# SecurPassword

**Tokenlose Zwei-Faktor-Authentifizierung, mit der der User sein Passwort selbst zurücksetzen kann.**

## Keine Helpdesk-Anrufe mehr!

***SecurPassword*** ermöglicht es den Usern, ihr Domain-Passwort mithilfe eines bestehenden persönlichen Geräts und zusammen mit einigen zuvor hinterlegten geheimen Fragen zum Identitätsnachweis, in Echtzeit zurückzusetzen.*

Angesichts unserer zunehmenden Abhängigkeit von der IT wird die Komplexität und Anzahl der Passwörter pro User zur echten Last. Jedes Mal, wenn ein Passwort geändert wird, werden IT-Helpdesks für gewöhnlich von frustrierten Usern, die sich aus ihrem Netzwerk ausgesperrt haben, geradezu bombardiert. ***SecurPassword*** bietet einen revolutionären Ansatz in Sachen Passwortsicherheit.

## Features

***SecurPassword*** kann als standortbasierte Softwarelösung oder als Managed Service von Ihrem MSP bereitgestellt werden:

- Passwörter werden mithilfe der tokenlosen Zwei-Faktor-Authentifizierung zurückgesetzt
- Identifizieren Sie sich mithilfe Ihres Mobiltelefons, bevor Sie das Passwort zurücksetzen
- Eine Benachrichtigung zum Ablauf des Passworts wird per SMS zugesandt
- Spart bis zu 90 % der laufenden Helpdesk-basierten Passwort-Resets
- Automatische Einbindung von Usern via LDAP-Gruppenmitgliedschaft
- Remote-Passwort-Reset via Browser
- Lokaler Passwort-Reset am Anmeldepunkt
- Fixe jährliche Kosten, Bezahlung pro Nutzer, keine versteckten Zusatzkosten

## Zwei-Faktor-Authentifizierung trifft auf selbständigen Passwort-Reset

Immer häufiger werden User dazu aufgefordert, ihr Passwort zu ändern und ein sichereres, d.h. komplexeres, Passwort zu erstellen. Das sorgt nicht selten für Verwirrung und Verlust von Passwörtern und stellt eine Herausforderung für den IT-Helpdesk dar – je größer das Unternehmen, desto höher die Belastung.

Wird ein Passwort vergessen, so bedeutet das nicht nur, dass dem User geholfen werden muss, es zurückzusetzen, es bedeutet auch, dass der User als derjenige identifiziert werden muss, der er zu sein angibt. Durch Einführung eines Zwei-Faktor-Authentifizierungsverfahrens als Self-Service ist der User selbst für den Prozess verantwortlich und in der Lage, sein Passwortproblem ohne Zuhilfenahme des Helpdesks zu lösen.

Über eine automatisierte Selbsthilfe-Webseite oder über die GINA-Anmeldung können die User ihr Passwort mithilfe der Zwei-Faktor-Authentifizierung zurücksetzen, indem sie aufgefordert werden, eine geheime Frage zu beantworten und entsprechend das Authentifizierungsgerät ihrer Wahl verwenden. Alternativ zur Beantwortung der geheimen Fragen können die User dazu aufgefordert werden, andere Informationen, wie beispielsweise ihre Mitarbeiternummer oder sonstige Angaben, die in der User-Repository hinterlegt sind, einzugeben.

Nach erfolgter Authentifizierung wird der User aufgefordert, ein neues Passwort einzugeben, das die unternehmensspezifischen Passwortregelungen erfüllt. ***SecurPassword*** setzt dann das Passwort in Echtzeit zurück.

Viele Unternehmen berichten, dass sich die Anschaffung des ***SecurPassword*** schnell bezahlt macht, wobei bei einigen von ihnen die Anfragen an den Helpdesk zum Reset von Passwörtern um 100 % zurückgegangen sind.


*User haben ein einziges Profil, mit dem sie jeweils nur auf einem Gerät aktiv sein können.

# *Flexible Authentifizierung*

**SecurEnvoy sind die Pioniere in der tokenlosen Zwei-Faktor-Authentifizierung. Unsere innovativen Lösungen bieten bequeme und sichere Authentifizierungsmöglichkeiten zu einem Bruchteil der Kosten tokenbasierter Alternativen und wurden bereits tausenden von Usern weltweit bereitgestellt.**

## *Der User hat die Wahl*

Wir sind der Meinung, dass der User selbst wählen können sollte, welches persönliche Gerät er zur Authentifizierung nutzen möchte, ob Mobiltelefon, Tablet-PC, Laptop oder sogar das Festnetztelefon. User sollten die Möglichkeit haben, ihre Einzelidentität von Gerät zu Gerät tragen zu können, ohne dass ihre Identität aufgrund veralteter Technologie auf der Strecke bleibt.

## *Eine Welt ohne Hardware-Tokens*

Hardware Tokens, vor über 30 Jahren erstmalig erschienen, stehen der Massenverbreitung der Zwei-Faktor-Authentifizierung im Wege, da sie kostenintensiv in der Bereitstellung und im Betrieb sind und sich nicht leicht skalieren lassen. Man kann nicht erwarten, dass der User für jeden Geschäftszweck – ob beruflich, für Bankgeschäfte oder Sonstiges – für den er sich einloggen muss, einen anderen Token benutzt, den er bei sich tragen muss. Die klare Antwort liegt auf der Hand: Er sollte dazu ein persönliches Gerät benutzen können, das er ohnehin bei sich trägt.

Als Originalerfinder der tokenlosen Authentifizierung ist es unser Ziel, weiterhin innovative Lösungen zu entwickeln, die sich die persönlichen Geräte der User zunutze machen und die Probleme lösen, die der umfassenden Verbreitung der Technologie hinderlich sind, wie beispielsweise Verzögerungen in der Übermittlung von SMS, fehlender Empfang oder Probleme bei der Synchronisierung.

## *Elegant und simpel*

Wir sind der Meinung, dass sich die Anmeldung so simpel wie möglich gestalten sollte und dass sich tausende von Usern sicher mit einem Mausklick anmelden können sollten. Unsere Designs greifen auf bestehende Infrastrukturen zurück, wie z. B. Active Directory als zentrale Datenbank, um simple, elegante Lösungen zu bieten.

*SecurEnvoy plc* | info@SecurEnvoy.com | www.SecurEnvoy.de