User Manual

MDSEC

Application Security Tool for the IBM i from Midrange Dynamics

Version 7.4

MDSEC - Table of Contents

1 Overview

The MDSEC Application-Security tool provides IT staff a user-friendly means to secure MDCMS and MDXREF, as well as their in-house applications, at a functional and object level. Security administrators then have a simple means to manage user authorities for application functions as well as easy management of IBM i authorization lists and DDM usage.

1.1 Terminology

Application

An application is a collection of functional security codes. MDCMS and MDXREF application codes are automatically opened in MDSEC and contain all security codes for the authorization to MDCMS and MDXREF functions. Application ***md*** contains the default and general authorizations for MDCMS and MDXREF.

Additionally, applications can be created in MDSEC to manage the authorizations to in-house functions.

Code

The application code is a security code that represents a function that requires authorization within MDSEC. Codes for MDCMS and MDXREF are between 0 (general access) and 99. In-house codes for applications used in MDCMS or MDXREF are 100 or higher. Codes for in-house applications are 0 or higher.

In-house codes can also use limits so that a user only has authority when the run-time value being checked against is within the allowed limits.

User Role

A user role is a collection of authorities. When a role is granted authority to 1 or more codes, every user having the role is automatically granted the same authority to those codes.

A user may belong to multiple roles, thus having authority to all codes granted to each role that the user belongs to.

The standard list of User Roles and an overview of their default capabilities is available in Appendix A.

User

A user is a profile that exists on the IBM i system that should have authority to one or more application codes based on role memberships and personally granted authorities.

2 Starting MDSEC

Type the command MDSEC from a command line. If using a suffix for a separate instance of MDSEC, then enter that value in the ENV parameter. For example, MDSEC ENV(XXXX).

MDSEC may also be accessed from the MDCMS Settings Menu option #7.

A user will only be able to view the current settings in MDSEC unless that user has either *SECOFR authority, *SECADM authority or has been granted security privileges within MDSEC.

2.1 MDSEC Menu

The Main menu for MDSEC. If the user does not have administration rights within MDSEC, then the menu will not be displayed and the user will automatically be shown the User listing screen.

```
SCLMENU                        Company Name                              9.03.10
SCRN1                           MDSEC Main Menu                         14:04:57

                   Opt  Description
                    1   User Roles
                    2   Users
                    3   Functional Security Codes
                    4   Authorization Lists
                    5   DDM Security

                    7   Report Generator

                    9   License Key
                   10   System Title




          Selection: __

F3=Exit    F6=Messages    F8=Submitted Jobs    F11=Output    F21=Sys Command
```

Option 1: User Roles
Manages the list of User Roles that have functional access to MDCMS, MDXREF, or in-house applications.

Option 2: Users
Manages the list of user profiles that have functional access to MDCMS, MDXREF, or in-house applications through user roles or personal authorities.

Option 3: Functional Security Codes
Manages the list of functional security codes to be used to secure in-house applications.

Option 4: Authorization Lists
Manages the authorization lists on the system as well as the user rights for users belonging to those lists.

Option 5: DDM Security
Manages the access rights and logging of DDM (Distributed Data Management) transactions.

Option 7: Report Generator
Allows the user to generate a variety of security reports for Users and Roles.

Option 9: License Key
Allows for the update of the MD license key in case the previous key is about to expire or a new MD product license is to be added.

Option 10: System Title
Defines the title to be displayed at the top of most MD product screens. If MDSEC is used in conjunction with MDCMS, this option is not available here and must be changed using MDCMS Settings menu option 11.

3 User Roles

3.1 User Role Listing

Option 1 from MDSEC Menu: all roles that are currently defined within MDSEC.

```
SCCGPD                          Company Name                              9.03.10
SCRN1                         MDSEC User Roles                           18:40:12

                Filter by Desc:_____________________      Appl: ____
Pos: _________            User:__________                 Code: ___

Type options, press Enter.
 A=Authority  U=Users  2=Edit  3=Copy  4=Delete

Opt  Role ID    Description                                        Users
 _   ADMIN      Administrator                                          1
 _   APPROVER   RFP Approver                                         3
 _   MDXREFUSER MDXREF User                                         6
 _   PROGRAMMER Programmer                                         15
 _   REQUESTER  Project Manager                                     2
 _   SALES      Marketing User                                      2




                                                                   Bottom
F3=Exit    F4=Browse    F5=Refresh    F6=Add
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list
Desc	only roles that have matching text anywhere within their description will be listed
Appl/Code	only roles with authorization to the entered application or combination of application/code will be listed
User	Only roles to which the entered user belongs will be listed

Fields

Role ID	A 10-Character value identifying a MDSEC Role
Description	Description of the role
Users	The number of users currently belonging to the role

Options

A user may edit the role list if their profile belongs to User Class *SECOFR or *SECADM or if the MDSEC Edit Auth flag is set to Y for the user.

A	View/Edit the applications and codes that the role is authorized to
U	View/Edit the list of users belonging to the role
2	Edit the description for the role
3	Copy the role to a new role. Optionally copy the authorities and or the user list to the new role.
4	Delete the role from MDSEC

Function Keys:
F3=Exit – Return to previous panel
F4=Browse – Browse a list of available values for a field
F5=Refresh – Refresh the panel
F6=Add – Add a new role to MDSEC. The role ID can be any 10 character value
F12=Exit – Return to previous panel

3.2 MDSEC Applications for Role

Option A=Authority from the MDSEC Role Listing: all Applications for which the role is authorized

```
SCCSCD                          Company Name                              9.03.10
SCRN1                  MDSEC Applications for Role                        18:57:01

Role: ADMIN       Administrator

Pos: ____          Filter by Desc: _____________________________________

Type options, press Enter.
 C=Codes  4=Remove from Role  9=Apply to all MD Apps
                                                              General
Opt  Appl  Description                                        Access
 _   md    MD Product Global Authorization Codes                 Y
 _   MD    MD Product                                            Y
 _   OPER  Operations Libraries                                  Y
 _   WEB   midrangedynamics.com                                  Y

                                                                      Bottom
F3=Exit   F5=Refresh   F6=Add
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list
Desc	only applications that have matching text anywhere within their description will be listed

Fields

Appl	An application defined either in MDCMS/MDXREF or from the Functional Security Codes list
Description	Description of the application
General Access	If general access (code 0) is granted to the application for the role. This allows for turning off authority for the application without removing codes for the application.

Options

A user may only edit the list if they have *SECOFR authority or if the MDSEC Edit Auth flag is set to Y for the user.

C	View/Edit the codes for the selected application that the role is authorized to
4	Remove all authorizations for the application from the role
9	Apply all code authorizations for application md to all MDCMS/MDXREF applications for the role. Option only valid for application md. The use of this option provides a rapid means to have the same authorizations regardless of the Application.

