

Safe AutoLogon for the Enterprise

Using the Safe AutoLogon client and the Safe AutoLogon Password Server for Seamless Automatic Logons

White Paper

Published: August, 2011

Software version: 3.7

www.wmsoftware.com



Contents

Introduction	1
Safe AutoLogon solution.....	1
Safe AutoLogon Password Server (SALPS) solution	2
Installing an SRV record for the SALPS on DNS.....	4
Installing and Configuring the SALPS	5
Safe AutoLogon client Installation and Configuration	6
Hardware and Software Requirements	6

Introduction

Starting with Microsoft Windows NT, there has been a way of automating the logon process by storing the username, password, and domain name in the registry database. This feature permits other users to start the computer and to use the account in the registry database to automatically log on. The registry key (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon) that stores this information is remotely readable by the Authenticated Users group.

However, using this feature can pose a serious security risk because the username, password, and domain name are all stored in unencrypted clear text, making it relatively easy for anyone to see.

Another problem arises when a user wants to bypass the automatic logon. The user can bypass automatic logon by holding down the SHIFT key as Windows is starting. The problem of bypassing the automatic logon feature is that the original DefaultUserName is no longer kept for subsequent logons, because the name of the last user to logon is retained in the Username box of the Welcome dialog box and the Registry. To re-enable the automatic logon once again, the original username and password must be entered again in the registry.

Safe AutoLogon solution

To enable automatic logon, WM Software created Safe AutoLogon. This software product stores the username, password, and domain in a AES/Triple DES 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.

The one issue for Enterprise customers wanting to enable automatic logon has been keeping the passwords synchronized 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 that option is unavailable.

Another way to automate the password updating is to update through the remote registry connection, but this is both manually intensive and it also requires the computer to be turned on and not logged on with the old password.

Another issue is how to handle computers that are not powered on for a time period after the password change has taken place.



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

Safe AutoLogon Password Server (SALPS) solution

To address the needs of the Enterprise customer, WM Software created a companion product to handle password updates, Safe AutoLogon Password Server (SALPS).

This solution allows passwords to be updated on the clients *before* the automatic logon takes place, thus eliminating any aforementioned problems that Enterprise customers can run into in trying to update their Safe AutoLogon client installation.

The SALPS software can be installed on any server running Windows 2003 or Windows 2008. It will also run on Windows XP, Vista, and Windows 7, though Enterprise customers will want to install on a Windows 2003 Server.

For the maximum availability for the Safe AutoLogon clients, it is highly desirable and recommended to install the SALPS software on each Domain Controller for the domain. The Safe AutoLogon client then does not need to have the SALPS servers listed in its configuration since the Domain Controllers will always be available and can be automatically found.

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

1. Before logon, the client contacts a SALPS server and sends to the SALPS server the encrypted user logon name and domain.
2. The SALPS server replies with the encrypted password.
3. The Safe AutoLogon client uses this new password to proceed with the automatic logon.

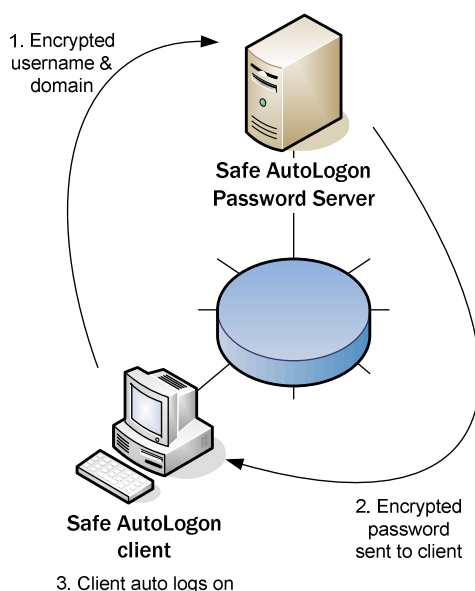


Fig 2. The SALPS and the Safe AutoLogon client interact before the automatic logon occurs. It is recommended to have 2+ SALPS servers on the network to ensure successful logons.

The SALPS server stores the logon names, passwords, and domain for the clients running Safe AutoLogon. It also stores the names of other SALPS servers so they can also receive the updated database information.

The database is 256-bit AES encrypted and is automatically replicated to other SALPS servers when changes are applied.

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.

To install the Safe AutoLogon Solution on an Enterprise network, you can simply install the SALPS component and point each client to the server. Or you can create an SRV record on your DNS server to point to the server(s) running SALPS.

