Enterprise-Class SaaS Provisioning

A New Approach to Federation for On-Demand Environments

A Conformity White Paper

EXECUTIVE SUMMARY

User provisioning provides the foundation for effective lifecycle management of user identity and access rights in complex IT environments. Historically, enterprises have addressed this critical need through a combination of business process and integration of premise-based applications with management tools. These tools have included local directory services, identity services and user provisioning and role management solutions. The recent rapid adoption of SaaS and cloud-based applications is now significantly straining the on-premise capabilities of existing IT models and approaches.

SaaS and cloud-based solutions are migrating mission critical applications outside the firewall, requiring organizations to take a new approach to provisioning and identity management. These organizations typically consider conventional offerings including installed application platforms and hosted identity solutions, but actually require a differing strategy that better unites the hosted and on-premise best practices. IT departments and the global SaaS industry require a new generation of solutions and services that fully address cloud-based user provisioning and permissions while leveraging enterprise controls.

This white paper focuses on the unique characteristics of the SaaS business model, the convergence of enterprise business process and on-demand environments, and the resulting requirements IT teams must internalize.

SAAS PROVISIONING – WHAT IS DIFFERENT?

SaaS and cloud computing introduce distinct provisioning challenges, especially in enterprise accounts. The migration of mission critical applications like CRM, ERP, and Human Resources to SaaS and cloud-based models has stretched enterprise control of policy, user identity, compliance, and security across the firewall boundary. Enterprises cannot rely on traditional solutions or targeted hosted services to adequately address this disconnect. In the absence of capable alternatives, organizations are discovering that SaaS provisioning is much more difficult than expected, leading to inefficiencies and possible compliance and security issues.

What specific aspects of SaaS and Cloud computing make provisioning and management difficult? The challenges fall into three primary areas: disconnects between SaaS and premise-based solutions, unexpected complexity of mission critical SaaS setup, and a lack of applicable and endorsed standards.

Disconnects between SaaS and Premise-based Solutions

The most obvious change is the introduction of disconnected business domains, with SaaS and on-premise environments and solutions needing to operate in tandem. Specific challenges include:

- **Siloed User Models:** SaaS and cloud applications enable management of user identities and permissions within their own hosted model, typically without mapping to the enterprise directory or identity solutions. As each SaaS application has been tailored for a target business purpose, the user accounts and discrete permissions have simultaneously evolved into proprietary models. Provisioning is directly impacted, as the granular user permissions and profiles managed onsite cannot be translated to SaaS attributes without manual intervention. This limitation, coupled with the fact SaaS applications are often adopted virally within the business units, leads to expanding “silos” of user identity and administration distributed across internal and external applications. These SaaS user silos are not only inefficient; they compromise compliance and security policies and may lead to stagnation of planned SaaS adoption.

- **Fragmented Policy Enforcement:** The expansion of the SaaS market into the mission critical application space has created a new requirement to ensure alignment with business policies. Applications like ERP, CRM, and Human Resources are typically managed by directory, identity, and systems management solutions. Enterprises struggle to align SaaS processes with these internal policies and systems, often resorting to manual reconciliation or administrator oversight. Over time, organizations with multiple cloud-based applications may find they are supporting unique business processes for each application.

» **Lack of Control:** The SaaS multi-tenant model delivers an efficient, highly scalable solution for ISVs, but also can neutralize traditional provisioning approaches. The delivery model creates an additional burden on enterprise technology teams by introducing just-in-time versioning and a "closed" software hosting model. To properly support the versioning, provisioning solutions must accommodate real-time updates to the SaaS service that are deployed on the *vendor's* schedule. While business users immediately utilize new releases, provisioning sources may need to be synchronized to ensure any required changes in ISV permission structure are recognized. In addition, multi-tenant SaaS models create a locked down environment typically closed to customer- or partner-requested software customization that can enable systems management or provisioning access. Provisioning must be achieved through vendor defined APIs or access models.

