



User Manual

MDSEC

Application Security Tool for the IBM i from Midrange Dynamics

Version 8.5
Published January 15, 2023



MDSEC - Table of Contents

1	OVERVIEW	3
1.1	Terminology	3
1.2	Starting MDSEC.....	4
1.3	MDSEC Menu	4
2	USER ROLES	6
2.1	User Role Listing.....	6
2.2	MDSEC Application Levels for Role.....	8
2.3	MDSEC Security Codes for Role	9
2.4	MDSEC Code Limits for Role	11
2.5	Users with Role	12
3	USERS.....	13
3.1	User Listing.....	13
3.2	Roles for User	16
3.3	Transfer Requests to a Different User.....	18
3.4	MDUPDUSR – Update MDSEC User command.....	20
4	FUNCTIONAL SECURITY CODES	22
4.1	Application Level Listing	22
4.2	Application Code Listing.....	24
5	EMBEDDING MDSEC INTO YOUR APPLICATIONS	25
5.1	MDSECAUT Parameter Table.....	25
5.2	Detailed Description of MDSECAUT Parameters.....	25
5.3	Programming Examples and Copybooks	26
6	MD COMMAND SECURITY	27
7	MDSEC REPORT GENERATOR.....	28
7.1	Role Authority	29
7.2	User Authority.....	31
7.3	Users with Role	33
7.4	Roles for User	34
7.5	Report Output.....	35
7.6	MDRUNRPT – Run Report command.....	36
7.7	MDEXPSPLF – Export Spooled File command.....	38
8	AUTHORIZATION LISTS	40
8.1	Listing of Authorization Lists	40
8.2	Authorization List Maintenance	41
8.3	Authorization List User Maintenance	42
9	DDM SECURITY	43
9.1	Overview	43
9.2	General Configuration.....	43
9.3	Data Filters.....	45
9.4	User Filters	45
10	API TOKENS	46
10.1	Overview	46
10.2	Generate a Token.....	46
10.3	Manage Existing Tokens	46
10.4	Example Request Header	46
11	SYSTEM SETTINGS	47
11.1	Setting the JVM to be used for MD Java Modules	48
12	EMAIL SETTINGS.....	49
12.1	Email Addresses	50
12.2	Email Log.....	51
APPENDIX A – STANDARD USER ROLES		52
APPENDIX B – MD PRODUCT SECURITY CODES.....		55

1 Overview

The MDSEC Application-Security tool provides IT staff a user-friendly means to secure MDCMS, MDOpen, MDXREF and MDWorkflow, 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 IBMi authorization lists and DDM usage.

1.1 Terminology

Application

An application is a collection of functional security codes. MD product 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 the MD products.

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

Level

The level represents an instance, or environment, of an application (development, test, production, etc.). The general application **md** doesn't contain levels, but each MDCMS/MDXREF level defined for an organization can have certain security functions limited to specific levels for a given user.

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 IBMi system that should have authority to one or more application codes based on role memberships and personally granted authorities.



1.2 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 #8.

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.

1.3 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
      6    MD Command Security
      7    Report Generator
      8    API Tokens

      9    License Keys

     11    System Settings
     12    Email Settings

      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.
This option is only available from the default instance of MDSEC.

Option 6: MD Command Security

Grants or Revokes permissions to execute MD commands that cause updates to MDCMS data or deployments.

Option 7: Report Generator

Allows the user to generate a variety of security reports for Users and Roles.

Option 8: API Tokens

Creates REST API tokens to be used for authenticating a REST client when invoking MDChange (MDCMS) REST APIs.

Option 9: License Keys

Allows for the update of the MD license keys in case the previous keys need to be adjusted or a new MD product license is to be added.

Option 11: System Settings

Defines various system-wide information for this instance of the MD Products.

Option 12: Email Settings

Defines the SMTP credentials and the list of recipient email addresses.



