

Author: DGV Team

# Security and Compliance Studio 10.0.39.43

**Release Notes** 

### Contents

1.	Introduction	6
1.1 1.2 1.3 1.4 1.5 1.6	Purpose Audience Product release information Deliverables Common features Certificate renewal.	6 6 7 7
2.	What's New in Security and Compliance Studio 10.0.39.43	10
2.1 2.2 2.3 2.4	User audit log for sensitive data Securable tree view Security request history track Enhanced SoD predefined list	12 15
3.	Features introduced in last few releases of Security and Compliance Studio	18
3.1 3.2 3.3 3.4 3.5 3.6 3.7 3.8	Segregation of duties sets Security requests enhancements and workflow Export security explorer objects to excel in a de-normalized format Merge security scenarios and match role Mark any Security Role as Active/Inactive Recording steps to scenario. Override permission based on scenarios Option to mark, track and audit security objects providing access to sensitive data	24 35 35 35 36 36
3.9 3.10	Option to create a duty from Matched Privileges grid in Match roles form Option to import and export data using Data Entities in Security and Compliance Studio	44
3.11 3.12	Option to compare Security Snapshots stored in the security setup Enhanced Audit log capability to capture all the changes from development space (AOT) as well into Audit Log	46
3.13	Option to create one or more privileges and also one or more duties while merging roles.	
3.14 3.15	Ability to create scenarios from D365 module menus Snapshots based performance and scalability enhancements	51

3.16	Improved "Create role wizard" based on a grid framework	54
3.17	Accessing Security Explorer from all D365 FOE forms	54
3.18	Option to create duties and SOD compliance check as well while merging roles	
3.19	Importing New Users while Synchronizing the group users with the Active	
	Directory group members	56
3.20	Uptake RapidValue BPM Suite Scenarios directly as SCS Security Scenarios	56
3.21	Enhanced Segregation of Duties	58
3.22	Organization risk Register	59
3.23	AAD related SoD Validations across SCS	
3.24	Security Explorer displaying Tables, Service operations and Data Entities entry	
	point's type	60
3.25	Performance Optimization	60
3.26	A new "Share" workspace	60
3.27	AAD groups' information in D365FO	61
3.28	Verify SoD rules in Stand in	62
3.29	Chart to give an overview of number of users and their last logging details	62
3.30	Asset classification User Interface	63
3.31	A List page with Workflow delegation details	64
3.32	User groups – combined two tabs in one	64
3.33	New export/import role functionality	
3.34	License count changes	65
4.	Bug fixes	68
4.1	Security and compliance studio 10.0.39.43	68
4.2	Security and compliance studio 10.0.37.42	
4.3	Security and compliance studio 10.0.36.41	
4.4	Security and compliance studio 10.0.36.40	
4.5	Security and compliance studio 10.0.34.39	
4.6	Security and compliance studio 10.0.32.38	
4.7	Security and compliance studio 10.0.31.37	
4.8	Security and compliance studio 10.0.29.36	
4.9	Security and compliance studio 10.0.28.34	
4.10	Security and compliance studio 10.0.27.33	
4.11	Security and compliance studio 10.0.26.32	
4.12	Security and compliance studio 10.0.26.31	
4.13	Security and compliance studio 10.0.25.30	
4.14	Security and compliance studio 10.0.24.29	
4.15	Security and compliance studio 10.0.22.27	
4.16	Security and compliance studio 10.0.18.1	
4.17	Security and compliance studio 10.0.12.5	
4.18	Security and compliance studio 10.0.12.9	
4.19	Security and compliance studio 10.0.12.3	
4.20		,5
	Security and compliance studio 10.0.12.2	73
	Security and compliance studio 10.0.12.2	
4.21 4.22	Security and compliance studio 10.0.12.2 Security and compliance studio 10.0.12.1 Security and compliance studio 10.0.10.1	73

4.23	Security and compliance studio 10.0.6.11	. 73
4.24	Security and compliance studio 10.0.6.10	. 73
4.25	Security and compliance studio 10.0.6.9	. 73
4.26	Security and compliance studio 10.0.6.8	. 74
4.27	Security and compliance studio 10.0.6.7	. 74
4.28	Security and compliance studio 10.0.6.6	. 74
4.29	Security and compliance studio 10.0.6.5	. 74
4.30	Security and compliance studio 10.0.6.4	. 74
4.31	Security and compliance studio 10.0.6.3	. 74
4.32	Security and compliance studio 10.0.6.2	. 75
4.33	Security and compliance studio 10.0.6.1	. 75
4.34	Security and compliance studio 10.0.3.3	. 75
4.35	Security and compliance studio 10.0.3.2	. 75
4.36	Security and compliance studio 10.0.3.1	. 75
4.37	Security and compliance studio 10.0.1.3	. 75
4.38	Security and compliance studio 10.0.1.2	. 75
4.39	Security and compliance studio 10.0.1.1	. 75
4.40	Security and compliance studio 81.3.2.1	. 76
4.41	Security and compliance studio 81.3.1.1	. 76
4.42	Security and compliance studio 81.2.1.1	. 76
4.43	Security and compliance studio 81.1.2.1	. 76
4.44	Security and compliance studio 81.1.1.1	. 76
4.45	Security and compliance studio 81.20.3.1	. 76
4.46	Security and compliance studio 81.20.2.2 *(This build was created as the earlier	
	deployable package had some issues)	. 76
4.47	Security and compliance studio 81.20.2.1	. 76
4.48	Security and compliance studio 81.20.1.1	
4.49	Security and compliance studio 1804.15.2.1	
4.50	Security and compliance studio 1804.15.1.1	. 77
4.51	Security and compliance studio 1712.12.1.1	. 77
5.	Changed or deprecated features	.78
5.1	Deprecated features 10.0.31.37	
5.2	Deprecated features older versions	. 78
6. Know	n issues	.79

## **Document Information**

Title	Security and Compliance Studio 10.0.39.43
Subtitle (Subject)	Release Notes
Solution Suite	GRC; Security and Compliance Studio
Category	Release Notes
Author	SCS Team
Published Date	4/3/2024
Status	Final

#### © Copyright To-Increase 2023. All rights reserved.

The information in this document is subject to change without notice. No part of this document may be reproduced, stored or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of To-Increase B.V. To-Increase B.V. assumes no liability for any damages incurred, directly or indirectly, from any errors, omissions or discrepancies between the software and the information contained in this document.

