DYNAMICSCON PRESENTATION

SEPTEMBER 14-16,
2022

Control Costs and Risks with Least Privilege Security and Licensing

Robin Finnell

Alex Meyer

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}

Robin Finnell

Master Data Architect

Tillamook County Creamery Association

Email: rfinnell@tillamook.com

LinkedIn

Background:

- 13 years working in Dynamics ERPs
- 4 years working in D365FO
- 9 years experience with NAV/BC
- Have presented at both Summit and Focus
- Past Chapter Co-Leader of Oregon (Portland) – AXUG

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}
DYNAMICSCON LIVE
DUG

Alex Meyer

Director of Customer Solutions

Fastpath

Email: meyer@gofastpath.com

Blog: http://msftcloudblogs.com

Security Class: http://d365fosecurity.com

LinkedIn

Microsoft MVP Profile

Background:

- Awarded Microsoft MVP in Business Applications since 2019
- Been working with AX for the last 8+ years
- Been working with D365FO for 6+ years
- Have spoken at Summit (US & Europe), Focus, and local chapters around AX/D365FO security and have done webinars around native controls in both versions

innovia CONSULTING

INGRAM MICRO CLOUD

SPS COMMERCE

Own {backup}

DYNAMICSCON LIVE

DUG

Audience Questions

- Do you implement least privilege security ideas at your organization?
- Are you comfortable with your understanding of how Microsoft does user licensing in D365FO?
- Is user licensing impact discussed during user role assignment and security changes?
- Do you perform a periodic licensing assessment of your D365FO environment looking to insure:
  - That you are correctly licensed
  - Instances where you could lower licensing costs

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

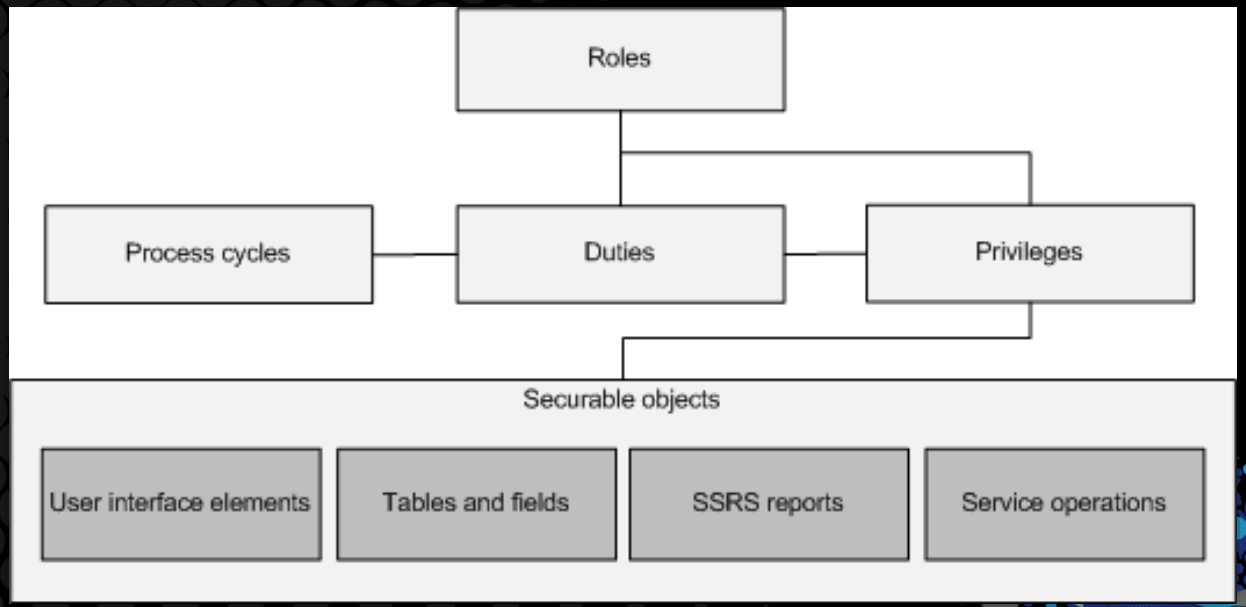
Agenda

- D365FO Security Model
- How Licensing is Tied to Security
- Least Privilege Security
- Licensing Methodologies
- End User Example - Tillamook

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}

D365FO Security Model

- Role based (users assigned one or more roles)
- Pessimistic security model
- Security Layers
  - Role
  - Duty
  - Privilege
- Securable Objects
  - Menu Items
  - Tables
  - Data Entities
  - Service Operations



innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
OwnBackup
DYNAMICSCON LIVE
DUG

Security Layers

- **Roles**
  - Broadest security layer
  - Represent a job function a user would perform
  - Account, Account Payable, etc
  - Made up of any number of sub-roles, duties, or privileges
- **Duties**
  - Middle security layer
  - Represents a general task a user would perform
  - Approve customer invoices, maintain budget plan, etc
  - Made up of any number of privileges
- **Privileges**
  - Most granular security layer, where object assignment occurs
  - Represents a very specific process a user would perform
  - Add a BOM Line, Edit Customer, etc

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}
DYNAMICSCON LIVE
DUG

Securable Objects

- **Menu Items**
  - Displays – linked to forms within D365FO, pages user goes to in UI
  - Outputs – reports users can export
  - Actions – actions users can perform (posting a PO/JE, cutting a check)
- **Tables**
  - Refers to SQL tables, where data is actually stored
- **Data Entities**
  - Combines multiple SQL tables to encapsulate a business concept (purchase orders, users, etc)
  - Allows for CRUD operations from external services
  - Does not require X++ knowledge to create
- **Service Operations**
  - Externally facing API endpoints that can be used by external services
  - Requires X++ knowledge to create

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

Implementing Least Privilege

Why is it important?

- Environment Risk – if a user has more access than needed, they may intentionally or inadvertently perform actions that could put your company at risk

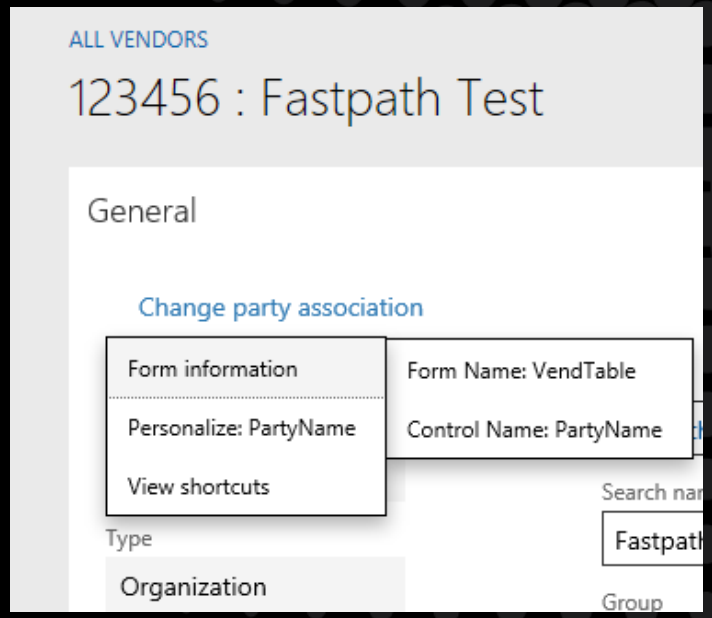
- User Licensing – since licensing is tied to user access, ensuring least privilege access is followed could save your company money on licensing costs

