WM Software
Safe AutoLogon™
Password Server

Centrally manage Windows® automatic logons securely with

Safe AutoLogon Password Server

Product Overview White Paper

Software version: 8.0
www.wmsoftware.com

WMSoftware

Contents

Introduction

Since Microsoft Windows NT, there has been a way of automating the logon process by storing the username, password, and domain name in the Registry. The key (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon) that stores this information is remotely readable by the Authenticated Users group, which is everyone that can login to the computer.

But using this feature poses a serious security risk because the logon credentials are stored in *unencrypted clear text*, making it easy for anyone to see. Another problem with the built-in automatic Registry logon is if the user wants to bypass automatic logon by holding down the Shift key as Windows is starting the logon name is cleared from the Registry (stored under DefaultUserName) and isn't available for subsequent automatic logon. To fix this, the username needs re-entered into the Registry (in clear text).

Another method for doing automatic logons is some programs utilize the Windows LSA to store the password encrypted format. While this may seem a good choice, the password stored in the LSA is easily cracked with one Windows API call, and there are dozens of programs out there that will do the extraction for you.

Safe AutoLogon

To enable secure, automatic logons that are easy to configure, WM Software developed Safe AutoLogon. This software stores ALL of the logon information (username, password, and domain) in an AES encrypted format using the maximum encryption the operating system is capable of, typically 256-bit. This high-strength encryption keeps the logon information safe from spy ware, viruses, mal ware, or malicious users that try and gain access to the logon information.

This single-software setup works just fine for one-computer automatic logons.

Enterprise customers need to manage many (even tens of thousands) of Safe AutoLogon clients, and they need to keep passwords synchronized with Active directory while avoiding the labor intensive process of manually updating each Safe AutoLogon client.

One way to automate this password updating is to use a logon script that contains the encrypted password string and updates the registry. However, the computer must be logging in with the very username that has had their password changed, so this option is unfeasible.

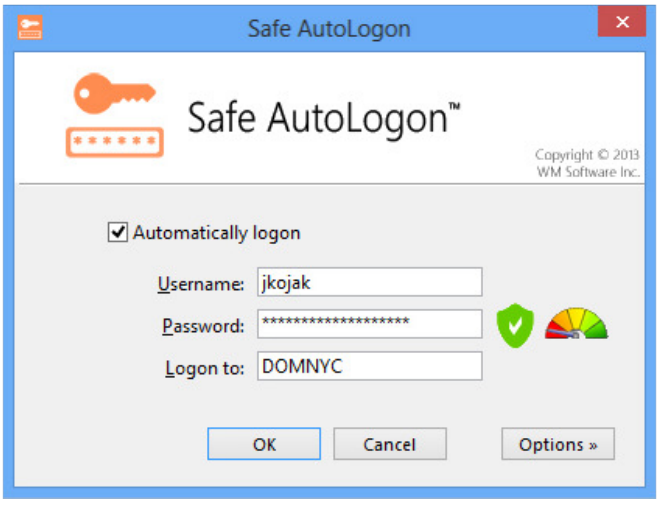


Fig 1. The main Safe AutoLogon client screen. The user selections are in the Options section.

Another way to automate the password updating is to update through a remote Registry connection, but this manually intensive and it also requires the computer to be turned on.

Neither of these manual solutions addresses the issue of how to handle computers that login with old credentials because the password has been changed since it last powered on.

Safe AutoLogon computers ***never need to be powered on to receive password changes***.

A Complete Solution: Safe AutoLogon + Safe AutoLogon Password Server

To address the needs of the enterprise, WM Software created software to manage usernames and passwords for clients running Safe AutoLogon, Safe AutoLogon Password Server (SALPS).

SALPS allows the Safe AutoLogon clients to retrieve their password automatically from the SALPS password database ***before the automatic logon even takes place***. SALPS also remotely manages software installs and settings for Safe AutoLogon clients, including Safe AutoLogon client template files that can be reused for multiple clients. Finally, SALPS enables companies to follow their own internal password complexity and configuration policies and be within HIPAA guidelines and compliance.

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 it the encrypted user logon name and domain stored on the client.
2. The SALPS server replies and sends the password to the client, encrypted.
3. The Safe AutoLogon client decrypts and this new password, then uses it to automatic logon.