## 1. Introduction

## 1.1 Purpose

This document highlights new features and enhancements that ship in the new **Security and Compliance Studio 10.0.39.43** release from To-Increase. This release is compatible with the version of Microsoft Dynamics 365 for Finance and Operations, **10.0.36 or later**.

## 1.2 Audience

This document is intended for new or current Security and Compliance Studio partners and customers. Some knowledge of D365 for Finance and Operations and prior versions of Security and Compliance Studio, previously Dynamic Security Management (DSM), for Microsoft Dynamics AX 2012 is assumed.

## 1.3 Product release information

**Security and Compliance Studio 10.0.39.43** for Dynamics 365 Finance and Dynamics 365 Supply Chain Management (10.0) is built upon D365 version [Minimum GA version required]. Since Microsoft maintains a no breaking changes policy, the fact that this release is built on this version means that it can be applied to an environment running on D365 version [Minimum GA version required] or any later version and the application should compile without any issues. However, as we have only functionally validated this version against D365 version [latest GA version], we recommend applying our TI product release on that MS version as well. If you deviate from this (and thus apply the release to a different version), we recommend performing a more thorough round of testing before applying the release to a production environment.

This is summarized in the following table.

Release of		[TI-Version	Minimum required	Validated against	Compatible with
[TI-Produc		number]	D365 version	D365 version	D365 version
05/04/20	23	10.0.39.43	10.0.36	10.0.39	10.0.36 and above

In case of an Error, To-Increase may provide a Hotfix on a reasonable efforts basis in a way it considers appropriate in its discretion. To-Increase cannot be obliged to provide Hotfixes if Client has not deployed the latest Release or the Release second to the latest Release and/or is not using a supported version of Microsoft Dynamics.

To ensure our customers can fully leverage the latest enhancements, features, and quality improvements, we are committed to providing increased support by keeping them updated with the most recent releases. Our data indicates that customers on the latest version experience fewer issues and requests, demonstrate greater resilience, and effectively enhance their organizational efficiency.

More information about our latest available product versions, the latest validate GA-versions from Microsoft as well as the Minimum MS version required, please visit this page : Knowledge Base - Support - To-Increase

## 1.4 Deliverables

Security and Compliance Studio is released on the following Microsoft Dynamics 365 for Operations Build.

Deliverable	Description
Solution package	Security and Compliance Studio is delivered as a Microsoft Dynamics Lifecycle Services (LCS) solution package.
Software deployable package	Security and Compliance Studio 10.0.39.43 and SCS-fix deployment issue
Release notes	This document is provided with the Security and Compliance Studio product deliverables.
Implementation methodology	The solution package contains a <i>Security and Compliance Studio</i> <i>implementation methodology</i> that provides detailed step-by-step instructions on how to install, learn, and implement Security and Compliance Studio.
Getting started BPM library	The solution package includes a <i>Getting started with the Security</i> <i>and Compliance Studio</i> BPM library. This library contains a number of task guides that showcase some of the key capabilities of Security and Compliance Studio.
Documentation BPM library	The solution package includes a <i>Security and Compliance Studio</i> <i>documentation</i> BPM library. This library contains a comprehensive set of task guides that document how to use <i>Security and</i> <i>Compliance Studio</i> for your BPM activities. This documentation is provided in U.S. English only.
Authentication assets	A To-Increase security certificate is provided to allow trusted installation of the provided model files and ISV license files.
Process data package	The solution package provides a simple Security and Compliance Studio <i>demo</i> process data package that can help you get started from LCS.

## 1.5 Common features

To-Increase is offering various different add-on solutions. Some features and technical solutions are common or could be common for all of our solutions on the Dynamics 365 Finance and Operations platform. As of November 2022, we will start leveraging a new common library model.

The common library model will be a centralized location where the new common features will be added automatically and customers don't have to make an additional effort to update the build pipelines after the first enablement of this model.

ISV licensing is technically supported with a code signing certificate. The certificate we have to use is expiring every three years, next up for renewal in 2023. In the near future, our solutions will refer to this common model for the code signing certificate, instead of maintaining it separately in all our solutions.

Next to technical content, the common library comes with features which are beneficial to our customers. E.g. a Solutions Management dashboard gives a clear view of currently installed versions, status of license, option to renew licenses without any downtime, easy access to release notes and documentation, and the ability to leave feedback through the in-app feedback system.

Filter	Installed only		Advanced Discrete Manufac	turing	>
Solution	↑ Installed version	Status			
Advanced Discrete Manufactu	ri	×		LUTION IS NOT INSTALLED	
Advanced Project Managemer	nt	×	Solution description		
Anywhere Mobility Studio		×	Help manufacturers solve prob	plems and streamline process flows.	
Business Integration Solution	10.0.99.999	$\oslash$			
Data Entry Workflow		$\times$	License	Status Expiry date	:
Data Modeling Studio		×	Construction	8	
Data Quality Studio	10.0.18.2	$\otimes$	Equipment	<b>A</b>	
DynaRent	10.0.28.43	0	Advanced Project Management	nt 🛆	
PLM Integration for Engineerir		×	Product Engineering a	8	
RapidValue BPM Suite	10.0.26.37	$\odot$			
Security and Compliance Stud		×			

On all To-Increase forms, there is on the left-top of the forms a smiley icon in the menu where you can provide us feedback, suggestions and ideas so we can learn how improve our solutions.

