okta

Solution Brief:

Enable Self-Service Password Resets

Executive Summary

As organizations grow, the needs of their user base, internal employees, and customers, will always put increasing demand on their IT departments. One particular drag on their resources is user account lockouts due to forgotten passwords.

While a password reset process may appear simple on the surface, organizations must strike a balance between managing user frustrations, allocating IT resources, and ensuring security standards are met. Recognizing these needs, many organizations have turned to self-service password reset solutions. By opting for an automated, yet secure process, organizations are able to maintain productivity levels for users while reducing burden on IT staff.

Challenges with Forgotten Passwords

The average company has over 80 apps, and even when accessed through single-sign on (SSO), it's inevitable that users will occasionally forget their one password[1]. A forgotten password usually results in a password reset process, which can create challenges and inefficiencies for both the end user as well as the IT department.

[1] https://www.okta.com/businesses-at-work/2019/#growing-appetite

For the end user, inability to access their account leads to frustration and productivity loss. Traditional IT workflows for password resets usually involve the creation of an IT helpdesk ticket or even a call to a live admin to assist the user in real time. Depending on how the organization assigns priorities for these tickets, it may be some time before a user's ticket is reviewed or someone from IT is able to reset their password. During this time, the user has no access to their critical apps..

Similar pains are felt on the IT side. Password reset requests can take up help desk time and resources. In fact, some reports cite up to 50% of help desk calls are due to password resets, which can result in significant costs.[2]

Passwords resets lead to user frustration and slows down IT and help desks

20% to 50% of all help desk calls are for password resets

The average help desk labor cost for a single password reset is **about $70**

Automating this process can help, but organizations need to ensure they are not introducing additional security risks. For example, sending out a password reset link through email. Anyone with access to that link, e.g., an attacker who's compromised the user's email account, can reset the password, gaining easy access to corporate resources. Even without automation, social engineering and phishing can compromise security as well.

Beyond such security challenges, IT departments may also have to deal with architectural and operational hurdles. If there are multiple sources of truth, an admin may have to reset passwords in multiple locations, or synchronize passwords. These hurdles add time, impede productivity and frustrate the end users, desperate for access.

A more efficient process is to allow users to reset their own passwords, combined with automation and strong authentication.

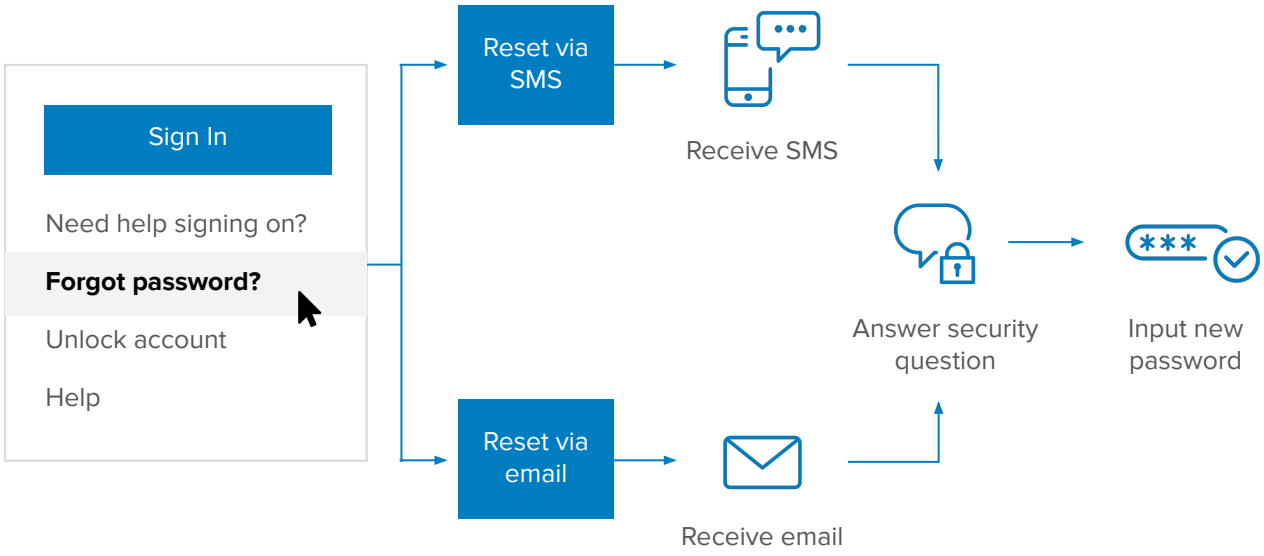
Enabling Secure Self-Service Password Reset

Allowing users to reset their own forgotten passwords has tangible benefits for all concerned: end users spend less time locked out of their accounts, and IT teams can re-allocate the time and resources previously spent resetting passwords.

[2] Gartner

A Simple, Three-Step Solution

Okta helps organizations achieve these secure, user-initiated, password reset flows. By using SSO, Universal Directory, and Multi-factor Authentication (MFA), users only need to follow three simple steps to reset their password.



1 2 3

Click on the password reset link

Include a *Click here to reset your password* link on the Okta Sign-On page so that users can intuitively initiate the password reset flow. By combining self-service password resets with SSO, not only can organizations reduce the number of required passwords (a security benefit, as well as end-user convenience) but users are able to access all their applications through a single password reset.

Receive either an email or an SMS message

The user has the option to receive either an email or an SMS message containing a password reset code. With both options, the user still has to answer a security question to verify identity before they are allowed to reset their password. This security question and answer is created when users enroll in Okta MFA.

Enter a new password

The newly created password can still impose the same password policies such as character length, number of special characters required, etc., ensuring a consistent password policy throughout the organization.

Benefits for IT Teams, Employees, and Customers

With this simple process, organizations can realize internal benefits as well as keep employees and customers happy.

For the organization and it's IT department, self-service password reset achieves the following benefits:

- ✓ Reduces help desk tickets
- ✓ Frees up IT time and resources
- ✓ Increases security posture

For employees and customers, self-service password reset allows for:

- ✓ Quicker access to applications
- ✓ Increased productivity
- ✓ Reduced frustration and a better experience

Okta's self-service password reset process is a single, elegant solution that supports multiple environments. Whether an organization has on-premises apps, cloud apps, or a mix of the two, Okta's solution supports them all. It also supports multiple Active Directory domains and forests, so users only have to reset their password one time to have those changes reflected across all systems.

We Are Here to Help

As organizations increasingly embrace cloud resources, invest in new applications, and grow, new risks and complexities emerge. Okta helps organizations combine SSO, Universal Directory, and MFA solutions to unify identity and access management while applying strong authentication policies. These solutions enable secure, automated processes to help customers scale, increase productivity, and provide great user experiences.

Customer Spotlight

MEDALLIA ThoughtWorks® nexteer AUTOMOTIVE Pivotal