DATASHEET

Enterprise Single Sign-on

Single sign-on made simple

Benefits

- Bases single sign-on on Active Directory or any other LDAP identity store
- Enforces security and access policy enterprise-wide
- Implements a single point of strong authentication for all resources
- Enhances IT and user efficiency
- Helps you achieve regulatory compliance

System requirements

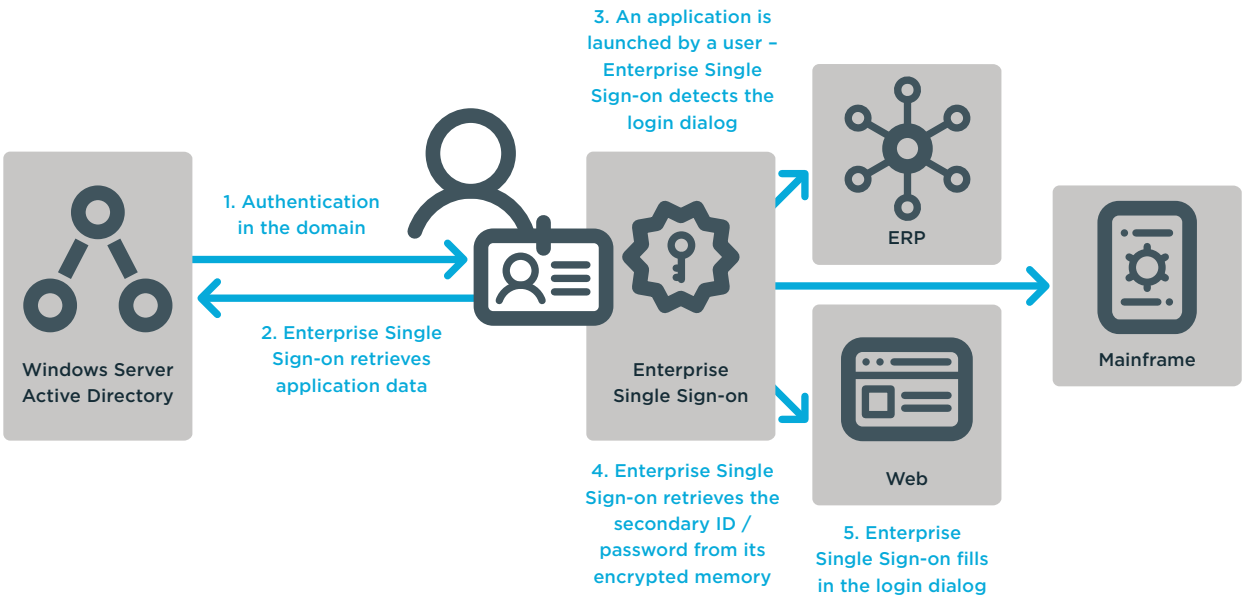
For a complete list of system requirements, visit quest.com/products/esso/

A consequence of today's increasingly decentralized IT environments is the proliferation of passwords and the burden they present to users. Organizations want to reduce this complexity while improving security and operational efficiency.

Single sign-on (SSO) can be the answer to these tough challenges. Unfortunately, most single sign-on solutions are limited in scope, require costly and hard-to-manage additional infrastructure, or demand ongoing maintenance. In many cases, these solutions actually increase the complexity they are supposed to simplify.

One Identity's Enterprise Single Sign-on solution addresses these challenges. As the industry's leading enterprise SSO solution, it makes single sign-on simple and secure. Enterprise Single Sign-on requires no

ONE IDENTITY



Enterprise Single Sign-on extends the Windows logon to all password-protected applications.

hard-to-manage infrastructure, and streamlines both user management and enterprise-wide administration of single sign-on.

Features

Active Directory-based single sign-on — Base single sign-on and access control for the entire enterprise on the existing identities, groups and policies built into your existing Active Directory deployment, without requiring additional authentication methods or a metadirectory.

Security & access policy enforcement — Use established access policies and Active Directory rules to apply similar controls to client-based SSO for the entire enterprise-wide range of applications and systems to which a user may need access.

A single point of strong authentication — Provide a single point of user authentication to any system and application. This includes standard username/password logins as well as the entire range of strong authentication options, such as smart cards, biometrics and token-based two-factor authentication.

Improved IT & user efficiency — Relieve IT staff of the burden of managing user access and resetting passwords across a wide range of applications. Enhance user productivity by freeing users from having to remember passwords for multiple systems and applications.

Compliance support — Achieve compliance with common requirements for access control, strong authentication and secure delegation of access rights by implementing a consistent, strong, Active Directory-based infrastructure for access policy enforcement.

Auditing and reporting — Generate audit reports from sign-on or LDAP data, including statistics if desired, from an intuitive, easy-to-use interface.

Drag-and-drop configuration — Adapt applications to your unique environment with ease, without modification or custom connectors.

Optional fast user switching — Enable users to share a physical workstation using individual authentication and real- time context switching.

Optional password reset — Enable users to manage their own network password resets by answering secret questions from a web interface or a Windows login interface.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

Learn more at OneIdentity.com

Datasheet-ESSO-US-KJ-23536

ONE IDENTITY