

MDSEC User Guide

Security Management for MDChange

Midrange Dynamics

Copyright © 2026 Midrange Dynamics

Table of contents

1. MDSEC	4
1.1 Welcome to MDSEC	4
1.2 Terminology	5
1.3 Starting MDSEC	6
1.4 MDSEC Menu	7
1.5 User Roles	8
1.5.1 User Roles	8
1.5.2 MDSEC Application Levels for Role	10
1.5.3 MDSEC Security Codes for Role	12
1.5.4 Users with Role	14
1.6 Users	16
1.6.1 Users	16
1.6.2 Roles for User	19
1.6.3 Transfer Requests to a Different User	20
1.7 Functional Security Codes	22
1.7.1 Filtering List	22
1.7.2 Fields	22
1.7.3 Options	23
1.7.4 Level Properties	23
1.8 Authorization Lists	24
1.8.1 Authorization List Listing	24
1.8.2 Authorization List Properties	24
1.8.3 Authorization List Users	25
1.8.4 3 Function Keys	25
1.9 DDM Security	26
1.9.1 Overview	26
1.9.2 General Configuration	26
1.9.3 Configuration Options	26
1.9.4 Function Keys	26
1.10 MD Command Security	28
1.10.1 User Special Values	28
1.11 MDSEC Report Generator	29
1.11.1 Reports	29
1.11.2 Function Keys	29
1.11.3 Criteria Selection	30

1.12	API Tokens	31
1.12.1	Overview	31
1.12.2	Generate a Token	31
1.12.3	Manage Existing Tokens	31
1.12.4	Example Request Header	31
1.13	MDUPDUSR - Update MDSEC User Command	32
1.13.1	Restrictions	32
1.13.2	Parameters	33
1.14	Appendix A - Standard User Roles	34
1.15	Appendix B - MD Product Security Codes	36
1.15.1	Column Definitions	36
1.15.2	Security Codes	37

1. MDSEC

1.1 Welcome to MDSEC

This is the User Guide for the MDSEC product within the MDChange Product Suite from Midrange Dynamics.

The MDSEC Product provides IT staff a user-friendly means to secure MDCMS, MDOpen, MDXREF and MDWorkflow 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.

Version of guide: 8.6.17 (May 23, 2026)

This guide is comprised of these sections:

- [Terminology](#)
- [Starting MDSEC](#)
- [MDSEC Menu](#)
- [User Roles](#)
- [Application Levels for Role](#)
- [Security Codes for Role](#)
- [Users with Role](#)
- [Users](#)
- [Roles for User](#)
- [Transfer Requests](#)
- [Functional Security Codes](#)
- [Authorization Lists](#)
- [DDM Security](#)
- [MD Command Security](#)
- [Report Generator](#)
- [API Tokens](#)
- [MDUPDUSR command](#)
- [Appendix A - Standard User Roles](#)
- [Appendix B - Security Codes](#)

You can download a PDF version of this guide [here](#).

1.2 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 MDChange functions. Application **md** contains the default and general authorizations for the MD products.

Additionally, an MDSEC application will be created for each MDCMS Application.

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 Promotion level defined for an organization can have certain security functions limited to specific levels for a given user role.

Code

The application code is a security code that represents a function that requires authorization within MDSEC. The full list of codes is available in [Appendix B](#).

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 one of the following: - A profile that exists as an IBM i User Profile on the system - A profile that exists virtually within MDSEC for usage of MDWorkflow - A virtual service profile for tracking transactions.

For a user to have access to the MDChange products, they must be registered in MDSEC. Their ability within the products is then granularly handled by the User Roles that they are members of.

1.3 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 Setup Menu option #8.

A user will only be able to view the current settings in MDSEC unless that user has administrative rights.

Administrative rights are granted when: - the IBM i user profile has either `*SECOPR` authority or `*SECADM` authority and is not explicitly denied MDSEC edit authority for the MDSEC user definition. - The MDSEC user definition for the user has MDSEC Edit Auth parameter set to Y.

1.4 MDSEC Menu

The Main menu for MDSEC.

