

Self Service Reset Password Management

Administrator's Guide



Version 4.00 (9 February, 2007)

Copyright © Tools4ever 1998 - 2008
<http://www.tools4ever.com>



*Copyright © 1998 - 2007, Tools4ever B.V.
All rights reserved.*

No part of the contents of this user guide may be reproduced or transmitted in any form or by any means without the written permission of Tools4ever.

DISCLAIMER - Tools4ever will not be held responsible for the outcome or consequences resulting from your actions or usage of the informational material contained in this user guide. Responsibility for the use of any and all information contained in this user guide is strictly and solely the responsibility of that of the user.

All trademarks used are properties of their respective owners.

Contents

1.	Welcome to SSRPM	1
<hr/>		
2.	How does SSRPM work?	2
<hr/>		
2.1.	SSRPM concept	2
2.2.	SSRPM architecture	2
2.2.1.	The SSRPM Service	2
2.2.2.	The SSRPM Admin Console	3
2.2.3.	The SSRPM User Client Software	3
2.3.	SSRPM security	5
3.	SSRPM installation	6
<hr/>		
3.1.	System requirements	6
3.2.	General installation	6
3.3.	The SSRPM Service installation	6
3.4.	The SSRPM User Client Software installation	7
3.4.1.	Evaluation installation	8
3.4.2.	Manual installation	9
3.4.3.	Distributed installation	10
4.	Using SSRPM	11
<hr/>		
4.1.	SSRPM Admin Console	11
4.1.1.	The dashboard overview	11
4.1.2.	The 'Enrolled Users' overview	12
4.1.3.	The 'Not-Enrolled Users' overview	12
4.1.4.	The 'Blocked Users' overview	13
4.1.5.	The 'Reports' overview	13
4.1.6.	SSRPM Profiles	13
4.2.	SSRPM Service	23
4.2.1.	Logging	23
4.2.2.	Database	23
4.2.3.	E-mail	23
4.2.4.	Security	24
4.2.5.	UMRA Connector	24
4.3.	SSRPM User Client Software	27
4.3.1.	Service communication	27
4.3.2.	The SSRPM Enrollment Wizard	28
4.3.3.	The SSRPM Reset Wizard	31
4.3.4.	Registry Settings	34
5.	Multilingual support	35
<hr/>		
5.1.	SSRPM User Client Software User Interface	35
5.2.	Questions	36
5.2.1.	Use the default language (English)	36
5.2.2.	Use another language	36
5.2.3.	Use multiple languages	37
5.2.4.	Translation	37

6.	Frequently Asked Questions (FAQ)	39
-----------	-----------------------------------------	-----------

7.	Appendices	41
7.1.	Appendix A: Windows services.....	41
7.1.1.	What is a service?	41
7.1.2.	The service account.....	41
7.1.3.	Service communication	41
7.2.	Appendix B: Group Policy Objects	42
7.2.1.	What is a Group Policy Object?.....	42
7.2.2.	GPO's in SSRPM	42
7.3.	Appendix C: SSRPM keywords	43

8.	Glossary	46
-----------	-----------------	-----------

9.	Index	48
-----------	--------------	-----------

1. Welcome to SSRPM

Welcome to Self Service Reset Password Management (from here on the abbreviation 'SSRPM' will be used). SSRPM is an application which allows users to reset their own (Active Directory) passwords. This eliminates the need for a helpdesk and/or system administrator to service these requests when a user has forgotten his or her password.

SSRPM provides:

- Less involvement of IT staff

Users can reset their password without having to wait until the helpdesk or system administrator can service their requests. This will drastically reduce the number of calls to your helpdesk.

- Immediate return of investment (ROI)

Password resets and user ID issues are responsible for 15 to 35 percent of all helpdesk calls. Using SSRPM these calls will be reduced close to zero.

- Reduction of user downtime

With locked-out users having faster access to the network again, user downtime is strongly reduced.

- Increased security

Security is increased by eliminating possible helpdesk errors. Furthermore, users will not have to write down passwords. Security threats such as password guessing and break-ins will be minimized.

- Easy usability

Once a user has enrolled with the SSRPM Enrollment Wizard, resetting a password is simply a matter of clicking a button on the Microsoft Windows logon dialog box and answering a series of challenge questions.

2. How does SSRPM work?

2.1. SSRPM concept

The main idea of SSRPM is that a user can reset his or her own password, by answering a set of challenge questions like for example: "What is the name of your first partner?". When these questions are answered validly, which will be determined by the SSRPM service, the user is allowed to do a password reset.

To use SSRPM, all users must enroll into SSRPM. When a user is enrolled, he or she can reset his or her password via an additional 'Forgot My Password' button on the Windows Logon screen.

2.2. SSRPM architecture

The main architecture of SSRPM is shown in the figure below:

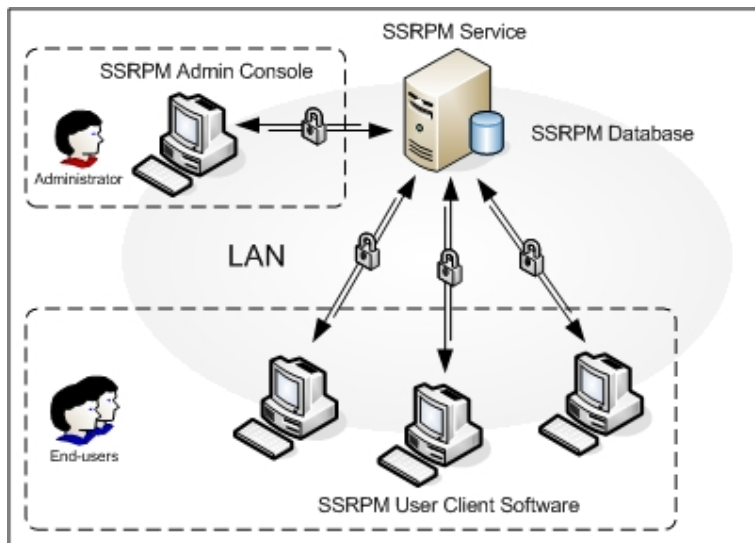


Figure 1: Communication between the different SSRPM components within a network

SSRPM is divided into three main software components, knowingly:

- The SSRPM Service (with the SSRPM Database)
- The SSRPM Admin Console
- The SSRPM User Client Software

2.2.1. The SSRPM Service

Like a normal service (see *Appendix A: Windows Services* on page 41, for more information about services), the SSRPM Service is running continuously in the background and handles requests from its clients, which are in this case: the SSRPM Admin Console and the SSRPM User Client Software.

Such a request can be, for instance, resetting a password or retrieving log information of current service actions which have taken place. Next to handling these requests, the SSRPM Service stores all questions and answers (encrypted) in an SSRPM database and can be fully configured by using the SSRPM Admin Console.

2.2.2. The SSRPM Admin Console

The SSRPM Admin Console is used by the system administrator and first of all guides you through the further installation and configuration of SSRPM (this will be explained within the chapter: *SSRPM Installation* on page 6). When SSRPM is installed completely, the SSRPM Admin Console can be used to configure SSRPM, in which the amount of challenge questions can be defined and security notification and settings can be setup.

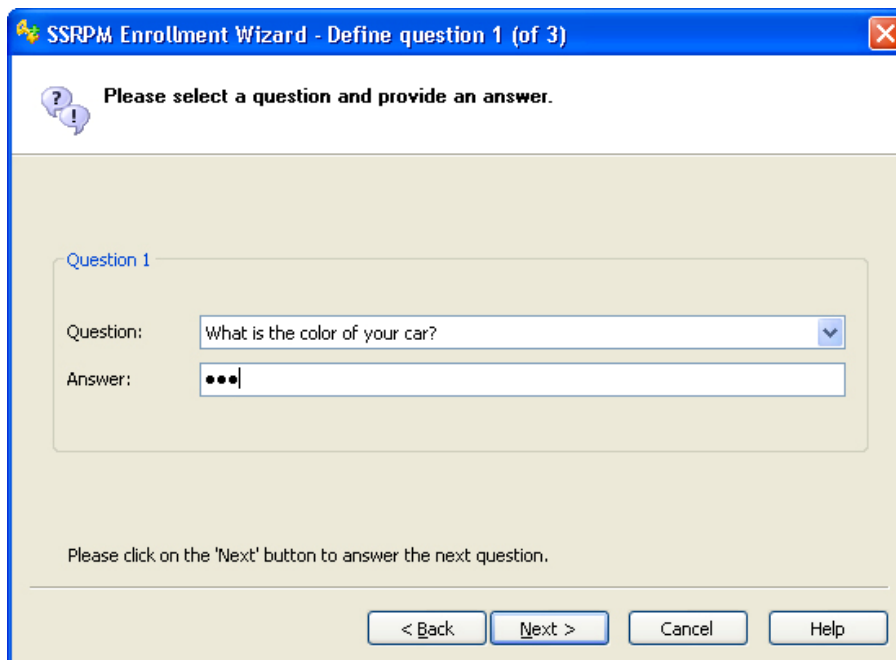
Through the dashboard, end-user overviews and a service log window, SSRPM can be monitored with the SSRPM Admin Console. In this way system administrators can get a clear and real-time overview about the status of enrollment (which users are enrolled, and which are not), password resets and user lockouts (blocked users) within SSRPM.

2.2.3. The SSRPM User Client Software

To make SSRPM available for the end-users within your network, these users must use specific SSRPM User Client Software, which consists of:

- The SSRPM Enrollment Wizard

Before an end-user can reset his or her password, it is necessary for each user to enroll into SSRPM with the SSRPM Enrollment Wizard. The enrollment consists of defining and answering a set of challenge questions.



The screenshot shows a Windows-style dialog box titled "SSRPM Enrollment Wizard - Define question 1 (of 3)". The dialog has a blue title bar with a question mark icon on the left and a close button on the right. Below the title bar, there is a message: "Please select a question and provide an answer." with a question mark and exclamation mark icon. The main area of the dialog is light beige and contains a section titled "Question 1" in blue. Inside this section, there is a "Question:" label followed by a dropdown menu showing "What is the color of your car?". Below that is an "Answer:" label followed by a text input field containing three black dots. At the bottom of the dialog, there is a message: "Please click on the 'Next' button to answer the next question." and four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 2: The SSRPM Enrollment Wizard

- The SSRPM Reset Wizard

When an end-user is enrolled into SSRPM, the user uses the SSRPM Reset Wizard to reset his or her password by answering his or her defined questions. This wizard is made available via a 'Forgot My Password' button at the bottom of the Windows logon dialog (or when running Windows Vista: via an extra 'Forgot My Password' link).



Figure 3: The SSRPM Reset Wizard

- The SSRPM GINA and SSRPM Credential Provider

For the creation of the extra 'Forgot My Password' button, an extension on top of the existing Windows logon software (GINA architecture) is needed. This is realized by the SSRPM GINA, which extends the Windows logon dialog with this extra functionality:



Figure 4: The SSRPM GINA DLL

In Windows Vista, the GINA architecture is replaced with a new Credential Provider model. Therefore, the SSRPM Credential Provider will be used instead of the SSRPM GINA, to provide the "Forgot My Password"-button functionality for Windows Vista. The SSRPM Credential Provider creates an extra 'Forgot My Password...'-link on the Windows Vista logon screen:



Figure 5: The SSRPM Credential Provider

The SSRPM Enrollment Wizard, SSRPM Reset Wizard, and SSRPM GINA (or SSRPM Credential Provider when running Windows Vista) will be installed on each client workstation of all end-users which must use SSRPM within one or more specified OU's.

2.3. SSRPM security

Because SSRPM is dealing with very sensitive information, like passwords and user answers, security is a very important issue. This is why SSRPM uses encrypted RPC as a communication protocol between the SSRPM Service, the SSRPM Admin Console and SSRPM User Client Software in the first place. In this way all information sent by SSRPM through your network is encrypted which transforms this information into an unreadable form.

The SSRPM Service stores all user data in an SSRPM database, which includes the user answers. It would be fairly unsafe to store these answers, and that's why (by default) only an MD5 encrypted irreversible hash value of each answer will be stored. This hash value can only be used by SSRPM when checking for answer validation (when a user resets his or her password).

Regarding its own functions, SSRPM can be configured at different security levels, which vary from weak to strong security. This can be very useful when you maintain different security requirements within several OU's in which you can let SSRPM act more secure.

3. SSRPM installation

3.1. System requirements

The system requirements of SSRPM are:

Operating Systems:

- Windows 2000 (all 32-bit versions with service pack 3 or higher installed)

Note: Windows Installer 2.0 or later is required when installing the SSRPM User Client Software.

- Windows XP (all 32-bit and x64 versions)
- Windows 2003 (all 32-bit and x64 versions)
- or Windows Vista

Minimal hardware:

- Processor: Pentium II/III 233 MHz or more, AMD K6-2/K6-III 266 MHz or more (300 MHz or more recommended)
- Memory: 128 Mb or more (256 Mb or more recommended)
- Hard disk space: 20 Mb or more (30 Mb or more recommended)

3.2. General installation

To install SSRPM, run the SSRPM setup executable, 'SetupSSRPM.exe', which is available for download from the *Tools4ever website* <http://www.tools4ever.com>. This executable contains all the needed SSRPM Software Components, knowingly: the SSRPM Admin Console, the SSRPM Service and the SSRPM User Client Software.

When the download is finished you can run 'SetupSSRPM.exe', which will start the SSRPM Setup Wizard. The wizard will guide you through the installation process of SSRPM, which by default only installs the SSRPM Admin Console.

Note: The user account which you'll use to install SSRPM must have administrative privileges on the target computer on which you want to install SSRPM.

Once you've finished the installation of SSRPM you can start the SSRPM Admin Console to continue with the further installation and configuration of SSRPM. When you've started the SSRPM Admin Console for the first time, the SSRPM Startup Wizard will be shown, which guides you through the installation of the SSRPM Service (see chapter: *The SSRPM Service Installation* on page 6) and the SSRPM User Client Software (see chapter: *The SSRPM User Client Software Installation* on page 7).

3.3. The SSRPM Service installation

Because you can't use SSRPM without a running service, you must install the SSRPM Service with the SSRPM Admin Console. If you've installed the SSRPM Service before, you can skip the SSRPM Service Installation Wizard. In this case you may want to continue reading at the next chapter: *The SSRPM User Client Software Installation* on page 7.

The SSRPM Service Installation wizard installs and starts the SSRPM Service. To upgrade or remove the SSRPM Service later on, the SSRPM Service Installation Wizard can be used as well.

