

[Deployment](#) > [Production readiness](#) > [Production checklist](#) >

# Production Checklist

---

After developing your project and deciding it's Production Ready, you should run through this checklist to ensure that your project:

is secure

won't falter under the expected load

remains available whilst in production

## Security

Ensure RLS is enabled

Tables that do not have RLS enabled with reasonable policies allow any client to access and modify their data. This is unlikely to be what you want in the majority of cases.

[Learn more about RLS.](#)

Enable replication on tables containing sensitive data by enabling Row Level Security (RLS) and setting row security policies:

Go to the Authentication > Policies page in the Supabase Dashboard to enable RLS and create security policies.

Go to the Database > Publications page in the Supabase Dashboard to manage replication tables.

Turn on [SSL Enforcement](#) (see: [dashboard](#))

Enable [Network Restrictions](#) for your database (see: [dashboard](#)).

Ensure that your Supabase Account is protected with multi-factor authentication (MFA).

If using a GitHub signin, [enable 2FA on GitHub](#). Since your GitHub account gives you administrative rights to your Supabase org, you should protect it with a strong password and 2FA using a U2F key or a TOTP app.

If using email+password signin, set up [MFA for your Supabase account](#).

Enable [MFA enforcement on your organization](#). This ensures all users must have a valid MFA backed session to interact with organization and project resources.

Consider [adding multiple owners on your Supabase org](#). This ensures that if one of the owners is unreachable or loses access to their account, you still have Owner access to your org.

Ensure email confirmations are [enabled](#) in the `Settings > Auth` page.

Ensure that you've [set the expiry](#) for one-time passwords (OTPs) to a reasonable value that you are comfortable with. We recommend setting this to 3600 seconds (1 hour) or lower.

Increase the length of the OTP if you need a higher level of entropy.

If your application requires a higher level of security, consider setting up [multi-factor authentication](#) (MFA) for your users.

Use a custom SMTP server for auth emails so that your users can see that the mails are coming from a trusted domain (preferably the same domain that your app is hosted on). Grab SMTP credentials from any major email provider such as SendGrid, AWS SES, etc.

Think hard about how *you* would abuse your service as an attacker, and mitigate.

Review these [common cybersecurity threats](#).

Check and review issues in your database using [Security Advisor](#).

## Performance

Ensure that you have suitable indices to cater to your common query patterns

[Learn more about indexes in Postgres](#).

`pg_stat_statements` can help you [identify hot or slow queries](#).

Perform load testing (preferably on a staging env)

Tools like [k6](#) can simulate traffic from many different users.

Upgrade your database if you require more resources. If you need anything beyond what is listed, contact [enterprise@supabase.io](mailto:enterprise@supabase.io).

If you are expecting a surge in traffic (for a big launch) and are on a Team or Enterprise Plan, [contact support](#) with more details about your launch and we'll help keep an eye on your project.

If you expect your database size to be > 4 GB, [enable](#) the Point in Time Recovery (PITR) add-on. Daily backups can take up resources from your database when the backup is in progress. PITR is more resource efficient, since only the changes to the database are backed up.

Check and review issues in your database using [Performance Advisor](#).

## Availability

Use your own SMTP credentials so that you have full control over the deliverability of your transactional auth emails (see Settings > Auth)

you can grab SMTP credentials from any major email provider such as SendGrid, AWS SES, etc. You can refer to our [SMTP guide](#) for more details.

The default rate limit for auth emails when using a custom SMTP provider is 30 new users per hour, if doing a major public announcement you will likely require more than this.

Applications on the Free Plan that exhibit extremely low activity in a 7 day period may be paused by Supabase to save on server resources.

You can restore paused projects from the Supabase dashboard.

Upgrade to Pro to guarantee that your project will not be paused for inactivity.

Database backups are not available for download on the Free Plan.

You can set up your own backup systems using tools like [pg\\_dump](#) or [wal-g](#).

Nightly backups for Pro Plan projects are available on the Supabase dashboard for up to 7 days.

Point in Time Recovery (PITR) allows a project to be backed up at much shorter intervals. This provides users an option to restore to any chosen point of up to seconds in granularity. In terms of Recovery Point Objective (RPO), Daily Backups would be suitable for projects willing to lose up to 24 hours worth of data. If a lower RPO is required, enable PITR.

Supabase Projects use disks that offer 99.8-99.9% durability by default.

