ADSync – Important Notes and TroubleShooting Details

Summary

This article provides you some Important Notes plus Troubleshooting details regarding MachPanel ADSync Utility.

Applies To

Applies to MachPanel v6 and UP, and requires ADSync latest version 4.1

Pre-Requisite

AD sync is a separate module and costs may apply. Kindly contact sales for further information.

ADSync installer can be downloaded from our website www.machsol.com by logging into your account. Please review more details at following KB:
http://kb.machsol.com/Knowledgebase/Article/51378

ADSync is installed as per details
here: http://kb.machsol.com/Knowledgebase/Article/50350

ADSync is configured as per details
here: http://kb.machsol.com/Knowledgebase/Article/50351

Basic Note:

- ADSync needs to be installed on Primary Domain Controller and ALL Additional Domain Controllers on Client-AD.
- After installation on all Additional Domain Controllers, configure basic information in ADSync Tool on Primary ADSync Server, then copy **SyncConfigurations.xml** from installation folder on Primary Domain Controller to each Additional Domain Controller. Registry on both types of servers will tell you correct location for configuration file. For old clients the path will be ***C:\Windows\System32*** folder, and for new clients the path to place this file will be ***C:\Program Files\ADSync***. You can confirm/fix the Registry for correct location of **SyncConfigurations.xml**.
- Ensure there are no copies of **SyncConfigurations.xml** anywhere on the Primary or Additional Domain Controllers. There should be one and only one file on each server named **SyncConfigurations.xml**.
- Make sure "Password must meet Complexity Requirements" is Enabled in Local domain

policy.

- To start ADSync to function you need to force all users to change password on On-Premises (Local/Client) AD, please do expire all user passwords and restart all domain controllers.
- If ADSync User Licenses (AULs) reaches it limit, ADSync will stop User syncing. See detail at troubleshooting note 10.

Important Note 1.

Error / Problem Statement: Access is denied when saving the ADSync configuration or saving user mapping.

Cause: The utility is trying to access a system resource (local file or active directory object) and has no sufficient privileges for read/write operation.

Resolution:

1. Please check that the user account provided in 'Admin Login/Admin Password' fields of ADSync configuration studio has sufficient permissions set to the ADSync installation directory and also to the selected logs folder. If not then provide read/write permission for provided user account
2. Also check that the utility is running under a user account which has access (read/write) to the installation directory and to the log files directory.
3. Please check that the user account provided in 'Admin Login/Admin Password' fields of ADSync configuration studio has valid permissions in active directory for all the local organizations (OUs) selected in sync profiles.

Important Note 2.

Error / Problem Statement: Authentication Exception when trying to fetch hosted organizations from machpanel control server or hosted organizations are not listing/fetched

Causes:

1. Sync web service at machpanel control server end is unable to validate the request due to invalid credentials provided for 'service username or service password'.
2. For hosted organizations not listing, the service provider may not have enabled the ADSync option from control server (service director > active directory > organizations)

Resolution:

1. Please provide valid credentials for the fields 'service username/service password'. These must be the credentials which are used to login to customer portal of machpanel. You can even option control panel URL on the AD server to ensure control panel URL is accessible and that using the credentials you are able to login as End Customer which is owner of organization in question.
2. Please verify that the organizations under the selected customer are enabled for ADSync from control server (service director > active directory > organizations). You have to login as provider and enable ADSync for the organization.

Important Note 3.

Error / Problem Statement: Information not syncing to the hosted

Causes:

There are several reasons due to which the ADSync may not be syncing information to the hosted active directory:

1. ADSync service not running on client AD
2. Sync configuration is corrupted
3. Data is uploaded but not syncing due to provisioning-svc on control server not running or having some error

Resolution:

There is no single resolution to this situation. Below are some guidelines to trace out the problem.

1. Please confirm ADSync svc is running on client AD
2. Re-configure the sync profiles (see below: Re-configure sync profiles)
3. Share logs with Machsol support from ADSync client logs folder and machpanel control server (ADSyncExceptions) logs folder

Important Note 4.

Error / Problem Statement:All information is syncing other than the password (password not syncing)

Cause: In this case we do have multiple scenarios which are resulting in failure to sync passwords for local users to hosted.

Resolution: Please see below check list for resolution to this problem.