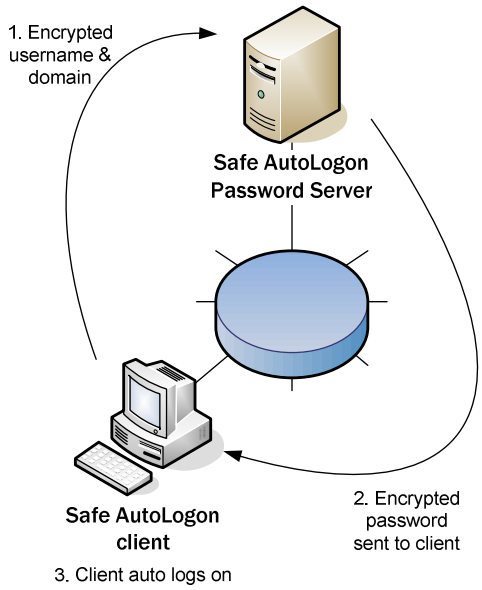


Fig 2. The SALPS and the Safe AutoLogon client interact before the automatic logon occurs. It is recommended to have 2+ SALPS servers on the network to ensure successful logons.

The SALPS server stores the user logon names and passwords for the Safe AutoLogon clients. It can also replicate with other SALPS servers. The database itself is 256-bit AES encrypted, and its fields are also 256-bit AES encrypted.

At the Safe AutoLogon client, the names of the SALPS servers are stored. These are saved in the Safe AutoLogon settings so, at boot, the Safe AutoLogon client knows the SALPS server names that contain the password for the given logon name.

How Safe AutoLogon clients find the SALPS server

As part of the logon process, the Safe AutoLogon client sends the logon domain, username, and other required information, to the SALPS server, as a 256-bit AES encrypted string. The SALPS server then matches the information and returns the password in a 256-bit AES encrypted string. The Safe AutoLogon client then decrypts the string and proceeds to login, if the credentials are correct.

In order for the Safe AutoLogon to know where the SALPS server is located, there are two ways an administrator can set this up. The first and most efficient method is to setup SRV records in the company's DNS server. The second method is to list the SALPS servers in each Safe AutoLogon client's settings. Both methods allow the configuration of multiple failover SALPS servers.

Method 1: Add an SRV record to a Windows Active Directory computer running DNS.

The following steps are taken from a Windows Server 2008 running the DNS role. These steps may vary on other operating systems - contact your domain administrator if necessary.

1. Run **DNS Manager**
2. Open the computer name branch, Forward Lookup Zones branch, then the fully-qualified domain name branch
3. Left-click on **_tcp**
4. Right-click in the right-hand pane and choose **Other New Records...**
5. Choose **Service Location (SRV)** and press **Create Record...**
6. Fill in the following fields and then press **OK** (See Fig 3)
    a. Service: **_wmssalps**
    b. Protocol: **_tcp**
    c. Port number: **445**
    d. Host offering this service: **[fqdn_of_salps_server_name]**
7. Press **OK** and then **Done.**

