important to synchronize new and existing encrypted data under your most recent encryption policy and keys.

When change happens, Salesforce is here to help you synchronize your data. We can encrypt existing data in the background to ensure data alignment with the latest encryption policy and tenant secret.

## When We Do and Don't Automatically Encrypt Your Data

- When you turn on encryption for specific fields or other data, newly created and edited data are automatically encrypted with the most recent key.
- Data that's already in your org doesn't automatically get encrypted. Our background encryption service takes care of that on request.

- When you change your tenant secret as part of your key rotation strategy, data that's already encrypted remains encrypted with the old tenant secret. Our background encryption service can update it on request. And don't worry, you always have access to your data as long as you don't destroy the old, archived keys.
- If you turn off encryption, data that's already there is automatically decrypted based on the relevant key. Any functionality impacted by having decrypted data is restored.
- If Salesforce support re-encrypts your data with a new key, any data that was encrypted with the destroyed key is skipped. To access data encrypted with a destroyed key, import a backup of the destroyed key.

Note: Synchronizing your data encryption does not affect the record timestamp. It doesn't execute triggers, validation rules, workflow rules, or any other automated service.

## How to Request Background Encryption Service

**Allow lead time**

Contact Salesforce support 2–3 business days before you need the background encryption completed. The time to complete the process varies based on the volume of data. It could take several days.

**Specify the objects and fields**

Provide the list of objects and field names you want encrypted or re-encrypted.

**Verify the list**

Verify that this list matches the set of standard fields selected on the Encrypt Standard Fields page, and the custom fields you selected for encryption on the Field Definition page.

Tip: Also check that your field values aren't too long for encryption.

**Include files and attachments?**

Encryption for files and attachments is all or nothing. You don't have to specify which ones.

**Include history and feed data?**

Specify whether you want the corresponding field history and feed data encrypted.

**Choose a time**

Salesforce Customer Support can run the background encryption service Monday through Friday between 6 AM and 5 PM in your time zone.

Tip: If you're not sure which data is already encrypted, visit the Encryption Statistics page, which keeps a record of all fields that you have encrypted.

## What If You Destroyed Your Key?

If your encryption key has been destroyed, your data can't be automatically decrypted. You have some options for handling this data.

- Reimport the destroyed key from a backup, then ask Salesforce Customer Support to synchronize your data with your encryption policy.
- Delete all the data that was encrypted with the destroyed key, then ask Salesforce Customer Support to synchronize your data.
- Ask Salesforce Customer Support to mass overwrite the data that was encrypted with the destroyed key with "?????".

Note: When you disable encryption for files that were encrypted with a key that's been destroyed, the files don't automatically go away. You can ask Salesforce support to delete the files.

# Fix Compatibility Problems

When you select fields or files to encrypt, Salesforce automatically checks for potential side effects and warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

If your results include error messages, you're probably running into one or more of these limitations:

**Portals**

You can't encrypt standard fields, because a customer portal or a partner portal is enabled in your organization. To deactivate a customer portal, go to the Customer Portal Settings page in Setup. To deactivate a partner portal, go to the Partners page in Setup.

Note: Communities are not related to this issue. They are fully compatible with encryption.

**Criteria-Based Sharing Rules**

You've selected a field that is used in a filter in a criteria-based sharing rule.

**SOQL/SOSL queries**

You've selected a field that's used in an aggregate function in a SOQL query, or in a WHERE, GROUP BY, or ORDER BY clause.

**Formula fields**

You've selected a field that's referenced by a custom formula field in an unsupported way. Formulas can use BLANKVALUE, CASE, HYPERLINK, IF, IMAGE, ISBLANK, ISNULL, and NULLVALUE, as well as concatenation (&).

**Flows and Processes**

You've selected a field that's used in one of these contexts.

- To filter data in a flow
- To sort data in a flow
- To filter data in a process
- To filter data in a dynamic record choice
- To sort data in a dynamic record choice

Note: By default, your results only list the first 250 errors per element. You can increase the number of errors listed in your results to 5000. Contact Salesforce for help.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

SEE ALSO:

Encrypt New Data in Standard Fields

# Use Encrypted Data in Formulas

Use custom formula fields to quickly find encrypted data. You can write formulas with several operators and functions, render encrypted data in text, date, and date/time formats, and reference quick actions.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ‘15 and later.

Available in both Salesforce Classic and Lightning Experience.

## Supported Operators, Functions, and Actions

Supported operators and functions:

- `&` and `+` (concatenate)
- `BLANKVALUE`
- `CASE`
- `HYPERLINK`
- `IF`
- `IMAGE`
- `ISBLANK`
- `ISNULL`
- `NULLVALUE`

Also supported:

- Spanning
- Quick actions

Formulas can return data only in `text`, `date`, or `date/time` formats.

## `&` And `+` (Concatenate)

| | |
|---|---|
| **This works:** | `(encryptedField__c & encryptedField__c)` |
| **Why it works:** | This works because `&` is supported. |
| **This doesn’t work:** | `LOWER(encryptedField__c & encryptedField__c)` |
| **Why it doesn’t work:** | `LOWER` isn’t a supported function, and the input is an encrypted value. |

## Case

`CASE` returns encrypted field values, but doesn’t compare them.

| | |
|---|---|
| **This works:** | `CASE(custom_field__c, "1", cf2__c, cf3__c))`<br>where either or both `cf2__c` and `cf3__c` are encrypted |

**Why it works:**

`custom_field__c` is compared to “1”. If it is true, the formula returns `cf2__c` because it’s not comparing two encrypted values.

**This doesn’t work:**

```
CASE("1", cf1__c, cf2__c, cf3__c)
```

where `cf1__c` is encrypted

**Why it doesn’t work:**

You can’t compare encrypted values.

## `ISBLANK` and `ISNULL`

**This works:**

```
OR(ISBLANK(encryptedField__c), ISNULL(encryptedField__c))
```

**Why it works:**

Both `ISBLANK` and `ISNULL` are supported. `OR` works in this example because `ISBLANK` and `ISNULL` return a Boolean value, not an encrypted value.

## Spanning

**This works:**

```
(LookupObject1__r.City & LookupObject1__r.Street) &
 (LookupObject2__r.City & LookupObject2__r.Street) &
  (LookupObject3__r.City & LookupObject3__r.Street) &
   (LookupObject4__r.City & LookupObject4__r.Street)
```

**How and why you use it:**

Spanning retrieves encrypted data from multiple entities. For example, let’s say you work in the customer service department for Universal Containers. A customer has filed a case about a distribution problem, and you want to see the scope of the issue. You want all the shipping addresses related to this particular case. This example returns all the customers’ shipping addresses as a single string in your case layout.

## Validation

The encryption validation service checks your org to make sure that it’s compatible with encrypted formula field types.

When you encrypt a given field, the validation service:

- Retrieves all formula fields that reference the field
- Verifies that the formula fields are compatible with encryption
- Verifies that the formula fields aren’t used elsewhere for filtering or sorting

## Limits

Up to 200 formula fields can reference a given encrypted custom field. A field that is referenced by more than 200 formula fields can’t be encrypted. If you need to reference an encrypted custom field from more than 200 formula fields, contact Salesforce.

When you specify multiple fields to encrypt at one time, the 200-field limit is applied to the whole batch. If you know that you are encrypting fields that have multiple formula fields pointing to them, encrypt those fields one at a time.

## Apply Encryption to Fields Used in Matching Rules

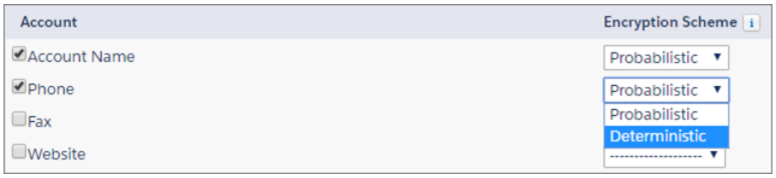
Matching rules used in duplicate management help you maintain clean and accurate data. Apply deterministic encryption to the fields to make them compatible with standard and custom matching rules.

Ask an administrator to enable **Deterministic Encryption** from the Platform Encryption Advanced Settings page. If you don't have a Data in Salesforce (Deterministic) type tenant secret, create one from the Platform Encryption Key Management page.

Important: Matching rules used in duplicate management don't support probabilistically encrypted data.

Follow these steps to add encrypted fields to existing custom matching rules.

1. From Setup, in the Quick Find box, enter `Matching Rules`, and then select **Matching Rules**.
2. Deactivate the matching rule that reference fields you want to encrypt. If your matching rule is associated with an active duplicate rule, first deactivate the duplicate rule from the Duplicate Rules page. Then return to the Matching Rules page and deactivate the matching rule.
3. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Policy**.
4. Click **Encrypt Fields**.
5. Click **Edit**.
6. Select the fields you want to encrypt, and select **Deterministic** from the Encryption Scheme list.



| Account | Encryption Scheme |
|---|---|
| ☑ Account Name | Probabilistic |
| ☑ Phone | Probabilistic |
| □ Fax | |
| □ Website | -------------------- |

7. Click **Save**.

   Tip: Standard matching rules are automatically deactivated when encryption is added to a field referenced by that rule. To encrypt fields referenced in standard matching rules, follow steps 3–8.

8. After you get the email verifying encryption's been enabled on your fields, reactivate your matching rule and associated duplicate management rule.
   Matching rules used in duplicate management now return exact and fuzzy matches on encrypted data.

Example: Let's say you recently encrypted Billing Address on your Contacts, and you want to add this field to a custom matching rule. First, deactivate the rule or rules you want to add this field to. Make sure that Billing Address is encrypted with the deterministic encryption scheme. Then add Billing Address to your custom matching rule, just like you would add any other field. Finally, reactivate your rule.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To enable encryption key (tenant secret) management:
- Manage Profiles and Permission Sets

When you rotate your key material, you must update custom matching rules that reference encrypted fields. After you rotate your key material, deactivate and then reactivate the affected matching rules. Then contact Salesforce to request the background encryption process. When the background encryption process finishes, your matching rules can access all data encrypted with your active key material.

Important: To ensure accurate matching results, customers who used the beta version of this feature must deactivate any matching rules that reference encrypted fields and then reactivate them. If your custom matching rule fails on reactivation, contact Salesforce for help reactivating your match index.

## Encrypt Data in Chatter

Enabling Shield Platform Encryption for Chatter adds an extra layer of security to information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

We recommend that you test Encryption for Chatter in a dedicated Sandbox environment before enabling it in production.

Unlike encryption for custom and standard fields, enabling encryption for Chatter encrypts all eligible Chatter fields.

1. Make sure that your org has an active encryption key. If you're not sure, check with your administrator.
2. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Policy**.
3. Click **Encrypt Chatter**.

The automatic Shield Platform Encryption validation service checks for settings that could block encryption. If the service finds potential problems, it sends you an email with suggestions for fixing the problems.

After you activate encryption for Chatter, new data that you enter into Chatter gets encrypted. To encrypt historic Chatter data, contact Salesforce Customer Support to request the background encryption service.

When you edit or update an encrypted Chatter field, the field's revision history is also encrypted. For example, if you update a post, the old version of the post remains encrypted.

If you enabled Encryption for Chatter in Spring '17 and you want to access the most up-to-date features, deselect **Encrypt Chatter** and then reselect **Encrypt Chatter**.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

# Encrypt Search Index Files

Sometimes you need to search for personally identifiable information (PII) or data that’s encrypted in the database. When you search your org, the results are stored in search index files. You can encrypt these search index files, adding another layer of security to your data.

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
2. Select **Search Index** from the picklist.
3. Select **Generate Tenant Secret**.
   This new tenant secret encrypts only the data stored in search index files.
4. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Policy**.
5. Select **Encrypt Search Indexes**.
   Your search indexes are now encrypted with the active Search Index tenant secret.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ’15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To enable encryption key (tenant secret) management:

- Manage Profiles and Permission Sets

# Encrypt Einstein Analytics Data

To get started with Einstein Analytics Encryption, generate a tenant secret with Shield Platform Encryption. Once you generate an Analytics tenant secret, Einstein Analytics Encryption uses the Shield Platform Encryption key management architecture to encrypt your Einstein Analytics data.

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
2. Select **Analytics** from the picklist.
3. Generate a tenant secret or upload key material.
4. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Policy**.
5. Select **Encrypt Einstein Analytics**.
6. Click **Save**.
   New datasets in Einstein Analytics are now encrypted.

   Note: Data that was in Einstein Analytics before encryption was enabled is not encrypted. If pre-existing data is imported from Salesforce objects through the dataflow, the data becomes encrypted on the next dataflow run. Other pre-existing data (such as CSV data) must be reimported to become encrypted. Although pre-existing data is not encrypted, it is still accessible and fully functional in its unencrypted state when encryption is enabled.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Einstein Analytics Platform and either Salesforce Shield or the Platform Encryption add-on.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To manage key material:
- Manage Encryption Keys

# Filter Encrypted Data with Deterministic Encryption

You can filter data that you have protected with Salesforce Shield Platform Encryption using deterministic encryption. Your users can filter records in reports and list views, even when the underlying fields are encrypted. Deterministic encryption supports WHERE clauses in SOQL queries and is compatible with unique and external ID fields. It also supports single-column indexes and single-column case-sensitive unique indexes. Shield Platform Encryption uses the Advanced Encryption Standard (AES) with 256-bit keys with CBC mode, and a static initialization vector (IV).

IN THIS SECTION:

By default, Salesforce encrypts data using a probabilistic encryption scheme. Each bit of data is turned into a fully random ciphertext string every time it’s encrypted. Encryption doesn’t generally impact users who are authorized to view the data. The exceptions are when logic is executed in the database or when encrypted values are compared to a string or to each other. In these cases, because the data has been turned into random, patternless strings, filtering isn’t possible. For example, you might run a SOQL query in custom Apex code against the Contact object, where LastName = 'Smith'. If the LastName field is encrypted with probabilistic encryption, you can’t run the query. Deterministic encryption addresses this problem.

Enable the deterministic encryption scheme, then apply deterministic encryption to fields.

# How Deterministic Encryption Supports Filtering

By default, Salesforce encrypts data using a probabilistic encryption scheme. Each bit of data is turned into a fully random ciphertext string every time it's encrypted. Encryption doesn't generally impact users who are authorized to view the data. The exceptions are when logic is executed in the database or when encrypted values are compared to a string or to each other. In these cases, because the data has been turned into random, patternless strings, filtering isn't possible. For example, you might run a SOQL query in custom Apex code against the Contact object, where LastName = 'Smith'. If the LastName field is encrypted with probabilistic encryption, you can't run the query. Deterministic encryption addresses this problem.

To be able to use filters when data is encrypted, we have to allow some patterns in our data. Deterministic encryption uses a static initialization vector (IV) so that encrypted data can be matched to a particular field value. The system can't read a piece of data that's encrypted, but it does know how to retrieve the ciphertext that stands for that piece of data thanks to the static IV. The IV is unique for a given field in a given org and can only be decrypted with your org-specific encryption key.

We evaluate the relative strengths and weaknesses of cryptographic approaches based on the types of attacks that can be launched against a particular algorithm. We also consider the length of time that it could take for the attack to succeed. For example, it is commonly said that a brute-force attack against an AES 256-bit key would take a billion billion years given current computing capabilities. Nevertheless, it is common practice to rotate keys regularly.

Certain kinds of attacks become a bit less far-fetched when you get away from purely random ciphertext. For example, an attacker could conceivably analyze deterministically encrypted ciphertext and determine that the cleartext string `Alice` always resolves to the ciphertext `YjNkY2JlNjU5M2JkNjk4MGJiNWE2NGQ5NzI5MzU1OTcNCg==`. Given enough time to eavesdrop, an attacker could defeat encryption by building a dictionary of cleartext values to ciphertext values.

The Salesforce Shield approach is to expose just enough determinism to enable bona fide users to filter on encrypted data while limiting it enough to ensure that a given plaintext value does not universally result in the same ciphertext value across all fields, objects, or orgs. Even if an attacker successfully matched cleartext to encrypted values for one field, the attacker would have to do it all over again for any other field, and again for the same field in another object.

In this way, deterministic encryption only decreases encryption strength as minimally necessary to allow filtering.

# Encrypt Data with the Deterministic Encryption Scheme

Enable the deterministic encryption scheme, then apply deterministic encryption to fields.

