FAQ

Licensing

How do i get a license?

Trial licenses and extension of existing trials are requested on https://my.atlassian.com. Licenses are bought from Atlassian Marketplace or through your preferred Atlassian Expert.

Can we extend our trial beyond 30 days?

Sure, here are direct links to where you can generate new licenses.

- New evaluation license for JIRA
- New evaluation license for Confluence
- New evaluation license for Bitbucket
- New evaluation license for Bamboo
- New evaluation license for FishEye/Crucible

Which license tier do I need when purchasing an add-on?

See Atlassian's licensing FAQ**:** **https://www.atlassian.com/licensing/marketplace#licensingandpricing-1**

"Purchase the license tier that matches the number of users you have licensed for your host application. For example, if you have a 25-user Confluence license, purchase the Confluence add-on at the 25-user tier.
The add-on will only function if its license matches or exceeds the tier of the host application – even if only some of your licensed users need to use the add-on."

For JIRA, the license has to match the **highest application tier**. If you have a 500-user JIRA Software license, and a 250-user Core license, then the license needs to be at the 500 level.

JIRA ServiceDesk customers can log in with our add on for free since they are not counted against the user tier.

Examples:

25 JIRA service desk agents and 10000 service desk customers = Kerberos 25 user license

50 JIRA service desk agents, 10000 service desk customers, 500 JIRA Software Users = Kerberos 500 user license

What happens when the trial expires?

Without a license our plugin will not log in users. Users are presented with the standard logon page. The Kerberos test page will still function, and will report whether a user can successfully log in or not.

Keytab files

How do I create a keytab file?

Keytab files are created with ktpass. Preferably on server 2008 or later. The user running ktpass must be member of domain admin or enterprise admin.
See this section for detailed instructions.

How do I merge keytabs?

Ketyabs are merged with ktutil (linux). Using ktpass will add a SPN to an excising keytab, bumping the version number if it exists.
See this section for detailed instructions

Key version mismatch in the test page

Either the latest generated keytab is not uploaded to our plugin or the clients holds on to an outdated ticket. Make sure the latest generated Keytab is uploaded to our plugin and run **klist purge** on the client to purge Kerberos tickets. Run the "Active Directory server test" to detect possible misconfigurations

Authentication

Browser sends an NTLM token instead of a Kerberos token

Browsers on Windows will first try to acquire a Kerberos token. If that fails for some reason, the browser falls back to sending an NTLM token.

The most common reason for Kerberos to fail is that the site is not in the Local Intranet Zone (IE and Chrome) or that the site is added to the trusted URL list in Firefox. See browser configuration for details.

Other common reasons for Kerberos to fail is that you have issued the keytab using the wrong Service Principal Name. See How Kerberos Works for details about how browsers determine the SPN.

I have to press the login button to be logged in.

Our plugin does not try to log in a user when Confluence would otherwise not have required that user to log in.

This means that all users will see the page anonymously. If they then press login or access content that requires authentication, then a Kerberos login will be attempted. When an attempted login fails (either because the end user is not a Kerberos user or because the user is not known to Confluence), then the plugin will fall back to showing Confluence's login page. The most common reason is Confluence with anonymous read permissions.

Links to filters does not automatically log in users.

Our plugin only tries to log in a user when JIRA would otherwise have required that user to log in. JIRA will show different results whether the user is logged in or not, and hence does not redirect to the login page for anonymous users. This results in Kerberos Authentication not being triggered.
Enabling "Preemptive authentication" forces Kerberos logon to filter URL`s.

Does application links work with our add-on?

Our add-on ignores does not affect how application links work. Because users don`t have to authenticate to each application, we recommend using OAuth Impersonation application links.

The user has to log on manually the first time

Make sure the Default Group Memberships is set. This setting can be found when editing the user directory. Make sure the group has global logon permissions.
Because of an unexpected behavior in confluence when checking if the user has logon permission try configuring "configured required group".

How can we limit who should be logged in with Kerberos

Our plugin supports IP white/ blacklisting. For IP white/ blacklisting to work our plugin needs to see the correct client IP.
Which client IP our plugin sees is shown under "Client IP restrictions".

User sessions time out after 4 or 5 hours, can we increase the session timeout?

Our plugin does not affect the session timeouts in the Atlassian products they run on. Please refer to Atlassian's documentation if you need to change this:

- JIRA: https://confluence.atlassian.com/jirakb/how-to-change-the-default-session-timeout-604209887.html
- Confluence: https://confluence.atlassian.com/confkb/how-to-adjust-the-session-timeout-for-confluence-126910597.html
- Bitbucket: https://confluence.atlassian.com/bitbucketserverkb/how-do-i-change-the-default-session-timeout-779171650.html

Alternative UPN Suffixes

When Active Directory is configured with alternative UPN suffixes (e.g. both example.com and example.local) Kerberos Authentication can be set to look up users with both. Configure additional user mappings to reflect the Alternative UPN suffixes in Active Directory Domains and Trusts.

Does single sign-on work with Bitbucket clients?

Yes, single sign-on can be configured also for Git clients. There is an option to enable Kerberos on the common /scm/* path and an alternative path. Enabling this will allow Git clients to clone from the alternate, Kerberos-enabled path /kerberos-scm/*

An alternate clone URL "HTTP+SSO" will also be added to the Bitbucket clone dialog.

See Kerberos for Git clients for details

Why am I asked for a password to enter the admin section?

