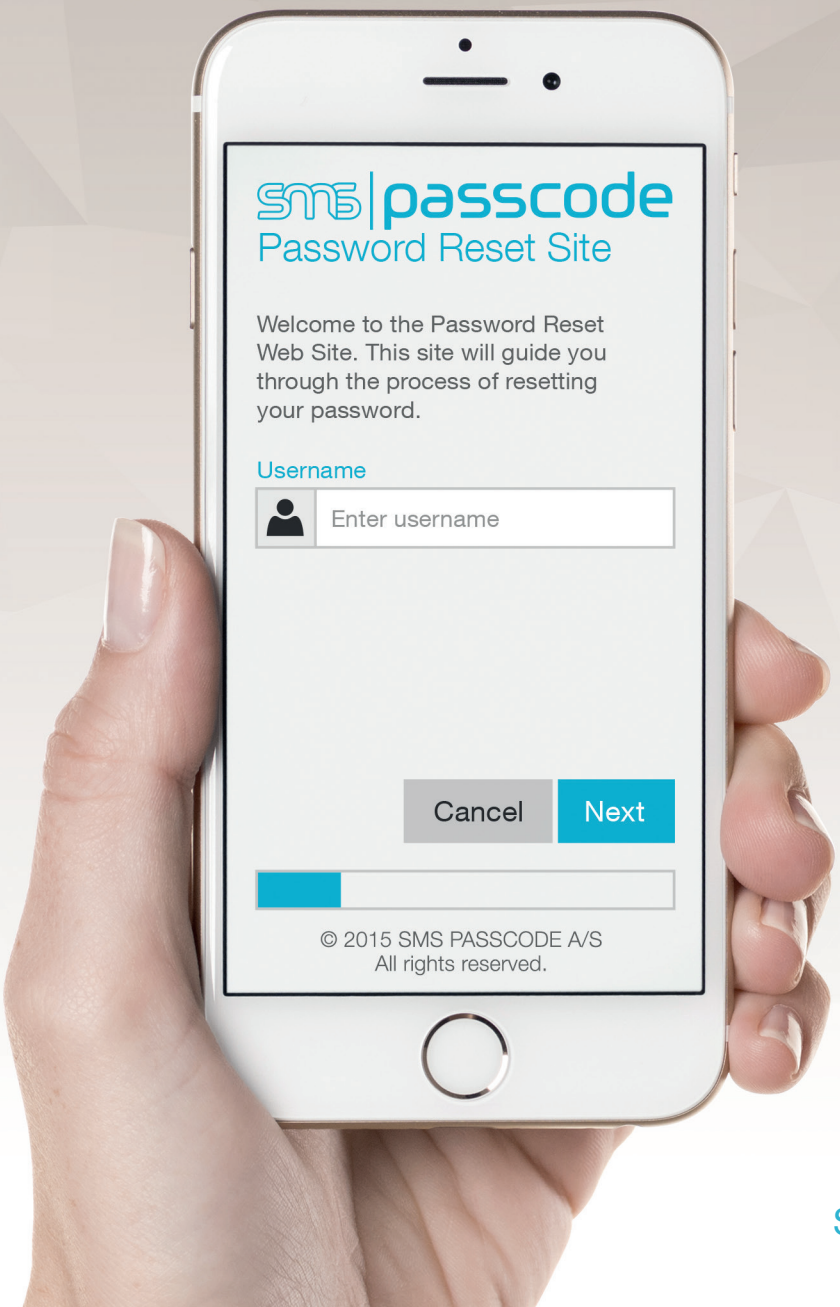
sms passcode
adaptive user authentication

Password Reset Module

Empower the users. Recharge your help desk.



Solutions Brief →

SMS PASSCODE offers a game chang
change passwords directly from their m
process, it instantly notifies users when
proactively sends out notifications whe

ging solution that allows users to
mobile phones! Integrated in the login
n they forget their passwords and it
en passwords are about to expire.

Today users must change passwords on a frequent basis. On top of that, password policies demand complex combinations of letters, numbers and special characters while not allowing repetition of passwords. As a result users tend to forget their passwords and have to contact IT for help. In fact password reset calls can be quite a burden for the IT help desk and statistics suggest that 30-50 percent of all help desk calls, are related to password problems.

SMS PASSCODE offers an intuitive self-service process that includes automated user notification. Here is how it works: The user receives a text message that explains the issue and gives instructions on how to resolve the problem. The notification includes a link to the self-service website where the user can immediately resolve the problem via their mobile phone or any other device with Internet access and a web browser.

