abridean

15 Rules for a Successful User Management and Provisioning Project

Table of Contents

Introduction

Organizations are increasingly challenged with the need to improve the security of their IT systems, to reduce the costs associated with managing their IT infrastructure, and to create appropriate safeguards to ensure that policies are properly enforced. With these goals in mind, organizations are adopting ***identity management*** initiatives to better standardize the processes and technical infrastructure for managing the people that access IT systems, the methods of authenticating those users, and the approaches for providing access to those systems. These initiatives include implementation of a wide variety of technologies, such as password management, encryption, intrusion prevention, user account management, access management, and provisioning. This can even expand beyond technical assets and involve the provisioning of everything a user needs to get his or her job done, from phone extensions to ID badges to parking spaces.

Identity management encompasses a wide variety of business process opportunities, as well as technical decisions, such that organizations rarely attempt to tackle the whole problem at once. Projects are prioritized based on the goal of achieving a balance of short-term and long-term benefits, with preference being given to projects that relieve short-term pain and position an organization for longer-term rewards. One area that is emerging as just such an opportunity is in the creation of a more secure and efficient ***user management and provisioning*** process.

Broadly speaking, user management and provisioning encompasses the processes and technologies that allow an organization to more securely and efficiently:

- Add, create, and delete users from its systems;
- Provision all the applications and resources a user needs to get his or her job done; and
- Enable users to manage their own profiles using self-service techniques.

When you consider all of the applications, networks, and devices that a user might need, each typically having its own implementation and user profile requirements, and each with its own set of administrative interfaces, it is no wonder most organizations find this problem to be both costly, and a major source of security risk.

To succeed with a user management and provisioning initiative, it is critical that you consider:

- Your organizational objectives;
- Your technical requirements and the capabilities available to you;
- Emerging approaches for gaining the most from your initiative;
- Your approach to managing directories; and
- The best practices of those companies that are running successful projects.

This paper contains 15 "Rules for Successful User Management Initiatives" that can help you get started!

Rule 1: Know why you are embarking on a user management and provisioning initiative

The reasons why each organization sets out to improve its user management and provisioning processes can differ widely. Ultimately, an automated user management process will curtail the skyrocketing cost of managing dynamic user environments*, improve security, provide necessary audit and compliance controls and reporting.

Prior to starting an initiative, it is critical that you can answer these questions for your organization:

- Enhancing Security
  - Are security policies being appropriately applied?
  - What does a user have access to?
  - Are we immediately de-provisioning users that leave?
  - Do we have a problem with dormant accounts?
  - Have we granted the minimum authority required for administrators?
- Meeting Compliance and Audit Requirements
  - Do we know what each user has access to, when it was granted, and who approved it?
  - Can we provide all necessary regulatory reporting?
  - Can we produce a complete audit trail of provisioning activities?
- Improving Efficiency and Reducing Cost
  - Does our user management process have a cost structure that will not grow out of control over time?
  - Have we delegated tasks to the lowest-cost personnel?
  - Are we providing access for users quickly enough?
  - Are we enhancing end-user productivity?
  - Are our end users happy with their service levels?
  - Have we automated as many processes as possible?
  - Are we enforcing efficient use of system resources?

User management and provisioning solutions can help you provide the right answers to each of these questions, but the priority that you place on each question will dictate how you manage your project and how you prioritize technical decisions.

* For information on why user management costs are skyrocketing, see Rule 4!

Rule 2: Clearly define how you will measure ROI

Numerous industry metrics exist for determining the return on investment (ROI) of a successful implementation of a user management and provisioning system.

According to The Gartner Group, "A broad range of factors — including the demands of enterprise resource planning implementation, regulatory compliance issues and the pressure to contain costs — are intensifying the focus on how enterprises manage the processes associated with granting users access to business information.

Identity and access management (IAM) solutions, which can offer three-year return on investment (ROI) in the triple-digit-percent range, are becoming essential tools for effective management of user account and access rights information across heterogeneous IT environments, for Web and non-Web applications."[i]. Typically, this return is generated through process improvements, savings on licensing costs, and the mitigation of security vulnerabilities.