2 User Roles

2.1 User Role Listing

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

```

SCCGPD                               Company Name                9.12.16
SCRN1                                MDSEC User Roles        10:37:00

Pos: _____  Filter by Desc: _____  Appl: _____
                    User: _____          Lvl: _____
                                         Code: _____

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

Opt  Role ID      Description                                Users
--  -
_   MD_ADMCMS    MDCMS Administration                            4
_   MD_ADMWF     MDWorkflow Administration                       4
_   MD_ADMXREF   MDXREF Administration                           4
_   MD_PGMR      MDCMS Programmer                               4
_   MD_PGMRADV   MD Programmer Advanced                         3
_   MD_PGMROPN   MDOpen Programmer                              3
_   MD_PROJAPR   MDCMS Authorize/Approve Involved Projects      3
_   MD_PROJEDT   MDCMS Edit Involved Projects                   4
_   MD_PROJMGR   MDCMS Create/Manage all Projects               3
_   MD_RFP_SBM   MDCMS RFP Submit                               3
_   MD_RFPAPR    MDCMS RFP Approve                              3
                                         More...

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	only roles with authorization to at least one code in the entered application will be listed
Lvl	only roles with authorization to at least one code in the entered level number will be listed
Code	only roles with authorization to the entered code will be listed. If application and/or level filter values are also entered, then only roles with the entered combination 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



2.2 MDSEC Application Levels for Role

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

SCCSCD	Company Name	9.03.10
SCRN1	MDSEC Application Levels for Role	18:57:01
Role: ADMIN	Administrator	
Pos: _____	Filter by Lvl: __ Desc: _____	
Type options, press Enter.		
C=Codes 4=Remove from Role 9=Apply to all Levels		
Opt	Appl Lvl Description	General Access
-	md MD Product Global Authorization Codes	Y
-	MD MD Product	Y
-	OPER 10 Operations Libraries	Y
-	WEB 80 midrangedynamics.com	Y
F3=Exit F5=Refresh F6=Add		Bottom

Positioning and Filtering List

Pos	the cursor will be positioned to the first application >= entered value
Lvl	only application levels for the entered number will be listed
Desc	only application levels containing the entered value in the description will be listed

Fields

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

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 level that the role is authorized to
4	Remove all authorizations for the application level from the role
9	Apply all code authorizations for application md to all MDCMS/MDXREF levels 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 Level.

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



2.3 MDSEC Security Codes for Role

Option C from the MDSEC Application Levels for Role Listing: all Security Codes for which the role is authorized within the selected Application Level

SCCSCD	Company Name	9.03.10
SCRN2	MDSEC Security Codes for Role	19:21:36
Role....: MD_ADMCMS MDCMS Administration		
Appl/Lvl: md MD Product Global Authorization Codes		
Pos: ____ Filter by Desc: _____		
Type options, press Enter.		
4=Remove from Role 9=Apply to all MD Apps		
Opt	Code	Description
		Application Specific
-		General Access
	1	MDXREF General Product Authorization
	2	MDCMS General Product Authorization
	3	Application Group Maintenance
	4	Promotion Level Maintenance
	5	Attribute Maintenance
	6	Attribute Command Maintenance
	7	Object Authority Maintenance
	8	Distribution Queue Maintenance
		More...
F3=Exit F5=Refresh F6=Add		

Positioning and Filtering List

Pos	the cursor will be positioned to the first code >= entered value
Desc	only codes containing the entered value in the 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 level but not another N – Authorization to the MDCMS or MDXREF function is checked against md and there is no differentiation amongst the application levels
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 application levels for the role. Option only valid for application <i>md</i> .

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



2.4 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
Lvl.: 10         Test level 10
Code: 100       custom code

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



2.5 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

F3=Exit  F5=Refresh  F6=Add

Bottom

```

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



3 Users

3.1 User Listing

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

```

SCCUPD                               Company Name                9.03.16
SCRN1                                MDSEC Users                 10:37:00

          Filters:
          Name: _____ Appl/Lvl: ____ _ Code: ____
Pos: _____ Role: _____ Role, *USER Ext ID: _____
          Grp Auth: _ Act: _ Sec: _

Type options, press Enter.
R=Roles T=Transfer Requests U=User Auth 2=Edit 3=Copy 4=Delete 5=View

Opt User ID      Name                               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 first user id >= entered value
Name	only users containing the entered value in the name will be listed
Appl	only users with authorization to at least one code in the entered application will be listed
Lvl	only users with authorization to at least one code in the entered level number will be listed
Code	only users with authorization to the entered code will be listed. If application and/or level filter values are also entered, then only users with the entered combination will be listed.
Role	Only users that belong to the entered role will be listed
Ext ID	only users containing the entered value in their External User ID will be listed
Grp Auth	Filter the users based on following group authority values: 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
Act	Filter the users based on the following Active status values 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
Sec	Filter the users based on the following Security Authority values: Y – the user may make changes within MDSEC N – the user is not permitted to make changes within MDSEC



Fields

User ID	The user profile of a user
User Name	Name or description of the user, leave blank to retrieve from user profile, if the User ID exists as a *USRPRF object
Email Address	Email Address of the user for emailing messages or reports from MD products. Optional field.
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 S – the user ID belongs to an automated process rather than an actual user. The ID is then applied as the user for processes invoking MDCMS commands, REST APIs, or as the user granting acceptance from a Pipeline job during the RFP acceptance phase.
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
Use CurUser Auth	If the User Profile of the User ID doesn't have authority to an MDSEC code, it can be permitted to have the authority checked for the current user of the job, in case a user role-swap is performed. Y – Current User authority checking is permitted in MDSEC when the job user doesn't have authority. N – Current User authority checking is not permitted
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
T	Transfer Active MDCMS Object Requests in the Object Manager and in the Send List to a different developer. See the section Transfer Requests to a Different User for more information.
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.



3.2 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 application levels 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 Level and Code authorities for a User. These can be in addition to, or instead of, Role authorities for the User

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 Application Levels for Role** panel, press the **F6=Add** function key. On the **Unauthorized MDSEC Application Levels** panel, select all Application Levels that the user will require personal authority to and press Enter. That action will result in the Application Levels selected being returned to the **MDSEC Security 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.



3.3 Transfer Requests to a Different User

Option T from the MDSEC User Listing: Transfer Active MDCMS Object Requests in the Object Manager and in the Send List to a different developer.

