



How-to series:

# Creating a Proof of Concept for Safe AutoLogon® and Safe AutoLogon Password Server®

*Software versions used:*
Safe AutoLogon 2309
Safe AutoLogon Password Server 2211
www.wmsoftware.com

WMSoftware

# Contents

## Introduction

This proof-of-concept document will walk you through quickly setting up a test environment for a pilot/proof-of-concept test. This document is written by WM Software engineers from how they setup a test environment. This should only take about 15-30min.

## Proof of concept environment

You will need the following to conduct your proof of concept:

- An Active Directory domain
- Four (4) VMs on one or more host computers (2 SALPS servers and 2 SAL clients) with a minimum of 1GB of RAM and two CPUs.
- You can bypass the Replication test and use just two VMs (1 SALPS server and 1 SAL client). However, In production, we recommend two SALPS servers on different hardware, for redundancy and to be able to service logons 24x7. However, for this proof of concept, we are creating all VMs on one Windows computer.
- The SALPS servers must be running on Windows Server 2012 R2 or higher and joined to the domain.
- The SAL client can be running on either client (Windows 7 or higher) or server operating systems (Windows Server 2012 R2 or higher) and joined to the domain.
- An existing DNS server to add SRV records (optional, but highly recommended)
- A domain user that has the delegated Active Directory right of "Reset user passwords" and is a local and remote administrator on all VMs in testing.

You can also create an Internal Switch on a host and bring up its own Active Directory VM with its own DNS and DHCP. This is how our engineers do initial testing.

In production, designate one SALPS server as the "primary" SALPS server that handles all modifications (password changes, automatic password generation, etc.) to keep changes centralized. The other SALPS servers can be setup as "read-only", which might even be of a benefit for help desk personnel.

## Steps to setup a proof of concept

After you configure the VMs, here are the steps to configure and test the SALPS and SAL clients:

Setup/Configure

1. Configure the VMs
2. Install the SALPS server software
3. Configure SALPS – setup redundancy
4. Configure SALPS - add computer names
5. Populate SALPS with Active Directory Users
6. Install the SAL client software
7. Setup DNS

8. Configure the Safe AutoLogon client

Testing

1. Testing the automatic logon
2. First test: Safe AutoLogon after a Restart
3. Further testing: Change the domain password in SALPS
4. Further testing: Test the SALPS server redundancy feature
5. Further testing: Using SALPS to configure multiple Safe AutoLogon clients

## Optional port configuration

Because of increased security risks, many organizations close well-known TCP ports (0-1023) on their clients and servers. If this applies to your company, you can utilize the iana.org TCP port assigned to WM Software, port 21801.

Both the SALPS and SAL software includes a utility to enable and open TCP port 21801 on the computer's built-in Windows firewall. If you are using a 3rd party firewall, you will need to refer your firewall's documentation to enable and open TCP port 21801.

You can also download the port utility from our website, www.wmsoftware.com.

By default, SALPS and SAL communicate over ports 135, 139, and 445. By enabling and opening port 21801, ports 135, 139, and 445 are no longer used by both SALPS and SAL.

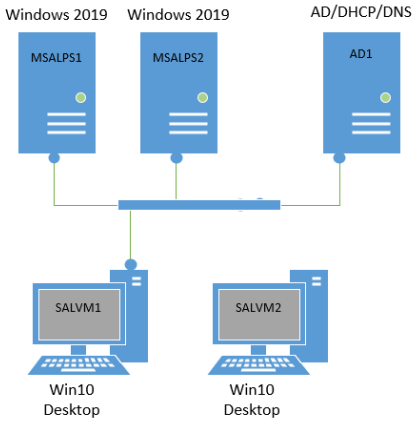
Also, by utilizing port 21801, the SALPS service no longer has to be a member of the remote computers' Administrators groups.

And another benefit of using port 21801 is the previous requirement of the Remote Registry running on the clients is removed.

# 1. Configure the VMs

Configure four VMs:

- For this Proof of Concept, create two VMs (MSALPS1, MSALPS2) that will run SALPS on Windows Server 2019. Two servers are needed to test the redundancy feature of SALPS.
    a. MSALPS1 will be designated the PRIMARY SALPS server. The PRIMARY SALPS server is where all of the operations take place.
    b. MSALPS2 will be designated the SECONDARY SALPS server. The purpose of the SECONDARY SALPS server is if the PRIMARY cannot be contacted due to OS or network issues.
- For this Proof of Concept, create two VMs (SALVM1, SALVM2) that will run Safe AutoLogon.
  One VM will run the Safe AutoLogon client on Windows 7.
  One VM will run the Safe AutoLogon client on Windows 10.