The menu is available for MDSEC administrators in edit mode and for any other registered users in view mode.

```

SCLMENU                               MD Dev                               27.05.26
SCRN1                                 MDSEC Main Menu                       20:21:45

      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
(C) COPYRIGHT MIDRANGE DYNAMICS 1998, 2026.  Build Date 2026-05-25  v8.6.17

```

Option 1: User Roles Manage the list of User Roles that have functional access to the MDChange products

Option 2: Users Manage the list of user profiles that have functional access to the MDChange products through assignment to user roles

Option 3: Functional Security Codes View/Manage the list of functional security codes

Option 4: Authorization Lists Manage the authorization lists on the system as well as the user rights for users belonging to those lists (administrators only)

Option 5: DDM Security Manage the access rights and logging of DDM (Distributed Data Management) transactions. This option is only available from the default instance of MDSEC (administrators only).

Option 6: MD Command Security Grant or Revoke permissions to execute MD commands that cause updates to MDCMS data or deployments

Option 7: Report Generator Define and Generate a variety of security reports for Users and Roles

Option 8: API Tokens Create REST API tokens to be used for authenticating a REST client when invoking MDChange (MDCMS) REST APIs.

Option 9: License Keys View/Manage the MD Product license keys

Option 11: System Settings Define various system-wide information for this instance of the MD Products.

Option 12: Email Settings Define the SMTP credentials and the list of recipient email addresses

1.5 User Roles

1.5.1 User Roles

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

```

SCCGPD                      T86 Dev/Test                      27.05.26
SCRN1                       MDSEC User Roles                          12:26:14
Filter by
Role ID: MD                 Desc: _____ Appl: _____
                             User: _____      Lvl: _____
                             Code: _____

Type options, press Enter.
A=Authority U=Users 2=Edit 3=Copy 4=Delete 7=Rename

Opt  Role ID      Description                                     Users
├── MD_ADMCMS    MDCMS Administration                             17
├── MD_ADMWF     MDWorkflow Administration                         18
├── MD_ADMXREF   MDXREF Administration                             16
├── MD_PGMR      MDCMS Programmer                                 15
├── MD_PGMRADV  MD Programmer Advanced                           14
├── MD_PGMROPN  MDOpen Programmer                                15
├── MD_PROJAPR  MDCMS Authorize/Approve Involved Projects        19
├── MD_PROJEDT  MDCMS Edit Involved Projects                     18
├── MD_PROJMGR  MDCMS Create/Manage all Projects                 18
├── MD_RFP_SBM  MDCMS RFP Submit                                 22
├── MD_RFPAPR   MDCMS RFP Approve                                19
└── More...

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

Filters

Field	Description
Role ID	Roles with IDs containing the entered string
Desc	Roles with Descriptions containing the entered string
Appl	Roles with authorization to at least one code in the entered application will be listed. Press F4 to select from list of values.
Lvl	Roles with authorization to at least one code in the entered level number will be listed. Press F4 to select from list of values.
Code	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. Press F4 to select from list of values.
User	Roles assigned to the entered user. Press F4 to select from list of values.

Fields

Field	Description
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

Option	Description
A=Authority	View/Edit the applications and codes that the role is authorized to. see Application Levels for Role
U=Users	View/Edit the list of users belonging to the role. see Users with Role
2=Edit	Edit the description for the role
3=Copy	Copy the role to a new role. Optionally copy the authorities and/or the user assignments to the new role.
4=Delete	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

1.5.2 MDSEC Application Levels for Role

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

```

SCCSCD          T86 Dev/Test          27.05.26
SCRN1          MDSEC Application Levels for Role  16:11:11

Role: MD_ADMWF  MDWorkflow Administration

Pos: _____  Filter by Lvl: ___  Desc: _____

Type options, press Enter.
C=Codes  4=Remove from Role  9=Apply to all Registered Levels

Opt  Appl  Lvl  Description  General
     [  md   0   MD Product Global Authorization Codes  Y
     [  APIS 100  API Test/QA Env                        Y
     [  APIS 300  API Production Env                      Y
     [  ASP  500  IASP01 Production                      Y
     [  CLM  100  Claims Base DEV                        Y
     [  CLM 109  Claims September DEV                   Y
     [  CLM 110  Claims October DEV                     Y
     [  CLM 111  Claims November DEV                    N
     [  CLM 112  Claims December DEV                    Y
     [  CLM 300  Claims Base INT                        Y

More...

