ALLOut Security

Introduction to JD Edwards EnterpriseOne Security Fundamentals

WHITEPAPER

Contents

03 About ALLOut

04 Abstract & Scope

05 Introduction

07 'Open' OR 'Closed'

09 Program Security

12 Data Security

14 UDO Security

16 System Security

17 Security Hierarchy

19 Security Cache

20 Conclusion

About ALLOut

Who we are

ALLOut is the market-leading security solution for JD Edwards, bringing you the enhanced functionality you need, directly in your E1 or World environment. It's easy to install! There's no need to work with your data outside of JD Edwards, reducing risk & allowing you to maximize existing ERP resource without the need for your team to learn a new system.

Our mission

Our mission is to deliver simple security, streamlined processes & auditable reporting. We believe in providing cost-effective solutions to simply secure and protect organizations against emerging risks. We're the market-leading security, audit & compliance toolset for JD Edwards.

Abstract & Scope

Abstract
JD Edwards EnterpriseOne has been around for many years under many different names. Over time, it has seen significant improvement in application functionality as well as in technical capabilities. The basics of security, however, have not changed over time although additional security types have been added and new concepts have been introduced.

Scope
This document is intended as a high-level overview of the concepts, processes, and options available within the EnterpriseOne product.

Not all concepts or security types are applicable to all releases of the software. The information presented here is based on ALLOut's extensive experience with EnterpriseOne as well as Oracle's published guides. This document is NOT intended to be used as a guide for the planning and implementation of security in your implementation, nor is it guaranteed to cover all types of security available within EnterpriseOne for all versions of JD Edwards. For detailed advice and guidance please contact info@alloutsecurity.com.

We're dedicated to security and compliance, making protecting your business our only mission.

Introduction

Security 'Levels'
Within JD Edwards, security records can exist at multiple “levels” within the table. Security can be applied automatically to all users by utilizing *PUBLIC, a unique role within the system. You can also have security records affect a group of users by assigning records to a role, which is then applied to users. Lastly, you can apply security to individual users of the system.

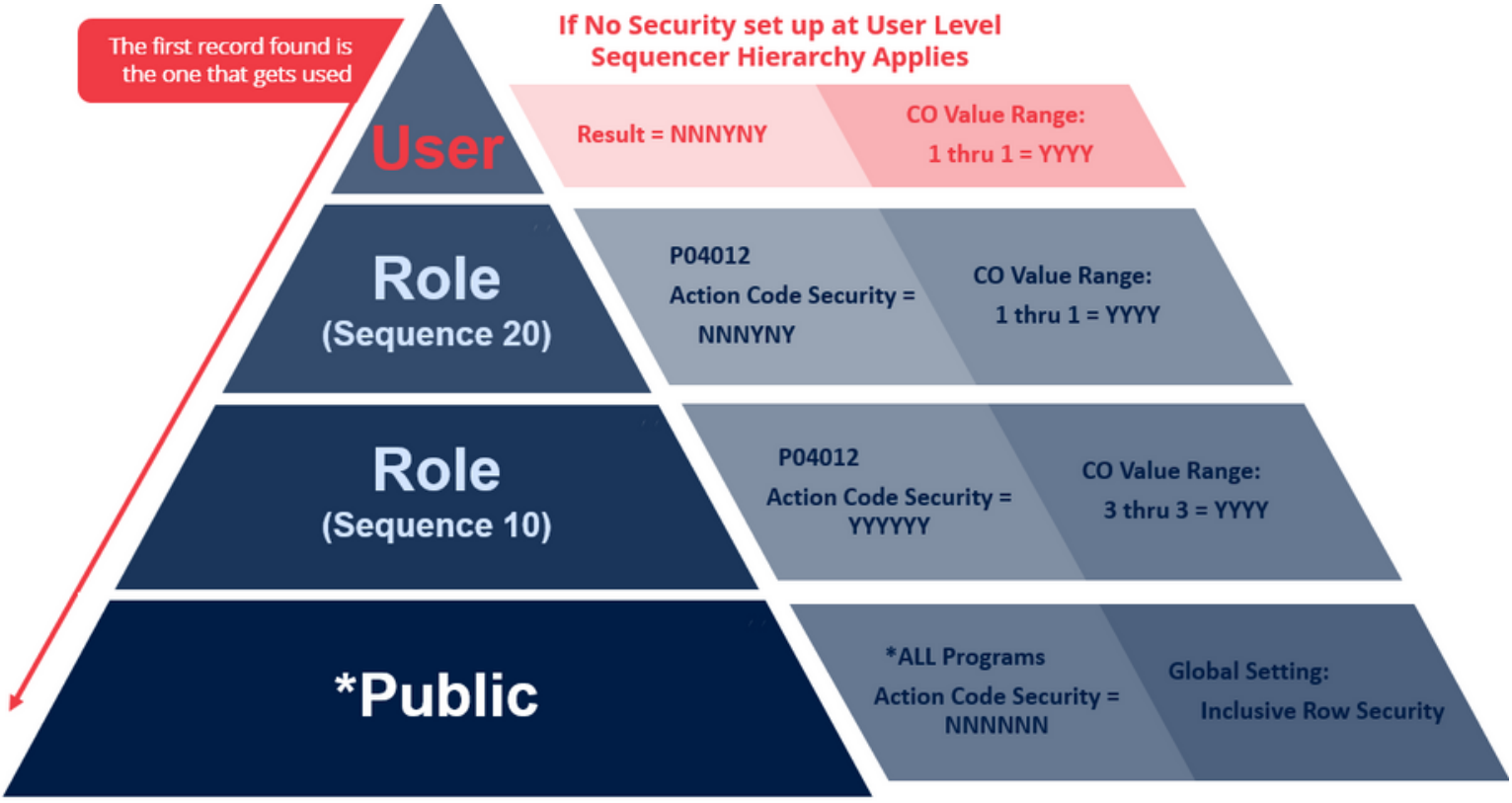
This sequence of applying security records is known as the JDE security ‘hierarchy’.

