ManageEngine
AD360

Migration from **PostgreSQL database to MS SQL Server**

www.manageengine.com/active-directory-360/

Document Overview

AD360 comes bundled with a PostgreSQL database to store product data. The solution also supports the usage of Microsoft SQL Server to store data and enables you to migrate product data from the built-in PostgreSQL to Microsoft SQL database. This guide will walk you through the database migration process.

Supported versions of Microsoft SQL Server: 2005, 2008 R2, 2012, 2014, 2016, 2017, 2019.

Important points to remember

- Take a backup of the database before you proceed.
- It is suggested to apply the Windows service packs and cumulative updates recommended by Microsoft while migrating to Microsoft SQL Server.

Prerequisites

1. The SQL Server browser must be up and running.
2. For SQL Server network configuration, TCP/IP protocol must be enabled.
3. All the client protocols must be enabled.
   Refer to Appendix A for configuring prerequisites 1, 2, and 3.
4. Microsoft SQL Server access is delegated to a user with sysadmin and db_owner permissions at the server and database levels respectively. For detailed instrcutions, refer to Appendix B.
5. Copy the bcp.exe and bcp.rll files from the directory where the SQL Server is installed and paste them in the AD360 bin folder (<AD360_installed_directory/bin).
   a. Location of the bcp.exe file: <MSSQL_installed_folder>\Client SDK\ODBC\130\Tools\Binn\bcp.exe. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\bcp.exe.
   b. Location of the bcp.rll file: <MSSQL_installed_folder>\Client SDK\ODBC\130\Tools\Binn\Resources \1033\bcp.rll. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools \Binn\Resources\1033\bcp.rll
6. For migration to Microsoft SQL, please install the corresponding SQL Native Client in the AD360 machine as per the Microsoft SQL Server version.

SQL Server version	Command Line Utilities (cmdlnutils)	Native Client (ncli)	ODBC Driver (odbc)
2008	https://www.microsoft.com/en-in/download/details.aspx?id=44272	https://www.microsoft.com/en-in/download/details.aspx?id=44272	Not needed.
2012	https://www.microsoft.com/en-in/download/details.aspx?id=29065	https://www.microsoft.com/en-in/download/details.aspx?id=29065	Not needed.
2014	https://www.microsoft.com/en-US/download/details.aspx?id=53164	Not needed.	https://www.microsoft.com/en-in/download/details.aspx?id=36434
2016, 2017, and 2019	https://www.microsoft.com/en-us/download/details.aspx?id=56833	Not needed.	https://www.microsoft.com/en-us/download/details.aspx?id=56833

7. If firewall is enabled in the Microsoft SQL Server machine, the TCP and UDP ports must be opened.
8. If the Microsoft SQL server you wish to migrate to has **Force encryption** enabled, follow the steps mentioned below.
   a. Convert your certificate to .cer format.
      i. Open **IIS Manager** in the machine that hosts the SQL server you are migrating to.
      ii. In the middle pane, click **Server Certificates.**
      iii. Open the certificate you want to use, and click the **Details** tab.
      iv. Click **Copy to file**.
      v. Click **Next** in the *Certificate Export Wizard* that appears.
      vi. In the **Export Private Key** screen, select **No, do not export the private key,** and click **Next.**
      vii. In the Export File Format screen, select either **DER encoded binary X.509 (.CER)** or **Base-64 encoded X.509 (.CER),** and click **Next.**
      viii. Enter a name for the file and click **Next,** and then **Finish.**

b. Open **Command Prompt** and navigate to <Installation directory>\jre\bin. Use the command below to associate the certificate with the Java KeyStore.
keytool -import -v -trustcacerts -alias myserver -file <pathofthecert>\<certname>.cer -keystore " ..\lib\security\cacerts" -keypass changeit -storepass changeit –noprompt
where <pathofthecert> is the location where the certificate has been stored and <certname> is the certificate name.
The certificate will be added to your Java KeyStore.