Function Keys:

F3=Exit – Return to previous panel
F5=Refresh – Refresh the panel
F6=Add – Add a new role to MDSEC. The role ID can be any 10 character value
F12=Exit – Return to previous panel

3.3 MDSEC Application Codes for Role

Option C from the MDSEC Role Application Listing: all Application Codes for which the role is authorized

```
SCCSCD                          Company Name                              9.03.10
SCRN2                 MDSEC Application Codes for Role                   19:21:36

Role: ADMIN       Administrator
Appl.: md          MD Product Global Authorization Codes

Pos: ___           Filter by Desc: ____________________________________________

Type options, press Enter.
 4=Remove from Role  9=Apply to all MD Apps
                                                              Application
Opt  Code  Description                                         Specific
 _         General Access                                        Y
 _     1   MDXREF General Product Authorization
 _     2   MDCMS  General Product Authorization
 _     3   Application Group Maintenance
 _     4   Promotion Level Maintenance                           Y
 _     5   Attribute Maintenance                                 Y
 _     6   Attribute Command Maintenance                         Y
 _     7   Object Authority Maintenance                          Y
 _     8   Distribution Queue Maintenance                        Y
                                                                        More...
F3=Exit    F5=Refresh    F6=Add
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list
Desc	only codes that have matching text anywhere within their description will be listed

Fields

Code	An application code defined either in MDCMS/MDXREF or from the Function Security Codes list to define authorization to a specific function
Description	Description of the code
Application Specific	For application md only: Y – Authorization to the MDCMS or MDXREF function will be checked against the corresponding MDCMS/MDXREF at run-time. This allows a role to have authority to one application but not another N – Authorization to the MDCMS or MDXREF function is checked again md and there is no differentiation amongst the applications
Limits	For non-md codes only: N – Limits not used or user is unauthorized for all checked values U – Users in role have unlimited authority to function Y – Users in role have limited authority to values between minimum and maximum

Options

A user may only edit the list if they have *SECOFR authority or if the MDSEC Edit Auth flag is set to Y for the user.

L	View/Edit the limits for a non-md code
4	Remove authorization for the code from the role
9	Apply the code authorization for application md to all MDCMS/MDXREF applications for the role. Option only valid for application ***md***.

Function Keys:
F3=Exit – Return to previous panel
F5=Refresh – Refresh the panel
F6=Add – Add a new role to MDSEC. The role ID can be any 10 character value
F12=Exit – Return to previous panel

3.4 MDSEC Code Limits for Role

Option L from the MDSEC Code Listing: numeric or alphanumeric value limits for an internal function security code

```
SCCSCD                          Company Name                              9.03.10
SCRN3                   MDSEC Code Limits for Role                       19:36:05

Role: ADMIN       Administrator

Appl.: TEST        Test App
Code.: 100         Limit Code


                           Minimum Value              Maximum Value
Numeric Limits  . . . Y    _____________55.000000     _____________60.000000

Alphanumeric Limits . Y    C_____________________     D_____________________


  Valid Limit values:
    N = Limits not used or user is unauthorized for all checked values
    U = User has unlimited authority
    Y = User has limited authority to values between minimum and maximum



Enter=Confirm   F12=Previous
```

Fields

Limits	N – Limits not used or user is unauthorized for all checked values U – Users in role have unlimited authority to function Y – Users in role have limited authority to values between minimum and maximum
Minimum Value	The minimum value allowed for the role at run-time, if the calling program requests that limits are checked. Not applicable for unlimited or non-limited codes
Maximum Value	The maximum value allowed for the role at run-time, if the calling program requests that limits are checked. Not applicable for unlimited or non-limited codes

Function Keys:
Enter=Confirm
F12=Previous

3.5 Users with Role

Option U from the MDSEC Role Listing: all users belonging to the role

```
SCCGPD                          Company Name                              9.03.10
SCRN3                         Users with Role                            19:45:04

Role: APPROVER    Installation Approver

Pos: _________  Filter by Desc: ________________   Ext ID: ________________

Type options, press Enter.
 U=User Auth  4=Remove from Role

Opt  User ID    Description                                    Ext ID
 _   MMORGAN    Michael Morgan                                 michael
 _   SD         Stephan de Diego

                                                                      Bottom
F3=Exit   F5=Refresh   F6=Add
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list
Desc	only users that have matching text anywhere within their description will be listed
Ext ID	only users that have matching text anywhere within their external ID will be listed

Fields

User ID	The system user profile ID for the user
Description	Description of the user
Ext ID	The external ID for the user. This is used for the mapping of LDAP network user ids to the internal system ID

Options

A user may only edit the list if they have *SECOFR authority or if the MDSEC Edit Auth flag is set to Y for the user.

U	View all authorities for the user, based on all roles that the user belongs to
4	Remove the user from the role

Function Keys:

F3=Exit – Return to previous panel
F5=Refresh – Refresh the panel
F6=Add – Add a new role to MDSEC. The role ID can be any 10 character value
F12=Exit – Return to previous panel

4 Users

4.1 User Listing

Option 2 from MDSEC Menu: all users that are currently defined within MDSEC.

```
SCCUPD                          Company Name                              9.03.10
SCRN1                           MDSEC Users                              20:53:24
                Filters:
                  Desc.: _____________________  Appl..: ____  Code: ___
Pos: _________    Role: ________   Role, *USER  Ext ID: _____________

Type options, press Enter.
 G=Roles  U=User Auth  2=Edit  3=Copy  4=Delete  5=Display

Opt User ID    Description                    Role ID     Ext ID     GA Act Sec
 _  BARTECH    Bartech, Roberto Munari        ADMIN     +            N   Y   Y
 _  MMORGAN    Michael Morgan                 *USER     + michael    N   Y   Y
 _  QSO        Secofr 2                       *USER                  Y   Y   N
 _  REN        René Unternährer               ADMIN       unti       N   Y   Y
 _  SD         Stephan de Diego               ADMIN     +            Y   Y   N



                                                                        Bottom
F3=Exit    F4=Browse    F5=Refresh    F6=Add
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list
Desc	only users that have matching text anywhere within their description will be listed
Appl/Code	only users with authorization to the entered application or combination of application/code will be listed
Role	Only users that belong to the entered role will be listed
Ext ID	only users that have matching text anywhere within their External User ID will be listed

Fields

User ID	The user profile of a user
Description	Description of the user
Role ID	The role that the user belongs to. If the user belongs to multiple roles, a + will be displayed
External User ID	The external ID for the user. This is used for the mapping of LDAP network user ids to the internal system ID when logging into MDWorkflow automatically. An IBMi user profile is not required when logging in over LDAP, but will be used if it exists.
Active	If the user profile is active in MDSEC Y – the user is active and the authorizations will be granted N – the user has been disabled within MDSEC and will not have authority to any codes in MDSEC
MDSEC Edit Auth	Edit Authority within MDSEC Y – the user may make changes within MDSEC N – the user is not permitted to make changes within MDSEC
Group Profile	The group profile that the user profile belongs to. This is a read-only parameter If the User ID (first parameter) is a valid user profile, but isn't defined in MDSEC, then that user id will have any authorities that the group profile attached to the user profile has within MDSEC. If the User ID is defined in MDSEC, and is attached to a group profile, then authority will be based on the Use Group Auth parameter
Use Group Auth	If the User Profile of the User ID is attached to a Group ID, the following values are possible: Y – MDSEC Authorities based on Group Profile N – MDSEC Authorities based on User Profile B – MDSEC Authorities based on the combination of the Group Profile and User Profile
CCSID Override	The Coded Character Set to use when communicating with this system using MDOpen or MDWorkflow. This ensures that characters are displayed in the form and order that is expected for the user's locale within those clients. A value is only necessary here if the user requires a different CCSID than the CCSID defined for the system in the MDCMS system settings.
Workflow Password	The password to be used for MDWorkflow users that do not have an IBMi User Profile. This password is to be entered together with the MDSEC User ID at the MDWorkflow login prompt. If the user id exists as an IBMi user profile, then the password for the IBMi profile will be used by MDWorkflow rather than this password.
Password Expired	N – the password is not expired Y – the password is expired. The user will be prompted and required to change the password the next time that they login to MDWorkflow.

Options

A user may edit the user list if their profile belongs to User Class *SECOFR or *SECADM or if the MDSEC Edit Auth flag is set to Y for the user.

R	View/Edit the list of roles that the user belongs to
U	View all authorities for the user, based on all roles that the user belongs to
2	Edit the properties for the user. The authorities for the user are edited using option R
3	Copy the user to a new user. Optionally copy the authorities to the new user.
4	Delete the user from MDSEC
5	Display the User properties

Function Keys:

F3=Exit – Return to previous panel
F4=Browse – Browse a list of valid values for a field
F5=Refresh – Refresh the panel
F6=Add – Add a new user to MDSEC. If the user requires access to MDCMS or MDOpen, then the user must be a valid IBMi user profile. If only MDWorkflow access is necessary, then a User Profile does not have to exist for the ID.
F12=Exit – Return to previous panel

4.2 Roles for User

Option R from the MDSEC User Listing: all roles that the user belongs to