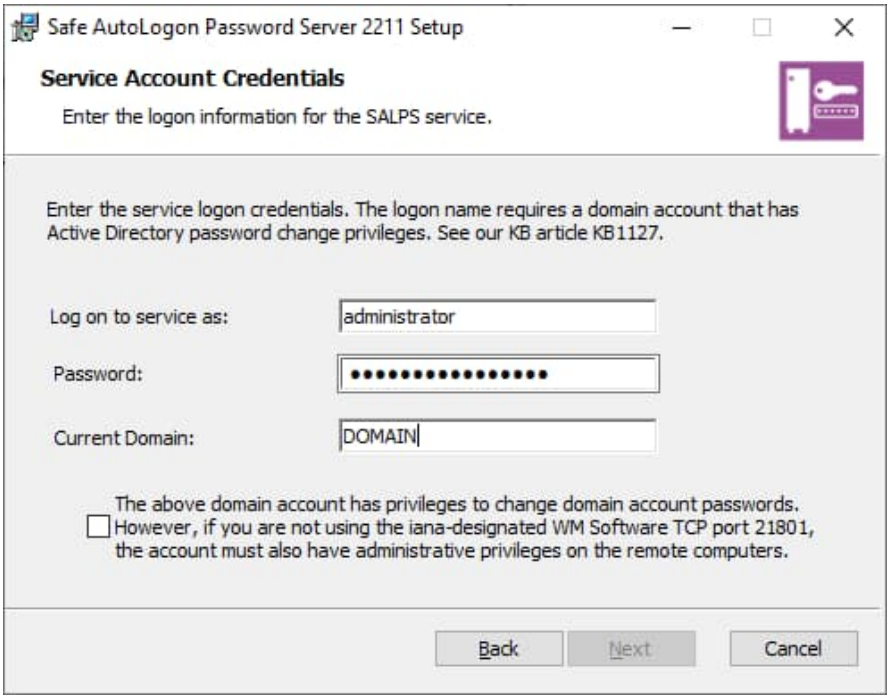



1. Configure the four VMs to each have a minimum of 2GB of RAM and 2 CPUs. The RAM usage of SALPS and SAL is less than 32MB. However, we recommend 4GB of RAM and four CPUs in each VM for the fastest testing.
2. Install Windows desktop OS (Windows 7 through 10) on the two Safe AutoLogon client VMs, and Windows server OS (2012 R2 and above) on the two Safe AutoLogon Password Server VMs. In this Proof-of-Concept document, we are running Windows Server 2022 and Windows 10.
3. Join all four VMs to the domain.
4. Login to all four VMs as a domain user with administrator rights.
5. Disable the Domain **fi**rewall on all VMs for PoC
6. Logon to all VMs as an administrator of the computer. Domain Admin logins work best for testing, but at minimum, you need administrative rights to install the software.

## 2. Install the SALPS software on the two server VMs

1. Logon to the Primary SALPS VM server - we recommend ONLY making changes on the Primary SALPS server
2. Double-click the safeautologonpwdsrvsetup.exe installation file to begin the installation process
3. Enter the user credentials for the service that is able to send password changes to Active Directory. The service runs in the background and is responsible for the Automatic Password Generation to Active Directory

   If you do NOT plan on using port 21801, the username must be a local administrator and remote administrator on the client computers



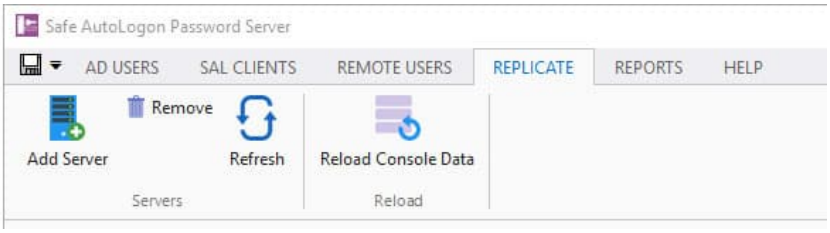

4. Step through the prompts and after a successful installation, press Finish
5. Finally, repeat the SALPS installation on the 'Secondary' SALPS VM server, MSALPS2

## 3. Configure SALPS – setup redundancy

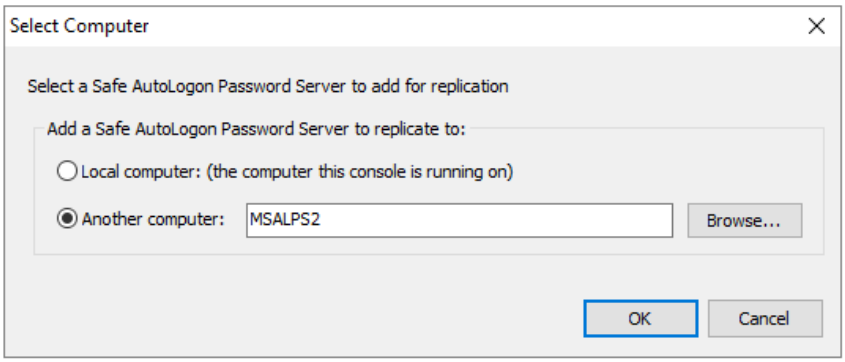
*Skip this step* if you are not interested in testing out the SALPS redundancy feature

1. Once SALPS is running, you may get warnings about no _wmssalps record in DNS and if the local firewall is active.
    a. You can ignore the DNS warning at this point.
    b. If the firewall message appears, disable the firewall for the Proof of Concept.

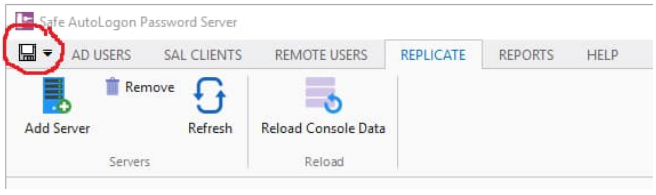
2. click on the REPLICATE tab.




3. On the Ribbon Bar, click the 'Add Server' button. On this dialog, enter the name of the other SALPS. In this example, the other SALPS server's name is MSALPS2:




4. Press the Save icon to save the changes to the SALPS database:

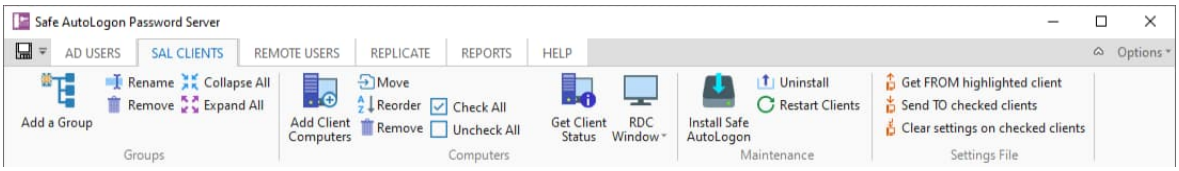



Now any changes that are saved will replicate to the other servers listed in the SERVERS tab. You can add as many replica servers as you want. Geographically, you may want to spread them out to service the closest users. We recommend a minimum of two SALPS servers

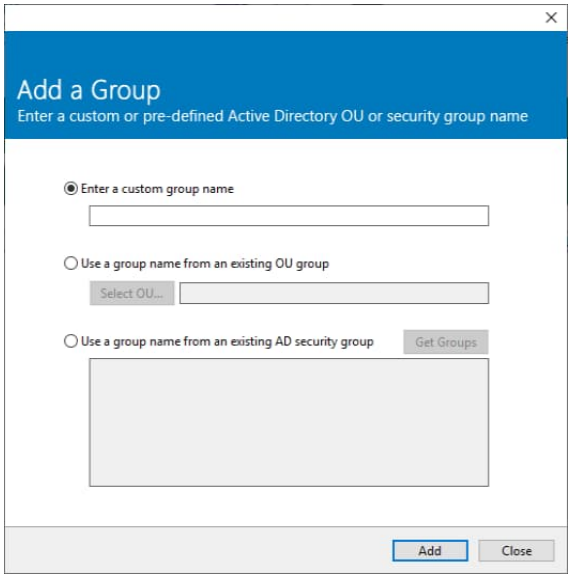
# 4. Configure SALPS - add computer names

The SAL CLIENTS tab holds a list of all computers running SAL. The clients are listed to facilitate remote installation of the Safe AutoLogon client. You can create groups and put the computers into them.