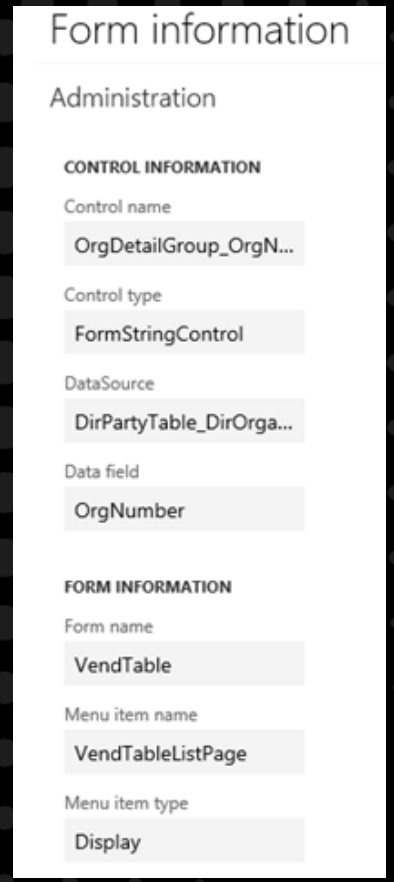
- Segregation of Duties – following the same idea as environment risk, if a user has more access than needed, they may have unnecessary segregation of duties violations that go unaddressed.

