



ebook

Microsoft Dynamics 365 F&O Security Roles - Creation & Optimization Guide

[executiveautomats.com](https://www.executiveautomats.com)

LIST OF CONTENTS

1. Security in Microsoft Dynamics 365

- 1.1. How does security work in Dynamics 365?
- 1.2. Security roles
- 1.3. Field level security
- 1.4. Hierarchy security
- 1.5. Challenges with creating custom security roles

2. Security Setup

- 2.1. Process-based security
- 2.2. Creating security roles
- 2.3. Main functionalities
- 2.4. Security roles vs. licensing
 - 2.4.1. How Security Setup influences the licensing costs



1. Security in Microsoft Dynamics 365

1.1. How does security work in Dynamics 365?

Security – understood as protection of IT systems and networks from damage, theft and disruption of service – is the shared responsibility between the provider and the customer. That is why security (and compliance) are the two fundamental aspects of Microsoft Dynamics 365 solutions. Security within Microsoft Dynamics 365 is critical for each organization. In order to control data access effectively, you need a mechanism that allows for modifications of security roles and, at the same time, protects the data and enables its safe handling. With Dynamics 365 granular level of security – role-based, record and field-level security, administrators can control access and privileges and ensure that each business user has the information they need to complete their job.

Whether during customizing or extending native functionality, the access to data (here, implemented by security roles) should be safeguarded and not overlooked.



While security is natively built into the app, the best practices and privacy requirements are more likely to be bypassed by developers. And breaking the security model can have substantial impact on the application and the business continuity as well.

Security implementation is one of the fundamental pillars in Microsoft Dynamics 365 implementation. In order to decide on the security architecture that would suit the apps in use, you need an extensive analysis of the current requirements and a thorough design. At the solution level, you need to create a security policy that will be implemented in the deployment phase.

Microsoft recommends that you have a process in place to change security roles and permissions for a given user when they, e.g. leave the company or change the department or if a third-party vendor for the company changes. With the growing number of business processes, the number of users and system usage, it might be quite a challenge to keep track of all customer data. Nevertheless, you need to identify who has access to the system and how the data is handled by each and every user. Based on the application's security requirements – as well as regional data-sharing policies – each organization manages access via security roles.

Security is no less important for the system than data maintenance. For Microsoft Dynamics 365 F&O, it is either a support team, system administrator or an audit person that needs to be responsible for security and access data. They need to gain an understanding of the application role-based security model and any related access policies. Managing system operations requires – among others – assigning users security roles, adding or revising new customer attributes, etc. You have to plan how to assign security roles for new users, what effects the changing of ownership might have or how to reassign the records owned by the user who moved or left. Especially reassigning a large volume of records can negatively impact the system's performance.



More often than not, security design is created late (if not as the last part) in the implementation phase. This can cause many issues such as inadequate testing or ineffective system design.



SECURITY AND TESTING

The system is used daily by multiple users who required different security roles and also licensing (this to be discussed further in 2.4). Certain personas might share the same security role, yet they perform different job functions. You need to make sure that users are created only in the environments to which they should have access. Giving appropriate security roles assignment should always take place before data migration (and afterwards it needs to be obviously validated, too). This will also facilitate running tests – e.g. UATs should be performed with correct security roles assigned to the users (personas), and not general or system admin profile.

However, if security access is designed and developed before UATs, this might cause “misleading” acceptance of the environment. Users will accept the system image but due to the fact that they were accepting as administrators or abnormally elevated access rights, they might be confused once they see the final security design. If this is not the case, there is a considerable risk of business processes going haywire later on due to existing security holes. Make sure that you only test the system with the right security roles that had been set up at the very beginning.



Security does affect performance, too. A user with an admin role will have better performance than one with limited access. That is why performance tests should be executed by users with proper security configuration. This is also crucial for training people – they should not have access to anything more than the required actions. For process testing, role security is crucial as you want to make sure that the segregation of duties is correct and when running the solution in production, different personas are able to operate as they should.

When talking about Microsoft Dynamics 365, security concerns can be classified as:

- × Access control
- × Data protection
- × Compliance and regulatory requirements
- × Transparency

We will be most interested in the first one in this publication.

