WM Software
Safe AutoLogon™

Automatically logon to Windows® Desktops and Servers with

Safe AutoLogon

Product Overview

Software version: 2005
wmsoftware.com

Contents

Introduction

Since 1993 with Windows NT, there has always been a way of automatically logging on to Windows by storing the username, password, and domain name in the Registry. TweakUI was a tool released by Microsoft to accomplish this task. But obviously this methodposes a serious security risk because it 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.

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 with dozens of publicly available programs.

With either of these methods, you end up with a dead workstation at a remote location if the network password has changed. And, an unscrupulous user can hack into the network with the stolen credentials, outside of the administrator's control.

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.

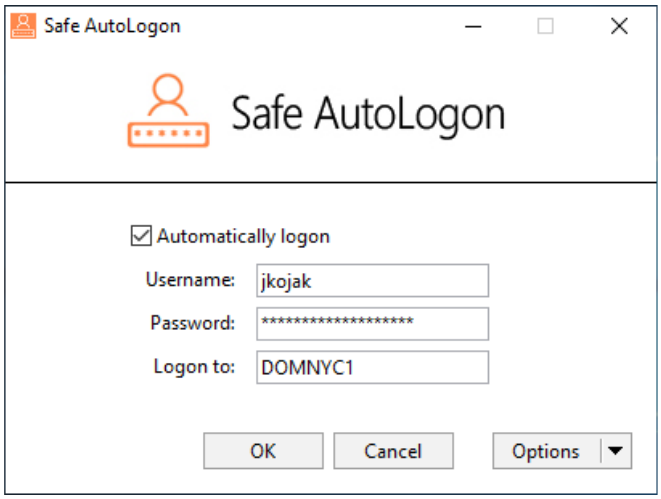

Fig 1. The main Safe AutoLogon client screen. The user selections are in the Options section.

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

Installation and Configuration

Install and configure the software as follows::

1. Log in to your computer running Windows XP or higher, preferably as an administrator, although this is not necessary.
2. Run the installation program. Click through the installation wizard.
3. After installation, launch the software. You will be presented with a window to Continue to run the software, Purchase the software, or Register the software. The window will show you how many days are left in the evaluation, which you can also check in the software product's Help/About menu. Click on the End User License Agreement to view it, then press Continue.
4. From here, you can begin to setup the software. The domain/computer-name will automatically be filled in. Enter the username and password you want to login with.
5. Now, reboot your computer and Safe AutoLogon will automatically logon!
6. For more choices in Safe AutoLogon, press the Options button. Settings allow you to keep the user logged on, lock the desktop after a logon, delay the automatic logon, and to optionally specify servers running Safe AutoLogon Password Server.

Hardware and Software Requirements

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

- **Software:**
  Windows Vista, 7, 8, 8.1, and 10
  Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019.

- **Hardware:**
  RAM: A system with 1 GB or more
  Drive space: 30 MB usage
  *Network packets sent between the Safe AutoLogon client and SALPS are encrypted and fit within the typical 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.