			?
To-Increase wou	ıld love y	our feed	back!
Please rate your experie	nce in using th	e All solution	is screen.
🔵 5 - Excellent			
4			
3			
2			
🔵 1 - Poor			
Please tell us why you ch would help us improve o			nsights
Thank you for providing	us feedback!		
Your privacy is importan don't include any persor			acy, please

## 1.6 Certificate renewal

The security certificate, that expires every 3 years, ensures that our customers have valid To-Increase software installed and not an unlicensed copy. This digital check is executed during installations and upon installing the license files, ensures that they have legitimate software installed. The previous security certificates for To-Increase solutions would expire on June 9, 2023.

This release (and releases beyond) contains the new certificate and a new feature within the Solution Management Workspace. After installing the update, the security certificate renewal can be completed in 3 simple steps.

Step 1: Install the update and navigate to the Solution Management Workspace

Step 2: Click the 'Retrieve available licenses' in the action pane

Step 3: Validate the licenses for correctness and completeness and click import

Click here for more information on the Solution Management Workspace.

# 2. What's New in Security and Compliance Studio 10.0.39.43

## 2.1 User audit log for sensitive data

A new feature will allow the system admin to trace potential security violations regarding business sensitive information.

Using the field picker tool or manually adding, the user can now record the fields that are providing access to sensitive data, creating a 'Sensitive data setup' that will be used to track any changes to those fields.

This new form can be found under *Security and Compliance Studio -> Inquires -> Sensitive data setup*. Please refer to the screenshot below:

DE	NO	reco	ording .   Standard vie	w V								
Se	en	sit	ive data setu	ıр								
Nan	ne			Crea	ted by	Created (	date and time	Security r	ecord status	Owner		
DE	МС	) rec	ording .	Ad	min	4/2/202	24 08:58:58 AM	Open				
De	esci	iptic	'n									
Ge	ene	ral										
+	- A	dd	Delete Field picker									
6	3	Table	name		Reference field name		Field label		displayObservat	ion		
		Logis	sticsLocation		Description		Name or description					
		Hcm	WorkerTitle		OriginalHireDateTim	ne	Original hire date		Table 'HcmWor	kerTitle' is dat	effective or support	s inheritance and
		DirPe	erson	$^{\vee}$	NameAlias	~	Search name					
-								1				
Qu	ler	y										
E	dit	quer	У									
0	3	Quer	y name	Tab	ole name							
		DirPe	erson 🗸	Dir	rPersonStaging							
1												
Us	ers											
+	- A	dd	🗓 Delete									
	С	С	User ID		Name	n	etworkAlias		networkDomain	1		
	9		fmihoc	~	fmihoc	f	mihoc@to-increase.com		https://sts.wind	dows.net/to-in	crease.com	
			icretu	1	icretu	i	cretu@toincrease.onmicro	soft.com	https://sts.wind	dows.net/		
			Admin		Admin	f	mihoc@toincrease.onmicr	osoft.c	https://sts.wind	dows.net/		
L												

This page has three sections:

displayObservation

- General section: In this section, user can use the 'Field Picker' option to navigate to desire forms and pick the fields that need are providing access to sensitive data, or you can use the 'Add' option to manually add the table and the field using the lookups.
- Query section: For each table recorded you can also add query conditions using the 'Edit query' option. For example, you can add fields from the Address table and then add query condition where the address is marked as Private. That means the address information is sensitive data only if it's marked as 'Private'.
- User: The user section denotes the users that can see the log generated for this current sensitive setup.

When recording /adding fields you might see the following observations:

Table 'HomWorkerTitle' is date effective or supports inheritance and it requires a staging table to be mapped in order to capture the log. Please navigate to 'Security and compliance studio -> Setup -> Sensitive data condition setup' and create table mapping Table 'DirPerson' is date effective or supports inheritance and it requires a staging table to be mapped in order to capture the log. Please navigate to 'Security and compliance studio -> Setup -> Sensitive data condition setup' and create table mapping.

Observation example: Table '(table name)' is date effective or supports inheritance and it requires a staging table to be mapped to capture the log. Please navigate to 'Security and Compliance studio -> Setup -> Sensitive data condition setup' and create table mapping."

This means that the selected table is part of an exception and cannot be used to validate the data against it, so we need to create a table mapping that will be replacing the original table in the validation process. The mapping table should be a staging table or a child table that has the field(s) in question (the fields we

are trying to mark as sensitive).

Navigating to Security and Compliance studio -> Setup -> Sensitive data condition setup' and create table mapping will open the form. Here we can create the mapping.

)	С	Main table	Stagi	ng tab	ble			
	_	DirPartyTable	DirPa	artyTa	bleAttachmentsStaging			
0		DirPerson	DirPe	DirPersonStaging				
		DirPersonName	NameHistoricalStaging					
		LogisticsPostalAddress	Logis	sticsPo	ostalAddressElectronicContactV2Staging			
+	Add	🗊 Delete 🛛 Generate n	napping					
+			napping					
+	Add	Main table field	napping	〕 ↑	Stagging table field			
+00			napping	〕 ↑	Stagging table field AnniversaryDay			
+ 0		Main table field	napping	〕 ↑				
+ 0		Main table field AnniversaryDay	napping	 ↑	AnniversaryDay			
+00		Main table field AnniversaryDay AnniversaryMonth	napping	↑	AnniversaryDay AnniversaryMonth			
+ 0		Main table field AnniversaryDay AnniversaryMonth AnniversaryYear	napping	↑	AnniversaryDay AnniversaryMonth AnniversaryYear			

The mapping can be manually created using the 'Add' button to add the field mapping. Or we can use the 'Generate mapping' option to automatically determine the field mapping. In this case the fields that have the same name on both tables will be added.

# NOTE: There are exceptions where the field name from 'Main table' is different from the field on the 'Staging table'. E.g.: 'BirthDay' and 'Day of birth'. Manual mapping is required in this case.