Microsoft Dynamics 365 – similarly to its previous AX 2012 version – continues to use user role-based security. What this means is that the permissions are not granted to the user but to the security roles that are assigned to a given user. Without these, users are not able to either access or use the Dynamics 365 application – security roles are fundamental security controls (more about security roles in the next chapter).



Within Dynamics 365, there are two new features that help configure custom security and create the system security architecture – those are security diagnostic and security configuration tools. The application provides you with a hierarchical model with **security roles** at the top, followed by **duties** (determining the business processes), **privileges** (determining the access level) and **permissions** (the securable objects that are accessed via the security model). Every user assigned a security role has access to the set of duties that are typically associated with this role. This set comprises various granular privileges. This means that if a user does not get assigned any role, they don't have any privileges.



Security roles

Roles grant access to Finance and Operations apps



Duties

Duties allow access to parts of business processes



Privileges

Privileges allow access to individual tasks



Permissions

Permissions grant access to individual securable objects

1.2. Security roles

In Microsoft Dynamics 365 Finance and Operations, security is role-based, which means it aligns with the business structure. To access the applications, users not only need a valid Azure AD account in the given tenant and a valid license – what they also need (upon their authentication) is role-based security to authorize access to individual elements within the Dynamics 365 F&O applications – data, services, menus and/ or other Dynamics 365 security capabilities and features.

Users are assigned security roles based on their responsibilities and daily operations. Once those have been set up, business managers can control day-to-day access to data. For Dynamics 365 Finance and Operations, by default you get 137 standard security roles with security duties and privileges that are most commonly associated with those roles. Security roles can be understood as a matrix of privileges and access levels across entities. They allow us to protect information from mishandling and ensure that users have the power to take actions that correspond with their job role/ position within the organization. Through setting precise and well-defined security roles for each user, you decide who gets access to which information, thus ensuring data confidentiality and integrity.

Microsoft Dynamics 365 security roles are pre-built elements with varied sets of duties and privileges. Users assigned with security roles can access security objects in the system – this means they have the visibility of certain menu items, forms, reports, buttons and inquires.

Standard roles are sufficient for the customers with basic security requirements. The administrator can either duplicate or modify the existing security roles according to business needs.



Bear in mind that standard security roles are subject to continuous One Version updates so that they can accommodate new or extended functionalities.

When designing security roles, you need to consider both compliance and scalability. When engaging the security team in the implementation, the appropriate segregation of duties framework (SOD) will allow to identify conflicts early on and create rules for duties that should be separated.

A business user assigned to a security role automatically gains all access and permissions that are attached with the given role. By editing roles and permissions of the users in certain departments and teams, you prevent any data leaks and unauthorized use of business and/ or personal data. Ideally, each employee only has access to the records that they should be seeing (how it looks in practice in Microsoft Dynamics 365 standard, we will try to show in detail in chapter 1.5.). For example, an accountant is assigned a set of privileges that are commensurate with their job responsibilities and daily operations. There might be users that are assigned multiple security roles – this means they get the sum total access and permissions of all of the assigned security roles.



Defining the roles and responsibilities of the users executing daily business process tasks and operations helps ensure proper access and security for those users. And measuring the number of users and licenses needed is a crucial consideration in the project budget.

Each Dynamics 365 security role consists of record-level privileges and task-based privileges. Security role privileges are cumulative: having more than one security role gives a user every privilege available in every role.

Record-level privileges



- × There are 8 different record-level privileges within Dynamics 365 that determine the level of access a user has to a specific record or record type. Those are: Create, Read, Write, Delete, Append, and Append To (for associating records), Assign, and Share.



Task-based privileges



- × at the bottom of the form, give a user privilege to perform specific tasks, such as publish articles

Authentication
(Azure Active Directory)

Users

Authorization

Security roles

Duties

Privileges

Permissions for application elements

Duties

Privileges

Privileges

Privileges

Data security

Data security policies

Table permissions framework

Database

Database

1.3. Field-level security

These are additional controls for the application security and field-level security and hierarchy security. Microsoft Dynamics 365 **field-level security** deals with the security options for each data field. The scope of this security encompasses the whole organization and applies to all data access requests. Field-level security is available for both the default fields on custom fields, custom tables and also most out-of-the-box tables. It is presented as a two-option setting in the schema which by default is disabled. Choosing any of the two options can either disable or enable field-level security. You can manage it via field-level security profiles in order to control the access to each data field and grant access privileges and permissions to each user role accordingly.

