

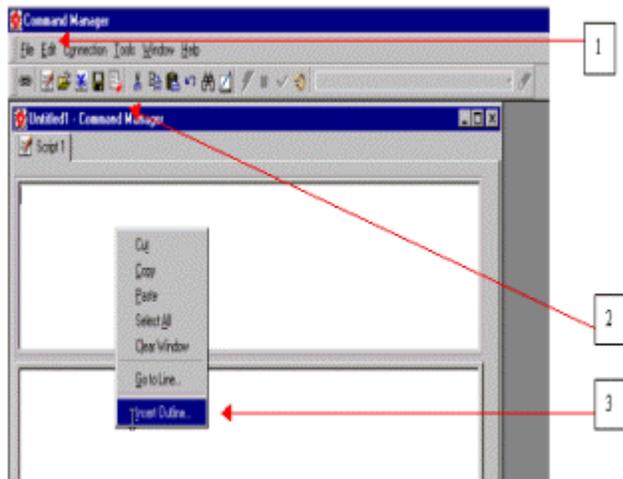
17 Appendix G – MicroStrategy and Informatica References

17.1 How to select, edit, create and run a script using MicroStrategy Command Manager 7.x

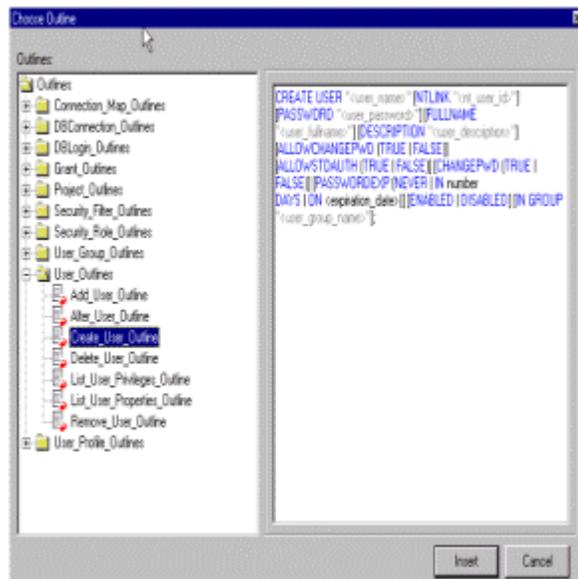
MicroStrategy Command Manager includes a complete set of script outlines. These outlines facilitate the script development by providing the command syntax for the instructions submitted to the Script Executor for object manipulation.

There are three ways to load an outline:

1. Insert option in the Edit menu.
2. Insert Outline icon in the toolbar.
3. Right-click on the Command Manager interface and select the Insert Outline option



All options open the Choose Outline window. This window is divided into two parts:



1. Left Pane: Complete list of all the available outlines divided into functional object groups
2. Right Pane: The template for the outline that is highlighted in the left pane is displayed on the right. Users can click on 'Insert' to modify the script. (Please refer to the list of available outlines below, and in the documentation included with MicroStrategy Command Manager.)

How to edit an outline

When users select and insert one of the outlines available on the 'Choose Outline' window, the template is similar to the following: (Example used is the Create User outline).

```
CREATE USER "<user_name>" [NTLINK "<nt_user_id>"] [PASSWORD "<user_password>"] [FULLNAME "<user_fullname>"] [DESCRIPTION "<user_description>"] [ALLOWCHANGEPWD (TRUE | FALSE)] [ALLOWSTDAUTH (TRUE | FALSE)] [CHANGEPWD (TRUE | FALSE)] [PASSWORDEXP (NEVER | IN number DAYS | ON <expiration_date>)] [ENABLED | DISABLED] [IN GROUP "<user_group_name>"];
```

The user fills in the fields between '<>'. The outline may include more options and commands than user needs, so it is important to manually delete unnecessary fields. Also, the user should manually delete the nesting elements such as '[' and ']' because leaving any of these in the script results in a syntax error.