USER PERMISSIONS

Generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Enable features on the Advanced Settings page

- Customize Application

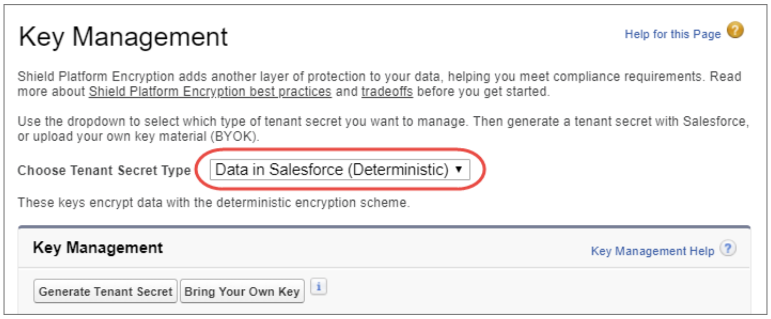
  AND

  Modify All Data

Important: To filter and execute queries on fields with unique attributes, synchronize new and existing encrypted data by the active Data in Salesforce (Deterministic) key material. See Synchronize Your Data Encryption with the Background Encryption Service for tips on timing and placing your background encryption service request.

1. From Setup, in the Quick Find box, enter *`Platform Encryption`*, and then select **Key Management**.
2. From the Choose Tenant Secret Type menu, select **Data in Salesforce**.
3. Generate or upload a tenant secret.
4. From Setup, in the Quick Find box, enter *`Platform Encryption`*, and then select **Advanced Settings**.
5. Enable **Deterministic Encryption**.
6. From Setup, select **Key Management**.
7. Select the **Data in Salesforce (Deterministic)** secret type.
8. Generate a tenant secret.

   You can mix and match probabilistic and deterministic encryption, encrypting some fields one way and some fields the other.



Key Management

Help for this Page

Shield Platform Encryption adds another layer of protection to your data, helping you meet compliance requirements. Read more about Shield Platform Encryption best practices and tradeoffs before you get started.

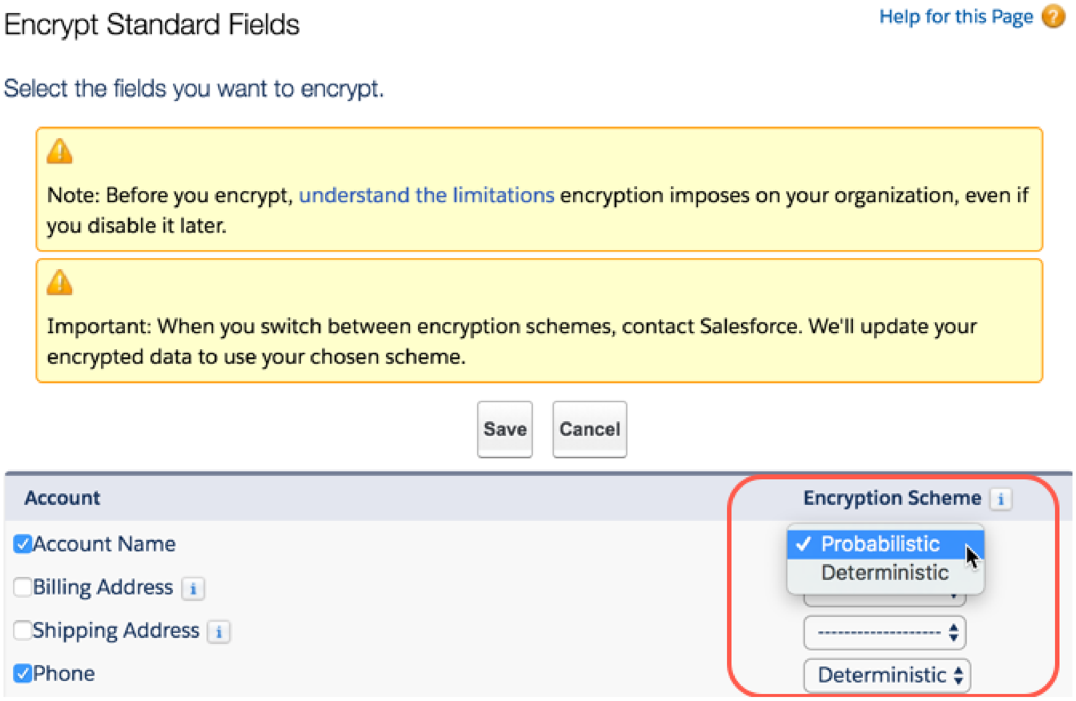
Use the dropdown to select which type of tenant secret you want to manage. Then generate a tenant secret with Salesforce, or upload your own key material (BYOK).

Choose Tenant Secret Type: Data in Salesforce (Deterministic)

These keys encrypt data with the deterministic encryption scheme.

9. Enable encryption for each field, specifying the deterministic encryption scheme. How you do that depends on whether it's a standard field or a custom field.

   - For standard fields, from Setup, select **Encryption Policy**, and then select **Encrypt Fields**. For each field you want to encrypt, select the field name, and then choose **Deterministic** from the Encryption Scheme list.



Encrypt Standard Fields

Help for this Page

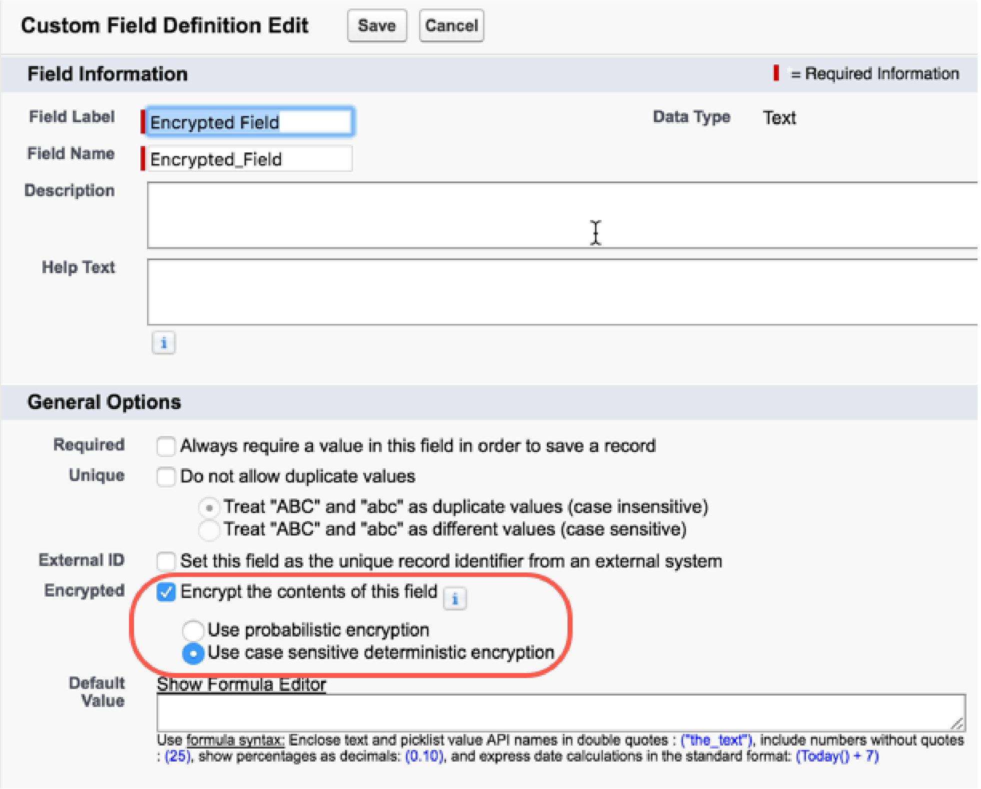
Select the fields you want to encrypt.

Note: Before you encrypt, understand the limitations encryption imposes on your organization, even if you disable it later.

Important: When you switch between encryption schemes, contact Salesforce. We'll update your encrypted data to use your chosen scheme.

| Account | Encryption Scheme |
|---|---|
| ☑ Account Name | ✓ Probabilistic<br>Deterministic |
| □ Billing Address | |
| □ Shipping Address | -------------------- |
| ☑ Phone | Deterministic |

   - For custom fields, open the Object Manager and edit the field you want to encrypt. Select **Encrypt the contents of this field**, and select **Use case sensitive deterministic encryption**.



**Custom Field Definition Edit** Save Cancel

**Field Information** ❙ = Required Information

| | | | |
|---|---|---|---|
| Field Label | Encrypted Field | Data Type | Text |
| Field Name | Encrypted_Field | | |
| Description | | | |
| Help Text | | | |

**General Options**

Required □ Always require a value in this field in order to save a record

Unique □ Do not allow duplicate values

● Treat "ABC" and "abc" as duplicate values (case insensitive)

○ Treat "ABC" and "abc" as different values (case sensitive)

External ID □ Set this field as the unique record identifier from an external system

Encrypted ☑ Encrypt the contents of this field

○ Use probabilistic encryption

● Use case sensitive deterministic encryption

Default Value Show Formula Editor

Use formula syntax: Enclose text and picklist value API names in double quotes : ("the_text"), include numbers without quotes : (25), show percentages as decimals: (0.10), and express date calculations in the standard format: (Today() + 7)

10. To encrypt your existing data with the active Data in Salesforce (Deterministic) key material, contact Salesforce Support. If you change the encryption scheme for a field from Deterministic to Probabilistic, contact Salesforce to re-encrypt data in that field with your active Data in Salesforce key material.

# Cache-Only Key Service (Beta)

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions. Requires purchasing Salesforce Shield or Platform Encryption.

Available in both Salesforce Classic and Lightning Experience.

Shield Platform Encryption's Cache-Only Key Service addresses a unique need for non-persisted key material. You can store your key material outside of Salesforce and have the Cache-Only Key Service fetch your key on demand from a key service that you control. Your key service transmits your key over a secure channel that you configure, and the Cache-Only Key Service uses your key for immediate encrypt and decrypt operations. Salesforce doesn't retain or persist your cache-only keys in any system of record or backups. You can revoke key material at any time.

Note: As a beta feature, Shield Platform Encryption Cache-Only Key Service is a preview and isn't part of the "Services" under your master subscription agreement with Salesforce. Use this feature at your sole discretion, and make your purchase decisions only from generally available products and features. Salesforce doesn't guarantee general availability of this feature within any particular time frame or at all, and we can discontinue it at any time. This feature is for evaluation purposes only. It's offered as is, and Salesforce has no liability for any harm or damage arising out of or in connection with it. All restrictions, Salesforce reservation of rights, obligations concerning the Services, and terms for related Non-Salesforce Applications and Content apply equally to your use of this feature. You can provide feedback and suggestions for Shield Platform Encryption Cache-Only Key Service in the IdeaExchange and through the Trailblazer Community. For information about enabling this feature in your organization, contact Salesforce.

IN THIS SECTION:

# How Cache-Only Keys Works

The Cache-Only Key Service lets you use a variety of key services to generate, secure, and store your key material. You can use an on-premises key service, host your own cloud-based key service, or use a cloud-based key brokering vendor.

Figures 1 and 2 show how Salesforce fetches keys on-demand from your specified key service. Whether you store your keys with an on-premises key service or a cloud-based key service, the flow is the same. When users access encrypted data, or add sensitive data to encrypted data elements, the Cache-Only Key Service makes a callout to your key service. Your key service passes key material, wrapped securely in JSON Web Encryption format, through a secure, authenticated channel that you set up.

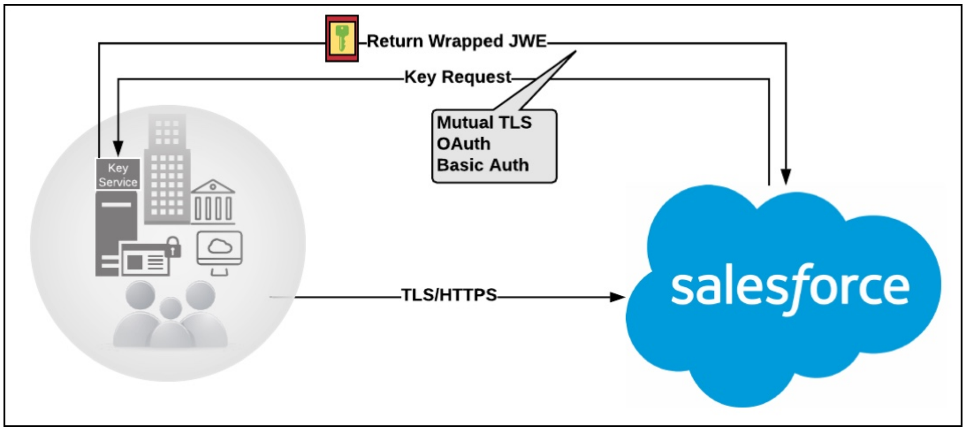


*Figure 1: On-premises Key Service*

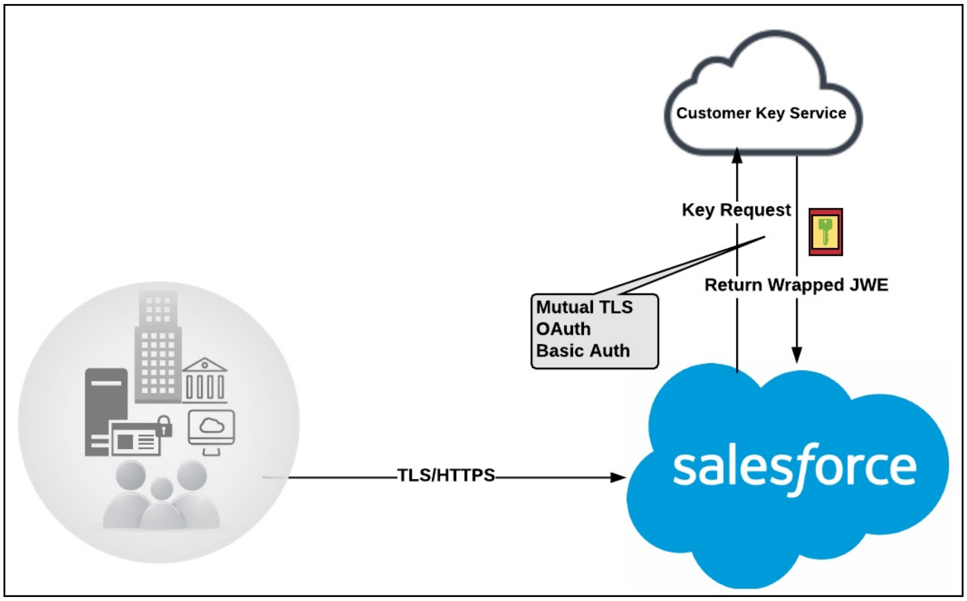


*Figure 2: Cloud-Based Key Service*

As a core offering of the Shield KMS, enhanced cache controls ensure that key material is stored securely while in the cache. The Shield KMS encrypts the fetched key material with an org-specific AES 256-bit cache encryption key and stores the encrypted key material in the cache for encrypt and decrypt operations. HSM-protected keys secure the cache encryption key in the cache, and the cache encryption key is rotated along with key lifecycle events such as key destruction and rotation.

The enhanced cache controls provide a single source of truth for key material used to encrypt and decrypt your data. Subsequent encryption and decryption requests go through the encrypted key cache until the cache-only key is revoked or rotated, or the cache is flushed. Once the cache is flushed, the Cache-Only Key Service fetches key material from your specified key service. The cache is regularly flushed every 72 hours, and certain Salesforce operations flush the cache on average every 24 hours. Destroying a data encryption key invalidates the corresponding data encryption key that's stored in the cache.

Because cache-only keys bypass the key derivation process, they're used to directly encrypt and decrypt your data.

# Prerequisites and Terminology for Cache-Only Keys

The Cache-Only Key Service offers you more control over your key material. When you use cache-only keys, you control more of the key management tasks. Before you start using the service, understand how to create and host your key material in a way that's compatible with Salesforce's BYOK service.

## Prerequisites

1. Generate and Host Key Material. The cache-only key exchange protocol and format requires that keys are wrapped in an opinionated JSON Web Encryption (JWE). This format uses RSAES-OAEP for key encryption and AES GCM for content encryption.

   Use a secure, trusted service to generate, store, and back up your key material.

2. Use and maintain a reliable high-availability key service. Choose a high-availability key service with an acceptable service level agreement (SLA), predefined maintenance procedures, and processes to mitigate any potential impact to business continuity.

   When the connection between Salesforce and your key service is broken, the Cache-Only Key Service can encrypt and decrypt data as long as your key material is in the cache. However, keys don't stay in the cache for long. The cache is regularly flushed every 72 hours, but some Salesforce operations flush the cache about every 24 hours.

   If your key material isn't in the cache, and the connection to your key service is broken, users can't encrypt or decrypt records. Make sure that you use a key service that Salesforce can connect to at any time. This is especially important during busy times like the end of year or end of quarter.