Field-level security allows you to restrict access to certain fields for specific users or teams. For example, you can only enable certain users to amend/ update the margin field. Few users are aware of this functionality. It is used, e.g. in the banking sector for fields that contain sensitive information (like Social Security Number) to control the visibility of the field and its value.



1.4. Hierarchy security

The **hierarchy security** model is an extension to the existing Microsoft Dynamics 365 security models that use, among others, security roles. It allows to access data from a user or position hierarchy perspective. In this way, hierarchy security enables you to get more granular access to certain records within the organization (e.g. managers can access records and perform tasks on reports' behalf). For hierarchy security, you can use either the manager or position hierarchy security models.

✓ **Manager hierarchy**

The manager hierarchy security model gives the manager access to the records that are owned either by the user or by the team (that a user is a member of) and to any data records that are directly shared with the user (or the user's team).

The manager hierarchy (for a manager to access the reports' data) requires that the manager be within the same business unit as the report (it can also be the parent business unit of the report's business unit). For the manager to see the report's data, apart from the manager hierarchy security model, they need to have (at least) the user level Read privilege on an entity. This security model is a preferred option for financial organizations (so that managers are prevented from accessing data outside their business units).

✓ **Position hierarchy**

With the position hierarchy, you can access data across business units. Contrary to the manager hierarchy, this one is not based on the direct reporting structure. Users do not have managers of other users. You define job positions within the organization, then arrange them in the position hierarchy. Users who own higher positions in the hierarchy will have access to the data of the users lower down in the hierarchy. Subsequently, users are added to any position (they get 'tagged' with a given position). Although one position can be used for multiple users, a user can only be tagged with one position. This is a helpful solution if managers need to access data in different business units.

Remember that while the hierarchy security model provides an additional level of access of data, it is worth combining it with other forms of security – such as Dynamics 365 security roles.



1.5. Challenges with creating custom security roles

How does the standard Microsoft Dynamics 365 security roles assignment work? The user can either:



Create roles based on task recordings and manually assign action menu items along with permissions. This requires a Visual Studio license.



Use standard role combination and cut out any unnecessary privileges and duties. As this is a very painstaking activity, it requires a lot of time and is inaccurate when it comes to the licensing level.



What Dynamics 365 offers when it comes to security roles creation is actually limited only to an automatic recognition of display menu items. Anything apart from that needs to be done manually in the security configuration. This is what makes the process ineffective in the first place.

What are the best practices recommended by Microsoft when it comes to security role management? It is to:

- ✗ **Grant the minimum access** required for users to do their job
- ✗ **Disable share rights** where possible in security roles (extensive sharing leads to performance issues)
- ✗ **Refrain from sharing automation**
- ✗ **Share only the absolutely necessary records** with the smallest number of users/ teams possible

The above recommendations, as obvious as they seem, might be, however, quite tricky to fulfil with what Microsoft Dynamics 365 F&O offers. In Microsoft Dynamics AX 2012, there used to be a separate Microsoft Security Development (SD) tool with which you could easily build custom security config. Nevertheless, the process was burdensome and security projects lasted forever. In Microsoft Dynamics 365 F&O, the security config process is even harder as there is no dedicated tool such as the SD tool.



Right now, there is no available extension for security configuration. What this means is that, although you can obviously create security roles within the standard Dynamics 365 F&O, it is an extremely complicated – and time-consuming – process.



For example, if standard security roles are used and then modified, it is quite difficult to distinguish between the standard and the modified roles. The organizations with enhanced security requirements might need to work with the copies of the standard roles and not modify the standard roles themselves. This, again, is quite a time-consuming process. For customers with more advanced requirements, it is not recommended to start with brand new custom roles. Although some companies are tempted to do so, they have to rely on standard security roles if they want to have access to the necessary functionalities. Yet, sometimes what the standard Microsoft Dynamics 365 F&O offers is not enough. If certain users need full access, they might require a combination of roles – this might come with excessive costs of such users' licensing (more about this in chapter 2.4).