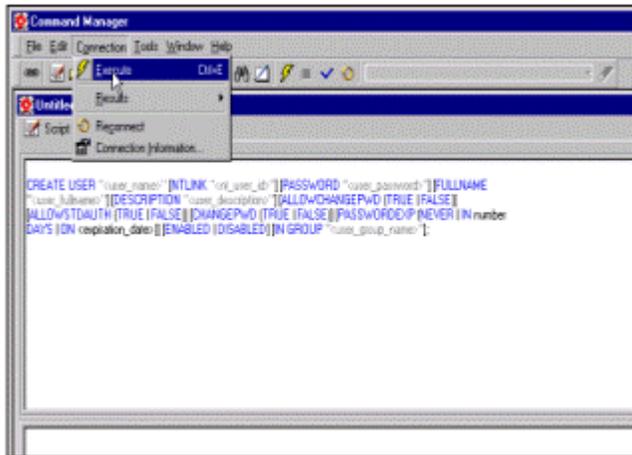
The script above could look similar to the one below using the personalized information and the correct syntax:

```
CREATE USER "Tester" NTLINK "dss_tester" PASSWORD "tester-secret" FULLNAME "Tester Smith" DESCRIPTION "User created for Command manager demo" ALLOWCHANGEPWD TRUE ALLOWSTDAUTH TRUE CHANGEPWD FALSE PASSWORDEXP NEVER ENABLED IN GROUP "administrative users";
```

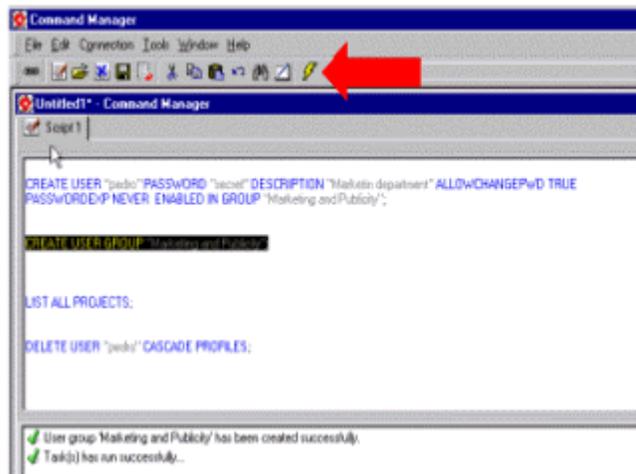
How to run a script

Once the user finishes creating a script, there are two options available to run the script:

1. Choose 'Execute' from the 'Connection' Menu.



2. Click on the Execute button on the toolbar.

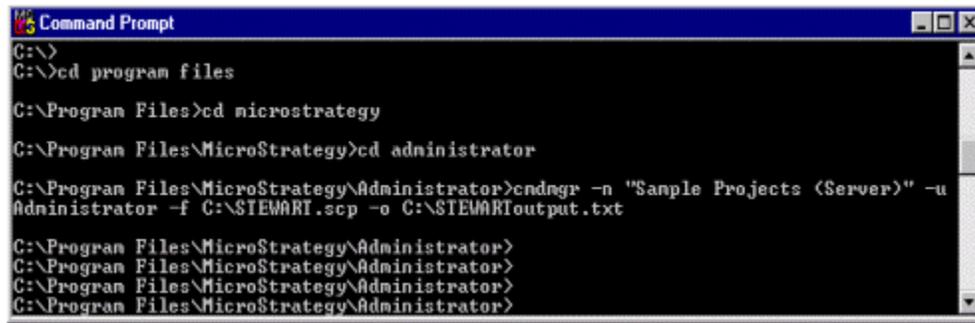


In this example, there are four different scripts ready to run on the dialog box. One will create a user, the other will create a user group, the third one lists all available projects in the project source and the fourth one deletes the user created on the first script.

If administrator uses the available options to run a script only the highlighted script will run. That would be the second one, create user group. Without highlighting a specific, script all the scripts in the window will be run.

