How-to series:

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

Software version: Safe AutoLogon 9.0, Safe AutoLogon Password Server 1910

www.wmsoftware.com

Contents

Introduction

This how-to document will show you how to quickly setup a test environment for a pilot and proof-of-concept test. This document is written by WM Software engineers from how they setup a test environment. This should only take about 15-20min.

Requirements

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

- An Active Directory domain
- Four (4) VMs on one or more computers (2 SALPS servers and 2 SAL clients) with a minimum of 1GB of RAM and two CPUs. You can test with just two VMs (1 SALPS server and 1 SAL client).
- The SALPS servers must be running on Windows Server 2008 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 2008 or higher) and joined to the domain.
- A DNS server to add SRV records (optional, but highly recommended)
- A domain user that has the delegated Active Directory right of “Reset user passwords”.

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

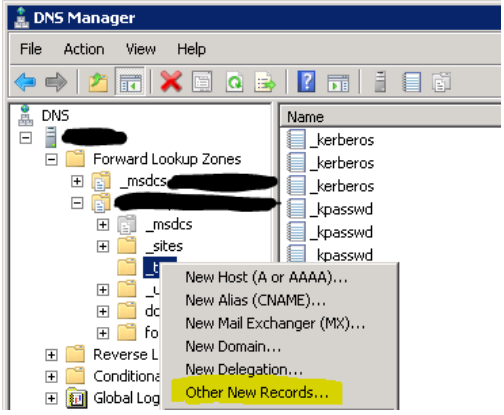
1. Setup DNS

Skip this step if: you do not want or cannot use a DNS server. The SALPS servers will need to be added to each Safe AutoLogon client.

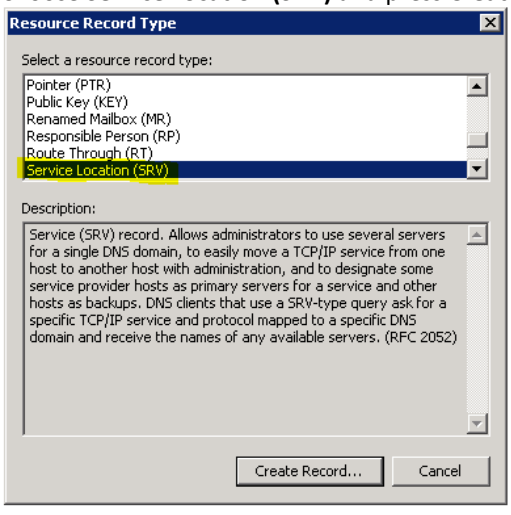
It is recommended to enter a DNS SRV record so the Safe AutoLogon clients can find the SALPS servers. This is how it will be setup in production.

The following steps are taken from a Windows Server 2008 R2 server running the DNS Server role. These steps may vary on other operating systems - contact your domain administrator if necessary.

1. Click Start/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…**

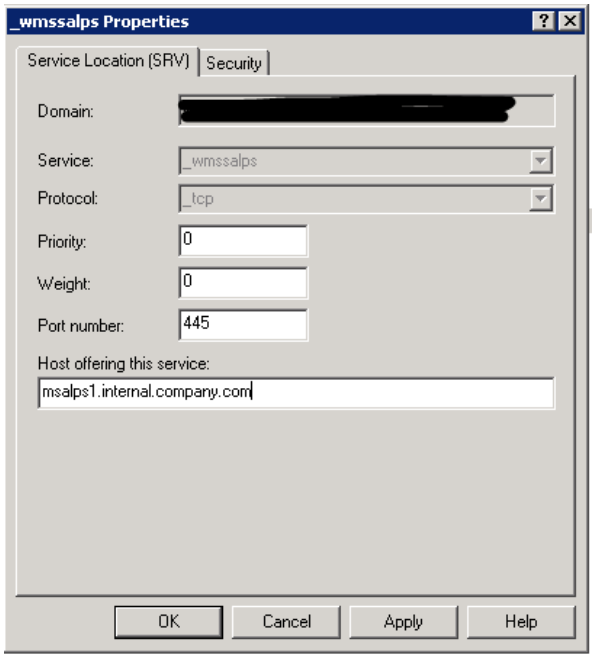


7. Choose **Service Location (SRV)** and press **Create Record…**

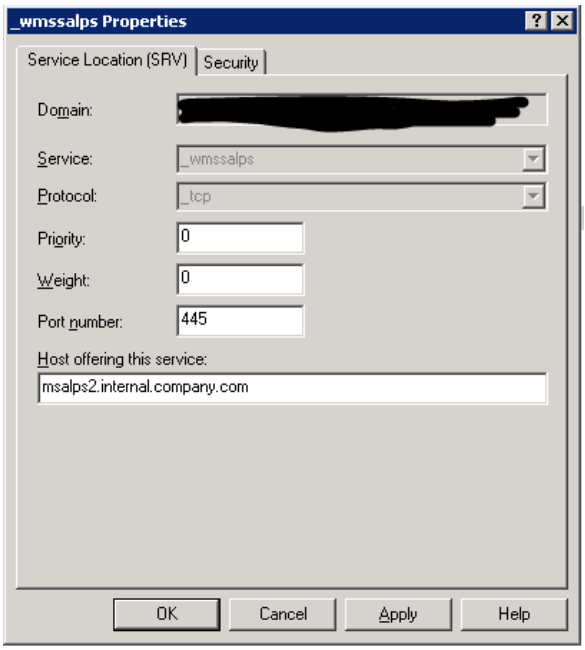


8. Fill in the following fields and then press **OK**

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:

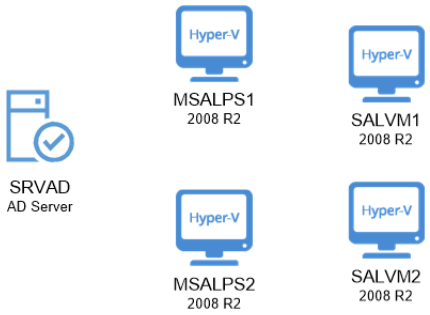


12. There should now be two SRV records for the two SALPS servers for _wmssalps:

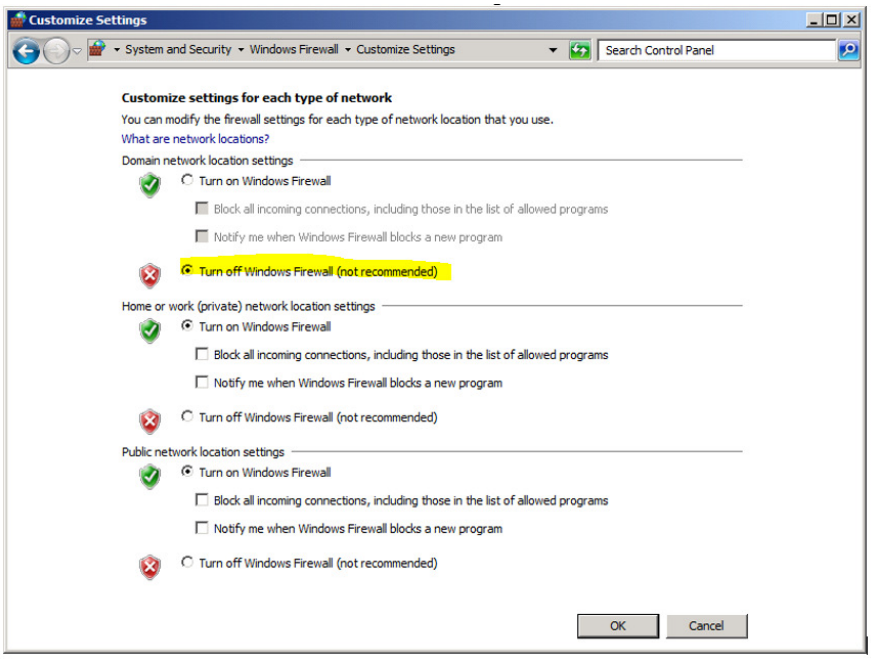
2. Configure the VMs

Configure **four VMs**:

- Two of the VMs (**MSALPS1, MSALPS2**) will be running Windows Server 2019 with SALPS (two servers are needed to test the redundancy feature of SALPS)
- One of the VMs should be running Windows 7 to test the Safe AutoLogon client.
  The other VMs should be running Windows 10 to also test the Safe AutoLogon client.
  Feel free to install whatever operating system you want to test Safe AutoLogon.
  SAL clients: **SALVM1, SALVM2**



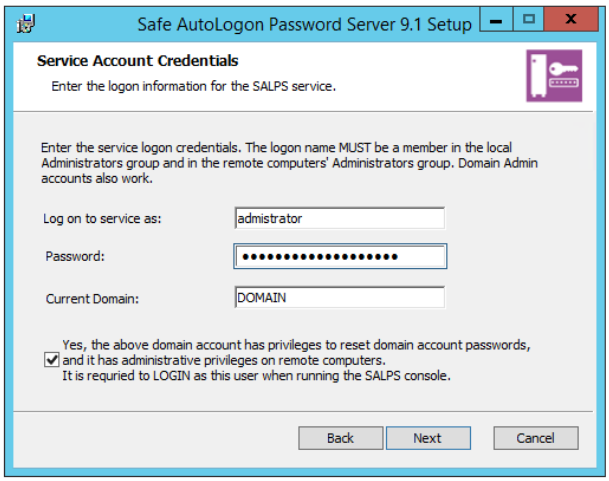
1. Create the four VMs and configure them to each have a minimum of 1GB of RAM and 2 CPUs. The RAM usage of SALPS and SAL is less than 25MB. We recommend 4GB per OS for testing and four CPUs for fastest testing.
2. Install the Windows operating systems on all four VMs
3. Join all VMs to the domain
4. Disable the Domain firewall on all four VMs:



5. 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.

3. Install the SALPS server software

1. Logon to one of the SALPS VM servers
2. Copy the safeautologonpwdsrvsetup.exe SALPS installation file to the desktop.
3. Double-click the icon to begin the installation process.
4. 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. The username running the SALPS console needs to either be the same user or one that has rights to also make changes to Active Directory.