3. Maintain a secure callout endpoint. The cache-only key exchange protocol requires that keys are wrapped in an opinionated JSON format. Host your wrapped key inside the key response at a location Salesforce can request.

   To ensure easy IP whitelisting, the Cache-Only Key Service uses named credentials to establish a secure, authenticated, whitelisted connection to external sites. You can configure your named credentials to use popular authentication formats, such as Mutual TLS and OAuth. You can change these authentication protocols at any time.

4. Actively monitor your key service logs for errors. While Salesforce is here to help you with the Shield Platform Encryption service, you're responsible for maintaining the high-availability key service that you use to host your key material. You can use the RemoteKeyCalloutEvent object to review or track cache-only key events.

   Warning: Because you're in control of your keys, you're responsible for securing and backing up your key material. Salesforce can't retrieve lost key material stored outside of our encrypted key cache.

5. Format and Assemble Your Key Material. You must format key material hosted outside of Salesforce in a way that's compatible with the Cache-Only Key Service. Make sure that you can generate the following components in the required formats.

**Table 1: Cache-Only Key Components**

| Component | Format |
|---|---|
| Data encryption key (DEK) | AES 256-bit |
| Content encryption key (CEK) | AES 256-bit |
| BYOK-compatible certificate | A 4096-bit RSA certificate who's private key is encrypted with a derived, org-specific tenant secret key |
| JSON Web Encryption content and header | See a sample in Github |
| Algorithm for encrypting the CEK | RSA-OAEP |
| Algorithm for encrypting the DEK | A256GCM |

| Component | Format |
|---|---|
| Unique key identifier | Allows numbers, uppercase and lowercase letters, periods, hyphens, and underscores |
| Initialization vector | Encoded in base64url |

Read more about assembling your key material in the Generate and Assemble Cache-Compatible Keys section. You can also look at our Cache-Only Key Wrapper in Github for examples and sample utility.

## Terminology

Here are some terms that are specific to the Cache-Only Key Service.

**Content Encryption Key**

For each key request, your key service endpoint generates a unique content encryption key. The content encryption key wraps the data encryption key, which is in turn encrypted by the key encrypting key and placed in the JWE header of the key response.

**JSON Web Encryption**

The JSON-based structure that the Shield Platform Encryption service uses to encrypted content. JSON Web Encryption, or JWE, uses RSAES-OAEP for key encryption and AES GCM for content encryption.

**Key Identifier**

The Key ID, or KID, is the unique identifier for your key. The KID is used as the suffix in the named credential and for validation of the KID in the response. In Setup, enter this identifier in the Unique Key Identifier field.

# Create and Assemble Your Key Material

The Cache-Only Key Service is compatible with 256-bit AES keys returned in a JSON response, and then wrapped using JSON Web Encryption (JWE).

Cache-only key material is wrapped in a JSON format. An example cache-only key is used throughout this article to illustrate how key material changes as you assemble it.

1. Generate a 256-bit AES data encryption key. You can use the cryptographically secure method of your choice.
2. Generate a 256-bit AES content encryption key using a cryptographically secure method.
3. Generate and download your BYOK-compatible certificate.
4. Create the JWE protected header. The JWE protected header is a JSON object with 3 claims: the algorithm used to encrypt the content encryption key, the algorithm used to encrypt the data encryption key, and the unique ID of the cache-only key. Here's an example header to get us started.

```
{"alg":"RSA-OAEP","enc":"A256GCM","kid":"982c375b-f46b-4423-8c2d-4d1a69152a0b"}
```

5. Encode the JWE protected header as BASE64URL(UTF8(JWE Protected Header)).

```
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00iLCJraWQiOiI5ODJjMzc1Yi1mNDZiLTQ0MjMtOGMy
ZC00ZDFhNjkxNTJhMGIifQ
```

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions. Requires purchasing Salesforce Shield or Platform Encryption.

Available in both Salesforce Classic and Lightning Experience.

6. Encrypt the content encryption key with the public key from the BYOK certificate using the RSAES-OAEP algorithm. Then encode this encrypted content encryption key as BASE64URL(Encrypted CEK).

```
l92QA-R7b6Gtjo0tG4GlylJti1-Pf-519YpStYOp28YToMxgUxPmx4NR_myvfT24oBCWkh6hy_dqAL7JlVO4
49EglAB_i9GRdyVbTKnJQ1OiVKwWUQaZ9jVNxFFUYTWWZ-sVK4pUw0B3lHwWBfpMsl4jf0exP5-5amiTZ5oP
0rkW99ugLWJ_7XlyTuMIA6VTLSpL0YqChH1wQjo12TQaWG_tiTwL1SgRd3YohuMVlmCdEmR2TfwTvryLPx4K
bFK3Pv5ZSpSIyreFTh12DPpmhLEAVhCBZxR4-HMnZySSs4QorWagOaT8XPjPv46m8mUATZSD4hab8v3Mq4H3
3CmwngZCJXX-sDHuax2JUejxNC8HT5p6sa_I2gQFMlBC2Sd4yBKyjlDQKcSslCVav4buG8hkOJXY69iW_zhz
tV3DoJJ90l-EvkMoHpw1llU9lFhJMUQRvvocfghs2kzy5QC8QQt4t4Wu3p7IvzeneL5I81QjQlDJmZhbLLor
FHgcAs9_FMwnFYFrgsHP1_v3Iqy7zJJc60fCfDaxAF8Txj_LOeOMkCFl-9PwrULWyRTLMI7CdZIm7jb8v9AL
xCmDgqUi1yvEeBJhgMLezAWtxvGGkejc0BdsbWaPFXlI3Uj7C-Mw8LcmpSLKZyEnhj2x-3Vfv5hIVauC6ja1
B6Z_UcqXKOc
```

7. Generate an initialization vector for use as input to the data encryption key’s AES wrapping. Then encode it in base64url.

```
N2WVMbpAxipAtG9O
```

8. Wrap your data encryption key with your content encryption key.

   a. Encode the JWE header as ASCII(BASE64URL(UTF8(JWE Protected Header))).

   b. Reform authenticated encryption on the data encryption key with the AES GCM algorithm. Use the content encryption key as the encryption key, the initialization vector (the bytes, not the base64URL encoded version), and the Additional Authenticated Data value, requesting a 128-bit Authentication Tag output.

   c. Encode the resulting ciphertext as BASE64URL(Ciphertext).

   d. Encode the Authentication Tag as BASE64URL(Authentication Tag).

```
63wRVVKX0ZOxu8cKqN1kqN-7EDa_mnmk32DinS_zFo4
```

and

```
HC7Ev5lmsbTgwyGpeGH5Rw
```

9. Assemble your JWE as a compact serialization of all the preceding values. Concatenate values separated by a period.

```
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00iLCJraWQiOiI5ODJjMzc1Yi1mNDZiLTQ0MjMtOGMy
ZC00ZDFhNjkxNTJhMGIifQ.l92QA-R7b6Gtjo0tG4GlylJti1-Pf-519YpStYOp28YToMxgUxPmx4NR_myvf
T24oBCWkh6hy_dqAL7JlVO449EglAB_i9GRdyVbTKnJQ1OiVKwWUQaZ9jVNxFFUYTWWZ-sVK4pUw0B3lHwWB
fpMsl4jf0exP5-5amiTZ5oP0rkW99ugLWJ_7XlyTuMIA6VTLSpL0YqChH1wQjo12TQaWG_tiTwL1SgRd3Yoh
uMVlmCdEmR2TfwTvryLPx4KbFK3Pv5ZSpSIyreFTh12DPpmhLEAVhCBZxR4-HMnZySSs4QorWagOaT8XPjPv
46m8mUATZSD4hab8v3Mq4H33CmwngZCJXX-sDHuax2JUejxNC8HT5p6sa_I2gQFMlBC2Sd4yBKyjlDQKcSsl
CVav4buG8hkOJXY69iW_zhztV3DoJJ90l-EvkMoHpw1llU9lFhJMUQRvvocfghs2kzy5QC8QQt4t4Wu3p7Iv
zeneL5I81QjQlDJmZhbLLorFHgcAs9_FMwnFYFrgsHP1_v3Iqy7zJJc60fCfDaxAF8Txj_LOeOMkCFl-9Pwr
ULWyRTLMI7CdZIm7jb8v9ALxCmDgqUi1yvEeBJhgMLezAWtxvGGkejc0BdsbWaPFXlI3Uj7C-Mw8LcmpSLKZ
yEnhj2x-3Vfv5hIVauC6ja1B6Z_UcqXKOc.N2WVMbpAxipAtG9O.63wRVVKX0ZOxu8cKqN1kqN-7EDa_mnmk
32DinS_zFo4.HC7Ev5lmsbTgwyGpeGH5Rw
```

For more detailed examples of this process, check out the sample Cache-Only Key Wrapper in Github. You can use either the utility in this repository or another service of your choosing.

# Configure Your Cache-Only Key Callout Connection

Use a named credential to specify the endpoint for your callout, and identify the key that you want to use to encrypt your data.

1. From Setup, enter `Named Credential` in the Quick Find box, then select **Named Credential**.
2. Tip: A named credential provides an authenticated callout mechanism through which Salesforce can fetch your key material. Because Salesforce whitelists named credentials, they're a secure and convenient channel for key material stored outside of Salesforce.

   Learn more about named credentials, how to define a named credential, and how to grant access to authentication settings for named credentials in Salesforce Help.

   Create a named credential. Specify a BYOK-compatible certificate and an HTTPS endpoint.
3. From Setup, enter `Platform Encryption` in the Quick Find box and select **Advanced Settings**.
4. Turn on **Allow Cache-Only Keys with BYOK**.
5. From Setup, enter `Platform Encryption` in the Quick Find box, then select **Key Management**.
6. Choose a key type from the Tenant Secret Type dropdown.
7. Select **Bring Your Own Key**.
8. Select a BYOK-compatible certificate from the Choose Certificate dropdown.
9. Select **Use a Cache-Only Key**.
10. For Unique Key Identifier, enter your KID—the unique key identifier for your data encryption key. Your identifier can be a number, a string (2018_data_key), or a UUID (982c375b-f46b-4423-8c2d-4d1a69152a0b).
11. In the Named Credential dropdown, select the named credential associated with your key. You can have multiple keys associated with each named credential.

## EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions. Requires purchasing Salesforce Shield or Platform Encryption.

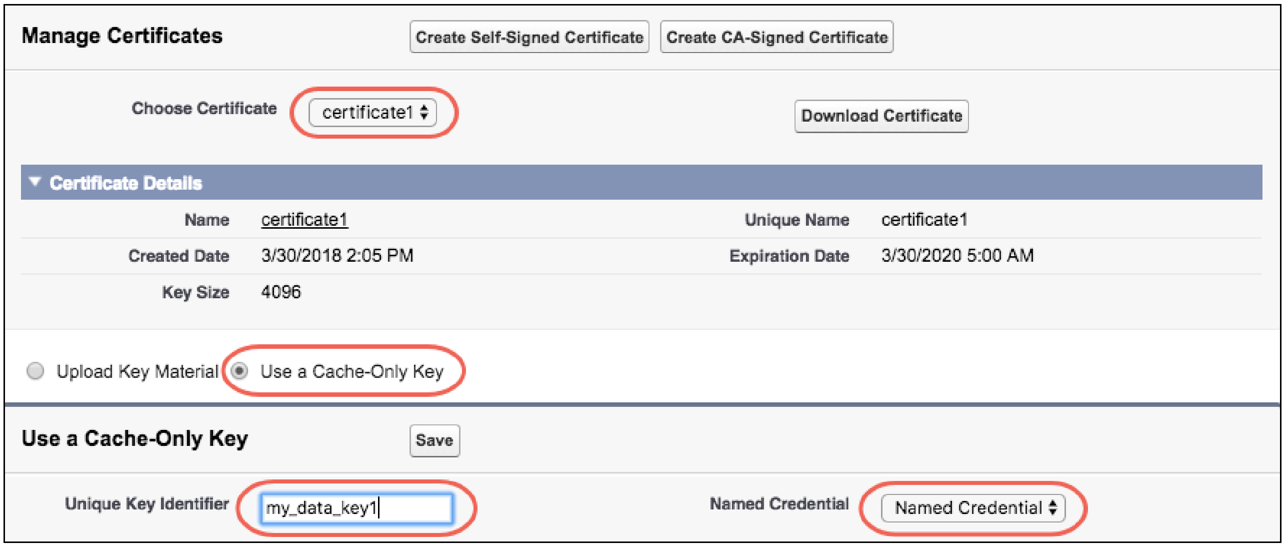
Available in both Salesforce Classic and Lightning Experience.

## USER PERMISSIONS

To create, edit, or delete named credentials:
- Customize Application

To enable features on the Advanced Settings page:
- Customize Application And Modify All Data

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:
- Manage Encryption Keys



**Manage Certificates**

Choose Certificate: certificate1

**Certificate Details**

| | | | |
|---|---|---|---|
| Name | certificate1 | Unique Name | certificate1 |
| Created Date | 3/30/2018 2:05 PM | Expiration Date | 3/30/2020 5:00 AM |
| Key Size | 4096 | | |

○ Upload Key Material ● Use a Cache-Only Key

**Use a Cache-Only Key**

Unique Key Identifier: my_data_key1

Named Credential: Named Credential

Salesforce checks the connection to the endpoint specified by the named credential. If Salesforce can reach the endpoint, the key specified for the Unique Key Identifier becomes the active key. If not, an error displays to help you troubleshoot the connection.

Cache-only key status is recorded as FETCHED on the Key Management page and in the API.

Tip: You can monitor key configuration callouts in the Setup Audit Trail. When a callout to an active or archived cache-only key is successful, the Setup Audit Trail logs an Activated status. Individual callouts are not monitored in Setup Audit Trail.

## Check Your Cache-Only Key Connection

Because your cache-only key material is stored outside of Salesforce, it's important to maintain a functional callout connection. Use the Callout Check page to monitor your connection and quickly respond to key service interruptions that could prevent the service from fetching your keys.

The Cache-Only Key: Callout Check page is accessible after you enable the Cache-Only Key Service in your org and make your first callout. Data presented as part of a callout check are never stored in the system of record.

1. From Setup, enter `Platform Encryption` in the Quick Find box, then select **Key Management**.
2. In the Actions column, next to the key material you want to check, click **Details**.
3. On the Cache-Only Key: Callout Check page, click **Check**.
   Details about your callout connection display on the page. It can take a few moments for the callout check to complete and display the results.

EDITIONS

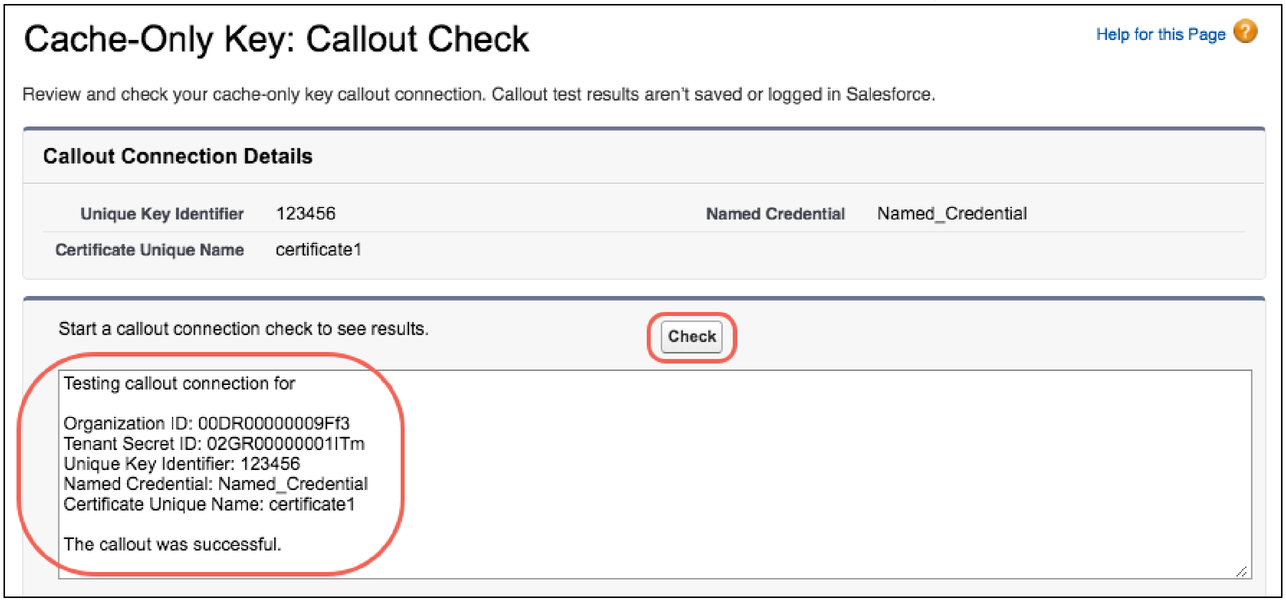
Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions. Requires purchasing Salesforce Shield or Platform Encryption.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys



Cache-Only Key: Callout Check

Review and check your cache-only key callout connection. Callout test results aren't saved or logged in Salesforce.