After the mapping is completed the message from the Observation will be removed. Now, when editing the fields from the Sensitive data setup will be capture under a log. The new log can be seen opening the "Security and Compliance studio -> Inquiries -> Sensitive data log".

nsitive data log								
tandard view ~								
ATE RANGE								
om date To da								
/1/2023	2024 🖽	IJ						
er ID Table	name							
	nume							
C Table label	Modified		Description	Event created by	Sensitive data setup name	Event date ⊽↓		
Addresses		sPostalAddress		Admin	Test from scratch	11/2/2023 12:44:54 PM		
Position details	2	itionDetail		Admin	HCMPositionDetail	11/2/2023 12:44:37 PM		
Customers	CustTab	le		Admin	Custtable - credit	11/2/2023 12:34:58 PM		
Customers	CustTab	le		Admin	Custtable - credit	11/2/2023 12:15:53 PM		
Customers	CustTab	le		Admin	Custtable - credit	11/2/2023 10:19:55 AM		
Order lines	SalesLin	e		Admin	InventDim	10/30/2023 11:47:26 AM		
Position details	HcmPos	sitionDetail		Admin	HCMPositionDetail	10/30/2023 11:31:10 AM		
Position details	HcmPos	sitionDetail		Admin	HCMPositionDetail	10/26/2023 12:13:17 PM		
Position details	HcmPos	itionDetail		Admin	Position - test	10/11/2023 7:03:43 AM		
Addresses	Logistic	sPostalAddress		Admin	Test worker address	10/10/2023 9:23:45 AM		
Addresses	Logistic	sPostalAddress		Admin	Test worker address	10/10/2023 9:23:31 AM		
User Information	UserInfo	, ,		Admin	User data	8/10/2023 10:36:58 AM		
User Information	UserInfo	, ,		Admin	User data	8/10/2023 10:36:40 AM		
Vendors	VendTab	ble		Admin	Vendor table	8/10/2023 10:31:55 AM		
Global address book	DirParty	Table		Admin	Vendor table	8/10/2023 10:31:24 AM		
User Information	UserInfo	, ,		Admin	User data	8/10/2023 10:12:12 AM		
User Information	UserInfo	•		Admin	User data	8/10/2023 10:08:32 AM		
TAILS							=	
Reference field name	Field label	Event type	Value from		Value to	Form name	Form label	Created date and time
) Street	Street	Record modified	413 Oak Street TES	г	413 Oak Street TDEMO1	LogisticsPostalAddr	ess Manage addresses	10/10/2023 9:23:31 AM

The Sensitive data log can be filtered based on date, user ID and table name.

NOTE: A part of the log can be seen only by the users that are assigned on the Sensitive data setup.

## 2.2 Securable tree view

This feature will allow an overview of the securable objects for a better and easier visibility and control on which objects are being used in what menu items to provide optimum security access.

By selecting a securable object (role, duty or privilege) you can immediately see in the menu lookalike tree node where the object has access to and drill down for more details.

rable tree view						
e permission on selected object	DETAILS					
object types Value						
Budget contributor	ch Explore					
ne Description	○ ② Name	1 AOT name	Description Ent	ry point type Object name	Object type	Access right
ETBUDGETCONTRIBUTO Enters and approves budget plan requests	General ledger parameters	LedgerParameters	Me	nu item display LedgerParameter	s Form	View ~
Menu Accounts payable					_	
Accounts receivable	Security diagnostics					
Asset management	Show all access 🖓 Explore					
Audit workbench Budgeting	ObjectType	AOT name	Label	Access level	License type (on-premise)	License type (cloud)
Cash and bank management	O Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor	View	Team members	Team members
Common	Duty	BUDGETBUDGETPROCESSPOLICIESINQUIRE	Inquire into budget process policies		Team members	Team members
Consolidations	Privilege	LedgerParametersView	View general ledger parameters	View	Team members	Team members
Cost accounting	· · · · · · · · · · · · · · · · · · ·	and the second second second	Anter Researce Ander bergulaters	1.1211		
Cost management						
Credit and collections						
Demo data						
Expense management						
Fiscal books	Form level details					
Fixed assets						
Fixed assets (Russia)	FORM MENU ITEMS					
Fleet management	🖧 Explore					
General ledger	Control name	Control label	Control type	Object name from menu item	Object type from menu	item
Allocations	<ul> <li>LedgerOppositeSignUpdate</li> </ul>		FormBuildFunctionButtonControl	LedgerOppositeSignUpdate	Action	
Calendars Chart of accounts	EximParameters_IN		FormBuildFunctionButtonControl	EximParameters_IN	Display	
Chart of accounts Currencies						
Deferrals						
Deferrals setup						
Financial report setup						
Financial reports setup						
Inquiries and reports	TABLE PERMISSIONS					
Journal entries	<ul> <li>Data source name</li> </ul>	Control type	DataSourceTable			
Journal setup	<ul> <li>LedgerParameters</li> </ul>	Data source	LedgerParameters			
Ledger setup	TaxParameters	Data source	TaxParameters			
Advance adjustment parameters	NumberSequenceReference	Data source	NumberSequenceReference			
Cash control configuration	AssetParameters	Data source	AssetParameters			
Cash position parameters	InventDimSetupGrid	Data source	InventDimSetupGrid			
Check voucher series	CustParameters	Data source	CustParameters			
Date intervals	FORM CONTROLS					
	Control name					
		Control type	Object name from menu item		Needed permissions	Ŷ
Fiscal calendars					Manual	
General ledger parameters	O UpdateDelimiter	FormBuildFunctionButtonContr	ol DimensionSegmentSeparato	orDataUpda Action	manual	
Fiscal calendars General ledger parameters INPC rates		FormBuildFunctionButtonContr	ol DimensionSegmentSeparato	orDataUpda Action	manyai	
Fiscal calendars General ledger parameters INPC rates Ledger		FormBuildFunctionButtonContr	ol DimensionSegmentSeparate	orDataUpda Action	manuar	
Fiscal calendars General ledger parameters INPC rates		FormBuildFunctionButtonContr	ol DimensionSegmentSeparato	rDataUpda Action	man Man	

After selecting a securable object, the tree node will update with blue markers based where access is provided. In this example the 'Budget contributor' role was selected and we can see all the modules where it has access.

We can expand the tree node to navigate to the entry points level for more details.