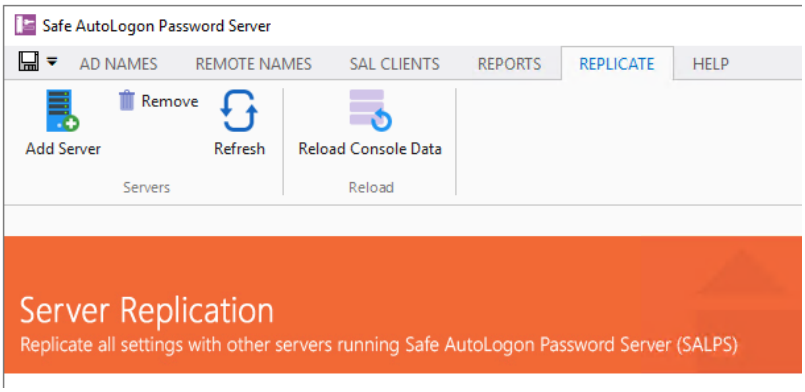
5. Step through the prompts and after a successful installation, press Finish.
6. Repeat the SALPS installation on the other server VM.

4. Configure SALPS – setup redundancy

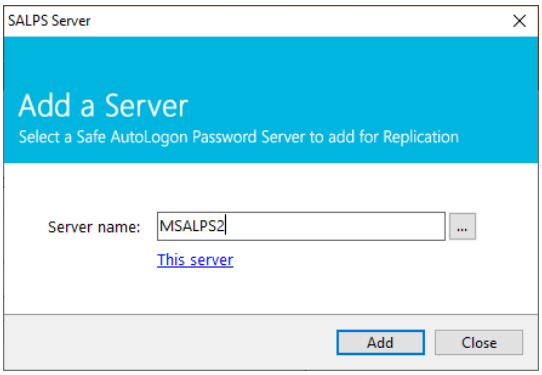
Skip this step if: you are not interested in testing out the SALPS redundancy feature

1. Now we will setup the redundancy feature with the other SALPS server. On MSALPS1, open up SALPS by double-clicking on the SALPS icon on the desktop:

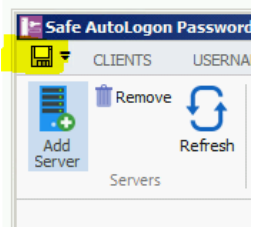
2. Click on the REPLICATE tab.



3. On the Ribbon Bar, click the 'Add Server' button. On this dialog, enter the name of the OTHER server running SALPS. In this example, the other SALPS server's name is MSALPS2. Press **Add** and then **Close**:



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.

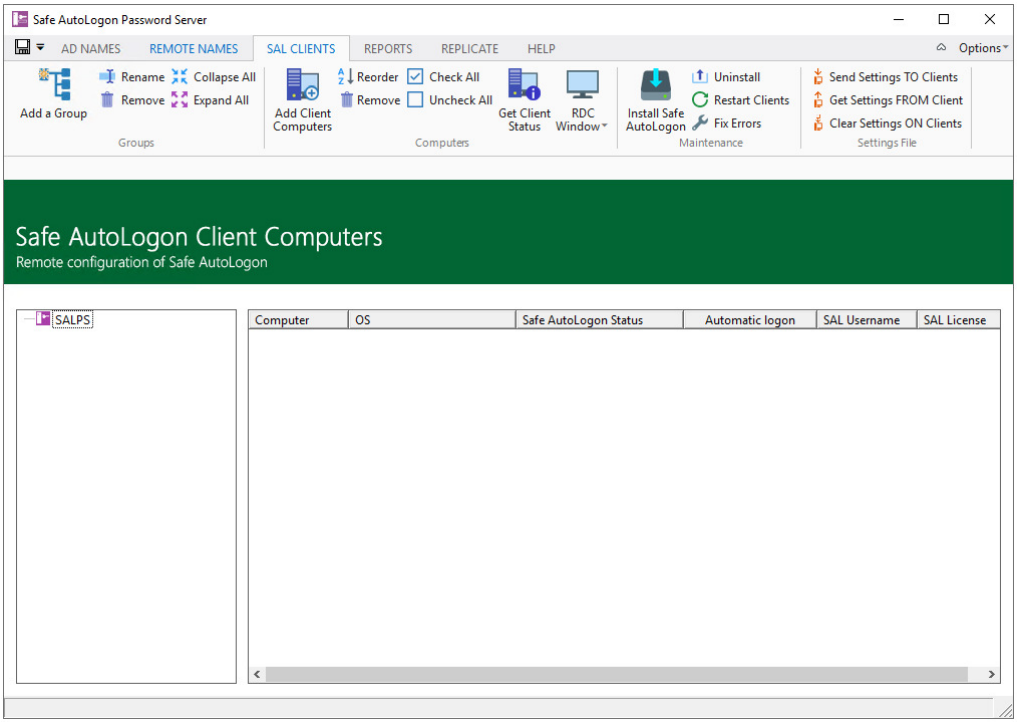


5. Now go to the MSALPS2 VM.
6. Add the MSALPS1 server to it on the REPLICATE tab.
7. Each SALPS server should now have both MSALPS1 and MSALPS2 in the list on their REPLICATE tabs.

