SSRPM

ARCHITECTURE & PREREQUISITES

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Index

Introduction

Self-Service Reset Password Manager (SSRPM) is as easy to install as it is to use. The solution's primary functionality provides users with a method to reset their passwords after completing pre-answered challenge questions to verify their identity. SSRPM integrates a wide choice of configuration options to provide your organization with greater flexibility. For example, configuration options allow system administrators to define or modify passwords as well as enforce multifactor authentication.

SSRPM allows:

- Network users with a domain computer to reset their password in case of forgotten credentials and/or locked accounts due to repeated incorrect entry.
- External network users who access services via Active Directory (AD) account (e.g., VPN, Intranet, Extranet, Messaging) to reset their password in case they have forgotten it or have been locked out.

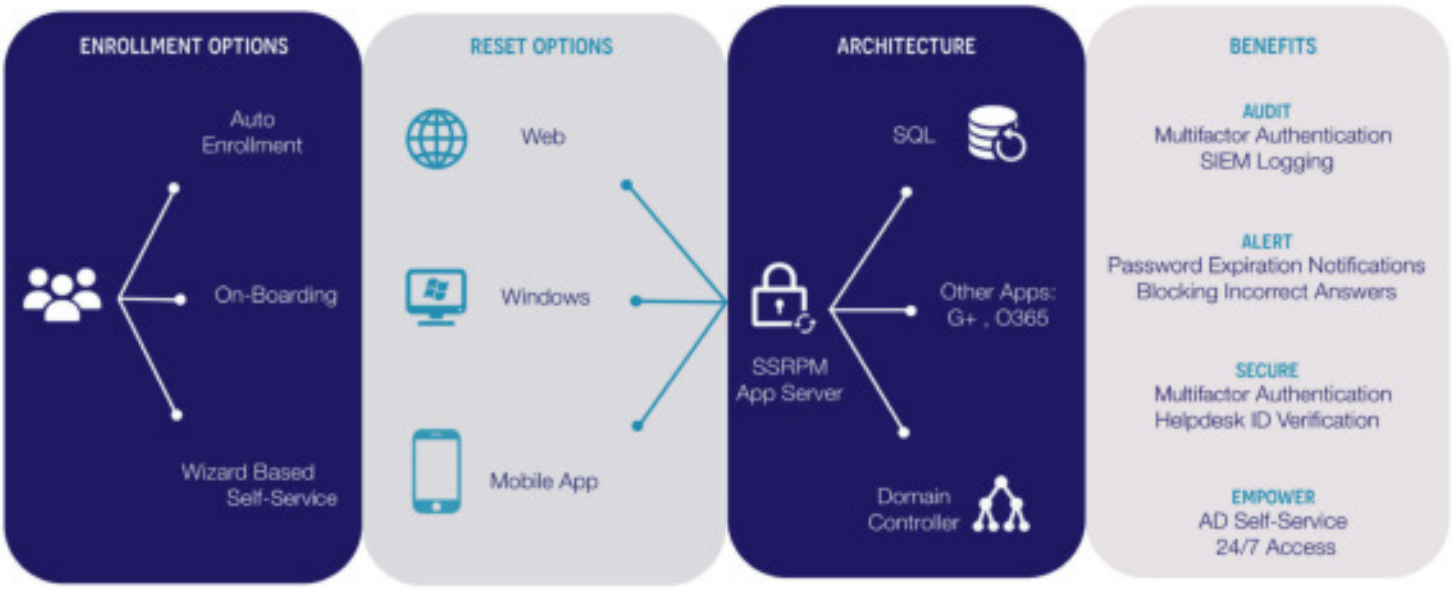
This document contains information regarding SSRPM's architecture and implementation prerequisites, providing a more technical understanding of the solution than can be found in our overview material.

Technical Architecture

SSRPM is an on-premise software package that installs on a Microsoft Windows server. It consists of the following elements:

- An application server, which hosts the SSRPM service. This is the service that fulfills requests to reset passwords or unlock accounts.
- An SQL database, which stores SSRPM configurations and user-provided information (e.g., answers to challenge questions).
- An IIS service, which hosts the application's graphical interfaces for end users.
- An SSRPM client deployed on network workstations, which allows users to register and then access the reset interface.