**Callout Connection Details**

| | | | |
|---|---|---|---|
| Unique Key Identifier | 123456 | Named Credential | Named_Credential |
| Certificate Unique Name | certificate1 | | |

Start a callout connection check to see results.

```
Testing callout connection for

Organization ID: 00DR00000009Ff3
Tenant Secret ID: 02GR00000001ITm
Unique Key Identifier: 123456
Named Credential: Named_Credential
Certificate Unique Name: certificate1

The callout was successful.
```

4. Review the details about your callout connection. If your callout connection was unsuccessful, you see a descriptive error message at the bottom of the results pane. Use this message to make the appropriate adjustments to your key service.

## Destroy a Cache-Only Key

When you destroy a cache-only key, you're destroying two things: the key in the cache, and the callout connection to the key service.

1. From Setup, enter `Platform Encryption` in the Quick Find box, then select **Key Management**.
2. Choose a key type from the Tenant Secret Type dropdown.
3. Click **Destroy**.
   Your key material's status is changed to Destroyed, and callouts to this key stop. Data encrypted with this key material is masked with "?????" in the app.

Note: Your cache-only key is unique to your org and to the specific data to which it applies. When you destroy a cache-only key, related data isn't accessible unless you reactivate it and make sure that Salesforce can fetch it.

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions. Requires purchasing Salesforce Shield or Platform Encryption.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

## Reactivate a Cache-Only Key

If you still have your named credential associated with a key that was destroyed in Salesforce, you can reactivate a destroyed cache-only key from Setup. Cache-only keys can't be reactivated programmatically. Reactivating a destroyed key makes it the active key. Before you reactivate a destroyed key, make sure that the corresponding key service connection is recovered.

1. From Setup, enter `Platform Encryption` in the Quick Find box, then select **Key Management**.
2. Next to cache-only key you want to reactivate, click **Activate**.

EDITIONS

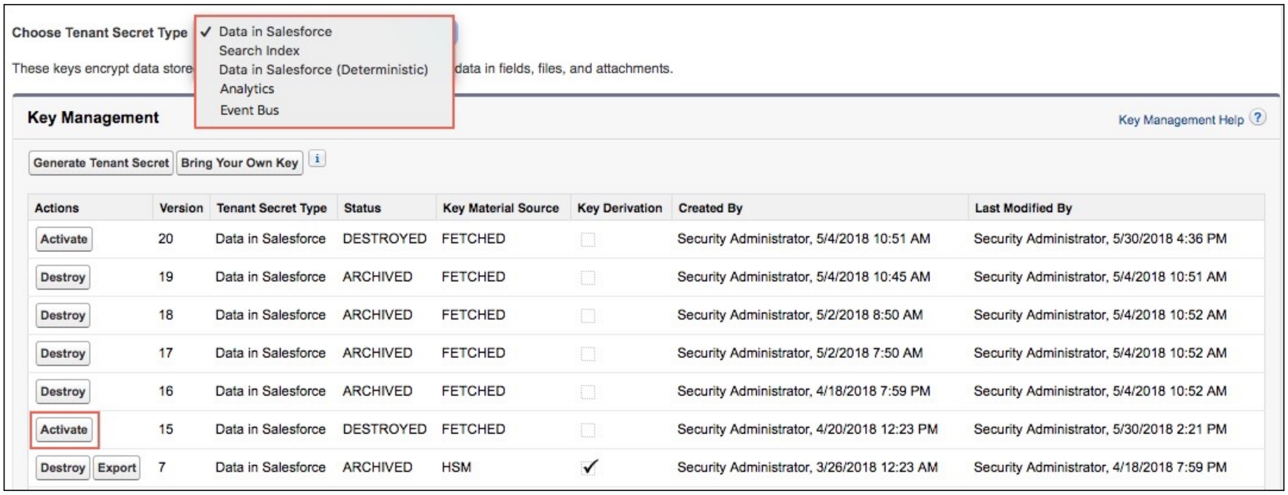
Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions. Requires purchasing Salesforce Shield or Platform Encryption.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys



Choose Tenant Secret Type

- ✓ Data in Salesforce
- Search Index
- Data in Salesforce (Deterministic)
- Analytics
- Event Bus

These keys encrypt data store data in fields, files, and attachments.

**Key Management**

| Actions | Version | Tenant Secret Type | Status | Key Material Source | Key Derivation | Created By | Last Modified By |
|---|---|---|---|---|---|---|---|
| Activate | 20 | Data in Salesforce | DESTROYED | FETCHED | □ | Security Administrator, 5/4/2018 10:51 AM | Security Administrator, 5/30/2018 4:36 PM |
| Destroy | 19 | Data in Salesforce | ARCHIVED | FETCHED | □ | Security Administrator, 5/4/2018 10:45 AM | Security Administrator, 5/4/2018 10:51 AM |
| Destroy | 18 | Data in Salesforce | ARCHIVED | FETCHED | □ | Security Administrator, 5/2/2018 8:50 AM | Security Administrator, 5/4/2018 10:52 AM |
| Destroy | 17 | Data in Salesforce | ARCHIVED | FETCHED | □ | Security Administrator, 5/2/2018 7:50 AM | Security Administrator, 5/4/2018 10:52 AM |
| Destroy | 16 | Data in Salesforce | ARCHIVED | FETCHED | □ | Security Administrator, 4/18/2018 7:59 PM | Security Administrator, 5/4/2018 10:52 AM |
| Activate | 15 | Data in Salesforce | DESTROYED | FETCHED | □ | Security Administrator, 4/20/2018 12:23 PM | Security Administrator, 5/30/2018 2:21 PM |
| Destroy Export | 7 | Data in Salesforce | ARCHIVED | HSM | ✓ | Security Administrator, 3/26/2018 12:23 AM | Security Administrator, 4/18/2018 7:59 PM |

The Shield Key Management Service fetches the reactivated cache-only key from your key service, and uses it to access data that was previously encrypted with it.

Note: You can sync your data to your active cache-only key just like you can with any other key material. When you rotate a cache-only key, contact Salesforce to request the background encryption service.

# Considerations for Cache-Only Keys

These considerations apply to all data that you encrypt using the Cache-Only Key Service.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

## Retry Policy

If Salesforce can't reach your external key service, the callout fails and your active cache-only key's status is set to Destroyed. This prevents excessive loads on both services. The Cache-Only Key Service then periodically retries the callout to help you minimize down time. Retries occur once per minute for five minutes, then once every five minutes for 24 hours. If the Cache-Only Key Service can successfully complete a callout during this retry period, your cache-only key's status is reset to Active.

At any point during a retry period, you can activate your key material through Setup or the API pending remote key service availability. If you reactivate your key material during the retry period, all retry attempts stop.

The RemoteKeyCalloutEvent object captures every callout to your key service. You can subscribe to this event with after insert Apex triggers, and set up real-time alerts that notify you when a callout fails.

## 401 HTTP Responses

In the event of a 401 HTTP response, Salesforce automatically refreshes any OAuth token associated with your named credential, and retries the request.

## Einstein Analytics

Backups of Einstein Analytics data are encrypted with your Shield Platform Encryption keys. If you encrypt data in Einstein Analytics datasets with a cache-only key, make sure that the Analytics cache-only key is in the same state as your Data in Salesforce-type cache-only key.

## Setup Audit Trail

Setup Audit Trail records activated cache-only key versions differently depending on whether a cache-only key with the Active status exists when you reactivate the key.

However, if you reactivate a destroyed key and there is already another key with the Active status, the Setup Audit Trail shows the reactivated key with an updated version number.

## Cache-Only Keys and Key Types

Use a separate cache-only key for each type of data you want to encrypt. You can't use a cache-only key with multiple key types. For example, you can't use a cache-only key to encrypt both search indexes and Einstein Analytics data.

## Service Protections

To protect against Shield KMS interruptions and ensure smooth encryption and decryption processes, you can have up to 10 active and archived cache-only keys of each type.

If you reach your key limit, destroy an existing key so that you can create, upload, reactivate, rearchive, or create a callout to another one. Remember to synchronize your data with an active key before destroying key material.

# Troubleshoot Cache-Only Keys

One or more of these frequently asked questions may help you troubleshoot any problems that arise.

**The callout to my key service isn't going through. What can I do?**

Callouts can fail for various reasons. Review the error message that displays and follow these tips for resolving the problem.

**Table 2: Cache-Only Key Service Errors**

| Error | Tips for Fixing the Problem |
|---|---|
| The remote key service returned an HTTP error: {000}. A successful HTTP response will return a 200 code. | To find out what went wrong, review the HTTP response code. |
| The remote key service returned an unsupported HTTP response code: {000}. A successful HTTP response will return a 200 code. | To find out what went wrong, review the HTTP response code. |
| The remote key service returned a content encryption key in the JWE that couldn't be decrypted with the certificate's private key. Either the JWE is corrupted, or the content | Check that you set up your named credential properly and are using the correct BYOK-compatible certificate. |

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

| Error | Tips for Fixing the Problem |
|---|---|
| encryption key is encrypted with a different key. | |
| The content encryption key couldn't decrypt the data encryption key that was returned in the remote key service's JWE. The data encryption key is either malformed, or encrypted with a different content encryption key. | Check that you set up your named credential properly and are using the correct BYOK-compatible certificate. Named credentials must call out to an HTTPS endpoint. |
| We can't parse the JSON returned by your remote key service. Contact your remote key service for help. | Contact your remote key service. |
| The remote key service returned a malformed JWE token that can't be decoded. Contact your remote key service for help. | Contact your remote key service. |
| The remote key service callout returned an empty response. Contact your remote key service for help. | Contact your remote key service. |
| The remote key service callout took too long and timed out. Try again. | If your key service is unavailable after multiple callout attempts, contact your remote key service. |
| The remote key service callout failed and returned an error: {000}. | Contact your remote key service. |
| The remote key service returned JSON with an incorrect key ID. Expected: {valid keyID}. Actual: {invalid keyID}. | Check that you set up your named credential properly and are using the correct BYOK-compatible certificate. |
| The remote key service returned a JWE header with an incorrect key ID. Expected: {valid keyID}. Actual: {invalid keyID}. | Check that you set up your named credential properly and are using the correct BYOK-compatible certificate. |
| The remote key service returned a JWE header that specified an unsupported algorithm (alg): {algorithm}. | The algorithm for encrypting the content encryption key in your JWE header must be in RSA-OAEP format. |
| The remote key service returned a JWE header that specified an unsupported encryption algorithm (enc): {your enc}. | The algorithm for encrypting the data encryption key in your JWE header must be in A256GCM format. |
| Data encryption keys encoded in a JWE must be 32 bytes. Yours is {value} bytes. | Make sure that your data encryption key is 32 bytes. |
| Your JWE header must use alg, enc, and kid parameters, but no others. Found: {parameter}. | Remove the unsupported parameters from your JWE header. |
| Authentication with the remote key service failed with the following error: {error}. | Check the authentication settings for your chosen named credential. |

The following key service errors can prevent the callout from completing. If you see errors related to these problems, contact your key service administrator for help.

- The JWE is corrupt or malformed.
- The data encryption key is malformed.
- The key service returned a malformed JWE token.
- The key service returned an empty response.

For uniform resource use, Salesforce limits the amount of time for each key service callout to 3 seconds. If the callout takes more than the allotted time, Salesforce fails the callout with a timeout error. Check that your key service is available. Make sure that your named credential references the correct endpoint—check the URL, including the IP address.

### Can I execute a remote callout in Apex?

Yes. Salesforce manages all authentication for Apex callouts that specify a named credential as the callout endpoint so that your code doesn’t have to. To reference a named credential from a callout definition, use the named credential URL. A named credential URL contains the scheme callout, the name of the named credential, and an optional path. For example: callout:My_Named_Credential/some_path.

See Named Credentials as Callout Endpoints in the Apex Developer Guide.

### Can I monitor my callout history?

If you want to review or track cache-only key events, use the RemoteKeyCalloutEvent standard object. Either use the `describeSObjects()` call to view event information, or an after insert Apex trigger to perform custom actions after each callout. For example, you can write a trigger that stores `RemoteKeyCallout` events in a custom object. When you store `RemoteKeyCallout` events in a custom object, you can monitor your callout history. See the RemoteKeyCalloutEvent entry in the SOAP API Developer Guide for more information.

The Setup Audit Trail tracks changes in key material state and named credential settings. Callout history isn’t recorded in log files.

### When I try to access data encrypted with a cache-only key, I see “?????” instead of my data. Why?

Masking means one of two things. Either the connection to your key service is broken and we can’t fetch your key, or the data is encrypted with a destroyed key. Check that your key service is available and that your named credential references the correct endpoint. If any key versions are marked as Destroyed as a result of a key service failure, recover the connection and manually activate the key version.

### Do I have to make a new named credential every time I rotate a key?

Nope. You can use a named credential with multiple keys. As long as you host your key material at the endpoint specified in an existing named credential, you’re all set. When you rotate your key material, change the key ID in the Unique Key Identifier field. Double-check that your new key is stored at the specified endpoint URL in your named credential.

### I’m still having problems with my key. Who should I talk to?

If you still have questions, contact your account executive or Customer Success manager. They’ll put you in touch with a support team specific to this feature.

# Manage Shield Platform Encryption

To provide Shield Platform Encryption for your organization, contact your Salesforce account executive. They'll help you provision the correct license so you can get started on creating your own unique tenant secret.

Assign the Manage Encryption Keys, Manage Certificates, and Customize Application permissions to people you trust to manage tenant secrets and certificates. Users with the Manage Encryption Keys permission can generate, export, import, and destroy organization-specific keys. It's a good idea to monitor the key management activities of these users regularly with the setup audit trail.

Users with both Manage Certificates and Manage Encryption Keys permissions can manage certificates and tenant secrets with the Shield Platform Encryption Bring Your Own Key (BYOK) service. You can also monitor these users' key and certificate management activities with the setup audit trail.

Authorized developers can generate, rotate, export, destroy, and reimport tenant secrets by coding a call to the TenantSecret object in the Salesforce API.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Encryption Keys

IN THIS SECTION:

Shield Platform Encryption Best Practices

Take the time to identify the most likely threats to your organization. This process helps you distinguish data that needs encryption from data that doesn't, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

Tradeoffs and Limitations of Shield Platform Encryption

A security solution as powerful as Shield Platform Encryption doesn't come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren't available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

SEE ALSO:

Which User Permissions Does Shield Platform Encryption Require?

The TenantSecret Object

## Generate a Tenant Secret

You can have Salesforce generate a unique tenant secret for your organization, or you can generate your own tenant secret using your own external resources. In either case, you manage your own tenant secret: you can rotate it, archive it, and designate other users to share responsibility for it.

When you generate a new tenant secret, any new data is encrypted using this key. However, existing sensitive data remains encrypted using previous keys. In this situation, we strongly recommend re-encrypting these fields using the latest key. Contact Salesforce for help with this.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

IN THIS SECTION:

Generate a Tenant Secret with Salesforce

Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

Manage Tenant Secrets by Type

Tenant secret types allow you to specify which kind of data you want to encrypt with a tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files or other data stored in tenant secret.

Generate Your Own Tenant Secret (BYOK)

When you supply your own tenant secret, you get the benefits of built-in Salesforce Shield Platform Encryption plus the extra assurance that comes from exclusively managing your tenant secret.

SEE ALSO:

Permission Sets

Profiles

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Encryption Keys

## Generate a Tenant Secret with Salesforce

Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

Only authorized users can generate tenant secrets from the Platform Encryption page. Ask your Salesforce admin to assign you the Manage Encryption Keys permission.

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
2. In the Choose Tenant Secret Type dropdown list, choose a data type.
3. Click **Generate Tenant Secret**.

   How often you can generate a tenant secret depends on the tenant secret type.

   - You can generate tenant secrets for the Data in Salesforce type once every 24 hours in production orgs, and once every 4 hours in Sandbox orgs.
   - You can generate tenant secrets for the Search Index type once every 7 days.

   Note: You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

   If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Encryption Keys

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

## Manage Tenant Secrets by Type

Tenant secret types allow you to specify which kind of data you want to encrypt with a tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files or other data stored in tenant secret.

