

Most SSO vendors claim to provide single sign-on for the enterprise, and while they technically may be able to demonstrate SSO in a test or RFI environment, buyers would be wise to consider the following additional capabilities and requirements which affect the security, feasibility, and cost of SSO deployments.

1. MS Windows Authentication. It is important that any SSO solution not replace or modify Microsoft's Graphical Interactive Network Authentication (GINA), because replacing the GINA can impact Microsoft's support and warranty for the OS. Some SSO solutions either modify or replace parts of GINA, causing problems down the road as the OS changes or other issues arise requiring Microsoft's support.
2. Application Support. SSO vendors typically provide application support using either scripting (scripts based on initiation from a tool bar or icon replacement) or event detection methods. If scripting methods are used, scripts must be written and maintained for each application. Scripting requires timing delays to ensure proper interfacing with application logons, and can be interrupted if users are simultaneously typing on their keyboards. If scripts encounter unexpected events while running, they can end up in an endless loop that consumes the full CPU. The better alternative is to use event detection, an intelligence-based approach that detects sign-on events based on the normal operation of an application. Event detection SSO solutions typically do not require scripts, agents or connectors to handle logon, password change and errors, and can be easier and cheaper to deploy.
3. Support for disconnected mode. Can the SSO vendor's product run in a disconnected mode? If your organization includes "on the go" or "field" users, it is important to consider how the SSO solution will support disconnected mobile users who don't have access to the corporate intranet or network, but still have SSO requirements and needs. Another important scenario is how the SSO solution performs in the event of network congestion or disruption; or the loss of a directory service. Can most users still accomplish their work when access to remotely stored credentials is lost or blocked?
4. Centralized Configuration, Deployment and Administration. Does the SSO vendor support software deployment using any deployment tool—Windows Installer (MSI), SMS, Tivoli, etc? Can the SSO vendor easily configure user environments to control password policies, system rules, UI functionality, re-authentication parameters, and other policy requirements? Does the SSO solution assist first-time use by supplying user credentials for specified applications? Does the SSO product enable to security or other authorized personnel to configure most product features globally, by application type, or by application?
5. Extensive Crypto Standards Support. Standards are ever changing so it is important that SSO vendors implement their solutions in such a way as to ensure compatibility with existing standards, as well as to provide the capability to easily change to new crypto standards that emerge. For example, while Triple DES has been popular in the past, AES is an emerging recognized standard for US Federal Government top secret data. Another standard is FIPS 140, required for many government and civilian projects.
6. Credential Protection. If credentials are stored locally or downloaded into local memory, SSO vendors should take great care to protect them. It is advisable to test SSO solutions to ensure that credentials are never stored "in the clear" in memory, a condition making them susceptible to detection and compromise.
7. Session Security. Does the SSO vendor use defensive mechanisms to ensure that a session is not breached by another process? With some SSO solutions, processes can be accessed and breached by simple developer tools, allowing another process to gain control and expose credentials.

8. Directory support. Is the solution dependent on a proprietary repository that requires separate administration and hosting? Or does the solution leverage your investment in your existing or future directory?
9. Directory Synchronization. Is directory synchronization timer or event based? Some solutions typically employ timer-based synchronization, exposing the possibility for a user's credentials to get out of synch if using multiple machines or sessions when the synch session is set too long. Conversely, if the synch session is too short, timer-based SSO solutions may cause significant and unnecessary directory traffic and activity.
10. Multiple Directory/Repository Support. Another important aspect to consider is support for multiple directories, an important capability facilitating migrations from one directory infrastructure to another. If the SSO vendor supports only one directory at a time, it can be difficult to transition or support complex multi-directory environments.
11. Credential Synchronization. When making a change to a user's single credential, check to see if the SSO vendor has to sync the entire "blob" of user credential data, including both the records that changed and those that did not. If the SSO vendor has to rewrite the entire blob, it creates unnecessary network and directory traffic as well as significant unnecessary directory write activity, and might negatively affect the ability of the SSO solution to scale at the enterprise level. Directory reads have almost no overhead on directory performance; however, frequent or large numbers of directory writes can adversely affect directory performance.
12. Product Memory Footprint. The size of the SSO product memory footprint can affect several areas of scalability and performance. For example, script-based products typically have a much larger product credential memory "footprint", limiting the number of credentials that can be placed on smart cards. The product memory footprint while in use is also a consideration since it will have an impact on user sessions (note that Outlook requires 17 MB), affects client performance, and limits the number of users per Terminal Services or MetaFrame server.



160 Pearl Street, 4th floor, New York, NY 10005
Tel: 212.825.9100 x 2 or 866.727.7564 x 2
Fax: 212.825.0326

Web: www.passlogix.com
Email: sales@passlogix.com