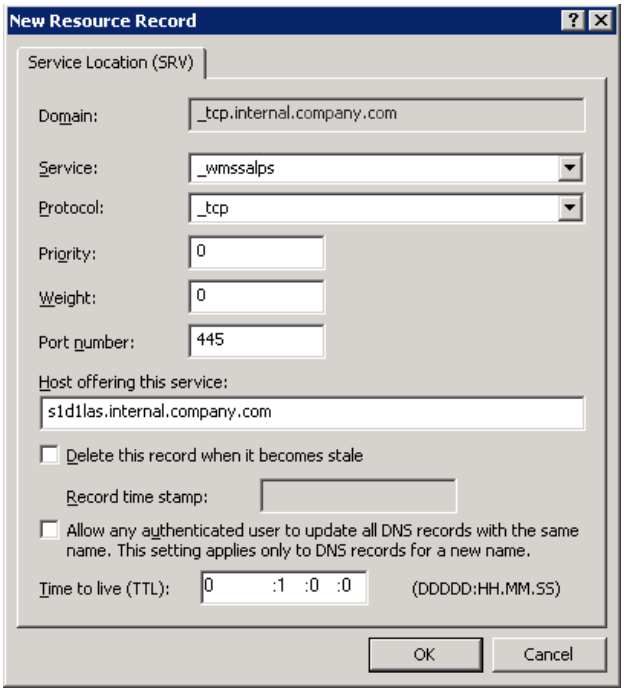


Fig 3. DNS SRV record on Windows Server 2008 R2

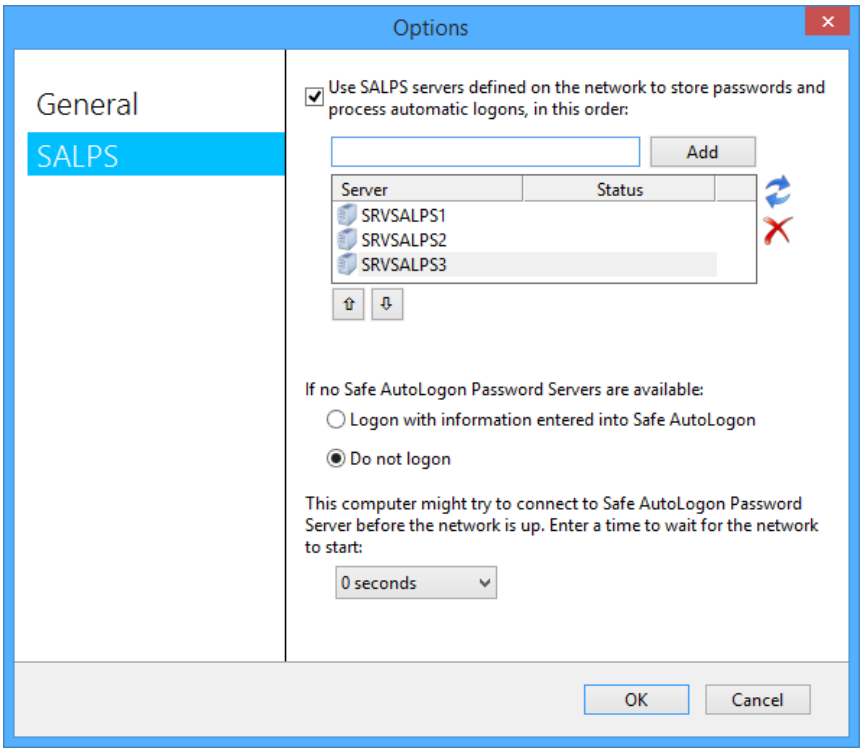
8. To add multiple SALPS servers for failover and redundancy, repeat these steps with the name of the other SALPS servers, one by one, so each SRV record contains just one SALPS server. If any SALPS servers go down, the other SALPS servers listed as SRV records in DNS will handle the request.

Method 2: Add multiple SALPS servers to a Safe AutoLogon client

The client must be on a domain to get access to the SALPS option from within the Safe AutoLogon client.

1. Open the Safe AutoLogon client
2. Click on the **Options** button
3. Click on the **SALPS** tab

4. Add the names of SALPS servers on the network to the list:



5. Press OK to save the settings.

Now, if any of the SALPS servers in the list go down, the other two servers will handle the request.

Installing the SALPS Software

Now that the Safe AutoLogon client can find the SALPS servers, this section will go over installing and configuring the Safe AutoLogon Password Server software:

1. Decide and identify which server(s) on the domain are available 24x7 to handle the logons of Safe AutoLogon client computers. Ideally, there should be 2+ servers identified as SALPS servers.
    - 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 service does not require any special username to login and can be left as the default Local System.

Configuring the SALPS Software

1. Once installed, SALPS is configured into four distinct areas: **CLIENTS**, **USERNAMES**, **SALPS SERVERS**, and **REPORTING**:
    - **CLIENTS**
      This is a list of Safe AutoLogon clients, which allows the administrator to:
        a. Remotely install/uninstall the Safe AutoLogon client software
        b. Get the Safe AutoLogon settings from a remote client and store it locally to a file
        c. Send the saved settings file to one or more remote Safe AutoLogon clients
        d. Clear/stop Safe AutoLogon from performing an automatic logon on one or more remote clients
        e. Check the logon information and general status of the Safe AutoLogon software
    - **USERNAMES**
      This is a list of all usernames and their passwords stored in the SALPS database. They are visible from within SALPS, but they are stored in 256-bit AES in the database.
        a. The usernames and passwords are not read from Active Directory, the administrator populates it. Passwords are manually added.
        b. Passwords are automatically pushed to Active Directory when a change is made. Passwords are not pulled from Active Directory to the SALPS server.
        c. So, for example, when adding a user into SALPS and a password is set for that user, changes are not made to Active Directory until the settings are saved from within SALPS.
        d. If a user's password is changed in Active Directory, SALPS is NOT made aware of the changes. Because of this, computers that logon using Safe AutoLogon and use a username in SALPS, if a password change was done on Active Directory and not in

SALPS, the Safe AutoLogon client will get the old password from SALPS and it will not logon. Too many attempts at this will lockout the account.

e. Best practice is to only make password changes for Safe AutoLogon client usernames from within SALPS.

f. For admins with reporting enquiries or client maintenance duties only, a password can be used to prevent viewing of the passwords.

