

thinSSO

Federated Single Sign On for Business Applications



thinSSO Features

- Zero sign for all web based applications
- Implicit support for Windows Native Authentication using NTLM and Kerberos
- Centralizes user authentication to AD without duplicating user base
- Platform Independent, light weight, very low foot print, does not require dedicated hardware
- All data transfer over SSL
- Identity negotiation between thinSSO and Oracle Applications using one-time use RSA encrypted keys. The tokens cannot be reused and expiration of tokens can be configured.
- Identity negotiation between thinSSO and Other Business Applications using industry standard SAML tokens
- Support for both Kerberos and NTLM. NTLM is the de facto single sign on framework for Microsoft products like Sharepoint, Web Outlook.
- Windows password is never sent to thinSSO web application or Business Applications
- thinSSO supports local non-AD authentication to be enabled for specific users.
- thinSSO supports overriding of Zero Authentication for Power users by forcing them to reconfirm their AD credentials.

Introduction

thinSSO is a light Federation Single Sign On engine to integrate business applications together at a fraction of cost of other Single Sign On products. Through a unique feature of Zero Sign In, thinSSO integrates cross domain geographically distributed applications without the heavy weight lifting of SOA, BPEL and other integration technologies.

thinSSO Security

thinSSO is designed around industry standard cryptographic algorithms and identity federation methodologies such as SAML.

thinSSO Data Sheet

- Built on Open Standards
- Simple to implement, Easy to administer and maintain

thinSSO Deployment

- Onsite prototype of thinSSO in 8 hours
- No dedicated hardware required even in production
- Platform independent, deployable on any J2EE compliant web server
- Simple High Availability topology

thinSSO Implementation

thinSSO implementation is much simpler and faster than other integration suites like SOA Suite, Identity Management Suite. We complete a fully functional onsite prototype of thinSSO in 8 hours and production deployment in 3 weeks time including user testing.

thinSSO Compliance

- **Centralized Authentication:** SOX recommends centralized authentication and user management. thinSSO further simplifies SOX controls and auditing by integrating the center piece of corporate user base Active Directory with business applications.
- **Risk mitigation for user termination exceptions:** Terminated Users are blocked from all integrated web applications and thus eliminates all the risks associated with this control exception and in effect makes it insignificant.
- **Audit Logs:** thinSSO access logs contain all the information needed to for SOX auditing and can be also used as evidence for exceptions in user termination control.
- **Password and Account Sharing:** SOX discourages account and password sharing which is very convenient and tempting for users in a decentralized authentication system.
- **Re-Verification for Power Users:** thinSSO can be configured to re-authenticate a user besides the implicit WNA user authentication for specific power users.