Here are some ways to measure ROI and build a business case:

- Determine the costs associated with current user management and provisioning activities and estimate the savings based on a new automated approach. Note that this could produce hard cost savings or free up resources to focus on more important issues (opportunity cost savings). Hint: outsourced help desks can be a major area for cost savings if you can reduce the number of support calls.
- Review the costs associated with compliance reporting and audits. Automated tools reduce reporting efforts and make audits happen faster.
- Calculate the probability of security breaches and estimate the potential risk and financial damage. It is important to note that the cost of damage caused by the breach itself is often secondary to the expense of validating the integrity of other data, the expense of securing the environment and the loss of reputation. Nelson Cicchitto, chief executive of a security software vendor, commenting on a CSI/FBI info-security study, confirmed that losses go "well beyond just the immediately obvious tangible costs." He says, "Their analysis indicated that, if thieves illegally wired $1 million from an online bank, the cost impact to the bank would be $106m."[ii]
- Calculate the employee productivity savings that would occur if they could get their applications configured faster.

Rule 3: Take a phased approach to user management and provisioning projects

While many solutions available in the market offer very broad coverage of applications, devices, and non-technical assets that can be provisioned (e.g., parking spaces), it is becoming evident that projects that attempt to provision everything a user needs on Day 1 simply do not deliver results fast enough. Why? Because there are too many organizational and technical hurdles to overcome and like any large project, task dependencies end up creating risk and delaying the deployment of features that could start offering immediate benefit.

Furthermore, software solutions that encompass the most breadth often have a tendency to sacrifice depth of functionality, resulting in projects that promise to deliver everything, but require an enormous amount of custom coding and services to get the job done.

Here are three ways that user management and provisioning projects can be phased:

- **Phased target support.** In this case, evaluate the most critical and high impact applications and resources that need to be provisioned and start there. If you try to deploy a system that provisions too many items at once, the initial deployment will be too complicated.
- **Phased role deployment.** The process of defining organizational roles that drive the provisioning process can be cumbersome and significantly slow down system deployment. Organizations can mitigate this risk by choosing a strategy that involves role-less provisioning and gradually add role-based provisioning over time. Read more about this approach in Rule 6.
- **Phased business functionality.** User management and provisioning is comprised of numerous interconnected business processes that can be deployed one step at a time. Organizations should look for ways to identify the processes that represent the biggest points of pain such as user, password, and group management, and seek to deploy a system that solves those pain points incrementally.

An enterprise's user management and provisioning needs will change over time and, in all likelihood, a need will arise for custom applications or industry vertical applications for which vendors will not have an out-of-the box solution. Therefore, acquiring a system with an easy-to-extend provisioning environment, which is based on standards such as XML and SPML (Service Provisioning Markup Language developed by OASIS), is more important in the long run than what applications or resources are automated first.

Rule 4: Choose a flexible approach to administration through a combination of automation, delegation and self-service

Every organization has a different business process for managing user administration and a user management and provisioning system must be flexible enough to adapt to these needs. Utilizing a combination of automation, delegation and self-service not only provides the best service to end-users but is key to achieving the operational efficiencies, scalability, security and ROI goals associated with enterprise provisioning. Therefore it is important that buyers choose a system that supports flexible administration.

Automated Administration

A recent report from The Burton Group stated, "Today, manually administered environments require a Full Time Equivalent (FTE) for approximately every 500 to 1,000 users, while automated environments can manage 5,000 or more users per administrative FTE."[iii]

A simple comparison of costs based on number of users is as follows:

With a properly defined set of user management policies organizations can easily automate the user setup and management process without requiring administrator intervention. This approach reduces errors, improves security, and lowers costs.

Increasingly, many companies are looking to leverage their enterprise human resources (HR) systems to drive user management provisioning events, particularly for new hires.

Delegated Administration

The benefits of delegated administration are clear. By empowering local administrators, help-desk and non-IT resources to manage elements of administration, senior level administrators (a more expensive resource) are able to focus on tasks that better leverage his or her expertise. Delegated administration improves efficiency and cuts down on administrative costs.

Day to day administration tasks such as adding and deleting user information is often mundane, and repetitive. With a secure user management and provisioning solution in place to shield non-IT administrator's delegation can be secure and easy. Without the right solution in place the risk is two-fold. User management and provisioning solutions provide organizations with a simple to use interface that shields administrators from the complexity of the native tools only allowing them to perform delegated tasks; ultimately enforcing organizational policies around administer access.