The diagram below describes the different functional options of SSRPM:



Server Prerequisites

SSRPM requires a Microsoft Windows server to operate. The requirements of which are as follows:

- Microsoft Windows Server from 2012r2 (May be physical or virtual)
- Domain member (or trust relationship with the domain) of the desired SSRPM perimeter
- 2 current CPUs
- 8 GB RAM
- 60 GB of HDD; a single partition is sufficient
- SQL server instance (version from 2008 (SQL Express is accepted and/or the instance may be hosted on another server (shared database server))
- Role IIS with .net 4.x (or higher), activated with Windows Authentication.
- An internal domain IIS certificate must be created in order for the interfaces to support HTTPS

SSRPM provides two options that allow external users to access the service via internet connection:

Option 1: Expose the IIS of the SSRPM server on the Internet via a reverse Proxy (type F5)

Option 2: (Recommended): Expose the SSRPM service via an additional server placed in your DMZ. The prerequisites for this server placed in your DMZ are as follows:

- Microsoft Windows Server from Server 2012r2 (May be physical or virtual)
- Domain member (or trust relationship with the domain) of the desired SSRPM perimeter
- 2 current CPUs
- 8 GB RAM
- 60 GB of HDD; a single partition is sufficient
- Role IIS with .net 4.x (or higher) enabled
- An Internet domain certificate (Wildcard) must be installed on the server so that interfaces support HTTPS

Service Account Prerequisites

SSRPM requires a service account installed on the application server to fulfill reset requests or unlock accounts. SSRPM service accounts require sufficient rights to operate, as specified below:

- Local admin of SSRPM server
- During implementation, the service account requires SysAmind rights, which are downgraded to DBOwner for operation. A a local SQL account may be used as an alternative to a Windows account for this.
- Email Send rights
- Delegation of AD rights as follows:
  - Object:
    - Read All Properties
    - Reset password
  - Properties:
    - Write pwdLastSet
    - Write userAccountControl
    - Write lockoutTime

Note that the service account can be an MSA (Managed Service Account). More MSA information may be found here: https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/managed-serviceaccounts-understanding-implementing-best / ba-p / 397009