Tenant secrets are categorized according to the kind of data they encrypt.

**Data in Salesforce**
Encrypts data using the probabilistic encryption scheme, including data in fields, attachments, and files other than search index files.

**Data in Salesforce (Deterministic)**
Encrypts data using the deterministic encryption scheme, including data in fields, attachments, and files other than search index files.

**Search Index**
Encrypts search index files.

**Analytics**
Encrypts Einstein Analytics data.

**Event Bus**
Encrypts data changes and the corresponding Change Data Capture event that contains them.

Note:

- Tenant secrets that were generated or uploaded before the Spring '17 release are categorized as the Data in Salesforce type.
- You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

  If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Certificates

  AND

  Manage Encryption Keys

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
2. In the Choose Tenant Secret Type dropdown list, choose a data type.

   The Key Management page displays all tenant secrets of each data type. If you generate or upload a tenant secret while viewing tenant secrets of a particular type, it becomes the active tenant secret for that data.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

# Generate Your Own Tenant Secret (BYOK)

When you supply your own tenant secret, you get the benefits of built-in Salesforce Shield Platform Encryption plus the extra assurance that comes from exclusively managing your tenant secret.

Controlling your own tenant secret entails contacting Salesforce Customer Support to enable Bring Your Own Keys, generating a BYOK-compatible certificate, using that certificate to encrypt and secure your self-generated tenant secret, then granting the Salesforce Shield Platform Encryption key management machinery access to your tenant secret.

IN THIS SECTION:

1. Generate a BYOK-Compatible Certificate

   To encrypt customer-supplied key material, use Salesforce to generate a 4096-bit RSA certificate. You can generate a self-signed or certificate-authority (CA) signed certificate. Each BYOK-compatible certificate's private key is encrypted with a derived, org-specific tenant secret key.

2. Generate and Wrap Your Tenant Secret

   Generate a random number as your tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the certificate you generated.

3. Upload Your Tenant Secret

   After you have your tenant secret, upload it to Salesforce. The Shield Key Management Service (KMS) uses your tenant secret to derive your org-specific data encryption key.

4. Opt-Out of Key Derivation with BYOK

   If you don't want Salesforce to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. Opting out gives you even more control of the key material used to encrypt and decrypt your data.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

To edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service:

- Manage Encryption Keys

  AND

  Manage Certificates

  AND

  Customize Application

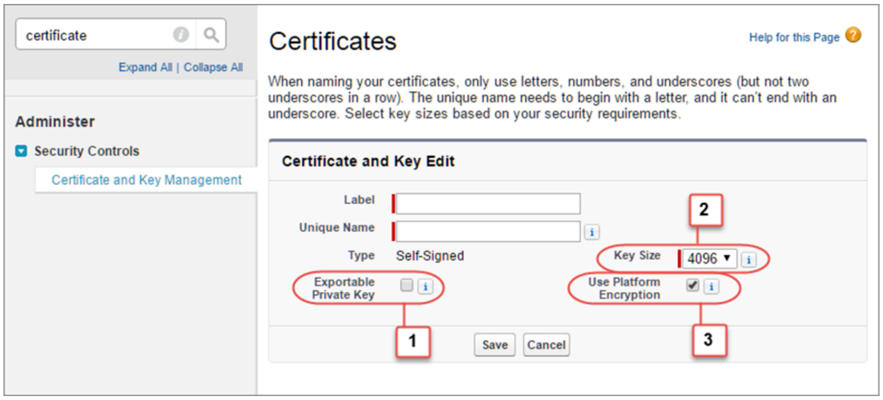
## Generate a BYOK-Compatible Certificate

To encrypt customer-supplied key material, use Salesforce to generate a 4096-bit RSA certificate. You can generate a self-signed or certificate-authority (CA) signed certificate. Each BYOK-compatible certificate’s private key is encrypted with a derived, org-specific tenant secret key.

To create a self-signed certificate:

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
2. Click **Bring Your Own Key**.
3. Click **Create Self-Signed Certificate**.
4. Enter a unique name for your certificate in the Label field. The Unique Name field automatically assigns a name based on what you enter in the Label field.

   The Exportable Private Key (1), Key Size (2), and Use Platform Encryption (3) settings are pre-set. These settings ensure that your self-signed certificate is compatible with Salesforce Shield Platform Encryption.



Certificates

When naming your certificates, only use letters, numbers, and underscores (but not two underscores in a row). The unique name needs to begin with a letter, and it can’t end with an underscore. Select key sizes based on your security requirements.

Certificate and Key Edit

Label

Unique Name

Type Self-Signed

Key Size 4096

Exportable Private Key ☐

Use Platform Encryption ☑

5. When the Certificate and Key Detail page appears, click **Download Certificate**.

   If you’re not sure whether a self-signed or CA-signed certificate is right for you, consult your organization’s security policy. See Certificates and Keys in Salesforce Help for more about what each option implies.

   To create a CA-signed certificate, follow the instructions in the Generate a Certificate Signed By a Certificate Authority topic in Salesforce Help. Remember to manually change the **Exportable Private Key**, **Key Size**, and **Platform Encryption** settings to ensure that your certificate is BYOK-compatible.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ’15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service

- Manage Certificates

  AND

  Customize Application

  AND

  Manage Encryption Keys

## Generate and Wrap Your Tenant Secret

Generate a random number as your tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the certificate you generated.

1. Generate a 256-bit tenant secret using the method of your choice.

   You can generate your tenant secret in one of 2 ways:

   - Use your own on-premises resources to generate a tenant secret programmatically, using an open-source library such as Bouncy Castle or OpenSSL.

     Tip: We've provided a script on page 50 that may be useful as a guide to the process.

   - Use a key brokering partner that can generate, secure, and share access to your tenant secret.

2. Wrap your tenant secret with the public key from the BYOK-compatible certificate you generated.

   Specify the OAEP padding scheme. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64.

3. Encode this encrypted tenant secret to base64.
4. Calculate an SHA-256 hash of the plaintext tenant secret.
5. Encode the SHA-256 hash of the plaintext tenant secret to base64.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service:

- Manage Certificates

  AND

  Customize Application

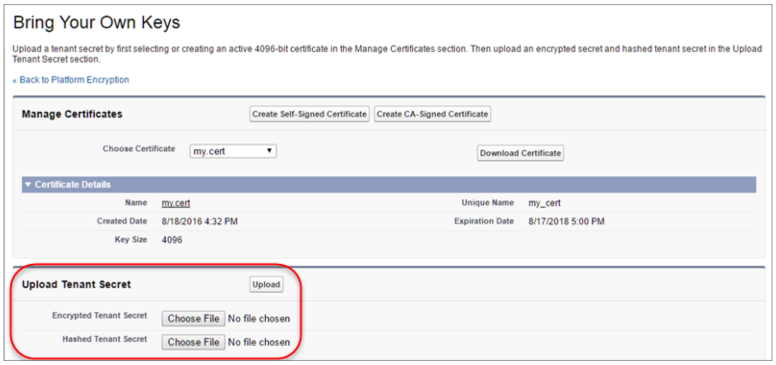
  AND

  Manage Encryption Keys

## Upload Your Tenant Secret

After you have your tenant secret, upload it to Salesforce. The Shield Key Management Service (KMS) uses your tenant secret to derive your org-specific data encryption key.

1. Make sure that your org has the Bring Your Own Keys feature enabled. To enable this feature, contact Salesforce Customer Support.
2. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
3. Click **Bring Your Own Key**.
4. In the Upload Tenant Secret section, attach both the encrypted key material and the hashed plaintext key material. Click **Upload**.



Bring Your Own Keys

Upload a tenant secret by first selecting or creating an active 4096-bit certificate in the Manage Certificates section. Then upload an encrypted secret and hashed tenant secret in the Upload Tenant Secret section.

« Back to Platform Encryption

Manage Certificates

Choose Certificate: my.cert

Certificate Details

| | | | |
|---|---|---|---|
| Name | my.cert | Unique Name | my_cert |
| Created Date | 8/18/2016 4:32 PM | Expiration Date | 8/17/2018 5:00 PM |
| Key Size | 4096 | | |

Upload Tenant Secret

Encrypted Tenant Secret: No file chosen

Hashed Tenant Secret: No file chosen

This tenant secret automatically becomes the active tenant secret.

Your tenant secret is now ready to be used for key derivation. From here on, the Shield KMS uses your tenant secret to derive an org-specific data encryption key. The app server then uses this key to encrypt and decrypt your users' data.

If you don't want Salesforce to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. For more information, see "Opt-Out of Key Derivation with BYOK" in Salesforce Help.

> Note: You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.
>
> If you reach the limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data that it encrypts with an active key.

5. Export your tenant secret, and back it up as prescribed in your organization's security policy.

   To restore a destroyed tenant secret, reimport it. The exported tenant secret is different from the tenant secret you uploaded. It's encrypted with a different key and has additional metadata embedded in it. See Back Up Your Tenant Secret in Salesforce Help.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

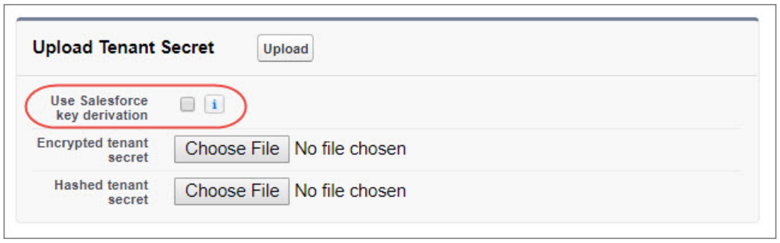
> Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

## Opt-Out of Key Derivation with BYOK

If you don’t want Salesforce to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. Opting out gives you even more control of the key material used to encrypt and decrypt your data.

Generate your customer-supplied data encryption key using a method of your choice. Then calculate an SHA256 hash of the key, and encrypt it with the public key from a BYOK-compatible certificate. See Upload Your Tenant Secret for details about how to prepare customer-supplied key material.

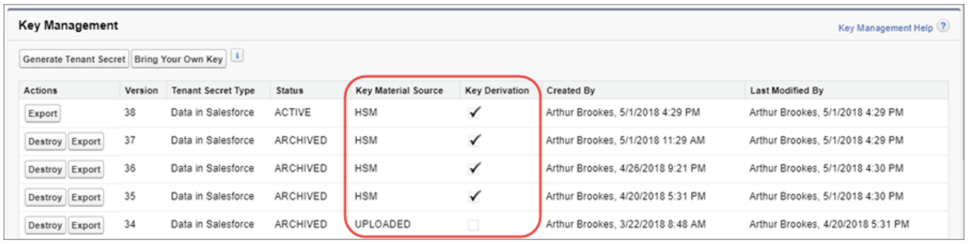
1. Make sure that your org has the Bring Your Own Keys feature enabled. To enable this feature, contact Salesforce Customer Support.
2. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Advanced Settings**.
3. Enable Allow BYOK to Opt-Out of Key Derivation.
   You can now opt out of key derivation when you upload key material.
4. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
5. Click **Bring Your Own Key**.
6. Uncheck **Use Salesforce key derivation**.



**Upload Tenant Secret** Upload

| | |
|---|---|
| Use Salesforce key derivation | □ |
| Encrypted tenant secret | Choose File No file chosen |
| Hashed tenant secret | Choose File No file chosen |

7. In the Upload Tenant Secret section, attach both your encrypted data encryption key and your hashed plaintext data encryption key.
8. Click **Upload**.
   This data encryption key automatically becomes the active key.



**Key Management** Key Management Help

Generate Tenant Secret | Bring Your Own Key

| Actions | Version | Tenant Secret Type | Status | Key Material Source | Key Derivation | Created By | Last Modified By |
|---|---|---|---|---|---|---|---|
| Export | 38 | Data in Salesforce | ACTIVE | HSM | ✓ | Arthur Brookes, 5/1/2018 4:29 PM | Arthur Brookes, 5/1/2018 4:29 PM |
| Destroy Export | 37 | Data in Salesforce | ARCHIVED | HSM | ✓ | Arthur Brookes, 5/1/2018 11:29 AM | Arthur Brookes, 5/1/2018 4:29 PM |
| Destroy Export | 36 | Data in Salesforce | ARCHIVED | HSM | ✓ | Arthur Brookes, 4/26/2018 9:21 PM | Arthur Brookes, 5/1/2018 4:30 PM |
| Destroy Export | 35 | Data in Salesforce | ARCHIVED | HSM | ✓ | Arthur Brookes, 4/20/2018 5:31 PM | Arthur Brookes, 5/1/2018 4:30 PM |
| Destroy Export | 34 | Data in Salesforce | ARCHIVED | UPLOADED | □ | Arthur Brookes, 3/22/2018 8:48 AM | Arthur Brookes, 4/20/2018 5:31 PM |

From now on, the Shield Key Management Service (KMS) skips the derivation process and uses your data encryption key to directly encrypt and decrypt your data. You can review the derivation status of all key material on the Key Management page.

9. Export your data encryption key and back it up as prescribed in your organization’s security policy.

   To restore your data encryption key, reimport it. The exported data encryption key is different from the data encryption key you uploaded. It is encrypted with a different key and has additional metadata embedded in it. See Back Up Your Tenant Secret in Salesforce Help.

### EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ’15 and later.

Available in both Salesforce Classic and Lightning Experience.

### USER PERMISSIONS

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

To enable features on the Advanced Settings page:

- Customize Application

  AND

  Modify All Data

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

# Rotate Your Encryption Tenant Secrets

You control the life cycle of your data encryption keys by controlling the life cycle of your tenant secrets. It's recommended to regularly generate a new tenant secret and archive the previously active one.

Consult your organization's security policies to decide how often to rotate your tenant secrets. You can rotate a tenant secret once every 24 hours in production orgs and every 4 hours in sandbox environments.

The key derivation function uses a master secret, which is rotated with each major Salesforce release. Master secret rotation doesn't impact your encryption keys or your encrypted data until you rotate your tenant secret.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Key Management**.
2. From the Choose Tenant Secret Type dropdown, choose a data type.
3. Check the status of the data type's tenant secrets. Existing tenant secrets are listed as active, archived, or destroyed.

   **ACTIVE**

   Can be used to encrypt and decrypt new or existing data.

   **ARCHIVED**

   Can't encrypt new data. Can be used to decrypt data previously encrypted with this key when it was active.

   **DESTROYED**

   Can't encrypt or decrypt data. Data encrypted with this key when it was active can no longer be decrypted. Files and attachments encrypted with this key can no longer be downloaded.

4. Click **Generate New Tenant Secret** or **Bring Your Own Key**. If uploading a customer-supplied tenant secret, upload your encrypted tenant secret and tenant secret hash.

   Note: You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

   If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

5. If you want to re-encrypt field values with your active key material, contact Salesforce Customer Support. We'll help you encrypt existing data in the background to ensure data alignment with your latest encryption policy and key material configuration.

   Warning: For clean and consistent results, we recommend that you contact Salesforce Customer Support for help reencrypting your data. You can apply your active key material to existing records by editing them through Setup, or programmatically through the API. Editing a record triggers the encryption service to encrypt the existing data again using the newest key material. This update changes the record's timestamp, and the update is recorded in the field history or Feed History. However, the field history in the History related list and Feed History aren't reencrypted with the new key material.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

# Back Up Your Tenant Secret

Your tenant secret is unique to your organization and to the specific data to which it applies. Salesforce recommends that you export your secret to ensure continued data access in cases where you need to gain access to the related data again.

1. In Setup, use the `Quick Find` box to find the Platform Encryption setup page.
2. In the table that lists your keys, find the tenant secret you want and click **Export**.
3. Confirm your choice in the warning box, then save your exported file.

   The file name is `tenant-secret-org-<organization ID>-ver-<tenant secret version numer>.txt`. For example, `tenant-secret-org-00DD00000007eTR-ver-1.txt`.
4. Note the specific version you're exporting, and give the exported file a meaningful name. Store the file in a safe location in case you need to import it back into your organization.

   Note: Your exported tenant secret is itself encrypted.
5. To import your tenant secret again, click **Import** > **Choose File** and select your file. Make sure you're importing the correct version of the tenant secret.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

## EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

## USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

# Destroy A Tenant Secret

Only destroy tenant secrets in extreme cases where access to related data is no longer needed. Your tenant secret is unique to your organization and to the specific data to which it applies. Once you destroy a tenant secret, related data is not accessible unless you previously exported the key and then import the key back into Salesforce.

You are solely responsible for making sure your data and tenant secrets are backed up and stored in a safe place. Salesforce can't help you with deleted, destroyed, or misplaced tenant secrets.