Within the SSRPM Service Installation Wizard, there are a few settings which you can specify, knowingly:

- The target computer, which is the computer on which you want to install the SSRPM Service. This is most likely a server or the same machine on which you're running the SSRPM Admin Console, which is specified by default.
- The installation directory, in which the SSRPM Service will be installed on the specified target computer. All SSRPM Service files including the SSRPM Database will be copied to this directory.
- The SSRPM Communication Port (see: *Appendix A: Windows Services* on page 41); the communication port which the SSRPM Admin Console and the SSRPM Service will use to communicate.
- The SSRPM Service Account (see: *Appendix A: Windows Services* on page 41), which is a user account with enough privileges to be able to reset passwords within the domain of which the specified target computer is a member of (or the OU in which the computer is located). When this account does not exist already, it will be created automatically for you. When the SSRPM Service starts, it will logon with this user account.
- The SSRPM Service Account Group; The SSRPM Service Account is configured as a member of this group. Through this group the service account should be granted access rights to actually reset the password of all target end-user accounts.
- The SSRPM Administer Group; a user group which is allowed to administer the SSRPM Service with the SSRPM Admin Console. Only the users, who are a member of this user group, can use the SSRPM Admin Console to configure or manage the SSRPM Service due to security reasons.
- E-mail configuration, which the SSRPM Service uses for sending notification e-mails (for instance, when a user resets his or her password).

Note: When running the SSRPM Service Installation Wizard, you must have administrative privileges on the specified target computer, so that the SSRPM Service can be installed and a service account can be created.

When the SSRPM Service Installation Wizard has completed successfully, the SSRPM Service has been started and will be running on the target computer (within the security context of the SSRPM Service Account).

You can see the running service in the services window (via: Start -> Run -> Services.msc):

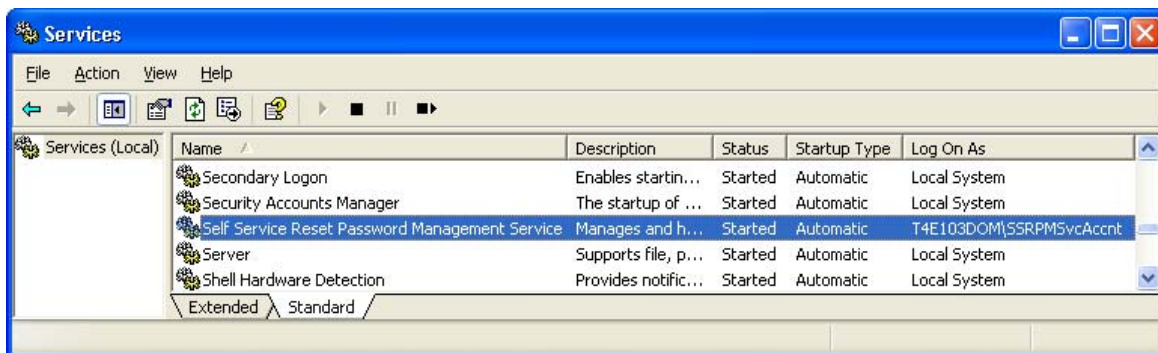


Figure 6: The running SSRPM Service within the Microsoft Services Window

3.4. The SSRPM User Client Software installation

Note: When you're running the SSRPM Admin Console Startup Wizard, you can select the language in which the end-users must see the questions presented to them. By default, the English language will be used for these questions. See chapter *Questions* on page 36 if you want to support other languages than English.

The SSRPM User Client Software must be installed on each workstation on which you want to use SSRPM to reset a user password.

This software contains the SSRPM Enrollment Wizard, the SSRPM Reset Wizard, the SSRPM GINA and SSRPM Credential Provider (for Windows Vista), and can be installed in three different ways, knowingly:

- Evaluation Installation (recommended, see chapter: *Evaluation Installation* on page 8), with the SSRPM Admin Console Startup Wizard;
- Manual Installation (see chapter: *Manual Installation* on page 9), with the shipped MSI-package; ('SsrpmUserClientSoftware.msi')
- Distributed Installation (see chapter: *Distributed Installation* on page 10), with the help of Group Policy Objects (GPO's).

Each of these ways will be explained within this paragraph, which starts with the most common way; the evaluation installation.

Note: When you're running the SSRPM Admin Console Startup Wizard, and you don't want to use SSRPM for evaluation purposes, you can skip the evaluation install by selecting the 'Nothing' option within the evaluation wizard page. This will end the SSRPM Admin Console Startup Wizard. In this case you may want to continue reading at the next paragraph: *Manual Installation* on page 9 or *Distributed Installation* on page 10.

3.4.1. Evaluation installation

For this installation you must start the SSRPM Admin Console Startup Wizard, which is started automatically on the first use of the SSRPM Admin Console. After the SSRPM Service Installation within the SSRPM Admin Console Startup Wizard (which is described in the previous paragraph: *The SSRPM Service Installation* on page 6), you will be presented a list of evaluation options. These evaluation options determine the way the SSRPM User Client Software will be installed.

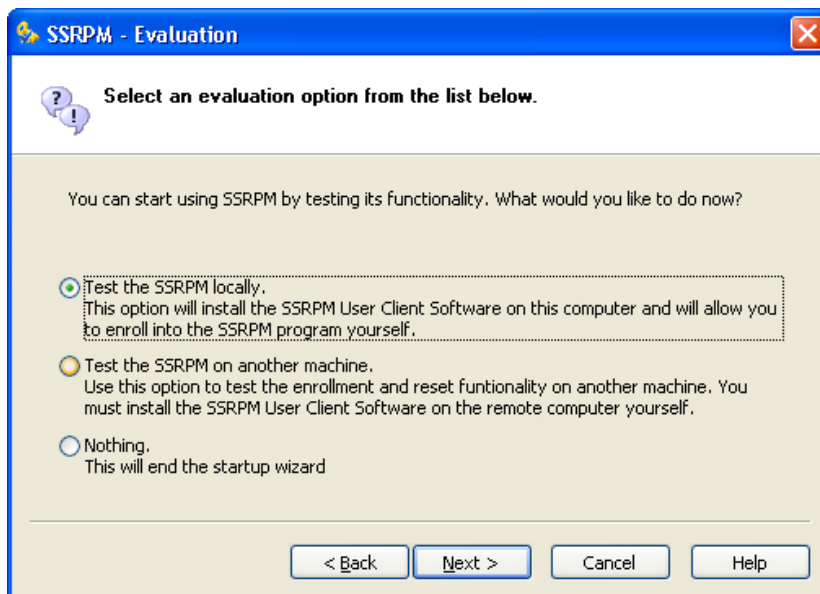


Figure 7: Evaluation options shown from the SSRPM Admin Console Startup Wizard

To evaluate SSRPM, you must choose between the first two evaluation options: 'Test SSRPM locally' or 'Test SSRPM on another machine'.

Both options will be described within this paragraph, starting with the first option.

Test SSRPM locally

When you want to test SSRPM on the same computer on which you've installed the SSRPM Admin Console, you must choose to test SSRPM locally, which is divided into the following actions:

1. Select a domain or OU for which you want to enable SSRPM, which is by default the domain of which the currently logged on user is a member of.

Note: The selected domain or OU will be assigned to the 'Default Profile' SSRPM Profile and will use the configuration stored in this SSRPM Profile. See paragraph *SSRPM Profiles* on page 13 for more information.

2. Install the SSRPM User Client Software on the local computer, which will be performed automatically by the SSRPM Admin Console Startup Wizard.
3. Enroll into the SSRPM program, using the SSRPM Enrollment Wizard. The SSRPM Enrollment wizard can be started immediately throughout the SSRPM Admin Console Startup Wizard if you want to enroll as the currently logged on user. To read more about how to use the SSRPM Enrollment Wizard, you may want to read chapter: *The SSRPM Enrollment Wizard* on page 28.
4. Reboot the computer, which can be done immediately when the SSRPM Admin Console Startup Wizard is finished. This is required to add the extra 'Forgot My Password' button on the Windows logon screen.
5. Reset a user password, via the extra 'Forgot My Password' button at the bottom of the windows logon screen using the SSRPM Reset Wizard.

Note: When running Windows Vista, an extra 'Forgot My Password' link will appear on the Windows Vista logon screen, which provides the same functionality.

To read more about how to use the SSRPM Reset Wizard, you may want to read chapter: *The SSRPM Reset Wizard* on page 31.

Note: If you want to test SSRPM with another user (for instance a test-user), you first must enroll as this user before performing a reboot. To do this, you must logon as this user, which will start the SSRPM Enrollment Wizard automatically when the user is logged on.

Test SSRPM on another computer

If you want to test SSRPM on a different computer than the computer on which you've installed the SSRPM Admin Console, you must choose to test SSRPM on another computer, which is divided into the following steps:

1. Select a domain or OU for which you want to enable SSRPM, which is by default the domain of which the currently logged on user is a member of.

Note: The selected domain or OU will be assigned to the 'Default Profile' SSRPM Profile and will use the configuration stored in this SSRPM Profile. See paragraph *SSRPM Profiles* on page 13 for more information.

2. Install the SSRPM User Client Software on the remote computer, which is explained in the SSRPM Admin Console Startup Wizard's Summary.

3.4.2. Manual installation

To perform a manual installation, you must run the SSRPM User Client Software Installer (on each workstation on which you want to use SSRPM) yourself. This installer is shipped with SSRPM as an MSI-package (called: 'SsrpmUserClientSoftware.msi') and can be found in the SSRPM subdirectory: 'Admin Console' which is located within your installation directory (this is by default: 'C:\Program Files\Tools4ever\SSRPM').

To install the SSRPM User Client Software manually, perform the following actions when you've located the MSI-package:

1. Copy the installer to the target computer (if the target computer is not the same computer on which you're running the SSRPM Admin Console)
2. Install the SSRPM User Client Software on target computer by running the MSI-package.

3. Run the Enrollment Wizard, which can be found at 'All Programs -> Tools4ever -> SSRPM -> Enrollment Wizard' in the Start menu. To read more about how to use the SSRPM Enrollment Wizard, you may want to read chapter: *The SSRPM Enrollment Wizard* on page 28.
4. Reboot the remote machine.
5. A 'Forgot my password' button should appear at the bottom of the login screen. Press this button which starts the SSRPM Reset Wizard to reset a user's password.

Note: When running Windows Vista, an extra 'Forgot My Password' link will appear on the Windows Vista logon screen, which provides the same functionality.

To read more about how to use the SSRPM Reset Wizard, you may want to read chapter: *The SSRPM Reset Wizard* on page 31.

Note: When you've installed the SSRPM User Client Software on one or more workstation(s), please make sure that you've enabled SSRPM for the current domain or organizational unit (OU) of which the users which log on to these workstations are a member of. This can be done by assigning profiles to each OU or the domain in which you want to enable SSRPM. See paragraph *SSRPM Profiles* on page 13 for more information about SSRPM Profile Assignment.

3.4.3. Distributed installation

Instead of installing the SSRPM User Client Software manually on each workstation, it is possible to distribute the SSRPM User Client Software automatically to each of these workstations. This can be done by using so-called Group Policy Objects (see: *Appendix B: Group Policy Objects* on page 42), and can save you a lot of time when installing SSRPM through your network.

See the "GPO Distribution Guide" for more information, of which the latest version is available on the *Tools4ever website* <http://www.tools4ever.com>.

4. Using SSRPM

4.1. SSRPM Admin Console

When you've successfully installed SSRPM (including the SSRPM User Client Software), SSRPM is ready for use. From this point SSRPM is running with default settings, which you may want to reconfigure with the SSRPM Admin Console. With the SSRPM Admin Console you can configure the SSRPM Service.

SSRPM can be monitored with the SSRPM Admin Console, for which several overview windows are available starting with the dashboard overview.

4.1.1. The dashboard overview

Each time when you start the SSRPM Admin Console, you'll immediately see a quick and real-time overview of the current status of SSRPM through the dashboard overview. Within this overview you can 'drill-down' to more detailed status information via links which are available on each information table, see the figure below:

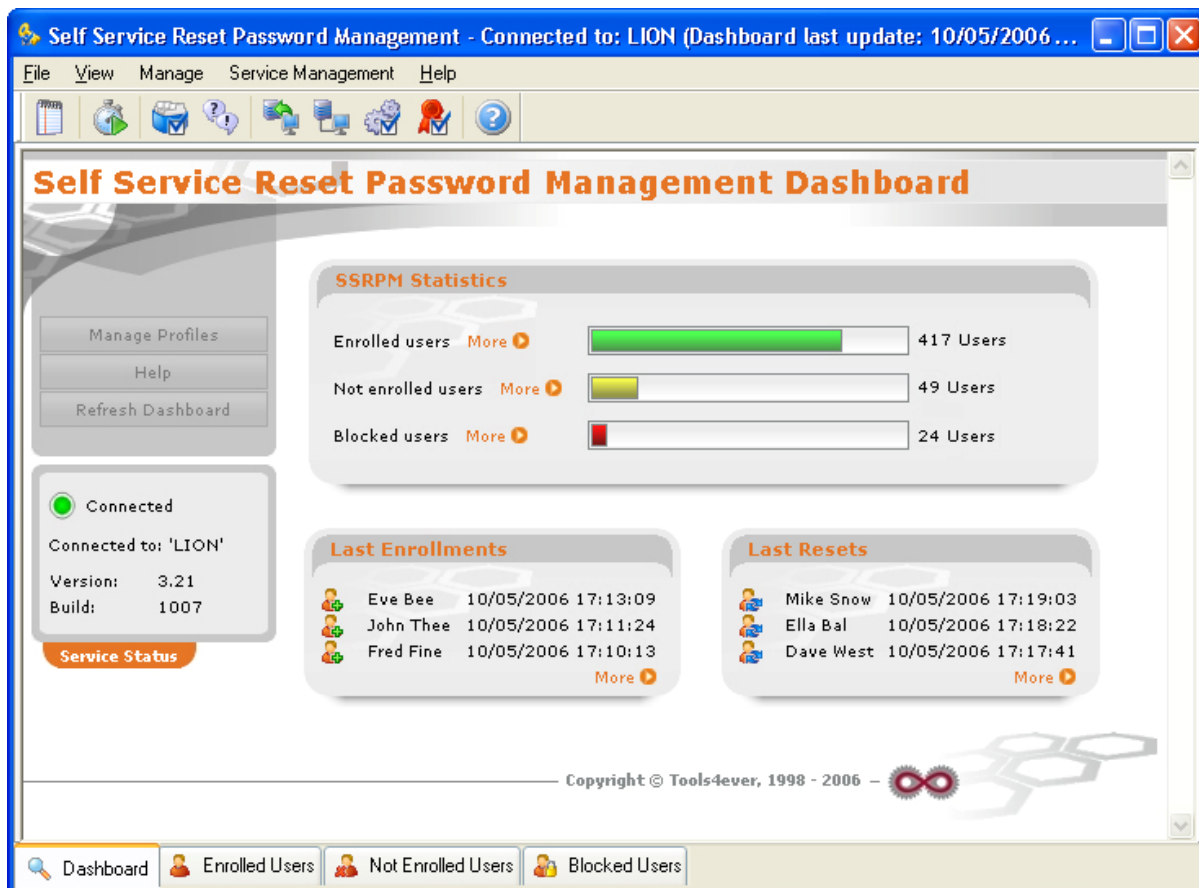


Figure 8: The Dashboard within the SSRPM Admin Console

In this manner three other, more detailed, overviews are available throughout the dashboard or via the tab-buttons beneath the overview window:

- The 'Enrolled Users' overview
- The 'Blocked Users' overview
- The 'Not-enrolled' overview

4.1.2. The 'Enrolled Users' overview

The 'Enrolled Users' overview provides a list of all users which have currently enrolled into SSRPM:



Figure 9: The Enrolled Users Overview within the SSRPM Admin Console

4.1.3. The 'Not-Enrolled Users' overview

The 'Not-Enrolled Users' overview provides a list of all not-enrolled users, see the figure below. Not-enrolled users are all users within the assigned domain(s) or OU(s) which still must enroll into SSRPM.