Ultimately, the movement of basic IT support down the administrative value chain provides significant returns on investment and makes the process considerably more scalable as the number of users increases.

Self-service Administration

The third form of administration is self-service. There are some tasks that are best handled by the actual end-user. This approach is very effective especially for handling simple, repetitive tasks that can overburden the help-desk and technical staff:

- Password reset
- Requesting access to distribution lists, new applications and resources
- Updating profile information across multiple corporate directories

Self-service administration is a great service for end-users as well as a great tool to improve efficiency and cut costs.

Rule 5: Centralize policy management

Policy management is one of the most crucial components of a user management and provisioning system and one of the most daunting administration tasks faced by organizations deploying these systems.

Policies can be defined differently by different organizations (and vendors). For the purposes of this paper, policies include all of the logic associated with translating business needs (create a new user, remove a user, etc.) into specific actions within the IT environment (configure an application, add a user to a directory, etc.). For example:

- The workflow associated with user management and provisioning tasks (e.g., creating users, changing roles, assigning roles, etc.).
- The approval processes required for different tasks.
- The data requirements needed to perform tasks (e.g., whether an administrator must specify a user role, or whether entitlements are determined from certain directory attributes).
- Logical rules for determining how users should be defined on target systems and applications. For example, rules that determine how to format an email address based on user information, rules to figure out what printer should be assigned to a user and rules to figure out which groups a user should be added to.

Ideally, a user management and provisioning system should have one centralized set of policies and be entirely policy-driven. Organizations should adopt tools and systems that allow them to define all of the workflow, approval processes, input and output parameters, and provisioning logic in *one place using one set of tools* and have those policies drive everything from the user interface to application provisioning processes. This approach:

- Avoids the pitfall inherent in many approaches where policies are stored in multiple places—a customized UI, a workflow engine, a rules database, and code-heavy application agents.
- Enables the ability to completely customize the user management and provisioning system to conform to an organization's exact user experience and processing requirements.
- Eliminates policies embedded in compiled agents by extracting policies from agent code and centrally managing them along with other policies.

To simplify policy maintenance and increase policy reuse across different systems, policies can also be divided into a flexible hierarchy such as:

- Process Policies- Policies that dictate high-level workflow for user management tasks, such as creating users and maintaining attributes.
- Role Policies - Policies that automate decisions and processes that are role centric, such as what resources and entitlements should be assigned to a user based on role.
- Application Policies - Policies that automate decisions and processes that are application-specific. Read more about this approach in Rule 9.

Taking a centralized approach to policy management ultimately leads to a solution that conforms to an organization's IT infrastructure and not the other way around.

Rule 6: Phase the use of role-based entitlements

Many organizations find the process of defining organizational roles that meet all of their needs too time consuming and cumbersome. Rather than delay the deployment of user management and provisioning systems until roles can be defined, organizations can utilize a role-less approach and evolve to role-based provisioning in phases.

The primary advantage of role-less provisioning is that organizations can create simple policies for granting user access to systems without having to define and test role definitions. Organizations can allow administrators to assign resources from a simple list, create a few "model" users that can be "cloned" when adding new users, or assign and configure entitlements based on user attributes (e.g. department, title, level, location, etc.).

In fact, a role-less user management and provisioning approach can allow an organization to most closely match and automate existing IT processes (because most organizations have not yet adopted role-based user management).

There are some approaches that simplify phased role deployment:

- Centralize user management and provisioning policies (Rule 5). Phased role deployment is made easier if all of the policies for provisioning a specific application or resource are managed in one place and not scattered in different systems (e.g., separate workflow specifications and rule definitions).
- Separate high-level user management policies from detailed policies for provisioning specific systems and applications. It is best to modularize policies that pertain to specific processes and target applications. Maintaining separate policies for overall business processes, role entitlements, and application-specific provisioning logic makes it easier to reuse each policy and build a system that can adapt to change.
- Build a flexible approval process for applications and resources. Once application and resource policies are centralized, organizations should build approval logic that can adapt to the way in which those policies are invoked. For instance, an application provisioning policy might perform its tasks automatically if it is invoked as part of a role because it "knows" that the role has been approved earlier and that role is authorized for the specific application. However, the same policy should contain logic that seeks approval from the appropriate administrator if it is not invoked as part of a role.