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

Positioning and Filtering List

Field	Description
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

Field	Description
Appl	An application defined either in MDCMS/MDXREF or "md" for the global codes
Lvl	A level defined either in MDCMS/MDXREF or "0" for the global codes
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

Option	Description
C=Codes	View/Edit the codes for the selected application level that the role is authorized to. See Security Codes for Role
4=Remove from Role	Remove all authorizations for the application level from the role
9=Apply to all Registered Levels	Replace all code authorizations for the Role in all other registered Application Levels with the codes for the selected Level. If using this Option for application "md", only level-specific code authorizations will be applied.

Function Keys

- **F3=Exit** - Return to previous panel
- **F5=Refresh** - Refresh the panel
- **F6=Add** - Add 1 or more Levels to the role. Only levels not already registered for the role will be listed for potential selection. If the Apply md Auth to New Levels property for md is set to Y, then all Level-Specific codes registered in md for the role will be applied to the new roles. Otherwise, only general authority will be applied.

1.5.3 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                T86 Dev/Test                27.05.26
SCRN2                 MDSEC Security Codes for Role 16:31:30

Role....: MD_ADMWF   MDWorkflow 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 Registered Levels

Opt  Code  Description                                     Application
     Code  Description                                     Specific
  _   _   _   _
  _   1   MDXREF General Product Authorization           Y
  _   2   MDCMS  General Product Authorization
  _   12  Email Settings Maintenance
  _   13  Email Address Maintenance
  _   16  Export Output via Email
  _   17  Export Output to IFS
  _   69  Create a Task for any Project
  _   70  Edit Tasks for any Project

                                     More...

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

Positioning and Filtering List

Field	Description
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

Field	Description
Code	An MDSEC Authorization Code securing a particular function. See Appendix B - Security Codes
Description	Description of the code
Application Specific	For application md only: Y - Authorization to the function will be checked against the corresponding MDCMS Promotion level at run-time. This allows a role to have authority to one application level but not another. blank - Authorization to the MDCMS or MDXREF function is checked against md and there is no differentiation amongst the application levels.

Options

Option	Description
4	Remove authorization for the code from the role
9	Apply the code authorization to all other registered levels for the role.

Function Keys

- **F3=Exit** - Return to previous panel
- **F5=Refresh** - Refresh the panel
- **F6=Add** - Add 1 or more Codes to the Level for the role. Only codes not already registered for the role will be listed for potential selection.

1.5.4 Users with Role

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

```

SCCGPD          T86 Dev/Test          27.05.26
SCRN3           Users with Role      17:19:06

Role: MD_RFPSND  MDCMS RFP Send

Pos: _____ Filter by Desc: _____ Ext ID: _____

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

Opt  User ID      Description                               Ext ID
┌    AKUMAR      Ankush Kumar
┌    DVERMA      Devendra Verma
┌    JENKINS     Jenkins Automated Testing User
┌    MARK        Mark Tregear
┌    MMORGAN     Michael Morgan
┌    MMORGANASP Michael Morgan for IASP01
┌    MMORGAN2    Michael Morgan 2nd account
┌    NISHA       Nisha Kanojia
┌    RASHIA      Rashi Argawal
┌    REN         René Unternährer                       Ren
More...

F3=Exit  F5=Refresh  F6=Add

```

Positioning and Filtering List

Field	Description
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

Field	Description
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

Option	Description
U=User Auth	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 1 or more users to the Role
- **F12=Exit** - Return to previous panel