Installing an SRV record for the SALPS on DNS

After installing the SALPS, you then register the computer running SALPS in DNS using an SRV record. Computers that startup and login will then know where the SALPS server is located, as they look for the **_wmssalps** SRV record using DNS. Here are the steps to manually add an SRV record to a Windows Active Directory computer running DNS. The following steps are taken from a Windows Server 2003 DNS server. These steps may vary on other operating systems - contact your domain administrator if necessary.

1. From Start/Run, type in `dnsmgmt.msc` and press OK
2. Left-click on **_tcp** under **DNS\[server_name]\Forward Lookup Zones\[fqdn]**
3. Right-click on **_tcp** and choose “**Other New Records...**”
4. Choose **Service Location (SRV)** and press **Create Record...**
5. Fill in the following fields and then press **OK** (See Fig 4)
 - a. Service: **_wmssalps**
 - b. Port number: **445**
 - c. Host offering this service: **[fqdn_of_salps_server_name]**
6. Press **OK** and then **Done**.

Now the clients will be able to find the host LAS server. See the following figure to

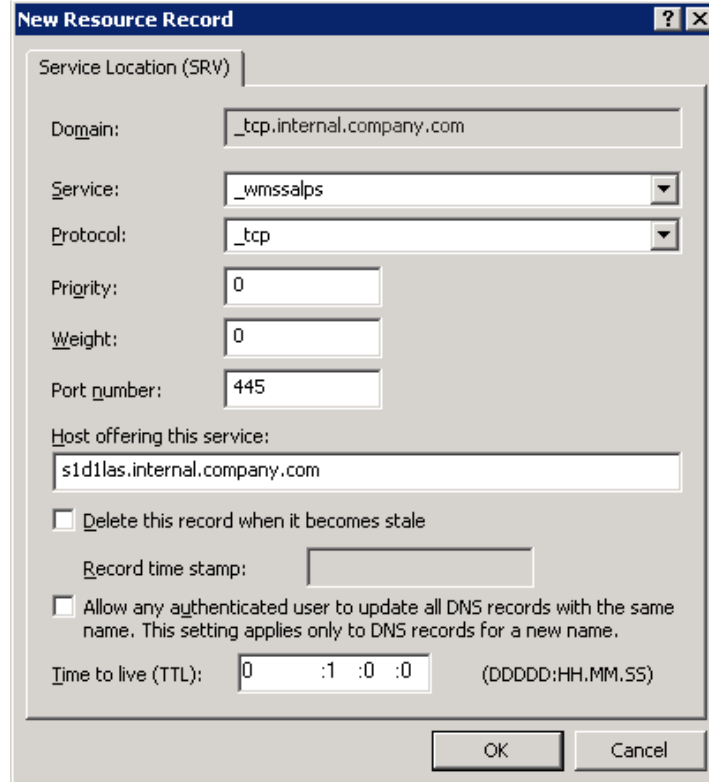


Fig 4. On Windows Server 2003.

Installing and Configuring the SALPS Software

To install and configure the Safe AutoLogon Password Server software:

1. Decide and identify which servers on the domain are available 24x7 to handle the uptime requirements of Safe AutoLogon client computers. There should be 2+ servers identified as SALPS servers. Additionally, the SALPS servers must reside on a domain member server.

For the maximum availability for the Safe AutoLogon clients, it is highly desirable and recommended to install the SALPS software on each Domain Controller for the domain. The Safe AutoLogon client then does not need to have the SALPS servers listed in its configuration since the Domain Controllers will always be available and can be automatically found. You can also specify a SALPS server through DNS, beginning with version 3.7 of the Safe AutoLogon client software.

2. Install the Safe AutoLogon Password Server software on the first server decided in step 1.
3. Enter the username/password/domain combinations that the Safe AutoLogon clients will be using on this first server. Save the changes (File/Apply changes).
4. Enter the other identified SALPS servers in the listbox, still on the first server. Save the changes (File/Apply changes).
5. Install the Safe AutoLogon Password Server software on the subsequent servers. When asked to replicate the database information from another server, type in the name of the first SALPS server.