Solutions Out There

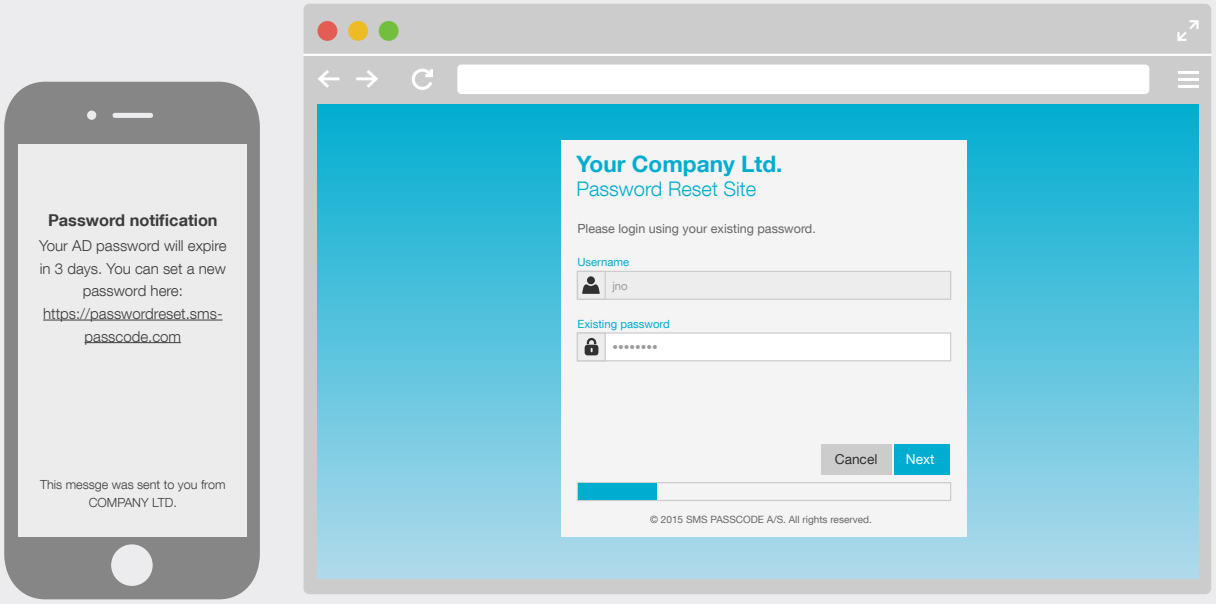
A number of self-service password reset solutions exist, with only subtle differences. Often these solutions come as part of an identity management system. And typically they rely on having to install a software client on each user's device or require the users to answer a list of challenge questions like "what is your favorite food?" or "what is your favorite movie?".

The general objective is of course to maintain productivity, while offering burden relief to the help desk. In reality though these types of solutions tend to fail due to three common flaws:

1) Users never spend time on answering the challenge questions or they forget the answers they gave in the first place.

2) The software client has not been installed, or the user is trying to connect from a device that has not been provisioned (e.g. a private iPad).

3) Most solutions only work at the office, which means that users trying to gain access from the outside – perhaps even outside business hours – cannot help themselves.



1

When a user's password is about to expire or in case of account lockout a notification is sent to the user's mobile phone via SMS text message.

2

The message includes a link to the password reset website. The user will be guided through the reset/ renewal process after appropriate authentication.