1.6 Users

1.6.1 Users

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

```

SCCUPD                               T86 Dev/Test                               27.05.26
SCRN1                                MDSEC Users                               17:22:47
Filter by
  User ID      Name: _____ Appl/Lvl: _____ Code: _____
              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      Description                    Role ID      Ext ID      GA Act Se
┌─── AKUMAR      Ankush Kumar                    MD_PGMR      +           N  Y  N
┌─── AUCTION     Auction Edge                     SUB          N           N  Y  N
┌─── BARTECH     Bartech                          LIC          N           N  Y  N
┌─── BIZUSER     Business User                    PROJ-USER    N           N  Y  N
┌─── BOB         Bob Anderson                    JUSTRFPAPR   boba@md-na N  Y  N
┌─── BOB2        Bob Anderson                    MD_PROJAPR+  boba2@md-n N  Y  N
┌─── DVERMA      Devendra Verma                  MD_ADMCMS    +           N  Y  N
┌─── ITECHSQL    iTech Solutions                  N           N  Y  N
┌─── JENKINS     Jenkins Automated Testing User MD_PGMRADV+  N  S  N
┌─── MARK        Mark Tregear                    MD_ADMWF     +           N  Y  N
┌─── MARYL       Mary Langen                      B           B  Y  N
More...

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

Filters

Field	Description
User ID	only User IDs containing the entered value
Name	only User Descriptions containing the entered value
Appl	only users with authorization to at least one code in the entered application
Lvl	only users with authorization to at least one code in the entered level number
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

Field	Description
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 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 ***SEC0FR** or ***SECADM** or if the MDSEC Edit Auth flag is set to Y for the user.

Option	Description
R=Roles	View/Edit the list of roles that the user belongs to. see Roles for User
T=Transfer Requests	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. see Transfer Requests
U=User Auth	View all authorities for the user, based on all roles that the user belongs to
2=Edit	Edit the properties for the user. The authorities for the user are edited using option R.
3=Copy	Copy the user to a new user. Optionally copy the role assignments to the new user.
4=Delete	Delete the user from MDSEC
5=View	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.

1.6.2 Roles for User

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

```

SCCUPD          T86 Dev/Test          27.05.26
SCRN3          Roles for User        18:01:26

User: BIZUSER   Business User
Pos: _____ Filter by Desc: _____

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

Opt  Role      Description
├──  PROJ-USER Project User

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

Positioning and Filtering List

Field	Description
Pos	the cursor will be positioned to the closest match in the list
Desc	only roles with descriptions containing the value

Fields

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

Options

Option	Description
A=Authority	View the application levels and codes that the role is authorized to
4=Remove from Role	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

1.6.3 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          T86 Dev/Test          27.05.26
SCRN1          Transfer Requests Owned by User 18:06:07

Change From User.  BIZUSER          Business User
To User.          _____

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

Filters (blank=all)
Application . . .  _____
Level . . . . .  _____
RFP Number . . .  _____
Project . . . . .  _____
Task Number . . .  _____
Subtask Number. .  _____

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

Fields

Field	Description
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                               T86 Dev/Test                               27.05.26
SCRN2                                Level Requests to Transfer                          18:09:08

From User: REN                       René Unternährer
To User: MMORGAN                     Michael Morgan

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] TEST01 100 Y  Y  Y  Y  /home/REN
[S] TEST01 100 Y  Y  Y  Y  /home/REN/TEST01/100
[S] TEST01 100 Y  Y  Y  Y  /www/mdrstt12/specs/cons/REN
[S] TEST01 100 Y  Y  Y  Y  AAAA00001
[S] TEST01 100 Y  Y  Y  Y  AAARE00001
[S] TEST01 100 Y  Y  Y  Y  AAARE00002
[S] TEST01 100 Y  Y  Y  Y  AAARE00003
[S] TEST01 100 Y  Y  Y  Y  AFALA00002
[S] TEST01 100 Y  Y  Y  Y  AFALA00006
[S] TEST01 100 Y  Y  Y  Y  HALLD00001
[S] TEST01 100 Y  Y  Y  Y  MMORGAN

More...

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

```

Options

Option	Description
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: you don't have the authority to change the programmer for that application/level (MDSEC code 32) 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 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.

1.7.3 Options

Option	Description
C=Codes	List the codes defined in the level
P=Properties	View/Edit the properties
U=Users	List all users that have authority to the Application Level

1.7.4 Level Properties

Field	Description
Active	Y = Users authorized to the level or any codes in the level may proceed with functioned secured by those codes. N = All codes for the level are deactivated
Apply md Auth to New Levels	only applicable for the "md" global level Y = When a new promotion Level is created, or when a level is added to a User Role, the authority for the md level for the role will be applied to the new level. N = only general authority to the level will be applied.

1.8 Authorization Lists

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

1.8.1 Authorization List Listing

```

SCCSAL                               T86 Dev/Test                27.05.26
SCRN4                                Authorization Lists          19:40:21

