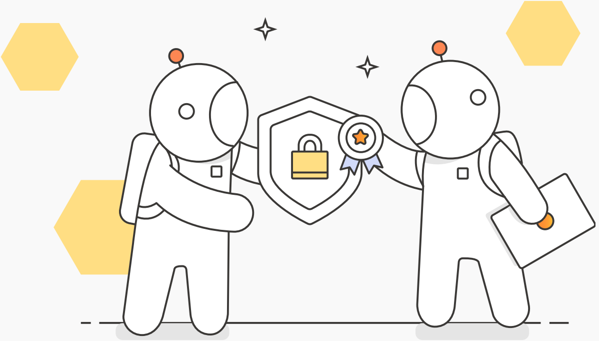
POSTMAN

Leveraging Postman Security Features

Security capabilities for control and insight into your Postman team and data.

Table of Contents

Building Trust



Security is at the core of how Postman innovates its products and services. We understand how critical your data security is to you, so it's important to us. We're building the most trusted API platform backed by the most trusted organization.

Postman maintains compliance with global industry security standards, manages vulnerabilities to secure our code, and fosters a security-first culture. We also give our community information about implementing Postman security best practices and governance controls. Furthermore, you can customize security controls that meet your organization's compliance needs.

This guide highlights security and governance features to secure your accounts and data, whether you're part of a small or a large company with enterprise-grade security needs. In addition, it gives you insight on how to leverage the features.

Security for Team Administration

An Admin can define security configurations at the team level. Postman's advanced administration features include single sign-on support, audit logs, and role-based access control (RBAC).

You can use Postman's RBAC system to manage your team's resource visibility, define the development workflow, and provide administrative and billing personnel access. Using our features also enables you to identify exposed proprietary and third-party tokens. Furthermore, you can manage your team's public resources to secure your data.

Single Sign-On

We support single sign-on (SSO) for enterprise teams using the SAML 2.0 standard and most identity providers, including Okta, OneLogin, and Duo. We recommend setting up SSO for your Postman team to get a seamless sign-in experience. Implementing SSO will also enforce team multi-factor authentication and help your organization meet regulatory compliance requirements.

User Provisioning

Postman supports the System for Cross-domain Identity Management (SCIM), which allows you to automate user provisioning and deprovisioning for your team. With SCIM enabled, you can deploy Postman to your organization and control who can access it using your identity provider.

Domain Capture

Use domain capture to manage all the Postman accounts that you created with your organization's domains or sub-domains. You can also consolidate all Postman users in your organization into a single team. In addition, you can enable SCIM provisioning and auto-flex, a flexible billing feature. Doing so can ease the process of onboarding new Postman team users when domain capture is enabled.

User Groups

Leverage user groups to organize your team members into functional groups that mimic your organizational structure. You can also assign specific roles to these groups and enable access to particular resources for all the members. We recommend using user groups to manage access control while seamlessly onboarding new Postman team members.

Roles and Permissions

Roles determine users' permissions within a Postman team, coupled with their level of access to Postman elements like collections, environments, mocks, and APIs. You can also set fine-grained access control rules for these entities by leveraging role based access control (RBAC). In Postman, you can assign various roles and permissions to a user or user group outlined below.

- **Admin**

  Users with an Admin role can define access for the Postman team members. Assign the Admin role to someone who manages your team, so they can manage all the team members and team settings.

- **Super Admin**

  A Super Admin role can manage their team settings, members, and resources in public, team, and private workspaces. Team members with a Super Admin role can perform all actions that Admin, Billing, Community Manager, and Developer roles can do (Enterprise plans only). In contrast to Admin role users, Super Admins have access to all of their team's resources to help a member make changes without the resource owner.

- **Developer**

  Developer role users have access to all team resources and workspaces. Assign the Developer role to users responsible for building and testing APIs but don't perform operational or managerial tasks.

- **Billing**

  Users with a Billing role manage a team's plan and payments. The Billing role can only be granted by a Super Admin or by another user with the Billing role.

