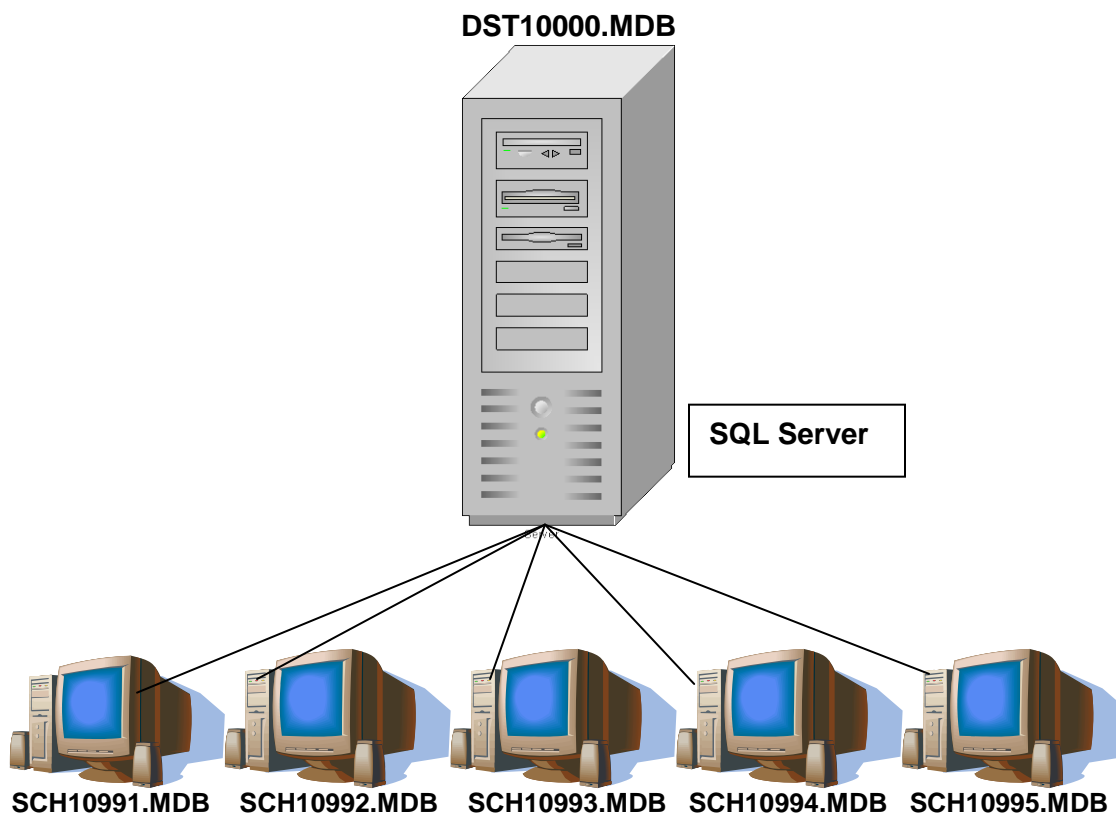# Aeries Client Server - Administration
December 5, 2010

The Client/Server version of Aeries has been created to provide a centralized district-wide database containing all student and related data. This version will utilize a Microsoft SQL Server 2000 database located at the district office.

DST10000.MDB

SQL Server

SCH10991.MDB   **SCH10992.MDB**   **SCH10993.MDB**   **SCH10994.MDB**   **SCH10995.MDB**

The actual software for the Client/Server version of Aeries is identical to the current version of Aeries, except for minor added calls to the server interface module.

SCHOOL USERS   When a **School User** first logs into Aeries Client Server, the user will be prompted with a log in screen where the school code will be entered. A cached copy of the SQL database will be created for the school selected. The cached database is named with the school year and school code requested, for example **SCH10994.MDB**.

The following is the **Aeries Client Server Log In** form. All information **MUST** be entered when logging in which includes the server name or IP address, database suffix, school code, school year, user name and password. Click on **LOGIN** and this information will be stored in the **Eagle1.INI** file. This information will automatically display on upcoming login attempts, except for the password.

If the **Log In** is unsuccessful a message will display. Verify **ALL** information entered. Correct any errors and **Login** again. If the user cannot access the database verify the user has permission to the database and that the correct password is being entered.

DISTRICT USERS   When the **District User** first logs into Aeries Client Server, the Login form utilized is the same as the **School User**. A local cached copy of the district SQL database is created. This database is named for the current school year, for example **DST10000.MDB**.

This cached database is also kept on each user's own computer, and the data will be downloaded from the server as required by the Aeries program selected. The district version of the Aeries software runs against this database, just as in the previous version of Aeries.

DOWNLOAD BASIC TABLES

After the Log In has completed the new blank school database is updated with data from the server with **ONLY** basic school tables. These include the LOC, COD, CRS, TCH, STU and various other major tables. A message will display in the left hand corner indicating which table is currently being downloaded.

After the basic tables are downloaded take note to the size of the database for SCH10994.MDB. The size of this database will not be very large due to the fact that only **Basic Tables** are initially copied to the **local database**.
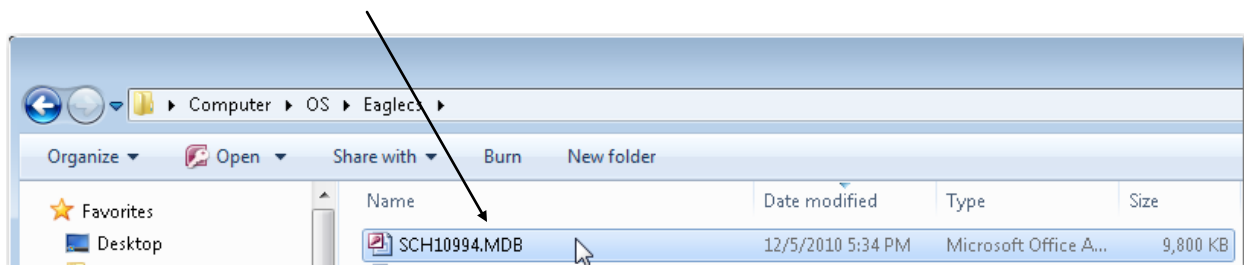

In comparison the district cached copy of the database will include students from all schools in your district making this cached database much larger.

AERIES FORMS AND REPORTS

After logging in the **Aeries Control Panel** will display and all forms and reports are available based on security. As different programs are accessed different tables will be required and will download based on security rights to the programs and/or tables. For example, if **Create New Grade Reporting Table** is generated one of the tables this program uses is the **ATT** table.

If the **ATT** table has not already been downloaded or was previously downloaded but changes occurred to **ATT**, it will automatically be downloaded from the server. Take note to the change in the size of the database after this program was generated and the required tables to run this program have been downloaded.
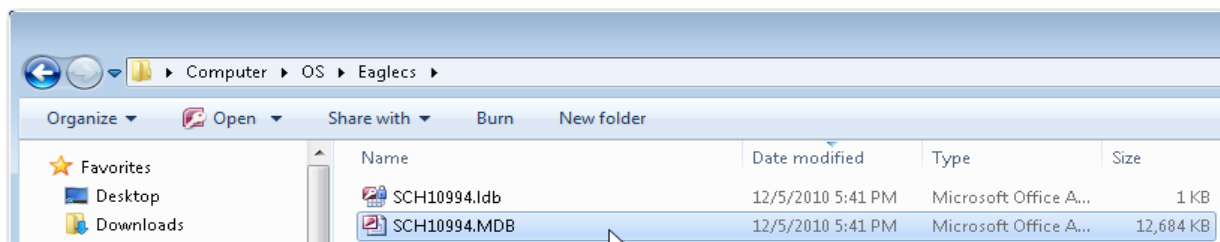
UTILIZING AERIES

The **Client/Server (CS) version of Aeries** generally runs identical to the current version of **AeriesXP**. The forms and reports are generated the same. The only difference is the need to update the server when there are any adds, changes or deletes to records in the local cache copy of the server data.

SQL SERVER DATA

The **SQL Server Data** is continually updated with the users local copies by the use of a date-time stamp kept in each record of every table. Every time a record is added, changed or deleted these timestamps are automatically updated. Deleted records are merely "tagged" as deleted and purged from the system by the Database Administrator.

The local cached data is also constantly updated as required from the server, even while the user is working in **Aeries**. Each record's local date-time stamp is compared against the server's version, and a new record downloaded if it has been changed.

As the user updates records there are also checks made to the server to guard against concurrent updating by other users.

This method allows the **Aeries** software to run faster. Much faster than if all the data were brought down from the server for each and every form or report.

DISTRICT SERVER DATABASE

The schools District SQL Database Administrator is responsible for setting up and maintaining their district SQL Server database. Eagle Software will provide an initial blank SQL database data definitions for each of the **Aeries** tables.

The district is responsible for setting up security to the database and programs, which includes creating the users, groups and roles. After the users are assigned User-IDs, passwords, and given permission to programs and data, they can begin to use the **Aeries** software.

The SQL Server database is initially converted and loaded from each school's Aeries Access MDB using a utility program in AdminCS. This program reads each table in the old school database and uploads it to the server. Once the data is on the server, it can be accessed and maintained using the new **Aeries Client Server** software.

Once a week ALL school and district cached databases are re-created automatically for each user to insure their integrity with the server data. The school databases are created on different days of the week to lessen the impact on the network when all data is being downloaded. On a regular basis the SQL Database Administrator will also purge records tagged for deletion from the server database.

DISTRICT RESPONSIBILITY

- Setup of SQL Server 2005/2008 and Windows 2008 Server

- Install of Microsoft Access XP or Access 2003/2007/2010

- An implementation support fee will be charged to cover the cost of the Eagle Software migration support services.

  a. SQL Server Hardware and Software Installation Consultation
  b. SQL Configuration and Maintenance Consultation
  c. Aeries Software Upgrade Consultation
  d. ABI Migration Assistance
  e. Data Conversion Consultation

- Data Conversion is to be done by the district. Eagle Software will provide the SQL Database and conversion tools along with a set of instructions. Under extenuating circumstances, Eagle Software will consider assisting with the data conversion. Prices for conversions including custom tables may differ.

- Prices for converting existing customizations to run against the SQL database will be extra and may vary.

- SQL Connectivity from the workstations to the SQL Server is the responsibility of the district.

- SQL Server Maintenance is the responsibility of the district.

- The district must have access to or a working relationship with a DBA or other person capable and responsible to install and maintain the SQL Server and the SQL Databases. Qualifications other than a certification must be verified by Eagle Software.

- The district must have access to or a working relationship with a Network Technician or Network Administrator to ensure connectivity to the district network.

