Choosing an SSO Solution—Ten Smart Questions

Looking for the best SSO solution? Asking these ten questions first can give your users the simple, secure access they need, save time and money, and improve IT security.

1. **Is the solution an easy one for users to adopt in their daily routine and quickly develop a comfort level with?**

SSO solutions change the way users interact with and access their applications. They eliminate sticky notes and handwritten password lists as well as Microsoft Word files and other insecure methods for storing passwords. Because they are meant to simplify the user’s life, SSO solutions should be easy and hassle-free for users to adopt in their daily routine and develop a comfort level with. This can be accomplished in a variety of ways. Users should not have to manually enter all of their secondary credentials the first time they use the product. Look for a solution that makes single sign-on completely transparent to the end user. The best software will pre-populate each user’s secondary credentials upon setup. It should also integrate with user provisioning products such as HP Select Identity, Courion AccountCourier and IBM Tivoli Identity Manager.

2. **Does the SSO solution enable users to change their passwords right from their desktops or unlock their accounts without calling the help desk?**

A password management solution should give you better management—not more to manage. For instance, can the solution allow users to reset their own passwords and unlock their Windows accounts? This will take the burden off your help desk.

Also look for SSO software that will automate routine password-related tasks, such as generating and changing passwords behind the scenes—eliminating the problem of forgotten passwords.

3. **Does the solution provide single sign-on for all applications—Windows, Web and host-based?**

Many SSO solutions provide single sign-on for Web applications only. Worse yet, some solutions simply provide password synchronization, where the password to all applications is the same. By contrast, enterprise single sign-on spans all applications with unique, strong passwords.
4. **Does the SSO Solution Provide Access to All Password Protected Applications Regardless of Whether the User is Connected to the Corporate Network?**

SSO solutions should be able to function when users are disconnected from the corporate network. Generally two sets of encrypted credential stores are used, one locally installed and one centrally located on the network. These two credential stores are then synchronized using built-in functionality. The result is that when users are disconnected, they will still be able to authenticate to local applications using their local credential store. This is a key convenience for users and increases their willingness to adopt and use the product.

5. **Do Your Users Roam or Share Workstations?**

Especially in environments like healthcare, retail and manufacturing, users share workstations and roam among devices. It can take minutes to log on and off at shared workstations. As a result, users leave the workstations open or IT administrators may use generic accounts to speed logons. Look for a solution that provides rapid logon and logoff to shared workstations. It should also be able to provide roaming users with a way to move among devices seamlessly.

6. **How Secure is the Solution?**

Users often create weak passwords in order to make them easy to remember. This makes them easy to guess. Poor password behavior also includes infrequent password changes. The best password management solution puts control in the hands of IT, allowing for tight password policies that reduce vulnerability and ensuring that passwords are changed regularly.

The solution should also:

- prevent end users from gaining access to other user settings and credentials
- protect against malicious administrator activity
- protect against credential store brute force attacks
- properly encrypt credentials while “at rest”
- properly encrypt credentials during transmission between the store and the agent

Don’t just take the vendor’s word for the security of the product. Be sure to look for third-party validation of their security methodology. Foundstone Labs, a division of McAfee, is one independent testing organization that tests and certifies SSO solutions according to rigid standards.
CHOOSING AN SSO SOLUTION—
TEN SMART QUESTIONS

7. DOES THE SOLUTION INTEGRATE WITH MULTIFACTOR AUTHENTICATION DEVICES?
Multifactor devices tighten security, but they can be difficult to integrate with enterprise SSO solutions. Find a solution that interoperates with multifactor authentication devices, including both certificate-based and password-based devices.

8. WILL THE SOLUTION HELP YOU MEET COMPLIANCE REQUIREMENTS OF SUCH LEGISLATION AS SARBANES-OXLEY AND HIPAA?
Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, the European Union Data Protection Directive and other regulations mandate a high level of internal control over resources. Be sure the solution you implement has logging processes and audit trails that make it easy to demonstrate effective password management for regulatory compliance.

9. DOES THE SOLUTION MAXIMIZE THE EFFICIENT USE OF SYSTEM RESOURCES (SUCH AS PROCESSOR AND MEMORY) IN EXISTING MULTIUSER OS ENVIRONMENTS?
Certain SSO solutions integrate very effectively in Microsoft Terminal Services and Citrix Presentation Server™ environments. Common license servers, minimal impact on existing environments, an integrated administration console, a single-client deployment mechanism, and adherence to strict development standards are just a few of the benefits you should expect.

10. HOW HARD IS IT TO IMPLEMENT?
Your password management should be very simple to configure. Top solutions employ a simple wizard-based approach to configuring applications. This wizard automatically identifies various log-in components on the log-in and password change screens. The administrator merely defines the role of these components by right-clicking on them and designating their purpose. For example, the password text box will be designated with the password role. In addition, the administrator identifies elements of the logon dialog that uniquely identify the screen so that the password manager agent will recognize the screen when it is displayed.