- **Community Manager**

  Community Manager role users can manage the public visibility of public resources such as workspaces, documentation, and collection JSON links. Assign the Community Manager role to individuals responsible for managing public elements in your Postman team.

- **API Network Manager**

  Your team can enable an optional approval process for your Private API Network as a quality control measure, so a user with the API Network Manager role must approve every added API. Users with this role can also add or remove APIs from the Private API Network.

Token Scanning With Custom Alerts

Your data security is our priority. The Postman Token Scanner searches for leaked sensitive tokens on public elements such as collections, environments, and documentation. Then, it sends an alert as soon as a leak is detected.

We support an extensive list of tokens, but the Token Scanner isn't limited to them. Admins can add their proprietary and third-party tokens by defining custom tokens alerts. Postman will scan these tokens in their team's context and provide alerts for any exposure.

Team Invite Management

Users with the Admin and Super Admin role in a Postman team can manage the team invite link with an option to delete multi-use team invite links. We recommend that you regularly review active team invite links and delete them if they're no longer needed.

Audit Logs

Audit logs track Postman account changes related to user management, team management, billing, and security. We strongly recommend regularly reviewing your Postman team's audit log data for potential security issues.

Public Elements Management

The Manage Public Elements dashboard gives you a central place to control collections and environments shared outside of your team for public consumption.

You'll need a Community Manager role in Enterprise teams to view and manage everything made public by your team. These include collections links, documentation, and workspaces. You can also turn off the creation of new JSON links for collections.

Enterprise Application Management

Organizations can leverage Postman Enterprise to deploy Postman at scale while getting enterprise-class support, security, reliability, and uptime. It is available as an MSI package for Windows and a PKG package for macOS. Other capabilities include silent and system-wide installation and additional configurations to control Postman installation on users' devices.

Audit Log API

Your Postman team's audit logs are also accessible via the Postman API. You can integrate a Security Information and Event Management (SIEM) tool of your choice with this API to set up a threat intelligence system.

Security for Developers

Postman provides developers with advanced security features, including configurable API encryption and a token scanner that searches for exposed sensitive information. Learn about our security capabilities below.

Variables

Postman enables you to store and reuse values in your collection, requests, and scripts as variables. The variables give access to different scopes (global, collection, and environment) to support your use cases and workflows. You can also leverage local scope variables to prevent data synchronization to Postman's servers.

Environment Variables

Postman environment variables are AES-256-GCM encrypted on the server before storage. You also can use a secret data type that is only available in environment variables. Using it masks the value of these secret variables, helping you avoid unintentionally sharing sensitive tokens, for example, to an unintended audience during screen sharing or live streaming. We recommend using environment variables with a secret data type to store sensitive data such as API keys, access tokens, or passwords.

Postman API Key Expiry

You can control the Postman API key's expiration period after inactivity. This setting will disable your API key if it hasn't been used for a defined period.

Two-Factor Authentication (2FA)

Enable 2FA for your Postman account to add an extra layer of security when you log in using a password. Using 2FA can reduce the potential risk of an attacker compromising your account if they know your password. You can enable the feature in your account settings or visit our Learning Center for a step-by-step guide.

Token Scanner

The security of your data is important to us. The Postman Token Scanner finds your leaked sensitive tokens on public elements such as collections, environments, and documentation. Then, it sends an alert as soon as a leak is detected. We have an extensive list of tokens that we support, but it's not limited to them. You can define custom token alerts to scan proprietary and third-party tokens.

Protecting Postman API Key in GitHub

Postman sends an alert when you accidentally commit a Postman API key to a public GitHub repository. This capability is key to responding before any unauthorized access to your Postman data. If you receive an email or in-app notification about a leaked Postman API key in GitHub, we recommend that you delete the leaked API key immediately.

Workspaces

Containers called Workspaces help you organize your Postman work and collaborate with teammates. For instance, you can group your projects with a workspace acting as the single source of truth for related APIs, collections, environments, mocks, monitors, and other linked entities. You can create unlimited workspaces with a Postman account.