1. In active directory on client platform "password must meet complexity requirements" under local security policy is set to true
2. VC++ 2010 runtime is installed (specific to OS platform i.e. x86/x64) on all PDC/ADC
3. Check that 'ADSyncPolicy.dll', 'ADSync.PolicyLogger.dll' and 'ADSync.ClienHelper.dll' files are placed inside the '$windir\System32' directory on all PDC/ADC
4. Check that there exists an entry for 'ADSyncPolicy' in following registry path 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Notification Packages' on all PDC/ADC
5. Are all the PDC and ADCs rebooted after installing and configuring the ADSync tool ?

If all of the above checklists are correct then the reason of issue may be configuration problem. Please perform following steps.

Re-configure the ADSync/Sync Profiles:

1. Delete all instances of the '**SyncConfigurations.xml**' file from ADSync host on all PDC/ADC. Even look for this file on other location because those instances may create issues too. You have to be sure that only 1 file exists after your configuration is completed. So, if you are looking for a complete fresh configuration, DELETE ALL SyncConfigurations.xml files.
2. Close ADSync configuration studio, re-open and re-configure sync profiles.
3. Copy the updated '**SyncConfigurations.xml**' file from PDC ADSync installation director to each Additional Domain Controller. Registry on both types of servers will tell you correct location for configuration file. For old clients the path will be **C:\Windows\System32** folder, and for new clients the path to place this file will be **C:\Program Files\ADSync**. You can confirm/fix the Registry for correct location of **SyncConfigurations.xml**.
4. Open the user mapping screen and unselect mapping for all the users by clicking twice on 'select all' box on top right of the users listing and then press save.
5. Exit the user mapping screen
6. Open the user mapping screen again and provide/verify appropriate user mapping and

then press save.

Important Note 5.

How does the utility update the information & how it should be operated?

Lets say you update some user information or password on Client-AD, the information will be replicated to Hosted-AD via control panel in around 15 minutes. Below is a step by step process how this utility shall be operated.

- Save Basic configurations in utility on Primary DC.
- Copy ***SyncConfigurations.xml*** file from PDC installation folder to all ADC(s) to appropriate folder. Registry on both types of servers will tell you correct location for configuration file. For old clients the path will be C:\Windows\System32 folder, and for new clients the path to place this file will be C:\Program Files\ADSync. You can confirm/fix the Registry for correct location of SyncConfigurations.xml.
- Provide On-Premises to Hosted user mapping using the ADSync config studio.
- After providing the mapping, modify the On-Premises Active Directory user account information (Including password).
- To force the sync process to start immediately, Press Sync Now from ADSync Configuration tool, or simply restart the ADSyncSvc using Services.MSC (Windows Services Manager) on PDC.
- This shall update the information to the control server.
- From there, control server uses its Provisioning Service to update the data on associated backend Hosted active directory server. You can also force the control server to process records instantly by restarting provisioning service on control panel server.
- Normally it should take a maximum of 15 minutes to updated the information from On-Premises to Hosted server. To force immediate update, restart ADSyncSvc on Client AD and "MachPanel Provisioning Service" on control server.

This should update the On-Premises active directory user information to the Hosted active directory user.

In case of any issues, you should Enable Logging from configuration studio of ADSync Tool and review that for any problems. Similar logs need to be review on MachPanel Control Server to see if there is any issue in processing of ADSync related data. You can also send the log files generated from inside the selected folder to us for review.

Important Note 6.

General Troubleshooting Notes:

1. Is logging enabled in ADSync Client Configuration Screen?

2. Does there exist "ADSyncPolicy, ADSync.ClientHelper, ADSync.PolicyLogger" dll files in "$windir\System32" folder?

3. Has the client enabled "Password Must meet complexity requirements" in user account policy?

4. Does there exist an entry for "ADSyncPolicy" in[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages]

5. Is ADSync utility installed on Primary Domain Controller and all Additional Domain Controllers?

6. Is Client using "DSA.msc" to change the password?

7. Does ADSync working fine for all the attributes other than password?

8. Does the user provided in ADSync Config Studio for "Local Admin" field has read/write permissions in local AD?

9. Does the Operating user of ADSync Utility has read/write permissions on installation directory and the directory specified for logging?

10. Is LDAP URL correct.

11. Does the On premises admin user have sufficient administrative rights?

12. Does the On Premises Admin user have rights on the installation directory of MachPanel and on the .XML file?

Important Note 7.

