Tokenization

Overview

Tokenization means protecting sensitive data by replacing it with algorithmically generated characters called tokens. It is a foundational technology enabling secure and simple eCommerce.

The Verifone Global Proprietary Tokenization Service is available globally to all merchants in all regions, allowing for transactions with stored credentials and cross-channel cardholder visibility.

To utilize the tokenization feature, you need an account in Verifone Central, an organization and an active Payment Provider Contract and a token scope assigned. Your user must be assigned to the Merchant Site organization to perform the API calls.

The token scope enhances Verifone's Global Proprietary Tokenization Service security. A token scope allows a merchant to limit the validity and the type of generated tokens. By linking a token scope to an organization, any individual token that is generated is only valid within the token scope requested for generation.

Proprietary Token Types

Reuse Token

Verifone's proprietary Reuse Token allows linking payment data to a token for future payments.

Analytics Token

Verifone's proprietary Analytics Token allows linking card data to a token to identify cardholders across sales channels. An Analytics Token cannot be used for payments.

> Verifone does not offer the possibility to de-tokenize a token into clear cardholder data once it was tokenized.

Use cases for Proprietary Tokens

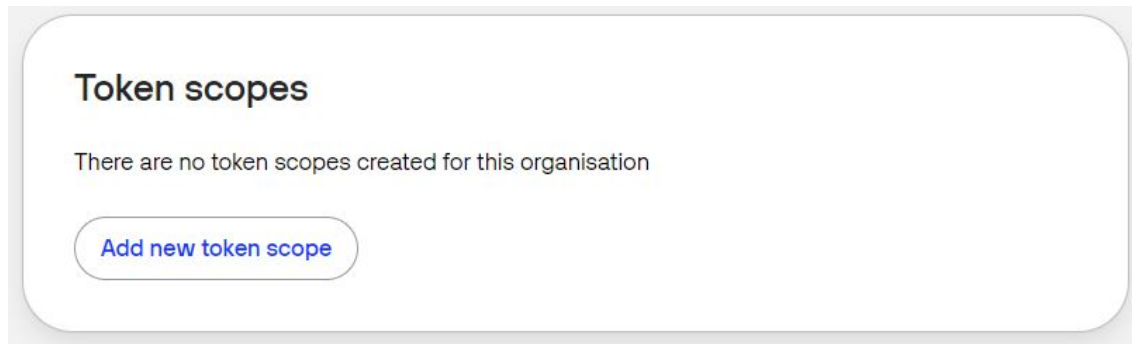| Token type	Use cases
Reuse Token	A Reuse Token can be used and stored to capture a payment method for future transactions with stored credentials or for omnichannel refunds. Store this token in your systems for future payments-related use.
Analytics Token	An Analytics Token can be used and stored for performing group transactions with the same Primary Account Number (PAN). Store this token in your own systems.

Using Verifone Tokenization

To use the Verifone Global Proprietary Tokenization Service follow the below steps:
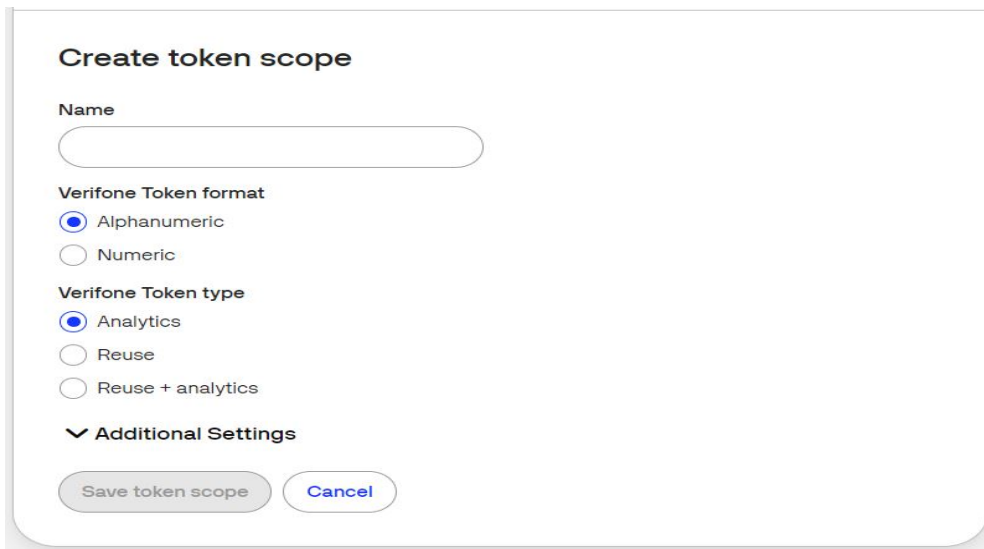
Creating a Token Scope in Verifone Central

Token scopes can only be created by organizations with type Merchant Company. The token scopes can be managed from the *Organization details* page, in Verifone Central. Token scopes are inherited from the parent merchant company.