Additional capabilities are setting a workspace's visibility to Personal, Team, Private, or Public. These configurations provide greater control of who can access your work.

For Postman Professional and Enterprise teams, a private workspace is a team workspace that is only visible to the user who created it, plus any invited team members. Private workspaces allow teams to restrict access to collections, environments, mocks, and monitors to only a particular group.

API Encryption Configuration

Postman gives you control to configure API encryption. We encourage API providers to leverage Transport Layer Security (TLS) to secure the data, content, and other resources transmitted during each API request and response. The following options are available to developers in Postman:

Use Server Cipher Suite During Handshake

You can choose the server's cipher suite order instead of the client's during the SSL/TLS handshake.

Disable Protocols During Handshake

Specify the SSL and TLS protocol versions that you want to be disabled during the handshake. All other protocols will remain enabled.

Custom Cipher Suite Selection

You can specify the order of the cipher suites that the SSL server profile uses to establish a secure connection.

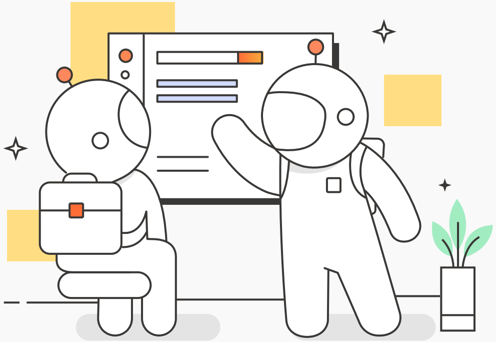
Client SSL Certificates

You can set Secure Sockets Layer (SSL) certificates on a per-domain basis when your servers require them for client authentication. If you're using HTTPS in production, this also allows your testing and development environments to mirror your production environment as closely as possible.

Plan Comparison of All Security Features

	Free	Basic	Professional	Enterprise
Users with Admin Role				
Single Sign-On (SAML SSO)	✗	✗	✓	✓
User Provisioning (SCIM)	✗	✗	✗	✓
Domain Capture	✗	✗	✗	✓
User Groups	✗	✗	✗	✓
Roles and Permissions	✗	✗	✓	✓
Super Admin Role	✗	✗	✗	✓
Audit Logs	✗	✗	✓ with 90 days of audit logs	✓ with 180 days of audit logs
Audit Log API	✗	✗	✓	✓
Token Scanning With Custom Alerts	✗	✗	✗	✓
Public Elements Management	✗	✗	✗	✓
Team Invite	✓	✓	✓	✓
Enterprise Application Management	✗	✗	✗	✓
Users with Developer Role				
Variables (with secret type)	✓	✓	✓	✓
Postman API Key Expiry	✓	✓	✓	✓
Two-Factor Authentication (2FA)	✓	✓	✓	✓
Token Scanner	✓	✓	✓	✓
Protecting Postman API Key in GitHub	✓	✓	✓	✓
Workspaces	✓	✓	✓ with private workspace	✓ with private workspace
Configure API Encryption	✓	✓	✓	✓

About Postman



Postman is the world's leading API platform, used by more than 20 million developers and 500,000 organizations worldwide for building and using APIs. Postman simplifies each step of the API lifecycle and streamlines collaboration, enabling you to create better APIs.

With Postman, you can easily store, catalog, and collaborate around your API artifacts on one central platform. Furthermore, you can keep and manage API specifications, documentation, workflow recipes, test cases and results, and metrics.

The platform also provides comprehensive tools to accelerate your API lifecycle—from design, testing, documentation, and mocking to API sharing and discoverability.

Other capabilities include advanced intelligence about your API operations by giving you alerts, security warnings, search, reporting, and more.

Postman integrates with most essential tools in your software development pipeline to enable API-first practices. Our platform is also extensible through the Postman API and open source technologies.

Contact Us

Reach out to our customer support team for questions about Postman. Also, visit our Trust Center for information about security, privacy, compliance, and reliability at Postman.

POSTMAN