```

SCCTRQ                MD Dev                27.11.21
SCRN1                  Transfer Requests Owned by User  22:29:29

Change From User.    MMORGAN      Michael Morgan
To User.            STUART_____ Stuart Milligan

Active Requests .   Y Y/N
Send Requests . .  Y Y/N

Filters (blank=all)
Application . .    _____
Level . . . . .   _____
RFP Number . .    _____
Project . . . .   MDS_____ MD Service Desk
Task Number . .   _____ 88 Report of objects not requested
Subtask Number.   _____

Enter=Next   F3=Exit   F4=Browse   F21=Sys Command
  
```

Fields

Change To User	The User ID of a user registered in MDSEC with request authority for at least one level.
Active Requests	Transfer active requests (those visible from the MDCMS Object Manager) to the new user
Send Requests	Transfer send requests (those visible from the MDCMS Send RFP to Remote System list) to the new user
Application	Filter the requests to a specific Application
Level	Filter the requests to a specific Promotion Level
RFP Number	Filter the requests to a specific RFP number
Project	Filter the requests to a specific Project
Task Number	Filter the requests to a specific Project Task
Subtask Number	Filter the requests to a specific Project Subtask

Use F4 to select any of the field values from a list.

Press Enter once the values are correct to continue to the next screen (nothing will be changed yet).



The next screen in the process shows each distinct target Promotion Level and Developer Library/Folder for requests assigned to the current user based on the filters from the initial screen.

```

SCCTRQ                      MD Dev                      27.11.21
SCRN2                        Level Requests to Transfer  01:22:27

From User: MMORGAN          Michael Morgan
To User:  STUART           Stuart Milligan

Type options, press Enter.
C=Copy to Diff Dev Lib   M=Move to Diff Dev Lib   O=Omit   S=Same Dev Lib

Opt Appl  Lvl Del Mig Mod Rcp Snd  Developer Library/Message
S  MD     16      Y  Y  Y  Y   MMORGAN
S  MD     16      Y  Y  Y  Y
/home/MMORGAN