The above approaches for designing policies will allow an organization to deploy a system quickly and add role policies over time, without having change existing policies or recode application agents.

Rule 7: Select the most appropriate authoritative identity source for your environment

All user management and provisioning solutions require a single, consistent directory of user identities to ensure a consistent process for provisioning resources and provide necessary audit and compliance controls. According to Phil Becker, Editor of Digital ID World Magazine, "The most significant evolution is the realization that the mission of identity management isn't to centralize identity data and access management, but rather to centralize only the policies that manage its administration and use while distributing and delegating the rest." [iv]

However, most organizations have identity information stored in multiple disparate directories and databases. It is not uncommon to find directories for network access, enterprise applications, ecommerce systems, custom applications, and different operating system platforms. While many of these applications sometimes utilize a common enterprise directory, many do not. It is not uncommon for organizations to have tens or hundreds of different identity sources, presenting a challenge to any deployment.

There are several approaches to solving this issue for user management and provisioning systems:

1. Deploy a system that imports identity data from multiple sources and creates a new, authoritative, identity source. This approach can be beneficial because the user management system has its own storage mechanism and does not rely on "live" system directories. However, the disadvantage to this approach is that there is the risk of directory proliferation by creating yet another directory that must be managed.
2. Choose a single directory to be the authoritative source and ensure that all other directories are synchronized to it. This approach has the advantage of being fairly straightforward to implement, however it does mean that the user management and provisioning system is relying on "live" directory data.
3. Use directory virtualization technology to create a "virtual" directory comprised of attributes from several directory sources. This approach is appealing if it is impossible to easily import data from multiple directories, yet attributes on those directories have to be used as part of the authoritative identity store. This is an effective approach to building a comprehensive identity source without having to create another directory.

Regardless of which approach is chosen, it is absolutely critical that the authoritative identity source strategy is well defined and adhered to.

Rule 8: Start with a clean directory foundation

As mentioned in Rule 7, most organizations maintain identity information across multiple standards-based and custom directories and it is critical to choose a strategy for creating an authoritative identity store. It is also critical that a user management and provisioning system resolve inconsistencies and issues in multiple directories before a full system is deployed.

An effective user management and provisioning strategy will:

- Simplify an organization's disparate directory infrastructure using identity virtualization or directory synchronization.
- Identify issues such as dormant accounts, invalid accounts and inconsistent user identifiers and attributes.
- Resolve these common identity issues using customizable policies that can then be used as the foundation for automated provisioning.

A general approach involves:

1. Creating an inventory of existing systems and directories.
2. Detecting inconsistencies through virtualization technology, meta-directory rules, or a custom process.
3. Isolating and locating orphan and dormant accounts.
4. Identifying inconsistent attributes (e.g., an employee phone number is different on two different directories) and invalid attributes (e.g., an employee phone number is different from the listing on an authoritative source).
5. Establishing a unique identifier linking identities and accounts across systems.
6. Applying customized policies to automate resolution and continuously monitor the directory infrastructure to guard against new inconsistencies emerging.

Rule 9: Consider ways to reduce "agent" complexity

One of the key requirements of a user management and provisioning system is to be able to access target applications and perform account setup and configuration. These actions are typically performed by application-specific "agents" that utilize API's to access target systems as well as logic that dictates how the provisioning process should occur. The terminology in the market varies by vendor, but some of the more common names include adapters, connectors, and agents.

There are two basic approaches taken by vendors in providing connectivity to target platforms:

- The delivery of large numbers of pre-built agents that contain the API's and a substantial amount of provisioning logic that has to be customized by each organization.
- The delivery of an "agent development toolkit" that allows rapid generation of agents and then permits customization.

Whichever approach is more appealing to an organization it is important to understand that no matter which approach is chosen, organizations should not underestimate the amount of customization that must still occur (even with pre-built agents). The reason is simple: The API's that connect to target applications are usually fairly straightforward. The difficulty of building an agent is the creation of specific logic that meets an organization's unique business needs. These needs differ from organization to organization so agents. Due to the unique needs of an organization agents generally will require customization.