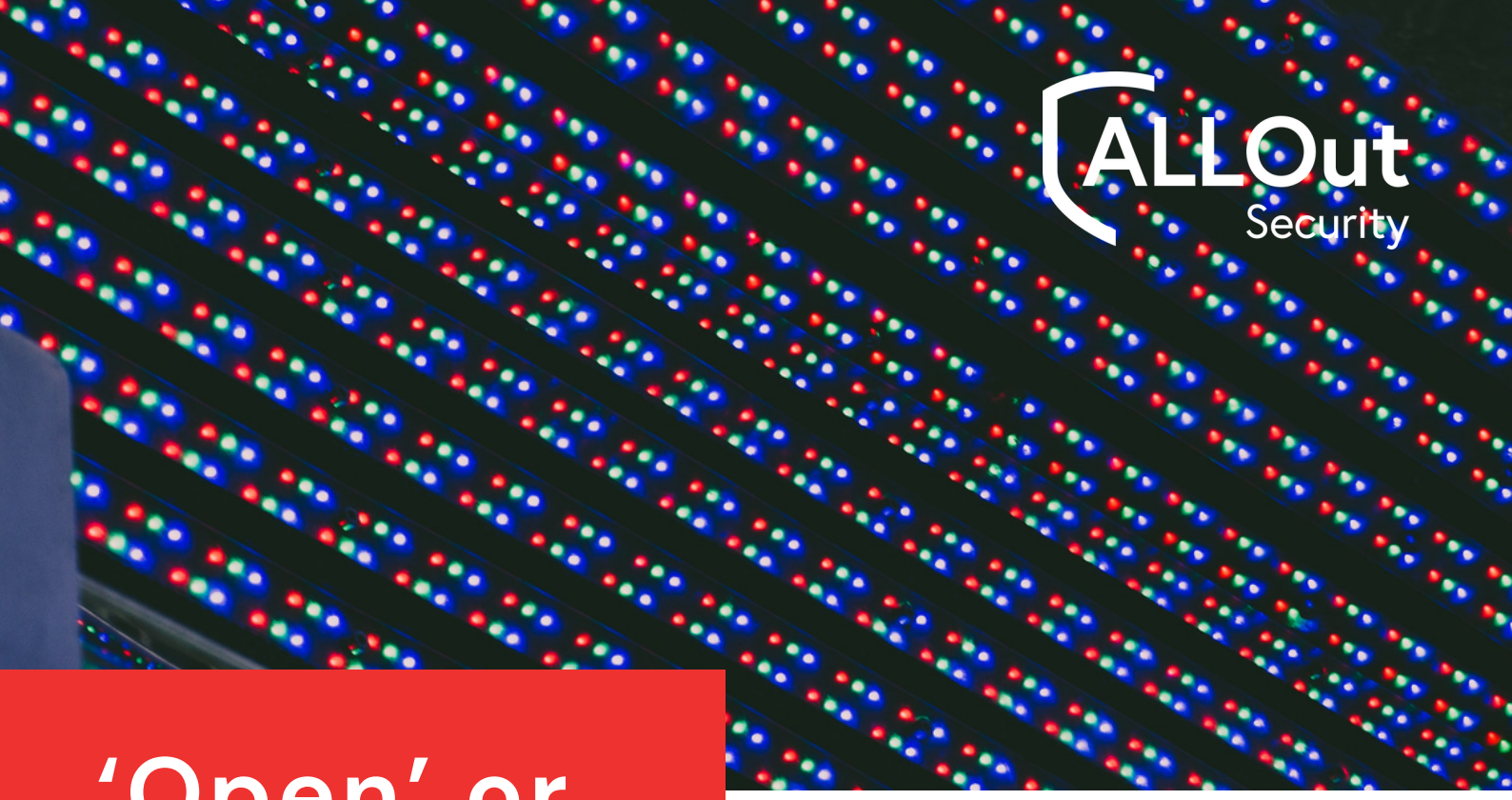
To interpret the security at the various levels, the system uses the following steps in sequence:

- JD Edwards checks security records at the user level first.
- Then, if there are no records for the specific action being attempted, JD Edwards will then look for security at the role level (for all roles the user has been assigned, starting with the highest sequence role in the hierarchy. See the hierarchy section for more details).
- Lastly, if there are still no applicable records JD Edwards will finally check for security at the *PUBLIC level.

The JDE Security Hierarchy

This sequence of applying security records is known as the JDE security 'hierarchy'.





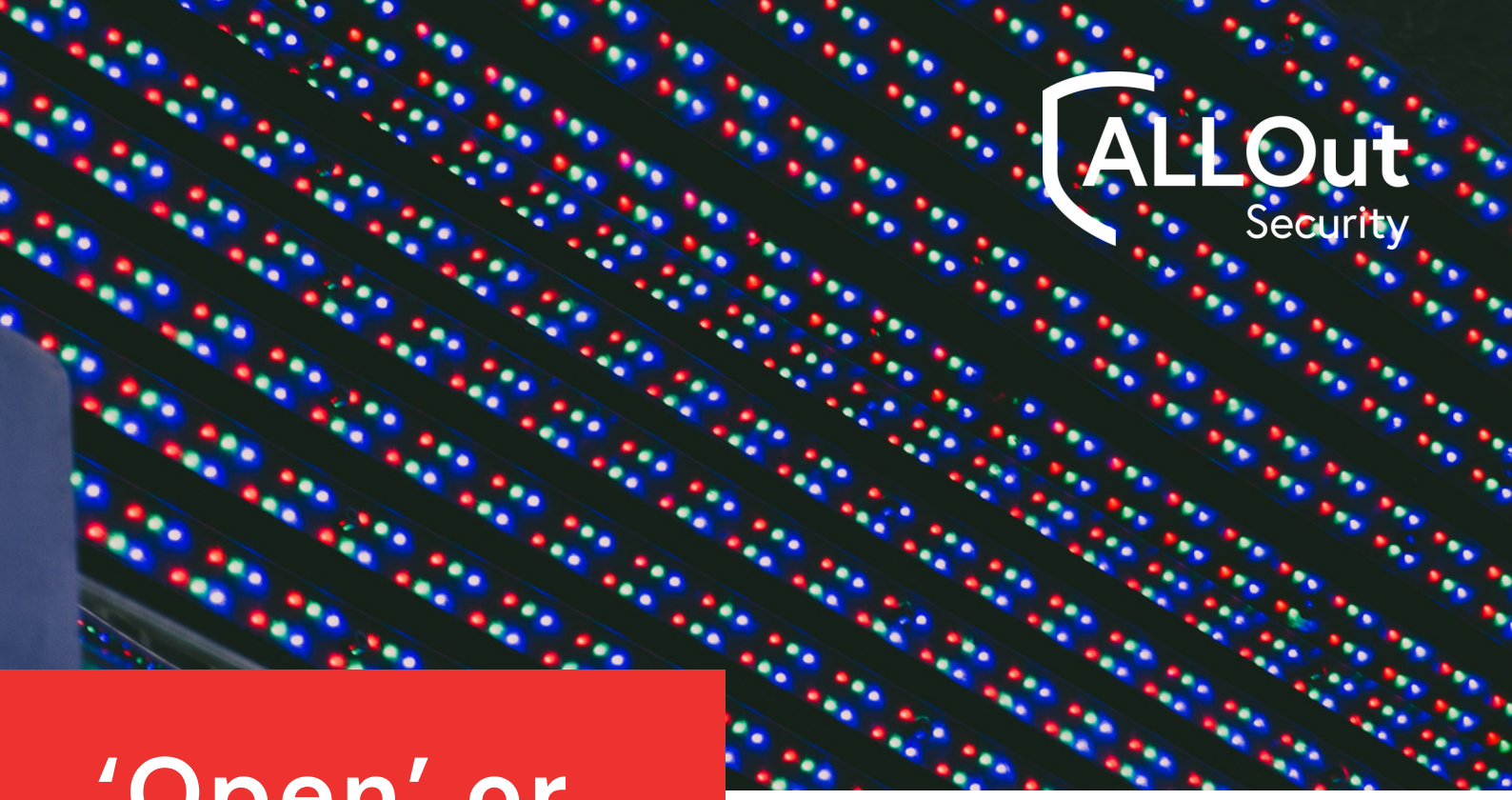
‘Open’ or ‘Closed’

