

Using Personal Access Tokens认证

除了Basic authentication认证方式以为，Personal Access Tokens是我们推荐使用的新认证方式，

个人访问令牌（PAT） 是一种使用脚本并将外部应用程序与 Atlassian 应用程序集成的安全方式。如果外部系统遭到入侵，您只需撤销令牌，而不是更改密码，从而在所有脚本和集成中更改密码。

个人访问令牌是使用用户名和密码对各种服务进行身份验证的安全替代方法。

可以在以下 Atlassian 应用程序的 Data Center 和 Server 版本中创建和使用个人访问令牌：

- Jira Core 8.14 及更高版本
- Jira Software 8.14 及更高版本
- Jira Service Management 4.15 及更高版本
- Confluence 7.9 及更高版本

 admin

汇总

个人访问令牌

已授权的应用

个人访问令牌

请将个人访问令牌用作通过用户名和密码进行身份验证的安全备选方案。[了解更多](#)

名称	创建日期	过期日期	上次身份验证时间	
test11	2024年3月22日 GMT+8 15:51:43	从不	2024年3月22日 GMT+8 16:04:48	撤销

创建令牌

创建个人访问令牌

请将个人访问令牌用作通过用户名和密码进行身份验证的安全备选方案。

 个人访问令牌与密码一样重要，因此应予以同等保护。

令牌名称 *

test22

剩余字符数：34

权限

个人访问令牌的权限级别已设置为您目前拥有的访问级别。

过期日期

出于安全原因，您可以将此令牌设置为自动过期。令牌创建之后，即无法更改过期日期。

☐ 自动过期

过期前剩余天数

90

该令牌永不过期。

创建

取消

已创建新的个人访问令牌

请复制该令牌并将其存储在安全空间中。单击之后，即无法再看到令牌 **关闭**。

NTQ0Njk0MjUzMTI3Ogty63gSzvTpvFcivQOZZyzK629L



关闭

如用JAVA的方式，代码示例如下：

```

import com.sun.jersey.api.client.*;

public class BaseClientMain {
    public static void main(String[] args) throws Exception {
        try {
            Client client = Client.create();
            WebResource webResource = client.resource("http://localhost:8080/rest
/api/2/issue/QA-31");
            ClientResponse response = webResource.accept("application/json")
                .header("Authorization", "Bearer
NTQONjkOMjUzMTI3Ogty63gSzvTpvFcivQ0ZZyzK629L")
                .header("X-Atlassian-Token", "no-check")
                .get(ClientResponse.class);

            String msgback = response.getEntity(String.class);
            System.out.println(msgback);
            response.close();
        } catch (UniformInterfaceException e) {
            e.printStackTrace();
        } catch (ClientHandlerException e) {
            e.printStackTrace();
        }
    }
}

```

说明

- header中使用的: NTQONjkOMjUzMTI3Ogty63gSzvTpvFcivQ0ZZyzK629L, 为admin的token 令牌