

Keytab files

What is a Keytab file and why do I need one?

Kerberos works by issuing and validating cryptographically signed tokens. When your user wants to log into JIRA (or Confluence etc), their browser will send a Kerberos token issued by the Key Distribution Center (typically an Active Directory Domain Controller).

The server then validates this token against a preconfigured Kerberos *keytab* file. The keytab file contains a secret which is shared between the add-on and the KDC. This secret allows the add-on to prove that the user's token could only have been issued by the KDC. In Active Directory, this secret is based on the password of the account which the Kerberos service is mapped to.

From a technical point of view, you can look at the keytab file as the result of a cryptographic function taking two inputs: the *service principal name* and the secret password.

The service principal name is a string looking like this:

```
HTTP/issues.example.com@EXAMPLE.LOCAL
```

Here, *issues.example.com* should be replaced with the full, canonical host name of your JIRA (or Confluence etc) instance, *EXAMPLE.LOCAL* should be replaced with your Kerberos Realm, this is typically the name of your top level node in Active Directory (dc=example,dc=local) in uppercase.