This is by design. If you would like users to be able to enter the admin section without entering their passwords, Atlassian has a way of disabling secure administrator sessions (WebSudo)

https://confluence.atlassian.com/adminjiraserver073/configuring-secure-administrator-sessions-861254024.html

Can we make SSO work for users with non UTF-8 characters in their username?

Non-UTF characters in usernames is not supported by Java's Kerberos implementation by default. To enable support for UTF-8, you need to set the property `-Dsun.security.krb5.msinterop.kstring=true` (typically in setenv.sh). This will allow usernames with characters such as ö, ü, ä to sign in log using Kerberos.

User Directories

How are Kerberos users mapped to accounts in User Directories?

Kerberos uses the sAMAccountName Active Directory attribute to identify users.

The add-on will extract this username from the client's Kerberos Principal Name and use that when looking up users in User Directories.

Example: If the Kerberos Principal Name is "johndoe@EXAMPLE.LOCAL", the add-on will search User Directories for the account "johndoe".

This means that if your accounts are named with the standard username attribute, you can use any of the User Directory types supported by Atlassian:

- Active Directory,
- Atlassian JIRA
- Crowd
- Generic LDAP
- Internal
- Internal with LDAP Delegation

If you have multiple User Directories, the user will be looked up in the same order as with manual logon.

Our Active Directory has a non-standard User Name Attribute, will that work?

Yes. Our add-on will automatically detect that your User Directory has a non-standard User Name Attribute. (Different from sAMAccountName, say "userPrincipalName")

If this is the case, the add-on will first look up the account in AD using the standard sAMAccountName, then map it to the configured User Name Attribute you configured, and finally perform a new search using that name.

Can we use a Crowd User Directory?

Yes. Our add-on will search your Crowd User Directory with the standard account name (sAMAccountName)

Can we use an Internal User Directory?

That's certainly possible, but to simplify user management we recommend you set up an Active Directory User Directory instead, perhaps using local groups.

Environment

Can SAML and Kerberos work in combination?

Yes! When both SAML and Kerberos is configured, Active Directory joined devices can benefit from password-less SSO with Kerberos, while mobile phones and other standalone devices are offered SAML SSO.

What server operating systems are supported?

Actually, JIRA/Confluence etc. may run on any operating system.

Does the server running the application have to be domain joined?

The server may or may not be domain joined.

Is SSO from multiple domains supported?

Yes. Create a keytab file. One for each domain. Merge the keytabs to one file and upload it.

How does Confluence collaboration (synchrony) work with Kerberos

Very large Kerberos tokens may affect Synchrony. If users are experiencing issues with collaboration, run the **Web Server Test** inside our add-on and it will tell you how to apply configuration to the proxy server. Sample configuration can be found here.

Can we use AES encryption with server 2003 / domain functional level 2003?

No, domain functional level must be 2008 or greater. Run the "Active Directory server test" in our plugin to determine the functional levels.

Advanced Encryption Standard (AES 128 and AES 256) support for the Kerberos protocol. In order for TGTs to be issued using AES, the domain functional level must be Windows Server 2008 or higher and the domain password needs to be changed.

Is Linux KDC supported?

Our plugin does not communicate with the KDC at all. We receive the SPNEGO token as an HTTP header and verify that against the uploaded/configured keytab file. Our plugin don't really care where the keytab file was created, as long as it is in the valid keytab file format and has keys with the right encryption type, version number, Service Principal Name and key material. There is no network traffic going on during this verification process.

Our built in Active Directory Test Page expects to test an Active Directory server. There is nothing preventing you from using a different KDC. As long as it is configured properly.

Manual login stops functioning after issuing a keytab

If the user used to bind to Active Directory is used when creating a keytab you may experience that all user logons fail. To fix the issue delete the user account in Active Directory and recreate use user with the same username and password as before. An alternative is to log in with a user in the internal user directory and alter the Active Directory user directory. A third option is to alter the settings directly in the database.

Kerberos plugin detects Duplicate SPN

Duplicate SPN (e.g. HTTP/jira.example.com) cannot exist in Active Directory. The Kerberos test page detects duplicate SPN. To the resolve the issue either delete the user in Active Directory that has the duplicate SPN. An alternative is to remove the SPN from the user object. **setspn -D HTTP/jira.example.com accountname**

Web proxy server configuration

How to configure Kerberos Authentication with Apache?

See this section for detailed instructions

Does Kerberos work with mod_proxy_ajp?

We have seen problems with Apache 2.2 combined with allowing large HTTP headers (using ProxyIOBufferSize). We recommend using HTTP instead of AJP, or using Apache 2.4.

How to configure Kerberos Authentication with Nginx?

Atlassian has documentation on how to configure Nginx. We have sample configuration available at this page

We get a blank page when authenticating

A blank page is in most cases a HTTP 400 error. More detail can be obtained by disabling http friendly error messages. Some Kerberos clients send Kerberos tokens which are so large they make the client request exceed the *maximum header size limit* of your server (typically around 8000 bytes for both Apache,Nginx and Tomcat). (IIS is about 16K)

Circumventing HTTP 400 can be done by appending ?nokernerberos to Dashboard.jspa or login.jsp

Bundled with the plugin there is a test to determine an appropriate value. (Maximum header size test page) Changes has to be made to both Tomcat and a proxy if one is used. Tomcat needs to be restarted to apply the changes.

The Usage counters reports a lot of client did not return a token

Improperly configured browsers will not reply with a Kerberos token. Monitoring software may also generate hits to this counter. The counter is reset with restart of the application.