



Identity Management with SSO
For Zero Day Provisioning, Increased Security and Compliance

INTRODUCTION

Corporate computing environments are becoming more complex. The presence of innumerable applications in a large computing environment coupled with the presence of knowledge workers, working from within the organization and remotely, the issues related to timely resource access/revocation are plenty.

There is also the issue of productivity wherein a new user joining an organization has to wait for numerous approvals and IT related issues to enable them to access the resources. This delay causes a lot of money in terms of lost productivity. Inability to scale Identity Management operations involving legacy or custom application servers can be a real pain. Industries seek out the best fit to meet their requirements at a given point in time. But as their workforce expands, organizations begin to feel the need to scale up their Identity Management infrastructure.

There have been lots of cases of application identities not being removed from the IT systems even after 2 years of employees' leaving the organization. This leaves an enterprise littered with orphan accounts which can potentially be used to compromise sensitive information.

Apere offers a solution to these problems with industry-standard and cutting-edge Identity Management solutions. Apere's low-cost, highly effective and easy-to-use Identity Management Access Gateway (IMAG), with its direct connectivity to a wide variety of applications through innovative mechanisms enables enterprises to achieve significantly greater ROI in a much shorter span of time.

MAKE EMPLOYEES PRODUCTIVE RIGHT FROM THE START

An integrated provisioning and SSO system gives employees instant, seamless access to applications without worrying about multiple passwords.

With this streamlined approach, the end user simply logs on once to his network domain and upon launching an application, all of his SSO-enabled applications – whether client/server, Web, Terminal Emulator (TE) or legacy - are automatically signed on and immediately available. There is no time lag between provisioning and SSO, and productivity issues associated with forgotten passwords are minimized.

Apere's IMAG500 with IMAG500 RCA has a unique approach towards identity management offering the best-in-class solution when compared to the existing identity management solutions offered by major software vendors.

Highlights

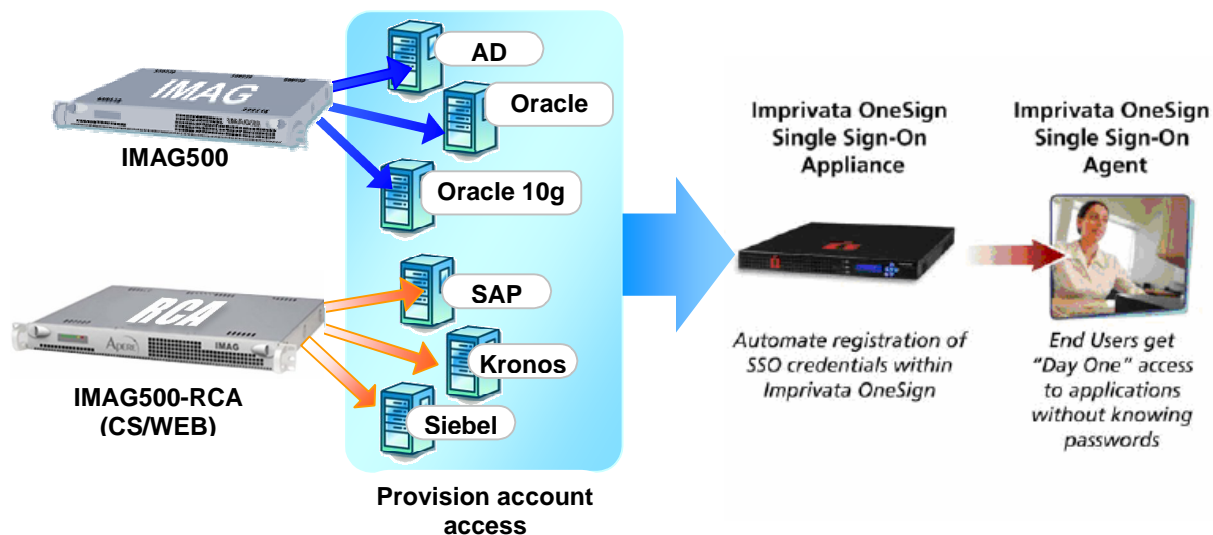
- Industry's first appliance based Identity management solution.
- Appliance turnkey deployment, no need of software experts
- AutoLearn quick deployment technology
- No API's or client agents, non-disruptive deployment
- RapidConnector platform to build connectors on the fly
- All in one platform – Password reset, Provision, Reports
-