In light of this fact, here are some tips on how to best proceed:

- Consider approaches that extract detailed provisioning logic and organizational policies from hard-coded agents. If an organization spends too much time custom-coding and compiling agents using programming languages it is harder to re-use common logic across multiple agents and it increases the skill level required to modify those policies. Ideally, policies should be able to be modified by business owners, and not require code-level programmers.
- Look for a provisioning solution that allows you to modify agent functionality in one place and does not require edits to both an agent and the user interface to accommodate customizations. This will substantially reduce ongoing maintenance efforts.
- As mentioned in Rule 5, if an organization can put all user management and provisioning logic in one place by centralizing all policies, they can avoid having critical policy information spread out in multiple places (workflow engines, agents, etc.) and do a better job of managing, securing, and maintaining those policies.

Rule 10: Ensure that every user management activity is logged and can be audited

Comprehensive audit logging is a mandatory feature of any user management and provisioning system. Knowing who did what to which object, when they did it, and how the object's services have now changed is vital information for internal audit activities and for meeting new regulatory compliance requirements.

Here are a few considerations:

- Many delegated administration products enable non-privileged users to securely perform administrative tasks. This is accomplished by using *"service accounts"* that actually perform the tasks transparently for the administrator. The benefits of such an approach are many; however, this can mean that audit logs may record the event under the name of the service account and not the name of delegated administrator, diminishing the usefulness of audit logs. Therefore, it is imperative that the audit functionality properly records the name of the delegated administrator who requested the transaction, and not simply records the event under the name of the service account.
- It is not uncommon that homegrown user management tools and "native" tools provided by software vendors require an organization to specifically grant authority to administrators to perform all of the tasks. This is impractical because it often results in granting too much access to un-trained administrators or creating overly complex and granular security authorization rules. This approach should be avoided.

Beyond just tracking the "who, what, where, when and how" of a single provisioning transaction, the complete transaction record of all applications, resources, and devices provisioned is critical. Systems that are XML centric and that log the entire transaction as it was performed offer the most options for integration and business recovery activities.

Audit logging used to just be a convenient analysis tool, but as a result of recent legislation in several industries it has become a mandatory aspect of user management and provisioning systems that must be strictly enforced.

Rule 11: Adhere to emerging standards

In response to organizations' need to have key business systems effectively share user identity information, market leaders in the space are working together to develop standards regarding the inter-connectivity between identity management solutions.

A major initiative is the Service Provisioning Markup Language (SPML) being developed by Organization for the Advancement of Structured Information Standards (OASIS). While SPML is designed to offer organizations a common XML-based framework to exchange identity management requests and information both within and between enterprises, it is not, in itself, a provisioning solution. It does however have the potential to greatly enhance the scope of provisioning solutions where it is utilized and is critical to taking a phased approach to deploying a user management and provisioning system.

Organizations that deploy user management and provisioning systems that are SPML-compliant will, in the future, likely be able to download or purchase scripts to provision certain applications and resources (or even receive those scripts as part of the application purchase) and be assured that those scripts will automatically work with their existing user management systems.

For more information on emerging standards download our free e-Book "The Administrator Shortcut Guide to User Management and Provisioning".

Rule 12: Secure the user management process

User management and provisioning systems administer most, if not all, of the users within an organization and typically interact with the most ubiquitous and business-critical applications and services. For this reason, it is essential that an enterprise choose a solution with proper security management.

There are three high-priority aspects of security that should be considered:

1. **Restricting and authenticating access to the user management system.** Access to a user management and provisioning system is typically through a Web-based user interface, which may be exposed outside the corporate firewall. The user interface must therefore support the native authentication policies and security protocols of the organization. In addition, administrative rights should be enforced at both the Web UI and back-end service. Commands from sources other than the UI (such as a corporate portal) will therefore only be executed if the administrator has the appropriate rights.
2. **Restricting administrators to only view and alter only those users, groups, and objects for which they are responsible.** The only available options should be those that are appropriate to the administrator's role and location within the organizational structure. This prevents administrators from making changes to users outside their area of authority or performing tasks beyond their scope. An administrator responsible for one business unit within an organization may therefore be completely partitioned from modifying or, indeed, seeing users in another department. Similarly, the provisioning system must be able to provide separation of business units so that administrators in one business unit do not see confidential information about users in other business units. This is a critical capability of any delegated user management process.
3. **Automating and simplifying the process of granting systems access to users.** Modifying security settings can become very complex and provide plenty of opportunity for human error. Due to the pervasiveness of a provisioning system, such errors may impact the entire organization. Automating the application of security policies is therefore highly recommended. This best practices philosophy should also be applied to data entry. Where data cannot be provided automatically, wizards or similar data entry aids should be employed within a consistent interface. Wherever possible, exposure of administrators to the complexity and risk associated with multiple native tools should be avoided.

