

SSO with Kerberos (IWA / Integrated Windows Authentication)

Integrated Windows Authentication / Kerberos gives the end user access to Atlassian products **without entering user name or password**. It is typically used in an enterprise LAN, and is the preferred choice for Windows domains and Microsoft Desktop environments.



- ✓ Secure authentication without passwords
- ✓ Works in combination with SAML SSO. Give users the best login experience on any network

IWA / Kerberos requires that client machines have access to a Key Distribution Center (KDC), which in the Windows world generally means Active Directory. For security reasons, AD is generally not reachable outside the local network/corporate intranet, making Kerberos mainly applicable within a company.

It is perfectly fine to combine IWA with other SSO mechanisms such as SAML. In such a combination, IWA provides hassle-free login experiences when the user is present at his desktop machine on the office, while SAML enable the user to log in when they on the run outside the office or when accessing from cellphones or other non-Kerberos compatible devices.

[Setup guide for Integrated Windows Authentication \(Kerberos\)](#)

[How Kerberos works](#)

[Kerberos FAQ](#)

[Requesting support](#)