ManageEngine
ADSelfService Plus

Three password management practices for efficient IGA in 2020

www.adselfserviceplus.com

Table of Contents

1. What is IGA?

The term identity governance and administration (IGA) gained prominence in 2013 once Gartner merged its earlier two Magic Quadrant (MQ) categories to form an MQ for IGA. IGA is a combination of two frameworks: identity governance and identity administration. Identity governance is a set of policies that define activities such as logging, reporting, segregating duties, and managing roles. Identity administration deals with activities such as the administration of accounts and passwords, managing entitlements, and access provisioning.

By combining these domains, an IGA system allows companies to stay compliant with regulations like the GDPR and HIPAA, automate the workflow of managing access requests, and monitor at all times if the right set of users have the right amount of permissions.

In this guide, we'll look at the differences between identity and access management (IAM) and IGA; three simple, easy-to-implement password security best practices that you can include in your organization as part of your IGA strategy for 2020; and a third-party solution for implementing the discussed practices.

2. IGA and IAM: How are they different?

Although many parallels can be drawn between IAM and IGA, they are quite different in the areas they cover. IAM focuses on using self-service to manage passwords and leveraging automated workflows to create and disable user accounts, assign permissions, deal with access permissions, and more. IGA, on the other hand, is a broader framework inside which IAM resides.

IGA encompasses everything that IAM covers, but the term also includes more capabilities such as auditing and generating reports to meet compliance requirements, monitoring roles in your organization, and certifying access permissions to make sure that the just-in-time and just enough access principles are upheld. In short, IGA adds an additional layer of intelligent governance on top of IAM.

3. Why the user as the base identity is important

In a well-managed IGA program, access decisions are based on identity, which is the foundation for all security. The first step in establishing a successful IGA program is to identify all user identities and determine what information they can access.

With user identities as the foundation for your IGA strategy, building access policies based on user accounts becomes easier and can easily be changed based on the organizational unit (OU) and group memberships of the users, ensuring just-in-time and just enough access to required resources.

Any change in the account access policy begins right from the password policies and password privileges that the user has, including the ability to reset or change their password remotely via VPN, utilize two-factor authentication for privileged accounts, and leverage single sign-on to enterprise applications protected by multi-factor authentication. If user identities do not form the foundation of your IGA strategy, it becomes difficult to set and modify access policies for your organization.

4. The three password management practices that IGA requires

Passwords are the most common method of authentication into various services. Consequently, a strong password management solution is imperative for enhanced security. Since passwords act as the key to your entire IT infrastructure, it makes sense to ensure that the password management practices followed in your organization build a proper foundation for an effective IGA strategy.

Here are three simple, easy-to-implement password security best practices that help in strengthening your IGA infrastructure.

Enable self-service password reset:

Enable users in your organization to reset their passwords or unlock their accounts for popular directory services such as Active Directory. The implementation of self-service ensures a smooth workflow for both the users and the IT help desk team. It is an added advantage if the self-service password reset policy configurations are controlled entirely by the IT team. This way, they can decide which of the users get to use the feature based on their privilege thereby striking a good balance between accessibility and security.

Implement stringent, granular password policies:

Organizations need to implement password policies that ensure users set strong passwords; don't use dictionary words, common words, or their username itself in passwords; and more.

Establish a data change approval workflow in tandem with a help desk application

Users should have the option to edit their own personal data, such as their name, phone number, or address, instead of depending on the help desk to make those changes. All requested data changes by end users should be monitored by an IT admin to ensure there is no discrepancy in user data, helping to find the right balance between user independence and data integrity.

4.1 Enabling self-service password reset for end users

Self-service password reset enables users to reset their passwords or unlock their accounts by themselves without relying on the help desk team. An end-user password management tool, such as ManageEngine ADSelfService Plus, comes in handy here. With the solution installed, your users can reset their passwords and unlock their accounts even when they're not in the office via a VPN, making the process extremely secure. ADSelfService Plus also gives IT admins the option to decide which users get such privileges based on their OU or group membership.

