Provisioning SSO
Governance Password

TOP 10 PASSWORD MANAGEMENT

BEST PRACTICES

The proven working guide for successful implementations.

2016 EDITION

Provisioning SSO
Governance Password

TOP 10
Steps to Success

Allowing business users to manage their own password changes can significantly reduce help desk calls.

Most importantly, having a centralized password management process and solution in place helps enforce strong password policies by automating IT operations across the organization.

Password Management With a Plan

Today's organizations are a study in change: New employees and contractors come on board, some leave, others transfer, while responsibilities continuously shift within the organization. Throughout all this change, password policies continue to enforce password changes, prompting endless calls to an already overburdened help desk. For IT professionals, the challenges are efficiently meeting increasing service-level demands, while also enforcing policy and security, maintaining stringent access audit controls, and addressing access governance and risk compliance requirements.

Luckily, self-service, automated password reset tools exist to unburden IT professionals, while at the same time ensuring bulletproof security. But it's not enough to simply purchase and install a password management solution and hope for the best. To achieve optimal results and measurable cost savings, the password management solution must be considered as part of an overall corporate strategic plan aimed at maximizing benefits across an entire enterprise.

In this guide, we define the top 10 critical items and best practices that help ensure maximum corporate buy-in and implementation success. And if you need additional guidance, we're here for you. Avatier experts are on hand to make sure you reach your password management strategic goals.

Provisioning SSO
Governance Password

TOP 10
Steps to Success

Step 1: Understand your organization's needs.

Before evaluating any password management solution, it is imperative to identify needs specific to your organization. To help focus your evaluation, organizational processes should first be documented and understood. Without the due diligence that leads to this understanding, the potential for loss of financial investment skyrockets, because you can end up with an expensive solution that delivers more than what you need.

Setting goals is part of this pre-evaluation phase for improving security and efficiency, reducing costs, and achieving password management governance, risk and compliance. And once your goals are set, you must establish metrics and define a baseline to measure the impact of your solution. For instance, you can determine help desk call volume, resource productivity and enrollment goals. Then look at process costs such as the average baseline cost for a password reset and unlock accounts, which represent password management metrics with measurable goals.

□ Approved by ____

□ Date completed _______________

Step 2: Consider a solution with options for automated reporting, alerts and unenrollment.

Automation is not only a big time-saver in organizations; it also eliminates any kind of human error that goes along with manual entries. When evaluating a password management system, consider a solution that automatically reports on configuration changes, account unlocks, enrollment, password resets and attempts, authorization failures, etc. Automatically generated alerts are also valuable, generating immediate notifications to a defined recipient list after an authorization failure, password change failure and configuration changes. Automatic unenrollment after someone leaves an organization ensures the ongoing integrity of your corporate systems.

□ Approved by ____

□ Date completed _______________

Provisioning SSO
Governance Password

TOP
10
Steps to Success

The key to success in deploying a password management solution is defining manageable, measurable steps that provide a strong foundation on which to build your initiative. Once you have a road map, you set a path to readily secure your organization with an efficient deployment and cost savings throughout the process.

Step 3: Take into account your overall corporate infrastructure.

Many organizations attempt to roll out a password management solution without consideration for their corporate infrastructure. This leads to significant problems down the line. Make sure to designate a separate or virtual machine to test upgrades and patches prior to a production deployment; otherwise, the potential for disruption to your systems could mean significant financial and productivity losses amounting to more than the cost of a test server. Depending on whether the environment is internal- or external-facing, high availability, fault tolerance and failover are a necessity for organizations that maintain 24x7 operations. Configuring your system to utilize a relational database system to store audit log information is also recommended to ensure high availability, scalability and performance.

□ Approved by ____

□ Date completed _______________

Step 4: Determine appropriate messaging.

With any password management solution, notifications are sent informing users about a variety of actions. Take the time to make sure the wording in these communications is clear. Customize messages to get the most value and efficiency out of your password management solution. Include password expiration notices, password change alerts and administrator messages. You should also include a help desk number.