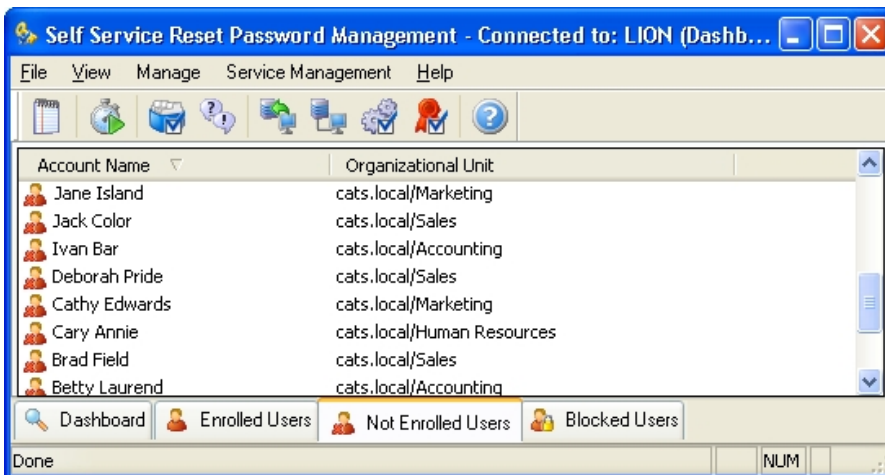


Figure 10: The Not Enrolled Users Overview within the SSRPM Admin Console

4.1.4. The 'Blocked Users' overview

The 'Blocked Users' overview provides a list of all users which are temporarily blocked from SSRPM, see the figure below. When account blocking is enabled within the applicable SSRPM Profile (see: *SSRPM Profiles* on page 13) a user will be blocked from SSRPM when too many questions are answered incorrectly. This prevents answer guessing by a possible attacker. A blocked user cannot use SSRPM's features.



Figure 11: The Blocked Users Overview within the SSRPM Admin Console

4.1.5. The 'Reports' overview

The reports overview displays all configured reports. It also displays the status of reports and at what time they will be generated.

4.1.6. SSRPM Profiles

SSRPM uses settings, like for instance the number of questions, or the way answers will be compared when they're checked. These settings are stored in so-called SSRPM Profiles. By default, these settings will be the same for all user accounts for which SSRPM is enabled (using the 'Default Profile' SSRPM Profile). An SSRPM Profile is applicable for one or more organizational units (OU's) or a whole domain.

An SSRPM Profile consists of the following settings:

- Questions
- Account blocking
- E-Mail notification
- Enrollment management
- Profile options

Questions

SSRPM allows you to define three types of questions:

- User Defined Questions
- Administrator Defined Questions
- Mandatory Administrator Defined Questions

User Defined Questions

User defined questions are questions which are created by a user itself. In this case the user must make up its own questions and answers when enrolling.

Administrator Defined Questions

Administrator defined questions are questions which are created by the administrator. Per SSRPM Profile a set of administrator defined questions can be configured from which a user must choose. These questions can be made available in multiple languages, see the section: *Questions* on page 36 for more information.

Mandatory Administrator Defined Questions

Administrator Defined Questions can be flagged 'Mandatory'. If an administrator defined question is made mandatory, the user must answer the flagged question.

Note: It is recommended to enable both 'Administrator Defined Questions' and 'User Defined Questions', which makes your SSRPM Profile more secure.

SSRPM is shipped with a list of default SSRPM Profiles. These profiles contain a default set of administrator defined questions in several languages, to which more questions can be added or edited.

Account blocking

Optionally, account blocking can be enabled to increase security. In this case a user can be temporary blocked from SSRPM when too many questions are answered incorrectly. This will prevent answer guessing by a possible attacker. When a user is blocked, the user cannot use SSRPM's features.

E-mail notification

E-mail notification can be enabled (increases security), in which case SSRPM can send a notification e-mail to one or more e-mail addresses when a special event occurs. These events are:

- User enrollment: when a user has enrolled successfully into the SSRPM program.
- Account reset: when a user has reset his or her password successfully.
- Account block: when a user will be blocked from SSRPM (when a user fails to answer the questions correctly several times and 'Account Blocking' is enabled).
- Account unlock: when a user has unlocked his account.

Note: Please make sure that you've specified a valid mail server within the SSRPM Service E-mail configuration if you enable the 'E-mail notification' setting. See the section: *SSRPM Service e-mail settings* on page 23 for more information (other settings, concerning e-mail notification, are described in this section as well).

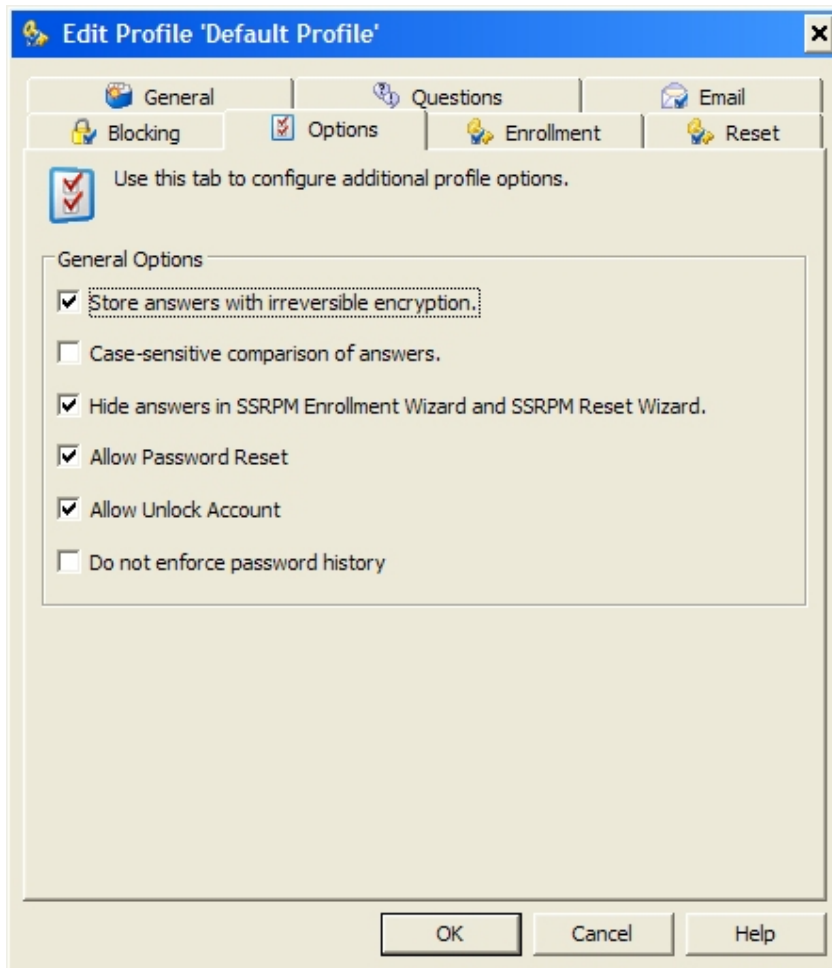
Profile options

Several SSRPM Profile options can be configured. There are three types of options:

- General Options
- Enrollment Options
- Reset Options.

General Options

These are the general profile options.



Store answers with irreversible encryption

When enabled, only the MD5 encrypted hash value of each answer will be stored.

▪ Case-sensitive comparison of answers

When enabled answers will be compared case sensitive. (which means that for instance 'Hello' and 'hello' are not the same)

Hide answers in the SSRPM Enrollment Wizard and SSRPM Reset Wizard

When enabled given answers are displayed as a series of asterisks (***) within the SSRPM Enrollment and Reset Wizard, so nobody else can see the answers typed by a user that enrolling or resetting his or her password.

Allow password reset*

Allows the user to reset his password using the SSRPM Reset Wizard

Allow Unlock Account*

Allows the user to unlock his account using the SSRPM Reset Wizard

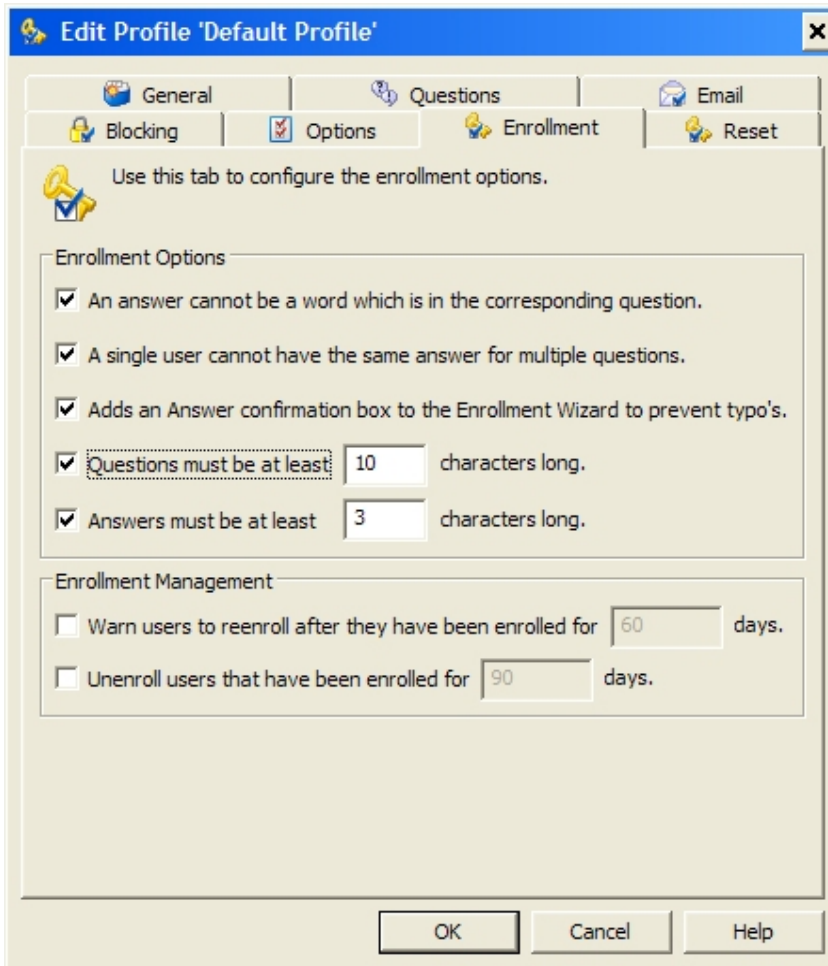
Do not enforce password history

When enabled the user can reset his password even if the new password has been used before.

**Please note that unchecking both 'Allows Password Reset' and 'Allow Unlock Account' will effectively disable the ability of a user to use the SSRPM Reset Wizard.*

Enrollment Options

These are the Enrollment Options.



The screenshot shows a Windows-style dialog box titled "Edit Profile 'Default Profile'". It has a tabbed interface with five tabs: "General", "Questions", "Email", "Enrollment", and "Reset". The "Enrollment" tab is selected and active. The dialog contains the following content:

Use this tab to configure the enrollment options.

Enrollment Options

- An answer cannot be a word which is in the corresponding question.
- A single user cannot have the same answer for multiple questions.
- Adds an Answer confirmation box to the Enrollment Wizard to prevent typo's.
- Questions must be at least characters long.
- Answers must be at least characters long.

Enrollment Management

- Warn users to reenroll after they have been enrolled for days.
- Unenroll users that have been enrolled for days.

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

An answer cannot be a word which is in the corresponding question

When enabled, it is not allowed for a user to provide an answer which is a word in the corresponding question. For instance if the challenge question is "What is the first name of your mother?", the answer cannot be any of the words "What", "is", "the", "first", "name", "of", "your", "mother".

A single user cannot have the same answer for multiple questions

When enabled, it will not be possible for a user to provide the same answer to multiple questions when enrolling. For instance, if the answer to the questions "What is your favorite color?" is "red", the answer to another question "What is the color of you car?" cannot be "red" as well.

Add an Answer confirmation box to the SSRPM Enrollment Wizard to prevent typos

When enabled, an Answer confirmation box will appear within the question and answer wizard page in the SSRPM Enrollment Wizard. This will prevent users to make typos while answering questions within the enrollment.

Questions must be at least ... characters long

When enabled, all questions (which users specify when they enroll) must contain a specified minimum number of characters.

Answers must be at least ... characters long

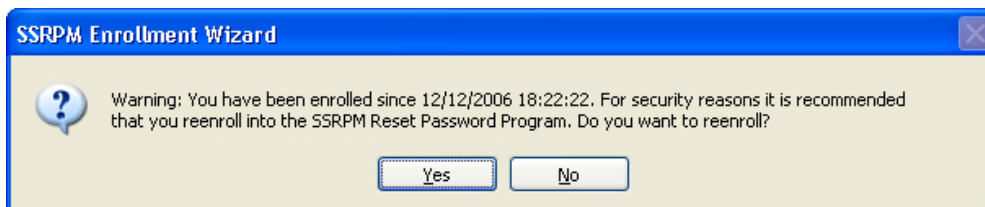
When enabled, all answers(which users specify when they enroll) must contain a specified minimum number of characters.