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

Opt List      Description      Default Authority  *PUBLIC Authority
  _  TLIST1    Test Autl 1        *USE              *USE

F3=Exit  F5=Refresh  F6=Add

Bottom

```

Options

Option	Description
2	Edit the properties of the Authorization List
4	Remove the Authorization List from MDSEC and optionally delete the Authorization List from the IBM i system
U	View/Edit the list of users that are members of 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 (and the IBM i system, when new)
- **F12=Exit** - Return to previous panel

1.8.2 Authorization List Properties

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:

Value	Description
*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 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 Y (Yes), then all existing users in the MDSEC User List will obtain the new default authority within the specific Authorization List.

1.8.3 Authorization List Users

Options

Option	Description
4	The "Remove from List" option will remove the user from the IBM i Authorization List. The user's authority to objects secured by the list will be limited to *PUBLIC authority.

Object Authority Values

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

1.8.4 3 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

1.9 DDM Security

1.9.1 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.

1.9.2 General Configuration

Option 5 from MDSEC Menu: DDM Security.

1.9.3 Configuration Options

DDM Filter

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

When option 1 (MDSEC DDM) is used, the following additional parameters are available:

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 - those transactions will not be included.

Allow Remote Commands

Y - Commands sent from a remote system via DDM are allowed.

N - Not allowed.

Allow DRDA (SQL)

Y - Remote SQL clients using Application Requester Driver (ARD) programs are allowed access to the local database.

N - Not allowed.

1.9.4 Function Keys

F3=Exit

Return to previous panel

F7=Data Filters

Manage the list of Database objects can be accessed using DDM.

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 specifically.

Usage

Value	Description
*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.

F9=User Filters

Manage the list of local User Profiles that may be used to connect to the Database using DDM

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.

User

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

F21=Sys Command

1.10 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                               T86 Dev/Test                               27.05.26
SCRN1                                  Secured MD Commands                               19:52:21

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                 *ALLSEC
┌ MDADDREQ       MDCMS       Add Object Request                           *ALLSEC
┌ MDADDSOG       MDCMS       Add Send Object Group                        *ALL
┌ MDADDSRQ       MDCMS       Add Send Object Request                      *ALL
┌ MDAPRRFP       MDCMS       Approve RFPs                                *ALLSEC
┌ MDAPRTMP       MDCMS       Maintain Approval Templates                 *ALLSEC
┌ MDAPRTMPO      MDCMS       Approval Template Objects                  *ALLSEC
┌ MDCLEAR        MDCMS       Clear ALL MDCMS Activity                    *ALL
┌ MDCLESSND      MDCMS       Close RFPs in Send List                     *ALLSEC
┌ MDCPYDATA      MDCMS       Copy Data between Libraries                 *ALL
┌ MDCRTOBJ       MDCMS       Create Object in Dev Library                *ALL
┌ MDCRTSCO       MDCMS       Create Send RFP w Changed Objs             *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.

1.10.1 User Special Values

Value	Description
*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

1.11 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                               T86 Dev/Test                               27.05.26
SCRN1                                MDSEC Report Generator                          19:58:39

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

                                     6=Role Assignment History
                                     7=Role Authority History
                                     8=User Authority History

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. To be able to reuse or schedule a report definition, Press F9=Save Def on the Report Criteria Screen to save the definition with a specific name for the definition.

1.11.1 Reports

- 1 - Role Authority** A list of User Roles and the Functional Security codes that are granted to those roles. This report is grouped by User Role or by Security Code.
- 2 - User Authority** A list of Users and the Functional Security codes that are granted to those users via their membership in 1 or more User Roles. This report is grouped by User or by Security Code.
- 3 - Users With Role** A list of User Roles and the users assigned to each role. This report is grouped by Role.
- 4 - Role Authority** A list of Users and the User Roles that they belong to. This report is grouped by User.
- 6 - Role Assignment History** An audit log of any changes to User Assignment for Roles.
- 7 - Role Authority History** An audit log of any changes to Authority granted to User Roles.
- 8 - User Authority History** An audit log of any changes to Authority granted to Users.

1.11.2 Function Keys

- **F3=Exit** - Return to previous panel
- **Enter=Confirm** - Confirm selection of the report and continue to the Criteria screen
- **F7=Load Def** - Load a saved Report Definition
- **F11=View Output** - Work with MD Output

1.11.3 Criteria Selection

The following is the complete list of possible criteria fields. Only criteria applicable for the selected report will be displayed.

Field	Description
Include Role/User Desc	Y - include the column for the Role or User Description in the report. N - do not include.
Include Level Desc	Y - include the column Level 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 Level/Code is the primary sort for the report. N - the Role or User is the primary sort for the report.
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 Date	For History Reports, Limit rows to transactions occurring on or after given date. See special values below for other options.
Maximum Date	For History Reports, Limit rows to transactions occurring on or before given date. Leave blank if using a special option for the Minimum Date

Special Values for History Report Date Range

- *CM - current Month
- *CW - current Month
- *CY - current Month
- *PM - prior Month
- *PW - prior Week
- *PY - prior Year

1.12 API Tokens

1.12.1 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.

1.12.2 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 a token:

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 it in a secure location. It will not be possible to view the value of the token again.

1.12.3 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.

To manage existing tokens:

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.

1.12.4 Example Request Header