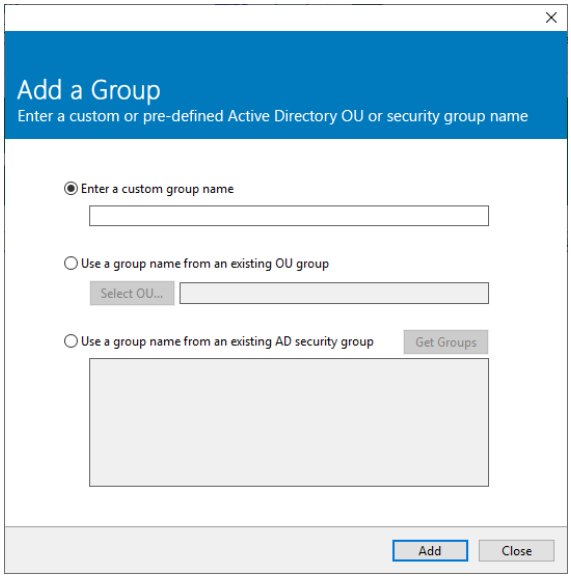
5. Configure SALPS - add computer names

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

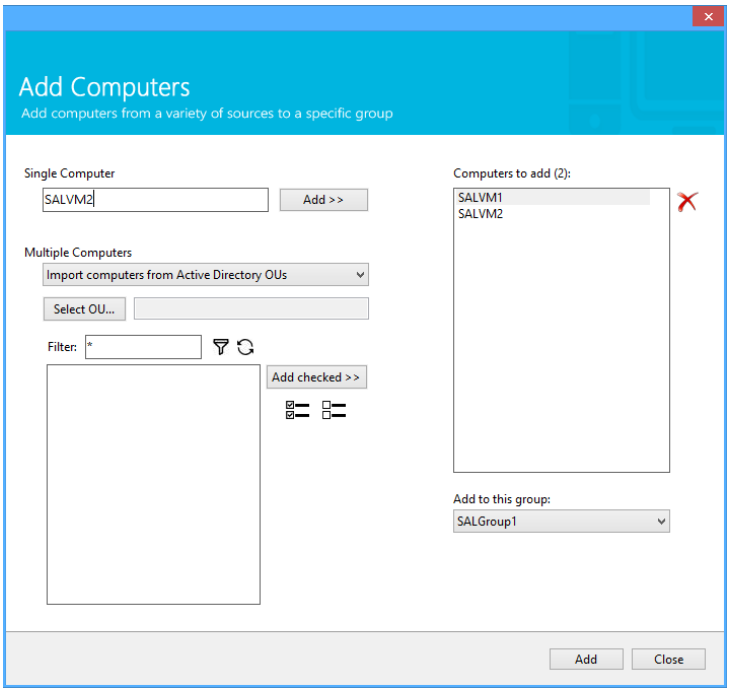
1. On one of the SALPS servers, from the Ribbon Bar, click on the SAL CLIENTS tab:



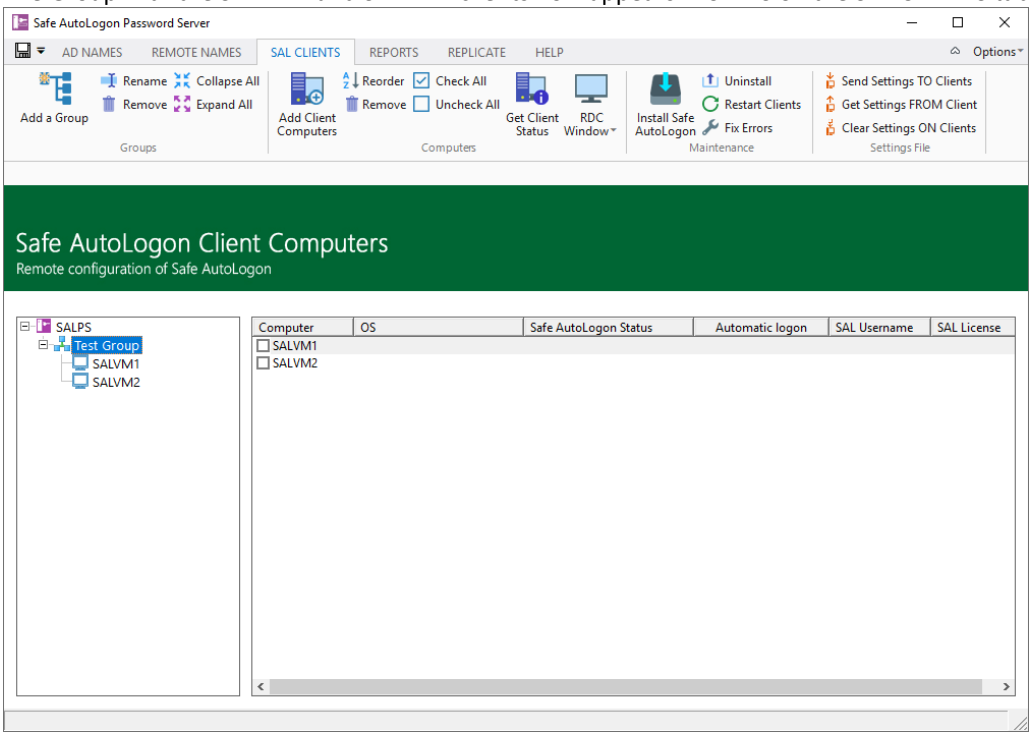
2. Click the '**Add a Group**' button. In this dialog, you can add a custom group name, or select an existing OU or AD Security Group:



3. Still on the SAL CLIENTS tab, click the '**Add Client Computers**' button. Enter the name of the VM clients "SALVM1" and "SALVM2". Press the '**Add >>'** button to add them to the list, then press the bottom **Add** button to add them to the tree. Press the **Close** button to close the dialog:



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



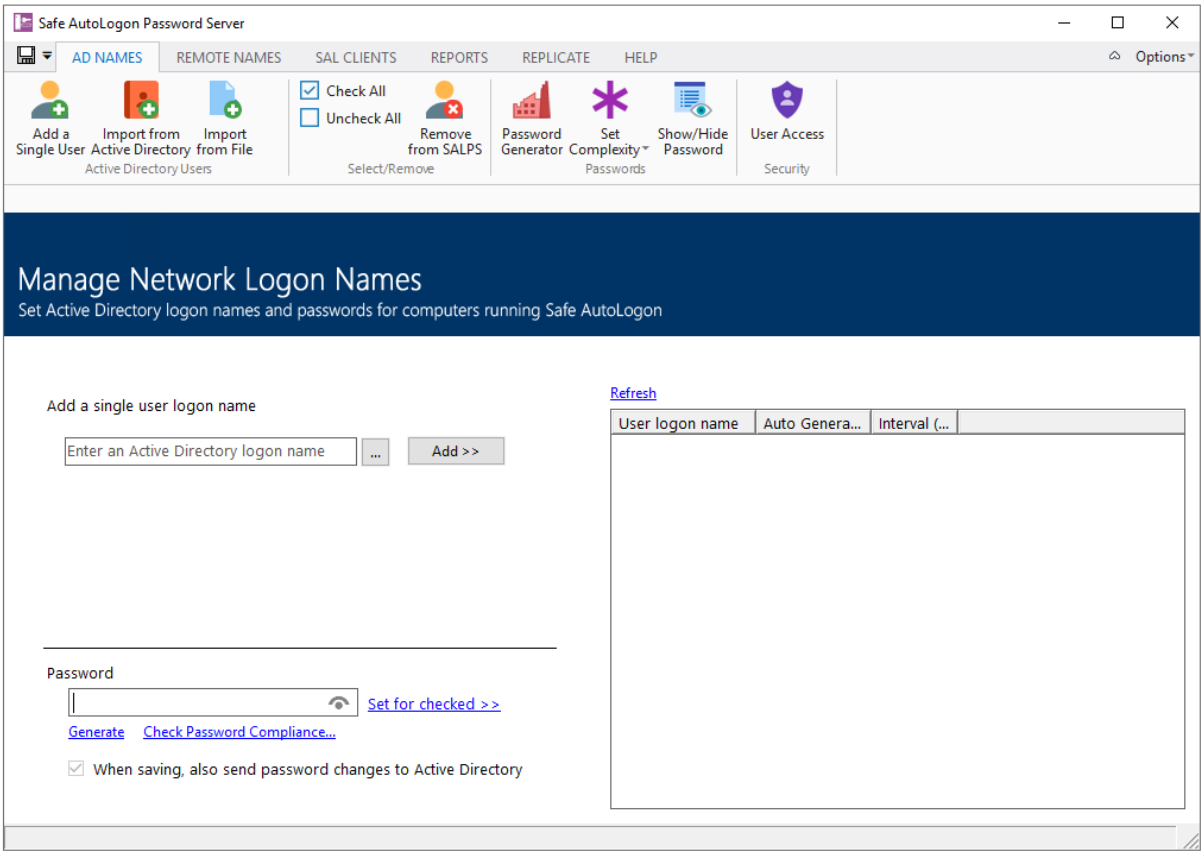
6. Populate SALPS with Active Directory Users

This is the heart of the SALPS/SAL installation. Usernames and passwords are stored on SALPS. When a Windows client running Safe AutoLogon logs in, it first sends its username (in 256-bit AES) to the SALPS server. The SALPS server decrypts, then looks up the username, and sends the corresponding password (in 256-bit AES) back to the Safe AutoLogon software.

