

Self Service Reset Password Management (SSRPM)

De nummer 1 van helpdesk call is het resetten van het wachtwoord voor een gebruiker. Vooral na de vakantieperiode maar ook na het weekend vergeten gebruikers hun wachtwoord en bellen ze de helpdesk voor het resetten van het wachtwoord. Met de invoering van een complex (moeilijk te onthouden) wachtwoord, wordt dit probleem verder vergroot. Het grote aantal calls naar de helpdesk voor het resetten van wachtwoorden betekent een hoge beheerslast voor de IT-afdeling. Daarnaast zijn gebruikers minder productief omdat zij geen toegang hebben tot het netwerk.

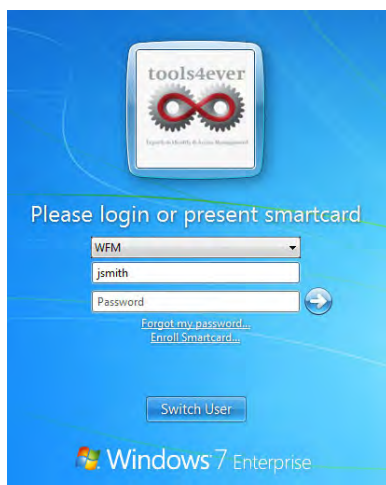
Met Self Service Reset Password Management (SSRPM) van Tools4ever kunnen eindgebruikers zelf hun wachtwoord resetten aan de hand van een aantal vastgestelde vragen, zoals 'Wat was de naam van uw eerste huisdier?' Zij hoeven niet langer te wachten totdat de helpdesk hun verzoek voor een password reset heeft behandeld. Hiermee wordt zowel productiviteit van eindgebruikers verbeterd als het aantal calls naar de helpdesk gereduceerd.

Hoe werkt SSRPM?

De basis van SSRPM is dat een gebruiker haar of zijn identiteit bevestigt door het beantwoorden van een aantal persoonlijke vragen en vervolgens zijn account kan unlocken of zelf een nieuw wachtwoord kan opgeven. De vragen zijn zodanig opgesteld dat de antwoorden zeer moeilijk sociaal te rechercheren zijn. De gebruiker heeft de vragen ooit eerder beantwoord toen de gebruiker nog normaal kon inloggen.

De eindgebruiker heeft toegang tot SSRPM via een button ("Wachtwoord vergeten") op alle inlogschermen (Windows 7, Vista XP, Outlook Web Acces, Citrix, etc.) of via een webformulier op het intranet.

SSRPM is zeer flexibel en nagenoeg alle denkbare configuratie-opties zijn mogelijk. De systeembeheerder kan de instellingen maken via een beheerdersconsole die vanaf een willekeurig werkstation gedraaid kan worden. Voorbeelden van instellingen zijn: zelf definiëren of veranderen van vragen, bepalen van complexiteit van het antwoord (lengte, zichtbaarheid, uitsluiten woorden, uitsluiten herhalingen, etc.) en bepalen wie en welk werkstation de toegang krijgt tot SSRPM.

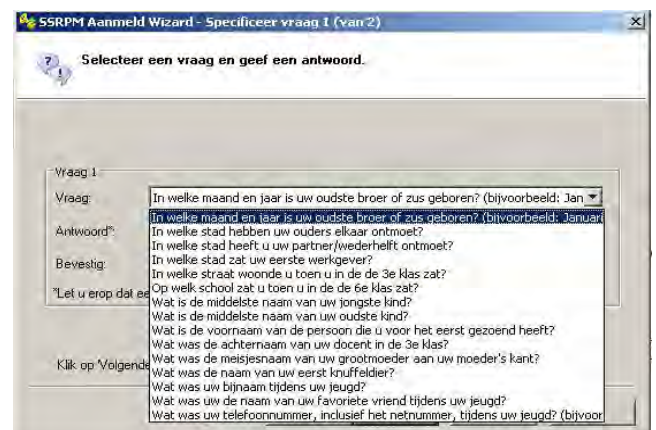


SSRPM bestaat uit drie delen:

- ▶ Een centrale Windows Service die de centrale afhandeling doet van de SSRPM instellingen (welke vragen, security instellingen, ed.) en de antwoorden van de gebruikers bijhoudt. De centrale service verifieert of de gegeven antwoorden juist zijn en voert de daadwerkelijk unlock of wachtwoord reset uit.
- ▶ De aanpassing op ieder loginscherm met een knop "Wachtwoord vergeten..." en een webformulier voor het intranet. Via deze interface kan de eindgebruiker de vragen beantwoorden en een unlock of een wachtwoord reset verzoeken aan de centrale serverservice.
- ▶ Een console voor de systeembeheerder waarmee de systeembeheerder instellingen kan doorvoeren op de centrale service en het wachtwoordproces kan monitoren en beheersen. De console kan vanaf ieder werkstation worden gedraaid.