```
SCCGPD                          Company Name                          9.03.10
SCRN3                         Roles for User                         21:04:58

User: MMORGAN     Michael Morgan

Pos: _____________   Filter by Desc: _____________________________

Type options, press Enter.
 A=Authority  4=Remove from Role

Opt  Role       Description
 _   ADMIN      Administrator
 _   APPROVER   Installation Approver


                                                                      Bottom
F3=Exit    F5=Refresh    F6=Add    F9=Add Personal Authorities
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list
Desc	only users that have matching text anywhere within their description will be listed

Fields

Role	A 10-Character value identifying a MDSEC Role
Description	Description of the role

Options

A user may only edit the list if they have *SECOFR authority or *SECADM authority or if the MDSEC Edit Auth flag is set to Y for the user.

A	View/Edit the applications and codes that the role is authorized to
4	Remove the user from the role

Function Keys:

F3=Exit – Return to previous panel
F5=Refresh – Refresh the panel
F6=Add – Add 1 or more Roles for the User
F9=Add Personal Authorities – Add Application and Code authorities for a User. These can be in addition to, or instead of, Role authorities for the User
F12=Exit – Return to previous panel

Adding Personal User Authority

The use of the F9=Add Personal Authorities function key will enable the MDCMS administrator to add, maintain, or remove a user's personal authorities. These authorities are in addition to authorities obtained through membership in other roles.

To grant an individual personal authority to specific codes follow these steps:

1. Go to the MDSEC Main Menu
2. Select Option 2 – Users
3. Take option R=Roles for a selected user
4. Press F9=Add Personal Authorities function key (see NOTE below). On the ***MDSEC Applications for Role*** panel press the ***F6=Add*** function key. On the ***Unauthorized MDSEC Applications*** panel select all Applications that user will require personal authority to and press Enter. That action will result in the Applications selected being returned to the ***MDSEC Application Codes for Role*** panel. Use the F6=Add function key to display the ***Unauthorized MDSEC Codes*** panel and proceed to use option 1=Select one or more Codes for each of the selected Applications. After completing the update and returning to the Roles for User panel the user will have a *USER Role value with a Description of Personal Authorities.
5. Use the A=Authority option from the ***Roles for User*** panel to maintain a user's personal authority

NOTE: If the ***F9=Add Personal Authorities*** function key is not displayed on the ***Roles for User*** panel the user will already have a Role entry of *USER. Once the *USER role is created, it can be maintained using the A=Authority option from within the ***Roles for User*** panel.

5 Functional Security Codes

5.1 Application Listing

Option 3 from MDSEC Menu: all applications to be functionally secured by MDSEC

```
SCCSBM                          Company Name                          9.03.10
SCRN1                       MDSEC Administration                     14:53:40

    Pos: ____

Type options, press Enter.
 2=Edit   3=Copy   4=Delete   5=View

    Opt  Appl  Description                                  Active
     _   md    MD Product Global Authorization Codes         Y
     _   ACCT  Accounting application                        Y
     _   INV   Inventory application                         Y




                                                                  Bottom
F3=Exit   F5=Refresh   F6=Add
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list

Fields

Appl	An application defined either in MDCMS/MDXREF or from this screen
Description	Description of the application
Active	N – Authorizations for all codes for this application have been disabled Y – Authorizations for all codes for this application are enabled

Options

A user may only edit the list if they have *SECOFR authority or *SECADM authority or if the MDSEC Edit Auth flag is set to Y for the user.

2	Edit the properties and codes for the application
3	Copy the Application to a new application and optionally copy the non-md codes to the new application too
4	Remove the Application from MDSEC – only allowed for applications that are not managed by MDCMS or MDXREF
5	View the properties and Codes for the Application

Function Keys:

F3=Exit – Return to previous panel
F5=Refresh – Refresh the panel
F6=Add – Add a new Application to MDSEC that will not be managed by MDCMS or MDXREF
F12=Exit – Return to previous panel

5.2 Application Code Listing

```
SCCSBM                              Company Name                          21.04.05
SCRN2                          Edit Application/Codes                     17:05:09

Appl: ACCT   Desc: Accounting application_____________________________ Active: Y
================================================================================
Pos: ___     Desc filter: _____________________________

Type options, press Enter.
 2=Edit  3=Copy  4=Delete

Opt  Code  Description
 _    31   Insurance values
 _    32   Ledger entries
 _    33   VAT entries
 _    34   Reverse Transactions