The following is an example of a network layout that could be used for the Aeries SQL configuration.

Parent Desktops

Teacher
Workstations

INTERNET

Administrative
Workstations

Private
PTP T1
(or greater)

Private
PTP T1
(or greater)

LAN

Router

Firewall

Router

Load Balancers

Parent Web
Server

Web Servers

Switch

See Aeries Hardware
Specifications for system
recommendations

SQL Server
with Licensing

Typical Configuration calls for single SQL Server

Gigabit connections between all servers

AERIES SQL CONFIGURATION - SAMPLE TOPOLOGY

**TABLE
BASICS**

A relational database system contains one or more objects called tables. The data or information for the database is stored in these tables. Tables are uniquely identified by their names and are comprised of columns and rows. Columns contain the column name, data type, and any other attributes for the column. Rows contain the records or data for the columns.

A large number of the tables within the Client Server database are Student Related Tables that have unique data for each school site. The majority of these tables have a School Number (STU.SC) and Student Number (STU.SN) relationship.

Tables can be changed to have a Permanent ID (STU.ID) based relationship in the SQL version. This can be performed at the beginning of the school year by using the Define Student Table Relationship program accessible through AdminCS. Tables cannot contain any data prior to changing the table relationship.
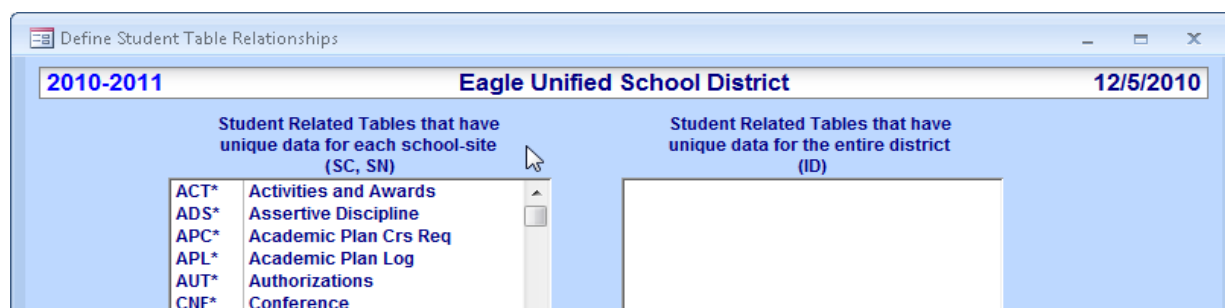
Certain tables in the Client Server database will also be considered Global District. This means that the table will be maintained by the district and will be downloaded to all schools with every login. For example:

- **COD** – Code Table
- **COL** – Colleges
- **CHI** – Course History Institutions
- **CRS** – Course Data
- **CSN** – Content Standard Names
- **CTL** – Testing Control Table
- **EMP** – Employers (Work Permit)
- **FLF** – Field Length Files
- **FLR** – Field Length Record Layouts
- **SBE** – Standards Based Setup
- **SBV** – Standards Based Valid Marks
- **SOC** – Suspendable Offense Codes
- **STN** – Standards
- **STR** – Street File
- **TTC** – Tables to Copy
- **VND** – Vendors

NOTE: **For new ID Based tables please refer to Field Level Permissions.**

PROGRAMS AND TABLES	The following is a list of programs and the tables that are utilized by these programs. When setting up security the user will need access to these tables if they will be using these programs.
AERIES BROWSER INTERFACE	ADS, ASL, ATL, COD, CRQ, DIS, EML, EMU, EVT, GBB, GBL, GTG, LNC, LNK, LOG, PAL, PWA, PWS, SSS, SMS, STG, WEB, WGM
ATTENDANCE	ABS, ACL, ATA, ATC, ATD, ATL, ATP, ATR, ATS, ATT, ATN, CAR, DAC, DAY, LOG, ODE, VER, YTD
BELL SCHEDULES	BEL, BSD, BST
BILLING	BIL, PAY, PSD, PST
CLASSES	CAR, MST, SAV, SEC
CONTACTS	CON, PWA, PWS
COUNSELING	CNF, VIS
DISCIPLINE	ADS, DIS, EXP, SOC
DISTRICT & SCHOOL SETUP	ADR, COD, CRS, DPT, LKR, LOC, LET, LTL, LTR, OPT, PRT, RPP, RUN, STR, TRM, TTC, ZFS
GRADES	GRC, GRD, GRH, GRP
GRADEBOOK	GBA, GBB, GBC, GBE, GBK, GBL, GBM, GBM, GBO, GBS, GBT, GBU
HISTORY / TRANSCRIPTS	CHI, COL, CRT, CTS, HIS, REQ, TDF, TTP, TTM
LANGUAGE ASSESSMENT	LAC, LAF, LAS, TST
MASS SCHEDULING	CRQ, SMS, SSS
MEDICAL	MED, MHS, IMM, DNT, HRN, VSN, HWO, SCO, MNO, VAC
QUERY	QRY, TXT
SCRIP	SCP, STO, STP

|	
SPECIAL ED	CSA, CSE, CSS, CSV (CSD, CSI old data)
STANDARDS BASED GRADE	COD, SBC, SBE, SBG, SBH, SBR, SBV, STN, TRM, USR
STUDENT	ACT, AUT, FEE, FLG, FRM, INV, PGM, RAL, RET, RJN, SSD, STU, SUP, TPS
STUDENT ASSESSMENT	SAD, SAP, SPP, SPS
TEACHERS	TCH, STF, STH
TESTING	CSN, CST, CTL, OBJ, PFT, SCS, STAR, TEX, TST
TESTING PRE-ID'S	PCT, PHE, PRE, PSA, XRF
TEXTBOOK	TBC, TBO, TBT, VND
WORK PERMITS	EMP, WPT

SQL SERVER 2005/08 MANAGEMENT STUDIO	Management Studio is the graphical interface used to manage SQL servers and databases. The core of your administrative tasks will be performed in Management Studio attaching to the Database Engine. The skill set required of the Database Administrative type person includes registering and connecting to SQL servers, backing up, restoring, detaching and attaching SQL databases, importing/exporting data, plus setting up and maintaining SQL user security.

Start **SQL Server Management Studio.**
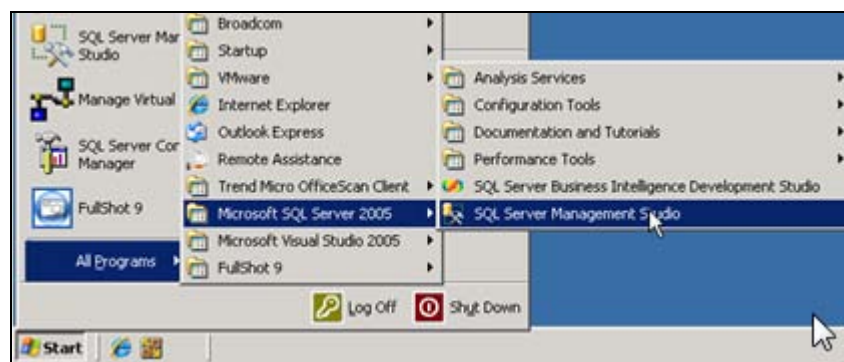
The dialog box Connect to Server will display on top of Microsoft SQL Server Management Studio.
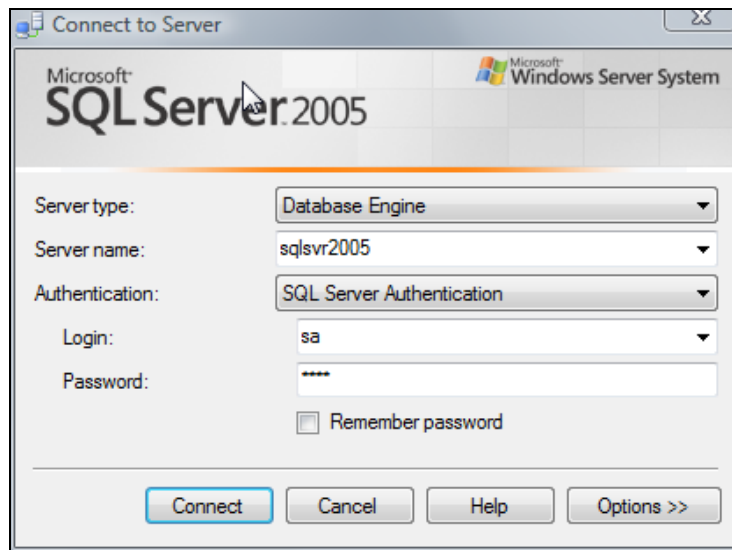

- **Server type** will be Database Engine.
- **Server name** will be localhost or the SQL Server you are attaching to.
- **Authentication** should start out as SQL Server Authentication. You may use Windows Authentication after setting up SQL Authentication logins.
- **Login** – use the 'sa' account. (A 'test' login account was used in the screenshot above)
- **Password** – may be blank for the 'sa' account upon first login. CHANGE the password from blank to a secure password.
- **Remember password** is an option and is not required.

Once connected to Microsoft SQL Server Management Studio, you may add additional SQL Server instances by clicking on Connect to start the Connect to Server dialog box. You may register additional SQL servers to startup by using Registered Servers (Ctrl+Alt+G).
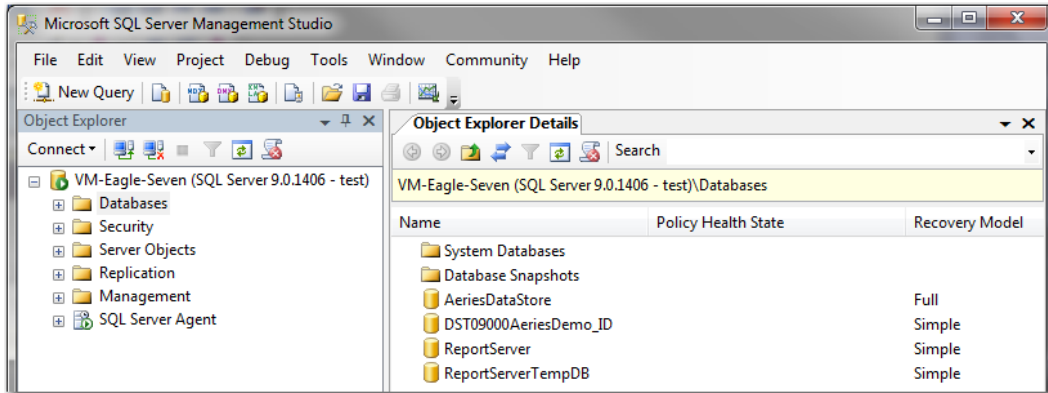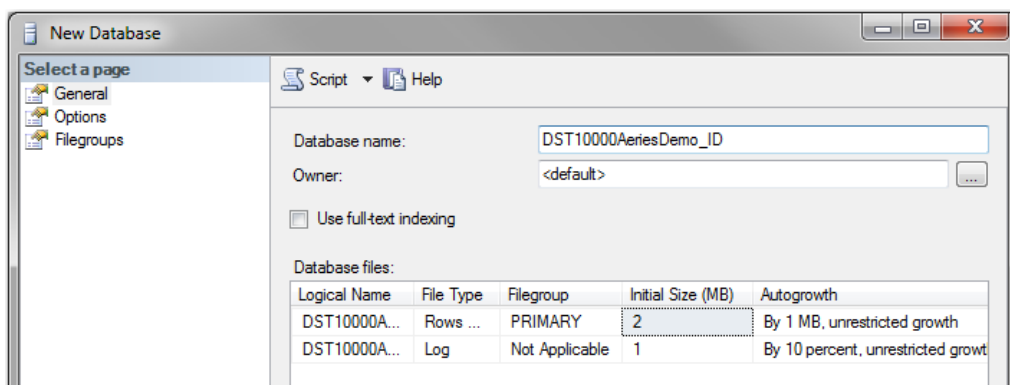