Security and Password Policy: Please note that password policy shall remain consistent between source(client) AD and Hosted (Cloud) AD, meaning that both ADs should have similar password policies. Best to have Complex Password Policy. Also there is no need to select the 'reversible password' option in source(client) AD for syncing password.

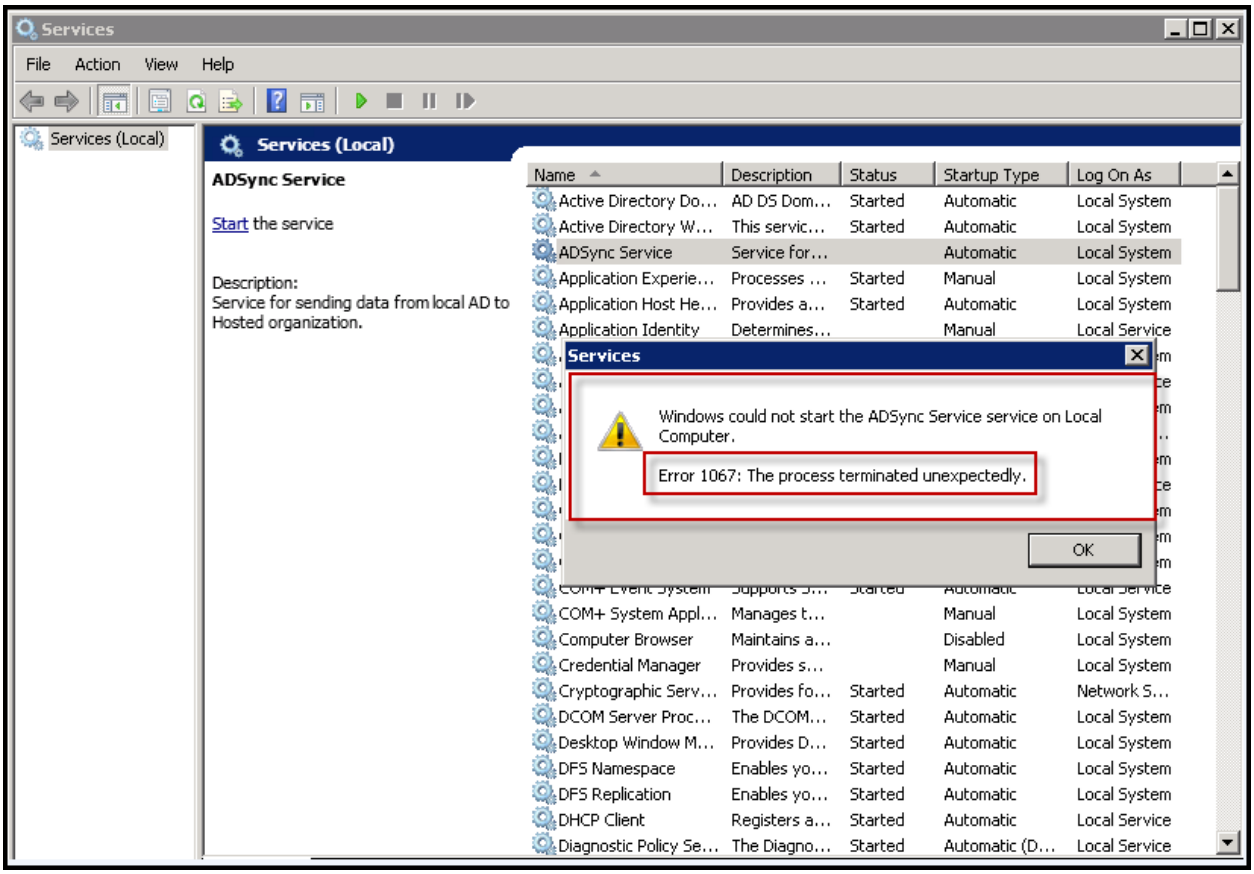
Password for a user account is secured by modern encryption schemes and is stored in a secured place.

