Stripe Restricted API Key Setup Guide

Overview

This document explains how to create a Stripe Restricted API Key with the required permissions enabled, based on the required Stripe permission configuration.

Restricted API keys are recommended for production integrations where applications should only have access to the minimum required Stripe resources.

Purpose

The purpose of this restricted API key is:

- Secure backend/server-to-server Stripe integration
- Limit access only to required Stripe resources
- Avoid using full Secret Keys in applications
- Follow the principle of least privilege

Prerequisites

Before creating the restricted API key:

- You must have Stripe Admin access
- Login to the Stripe Dashboard
- Ensure you are in the correct Stripe account/environment

Navigation Steps

1. Login to Stripe Dashboard
2. Go to:

```
Developers → API Keys
```

1. Under “Restricted keys”, click:

```
Create restricted key
```

Key Configuration

Key Name

Use a meaningful name.

Example:

```
Application Backend Restricted Key
```

Permission Configuration

Configure the permissions exactly as required for the application.

The configuration includes a combination of:

- Read
- Write
- None

permissions depending on the resource.

Recommended Enabled Permissions

Core Permissions

Resource	Permission
Charges	Write
Customers	Write
Payment Intents	Write
Payment Methods	Write
Checkout Sessions	Write
Refunds	Read
Balance	Read
Events	Read
Files	Read

Security Recommendation

Important

Never expose the restricted API key:

- In frontend/mobile applications
- In public repositories
- Inside client-side JavaScript

The restricted API key should only be used:

- On secure backend servers
- Inside environment variables
- In protected infrastructure

Environment Variable Setup

Example:

```
STRIPE_SECRET_KEY=rk_live_xxxxxxxxxxxxxxxx
```

For local development:

```
STRIPE_SECRET_KEY=rk_test_xxxxxxxxxxxxxxxx
```

After Creating the Key

After clicking:

```
Create key
```

Stripe will display the restricted key once.

Immediately:

1. Copy the key
2. Store it securely
3. Add it to environment variables
4. Do not share it over email/chat

Verification Checklist

Before using the key in production:

- Verify payment creation works
- Verify customer creation works
- Confirm unauthorized APIs are blocked
- Test with Stripe test mode first

Best Practices

Recommended

- Use separate keys for each environment
- Rotate keys periodically
- Grant minimum required permissions
- Monitor Stripe logs and API activity
- Revoke unused keys immediately

Example Use Cases

Backend Payment Service

Recommended permissions:

- Customers → Write
- Payment Intents → Write
- Charges → Write
- Refunds → Write
- Events → Read

Reporting Service

Recommended permissions:

- Balance → Read
- Charges → Read
- Payouts → Read
- Reports → Read

Troubleshooting

Permission Denied Error

If Stripe returns:

```
You do not have permission to perform this request
```

then:

1. Open Restricted Key settings
2. Enable required resource permission
3. Save changes
4. Retry the API request

Notes

- Use restricted keys instead of full secret keys whenever possible.
- Production systems should always follow least-privilege access.
- Keep separate restricted keys for different services/modules.

Reference

Stripe Official Documentation:

- Restricted API Keys
- API Authentication
- Stripe Security Best Practices