The usability, effectiveness and ease of security role creation in Dynamics 365 F&O leaves much to be desired. Security – when using the standard solution – is not only time-consuming but also frustrating to test. That is why leading the security team through the implementation can be particularly challenging. The security forms in Dynamics 365 F&O are structured in such a way that it is difficult to see what is on them. By navigating to **System administration>Security>Security** configuration, you can view the security configuration form. However, it only displays the duties and privileges related to the specific security role and the selected duty. This is a serious limitation for the security project team as they need to see all the security roles, duties and associated privileges.



Therefore, for a proper and bulletproof security matrix and security roles assignments for the business users, standard Dynamics 365 F&O security role config and setup is not enough.

Security project duration

Microsoft standard is built on the requirements/ needs of the US market. Those can be useful; however, these are too general for system access. For the alternative – to create security access from scratch – you need to use a lot of Visual Studio to track down the details and identify each element by element. Around 10% of security objects are so deeply embedded within the application that you need skilled developers hired to do this for you. If you would like to have tailored security roles, the project is so complicated and costly that it would take 1 year to complete an implementation of Microsoft Dynamics 365 F&O in a mid-size company. And for Dynamics 365 Finance, Supply Chain Management and Commerce for security development, extension and customization require a Visual Studio Professional license for which you need to pay additionally.



You should be thinking of security design and config as a critical part of your Dynamics 365 F&O implementation and maintenance. While you make fair use of the security provided within the application, consider thoroughly using a separate tool like Security Setup for enhancing data security and shortening the time of security projects to a minimum.

2.Security Setup

2.1. Process-based security

Security Setup is a tool that addresses security role creation. The aim of the tool is to optimize and facilitate the role creation process across the organization and business areas in which Microsoft Dynamics 365 F&O is used on a daily basis. It gives you custom security setup for each role (each business user and their position) within the organization.

Security Setup supports the unique method of security creation. Security roles are position-based (and so are security duties and privileges). This approach allows you to build new roles according to the organization hierarchy structure and base them on actual business and operational processes.


Based on our experience with multiple clients, we have proven that extracting business processes from each position within the organization and their conversion into security duties is the simplest, cheapest and most efficient way. This gives a full understanding of all operations and process owners in the system. And most importantly, a process-based approach to security role generation optimizes the license costs for Dynamics 365 F&O.

Once the business structure and process flows have been designed, business roles (personas) can be easily identified. The next recommended step is to map the business users with the system security roles. Such a security design – although the most desirable – is, however, very challenging and ineffective with what Microsoft Dynamics F&O has to offer.

Both the customer and the partner (system provider) have to have clear views on exact roles and responsibilities between the teams. To avoid confusion and miscommunication at the time of implementation, it is highly important to focus on the details of activities, define the scope for security design and consider carefully the role assignment. This results in proper alignment of business users with their security roles.

Security roles vs. data fraud

As mentioned already in chapter 1.2., Microsoft applies changes (One Version updates) that apply to security roles, too. It is highly likely that if you are using the Dynamics 365 F&O role assignment, you might be deploying unverified roles to the system. As a result, business users are given a number of unknown, and most likely redundant) security items. With each update, existing roles are extended – new functionalities are added or the existing ones are modified – which carry a potential data fraud (these might be related to deal profitability, margins, etc.).



With Security Setup, you are mitigating the risk of data fraud to a large extent. Users assigned with precise, tailored security roles have access only to the security objects that they need to perform their daily work.





The common challenge that we are facing when carrying out automated testing projects is that **security roles are often not considered as part of test automation**. However, test automation projects should be executed with the role that is handling the specific business process. The idea behind this is that you test the environment in the exact way that it was created and developed. Multiple issues can be (and are) encountered in the production environment is that the testing cycle seems to have been successfully completed. However, on closer look, it turns out that in the end, there was no role assigned with an action access to action items with a certain functionality (such as posting). Such small aspects – establishing the personas (business users and their roles), when overlooked in production, are responsible for a high number of issues and errors. Therefore, security verification might be a problem later on.