CREATE AN AERIES DATABASE

Right click on Database, select New Database…
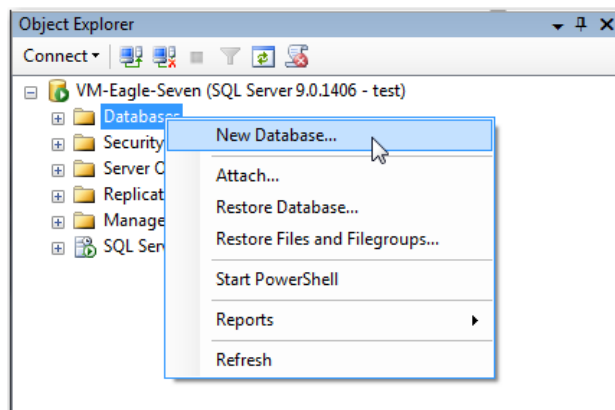
All Aeries databases are created with similar prefix as follows: DSTXX000 where XX is the two digit school year. The suffix will be the name of your database. Example: DST10000Eagle, DST10000TEST.

After typing in the name of your database. Click on **OK**. Now that your database is created Aeries tables need to be created in your new database. Click on **New Query** to open a query tab.
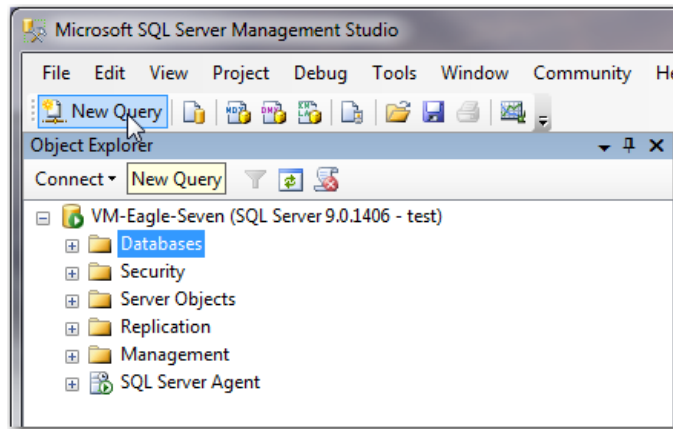
Navigate to the c:\eagle directory and select SQLMODEL.SQL. (FILE | OPEN) SQLMODEL.SQL is the script used to create the Aeries tables. Ensure you are running the script against the new database. Click on Execute or F5 to run the script against the new database.
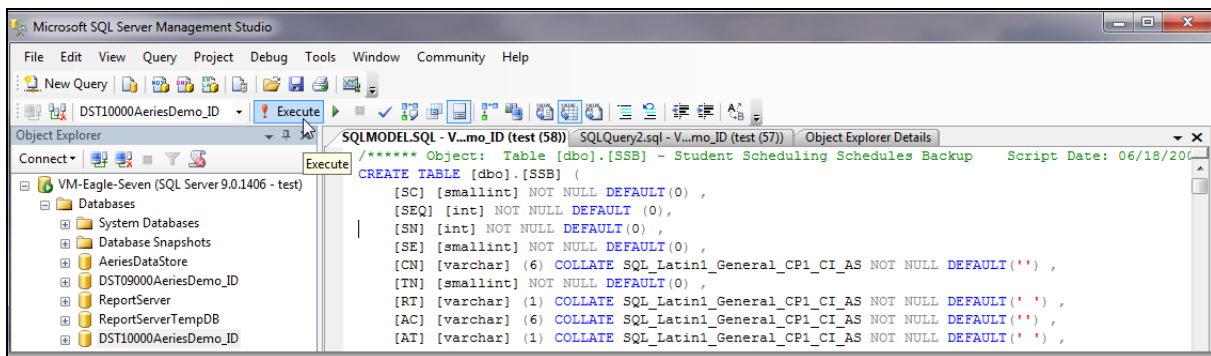
Verify your tables have been created.
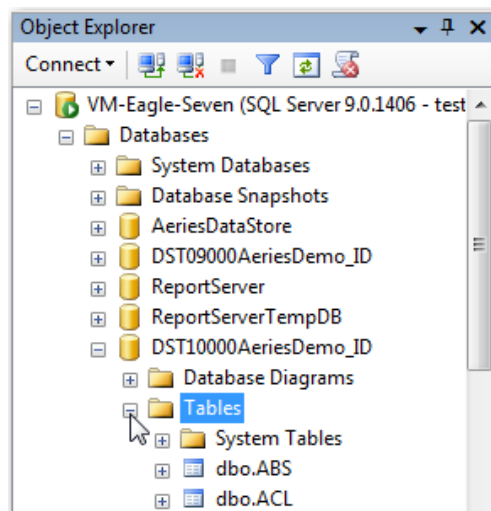
| **SETTING UP SECURITY FOR CLIENT SERVER USERS** | The security for Aeries Client Server utilizes the Microsoft SQL Server 2005/2008. It is required that you know how to setup user accounts and permissions through Management Studio on the SQL server. |

Prior to setting up SQL Client Server Security it is important to determine the different responsibilities of the users. This document will outline some basic set up procedures, and give insight into what tables are required for certain job functions in a typical school district.

One of the benefits of using the SQL server security is that it gives freedom in creating your own "roles", "security groups" or "job duty tasks". This will also allow you to customize permissions to a specific job position.

For example you can create an "Elementary Secretary" role. Give this role appropriate permission to specific tables and/or additional roles like Update Attendance, that will allow this user group to complete the job tasks required for an Elementary Secretary.

PERMISSIONS

The following is a listing of permissions that are available when setting up your user groups.

- **SELECT** – allows user to select and only display data

- **UPDATE** – allows user to select and update data

- **INSERT** – allows user to select and insert or add data

- **DELETE** – allows user to select and delete data

Any combination of permissions can be used to fulfill specific requirements. To view what the table is used for, please refer to Table Definitions.

NOTE: **This document is intended for Database Administrators only**

SETTING UP USERS GROUPS OR ROLES

The following are **examples** of possible job functions and the tables required for the user groups to perform certain tasks. The group list begins with **ALL Aeries Users**. This is a starting point for setting up the user groups or roles and these tables are the minimal tables required to log into Aeries. Also, if the LOG Database Configuration is implemented, required permissions MUST be given to either each group or the group common to all groups.

The **View Only** group would be determined by the district and would contain various tables that allow users to only display data.

The **Admin User** group would also be determined by the district and would give the user full control over tables that are considered secure, such as free and reduced.

|	
A L L A E R I E S U S E R S	**Must have FULL Control:** LTL, OPT, PRT, USO **Must at least have SELECT ONLY:** BEL, COD, CRS, DAY, ENR, IDN, LOC, LTR, SEC, SSD, STR, STU, SUP, TCH, TFR, TRM, TXT, USR **SELECT, UPDATE, INSERT:** QRY
LOG CAPABILITIES	**SELECT, INSERT:** LOG, ATL, EML, GBL
VIEW ONLY	**SELECT ONLY:** Any Aeries Tables
ADMIN USERS	*FULL Control: **Any Aeries Tables that requires security such as FRM, USR etc.***
ASSISTANT PRINCIPAL OR PRINCIPAL	*Changes student classes* **FULL Control:** CAR, MST, SAV, SEC *Creates Schedule Master Schedule* **FULL Control:** SMS, SSS *Enters any conference, discipline, intervention* **FULL Control:** ADS, CNF, DIS, EXP, INV, SOC, VIS Additional Tables **FULL Control:** REQ
ATTENDANCE CLERK	**Updates attendance, creates absence letters, monthly reports** **FULL Control:** ACL, ATL, ATN, ATT, CAR, DAC, DAY, ODE, VER, YTD **At least SELECT ONLY:** ABS, ADR **SELECT ONLY on fields in:** STF (ID, LN, FN, NM, DEL)
COUNSELORS –	*Changes student classes, enters conference and discipline* ♦ **Add to Assistant Principal/Principal group** Enters Course Requests **FULL Control:** CRQ *Creates work permits* **FULL Control:** EMP, WPT
ELEMENTARY SECRETARY	*Updates attendance, creates absence letters, monthly reports* ♦ **Add to Attendance Clerk Group** *Enters all medical info and visits to the nurse* ♦ **Add to Health Clerk Group** *Creates Standards Based Grades & generates Report Cards* **FULL Control:** COD, SBC, SBE, SBG, SBH, SBV, STN, TRM, USR Updates student data **FULL Control:** ACT, AUT, CON, FEE, FRM, INV, PGM, RAL, RET, RJN, SSD, STU, SUP

HEALTH CLERK	*Enters all medical info and visits to the nurse* **FULL Control:** HRN, HSC, HSE, HWO, IMM, MED, MHS, PFT, SCO, VSN
LIBRARIANS	*Enters vendors, textbooks, checkouts, returns, students fees* **FULL Control:** FEE, TBC, TBO, TBT, VND
LANGUAGE ASSESSMENT CLERK	*Enters all language assessment info* **FULL Control:** LAC, LAF, LAS, PGM, SSD
REGISTRARS	*Creates schedules and course requests* **FULL Control:** CRQ, SMS, SSS
	Updates master schedule and changes students classes **FULL Control:** CAR, MST, SAV, SEC
	Enters/Updates student data **FULL Control:** ACT, AUT, CON, FEE, FRM, INV, PGM, RAL, RET, RJN, SSD, STU, SUP
	Enters/updates student grades **FULL Control:** GRD, PRG **At least SELECT ONLY:** GRC, GRP
	Updates history and creates transcripts **FULL Control:** CRT, CTS, HIS **At least SELECT ONLY:** CHI, COL, REQ, TDF, TTP
SPECIAL ED CLERK	*Enters all special education info* **FULL Control:** CSA, CSD, CSE, CSI, CSS, PGM
TESTING	*Creates all pre-id files* **FULL Control:** PCT, PHE, PRE, PSA, XRF
	Loads all test scores **FULL Control:** CSN, CST, CTL, OBJ, SCS, STAR, TEX, TST
	Sets up and maintains student assessment **FULL Control:** SAD, SAP, SPP, SPS

