WM Software
Safe AutoLogon™
Password Server

Centrally manage Windows® automatic logons securely with

Safe AutoLogon Password Server

Product Overview

Software version: 9.1
wmsoftware.com

Contents

Introduction

There has always been a way of automatically logging on to Windows by storing the username, password, and domain name in the Registry. But this poses a serious security risk because using the built-in Windows Registry method stores its logon credentials in ***unencrypted clear text***. This is an obvious security hole and risk. Another problem with this method is the user in a remote location can clear out the entry by simply holding down the Shift key as Windows is starting.

With either of these methods, you end up with a dead workstation at a remote location, or an unscrupulous user can hack into the network, outside of the administrator's control.

There is another method for doing automatic logons that utilizes the Windows LSA to store the password in a weak, but encrypted, format. While this may seem a good choice, the encryption is easily cracked, and there are dozens of publicly available programs that will do the extraction for you.

Neither of these methods allow mass password changes, and the workstations must remain on if any password changes are done so they can be updated.

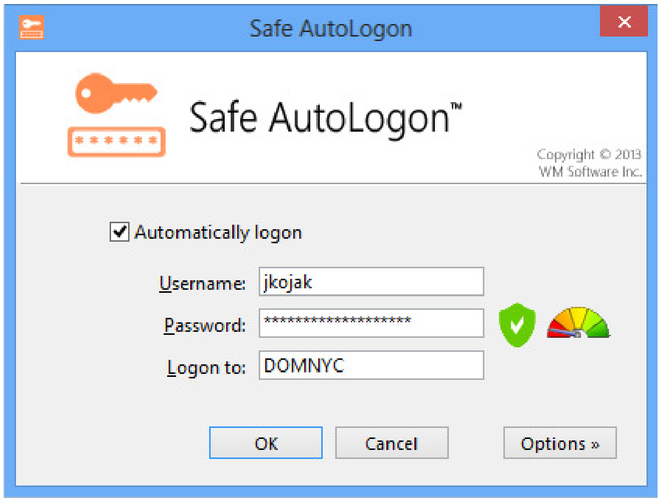
Safe AutoLogon

To enable secure, automatic logons for use on Windows desktops, WM Software developed Safe AutoLogon. The username and password are stored in AES 256-bit encryption to keep them safe from spy ware, viruses, malware, or malicious users that try and gain access to the logon information.

Setting up Safe AutoLogon works just fine for a few dozen computers that need automatic logons.

However, enterprise customers who want automatic logon on hundreds or thousands of computers, cannot enter the password into the Registry in clear text on those workstation. Not only is it unfeasible, but it poses a high security risk and can become an administration headache and time waster.

Manually updating passwords using old methods does not address how to handle computers that login with old passwords when the password has been changed since it last powered on. This can cause user account lockout, so now the administrator is faced with unlocking the account and fixing the problem on hundreds to thousands of computers, amounting to downtime and lost business.



☑ Automatically logon

Username: jkojak

Password: *******************

Logon to: DOMNYC

Fig 1. The main Safe AutoLogon client screen. The user selections are in the Options section.

With Safe AutoLogon Password Server, computers can be off for days, week, months, or years, and will always receive the current password.

The Complete Solution:
Safe AutoLogon with Safe AutoLogon Password Server

With Safe AutoLogon Password Server (SALPS), computers running Safe AutoLogon automatically retrieve their password from the SALPS server ***before the automatic logon even takes place***. SALPS can also remotely manage Safe AutoLogon software installs and settings. Templates can be created for different usernames the company wants, and these can be sent down to clients and then reused for other clients.

SALPS also adheres to a company's internal password complexity requirements, and ensures compliance with HIPAA guidelines.

The process the Safe AutoLogon client uses to logon is as follows:

1. Before logon, the client looks up and contacts a SALPS server, sending the SALPS server the user logon name and domain (in 256-bit AES encrypted format).
2. The SALPS server looks up the user's password, and sends it back to the client, also encrypted.
3. The Safe AutoLogon client receives the encrypted password, decrypts it, then uses it to logon.