Both these options run, by order of appearance, all the available scripts in the dialog box. To run only one script, the user can highlight only that script. MicroStrategy Command Manager also provides the option to create, modify and submit scripts directly from the command line. The syntax for creating and modifying scripts using the command line is as follows:
cmdmgr -n Project_Source_Name -u Username [-p Password] -f Inputfile [-o Outputfile]

(i.e., cmdmgr -n "SampleProjects (Server)" -u Administrator -f C:\Stewart.scp -o C:\STEWARToutput.txt)



```
Command Prompt
C:\>
C:\>cd program files
C:\Program Files>cd microstrategy
C:\Program Files\MicroStrategy>cd administrator
C:\Program Files\MicroStrategy\Administrator>cmdmgr -n "Sample Projects (Server)" -u
Administrator -f C:\STEWART.scp -o C:\STEWARToutput.txt
C:\Program Files\MicroStrategy\Administrator>
C:\Program Files\MicroStrategy\Administrator>
C:\Program Files\MicroStrategy\Administrator>
C:\Program Files\MicroStrategy\Administrator>
```

17.2 Encryption in MicroStrategy 7

What encryption methods are used in MicroStrategy 7?

MicroStrategy 7 employs two main encryption algorithms. These are the Tiny Encryption Algorithm (TEA) and the RACE Integrity Primitives Evaluation MD-160 (RIPEMD-160) fast cryptographic hash function method.

- **Tiny Encryption Algorithm**

The Tiny Encryption Algorithm (TEA) is a cryptographic algorithm that uses operations from orthogonal algebraic groups. It encrypts in a 64-bit block cipher with a 128-bit key length. TEA is very secure; to date, there have been no known successful cryptanalyses of TEA. More information can be found about this algorithm at the Needham and Wheeler's original paper at [Cambridge University Computer Lab](#) or at University of Bradford's [Cryptography & Computer Communications Security Group](#).

- **RIPEMD-160**

RIPEMD-160 is a 160-bit cryptographic fast hash function tuned for 32-bit processors. In general, a hash function is a transformation that takes an input m and returns a fixed-size string, which is called the hash value h (that is, $h = H(m)$). Its primitive operations are: left-rotation (or "left-spin") of words, bitwise Boolean operations (AND, NOT, OR, exclusive-OR) and, two's complement modulo 232 addition of words. RIPEMD-160 was proposed when 128-bit hash functions no longer offered enough security under brute force collision search attacks. More information can be found about RIPEMD-160 at RSA Security's CryptoBytes Technical Newsletter [Volume 3, No. 2 - Autumn 1997](#).

Where are the encryption methods used in MicroStrategy 7?

- **Browser (4-tier mode client) to MicroStrategy Web/Web Server:**

When a user first logs in to a MicroStrategy project in MicroStrategy Web, the browser transmits the user password in clear text by default under standard authentication. A Digital Certificate may be used to validate users and the website. Secure Socket Layer may be used to encrypt this communication. If NT Authentication is used, standard NT validation takes place via NT security. Once the user is logged in, the user password is encrypted using RIPEMD-160 in any subsequent communications between the browser and MicroStrategy Web/Web Server in the same web session.

- **Browser Cookie:**
If the user checked the 'Save Password' option at the MicroStrategy Web login screen, the password is stored in the cookie unencrypted. This option can be removed by checking the 'Display the 'Remember My Password' checkbox on the login page' setting under login settings under Project Preferences in MicroStrategy Web 7.1 and above.
- **Client (3-tier mode client) machines to MicroStrategy Intelligence Server:**
When the user logs into a MicroStrategy project using a 3-tier mode client such as MicroStrategy Agent, MicroStrategy Architect, and/or MicroStrategy Administrator - Object Manager, the user password is encrypted using RIPEMD-160 before transmission to MicroStrategy Intelligence Server.
- **MicroStrategy Web/Web Server to MicroStrategy Intelligence Server:**
From MicroStrategy Web/Web Server to MicroStrategy intelligence Server, the user password is encrypted using RIPEMD-160.
- **MicroStrategy Intelligence Server Server Definition:**
As the MicroStrategy Intelligence Server is a Microsoft Windows NT service, it will need to connect to the Metadata database automatically. The metadata password is stored in the local machine's registry and is encrypted via TEA.
- **Client machines Project Source Definition:**
When client machines (e.g., MicroStrategy Agent, MicroStrategy Architect, and/or MicroStrategy Administrator - Object Manager) connect using Direct connections to MicroStrategy project (i.e., not through MicroStrategy Intelligence Server), the metadata password is stored in the local machine's registry. This is encrypted via TEA.
- **MicroStrategy project DBLogin:**
In order to connect to the Warehouse database on behalf on the MicroStrategy 7 user, the warehouse database password is stored in the DBLogin object in the MicroStrategy metadata. This password is stored encrypted via TEA.