1. Log into Verifone Central.
2. Navigate to the organization with type *Merchant Company*.

3. In the **Token Scope** section, click **Add new token scope** and enter all mandatory information.

- **Name** - the name for the token scope. Use this field for an easy identification of the token scope
  - This name is different from the Token Scope UUID that is being used in the [Verifone eCommerce API](https://...) to recognize the token scope
- **Verifone Token format** - use this field to define whether the generated Reuse Tokens are alphanumeric or numeric only
  - This selection only affects Reuse Tokens, as the Analytics Token has a fixed format, 29-digits: 'VF' + 27 digit alphanumeric

- **Verifone Token type** - use this field to define which type of tokens are allowed to be created under this token scope

  - If **Reuse + analytics** is selected, two token values will be returned in one response

- In the **Additional Settings** section, you can optionally influence the following technical details for Reuse Tokens. For example, you want to create format-preserved tokens. If you leave the fields blank, the default settings will apply.
    - **Token length** - the token length can be a number between 1 and 255
    - **Card prefix length** - determines how many digits from the original Primary Account Number (PAN) are included as a prefix for tokens under this scope
    - **Card suffix length** - determines how many digits from the original PAN are included as a suffix for tokens under this scope
    - **Fixed prefix** - the provided value is left-padded with the tokens under this scope. The maximum length should not exceed 6 characters.
    - **Fixed suffix** - the provided value is right-padded with the tokens under this scope. The maximum length should not exceed 4 characters.
    - **Token expiration time** - the number of days before a token expires under this scope
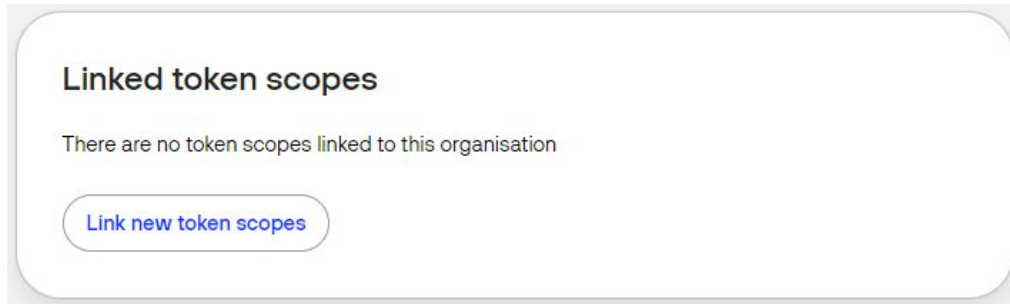
4. Save the token scope.

Linking a Token Scope in Verifone Central

Token scopes can be linked for Merchant Site organizations. Linking token scopes to certain organizations can be done via the same interface on the *Organization details* page.

1. Log into Verifone Central.

2. Navigate to any organization with a type other than *Merchant Company*.

3. In the *Token Scope* section, click **Link new token scope** and select the token scopes which should be added to the organization.
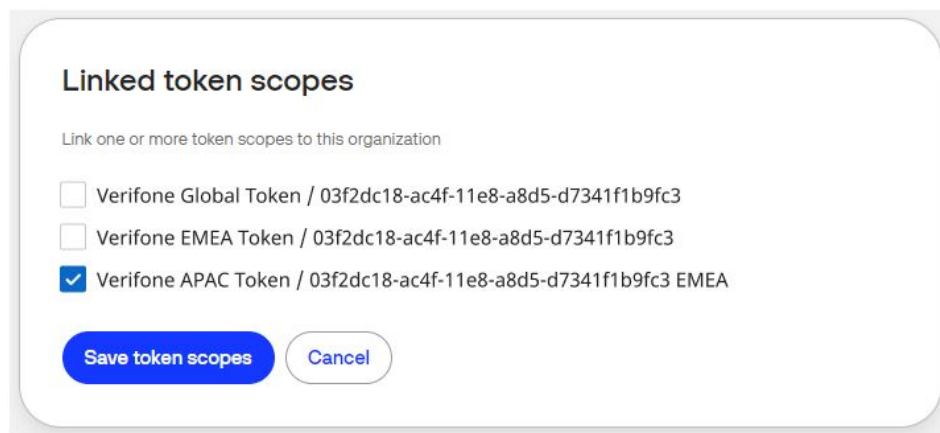

> You can link any number of token scopes to any number of organizations, but when requesting a token, only one token scope can be used

4. To link token scope(s), select the name(s) you gave to the token scope and the token scope UUID. You need the Token Scope UUID when requesting a token.

