The key to secure, accurate self-service operations

ManageEngine
ADSelfService Plus

Making self-service safe, consistent, and easy to use

Convenience is a hallmark of self-service solutions, but a few challenges are just as common. Take security for example. Even when solutions have built-in security measures, attackers may still find a way to game the system and gain unauthorized access, which could lead to sensitive information leaks. And then, there are times when employees update data themselves that's erroneous or doesn't follow a certain format as defined in the organization's policies. Furthermore, not all employees are adept at using a self-service system. Many users may still contact the help desk for assistance with their IT issues.

Organizations need a secure method that allows help desk staff to assist users without increasing the number of service desk requests. In this guide, we will focus on how to verify and validate end users' self-service actions to ensure security and data quality using ADSelfService Plus, without affecting the freedom users get from a self-service IT model.

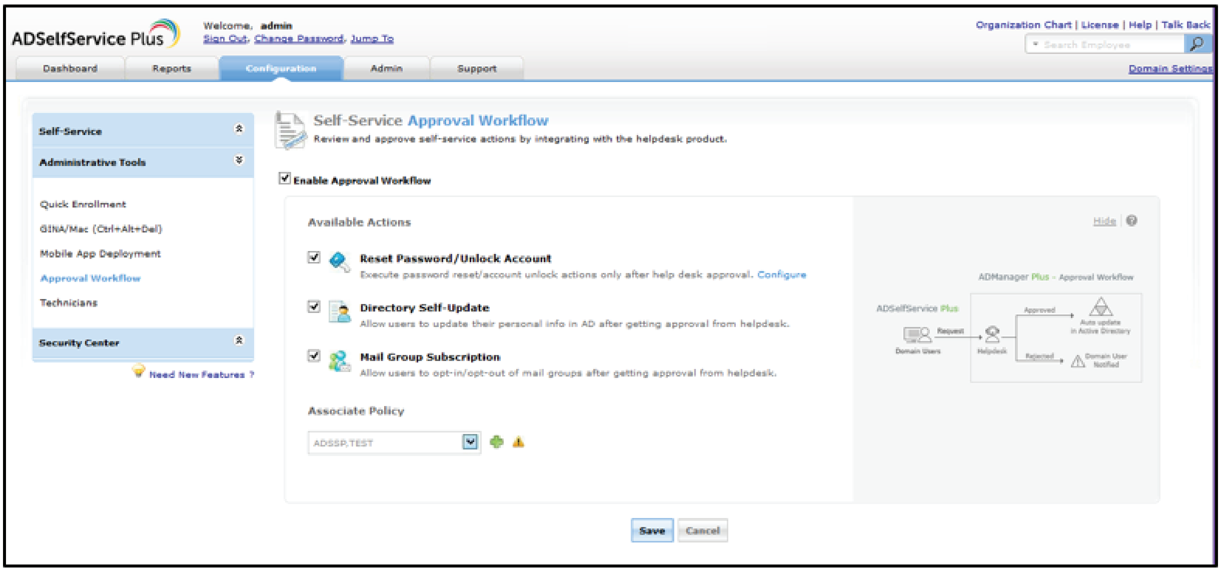
Giving help desk staff control over users' self-service actions

ADSelfService Plus—an integrated Active Directory self-service password management and single sign-on solution—lets IT admins and help desk staff take control of users' self-service actions. It has an approval workflow module, which redirects all self-service actions by end users to the help desk staff in the form of requests (Fig. 1). Help desk staff can then verify the self-service actions for consistency or, for password resets and account unlocks, accurately verify the users' identities.

At no time in this process are end users required to call the help desk. Instead, end users can track the status of their requests in the self-service portal.

Approval workflow for self-service requests

To enable an approval workflow for self-service, you need to integrate ADSelfService Plus with ADManager Plus—an Active Directory management, reporting, and automation tool. ADManager Plus allows you to build a customized workflow structure with as many workflow agents as you need.



Self-Service Approval Workflow

Review and approve self-service actions by integrating with the helpdesk product.

☑ Enable Approval Workflow

Available Actions

☑ **Reset Password/Unlock Account**
Execute password reset/account unlock actions only after help desk approval. Configure

☑ **Directory Self-Update**
Allow users to update their personal info in AD after getting approval from helpdesk.

☑ **Mail Group Subscription**
Allow users to opt-in/opt-out of mail groups after getting approval from helpdesk.

Associate Policy

ADSSP.TEST

Figure 1: Self-service approval workflow settings in ADSelfService Plus.

Once the approval workflow is in place, all self-service requests are raised by end users through ADSelfService Plus' web console. The requests are then reviewed and approved by the help desk staff or IT admins in accordance with the workflow structure configured in ADManager Plus.