1. In Setup, use the `Quick Find` box to find the Platform Encryption setup page.
2. In the table that lists your tenant secrets, go to the row that contains the one you want to destroy and click **Destroy**.
3. A warning box appears. Type in the text as shown and select the checkbox acknowledging that you're destroying a tenant secret, then click **Destroy**.

File previews and content that was already cached in the user's browser may still be visible in cleartext after you destroy the key that encrypted that content, until the user logs in again.

If you create a sandbox organization from your production organization and then destroy the tenant secret in your sandbox organization, the tenant secret still exists in the production organization.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

# Disable Encryption on Fields

At some point, you may need to disable Shield Platform Encryption for fields, files, or both. You can turn field encryption on or off individually, but file encryption is all or nothing.

When you turn off Shield Platform Encryption for a field, most encrypted data is automatically mass-decrypted. The decryption starts automatically after you disable encryption for specific fields and save your changes. When data is decrypted, any functionality that was limited or unavailable when the data was encrypted is also restored. Salesforce notifies you by email when the decryption process is complete.

Long text area and rich text area field types can't be automatically decrypted. If you decrypt data encrypted with a destroyed key, that data can't be mass-decrypted.

Note: If you disable Shield Platform Encryption and can't access data in fields that were previously encrypted, contact Salesforce for help.

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Encryption Policy**.
2. Click **Encrypt Fields**, then click **Edit**.
3. Deselect the fields you want to stop encrypting, then click **Save**.
   Users can see data in these fields.
4. To disable encryption for files or Chatter, deselect those features from the **Encryption Policy** page and click **Save**.

The functionality that was limited or changed by Platform Encryption is restored for your data after it's decrypted.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To disable encryption:

- Customize Application

# Require Two-Factor Authentication for Key Management

Two-factor authentication is a powerful tool for securing access to data and resources. You can require two-factor authentication for key management tasks like generating, rotating, or uploading key material and certificates.

Important: Make sure that you provide security administrators a way to get a time-based, one-time password. This password is their second authentication factor. Otherwise, they can't complete encryption key-related tasks.

1. From Setup, in the Quick Find box, enter `Identity Verification`, and then select **Identity Verification**.
2. Select **Raise session to high-assurance** from the Manage Encryption Keys dropdown.
   All admins with the Manage Encryption Keys permission must use a second form of authentication to complete key management tasks through Setup and the API.

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To assign identity verification for key management tasks:

- Manage Encryption Keys

# How Shield Platform Encryption Works

Shield Platform Encryption relies on a unique tenant secret that you control and a master secret that's maintained by Salesforce. We combine these secrets to create your unique data encryption key. We use that key to encrypt data that your users put into Salesforce, and to decrypt data when your authorized users need it.

Encrypting files, fields, and attachments has no effect on your organization's storage limits.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Can I Bring My Own Encryption Key?

Yes. You can generate and store your customer-supplied key material outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

Which Standard Fields and Data Elements Can I Encrypt?

You can encrypt certain fields on standard and custom objects, data in Chatter, and search index files. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

Which Custom Fields Can I Encrypt?

You can encrypt the contents of fields that belong to one of these custom field types, on either standard or custom objects.

Which Files Are Encrypted?

When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it's uploaded.

Which User Permissions Does Shield Platform Encryption Require?

Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or key material. Enable these permissions for user profiles just like you would any other user permission.

Why Isn't My Encrypted Data Masked?

If the encryption service isn't available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don't want some users to see, revisit those users' field-level security settings, record access settings, and object permissions.

Behind the Scenes: The Shield Platform Encryption Process

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn't there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The encryption service then encrypts the data on the application server.

Behind the Scenes: The Search Index Encryption Process

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

How Do I Deploy Shield Platform Encryption?

When you deploy Shield Platform Encryption to your org with a tool such as Force.com IDE, Migration Tool, or Workbench, the Encrypted field attribute persists. However, if you deploy to orgs with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target org.

How Does Shield Platform Encryption Work In a Sandbox?

Refreshing a sandbox from a production organization creates an exact copy of the production organization. If Shield Platform Encryption is enabled on the production organization, all encryption settings are copied, including tenant secrets created in production.

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.

What's the Difference Between Classic Encryption and Shield Platform Encryption?

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

## Can I Bring My Own Encryption Key?

Yes. You can generate and store your customer-supplied key material outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

To work with our key management machinery, your customer-supplied key material needs to meet these specifications:

- 256-bit size
- Encrypted with a public RSA key that is extracted from the downloaded BYOK certificate, then padded using OAEP padding
- Once it's encrypted, it must be encoded in standard base64

To work with encryption keys, you'll need the Manage Encryption Keys permission. To generate BYOK-compatible certificates, you'll need the Customize Application permission.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Why Bring Your Own Key?

Bring Your Own Key (BYOK) gives you an extra layer of protection in the event of unauthorized access to critical data. It may also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. Once you've set up your key material, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

Take Good Care of Your Keys

When you create and store your own key material outside of Salesforce, it's important that you safeguard that key material. Make sure that you have a trustworthy place to archive your key material; never save a tenant secret or data encryption key on a hard drive without a backup.

Sample Script for Generating a BYOK Tenant Secret

We've provided a helper script that may be handy for preparing your tenant secret for installation. It generates a random number as your tenant secret, calculates a SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

Troubleshooting Bring Your Own Key

One or more of these frequently asked questions may help you troubleshoot any problems that arise.

## Why Bring Your Own Key?

Bring Your Own Key (BYOK) gives you an extra layer of protection in the event of unauthorized access to critical data. It may also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. Once you've set up your key material, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

Shield Platform Encryption enables Salesforce administrators to manage the lifecycle of their data encryption keys while protecting these keys from unauthorized access. By controlling the lifecycle of your organization's tenant secrets, you control the lifecycle of the data encryption keys derived from them. Alternatively, you can opt out of key derivation altogether and upload a final data encryption key.

Data encryption keys aren't stored in Salesforce. Instead, they're derived from the master secret and tenant secret on demand whenever a key is needed to encrypt or decrypt customer data. The master secret is generated once per release for everyone by a hardware security module (HSM). The tenant secret is unique to your org, and you control when it is generated, activated, revoked, or destroyed.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

You have three options for setting up your key material.

- Use the Shield Key Management Service (KMS) to generate your org-specific tenant secret for you.
- Use the infrastructure of your choice, such as an on-premises HSM, to generate and manage your tenant secret outside of Salesforce. Then upload that tenant secret to the Salesforce KMS. This option is popularly known as "Bring Your Own Key," although the element you're really bringing is the tenant secret from which the key is derived.
- Opt out of the Shield KMS key derivation process with the Bring Your Own Key service. Use the infrastructure of your choice to create a data encryption key instead of a tenant secret. Then upload this data encryption key to the Shield KMS. When you opt out of derivation on a key-by-key basis, the Shield KMS bypasses the derivation process and uses this key material as your final data encryption key. You can rotate customer-supplied data encryption keys just like you would rotate a customer-supplied tenant secret.

## Take Good Care of Your Keys

When you create and store your own key material outside of Salesforce, it's important that you safeguard that key material. Make sure that you have a trustworthy place to archive your key material; never save a tenant secret or data encryption key on a hard drive without a backup.

Back up all imported key material after you upload them to Salesforce. This ensures that you have copies of your active key material. See Back Up Your Tenant Secret in Salesforce Help.

Review your company policy on key rotation. You can rotate and update your keys on your own schedule. See Rotate Your Encryption Keys.

Important: If you accidentally destroy a tenant secret that isn't backed up, Salesforce won't be able to help you retrieve it.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

## Sample Script for Generating a BYOK Tenant Secret

We've provided a helper script that may be handy for preparing your tenant secret for installation. It generates a random number as your tenant secret, calculates a SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

1. Download the script from the Salesforce Knowledge Base. Save it in the same directory as the certificate.
2. Run the script specifying the certificate name, like this: `./secretgen.sh my_certificate.crt`

   Replace this certificate name with the actual filename of the certificate you downloaded.

   Tip: If needed, use `chmod +w secretgen.sh` to make sure you have write permission to the file and use `chmod 775` to make it executable.
3. The script generates a number of files. Look for the two files that end with the .b64 suffix. The files ending in .b64 are your base 64-encoded encrypted tenant secret and base 64-encoded hash of the plaintext tenant secret. You'll need both of these files for the next step.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

## Troubleshooting Bring Your Own Key

One or more of these frequently asked questions may help you troubleshoot any problems that arise.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

**I'm trying to use the script you provide, but it won't run.**

Make sure that you are running the right script for your operating system. If you are working on a Windows machine, you can install a Linux emulator and use the Linux script. These issues can also prevent the script from running:

- You don't have write permission in the folder you're trying to run the script from. Try running the script from a folder that you have write permission for.
- The certificate that the script references is missing. Make sure you've properly generated the certificate.
- The certificate is missing or is not being referenced by the correct name. Make sure you've entered the correct file name for your certificate in the script.

**I want to use the script you provide, but I also want to use my own random number generator.**

The script we provide uses a random number generator to create a random value that is then used as your tenant secret. If you would like to use a different generator, replace `head -c 32 /dev/urandom | tr '\n' =` (or, in the Mac version, `head -c 32 /dev/urandom > $PLAINTEXT_SECRET`) with a command that generates a random number using your preferred generator.

**What if I want to use my own hashing process to hash my tenant secret?**

No problem. Just make sure that the end result meets these requirements:

- Uses an SHA-256 algorithm.
- Results in a base64 encoded hashed tenant secret.
- Generates the hash of the random number BEFORE encrypting it.

If any of these three criteria aren't met, you won't be able to upload your tenant secret.

**How should I encrypt my tenant secret before I upload it to Salesforce?**

If you're using the script provided, the encryption process is taken care of. If you do not use the script, specify the OAEP padding scheme when you encrypt your tenant secret. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64. If either of these criteria are not met, you won't be able to upload your tenant secret.

If you choose to not use the script provided, follow the instructions in the Generate And Wrap Your Tenant Secret Help topic.

**I can't upload my Encrypted tenant secret and Hashed tenant secret.**

A handful of errors can prevent your files from uploading. Use the chart to make that sure your tenant secrets and certificates are in order.

| Possible cause | Solution |
|---|---|
| Your files were generated with an expired certificate. | Check the date on your certificate. If it has expired, you can renew your certificate or use another one. |
| Your certificate is not active, or is not a valid Bring Your Own Key certificate. | Ensure that your certificate settings are compatible with the Bring Your Own Key feature. Under the Certificate and Key Edit section of the Certificates page, select a 4096-bit certificate size, disable Exportable Private Key, and enable Platform Encryption. |
| You haven't attached both the encrypted tenant secret and the hashed tenant secret. | Make sure that you attach both the encrypted tenant secret and hashed tenant secret. Both of these files should have a .b64 suffix. |

| Possible cause | Solution |
|---|---|
| Your tenant secret or hashed tenant secret wasn't generated properly. | Several problems can cause this error. Usually, the tenant secret or hashed tenant secret wasn't generated using the correct SSL parameters. If you are using OpenSSL, you can refer to the script for an example of the correct parameters you should use to generate and hash your tenant secret. If you are using a library other than OpenSSL, check that library's support page for help finding the correct parameters to both generate and hash your tenant secret.<br>Still stuck? Contact your Salesforce account executive. They'll put you in touch with someone at Salesforce who can help. |

**I'm still having problems with my key. Who should I talk to?**

If you still have questions, contact your account executive. They'll put you in touch with a support team specific to this feature.

## Which Standard Fields and Data Elements Can I Encrypt?

You can encrypt certain fields on standard and custom objects, data in Chatter, and search index files. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

When you encrypt a field, existing values aren't encrypted immediately. Values are encrypted only after they are touched. Contact Salesforce for help encrypting existing data.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

### Encrypted Standard Fields

You can encrypt the contents of these standard field types.

**Accounts**

- Account Name
- Account Site
- Billing Address (encrypts Billing Street and Billing City)
- Description
- Fax
- Phone
- Shipping Address (encrypts Shipping Street and Shipping City)
- Website

Note: If your org has enabled Person Accounts, certain account and contact fields are combined into one record. In that case, you can enable encryption for a different set of Account fields.

**Accounts (if Person Accounts enabled for your org)**

- Account Name
- Account Site
- Assistant
- Assistant Phone
- Billing Address (encrypts Billing Street and Billing City)
- Description

- Email
- Fax
- Home Phone
- Mailing Address (encrypts Mailing Street and Mailing City)
- Mobile
- Other Address (encrypts Other Street and Other City)
- Other Phone
- Phone
- Shipping Address (encrypts Shipping Street and Shipping City)
- Title
- Website

### Activities

- Description—Event

Note: Encrypting Description—Event also encrypts Comment—Task.

### Cases

- Description
- Subject

### Case Comments

- Body (including internal comments)

### Contacts

- Assistant
- Assistant Phone
- Description
- Email
- Fax
- Home Phone
- Mailing Address (encrypts Mailing Street and Mailing City)
- Mobile
- Name (encrypts First Name, Middle Name, and Last Name)
- Other Address (encrypts Other Street and Other City)
- Other Phone
- Phone
- Title

### Contracts

- Billing Address (encrypts Billing Street and Billing City)
- Shipping Address (encrypts Shipping Street and Shipping City)

### Custom Objects

- Name

### Email Messages (beta)

- From Name
- From Address
- To Address
- CC Address
- BCC Address
- Subject
- Text Body
- HTML Body
- Headers

If you use Email-to-Case, these fields are also encrypted on the customer emails that generate cases.

### Email Message Relations (beta)

- Relation Address

### Leads

- Address (Encrypts Street and City)
- Company
- Description
- Email
- Fax
- Mobile
- Name (Encrypts First Name, Middle Name, and Last Name)
- Phone
- Title
- Website

### List Emails

- From Name
- From Address
- Reply To Address

### List Email Sent Results

- Email

### Opportunities

- Description
- Next Step
- Opportunity Name

### Service Appointments

- Address (Encrypts Street and City)
- Description
- Subject

### Work Orders

- Address (Encrypts Street and City)
- Description
- Subject

### Work Order Line Items

- Address (Encrypts Street and City)
- Description
- Subject

## Other Encrypted Fields and Data Elements

### Individual

- Name

Note: The Individual object is available only if you enable the org setting to make data protection details available in records.

### Chatter Feed

Encrypted Chatter data includes data in feed posts and comments, questions and answers, link names and URLs, poll choices and questions, and content from your custom rich publisher apps.

The revision history of encrypted Chatter fields is also encrypted. If you edit or update an encrypted Chatter field, the old information remains encrypted.

Chatter data is stored in the Feed Attachment, Feed Comment, Feed Poll Choice, Feed Post, and Feed Revision objects. The database fields on these objects that house encrypted data are visible from the Encryption Statistics page in Setup.

- ChatterExtensionInstance—Payload
- ChatterExtensionInstance—PayloadVersion
- ChatterExtensionInstance—TextRepresentation
- ChatterExtensionInstance—ThumbnailUrl
- ChatterExtensionInstance—Title
- FeedAttachment—Title
- FeedAttachment—Value
- FeedComment—RawCommentBody
- FeedPollChoice—ChoiceBody
- FeedPost—LinkUrl
- FeedPost—RawBody
- FeedPost—Title
- FeedRevision—RawValue

Some fields listed in the Encryption Statistics aren’t visible in the UI by the same name, but they store all encrypted data that’s visible in the UI.

Note: Enabling Encryption for Chatter encrypts all eligible Chatter fields. You can’t choose to encrypt only some Chatter fields.

### Search Indexes

When you encrypt search indexes, each file created to store search results is encrypted.

### Einstein Analytics

Encrypts new Einstein Analytics datasets.

Note: Data that was in Einstein Analytics before encryption was enabled is not encrypted. If existing data is imported from Salesforce objects through the dataflow, the data becomes encrypted on the next dataflow run. Other existing data (such as CSV data) must be reimported to become encrypted. Although existing data is not encrypted, it is still accessible and fully functional in its unencrypted state when encryption is enabled.

### Change Data Capture

Change Data Capture provides near-real-time changes of Salesforce records, enabling you to synchronize corresponding records in an external data store. If a Salesforce record field is encrypted with Shield Platform Encryption, changes to encrypted field values generate change events. You can encrypt these change events by selecting **Encrypt and deliver Change Data Capture events** on the Encryption Policy page in Setup.

### Health Cloud

Note: Health Cloud standard objects and fields are available to users who have the Health Cloud Platform permission set license.