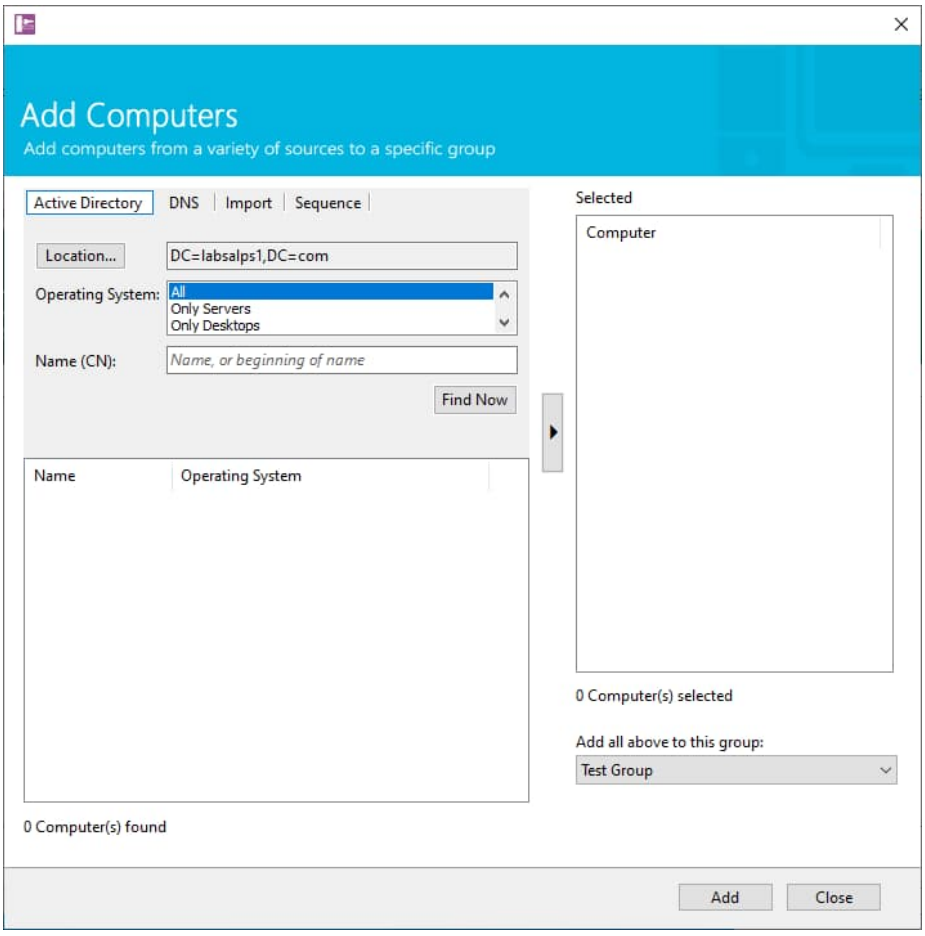
1. On one of the SALPS servers, from the ribbon bar, click on the SAL CLIENTS tab:



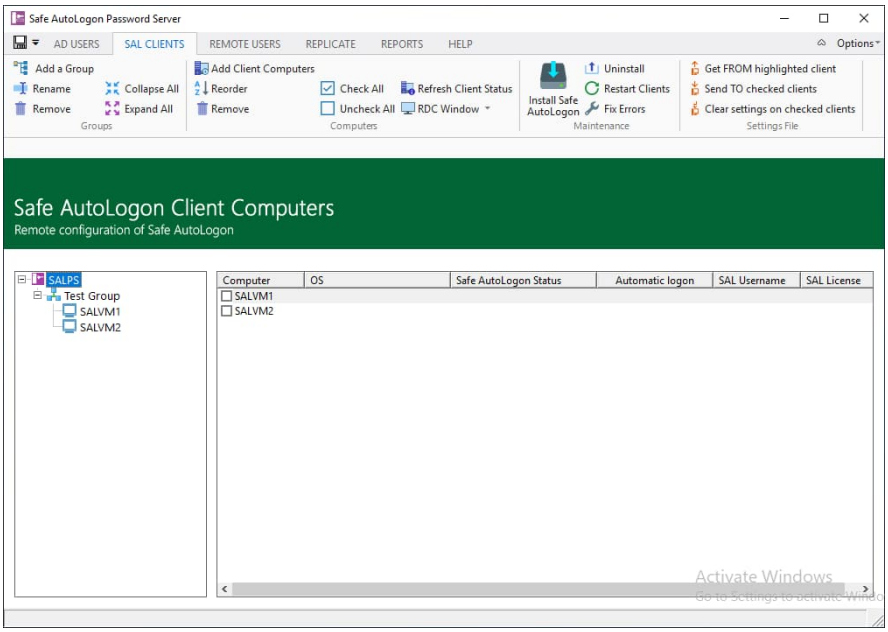

2. Click the 'Add a Group' button on the ribbon bar. In this dialog, you can add a custom group name, or select an existing OU or AD Security Group. For this proof of concept, enter a custom group name called Test Group. Press Add, then Close:



3. Now we will add computers to the group 'Test Group'. On the SAL CLIENTS tab, click the 'Add Computers' button. Enter the name of the VM clients SALVM1 and SALVM2 on the DNS tab, or you can search for them on the Active Directory tab. Add them to the Selected list, then press the bottom Add button to add them to the tree. Press the Close button to close the dialog. In this example, we are on the labsalps1.com domain:



4. The Group with the SALVM1 and SALVM2 clients now appears in SALPS on the SAL CLIENTS tab:




The SAL CLIENTS tab also allows you to remotely install (only if not using port 21801) and uninstall the SAL client, check client status for running Safe AutoLogon, restart clients, and get/send settings from/to other SAL client computers.