Enter=Confirm   F5=Refresh   F12=Cancel   F21=Sys Command
  
```

Options

C	Transfer the requests to the new user and copy the source and/or object from the current checkout library/folder to a different library/folder for the new developer. You will be prompted for the name of the new library/folder
M	Transfer the requests to the new user and move the source and/or object from the current checkout library/folder to a different library/folder for the new developer. You will be prompted for the name of the new library/folder
O	Don't transfer the requests to the new developer. MDCMS will automatically omit requests for an application/level if: 1) you don't have the authority to change the programmer for that application/level (MDSEC code 32) 2) the new user doesn't have authority to add, modify, delete objects for the level (MDSEC code 28) and such requests exist for the current user 3) the new user doesn't have authority to recompile or update objects for the level (MDSEC code 30) and such requests exist for the current user
S	Transfer the requests to the new user, but leave the source and objects where they are.

Once the options have been set, press Enter to process the user change for all relevant requests. If any libraries or source files need to be created, you will be prompted for the parameters to do so.



3.4 MDUPDUSR – Update MDSEC User command

The Update MDSEC User (MDUPDUSR) command provides the ability to systematically add, update or remove a user in MDSEC.

All MDUPDUSR transactions are logged in file MDCMS(ENV)/MDDUUSR

Restrictions:

- The job user must be authorized to command MDUPDUSR in MDSEC. See section MD Command Security for more information.

MDUPDUSR Parameters

PARM	Label	Length	Description
USER	User ID	10	the user ID (required) *ALL - all user IDs - may only be used for option *UPDADD to add or remove roles, change Group Auth usage, Current User Auth usage or CCISD for all defined users.
OPT	Option	7	Specifies the option to be taken with this command. *UPDADD - If the user already exists in MDSEC, it will be updated with the provided information. Otherwise, the user will be added. *ADD - Add the provided information only if the user isn't already defined in MDSEC. *REMOVE - Remove the user from MDSEC
DESC	Description	50	The user description. *SAME - Don't update the description. If for a new user, the description will be retrieved from the IBM i user profile.
ADDR	Email Address	60	The email address of the user. *SAME - Don't update the email address. Will be ignored for a new user. *NONE - remove the email address, if currently defined
EXTU	External User ID	20	The external user ID, if mapping from LDAP for the usage of MDWorkflow. *SAME - Don't update the external User ID. Will be ignored for a new user. *NONE - remove the external User ID, if currently defined
ACT	Active	5	Specifies if the user profile is activated (enabled) in MDSEC. *SAME - Don't update the Active flag. If for a new user, the flag will be set to *YES=Activated. *YES - The user is activated in MDSEC in MDSEC. *NO - The user is deactivated in MDSEC



GRPA	Use Group Auth	5	<p>Specifies if authority for the user should be based on the authority permitted for the primary group that the user belongs to.</p> <p><u>*SAME</u> - Don't update the Use Group Auth flag. If for a new user, the flag will be set to *NO=Not based on group authority.</p> <p>*YES - The user's authority is based solely on the authority permitted for the primary group that the user belongs to. in MDSEC.</p> <p>*NO - The user's authority is based solely on the authority permitted for the user themselves.</p> <p>*BOTH - The user's authority is based on the combination of the authority for the group and the specific user.</p>
CURA	Use Current User Auth	5	<p>Specifies if authority for the current user is allowed to be used if the job user isn't authorized to a function.</p> <p><u>*SAME</u> - Don't update the Use Current User Auth flag. If for a new user, the flag will be set to *NO=Not allowed to check current user authority.</p> <p>*YES - Current User authority checking is permitted in MDSEC.</p> <p>*NO - Current User authority checking is not permitted</p>
CCSID	CCSID Override	5	<p>The CCSID to use for the user, instead of the CCSID defined for the MDCMS instance. This value is used for character translation between the MDCMS database and MDOpen/MDWorkflow.</p> <p>If not using special values *SAME or *NONE, the entered value must be numeric and must exist in the MD CCSID translation table list, which can be viewed by pressing F4 on the CCSID field within the user maintenance screen in MDSEC or within the System Settings.</p> <p><u>*SAME</u> - Don't update the CCSID Override value. Will be ignored for a new user.</p> <p>*NONE - remove the CCSID Override value, if currently defined</p>
ADDROLE	Add Role	10	<p>The list of up to 20 MDSEC authority roles that should be granted to the user.</p> <p>*ALL - Grant every defined role to the user.</p>
RMVROLE	Remove Role	10	<p>The list of up to 20 MDSEC authority roles that should be revoked for the user.</p> <p>*ALL - remove the user from every role that they currently belong to.</p>
ENV	Environment ID	5	<p>Specifies the MDCMS environment that the Project exists in. The ID correlates to the suffix of the MDCMS library name.</p> <p><u>*DFT</u> - The default environment will be used. This correlates to library MDCMS.</p> <p>*SAME - The environment of the current library list will be used</p>



4 Functional Security Codes

4.1 Application Level Listing

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

```

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

Filter by Appl: ____ Lvl: __ Desc: _____ Active: __

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

Opt  Appl  Lvl  Description                                     Active
-    md    -    MD Product Global Authorization Codes           Y
-    ACCT  90  Accounting application                           Y
-    INV   10  Inventory application                             Y

F3=Exit  F5=Refresh  F6=Add

Bottom
  
```

Filtering List

Appl	filter rows by application ID
Lvl	filter rows by level number
Desc	only levels containing the entered value in the description will be listed
Active	filter rows based on following Active values: N – Authorizations for all codes for this level have been disabled Y – Authorizations for all codes for this level are enabled

Fields

Appl	An application defined either in MDCMS/MDXREF or from this screen
Lvl	the application level defined either in MDCMS/MDXREF or from this screen
Description	Description of the application level
Active	N – Authorizations for all codes for this level have been disabled Y – Authorizations for all codes for this level 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 level
3	Copy the level to a new application level and optionally copy the non-md codes to the new level too
4	Remove the Application Level from MDSEC – only allowed for applications that are not managed by MDCMS or MDXREF
5	View the properties and Codes for the Application Level

Function Keys:



F3=Exit – Return to previous panel

F5=Refresh – Refresh the panel

F6=Add – Add a new Application Level to MDSEC that will not be managed by MDCMS or MDXREF



4.2 Application Code Listing

```

SCCSBM                               Company Name                21.04.05
SCRN2                                Edit Security Codes      17:05:09

Appl: ACCT  Lvl: 10  Desc: Accounting application                Active: Y
=====
Pos: ____   Filter by Desc: _____

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

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 Security Code
Active	N – Authorizations for all codes for this application level have been disabled Y – Authorizations for all codes for this application level 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 Level. The Code must be higher than 99 if the Application is managed by MDCMS or MDXREF



5 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.

5.1 MDSECAUT Parameter Table

Parameter	Usage	Type	Length	Short Description
User ID	Input	String	10	User ID, *USER, blank
Application	Input	String	6	MDSEC Application Code
Level	Input	Number	3	MDSEC Application Level
Code	Input	Number	3	Security Code within Level
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

5.2 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.

Level: The 2-digit MDSEC level (environment) of the application that the function belongs to. This value may be 0 if the application isn't split into multiple levels.

Code: The 3-digit MDSEC code within the application level 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.

5.3 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.



