# managing SSO with shared credentials

## Introduction to Single Sign On (SSO)

All organizations, small and big alike, today have a bunch of applications that must be accessed by different employees throughout the day. Single Sign On (SSO), which many organizations deploy, is an access management capability that enables employees to access multiple disparate systems by just having to authenticate once.

The legacy approach to signing-on to multiple systems required users to maintain multiple user names and authentication information like passwords, tokens, etc. System administrators used to manage user accounts within each of the multiple systems to be accessed in a coordinated manner in order to ensure integrity of security policies. This is represented in the figure 1 below.

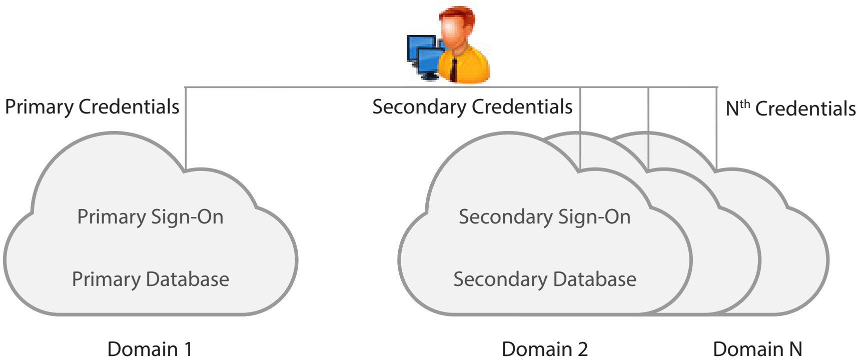


Figure 1: Legacy Approach to Sign-On to multiple systems

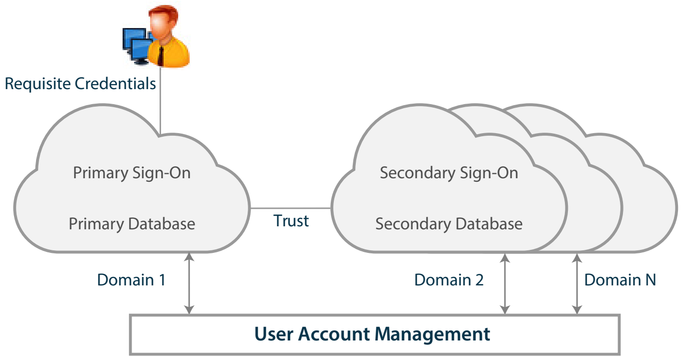


Figure 2: SSO approach to Sign-On to multiple systems

Whereas now with the SSO approach, when a user logs in for the first time, an SSO capability authenticates the user once, translates and stores the authentication parameters. Whenever the user accesses applications, the SSO shares the credential as per the authentication mechanism supported by the application. In this approach the primary system is required to collect all the identification and user credential information, from the user logging in, which is necessary to support the authentication of the user to each of the secondary domains that the user may potentially require to interact with. The information supplied by the user is then used by SSO Services within the primary domain to support the authentication of the end user to each of the secondary domains with which the user actually requests to interact. This flow is represented in the figure 2.

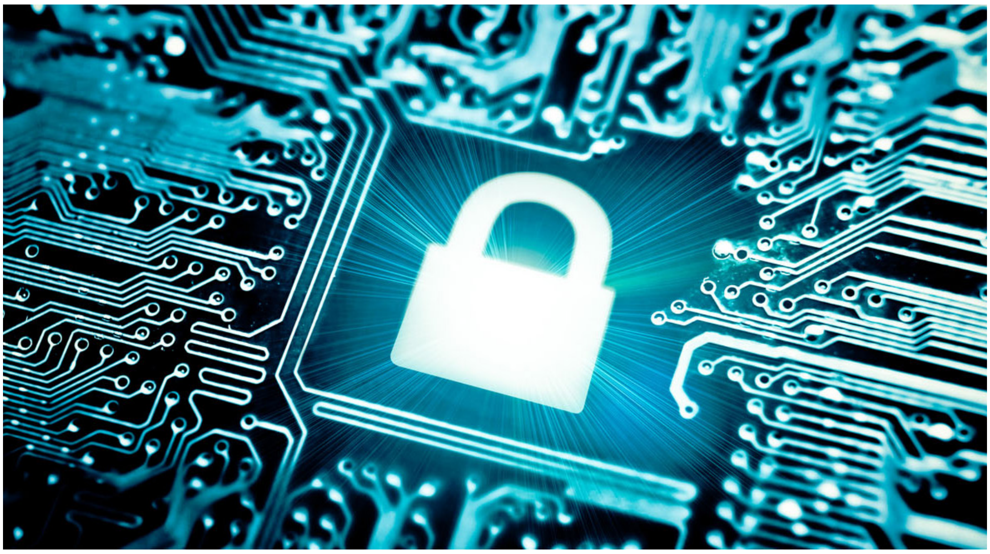
The information supplied by the end-user as part of the Primary Domain Sign-On procedure can be used in support of other domain sign-on in severalways:

- Straight-Away, the information provided by the user logging in is passed to a secondary domain as part of a secondary sign-on.
- Indirectly, the information provided by the user logging in is used to get other user identification and user credential information stored within the SSO management database. The information obtained is then used as the basis for a secondary domain sign-on operation.

The information obtained is then used as the basis for a secondary domain sign-on operation.