Benefits of an Integrated Identity Management and SSO Solution

- Provide first-day access to all relevant applications to the new employees without them having to worry about different userIDs and passwords – day-one single sign-on.
- Reduce internal and external security breaches by preventing and removing access to all the corporate resources as employees leave, in other words zero-day decommissioning of users.
- Hugely reduce the IT administrative costs by providing employee self service facility in terms of having the password management feature for variety of applications.
- Automate the work flow based procedures for granting / denying access to the applications.
- Simplify compliance with government regulations.
-

Now there is an integrated provisioning and SSO solution that automatically provides immediate and secure access to applications and networks, from the moment an employee begins working, enabling full productivity from day one. The linking of initial account provisioning with the generation and ongoing management of user credentials in a seamless manner delivers a complete user access solution that immediately boosts user productivity and ensures greater overall security. Also of equal importance, this linking provides the ability to efficiently revoke access the moment the employee resigns or is terminated. In most industries, the provisioning and de-provisioning of application access is no longer just a capability that provides a competitive advantage, it has become an important mandate.

The Apere IMAG - Imprivata OneSign® Connector: Here is how it works.



With Apere IMAG’s Imprivata OneSign Connector, users’ application credentials are automatically provisioned within the OneSign appliance. Once the user has logged on, the OneSign Agent automatically downloads access policies and application credentials from the OneSign Appliance providing “Day One” single sign-on:

- Users never have to be given starting application passwords to individual applications, increasing application security.
- Users don’t have to search through emails looking for passwords, increasing productivity and eliminating password-related help desk calls.
- Single sign-on credentials are guaranteed to always be in sync with application credentials.

TIGHTEN ENTERPRISE SECURITY

The combined solution provides the ability to change password constraints (minimum/maximum length, reset intervals, auto resets), manage authentication challenges, and accommodate application-generated password reset requests automatically. Another powerful feature of an integrated system is the ability to assign authentication and desktop policies to specific computers, essentially overriding user-level settings. This gives IT greater flexibility over assigning policies, allowing organizations to make exceptions to the rule when necessary. The combination of two factor authentication and SSO ensures greater network security and user convenience without increasing help desk calls due to forgotten cards, badges or tokens.

SIMPLIFY COMPLIANCE WITH GOVERNMENT REGULATIONS

The inability to achieve compliance can bring enterprise operations to a halt. Global enterprises which handle project sensitive and confidential information are mandated to stay compliant ensuring that they have best practices in place to secure information access. ISO/IEC 27001 and other standards including ISO/IEC 17799:2005, ISO/IEC 13335-1:2004, ISO/IEC TR 13335-3:1998, ISO/IEC TR 13335-4:2000, ISO/IEC TR 18044:2004 and the “OECD Guidelines for Security of Information Systems and Networks” require organizations to establish a process and implement controls that monitor and secure financial, personnel, and patient health care data.

The unified Identity Management and SSO solution from Apere’s IMAG and Imprivata’s OneSign helps customers to significantly reduce operating costs and enable them to meet regulatory requirements including BS-7799. This integrated solution addresses complicated policies in an efficient and affordable way, by eliminating insecure password delivery practices, and enabling implementation of stronger password composition policy (stronger passwords and more frequent expiration/refresh) without burdening the end user.

Apere’s IMAG and Imprivata’s OneSign Unified Solution-Highlights

- The solution simplifies the management of shared user accounts across multiple applications and networks
- The solution improves security for regulatory compliance, and maximized administrative and user productivity
- The solution ensures complete accuracy, and reduces the process for creating or changing user accounts from days to minutes, significantly reducing administrative burden
- The solution delivers a simple, consolidated view into identity access information to validate security posture and compliance with required regulations