Belangrijkste voordelen SSRPM

- ▶ Reductie van wachtwoord gerelateerde calls naar de helpdesk met 90%;
- ▶ Eindgebruikers blijven productief omdat zij niet hoeven wachten op een nieuw wachtwoord;
- ▶ Verbetering van helpdesk service level door 24/7 aanbieden van wachtwoord reset;
- ▶ Eliminatie van frauduleuze aanvragen voor een wachtwoord reset;
- ▶ Naleven compliancy dankzij SSRPM audit log.



Technical features

Installatie

- ▶ Installatie mogelijk in minder dan twee uur;
- ▶ Instructies beschikbaar om werking toe te lichten aan eindgebruikers (enrollment plan).

Configuratie

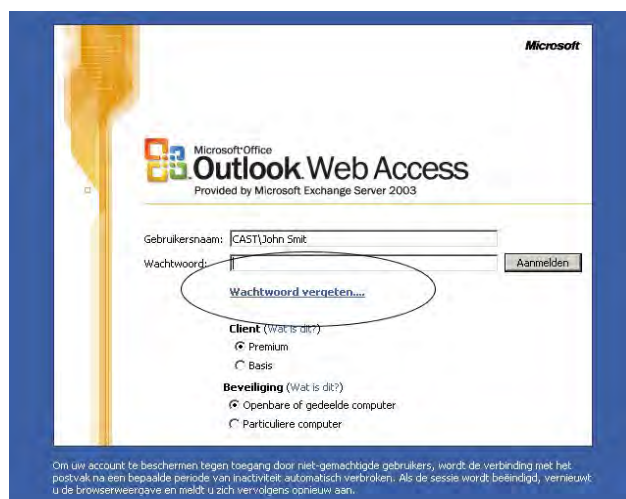
- ▶ Configuratie mogelijk per domain of OU;
- ▶ De GUI van de Admin Console, configuratie en rapportagemogelijkheden kunnen naar wens worden aangepast;
- ▶ Complexiteit van het wachtwoord is aanpasbaar;
- ▶ Alle denkbare opties met betrekking tot de vragen en antwoorden zijn instelbaar, de lengte van de antwoorden, hoeveelheid vragen, de vragen zelf, de taalkeuze, complexiteit van de antwoorden, etc.

Security

- ▶ Antwoorden van eindgebruikers worden encrypted en onomkeerbaar opgeslagen in de SSRPM database;
- ▶ Verschillende beveiligingsniveaus kunnen worden ingesteld, van zwak tot sterk;
- ▶ Authenticatie via e-mail (ontvangen van PIN-code) en SMS worden ondersteund (two-factor authentication).

Overig

- ▶ Gedetailleerde rapportage mogelijkheden over alle aspecten van het wachtwoord reset proces. Bijvoorbeeld: status enrollment, uitgevoerde wachtwoord resets, wie heeft wanneer vragen verkeerd beantwoord, in SSRPM geblokkeerde gebruikers, etc. De rapportages kunnen automatisch gegenereerd en beschikbaar gesteld worden op het intranet of ge-e-mailed worden naar systeembeheer;
- ▶ Multi-platform ondersteuning, wachtwoorden kunnen op alle denkbare applicaties en systemen gereset worden;
- ▶ E-mail notificatie naar beheerders mogelijk wanneer een event zich voordoet. Bijvoorbeeld als een gebruiker meerdere keren verkeerde vragen beantwoordt;
- ▶ Het is mogelijk om bepaalde SSRPM-systeembeheertaken op een veilige manier te delegeren naar een medewerker van de helpdesk. Bijvoorbeeld het geforceerd uit laten voeren van een re-enrollment van een eindgebruiker.



Systemeisen

- ▶ **Hardware:**
Pentium 4 of hoger, tenminste 1 GB RAM, tenminste 1 GB diskruimte aanbevolen
- ▶ **Software:**
Windows Operating Systems (vanaf Windows 2000), zowel 32-bits als 64-bits, Windows Terminal Server, Citrix
- ▶ **Databases:**
MS Access, MS SQL 2000 of hoger (alle versies)