The group or roles listed above can be created using an SQL script similar to the following script for creating the Aeries User group or role.

```
--Grant Access to Aeries DB (To all DB USERS)
EXEC sp_addrole 'Aeries Users'
GRANT SELECT, INSERT, UPDATE, DELETE ON LTL TO [Aeries Users]
GRANT SELECT, INSERT, UPDATE, DELETE ON OPT TO [Aeries Users]
GRANT SELECT, INSERT, UPDATE, DELETE ON PRT TO [Aeries Users]
GRANT SELECT, INSERT, UPDATE, DELETE ON USO TO [Aeries Users]
GRANT SELECT ON ABS TO [Aeries Users]
GRANT SELECT, INSERT ON ATL TO [Aeries Users]
GRANT SELECT ON BEL TO [Aeries Users]
GRANT SELECT ON CHI TO [Aeries Users]
GRANT SELECT ON COD TO [Aeries Users]
GRANT SELECT ON CRS TO [Aeries Users]
GRANT SELECT ON DAY TO [Aeries Users]
GRANT SELECT ON DSD TO [Aeries Users]
GRANT SELECT ON ENR TO [Aeries Users]
GRANT SELECT ON IDN TO [Aeries Users]
GRANT SELECT ON IMM TO [Aeries Users]
GRANT SELECT ON LOC TO [Aeries Users]
GRANT SELECT, INSERT ON LOG TO [Aeries Users]
GRANT SELECT ON LTR TO [Aeries Users]
GRANT SELECT ON SEC TO [Aeries Users]
GRANT SELECT ON SSD TO [Aeries Users]
GRANT SELECT ON STR TO [Aeries Users]
GRANT SELECT ON STU TO [Aeries Users]
GRANT SELECT ON SUP TO [Aeries Users]
GRANT SELECT ON TCH TO [Aeries Users]
GRANT SELECT ON TFR TO [Aeries Users]
GRANT SELECT ON TRM TO [Aeries Users]
GRANT SELECT ON TXT TO [Aeries Users]
GRANT SELECT ON USR TO [Aeries Users]
GRANT SELECT ON VAC TO [Aeries Users]
GRANT SELECT, INSERT, UPDATE ON QRY TO [Aeries Users]
```
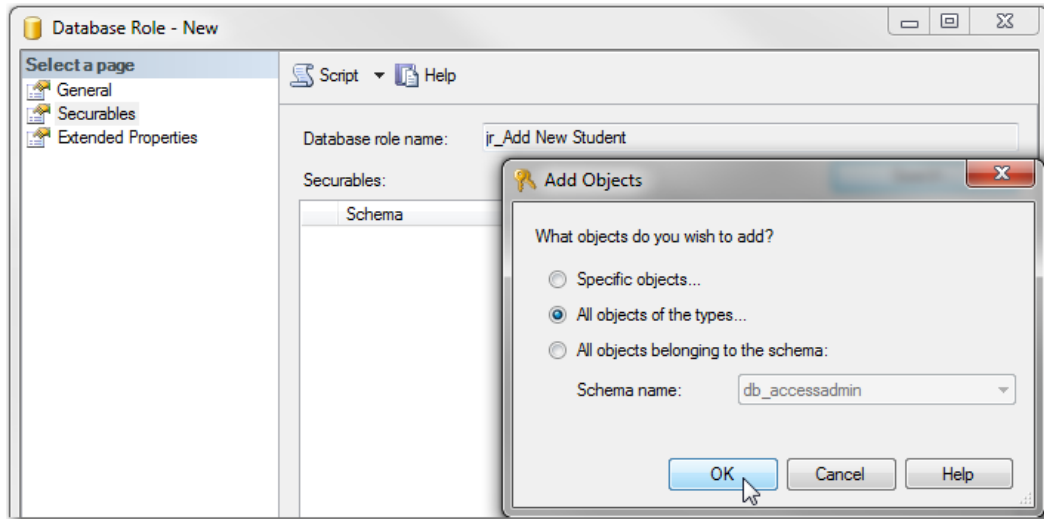
ADDING ROLES

Roles, groups or tasks can now be added to your database. Click the mouse on **New Database Role**. The first roles to be created are the **Aeries Users**, **View Only** and **Admin Users**.
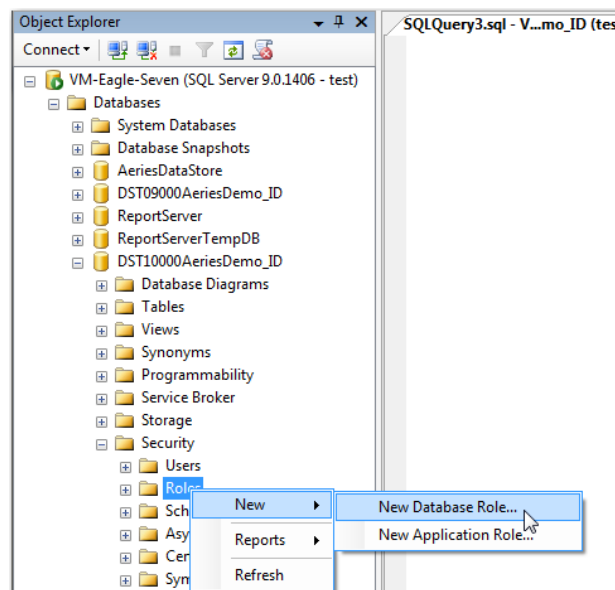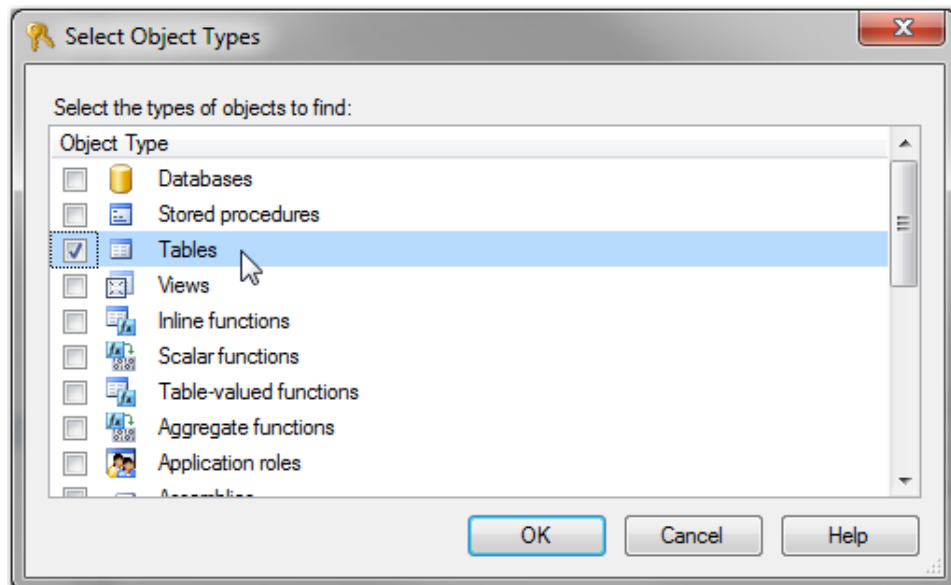
On the **General** page type in the new role name and dbo as the owner.
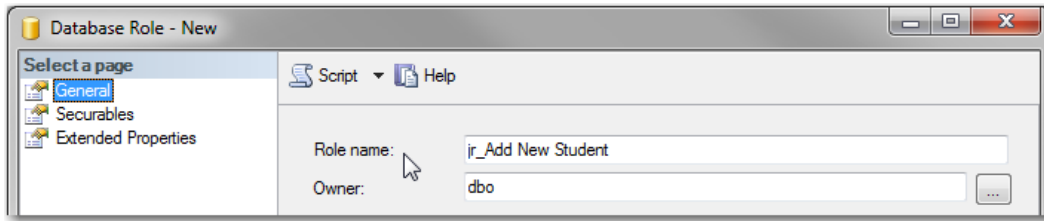
Click on **Securables**, click on **ADD** then select All objects of the types. Click on **OK**.

Select **Tables** and click on **OK** to view all tables within the database.

Hi-light a table by clicking on it within the **Securables** window. The Explicit permissions frame will show you the permissions associated with the table you selected. Aeries uses **SELECT**, **INSERT**, **UPDATE** and **DELETE**. Check mark the appropriate permission under **GRANT**. DENY permissions will be discussed later in this documentation.
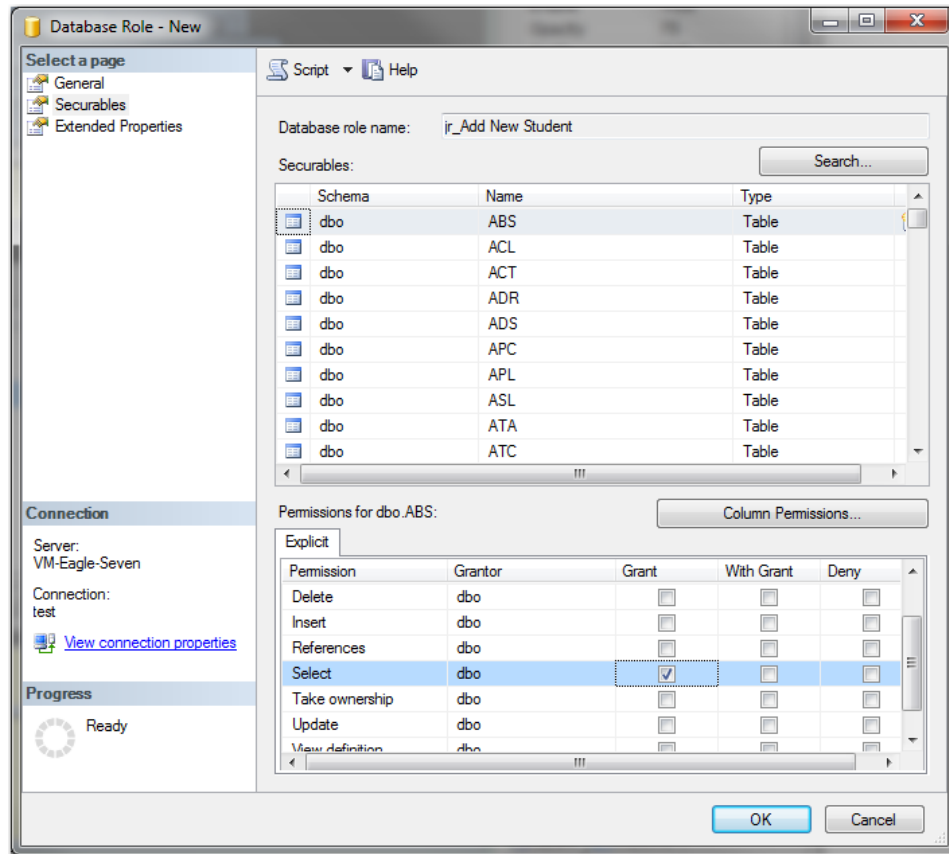
After the permissions have been setup the additional **Role Members** can be added. For example, Aeries Users, which are assigned to **ALL** roles. Aeries Support team can supply sample SQL Scripts to create your Roles, groups or job duty tasks.

