Rule Engine

The Rule Engine is a software component designed for tokenization fraud detection. Its primary purpose is to analyze various aspects of tokenization and determine whether it exhibits any suspicious or fraudulent characteristics. The Rule Engine consists of a collection of predefined rules that are applied to each tokenization, depending on the requirements of Issuers, Token Service Providers, and Token Requestors.

Rule

Each rule accepts different data points provided by Token Service Providers, Issuers, and Token Requestors and based on its logic returns a result, which can be one of the following values:

- **Green** - Rule is not violated.
- **Yellow** - Rule is violated, downgrade to **Yellow** path.
- **Orange** - Rule is violated, downgrade to **Orange** path.
- **Red** - Rule is violated, downgrade to **Red** path.

Each rule is executed only if applicable in a given tokenization context.
The result of each rule is saved for auditing purposes and available in the Admin Panel on the Rules tab.

Available Rules

Card Verification Rule

This rule makes sure the card information is right:

- The card number is valid.
- The expiration date is valid.
- The security code is valid.
- The card is not blocked by the bank.

If any of these checks fail, the tokenization is downgraded to **Red**.

> This rule uses Lifecycle API data source or calls Issuer Card Verification API.

Account Source Rule

This rule checks the account source - entered manually or via mobile app. Tokenizations with manually entered card data are downgraded to **Yellow** path.

>

> Applicable only for Apple Pay and Google Pay.

Available Tokens Rule

This rule checks the number of tokens for a card that is being tokenized.

If the limit is exceeded - tokenization is downgraded to **Red**.

> Applicable only for Apple Pay and Google Pay.
> The rule is configurable - the default limit is 10 tokens per card.

Device Score Rule

This rule checks the device score provided by the Token Requestor.

If the device score is 1 - tokenization is downgraded to **Red**.

> Applicable only for Apple Pay and Google Pay.

Wallet Recommendation Rule

This rule checks the wallet recommendation provided by the Token Requestor.

- Wallet recommendation is to require additional authentication - downgrade to **Yellow**.
- Wallet recommendation is to decline - downgrade to **Red**.
- Wallet recommendation is to approve - **Green**.

Geolocation Rule

This rule checks the geolocation data provided by the Token Requestor.

If the geolocation is not inside the configured country - the tokenization is downgraded to **Orange**.

> The allowed list of countries is configurable. This rule is not enabled by default.

Source IP Rule

This rule checks the source IP of the device provided by the Token Requestor.

If the source IP is not from the allowed country - the tokenization is downgraded to **Orange**.

>

> The allowed list of countries is configurable. This rule is not enabled by default.

High-Risk Flag Rule

This rule checks if the tokenization is not flagged as high risk by the Token Requestor.

If it is flagged - the tokenization is downgraded to **Orange**.

> Applicable only for Apple Pay and Google Pay.

Invalid Attempts Rule

This rule limits the number of tokenization attempts for a single card with an invalid expiry date or security code.

If the limit is exceeded - the tokenization is downgraded to **Red**.

> The limit is configurable and by default is 3 attempts during 24 hours.

M4M CVC Rule

This rule checks the status of security code verification for M4M tokenizations. Depending on the account source, a missing or invalid security code might result in a different authorization path.

- Security code is invalid - downgrade to **Red**.
- Security code is not present and the account source is "card on file" - downgrade to **Yellow**.
- Security code match, account source is one of "manual" or "card of file" or "existing token credentials" - downgrade to **Yellow**.

> Applicable only for Mastercard M4M (MDES for Merchants) tokenizations.

Phone Number Rule

This rule checks if the phone number provided by the Token Requestor matches the phone number in the Issuer system.

If the phone number doesn't match - the tokenization is downgraded to **Orange**.

If the phone number is not provided by the Token Requestor - the result of this rule is **Green**.

>

> This rule is not enabled by default.

Decisioning Rule

This rule determines the final decision returned to Mastercard or Visa depending on the results of all Rules executed for this tokenization.

- If all executed rules are **Green** - the final decision is to approve the tokenization.
- If at least one rule is **Yellow** - the final decision is to require additional authentication with the SMS OTP code.
- If at least one rule is **Orange** - the final decision is to require additional authentication via the Issuer call center.
- If at least one rule is **Red** - the final decision is to decline the tokenization.

Admin Panel

On the admin panel, you can check all rules executed for a tokenization. Detailed reason or error is provided.

image-1711370519978.png
Image not found or type unknown

Customization

Each optional rule can be disabled, modified, or customized for each Issuer based on preferences or local regulatory requirements.

New rules can be added with the following possibilities:

- Processing data points from Token Requestors included in tokenization requests.
- Processing data points from Mastercard or Visa included in tokenization requests.
- Processing data points from the Issuer system, ex. via calling additional APIs or external services during the tokenization.
- Processing data points from Verestro's own database.

> The tokenization process is limited by time - 5 seconds.

Revision #10
Created 22 March 2024 15:37:03 by Vadym Dudnyk
Updated 23 April 2024 06:38:01 by Vadym Dudnyk