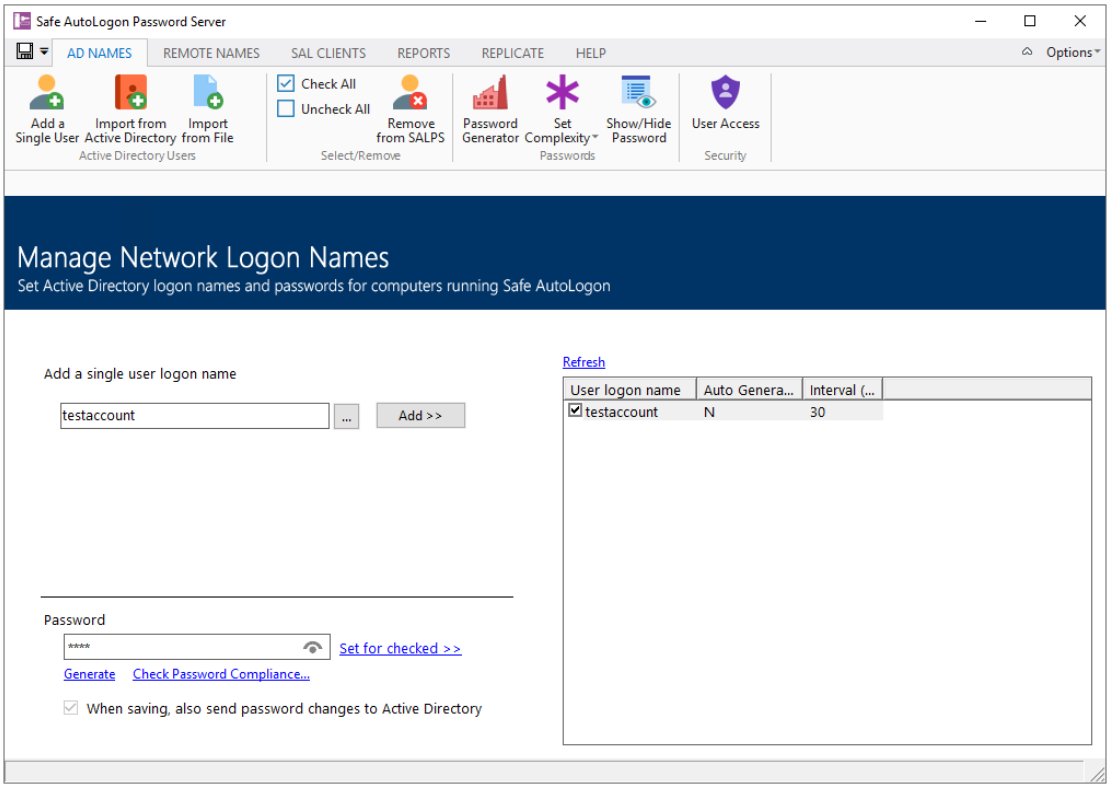
The usernames and passwords are also stored within the encrypted database as encrypted strings using 256-bit AES. SALPS and SAL give you end-to-end 256-bit AES security.

Passwords changed in Active Directory are *not* populated automatically to SALPS. The password must always be entered in SALPS. If a password *is* entered in Active Directory first, then SALPS must then be updated with the same password.

1. On the Ribbon Bar, click on the AD NAMES tab:



2. Type a domain username into the 'Add a single user logon name' field and click '**Add >>**'. This example uses the domain account 'testaccount':



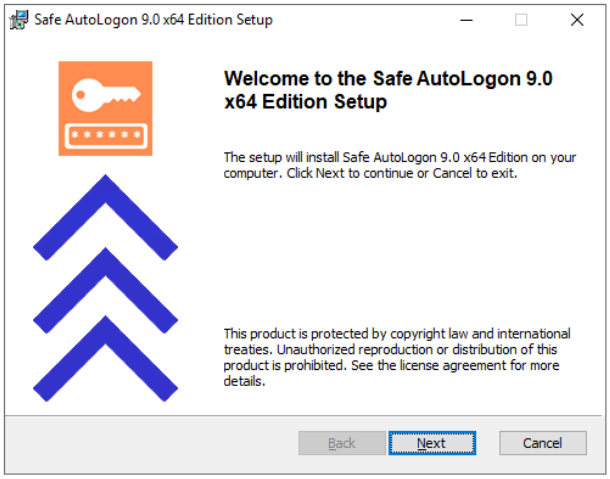
3. Now, we need to tell SALPS what password to use for this account. You can match the password in Active Directory for this account, or you can create a new password.
4. Next, click the '**Set for checked >>**' link to set the password for the checked usernames (if a username is not checked, it will not have its password set).
5. Finally, press the Save icon to save the changes to the SALPS database. This will send the password to the Active Directory Domain Controllers. After this is successful, the database will be sent to the other server for replication.

7. Install the SAL client software

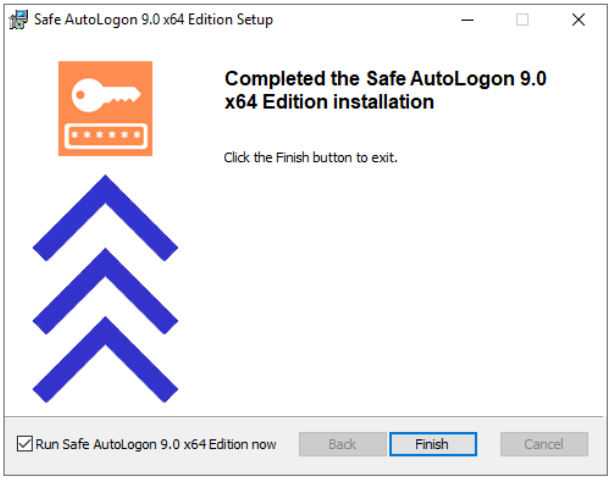
Now that the SALPS server is setup with the usernames and the clients, you can either install the SAL client to the SALVM1 and SALVM2 from within SALPS on the SAL CLIENTS tab, or manually on the SAL clients.