ADDING ROLE MEMBERS

Setup SQL Accounts for Aeries administrators and **CHANGE** the password for the 'sa' account. All users will be added to Security whether they access using the preferred method of SQL Authentication or by Windows Authentication. SQL Authentication adds a second layer of security. Windows Authentication is more complex and requies district Network Administrative assistance.

Add a user by navigating to **Security**, **Logins**. Left click on **Logins** to high-light. Right click on **Logins** or anywhere on the Summary tab located on the right side of the Management Studio window. Left click on **New Login**.
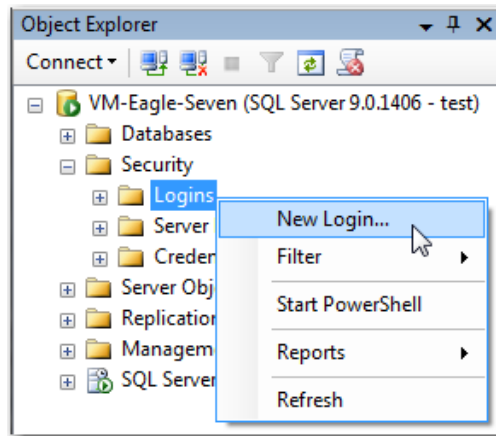
On the **Login – New**, select the **General** page. Type the SQL administrator login name. Select **SQL Server authentication**. Give the SQL administrator account a secure password. Be aware that SQL 2005/2008 passwords are case sensitive. Uncheck **Enforce password policy**.
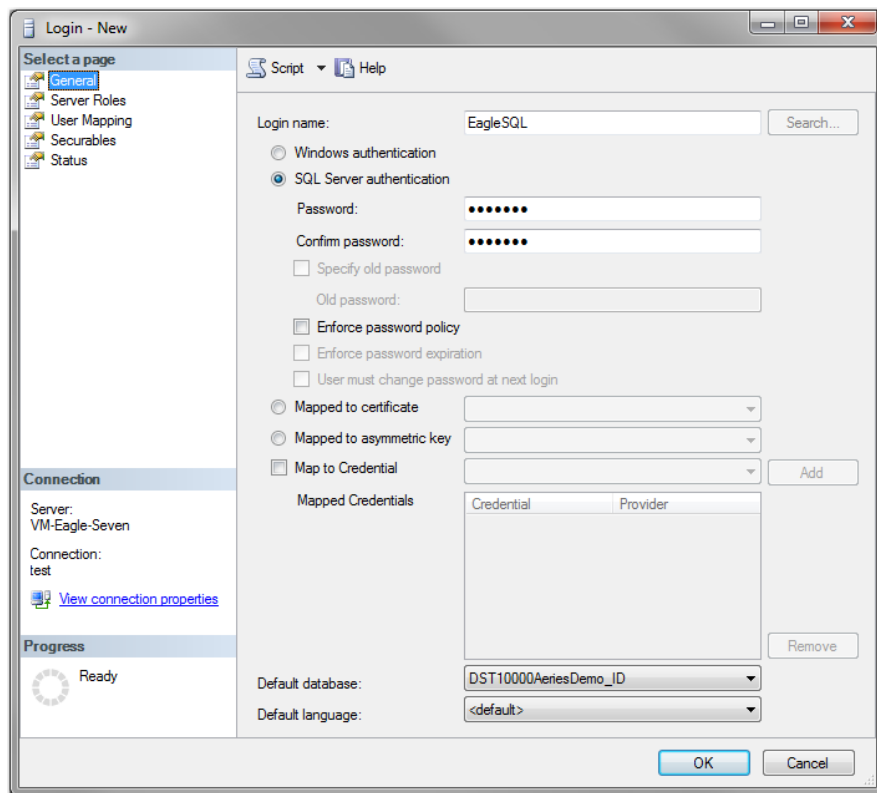
Click on the **Server Roles** page. Give your administrator account
permissions to all server roles. Regular users will not belong to any of these
server role functions.
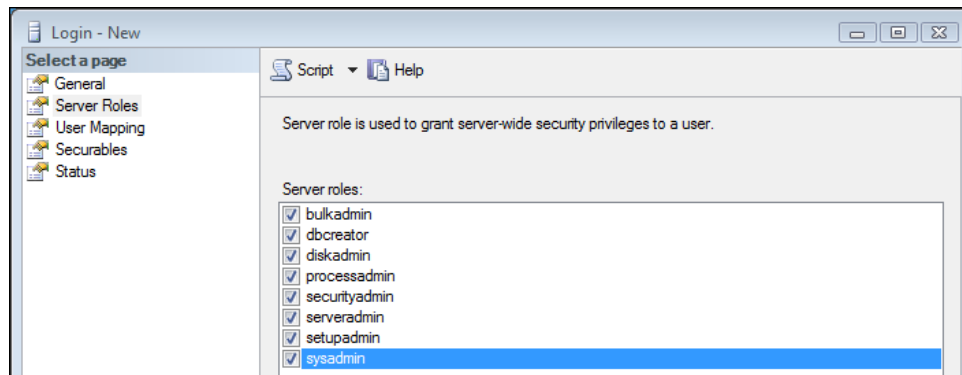
Click on the User Mapping page. Highlight the Master database. Select
db_owner. In the example below a database has been created with roles.
ALL SQL administrator accounts will belong to db_owner, and Aeries Admin
roles including the roles of public and Aeries User which **ALL** users will
belong. Click OK to complete the creation of administrative user account.
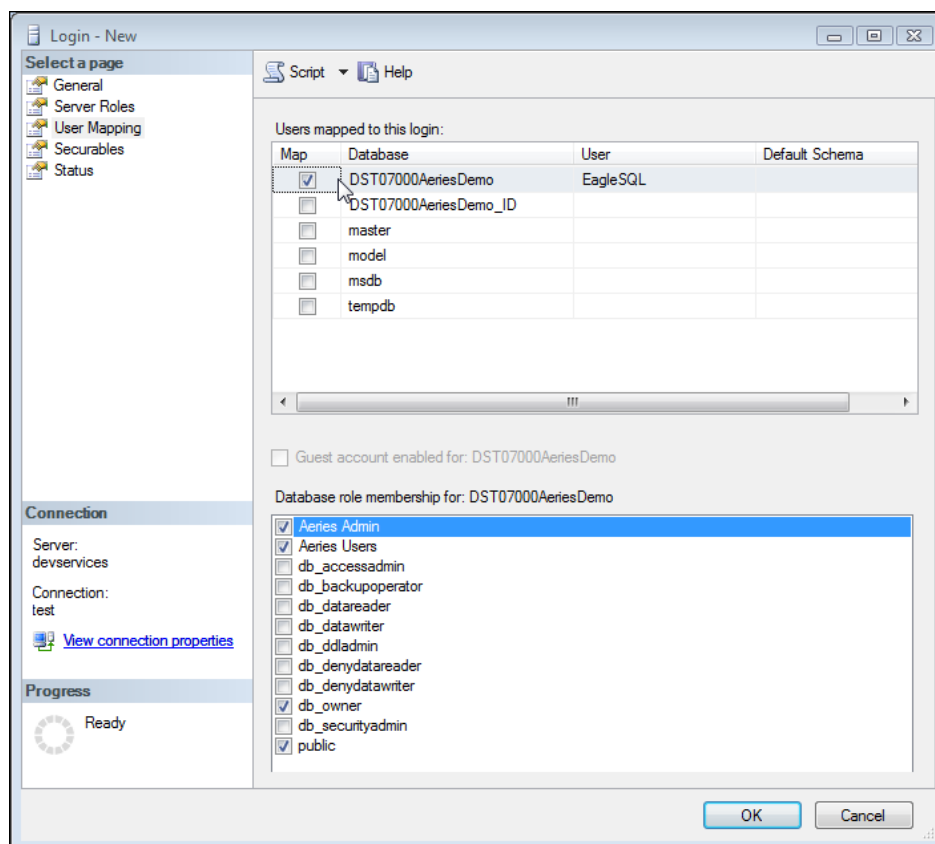
FIELD LEVEL PERMISSION

Administrators of Aeries SQL Databases have full discretion to implement security of the database. But sometimes in order to achieve the desired permissions in Aeries for groups of users, the obvious table level permissions are not enough.

Sometimes field/column level permissions are needed. The Administrator **must** have full understanding on how various permissions will affect the users and their access to the Aeries programs.

ADDING FIELD LEVEL PERMISSION

Below are detailed steps in adding Field Level Security to a Role that has already been setup.

The example used below in adding Field Level Security is for a Counselor that must be allowed to modify a student's class schedule but not overload the class. Field level security must be added to certain fields in the MST table to give the Counselor certain field level permissions.