‘Open’ or ‘Menu’ Security
The default model of security for JD Edwards is open access or all doors open security. In this model, you must restrict users from accessing objects that are not required as part of their jobs.

The technique that was traditionally used was to define menus that matched the users’ requirements and then create security to prevent the user from leaving that menu. However, this ‘menu’ security or task view filtering is not a viable alternative from a control perspective because all it really does is hide the objects

Even though the objects may be hidden, users can often still run them using row and form exits from other programs. There are often literally thousands of objects in the system that must be secured because they can be accessed from these exits. This means that proving compliance to your auditors in this method is very difficult if not impossible.

The default model of security for JD Edwards is open access or all doors open security.



‘Open’ or ‘Closed’

‘Open’ or ‘Menu’ Security

The advised model of security for JD Edwards (by all consultancies, auditors and JD Edwards themselves) is Deny All and grant back access, or all doors closed security. In this model, there is no access to any programs by default and you define what access users may have to the system. This permits change control and it enables you to prove the access that is available to your system to auditors and management.

ALLOut, as a software vendor, has made it their business to help clients achieve the closed system with the maximum efficiency possible while at the same time ensuring that long-term maintenance and compliance requirements are met.

Program Security

Controlling access to programs

Application Security - This defines whether or not a user is allowed to run a specified application. Valid values are either Y or N for Run.

Action Security - This defines the actions that can be taken for a specified application once a user is able to access it. Allowed actions are:

Security Flag	Allowed Activity
Add	Controls adding a new record within the application.
Change	Controls changing existing data within the application.
Delete	Controls deleting existing data records within the application. (the Change function will allow you to delete data from one field on a record if the system allows that field to be blank. This relates only to removing an entire record.)
OK/Select	Controls the use of the OK or select button within the application. In many applications, this enables you to open the record to see additional details.
Copy	Controls copyinga record or range of records within the application.
Scroll to End	This controls whether a user canreturn ALL records within an application based on any QBE filters that have been applied. If no QBE filters have been applied, ALL data will be returned

Program Security

Processing Option & Data Selection Security

This security is necessary to prevent users from overriding the configuration of versions that have been set up to meet specific requirements. Note that this risk can be mitigated to some extent by defining menu tasks to execute programs immediately when selected rather than prompting the user for version or data selection/processing option values. In Tools Release 8.98.4.2 and higher, there are additional options available.

Security Flag	Allowed Activity
Change	Controls changingprocessing option values.
Prompt for Values	Controls theviewing ofprocessing option values. Thechange security flag above controls the ability to change values.
Prompt for Versions	Controlsoverriding the selectedversion at runtime.
Prompt for Data Selection*	Controls overriding pre-defined UBE Data Selection. In TR 8.98.4.2 and higher this option controls the ability to view the Data Selection only whilst the ability to add or modify is controlled through new security flags available as described below.