2.2. Creating security roles

Each security role created with Security Setup has a tailored row for an individual business user. It only requires the minimal number of security objects. You do not need to use the Visual Studio license at all. It is enough to understand the organizational structure to create and confirm a specific role. The ultimate goal is to set up one row for each position within the organization (alternatively, you might want to set up one row plus one supplemental role). The overall idea is to apply the minimum number of rows for each Dynamics 365 security role so that later on, system maintenance and future modifications (updates, etc.) are easier.

How to create a security role?

1. Let's take the sales department as an example of an area. Within this area, we can have various positions (each of them kept by multiple business users).
2. One of the positions may be Sales Representative. We can apply many business processes to this position (such as Reporting in Collections, Sales Create, etc.). Within Security Setup tool, they are uploaded underneath that position as three separate task recordings and then converted automatically into duties.
3. For each of the display items within each duty, we can see the access level and also have an option to either correct, delete or invoke it. This means that each access can be modified after the recording has been uploaded and converted into a duty under a specific position, and permissions can be added/ updated.
4. You can also use existing security roles from the standard and extend them with duties and privileges to help you along the way of security creation. In case you find any missing objects, which are deeply hidden in the system, you can always rely on standard privileges. In most cases, it does the trick and helps you limit the time spent in Visual Studio.



Different ways of security creation with Security Setup

- ✓ **Detailed security creation:** the goal is to create precise security setup with a sufficient number of entry points. Business processes are converted into security duties. Then, the created duties are combined into security roles. Finally, the role is applied to the business user.
- ✓ **General security creation:** the business processes are mapped onto security roles. The roles are applied to the users on the basis of the standard system privileges. This is intended to fill the gaps that were found in the business processes recordings to make them more effective. The number of entry points allocated per user gets significantly reduced.
- ✓ **Extension of the existing security setup:** Security Setup can also be used to re-modify the existing security setup within Microsoft Dynamics 365 F&O and change current security roles.

Once the role has been created, you can always go back to see role requirements and the whole security context. If you want to understand an even broader context and all entry points embedded on the confirmation page, you can also view permissions for each duty/ role and add selected entry points onto the created process.

Creating roles based on task recordings

We need to think of a security role as an individual position in the organization and the duty as a business process to handle. Such an approach brings full understanding of all the operations and process owners in the system.



With Security Setup, you have a possibility to record business processes and use them as a source of information when creating security roles and security structure in the organization.

The process owners should be able to give all information regarding what their role entails from the access perspective.

We extract all types of positions within the organization (be it warehouse, logistics, management, finance and accounting, etc.) and identify their daily tasks and responsibilities.

We record those business processes as duties. Then, all of the processes are built into the task recordings and you can create security roles in Dynamics 365 F&O using those processes as independent Duties underneath each new (or existing) role. The processes recorded can also be merged and loaded as one security duty (they will include all entry points as identified by the system). You are also able to extract and load individual entry points onto each role (table permissions and/or control permissions). In this way, you create an organizational security structure of roles and duties assigned to each role in the system.



When the role is created, it gets automatically published in Dynamics 365 F&O (you can look up the role in the Security Configuration display). Then, you apply the role to an individual business user and they can run the acceptance test to verify they have the required access.

Security project with Security Setup

Security Setup guarantees for our clients that their business users have only the access that they need. When we work with our clients, we find out all the areas that are in use for business. Under each of these areas, we identify and define all positions (they can be held by multiple business users), then we map the business processes onto each of the roles (position within the organization). Each business process is recorded separately. Once they have been applied onto the roles as duties, we also run thorough cross-checks to make sure that all security roles meet the necessary requirements (system- and business-wise).

The process-oriented security project speeds up the delivery of new roles for the new positions. Converting business processes into duties also means fast adjustment/ modification of the existing roles. For example, with new One Version functionalities, you can simply extend the existing rows with new functionalities. New Microsoft privileges can be applied in the same way to each of the security duties.