From the Management Studio click the mouse on Roles and all roles setup will display on the right hand side. Double-click the mouse on the Role to be updated, such as, Counselor.
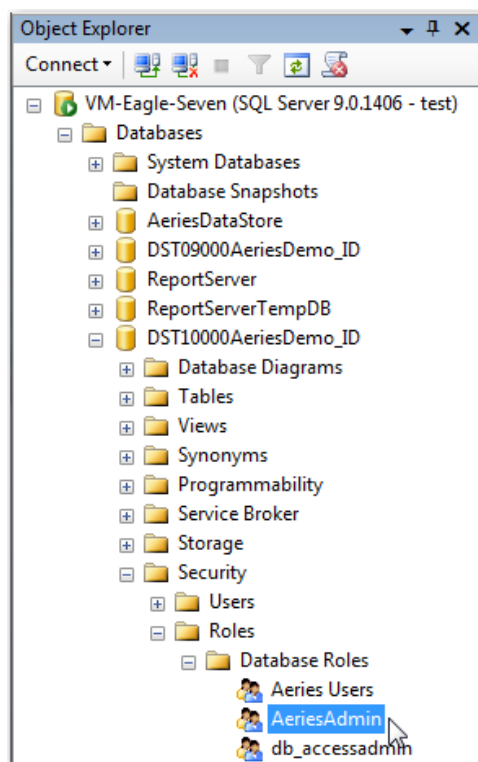
Locate and click on the MST table under **Securables** where **Field Level Permissions** will be added. Under Explicit permissions for dbo MST: click **UPDATE** permission to hi-light. Click the mouse on **Columns Permissions**.
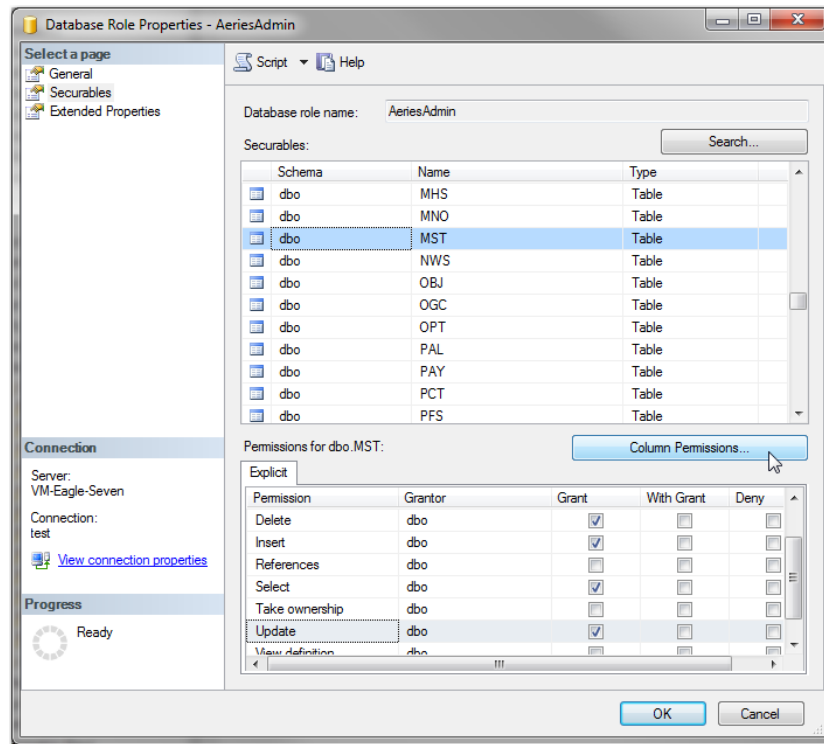
The **Column Permissions** will display. Locate the fields or **Columns** that additional permissions will be added to. Click the mouse on **UPDATE** for the **Column** selected. Ensure you include permissions to the Primary_Key fields and the DTS field. For example, adding update to the **TB**, **TG**, and **TS** fields will now give the Counselor Role the ability to modify a student's class schedule but not overload the class.
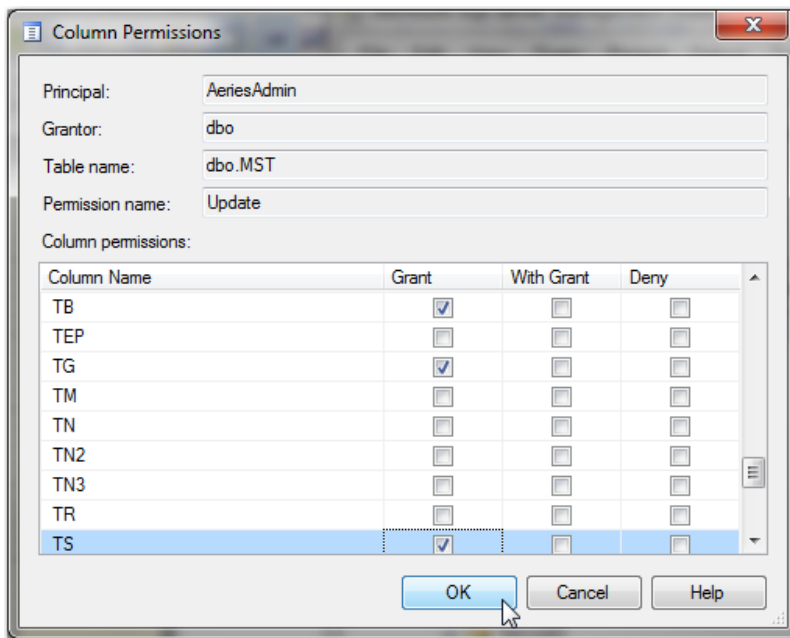
FIELD LEVEL PERMISSION EXAMPLES	The following are examples for adding Field Level Security and what they will accomplish.

FIELD LEVEL PERMISSION FOR NEW TABLES	Anytime a new Student related table is added to Aeries, users must be given certain permission in order to view that data on the related form and also granted certain permissions to transfer students.

When a new table is added to Aeries it is usually released prior to the new form in order to give Districts time to setup permissions to it well in advanced of implementing the version that will use the new table.

The permissions needed for a new ID based table, such as the FRE table are no different than any other ID-Based table, like the CSE, LAC or any Student related table that your District selects to setup as ID-Based in your database, like TST, HIS, ADS etc.

- If the table is ID-based (related to IDN at the district), then you need only give SELECT permissions to the "PrimaryKey" fields, and Field-level update to the Date Time Stamp (DTS) field. This allows your Registrars to transfer records from one school to another without the ability to view the data on the related form. This logic is the standard in Aeries and applies to prior years and new Id-Based tables.

- If the table is SN-based (related to STU at the district), then you need SELECT and INSERT rights to "transfer" any existing records. .

Specific tables are setup as ID-based specifically so you do **NOT** need to give Read (SELECT) permissions to the whole table. We are aware of the confidentiality and sensitivity of specific data.

ADDING FIELD LEVEL PERMISSION FOR ID BASED TABLE	*The example used below in adding Field Level Security is for an ID Based table and is for a Registrar or Secretary at an Elementary School that must be able to add or transfer a student **without** being able to view the records.*

Field/Column – Level Permissions:

FRE.ID – SELECT
FRE.SQ – SELECT
FRE.DTS – UPDATE

MODIFY STUDENT CLASS SCHEDULES	**Table Permissions:** **SEC – UPDATE, INSERT, DELETE** **CAR – UPDATE, INSERT, DELETE** **Field/Column – Level Permissions:** **MST.TS – UPDATE** **MST.TB – UPDATE** **MST.TG – UPDATE** **NOTE:** Full rights given to the MST table will allow a user, such as a counselor to overload sections. To allow the user to still make schedule changes but not overload sections, the above minimum permissions should be given.
MODIFY STUDENT FIELDS (ONLY READ PERMISSION TO STU)	The following examples are for various users that only have READ permission to the STU table but have UPDATE permission to other tables, such as, the MED or LAC table. A field may display on a form that they need to update but the data is stored in the STU table. **Table Permissions:** **STU – READ Only** **Field/Column – Level Permissions :** **STU.CID - UPDATE** *Create CSIS Data Files - Update STU.CID button **STU.CCG - UPDATE** *Citizenship GPA – Re-compute HIS (CCG) button **STU.GCG - UPDATE** *Citizenship GPA - Recompute GRD (GCG) button **STU.LF – UPDATE** **STU.HL - UPDATE** *Language Assessment Data form – Update Home Language (HL), Language Fluency (LF) **STU.HP - UPDATE** **STU.BCY - UPDATE** **STU.BST - UPDATE** **STU.BCU - UPDATE** *Medical form - Health Problems (HP), Birth City (BCY), State (BST), Country (BCU) **STU.CU - UPDATE** *Elementary Classes - "Input" and Move(All/Grade/Tagged) buttons

STU.NT - UPDATE
*Elem...for Next Year - "Input" and Move(All/Grade/Tagged) buttons

STU.SEM - UPDATE
STU.PEM - UPDATE
*Emergency Contacts - Student Email (SEM), Parent Email (PEM)

STU.BM - UPDATE
*Photograph Setup - "Update" button
STU.BM - UPDATE
STU.HC - UPDATE
STU.EY - UPDATE
STU.HT - UPDATE
STU.WT - UPDATE
*ID Card Setup&Print - Photo (BM), Hair (HC), Eye (EY), Height (HT), Weight (WT)
STU.FK - UPDATE
*Siblings - "Renumber" button

STU.SQ – UPDATE
*Running Scheduling Course Request/Selection Scanner Sheets Student numbers exceed 9999

Table Permissions:

STU – READ Only

STU.PT – UPDATE
*Master/Scheduling Master Schedule "Move" option
*Student Class Schedules – Upon Add/Delete/Change of Class (to print change locator)
*Student Enrollment Form – Add/Delete/Change of Class or Reschedule (to print change locator)

STU.RN – UPDATE
*Schedule All Students into Classes (From Scheduling Cycle) – option to schedule random
Field level permissions can be added using a SQL script like the following sample for STU records related to the Medical Form:

```
GRANT UPDATE (SC,SN,DTS,HP,BCY,BST,BCU) TO STU ON [ROLE OR
GROUP NAME]
```

NEGATIVE FIELD LEVEL SECURITY (DENY PERMISSIONS)

AeriesCS will support negative field-level permissions to be established for individuals or groups of individuals. Previously only affirmative field-level permissions on specific fields were supported. This continues to be the case for affirmative field-level permissions and these fields are listed under Field Level Permissions. Support for negative field-level permissions is only for UPDATE permission. Specific negative READ permissions are NOT supported.

To understand how to properly secure Aeries you must understand how the AeriesCS security model works. This entire process assumes that the SQL System Administrator has already established security permissions for various tables inside the AeriesCS SQL database. Every time AeriesCS is opened, AeriesCS reads those permissions through a series of T-SQL queries specifically addressing each table inside the AeriesCS database.

As permissions for each table are retrieved from the SQL Server the equivalent set of permissions are established on the local AeriesCS Access Cache Database. This allows the forms inside of AeriesCS to automatically detect the local Access permissions set on the cache database and can lock the tables and forms accordingly. This process works well until we get into security features of SQL Server that MS Access does not support like field-level permissions. In order to support field-level permissions, AeriesCS makes a few assumptions with the security permissions.