Complexity of Enablement

Complex SaaS enablement is an additional challenge to a centralized provisioning model. As SaaS adoption increases in scope and level of assumed business process, organizations are faced with more involved deployments and integrations requiring provisioning and management solutions to address the growing systems requirements. Some examples of cloud-based complexities include:

» **Multiple-Stage Setup:** More robust SaaS applications may require multi-step user establishment through provisioning. Users cannot be instantiated by merely creating an account with login credentials, but must be created and subsequently applied to business level objects. Login alone is insufficient to ensure the target user is *functional*, an expected outcome of any provisioning process.

» **Application Coordination:** Organizations that are endorsing SaaS for mission critical solutions will often need to coordinate and sequence applications and permissions. Examples might include sales processes with lead generation, sales automation, and compensation management tools. Successful application alignment may require coordinated provisioning of granular permissions across multiple SaaS applications and sequencing of user instantiation.

» **Multi-Level Licensing:** As SaaS solutions grow in complexity and scope, ISVs are invariably introducing additional licensing schemes to recognize the added value. Organizations attempting to embrace these models cannot assume a single user image is sufficient without incurring unnecessary licensing costs and possible compliance and security issues. Common examples include added licenses for mobile access, application visibility or data extensions.

Lack of Standards and Best Practices

Finally, the lack of adoption and creation of the needed industry standards and best practices has further hampered the ability for the market and enterprise IT teams to address the provisioning challenges (Appendix A provides additional information on selected standards). Industry standards face the following hurdles to address the enterprise provisioning needs:

- **SaaS ISV Endorsement:** In many cases, industry leading SaaS ISVs have elected to not move forward and invest until a clear, dominant set of standards emerge. Where utilized, the standards are not yet addressing the required depth of provisioning and management.
- **Accelerated SaaS Evolution:** The rapid evolution of complex SaaS provisioning and user profiles has outpaced standards efforts, especially when considered as part of a complex business processes. Many of the standards have not been materially updated in three to four years while the aggressive pace of SaaS development has created multiple, distinct user and business models.
- **Disconnected Services:** Industry standards must contend with both remote cloud deployments and the associated enterprise solutions. To date, most standards have gained acceptance in only one of the delivery models and are unable to coordinate the extended business processes.

EMERGING MARKET SOLUTIONS

The challenges presented by cloud-based applications are similar in many ways to those presented by the rapid adoption of distributed computing in the 1980s and 1990s. Manual processes were unable to meet the challenges, while existing mainframe tools were not able to adapt. Like many early stage technologies, the core solutions outpaced the tools and processes needed to fully recognize the opportunity. To realize the distributed computing benefits, a specialized vendor community emerged that focused on systems management for unique computing systems and vendor suites like Microsoft or IBM.

Similar to the distributed computing wave, SaaS applications have evolved much more rapidly than the supporting infrastructure creating a solutions vacuum. As organizations embracing SaaS outgrow the manual spreadsheets and local business user expertise, they encounter a mixed set of SaaS management alternatives. Recent marketing may lead customers to believe SaaS is merely a delivery mechanism and a simple “blade” approach with legacy systems or identity management is the most direct approach. Alternatively, some cloud-based identity services are claiming to cover the breadth of SaaS provisioning and management by repurposing industry standards and complementary technologies. With proven track records, why have these solutions not successfully addressed the management and provisioning requirements for SaaS?

Legacy Enterprise Software Vendors

Where deployed, enterprise systems management, role management and identity management suites may be evaluated as SaaS options by customers, but these solutions are not architected to embrace the cloud-based environments today. Specific challenges are presented by:

- **Technical Architecture:** These vendors have relied on some form of standards or instrumentation of the candidate applications to interweave management for disparate systems. Neither option is currently possible with SaaS due to lack of standards adoption (more on that point later in this paper) and inability to install co-resident code on SaaS instances.
- **IT Focus:** Many technical IT solutions focus on supporting basic IT functionality and processes, electing to not engage at the application business logic level. SaaS disrupts this approach by blending the IT processes with the integrated business logic. Provisioning SaaS applications correctly requires a correlation of localized business knowledge and technical instrumentation.
- **Solution Flexibility -** Many solutions from on-premise identity and systems management vendors require significant investment in time and resources to extend their solutions to support new SaaS applications and corresponding user role models. In many cases the customization costs become nearly prohibitive, especially for midsize enterprises.