Look for solutions that enable a large percentage of applications to be configured in a matter of minutes. Script-level programming should not be required to set up applications. In addition, no API-level programming should be required to configure applications. Thus, an entire environment can be configured in a matter of days versus the months it requires to single-sign-on-enable applications via a script-based approach. Instead of requiring scripting, application-level integration, or significant
changes to existing infrastructure, your password management solution should do all of these things out of the box.

**CHECK OFF THE LIST—WITH CITRIX PASSWORD MANAGER**

With over 2,100 customers, Citrix Password Manager™ is the most secure, efficient and easiest-to-deploy enterprise single sign-on solution for accessing password-protected applications.

Users authenticate once with a single password, and Password Manager automatically does the rest: logs onto password-protected information resources, enforces password policies, monitors password-related events and automates end-user tasks—even password changes. As a standalone solution of the Citrix® Access Platform or bundled into the Citrix Access Suite™, Password Manager delivers the best access experience for everyone: improved password security and regulatory compliance for the business, single-logon access for users and lower support costs for IT.

**SIMPLICITY FOR USERS**

Password Manager is simple for users to learn and use. To register credentials, users log onto an application as usual and request that their username and password be stored in Password Manager. From that point forward, they are single-sign-on-enabled for that application.

Password Manager also has the ability to preprovision users through its batch credential provisioning capability, so that at first use, users are single-sign-on-enabled for all of their applications. Integration with third-party user provisioning products allows seamless user adds/changes/deletes. These products include HP Select Identity, Courion AccountCourier and IBM Tivoli Identity Manager. Furthermore, provisioning is extensible through provisioning APIs.

**SELF-SERVICE PASSWORD RESET**

Eliminate help desk calls with Password Manager—the first ESSO product to include self-service password reset and account unlock. Other vendors charge up to $10 per user for this functionality.

**ENTERPRISE SSO—ONE LOGON FOR ALL APPLICATIONS**

Password Manager provides access to all applications—Web, Windows or host-based—with a single sign-on. This distinguishes it from other “SSO” solutions, which provide single sign-on to Web applications only.
AVAILABLE ONLINE AND OFF
Password Manager is fully functional in a disconnected state when the agent is installed locally. Therefore, when users are disconnected, they will still be able to authenticate to local applications using their local credential store. Password Manager does not require any dedicated server hardware, as it relies on existing hardware components (file shares or user directory) for its central credential store.

HOT DESKTOP AND SMOOTHROAMING INTEGRATION
With Hot Desktop, a feature of Password Manager, users can log on and off in seconds—not minutes. This eliminates generic logons and erases the problem of users leaving workstations open and exposing resources. The Citrix SmoothRoaming™ feature of Presentation Server allows users to move seamlessly from device to device. Other vendors charge up to $30 per user for this functionality.

THE MOST SECURE ARCHITECTURE
Password Manager is secure by design, which means that security is designed in, not bolted on. Password Manager allows password policy enforcement so that IT administrators can specify strong password characteristics such as length, character repetition and alphanumeric requirements on a per-application basis. Administrators can also automate password creation and force password changes in order to eliminate users’ undesirable behaviors. It’s even possible to enforce password changes for applications that do not have password change functionality.

Password Manager has strong encryption and buffer overflow prevention and makes appropriate use of operating system and registry permissions and anti-tampering techniques such as checksums to prevent unauthorized changes in data. Password Manager is the only SSO solution to undergo and pass a rigorous third-party security audit. Foundstone Labs, a division of McAfee, has certified that Password Manager conforms to security industry best practices.

MULTIFACTOR AUTHENTICATION DEVICES
Password Manager works with the Windows security subsystem and integrates out of the box with the broadest array of third-party multifactor authentication devices, including tokens, smart cards and biometric devices.
**COMPLIANCE**

Password Manager assists with regulatory compliance by enforcing strong password policies—even for systems without this capability—and providing automated password changes. It logs end-user events such as logon, password change and authentication, and saves them to the Windows Event Log.

With Password Manager, there is only one door to close to terminate access—the primary network logon—when users leave the organization. Password Manager controls all users’ passwords, ensuring that passwords are strong and that they remain hidden from users.

**INTEGRATION WITH CITRIX PRESENTATION SERVER**

If you have Citrix Presentation Server, you can easily provide a single logon to hosted applications with Password Manager. Password Manager and Presentation Server also share the same management console. Once you’ve SSO-enabled your Presentation Server applications, install Password Manager on the desktop, extending SSO to all other applications.

**EASY TO IMPLEMENT**

Password Manager is easy to deploy—no scripting, no application-level integration and no changes to the infrastructure are required. And if you have Presentation Server, installing Password Manager is a snap. It’s a simple task, not a separate IT project.