                                                                        Bottom
F5=Refresh   F6=Add   F12=Previous
```

Positioning and Filtering List

Pos	the cursor will be positioned to the closest match in the list
Desc	only codes that have matching text anywhere within their description will be listed

Application Fields

Appl	An application defined either in MDCMS/MDXREF or from this screen
Description	Description of the application
Active	N – Authorizations for all codes for this application have been disabled Y – Authorizations for all codes for this application are enabled

Code Fields

Code	A 3 digit number to identify a function to be secured. For applications that are managed by MDCMS or MDXREF, the number will be between 1 and 99 and custom codes for in-house applications must have a value between 100 and 999.
Description	Description of the code

Options

A user may only edit the list if they have *SECOFR authority or *SECADM authority or if the MDSEC Edit Auth flag is set to Y for the user.

2	Edit the code description – only allowed for in-house codes
3	Copy the code to a new code for this application or to a new code in another application
4	Remove the code from MDSEC – only allowed for in-house codes

Function Keys:

F3=Exit – Return to previous panel
F5=Refresh – Refresh the panel
F6=Add – Add a new Code to the Application. The Code must be higher than 99 if the Application is managed by MDCMS or MDXREF
F12=Exit – Return to previous panel

6 Embedding MDSEC into your Applications

In order to check if a user is authorized to a function, program **MDSECAUT** is to be called. It is necessary to have library MDSEC in the library list for every job that contains a program call to MDSECAUT.

6.1 MDSECAUT Parameter Table

Parameter	Usage	Type	Length	Short Description
User ID	Input	String	10	User ID, *USER, blank
Application	Input	String	4	MDSEC Application Code
Code	Input	Number	3	Security Code within Application
Return Code	Output	String	1	0=ok, 1-9=not ok
Check Numeric Value	Input	String	1	Flag for checking numeric limits
Numeric Value	Input	Number	18,6	Value to check against limits
Check Alphanumeric Value	Input	String	1	Flag for checking alphanumeric limits
Alphanumeric Value	Input	String	25	Value to check against limits

6.2 Detailed Description of MDSECAUT Parameters

User ID: Optional value to be passed to indicate which user is to be checked for authorization. If the value is *USER or blank, MDSEC uses the job's user.

Application: The 4-character MDSEC code for the application that the function belongs to.

Code: The 3-digit MDSEC code within the application that designates the function itself.

Return Code: The 1-character return code to tell your application whether or not the user is authorized. The values and their meaning:

0	user is authorized to function
1	user not defined in MDSEC
2	user deactivated
3	application not defined in MDSEC
4	application deactivated
5	code not defined in MDSEC
6	user not authorized
7	numeric value outside limits for user
8	alphanumeric value outside limits for user
9	system failure

Check Numeric Value: A flag specifying if the passed numeric value is to be checked against the authorized limits for the user. Y = check limits, N = do not check limits.

Numeric Value: The value to be checked against the authorized limits for the user.

Check Alphanumeric Value: A flag specifying if the passed alphanumeric value is to be checked against the authorized limits for the user. Y = check limits, N = do not check limits.

Alphanumeric Value: The value to be checked against the authorized limits for the user.

6.3 Programming Examples and Copybooks

Within file QCPYSRC in library MDSEC are coding examples in COBOL, CL, RPG and ILE RPG. The examples are located in separate members all starting with EXAMP.

QCPYSRC in library MDSEC also contains copybooks for the MDSECAUT parameter data structure. Copybooks are available for the languages COBOL, RPG and ILE RPG. The copybooks are located in separate members all starting with MDSEC.

7 MDSEC Report Generator

Option 7 from the MDSEC Main Menu gives the user access to a variety of security reports for Users and Roles.

```
SCCRPT                          Company Name                          11/26/11
SCRN1                     MDSEC Report Generator                      10:07:12


    Report  . . . . . . . . . .  _       1=Role Authority
                                         2=User Authority
                                         3=Users with Role
                                         4=Roles for User




Enter=Confirm    F7=Load Def    F11=View Output
```

Each report is customizable based on the set of criteria available for User and Role authorities to your application's functions and can be run or scheduled using the ***MDRUNRPT*** API.

Function Keys:
F3=Exit – Return to previous panel
Enter=Confirm – Confirm selection with Enter key
F7=Load Def – Load a saved Report Definition
F11=View Output – Work with MD Output
F12=Exit – Return to previous panel

7.1 Role Authority

```
SCCRPT                          Company Name                              11/26/11
SCRN2                       MDSEC Report Generator                        10:07:12

    Report  . . . . . .  1       MDSEC Role Authority

    Include Role/User Desc  .  Y       Y/N
    Include Appl Desc . . . .  N       Y/N
    Include Code Desc . . . .  Y       Y/N
    Sort by Auth Code . . . .  Y       Y/N
    Minimum Limit Info  . . .  X       A=Alpha, N=Numeric, B=Both, X=Exclude
    Maximum Limit Info  . . .  X       A=Alpha, N=Numeric, B=Both, X=Exclude

    Filter by:
      User  . . . . . .  __________   generic*
      Role  . . . . . .  __________   generic*
      Application . . . .  ____       generic*
      Code  . . . . . .  ___
      Minimum Numeric Limit .  __________      .000000
      Maximum Numeric Limit .  __________      .000000
      Minimum Alpha Limit . .  __________
      Maximum Alpha Limit . .  __________

Enter=Confirm   F4=Browse   F9=Save Def   F11=View Output
```

Criteria Selection:

Include Role/User Desc	Y – include the column for the Role or User Description in the report N – do not include
Include Appl Desc	Y – include the column Appl Description in the report N – do not include
Include Code Desc	Y – include the column Code Description in the report N – do not include
Sort by Auth Code	Y – the Application/Code is the primary sort for the report N – the Role or User is the primary sort for the report
Minimum Limit Info	A – include the column for minimum alphanumeric limits N – include the column for minimum numeric limits B – include the column for minimum alphanumeric and numeric limits X – exclude any columns for minimum limits from the report
Maximum Limit Info	A – include the column for maximum alphanumeric limits N – include the column for maximum numeric limits B – include the column for maximum alphanumeric and numeric limits X – exclude any columns for maximum limits from the report
Filter by:	
User	limit the rows to a user or users matching generic value
Role	limit the rows to a role or roles matching generic value
Application	limit the rows to an application or applications matching generic value
Code	Limit the rows to a specific code
Minimum Numeric Limit	Limit rows to unlimited authorizations or to authorizations limited to at least the value entered
Maximum Numeric Limit	Limit rows to non-limited authorizations or to authorizations limited to no more than the value entered. If the Minimum Limit filter is also used, the range for the role or user must be between the minimum and maximum filter values.

Minimum Alpha Limit	Limit rows to unlimited authorizations or to authorizations limited to at least the value entered
Maximum Alpha Limit	Limit rows to non-limited authorizations or to authorizations limited to no more than the value entered. If the Minimum Limit filter is also used, the range for the role or user must be between the minimum and maximum filter values.

Function Keys:
F3=Exit – Return to previous panel
Enter=Confirm – Confirm selection with Enter key
F4=Browse – Browse a list of available values
F9=Save Def – Save a Report Definition
F11=View Output – Work with MD Output
F12=Exit – Return to previous panel

7.2 User Authority

```
SCCRPT                          Company Name                              11/26/11
SCRN2                       MDSEC Report Generator                        10:07:12