For the purposes of this pilot, we will be installing Safe AutoLogon directly on the test pilot clients.

1. Logon to the Windows client you are going to use for the automatic logon with an administrator's account.
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. This will run Safe AutoLogon for the next step:



8. Configure the Safe AutoLogon client

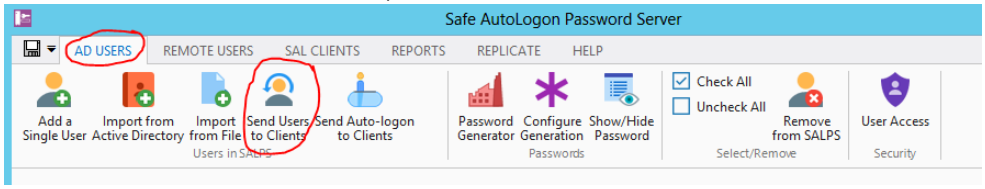
After installing the software on the client computer, either by using SALPS or on the local computer, there are three ways to setup the client:

1. From SALPS, on the AD Users tab, click the ribbon button 'Send Users to Clients'
2. On the client, run Safe AutoLogon and enter the username, then click OK to save the changes.
3. Once you have Safe AutoLogon and SALPS implemented, there are other ways of sending configuration settings down to clients:
   i. From a .salset file that has been 'pulled' from a client, it can be pushed to another computer.
   ii. If you have sccm or other way of pushing a Registry file, you can export the Safe AutoLogon Registry settings from a working configuration, then take that .reg file and use it.

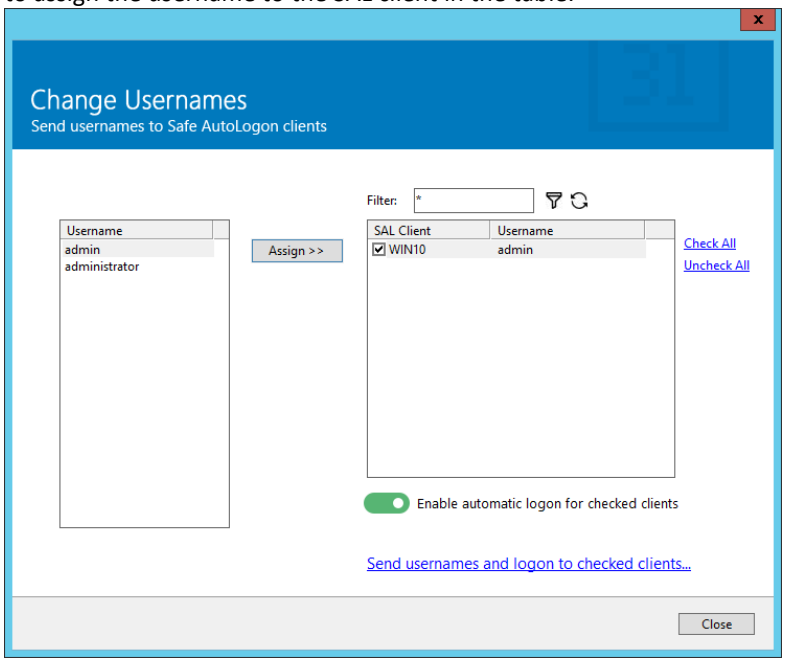
For the purposes of this pilot, we will be using SALPS to send usernames we just entered into SALPS to the client computers.

A. Send usernames to clients from SALPS

1. Click on the 'AD Users' tab in SALPS, then click on the ribbon button 'Send Users to Clients':



2. Within the dialog, highlight the users you want to send to the client computers. Then click Assign to assign the username to the SAL client in the table:

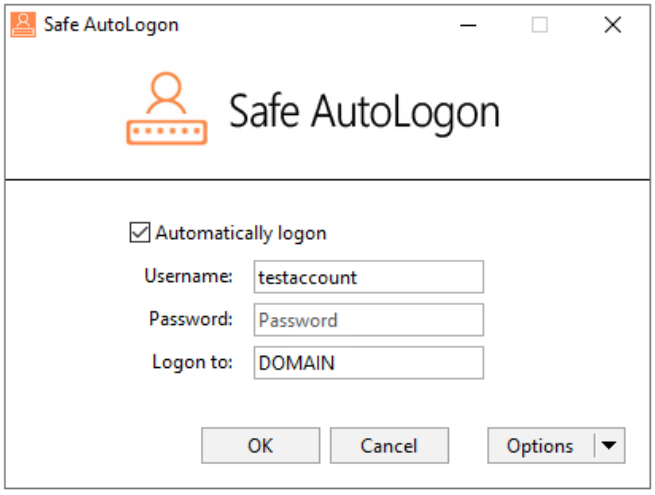


3. Finally, click the 'Send usernames and logon to checked clients' link to update the checked SAL Clients with the usernames you designate. No need to enter anything or 'touch' the client.

