POSTMAN

Leveraging Postman Security Features

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

December 2023

Table of Contents

Introduction

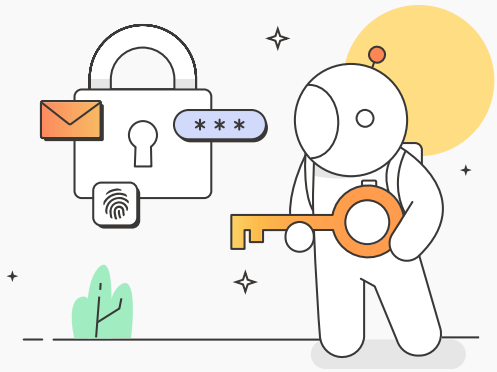
This guide covers Postman's security and governance features to protect your accounts and data. Postman maintains your trust by adhering to global industry security standards, actively addressing potential code vulnerabilities, and fostering a security-focused environment and culture.

We also share information about implementing Postman security best practices and governance controls with our community. Plus, you can tailor security measures to meet your organization's compliance requirements.

However, data security is a shared responsibility between Postman and users. Although we prioritize product security and safety, you play a crucial role in safeguarding your data and credentials in Postman. Read our shared responsibility model for security best practices.

Additionally, you can access assurance reports validating our company's security posture and standards on the Postman Security and Trust Portal.

Security for Team Administration



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

For example, Postman's RBAC system helps you manage team resources, define workflows, and control access. Our security features help detect exposed proprietary and third-party tokens. You can also secure your data by managing your team's public resources.

Learn more below.

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.

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 onboarding new Postman team members.

Security for Team Administration

Roles and Permissions

Roles define user permissions within a Postman team and a user's level of access to a Postman element, including collections, environments, mocks, and APIs. You can also set detailed 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

Admins control access and settings for Postman team members. However, they cannot access team resources, including workspaces and collections. Assign the Admin role to your team manager for complete team management.

Super Admin

As a Super Admin, you can manage team settings, members, and resources across public, team, and private workspaces. This role grants you access to all the actions that Admin, Billing, Community Manager, and Developer roles can do (Enterprise plans only). Unlike Admin role users, Super Admins can access 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 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

Users with the Community Manager role can oversee the visibility of public resources, including workspaces, documentation, and collection JSON links. Assign the Community Manager role to individuals responsible for managing these public elements within 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.

Security for Team Administration

Secret Scanning With Custom Alerts

The Postman Secret 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. If you're on an Enterprise Ultimate plan, Secret Scanner will monitor team workspaces in addition to public workspaces. We support an extensive list of tokens, but the Secret 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, helping secure your data.

Postman API Key Management

Team Admins can manage the Postman API keys your team creates at scale, ensuring you maintain compliance and security across your organization. Teams can control the creation of API keys, their expiration dates, and revoke keys when needed. You must be a Team Admin or Super Admin to use the Postman API key management dashboard.

In addition, Super Admin and Admin users in Postman can view publicly exposed API keys by visiting the Manage Postman Keys page. This includes Postman API keys detected in public repositories on GitHub and GitLab (only Ultimate projects supported on GitLab.com) and Postman's public workspaces. You can also revoke the publicly exposed keys manually or by enabling a setting to automatically revoke a Postman API key.

Team Invite Management

Users with the Admin and Super Admin roles 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.

Audit Log API

Your Postman team's audit logs are accessible through the Postman API. You can also integrate a security information and event management (SIEM) tool with this API to set up a threat intelligence system.

Public Elements Management

The Manage public elements dashboard gives you a central capability to control collections and environments shared outside 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 support, security, reliability, and uptime.

The Postman Enterprise app is available as a Windows MSI package and a macOS PKG package. Other capabilities include silent and system-wide installation and additional configurations to control Postman installation on users' devices.

Security for Developers

Postman provides developers with security features, including configurable API encryption and a secret scanner that searches for exposed sensitive information. You can also use security rules and capabilities to improve API governance and security.

Read more about our security and trust features 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 can also 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 Expiration

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 the Postman Learning Center for a step-by-step guide.

Secret Scanner

The Postman Secret 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.

All Postman plans include the Secret Scanner, which is turned on by default. The Secret Scanner actively monitors team and public workspaces for users on an Enterprise Ultimate plan.

For example, Super Admin and Admin users can access all identified secrets within their team and public workspaces.

Security for Developers

Workspaces

Containers called Workspaces help you organize your Postman work and collaborate with teammates. You can group your projects within a workspace, serving as the single source of truth for related APIs, collections, environments, mocks, and monitors.

Moreover, you can assign different role types in Postman workspaces, including Admin, Editor, and Viewer. Doing so enables you to control access at a workspace level. Additionally, you can create unlimited workspaces with a Postman account.

Other additional capabilities include setting a workspace's visibility to Personal, Team, Private, or Public. These configurations provide greater control over who can access your work.

Securing Postman API Keys in GitLab

You can leverage our integration with GitLab Secret Detection to protect your Postman API keys in GitLab public repositories. This service will notify you if you accidentally commit a valid Postman API key to a public repository on GitLab.com.

You can enable GitLab Secret Detection in an Ultimate project on GitLab. com to activate this protection. Doing so will enable you to respond quickly and help prevent any unauthorized access to your data in Postman.

Protecting Postman API Keys 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.

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.

Turn Off 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.

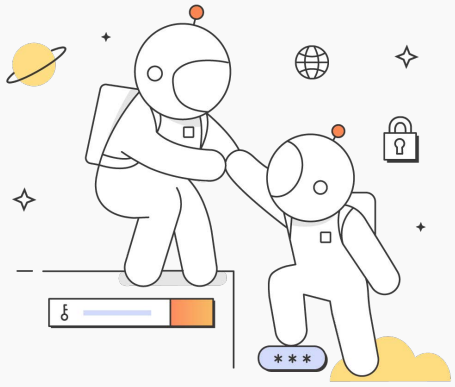
Custom Cipher Suite Selection

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 per-domain basis when your servers require them for client authentication. Using HTTPS in production also allows your testing and development environments to mirror your production environment as closely as possible.

About Postman



Postman is an API platform trusted by more than 30 million developers and 500,000 organizations worldwide for building and using APIs. Postman simplifies each step of the API lifecycle and streamlines collaboration so you can create better APIs—faster.

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

The API Platform also provides tools to accelerate your API lifecycle—from design, testing, documentation, and mocking to API sharing and discoverability. Other capabilities include intelligence about your API operations by giving you alerts, security warnings, search, reporting, and more.

Also, Postman integrates with 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.

Questions and Resources

- Contact our customer support team for Postman inquiries. You can also notify Postman about potential errors in security information on our external web pages.
- Compare security features among the different plans by visiting the Postman API Platform's plans and pricing resource.
- Access our Security and Trust Portal for our company's security, privacy, compliance, and reliability information.
- Check out the docs and support resources on our Learning Center to learn how to use Postman.
- We also recommend that you read our Security Content Hub for the latest resources on API security, product safety and trust. You can also find answers to some of our company's most common security questions.

Help Secure Postman

We invite anyone to identify and report potential security vulnerabilities in the API Platform. Access our security reporting guidelines and policy.

POSTMAN