Enrollment management

Many companies require users to change password periodically, for instance: every 90 or 180 days. Within the enrollment management configuration, this can be configured likely for all questions and answers specified by users within the enrollment process. In this case a user must re-enroll after a certain period to change his or her questions and answers.

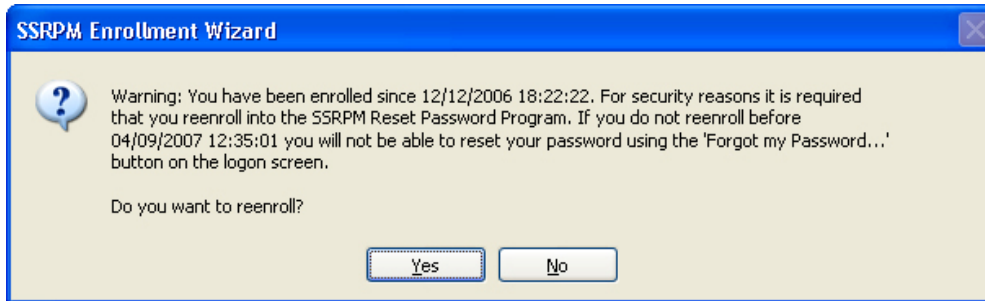
This can be configured in two ways:

- Users can be warned automatically (increases security) that they must re-enroll after they have been enrolled for a certain period. In this case a user will receive a warning when this period has expired, which allows the user to re-enroll immediately:



- Users can be unenrolled automatically (increases security) after they have been enrolled for a certain period (for instance: 90 days). In this case all user questions and answer will be valid for this period. When this period expires users cannot use SSRPM unless they re-enroll.

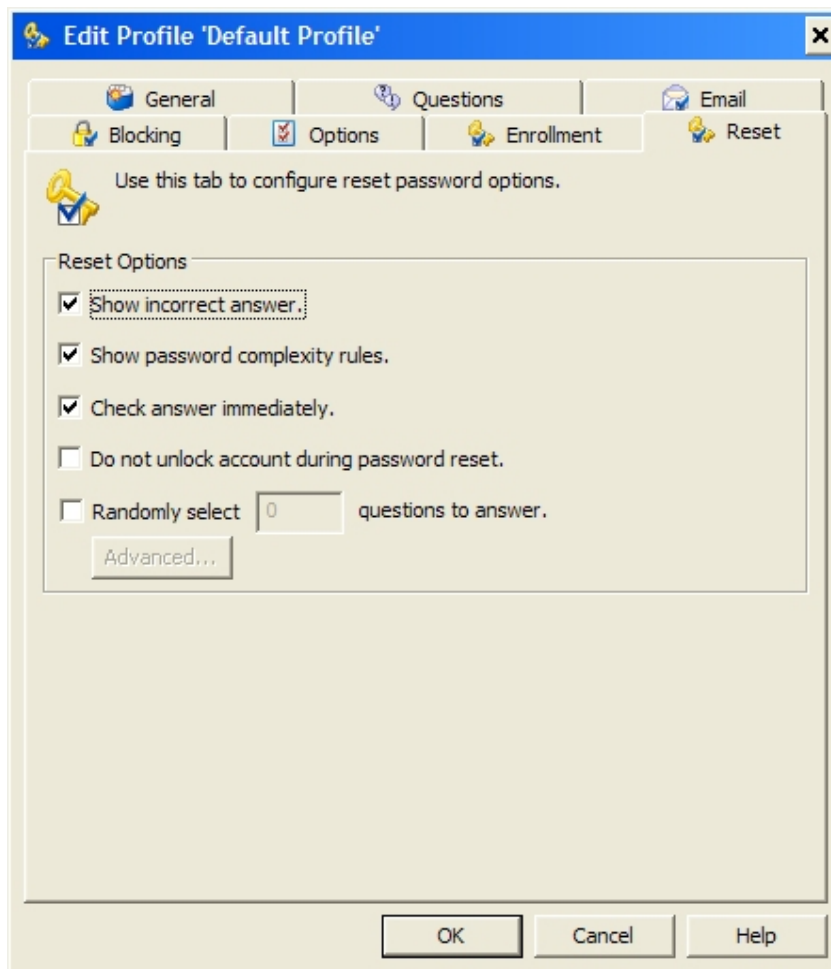
To let users re-enroll before the unenrollment period expires a user it is recommended to configure that users will be automatically warned as well:



In this case the specified period (which must expire before users will receive the warning) must be shorter than the unenrollment period (for instance: 60 days when the unenrollment period is 90 days).

Reset Options

These are the reset options.



Show incorrect answer

When enabled, the user will be shown which question(s) is answered incorrect within the SSRPM Reset Wizard.

Show password complexity rules

When enabled, the password complexity rules will be shown to the user within the SSRPM Reset Wizard when a new password must be entered.

Check answers immediately

When enabled, the given answers will be checked per wizard page within the SSRPM Reset Wizard. This setting is only applicable when the current SSRPM Profile contains more than four questions, in which case the questions will be asked on multiple wizard pages within the SSRPM Reset Wizard.

Do not unlock account during password reset

By default the users account is unlocked by SSRPM during a password reset. Check this option to disable the unlocking of user accounts during password reset.

Randomly select ... questions to answer.

When enabled, the user must answer a random set of questions when he runs the SSRPM Reset Wizard. These questions are a subset of the questions that the user answered during enrollment.

SSRPM Profile assignment

SSRPM is shipped with a default set of SSRPM Profiles, which vary in security level, see the figure below:

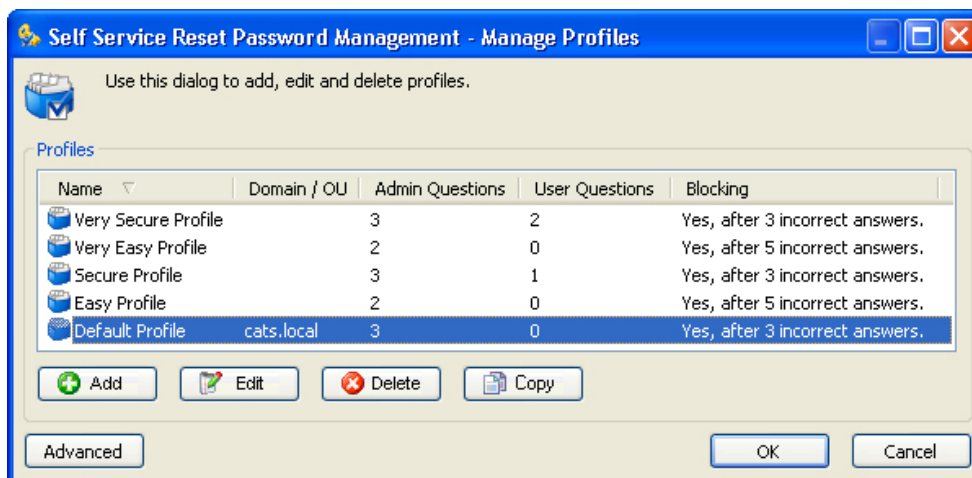


Figure 12: SSRPM Profile Management within the SSRPM Admin Console

Note: Each of these SSRPM profiles, contain a copy of the default question list, which are shipped with SSRPM.

An SSRPM Profile can be assigned to one or more OU's. Depending on your network configuration and levels of security within your network, you may want to assign different profiles to one or more OU's within your network.

Example:

Let's say we have a domain called 'tools4ever.com' with an OU: 'tools4ever.com/users', which contains normal user accounts and three child-OU's:

- 'tools4ever.com/employees/guests' - contains user accounts which have very limited access to network resources comparing to the normal user accounts. A lower level of security is applicable within this OU.
- 'tools4ever.com/employees/consultants' - contains user accounts which have extra access to special network resources comparing to the normal user accounts. In this case a higher level of security is applicable.
- 'tools4ever.com/employees/staff' - contains user accounts for which can manage and configure network resources. In this case the highest security level is applicable. Because of this we don't want to use SSRPM within this OU.

The 'tools4ever.com' domain is assigned to the 'Default Profile'. Because of the variety of security level, the child OU's within the 'tools4ever.com/users' OU are assigned to different SSRPM Profiles:

- Easy Profile (less secure)

The 'tools4ever.com/employees/guests' OU is assigned to the 'Easy Profile', which will make the password reset usability easier for these end-users.

- Secure Profile (more secure)

The 'tools4ever.com/employees/consultants' OU is assigned to the 'Secure Profile', which makes the password reset usability more difficult and more secure to reset a password for these users.

- No profile (excluded)

The 'tools4ever.com/employees/staff' OU is excluded from SSRPM, which means that all users in this OU will not be able reset their password using SSRPM.

See the figure below for an example of SSRPM Domain/OU exclusion within the SSRPM Admin Console:

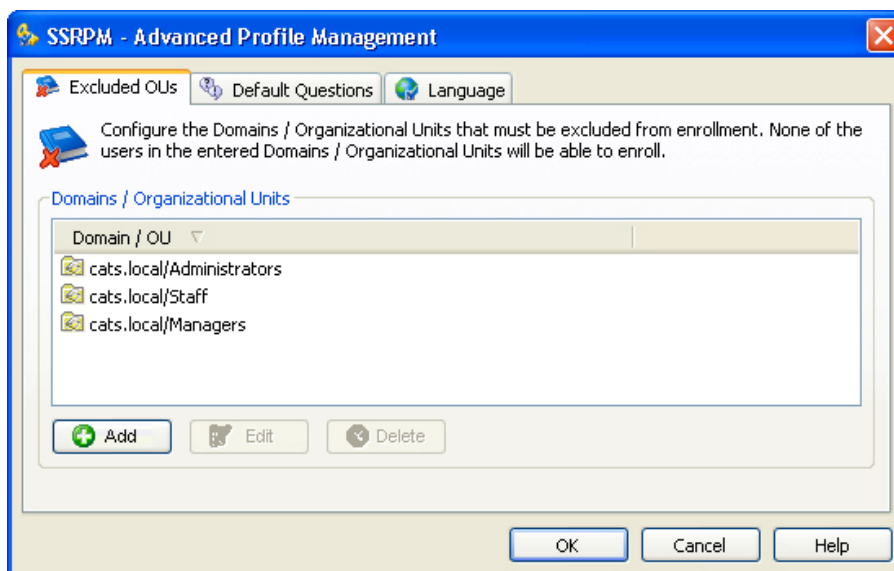


Figure 13: Domain/OU exclusion with the SSRPM Admin Console Profile Management

4.2. SSRPM Service

The SSRPM Service, which processes all password reset requests, can be fully controlled and configured through the SSRPM Admin Console. This section describes all configurable SSRPM Service settings, which are:

- Logging
- Database
- E-mail
- Security
- UMRA Connector

4.2.1. Logging

The SSRPM Service writes log messages to a certain log file (which is located by default at: 'C:\Program Files\SSRPM Service\Logging\SSRPMLog.log'). This log file can help identify and diagnose the source of a current problem.

Note: The log file will be cleared when it reaches the specified maximum size (which is 5 Mb by default).

The log messages are divided into three severity levels:

- Information: General information messages.
- Errors: Error messages.
- Debug Information: Additional information about events and errors.

If you want to use another log file, which is located elsewhere you can specify the location to this file within the SSRPM Service Configuration.

Note: If you specify another log file, make sure that the SSRPM Service has write access to the specified file.

4.2.2. Database

All questions and (irreversible encrypted) answers, which are defined by end-users, are stored in the SSRPM Database. Currently SSRPM supports the Microsoft Jet engine (Default) and Microsoft SQL Server 2000 and 2005 (All versions).

If the Microsoft Jet engine is used, the SSRPM Database (called: 'SSRPMDatabase.mdb') is installed on the same computer on which the SSRPM Service is installed and by default located at: 'C:\Program Files\SSRPM Service\Database\'. It is also possible to change the location of the database.

4.2.3. E-mail

The SSRPM Service can send a notification e-mails. This can be configured differently per SSRPM Profile, see paragraph: *E-mail notification* on page 15 for more information. The SSRPM Service uses the specified mail server and port to send all notification e-mails to one or more recipient(s), which are specified in the applicable SSRPM Profile.

The notification e-mails can be sent as either plain text or html. The content of these e-mails is determined by several e-mail content files, so that this can be modified easily. These files are stored on the same computer on which the SSRPM Service is installed (located by default at: 'C:\Program Files\SSRPM Service\Email\'). For each notification e-mail separate html and text e-mail content files are available, knowingly:

- Account enrollment notification e-mail files: Enrollment.txt (for plain text) or Enrollment.html (for html)
- Account reset notification e-mail files: ResetAccount.txt (for plain text) or ResetAccount.html (for html)
- Account block e-mail notification files: Block Account.txt (for plain text) or Block Account.html (for html)

You can modify these files to change the e-mail content which will be used for each notification e-mail. In this case several keywords can be used, which will be replaced with current values, when the SSRPM Service sends the e-mail. See *Appendix C: SSRPM keywords* on page 43 for a list and explanation of all keywords, which can be used.

4.2.4. Security

The SSRPM Service distinguishes three types of users who have access to the SSRPM Service, knowingly:

- *Administrators*
Administrators are those users or groups which have the right to manage and have full control over the SSRPM Service (which is by default: the 'Domain Admins' user group).
- *Operators*
Operators are those users or groups who are allowed to unblock or unenroll users from SSRPM (which is by default: the 'Domain Admins' user group). For instance: to allow the helpdesk to unblock users with the SSRPM Admin Console.
- *Users*
Users are those users or groups who are allowed to enroll and use SSRPM (which is by default: the 'Everyone' user group). If a user has administrative privileges, this user will not be allowed to enroll into SSRPM, see below for more information:

Due to security reasons, users which are member of the 'Domain Admins' domain user group are never allowed to enroll into SSRPM. This is, because we believe it is very insecure to use SSRPM with a user which has domain Administrative Privileges.

If such a user tries to enroll into SSRPM he or she will receive an error message which tells the user that access to SSRPM is denied and the SSRPM Enrollment Wizard will be exited.

Additional users or groups can be added to deny enroll access (which are: 'Excluded Users') like users with Administrative Privileges Security administrators may prefer this for specific users who have specific access to important network resources (like for instance: staff users).

4.2.5. UMRA Connector

SSRPM can connect with other systems, like: UNIX, Linux, Novell and a lot more. For instance to reset the password of a user account on another system when a user resets his or her password with SSRPM. For this SSRPM must connect to Tools4ever's product: User Management Resource Administrator (UMRA) via SSRPM's UMRA Connector.

UMRA delivers out-of-the box many different network actions, database options and application integration, which can be evoked by SSRPM on two SSRPM Events:

- Enrollment, in which case UMRA actions will be evoked when a user enrolls into SSRPM;
- Reset Account, in which case UMRA actions will be evoked when a user resets his or her password with SSRPM.