17.3 Encryption in MicroStrategy 7

System Requirements:

Web Server Hardware:

Requirement	Minimum Recommended
-------------	---------------------

Server	PC-compatible
Processor	300 MHz Pentium or equivalent
RAM	256 MB
Available hard drive space	2 GB (100 MB for product with common files)

NOTE: Please contact MicroStrategy for hardware recommendations for larger numbers of concurrent users.

Web Server Software Requirements:

- Microsoft Workstation, Windows NT Server 4.0 (Service Pack 6, or higher), Windows 2000 Server or Windows 2000 Advanced Server
- Microsoft Internet Information Server 4.0 or Microsoft Internet Information Server 5.0
- Microsoft Internet Explorer 5.0 SP1 (or later)

Web Server Open Database Connectivity (ODBC):

- None required!

Web Client Hardware:

Requirement	Minimum for Pure HTML Interface
Processor	486 or higher
RAM	16 MB

Web Client Software:

- At a minimum, browser must support HTML tables and cookies.
- Recommended browsers that include CSS support.
- Recommended resolution for the browser monitor is 800 x 600 or higher with 256 color palette minimum.
- Excel 97 and Excel 2000 with SR1 or SR1a are supported for exporting to Excel feature.
- Any spreadsheet application that supports CSV file type can be used as an export alternative.

For more information on certified and supported browser configurations, please refer to the Certified and Supported Configurations section.

MicroStrategy Environment:

Before you attempt to run MicroStrategy Web 7.1.5 you need to set up your MicroStrategy Environment. This includes:

- Web server configured and running.

- Web client browser installed and running.
- MicroStrategy 7 (or later) project running in a three-tier environment.

Compatibility and Interoperability:

For the complete MicroStrategy 7 Platform Compatibility and Interoperability specification, please see the MicroStrategy 7 General Information - Readme. To obtain the latest information, please contact MicroStrategy Technical Support.

Installation Procedure:

To Install MicroStrategy Web:

NOTE: Refer to the Installation and Configuration Guide, chapter 2, for full details on this and other installation options (such as silent installs, response files, Systems Management Server (SMS) environments).

1. Insert the MicroStrategy 7 Disk 1 and wait a few moments as the MicroStrategy Platform Explorer automatically appears. If the MicroStrategy Platform Explorer does not appear, run Setup.exe from the Disk 1 MicroStrategy7Installation\QueryReportingAnalysis directory.
2. By default, the application files for new installations are installed in C:\Program Files\MicroStrategy\Web.
3. When installing MicroStrategy Web 7.1.5 over earlier versions, the application files will always be installed in the directory in which the previous version of Web was installed. If you choose to install MicroStrategy 7.1.5 in the same folder as a previous version, you will be prompted to confirm the action. If you proceed, all files are replaced with the new files.

If you would like to place the new version of MicroStrategy Web elsewhere, you are asked to first uninstall the product, then run the set up program to reinstall the product.

If you are installing the product the first time, and you would like to place it elsewhere (not the default directory) , click the Browse button and specify a path. To install on a shared drive, begin with the drive letter (for example, F:).