## 5. Populate SALPS with Active Directory Users

This is the strength of the combination of the SALPS server and the SAL clients:

1. An Active Directory username is sent to the SALPS server from a SAL client
2. The SALPS server does a lookup and sends back the corresponding encrypted password to the SAL client
3. The SAL client decrypts the encrypted password and automatically logs on

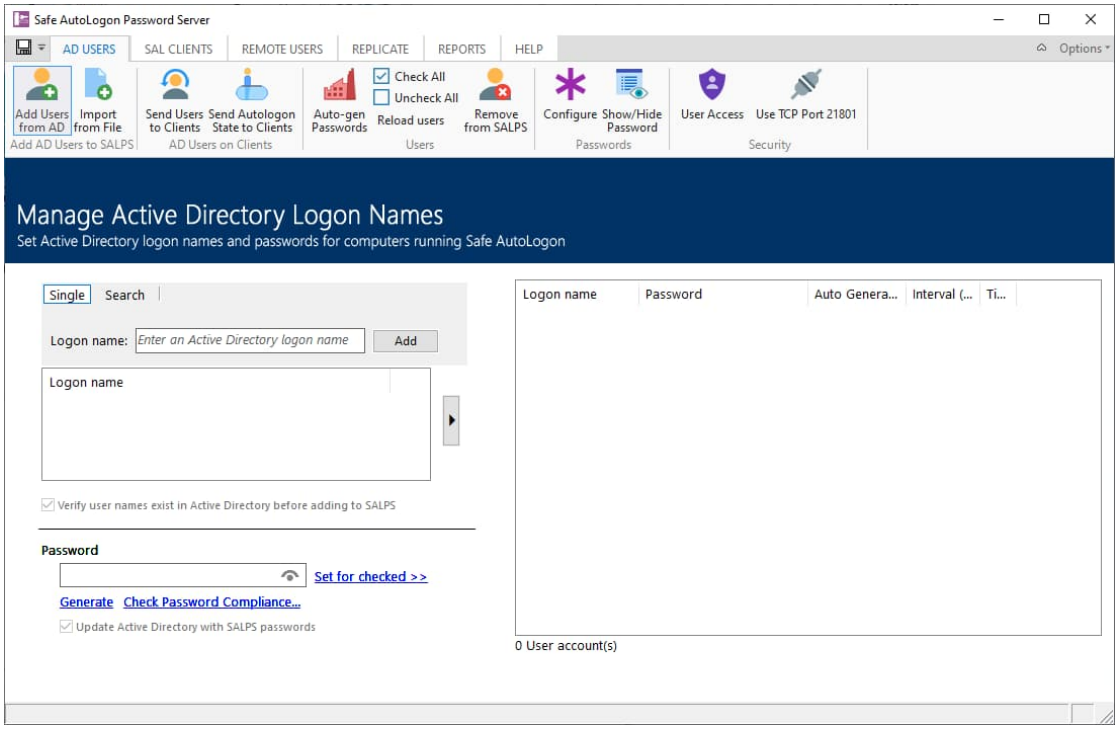
Usernames and passwords in the SALPS database are stored encrypted in 256-bit AES, and the entire SALPS database itself is encrypted. The SALPS application itself is also encrypted to protect against memory dumps exposing any passwords.

Both SALPS and SAL give end-to-end 256-bit AES security.

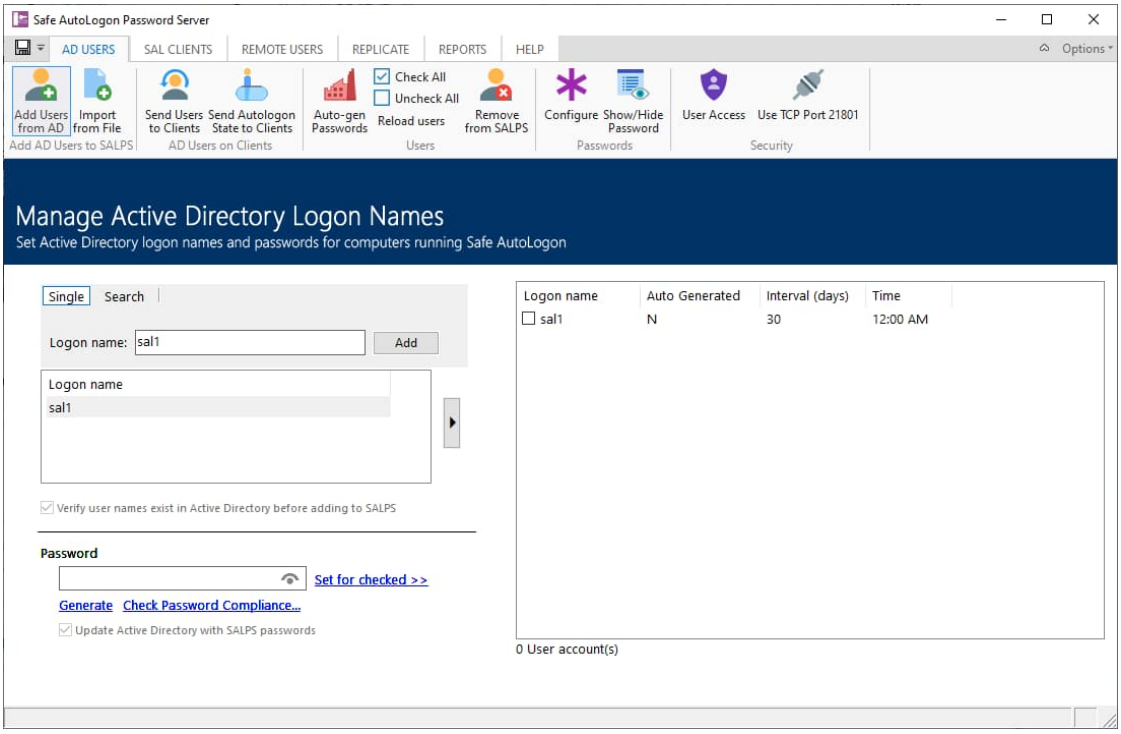
*Note: passwords changed in Active Directory are not sent to a SALPS server. The password must always be entered in SALPS **fi**rst. If a password is entered in Active Directory first, then SALPS must be updated with the same password. This is because we assume no organizations allow storing passwords in Active Directory using reversible encryption.