To make communication even more secure, one must apply/enable SSL certificate for

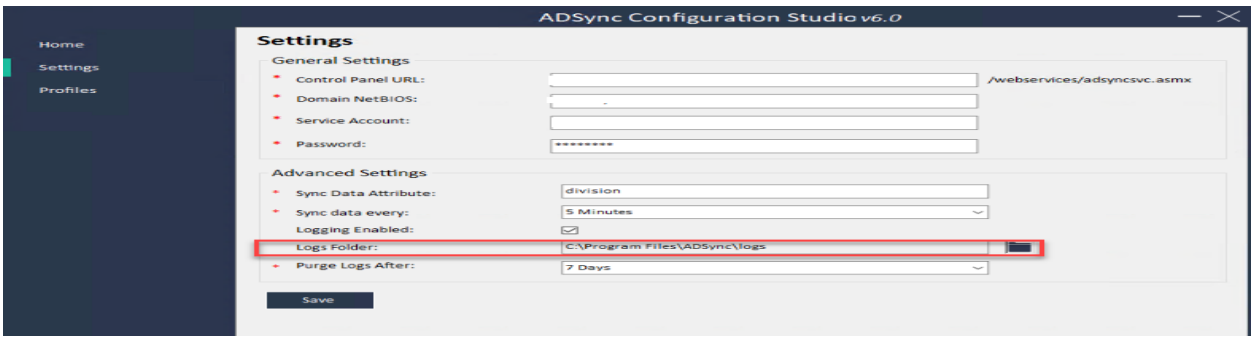
MachPanel Control Panel website and use the ADSync Web Service address as **https://** (like https://cp.providerdomain.com/webservices/Adsyncsvc.asmx)

Important Note 8.

You will face following issue if Log path in ***ADSync Registry*** is incorrect: i.e. it should be same as *C:\Program Files\ADSync\Logs* as shown in the snapshots below:



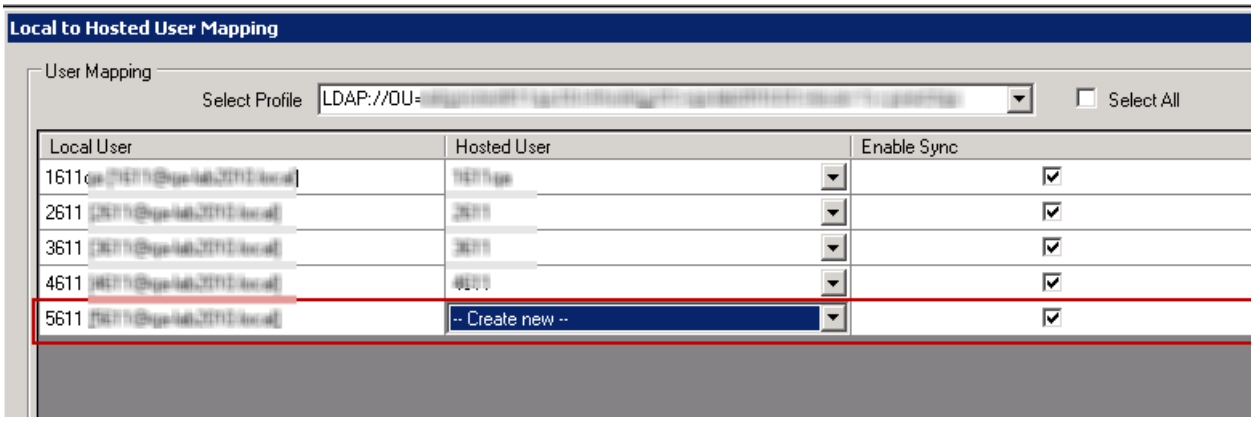
\\



Important Note 9.

Scenario:

If ADSync User Licenses (AULs) limit reaches at "/PCC/System/Licenses.aspx" , User syncing will stop (at local AD: as data of user 5611 being sent normally but not being synced)

