

SELF SERVICE RESET PASSWORD MANAGEMENT
IMPLEMENTATION GUIDE

*Copyright © 1998 - 2020 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.
www.tools4ever.com*

Contents

| | |
|--|-----------|
| 1. Introduction | 1 |
| 2. Software Requirements | 1 |
| 3. Common Scenario | 1 |
| 3.1. Admin Console | 1 |
| 3.2. SSRPM Service | 2 |
| 3.3. SSRPM User Client Software | 3 |
| 3.3.1. Components | 3 |
| 3.3.2. Installation | 4 |
| 4. Advanced Configuration Options | 4 |
| 5. Frequently Asked Questions (FAQ) | 5 |
| 6. Known Implementation Issues | 6 |
| 6.1. General | 6 |
| 6.2. SSRPM User Client Software | 6 |
| 6.3. GINA | 7 |
| 6.4. Web Interface | 7 |
| 6.5. Common Error Codes | 8 |
| 7. Index | 11 |

1. Introduction

The document describes the most common implementation scenario for SSRPM. The document describes which steps must be taken to install SSRPM in the network. Detailed information on how to install specific parts of SSRPM can be found in the Administrator's Guide, the COM Object Guide and the GPO Distribution Guide.

A separate chapter called 'Known Implementation issues' describes problems that can be encountered when implementing SSRPM in the network.

2. Software Requirements

Operating Systems:

- Windows Server 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
- Windows Vista
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

Databases:

- Microsoft Jet Engine (Installed by default on all supported OSes)
- Microsoft SQL Server (2005, 2008, 2012 or 2014 and Express, Standard or Enterprise)

3. Common Scenario

To implement SSRPM in the network several programs must be installed. This chapter describes which programs must be installed, how they must be installed and what they do.

3.1. Admin Console

The first program that must be installed is the SSRPM Admin Console. The Admin Console is used by administrators to install, update and configure the SSRPM Service. Detailed status information can also be viewed with the Admin Console.

Admin Console Main Features:

- Show enrolled users, not enrolled users and blocked users
- Show Service Events
- Create and Edit reports
- Create and Edit Enrollment Profiles
- Install and Update SSRPM Services
- Add licenses.

Admin Console Installation:

The Admin Console can be installed on any Windows 2008, 2012, 7, 8 or 10 machine using the SSRPM setup that can be downloaded from www.tools4ever.com The setup is called 'SetupSSRPM.exe'.

3.2. SSRPM Service

The SSRPM Service is the 'workhorse' of SSRPM. The Admin Console and the SSRPM User Client Software all connect to this service to view information, configure, enroll and reset.

SSRPM Service Main Features:

Generate and send scheduled reports.
Enroll users, check user answers, reset passwords.
Manage the SSRPM configuration.

SSRPM Service Installation:

The SSRPM Service can be installed using the Admin Console. The "Administrators Guide" and the Admin Console Online help contain detailed information on how to install the SSRPM Service.

3.3. SSRPM User Client Software

3.3.1. Components

The SSRPM User Client Software is installed on every workplace in the network. The SSRPM User Client Software consists of six parts:

Client launcher:

The client launcher is automatically run when

1. A user logs on to his machine
2. The shortcuts are used
3. The user clicks on the 'Forgot my password...' button at the Windows Logon screen.

The launcher determine which client application should be started, the browser client, the enrollment wizard or the reset wizard.

It does so based certain settings and parameters, some of which can be configured using GPO settings. By default will try detect which client it should start, where it will always try to start the Client Browser.

In order for it to start the Client Browser some requirements that have to be met:

1. It needs to be able to connect to the SSRPM service.
2. The Browser Client requires that the URL related to the action is a valid URL.
3. The web interface has to use HTTPS.
4. The URL has to point to the SSRPM web interface, other web sites are not allowed.

If either of these requirements is not met, it will default back to the enrollment- or reset wizard.

If the client launcher is automatically run when a user logs on to his machine, it will check if the user is enrolled. If the user is not enrolled, it will start the Browser client or the Enrollment Wizard so that the user can enroll into SSRPM.

Browser Client:

The browser client connect to the SSRPM web interface and based on the parameters it receives form the Client Launcher it can be used for enrollment or for resetting the user's password.