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}
DYNAMICSCON LIVE
DUG

Get Form Information

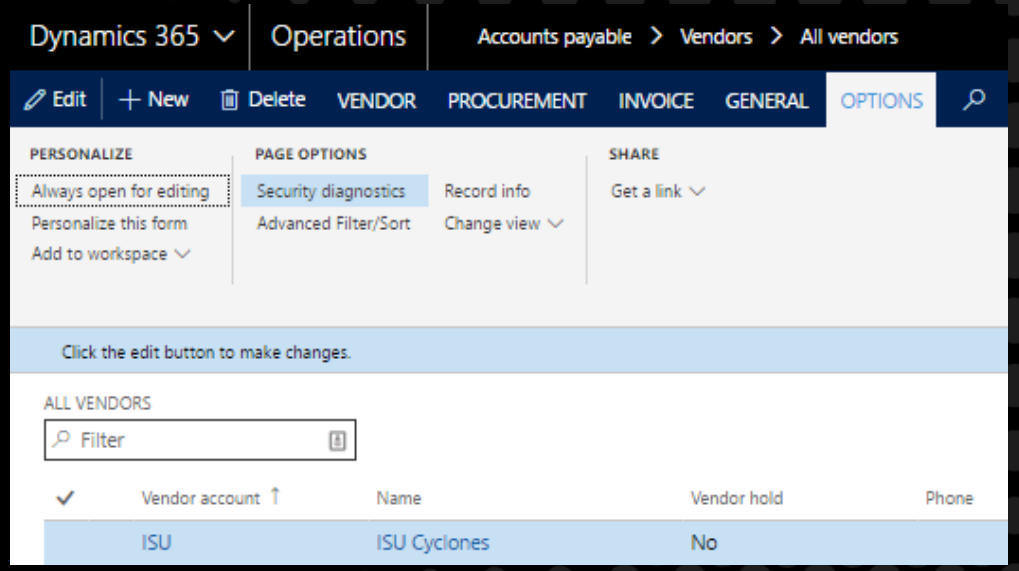
Right click on form -> Form Information

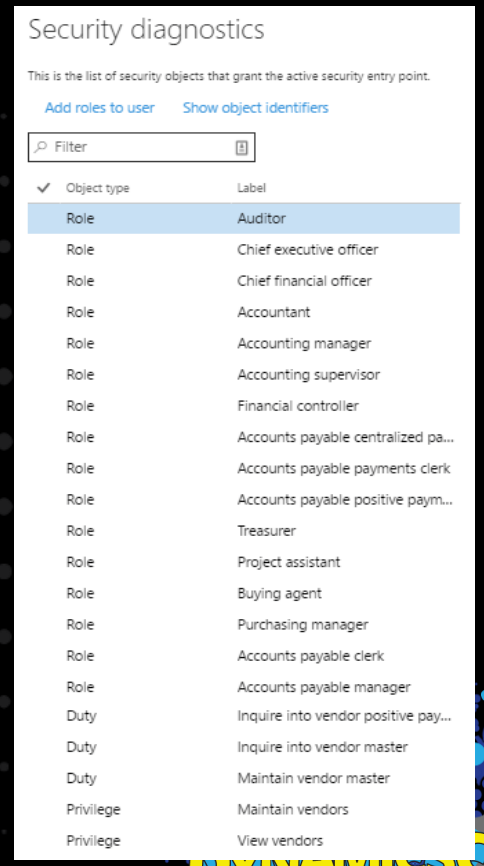




Security Diagnostics

- On a Form -> Options -> Security Diagnostics

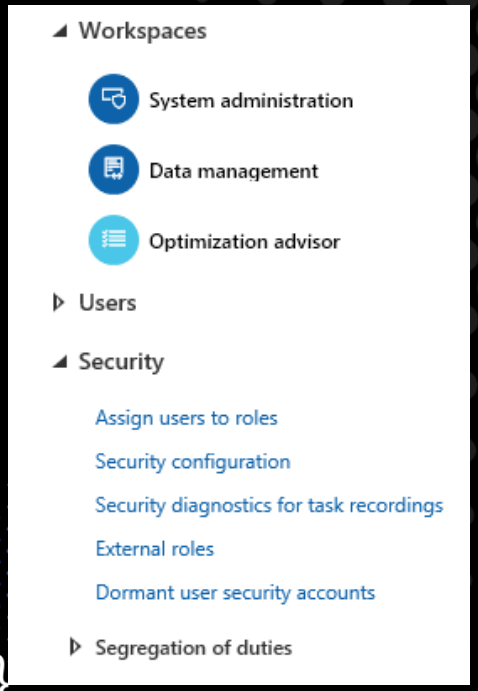


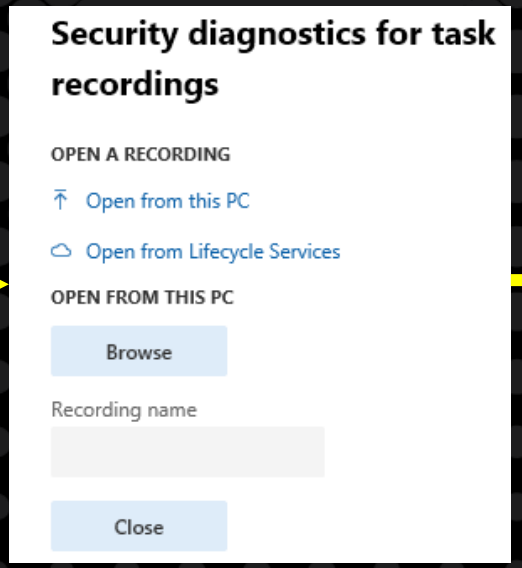


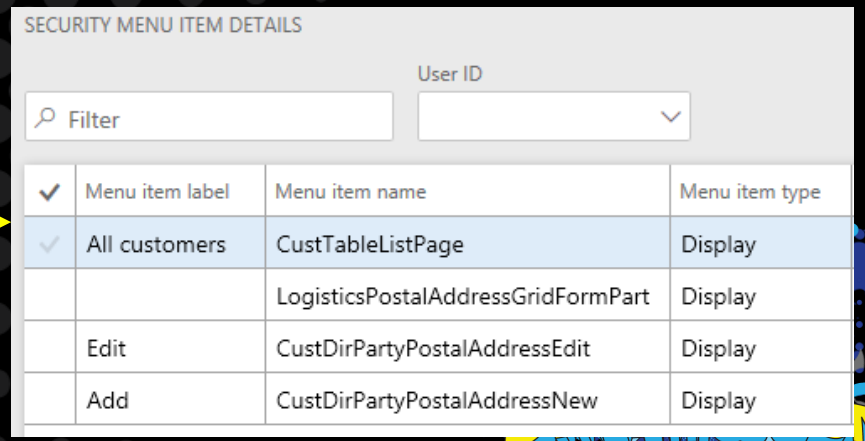
innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

Task Recordings

- What is it?
- How to use it?
- How can it be used to set up security?







innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
LIVE

Implementing Least Privilege Security

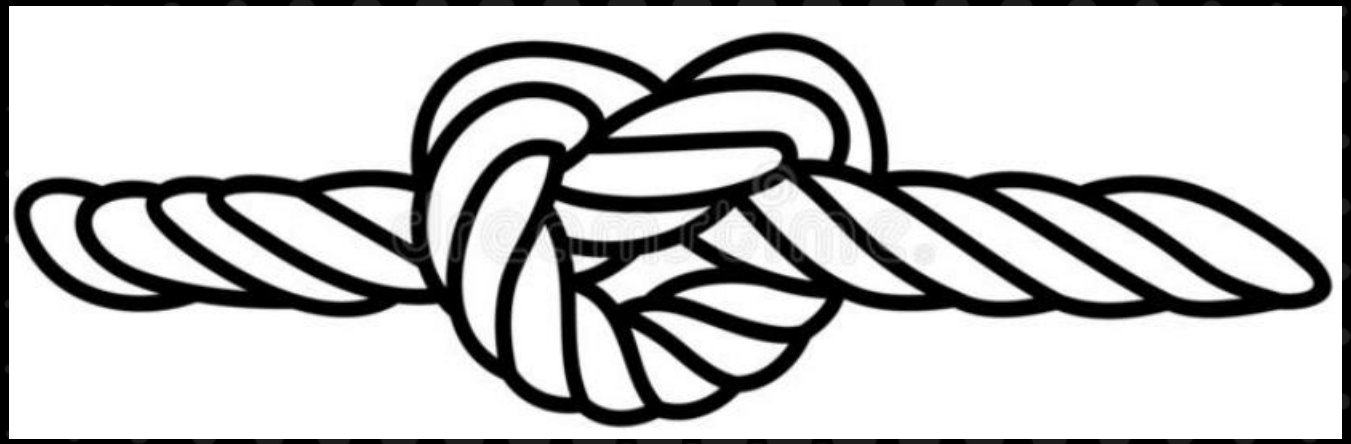
Steps

1. Determine tasks a user will perform, making sure to not overprovision
   This D365FO Security Matrix from Fastpath may assist with this process
2. Isolate menu items from process/task
   Task Recorder – perform the task the user will need to do while recording it using the task recorder function
   Use the Task Recorder Parser for AX 2012 or D365FO or Security Diagnostic for Task Recordings in D365FO to extract menu items consumed during task recording
3. Determine correct permissions for menu items
   For D365FO, remember that menu item security is honored at table level
   If you would like additional help, the Fastpath Security Designer module will provide this information
4. If necessary (esp. for AX 2012), modify table level access to allow/restrict access to certain tables/fields
5. Test and validate – always be sure to test solution prior to deployment
   *Users will not complain about having too much access