5. Save the token scope.

Requesting a token via API

Once at least one token scope is linked to at least one organization, that organization can request a token to be generated in either of the following ways:

- By filling out the `token_preference` object in a [Create a checkout](#) request or
- By filling out the `token_preference` object in an [EncryptedCardPaymentRequest](#) or
- By filling out the `token_preference` object in an [Initiate a wallet payment request](#) or
- By submitting a [Create/Update Token Details request](#)

Parameter	Description
token_scope	(required field) - refers to the token scope UUID under which the token is created
encrypted_card	(required field) - refers to the cardholder data encrypted using the Verifone provided public key (only in the Create/Update Token Details request)
token_type	(optional field) - allows you to optionally limit which type of token(s) you would like to receive as a response to this call
token_expiry_date	(optional field) - allows you to optionally limit the expiry date of the token you want to receive as a response to this call
public_key_alias	refers to the public key the cardholder data is encrypted with (only in the Create/Update Token Details request)

Scenarios for create/update token details requests

- if the token_scope allows for the creation of both a Reuse and an Analytics Token, but the merchant decides that as a response to this call, an Analytics Token is sufficient
- if the default token_expiry_date is further in the future than what the merchant needs for this token

The create/update token details request either creates a token, if one does not yet exist for the given encrypted_card details in the requested token scope or it updates the token details with the expiry date.

Receiving a token

If the API call is approved, Verifone will return a token in the response.

After a first API call where a Reuse Token is requested and created, any following API calls with the same token scope and encrypted_card details will result in the same Reuse Token.

After a first API call where an Analytics Token is requested and created, any following API calls with the same encrypted_card details will result in the same Analytics Token.

An approved API will result in a '201' (or '200' for a Create/Update Token Details request) message, where in the token_details object, is a list of possible responses.

Parameter	Definition
reuse_token	(if requested) - the Reuse Token that must be saved and stored
analytics_token	(if requested) - the Analytics Token that must be saved and stored

Parameter	Definition
token_expiry_date	the expiration date for the token(s)
token_scope	stating under which token scope this token(s) was created
token_status	the status of the token(s)
created_at	the date when the token(s) was first created
updated_at	the last date when the token(s) was last updated and various card information-related fields

A merchant can receive a 'Non Active' status back if a token was already created for this token scope and `encrypted_card details`, and it is already 'Deleted' or 'Suspended'. See the Using the Token section below to learn how to change the Token status.

Storing the Token

Verifone currently does not offer features that allow the merchant to view their available tokens at once. That is why we recommend storing the Verifone token ID yourself at the time you receive the response. There are two other ways how to obtain token IDs after the approved response:

- If the merchant knows the encrypted card details, they can submit a Create/Update Token Details request, where the response will contain the token details associated with that token scope and with those encrypted card details.
- If the merchant knows the transaction UUID associated with the transaction that originally resulted in a token, they can search for the transaction in Verifone Central. In the transaction details tab of the transaction, the Reuse Token associated with that transaction can be found.

Stored Credential details

Type
Sign up

Status
Stored now

Model details
Recurring

Re-use Token ID
123e4567-e89b-12d3-a456-426614174000

Scheme reference
123e4567-e89b-12d3-a456-426614174000

Using the Token

Verifone currently offers the following ways how a merchant can use the tokens:

- The merchant can initiate a transaction with a Reuse Token by submitting the TokenPaymentRequest API call
    - A Reuse Token is linked to a token scope, therefore a Reuse Token provided as part of a token scope can only be reused by the Merchant Entity that is part of the same token scope
- The merchant can do transactions with stored credentials where the Reuse Token might also be needed (see the transactions with stored credentials section for further information)
- The merchant can do various token management activities via Token Management API calls
- Token scopes can only be used by organizations with type Merchant Site