Defining and mapping the security roles against the business processes as part of the security design is extremely helpful and cost-effective. Such roles can be directly used for testing the application as well as for generating role-based training. With the whole security project approach being process-focused, it will help prior to go-live but also can be used with onboarding new hires and when users change roles.

Creating security roles with Executive Automats

For users who have Executive Automats testing tool, test cases that have been created can be easily reused and extracted for the purpose of security creation. You need to create a separate project called Security Role Creation and copy the existing test cases to go under that project in order to recreate the organizational structure. By going into the specific role and duty, we can load testing scripts from Executive Automats that were previously used for testing. Afterwards, you run a verification to double check if the recorded processes are exactly the business processes (duties) that we need for each role.

You can extract individual security objects, specific paths and permissions also in the form of RSAT recordings to build a whole context for security configuration if needed.



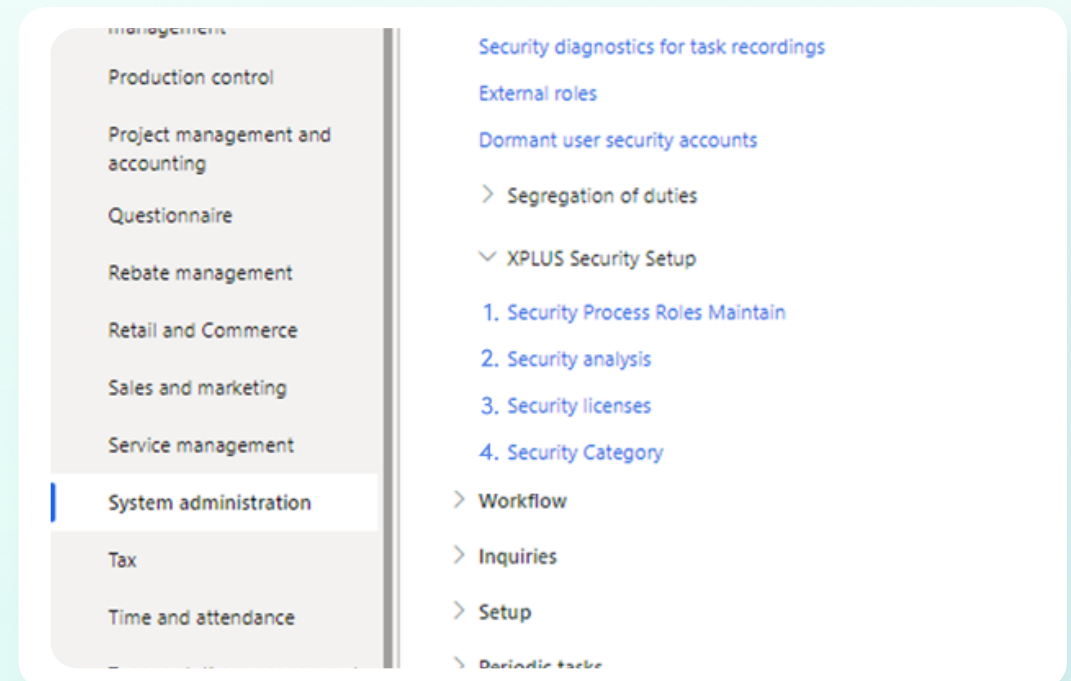
2.3. Main functionalities

Security Setup tool supports the security creation as well as security roles maintenance. The available functions allow us to optimize the licensing costs, increase data security and enhance UI effectiveness. Security roles – if built properly and maintained effectively – lower the development costs during security upgrade.

Once the package has been deployed, the following functionalities are available:

- ✔ **Security Process Roles Maintain:** this is the place where users can extract entry points from tasks recordings (Executive Automats scripts) that are based on business processes. Furthermore, they can build the required roles, duties and privileges for the whole organization structure.
- ✔ **Security Analysis:** analytics tool that allows the users to identify any gaps (potential risks) with security roles assignment. It contains tables with security permissions within the Dynamics 365 system (like custom module security). It enables security fraud prevention. Based on the role, you can assign specific privileges, apply existing security roles to each user. You can also cross-check whether individuals with the same duty have exactly the same privileges.