This page contains the following section:

- **Details**: The details section shows the selected menu items or the menu items from the selected group.
- Security diagnostics: This section shows the securable objects where the selected menu item has access to. Here there are two options Show all access button/ Show access based on selection (same button, label will toggle based on clicking it) :
  - a) Show all access button that will show all the security objects (roles, duties and privileges) from the system where the selected menu items have access to
  - b) Show access based on selection button (default option) will show all the security objects from the main selected object (in this example 'Budget contributor' role)

now all access 🖓 Explore			
ObjectType	AOT name	Label	Access leve
) Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor	View
Duty	BUDGETBUDGETPROCESSPOLICIESINQUIRE	Inquire into budget process policies	View
Privilege	LedgerParametersView	View general ledger parameters	View
	on & Explore		
iow access based on selecti	on 🖧 Explore AOT name	Label	Access lev
ow access based on selecti		Label Auditor	Access leve View
now access based on selecti	AOT name		
ow access based on selecti ObjectType Role	AOT name AUDITPOLICYMANAGER	Auditor	View
objectType Role Role	AOT name AUDITPOLICYMANAGER BUDGETBUDGETCLERK	Auditor Budget clerk	View View
Role Role Role	AOT name AUDITPOLICYMANAGER BUDGETBUDGETCLERK BUDGETBUDGETCONTRIBUTOR	Auditor Budget clerk Budget contributor	View View

# NOTE: Security diagnostics section is similar with the 'Security diagnostics' option from standard D365FO that can be found on every form.

- Form level details: This section it's divided into three grids as follows:
  - a) <u>Form menu items</u>: if the selected entry point (from Details grid) is form type it will display all the other menu items that are found on the form's level.

On form level there are multiple options/buttons that are opening other forms. Here these forms are displayed so you will know that if you want to provide full access to a form you need to provide access to the forms that are opening from the buttons available on that form.

- b) <u>Table permissions:</u> it will display all the tables behind the datasources of the selected entry point on the Details grid.
- c) <u>Form Controls</u>: some form control require 'manual persmission' that is set on the form's properties by the developer/Microsoft. These controls require the specific access in order to access them.

In the Details grid you can modify the 'Access level' of the entry points. This will enable the 'Override permission on selected object' button that will allow you to modify the access level of the item.

Securable tree view								
Override permission on selected object								
Security object types Value Role V Budget contributor								
AOT name Description	0	⊘ Name ↑	AOT name	Description	Entry point type	Object name	Object type	Access right
BUDGETBUDGETCONTRIBUTO Enters and approve	budget 🥥	General ledger parameters	LedgerParameters		Menu item display	LedgerParameters	Form	Full control V
R plan requests							l	
Expense management     Fiscal books						-		

When using the option, a dialog form will be opened with the summary of the changes. Clicking 'Ok' it will apply the new changes, modifying the access level of the security object and refresh the tree node.

	rride permissio troles to assign overrie ObjectType		AOT name	
0	Role	Budget contributor	LedgerParameters	
0	AOT name	Name	Entry point type	Access rig
0		Name General ledger p		Access rig

OK Cancel

## 2.3 Security request history track

We had a request to have a **Workflow-enabled user changes requests history,** to link the Audit Log entries to the Security Request, for example, when a new user requested has been approved and the user has been created a new Audit Log record will be recorded, but we are not able to track it if it was generated by now we know that the Audit Log record has been created from a Security Request and we know who approved it and when that did happen.

For this we have added a new column into the 'Security history' that can be access from *Security and Compliance -> Workspaces -> Security audit.* 

The new column will display the name of the 'Security Request' if the audit trails was generated by one. A new button was added, and it will be enabled when a record with 'Security request' has been selected.

Audit						
Security history	Audit log report Open securit	ty request history ···· Me	pre			
Role history	₽ Filter					
User history	<ul> <li>Event date and time 3/13/2024 12:03:05 PM</li> </ul>	Event created by Admin	Event type Duty created	Company *	Description Duty DutyUniqueProjectTest1 created	Security request refere
Segregation of duties rules	3/13/2024 12:03:04 PM	Admin	Role created	*	Role RoleUniqueProjTest1 created	
Segregation of duties conflicts	3/12/2024 10:53:41 AM	Admin	Role modified	*	Role Purchasing agent modified	
Stand-ins	3/12/2024 10:53:41 AM	Admin	Duty modified	*	Duty Approve request for quotations modified	
	3/11/2024 1:02:57 PM	Admin	Role unlocked	*	Role Warehouse worker unlocked	Unlock role
Data security	3/11/2024 1:02:57 PM	Admin	Stand-in rule created	*	Stand-in rule for user " has been created	Add stand-in
Azure AD domains	3/11/2024 1:02:45 PM	Admin	Stand-in rule deleted	*	Stand-in rule for user 'Lola' has been deleted	Cancel stand-in
Asset classification	3/11/2024 1:01:58 PM	Admin	Duty modified	*	Duty Inquire into vendor master was modified from Override permissions on roles	Modify role
Snapshots	3/11/2024 1:01:58 PM	Admin	Duty modified	*	Duty Maintain vendor invoices was modified from Override permissions on roles	Modify role
snapsnots	3/11/2024 1:01:57 PM	Admin	Duty modified	*	Duty Maintain product receipt was modified from Override permissions on roles	Modify role
Roles – Sensitive data access	3/11/2024 1:01:56 PM	Admin	Duty modified		Duty Inquire into voyage costs was modified from Override permissions on roles	Modify role
Duties – Sensitive data access	3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_CostedProcessDuty was modified from Override permissions on roles	Modify role
Privileges – Sensitive data access	3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_DocReceivedProcessDuty was modified from Override permissions on roles	Modify role
-	3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_InTransitProcessDuty was modified from Override permissions on roles	Modify role
Users – Sensitive data access	3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_ReadyForCostingProcessDuty was modified from Override permissions on roles	Modify role
Charts	3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdateFolio_DocReceivedProcessDuty was modified from Override permissions on roles	Modify role
	3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty Maintain cost estimates was modified from Override permissions on roles	Modify role

Using the 'Open security request history' button it will navigate you to a new form that will have a summary of the security request history where information related to the Security Request and the workflow history can be seen.