Verify that you have sufficient disk space to perform the installation. This is indicated at the bottom of the Select Components window (note that the total space required is the addition of the space required for the installation of the product specific files and the common files required by the MicroStrategy 7 product suite). If you do not have sufficient space, cancel the installation, move or delete some files from the drive to free up enough space for installation, then begin again.

4. Installation detects the version of MicroStrategy Web 7 you are currently running on the machine, and a confirmation is requested from you in order to overwrite the previous files. After confirming your actions by clicking Yes, all files in the previous directory will be replaced with the new files.
5. Installation stops Internet Information Service for you during installation, in case it is still running. Click Yes to confirm the action.
6. With Setup Program Folder, you can create a new program group or you can choose to overwrite the existing one. The default program group for new installations is MicroStrategy7. Click Next to proceed.

7. After verifying the installation information on Start Copying Files, you can click Next to proceed. At the end of the process, you are prompted whether you wish to view the ReadMe files.
8. When the installation procedure is complete, you are prompted to reboot your machine to run MicroStrategy Web properly. (If you need to reboot your machine, please remember to log in as a user with administrative privileges.)

If you encounter problems during the installation procedure, please refer to the Release Notes or contact MicroStrategy Technical Support.

Directory Structure:

The default directory structure after an installation with no previous Web versions installed is shown in the table below.

NOTE: Web is the default folder. If installing over previous versions of Web, the folder remains the same:

Directory	Contents
\WEB\	Root MicroStrategy Web directory and Interface ASP files
\WEB\Admin\	MicroStrategy Web Administrator Directory
\WEB\CustomLib\	MicroStrategy Web Custom Library Files
\WEB\Help\	MicroStrategy Web Online Help Files
\WEB\Images\	MicroStrategy Web Image Files
\WEB\Internationalization\	MicroStrategy Web International Files
\WEB\Logs\	MicroStrategy Web Log Files
\WEB\Style\	MicroStrategy Web CSS Files
\WEB\WebTemp\	MicroStrategy Web Temp Files (necessary for exporting in IE 4.X browsers)

Common files needed to run MicroStrategy 7.1.5 are placed in the C:\PROGRAM FILES\COMMON FILES\MicroStrategy\ directory by default.

To Uninstall MicroStrategy Web:

1. The Installation procedure for MicroStrategy Web 7 automatically stops the web server upon uninstall.
2. Double-click the Add/Remove Programs icon from the Control Panel, select MicroStrategy Web, and then click Add/Remove. MicroStrategy Web 7 is uninstalled.
3. Choose Yes at the end of the uninstallation to delete the MicroStrategy Web 7 virtual directory from IIS.
4. Manually delete all cookies in c:\winnt and files in the MicroStrategy Web folders.

Upgrade Procedure:

To upgrade from a previous version of a MicroStrategy 7 product:

Full installation:

1. Uninstall the previous version. Follow the uninstall instructions.

2. Install MicroStrategy Web 7.1.5. Follow the installation instructions

If you encounter problems during the installation procedure, please contact MicroStrategy Technical Support.

Certified and Supported Configurations:

The combination of a language, operating system for the client and server components, and client applications from other providers, is a configuration.

A certified configuration was tested at MicroStrategy with MicroStrategy 7 products.

Supported configurations include configurations tested at customer or partner sites, older versions of RDBMS's that were certified for previous releases of MicroStrategy software, and other combinations that may not have been tested in the exact combination listed.

The following are certified languages, operating systems, and browsers.

Languages:

Language	Status
English (US)	Certified
German	Certified
Spanish	Certified
French	Certified
Japanese	Certified
Korean	Certified
Italian	Supported
Swedish	Supported
Portuguese (Brazilian)	Supported

For details on the configurations tested in-house by MicroStrategy, please contact MicroStrategy Technical Support.