Like the mentioned connection with other systems a lot more UMRA actions can be evoked from SSRPM and configured using UMRA's simple drag-and-drop user interface.

Implementation examples are:

- Integration with any helpdesk system: create new trouble tickets, update and optionally close existing tickets, update reports and more.
- Update a custom company database with a password reset request.
- Create dynamic cost justification reports with the number of password resets per organization unit. These reports can be scheduled, e-mailed, presented in a web service and more.
- Create advanced custom e-mail notification schemas. For instance: send a reset password e-mail notification to the manager of the employee or send a notification to a security officer per organization division of the employee.

This is just a small set of examples. Tools4ever has many more UMRA projects available who smoothly integrate with SSRPM. See the *Tools4ever website* <http://www.tools4ever.com> for more examples and information.

Setup the UMRA connection

Note: Basic knowledge of UMRA is required when creating a connection with UMRA, in which case you must know how UMRA works and how to create and configure projects within UMRA. See the *Tools4ever website* <http://www.tools4ever.com> for more information about UMRA.

To create a connection with UMRA, using SSRPM's UMRA Connector, the following main steps must be performed:

1. Install and setup UMRA.
2. Create an UMRA project.
3. Configure the SSRPM Service.

Step 1: Install and setup UMRA

First of all, UMRA must be installed by running the UMRA setup executable (called: 'SetupUserManagement.exe'), which is available for download from the *Tools4ever website* <http://www.tools4ever.com>.

In order to use the UMRA Connector, at least two UMRA software components must be installed (this can be selected within the UMRA Installation Wizard which starts throughout the UMRA setup executable):

- The UMRA Console: to create and run UMRA projects and setup and manage the UMRA Service;
- UMRA Automation: to be able to execute UMRA projects by SSRPM.

Once the installation of UMRA has been finished, the UMRA Console must be started to configure, install and start the UMRA Service with the UMRA Service Wizard. See the *Tools4ever website* <http://www.tools4ever.com> for more information.

Step 2: Create an UMRA project

When UMRA has been setup successfully, an UMRA project must be created with the UMRA Console. This project must contain the UMRA script with all UMRA actions that have to be performed. For instance: actions to reset a user's password on another system or to store user specific values (like user questions) in a database etc.

SSRPM is shipped with two example UMRA scripts: 'SSRPMEnroll.usc' and 'SSRPMReset.usc'. These scripts can be found in the '\Examples\UMRA COM' directory within the SSRPM Admin Console directory (which is by default: 'C:\Program Files\Tools4ever\SSRPM\Admin Console'), and can be imported into an UMRA project.

The purpose of both scripts is to store all available SSRPM Keywords (see: *Appendix C: SSRPM keywords* on page 43) into a CSV (comma-separated values) file.

The UMRA script will be evoked by the SSRPM Service and executed by the UMRA Service when an SSRPM event occurs.

Note: Please make sure that the SSRPM Service Account has enough privileges to execute the UMRA project script. Verify this with the UMRA project's security properties in the UMRA Console.

Step 3: Configure the SSRPM Service

When an UMRA project has been created, the SSRPM Service must be configured, to be able to evoke the created UMRA project via the UMRA Connector. For this, the UMRA Service location and name of the UMRA project must be specified in the SSRPM Service configuration within the SSRPM Admin Console:

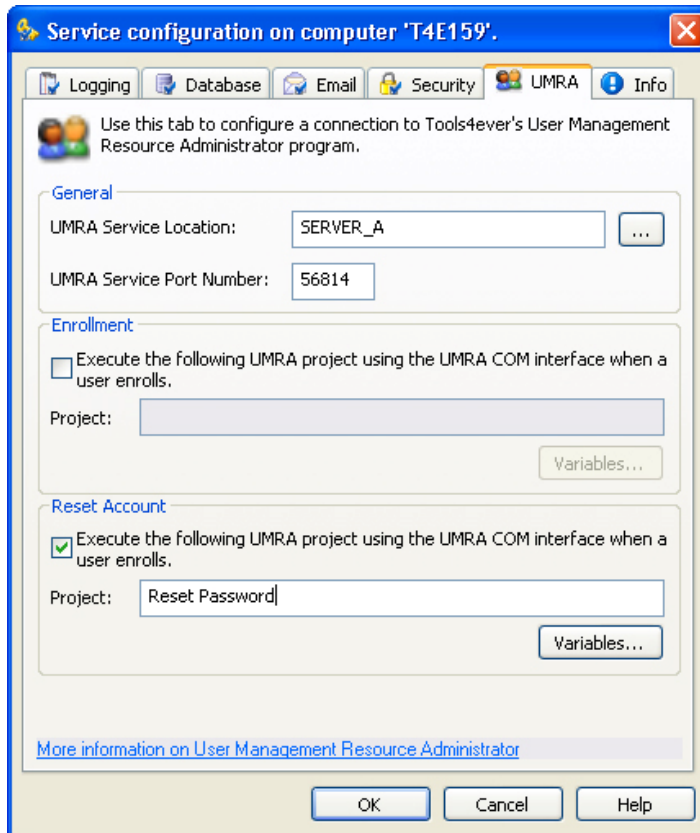


Figure 14: The SSRPM Service UMRA configuration within the SSRPM Admin Console

Separate UMRA Projects (which contains several UMRA actions) can be specified for the enrollment or reset account event.

By default, certain UMRA variables are selected and assigned to certain SSRPM keywords. This means that, when the SSRPM Service evokes an UMRA project, these UMRA variables will contain the value which is stored in the SSRPM keyword to which an UMRA variable is assigned.

These variables will be passed to the UMRA Service when the SSRPM Service evokes the UMRA project and can be used within the accompanying UMRA project script. For instance: to identify the user or to retrieve the new password specified by a user during a password reset when the UMRA project script is executed.

An example of using these variables within UMRA can be found in the available example UMRA scripts (mentioned in: *Step 2: Create an UMRA project* on page 25).

Note: Optionally, additional UMRA variables can be assigned to SSRPM Keywords and passed to the UMRA Service. See: *Appendix C: SSRPM keywords* on page 43 for more information about all available SSRPM Keywords.

When the SSRPM Service has been configured successfully the specified UMRA project(s) will be executed, according to the following procedure:

Note: With this procedure an UMRA project has been specified for the Reset Account event only. When an UMRA project has been specified for the enrollment event, the UMRA project will be evoked when a users enrolls into SSRPM using the SSRPM Enrollment Wizard.

1. Reset Account event occurs:
A user resets his or her password on a client workstation using the SSRPM Reset Wizard.
2. The password reset request will be handled by the SSRPM Service:
 1. The SSRPM Service connects to the UMRA Service.
 2. The SSRPM Service sets UMRA variables with the information stored within the corresponding assigned SSRPM Keywords.
 3. The SSRPM Service will request the UMRA Service to execute the specified UMRA project, and passes the assigned UMRA variables to the UMRA Service.
3. The UMRA Service executes an UMRA project:
The UMRA Service executes the UMRA project (which is specified in SSRPM) with the UMRA variables (who contain all values which are set by SSRPM).
Example: The UMRA project script resets the password of the user account on another system by using the values which are stored within the passed UMRA variables.

4.3. SSRPM User Client Software

As described earlier, the SSRPM User Client Software (the SSRPM Enrollment Wizard, the SSRPM Reset Wizard, the SSRPM GINA and SSRPM Credential Provider (for Windows Vista)) must be installed on all client workstations, which are used by end-users which are member of a configured domain (or located in a configured OU) within SSRPM. A configured domain or OU is a domain or OU to which an SSRPM Profile is assigned.

This section describes how the SSRPM User Client Software works and can be used.

Note: By default, the language which is used by the operating system will be used by the SSRPM Client Software as well (if available). In this case, all user interface text of the SSRPM Enrollment Client, SSRPM Reset Client and SSRPM GINA (or SSRPM Credential Provider when running Windows Vista) will be shown in this language. See chapter *SSRPM User Client Software user interface* on page 35 for more information.

4.3.1. Service communication

The SSRPM Enrollment Wizard and the SSRPM Reset Wizard must communicate with the SSRPM Service. If one of the wizards is started manually, a dialog box pops up to ask the location of the SSRPM Service. The wizard will then store the provided service location in the registry. If the wizards are distributed through the network, the SSRPM Service location can also be set using GPO. Please refer to the "GPO Distribution Guide" for more information on this subject.

Note: See: *Service communication* on page 41 for more general information.

4.3.2. The SSRPM Enrollment Wizard

To let a user enroll immediately into the SSRPM program, the SSRPM Enrollment Wizard will be started automatically when a user logs on until this user has successfully enrolled. The SSRPM Enrollment Wizard will not be started if the current user already has enrolled or no SSRPM Profile has been configured, which will be checked with the SSRPM Service at startup.

Within the SSRPM Enrollment Wizard, an end-user must define his or her answers to the challenge questions according to the applicable SSRPM Profile.

When administrator defined questions are enabled within the SSRPM profile which is applicable for the current end-user, the user must choose from one or more pre-defined questions, which is shown in the figure below:

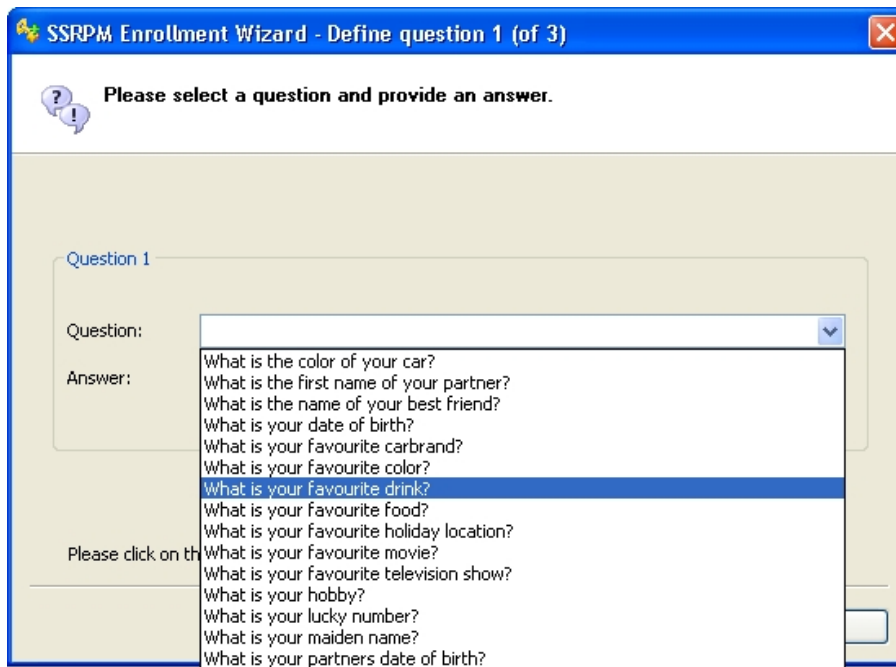


Figure 15: Select an Administrator Defined Question within the SSRPM Enrollment Wizard

Note: The administrator defined questions, can be shown in multiple languages. See *Questions* on page 36 for more information.

Next to the administrator defined questions, if enabled, the user must define a number of user defined questions, see the figure below:

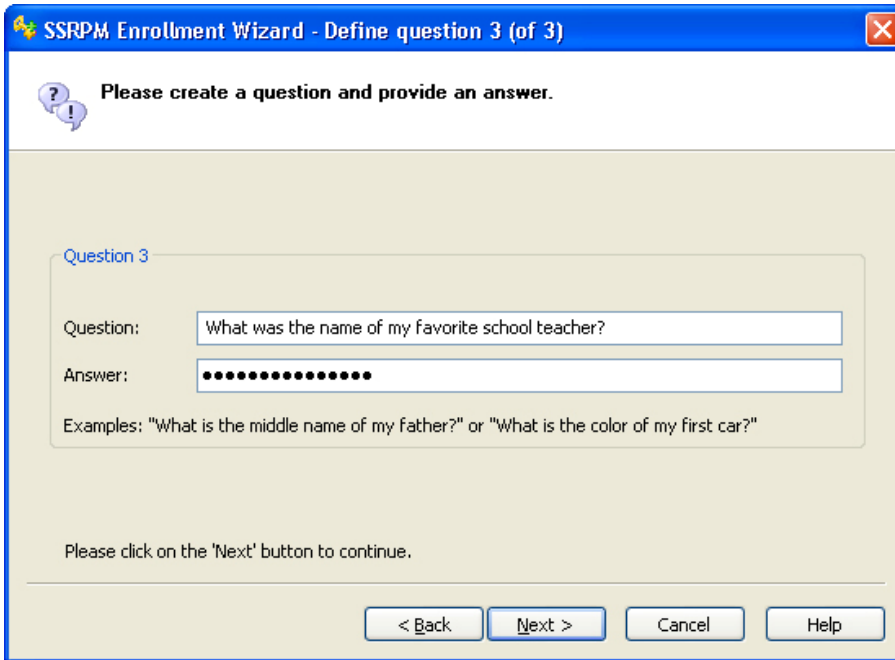


Figure 16: Create a User Defined Question within the SSRPM Enrollment Wizard

When a user completes the SSRPM Enrollment Wizard successfully, all questions and answers will be sent to the SSRPM Service (via encrypted RPC). The SSRPM Service stores the questions and (irreversible encrypted) answers in the SSRPM Database and the SSRPM Enrollment Wizard will not show up again at user logon, unless the user has been un-enrolled (for instance: by the administrator with the SSRPM Admin Console).

When an end-user has enrolled, he or she can use the SSRPM Enrollment Wizard (which is available from the start menu: 'All Programs -> Tools4ever -> SSRPM -> SSRPM Enrollment Wizard') to re-enroll into or un-enroll from SSRPM.