```
Authorization: Bearer MTgzNTg1NDIxMDA1MzkxNzIyOTYzMTA3Mjk3O3U2Nzg5ODAxNDY2NTAyNzMxMTY1
```

1.13 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`.

1.13.1 Restrictions

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

1.13.2 Parameters

PARAM	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 CCSID 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. *NO - The user is deactivated in MDSEC.
GRPA	Use Group Auth	5	Specifies if authority for the user should be based on the authority permitted for the primary group that the user belongs to. *SAME - Don't update the Use Group Auth flag. If for a new user, the flag will be set to *NO . *YES - The user's authority is based solely on the authority permitted for the primary group. *NO - The user's authority is based solely on the authority permitted for the user themselves. *BOTH - The user's authority is based on the combination of the authority for the group and the specific user.
CURA	Use Current User Auth	5	Specifies if authority for the current user is allowed to be used if the job user isn't authorized to a function. *SAME - Don't update the flag. If for a new user, the flag will be set to *NO . *YES - Current User authority checking is permitted in MDSEC. *NO - Current User authority checking is not permitted.
CCSID	CCSID Override	5	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. *SAME - Don't update the CCSID Override value. Will be ignored for a new user. *NONE - remove the CCSID Override value, if currently defined.
ADDROLE	Add Role	10	The list of up to 20 MDSEC authority roles that should be granted to the user. *ALL - Grant every defined role to the user.
RMVROLE	Remove Role	10	The list of up to 20 MDSEC authority roles that should be revoked for the user. *ALL - remove the user from every role that they currently belong to.
ENV	Environment ID	5	Specifies the MDCMS environment that the Project exists in. The ID correlates to the suffix of the MDCMS library name. *DFT - The default environment will be used (library MDCMS). *SAME - The environment of the current library list will be used.

1.14 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; 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	Confirm RFP Test Acceptance/Rejection; Comment on any Project; View any Project; Edit any Project; Authorize any Project; Approve any Project; Create Tasks for any Project; Edit any Task; Edit any Subtask.
MD_PROJAPR	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.
MD_PROJEDA	Edit any Project; Comment on any Project; Create Tasks for any Project; Edit any Task.
MD_PROJEDT	Edit involved Projects; Comment on involved Projects; Create Tasks for involved Projects; Edit any Task for involved Projects.
MD_PROJMGR	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.
MD_RFP_SBM	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.
MD_RFPAPR	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.
MD_RFPINS	Create and Edit RFPs; 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

1.15 Appendix B – MD Product Security Codes

1.15.1 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. 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.

1.15.2 Security Codes

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
4	Y	Manage Application Promotion Levels in MDCMS
5	Y	Manage MDCMS Attributes
6	Y	Manage Attribute and *RFP Commands or Scripts
7	N	Manage MDCMS Templates (except Object Approval or Data Copy 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
22	N	Manage Object Approval Templates
23	Y	Assign Object to Object Approval Template
24	N	Manage Data Copy Templates
25	N	Execute the Copy of Data via Data Copy Templates
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

Code	Appl Specific	Description
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"

Code	Appl Specific	Description
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
93	N	Edit MDTest Definitions
94	N	Manually Run MDTest Definitions