    Report  . . . . . .  2       MDSEC User Authority

    Include Role/User Desc  .  Y       Y/N
    Include Appl Desc . . . .  N       Y/N
    Include Code Desc . . . .  Y       Y/N
    Sort by Auth Code . . . .  Y       Y/N
    Minimum Limit Info  . . .  X       A=Alpha, N=Numeric, B=Both, X=Exclude
    Maximum Limit Info  . . .  X       A=Alpha, N=Numeric, B=Both, X=Exclude

    Filter by:
      User  . . . . . .  __________   generic*
      Role  . . . . . .  __________   generic*
      Application . . . .  ____       generic*
      Code  . . . . . .  ___
      Minimum Numeric Limit .  __________      .000000
      Maximum Numeric Limit .  __________      .000000
      Minimum Alpha Limit . .  __________
      Maximum Alpha Limit . .  __________

Enter=Confirm   F4=Browse   F9=Save Def   F11=View Output
```

Criteria Selection:

Include Role/User Desc	Y – include the column for the Role or User Description in the report N – do not include
Include Appl Desc	Y – include the column Appl Description in the report N – do not include
Include Code Desc	Y – include the column Code Description in the report N – do not include
Sort by Auth Code	Y – the Application/Code is the primary sort for the report N – the Role or User is the primary sort for the report
Minimum Limit Info	A – include the column for minimum alphanumeric limits N – include the column for minimum numeric limits B – include the column for minimum alphanumeric and numeric limits X – exclude any columns for minimum limits from the report
Maximum Limit Info	A – include the column for maximum alphanumeric limits N – include the column for maximum numeric limits B – include the column for maximum alphanumeric and numeric limits X – exclude any columns for maximum limits from the report
Filter by:	
User	limit the rows to a user or users matching generic value
Role	limit the rows to a role or roles matching generic value
Application	limit the rows to an application or applications matching generic value
Code	Limit the rows to a specific code
Minimum Numeric Limit	Limit rows to unlimited authorizations or to authorizations limited to at least the value entered
Maximum Numeric Limit	Limit rows to non-limited authorizations or to authorizations limited to no more than the value entered. If the Minimum Limit filter is also used, the range for the role or user must be between the minimum and maximum filter values.

Minimum Alpha Limit	Limit rows to unlimited authorizations or to authorizations limited to at least the value entered
Maximum Alpha Limit	Limit rows to non-limited authorizations or to authorizations limited to no more than the value entered. If the Minimum Limit filter is also used, the range for the role or user must be between the minimum and maximum filter values.

Function Keys:
F3=Exit – Return to previous panel
Enter=Confirm – Confirm selection with Enter key
F4=Browse – Browse a list of available values
F9=Save Def – Save a Report Definition
F11=View Output – Work with MD Output
F12=Exit – Return to previous panel

7.3 Users with Role

```
SCCRPT                          Company Name                              11/26/11
SCRN2                       MDSEC Report Generator                        10:07:12

    Report  . . . . . .  3       MDSEC Users with Role

    Include Role/User Desc  .  Y       Y/N




    Filter by:
      User  . . . . . .  __________   generic*
      Role  . . . . . .  __________   generic*



Enter=Confirm   F4=Browse   F9=Save Def   F11=View Output
```

Criteria Selection:

Include Role/User Desc	Y – include the column for the Role or User Description in the report N – do not include
Filter by:	
User	Limit the rows to a user or users matching generic value.
Role	Limit the rows to a role or roles matching generic value.

Function Keys:
F3=Exit – Return to previous panel
Enter=Confirm – Confirm selection with Enter key
F4=Browse – Browse a list of available values
F9=Save Def – Save a Report Definition
F11=View Output – Work with MD Output
F12=Exit – Return to previous panel

7.4 Roles for User

```
SCCRPT                          Company Name                          11/26/11
SCRN2                       MDSEC Report Generator                    10:07:12

    Report  . . . . . . . . . .  4       MDSEC Roles for User

    Include Role/User Desc  .  Y       Y/N

    Filter by:
      User  . . . . . . . . . .  __________   generic*
      Role  . . . . . . . . . .  __________   generic*

Enter=Confirm   F4=Browse   F9=Save Def   F11=View Output
```

Criteria Selection:

Include Role/User Desc	Y – include the column for the Role or User Description in the report N – do not include
Filter by:	
User	Limit the rows to a user or users matching generic value.
Role	Limit the rows to a role or roles matching generic value.

Function Keys:
F3=Exit – Return to previous panel
Enter=Confirm – Confirm selection with Enter key
F4=Browse – Browse a list of available values
F9=Save Def – Save a Report Definition
F11=View Output – Work with MD Output
F12=Exit – Return to previous panel

7.5 Report Output

Reports (MD Output) generated within MDSEC, MDXREF and MDCMS can be viewed, printed, exported or emailed by pressing **F11** from most screens.

```
MDCOUTF                          MD Production 6.1                          10.03.12
SCRN1                                MD Output                              17:47:05
           User     Report   Object
Filter by: MMORGAN  ________ __________

Type options, press Enter.
 3=Copy to PF  4=Delete   5=Display   6=Print   E=Export

Opt User         Date     Time    Report  Object     Library        Length Width
 _  MMORGAN    24.02.11 17:36:18 PGMSRCH MDDCLWD    MDCMST            107    80
 _  MMORGAN    31.03.11  9:10:05 RFPHIST                              142    92
 _  MMORGAN    14.04.11 21:34:18 LIBCOMP MDCMS      MDCMST             28   120
 _  MMORGAN    23.05.11 20:50:20 COMPARE MDDCMSE    MDCMST            121   315
 _  MMORGAN    23.05.11 20:53:01 JOURNAL MDACST     MDADM              15   643
 _  MMORGAN    23.05.11 21:01:39 PGMSRCH MDDCMSD    MDCMST            200    80
 _  MMORGAN    29.09.11  9:23:16 PROJECT                              25    92
 _  MMORGAN    15.11.11 22:27:49 FLDLIST MDDTASK    MDCMST             56   112
 _  MMORGAN    22.02.12 13:42:05 JOURNAL MDAINV     MDADM              41   130
 _  MMORGAN     5.03.12 16:03:41 RFPHIST                              27    92


                                                                        Bottom
 F3=Exit    F4=Browse    F5=Refresh    F7=Spooled Output    F17=Top    F18=Bottom
```

Filters
Enter a value into a filter field to limit the listing to items matching the filter(s). Possible values may be selected by pressing **F4=Browse** while the cursor is positioned on the filter field.

Options
3=Copy to PF – Copy the detail contents of the report into a formatted table (DDS Physical File). This provides a simple means to extract information out of the MD database for use in SQL, Queries or programs.
4=Delete – permanently delete the report
5=Display – view the report contents directly in the screen
6=Print – print the report contents to a spooled file
E=Export – Export the report to a CSV, PDF, TXT or XLS formatted file. The file can be placed in IFS or emailed to one or more recipients. See the parameters for command MDRUNRPT for more information.

Function Keys:
F4=Browse – Browse possible values for a filter field
F5=Refresh
F7=Spooled Output – Display and manage spooled files
F17=Top – Position Cursor to the first entry in the list
F18=Bottom – Position Cursor to the last entry in the list

7.6 MDRUNRPT – Run Report command

Certain reports within MDSEC, MDXREF and MDCMS allow for saved report definitions to be run directly from a command line. This gives the users the ability to schedule reports to be run on a periodic basis and to have the output automatically printed or exported. This is also helpful during Project testing to allow the same parameters to be quickly used after each phase of a test.

The following screen is displayed to get the report run parameters.