6 MD Command Security

Option 6 from the MDSEC Main Menu gives the user access to provide or revoke permissions to users in order to execute specific MD commands that cause updates to MDCMS data or deployments.

```

MDCCMDS                      MD Dev                      26.08.18
SCRN1                         Secured MD Commands  22:59:12

Filter by Cmd: _____ Lib: _____ Desc: _____ User: _____

Type options, press Enter.
U=Users

Opt Command  Library  Description  Authorized Users
- MDADDCMD   MDCMS   Add Command to Object Request *ALL
- MDADDREQ   MDCMS   Add Object Request *ALL
- MDADDSOG   MDCMS   Add Send Object Group *ALL
- MDCLEAR    MDCMS   Clear ALL MDCMS Activity *ALL
- MDCPYDATA  MDCMS   Copy Data between Libraries *ALL
- MDCRTOBJ   MDCMS   Create Object in Dev Library *ALL
- MDCRTSET   MDCMS   Create MD Settings Appl *ALL
- MDDELRFPP  MDCMS   Delete RFPs *ALL
- MDINSRFP   MDCMS   Install RFPs *ALL
- MDLCKAMGS  MDCMS   Lock Auto-Merge of Send RFPs *ALL
- MDLOCPWD   MDCMS   Change PW for MD Locations *ALL
- MDMIGMD    MDCMS   MDCMS Merge Data *ALL

More...

F3=Exit

```

When the program called by a command in this list is invoked, this table is checked to see if the job user is entitled to execute the command. If not, the program will terminate and the log entry for the command, if applicable, will be updated to reflect that the job user is not authorized.

When the command is invoked via a corresponding REST API, the user that is checked is the user that owns the Token. Tokens are generated in MDSEC option API Tokens.

A user can make changes to command permissions from this screen if they are registered with MDSEC Edit Authority in MDSEC.

Use option U to view/modify the list of users permitted to execute a particular command.

User special values:

- *ALL – any user on the system (including users not registered in MDSEC) can execute the command.
- *ALLSEC – any user that is registered in MDSEC and has been granted authority to the function carried out by the command (recommended).
- *NONE – no user may execute the command



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



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*
Level . . . . . _____
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
Level	limit the rows to a specific level
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



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*
Level . . . . . _____
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
Level	limit the rows to a specific level
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



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



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



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
_  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
_  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
_

                                          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 . . . . . XLSX          CSV, PDF, TXT, XLSX
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

```

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
- PRJTIME – the MDCMS Project Time Entry 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 .XLSX) 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 YYYYMMDD_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.
- XLSX – the exported report will be converted to the excel format. JVM 1.5 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 YYYYMMDD_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)/MDPDFLAYOUT

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

Opt List      Description                                Default Authority  *PUBLIC Authority
_ ACCT_T      Accounting Test environment                    *CHANGE          *EXCLUDE
_ ACCT_P      Accounting Production environment            *USE             *EXCLUDE

F3=Exit  F5=Refresh  F6=Add

Bottom
  
```

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 IBMi 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 be 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		
Opt	User	Description
—	*PUBLIC	Authority for users not in list
—	PELS	Peloso Sandro
—	SIMJ	Simunek Jan
—	ORLM	Maurizio Orlando
—	MORM	Michael Morgan
		Object Authority
		*EXCLUDE
		*USE
		*USE
		*USE
		*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 be 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 IBMi system using programs running on a local IBMi 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	<u>1</u>	1=Managed by MDSEC filter program 2=Completely unblocked 3=Completely blocked 4=Managed by another program
Log DDM Usage	<u>Y</u>	Y/N (entries written to MDSEC/SCDLOG)
Include MDCMS in Log . . .	<u>N</u>	Y/N
Allow Remote Commands . . .	<u>N</u>	Y/N
Allow DRDA (SQL)	<u>N</u>	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 as 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



10 API Tokens

10.1 Overview

MDCMS provides for the ability to retrieve and update information within MDCMS using REST APIs, which are exposed by the MDCMS HTTP server.

In order to protect MDCMS information from unauthorized access, a **bearer token** is expected to be included in the API request header. If the token is not present, MDCMS will return a 401-Unauthorized status.

If the token is present, it will be checked against the list of unexpired tokens. If not found, MDCMS will return a 401-Unauthorized status. If found, MDCMS will proceed further with carrying out the request based on the user that owns the token.

10.2 Generate a Token

Any user that is registered in MDSEC may generate a token for themselves. Any user that has MDSEC Administration rights may additionally generate tokens for other users. This can be useful when using a token applied to a service user rather than a human user.

To generate, do the following:

- 1) Within a 5250 session, type command MDSEC and press Enter
- 2) Select option 8 = API Tokens and press Enter
- 3) Press F6 = Add
- 4) Provide a description of the Token and a Valid Until Date and press Enter
- 5) The API Token will appear on the screen.

