

JD Edwards World

Table of Contents

1. [Review and lock down user profiles.](#)
2. [Lock down cost center access](#)
3. [Restrict add, change or delete of records](#)
4. [Lock down new employee setup](#)
5. [Lock down menu items](#)
6. [Lock down payroll access - Separating production files.](#)
7. [Lock down Menu Travel](#)
8. [Originators should not be an approver.](#)
9. [Search Type Security](#)
10. [An approver should not have access to change, delete or add purchase orders.](#)
11. [User Information Revisions - Output Queue](#)
12. [User Information Revisions - Initial Menu](#)
13. [User Information Revisions - Fast Path](#)
14. [User Information Revisions - Command Entry](#)
15. [User Information Revisions - Future Mask \(F\)](#)
16. [User Information Revisions - Departmental Mask \(DP\)](#)
17. [User Information Revisions - Knowledge Mask \(K\)](#)
18. [User Information Revisions - Job Mask \(J\)](#)
19. [User Information Revisions - Authorization Mask \(A\)](#)
20. [Approval Delegation](#)

1. Review and lock down user profiles.

User profiles is the first and most important step of securing users. It holds numerous capabilities. These following five security settings are part of what Oracle is calling menu masking and key settings within JDE World. Menu masking allows us to secure access to menus and menu selections.

Menu Masking Types:

- A = Authorization Mask
- J = Job Mask
- K = Knowledge Mask
- DP = Departmental Mask
- F = Future Mask

All of the menu masking types (Authorization Mask, Job Mask, Knowledge Mask, Departmental Mask and Future Mask) are working in conjunction. If on test fails access is denied.

Another set of controls are listed below. Users are not longer restricted to their menu options instead of they are able to roam freely within the menu system. Just enter the name of the menu in command line.

While the security settings listed above are still in place and enforced the settings below will not increase user access but they carry a high risk if security settings are not properly in place.

- Allow Command Entry
- Allow Menu Traveling
- Allow Fast Path

All settings above will be explained in more detail.

MAINOPTIONS

Compliance: Privacy

Control Type: Access Control, Configuration, Segregation of Duties, Business Continuity

Applications: Address Book, Procurement, Approvals, Payroll, JDE Security

Operating System: OS/400 V5R4

Platform: IBM iSeries

Security: High

Product Version: A7.3 Cume16

2. Lock down cost center access

Employees should only have access to their dedicated cost center.No entries mean that the user has access to all business units.

MAINOPTIONS

Control Type: Access Control, Configuration

Applications: JDE Security

Operating System: OS/400 V5R4

Platform: IBM iSeries

Security: High

3. Restrict add, change or delete of records

Action Code Security allows/disallows users from performing certain actions (Add, Change or Delete). The default action is view only.

MAINOPTIONS

Control Type: Access Control, Configuration, Segregation of Duties
Applications: JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16

4. Lock down new employee setup

Only assigned employees should have the capability to setup new employees.

MAINOPTIONS

Control Type: Access Control, Segregation of Duties
Applications: Payroll, JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16

5. Lock down menu items

Menu items can be locked down via menu security. It prevents users from executing programs.

MAINOPTIONS

Control Type: Access Control, Configuration, Segregation of Duties
Applications: JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Product Version: A7.3 Cume16

6. Lock down payroll access - Separating production files.

Restricting payroll access can be accomplished by having your production files divided into two or more libraries instead of one.

Example:

1. Production library called Payroll: Contains all payroll files

2. Production library called Others: Contains all other files

Utilizing the library list concept of the iSeries to allow/disallow access to payroll files.

Library list: Payroll Access allowed

1. Library x
2. Library y
3. Library z
4. Library: Payroll
5. Library: Others

Library list: Payroll access disallowed:

1. Library x
2. Library y
3. Library z
4. Library: Others

Because a library list will be assigned to the user profile you are able to restrict access at an early phase. Programs opened by the user will search the library list from the top down until the file is found requested by the program. If the file isn't found the program will generate an error.

MAINOPTIONS

Control Type: Access Control, Configuration
Applications: Payroll, JDE Security, IBM Security
Operating System: OS/400 V5R4
Security: High
Product Version: A7.3 Cume16

7. Lock down Menu Travel

Menu travel allows you to access a menu directly without going thru the menu system. Users appreciate menu travel but if your menus are not properly secured it increases the risk of unauthorized access.

blank = Indicates the user is allowed to menu travel.
Y = Indicates the user is allowed to menu travel.
N = Indicates the user is NOT allowed to menu travel.

MAINOPTIONS

Compliance: Privacy
Control Type: Authentication, Access Control, Configuration, Segregation of Duties
Applications: JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16

8. Originators should not be an approver.

An originator of a purchase order should not be the approver.

The program Approval Level Revisions is setting up approvers and the amount they are able to approve. Action Code Security secures users with add, change and delete access of purchase orders . By default Action Code Security should be set to *public with add, change and delete = N.