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}
DYNAMICSCON LIVE
DUG

Licensing Directly Tied to Security

Security



Licensing

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}

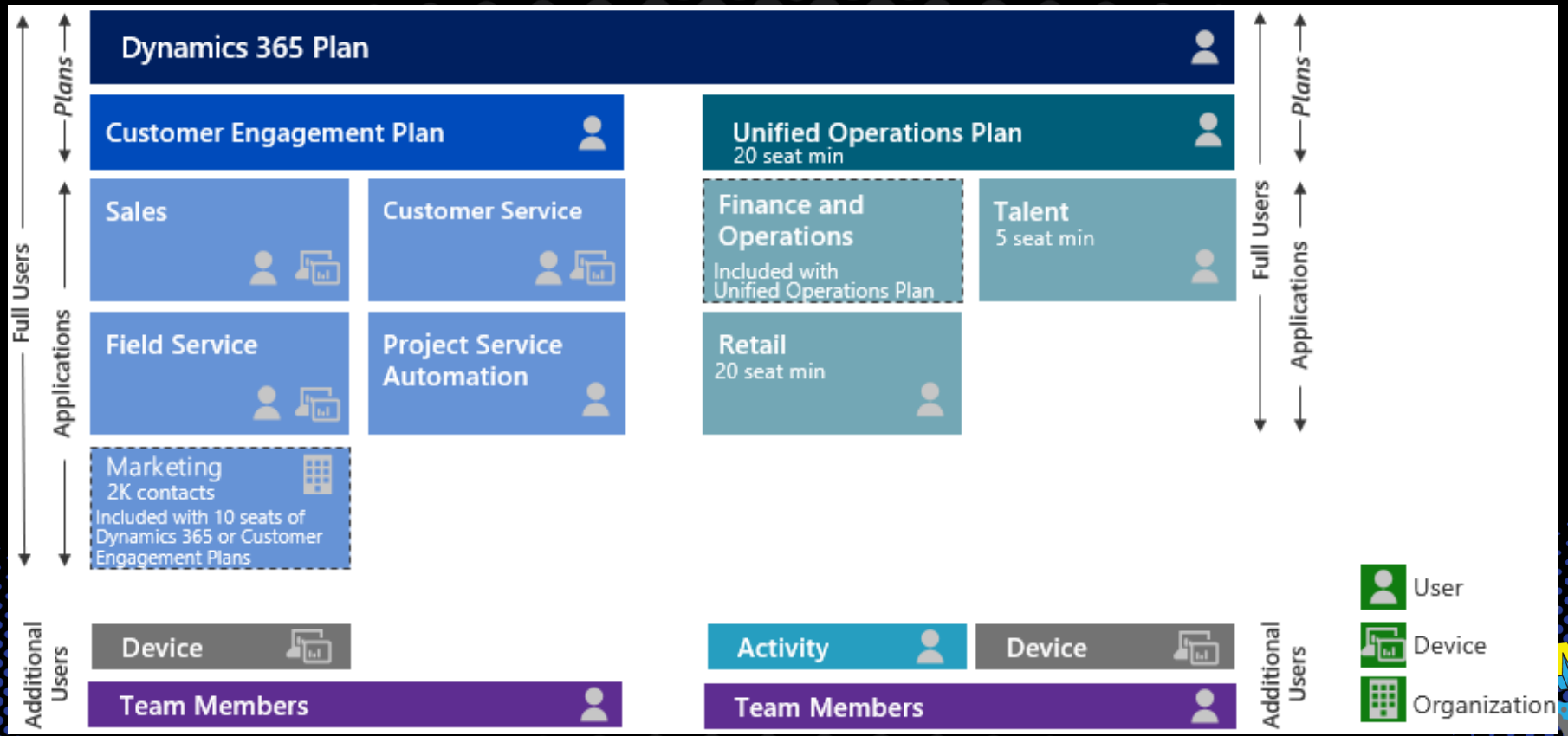
DYNAMICSCON LIVE
DUG

Audience Questions

- What is your current process for determining user licensing?
- Do security changes get analyzed for licensing impact before being implemented?
- Do you perform any sort of licensing analysis to see if you can reduce licensing costs?
- Has anyone gone through a license upgrade from AX 2012 -> D365FO? If so, what process did you use?

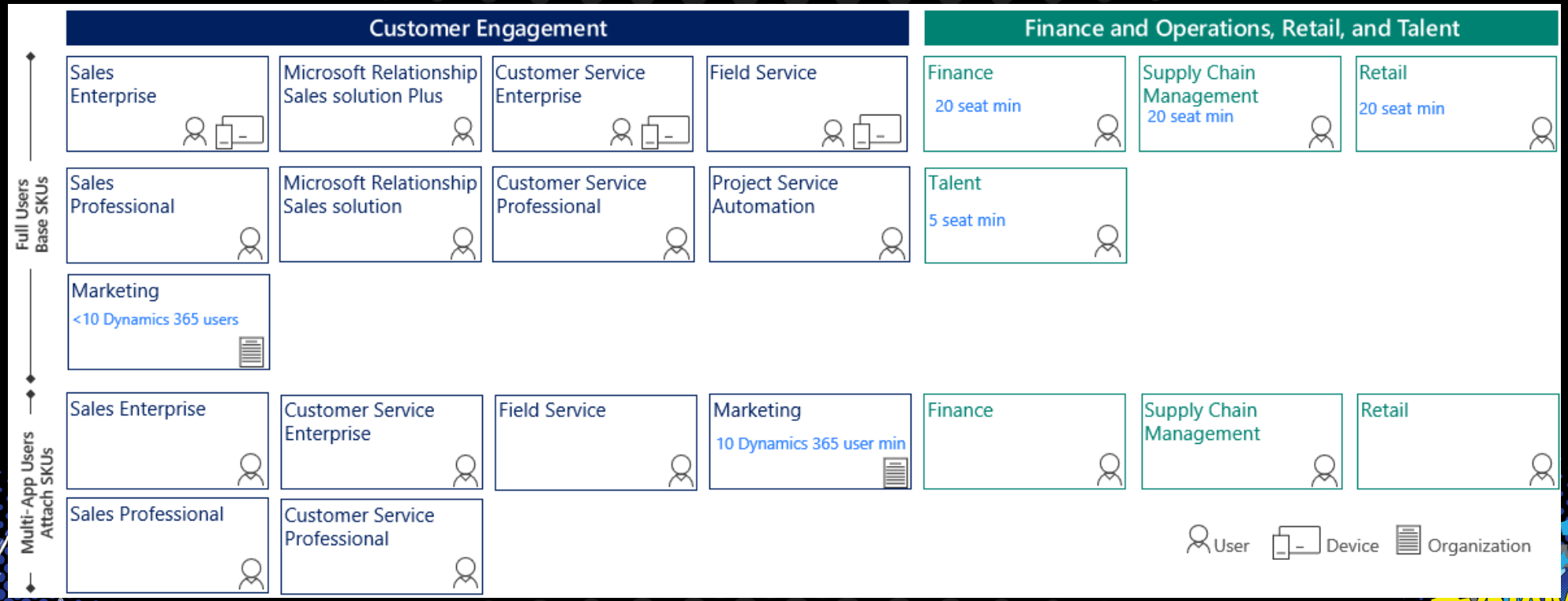
innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}
DYNAMICSCON LIVE
DUG

Old D365FO Licensing (Pre Oct 2019)



innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
NAMICSCON LIVE
DUG

New D365FO User Licensing



innov CONSULT
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

Base / Attach Combinations

Dynamics 365 base licenses per user	Dynamics 365 attach licenses per user										
	Commerce	CS Ent	CS Pro	Field Svc	Finance	HR	Proj Oper.	RA	Sales Ent	Sales Pro	SCM
Business Central Essentials			●							●	
Business Central Premium			●							●	
Commerce		●	●	●	●	●	●		●	●	●
Customer Service Enterprise (CS)				●					●	●	
Customer Service Professional (CS)											
Field Service		●	●					●	●	●	
Finance	●	●	●	●		●	●		●	●	●
Guides											
Human Resources (HR)		●	●	●			●		●	●	
Microsoft Relationship Sales solution Plus (MRSs Plus)		●	●	●		●	●				
Project Operations (Proj Oper.)		●	●	●		●			●	●	
Remote Assist (RA)											
Sales Enterprise		●	●	●							
Sales Premium		●	●	●		●	●				
Sales Professional			●								
Supply Chain Management (SCM)	●	●	●	●	●	●	●		●	●	