Care Request

- Admission Notes
- Disposition Notes
- Facility Record Number
- First Reviewer Notes
- Medical Director Notes
- Member First Name
- Member Last Name
- Member ID
- Member Group Number
- Resolution Notes
- Root Cause Notes

Care Request Drug

- Prescription Number

Coverage Benefit

- Benefit Notes
- Coinsurance Notes
- Copay Notes
- Deductible Notes
- Lifetime Maximum Notes
- Out-of-Pocket Notes
- Source System Identifier

Coverage Benefit Item

- Coverage Level
- Notes

- Service Type
- Service Type Code
- Source System Identifier

Member Plan

- Affiliation
- Group Number
- Issuer Number
- Member Number
- Primary Care Physician
- Source System Identifier

Purchaser Plan

- Plan Number
- Service Type
- Source System
- Source System Identifier

Purchaser Plan Association

- Purchaser Plan Association ID
- Status
- Source System
- Source System Identifier

Note: Deterministic encryption is not available for long text fields. This includes any field with "Notes" in its name.

SEE ALSO:

Encrypt New Data in Standard Fields

## Which Custom Fields Can I Encrypt?

You can encrypt the contents of fields that belong to one of these custom field types, on either standard or custom objects.

- Email
- Phone
- Text
- Text Area
- Text Area (Long)
- Text Area (Rich) (beta)
- URL
- Date
- Date/Time

After a custom field is encrypted, you can't change the field type. For custom phone and email fields, you also can't change the field format.

Important: When you encrypt the Name field, enhanced lookups are automatically enabled. Enhanced lookups improve the user's experience by searching only through records that have been looked up recently, and not all existing records. Switching to enhanced lookups is a one-way change. You can't go back to standard lookups, even if you disable encryption.

You can't use Schema Builder to create an encrypted custom field.

To encrypt custom fields that have the `Unique` or `External ID` attribute, you can only use deterministic encryption.

Some custom fields can't be encrypted:

- Fields on external data objects
- Fields that are used in an account contact relation

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Encrypt New Data in Standard Fields

## Which Files Are Encrypted?

When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it's uploaded.

These kinds of files are encrypted when you enable file encryption:

- Files attached to email
- Files attached to feeds
- Files attached to records
- Images included in Rich Text Area fields
- Files on the Content, Libraries, and Files tabs (Salesforce Files, including file previews, and Salesforce CRM Content files)
- Files managed with Salesforce Files Sync and stored in Salesforce
- Files attached to Chatter posts, comments, and the sidebar
- Notes body text using the new Notes tool
- Files attached to Knowledge articles
- Quote PDFs

These file types and attachments aren't encrypted:

- Chatter group photos
- Chatter profile photos
- Documents
- Notes previews in the new Notes tool
- Notes and Notes previews in the old Notes tool

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

# Which User Permissions Does Shield Platform Encryption Require?

Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or key material. Enable these permissions for user profiles just like you would any other user permission.

| | Manage Encryption Keys | Customize Application | View Setup and Configuration | Manage Certificates | Modify All Data |
|---|---|---|---|---|---|
| View Platform Encryption Setup pages | | ✓ | ✓ | | |
| Edit Encryption Policy page settings | ✓ (Optional) | ✓ | | | |
| Generate, destroy, export, import, and upload tenant secrets and customer-supplied key material | ✓ | | | | |
| Query the TenantSecret object via the API | ✓ | | | | |
| Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service | ✓ | ✓ | | ✓ | |
| Enable features on the Advanced Settings page | | ✓ | | | ✓ |

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

The Customize Application and Manage Certificates permissions are automatically enabled for users with the System Administrator profile.

## Restrict Access to Encryption Policy Settings

You can require admins to also have the Manage Encryption Keys permission to complete encryption policy tasks. These tasks include changing the encryption scheme on fields, enabling and disabling encryption on fields, files, and attachments, and other data elements.

To opt in to this feature, you need the Manage Encryption Keys permission. Then opt in from the Advanced Settings page.

1. From Setup, in the Quick Find box, enter `Platform Encryption`, and then select **Advanced Settings**.
2. Select **Restrict Access to Encryption Policy Settings**.

This restriction applies to actions taken through the API or from Setup pages, such as the Encryption Policy page or the Object Manager.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Manage Shield Platform Encryption

## Why Isn’t My Encrypted Data Masked?

If the encryption service isn’t available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don’t want some users to see, revisit those users’ field-level security settings, record access settings, and object permissions.

Encryption prevents outsiders from using your Salesforce data even if they manage to get it. It is not a way to hide data from authenticated users. User permissions are the only way to control data visibility for authenticated users. Encryption at rest is about logins, not permissions.

With Shield Platform Encryption, if a user is authorized to see a given set of data, that user sees that data whether it’s encrypted or not.

- Authentication means that making sure only legitimate users can get into your system. For example, a company’s Salesforce org is only for use by active employees of that company. Anyone who is not an employee is not authenticated; that is, they are barred from logging in. If they do somehow get their hands on the data, it’s useless to them because it is encrypted.
- Authorization defines which data or features an authenticated user can use. For example, a sales associate can see and use data in the Leads object, but can’t see the regional forecasts, which are intended for sales managers. Both the associate and the manager are properly logged in (authenticated), but their permissions (authorization) are different. That the data is encrypted doesn’t make any difference to them.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ‘15 and later.

Available in both Salesforce Classic and Lightning Experience.

In general, data can be masked but not encrypted, or encrypted but not masked. For example, regulators often require that only the last four digits of a credit card number be visible to users. Applications typically mask the rest of the number, meaning they replace the digits with asterisks on the user’s screen. Without encryption, you can still read the digits that are masked if you can get to the database where they are stored.

Masking might not be enough for your credit card numbers. You may or may not want to encrypt them in the database as well. (You probably should.) If you do, authenticated users will still see the same masked values.

In this way, masking and encryption are different solutions for different problems. You mask data to hide it from users who are authenticated but not authorized to see that data. You encrypt data to prevent someone from stealing the data. (Or, more precisely, to make the data useless if someone does steal it.)

The following table shows the fields that use masking. All others don’t.

| Field Type | Mask | What It Means |
|---|---|---|
| Email, Phone, Text, Text Area, Text Area (Long), URL | ????? | This field is encrypted, and the encryption key has been destroyed. |
| | !!!!! | This service is unavailable right now. For help accessing this service, contact Salesforce. |
| Custom Date | 08/08/1888 | This field is encrypted, and the encryption key has been destroyed. |
| | 01/01/1777 | This service is unavailable right now. For help accessing this service, contact Salesforce. |
| Custom Date/Time | 08/08/1888 12:00 PM | This field is encrypted, and the encryption key has been destroyed. |
| | 01/01/1777 12:00 PM | This service is unavailable right now. For help accessing this service, contact Salesforce. |

You can’t enter these masking characters into an encrypted field. For example, if a Date field is encrypted and you enter 07/07/1777, you must enter a different value before it can be saved.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

## Behind the Scenes: The Shield Platform Encryption Process

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn’t there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The encryption service then encrypts the data on the application server.

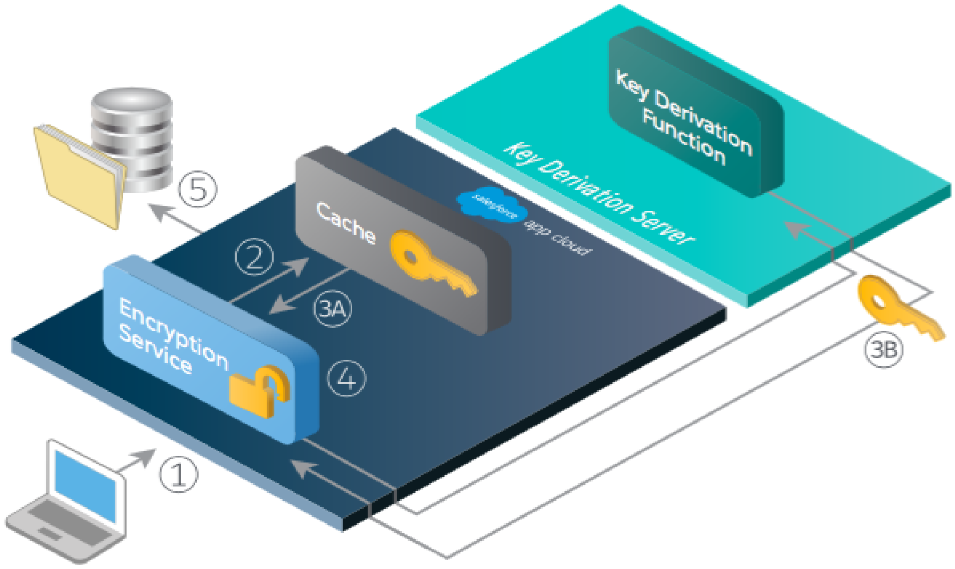
Salesforce securely generates the master and tenant secrets by using Hardware Security Modules (HSMs). The unique key is derived by using PBKDF2, a Key Derivation Function (KDF), with the master and tenant secrets as inputs.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ’15 and later.

Available in both Salesforce Classic and Lightning Experience.

**Shield Platform Encryption Process Flow**



1. When a Salesforce user saves encrypted data, the runtime engine determines from metadata whether to encrypt the field, file, or attachment before storing it in the database.
2. If so, the encryption service checks for the matching data encryption key in cached memory.
3. The encryption service determines whether the key exists.
   a. If so, the encryption service retrieves the key.

   b. If not, the service sends a derivation request to a key derivation server and returns it to the encryption service running on the Salesforce Platform.

4. After retrieving or deriving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using 256-bit AES encryption.
5. The ciphertext is saved in the database or file storage. The IV and corresponding ID of the tenant secret used to derive the data encryption key are saved in the database.

Salesforce generates a new master secret at the start of each release.

## Behind the Scenes: The Search Index Encryption Process

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

Leveraging Shield Platform Encryption's HSM-based key derivation architecture, metadata, and configurations, Search Index Encryption runs when Shield Platform Encryption is in use. The solution applies strong encryption on an org-specific search index (.fdt, .tim, and .tip file types) using an org-specific AES-256 bit encryption key. The search index is encrypted at the search index segment level, and all search index operations require index blocks to be encrypted in memory.

The only way to access the search index or the key cache is through programmatic APIs.

A Salesforce security administrator can enable Search Index Encryption from Setup. The administrator first creates a tenant secret of the Search Index type, then enables Encryption for Search Indexes. The admin configures their encryption policy by selecting fields and files to encrypt. An org-specific HSM-derived key is derived from the tenant secret on demand. The key material is passed to the search engine's cache on a secure channel.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

The process when a user creates or edits records:

1. The core application determines if the search index segment should be encrypted or not based on metadata.
2. If the search index segment should be encrypted, the encryption service checks for the matching search encryption key ID in the cached memory.
3. The encryption service determines if the key exists in the cache.
   a. If the key exists in the cache, the encryption service uses the key for encryption.
   b. Otherwise, the service sends a request to the core application, which in turn sends an authenticated derivation request to a key derivation server and returns the key to the core application server.
4. After retrieving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using NSS or JCE's AES-256 implementation.
5. The key ID (identifier of the key being used to encrypt the index segment) and IV are saved in the search index.

The process is similar when a user searches for encrypted data:

1. When a user searches for a term, the term is passed to the search index, along with which Salesforce objects to search.
2. When the search index executes the search, the encryption service opens the relevant segment of the search index in memory and reads the key ID and IV.
3. Steps 3 through 5 of the process when a user creates or edits records are repeated.
4. The search index processes the search and returns the results to the user seamlessly.

If Salesforce admins disable encryption on a field, all index segments that were encrypted are unencrypted and the key ID is set to null. This process can take up to seven days.

## How Do I Deploy Shield Platform Encryption?

When you deploy Shield Platform Encryption to your org with a tool such as Force.com IDE, Migration Tool, or Workbench, the Encrypted field attribute persists. However, if you deploy to orgs with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target org.

Regardless of how you deploy, Salesforce automatically checks to see if the implementation violates Shield Platform Encryption guidelines.

| Source Organization | Target Organization | Result |
|---|---|---|
| Shield Platform Encryption enabled | Shield Platform Encryption enabled | The source Encrypted field attribute indicates enablement |
| Shield Platform Encryption enabled | Shield Platform Encryption not enabled | The Encrypted field attribute is ignored |
| Shield Platform Encryption not enabled | Shield Platform Encryption enabled | The target Encrypted field attribute indicates enablement |

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

## How Does Shield Platform Encryption Work In a Sandbox?

Refreshing a sandbox from a production organization creates an exact copy of the production organization. If Shield Platform Encryption is enabled on the production organization, all encryption settings are copied, including tenant secrets created in production.

Once a sandbox is refreshed, tenant secret changes are confined to your current organization. This means that when you rotate or destroy a tenant secret on sandbox, it doesn't affect the production organization.

As a best practice, rotate tenant secrets on sandboxes after a refresh. Rotation ensures that production and sandbox use different tenant secrets. Destroying tenant secrets on a sandbox renders encrypted data unusable in cases of partial or full copies.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

## 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.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

**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, 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 the Shield Key Management Service (KMS) 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 persisted on disk. Salesforce supports encryption for fields stored in the database; documents stored in files, content, libraries, and attachments; search index files; Einstein Analytics datasets; and archived data.

**Encryption Key Management**

Refers to all aspects of key management, such as key generation, 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.

**Shield Key Management Service (KMS)**

Generates, wraps, unwraps, derives, and secures key material. When deriving key material, the Shield KMS 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 (customers can opt out of key derivation). The master secret is rotated each release by Salesforce and encrypted using the per-release master wrapping key, which is in turn encrypted with the Shield KMS's 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.*

## What’s the Difference Between Classic Encryption and Shield Platform Encryption?

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ‘15 and later.

Available in both Salesforce Classic and Lightning Experience.

| Feature | Classic Encryption | Platform Encryption |
|---|---|---|
| Pricing | Included in base user license | Additional fee applies |
| Encryption at Rest | ✓ | ✓ |
| Native Solution (No Hardware or Software Required) | ✓ | ✓ |
| Encryption Algorithm | 128-bit Advanced Encryption Standard (AES) | 256-bit Advanced Encryption Standard (AES) |
| HSM-based Key Derivation | | ✓ |
| Manage Encryption Keys Permission | | ✓ |
| Generate, Export, Import, and Destroy Keys | ✓ | ✓ |
| PCI-DSS L1 Compliance | ✓ | ✓ |
| Masking | ✓ | |
| Mask Types and Characters | ✓ | |
| View Encrypted Data Permission Required to Read Encrypted Field Values | ✓ | |
| Encrypted Standard Fields | | ✓ |
| Encrypted Attachments, Files, and Content | | ✓ |
| Encrypted Custom Fields | Dedicated custom field type, limited to 175 characters | ✓ |
| Encrypt Existing Fields for Supported Custom Field Types | | ✓ |

| Feature | Classic Encryption | Platform Encryption |
|---|---|---|
| Search (UI, Partial Search, Lookups, Certain SOSL Queries) | | ✓ |
| API Access | ✓ | ✓ |
| Available in Workflow Rules and Workflow Field Updates | | ✓ |
| Available in Approval Process Entry Criteria and Approval Step Criteria | | ✓ |

## Shield Platform Encryption Best Practices

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Take the time to identify the most likely threats to your organization. This process helps you distinguish data that needs encryption from data that doesn't, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

1. Define a threat model for your organization.

   To identify the threats that are most likely to affect your organization, walk through a formal threat modeling exercise. Use your findings to create a data classification scheme, which can help you decide what data to encrypt.

2. Encrypt only where necessary.
   - Not all data is sensitive. Focus on information that requires encryption to meet your regulatory, security, compliance, and privacy requirements. Unnecessarily encrypting data impacts functionality and performance.
   - Evaluate your data classification scheme early and work with stakeholders in security, compliance, and business IT departments to define requirements. Balance business-critical functionality against security and risk measures and challenge your assumptions periodically.

3. Create a strategy early for backing up and archiving keys and data.

   If your tenant secrets are destroyed, reimport them to access your data. You are solely responsible for making sure that your data and tenant secrets are backed up and stored in a safe place. Salesforce cannot help you with deleted, destroyed, or misplaced tenant secrets.

4. Read the Shield Platform Encryption considerations and understand their implications on your organization.
   - Evaluate the impact of the considerations on your business solution and implementation.
   - Test Shield Platform Encryption in a sandbox environment before deploying to a production environment. Encryption policy settings can be deployed using change sets.
   - Before enabling encryption, fix any violations that you uncover. For example, if you reference encrypted fields in a SOQL ORDER BY clause, a violation occurs. Fix the violation by removing references to the encrypted fields.
   - When requesting feature enablement, such as pilot features, give Salesforce Customer Support several days lead time. The time to complete the process varies based on the feature and how your org is configured.

