Inclusive Vs Exclusive Row Security

Row security is used by JD Edwards to limit the ability of users to add, update or delete data as well as to limit the ability to view records.

It allows the definition of valid ranges of values in the F00950 Security Table so the user (or role or *group) of those security records has access to only records within that range.

- Inclusive Row Security allows the definition of valid ranges of values in the F00950 that can be accessed.
- Exclusive row security allows the definition of ranges of values in the F00950 that cannot be accessed.

At a system level, the decision must be made to use either inclusive or exclusive row security. They cannot be used in combination.

- Inclusive Row Security has been available in all JD Edwards versions for many years starting with Service Pack 16.
    - Prior to this Service Pack level, only exclusive row security was available – this is why many sites still use exclusive row security.
- To set inclusive row security you need to create a record in F00950 where the user is 'EXCLUSIVE' and the field FSATN3 is set to '1'.
    - If either no record exists, or the flag is set to '0' the security will be exclusive.
    - A form exists to do this within ALLOut software, later versions of JD Edwards or you can use SQL.

How Does Row Security Work?

Row security affects the ability to view, add, change and delete data. However the simplest explanation is as follows:

- When a user presses FIND from within a JD Edwards screen or in any other way reads records from the database, if any relevant row security exists, the system will add a 'WHERE' clause to the SQL statement it generates to restrict the retrieval of data from the database.

- When exclusive security is effective, JD Edwards uses the records where the 'view' flag is set to 'N'. When inclusive security is effective, JD Edwards does the opposite and applies the records where the 'view' flag is set to 'Y'.
- This means that many records that are set up in your system may never actually be used.

Rules governing complex scenarios - for example, what happens if you use exclusive security but all the records have View = 'Y', are set out in the first appendix of this document.

Advantages of Inclusive

Performance

Depending on security setup, inclusive row security can increase performance over exclusive row security.

- The reason for the performance increase is due to the select and update statements that are generated by the middleware.
  - Performance can be improved when the use of inclusive row security results in a smaller range of valid values rather than a larger range of secured values applied using exclusive row security.

Simplicity

The primary advantage is simplicity of maintenance – it is far simpler to maintain valid ranges than it is to maintain secured ranges.

- The consensus amongst the JD Edwards community is that is always better to implement inclusive security rather than exclusive security; therefore whereas many companies choose to migrate away from exclusive, there is no movement in the opposite direction.
- It is a lot easier to merge valid ranges than it is to merge secured ranges. (For example, if you merge the security of 2 roles that deny access to different companies, the result will be no access to either company.)

Do you need 3rd Party Software or Services?

It is a very simple process to activate inclusive security that does not require any special knowledge. Changing the actual flag that controls your row security from 'exclusive' to 'inclusive' (or indeed vice versa) takes seconds.

However, you will need to convert the actual ranges of your data from 'exclusive' to 'inclusive'.

- This can be done either manually or you can use AL LOut Security's exclusive conversion program.
  - This takes minutes to run and you can see exactly how it will work using the proof mode.
  - It comes with full installation and usage support so making the realistic application of inclusive row security a maximum of one day's work.
  - It is realistically priced to provide value to clients needing to convert large numbers of row security records.
  - The software has been tried and tested at many ALLOut clients. References are available.

Appendix 1: Example

In the examples below user JOHNDOE should be able to view records in the Address Book table (F0101) with a business unit value between 1 to 20 and between 51 to 70. However, the user should only be allowed to update records in the Address Book table with a business unit value between 1 to 20.

How does Inclusive Work?

If inclusive row security is set, only the records in blue (View= 'Y') would be used by JD Edwards, the records in red (View= 'N') would simply be ignored.