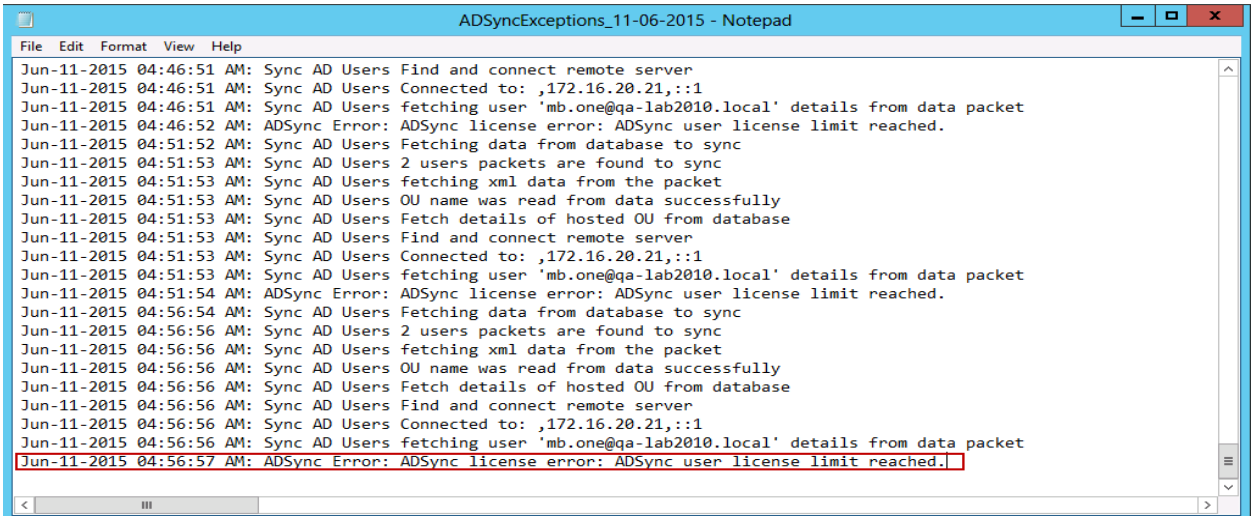


Resolution:

In this case you have to look into logs at control server at *C:\Program Files\MachSol\MachPanel Control Server\Logs* (File: ADSyncExceptions)

ADSync Error: ADSync license error: ADSync user license limit reached.

Contact MachSol Support\Machsol Sales to update licenses. After updating licenses, User syncing will start working again as per ADSync Configuration.



Important Note 10.

Problem:

Password sync working from PDC but not working from ADC.

Verification to Resolve issue.

1. Verify configuration file path in registry and file location in windows.
2. Confirm Notification packages entry in registry
3. Confirm Microsoft Visual C++ 10 Runtime installed
4. Confirm ADC is rebooted
5. Confirm ADSync files exists in system32 folder.

Important Note 11.

Problem:

Utility prompts to restart the machine: ADSync config studio, on application load verifies the required VC++ 10 module installation and custom module registration in windows filters, If either the VC++ 10 installation missing or custom module registration is missing, the utility prompts to restart the machine.

Verification to Resolve issue.

- Check in windows program & features that VC++ 10 is installed and no other version is installed (if there exist multiple versions and are required, then the VC++ 10 installation shall be later one)
- Run 'msinfo32' command in windows command then navigate to 'software components' then to 'loaded modules'. See if 'ADSyncPolicy' module is listed in the loaded modules

Solution:

If 'ADSyncPolicy' module is not present in loaded modules, then perform following steps

- Verify and make sure that 'ADSyncPolicy.dll', 'ADSync.PolicyLogger.dll' and 'ADSync.ClienHelper.dll' files are placed inside the '$windir\System32'
- Verify and make sure that there exists an entry for 'ADSyncPolicy' in following registry path 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Notification Packages'
- If both of the above are verified, then reboot the system and perform the step 2 described in verification process to verify the module is loaded

Important Note 12.

Scenario:

Using default OU 'Users' under sync profile.

Details:

'Users' container 'ObjectCategory' is 'Container' and is system/DC created container whereas admin created container/Ous have 'ObjectCategory' is 'Organizational-Unit'. This is why its available in selection list.

However there's a way around as below.

Workaround:

- Open/Edit 'SyncConfigurations.xml' file of ADSync

ADSync – Important Notes and TroubleShooting Details

- Delete all sync profiles (Inside SyncProfiles). Save and re-open ADSync Config Studio
- Add a profile with some random Local OU selection without "Auto Mapping On", and do not do manual mapping too and Save
- Close Adsync Configuration Studio
- Find and replace highlighted part with 'distinguishedName' attribute value of 'User' container and Save

```
<SyncProfiles value="usersyncprofiles">
<profile id="LDAP://OU=fabricam,DC=contoso,DC=com">
.....
</profile>
</SyncProfiles>
```

MachPanel Knowledgebase
https://kb.machsol.com/Knowledgebase/53477/-ADSync---Important-Notes-and-Tr...