- **SALPS Servers**

  For redundancy, when password changes are done on one SALPS server, the other SALPS servers that service Safe AutoLogon clients (those listed in the _wmssalps SRV records) need to also be listed here.

  a. Password changes are automatically synched with the other SALPS servers in the list.

  b. Though not required, it is highly recommended to have multiple SALPS servers for redundancy.

- **REPORTING**

  All reports about password changes, password access, password age, administrative events, client logons, etc., can be found here. Date and text searches can also be done. Here are some of the types of reports that can be generated (this list is usually updated with each new build or major/minor version):

  a. A user logged into the SALPS software

  b. Username tab is clicked on

  c. Usernames added/removed from the SALPS database

  d. Password changes that failed or succeeded

  e. When Safe AutoLogon clients request a password from the SALPS server

2. On the CLIENTS tab, add a group (i.e. SALGroup1) and add a few client computers to the group. Clients must be the actual names of the remote computers that are running Safe AutoLogon. The clients are organized into one or more groups. The ordering of groups or the naming of groups is of no issue.

3. Now let's populate the SALPS database with an existing Active Directory username. First, click on the USERNAMES tab, type an existing user's logon name into the "Enter a user name" box, then press "Add". Place a checkbox next to this username.
   Next, enter the user's password that matches what is in Active Directory, and click "Set for checked". Now save the changes by pressing the Save icon at the top left of SALPS. This action up-dates the SALPS database.

4. Next, setup Safe AutoLogon on a client computer with this new username. On the remote computer running Safe AutoLogon, ONLY enter the username just entered into SALPS and press OK (do NOT enter a password. Clear it out if one is listed).
5. Restart the Safe AutoLogon client. It should automatically connect to the SALPS server, retrieve the password, and logon.

Using SALPS to configure multiple Safe AutoLogon clients

Now that you have an understanding of how SALPS works with Safe AutoLogon clients, you can now begin using the 2nd power of SALPS – sending username changes down to multiple client computers.

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. Here are the basic steps:

1. Configure Safe AutoLogon client for "template" for populating other Safe AutoLogon clients.
    a. Install SAL on two Windows VMs (for this example, we'll name them PC1 and PC2). The operating systems do not matter, just keep them the same OS and 32/64-bit version between them.
    b. Turn off the Windows Firewall on both PC1 and PC2 (or just open the ports 139 and 445 on PC1)
    c. Install Safe AutoLogon manually on PC1.
    d. Configure PC1 with the username that matches what is in SALPS. Everything else can be left at their defaults if you have an SRV record setup
2. Get the settings from the remote Safe AutoLogon client from SALPS
    a. Add a group in SALPS (call it 'Group1')
    b. Add PC1 to 'Group1' in SALPS
    c. Add PC2 to 'Group1' in SALPS
    d. Press the Save icon to save the clients and group to the database
    e. Left-click on the group 'Group1' in SALPS
    f. in the list on the right, highlight/click on PC1
    g. Place a checkmark in front of PC1
    h. Click the "Get Settings from Client" on the CLIENTS tab.
    i. Enter the name of the template file to save to (.salset file)
3. Install SAL and send the template settings to a remote computer
    a. Now, put a checkmark only in front of PC2
    b. Click the Install Safe AutoLogon icon and give the wizard the name of the .salset file
    c. Give the wizard the setupsafeautologon.exe installation file
    d. Installation will proceed with the username and settings intact!
    e. Go to PC2 to verify

It's helpful to name the .salset files the name of the username so you can easily deploy. You may also want to organize the .salset files into multiple folders on the SALPS server.

Hardware and Software Requirements

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

- **Software:**
  Safe AutoLogon Password Server: Windows Server 2003 with Service Pack 2 or later, Windows Server 2008 with Service Pack 1 or later, Windows Server 2008 R2, Windows Server 2012, 2012 R2, Windows Server 2016.
  Safe AutoLogon client:
  Windows client operating systems: Windows XP Professional with Service Pack 3 or later, Windows Vista with Service Pack 1 or later, Windows 7, Windows 8, Windows 8.1, or Windows 10.
  Windows servers operating systems: Windows 2008 or above.

- **Hardware:**
  A system with at least 500MB of free RAM
  One or more 1Gbps network connections
  If a VM, running on a low-usage hypervisor
  Network packets between the Safe AutoLogon client and SALPS are well within the typical maximum MTU size of 1500 bytes