For this proof of concept, either create a test user in Active Directory, or use an existing user. Here we added a user named ‘sal’ to Active Directory. Now let’s add this user to SALPS.

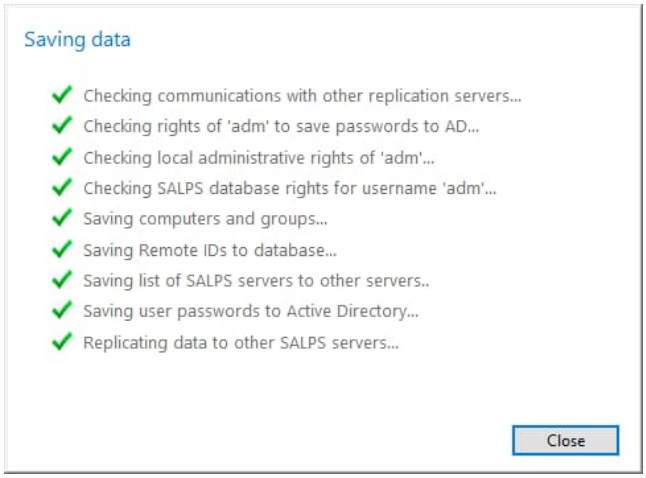
1. On the Ribbon Bar, click on the AD USERS tab and click the tab ‘Single’ for single user:




2. Type a domain username into the ‘Add a single user logon name’ field, then click ‘Add >>’. In this example, we have a domain user named ‘sal1’:




3. Enter the password for this user into SALPS in the Password field. You can match the password in Active Directory for this account, you can type in a new password, or click Generate for SALPS to generate a new password. Click the link 'Check Password Compliance' to check the password against the domain password complexity.
4. Now click the 'Set for checked >>' link to set the password for the checked usernames (if a username is not checked, it will not have its password set).
5. Finally, press the Save icon. This will save the password for this user to the SALPS database and also send the password to an Active Directory Domain Controller. After both of these happen successfully, the user and password will be sent to the other SALPS replica server:



6. If you are testing replication of two SALPS servers, at this point bring up the other SALPS VM and you will see the user has populated automatically to the other SALPS server, MSALPS2.

# 6. Install the SAL client software

Now that the SALPS servers are setup with a username and the clients are listed, you can either install the SAL client to the Windows 10 VMs (SALVM1 and SALVM2) from within SALPS or manually on the SAL clients. Remote installation of the Safe AutoLogon client software will only work if port 21801 is not enabled.

For this proof of concept, we will install Safe AutoLogon directly on one SAL client and from the SALPS console to the other SAL client.

## Install Safe AutoLogon on the first VM from within its Windows client

1. Logon to SALVM1 with an administrator's account that has rights to install software.
2. Download and copy the Safe AutoLogon installation file (setupsafeautologon.exe) to the desktop.
3. Double-click the icon to begin the installation process.
4. Step through the prompts and after a successful installation, press Finish.
5. Do not run or configure the SAL client at this time.

## Install Safe AutoLogon on the second VM from the SALPS console

1. From within the SALPS console, click on the SAL CLIENTS tab
2. Click the group 'Test Group' in the tree so the list is populated with both SAL client computers
3. On the ribbon bar, click Install Safe AutoLogon
4. Click No on the 'Check Client Status First' window
5. Since we already installed Safe AutoLogon manually, we will only install Safe AutoLogon remotely in front of SALVM2.
6. Browse to and select the Safe AutoLogon installation file, setupsafeautologon.exe
7. Skip the box asking for a .salset file.
8. Click the **Begin installation** link. The software will install and SALPS will notify along the way.
9. Once Safe AutoLogon installed, if you are not yet using DNS SRV records to find the SALPS server, go to the Safe AutoLogon software and manually add one (or both) SALPS servers.

# 7. Using assigned iana port 21801

iana.org has assigned TCP port 21801 to WM Software. SAL and SALPS can use this port to communicate instead of previous versions that required clients to either have their firewall turned off or have:

- Port 135 and 445 open on the inbound PC firewall
- Use a service account that is a member of the SALPS and SAL clients' Administrators group
- Enable the SAL clients' Remote Registry service

These settings are not feasible to enable for organizations who have well-known TCP ports closed and/or have a firewall enabled on client and server operating systems.

Because of this and increased security risks, WM Software has added an option to use the iana.org TCP port assigned to WM Software, TCP port 21801, to communicate between clients and servers.

Both the SALPS and SAL software include a utility to enable and open TCP port 21801 on the computer's built-in Windows firewall. If you are using a 3rd party firewall, you will need to refer your firewall's documentation to enable and open TCP port 21801.

The port changing utility is installed with both SAL and SALPS in their respective Program Group. You can also download the port utility from our website, www.wmsoftware.com.

Running the utility and enabling port 21801 will restart the product's service and application. Both SAL computers and SALPS servers require the same configuration.

At this point in this Proof of Concept, if you want to use port 21801, run the utility on each VM client and server running SALPS. The utility creates an Inbound Rule named WMSCommPort21801. It also adds a Registry entry so the software knows to use port 21801.

# 8. Setup DNS

Safe AutoLogon clients do a DNS lookup for an SRV record to get the name of the SALPS server to query for their password.