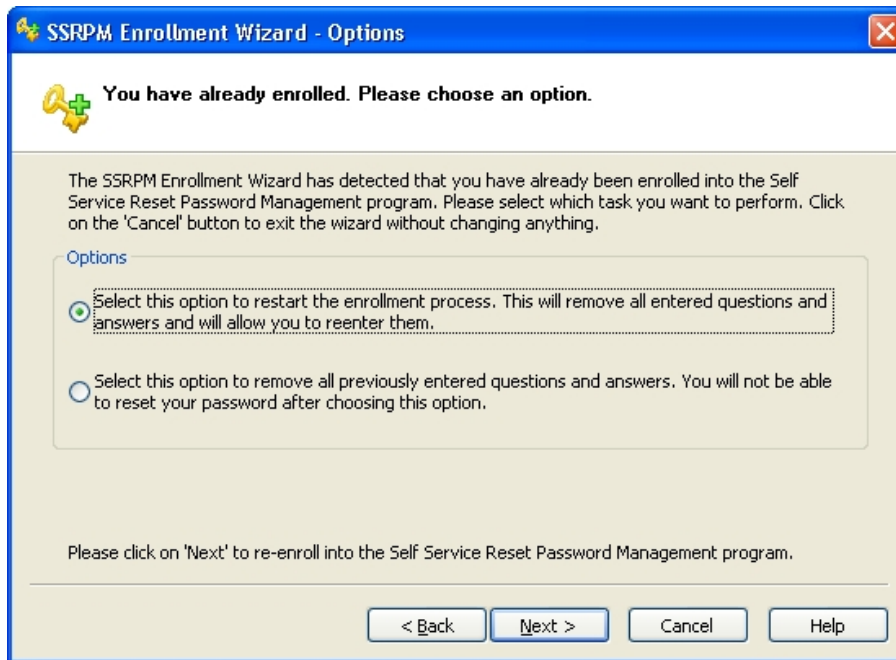


Figure 17: Options shown within the SSRPM Enrollment Wizard (when already enrolled)

Within the re-enrollment (the first option) the user can redefine his or her answers and questions. In this case his or her old questions and answers will be overwritten. If the user chooses to un-enroll from SSRPM (the second option), the end-user's defined questions and answers will be deleted from SSRPM. From this point the user cannot use SSRPM, unless he or she enrolls again later on.

Note: There are several registry options available to modify the default behaviour of the SSRPM Enrollment Wizard. Please refer to the "GPO Distribution Guide" for a complete list of available settings.

4.3.3. The SSRPM Reset Wizard

When an end-user starts his or her computer (or the computer is locked), and the SSRPM User Client Software has been installed, the 'Forgot My Password' button will be shown at the bottom of the Windows logon dialog:



Figure 18: The 'Forgot My Password' shown at the bottom of the default Windows logon screen

When running Windows Vista an extra 'Forgot My Password' link will appear on the Windows Vista Logon screen, which provides the same functionality:

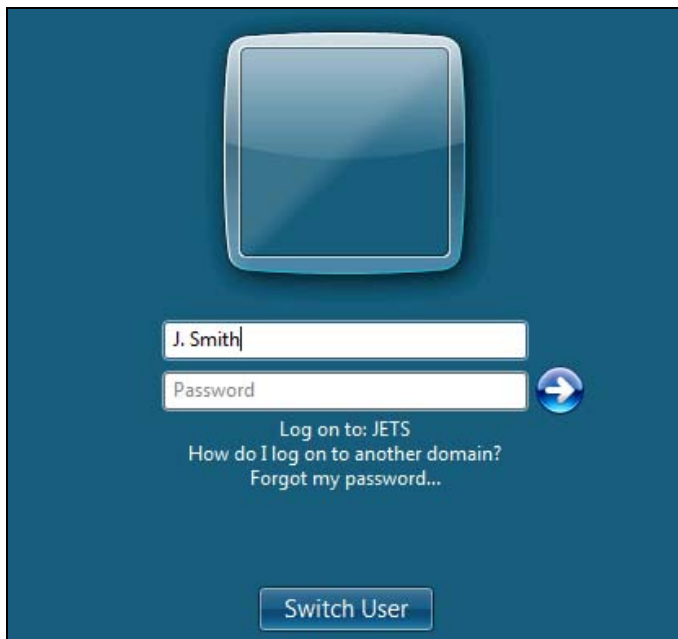


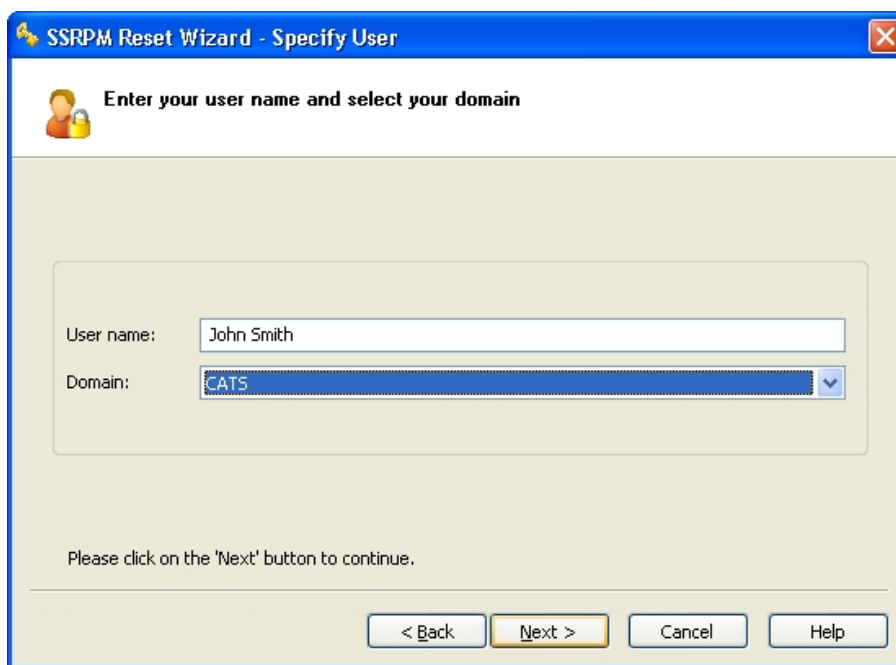
Figure 19: The 'Forgot My Password' link shown on the Windows Vista logon screen

When the user has forgotten his or her password, he or she can click on this button (or link when running Windows Vista) to start the SSRPM Reset Wizard.

Within the SSRPM Reset Wizard an end-user must answer all of his or her questions to eventually reset his or her password. The SSRPM Reset Wizard uses the name of an enrolled user to identify a user, so the questions of this user can be shown. The user name can be specified by the user itself or the SSRPM Reset Wizard can use the name of the user which has last logged on (the last logged on user).

By default, the SSRPM Reset Wizard will use the last logged on user to identify. This is preferred, because it is most likely that this is the same user as the user which wants to reset his or her password, unless a client workstation is used by multiple users.

If the currently last logged on user does not exist within SSRPM or is not the same as the user, which wants to reset his or her password, the user must specify his or her own credentials (user name and (if necessary) domain).



SSRPM Reset Wizard - Specify User

Enter your user name and select your domain

User name: John Smith

Domain: CATS

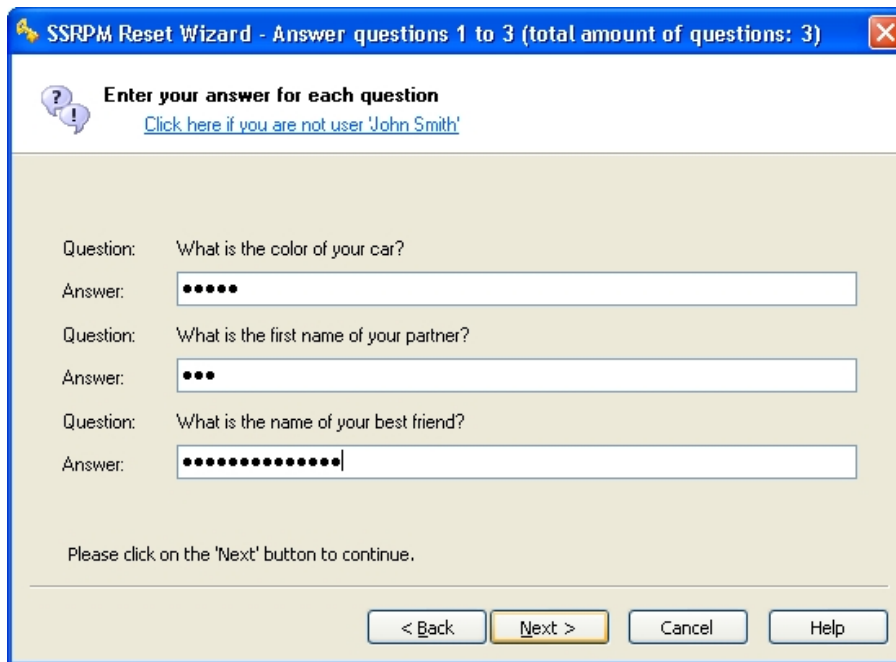
Please click on the 'Next' button to continue.

< Back Next > Cancel Help

Figure 20: Specify a user name and domain within the SSRPM Reset Wizard

When the user is valid and has enrolled, the user must answer the questions which he or she selected and/or defined within the enrollment.

When the service has determined that the user has answered his or her questions correctly, the user can reset his or her password:



The screenshot shows a dialog box titled "SSRPM Reset Wizard - Answer questions 1 to 3 (total amount of questions: 3)". The dialog has a blue title bar with a question mark icon and a close button. The main content area is light beige and contains the following text:

Enter your answer for each question
[Click here if you are not user 'John Smith'](#)

Question: What is the color of your car?
Answer: [.....]

Question: What is the first name of your partner?
Answer: [...]

Question: What is the name of your best friend?
Answer: [.....]

Please click on the 'Next' button to continue.

At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help". The "Next >" button is highlighted with a yellow border.

Figure 21: Answer questions within the SSRPM Reset Wizard

When the user resets his or her password by providing a new password, the SSRPM Reset Wizard will check the new password with the Microsoft password policy settings of the current domain:

- Password complexity policy: if enabled, SSRPM will check if the new password complies with the Microsoft password complexity requirements. The password complexity policy defines that a password has to meet certain requirements.
- Minimum password length policy: if enabled, SSRPM will check if the new password length complies with the specified minimum password length. The minimum password length policy determines the minimum number of characters a password must have.
- Enforce password history policy: if enabled, SSRPM will check if the password was not used in the recent past. The Password history policy determines the number of unique new passwords a user must use before an old password can be reused.
- Minimum password age policy: if enabled, SSRPM will check the period of time (in days) that a password must be used before the user can reset his or her password. The minimum password age policy determines how many days a new password must be kept before the user can change it.

If one or more of these policies are enabled and the new password does not comply one of these (enabled) policies, the user will receive an error and the password will not be reset. In this case, the user must provide another password which does comply.

If the 'Show password complexity rules' option has been enabled within the applicable SSRPM Profile (see: *Profile options* on page 15), the new password can be checked with the password complexity and password length policies while a user enters a new password.

This is shown in the figure below:

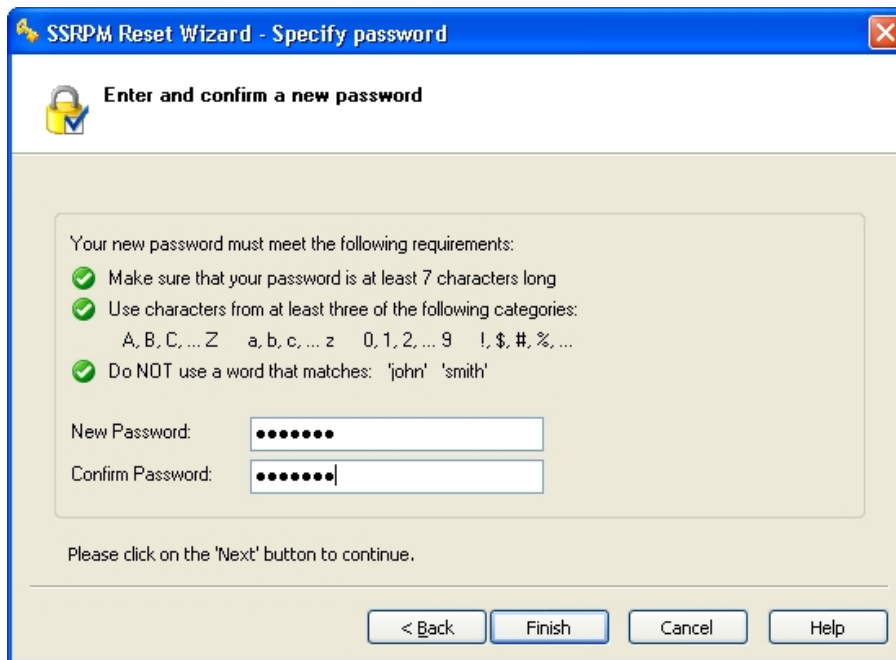


Figure 22: Specify a new password within the SSRPM Reset Wizard

When the user has provided a new password successfully and finished the SSRPM Reset Wizard, he or she can immediately logon via the Windows logon dialog with the new password.

Note: There are several registry options available to modify the default behaviour of the SSRPM Reset Wizard. Please refer to the "GPO Distribution Guide" for a complete list of available settings.

4.3.4. Registry Settings

The main behavior of the SSRPM User Client Software modified with several registry settings. These registry settings can be automatically pushed to workstations using a GPO. See the "GPO Distribution Guide" for more information on GPO's and the available registry settings. The "GPO Distribution Guide" can be downloaded from the *Tools4ever website* <http://www.tools4ever.com>.

5. Multilingual support

SSRPM supports multiple languages, which are: English, French, German, Italian, Spanish, Polish, Portuguese and Dutch. SSRPM provides three possibilities concerning multilingual support:

1. Only use the English language. Any other language options do not must be configured. This will be used by default.

Note: When you're running the SSRPM Admin Console Startup Wizard, the English language is selected by default within the 'Language Settings' wizard page. In this case you won't have to do anything, and leave this setting.

2. Use a single specific language. The specified language will be used for all text which can be modified.
3. Use multiple languages. Used within (mostly larger) companies with multi-language environments.

The user interface text of the SSRPM Admin Console, which is used by the administrator, will always use the default language: English. All text, which is presented to the end-user, supports multiple languages. This text will appear at two places within the SSRPM User Client Software:

- SSRPM User Client Software user interface: the text which is used for all buttons and dialogs (the user interface) for the SSRPM Enrollment Wizard, SSRPM Reset Wizard and SSRPM GINA.
- Questions: the questions which are specified by users when they enroll with the SSRPM Enrollment Wizard and which are shown in the SSRPM Reset Wizard.

5.1. SSRPM User Client Software User Interface

To be able to show all text, which is used for the user interface of the SSRPM User Client Software, in multiple languages, the SSRPM Enrollment Wizard, SSRPM Reset Wizard and SSRPM GINA and SSRPM Credential Provider each are shipped with a so-called locale file. A locale file is a text file, which contains the text of the user interface in several languages.

By default, the SSRPM User Client Software will use the default operating system language of the current client workstation, when the corresponding locale file contains the user interface text for this language as well. If the locale file does not contain this language, the default language will be used (English).