Enrollment Wizard:

The enrollment wizard is the legacy desktop client. And can be started by the client launcher depending on the settings.

Reset Wizard:

The reset wizard is the legacy desktop client. And can be started by the client launcher depending on the settings. This wizard asks the user to answer the specified amount of questions. If the user answers them correctly, he will asked to enter a new password. After clicking on the finish button, the password will be reset and (optionally) the account will be unlocked.

SSRPM GINA:

The SSRPM GINA is a 'GINA extension'. A GINA extension can be used for instance to alter the windows logon screen. SSRPM uses the GINA extension to place the 'Forgot my password...' button on the logon screen. The GINA is only used Windows XP and Windows Server 2003.

SSRPM Credential Provider:

The SSRPM Credential Provider is a 'Credential Provider'. A Credential Provider can be used for instance to alter the windows logon screen. SSRPM uses the Credential Provider to place the 'Forgot my password...' button on the logon screen.

3.3.2. Installation

There are multiple ways to install the SSRPM User Client Software, the common methods are manually, by using GPO distribution or by using other software deployment utilities (MS SCCM, Altiris, CA IT Client Manager, etc.). To install the SSRPM User Client Software manually, go to the Admin Console installation directory. (Usually c:\program files\tools4ever\SSRPM\Admin Console). Double click on the 'SsrpmUserClientSoftware.msi' MSI package and follow the wizard. To install the SSRPM User Client Software using GPO distribution, please refer to the "GPO Distribution Guide" for detailed information in this subject.

4. Advanced Configuration Options

SSRPM contains several advanced options that administrators can modify using the registry editor. Please note that these settings can only be applied on the machine on which the SSRPM service is installed and only when the SSRPM Service is stopped. All of the registry keys are located in HKEY_LOCAL_MACHINE.

Name: AllowAdminsToEnroll

Description: By default administrators are not allowed to enroll into SSRPM. Set this setting to '1' to allow administrators to enroll into SSRPM. *Warning: If an administrator resets his password and fails, the password of the Administrator can be changed to a very strong random password. Because of this the administrator will not be able to log in any more.*

Location: SOFTWARE\Tools4ever\SSRPM\Service\Security

Type: REG_DWORD

Values: Disabled = 0 (default), Enabled = 1

Name: UseRpcServerRegisterIfEx

Description: As of Windows 2003 SP1 the Windows RPC interface has changed. RPC calls must be authenticated before they are accepted. Because the SSRPM reset wizard runs from the logon screen, SSRPM RPC calls are not always authenticated. SSRPM can however request the operating system to allow unauthenticated RPC calls to SSRPM. Set this value to '1' to have SSRPM request that unauthenticated RPC calls are allowed (for SSRPM only)

Location: SOFTWARE\Tools4ever\SSRPM\Service\Connection

Type: REG_DWORD

Values: Disabled = 0 (default), Enabled = 1

Name: CustomDomainControllers

Description: Use this setting to instruct SSRPM to use a specific domain controller. If the specified domain controller is offline, SSRPM will use the next one in the list. If all of the domain controllers in the list are unavailable, SSRPM will search for an available domain controller.

Location: SOFTWARE\Tools4ever\SSRPM\Service\Advanced

Type: REG_MULTI_SZ

Values: domain1.local:domaincontroller1.domain1.local,domaincontroller2.domain1.local
domain2.local:domaincontroller1.domain2.local,domaincontroller2.domain2.local

Name: DsGetDCOptions

Description: Changing this options changes the way that SSRPM locates domain controllers. For instance settings this value to 128, will instruct SSRPM to search for and use the primary domain controller in the domain. Setting this value to 64 will instruct SSRPM to search for and use a domain controller that contains a global catalog.

Location: SOFTWARE\Tools4ever\SSRPM\Service\Advanced

Type: REG_DWORD

Values: 1= Force Rediscovery, 64 = Global Catalog Required, 128 = PDC Required

Name: UseNetUserChangePassword

Description: By default SSRPM uses the ADSI interface to reset passwords. Set this setting to 1 to disable the ADSI interface and to instruct SSRPM to use 'Net' calls to reset the users' password.