```
                        Run MD Report (MDRUNRPT)

 Type choices, press Enter.

 Report Name  . . . . . .  _______      COMPARE, JOURNAL, MDSEC...
 User Profile . . . . . .  __________   User Profile
 Report Definition  . . . . . .  ____________________________________________
_____
 MDCMS Instance . . . . . .  *DFT       *DFT, *SAME, Instance
 Print result to spooled file . .  *NO  *YES, *NO
 Copy result to physical file . .  *NO  *YES, *NO
 Export result to IFS file  . . .  *NO  *YES, *NO
 Email result . . . . . .  *NO          *YES, *NO
 Filename . . . . . .  ____________________________________________
_____
 Append Timestamp to filename . .  *YES *YES, *NO
 Directory  . . . . . .  ____________________________________________
 _____

 Report Format  . . . . . .  XLS        CSV, PDF, TXT, XLS
 csv Field Delimiter  . . . . . .  ','  Field Delimiter
 Address to receive Email . . . .  *NONE____________________________________
 _____
 User to receive Email  . . . . .  *NONE  User ID
 Group to receive Email . . . . .  *NONE  Group ID

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Use **F9=All parameters** to see all available parameters for command.

Report Name
COMPARE – the MDXREF Data Comparison Report
JOURNAL – the MD Journal Analysis Report
MDSEC – the MDSEC Authorization Report
NOTCMS – the MDCMS Audit Report listing object changes made outside of MDCMS
PROJECT – the MDCMS Project Report
PRJTASK – the MDCMS Project Task Report
RFPHIST – the MDCMS Audit Report listing object changes made within MDCMS

User Profile
The name of the user profile that defined the report definition

Report Definition
The name of the report definition

Print result to spooled file
*NO – the resulting report will not be automatically printed to a spooled file
*YES – the resulting report will be automatically printed to a spooled file

Copy result to physical file
*NO – the resulting report will not be automatically exported to a physical file
*YES – the resulting report will be automatically exported to a physical file (table)

Export result to IFS file
*NO – the resulting report will not be automatically exported to an IFS file
*YES – the resulting report will be automatically exported to an IFS file

Email result
*NO – the resulting report will not be automatically emailed to recipients
*YES – the resulting report will be automatically emailed to recipients

Copy to Physical file
The name of the physical file (table) to contain the detail contents of the report. Each column in the report will be placed in a separate formatted field. If the file already exists, it will be replaced.

Copy to Library
The IBM i library that is to contain the Physical file

Filename
If the results are to be exported or emailed, this is the name of the IFS file to receive the results. The file type (.CSV, .PDF, .TXT or .XLS) will be automatically appended to the end of the name.

Timestamp
*NO – a timestamp will not be appended to the file name
*YES – a timestamp in the format of YYYMMDD_HHMMSS will be appended to the file name

Directory
If the results are to be exported, this is the name of the IFS directory to receive the results. The directory path should begin with the root character "/".

Report Format
CSV – the exported report will be placed in a comma separated value file which can then be opened in Microsoft excel or similar spreadsheet programs.
PDF - the exported report will be converted to PDF. JVM 1.5 or higher is required
TXT – the exported report will be placed in a text file with the same layout as the on-line report.
XLS – the exported report will be converted to the excel format. JVM 1.4 or higher is required

csv Field Delimiter
The character to be used to separate fields in a csv file

Address to receive Email
A specific email address to receive the report

User to receive Email
A user id to receive the report - the address for the user will be retrieved from the MDCMS email address table.

Group to receive Email
All users for the entered group id to receive the report – this parameter requires MDWorkflow groups to be present.

7.7 MDEXPSPLF – Export Spooled File command

The MDEXPSPLF command provides the functionality to export any spooled file to a text or PDF file.

The following screen is displayed to get the parameters.

```
                    MD Export Spool File (MDEXPSPLF)

 Type choices, press Enter.

 Spool Name . . . . . .          _________     Spool Name
 Job Name . . . . . .            *CURRENT      *CURRENT, Job Name
 Job Number . . . . . .          ______        Job Number
 Job User . . . . . .            __________    Job User
 Spooled file number  . . . . .  *LAST         *LAST, 1-999999
 MDCMS Instance . . . . . .      *DFT          *DFT, Instance
 Format . . . . . .              PDF           PDF, TXT
 File Name  . . . . . .          ____________________________________________
_____________________________________
 Append Timestamp to filename . .  *YES        *YES, *NO
 Report Title . . . . . .        ____________________________________________
_____________________________________
 Page Layout  . . . . . .        *DFT          *DFT, AUTOMATIC, LANDSCAPE
 Page Size  . . . . . .          *DFT          *DFT, A3, A4, A5, B5...
 Add Page Number to each Page . .  *NO         *YES, *NO
 Export result to IFS file  . . . > *YES       *YES, *NO
 Email result . . . . . .        > *YES        *YES, *NO
 Directory  . . . . . .
 Address to receive Email . . . .  *NONE_____________________________________
 User to receive Email  . . . . .  *NONE       User ID
 Group to receive Email . . . . .  *NONE       Group ID
```

Spool Name
The name of a spooled file

Job Name
The name of the job that generated the spooled file or *CURRENT to look for the spooled file in the current job

Job Number
The number of the job that generated the spooled file

Job User
The user profile of the job that generated the spooled file Report Header

Spooled File Number
The number of the spooled file within the job or *LAST to use the most recently generated spooled file of the given name for the given job.

MDCMS Instance
A 1-4 character string of the suffix for an existing instance of MDXREF or *DFT to use MDXREF

Format
PDF – the spooled file will be converted to the PDF format. JVM 1.5 and MDCMS is required
TXT – the spooled file will be converted to a text file

File Name
If the results are to be exported or emailed, this is the name of the IFS file to receive the results. The file type (.pdf or .txt) will be automatically appended to the end of the name.

Append Timestamp
*NO – a timestamp will not be appended to the file name
*YES – a timestamp in the format of YYYMMDD_HHMMSS will be appended to the file name

Report Title
The title to place in the header of the PDF file and in the subject line of the email

Page Layout
Values for PDF format:
*DFT – the layout defined in data area MDSEC(instance)/MDPDFLOUT
AUTOMATIC – the layout is determined automatically based on the width of the spooled file
LANDSCAPE – the paper is rotated so that the wide edge is horizontal
PORTRAIT – the paper is rotated so that the wide edge is vertical

Page Size
Values for PDF format:
*DFT – the size defined in data area MDSEC(instance)/MDPDFSIZE
A3, A4, A5, B5, LEGAL, LETTER

Add Page Number to each Page
*NO – a page number will not be added to each page
*YES – a page number will be added to each page in the bottom right corner

Export result to IFS file
*NO – the resulting report will not be automatically exported to an IFS file
*YES – the resulting report will be automatically exported to an IFS file

Email result
*NO – the resulting report will not be automatically emailed to recipients
*YES – the resulting report will be automatically emailed to recipients. MDCMS is required.