Several options can be configured using GPO settings. Please refer to the "GPO Distribution Guide" for more information on this subject.

- Custom locale file. The default locale files can be modified to contain customized text.
- Force language. The automatic language detection can be overridden by manually specifying a language.

5.2. Questions

Within the SSRPM Admin Console you can define the language(s) in which the questions must be shown within the SSRPM Enrollment Wizard. For this setting three options are available, see the Figure below:

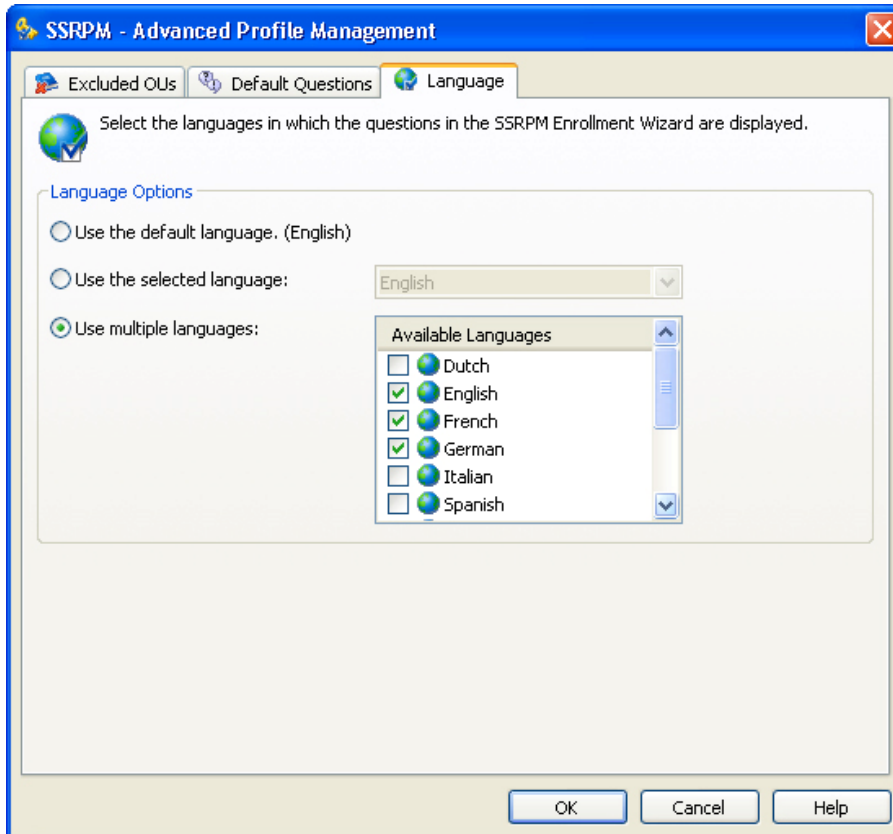


Figure 23: Language settings in which the administrator defined questions in the SSRPM Enrollment Wizard will be shown

5.2.1. Use the default language (English)

When you use the default language, the administrator defined questions always will be shown in the default language, which is: English.

Note: When you're running the Admin Console Startup Wizard, this setting is used by default, in which case only 'English' has been selected within the 'Language Settings' wizard page.

5.2.2. Use another language

If you select a specific language, the administrator defined questions will always be shown in the language which has been selected.

Note: When you're running the Admin Console Startup Wizard, this setting will be used when 'English' has been de-selected and one other language has been selected within the 'Language Settings' wizard page.

5.2.3. Use multiple languages

When you've selected multiple languages, the SSRPM Enrollment Wizard will show the administrator defined questions in the same language, which is used by the operating system of the current client workstation.

If the default operating system language does not match with one of the languages which are selected, the SSRPM Enrollment Wizard will use the default language (English). When the default language is not available as well, the SSRPM Enrollment Wizard will use the first language which is in the selected language (using alphabetical order).

Note: When you're running the Admin Console Startup Wizard, this setting will be used when two or more languages have been selected, within the 'Language Settings' wizard page.

When you add administrator defined questions to an SSRPM Profile or to the default questions list later on, each question must be available in the specified language(s). If this is not the case, you must translate each added question to the specified language(s):

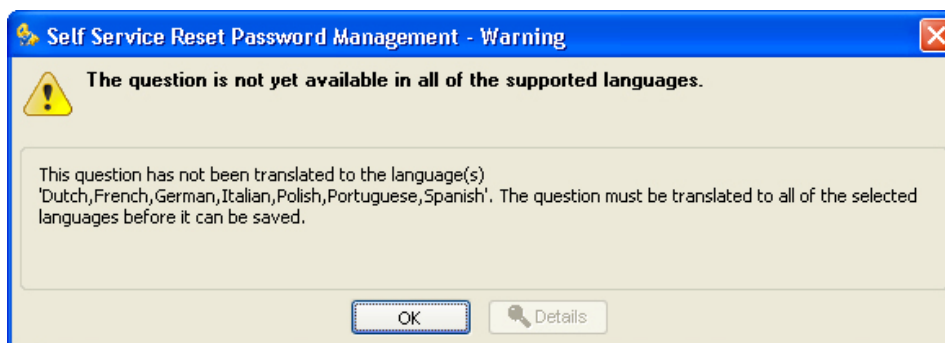


Figure 24: A warning message, which will be shown when an added question is not available in the specified language(s)

5.2.4. Translation

When choosing a language option, it is possible that not all questions are available in the specified language(s). For instance when you've added one or more questions in English only and choose to support another language as well. If this is not the case you must translate these questions to the specified language(s).

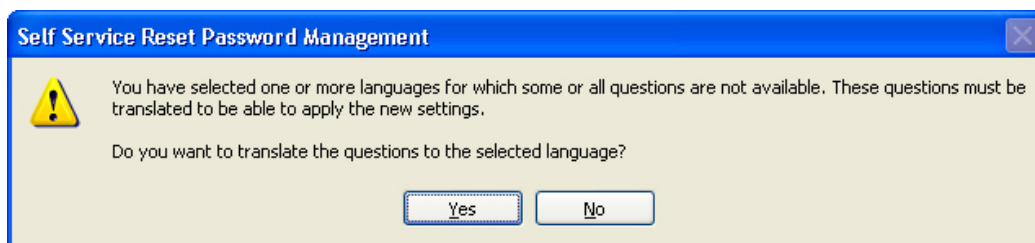


Figure 25: Warning message, which is shown when not all questions are available in the specified language(s)

If you choose to translate the questions to the selected language(s), a list of all questions (which must be translated) will be shown:

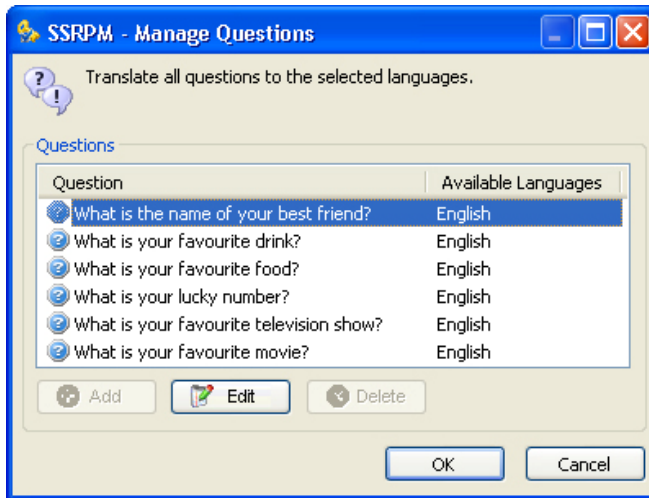


Figure 26: List of questions, which are not available in the selected language(s)

When you edit a question in this list, you will see a list of all available languages of the selected question. Add one or more languages to translate the question to the specified language(s):

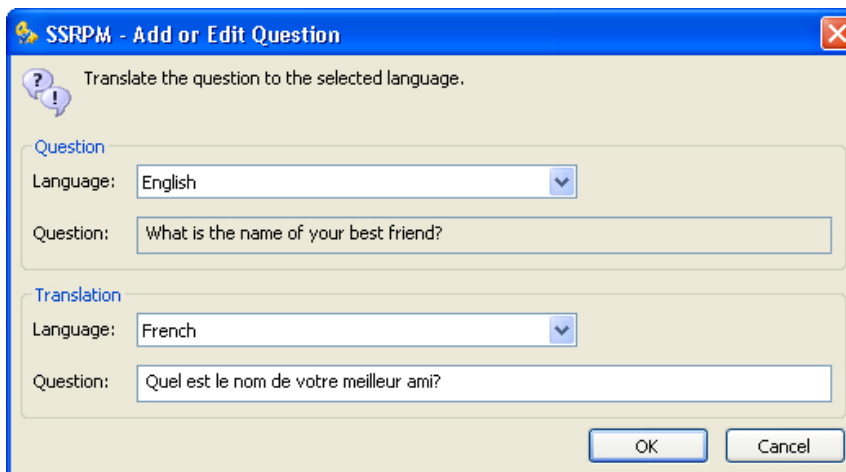


Figure 27: Translate a question to another language

When all questions are translated, the specified language(s) can be used for all questions.

6. Frequently Asked Questions (FAQ)

Do I need to install the SSRPM Service?

Yes. SSRPM will not work without the SSRPM Service, and must be installed and running when using SSRPM. The SSRPM service eventually handles all SSRPM functionality. In most cases only one SSRPM Service must be installed.

How does SSRPM identify users who have forgotten their password?

A user will be identified, by answering a set of personal questions like for example: "What is the name of your first partner?". When these questions are answered validly, which will be determined by the SSRPM service, the user is allowed to do a password reset.

Can I define my own default questions?

Yes. SSRPM is shipped with a list of default questions (in multiple languages), which you can edit. You can define your own default questions as well. These questions can be used for one or more profiles.

Do I need to install the SSRPM User client Software on each workstation?

Yes. The SSRPM User Client Software is needed for all end-users which need to use SSRPM. That's why the software must be installed on each of these end-user's workstation(s). Alternatively you can use GPO's (see: *Appendix B: Group Policy Objects* on page 42) to distribute the SSRPM User Client Software through your network. See the "GPO Distribution Guide" for more information, of which the latest version is available on the *Tools4ever website* <http://www.tools4ever.com>.

Is it possible to distribute the SSRPM User Client Software through my network?

Yes. This can be done with the use of GPO's (see: *Appendix B: Group Policy Objects* on page 42). See the "GPO Distribution Guide" for more information, of which the latest version is available on the *Tools4ever website* <http://www.tools4ever.com>.

How can I install the User Client Software without the use of a GPO?

You can run the SSRPM User Client Software installer ('SsrpmUserClientSoftware.msi', which is located by default at: 'C:\Program Files\Tools4ever\SSRPM\Admin Console' on the computer on which the SSRPM Admin Console is installed) on each client workstation.

Will the user be notified that he or she needs to enroll into SSRPM?

The enrollment process is integrated in the user logon procedure. During a user logon the SSRPM Enrollment Wizard will check if a user has already enrolled into SSRPM. If this is not the case, this Wizard will start the enrollment process automatically.

Is the communication within SSRPM secure?

Yes. SSRPM uses encrypted RPC as a communication protocol, and stores all the end-user answers as an irreversible MD5 encrypted hash value.

Does SSRPM store all user answers?

No. Only an irreversible MD5 hash will be stored. These hashes cannot be converted back to the original user answers.

Do I need to have Microsoft Access installed for the database?

No. For the database storage, SSRPM will use the standard JET engine, which is running by default on each Windows machine.

Is it possible that another GINA extension is installed on a client computer?

Yes. There are a lot other extensions which add extra functionality to the windows logon system. If such a GINA is installed on a client machine the SSRPM GINA extension will extend this GINA. In this way the functionality of the other GINA extension will stay. This concept is called GINA Chaining.

When are users blocked from SSRPM?

When a user answers several questions incorrectly after several configurable number of retries which prevents answer guessing by a possible attacker.

When a user is blocked from SSRPM, is this user locked out from Windows as well?

No. The user will only be locked out from SSRPM, which means that the user (temporarily) cannot use the SSRPM functionality.

Is it possible for a user to do a password reset when he or she is locked out from Windows?

Yes. During a password reset, the SSRPM Service will check if the user is currently locked out from Windows. If so, the service will automatically unlock the user.

Does SSRPM support multiple platforms?

Yes. SSRPM supports multiple platforms, databases, applications and a lot more via User Management Resource Administrator (UMRA) with SSRPM's UMRA Connector. See: *UMRA Connector* on page 24 for more information.

Does SSRPM sent notifications when a user resets his or her password?

Yes. Within SSRPM you can configure e-mail notification per notification type. In this case a notification e-mail can be sent to multiple e-mail addresses, when a user resets his or her password. See: *E-mail notification* on page 15 for more information.

Does SSRPM support multiple languages?

Yes. SSRPM provides multilingual support for the languages: English, French, German, Italian, Spanish, Polish, Portuguese and Dutch. See: *Multilingual support* on page 35 for more information.

Does SSRPM support Windows Vista?

Yes. SSRPM fully supports Windows Vista and is shipped with an SSRPM Credential Provider to provide the 'Forgot My Password' button functionality within Windows Vista. In this case an extra 'Forgot My Password' link will be created on the Windows Vista desktop (See: *The SSRPM Reset Wizard* on page 31).

7. Appendices

7.1. Appendix A: Windows services

7.1.1. What is a service?

A service is a system application which is running continuously in the background without any visual output. Like the name, these 'long-running' applications are providing a 'service' for other applications called 'clients'. One or more client(s) can connect with a service which handles specific requests from these clients (sometimes at the same time).

7.1.2. The service account

A service must log on to the network, just like a user does. The service account is the user account that is used to allow a service to run on a server or workstation.

The SSRPM Service

By default the SSRPM creates a service account (unless it already exists) within the 'Service installation wizard', which will be created for the SSRPM Service only. This account must be a member of an existing group which has enough access rights to make changes in the Active Directory (by default the user group 'Domain Admins' is used). In this way the SSRPM Service can unlock accounts and reset passwords.

7.1.3. Service communication

Clients communicate with a service via a TCP/IP communication protocol and port on which this service is continuously listening. This means that this port must be available (so that no other application is using this port) on the machine where the service is running on.

The SSRPM Service

The SSRPM Service uses encrypted RPC as a communication protocol on top of TCP/IP and listens on port 37946 by default. This port number will be used by the SSRPM Enrollment Wizard and SSRPM Reset Wizard, when they connect to the SSRPM Service.

When the SSRPM Service uses another port number, the SSRPM Enrollment Wizard and SSRPM Reset Wizard must use the same port number as well. In this case, the port number must be specified in the client workstation's registry on which the SSRPM User Client Software is installed.