Steps to migrate a database

Migrating data from AD360's PostgreSQL database to Microsoft SQL consists of the following two steps:

1. Backing up the AD360 database
2. Migrating PostgreSQL data to Microsoft SQL

Backing up the AD360 database

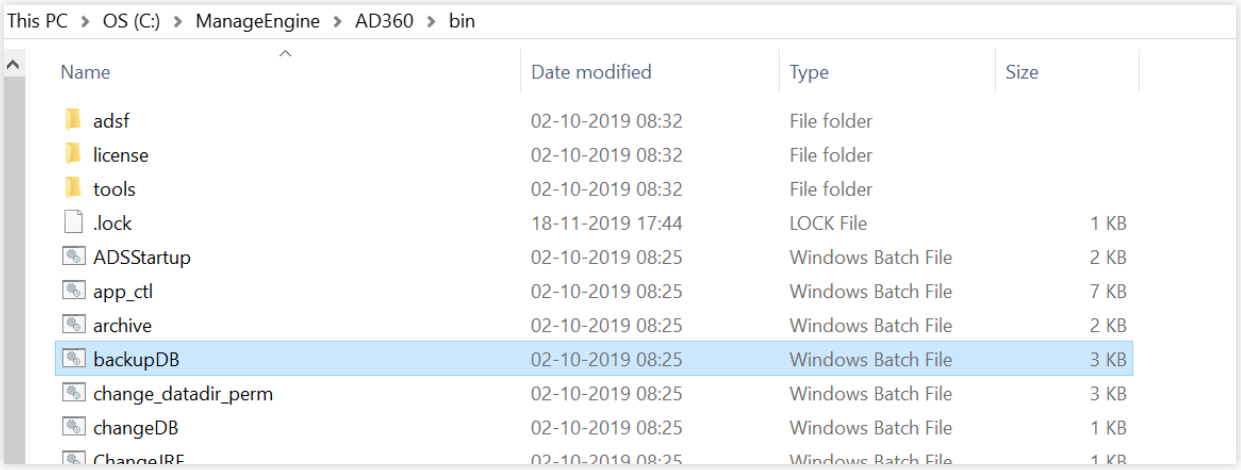
You can skip this step if you are migrating the database of a new AD360 installation.

1. Navigate to <AD360 installation directory>\bin.

   Note: By default, AD360 is installed in: C:\Program Files\ManageEngine\AD360

2. Run the **backupDB.bat** file as an administrator. Do not terminate until the process is finished.

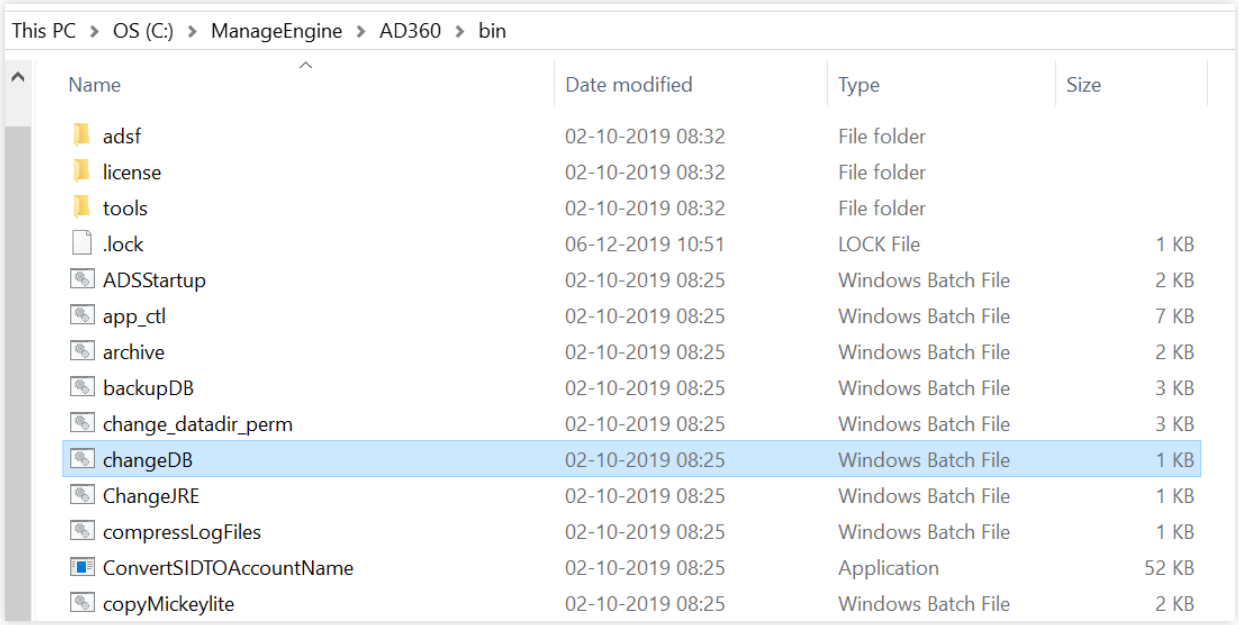
   Note: If you run the backupDB.bat in your local machine, the server needs to be stopped. But using the path – Admin > General Settings > Database Settings > Database Backup in AD360 product console, you can directly make online backup of database without stopping the product.