IMPORTANT: Copy the token value and store in a secure location. It will not be possible to view the value of the token again

10.3 Manage Existing Tokens

Any user that is registered in MDSEC may manage their own tokens. Any user that has MDSEC Administration rights may additionally manage tokens for other users. This can be useful when using a token applied to a service user rather than a human user.

To manage, do the following:

- 1) Within a 5250 session, type command MDSEC and press Enter
- 2) Select option 8 = API Tokens and press Enter
- 3) Use option 2 to edit the description or Valid Until Date, use option 3 to copy the token or use option 4 to delete the token

10.4 Example Request Header

Authorization: Bearer MTgzNTg1NDIxMDA1MzIxNzlyOTYzMTA3Mjk3O3U2Nzg5ODAxNDY2NTAyNzIxMxMTY1



11 System Settings

```

MDCSYSI                               System Settings                               04.09.08
SCRN1                                  SCRN1                                  10:37:42

Location Title . . . . . COMPANY NAME
Location ID . . . . . COMPl
Send Prefix . . . . . 6                0-9, A-Z
Send Prefix . . . . . 1                0-9, A-Z
Java Connect User Profile . . . . . MDCONNECT *NONE, Profile
Java Version . . . . . jdk80/64bit
Sign Objects . . . . . Y                Y/N
Default CCSID . . . . . 1148
Internal Task Ref Label . . . . . Team Ref
                                           MDCMS ONLY

Temporary Library Prefixes:
RFP Backup . . . . . SAV                SAV1234567
RFP Installation . . . . . CMS           CMS1234567
RFP Receipt . . . . . MD0              MD01123456
RFP Rollback . . . . . MDB             MDB1234567
Backup Lib Retention in days. . . . . 0-999

MD Build Date . . . . . 01.05.21
MD Installation Date . . . . . 01.05.21

F3=Exit   F4=Browse   F8=Patch History
  
```

The system settings can be managed from MDSEC menu option 11.

Location Title

The title to be displayed at the top of nearly all MD Product screens to help the user identify which system they are currently working on.

Location ID

A 10-Character ID to uniquely identify this system. The ID for this system must match the ID defined in the OS/400 location settings for any partition that will be connecting to this system.

Send Prefix

A 1-Character ID to uniquely identify distributions from this system. This is used to avoid conflicts in case multiple systems send Promotions to the same remote system. The temporary receiving library on the remote system will use this character in the 4th position of the library name.

Java Connect User Profile

The technical user profile on this system to be used to run MD java modules.

Java is used in MD for Excel and PDF report generation, sending emails, and Zip compression. F4 may be used to browse user profiles.

*NONE – java modules should not be used on this system. Recommended only if a JVM with minimum version of 1.4 is not present on the system.

Sign Objects (MDCMS Only)

Y – Sign Objects as they are being installed to ensure that they are not manually changed during the promotion process
N – Do not sign objects. Recommended only if the necessary IBM Java Encryption Libraries are not present on the system.

Default CCSID (MDCMS Only)

The Coded Character Set to use by default 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. If certain users require a different CCSID, that value can be defined for the user in MDSEC. F4 may be used to browse the list of CCSIDs defined for use in MDCMS.

Internal Task Ref Label

The label to use for the Internal Reference Code field for Tasks and Subtasks. This value will be used as the label throughout MDCMS, MDOpen and MDWorkflow.

Temporary Library Prefixes (MDCMS Only)

The prefix string to add to the front of each type of temporary library in MDCMS. The prefix may be changed so that conflicts can be avoided when multiple instances of MDCMS exist on the same system.

Backup Lib Retention in Days

When an RFP is installed, the number of days to retain the temporary backup library before it is deleted. If the value is blank, the library will be deleted as soon as the RFP is finished.

MD Build Date

The date that this version of MD was built by Midrange Dynamics

MD Install Date

The date that this version of MD was installed onto this system

11.1 Setting the JVM to be used for MD Java Modules

MD uses Java for various processes relating to Excel generation, PDF generation, SMTP, and Zipping. In order to carry out these processes, a JVM (minimum 1.6) must be installed on each system partition where MD will be used.

Data area MDSEC(instance)/MDJAVAHOME designates which installed JVM is to be used.

The valid values for this data area are:

*DFT – use the default JVM

*PROFFILE – load the JVM based on the settings in property file /mdcms/JAVA/mdcms.properties

A pathname pointing to a JVM (for example: /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit)

If a JVM is not available on the system, *NONE can be specified for the Java Connect User in the System Settings (MDSEC Menu Option 11). This will disable all java-related functionality, while still allowing all MD core functionality to be performed.



ZIP Attachments

*ALWAYS – attached files will be always be zipped to reduce the size of the emails

*NEVER – attached files will never be zipped

n KB – an attached file will only be zipped if it is larger than the entered number of Kilobytes

MDWorkflow URL

The context path for links to the MDWorkflow application. This must include http or https, the server address, port number if not 80 and the name of the web application.