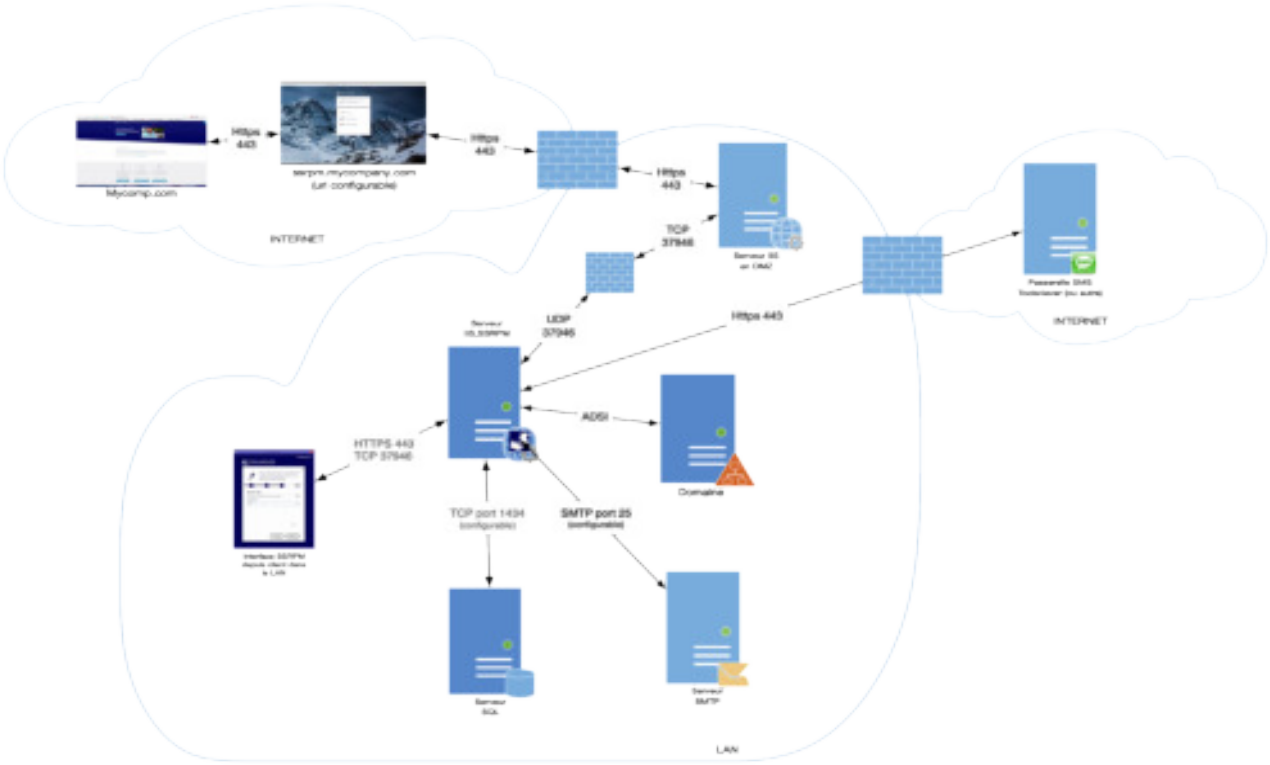
Network Prerequisites

SSRPM requires that several network ports be accessible to operate properly:

- Port 37946 from workstations to SSRPM server
- Port 37946 between the DMZ server and the application server (if DMZ option chosen)
- Port 25 from the SSRPM server to the SMTP server (configurable port)
- Port 443 (https) from the SSRPM application server to the SMS gateway
- Port 1434 between the SSRPM server and the database server (if different)

The Architecture Diagram below describes these flows:

Note: The 3 “server” components, namely the SSRPM service, the IIS Role, and the SQL instance can be hosted on the same server (physical or virtual).



FAQ

This chapter answers the most frequently asked SSRPM questions regarding architecture and prerequisites.

1. How do you trace the actions? Do we have access to logs?

In addition to the domain controllers' standard security logs, all actions performed through the application are recorded into a table in the SSRPM database.

Logged actions are: Registration, Reset, Unlocking, and Unsuccessful Attempts (including incorrect answers to challenge questions or MFA prompts). SSRPM generates exhaustive reports from this data according to a configured schedules (e.g., weekly, monthly, yearly).

2. Should SSRPM be implemented on each domain of the AD forest? How does SSRPM manage a multi-domain environment?

One service is sufficient. For multi-domain environments, the service account must be approved by all domains with the rights to reset passwords or unlock accounts.

3. How does SSRPM remain GDPR compliant in regards to emails and phone usage?

All email and phone data is stored in an encrypted database with a certificate as an internal "secret" within SSRPM. Answers to challenge questions are irreversibly encoded via SSHA 256 to make the data unusable outside of SSRPM.

When individual users register with SSRPM, they will be presented with an explanation of this encryption as well as how the data will be used.

4. Where will the “forgotten password” link be?

The “forgotten password” link can be found:

- Integrated with the initial login prompt required to authenticate into AD on a domain computer
- On the home page of an integrated portal (e.g., HelloID, intranet, extranet, or other web portal)

5. What is the difference between “Change Password” and “Forgotten Password”?

- “Change Password” allows a user to change their password after having already logged in.
- “Forgotten Password” allows a user to change their password before logging in by answering challenge questions or providing a PIN code to authenticate themself.

6. How does SSRPM manage individual user enrollment and registration?

Users are prompted to enroll and register upon opening a guide.

7. How does SSRPM manage users following their deactivation or removal?

If a given user is deactivated or removed from AD, they are automatically removed from the SSRPM system. The same removal occurs if revoking a given user’s SSRPM authorization without other AD changes. SSRPM authorizations are configured according to OUs and group memberships.

8. Is SSRPM compatible with Citrix Storefront/TSE?

Yes, SSRPM is compatible with Citrix and Terminal Server. Specific documentation on the operation of SSRPM with Citrix and TSE is available on our website.

About Tools4ever

Tools4ever is one of the largest vendors in Identity Governance & Administration with over 10 million managed user accounts.

For over 20 years, Tools4ever has developed and delivered several software solutions and consultancy services such as User Provisioning, Downstream Provisioning, Workflow Management, Employee Self-Service and Access Governance (RBAC). In the area of Password Management, Tools4ever offers Single Sign-On and Self-Service Password Reset among others.

Tools4ever's Identity Governance & Administration (IGA) solutions are installed in organizations from various sectors ranging in size from 300 to over 200,000 user accounts.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER New York

Address 300 Merrick Road, Suite 310
Lynbrook NY 11563
USA

Phone 1-866-482-4414
Website tools4ever.com

Info nainfo@tools4ever.com
Sales nasales@tools4ever.com

TOOLS4EVER Washington

Address 11515 Canyon Road E
Puyallup WA 98373
USA

Phone 1-888-770-4242
Website tools4ever.com

Info nwsales@tools4ever.com
Sales nwsales@tools4ever.com