When a SQL user is granted full UPDATE permissions to a table, SQL reports the current SQL user's permissions as "UPDATE ALL". But, if a single field cannot be updated because of the system administrator establishing field level restrictions, SQL Server reports the current user's permissions as "UPDATE SOME".

In a parallel situation, when a user does NOT have UPDATE permissions to a table but specific field-level UPDATE permissions have been established for a select set of fields, SQL reports the permissions as "UPDATE SOME".

This makes it difficult for AeriesCS to establish whether or not the SQL Administrator intended the user to be able to change the entire record EXCEPT a few fields, or able to change ONLY a select set of fields.

The correct answer is important because it translates into specific table-level permissions being established in the AeriesCS Access cache database. AeriesCS determines the difference between the 2 types of "UPDATE SOME" permissions by using a secondary check on the fields that make up the Primary Key in the table. If the current SQL user has permission to change EVERY field that makes up the Primary Key, it is assumed that the user has permissions to the table and only a few fields are restricted. UPDATE permissions are then established on the local cache database. If the user does not, it is assumed they have been granted affirmative permissions and will lock the table in the local cache and rely on specific code in AeriesCS to override those permissions.

Support for negative field-level permissions is done when each form opens by dynamically locking the particular fields that a user does not have permission to change. The record is updatable but the fields the user does not have change permissions to are locked and cannot be changed.

This does have some quirks. If a particular form that allows updating of a table and field that has had specific negative UPDATE permissions set for a field has not been modified to support field level security, changing that particular field will result in errors being generated by the system. In that case, it will be unclear whether or not the data that was changed was actually saved onto the SQL database.

This situation is most likely to occur through the use of the Aeries Query CHANGE command or through the use of the Aeries Query Change button. It is not anticipated that these features will ever support field-level security, so proper training of your end-users is necessary to avoid any problems or confusion.

NEGATIVE FIELD LEVEL SECURITY EXAMPLE

Create the following Database role called DenySTU. Add the Test user as a member of the role DenySTU group by clicking on ADD then browse to the Test user and click OK.
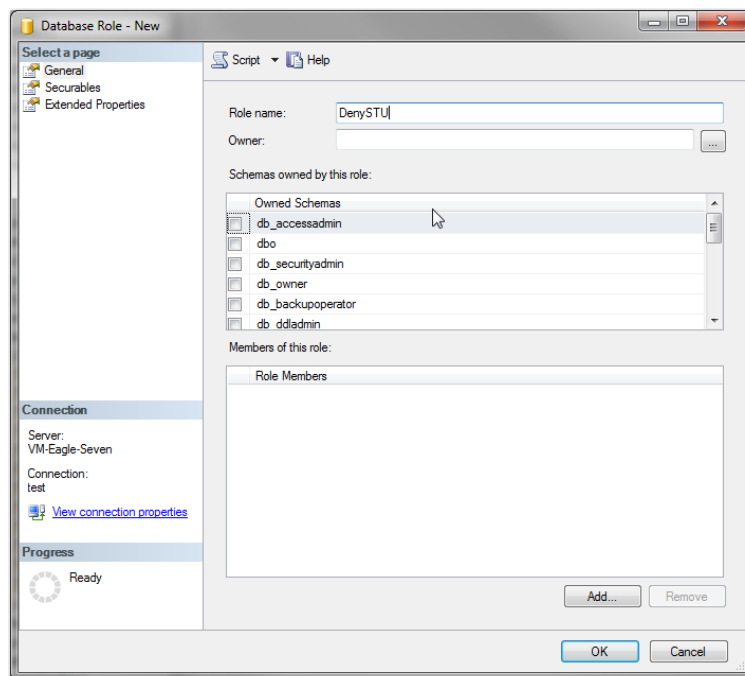
Specific DENY permissions are set on the Test user to the STU.LF and STU.HL fields.
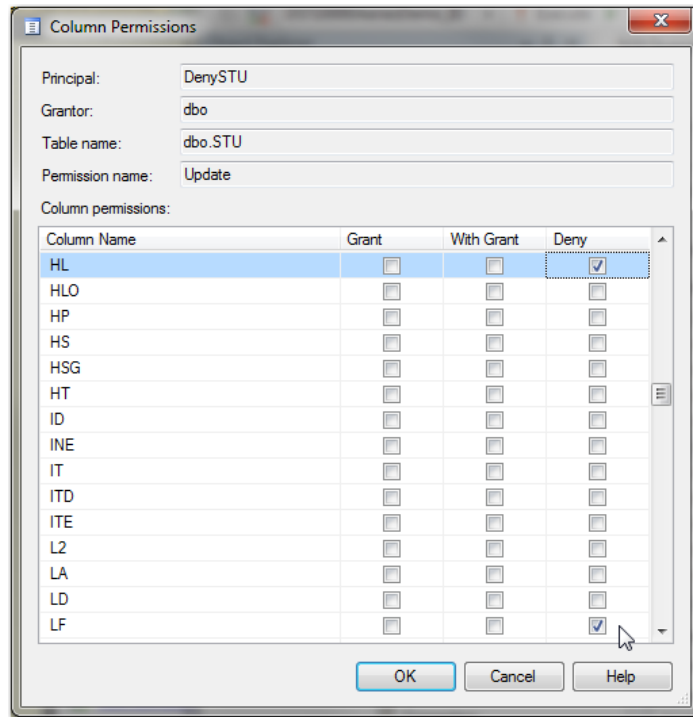
You may create a SQL Script to add DENY permissions to any existing role.

```
DENY UPDATE (LF,HL) ON STU TO [EXISTING ROLE OR GROUP]
```

The **Student Data** form in Aeries will "Grey-Out" the specific fields that the user cannot update. Notice the "HmLng" and "LepFep" fields below. These fields cannot be updated through AeriesCS for the Test user.

RECOMMENDED SQL DATABASE MAINTENANCE PROCESSES

There are many different processes available to keep SQL databases in an "optimum performance" status. These processes are part of the Microsoft SQL Server program and complete documentation is available on the Microsoft SQL Server website and Microsoft Press. Listed below are a few that keep Aeries databases in peak performance status.

MAINTENANCE PLANS

Maintenance plans should be the MINIMUM level of backup and routine maintenance expended on Aeries databases. Maintenance plans give the opportunity to schedule routine Shrinking, Re-indexing, and Performing Incremental Database Back Ups on a regular basis.

The suggested plans for you to consider are an Hourly maintenance plan that backs up the current year's database on an hourly basis during the regular school operating time, and a Daily maintenance plan that will completely backup the current year's database and create a "Set" of backup files that can be used to restore data to a specified "Point In Time" status. These files can be then offloaded to a location that can be backed up to a removable media drive, such as a tape drive/library or a SAN setup.

Additionally, a Maintenance plan that performs a periodic "full" backup of non current year databases should also be setup. These periodic and incremental backup sets will prove invaluable not only in the event of a catastrophic failure, but also for the common deletion mistakes that are made by district staff, such as removal of a current schedule or replacement of student data such as Free and Reduced status and Program participation records.

DOWNLOADING AN APPLICATION OF MICROSOFT SQL SERVER UPDATES AND SERVICE PACKS

Microsoft releases updates and service packs on an unscheduled periodic basis. These updates and service packs enhance the server performance, as well as apply repaired code for anomalies that are produced by Microsoft SQL Server. The scheduled checking, evaluation and application of updates and service packs from Microsoft will ensure that the Microsoft SQL Server is running at peak performance, which will help to ensure peak performance for AeriesCS.

INDEX MANAGEMENT

Index management on the Aeries' SQL databases is very important to maximize performance and to aid in "dropped connection" related issues. The SQL Query script below will assist in the Index Management process by identifying potential candidates for Index Management:

DBCC SHOWCONTIG WITH ALL_INDEXES.

Any table with a "Pages Scanned" greater than 8 should adhere to the following guidelines:

1. **Scan Density** should be as close to 100% as possible
2. **Logical Scan Fragmentation** should be within the range of 0% and 10%
3. **Extent Scan Fragmentation** should have a value as close to 0% as possible
4. **Average Page Density** should be as close to 100% as possible

Any values conflicting with the 4 guidelines mentioned above will most likely cause "connection timeout" issues. A good guide to resolutions for correcting index fragmentation is available via the internet at the following website:

http://www.sql-server-performance.com/rd_index_fragmentation.asp.

The DBCC script process above should be done regularly (once a month for most large districts, 4-5 times per year for small districts) in order to maintain optimum system performance.

Aeries tables that you should pay special attention to are:
IDN, STU, SUP, ENR, ATT, CAR, SEC, CRS, MST, TCH, TST, HIS, GRD, GBK, GBU, GBA, GBS, GBE, GBO, GTG, GBT

| **IMPORT/EXPORT DATA – SQL 2005/2008** | A useful tool provided with **Microsoft SQL Server – Import/Export Data** can be utilized to export, import, restore, and transfer data from within Microsoft SQL Management Studio. Transactions are performed by creating a "packet" that is a script created. |
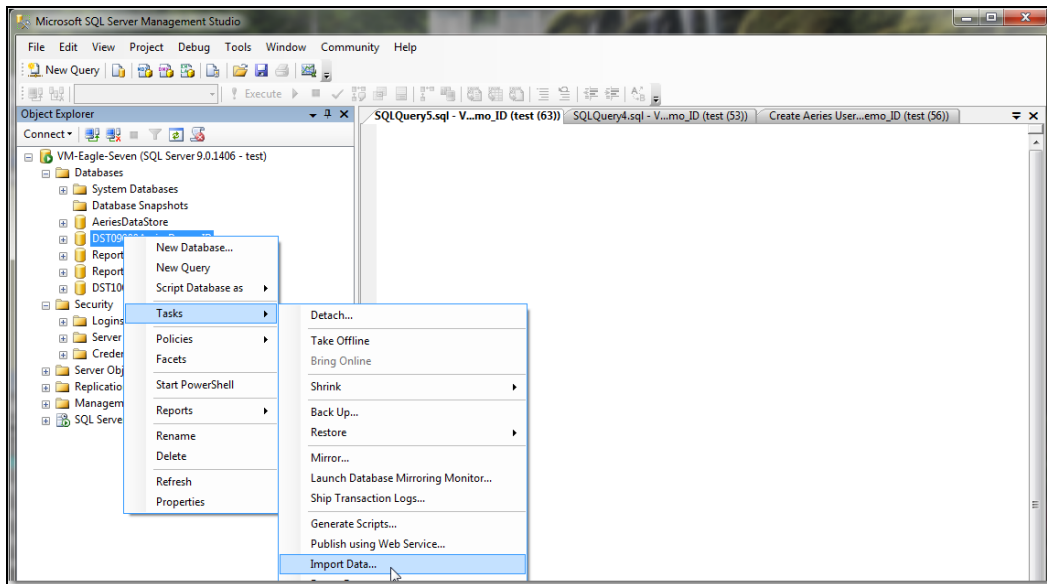
The **SQL Server Import/Export Wizard** box will display. Click the mouse on **Next**.
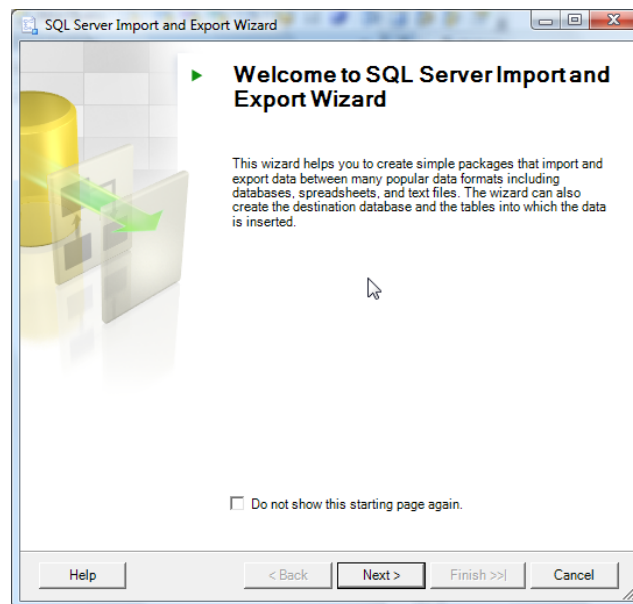
You will be prompted to **Choose a Source Data**. The source can be several file types: SQL database, MS Access database, MS Excel spreadsheet, or Text file. Additional parameters will be required if an Aeries data file is used (system.mdw credentials).