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}

DYNAMICSCON LIVE
DUG

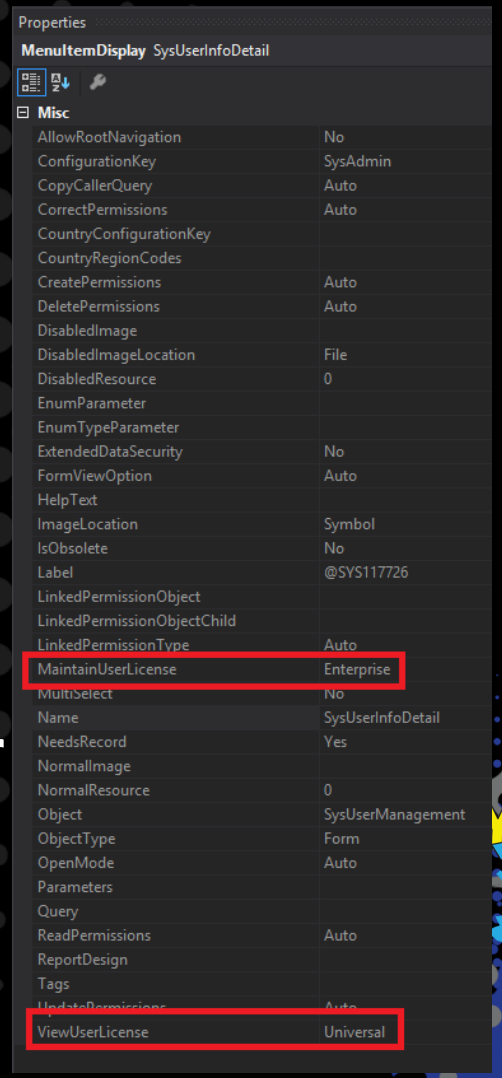
D365 User Licensing Mechanisms

- **Two licensing mechanisms:**
  - Entry Point Based
  - Privilege Based
- **Entry Point Licensing**
  - Three license types
    - Operations
    - Activity
    - Team Member
- **Privilege Based Licensing**
  - Breaks Operations level license down into different module SKUs
    - Finance
    - Supply Chain Management
    - Commerce
    - Project Operations
  - If user requires multiple licenses, then additional licenses can be ‘attached’ at a reduced price
  - User **must** be assigned a ‘base’ license before any ‘attach’ licenses can be used

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}
DYNAMICSCON LIVE
DUG

Entry Point Based Licensing

- **Based on access to entry points (menu items etc)**
- **Each entry point has two parameters**
  - MaintainUserLicense – used if access is Created, Update, Delete
  - ViewUserLicense – used if access is Read
- **It only takes one access at a higher license level for the user/role to require that higher license level**



Privilege Based Licensing

- Microsoft has designated certain privileges to require a particular license type
- Associations can be found in the LicensingServicePlansPrivilege table
- If user is assigned a privilege with IsUnique = 1 then that license is required
  - If multiple licenses are required will follow a base/attach model
- If IsUnique = 0 then any license listed will satisfy license requirement

SQLQuery8.sql - fp...inb0c62338a2 (100))* | SQLQuery7.sql - fp...inb0c62338a2 (96)) | SQLQu

```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT [SKUNAME]
      ,[PRIVILEGEIDENTIFIER]
      ,[PRIVILEGERECID]
      ,[ISUNIQUE]
  FROM [AxDB].[dbo].[LICENSINGSERVICEPLANSPRIVILEGE]
```

100 %

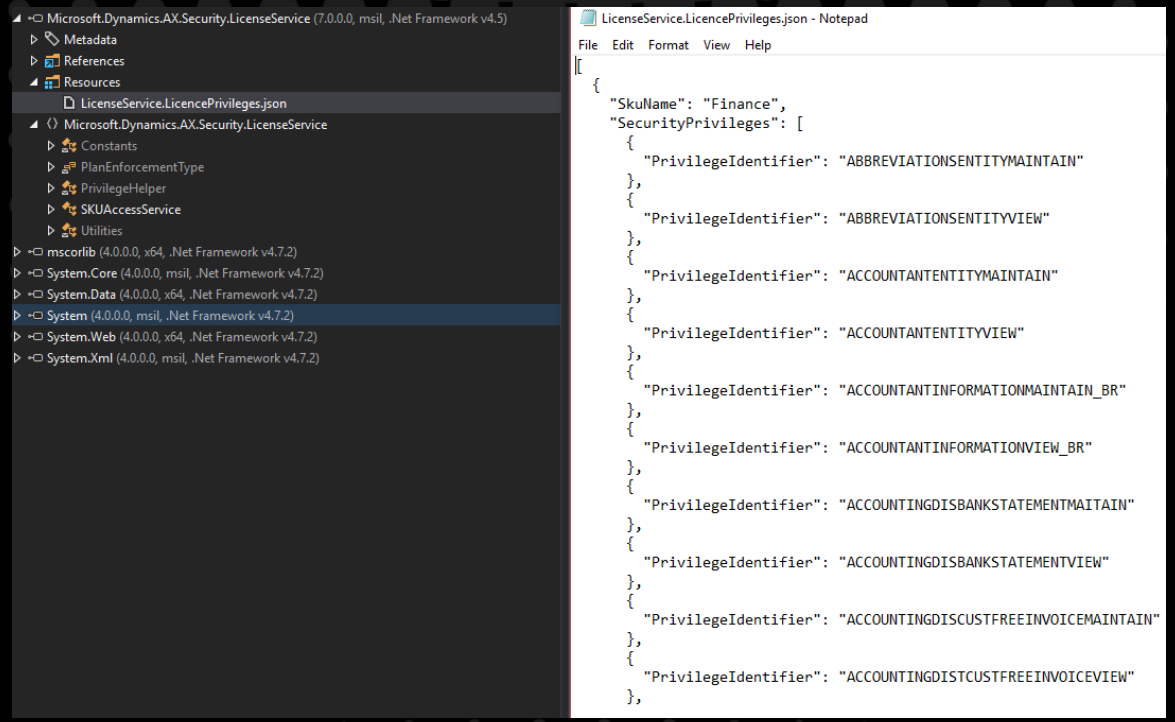
Results | Messages

	SKUNAME	PRIVILEGEIDENTIFIER	PRIVILEGERECID	ISUNIQUE
1	Finance	ABBREVIATIONSENTITYMAINTAIN	15252	0
2	Finance	ABBREVIATIONSENTITYVIEW	15254	0
3	Finance	ACCOUNTANTENTITYMAINTAIN	10473	1
4	Finance	ACCOUNTANTENTITYVIEW	10472	1
5	Finance	ACCOUNTANTINFORMATIONMAINTAIN_BR	2	1
6	Finance	ACCOUNTANTINFORMATIONVIEW_BR	3	1
7	Finance	ACCOUNTINGDISBANKSTATEMENTMAITAIN	4	1
8	Finance	ACCOUNTINGDISBANKSTATEMENTVIEW	5	1
9	Finance	ACCOUNTINGDISCUSTFREEINVOICEMAINTAIN	6	1