Despite the challenges outlined above, enterprise software vendors do have a critical role in SaaS management and provisioning. If the discussion set is expanded to include directory vendors like Microsoft, these solutions are typically the source of much of the organizational policy and permissions. A robust SaaS provisioning solution must integrate with these sources, versus trying to replicate them or enable their migration out of the enterprise.

Cloud-Based Identity Solutions

Recently, the consideration set for SaaS and cloud-based provisioning solutions has expanded with aggressive market positioning from cloud-based identity services. These vendors, historically focusing on single sign-on and credential security, play an important, complementary role in SaaS integration and IT processes. While providing cloud-based identity services, most of these applications do not address the required depth of provisioning and management. Specific challenges include:

- **Transactional Basis:** The identity solutions are based on a transactional model – user accessing credential information through login – to take action. This is often called the “just-in-time” model and is tailored for the on-demand single instance use case, well aligned for securing credentials, but extremely limited for provisioning. As discussed previously, business-level provisioning requires alignment with business process, not user actions.

- **Depth of Attributes:** Identity solutions are optimized to securely verify credentials and authorize access. Despite recent efforts to expand identity standards with attribute information, the depth of permissions is basic and adoption of the expanded standards models is minimal (see standards section).
- **Business Domain Knowledge:** Finally, this solution set is derived from the security world and addresses a technical problem. As such, the model can struggle with the business aspects and knowledge required to ensure successful SaaS adoption and management of *functional* users and permissions. Provisioning distinct applications like ERP, CRM, collaboration, and HR properly requires far more than account setup. SaaS provisioning solutions for business-level applications must provide utility in aligning organizational business process and profiles with SaaS permissions and attributes.

The identity vendors are complementary to full-featured provisioning solutions and, in basic cases, can provide limited account provisioning capabilities. For mission critical applications and solutions enabling business data and users, SaaS provisioning and management dictates a much broader solution set.

SaaS Vendors

The SaaS ISVs themselves offer another suggested solution for the industry-wide provisioning and management requirements. It can be argued the SaaS vendors are best positioned to address the challenges by removing their own enterprise barriers to adoption. However, the ISVs are limited in their ability to affect the larger market need and must contend with conflicting market pressures. ISVs will remove *application-specific* barriers to adoption as they transition their products into larger enterprises, but will likely stop short of creating their own industry-wide solutions due to:

- **Business Priorities:** Cloud solutions providers are in the midst of a rapidly expanding market, and must continue to address emerging market requirements and new markets. As such, ISVs prioritize requirements that continue to expand use of their product and associated revenue; they are typically not resourced to address the management needs of the expanded SaaS and cloud markets.
- **Focused Domain Expertise:** SaaS ISVs have built best-of breed products by focusing on the application area and rapidly meeting market challenges. Each ISV is a domain expert in their focus area, but typically stops short of attempting to understand distinct provisioning and management requirements for other SaaS vendors and spaces.
- **Application Focus:** Finally, ISVs have been built with a strong application focus and expertise set. In fact, many of the SaaS ISVs are funded by or linked to traditional enterprise software providers. Management and provisioning solutions require a different set of domain expertise, typically drawn from the systems management and identity management spaces.

Despite the arguments against creating their own provisioning and management solutions, SaaS ISVs are required to be an integral part of the industry capabilities that must be developed. Instead of each vendor building out unique management capabilities, ISVs can best engage by advancing their own application integration capabilities now to help remove adoption roadblocks. Once the problem is well understood, the same vendors can assume a leadership position in creating the right standards.

DEFINING THE RIGHT SAAS PROVISIONING SOLUTION

A number of market sources now claim that the ROI benefits of SaaS and cloud technology diminish as the deployments mature. Though part of this can be attributed to unrealistic expectations from SaaS conversions at the outset, it is likely that enterprises are also not recognizing the integration and management requirements *prior* to initiating adoption. Continued dispersion of rights and permissions and use of basic tools such as spreadsheets breaks down just as the SaaS applications themselves take hold. The marketplace is now starting to focus on solutions that are enablers for SaaS success, by providing the business-line focus and flexibility needed for a strong return on investment.