Client:

Web Client Operating System:

Operating System	Status
Windows 2000 (Professional, Server, Advanced Server)	Certified
Windows 2000 SP1 or Higher (Professional, Server, Advanced Server)	Supported
Windows 98	Certified
Win NT 4.0 Workstation	Certified
Win NT 4.0 Server (SP5 or higher)	Certified
Win NT 4.0 Server (SP4)	Supported
Windows 95	Supported
OS which runs browsers that have HTML Tables, HTML forms, cookies and CSS (e.g. Mac OS)	Supported

Web Client Browser:

Browser	Status
Microsoft Internet Explorer 6.0	Certified
Microsoft Internet Explorer 5.5 SP2	Certified
Microsoft Internet Explorer 5.5 SP1	Certified
Microsoft Internet Explorer 5.5	Certified
Microsoft Internet Explorer 5.01 Sp2	Certified
Microsoft Internet Explorer 5.01 Sp1	Certified
Microsoft Internet Explorer 5.0	Certified
Microsoft Internet Explorer 4.01 SP2	Certified
Microsoft Internet Explorer 4.01 SP1	Supported
Microsoft Internet Explorer 4.01	Supported
Microsoft Internet Explorer 3.02	Supported
Netscape Navigator 6	Supported
Netscape Navigator 4.7x	Certified
Netscape Navigator 4.6x	Certified
Netscape Navigator 4.5x	Certified
Netscape Navigator 4.0x	Certified
Netscape 3.x	Supported
Any browser that supports HTML Tables, forms, cookies and/or CSS	Supported

To obtain the latest information about certified client systems, please contact MicroStrategy Technical Support.

Web Server:

Web Server Operating System:

Operating System	Status
Win NT 4.0 with SP4	Supported
Win NT 4.0 with SP5	Certified
Win NT 4.0 with SP6, SP6a	Certified
Win NT Workstation 4.0	Certified
Windows 2000 Server (and SP1 and SP2)	Certified

Windows 2000 Advanced Server (and SP1 and SP2)	Certified
--	-----------

Internet Explorer version:

Internet Explorer version (msxml.dll)	Status
IE 5.01 (and SPs)	Certified
IE 5.5 (and SPs)	Certified
IE 6 (on Windows 2000 only)	Supported

Web Server Software:

Application	Status
Microsoft Internet Information Server 4.0	Certified
Microsoft Internet Information Server 5.0	Supported

17.4 Informatica Application Level Security

The Informatica Client, Server, and repository offer several layers of security that you can customize for your repository. You can plan and implement security using these features:

- **User groups.** Repository groups for usernames. You can assign users to multiple groups. You can also assign privileges to groups. Every user in a group receives the privileges for that group. You also use groups to handle Owner's Group folder permissions.
- **Repository users.** Username used to access the repository. You can assign privileges to individual usernames. Each user must have a unique repository username to use folder and object locking properly. You must assign each user to at least one user group.
- **Repository privileges.** The ability to perform actions within the repository and to start and stop the Informatica Server. You assign repository privileges to users and groups. Even if you have the repository privilege to perform certain tasks in the repository, you may require permission to perform the task within a given folder.
- **Folder permissions.** The ability to perform tasks within an individual folder. You can grant permissions on three levels: to the folder owner, a group to which the owner belongs, and the rest of the repository users. You can perform some tasks with folder permissions only. Most tasks also require the appropriate repository privileges.
- **User connections.** You can use the Repository Manager to monitor user connections to the repository. You can end connections when necessary, but to avoid repository inconsistencies, you need to determine if the user has an active connection before closing the connection.

- **Locking.** The repository locks repository objects and folders by user. The repository creates five kinds of locks depending on your task: in-use, write-intent, execute, fetch, and save. The Repository Server locks and unlocks all objects in the repository. You can manually release a lock on an object by ending the connection of the user holding the lock. To avoid repository inconsistencies, you need to determine if the owner of the lock is using the object.

17.4.1 User and Group Administration in PowerCenter

The Repository Manager tool handles all of the user and group access and setup for the PowerCenter application. Access to applications and components within the various PowerCenter applications is determined by privileges granted in the Repository Manager. Individual users can be created and granted privileges; however, Informatica recommends setting up groups, adding users to the groups, and granting privileges to the groups. It's further recommended that the groups be created before the users, so group assignment can occur at user-creation time.