A Game Changing Approach

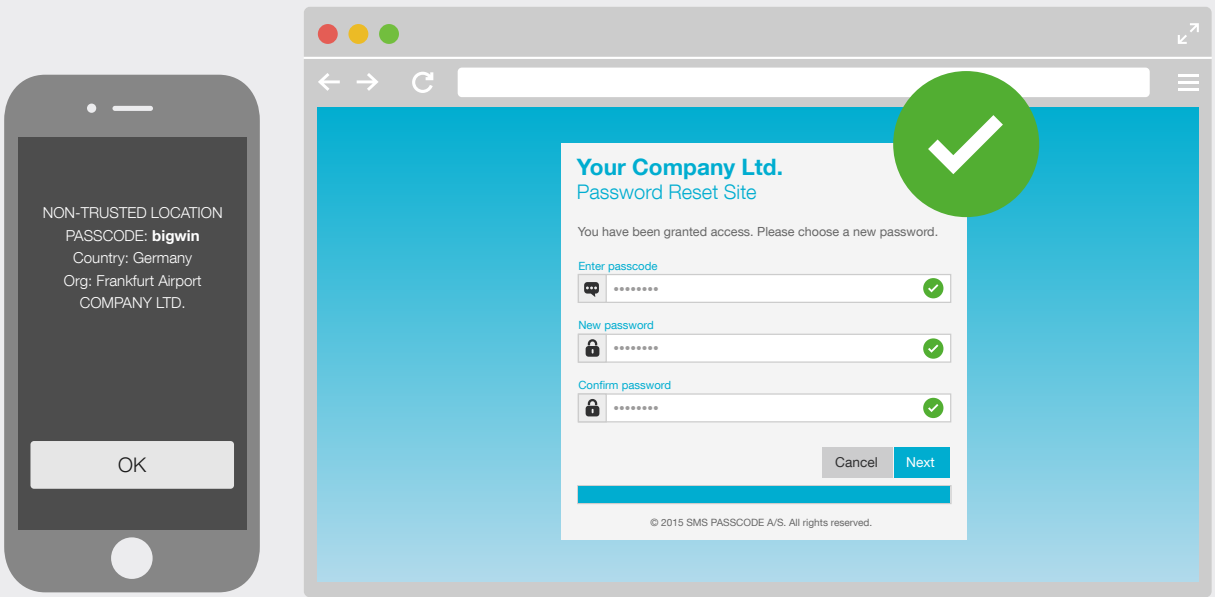
SMS PASSCODE took a thorough look at this category, and found that there was room for improvement. Based on SMS PASSCODE's patented and unique ability to verify the identity of users in real-time comes a solution that is easy for IT to deploy, requires no training of the users, and is so intuitive that it significantly reduces the impact of forgotten passwords.

You need a self-service password reset solution in three different situations;

Windows logon: When logging into Windows at the office and you have forgotten your password - typically after a weekend or holiday. In this case the solution detects that you are logged out from AD (ActiveDirectory) and immediately sends you a notification with a link to change your AD password.

Password expiry: If you either ignore the password expiration alerts or you don't get the messages because you are not on the LAN (working from home, traveling, etc.). In this case the solution sends you a notification with a link to change your password.

Remote access: When you are trying to use Citrix, VPN, OWA or similar from a remote location but have forgotten your password. In this case the solution detects that an invalid password is entered and sends you a notification with a link to reset your password.



3

When the user's identity has been validated by the system he/she will be asked to enter and confirm the new password.

4

The process - beginning to end can be done in less than a minute, ensuring that the user is quickly back online without support.

Key Benefits of the Solution

Get the user back online: Automated user notifications ensure that the user quickly realizes the need to reset his/her password and guide the user to the self-service website to resolve the problem without any hassles.

Intuitive user experience: Provides users with a straight forward and reassuring process for verifying their identities and resetting passwords in Active Directory.

Expiration notification: The user automatically receives an SMS i.e. three days before password expiration, including a link the password reset self-service site. The user is guided through the process of renewing his/her password.

Lockout notification: When a user tries to log-in remotely using VPN, Citrix, Webmail or similar and mistypes the password three times, a lockout notification is sent via SMS to the user with a link to the self-service web site.

Easy roll out: Password Reset Module is installed and maintained centrally, making it very easy to roll out. No need for additional user instructions or device installations, leaving zero footprint.

Tight AD integration: Allows you to grab relevant user information like employee ID, phone number, department code etc. directly from Active Directory. It is however also possible to perform mass-enrollment by asking users to provide relevant account information.

Reduce help desk requests: By empowering the users to take action themselves the burden on the help desk is reduced, allowing them to focus resources on more “high priority” tasks.

Context Based Authentication

Password Reset Module offers three security modes; Simple, Flexible and Strict. In Simple-mode authentication with username and OTP (one time passcode) is required. This would typically be used on-premise only. In Flexible-mode the system dynamically adapts the security level based on the whereabouts of the user. To endorse the highest possible security level, turn on Strict-mode. Strict-mode dictates both users in the office and remote users to authenticate with username, OTP and an additional factor.

The Business Case

Usually 30-50 percent of help desk calls are password reset related. In an organization with 10,000 users you probably have about 10-20,000 password related calls annually. At a cost of $10-20 per call this sums up to **an annual cost of up to $200,000**.

Taking into account the added productivity on the user side, and the burden relief on the help desk side, the annual benefit is at least the same dollar-amount by reducing the number of password related help desk calls by just 50 percent. And by introducing password change notifications this reduction is easily achieved.

For more information visit: **www.smspasscode.com/passwordreset/**

www.smspasscode.com

sms passcode
adaptive user authentication

PRM 01-1 2015