ADSelfService Plus takes the huge burden of resolving password reset tickets off the shoulders of your organization's IT team, allowing them to focus on more critical tasks that require their expertise. By implementing self-service password reset capabilities, your organization can decentralize the process but still have control over the password change process, thereby removing the middleman (your help desk).

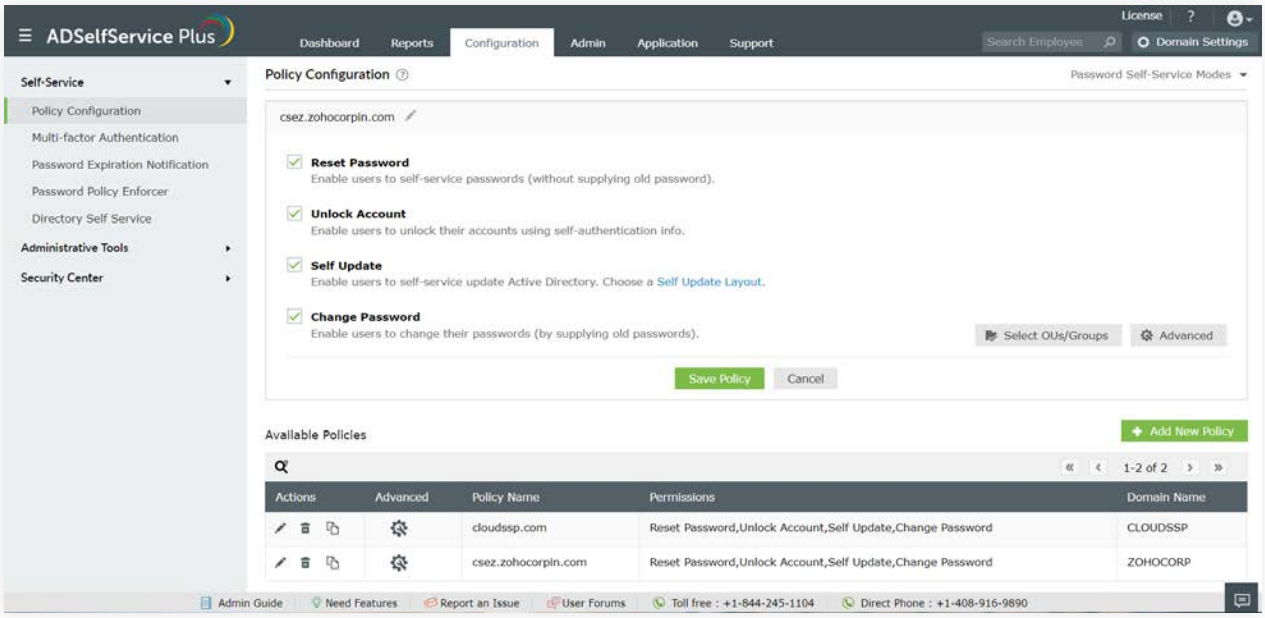

Fig 1: The Policy Configuration tab for self-service password reset in ADSelfService Plus.

4.2 Implementing stringent password policies

The built-in password policy configurations that come along with popular directory services such as Active Directory are rudimentary, and are not set strongly by default.

The default policies leave critical gaps for hackers to explore, such as:

1. The default password policy features offered in Active Directory follow a "one size fits all" principle. Administrators find it challenging to set unique password policies for users based on their group or OU memberships within the domain.

2. The password policy fails to restrict the use of common password patterns, like “asdf,” “1234,” and “qwerty,” as well as incremental passwords like “password1,” “password2,” and “password3.”

3. The password policy can’t prevent dictionary words or usernames from being used as passwords.

ADSelfService Plus offers a comprehensive set of password policies that allow your organization’s IT admins to control how users set their passwords. These policies offer many additional features and more granularity than the default password policies, such as restricting the use of dictionary words, palindromes, common patterns, and incremental strings in passwords. These stronger policies ensure users set passwords with a high entropy, protecting user identities.