7.2. Appendix B: Group Policy Objects

7.2.1. What is a Group Policy Object?

A Group Policy Object or GPO is a Microsoft technology in which you can manage specific Microsoft Windows configuration parameters centrally within an Active Directory environment. In this way multiple computers (a machine GPO) or users (a user GPO) can be updated via a simple change to a single GPO.

Each time when you start a computer which is member of a domain or OU, this computer checks for GPO's. When starting, the computer will check and apply installed machine GPO's first of all (even before you'll see the windows logon dialog). During a user logon, the computer will check and apply installed user GPO's, which are only applicable for the currently logged on user. This means that if another user logs on using the same computer, the installed user GPO's will be applied again for that user. This will only happen once per each user during the user's logon.

With a GPO you can control a target's (which can be a user or a computer) registry, NTFS security audit and security policy, logon/logoff scripts, folder redirection, Internet Explorer settings, software installation and more.

7.2.2. GPO's in SSRPM

With SSRPM, you can use GPO's to distribute the SSRPM User Client Software through your network. In this case you'll use a GPO to apply settings within the target's (one or more workstation(s) on which you want to install the SSRPM User Client Software) registry and software installation. See the "GPO Distribution Guide" for more information, of which the latest version is available on the *Tools4ever website* <http://www.tools4ever.com>.

7.3. Appendix C: SSRPM keywords

An SSRPM Keyword is a variable which can contain information, like for instance: the computer name from which a user performs a password reset. SSRPM Keywords can be used for notification e-mails or passing information to User Management Resource Administrator (UMRA) when evoking UMRA Projects (when a password reset or enrollment event occurs).

This section contains lists of all SSRPM keywords which can be used. These lists are divided into the following columns:

- *Short Description*: a brief description of the SSRPM keyword. A longer description can be found in the SSRPM Service Configuration (variable list within the UMRA tab) within the SSRPM Admin Console.
- *SSRPM Keyword*: the keyword name, which represents a particular value (such as for instance: Block Time, account name etc.)
- *UMRA Variable*: the UMRA Variable which is assigned to the SSRPM Keyword. This variable will contain the value of the SSRPM Keyword when an UMRA Project will be evoked throughout SSRPM. See: *UMRA Connector* on page 24 and: *Setup the UMRA connection* on page 25 for more information. By default, certain UMRA Variables are assigned to SSRPM Keywords.
- *Type*: the type of keyword, which is divided into:
 - String: a sequence (array) of characters, like for instance: "John"
 - MultiString: Comma-separated list of strings, like for instance: "john@tools4ever.com, sally@tools4ever.com" etc.
 - Time: The date and time formatted as: "year/month/day hours:minutes:seconds", for instance: "01/10/2007 14:05:27"
 - Number.
- *Available*: indicates when the keyword contains a value, which can be when a user enrolls (enrollment), resets his or her password (Reset Account) or both (Always).

User keywords

User keywords are SSRPM keywords which are applicable for a user. See below for a list of all available user keywords:

Short Description	SSRPM Keyword	UMRA Variable	Type	Available
Distinguished Name	%DISTINGUISHEDNAME%	%UserODN%	String	Always
Enrollment Time	%ENROLLMENTTIME%	%SsrpmEnrollmentTime%	Time	Always
Block Time	%BLOCKTIME%	%SsrpmBlockTime%	Time	Always
Reset Time	%RESETTIME%	%SsrpmResetTime%	Time	Always
Profile used to enroll	%USERPROFILE%	%SsrpmUserProfile%	String	Always
Block Count	%BLOCKCOUNT%	%SsrpmBlockCount%	Number	Always
Reset Count	%RESETCOUNT%	%SsrpmResetCount%	Number	Always
Account ID	%ACCOUNTID%	%SsrpmAccountID%	Number	Always
Account Name	%ACCOUNTNAME%		String	Always
Profile options used to enroll	%ENROLLMENTOPTIONS%		Number	Always

Profile keywords

Profile keywords are SSRPM keywords which are applicable for an SSRPM Profile. See below for a list of all available profile keywords:

Short Description	SSRPM Keyword	UMRA Variable	Type	Available
SSRPM Profile Name	%PROFILENAME%		String	Enrollment
SSRPM Profile Options	%PROFILEOPTIONS%		Number	Enrollment
Number of administrator defined questions	%ADMINDEFINED QUESTIONS%		Number	Enrollment
Number of user defined questions	%USERDEFINED QUESTIONS%		Number	Enrollment
The time a user has been blocked	%BLOCKDURATION%		Number	Enrollment
Number of incorrect questions needed to block a user	%BLOCKONINCORRECT ANSWERCOUNT%		Number	Enrollment
The time to reset the invalid answer count	%BLOCKONINCORRECT ANSWERCOUNT RESETTIME%		Number	Enrollment
Minimum answer length	%MINIMUM ANSWERLENGTH%		Number	Enrollment
Enrollment notification e-mail addresses	%NOTIFYENROLLEMAIL%		MultiString	Enrollment
Reset notification e-mail addresses	%NOTIFYRESETEMAIL%		MultiString	Enrollment
Block notification e-mail addresses	%NOTIFYBLOCKEMAIL%		MultiString	Enrollment
Notification types	%NOTIFICATIONTYPES%		Number	Enrollment
Excluded OU's	%EXCLUDEDOUS%		MultiString	Enrollment

Question and answer keywords

Question and answer keywords contain a list of questions or answers provided by the user. See below for a list of all available question and answer keywords:

Short Description	SSRPM Keyword	UMRA Variable	Type	Available
Questions selected by the user	%QUESTIONS%	%SsrpmUserQuestions%	MultiString	Always
Answers (if available) provided by the user.	%ANSWERS%	%SsrpmUserAnswers%	MultiString	Enrollment
Encrypted answers (if available) provided by the user.	%ENCRYPTEDANSWERS%		MultiString	Enrollment

Computer keywords

Computer keywords contain information about the computer from which a user resets his or her password or enrolls into SSRPM. See below for a list of all available computer keywords:

Short Description	SSRPM Keyword	UMRA Variable	Type	Available
Source Computer	%USERCOMPUTER%	%SsrpmUserComputer%	String	Always
Source IP-address	%USERIPADDRESS%	%SsrpmUserIPAddress%	String	Always

Other keywords

See below for a list of all remaining keywords:

Short Description	SSRPM Keyword	UMRA Variable	Type	Available
New password provided by the user.	%PASSWORD%	%SsrpmUserPassword%	String	Reset Account
Event type: ENROLL, RESET, or BLOCK	%EVENT%	%SsrpmEvent%	String	Always

SSRPM Service computer	%SSRPMSERVICE COMPUTER%	%SsrpmServiceComputer%	String	Always
SSRPM Service domain	%SSRPMSERVICE DOMAIN%		String	Always

E-mail keywords

The E-mail keywords are extra keywords which can only be used within a notification e-mail and cannot be assigned to an UMRA variable. See below for a list of all available e-mail keywords:

Description	SSRPM Keyword	Type	Available
The name of the OU in which the user is located.	%OU%	String	Always
The number of times the current user has failed to reset his or her password.	%FAILEDRESETCOUNT%	Number	Always
The canonical name of the user.	%CANONICALNAME%	String	Always

8. Glossary

A

Active Directory

A hierarchical collection of network resources, which can contain users, computers, printers, and other Active Directories. Active Directory Services (ADS) allow administrators to handle and maintain all network resources from a single location.

Administrator Defined Questions

Questions which are selected from the 'Default questions'-list. The default questions are shipped with SSRPM, which are editable.

C

Client

A piece of software that accesses services from another piece of software (a server), often remotely over a computer network.

D

Domain

A Windows Domain is a logical grouping of computers that share security and user account information.

Domain Controller

A server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources. A DC stores user account information, authenticates users and enforces security policy for a Windows domain.

E

Encrypted RPC

RPC data which is send encrypted, using an encryption algorithm. This increases security between clients and services.

Encryption

The transformation of data or plain text into an unreadable form through a mathematical process, which is an effective way to achieve data security.

G

GINA

An abbreviation for "Graphical Identification aNd Authentication", which is a DLL file called msgina.dll that's responsible for the bit of code that displays the "Press CTRL+ALT+DEL to log on" and that accepts your username and password.

GINA Chaining

In case more than one GINA extensions are installed (in a specific order) on a computer. The "Winlogon" system calls the last installed extension, which calls the next installed extension and eventually the standard Microsoft GINA (msgina.dll).

GINA Extension

An extension on the standard Microsoft GINA, to add extra functionality. SSRPM extends the GINA with its own GINA extension called SSRPMGINA.dll.

Group Policy Object

A Microsoft technology in which you can manage specific Microsoft Windows configuration parameters centrally within an Active Directory environment.

H

Hash value

An irreversible unique value, which is the result of a mathematical process, with the help of a hash algorithm (like MD5). Commonly known as "fingerprint".

M

MD5

A (Message Digest) hash algorithm, which can be used for the creation of an irreversible hash value. Commonly used hash algorithms are: MD2, MD5, SHA and Blowfish.

MSI-Package

An installer package to install third party software. Can be used within a GPO to install software within a Windows 2000 or Windows 2003 environment.

O

Organizational Unit

An Active Directory container object which can contain users, computers, groups, resources, and other Organizational Units (OU's).

P

Password Complexity

A password requirement (containing a set of password rules), which prevents weak passwords for better password security.

R

RPC

An abbreviation of Remote Procedure Call, a communication protocol, which allows communication between client and server.

S

Service

An application which is running continuously (most likely on a server) in the background without any visual output, providing functionality for clients which communicate with this service.

SSRPM Admin Console

Used by the system administrator to install, manage, configure and monitor the SSRPM Service.

SSRPM Credential Provider

A component of the SSRPM User Client Software, for the creation of an extra 'Forgot My Password...' link on the Windows Vista logon screen. In Windows Vista, the GINA architecture is replaced with a new Credential Provider model. Therefore, the SSRPM Credential Provider will be used instead of the SSRPM GINA, to provide this functionality.

SSRPM Enrollment Wizard

Before an end-user can reset his or her password, it is necessary for each user to enroll into SSRPM with the SSRPM Enrollment Wizard. The enrollment consists of defining and answering a set of challenge questions.

SSRPM GINA DLL

A component of the SSRPM User Client Software. For the creation of the extra 'Forgot My Password' button, an extension on top of the existing Windows logon software (GINA) is needed. This is realized by the SSRPM GINA DLL, which extends the Windows logon dialog with this extra functionality.

SSRPM Keywords

SSRPM Keywords are values in which information is stored. For instance: the new password specified by a user when this user resets his or her password. See: *Appendix C: SSRPM keywords* on page 43 for more information and a list of all available SSRPM Keywords.

SSRPM Profile

An SSRPM configuration (security settings and questions) with one or more assigned OU's or a domain.

SSRPM Reset Wizard

When an end-user is enrolled into SSRPM, the user uses the SSRPM Reset Wizard to reset his or her password by answering his or her defined questions. This wizard is made available via a "Forgot My Password" button at the bottom of the Windows logon dialog.

SSRPM Service

A Service which handles requests from the Admin Client and User Client Software and stores all user data in a database.

SSRPM User Client Software

Software available for all end-users to use SSRPM, which needs to be installed on each client workstation.

U

User Defined Questions

Questions which the end-user needs to define when the user is enrolling.

9. Index

A

- Account blocking • 15
- Active Directory • 46
- Administrator Defined Questions • 46
- Appendices • 41
- Appendix A
 - Windows services • 2, 7, 41
- Appendix B
 - Group Policy Objects • 10, 39, 42
- Appendix C
 - SSRPM keywords • 24, 25, 26, 43, 47

C

- Client • 46

D

- Database • 23
- Distributed installation • 8, 10
- Domain • 46
- Domain Controller • 46

E

- E-mail • 15, 23
- E-mail notification • 15, 23, 40
- Encrypted RPC • 46
- Encryption • 46
- Enrollment management • 19
- Enrollment Options • 18
- Evaluation installation • 8

F

- Frequently Asked Questions (FAQ) • 39

G

- General installation • 6
- General Options • 16
- GINA • 46
- GINA Chaining • 46
- GINA Extension • 46
- GPO's in SSRPM • 42
- Group Policy Object • 46

H

- Hash value • 46
- How does SSRPM work? • 2

L

- Logging • 23

M

- Manual installation • 8, 9
- MD5 • 46
- MSI-Package • 46
- Multilingual support • 35, 40

O

- Organizational Unit • 46

P

- Password Complexity • 47
- Profile options • 15, 33

Q

- Questions • 7, 14, 28, 36

R

- Registry Settings • 34
- Reset Options • 20
- RPC • 47

S

- Security • 24
- Service • 47
- Service communication • 27, 41
- Setup the UMRA connection • 25, 43
- SSRPM Admin Console • 11, 47
- SSRPM architecture • 2
- SSRPM concept • 2
- SSRPM Credential Provider • 47
- SSRPM Enrollment Wizard • 47
- SSRPM GINA DLL • 47
- SSRPM installation • 3, 6
- SSRPM Keywords • 47
- SSRPM Profile • 47
- SSRPM Profile assignment • 21
- SSRPM Profiles • 9, 10, 13
- SSRPM Reset Wizard • 47
- SSRPM security • 5
- SSRPM Service • 23, 47
- SSRPM User Client Software • 27, 47
- SSRPM User Client Software User Interface • 27, 35
- Step 1
 - Install and setup UMRA • 25
- Step 2
 - Create an UMRA project • 25, 26
- Step 3
 - Configure the SSRPM Service • 26
- System requirements • 6

T

- Test SSRPM locally • 9
- Test SSRPM on another computer • 9
- The 'Blocked Users' overview • 13
- The dashboard overview • 11

- The 'Enrolled Users' overview • 12
- The 'Not-Enrolled Users' overview • 12
- The 'Reports' overview • 13
- The service account • 41
- The SSRPM Admin Console • 3
- The SSRPM Enrollment Wizard • 9, 10, 28
- The SSRPM Reset Wizard • 9, 10, 31, 40
- The SSRPM Service • 2, 41
- The SSRPM Service installation • 6, 8
- The SSRPM User Client Software • 3
- The SSRPM User Client Software installation • 6, 7
- Translation • 37

U

- UMRA Connector • 24, 40, 43
- Use another language • 36
- Use multiple languages • 37
- Use the default language (English) • 36
- User Defined Questions • 47
- Using SSRPM • 11

W

- Welcome to SSRPM • 1
- What is a Group Policy Object? • 42
- What is a service? • 41