This URL is used within MDMAILF email bodies to allow the user to navigate directly to a specific RFP and is used when generating Project, Task or Subtask mails out of MDWorkflow.

URL for MDOpen

Y – A column in the MDOpen Project, Task and Subtask list views will provide the URL icon to be clicked to open a browser to show the given element from within MDWorkflow.

N – The MDWorkflow URL column won't be visible in MDOpen

12.1 Email Addresses

The email addresses of the recipients can be maintained by pressing F8 from the Email Settings screen. If DDM connections are defined, the updates will be synced to all locations.

User ID

The user profile of the user. If the user does not have a profile on the system, any other ID of up to 10 characters can be used.

Name

The Name to be recipient to be displayed in the mail header

Address

The email address of the recipient



12.2 Email Log

Each time the MDMAIL job is used to send an email, a log entry will be written to MDSEC file MDDEMLL with the following information:

Date, Time, Job, Recipients, Subject, Attachments and Error Message

F10 can be pressed from the Email Settings screen to view/search log entries

Additionally, the MDMAIL service logs information to the IFS which can be viewed from the Services listing.

12.2.1 MDSTRMAIL – Start MDMAIL Client command

In order for MDWorkflow, the MDMAIL API or the MDMAILF API to send an email, the MDMAIL SMTP client must be running. This will happen automatically if the MDMAIL service is set to start automatically. Alternatively, command MDSEC(Instance)/MDSTRMAIL can be added to a scheduled job for a fixed starting time.

MDSTRMAIL Parameters

Environment ID	The name of the MDCMS instance (or suffix) - *DFT refers to MDCMS being used in library MDCMS. For a different library suffix, this would be entered for the environment ID.
Submit Job	*YES – a job named MDMAIL(instance) will be submitted to the entered Job Queue *NO – the MDMAIL process will run within the current job
Job Queue	*DFT – submit to the queue defined for the MDMAIL service *JOBQ – submit to the default queue for the running job profile The name of the job queue to submit MDMAIL to
Job Queue Library	The library of the job queue to submit MDMAIL to or *LIBL if the job queue is located in the current library list
Time of Day to auto-end Job	*DFT – end at the time defined for the MDMAIL service *NEVER – the MDMAIL job shouldn't end automatically – it should run until the job is forcibly ended or command MDENDMAIL is invoked. A specific time to end in format HH:MM:SS

12.2.2 MDENDMAIL – End MDMAIL Client command

The MDMAIL job can be set to end automatically at a certain time, or it can be ended at any time using command MDSEC(Instance)/MDENDMAIL. Once MDENDMAIL is run, MDMAIL will cleanly stop within 30 seconds.

MDENDMAIL Parameters

Environment ID	The name of the MDCMS instance (or suffix) - *DFT refers to MDCMS being used in library MDCMS. For a different library suffix, this would be entered for the environment ID.
----------------	--



Appendix A – Standard User Roles

The following table explains the primary (in **bold**) and secondary functional authorities for each role that are shipped as defaults when MDSEC is installed.

Role	Overview
MD_ADMCMS	Administrative Authority for all configuration settings in the MDCMS Setup Menu or MDOpen Settings section
MD_ADMWF	Administrative Authority for all settings in the MDWorkflow Settings Menu and corresponding Workflow settings in MDOpen
MD_ADMXREF	Administrative Authority for MDCMS or MDXREF Applications and Levels (intended when MDXREF used as Standalone product)
MD_PGMR	Request to add, modify or delete Objects in MDCMS (green screen). This is security code 28, which also requires that the MDCMS license key allows for as many developers as have been given access to this code within MDSEC. Request to recompile or update Objects Retrieve Archived Source or Object Create and Edit RFPs Submit RFPs for Promotion (installation preparation step) Edit RFP in Send List Receive RFP Set involved Projects to Test-Ready Comment on involved Projects Edit involved Tasks Edit involved Subtasks
MD_PGMRADV	Edit other user's Object Requests Change programmer for Object Request Request Source from a different location than defined path or search template for attribute Ignore Existing Objects in other Versions Edit involved Projects Create Tasks for involved Projects Edit any Task for involved Projects Edit any Subtask for involved Tasks Merge other Users into RFP
MD_PGMROPN	Request to add, modify or delete Objects in MDOpen . This is security code 29, which also requires that the MDOpen license key allows for as many developers as have been given access to this code within MDSEC. Request to recompile or update Objects Retrieve Archived Source or Object Create and Edit RFPs Submit RFPs for Promotion (installation preparation step) Edit RFP in Send List Receive RFP Set involved Projects to Test-Ready Comment on involved Projects Edit involved Tasks Edit involved Subtasks
MD_PROJAPA MD_PROJAPA (continued)	Confirm RFP Test Acceptance/Rejection Comment on any Project View any Project Edit any Project Authorize any Project