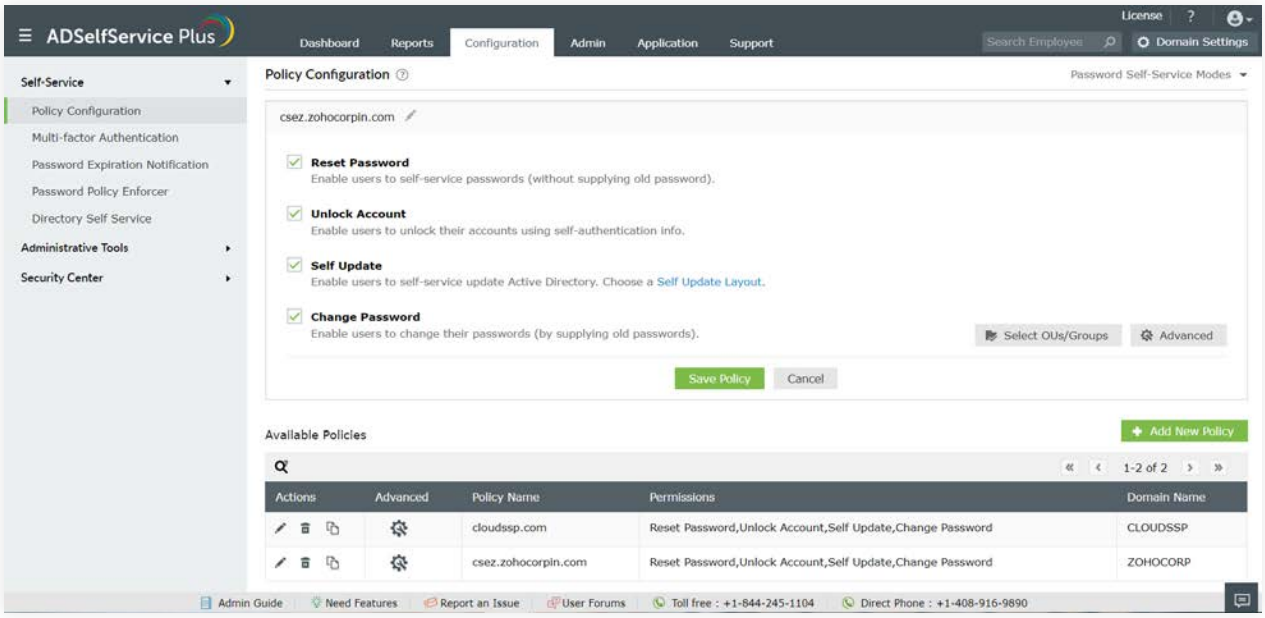

Fig 2: The Password Policy Enforcer tab in ADSelfService Plus.

What's more? ADSelfService Plus even has a built-in password expiration notifier that IT admins can use to send end users scheduled reminders about changing their soon-to-expire passwords. IT admins have complete control over how often users are reminded, the message in the reminder, and the number of days before users have to be reminded.