Program Security

Security Flag	Allowed Activity
Full Access Data Selection*	Controls adding, modifying, or deleting data selection.
Modify Data Selection*	Controls the ability to modify existing data selection values only. It does not affect the ability to define additional selections or delete data selection.
Add Data Selection*	This will allow you to add data selection to a UBE. This requires either full access data selection and/or Modify data selection to also be permitted.
Full Access Data Selection*	Controls adding, modifying, or deleting data selection.

***Data Selection security is only applicable to Web Clients**

Hyper-Exit Security

This defines whether a user or role is permitted to use a program's row or form exit. This can be opening another program, calling a UBE, or performing an update defined in the exit. If application security restricts the use of a program called by the exit, this type of security is not needed because application security controls the use of a program irrespective of the route that is used to reach it. Valid values are either Y or N for Run.

Data Security

Row Security - Controlling access to data

Row Security This security allows the control of data within the system is most commonly used in relation to companies and cost centers\business units. The security can be applied to either all tables or to individual tables. As a best practice, all tables are normally used.

JD Edwards offers two methods of applying row security, inclusive and exclusive. Exclusive security blocks access to a secured range of values (the Row Security 'View' flag is set to 'N'). All ranges of values outside of the designated range would be available.

Inclusive records grant access to a valid range of values (the Row Security 'View' flag is set to 'Y'). When using inclusive, all values outside of the included range are automatically denied. Inclusive is available from SP16 and is highly recommended as it provides much better performance for clients that utilize row security – it also enables multiple roles of row security more effectively and dramatically simplifies maintenance.

If you are using the exclusive mode of row security, ALLOut advises you to convert to 'inclusive'. We have a mechanism of converting all your row security automatically in minutes to save you time.

Data Security

Row Security - Controlling access to data

This secures users from viewing or updating specific fields of information. You can set up column security on a table, an application, an application version, or a form. Even if an application uses a business view that does not contain the data item that you want to secure, you can still secure it, as long as the item appears on a form in the application. You are allowed to set the access to Add, View, or Change the specified data set.

UDO Security

EnterpriseOne provides features for users to create custom grid formats, watchlists, queries, and other items, which are saved as user-defined objects (UDOs) in EnterpriseOne. For example, if a user creates a query using the Query Manager, the query is saved as a UDO in an EnterpriseOne table. er, have not changed over time although additional security types have been added and new concepts have been introduced.

UDO Feature Security
This security activates or deactivates each type of UDO feature globally in your system. Each feature is secured by default and can be activated.

UDO Action Security This security determines the actions users can perform with a particular UDO feature. UDO action security is set up by the UDO feature for a user, role, or *PUBLIC (all users). UDO Action security options include:

- **Create.** Authorize users to create UDOs for their own personal use.
- **Create and Publish.** Authorize users to create and share personal UDOs with others.
- **Create, Publish, and Modify.** Includes the preceding permissions plus the ability to modify UDOs created by other users.

UDO Security

UDO View Security

View security enables access to shared UDOs. You can apply UDO view security to each individual shared UDO for a user, role, or *PUBLIC. Or you can apply UDO view security to all shared UDOs of a particular UDO type.

UDO Content Security (Composite Page and Application Framework UDOs only) (Release 9.2.0.2)

This applies to Composite Page and Composite Application Framework UDOs.

In addition to setting up view security for Composite Page and Composite Application Framework UDOs, you must also set up content security to authorize users to view or work with the contents of a Composite Page and Composite Application Framework UDO.

System Security

Controlling access to the system.

Solution Explorer Security - This allows the control of the users; interface into JD Edwards, outlined below:

Security Flag	Allowed Activity
Menu Design	Secured, View or Change -Secured access prevents all access to the feature, View allows to view menu design, Change allows to view and Change menus.
Menu Filtering	Secured, View or Change -Secured access prevents all access to the feature, View allows to view Finecut, Change allows to view and Change Finecut
Favorites	Secured, View or Change -Secured access prevents all access to the feature, View allows users to view favorites, Change allows to view and Change favorites.
FastPath	Secured, View or Restricted View - Secured access prevents all access to the feature, View allows full access to FastPath, Restricted View allows limited access to FastPath (menu navigation & mnemonics only)
Documentation	Secured, View orChange -Secured access prevents all access to the feature, View allows to view documentation, Change allows to view and Change documentation.
OMW Logging	OMW logging is either on or off

Security Hierarchy

JD Edwards uses a hierarchy to determine what security is “effective” for the user.