Enterprises adopting SaaS and cloud-based applications must recognize the full set of requirements that will ensure successful SaaS deployments and ongoing usage. The corresponding solutions need to be tailored for the cloud-based models including the multi-tenant architectures and business-driven permissions sets. Attempting to force existing solutions designed for on-premise applications or cloud-based identity will not provide the compliance, security, and IT efficiency benefits required to ensure ongoing adoption.

As IT organizations work with lines of business to define the best approach, the following areas should be carefully considered when evaluating the right enterprise solution for user provisioning:

- **Coordination of Business and IT:** Provisioning and management solutions must coordinate the functional domain knowledge in the line of business, the compliance bias of finance and security groups, and the application and technology skills of the IT departments. Role-based visibility and control are critical to address the different drivers in the enterprise while leveraging application owners in the lines of business.
- **Leverage Business and IT Processes:** A robust solution will integrate with key points in the enterprise to ensure SaaS adoption is aligned with organizational policy and workflow. Integration points may include HR or directory solutions, systems management or ID management deployments, reporting solutions and data stores, and help desk processes.

» **User Life Cycle Management:** Potential options must address the differing needs and security for a heterogeneous user base including employees, administrators, consultants, and customers. For each of these constituents, provisioning options must manage the lifecycle in the context of the business process and needs. Any provisioning process should extend beyond simple account setup and credentials, possibly addressing the following example use cases:

- **User Onboarding:** Onboarding often requires a multi-step process and management of multiple applications or systems, including critical SaaS applications. Users may need to be activated *asynchronously* to their login or first application access. As an example, new sales users may be instantiated in sales automation and compensation solutions prior to their first login, enabling account assignment and creation of a compensation plans. Additionally, IT may create user access and permissions for help desks as part of their employee onboarding program prior to the employee's first day.
- **User Status Change:** As users change assignments or are promoted, human resources changes may require re-provisioning or deactivation in SaaS applications based on the business process. These users can require a number of SaaS identity changes commensurate with the organizational updates that are created without manual user or administrator activity. Examples of coordinated changes include:
  - Modification of granular scope and rights for ERP packages or CRM solutions
  - Detailed updates in sales automation packages that represent new territories, compensation plans or reporting managers
  - Access to new SaaS applications or modules including expense reporting solutions or mobile access for expected travel needs
- **User De-Provision:** Employee de-provisioning often extends beyond simple login revocation. Users separating from a company may be subject to multiple policies, based on organizational best practices, user type (employee, contractor, partner), and terms of separation. Some possible use cases include:
  - While still employed, exiting users may be provisioned into a new profile that limits access and expands auditing visibility. These users still need SaaS access to complete obligations, but

should be limited in scope to match compliance and security policies.

- Users may not be fully deactivated from candidate applications when they exit the organization. Users may require transitional access to SaaS applications, allowing them to complete expense reports, monitor incentive-based compensation, or help transition accounts and responsibilities. Special policies and permissions can be established to allow access while minimizing organizational risk.
- Finally, once the need for access is complete, de-activation of user accounts must be promptly executed based on IT policy and systems changes. Delays based on administrator responsiveness or messaging is not acceptable.

- **Complete Provisioning:** A complete solution will normalize data to common profiles, leveraging the organizational attributes and grouping structure, and ensuring users are provisioned as *fully functional* (not just an account setup). SaaS permissions and attributes will be granular and will include core ISV permissions, ISV licensable attributes, and customized fields where applicable. SaaS customers must verify the depth of attributes provisioned and the model for handling complex setup in any candidate solution.
- **Deliver Complete Visibility:** Any provisioning or management option must audit all events, providing role-based event visibility and reporting. The data must support security, compliance, and SaaS optimization requirements from multiple groups. This capability is required in regulated organizations including those that are publicly traded, part of the health care industry, or managing credit card transactions.
- **Embrace Aligned Standards:** Candidate technologies or solutions must embrace standards where applicable and be willing to forward standards in the industry. With that said, the immaturity of standards in the industry will require vendor flexibility until the right models are defined and proven in SaaS deployments.

SaaS and cloud computing introduce significant changes to the IT and business processes, and require a recalibration of the associated best practices. With this emerging market, no single solution can fully address the target requirements listed above across all potential vendors. IT departments, working with the SaaS marketplace, should strive for the same robust industry solutions that are available for traditional applications. The marketplace is just now starting to focus on IT solutions that are truly enablers for SaaS success, while still providing the business-line focus and flexibility needed for a strong return on investment. By managing the identity lifecycle of the broad base of SaaS or cloud users, the provisioning solutions can provide a solid foundation for auditing, regulatory and organization compliance, and license utilization.