The following sections are a summary of the information available in the Repository Security chapter of the Administrator Guide provided with the PowerCenter software. It is recommended that administrators read that chapter for more detailed information.

17.4.2 Creating a Group in PowerCenter

To create a group in PowerCenter:

1. **In the Repository Manager, select the Security->Manage Groups... item.**

The Manage Group window opens, listing all of the currently defined groups.

2. **Click the Add... button**

This brings up the New Group window for naming and describing a new group.

3. **Name the group, and provide a description if desired, then press the OK button to create the new group.**

17.4.3 Creating a User in PowerCenter

To create a user in PowerCenter, follow these steps:

1. **In the Repository Manager, select the Security->Manage Users... item.**

This brings up the Manage Users window which lists the currently defined users.

2. Hit the Add... button to create a new user.

Once the New User window appears, provide the Username, Description (if desired), and Password in the appropriate fields.

3. Confirm the password by repeating it in the Confirm Password field.

If the two are different, a warning window will appear when you click on either the OK button or the Group Membership tab.

4. Once the information has been added in the General tab, click on the Group Membership tab.

The new user will automatically be a member of the Public group, because the user must belong to at least one group.

5. To add a user to a group, click on the name of the user's new group, and press the Add button.

6. To remove them from a group, click on the name of the group the user is leaving, and press the Remove button.

Users must belong to at least one group, so the administrator cannot remove a user from Public without first assigning them to a different group.

7. When the information in both tabs is complete and satisfactory, press the OK button to add the user to the Informatica repository.

17.4.4 Managing Privileges in PowerCenter

After all new users have been created and assigned to groups, the administrator needs to assign privileges to the groups (individual users can also be granted privileges, but as that is not the recommended operating procedure, it will not be documented here).

To create a group in PowerCenter:

1. In the Repository Manager, select the Security->Manage Privileges... item.

The Manage Privileges window opens. The window has a drop-down select box at the top that contains a menu of all of the privileges available within the PowerCenter tools, followed by a block of cells showing what groups and users (differentiated with different icons which map to those used in the Manage Groups and Manager Users components described above) have the currently selected permission.

2. To add a privilege to a group, select the desired privilege and press the Add... button.

The Add Groups and Users window opens. This window will display all of the available groups that do not currently have the selected privilege.

3. Select the group to be granted the privilege and press the Add button.

The group will now appear in the “Grant To:” cells below the listed privilege.

4. Repeat this procedure for any other privileges that need to be granted.

17.4.5 Available PowerCenter Privileges

The following is a complete list of privileges available in PowerCenter version 5.1.2. The descriptions provide a summarized list of functionality that each privilege grants in the various tools and components of the PowerCenter application. More complete and detailed information is available in the Repository Security chapter of the Administrator Guide provided by Informatica.

- Use Designer – This privilege allows users to connect to the repository and configure connection information using the Designer tool.
- Browse Repository – This privilege allows users to connect to the repository, search by keywords, and change the password (only for the current user), all in the Repository Manager.
- Create Sessions and Batches – This privilege grants the ability for users to connect to the repository, and configure database, FTP, and external loader connections, all using the Server Manager tool.
- Session Operator – This privilege grants users the ability to start, stop, view, and monitor sessions and batches, and view log files, session, and performance details in the Server Manager tool. It also grants the ability to start or stop a session or batch using the UNIX pmcmd tool.
- Administer Repository – This privilege gives the user the ability to connect to, create, upgrade, backup, delete, and restore the repository; copy folders into the repository; and manage passwords, users, groups, and privileges, all using the Repository Manager tool.
- Administer Server – This privilege grants a user the ability to register a server with the repository, edit server variable directories, and start or stop a server using the Server Manager tool.
- Super User – This privilege allows the user to perform all tasks across all folders in the repository, including unlocking all locks in the repository. This privilege supersedes all folder-level permissions.