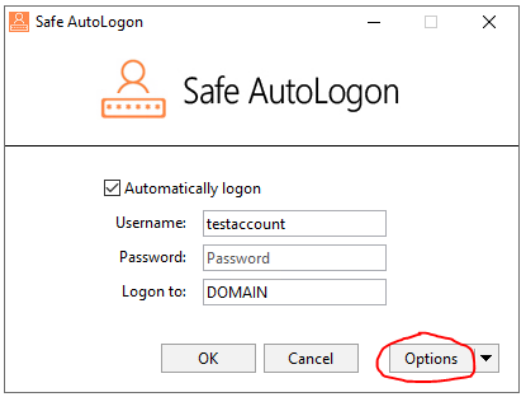
B. Change username in Safe AutoLogon directly on the client

If you would rather enter the username on the Safe AutoLogon software, follow these instructions:

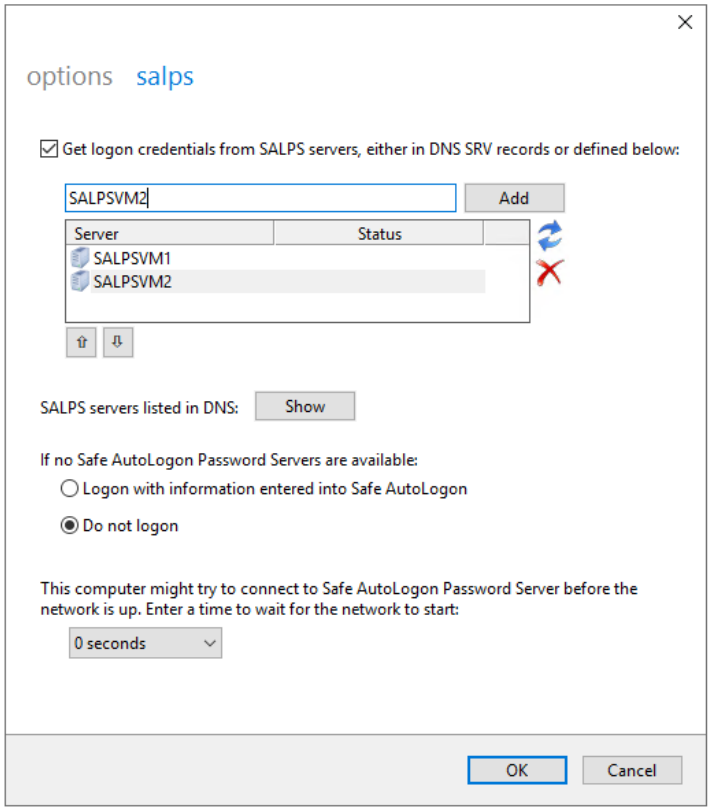
1. On one of the client VMs, open Safe AutoLogon and check the box '**Automatically logon**'. Then, enter the username you created for the test account. We used the account named 'testaccount':



2. **Do not enter a password!** The SAL client will get it from the SALPS server.
3. The Domain field should be populated with the name of the current domain. We recommend using the NetBIOS equivalent name for the domain. In this example, we have a generic domain named "DOMAIN".
4. **Follow this step if:** you cannot setup an SRV record on a DNS server.
   Instead of adding the names of the servers to DNS, you can add the names of the SALPS servers directly into the Safe AutoLogon client software as follows:
   a. Press the Options button from the main window:



   b. Click on the 'salps' header, then enter the names of the SALPS servers:



c. Now the SAL client to lookup the names of the SALPS servers without using DNS. This option must be done on all SAL client computers if you are unable to add an SRV record to the network's DNS.

d. Press OK to close the Options window and save the SALPS servers.

5. Press OK on the main Safe AutoLogon window to save the changes.

- There is no need to enter a password – SAL will get it from SALPS
- If you have your SALPS servers added to DNS, there is no need to press the Options button. Safe AutoLogon is designed to look for SALPS servers via DNS on the network and use them if the SRV record(s) exist.
- The domain name should be already filled in for the current domain.

First test: Safe AutoLogon after a Restart

Now, restart the VM running the Safe AutoLogon client. It 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 **'New 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.

Further testing: Test the SALPS server redundancy feature

This will test the redundancy of the other SALPS server:

1. Power down one of the SALPS servers
2. Restart the client running Safe AutoLogon.
3. The SAL client will automatically logon using the other SALPS server.

Further testing: Test the Automatic Password Generator feature

This tests 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 USERNAME tab in the SALPS console
2. Place a checkmark by a username
3. Click the Password Generator icon: 
4. Place a checkmark by “Enable automatic password generation”
5. Set the interval to every day by putting a “1” in the Interval field.
6. Click the link “Set values for checked computer”
7. Save the changes by pressing the Save icon in the upper-left corner of SALPS
8. Wait until after 12:00:00 AM (00:00:00)
9. Restart the client running Safe AutoLogon
10. The SAL client will automatically logon using the new password
    Note: to verify the password, choose the “All usernames and passwords” on the REPORTS tab

Using SALPS to configure multiple Safe AutoLogon clients

Now we will go over how to remotely distribute SAL settings to client computers that are (and are not) running SAL.

When you want to update or install SAL to one, tens, or hundreds of client computers with a particular username or setting, manually doing these tasks would consume a huge amount of time. SALPS automates both of these tasks – installing SAL and setting the SAL settings remotely. 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 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 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 Server 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