MAINOPTIONS

Control Type: Access Control, Segregation of Duties

Applications: Procurement, Approvals

Operating System: OS/400 V5R4

Platform: IBM iSeries

Security: Medium

Product Version: A7.3 Cume16

9. Search Type Security

Access to the address book can be limited through search type security. The search types are coded within the address book. If you assign only certain search types to users you are able to limit access.

Example of search types:

Search type C = Customer, V = Vendor, E = Employee, O = Others, F = Facilities, I = Investors

MAINOPTIONS

Compliance: Privacy

Control Type: Access Control, Segregation of Duties

Applications: Address Book, JDE Security

Operating System: OS/400 V5R4

Platform: IBM iSeries

Security: Medium

Product Version: A7.3 Cume16

10. An approver should not have access to change, delete or add purchase orders.

An approver shouldn't be able to change any purchase orders. Changes should be made by the originator only.

The program Approval Level Revisions is setting up approvers and the amount they are able to approve.

Action Code Security secures users with add, change and delete access of purchase orders . By default Action Code Security should be set to *public with add, change and delete = N.

MAINOPTIONS

Control Type: Access Control, Segregation of Duties

Applications: Procurement, Approvals, JDE Security

Operating System: OS/400 V5R4

Platform: IBM iSeries

Security: High

11. User Information Revisions - Output Queue

The output queue determines where all reports are going to print to. If the field is left blank, most likely it will go to the queue defined in your iSeries profile (QPRINT).

Think about critical payroll data you don't want to be exposed. Instead of printing to the default queue like everybody else does, print to your payroll queue. Exposure is limited because Payroll Personnel have access to payroll data per default.

MAINOPTIONS

Compliance: Privacy
Control Type: Access Control, Configuration, Segregation of Duties
Applications: Payroll, JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16

12. User Information Revisions - Initial Menu

It doesn't look like as security feature but it is one. Think about if you would like to lock down a user or group of users to a certain menu.

REFERENCE

MAINOPTIONS

Compliance: Privacy
Control Type: Access Control, Configuration, Segregation of Duties
Applications: JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: Medium
Product Version: A7.3 Cume16

13. User Information Revisions - Fast Path

Fast Path is similar to shortcuts. They allow you to access menus or execute programs depends on the assigned action. Please review the Fast Path UDC table to be aware what has been assigned to a fast path.
blank = Indicates the user is allowed to use fast path.Y = Indicates the user is allowed to use fast path.N = Indicates the user is NOT allowed to use fast path.

MAINOPTIONS

Compliance: Privacy

Control Type: Authentication, Access Control, Configuration, Segregation of Duties
Applications: JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16

14. User Information Revisions - Command Entry

The Command entry option is very helpful if you have to maneuver around. You are able to leave the menu system and execute operation system commands. blank = Indicates the user has command entry
Y = Indicates the user has command entry. N = Indicates the user doesn't have command entry.

MAINOPTIONS

Compliance: Privacy
Control Type: Authentication, Access Control, Configuration, Segregation of Duties
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16

15. User Information Revisions - Future Mask (F)

In order to gain access to menus and menu selection you have to have the proper rights. Future masking is one of the key elements. Possible entries are any letters or numbers. If the field is empty no security has been set. A "*" as an entry stands for access to all levels. Future mask isn't setup hierarchical like the authorization mask the setting has to match. That means, if you have a future mask level of B, you have only access to all menus and selections coded with B and empty settings as well. . All of the menu masking types (Authorization Mask, Job Mask, Knowledge Mask, Departmental Mask and Future Mask) are working in conjunction. If on test fails access is denied. Example: Menu Departmental
maskingMenu Budget BMenu Employee Setup emptyMenu Accounts
Receivable empty User Departmental maskingJohn Doe
emptyRoger Wolters B Based on the user and menu settings:John Doe
has access to the Employee Setup and Accounts Receivable menu.Roger Wolters has access to the Employee Setup, Accounts Receivable and Payroll menu.

MAINOPTIONS

Compliance: Privacy
Control Type: Authentication, Access Control, Configuration, Segregation of Duties, Business Continuity
Applications: Address Book, Approvals, JDE Security
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16

16. User Information Revisions - Departmental Mask (DP)

In order to gain access to menus and menu selection you have to have the proper rights. Departmental masking is one of the key elements. Possible entries are any letter and number combination. If the field is empty no security has been set. A '*' as an entry stands for access to all levels. Departmental mask isn't setup hierarchical like the authorization mask the setting has to match. That means, if you have a departmental level of TR. You have only access to all menus and selections coded with TR and empty settings as well. All of the menu masking types (Authorization Mask, Job Mask, Knowledge Mask, Departmental Mask and Future Mask) are working in conjunction. If on test fails access is denied. Example:

Menu	Departmental masking	Menu Tax Records	TRMenu
Employee Setup	empty	Menu Accounts Receivable	empty User
Departmental masking	John Doe	empty	Roger Wolters

TR Based on the user and menu settings: John Doe has access to the Employee Setup and Accounts Receivable menu. Roger Wolters has access to the Employee Setup, Accounts Receivable and Payroll menu.