curity request details										
Open request details										
equest	Area	Created date a		End date	Owner		Security record status	Scenario	Description	
Modify role	Created by	4/3/2024 07:	14:10 AM		Admin		Completed			
ype Modify role	Admin	Start date		Origin User requests	Priority Normal		Modified by Admin			
induity fore				Oserrequests			Admin			
orkflow approval history										
Open workflow approval details	1									
istance ID	Workflow ID	Status		Document	Document type		Workflow	Version	Submitting user	Company accounts I
000001	000014	Completed		Quotation: QN0000002, City	Sales quotation		Review project quotations	1.0.0.0	JUNE	ussi
Context	Action Submission	Name 000001: Quotation: QN00	Message Submitted by: JUNE	Comment	Created date and time 1/1/2016 8:35:13 PM	User				
0										
Workflow	Creation	000001: Quotation: QN00	Workflow 000014 PSAProjQuotationTem	plate	1/1/2016 8:35:29 PM	JUNE				
Approval	Creation	Project Quotation Approv			1/1/2016 8:35:34 PM	JUNE				
Approval	Auto complete condition		Auto-completion condition: Project		1/1/2016 8:35:42 PM	JUNE				
Approval	Completion	Project Quotation Approv			1/1/2016 8:35:44 PM	JUNE				
O Workflow	Completion	000001: Quotation: QN00			1/1/2016 8:35:49 PM	JUNE				
udit log details										
Event date and time	Description		Event type	Reference Company	Event created by					
O 3/11/2024 1:01:46 PM	Duty Landed cost agent (dis	splay) was created from Overri	Duty created	0 *	Admin					
3/11/2024 1:01:53 PM	Privilege Landed cost agent	t (display) was created from Ov	Privilege created	0 *	Admin					
3/11/2024 1:01:54 PM	Role Landed cost agent was	s modified from Override perm	i Role modified	0 *	Admin					
3/11/2024 1:01:54 PM		splay) was created from Overri		0 *	Admin					
3/11/2024 1:01:54 PM		for operations master was more		0 *	Admin					
3/11/2024 1:01:55 PM	Duty Maintain receipt opera	ations was modified from Over	r Duty modified	0 *	Admin					
	Name	;	Reference type	Reference	table type					
Reference description     Duty Landed cost agent (di			Duty	Duty						

Of course, for in deep analysis options like 'Open request details' and 'Open workflow approval details' are available.

## 2.4 Enhanced SoD predefined list

A list of predefined enhanced SoDs rules has been created. The rules are based on privilege and entry points (segregation security sets).

The file will be available from our support teams. Do not hesitate to request it.

The file can be imported using the standard Data Management Framework (DMF) where a new import project needs to be created and a package file type needs to be added.

Import   AX: Operations   My view DEMO import	~				
Import 1					
Group name DEMO import	Description		Data project operation type Import	Project category Project	$\checkmark$
Selected entities + Add file $\checkmark$ + Add template $\checkmark$	🗊 Remove entity	Open in Excel Res	sequence ∽ Sort by ∽ Disable ∽	Entity attribute	
Add file JOB DETAILS Source data format		View map	Executi 1 Level in ex	Sequence Obsolete	Source of
Package VILOAD IMPORT FILES	2				
Upload	and add 3				

After the file upload three data entities will be added to the import project.

mpor	t					
DEM(				ata project ope Import	ration type	Project catego Project
Select	ed e	ntities				
		ntities $e \checkmark +$ Add template $\checkmark$ I Remove entity Open in E	xcel Reseque	ence∨ Sort b	oy∨ Disable	e ∽ Entity attribute
+ Ad	ld fil		xcel Reseque	ence∨ Sort k Executi ↑	-	Entity attribute
+ Ad	ld fil	e $\rightarrow$ + Add template $\sim$ in Remove entity Open in E	-		-	-
+ Ad	ld fil	e ∽ ) + Add template ∽	View map		-	-

Import the file and the result should look like this:

Entity processing status							
🖺 View staging data 🛛 🖓 Filter 🗠						7	
O Entity		Status	Pending	In staging	Created	Updated	Total
Segregation security sets	$\checkmark$	Succeeded	0	41	41	0	41
Segregation security set lines	~	Succeeded	0	435	435	0	435
Enhanced SoD rules	$\checkmark$	Succeeded	0	106	106	0	106

This will import the segregation security sets and afterwards the enhanced SoD rules.

The rules should be 106.

NOTE: 106 rules will be imported, but children records will be automatically created on the import. Overall a number of 2421 rules will be generated.

# 3. Features introduced in last few releases of Security and Compliance Studio

Some important features from the last few releases includes a number of important new capabilities and enhancements requested by customers and partners, such as:

- Security requests enhancements and workflow. Security requests functionality has been introduced to new exciting features that will help your organization to better handle user requests. The form has been enhanced and for a better control we also introduced the workflow component that will allow you to review/approve/deny/reject the security requests. One of the greatest enhancements brought to you is the automated process that will create security requests once it is approved.
- Export security explorer objects to excel in a de-normalized format. You can now export securable objects in a "De-normalized form" from security explorer. All Securable objects related to a particular role/user/duty/privilege/entry points can be exported into an Excel sheet for further analysis.
- Merge security scenarios and match role. You can now merge more than one scenario into one new scenario if required by business and change in organization setup. This feature is very useful in combining more than one scenario then create a role which can perform all the business process recorded in the scenarios.
- Mark any Security Role as Active/Inactive. Mark any security role as "Inactive". Once the role is inactive, it cannot be assigned to any user in SCS. This feature is very useful in limiting the number of security roles that can be assigned to users. Also if you want to preserve a set of roles that should not be updated like standard Microsoft security roles for reference. With SCS, it is useful in helping prevent update standard MS roles by mistake.
- **Recording steps to scenario.** You can now record Business process steps along with entry points while creating a security scenario for more information.
- Override permission based on scenarios. You can now override permission on existing roles based on your recording or a security scenario. This helps security administrators to deny access to some entry points on a particular role. Customized permission can also be set for other access types. Very useful if you want to merge roles and just exclude limited entry points
- Option to mark, track and audit security objects providing access to sensitive data. You can now use SCS in defining and managing the security objects access to sensitive data. Specific definition of sensitive data might be different for different industries or countries. An organization can define specific definition for sensitive data as per their industry, country and policies. For some organizations, sensitive data might be any data that is related to finance, human resource or personal. It is up to an organization to define sensitive data. In D365FO we assign security roles to users. Security roles grant access to perform business operations, it might provide access to sensitive data as well. In SCS we can specify which role, duty, privilege or entry point provides access to sensitive data.
- Option to create a duty from Matched Privileges grid in Match roles form. You can now create a duty from selecting one or more privileges in the Match roles form to design a security role matching the user work scenario at the least license cost.
- Option to import and export data using Data Entities in Security and Compliance Studio. In this release we have added some data entities currently supported for Security and Compliance Studio.