Location: SOFTWARE\Tools4ever\SSRPM\Service\Advanced

Type: REG_DWORD

Values: Disabled = 0 (default), Enabled = 1

5. Frequently Asked Questions (FAQ)

Where can I find SSRPM documentation?

A list of SSRPM documentation can be found here: [Documentation](#)

Does SSRPM Support password complexity rules?

Yes, SSRPM supports the default windows password complexity Rules.

What do the default password complexity rules enforce?

- A minimum password length of 8 characters.
- Use characters from at least three of the following categories: A, B, C, ... Z a, b, c, ... z 0, 1, 2, ... 9 !, \$, #, %, ...
- The password does not contain all or part of the account name of the user. Part of an account name is defined as three or more consecutive alphanumeric characters delimited on both ends by white space such as space, tab, and return, or any of the following characters: comma (,), period (.), hyphen (-), underscore (_), or number sign (#).

What about the rest of the password policy? (Like minimum password age)

SSRPM does enforce password history and minimum password length. Minimum and maximum password age are not enforced by SSRPM.

Is the communication between the clients and the SSRPM Service secure?

Yes. All of the communication between the clients is encrypted.

Which options are available through the GPO settings?

The "GPO Distribution Guide" contains a complete list of all available settings and a description of these settings.

Are the answers provided by users stored encrypted?

Yes, SSRPM uses an irreversible MD5 encryption to store the answers provided by users.

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 the "GPO Distribution Guide" for more information.

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.

Which databases does SSRPM support?

Currently SSRPM supports Microsoft SQL Server and Microsoft Jet (Access).

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.

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 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.

Does SSRPM support Windows 7 and higher?

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.

Does SSRPM have a reporting feature?

Yes. Reports can be scheduled to be generated at specific times. They can also automatically be emailed to specified email addresses.

Can I edit these reports?

Yes. The reports and their components can be fully customized.

6. Known Implementation Issues

This chapter describes known implementation issues as well as common error codes.

6.1. General

I am trying to do something, but I keep getting errors like 0x80005008. What is the problem?

The error that you receive can have several causes. It is however likely that it is a problem with the database. Please view the 'Common Error Codes' chapter for possible solutions.

6.2. SSRPM User Client Software

I installed the SSRPM Client Software on a machine and now it won't boot any more!

This is commonly caused by a conflict of the SSRPM GINA with a custom GINA that was already installed on the machine. Please check the GINA chapter for solutions on how to fix this problem.

How can I distribute the SSRPM Client Software to every machine in my network?

This can be done through a Group Policy Object (GPO). Please refer to the 'GPO Distribution Guide' for a detailed description.

I keep getting error ... when running one of the wizards!

Please refer to the 'Common Error Codes' chapter for information on most common errors.

The Enrollment Wizard does not start automatically when I log in!

The Enrollment Wizard only runs if a user is not enrolled. However the Enrollment Wizard does not check if a user is enrolled every time to minimize the load on the SSRPM Service. This behaviour can be changed by editing the 'SSRPM Enrollment Wizard Enrollment Check Interval' in the SSRPM GPO. Set the value to 0 to have the Enrollment Wizard always check if the user is enrolled.

The Enrollment Wizard generates errors when a user logs in, how do I disable them?

Enable the settings 'Disable messages during Enrollment Wizard autostart' in the GPO. For a complete guide on the SSRPM GPO, please refer to the "GPO Distribution Guide".

6.3. GINA

I installed the GINA on a machine and now it won't boot anymore!

The most common reason why this happens, is if another incompatible GINA has been installed on the machine. This can either result in an error message like: 'SSRPMGINA.dll failed to load' or a blue screen. The machine can be made available again using the following method:

1. Boot the machine in safe mode. (Press F8 during boot and select 'safe mode' from the menu)
2. When logged on, open the registry editor. (Go to Start --> Run... and type 'regedit', then click on OK)
3. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Tools4ever\SSRPM\GINA and write down or copy the value data that is specified in the 'Old GINA Location'. (Please note that this value is not always available)
4. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\WinLogon
5. If a value was present in the 'Old GINA Location', paste it in the 'GINADLL' value data. If the value 'Old GINA Location' was empty or did not exist, delete the 'GINADLL' value.
6. Reboot.