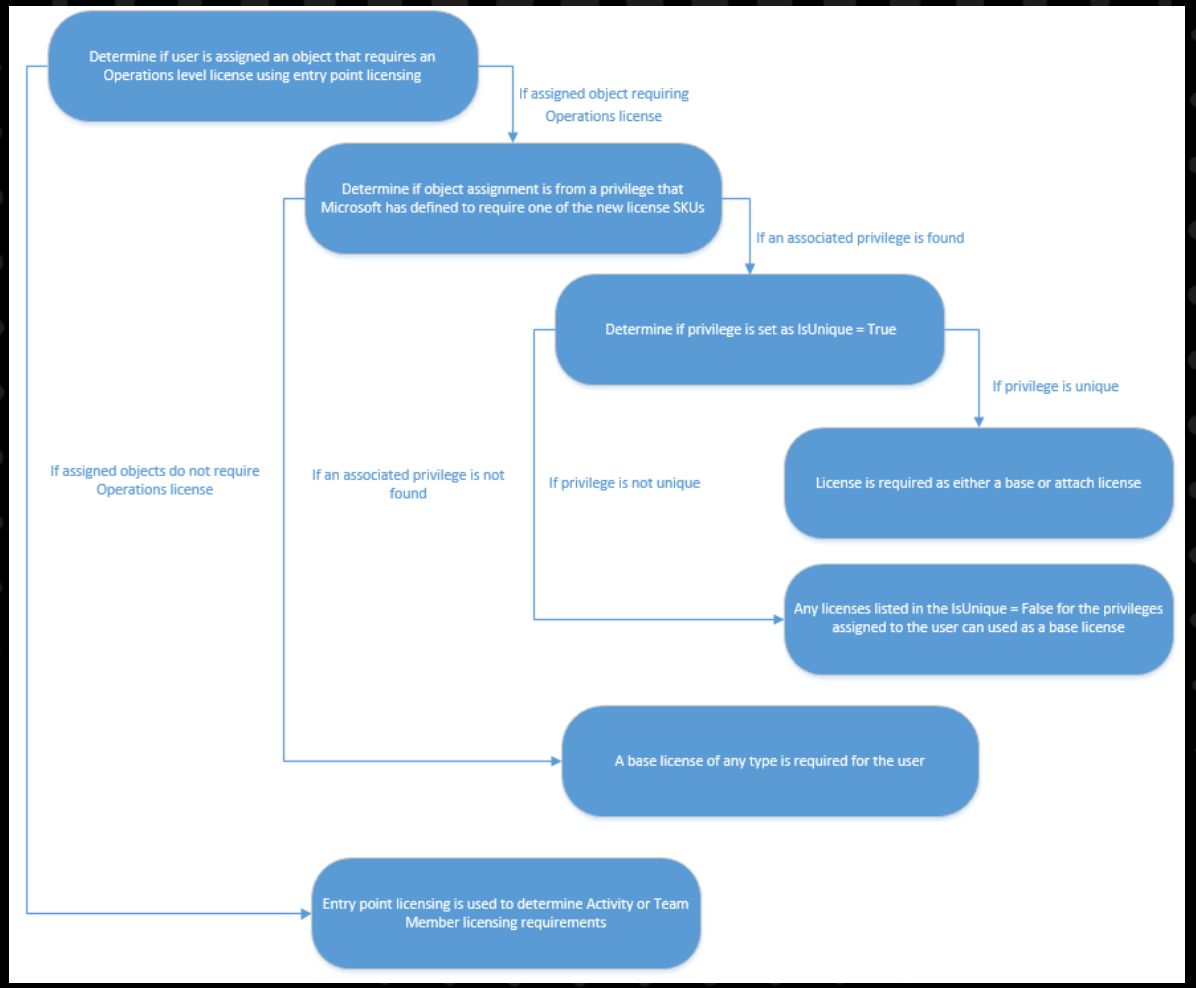
innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

Privilege Based Licensing

- **How is the LicensingServicePlansPrivilege table populated?**
  - Executing the User License Estimator Report
  - Populated by a static .json file that is stored in a DLL



How Do We Bring These Licensing Methodologies Together?

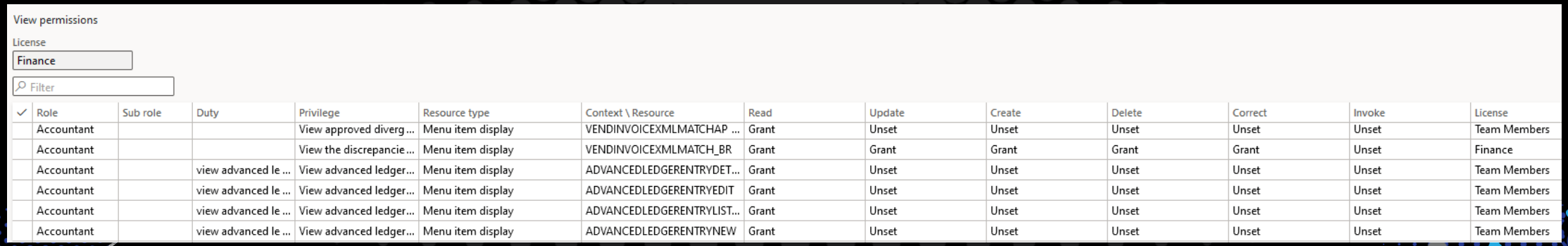


innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}

DYNAMICSCON LIVE
DUG

License Reporting in D365FO

- In System Administration -> Security Configuration -> For any role/duty/privilege select View Permissions