Collecting quality data during self-update and authorizing self-service group management actions

ADSelfService Plus' self-update feature helps keep employee profile details, such as their contact information, up-to-date in Active Directory without any effort from the help desk staff or IT admins. These details are normally used in business white pages, Outlook Web App (OWA), and HR systems accessed by other employees and customers. So it is important that employee data is not only up to date, but accurate as well. With an approval workflow, help desk staff can view and validate the data users enter in the self-update form.

When employees change teams, they must be granted membership access to their new team's distribution and security groups. Moreover, they must do so without involving help desk or IT admins so that they have immediate access to the team's resources and are part of all team communication. Self-service group management enables employees to securely gain group memberships with approval from the help desk or group owners.

Scenario: Each country has its own telephone number format. As such, organizations may have policies that specify whether a telephone number should begin with a “0” or "+" symbol. Without any control measures, employees can use a self-service solution to enter the mobile number in any format they see fit. When this bad data is entered into business systems, other employees and customers will find the system to be unusable. To ensure that the telephone numbers updated by users are in the right format, employee data should be validated before it gets updated in Active Directory.

Here’s how the validation workflow works:

- A user logs in to the self-service portal of ADSelfService Plus, updates his/her phone number, and clicks Create Request.

- Instead of directly updating the phone number in Active Directory, ADSelfService Plus forwards the data to the workflow engine in ADManager Plus as a new request.

- Help desk staff and IT admins, who are designated as reviewers in ADManager Plus, instantly receive an email notification about the request. They then view and validate the user's new phone number.

- Once approved, the user's new phone number is automatically updated in Active Directory. The user can view the status of his/her request in the self-service portal itself.

Authenticating users for password reset and account unlock

The main goal of a self-service password management solution is to completely eliminate password-related help desk calls. However, that pursuit is not always possible because of security concerns or users’ inability to use the system correctly. To help users successfully use the self-service system while keeping it secure, ADSelfService Plus lets help desk staff assist and authenticate users during the self-service password reset and account unlock processes.

When an approval workflow is enabled, users will be asked to answer a set of Active Directory-based security questions (e.g., "What is your employee ID number?" or "What is your license number?") before accessing any of the self-service options. Once users complete the security questions, their answers are automatically validated by ADManager Plus and the results are displayed to the help desk staff. Once approved, an email containing a secure password reset link is sent to the users' secondary email addresses, which the users can use to reset their Active Directory passwords.

Scenario: A few users, despite receiving multiple enrollment notifications, are not enrolled for password self-service. When these users forget their passwords, they inevitably call the help desk for assistance. Now, the help desk staff have to spend even more time verifying the users' identities. Moreover, not all organizations provide permissions for Active Directory password resets to their help desk staff. So, how do you allow help desk staff to securely authenticate users and then reset their passwords in Active Directory without elevating their permissions?

Here's how:

- Admins configure Active Directory attribute-based security questions in ADSelfService Plus.

- Users who have forgotten their passwords start the reset password wizard in ADSelfService Plus.

- Users answer the Active Directory attribute-based security questions and create a request for a password reset. The request, along with the users' answers, are forwarded to ADManager Plus.

- Help desk staff or group admins—who are designated as reviewers in ADManager Plus—are immediately notified via email or push notification about the request.

- ADManager Plus automatically validates the answers submitted by users against the values in Active Directory and displays the results (in the form of warning and check mark icons) to the help desk staff. Reviewers can hover their mouse over the icons to see the actual values too.

- If the answers are correct, the help desk staff can approve the request.

- Once approved, an email containing a secure reset password link is sent to the users' secondary (personal) email address.

Tracking self-service requests and help desk actions

All actions by both end users and help desk staff are logged, meaning managers can track self-service requests using the built-in audit reports available in ADSelfService Plus and ADManager Plus. Best of all, at no point during the approval process does the help desk staff (the reviewer) need administrative access to Active Directory where the data and password are being updated.

Get started

Want to try implementing approval workflows for self-service right away? Download ADSelfService Plus and ADManager Plus. Watch this **video** for step-by-step instructions on how to integrate the two tools and enable approval workflows.

About ManageEngine ADSelfService Plus

ADSelfService Plus is an integrated Active Directory self-service password management and single sign-on solution. It offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and single sign-on for cloud applications. ADSelfService Plus supports the IT help desk by reducing password reset tickets and spares end users the frustration caused by computer downtime. For more information, please visit www.manageengine.com/products/self-service-password.

To learn more about the products and solutions available from ManageEngine, please visit www.manageengine.com.