- Each type of security works independently.
- Xe and ERP8 systems use *Groups while 8.9++ systems use roles. All versions utilize *PUBLIC and user-specific settings.
  - Roles use the ‘Role Sequencer’ (accessed off P0092 and stored in F00926) to determine the order in which they are checked. Roles with the higher numbers are the ‘more powerful’ and are checked first.

The database is checked for records in the following sequence:

- For the User, then if necessary:
- For the *Group (In XE) or for the roles (in 8.9++), then if necessary:
  - Each role will be checked in turn starting with the highest priority role and finishing (if necessary) with the lowest priority role.
- For *PUBLIC

For each User, *Group, Role, and *Public the following records are searched for in the following sequence. When a security record is discovered, records that exist “lower” in the hierarchy are ignored. (i.e. As soon as JD Edwards determines security for something it stops searching further down the scale.) For example, this means that if security is applied to a version, that security will be used in preference to any security applied to a program only.

Security Hierarchy

- The specific program where security is applied to:
  - The specific Version/Form only (where Version level security is available)
  - The specific Form only
  - The specific Version/Program only (where Version level security is available)
  - The specific Program
- “*ALL” programs

Security Cache

Security in JD Edwards is applied to the session when the user signs on (in the case of fat clients and Citrix) and when the security cache of the server is created (in the case of the web server). This means that changes made to a user's security, whether at the user, role, or *PUBLIC level are not realized until either the user logs out and back in, or the server's security cache is cleared and recreated.

In the event more than one security table is in use, the first user to log on to the server determines the security table that is cached for a web server.

This is important to understand in the event you wish to utilize multiple security tables. In this instance, it is critical to have each security environment utilizing a separate JAS instance.

Conclusion

Security in EnterpriseOne can be defined in many different ways, and if not planned out and executed well, it will create headaches for years to come and be a nightmare to maintain. We have not attempted to go into great detail about all aspects of EnterpriseOne security, but to provide a high-level overview of the major security types and what you can do with them.

If you would like an in-depth analysis of your specific security scenario or would like to discuss how to resolve your ongoing security issues, please contact Info@ALLOutSecurity.com.