View permissions

License

Finance

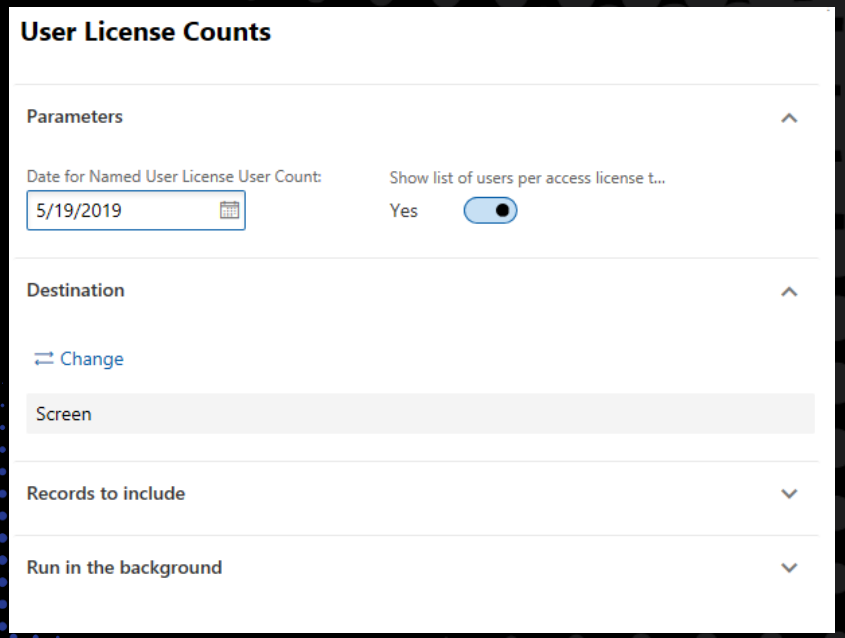
Filter

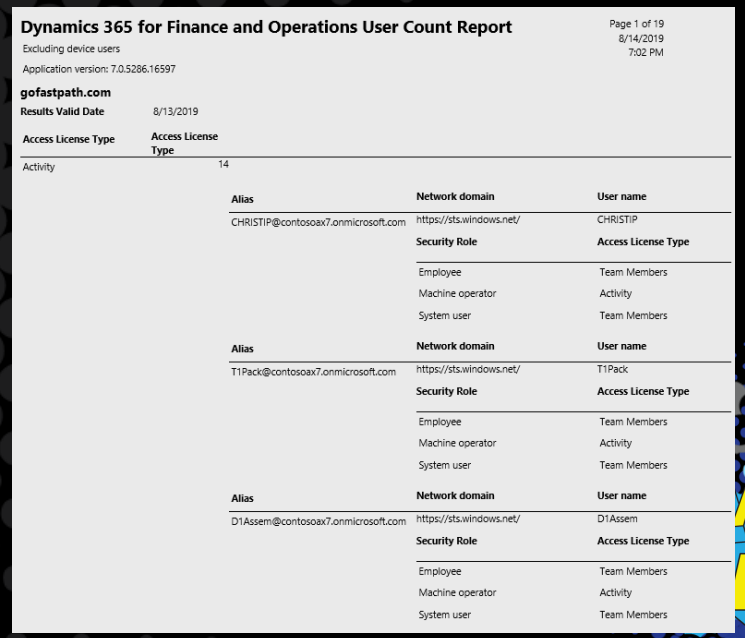
Role	Sub role	Duty	Privilege	Resource type	Context \ Resource	Read	Update	Create	Delete	Correct	Invoke	License
Accountant			View approved diverg ...	Menu item display	VENDINVOICEXMLMATCHAP ...	Grant	Unset	Unset	Unset	Unset	Unset	Team Members
Accountant			View the discrepancie ...	Menu item display	VENDINVOICEXMLMATCH_BR	Grant	Grant	Grant	Grant	Grant	Unset	Finance
Accountant		view advanced le ...	View advanced ledger...	Menu item display	ADVANCEDLEDGERENTRYDET...	Grant	Unset	Unset	Unset	Unset	Unset	Team Members
Accountant		view advanced le ...	View advanced ledger...	Menu item display	ADVANCEDLEDGERENTRYEDIT	Grant	Unset	Unset	Unset	Unset	Unset	Team Members
Accountant		view advanced le ...	View advanced ledger...	Menu item display	ADVANCEDLEDGERENTRYLIST...	Grant	Unset	Unset	Unset	Unset	Unset	Team Members
Accountant		view advanced le ...	View advanced ledger...	Menu item display	ADVANCEDLEDGERENTRYNEW	Grant	Unset	Unset	Unset	Unset	Unset	Team Members

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

License Reporting in D365FO

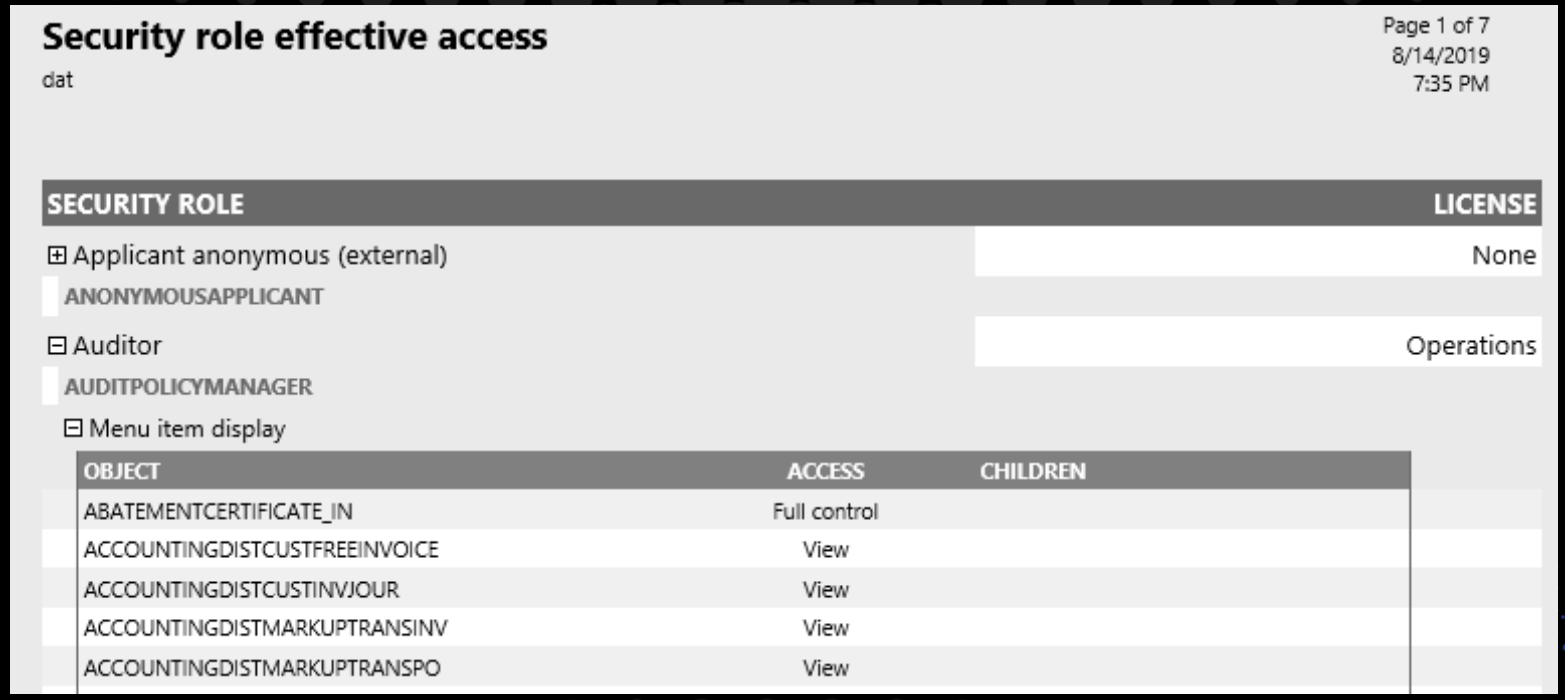
- **User License Counts**
  - System Administration -> Inquiries -> License -> User License Counts





