

Personal access tokens

Personal access tokens were added in [Bitbucket Server 5.5](#) and can be used to replace passwords over https, or to authenticate using the Bitbucket Server REST API over Basic Auth.

On this page

Using personal access tokens

For git operations, you can use your personal access tokens with your REST API.

In addition to basic auth over REST API, you can use it as a bearer token, by setting the personal access token as a header value, instead of providing user name and password.

Below is an example of a REST request using a bearer token.

```
curl -H "Authorization: Bearer MDM0MjM5NDc2MDxxxxxxxxxxxxxxxxxxxxxxxx"
http://localhost:7990/bitbucket/rest/api/1.0/projects/WORK/repos/my-repo/commits/?until=master
```

Generating personal access tokens

To generate a personal access token from within Bitbucket Server go to Manage account > Account settings > **Personal access tokens**.

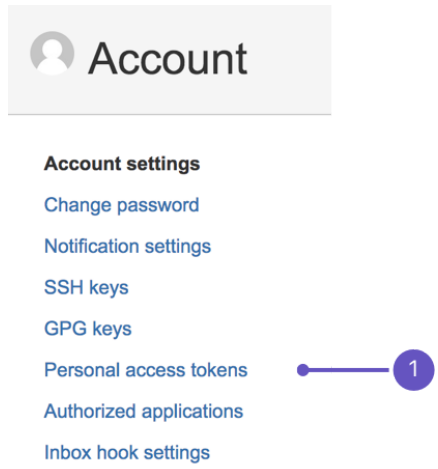


Admins **cannot** create tokens for users.

Admins **can** change and revoke tokens from the users personal tokens page.


Permissions and how they work

From here, you can modify permissions or revoke tokens.



Modifying permissions to get the correct access

Permissions will default to your existing level of access. Because of this, it is recommended that you restrict the token's permission to the level it will need. Permissions here are intended to restrict what the token can do, with the maximum bound being what the associated user can do.

 Repo permissions are inherited from the project permissions.

When creating an access token you can limit its project and repository permission. Note that repository permission is at least as permissive as the project permission, so if you give a token project write, you are unable to give it only repo read (it must be write-level or higher).

Permissions table

The following table summarizes the possible permissions that can be assigned to a personal access token.

	Project read	Project write	Project admin
--	--------------	---------------	---------------

	Project read	Project write	Project admin
Repository read	<ul style="list-style-type: none"> ✓ Pull and clone repositories 	<ul style="list-style-type: none"> ✗ 	<ul style="list-style-type: none"> ✗
Repository write	<ul style="list-style-type: none"> ✓ Perform pull request actions ✓ Push, pull, and clone repositories 	<ul style="list-style-type: none"> ✓ Perform pull request actions ✓ Push, pull, and clone repositories 	<ul style="list-style-type: none"> ✗
Repository admin	<ul style="list-style-type: none"> ✓ Perform pull request actions ✓ Update repository settings and permissions ✓ Push, pull, and clone repositories 	<ul style="list-style-type: none"> ✓ Perform pull request actions ✓ Update repository settings and permissions ✓ Push, pull, and clone repositories 	<ul style="list-style-type: none"> ✓ Perform pull request actions ✓ Update repository settings and permissions ✓ Update project settings and permissions ✓ Push, pull, clone, and fork repositories ✓ Create repositories

Security and encryption

Personal access tokens are a secure way to use scripts and integrate external applications with Bitbucket Server.

If an external system is compromised, you simply revoke the token instead of changing password, and consequently changing it in all scripts and integrations.



Atlassian recommends you only map one token per integration.

If the system is compromised, you can remove that token and not affect any of the other integrations.

Last modified on Sep 27, 2018