Select the server to copy data to, use your SQL Server Authentication administrative user account and select the source from which to copy data. Click on **Next**.


The next dialog prompts to **Choose a Destination** for the "packaged" data. The normal for importing will be SQL database. Select the appropriate SQL Server name, use SQL Server Authentication administrative user account, and the database you are copying data to. Click on **Next**.

The next dialog box prompts to **Specify the Table Copy or Query**.
Select the **Copy Tables and View** option and review the graphic that
depicts the data flow. Click the mouse on **Next**.
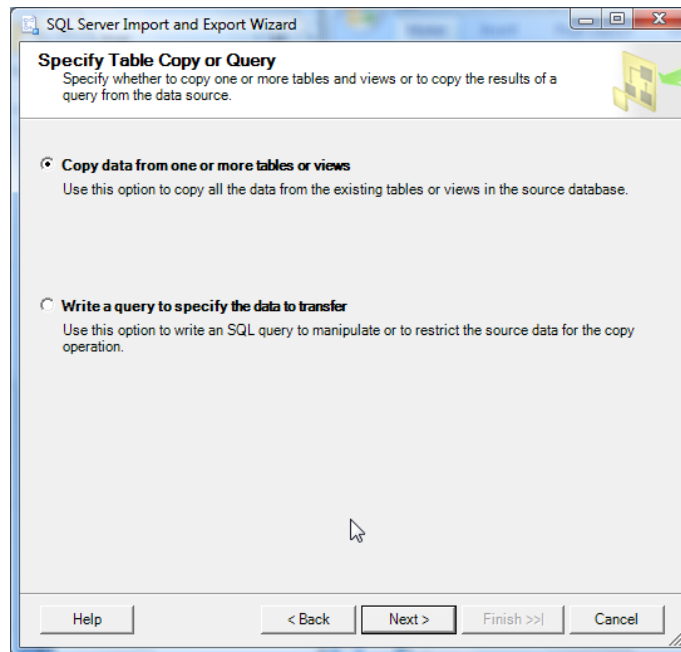
The following dialog box displays all of tables in the source and destination
files. It is important to rename any destination differently than the actual
table to preserve data integrity. Since the occurrence of duplicate data is
common between source data and data already present in the SQL
database table, it is strongly suggested that the temporary table creation
process be utilized.
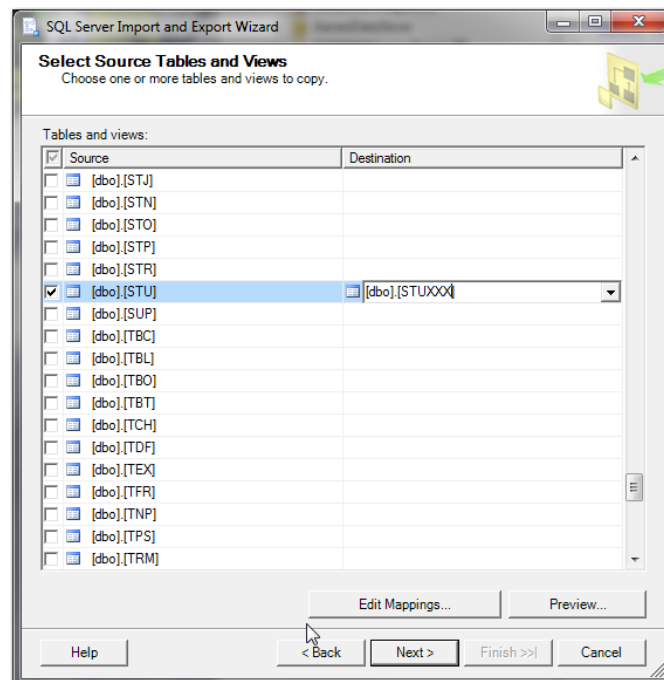
A common naming convention technique is to add additional characters to an existing name (eg CODxxx for COD data imported for eventual insertion into the COD table).

It is also important to choose a temporary naming convention that does not affect Aeries. It is suggested that the temporary table name is at least 6 characters in length so that Aeries will ignore the presence of the temporary table. When finished, click on **Next**.

The next dialog box allows the user to save the Import/Export package for running later, or allows the package to be run immediately. If the package is saved, it can be recalled and run again at any time.
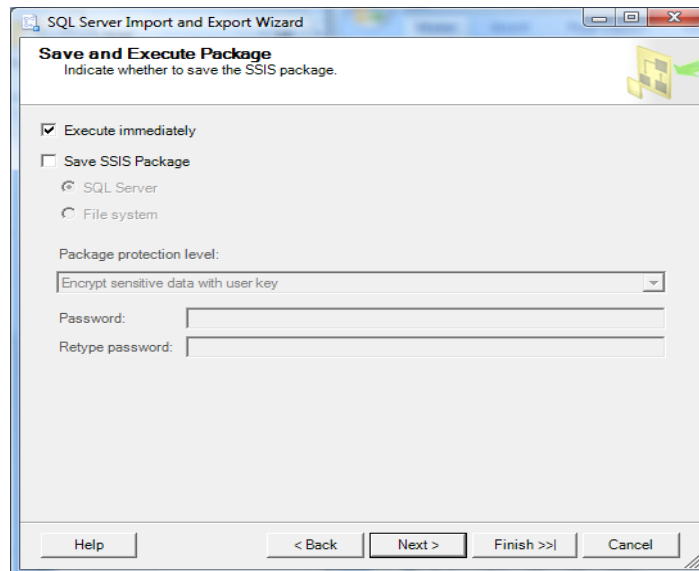
Clicking on **Finish** on the Completion dialog box to either run or save the Import/Export package.
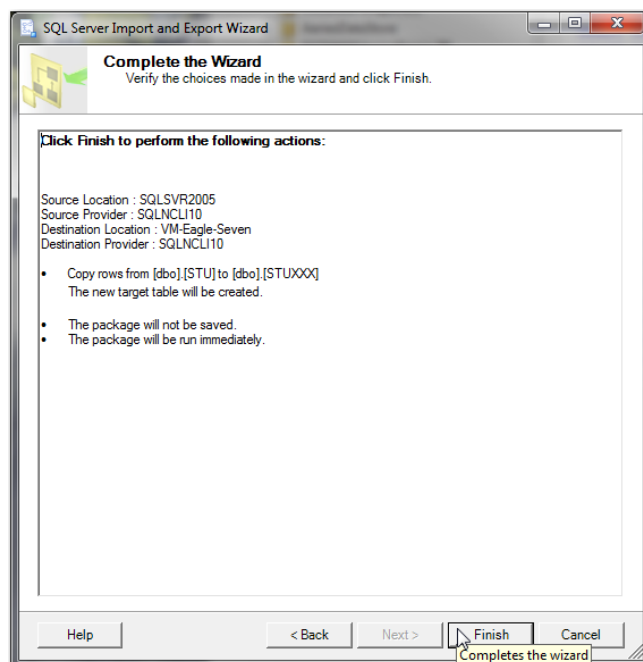
After running the Import/Export package, a dialog box will display showing the progress of the package execution. This will show the creation of the new table and the population of the data. At this point, the data can be imported into an existing Aeries table to complete the import process.
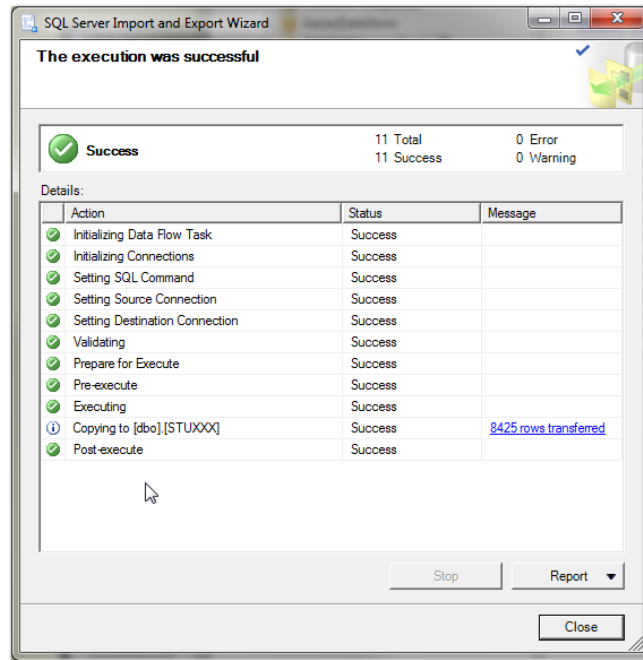
Import/Export is most commonly used to import data into AeriesCS from third party sources, such as Library programs, School Nutrition programs, test scores, and demographic data.

The Import/Export process is an excellent tool to restore data that has been corrupted or deleted without a complete restoration of the database. It is also useful for the creation of listings of Aeries data such as spreadsheets, mailing lists, etc.

For more complete information as to the capabilities and functions of Import/Export, consult the Microsoft SQL server documentation.