□ Approved by ____

□ Date completed _______________

Step 5: Provide proper secure identity questions.

To ensure effective utilization of a self-service solution, offer identity challenge questions that require exact answers. Consider questions that prompt answers utilizing long-term memory questions, such as "In what city did you meet your significant other?" Also, when punctuation or abbreviation is a possibility, do not consider it for question selection, as it leaves too much room for arbitrary answers. Finally, avoid questions with answers that can change over time, such as "What is your favorite restaurant?" Always select questions that are easy to remember with one consistent response.

□ Approved by ____

□ Date completed _______________

Step 6: Align password policies.

Organizations often try to make their password management solution adapt to numerous different password policies on their source systems. While a strong password management solution can do this, it often makes more sense to take a little time to evaluate your password policies on each system to see if they can be unified to a common policy. By setting strength and expiration policies to common values, a number of challenges can be resolved while simplifying you environment.

□ Approved by ____

□ Date completed ______________

Step 7: Increase scope.

While increasing scope goes against most project management practices, synchronizing passwords across every system in your environment will dramatically improve operations. So rather than limiting it to try and address only a few key systems, leverage the power of your password management solution to synchronize passwords across all your systems. This makes it much easier for users, reduces help desk calls to your data center, and better prepares your organization for longer-term IAM initiatives to those other systems.

□ Approved by ____

□ Date completed ______________

Step 8: Develop an account mapping plan.

In order to maximize the password synchronization benefits of a password management solution, you must know which user has what logon account on each IT system of your organization's systems. This also facilitates account management across multiple platforms. For example, you could incorporate of an account-mapping database of all users, their various accounts, and the target systems they access in the organization.

□ Approved by ____

□ Date completed ______________

Step 9: Define an exclusion list.

Define an exclusion list. For compliance and operational reasons, certain users and user groups must be excluded from enrolling in and utilizing the functionality of a password management solution. Consider defining and documenting these individual users before deployment, which will enable a more efficient rollout during the configuration phase.

□ Approved by ____

□ Date completed _______________

Step 10: Select which client interfaces to deploy.

To roll out a password manager, organizations must plan for each
password management interface, and identify the pros and cons of deploying the following options:

- A Web interface is the easiest from an IT perspective, since a Web browser is included with almost all operating systems. The Web interface may require an Active/X control to reset locally cached credentials, but this control is only necessary in Microsoft environments that have enabled "change password." This function typically is enabled only when password synchronization is also enabled to allow the Microsoft Windows password to be pushed to all target systems.

- Deployment of a customized graphical identification and authentication page that provides pre-network logon access to the password management solution requires installation of a Microsoft Installer (MSI) package on each workstation. Your organization must have a software distribution mechanism in place to ensure the installer package is delivered and successfully installed on the workstations. Additionally, users must be notified and trained to prepare for the new logon screen they will see on their desktops the next time they boot their computers. As part of rollout, your change management and training plan will promote adoption and reduce help desk calls.

- To successfully enable using a telephone to reset forgotten passwords and unlock an account, consider adding hardware requirements including the telephony interface board, the server it will run on as well as connectivity to the phone lines. Decisions must be made as to whether to use an analog or IP-based (SIP)
phone line.

□ Approved by ____

□ Date completed _______________

Provisioning SSO
Governance Password

TOP 10
Steps to Success

PASSWORD MANAGEMENT DEPLOYMENT

Password Management Success

The ultimate goal of a password management solution is to give your users timely access to the resources they need to do their jobs and stay productive, no matter how often or how quickly their roles and responsibilities change. At the same time, an effective password management solution will free your IT professionals to focus on other important organizational issues.

But without first evaluating your needs and assessing your current environment, your solution might fall short of expectations. Indeed, the best results come when your project takes a focused step-by-step approach with your business goals in mind. Only then will you end with a password management solution with the potential to change the way you perform core processes to ultimately yield a more efficient, productive, secure and risk-free organization.

TOP
10
Steps to Success

Notes