Directory
If the results are to be exported, this is the name of the IFS directory to receive the results. The directory path should begin with the root character "/".

Address to receive Email
A specific email address to receive the report

User to receive Email
A user id to receive the report - the address for the user will be retrieved from the MDCMS email address table.

Group to receive Email
All users for the entered group id to receive the report – this parameter requires that MDWorkflow groups are present.

8 Authorization Lists

8.1 Listing of Authorization Lists

Option 4 from MDSEC Menu: IBM i Authorization Lists to be managed by MDSEC

```
SCCSAL                          Company Name                              9.03.10
SCRN4                       Authorization Lists                          15:02:10

Type options, press Enter.
 2=Edit   4=Delete   U=Users
                                                          Default     *PUBLIC
Opt List       Description                               Authority   Authority
 _  ACCT_T     Accounting Test environment               *CHANGE     *EXCLUDE
 _  ACCT_P     Accounting Production environment         *USE        *EXCLUDE









                                                                        Bottom
F3=Exit   F5=Refresh   F6=Add
```

Authorization List Options

2	Edit the description, default authority, and *PUBLIC authority for the Authorization List
4	Delete the Authorization List from MDSEC and may also optionally be removed from the IBM i system
U	View/Edit the list of user that are specified for the Authorization List

Function Keys:
F3=Exit – Return to previous panel
F5=Refresh – Refresh the panel
F6=Add – Add a new Authorization List to MDSEC/IBM i system
F12=Exit – Return to previous panel

8.2 Authorization List Maintenance

```
SCCSBM                          MDSEC Administration                          21.04.05
SCRN5                                 Edit List                               17:08:14


 Authorization List . . . . ACCT_T

 Description  . . . . . . . Accounting Test environment_____________

 Default Object Authority . *CHANGE__

 *PUBLIC Authority  . . . . *EXCLUDE_

     Set Default value for existing users in Authorization List? N  Y/N
     Set Default value for existing users in MDSEC?              N  Y/N




F3=Exit    F4=Browse
```

Authorization List Fields

Description: The description of the Authorization List object, which is stored on the iSeries System.

Default Object Authority: The default authority to objects for users. The default value may be applied at any time to all relevant users. The possible values are:

*ALL	complete authority to objects
*CHANGE	update authority to objects
*USE	objects may by viewed/used, but not changed
*EXCLUDE	no authority to objects
*PUBLIC	user not explicitly in list – has public authority. If user is in the List when this value is applied, then the user will be removed from the list.

***PUBLIC Authority:** The authority to objects for users that are not specified in the authorization list.

Set Default value for existing users in Authorization List?: If the answer to this question is Y (Yes), then all existing users in the Authorization List will obtain the new default authority.

Set Default value for existing users in MDSEC?: If the answer to this question is Y (Yes), then all existing users in the MDSEC User List will obtain the new default authority within the specific Authorization List.

Function Keys:
F3=Exit – Return to previous panel
F4=Browse – Browse the list of possible Authority values
F12=Exit – Return to previous panel

8.3 Authorization List User Maintenance

The list of authorization lists may be modified by pressing F10 from the administration screen which is reached by pressing F9 from the initial screen within MDSEC.

```
SCCSBM                        MDSEC Administration                          21.04.05
 SCRN6                      Authorization List Users                        17:08:48
                                List: ASW_Q
Scan: __________    Desc Filter: ____________________    Authority: __________

 Type options, press Enter.
  4=Remove from List
                                                                  Object
  Opt User       Description                                     Authority
   _  *PUBLIC    Authority for users not in list                 *EXCLUDE
   _  PELS       Peloso Sandro                                   *USE____
   _  SIMJ       Simunek Jan                                     *USE____
   _  ORLM       Maurizio Orlando                                *USE____
   _  MORM       Michael Morgan                                  *USE____


                                                                        Bottom
 F3=Exit    F4=Browse    F5=Refresh    F6=Add
```

Positioning and Filtering List

If text is entered in the Scan field, the cursor will be positioned to the closest match in the list of users. If text is entered in the Desc Filter field, only users that have matching text in their user description will be listed. For example, if MICHAEL would be entered in the above screen, only the user MORM will be displayed, because the string Michael is in the description.
If an Authority value is entered in the Authority filter, then only users with the matching authority will be listed.

User Options

4	The "Remove from List" option will remove the user from the IBM i Authorization List. The users authority to object secured by the list will be limited to *PUBLIC authority

Object Authority: The authority to objects for the specific user. The possible values are:

*ALL	complete authority to objects
*CHANGE	update authority to objects
*USE	objects may by viewed/used, but not changed
*EXCLUDE	no authority to objects

Function Keys:
F3=Exit – Return to previous panel
F4=Browse – Browse the list of possible Authority values
F5=Refresh – Refresh the panel
F6=Add – Add a new user to the Authorization List
F12=Exit – Return to previous panel

9 DDM Security

9.1 Overview

DDM stands for Distributed Data Management and provides a simple means for accessing and updating data on a target iSeries system using programs running on a local iSeries system. MDCMS, for example, uses DDM for synchronizing Project and Workflow information as well as for tracking object migrations across systems.

If DDM is allowed to be used without sufficient security measures in place, then a significant risk exists that data could be read and manipulated by otherwise unauthorized persons. The DDM Security feature of MDSEC can be used to exclude unauthorized users as well as to manage which Data objects may be accessed or manipulated via DDM.

9.2 General Configuration

Option 5 from MDSEC Menu: DDM Security

```
SCLSDM                          Company Name                          9.03.10
SCRN1                           DDM Security                         15:47:55


DDM Filter  . . . . . .  1   1=Managed by MDSEC filter program
                             2=Completely unblocked
                             3=Completely blocked
                             4=Managed by another program

Log DDM Usage   . . . . .  Y   Y/N  (entries written to MDSEC/SCDLOG)
Include MDCMS in Log  . . .  N   Y/N

Allow Remote Commands . . .  N   Y/N

Allow DRDA (SQL)  . . . . .  N   Y/N









F3=Exit   F7=Data Filters   F9=User Filters   F21=Sys Command
```

Configuration Options

DDM Filter

1) The MDSEC DDM filter program is used as the exit point program for the DDM listener. (Network Attribute DDMACC = MDSEC/MDLDDMF)
2) No filtering is performed (Network Attribute DDMACC = *OBJAUT)
3) DDM completely blocked (Network Attribute DDMACC = *REJECT)
4) Another program is used is the exit point program for the DDM listener. It is displayed for informational purposes only and cannot be selected.