The approach has been to enable data entities for all tables where relevant in Security and Compliance Studio in order to provide import and export capabilities.

- Option to compare Security Snapshots stored in the security setup. Building upon what we already have implemented in the fall release (security snapshots) we have gone furthered and added the possibility of comparing the existing security snapshots. Snapshot comparison feature allows security officers and administrators to do a detailed comparative analysis between any two security snapshots for all security objects in D365 FOE setup i.e. Users, roles, duties, privileges. Both single record compare and full compare options for the selected snapshots are supported along with multiple views. The comparison option will allow the user to see what modifications had occurred in the security setup since the last changes. The users can keep track of the changes, comprehend and analyze them in order to strengthen the security further.
- Enhanced Audit log capability to capture all the changes from development space (AOT) as well into Audit Log

This release enhances the audit log feature within Security and Compliance studio in order to capture and register the changes made directly on the security objects from the development space (visual studio). Now, when a new snapshot is created; automatically the new snapshot will be compared with the last one. In this way all the changes made in security configuration will be captured in the Audit log.

This comes as a solution of capturing all the changes no matter if they took place in the *UI (user interface)* or directly into *development space (in Visual Studio)*.

- Option to create one or more privileges and also one or more duties while merging roles. "Merge role" feature now comes with an option to create only one merged privilege for all entry point types in addition to the existing options to create multiple privileges and one or more duties. Previously you can split up entry points in separate privileges and duties by entry point type. Now you can create also only one privilege for the merged roles.
- Ability to create scenarios from D365 module menus. You can now model security scenarios for D365 modules. "Add module access" feature helps you to create a new scenario based on the complete list of a module menu items with a desired level of access types. This is of great help when you desire to have a security role providing you access to all or most of one module features.
- Snapshots based performance and scalability enhancements. The entire functionality for Rebuild Data, Security Explorer and Match Roles revolves around the security objects (roles, duties, privileges and entry points) and the associations between them (duties assigned to role; privileges assigned to each duty, etc.). All of these are kept in standard code that was preserved, externally, into a DLL. Using this DLL for multiple scopes in Security and Compliance Studio end up with a performance issues on the above mentioned business logics/functionalities. We now have created a structure of tables to keep the data related to each security object and the association between them and easily access it directly from tables and also much faster. This has led to drastic improvement in the "Match roles" and "Rebuild data" programs performance.
- Improved "Create role wizard" based on a grid framework. "Create role wizard" is now based on a new grid framework making it a great user experience. This wizard helps you to create a new security role based on duties and privileges with letting you know the license type before role creation.
- Accessing Security Explorer from all D365 FOE forms. This release comes with Security and compliance studio security explorer embedded in all D365 FOE forms. This provides a very useful way to analyze users and associated security objects (roles, duties, privileges, entry points) that have access to that D365 FOE form.
- Option to create duties and SOD compliance check as well while merging roles. "Merge role" feature now comes with an option to create duties along with the privileges. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.).
- Importing New Users while Synchronizing the group users with the Active Directory group members. We added a new small feature to our Azure AD group synchronization job. On the dialog

of the Synchronize the group users with the Active Directory group members, we introduced a new parameter to import users.

- Licensing changes To help our customers we have implemented new licensing changes within SCS. Microsoft has taken a commercial decision last year to split the license to Finance, SCM, and project, for more details you can have a look at Microsoft's new licensing guide. These changes left customers confusing about how they can be compliant with new license changes. That's why we have decided to build this feature, now customers can see a new license type field in SCS forms such as security explorer, match roles, license optimization workspace, etc.
- Uptake RapidValue Scenarios directly as SCS Security Scenarios Customers can now directly upload the RapidValue Scenario task guides per security roles (Procedure activities which include flows across multiple roles) as a Security scenario in Security and Compliance Studio. This will be very useful where both RapidValue BPM Suite and Security and Complicate Studio are implemented. You might be aware that now in RapidValue, you can have Business process hierarchy with its linked task guides exported from RapidValue to a user defined local Windows folder. Export logic takes care of both the modeling techniques where customer is using Flow-Activity way of modeling and also the Scenario" Procedure Activity" way of capturing flow variations.
- Enhanced Segregation Of Duties In standard D365FSC, we can only define SoD rules at duty level which is rarely useful. In SCS, with this release user can now define SoD rulesets at any level (Duty, Privilege or Entry Point) in the security hierarchy in D365FSC. This makes this feature more practical and extremely useful for customers seeking better regulatory compliance like ISO 27001 section 6.1.2, SOX Control 404 and in general much improved security design better equipped to prevent frauds.
- Organization Risk Register- All Organizational risks can be now mapped in SCS "Integrated risk Management workspace". They may be financial risks related to SoD violations or can be related to any other organizational strategy or operational aspect. This feature will evolve in coming quarters in a full-fledged "Risk Management" capabilities within SCS enabling Organizations to register, assess, monitor, mitigate and close it.
- AAD related SoD Validations across SCS SCS now ensures that SoD violation checks also consider Security roles acquired by a user from being associated within an AAD. This is applicable all across SCS features. This helps in better handling of internal controls.
- Security Explorer displaying Tables, Service operations and Data Entities entry point's type -Security expirer has been enhanced to now include also the following entry point's type: Tables, Service Operations and Data Entities.
- **Performance Optimization** Significant performance improvement in the following programs: Create snapshot; Security Explorer pinning, Match roles and Marking a record as sensitive.
- A new "Share" Workspace A new workspace "Security and compliance file share" is added to manage task recording and images being used at various places in security & compliance studio.
- AAD groups' information in D365FO- In standard D365FO, we cannot check what all the users added to AAD groups and we have to login to azure portal. Now in SCS, we can check what all the users added to AAD groups in D365FO itself along with all related audit tracking for AAD groups in SCS itself.
- Verify SoD rules in Stand in You can now use "Validate Sod rules " functionality while defining new stand-ins in SCS to know in advance, if there will be any SoD violation when security roles of user will be assigned to stand in user.