Rule 13: Consider triggering user management and provisioning processes from your HR system

Increasingly, many companies are evaluating, and adopting, a process change that leverages the enterprise Human Resources (HR) system to drive user management and provisioning events, particularly for new hires.

The reason for this is that the HR system is typically the most accurate source of basic employee information within an enterprise, because:

- Employees are motivated to ensure their name, title, office location and contact information are correct, since errors may result in problems receiving paychecks or other benefits.
- The HR department needs to have accurate information to justify disbursements, particularly when employees are being hired, transferred or terminated.
- There is little incentive to rigorously maintain or audit stores of user information that are not directly tied to payroll.

Too often, the process for provisioning a new employee with the digital and physical assets is completed long after the employee's first day on the job. It can take days or weeks to get an employee set-up and this represents lost employee productivity and costly activity within the IT organization. It is also not uncommon that the series of manual steps required to set up a user results in the user getting access to systems that they do not need. By automating this process, organizations can avoid losing employee productivity and ensure that employees only get access to the systems and resources that they need.

By integrating these HR and IT processes, organizations can also reduce security vulnerabilities when an employee leaves. The system ensures that email access is fully removed (both from inside the corporate network and through modern web-based methods for accessing email) and that access to confidential information and applications is immediately revoked immediately. Any lag between the time an employee officially leaves (as indicated in the HR system) and the complete de-provisioning of the user's access rights is a significant security threat, and one that can now be eliminated.

Here are a few considerations:

- Organizations should carefully map the data from the HR system that will be used to trigger user management and provisioning transactions. For example, the user's Role definition in the HR system might not be the same as role definitions in other IT systems. The user management and provisioning system should handle these data transformations as part of the overall set of security policies.
- Organizations can choose to automate some processes but leave others in the hands of administrators. For example, triggering new and terminated employee processes from HR but leaving profile updates and new entitlements to delegated administrators or a help desk.
- The process of transferring (or moving) a user from one department (or role) to another can be tricky. It typically requires the ability to assign multiple roles to a user and set timeframes for allowing overlapping sets of entitlements to ensure that users do not lose access to information that they might need during a transition.

Rule 14: De-provisioning users is just as important as provisioning

Enterprises are typically *very* efficient at taking an employee off of payroll when they complete their employment, but the practice of de-provisioning an employee's assets, such as network accounts, application access, IT resources (e.g., storage used), or even telephone calling cards, is less than perfect.

Consider the real example of a company with more than 13,000 active accounts on its environment, but only 8,000 employees. The 5,000 accounts represent significant security vulnerability, resulting from a lack of properly executed processes for terminating user accounts when employees leave the company. User management and provisioning initiatives must make de-provisioning a priority.

Provisioning saves time, saves money, and accelerates an employee's productivity. Consistency ensures that tasks are performed the same way each time and that security vulnerabilities are not introduced into the environment as a result. In most cases, the benefits and ROI are easily predicted. However, terminating an employee introduces a significant amount of process risk, which is harder to predict and measure, but can be potentially devastating. In this context, de-provisioning may be more important than provisioning.

An important part of de-provisioning is ensuring that the user's data is maintained according to corporate policy:

- Should files and messages be deleted or retained?
- Should mailboxes remain active and able to accept mail?
- Should ID's be deleted or just deactivated?

Answering these questions is a critical part of an organization's user management and provisioning approach.

Simply stated, the tasks for de-provisioning a user are the opposite of provisioning and must be completely automated to ensure proper security:

- Remove access to all systems and applications
- Reclaim or archive system resources such as mailboxes and files
- Create an audit log of every action

Rule 15: Implement best practices from other successful user management and provisioning projects

With user management and provisioning projects being relatively new initiatives for enterprises, there are very few documented experiences and approaches to use as a guide an enterprise implementation project.