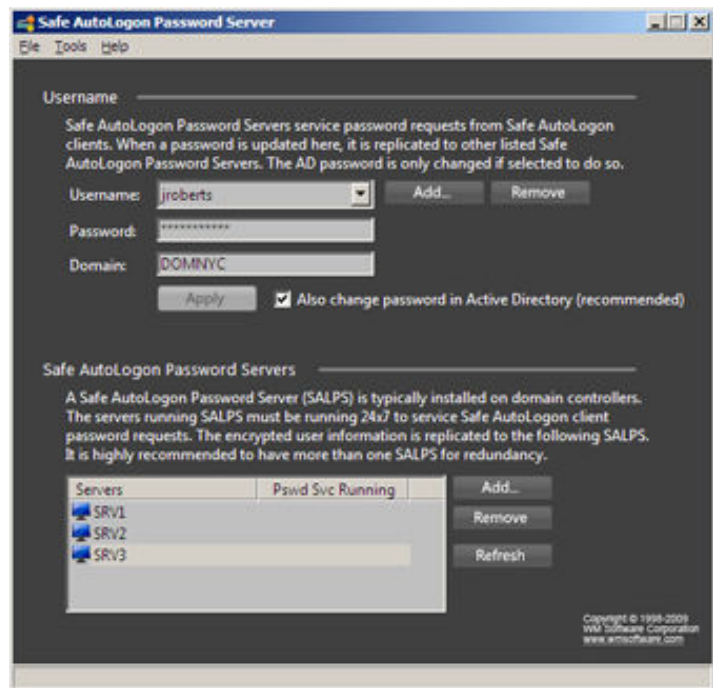


Fig 3. The SALPS software showing the username and other SALPS servers. Each username has its own password and domain associated with it.

Safe AutoLogon client Installation and Configuration

Install the Safe AutoLogon client:

1. Install Safe AutoLogon on the first client.
2. Configure the Password Servers settings (Options/Settings/Password Servers - see Figure 3).
3. Choose where the SALPS software are located (on Domain Controllers or other servers)
The names of the Domain Controllers can also be in the list, but by selecting the option to use Domain Controllers, the Safe AutoLogon client will find them automatically.
4. Enter the SALPS server names in the list.
5. Choose the action to take if Safe AutoLogon is unable to connect to the SALPS servers.

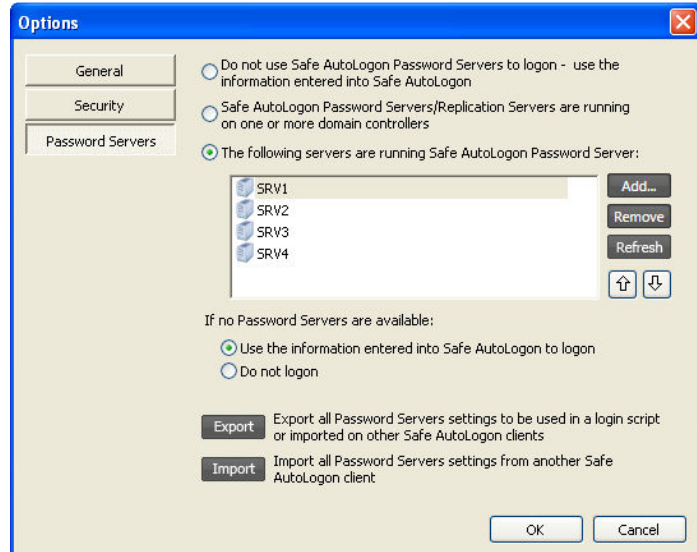


Fig 4. In this configuration, the SALPS servers are listed with the option to use them. Also, this client will use the information stored locally if no SALPS servers are available. This is an administrative decision; the user name could get locked out of the domain if too many unsuccessful logon attempts are made.

Hardware and Software Requirements

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

- **Operating System.**
Safe AutoLogon client: Windows XP Professional with Service Pack 2 or later installed, Windows Vista, Windows 7, Windows Server 2003 with Service Pack 1 or later installed, Windows Server 2008, Windows Server 2008 R2.
Safe AutoLogon Password Server: Windows XP Professional with Service Pack 2 or later installed, Windows Vista, Windows 7, Windows Server 2003 with Service Pack 1 or later installed, Windows Server 2008, Windows Server 2008 R2.
- **Hardware.** A system with at least 256 Mb of RAM and a Pentium 4 or better CPU is required. The client consumes approximately 200kB RAM and 2MB Hard Drive space.

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.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of WM Software Corporation.

WM Software may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from WM Software, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© WM Software Corporation. All rights reserved.

Microsoft, Windows, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.