Log DDM Usage

Y – DDM transactions will be logged to file MDSEC/SCDLOG
N – DDM transactions will not be logged

Include MDCMS in Log
Y – DDM transactions for files in MDCMS* or MDXREF* will be included in the log
N – DDM transactions for files in MDCMS* or MDXREF* will not be included in the log

Allow Remote Commands
Y – Commands sent from a remote system via DDM are allowed
N – Commands sent from a remote system via DDM are not allowed

Allow DRDA (SQL)
Y – Remote SQL clients using Application Requester Driver (ARD) programs are allowed access to the local database
N – Remote SQL clients using Application Requester Driver (ARD) programs are not allowed access to the local database

Function Keys:
F3=Exit – Return to previous panel
F7=Data Filters – Manage the list of Data Objects that may be accessed using DDM
F9=User Filters – Manage the list of local User Profiles that may be used to connect to the Database using DDM
F21=Sys Command

9.3 Data Filters

If the MDSEC filter program is used, the data filters are checked to see if a transaction for a particular file, data queue, or data area may take place. By default, if the library and/or object are not defined in the list, then the transaction will be blocked.

Field Information

Library
The name of a library on the local system

Object
The name of an object within the library or *ALL to indicate the default allowed usage for any objects in the library that are not specifically defined in the list.

For example: ALIB/*ALL *UPDATE could be defined to allow updates to all data objects in library ALIB. A second entry of ALIB/AFILE *EXCLUDE could be defined to exclude file AFILE.

Usage
*INPUT – a DDM transaction may only view the data. Updates are not allowed.
*UPDATE – DDM transactions may view or update the data.
*EXCLUDE – DDM transactions are not allowed

Function Keys
F3: Return to the Configuration Screen
F4: Browse list of Libraries or Objects (if MDXREF is also installed)

9.4 User Filters

If the MDSEC filter program is used, the user filters are checked to see if the locally utilized user profile may be used to connect to the database via DDM. By default, if the user is not defined in the list, then the transaction will be blocked.

Field Information

User
The name of a user profile on the local system or *ALL to indicate that any user profile may be used

Function Keys
F3: Return to the Configuration Screen
F4: Browse list of user profiles

Appendix A – Standard User Roles

Role	Overview
MD_ADMCMS	Change Authority to all settings in the MDCMS Setup Menu
MD_ADMWF	Change Authority to all settings in the MDWorkflow Settings Menu
MD_ADMXREF	Change Authority to MDCMS or MDXREF Applications and Levels (intended when MDXREF used as Standalone product)
MD_PGMR	Request Objects Create and Edit RFPs Submit RFPs for Promotion (installation preparation step) Edit RFP in Send List Receive RFP
MD_PGMRADV	Edit other user's Object Requests Request Source from a different location than defined path or search template for attribute
MD_PROJAPR	Edit Projects Authorize work to begin for Projects Approve Projects Task Maintenance MDWorkflow Report Settings
MD_PROJMGR	Create and Edit RFPs Create Projects Edit Projects Authorize work to begin for Projects Set Projects to Test-Ready Close Projects Task Maintenance MDWorkflow Report Settings
MD_RFPAPR	Create and Edit RFPs RFP Approval
MD_RFPINS	Create and Edit RFPs Submit RFPs for Promotion (installation preparation step) RFP Installation RFP Rollback Receive RFP
MD_RFPSND	Edit RFP in Send List Send RFP
MD_USER	Read-Only access to MDCMS and MDXREF

Appendix B – MD Product Security Codes

Column Definitions

Code

The MDSEC Functional Security Code for MDSEC Application "md"

Appl Specific

Y – The code value for a role or user is defaulted in application md, but can be refined by the organization's MDCMS application code – in other words, a user may have authority to a function in application ABC but not in application XYZ.

N – The code value is in effect across all applications

Description

Describes the function for which the Code provides authorization.
Any authority granted for MDCMS is also valid for MDOpen.

Code	Appl Specific	Description
1	N	Read Access to the MDXREF product
2	N	Read Access to the MDCMS product
3	N	Manage Application Codes in MDCMS (or MDXREF if MDXREF is installed without MDCMS)
4	Y	Manage Application Promotion Levels in MDCMS (or MDXREF if MDXREF is installed without MDCMS)
5	Y	Manage MDCMS Attributes
6	Y	Manage Attribute and *RFP Commands or Scripts
7	Y	Manage MDCMS Templates
8	Y	Manage Distribution Levels
9	N	Manage list of target OS/400 locations
10	N	Manage MDOpen Server Locations
11	N	Manage System Settings
12	N	Manage Email Settings
13	N	Manage Email Addresses
14	N	View MD Output generated by other Users
15	N	Delete MD Output generated by other Users
20	Y	Send Entire Application Settings to other Systems
21	Y	Send Attribute Settings to other Systems
30	Y	Request (check out) Objects
31	Y	Edit or Delete the Request Records of other users
32	Y	Change the User assigned to an Object Request
33	Y	Request (check out) source from a different location than the location that MDCMS recommends to the user
34	Y	Retrieve Source or Object from the MDCMS archive
35	Y	Allows ignoring the pre-submit Warning when files are changed and not all programs that access records in the file are included in the RFP
36	Y	Allow the option Ignore in the Version Conflict view for objects in a dependent level
40	Y	Create and Edit RFPs
41	Y	Submit RFP for Promotion (pre-installation step)
42	Y	Approve RFP for Installation, if RFP was submitted by different user
43	Y	Approve RFP for Installation, even if Source or Objects in the RFP were manually modified since installation into prior level. User must also have authority to code 42 or 52 depending on submit user

Code	Appl Specific	Description
44	Y	Install RFP approved by different user
45	Y	Edit RFP Reserve Date in MDWorkflow after Installation complete in order to expand Installation Test window
46	Y	Confirm RFP Test Acceptance or Rejection in MDWorkflow
47	Y	Roll Back previously installed RFP
48	Y	Edit contents of RFP in Send List
49	Y	Send RFP to another System
50	Y	Send Data (*DATA/*DTAGRP requests) to another System User must also have authority to code 49
51	N	Receive RFP on target System
52	Y	Approve RFP for Installation, if RFP was submitted by same user
53	Y	Install RFP approved by same user
54	Y	Close/Ignore Unsent RFP in Send List
60	N	Create Projects
61	N	Edit Projects
62	N	Authorize work to be performed for Projects
63	N	Set Projects to status “Ready to Test”
64	N	Approve Projects
65	N	Close Projects
70	N	Manage Project Tasks
71	N	Manage MDWorkflow Group Types
72	N	Manage MDWorkflow Groups
73	Y	Manage MDWorkflow Group Types Required for Test Acceptance for specific Application Levels
74	N	Manage Custom Field, Custom Status and Task Type settings for Projects of Tasks
75	N	Manage MDWorkflow Object Group settings
76	N	Manage MDWorkflow Public Report settings
77	N	Manage MDWorkflow Conflict List settings