MAINOPTIONS

Compliance: Privacy
 Control Type: Authentication, Access Control, Configuration, Segregation of Duties, Business Continuity
 Applications: Address Book, Approvals, JDE Security
 Operating System: OS/400 V5R4
 Platform: IBM iSeries
 Security: High
 Product Version: A7.3 Cume16

17. User Information Revisions - Knowledge Mask (K)

In order to gain access to menus and menu selections you have to have the proper rights. Knowledge masking is one of the key elements. A blank represents the highest level of authority. A through Z are the next levels, then 0 through 9. Exception: A '*' as a knowledge mask stands for access to all levels. That means, if you have a knowledge mask level of 4. You have access to all menus and selections coded with 4, 5,6,7,8, and 9. All of the menu masking types (Authorization Mask, Job Mask, Knowledge Mask, Departmental Mask and Future Mask) are working in conjunction. If on test fails access is denied. Example:

Menu	Knowledge masking	Menu Payroll	2Menu
Employee Setup	empty	Menu Accounts Receivable	empty User
Knowledge masking	John Doe	empty	Roger Wolters

2 Based on the user and menu settings: John Doe has access to the Employee Setup and Accounts Receivable menu. Roger Wolters has access to the Employee Setup, Accounts Receivable and Payroll menu.

MAINOPTIONS

Compliance: Privacy
 Control Type: Authentication, Access Control, Configuration, Segregation of Duties, Business Continuity
 Applications: Address Book, Approvals, JDE Security
 Operating System: OS/400 V5R4
 Platform: IBM iSeries
 Security: High
 Product Version: A7.3 Cume16

18. User Information Revisions - Job Mask (J)

In order to gain access to menus and menu selections you have to have the proper rights. Job masking is one of the key elements. Possible levels are A through Z, then 0 through 9. Exception: A '*' means the user has

access to all levels. Job masking isn't setup hierarchical like the authorization mask the setting has to match. That means, if you have a job level of E. You have only access to all menus and selections coded with E and empty settings as well. All of the menu masking types (Authorization Mask, Job Mask, Knowledge Mask, Departmental Mask and Future Mask) are working in conjunction. If on test fails access is denied. Example:

Menu	Job masking	Menu Payroll	E
Setup	empty	Menu Accounts Receivable	empty
User settings	John Doe	empty	Roger Wolters

E Based on the user and menu settings: John Doe has access to the Employee Setup and Accounts Receivable menu. Roger Wolters has access to the Employee Setup, Accounts Receivable and Payroll menu.

MAINOPTIONS

Compliance: Privacy
 Control Type: Authentication, Access Control, Configuration, Segregation of Duties, Business Continuity
 Applications: Address Book, Approvals, JDE Security
 Operating System: OS/400 V5R4
 Platform: IBM iSeries
 Security: High
 Product Version: A7.3 Cume16

19. User Information Revisions - Authorization Mask (A)

In order to gain access to menus and menu selections you have to have the proper rights. Authorization masking is one of the key elements. A blank represents the highest level of authority. A through Z are the next levels, then 0 through 9. If a user has '*' as an authorization level the user has access to all levels. That means, if you have an authorization level of 4 you have access to all menus and selections coded with 4, 5,6,7,8, and 9. All of the menu masking types (Authorization Mask, Job Mask, Knowledge Mask, Departmental Mask and Future Mask) are working in conjunction. If on test fails access is denied. Example:

Menu	Authorization setting	Menu Payroll	4
Employee Setup	5	Menu Accounts Receivable	6
User setting	John Doe	5	Roger Wolters

4 Based on the user and menu settings: John Doe has access to the Employee Setup and Accounts Receivable menu. Roger Wolters has access to the Employee Setup, Accounts Receivable and Payroll menu

MAINOPTIONS

Compliance: Privacy
 Control Type: Authentication, Access Control, Configuration, Segregation of Duties, Business Continuity
 Applications: Address Book, Approvals, Payroll, JDE Security
 Operating System: OS/400 V5R4
 Platform: IBM iSeries
 Security: High
 Product Version: A7.3 Cume16

20. Approval Delegation

Some instances require that an approver has to delegate the authority to approve purchase orders. The delegation process is fairly simple, but generates issues:

1. Is the new approver also an originator?
2. Has somebody initiated the delegation process without proper authorization?
3. Has somebody initiated the delegation process and rolled it back after the order has been approved?

Another drawback is, that the process cannot be controlled by Action Code Security.
Only a controlled number of users should have access to initiate the delegation process.

MAINOPTIONS

Compliance: S-OX
Control Type: Access Control
Applications: Procurement, Approvals
Operating System: OS/400 V5R4
Platform: IBM iSeries
Security: High
Product Version: A7.3 Cume16