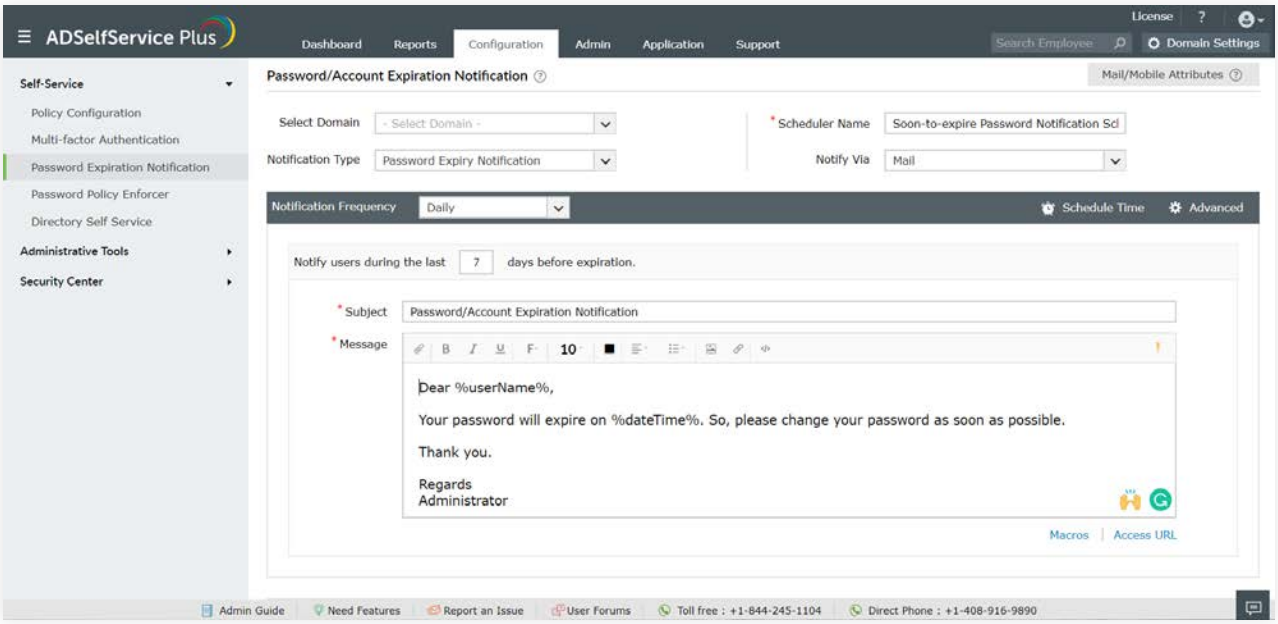

Fig 3: The Password Expiry Notification tab of ADSelfService Plus.

4.3 Establishing a Self-Service Approval Workflow for data changes that originate from users

ADSelfService Plus gives IT admins the option to decide which end users can update their personal information (e.g. their phone number or address) using ADSelfService Plus' web portal. Although self-service user data modifications are convenient for users and the IT team, they can cause problems, such as discrepancies in your organization's directory data, if users make unintentional errors while updating their information.

A data change approval workflow, like the one offered by ADSelfService Plus, can help prevent incorrect data changes without restricting the freedom of end users to edit their own data. ADSelfService Plus' data change approval workflow is available once the product is integrated with an Active Directory management and reporting solution like ManageEngine ADManager Plus.

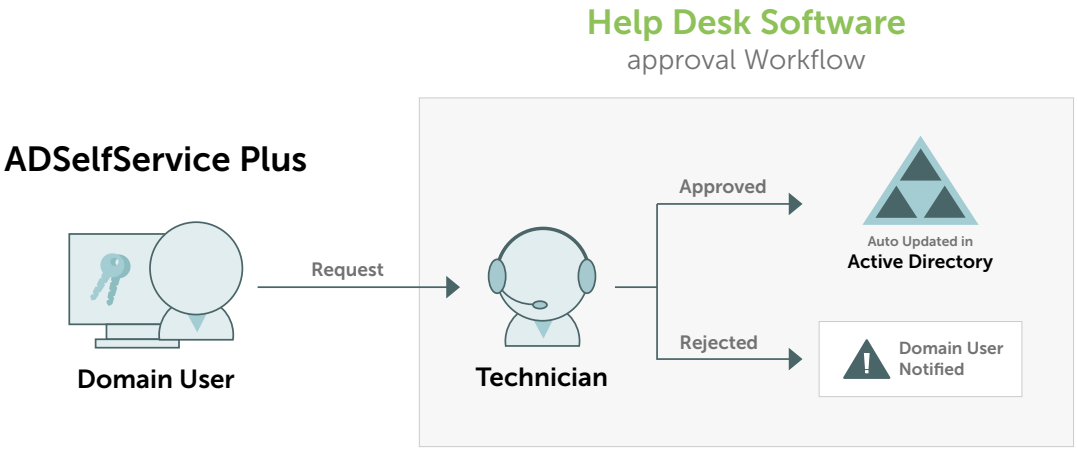

Fig 4: How the Self-Service Approval Workflow works in ADSelfService Plus.