User management and provisioning systems are heavily dependent on an organization's directory strategy and often implemented at the same time as directory deployments and migrations. Best practices for those projects are readily available and should be part of your plan. If your organization is already planning to embark on a new directory deployment, consider combining that project with the implementation of a user management and provisioning system for several reasons:

- Migrating to a configured user management and provisioning system tightens security from Day 1 and this, of course, is a priority.
- It minimizes disruption to users by making changes at one time rather than two; the user disruption level is typically what defines, in the view of some audiences, how "successful" projects are!
- The users' environment remains consistent after the migration and does not contract. For example, during a mail migration, deploy a mailbox quota via the provisioning solution during the migration phase, rather than migrating users and then later constricting the mailbox size. The principal here is that it is easier to grant more services/capacity to users than to it is to take them away.

Below is a collection of best practices for implementing a user management and provisioning system. These practices are based on feedback from organizations that are planning, undergoing, or have completed the implementation of an enterprise user management and provisioning initiative:

- Create a multi-disciplinary team. Knowledgeable people, including experts in business requirements, technology, databases, directories and security, are necessary;
- Develop a comprehensive list of objectives that are well grounded in business requirements. Determine how the objectives will be met. Perform an external information survey to determine user management and provisioning issues and approaches;
- Review the enterprise's identity management and security policies. From this, develop a user management and provisioning policy;
- Understand that effective user management and provisioning initiatives are more complicated than deploying a few tools, so follow standard project management and packaged system selection and implementation methodologies;
- Create a list of vendors to which the request for proposal will be sent. Optionally, a request for information may precede the request for proposals;
- Issue RFI/RFP. Evaluate each response;
- Select a user management and provisioning system that is strongly based on characteristics such as delegated administration and role management;

- Look for solution that eliminates the need for redundant system management systems such as Microsoft Active Directory and Exchange third-party ("native") management solutions that could create audit and compliance issues;
- Evaluate the value of supporting emerging provisioning standards, such as SPML, both within your organization and as an externally facing interface for partners to access.
- Structure the project (work breakdown structure) so that early phases focus on the provisioning of ubiquitous (and high impact) applications such as messaging, network access, and those applications services that are pervasive throughout the enterprise;
- Establish consensus early among key business stakeholders whose support is critical to the project's success;
- Consider integrating the corporate human resource system with the user management and provisioning system in a phased approach that initially focuses on the mitigation of security vulnerabilities; and,
- After each phase of the project, develop and communicate metrics on the project's impact on the enterprise including ROI and customer satisfaction benefits.

Conclusion

User management and provisioning technology has advanced into a powerful and flexible set of software products and techniques that can deliver a rapid return on investment. Its adoption in the enterprise is growing exponentially; however, the successful deployment of these systems needs to be managed closely, as does any major piece of corporate IT infrastructure. Critical concepts to remember:

- User management and provisioning must be a component of an enterprise identity management strategy, or the potential benefits may not materialize.
- The real value of user management and provisioning can only be achieved if you securely automate processes or delegate them to lower-cost employees.
- The deployment of user management and provisioning systems must be phased with an initial focus on ubiquitous enterprise applications such as messaging and network access. "Big bang" approaches that provision everything at once rarely succeed.
- Policy management is a crucial aspect of the system and it should be centralized to speed deployment and improve maintainability.
- Organizations should look for user management and provisioning systems that can be completely customized to adapt to an IT infrastructure and not the other way around.
- Choosing an extensible, standards-based architecture for user management and provisioning is critical to ensure that your platform can accommodate future needs as you embark on a phased deployment.
- Only after a successful deployment of core applications and services should the scope be expanded.
- Since user management and provisioning systems are relatively new to the enterprise, implement best practices from other large multi-department, projects.

Following these rules will get you and your organization on the path to a successful deployment of a user management and provisioning solution, and ultimately create a more secure and lower cost user environment.

We Want Your Feedback!

If you have any questions or would like to comment on this paper, please write to us at 15rules@abridean.com!

---

[i] "*ROI Drives Identity and Access Management Implementation*", R. Witty, Gartner, 3 December 2002 (Note Number: SPA-18-9500)
[ii] "*Access management. Part One: Sound ROI with Security Benefits*", Illena Armstrong, SC Magazine. October 2002
[iii] "User Management", Burton Group, November 21, 2002
[iv] "*The most significant evolution is the realization*", Phil Becker, Digital ID World Magazine. September/October 2004.