

# Self Service Reset Password Management (SSRPM)

The single most frequent helpdesk call is a request to reset a user password. Particularly after the holiday period or weekends, users forget their passwords and phone the helpdesk to have them reset. The problem occurs even more frequently if complex (difficult to remember) passwords are used. The large volume of helpdesk calls involving passwords reset requests imposes a significant management burden on the IT department. Users also become less productive because they are denied access to the network.

Self Service Reset Password Management (SSRPM) by Tools4ever enables end-users to reset their passwords themselves by answering several predefined questions, such as 'What was the name of your first pet?' This means users will no longer have to wait for the helpdesk to handle their password reset request. That increases end-user productivity and reduces the number of helpdesk calls.

## How SSRPM works

The basic SSRPM procedure involves end-users confirming their identity by answering a series of personal questions. After providing the correct answers, they can unlock their user account or specify a new password themselves. The questions have been formulated in such a way that the answers are very difficult to obtain through social engineering techniques. The questions are those the user answered previously when he or she was still able to log in normally.

End-users can access SSRPM by clicking a button ('Forgot my password') in any login screen (Windows 7, Vista XP, Outlook Web Access, Citrix etc.) or through a web form on the Intranet.

SSRPM is a highly flexible solution supporting virtually any imaginable configuration option. Systems administrators can configure settings from a management console they can use on any workstation. Among other things, it is possible to define or modify user questions, to define the complexity of answers to questions (length, visibility, exclude words, exclude repetitions etc.) and to determine who and which workstation is able to access SSRPM.

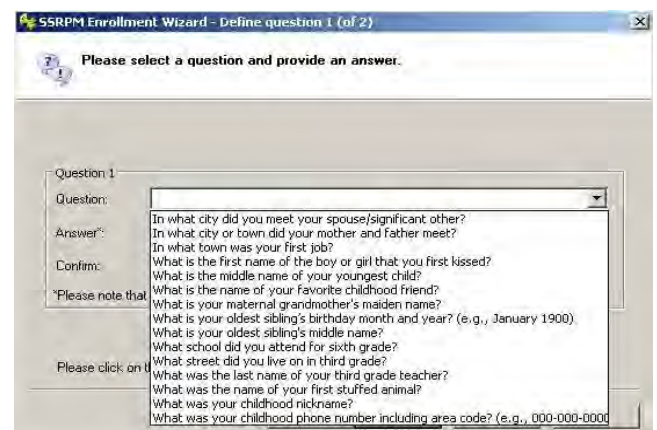
### SSRPM comprises three components:

- ▶ A central Windows service handles the SSRPM settings centrally (password questions, security settings etc.) and retains the answers to password questions provided by users. The central service verifies whether the answers are correct and handles the actual unlocking of accounts and password reset operations.
- ▶ The addition of the 'Forgot password ...' button to the login screen of each application and a web form for the Intranet. Through this interface, end-users can answer password questions or request that the central service unlock an account or reset a password.
- ▶ A management console allowing systems administrators to implement changes to the central service and monitor and control the password process. The console can be used on any workstation.

## Main benefits

**SSRPM**

- ▶ A 90% reduction in password-related helpdesk calls;
- ▶ End-users can remain productive because they won't have to wait for a new password;
- ▶ An improvement in the helpdesk's service level through 24/7 password reset support;
- ▶ Elimination of password reset requests by unauthorized parties;
- ▶ Compliance thanks to the SSRPM audit log.



# Technical features

## Installation

- ▶ The solution can be operational in less than two hours;
- ▶ End-users are provided with instructions (enrolment plan).

## Configuration

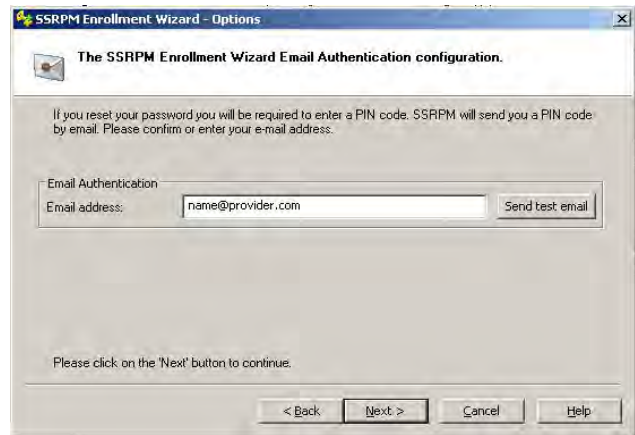
- ▶ Configuration per domain or OU;
- ▶ The GUI of the Admin Console, configuration and reporting capabilities can be customised at will;
- ▶ Password complexity can be modified;
- ▶ A virtually unlimited range of options for setting questions and answers, the length of answers, language choice, answer complexity etc.

## Security

- ▶ Answers by end-users are encrypted and stored irreversibly in the SSRPM database;
- ▶ Ability to set various security levels, from weak to strong;
- ▶ Support for authentication via e-mail (reception of a PIN code) and SMS messages (two-factor authentication).

## General

- ▶ Detailed reporting capabilities for all aspects of the password reset process, e.g. status enrolment, completed password resets, who provided an incorrect answer when, users blocked in SSRPM etc. The reports can also be generated and made available on the Intranet or e-mailed to the system administrators;
- ▶ Multi-platform support; ability to reset passwords for any application or system;
- ▶ Possibility of e-mail notification to managers in case of a particular event, e.g. when a user repeatedly provides the wrong answer to questions;
- ▶ Secure delegation of a select number of SSRPM system administration tasks to a helpdesk agent, e.g. to enforce the re-enrolment of an end user.



## System Requirements

- ▶ **Hardware:**  
Pentium 4 or higher, at least 1 GB RAM, at least 1 GB disc space recommended
- ▶ **Software:**  
Windows Operating Systems (from Windows 2000), 32-bits and 64-bits, Windows Terminal Server, Citrix
- ▶ **Databases:**  
MS Access, MS SQL 2000 or higher (all versions)