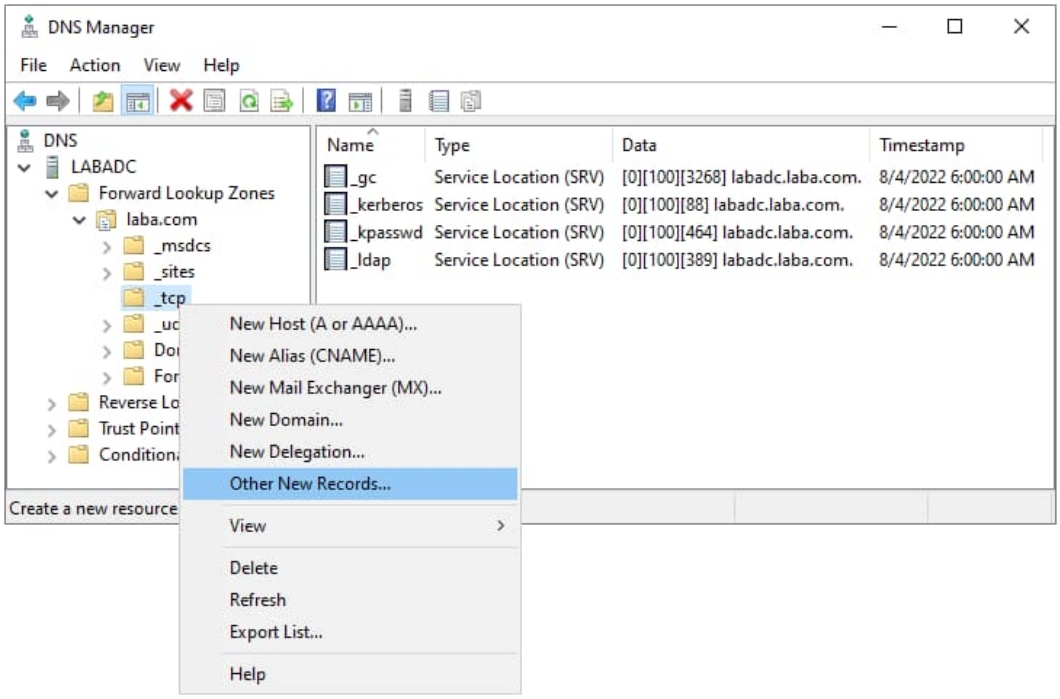
If you are unable to modify your company's DNS servers, skip ahead to ***Section 2***. In production setup, it is highly recommended to use your company's DNS servers for the SRV record.

### *Section 1*

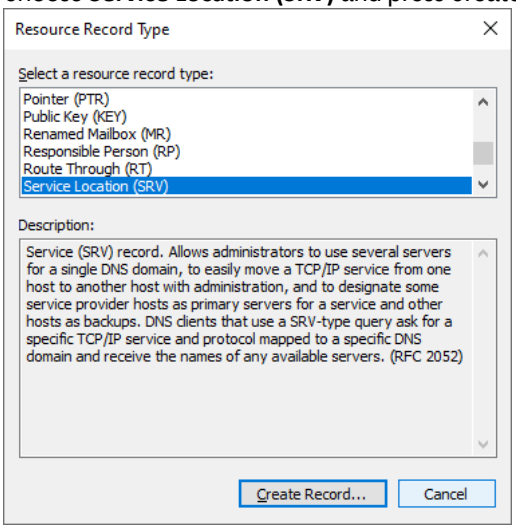
The following steps are taken from a Windows Server 2022 server running the DNS Server role. These steps are the same on 2012 R2, 2016, and 2019 servers running the DNS Server role.

1. Click Start/Windows Administrative Tools/DNS to open the DNS Manager.
2. Double-click on the computer name in the tree to open its branch.
3. Double-click on the Forward Lookup Zones branch
4. Double-click on the fully-qualified domain name in the tree.
5. Single-click on _tcp in the tree.

6. Right-click _tcp and choose Other New Records...



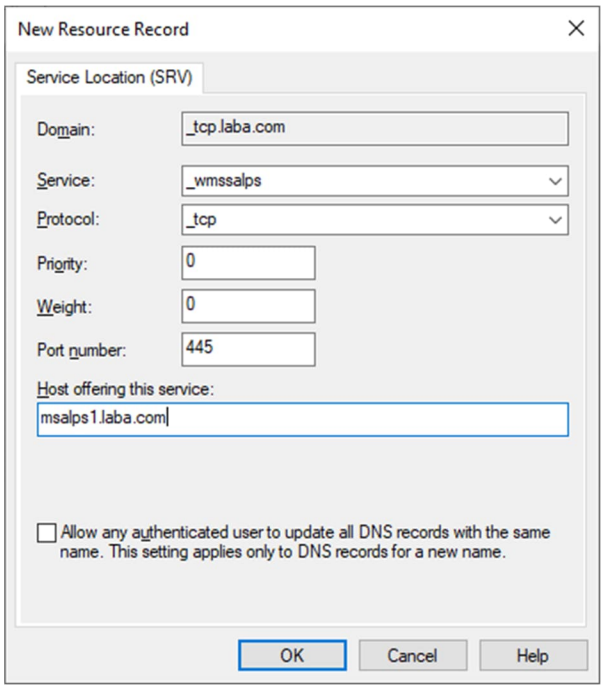

7. Choose **Service Location (SRV)** and press Create Record...




8. Fill in the following fields and then press OK

   a. Service: _wmssalps
   b. Protocol: _tcp
   c. Priority: 0
   d. Weight: 0
   e. Port number: 445

f. Host offering this service: [fqdn_of_salps_server]
-> If your SALPS server is MSALPS1 and your domain is internal.company.com, the FQDN would be msalps1.internal.company.com:

