

# Basic Authentication认证方式

Basic authentication方式主要是将用户的用户和密码写入到http的请求header中。具体的实现原理可以查看：[https://en.wikipedia.org/wiki/Basic\\_access\\_authentication](https://en.wikipedia.org/wiki/Basic_access_authentication)

采用Basic authentication，用户名和密码通过请求反复发送，会缓存在Web浏览器上，相对来说并不是太安全。

REST API是由通过认证标准的Web界面，提供相同的限制保护。也就是说，如果你没有登录，你即为匿名访问JIRA。

此外，如果你登录了，但些账户在Atlassian产品中并没有相关权限在那些你还是无法查到所需要的资源（即REST API对你来说是不可用的）。

以下我们将展示相关采用Basic authentication的例子

```
curl -D- -u fred:fred -X GET -H "Content-Type: application/json" http://localhost:8080/rest/api/2/issue/QA-31
```

或者

```
curl -D- -X GET -H "Authorization: Basic YWRtaW46YWRtaW4=" -H "X-Atlassian-Token: no-check" -H "Content-Type: application/json" "http://localhost:8080/rest/api/2/issue/QA-31"
```

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", "Basic YWRtaW41M0FhZG1pbG==")
                .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：YWRtaW41M0FhZG1pbG==，为admin:admin字串在经过base64位编码后的值
- admin:admin中间有一个冒号
- BasicYWRtaW46YWRtaW4=