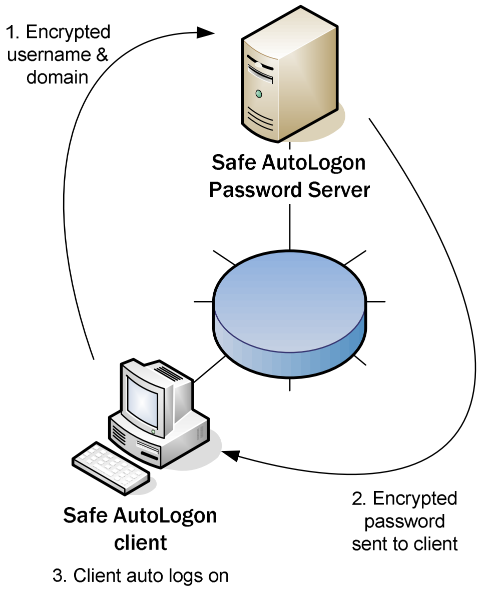

1. Encrypted username & domain
Safe AutoLogon Password Server
Safe AutoLogon client
3. Client auto logs on
2. Encrypted password sent to client

Fig 2. The SALPS and the Safe AutoLogon client interact before the automatic logon occurs. It is recommended to have 2+ SALPS servers on the network for redundancy.

SALPS can also replicate with other SALPS servers, so, in case of server or network issues, clients always have access to logon information. The SALPS database itself is 256-bit AES encrypted, and the data in the database fields are also 256-bit AES encrypted.

How Safe AutoLogon clients find the SALPS server

Safe AutoLogon can find the SALPS server in two different ways. The recommended method is to setup SRV records in the company's DNS servers. For testing, or in environments where an SRV record cannot be added to a company's DNS server, the second method is to hard code the SALPS servers in each Safe AutoLogon client's settings. Both methods allow the configuration of multiple failover SALPS servers.

Installing the SALPS Software

Assuming DNS is setup and the Safe AutoLogon clients can find the SALPS servers listed, the SALPS software is ready to be installed. Some points to be aware of:

1. SALPS can only run on Windows Server, versions 2008 R2 through 2019. It must be a server that is running 24/7. Ideally, there should be two or more on the network for redundancy.
   - ➢ The SALPS servers must reside on a domain member server.
   - ➢ It is not recommended to put the SALPS servers on Domain Controllers.
2. Run the setup program to install the Safe AutoLogon Password Server software.
   - ➢ The installation asks for a logon to use for its service. The SALPS service requires a domain account that has privileges to reset domain account passwords, and it also requires administrative privileges on remote computers. This, of course, can be a Domain Admin, or a domain user that is configured with these privileges.

SALPS Templates

Now that you have an understanding of how SALPS works with Safe AutoLogon clients, you can now send username changes down to multiple client computers using templates. When you want to update tens, hundreds, or thousands of Safe AutoLogon clients with a particular username or setting within Safe AutoLogon, manually doing it would consume a huge amount of time. SALPS automates this task also.

The Safe AutoLogon client on the workstation is configured manually with the username, domain, and other settings you want to configure. Safe AutoLogon is then closed, and back on the SALPS server, you "pull" the settings from that client into a ".salpsset" file. This file can then be sent to other Safe AutoLogon clients. You may want to create a different file for each username you are managing in SALPS.

Passwords in SALPS and Active Directory

SALPS stores passwords for Active Directory account names. When the password is changed in SALPS, it sends the changes to AD. This is the only direction password changes can take place. If the password of an account is changed in AD, it will not be updated in SALPS. Password changes MUST take place on the SALPS server. Otherwise, logins will not take place on the Safe AutoLogon clients and those user accounts could get locked out.

Hardware and Software Requirements

The following hardware and software requirements are necessary to use this software:

- **Software:**
  Windows Server 2008 R2, 2012, 2012 R2, 2016, or 2019.
- **Hardware:**
  RAM: A system with 2GB or more
  One or more 1Gbps network connections
  *Network packets sent between the Safe AutoLogon client and SALPS are encrypted and fit within the typical maximum MTU size of 1500 bytes

The Safe AutoLogon software and the Safe AutoLogon Password Server software are patent-pending and developed exclusively by WM Software.

The information contained in this document represents the current view of WM Software Corporation on the issues discussed as of the date of publication. Because WM Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of WM Software, and WM Software cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. WM SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.