5. Analyze and test AppExchange apps before deploying them.
   - If you use an app from the AppExchange, test how it interacts with encrypted data in your organization and evaluate whether its functionality is affected.

- If an app interacts with encrypted data that's stored outside of Salesforce, investigate how and where data processing occurs and how information is protected.
- If you suspect Shield Platform Encryption could affect the functionality of an app, ask the provider for help with evaluation. Also discuss any custom solutions that must be compatible with Shield Platform Encryption.
- Apps on the AppExchange that are built exclusively using Lightning Platform inherit Shield Platform Encryption capabilities and limitations.

6. Use out-of-the-box security tools.

   Shield Platform Encryption is not a user authentication or authorization tool. To control which users can see which data, use out-of-the-box tools such as field-level security settings, page layout settings, and sharing rules, rather than Shield Platform Encryption.

7. Grant the Manage Encryption Keys user permission to authorized users only.

   Users with the Manage Encryption Keys permission can generate, export, import, and destroy organization-specific keys. Monitor the key management activities of these users regularly with the setup audit trail.

8. Synchronize your existing data with your active key material.

   Existing field and file data is not automatically encrypted when you turn on Shield Platform Encryption. To encrypt existing field data, update the records associated with the field data. This action triggers encryption for these records so that your existing data is encrypted at rest. To encrypt existing files or get help updating other encrypted data, contact Salesforce. We can encrypt existing file data in the background to ensure data alignment with the latest encryption policy and key material.

   When you contact Salesforce support to request the background encryption service, allow at least a week before you need the background encryption completed. The time to complete the process varies based on the volume of data involved. It could take several days.

9. Handle currency and number data with care.

   Currency and Number fields can’t be encrypted because they could have broad functional consequences across the platform, such as disruptions to roll-up summary reports, report timeframes, and calculations. You can often keep private, sensitive, or regulated data of this variety safe in other encryption-supported field types.

10. Communicate to your users about the impact of encryption.

    Before you enable Shield Platform Encryption in a production environment, inform users about how it affects your business solution. For example, share the information described in Shield Platform Encryption considerations, where it's relevant to your business processes.

11. Encrypt your data using the most current key.

    When you generate a new tenant secret, any new data is encrypted using this key. However, existing sensitive data remains encrypted using previous keys. In this situation, Salesforce strongly recommends re-encrypting these fields using the latest key. Contact Salesforce for help with re-encrypting your data.

12. Use discretion when granting login as access to users or Salesforce Customer Support.

    If you grant login access to a user, and they have field level security access to an encrypted field, that user is able to view encrypted data in that field in plaintext.

If you want Salesforce Customer Support to follow specific processes around asking for or using login as access, you can create special handling instructions. Salesforce Customer Support follows these instructions in situations where login as access may help them resolve your case. To set up these special handling instructions, contact your account executive.

SEE ALSO:

Tradeoffs and Limitations of Shield Platform Encryption

## Tradeoffs and Limitations of Shield Platform Encryption

A security solution as powerful as Shield Platform Encryption doesn't come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren't available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

General Shield Platform Encryption Considerations

These considerations apply to all data that you encrypt using Shield Platform Encryption.

Which Salesforce Apps Don't Support Shield Platform Encryption?

Some Salesforce features work as expected when you work with data that's encrypted with Shield Platform Encryption. Others don't.

Considerations for Using Deterministic Encryption

These considerations apply to data encrypted with Data in Salesforce (Deterministic) key material.

Shield Platform Encryption and the Lightning Experience

Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

Field Limits with Shield Platform Encryption

Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these limits.

SEE ALSO:

Shield Platform Encryption Best Practices

## General Shield Platform Encryption Considerations

These considerations apply to all data that you encrypt using Shield Platform Encryption.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

### Leads

Lead and Case assignment rules, workflow rules, and validation rules work normally when Lead fields are encrypted. Matching and de-duplication of records during lead import works with deterministically encryption, but not probabilistic encryption. Einstein Lead Scoring is not available.

Apex Lead Conversion works normally, but PL-SQL-based lead conversion is not supported.

### Flows and Processes

You can reference encrypted fields in most places in your flows and processes. However, you can't reference encrypted fields in these filtering or sorting contexts.

| Tool | Filtering Availability | Sorting Availability |
|---|---|---|
| Process Builder | Update Records action | n/a |
| Cloud Flow Designer | Dynamic Record Choice resource<br>Fast Lookup element<br>Record Delete element<br>Record Lookup element<br>Record Update element | Dynamic Record Choice resource<br>Fast Lookup element<br>Record Lookup element |

You can store the value from an encrypted field in a variable and operate on that value in your flow's logic. You can also update the value for an encrypted field.

Paused flow interviews can result in data being saved in an unencrypted state. When a flow or process is waiting to resume, the associated flow interview is serialized and saved to the database. The flow interview is serialized and saved when:

- Users pause a flow
- Flows execute a Wait element
- Processes are waiting to execute scheduled actions

If the flow or process loads encrypted fields into a variable during these processes, that data might not be encrypted at rest.

### Custom Fields

You can't use encrypted custom fields in criteria-based sharing rules.

Some custom fields can't be encrypted.

- Fields that have the `Unique` or `External ID` attributes or include these attributes on previously encrypted custom fields (applies only to fields that use the probabilistic encryption scheme)
- Fields on external data objects
- Fields that are used in an account contact relation

You can’t use Schema Builder to create an encrypted custom field.

You can’t use Shield Platform Encryption with Custom Metadata Types.

### SOQL/SOSL

- Encrypted fields that use the probabilistic encryption scheme can’t be used with the following SOQL and SOSL clauses and functions:
  - Aggregate functions such as MAX(), MIN(), and COUNT_DISTINCT()
  - WHERE clause
  - GROUP BY clause
  - ORDER BY clause

  For information about SOQL and SOSL compatibility with deterministic encryption, see Considerations for Using Deterministic Encryption in Salesforce Help.

  Tip: Consider whether you can replace a WHERE clause in a SOQL query with a FIND query in SOSL.

- When you query encrypted data, invalid strings return an `INVALID_FIELD` error instead of the expected `MALFORMED_QUERY`.

### Portals

If a portal is enabled in your organization, you can’t encrypt standard fields. Deactivate all customer portals and partner portals to enable encryption on standard fields. (Communities are supported.)

To deactivate a customer portal, go to the Customer Portal Settings page in Setup. To deactivate a partner portal, go to the Partners page in Setup.

### Search

If you encrypt fields with a key and then destroy the key, the corresponding search terms remain in the search index. However, you can’t decrypt the data associated with the destroyed key.

### Accounts, Person Accounts, and Contacts

When Person Accounts are turned on, encrypting any of the following Account fields encrypts the equivalent Contact fields, and vice versa.

- Name
- Description
- Phone
- Fax

When you encrypt any of the following Account or Contact fields, the equivalent fields in Person Accounts are also encrypted.

- Name
- Description
- Mailing Address
- Phone
- Fax
- Mobile
- Home Phone

- Other Phone
- Email

When the Account Name or Contact Name field is encrypted, searching for duplicate accounts or contacts to merge doesn’t return any results.

When you encrypt the First Name or Last Name field on a contact, that contact appears in the Calendar Invite lookup only if you haven’t filtered by First Name or Last Name.

## Email to Salesforce

When the standard Email field is encrypted, the detail page for Contacts, Leads, or Person Accounts doesn’t flag invalid email addresses. If you need bounce processing to work as expected, don't encrypt the standard Email field.

## Salesforce for Outlook

If you encrypt the same fields that you filter in Salesforce for Outlook data sets, Salesforce for Outlook doesn’t sync. To get Salesforce for Outlook to sync again, remove the encrypted fields from your filters in your data sets.

## Campaigns

Campaign member search isn’t supported when you search by encrypted fields.

## Notes

You can encrypt the body text of Notes created with the new Notes tool. However, the Preview file and Notes created with the old Notes tool aren’t supported.

## Field Audit Trail

Data in a previously archived Field Audit Trail isn’t encrypted when you turn on Platform Encryption. For example, say that your org uses Field Audit Trail to define a data history retention policy for an account field, such as the phone number field. When you turn on encryption for that field, new phone number records are encrypted as they are created. Previous updates to the phone number field that are stored in the Account History related list are also encrypted. However, phone number history data that is already archived in the `FieldHistoryArchive` object is stored without encryption. To encrypt previously archived data, contact Salesforce.

## Communities

If you encrypt the Account Name field and you’re not using Person Accounts, encryption affects how users’ roles are displayed to admins. Normally, a community user’s role name is displayed as a combination of their account name and the name of their user profile. When you encrypt the Account Name field, the account ID is displayed instead of the account name.

For example, when the Account Name field is not encrypted, users belonging to the Acme account with the Customer User profile would have a role called `Acme Customer User`. When Account Name is encrypted (and Person Accounts aren’t in use), the role is displayed as something like `001D000000IRt53 Customer User`.

## Data Import

You can’t use the Data Import Wizard to perform matching using master-detail relationships or update records that contain fields that use the probabilistic encryption scheme. You can use it to add new records, however.

## Reports, Dashboards, and List Views

- Report charts and dashboard components that display encrypted field values might be cached unencrypted.
- You can't sort records in list views by fields that contain encrypted data.

## Encryption for Chatter

When you embed a custom component in your Chatter feed using Rich Publisher Add-Ons, the data related to those add-ons is encoded, but it isn't encrypted with the Shield Platform Encryption service. Unencrypted data in Rich Publisher Add-Ons includes data stored in the Extension ID, Text Representation, Thumbnail URL, Title, Payload, and PayloadVersion fields.

## Encryption for Custom Matching Rules Used in Duplicate Management

Custom matching rules can only reference fields encrypted with the deterministic encryption scheme. Probabilistic encryption isn't supported. When you rotate your keys, you must deactivate and then reactivate custom matching rules that reference encrypted fields. If you don't take this step after updating your key material, matching rules don't find all your encrypted data.

Standard matching rules that include fields with Shield Platform Encryption don't detect duplicates. If you encrypt a field included in standard matching rules, deactivate the standard rule.

Service protections ensure that loads are balanced across the system. The matching service searches for match candidates until they find all matches or up to 200 matches. With Shield Platform Encryption, the service search maximum is 100 candidates. With encryption, you could find fewer or no possible duplicate records.

Duplicate jobs aren't supported.

## General

- Encrypted fields can't be used in:
  - Criteria-based sharing rules
  - Similar opportunities searches
  - External lookup relationships
  - Filter criteria for data management tools
- Live Agent chat transcripts are not encrypted at rest.
- Web-to-Case is supported, but the Web Company, Web Email, Web Name, and Web Phone fields are not encrypted at rest.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

## Which Salesforce Apps Don't Support Shield Platform Encryption?

Some Salesforce features work as expected when you work with data that's encrypted with Shield Platform Encryption. Others don't.

These apps don't support data encrypted with Shield Platform Encryption. However, you can enable Shield Platform Encryption for other apps when these apps are in use.

- Connect Offline
- Commerce Cloud
- Data.com
- Einstein Engine
- Heroku (but Heroku Connect does support encrypted data)
- Marketing Cloud (but Marketing Cloud Connect does support encrypted data)
- Pardot (but Pardot Connect supports encrypted contact email addresses if your Pardot org allows multiple prospects with the same email address)
- Salesforce CPQ
- Salesforce IQ
- Social Customer Service
- Thunder
- Quip

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Legacy portals (customer, self-service, and partner) don't support data encrypted with Shield Platform Encryption. If legacy portals are active, Shield Platform Encryption can't be enabled.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

## Considerations for Using Deterministic Encryption

These considerations apply to data encrypted with Data in Salesforce (Deterministic) key material.

### Key Rotation and Filter Availability

To filter and execute queries on fields with unique attributes, new and existing encrypted data must be encrypted with the active Data in Salesforce (Deterministic) key material. See Synchronize Your Data Encryption with the Background Encryption Service for tips on timing and placing your background encryption service request.

### Available Fields and Other Data

The deterministic encryption option is available for custom URL, email, phone, text, and text area field types. It isn't available for the following types of data:

- Custom date, date/time, long text area, or description field types
- Chatter
- Files and attachments

## Filter Operators

In reports and list views, the operators “equals” and “not equal to” are supported with deterministic encryption. Other operators, like “contains,” “or “starts with,” don’t return an exact match and aren’t supported.

## Case Sensitivity

When you use deterministic encryption, case matters. In reports, list views, and SOQL queries on encrypted fields, the results are case-sensitive. Therefore, a SOQL query against the Contact object, where LastName = 'Jones’, returns only Jones, not jones nor JONES. Similarly, when the filter-preserving scheme tests for unicity (uniqueness), each version of “Jones” is unique.

## API Options to Identify Filterable Fields

Fields encrypted using the deterministic encryption scheme are filterable. You can use the `isFilterable()` method to determine the encryption scheme of a particular encrypted field. If the field is filterable, the method returns true.

However, you can’t explicitly detect or set the deterministic encryption scheme via the API.

## External ID

You can enable the external ID for deterministically encrypted fields when you use the Unique - Case-Sensitive attribute. First mark your external ID field as Unique - Case-Sensitive and click **Save**. Then edit your field and add encryption. You can’t save changes to both Unique - Case-Sensitive and Encrypted options at the same time.

External ID isn’t available for email field types.

## Compound Names

Even with deterministic encryption, some kinds of searches don’t work when data is encrypted. Concatenated values, such as compound names, aren’t the same as the separate values. For example, the ciphertext for the compound name “William Jones” is not the same as the concatenation of the ciphertexts for “William” and “Jones”.

So, if the First Name and Last Name fields are encrypted in the Contacts object, this query doesn’t work:

```
Select Id from Contact Where Name = 'William Jones'
```

But this query does work:

```
Select Id from Contact Where FirstName = 'William’ And LastName ='Jones'
```

## Filter Records by Strings

You can search for records using strings. However, commas in strings act as OR statements. If your string includes a comma, use quotation marks around the string. For example, a search for *“Universal Containers, Inc, Berlin”* returns records that include the full string including the comma. Searches for *Universal Containers, Inc, Berlin* returns records that include *Universal Containers* or *Inc* or *Berlin*.

## SOQL GROUP BY Statements

You can use most of the SOQL statements with deterministic encryption. One exception is GROUP BY, which isn’t supported, even though you can group report results by row or column.

### SOQL LIKE and STARTS WITH Statements

Deterministic encryption only supports exact, case-sensitive matches. Comparison operators that return partial matches aren't supported. For example, LIKE and STARTS WITH statements aren't supported.

### SOQL ORDER BY Statements

Because deterministic encryption doesn't maintain the sort order of encrypted data in the database, ORDER BY isn't supported.

### Indexes

Deterministic encryption supports single-column indexes, single-column case-sensitive unique indexes, two-column indexes, and custom indexes on standard and custom fields.

## Shield Platform Encryption and the Lightning Experience

Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

**Notes**

Note previews in Lightning are not encrypted.

**File Encryption Icon**

The icon that indicates that a file is encrypted doesn't appear in Lightning.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

## Field Limits with Shield Platform Encryption

Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these limits.

| | API Length | Byte Length | Non-ASCII Characters |
|---|---|---|---|
| Assistant Name (Contact) | 40 | 120 | 22 |
| Address (To, CC, BCC on Email Message) (beta) | 3000 | 4000 | 2959 |
| City (Account, Contact, Lead) | 40 | 120 | 22 |
| Email (Contact, Lead) | 80 | 240 | 70 |
| Fax (Account) | 40 | 120 | 22 |
| First Name (Account, Contact, Lead) | 40 | 120 | 22 |

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

| | API Length | Byte Length | Non-ASCII Characters |
|---|---|---|---|
| Last Name (Contact, Lead) | 80 | 240 | 70 |
| Middle Name (Account, Contact, Lead) | 40 | 120 | 22 |
| Name (Custom Object) (beta) | 80 | 240 | 80 |
| Name (Opportunity) | 120 | 360 | 110 |
| Phone (Account, Contact) | 40 | 120 | 22 |
| Site (Account) | 80 | 240 | 70 |
| Subject (Email Message) (beta) | 3000 | 3000 | 2207 |
| Title (Contact, Lead) | 128 | 384 | 126 |

Note: This list isn’t exhaustive. For information about a field not shown here, refer to the API.

## Case Comment Object

The Body field on the Case Comment object has a limit of 4,000 ASCII characters (or 4,000 bytes). However, when these fields are encrypted, the character limit is lower. How much lower depends on the kind of characters you enter.

- ASCII: 2959
- Chinese, Japanese, Korean: 1333
- Other non-ASCII: 1479

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Encrypt New Data in Standard Fields