I installed the GINA on a machine, but the controls overlap with another GINA extension that is installed.

The SSRPM GINA as well as other GINA's usually places the controls (Like the 'Forgot my password...' button) relative to the bottom of the logon screen. This is not a problem if only one GINA extension is installed. However if two GINA's are installed that both position the controls relative to the bottom of the screen, they will overlap. To solve this problem, the SSRPM GINA can be configured to position the controls relative to the 'OK' button on the logon screen. To do this, set the 'GINAControlPosition' value in the SSRPM GPO to 1. (For more information on GPO's, please refer to the GPO Distribution Guide)

Which programs with a GINA extension are compatible with SSRPM?

- Entrust Entelligence
- NetPro SelfServiceAdmin
- OneSign SSO
- Citrix / Terminal Server

Which programs with a GINA extension are not compatible with SSRPM?

- Novell Client

I have a program with a GINA extension that is not listed as compatible. Can I use SSRPM?

Yes. Most GINA extensions are compatible with SSRPM.

6.4. Web Interface

How do I install the SSRPM Web Interface?

The "Web Interface Guide" describes how to install the Web Interface in detail.

6.5. Common Error Codes

| | |
|-------------|--|
| -1 | General error. |
| -2 | Version Mismatch. This usually means that the version of the SSRPM Service and the client do not match. Please upgrade all SSRPM Software to the same version. |
| -3 | Operation canceled. |
| -4 | Operation timed out. |
| -5 | Unknown archive version. |
| -6 | SID invalid, |
| -7 | Service unavailable. |
| -8 | SMTP communication failed. |
| -9 | If a user receives error code -9, it means that he has answered too many questions incorrectly and is blocked from SSRPM for a specified amount of time. |
| -10 | If a user receives error code -10, it means that a profile for his domain/OU has not been configured. |
| -11 | Incorrect answers. |
| -12,-13,-14 | This error is generated if none of the installed licenses are valid for the user trying to enroll/reset his password. |
| -15 | Server not specified. |
| -16 | Service is unreachable. |
| -17 | Incorrect type. |
| -18 | Incorrect size. |
| -19 | Pointer is null. |
| -20 | Error cracking name. |
| -21 | The user trying to enroll/reset his password is in a domain/OU that has been excluded from SSRPM. Excluded OU's can be configured in the advanced profile configuration in the SSRPM Admin Console. |
| -22 | Incorrect answer index. |
| -23 | Immediately checking is not allowed. |
| -24 | Unknown question. |
| -25 | Item already exists. Occurs usually during updating the database or templates files. In case of the template files it usually means that one of the included files (e.g. logo) is already stored in the database. |
| -26 | The password reset functionality has been disabled. |
| -27 | The unlock account functionality has been disabled. |
| -28 | No questions were specified |
| -29 | Access denied: There are several reasons to why the error occurs. |
| 5 | -The user is a member of 'Domain Admins'. For security reasons, Domain Admins are not allowed to enroll in SSRPM. -The user is not a member of the group(s) specified in the SSRPM Service Security settings for 'Users'. Go to 'Service Management --> Configure...' in the Admin Console and select the 'Security' tab to configure the users that are allowed to enroll/reset. -The user is explicitly denied access to the SSRPM Service in the SSRPM Service Security settings. Go to 'Service Management --> Configure...' in the Admin Console and select the 'Security' tab to configure which users/groups are explicitly denied access. -The remote server running the SSRPM Service is blocking the connection. This can have several causes. 1. The server is running a firewall and blocking the connection from the SSRPM Wizards to the service. 2. A secure channel could not be created between the machine running the SSRPM User Client Software and the machine running the SSRPM Service. This issue can occur for instance when the machine is not a member of the domain or when the trust relation between the machines fails. -The machine running the SSRPM Service does not allow unauthenticated RPC calls. This can be resolved by enabling the advanced option 'UseRpcServerRegisterIfEx' described in the 'Advanced Configuration Options' chapter. |
| -30 | User doesn't have enough rights to use SSRPM. |
| -31 | User has been denied access to SSRPM. |
| -32 | Administrators have been denied access to SSRPM. |
| -33 | The license key is corrupt. Ask your sales contact for a new license key. |
| -34 | The password has been reset too many times in the last x minutes. Either adjust the profile settings or wait the configured time before trying again. |