The approval workflow ensures that the data change requested by the user is updated in your organization's directory only if an IT admin or technician approves the change from your help desk application. If the change is not approved, the data change is not made and the user is notified on ADSelfService Plus' user portal, the application the data change request originated from. ADSelfService Plus' approval workflow feature aims to make it easier for users to update their information, and even aids users in editing their email group subscriptions. The final say over directory changes always resides with the IT admin to ensure there is a healthy balance between usability and security.

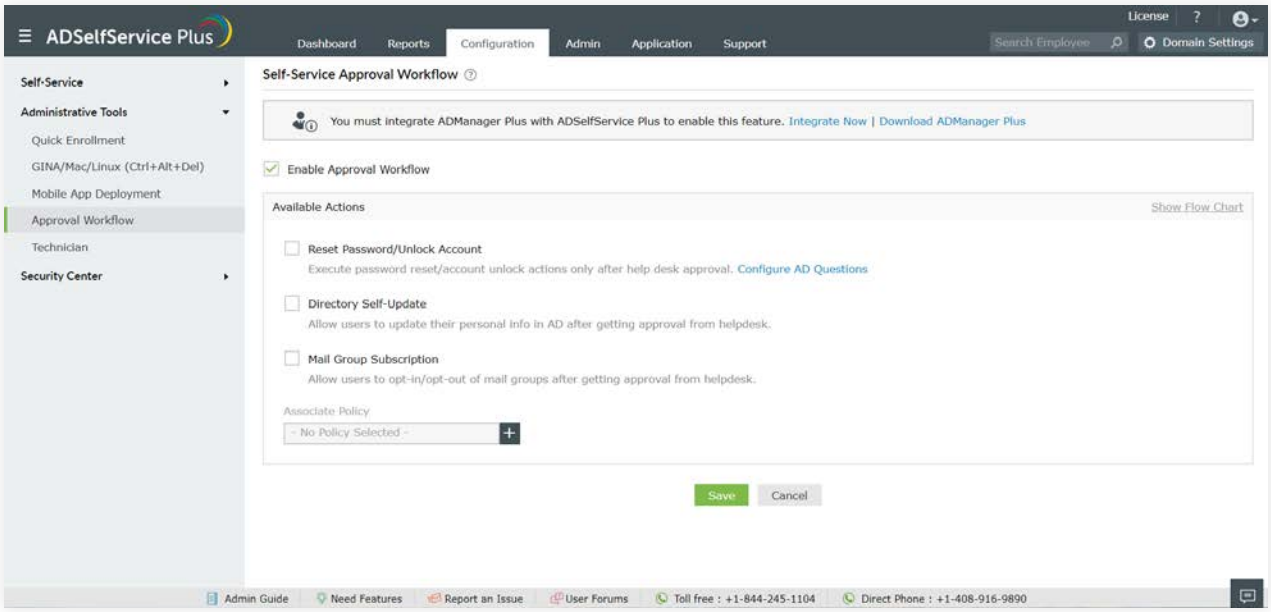

Fig 5: The Self-Service Approval Workflow tab in ADSelfService Plus.

5. Summary

An important part of verifying that your IGA strategy is robust is ensuring that all the passwords in your IT network are well-monitored, as they could be used as loopholes to enter your network. Using a password management application like ADSelfService Plus not only helps to govern your end users' passwords, but also frees your IT help desk from password management tasks. The solution also generates comprehensive reports for admins to analyze and flag any anomalous behavior if necessary.

Implementing the password management practices discussed in this e-book with the help of ADSelfService Plus will surely give your organization a strong foundation of strictly governed user identities on which the majority of your IGA strategy will depend on in 2020 and for years to come.