User	Table	Data Item	From Value	Thru Value	Add	Chg	Dlt	View
JOHNDOE	F0101	CostCenter	1	20	Y	Y	Y	Y
JOHNDOE	F0101	CostCenter	21	50	N	N	N	N
JOHNDOE	F0101	CostCenter	51	70	N	N	N	Y
JOHNDOE	F0101	CostCenter	71	ZZZZZZ	N	N	N	N

- Selects performed against the F0101 table would look like:

  - SELECT * FROM TESTDTA.F0101 WHERE (ABMCU BETWEEN '1' AND '20' OR ABMCU BETWEEN '51' AND '70')

- Updates on the F0101 (in this example changing JOHNDOE's cost center) would look like:

  - UPDATE TESTDTA.F0101 SET ABMCU = '60' WHERE (ABAN8 = 12345) AND (ABMCU BETWEEN '1' AND '20')

How does Exclusive Work?

If exclusive row security is set, only the records in blue (View= 'N') would be used by JD Edwards, the records in red (View= 'Y') would simply be ignored – unless the 'Add', 'Change' or 'Delete' flags are used.

User	Table	Data Item	From Value	Thru Value	Add	Chg	Dlt	View
JOHNDOE	F0101	CostCenter	1	20	Y	Y	Y	Y
JOHNDOE	F0101	CostCenter	21	50	N	N	N	N
JOHNDOE	F0101	CostCenter	51	70	N	N	N	Y
JOHNDOE	F0101	CostCenter	71	ZZZZZZ	N	N	N	N

- Selects performed against the F0101 table would look like:

  o SELECT * FROM TESTDTA.F0101 WHERE (ABMCU NOT BETWEEN '21' AND '50' AND ABMCU NOT BETWEEN '71' AND 'ZZZZZZ')

- Updates on the F0101 (in this example changing JOHNDOE's cost center) would look like:

  o UPDATE TESTDTA.F0101 SET ABMCU = '60' WHERE (ABAN8 = 12345) AND (ABMCU NOT BETWEEN '21' AND '50' AND ABMCU NOT BETWEEN '51' AND '70' AND ABMCU NOT BETWEEN '71' AND 'ZZZZZZ')

Appendix 2: Rules Governing Complex Scenarios

All scenarios apply to records being effective for the single user, *group or role.

In Exclusive mode

- Question: If no exclusive records exist (where the View flag = 'N'), are inclusive records (where the View flag = 'Y') used by JD Edwards when fetching records?

  o Answer: The inclusive records are ignored and all records are returned by select statements.

- Question: Does JD Edwards use the ACD flags if the View flag is set to 'Y'?:

  o Answer: The ACD of the inclusive record is still effective.

- Question: How does JD Edwards handle ACD conflicts within overlapping ranges?:

  o Answer: If you have 2 records both showing View = Y with overlapping ranges where one record allows ACD and one record prevents ACD – the N flags will be those used.

- Question: If no exclusive records exist (where the View flag = 'N') does JD Edwards look further within hierarchy (i.e. next role/*group etc) to find security?
  - Answer: Even if only inclusive records exist (where the View flag = 'Y') JD Edwards still does not look further within the security hierarchy for additional security records.

In Inclusive mode

- Question: If no inclusive records exist (where the View flag = 'Y'), are exclusive records (where the View flag = 'N') used by JD Edwards when fetching records?
  - Answer: JDE will output messages as below and <u>no</u> records are returned by select statements.

    Jan 26 14:44:10.500 – 9168/6288 Inclusive Insert Row security disabled for USER JOHNDOE on TABLE F0006 because COLUMN MCMCU did not have a F00950 Y entry
    Jan 26 14:44:15.484 – 9168/6288 JDB9900409 – Inclusive Row Level Security Violation: JOHNDOE attempted a SELECT in table F0006

- Question: Does JD Edwards use the ACD flags if the View flag is set to 'N'?:
  - Answer: The ACD of the exclusive record will not be used because only records with View = 'Y' are used.

- Question: How does JDE handle ACD conflicts within overlapping ranges?:
  - Answer: If you have 2 records both showing View = Y with overlapping ranges where one record allows ACD and one record prevents ACD – the <u>Y</u> flags will be those used.

- Question: If no inclusive records exist (where the View flag = 'Y') does JD Edwards look further within hierarchy (i.e. next role/*group etc) to find security?
  - Answer: Even if only exclusive records exist (where the View flag = 'N') JD Edwards still does not look further within the security hierarchy for additional security records.