Home

Use PITR if you require durability resilience to a disk failure event

Upgrading to the Supabase Pro Plan will give you [access to our support team](#).

## Rate limiting, resource allocation, & abuse prevention

Supabase employs a number of safeguards against bursts of incoming traffic to prevent abuse and help maximize stability across the platform

If you're on a Team or Enterprise Plan and expect high load events, such as production launches, heavy load testing, or prolonged high resource usage, open a ticket via the [support form](#) for help. Provide at least 2 weeks notice.

### Auth rate limits

The table below shows the rate limit quotas on the following authentication endpoints. You can configure the auth rate limits for your project [here](#).

Endpoint	Path	Limited By	Rate Limit
All endpoints that send emails	<code>/auth/v1/signup</code> <code>/auth/v1/recover</code> <code>/auth/v1/user</code> <code>[^1]</code>	Sum of combined requests	As of 3 Sep 2024, this has been updated to 2 emails per hour. You can only change this with your own <a href="#">custom SMTP setup</a> .
All endpoints that send One-Time-Passwords (OTP)	<code>/auth/v1/otp</code>	Sum of combined requests	Defaults to 360 OTPs per hour. Is customizable.
Send OTPs or magic links	<code>/auth/v1/otp</code>	Last request	Defaults to 60 seconds window before a new request is allowed. Is customizable.
Signup confirmation request	<code>/auth/v1/signup</code>	Last request	Defaults to 60 seconds window before a new request is allowed. Is customizable.

Endpoint	Path	Limited By	Rate Limit
Password Reset Request	<code>/auth/v1/recover</code>	Last request	Defaults to 60 seconds window before a new request is allowed. Is customizable.
Verification requests	<code>/auth/v1/verify</code>	IP Address	360 requests per hour (with bursts up to 30 requests)
Token refresh requests	<code>/auth/v1/token</code>	IP Address	1800 requests per hour (with bursts up to 30 requests)
Create or Verify an MFA challenge	<code>/auth/v1/factors/:id/challenge</code> <code>/auth/v1/factors/:id/verify</code>	IP Address	15 requests per minute (with bursts up to 30 requests)
Anonymous sign-ins	<code>/auth/v1/signup[^2]</code>	IP Address	30 requests per hour (with bursts up to 30 requests)

## Realtime quotas

Review the [Realtime quotas](#).

If you need quotas increased you can always [contact support](#).

## Abuse prevention

Supabase provides CAPTCHA protection on the signup, sign-in and password reset endpoints. Refer to [our guide](#) on how to protect against abuse using this method.

## Email link validity

When working with enterprise systems, email scanners may scan and make a `GET` request to the reset password link or sign up link in your email. Since links in Supabase Auth are single use, a user who opens an email post-scan to click on a link will receive an error. To get around this problem,

consider altering the email template to replace the original magic link with a link to a domain

you control. The domain can present the user with a "Sign-in" button which redirect the user to the original magic link URL when clicked.

When using a custom SMTP service, some services might have link tracking enabled which may overwrite or disform the email confirmation links sent by Supabase Auth. To prevent this from happening, we recommend that you disable link tracking when using a custom SMTP service.

## Subscribe to Supabase status page

Stay informed about Supabase service status by subscribing to the [Status Page](#). We recommend setting up Slack notifications through an RSS feed to ensure your team receives timely updates about service status changes.

### Setting up Slack notifications

#### 1 Install the RSS app in Slack:

Visit the [RSS app page](#) in the Slack marketplace

Click [Add to Slack](#) if not already installed

Otherwise you will get straight to next step, no need to reinstall the app

#### 2 Configure the Supabase status feed:

Create a channel (e.g., [#supabase-status-alerts](#)) for status updates

On the [RSS app page](#) go to *Add a Feed* section and set Feed URL to

<https://status.supabase.com/history.rss>

Select your designated channel and click "Subscribe to this feed"




Once configured, your team will receive automatic notifications in Slack whenever the Supabase Status Page is updated.

For detailed setup instructions, see the [Add RSS feeds to Slack](#).

# Next steps

This checklist is always growing so be sure to check back frequently, and also feel free to suggest additions and amendments by making a PR on [GitHub](#).

Edit this page on GitHub [↗](#)

-  Need some help? [Contact support](#)
-  Latest product updates? [See Changelog](#)
-  Something's not right? [Check system status](#)

---

© Supabase Inc

Contributing

Author Styleguide

Open Source

SupaSquad

Privacy Settings