3. Data in the default database of AD360 will be backed up and stored under <AD360 installation directory>\backup\ AD360_Backup _<Backup Date_ Time> if you have taken an online backup. On performing an offline backup operation, data will be stored under <AD360 installation directory>\backup\ Offline Backup _<Backup Time>.

Migrating PostgreSQL data to Microsoft SQL

1. Open **Command Prompt** and navigate to <AD360 home>\bin where <AD360 home> is the location where the instance of AD360 is installed.
2. Stop AD360 by running **shutdown.bat.**
3. Run **ChangeDB.bat.**



4. From the **Select Database Server** menu, select **Microsoft SQL.**
5. In the **DB Server Name/IP** and **Port fields,** enter the host name or IP address and the port number of the Microsoft SQL database server.
6. In the **Select Server Instance** field, select the SQL Server instance you want to use.
7. For **Authentication,** you can either use Windows credentials or a SQL Server user account.
   a. If you want to use a **SQL Server user account,** then select SQL Server in the Authentication field, then enter the **Username** and **Password.**
   b. If you want to use Windows Authentication, select **Windows** in the Authentication field, then enter the **Username** and **Password** of a Windows domain user account.

Note:

i. The user account entered must have permission to create a database in the selected Microsoft SQL Server.

ii. The bcp.exe and bcp.rll files must be manually moved to the AD360 bin folder as mentioned in the prerequisites section.

8. If the Microsoft SQL server you wish to migrate to has Force encryption on, select the check box against **SSL connection**.
9. Check the box next to Migrate Existing Data to copy the data from your old database to the new database.

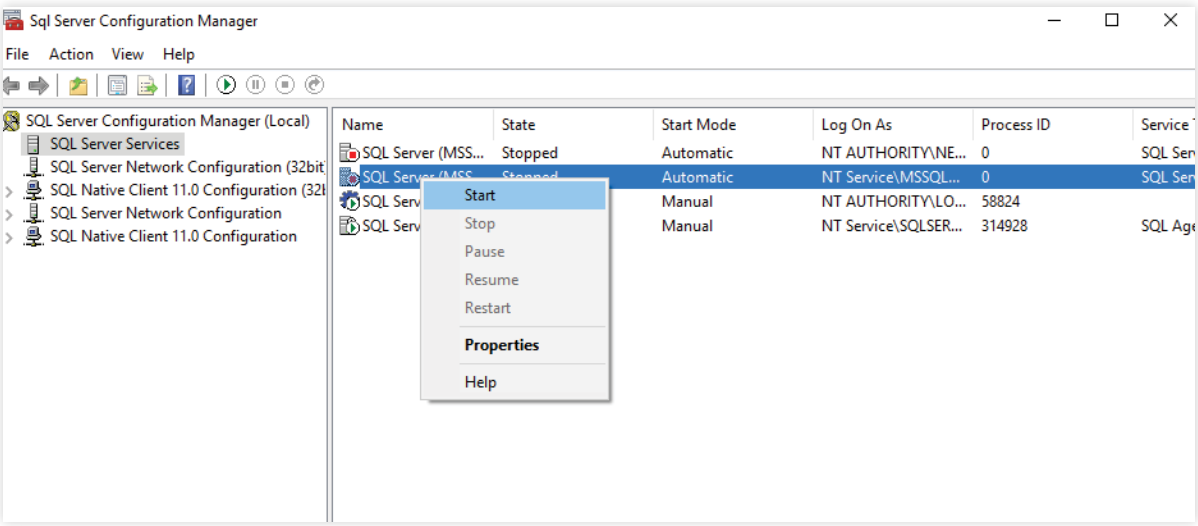
   IMPORTANT: Leave this box unchecked only if you want to change the database of a fresh installation of AD360 or its components.
10. Click **Configure DB.**
11. The Microsoft SQL server will be configured and you can view the status of the configuration once the action is complete.