- ✔ **Security Licenses:** enables the analysis of licensing level applied to every user/ role/ duty/ privilege. In User Licensing Summary, you can view your current licensing costs (TCO for your Dynamics 365) and also verify individual user licenses. With Security Summary, you are able to view all the security roles within the system and analyze the license level of each of these roles.
- ✔ **Security Category:** the depository of all the categories user for aggregation in the Process Roles Maintain module. You can define categories that will help you create new roles for a specific workflow/ business department.





2.4 Security roles vs. licensing

Your Dynamics 365 application can have multiple end users who use the system daily. They are separated by licensing, security roles or different application modules (FSCM vs Power Platform). Licensing a Dynamics 365 user can be done at the point of creating their user account – or later on. It is mandatory – user without a relevant license is not able to access your organization's system. For sign-in, any active user record needs one user license per person. Their Dynamics 365 access can be controlled by defining security roles (based on access levels and permissions).

User licenses within Dynamics 365 Finance and Operations are determined through analyzing the access to menu items (entry points). There are three types of F&O licenses that follow the hierarchy structure:

- ✘ Operations (listed as Enterprise in AOT)
- ✘ Activity
- ✘ Team Members (listed as Universal in AOT)

When it comes to pricing, the higher the license type is in the above hierarchy, the more expensive that license is.

The problem with standard licensing within Microsoft Dynamics 365 is that when you, e.g. license Commerce, all users with Commerce security roles become entitled to all Fraud Protection capabilities (including transaction capacities). That means that a Warehouse Clerk is automatically assigned the same functionalities as – let's say – an Operations Manager. Also, when we talk about Dynamics 365 F&O specifically, it is enough if the user, e.g. requires access to 100 entry points and only one being at the Operations level – the user is required (assigned) an Operations license. Therefore, it is quite simple to overprovision a user's access and be charged for a higher license that is actually needed.

In reality, it might turn out that the majority of the business users need the Team Member license – however, assigning additional entry points to their security roles outside of their hierarchy level is simply not feasible. Also, the Visual Studio license that you need for any security development, customization or extension for Dynamics 365 FSCM or Commerce are not included as part of these modules' licensing and has to be acquired (paid for) separately.

Another important aspect is the data fraud risk. With Dynamics 365 F&O full user license (Operations), Activity and Team Members use rights are included. What this means is that a Finance user has access that they do not necessarily need – not only both to Commerce and SCM as well but they also get use rights for Team Members level access to workloads in all modules.



Within Microsoft Dynamics 365 Finance or SCM, you can extract reports regarding license roles, however they are quite basic, don't give precise information and are quite complicated to decipher. Therefore, licensing has become quite challenging to estimate.

With Security Setup, we want each business user to understand the specific role requirements, what kind of license level everyone needs, what is the total scope of licenses you need to purchase for your system. It might be the case that a number of high-level licenses across the organization are redundant.

2.4.1. HOW SECURITY SETUP INFLUENCES THE LICENSING COSTS

As your application matures, it is critical to keep track of the rate of licenses consumed. Insight into the number of used licenses not only allows better planning but most importantly, the usage volume impacts the operational costs. That is why you need to keep the license rate to the minimum.

With Dynamics 365 F&O, you can extract reports regarding licensing roles, however, these are quite basic and complex. Therefore, to estimate the licensing costs in case of any changes is quite a challenge.

With Security Setup, you are able to understand the specific role requirements. You know exactly what kind of license everyone requires, and the scope of licenses that you need to purchase for your system. Precise reporting and analytics offered by the tool allow you to discover which licenses are redundant across the organization, with no detrimental effect for your business operations.

Thanks to the Security Licenses module, you are able to analyze each security roles and verify if the entry points embedded in the role are necessary. You can easily exclude the redundant security objects which impact the licensing, thus optimizing the costs and UI. Standard Microsoft Dynamics 365 security roles include hundreds of entry points. Based on our experience with clients who have implemented Security Setup, around 90% of entry points that are embedded within standard Dynamics 365 F&O security roles are not needed.



[Start Free Trial Today!](#)



EXECUTIVE AUTOMATS
SECURITY SETUP

executiveautomats.com