- Instantly, to establish a session with a secondary domain as part of the primary session setup. Thus the application clients are automatically invoked and communications established at the time of the primary sign-on operation.
- Interim - Credentials provided by the user is either stored or cached and used at the time a request for the secondary domain services is made by the user.

# benefits of implementing SSO



As most of us would guess, SSO brings in multiple benefits for an organization. The IT team does not need to maintain different authentication systems and as a consequence the number of calls to the support center (for password resets, forgotten and user name blocks) reduces significantly. Administrative activities of adding, deleting, updating user credentials are easier. The employees on the other hand do not need to spend time memorizing and typing a number of difficult and complicated passwords.

While there are many advantages of SSO implementation, additional security must be enabled for the SSO implementation so that the single server repository of authentication and access can be guarded against external threats.

**users**

- Single User Name Passwords for all applications - Easier to remember, Convenient to change periodically, no need to write down passwords on a paper or digitally
- Greater tendency to use strong passwords
- Reduced time taken to log into applications

**IT**

- Single authentication system to maintain
- Easer Administration activities of adding, deleting, updating user credentials
- Enables faster development and release cycle

**security**

- Limited number of credentials imply improved Security and controlled entry points
- Tends to reduce phishing as the user is used to seeing one screen for logging in.

**customer support**

- Less Number of calls to Reset Passwords, and login Queries, user name blocks

Figure 2: Advantages to various identities by using SSO

# various SSO implementations

There are many commercially available SSO offerings in the market today. Some of the key services are – Active Directory Federation Service, Facebook Connect, JBoss SSO, IBM Tivoli Access Manager. Some of the commonly used protocols are: Kerberos (including Lightweight Directory Access Protocol - LDAP), Security Assertion and Markup Language (SAML) and Pubcookie.Role based access controls (RBAC) which is used in few SSO implementations simplify routine account management operations and facilitate security audits. Using this methodology, system administrators do not assign permissions directly to individual user accounts. Instead, individuals acquire access through their roles within an organization, which eliminates the need to edit a potentially large number of resource permissions and user rights assignments when creating, modifying, or deleting user accounts.

Today, many tools and protocols are available that allow SSO's to work across multiple domains. For e.g. an Active Directory service can work on a unix domain by leveraging LDAP services.

SAML is considered to be a benchmark for SSO implementation in applications, especially the ones hosted in the cloud. It uses digital signatures to establish trust between the identity provider and the application.

# latest trends

Many organizations are also implementing a hybrid IT strategy, where some applications are locally hosted within a private datacenter and others hosted in the cloud. Organizations of all sizes are adopting Software-as-a-Service (SaaS) applications at an accelerated pace, and not just for customer relationship management but in every application category traditionally deployed as software including personal productivity, project planning and communication, supply chain and business intelligence.

Saas enables business initiatives faster than the traditional cycle of implementation, integration and on-going maintenance associated with on-premise applications. Additionally, IT and business lines alike hope to leverage SaaS in a cost constrained environment to shift from a capital to operational expense model.Not only has the infrastructure strategy changed in the last few years (on premise – to hybrid including cloud), but so has the access mechanism. Now more and the access mechanism. Now more and more users are accessing application on their mobile, tablets and now even phablets. Access through mobile version of the app is increasing.

To complement the new trends, many vendors are providing cloud based identity and access management features along with Single Sign On capabilities that make it easier for organizations to manage and secure applications both behind the firewall and in the cloud. Many new third party login ID providers are now playing an active part in the online community. Some of them are OpenID, Facebook, Janrain, Freelancer etc. Many websites do not even provide a choice for users to create a separate ID, but leverage only third party one click SSO's. While the information is very secure in these third party databases, but the fact that they are concentrated in one system is a cause of concern.

# role of PIM in SSO

Internal security threats are one of the biggest security concerns for any organization and these cause significant number of the information security incidents every year. To alleviate this concern, identity and access management (IAM), including Privilege Identity Management (PIM) are critical with an SSO setup. This becomes even more important when credentials are shared with more than one user (Common access to account ID's and passwords). IAM creates a layer between the user and the access repository. Many IAM and PIM solutions have ready to use integration with Active Directory services and other SSO capabilities.

In an SSO scenario, where a single credential leak can compromise the entire system, PIM solutions provide the perfect cover. The main aim of PIM in itself is to manage credentials that have privileged access, where single credentials may be shared across a group of people. By abstracting the underlying base credentials, and providing each user with their own access, every action logged and audited, PIM solutions provide enterprise grade security from an identity management perspective.

Another implication of a PIM deployment is that this abstraction simulates SSO across disparate systems that have no SSO integration solutions. An employee can use the same credentials for logging into the database as the company's internal web portal. With the added benefit of logging, auditing, access control, IAM, etc, PIM solutions have SSO well in hand.

An employee can be provided with a customized interface which is extremely personalized, show him the list of authorized applications and automatically take care of approved ways of logging in. User has simply to click on desired application and they are automatically logged in with allowed level of access.

PIM solution also has other powerful features to ensure smooth handling of critical situations. Should there be an urgent and critical regulatory change or slight hint of a compromised privileged credential, a PIM can almost immediately and seamlessly implement changes (Passwords or Policies) across entire enterprise fabric. Further to this a PIM can be customized to automatically block malicious scripts or command which could have been executed accidently or intentionally. In conclusion, PIM is an absolutely essential way to securely enable SSO in an organization.

# About ARCON

## about ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched in identifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.