Appendix A

Configuring Microsoft SQL Server

If you already have a functional Microsoft SQL Server, then this step is not required. Follow the steps below to configure a new Microsoft SQL Server installation.

1. Open SQL Server Configuration Manager, or run **compmgmt.msc** in **Command Prompt.**
2. Go to **SQL Server Services > SQL Server Browser.** Make sure the SQL Server Browser is running.



3. Go to **SQL Server Network Configuration** and double-click **Protocols for <Instance _Name>.**
4. Click **TCP/IP protocol,** and enable it.
5. Restart the SQL Server Service for the changes to take effect.

Note: SQLEXPRESS is the instance name provided while configuring Microsoft SQL Server in general, however, it can be changed. This name will be used for reference.

6. Go back to SQL Server Configuration Manager. In the left pane:

a. Navigate to **SQL Server Network Configuration > Protocols for SQLEXPRESS,** and enable all the protocols.

b. Navigate to **SQL Native Client Configuration > Client Protocols,** and enable all the protocols.

Appendix B

Delegating Microsoft SQL Server access to users

It's necessary to add a login for users to access the configured Microsoft SQL Server either using Windows Authentication or SQL Server Authentication. However, it's not mandatory to create a new login. You can use existing service accounts too. If there are none, then follow the steps given below to create a New Login and equip the user with the necessary permissions.

1. Log in to **SQL Server Management Studio.**
2. In the left pane, navigate to **Machine Name > SQLEXPRESS > Security > Logins.**
3. Right-click on **Logins,** and select **New Login.**
4. Provide a **Login Name,** and choose whether to use **Windows Authentication** or **SQL Server Authentication.**

i. If you choose **Windows Authentication,** enter the Windows NT name of the user to whom access must be granted.

ii. If you choose **SQL Server Authentication,** you will be prompted to create a new **Username** and **Password.**

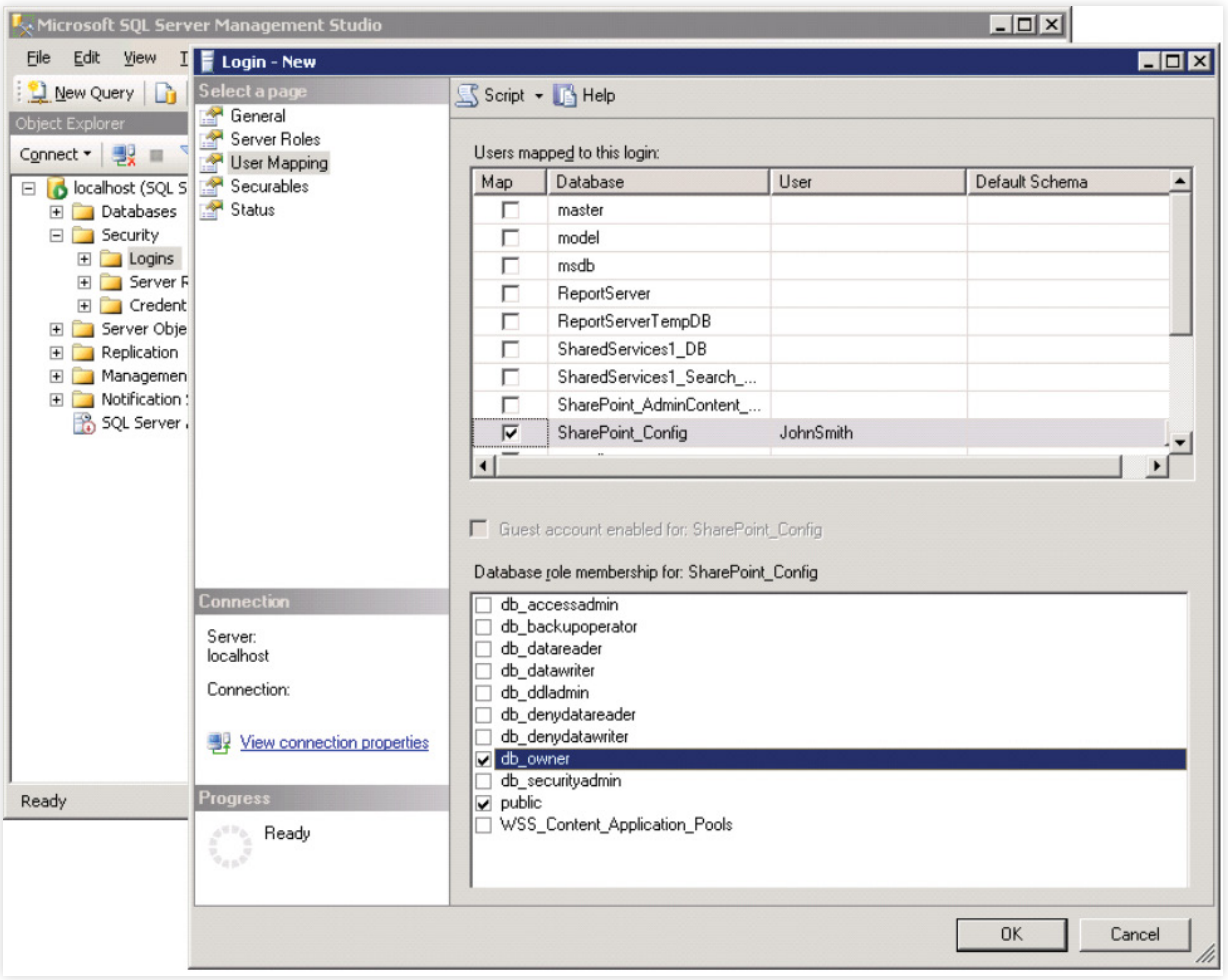
5. The new user must have the **sysadmin** role in the server level and **db_owner** role in the database level. Follow these steps to provide the sysadmin and db_owner role permission:

a. Navigate to **Machine Name > SQLEXPRESS > Security > Logins.**

b. Right-click the user and select **Properties.**

c. Go to **Server Roles,** select the **sysadmin** check box, and click **OK.**

d. Go to **User Mapping** in the left pane. In the **Users mapped to this login** list, check the database and in the **Database role membership** for list, select **db_owner,** and click **OK.**


Microsoft SQL Server Management Studio
File Edit View
New Query
Object Explorer
Connect
localhost (SQL S
Databases
Security
Logins
Server R
Credent
Server Obje
Replication
Managemen
Notification
SQL Server
Ready
Login - New
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Users mapped to this login:
Map
Database
User
Default Schema
master
model
msdb
ReportServer
ReportServerTempDB
SharedServices1_DB
SharedServices1_Search_...
SharePoint_AdminContent_...
SharePoint_Config
JohnSmith
Guest account enabled for: SharePoint_Config
Database role membership for: SharePoint_Config
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
public
WSS_Content_Application_Pools
Connection
Server:
localhost
Connection:
View connection properties
Progress
Ready
OK
Cancel

Note: For details about user roles, refer to the following documents:

For Server-Level Roles: http://msdn.microsoft.com/en-us/library/ms188659.aspx

For Database-Level Roles: http://msdn.microsoft.com/en-us/library/ms189121.aspx

In general, the configured account needs one of these three sets of privileges to complete the migration process successfully.

	Required database role	Required permissions
Set 1	db_owner	Not required
Set 1	db_datareader, db_datawriter, db_ddladmin, db_backupoperator.	Not required
Set 3	db_ddladmin	ALTER ANY TABLE, ALTER ANY AGGREGATE, ALTER ANY DEFAULT, ALTER ANY FUNCTION, ALTER ANY PROCEDURE, ALTER ANY QUEUE, ALTER ANY RULE, ALTER ANY SYNONYM, ALTER ANY TYPE, ALTER ANY VIEW, ALTER ANY XML SCHEMA COLLECTION, ALTER ANY REFERENCES, CONTROL ON CERTIFICATE::[ZOHO_CERT] TO [user], CONTROL ON SYMMETRIC KEY::[##MS_DatabaseMasterKey##] TO [user], CONTROL ON SYMMETRIC KEY::[ZOHO_SYMM_KEY] TO [user]

Important:

Please note that you must have the db_owner permission while migrating PostgreSQL to Microsoft SQL for the first time. After a successful migration, you can revoke the db_owner permission for the account, and provide the set 2 or set 3 permissions.