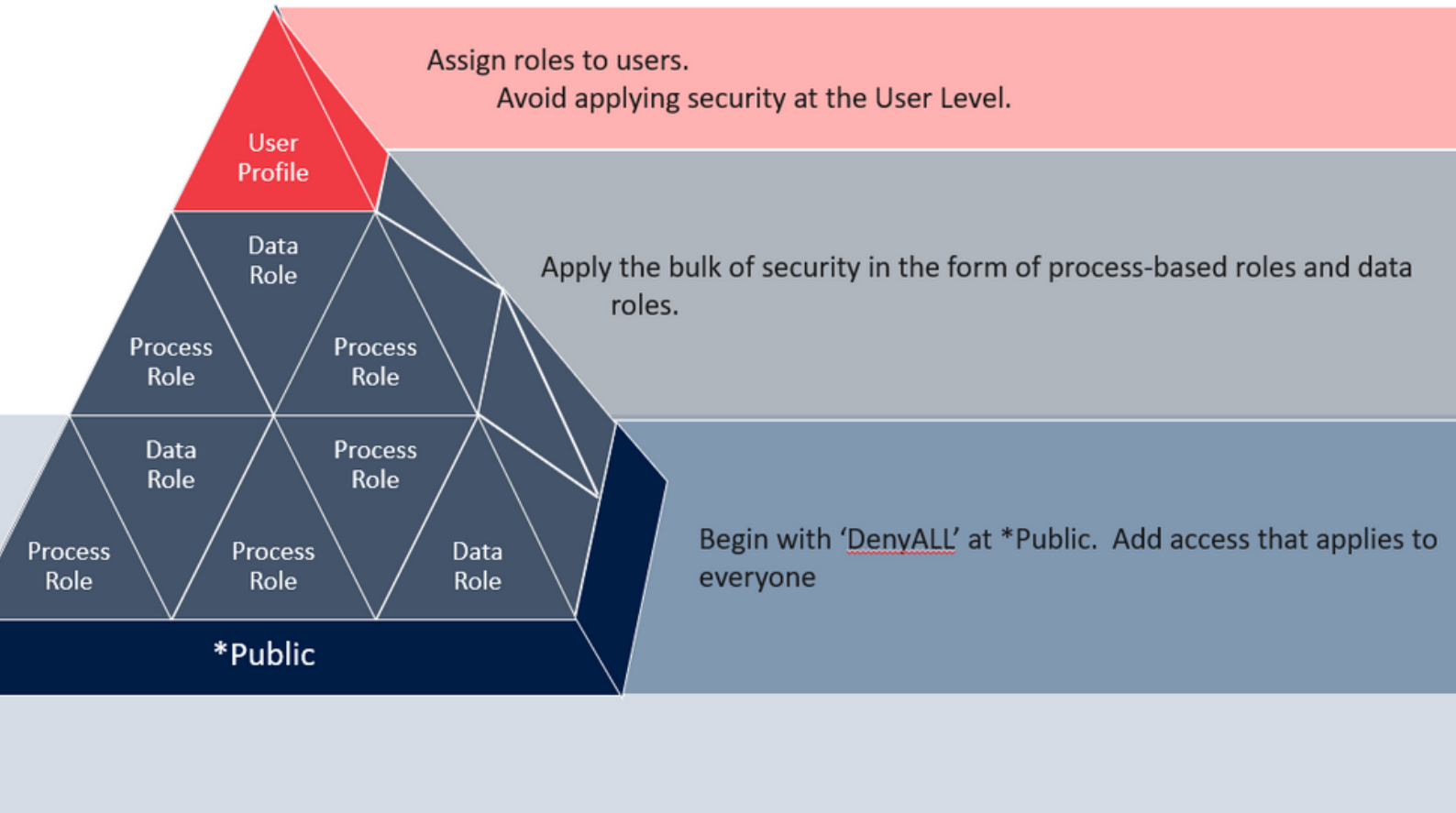
As you move through your security implementation, we offer the following advice:

Keep it Simple and Maximize the Return on your Security Efforts

- Align your UDO security with your standard security roles to reduce the complexity of managing this additional feature and assigning access to users during provisioning.
- This is the easiest thing to do – with experience. For example, manage what access the users have separately from ensuring that individual roles that you create have the access they need to perform a given function. In other words, if your roles are small and process-based so that individual roles do not provide access to multiple business functions, then access to roles can be managed separately from creating and testing those roles. This will also allow you to apply and reutilize these roles.

Tips for Roles & Profiles

You can use the method of re-using security roles for different job functions by tracking and applying the base roles created or simplify even further using ALLOut Security CombiRoles to develop the larger job function roles based on your small process based roles to get the “best of both worlds”.



Conclusion

Open or Closed

- An open system is many times more difficult to maintain than a closed system. Do not ignore the long-term maintenance overhead of an open system because short-term pressure dictates moving forward rapidly without understanding and explaining the long-term consequences to management.
- If you do have short-term pressure to produce results, especially seek advice. ALLOut can advise on leveraging your existing open security investment and applying it to a closed system.
- A closed system is in fact relatively easier to maintain than an open system. Do not attempt to achieve via menu design what is best achieved via program security; do not attempt to achieve via data security what is best achieved via program security.

Multiple Roles

- Use multiple roles – JDE would not have created them and changed their access model from single *Groups (as in Xe) to multiple roles unless they helped customers realize their objectives. Which roles are assigned to users should be transparent to users.
- Consider using ‘Menu Filtering’ or ‘Finecut’ – It is a simple way to help improve user productivity.
- Create roles based on processes not users as shown above – for example roles called ‘Voucher maintenance’ and ‘Payment processing’ are a lot simpler to create and administer than a role called ‘AP Clerk’. It is much harder to get Segregation of Duties compliant (should that be necessary either now or in the future) with broader roles such as ‘AP Clerk’.

ALLOut Security

Get in touch

Find us & Connect

sales@alloutsecurity.com

8400 E. Prentice Ave.
Suite 1500
Greenwood Village
CO 80111
United States4