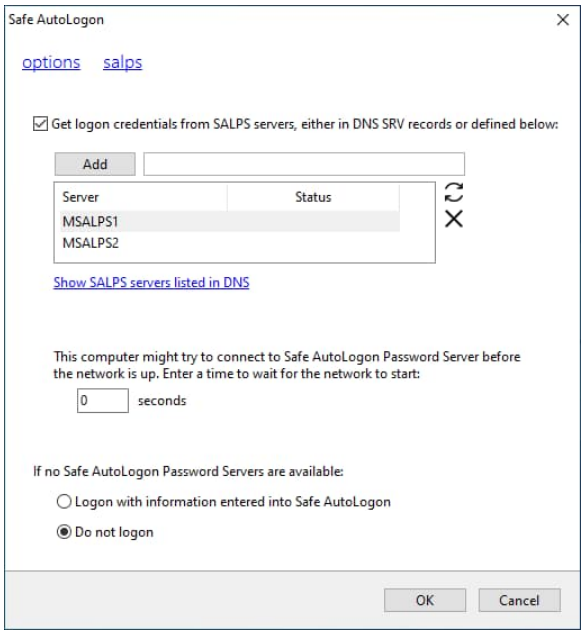


9. Do not checkmark “Allow any authenticated…”
10. Press OK and Done.
11. Repeat the above process for the 2nd SALPS server
12. There should now be two SRV records for the two SALPS servers for _wmssalps:

### *Section 2*

If you are unable to update your company's DNS servers with an SRV record pointing to the SALPS server, you can alternatively add it to the Registry.

1. On each client computer, run Safe AutoLogon, then go to Options
2. Click on salps at the top and add the two SALPS servers to the client:




3. Press OK to save the changes.

## 9. Configure the Safe AutoLogon client

Now that the client software is installed, there are two ways to setup the client:

1. Change username in Safe AutoLogon directly on the client

   Username can also be entered directly in the Safe AutoLogon client. Follow these instructions:

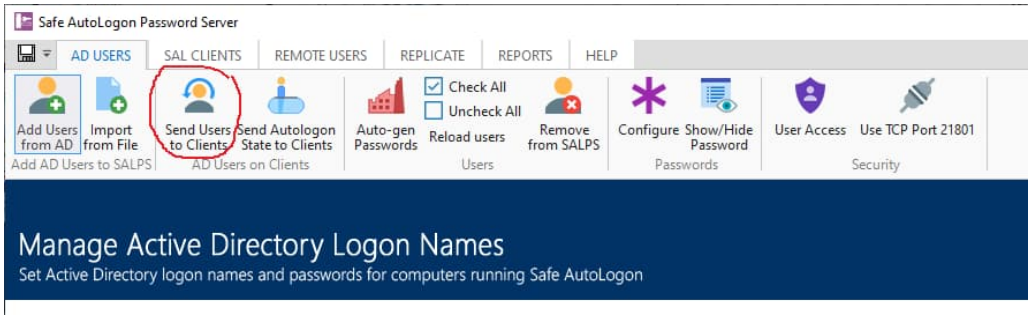
   a. On one of the client VMs, open Safe AutoLogon and check the box '**Automatically logon**'. Then, enter the username you created for the test account. We used the account named sal:


   b. Do not enter a password. The SAL client will get it from the SALPS server.

   c. The Domain field should be populated with the name of the current domain. We recommend using the NetBIOS equivalent name for the domain.

2. Send usernames to clients from SALPS

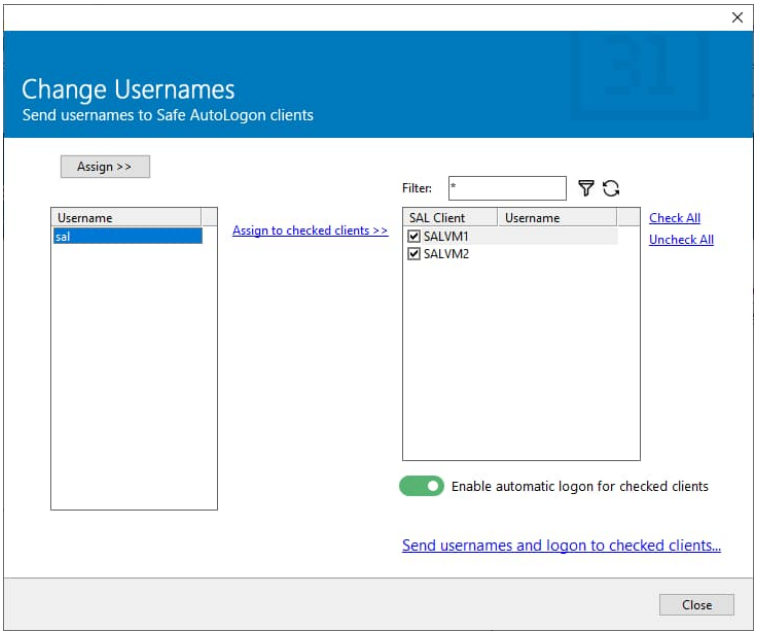
   a. From SALPS, click the AD USERS tab, then click on the ribbon button Send Users to Clients:




   b. Within the dialog, highlight the users you want to send to the client computers on the left.

   c. Checkmark the destination computers. In this proof of concept, we are sending the username ‘sal’ to both Windows clients running Safe AutoLogon.

   d. Then click Assign to checked clients to assign the username to the SAL client in the table:




   e. Finally, click the link Send usernames and logon to checked clients to update the checked SAL Clients with the usernames you designate.

This dialog allows you to change users on remote SAL clients without having to remotely or physically ‘touch’ the clients.

Now, run Safe AutoLogon on the clients and you will see the username appear.

## First test: Test Safe AutoLogon by automatically logging on with a Restart

Restart the VMs running the Safe AutoLogon client. They should automatically login after connecting to the SALPS server to retrieve the password. This might take a minute or shorter.

## Further testing: Change the domain password in SALPS

This will show you how to utilize SALPS to automate changing domain passwords for usernames

1. Run the SALPS software and click on the AD NAMES tab.
2. In the Password field, type a new domain password for the checked user.
3. Then, click the 'Set for checked >>' link to set the password for the checked usernames (if a username is not checked, it will not have its password set).
4. Press the Save icon to save the changes to the SALPS database. This also saves the password to the Active Directory Domain Controllers.
5. Go to the other VM running SALPS. Click Yes so the changes made get transferred to the other SALPS server.
6. Restart the VMs running the Safe AutoLogon client. They should automatically logon to Windows.
7. To show that SAL is using the new password, logoff a VM, then logon with the new password manually.