ABOUT CONFORMITY

Conformity provides on-demand solutions that enable organizations to govern manage and control the software-as-a-service (SaaS) and cloud based applications proliferating across their environments. The Conformity platform enables organizations to centrally manage their SaaS applications, users and data, reducing security and compliance risk and providing visibility into operational costs associated with SaaS usage in their environments. Based in Austin, Texas, the Conformity team includes former executives and founders of pioneering companies in the systems and identity management software market. For more information about Conformity, please visit www.conformity-inc.com or email info@conformity-inc.com.

APPENDIX A

A number of standards have been proposed to help address select SaaS management issues. Selected examples of existing standards included in the SaaS and cloud provisioning discussions include:

» **Identity: SAML and WS-Fed:** (Security Assertion Markup Language and WS-Federation, respectively). Both models focus on authentication of cross-domain security credentials or identity, though it is possible to include additional user attributes. Of the two, SAML has achieved adoption in the SaaS space with select ISVs and cloud identity vendors supporting it for Single Sign-On (SSO). SAML version 2.0 was introduced in March 2005 and represented a major change from the previously deployed 1.0 and 1.1 versions. From a business *provisioning and management* perspective, SAML has limitations in its current instantiation including:

- As a SSO model, SAML 2.0 deployments are typically Just in time (JIT) in nature, with actions driven by user access events. This model aligns provisioning events with the restricted transactional use case, limiting the ability to address business-driven events or bulk changes to policy.
- SaaS and cloud ISVs are not universally standardized on SAML for SSO, though coverage is improving. Existing implementations may be split across SAML 1.x and 2.0 versions which are not fully compatible.
- SAML was derived from the web browser security space, and has minimal adoption with legacy enterprise applications leading to possible gateway requirements in identity coordination.

» **XACML:** (eXtensible Access Control Markup Language.) XACML is an access control policy language that focuses on managing and interpreting organizational policy in a consistent manner. XACML v2.0 was approved in February of 2005 and v3.0 has been under development for some time. Some industry proposals suggest XACML can be combined with SPML (below) to enable a policy-driven provisioning solution. Similar to SAML, the current form of XACML has limitations with regards to SaaS provisioning and management including:

- XACML is built for managing organizational policy and does not necessarily lend itself to granular, vendor-unique provisioning and transport (thus the aggregation with SPML).
- SaaS and Cloud ISVs do not yet appear to be supporting XACML alone or in tandem with other standards.
- XACML has targeted adoption in the enterprise around the role-based access control (RBAC) efforts, but does not appear to be widely embraced or promoted to extend RBAC outside the firewall.

» **SPML:** (Service Provisioning Markup Language). SPML was developed to address distributed provisioning requirements and is considered to be complementary to SAML, addressing the broader business provisioning needs. SPML v2.0 was introduced in April of 2006 and also has yet to be materially adopted in the SaaS market. With that said, SPML is the most likely standard to address provisioning needs and future modifications may increase its utility in the SaaS environments. Potential *current* SPML challenges in the SaaS and cloud space include:

- SPML defines the transport mechanisms but is not necessarily intended to normalize of unique data structures or business language across applications.
- SaaS and cloud-based vendors have typically not embraced SPML, though a number of enterprise applications do include basic SPML integration points.

» **Microsoft Geneva / Info Card:** Possibly a stretch as an "established" technology, Microsoft's emerging identity management strategy deserves mention. While maintaining compatibility with industry standards like SAML and WS-Fed, the Microsoft initiatives appear to be poised for broader support for federation and user identity. The enterprise use cases merging on premise and cloud-based applications may align well with Geneva as it gains adoption.

Provisioning SaaS Applications for the Enterprise
May 2009
Author: Brian Kerns
Version: 1.0

Conformity
6300 Bridge Point Parkway, Building 1
Austin, TX 78730
U.S.A.

For More Information:
Phone: +1.512.795.5826
Fax: +1 512.795.5849
www.conformity-inc.com