License Reporting in D365FO

- System Administration -> Inquiries -> Security -> Security Role Access



Security role effective access

dat

Page 1 of 7
8/14/2019
7:35 PM

SECURITY ROLE	LICENSE
⊞ Applicant anonymous (external)	None
ANONYMOUSAPPLICANT	
⊟ Auditor	Operations
AUDITPOLICYMANAGER	
⊟ Menu item display	

OBJECT	ACCESS	CHILDREN
ABATEMENTCERTIFICATE_IN	Full control	
ACCOUNTINGDISTCUSTFREEINVOICE	View	
ACCOUNTINGDISTCUSTINVJOUR	View	
ACCOUNTINGDISTMARKUPTRANSINV	View	
ACCOUNTINGDISTMARKUPTRANSPO	View	

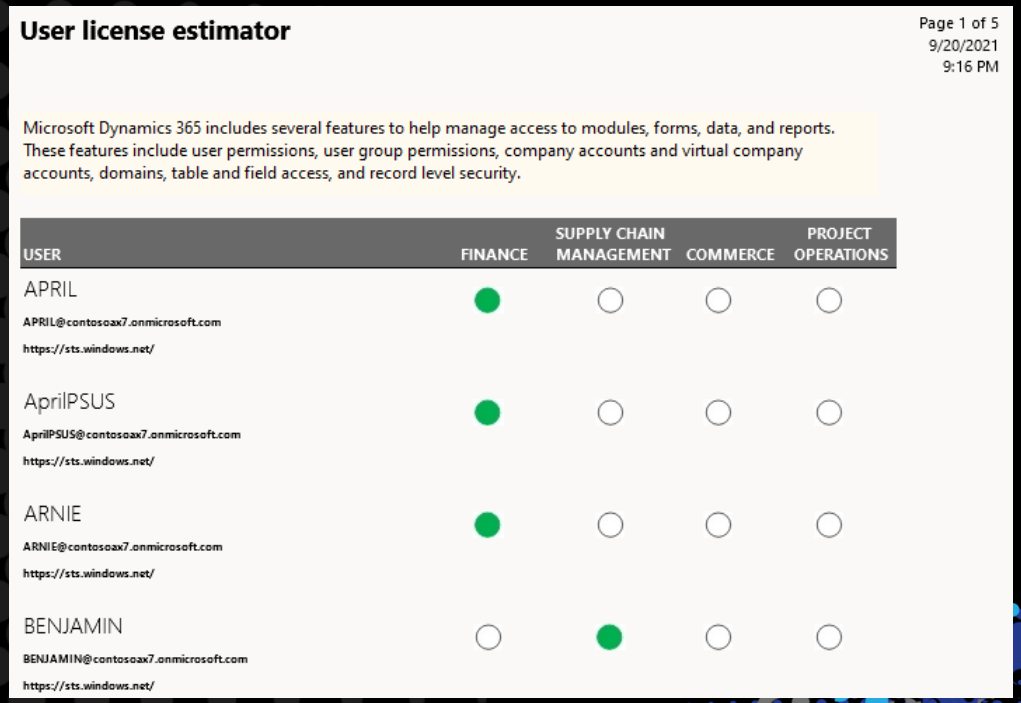
innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
OwnBackup
DYNAMICSCON LIVE
DUG

User License Estimator Report

- **Located at System Administration -> Inquiries -> License Reports -> User License Estimator**

- **Historically has had many issues and may show Incorrect results (PU31-PU36 all have some bug/issue with them)**

- **Current licenses (as of 10.0.25 are):**
  - Finance
  - Supply Chain Management
  - Commerce
  - Project Operations



User license estimator

Page 1 of 5
9/20/2021
9:16 PM

Microsoft Dynamics 365 includes several features to help manage access to modules, forms, data, and reports. These features include user permissions, user group permissions, company accounts and virtual company accounts, domains, table and field access, and record level security.

USER	FINANCE	SUPPLY CHAIN MANAGEMENT	COMMERCE	PROJECT OPERATIONS
APRIL APRIL@contosoax7.onmicrosoft.com https://sts.windows.net/	●	○	○	○
AprilPSUS AprilPSUS@contosoax7.onmicrosoft.com https://sts.windows.net/	●	○	○	○
ARNIE ARNIE@contosoax7.onmicrosoft.com https://sts.windows.net/	●	○	○	○
BENJAMIN BENJAMIN@contosoax7.onmicrosoft.com https://sts.windows.net/	○	●	○	○

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

Current Gaps with User License Estimator Report

- **Modifying out of box security**
  - Removing/adding access
  - Deny permissions
- **Doesn't show why a user requires a particular license**
- **Doesn't show based/attach options**
- **Doesn't give an overview of number of licenses of each type required**

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own {backup}

Manual Reporting Options

- Need to first determine user access to entry points
- Determine highest level of license required
- If Operations level license required, need to determine privileges assigned to user
- Reference data from LicensingServicePlansPrivilege table to determine required licenses
- D365FO Security Layer Licensing Excel File
- AX 2012 -> D365FO Licensing Comparison Excel File
- **For an automated solution for license reporting, please visit with a Fastpath team member**

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}

DYNAMICSCON LIVE
DUG

Steps to Save Money on Licensing Costs

- **Ensure current license assignments match user's requirements based on security**
- **Implement least privilege security for users**
  - Take a risk-based approach to implementing
- **Look for instances where users or roles are over provisioned and either:**
  - Remove offending access
  - Create a new role with correct security

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

Tillamook Experience

- Originally, purchased the FastPath solution
- Had SMEs complete task recordings to assign privileges
- We decided it was too granular and hard to maintain
- Instead, we assigned based on Active Directory
- Security is based on roles in the active directory, not at the individual level
- Now we are revisiting to ensure Segregation of Duties

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
OwnBackup
DYNAMICSCON LIVE
DUG

Resources

- Task Recorder – D365FO
- Task Recorder – AX 2012
- D365FO Blog
- Develop and Implement Least Privilege Security for D365FO
- Task Recorder Parser GitHub Project
- Microsoft Dynamics 365 Licensing Guide – Aug 2022
- Current State of D365FO User Licensing
- D365FO User Licensing Blog Post Series
- Least Privilege Security Whitepaper
- D365FO Security Blog
- D365FO Security Audit Field Manual
- D365FO Resources From Fastpath

innovia CONSULTING
INGRAM MICRO CLOUD
SPS COMMERCE
Own{backup}
DYNAMICSCON LIVE
DUG

Questions?

Alex Meyer

Email: meyer@gofastpath.com
Blog: http://msftcloudblogs.com
GitHub: https://github.com/ameyer505
Twitter: https://twitter.com/alexmeyer_ITGuy
D365FO Security Course: http://d365fosecurity.com

Robin Finnell

Email: rfinnell@tillamook.com
LinkedIn: linkedin.com/in/tillamookrobinfinnell

PowerPoint available at:
https://alexdmeyer.com/resources/downloads/