## Further testing: Test the SALPS server redundancy feature

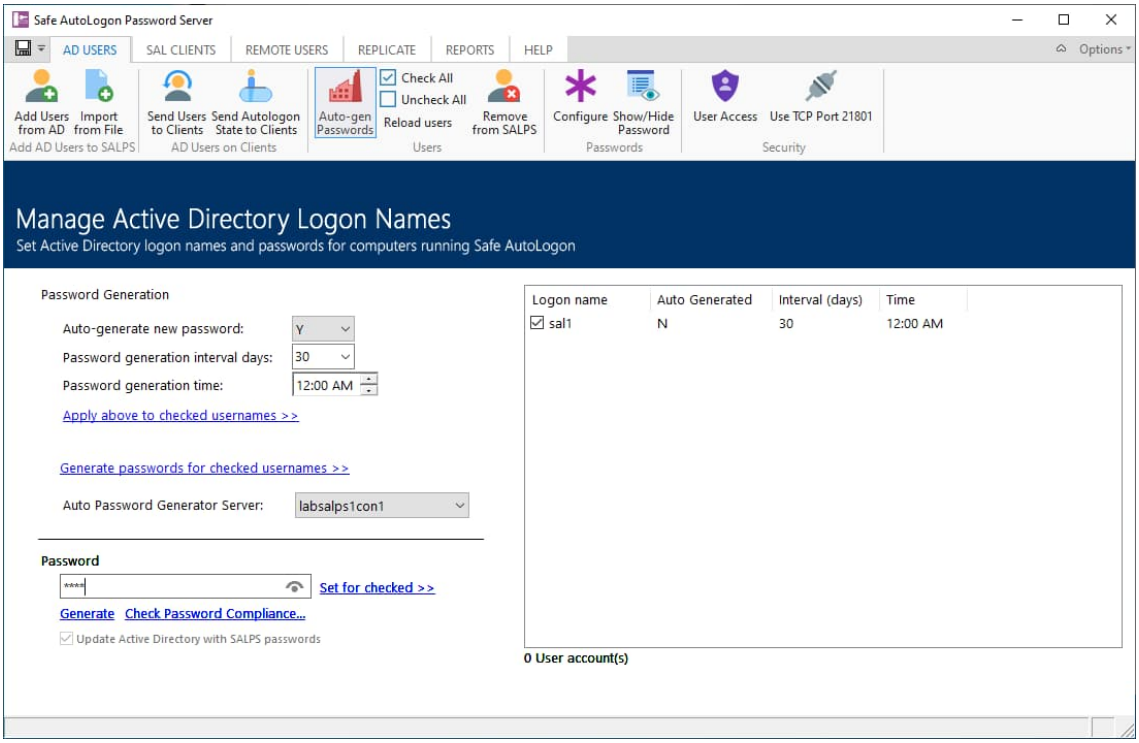
This will test the redundancy of the other SALPS server:

1. Pause the VM on one of the SALPS servers.
2. Restart a Safe AutoLogon client.
3. The SAL client will automatically logon using the other SALPS server.

## Further testing: Test the Automatic Password Generator feature

Now we will test passwords being automatically created and the Safe AutoLogon clients using the new password. For testing, we will change the password to daily (every 1 day).

1. Click on the AD USERS tab in the SALPS console
2. Place a checkmark by a username
3. Click the Password Generator icon. The console will display settings for automatic password generation:




4. Choose 'Y' in the 'Auto-generate password' dropdown
5. Set the interval to every day by putting a "1" in the Interval field.
6. Click the link "Apply to checked usernames"
7. Save the changes by pressing the Save icon in the upper-left corner of SALPS
8. On the following day, after the time entered, the password will change and will meet complexity requirements.
9. Click the Show/Hide Password to see the password. It should have changed.
10. Restart a client running Safe AutoLogon
11. The SAL client will automatically logon using the new password
    Note: also verify the password choosing the "All usernames and passwords" on the REPORTS tab

## Using SALPS to configure multiple Safe AutoLogon clients

Now let's show how to remotely distribute SAL settings to client computers that are (and are not) running SAL.

When you want to update SAL client computers with a username or settings, manually doing these tasks would consume a huge amount of time. SALPS automates these tasks Let's follow these basic steps:

1. Configure a SAL client as the "template" settings to populate other SAL clients.
    a. Install SAL on two Windows VMs (for this example, we'll name them PC1 and PC2). The operating system names do not matter, you will just need to keep separate saved files for the same Windows architectures (32/64-bit). You can also use the SAL client VMs you created in this document.
    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.
    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. Highlight PC1
    h. On the SAL CLIENTS tab, click the "Get FROM highlighted client" button.
    i. Enter the name of the template file to save to (.salset file). This file will contain all the SAL settings on PC1. This file is then used to send to other SAL client computers.
3. Send the settings file to a remote SAL client
    a. Now, put a checkmark only in front of PC2
    b. ON the SAL CLIENTS tab, click the "Send TO checked clients" button.
    c. Choose the .salset file and it will be sent to the remote computer, with the results displayed.
    d. You can also send a .salset file when installing Safe AutoLogon remotely. Click the "Install Safe AutoLogon" and enter the name of the .salset file. Also enter the name of the Safe Autologon installation file.
    e. Installation will proceed and send the username and settings to the remote computer!
    f. 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 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022
  Safe AutoLogon client:
  Windows client operating systems: Windows Vista with Service Pack 2 or later, Windows 7, Windows 8, Windows 8.1, Windows 10, or Windows 11
  Windows server operating systems: Windows 2012 R2 or above.
- Recommended Hardware:
  A system with at least 500MB of free RAM
  One or more 1Gbps or faster network connections
  If SALPS runs in a VM, it is recommended to run on a low-usage hypervisor
  Network packets between the Safe AutoLogon client and SALPS fit within the typical MTU size of 1500 bytes