- 35 The license key is no longer supported
- 36 The specified phonenumber is invalid.
- 37 The specified email address is invalid.
- 38 Advanced authentication has been disabled.
- 39 Unknown advanced authentication method.
- 40 The specified PIN code is incorrect.
- 41 The SMS bundle is invalid.
- 42 The SMS gateway's response was invalid.
- 43 An error occurred while sending the SMS.
- 44 The HD caller ID functionality can not be used due to a wrong encryption method.
- 45 The HD caller ID functionality has been disabled.
- 46 Invalid account name.
- 47 Uninitialize data. In most cases this means that the function of the COM object requires another function to be called first.
- 48 The specified e-mail address has been denied because it is part of the excluded e-mails domains specified in the profile.
- 49 The offline logon functionality has been disabled.
- 50 The change passowrd functionality has been disabled.
- 51 Invalid authentication sequence type.
- 52 The user did not earn enough authentication credits to reset his password.
- 53 Unable to authenticate user. This error means that there is no available means to reset the user's password i.e. no questions/answers, no e-mail address and no mobile phone number. If the advanced authentication sequence is enabled it usually means that the user is unable to collect sufficient credits due to a bad configuration.
- 54 An error occurred while decrypting data. This can occur when the service account has been changed.
- 55 The selected option has been disabled.
- 56 The user must specify either a e-mail address or a phone number to continue.
- 57 The specified answer and confirmation answer don't match.
- 58 An specified password is invalid. The password is empty or does not meet the requirements.
- 59 The web token expired. The browser client expects a token in the web interface to proof that the shown web site is the SSPRM web site. This web token is only valid for a limited time.
- 60 The web token invalid. The browser client expects a token in the web interface to proof that the shown web site is the SSPRM web site. If this token is missing or incorrect this error message is shown. Common issues include a not specifying the server name, SSL certificate issues or starting the browser client directly.
- 61 The specified phone number has not been validated by PIN during enrollment.
- 62 The specified e-mail address has not been validated by PIN during enrollment.
- 63 The specified password and confirmation password do not match.
- 64 The specified input value can not be empty. The input for that specific AD attribute can't be empty.
- 65 The specified input value is invalid. The input for that specific AD attribute does not meet the validation requirements specified in the profile.
- 66 The AD self service functionality has been disabled.
- 67 The AD self service is enabled but no attributes have been configured. Use the Admin Console to properly configure this functionality.
- 68 The specified answer can't be contained within the question.
- 69 The user is trying to onboard but the onboarding start date of the user is later than the current date.
- 70 The SMS bundle is empty
- 71 Too many message (SMS) were sent by the user today.

0x80005008, Database problem. This can have several causes:
0x80040E14, -Database failed to upgrade. This can be solved by manually forcing a database upgrade. Go to
0x80040E21, 'Service Management --> Configure...' and select the 'Database' tab. Then click on the 'Database
0x80040E1D Maintenance' button. Check the 'Force Full Upgrade' checkbox and click on the 'Upgrade Database'
button. You will most likely receive one or more errors which can safely be ignored.
-Database unavailable. Please make sure that the connection to the database is up and running. Go
to 'Service Management --> Configure...' and select the 'Database' tab. Click on 'Connection String
Wizard...' to recreate the connection string and verify the connection.

0x8007202F, This error usually occurs when a user tries to reset his password and fails because one of the rules
0x800708C5 specified in the password policy is violated.
2245

7. Index

A

Admin Console • 1
Advanced Configuration Options • 4

C

Common Error Codes • 8
Common Scenario • 1
Components • 3

F

Frequently Asked Questions (FAQ) • 5

G

General • 6
GINA • 7

I

Installation • 4
Introduction • 1

K

Known Implementation Issues • 6

S

Software Requirements • 1
SSRPM Service • 2
SSRPM User Client Software • 6
SSRPM User Client Software • 3

W

Web Interface • 7