	<p>Approve any Project Comment on any Project Create Tasks for any Project Edit any Task Edit any Subtask</p>
MD_PROJAPR	<p>Confirm RFP Test Acceptance/Rejection Comment on any Project View any Project Edit involved Projects Authorize involved Projects Approve involved Projects Comment on involved Projects Create Tasks for involved Projects Edit any Task for involved Projects Edit involved Tasks Edit any Subtask for involved Tasks Edit involved Subtasks</p>
MD_PROJEDA	<p>Edit any Project Comment on any Project Create Tasks for any Project Edit any Task</p>
MD_PROJEDT	<p>Edit involved Projects Comment on involved Projects Create Tasks for involved Projects Edit any Task for involved Projects</p>
MD_PROJMGR	<p>Create and Edit RFPs Create Projects Authorize any Project Set any Project to Test-Ready Approve any Project Close any Project Comment on any Project View any Project Create any Task Edit any Task MDWorkflow Report Settings Manage Time Entry for other Users Merge other Users, Projects or Tasks into RFP</p>
MD_RFP_SBM	<p>Request to Recompile or Update Objects Ignore Requirement to Request Related Objects RFP Maintenance RFP Submission Receive RFP from Remote System Set involved Projects to Test-Ready Comment on involved Projects Edit involved Tasks Edit involved Subtasks</p>
MD_RFPAPR	<p>Create and Edit RFPs Merge other Users, Projects or Tasks into RFP RFP Approval when submitted by different user RFP Approval for manually changed Objects Edit RFP Reserve Date after Install RFP Approval when submitted by same user</p>
MD_RFPINS	<p>Create and Edit RFPs</p>



	Merge other Users, Projects or Tasks into RFP RFP Installation when approved by different user Edit RFP Reserve Date after Install RFP Rollback Receive RFP from Remote System RFP Installation when approved by same user
MD_RFPSND	Edit RFP in Send List Send RFP Send Data to Remote System Close/Ignore Unsent RFP in Send List
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 and level – in other words, a user may have authority to a function in application ABC, level 10 but not in application XYZ, level 10 or in application ABC, level 20.

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, except for code 28.

Code 29 is only valid for MDOpen.

Administrative, RFP and Project-Specific codes are valid in MDCMS, MDOpen and MDWorkflow.

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
16	N	Export Output from reports, spool files and database files via Email
17	N	Export Output from reports, spool files and database files to an IFS Folder
20	Y	Send Entire Application Settings to other Systems
21	Y	Send Attribute Settings to other Systems
28	Y	Request to add, modify or delete Objects in MDCMS (green screen). The use of this code also requires that the MDCMS license key allows for as many developers as have been given access to this code within MDSEC.
29	Y	Request to add, modify or delete Objects in MDOpen. The use of this code also requires that the MDOpen license key allows for as many developers as have been given access to this code within MDSEC.
30	Y	Request to recompile or update objects
31	Y	Edit or Delete the Request Records of other users
32	Y	Change the User assigned to an Object Request. Additionally, this code is checked if the source being checked out is different than the source in the production comparison level for the application and the prior installation of the source into the target level was made by a different user.



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
37	Y	Edit your own object request details, such as RFP number, project, etc.
38	Y	Delete object requests owned by you
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
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
55	Y	Assign or Merge additional Object Requests into an RFP that doesn't already contain Object Requests for the Users assigned to the additional Requests.
56	Y	Assign or Merge additional Projects to requests in an RFP that doesn't already impact those projects.
57	Y	Assign or Merge additional Tasks for the same Project to requests in an RFP that doesn't already impact those tasks.
58	Y	Override Code Review Quality Gate for an RFP that didn't pass a Code Review to allow the next step in the migration path to occur.
59	Y	Override Automated Testing Quality Gate for an RFP that didn't pass an Automated Test to allow the next step in the migration path to occur.
60	N	Create Projects
61	N	Edit any Project
62	N	Authorize work to be performed for any Project. An object can't be assigned to a project if it isn't already authorized, unless the developer has authority to this code.
63	N	Set any Project to status "Ready to Test"
64	N	Approve any Project
65	N	Close any Projects
66	N	Comment on any Project
67	N	View any Project. If not authorized to this code, only projects that the user is involved with (either directly or part of a group) will be visible.
69	N	Create a Task for any Project
70	N	Edit Tasks for any Project
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 or Tasks
75	N	Manage MDWorkflow Object Group settings
76	N	Manage MDWorkflow Public Report settings
77	N	Manage MDWorkflow Conflict List settings
78	N	Manage Project Cost settings
81	N	Edit involved Projects
82	N	Authorize involved Projects
83	N	Set involved Projects to Test-Ready
84	N	Approve involved Projects
85	N	Close involved Projects
86	N	Comment on involved Projects
87	N	Create Tasks for involved Projects
88	N	Edit any Task for involved Projects
89	N	Edit involved Tasks
90	N	Edit any Subtask for involved Tasks
91	N	Edit involved Subtasks
92	N	Manage Time Entry for other Users