17.5 REPORT AND FUNCTION GROUP ASSOCIATIONS

SAMF

MBR006 REASONABILITY QUARTERLY FORM 2000
MBR007 ACCOUNTS MAINTENENCE FEE EXTRACT
MBR008 LOAN PROCESSING AND ISSUANCE FEE
MBR009 REASONABILITY QTRLY BACKUP F2000
MBR010 REASONABILITY YEARLY FORM 2000
MBR011 REASONABILITY ANNUAL BACKUP F2000
MBR012 FEDERAL RECEIVABLES EXTRACT
MBR016 FORM 2000 GA SUMMARY COMPUTATION

SDATAINT

APR029 LENDER LOAN PORTFOLIO REPORT

SED

APR001 REPORT OF FFEL LOAN DISBURSEMENTS
APR002 AGENCY PORTFOLIO STATUS REPORT
APR003 LENDER PORTFOLIO STATUS REPORT
APR028 LOANS HELD BY LENDER
DER002 DATE ENTERED REPAYMENT BY SCHOOL
DRC010 SCHOOL REPAYMENT INFO LOAN DETAIL
DRC029 ED COHORT DEFAULT RATE HISTORY RPT
EBA005 PEPS SCHOOL VOL AGGREGATE EXTRACT
GAERRS GA LOAN ERROR RATES & TOP 10 ERRORS
GA005A LOAN PROFILE DATA BY SSN
OVP002 SCHOOL OVERPAYMENT REPORT
RCS002 LENDER LOAN CANCELLATION REPORT
SCHER2 ENROLLMENT REPORTING SUMMARY REPORT

SCH01A EXIT COUNSELING BY SSN
SCH01C EXIT COUNSELING BY SCHOOL
SCH07A TRANSFER MONITORING SUMMARY REPORT

§EDCDR

DRC075 ED REPAY HIST SUMMARY RPTS
DRC076 ED CDR PREVIEW SUMMARY RPTS

§EDDEF

DRC030 ED DM COHORT DEFAULT RATE HIST RPT
DRC075 ED REPAY HIST SUMMARY RPTS
DRC076 ED CDR PREVIEW SUMMARY RPTS
DRC080 ED DM SUMMARY REPORTS

§EDDMD

DRC029 ED COHORT DEFAULT RATE HISTORY RPT
DRC030 ED DM COHORT DEFAULT RATE HIST RPT
DRC075 ED REPAY HIST SUMMARY RPTS
DRC076 ED CDR PREVIEW SUMMARY RPTS
DRC080 ED DM SUMMARY REPORTS

§EDFPPS

DRC031 FPPS COHORT DEFAULT RATE HISTORY RPT

§EDNSLBR

APR029 LENDER LOAN PORTFOLIO REPORT

§GADPC

DRC040 GA COHORT DEFAULT RATE HISTORY RPT

SGAINQ

DRC040 GA COHORT DEFAULT RATE HISTORY RPT
GAERR2 GA LOAN ERROR RATES & TOP 10 ERRORS
GA005A LOAN PROFILE DATA BY SSN

SLENDER

DRC045 LENDER COHORT DEFAULT RATE HIST RPT

SNSLDPG

APR029 LENDER LOAN PORTFOLIO REPORT

SSCHDPC

DRC015 SCHOOL REPAYMENT INFO LOAN DETAIL

SSCHFAT

DER001 DATE ENTERED REPAYMENT REPORT
DRC015 SCHOOL REPAYMENT INFO LOAN DETAIL
DRC035 SCHOOL COHORT DEFAULT RATE HIST RPT
FAT001 REQUEST FOR FINANCIAL AID HISTORY
OVP001 SCHOOL OVERPAYMENT REPORT
SCHER1 ENROLLMENT REPORTING SUMMARY REPORT
SCH01A EXIT COUNSELING BY SSN
SCH01B EXIT COUNSELING
SCH07B TRANSFER MONITORING SUMMARY REPORT

SSCHSCR

DRC015 SCHOOL REPAYMENT INFO LOAN DETAIL
DRC035 SCHOOL COHORT DEFAULT RATE HIST RPT