- Chart to give an overview of number of users and their last logging details- SCS now comes with a chart to categorize all users with their login details and time series analytics. This helps a lot in both compliance needs and optimizing license costs to deactivate or remove users based on an organization's security policy.
- Asset classification User Interface SCS provides user interface, which shows all the fields with their asset classification. Chart to get the overview of different asset classification and how many field has the same asset classification. Asset classification is a table field property, classifying type of data it contains. Tagging a column helps easily marking data in scope for GDPR/GxP and many other such compliance regulations.
- A List page with delegation details This one is a UI improvements to make it easier for SCS administrators to manage and track "*Workflow Delegations*". Every user has to login by himself to delegate work flow to other user, in D365FO. Now using SCS, administrator can delegate workflow to any user for a particular time period.
- User groups combined two tabs in one This one is a UI improvements to make it easier for SCS administrators to manage a simplified standard user group's form. Users who are outside the organization hierarchy for budget planning must work with budget plans, you can assign budget plans to user groups. You can also set up restrictions for journal posting that are based on user groups. Users can be added to different groups using same tab. Also in SCS now a list of added users to different groups can be exported to excel using list tab.
- **Dynamic snapshot** We got a lot of feedback and learnings related to the security snapshot. A lot of features depend on having actual data in the snapshot. New changes in the snapshot framework have been introduced where the snapshot no longer requires to updated via a batch job after security changes have been made.

NOTE: 'Creating snapshot' functionality is still available, and it will remain to be used as a safe net. We advise you to create a new snapshot from time to time to make sure that security inconsistency will not appear. Using the snapshots, you can create static versions of the security at a certain point in time.

This is a change that has an impact on the product. Please provide feedback so we can further improve the dynamic snapshot feature.

#### • New export/import role functionality

- 1. <u>Problem</u>: For a couple of years, we have discovered and reported to Microsoft a standard bug that for AOT Privileges the node 'FormControlOverrides' is not readable from code and that is affecting, for example, the current SCS Export / Import functionality.
- 2. <u>Issue that is generated by the bug explained:</u> When exporting a role using SCS Export function the XML file generated does not contain the entries under the 'FormControlOverrides' from AOT Privileges.

After the SCS Import function runs, the content from the XML file is applied to the target environment. Since the 'FormControlOverrides' node is empty in the XML file, the algorithm interprets it as a change (entries removed from node by user) therefor it will override the privilege in target environment and the entries will be removed.

3. **Solution:** Since the only framework that was exporting the 'FormControlOverrides' is the standard 'Export' from Security Configuration form (which exports only the customizations and all of them) we decided to use that and make it more practical for the end user, where now, with the new functionality you can export the customizations for a selection of roles.

# The 'Export role configuration' / 'Import role configuration' can be found on *Security and Compliance -> Security management workspace -> Roles tab*

A new column has been introduced to show all the roles that due have customizations and can be exported. The 'Export role configuration' button will be enabled when a record marked as 'Has configuration' is selected.

NOTE: This is working the same as standard security configuration export, except the fact that you can export them per roles.

• License count changes - New options have been added in the *Security and Compliance Studio ->* Setup -> Parameters form, under License count tab.

For all cloud licenses (Finance, Commerce, HR, Project operations, SCM) a new input option has been added called '- attached license' (E.g. Finance – attach license) where the user can add the number of attached licenses that have been bought, not only the base number.

These changes will reflect in the 'License optimization' workspace on the 'Usage' tab.

The new license calculation formula will now: (Base license + Attached license) – Actual user count. In order to separate the 'cloud license' from 'On premise' licenses we added the "View on

premise" / "View cloud license" button that can toggle this view.

## 3.1 Segregation of duties sets

A new way of creating Enhanced SoD rules for entry points type, has been introduced. This new method will consists in creating a set of entry points ( a list ) that you desire to be part of the rules and then, using Security requests, the rules will be created automatically.

1. Navigate to 'Security and Compliance Studio -> Setup -> and open Segregation security sets' form to define a list of entry points.

P Filter	Standard view ~ Segregation security sets							
<b>Tralaalalal</b> Traslalaa	Segregation security sets Desc	2						
Trat2	Segregation security set line	s						
	+ Add 🗊 Remove							
	<ul> <li>Securable object</li> </ul>	Securable object type	Access level					
	<ul> <li>Accountant_BR</li> </ul>	Menu item display	View					
	ACOJournalPost_BR	Menu item action	View					
	AdvanceAdjustmentPa	ra Menu item display	Full control					
	AssetChangeGroup	Menu item action	Correction					

- 2. Navigate to 'Security and Compliance Studio -> Security -> and open Security requests' form in order to create a new request for SoD rules.
  - a. Create new Security request of type 'Create rule'
  - b. In the 'Enhanced SoD rules' tab add new record of type 'Segregation security sets' and select the set from the lookup in 'First' column.
  - c. Submit and approve the request.

Security requests   My view∨ Test sod sets			
General			
Request Test sod sets	Type Create rule	Origin Area	$\sim$
Status			
Priority Normal	Security record status Open	Owner (Admin	
Enhanced SoD rules			
+ Add 🗊 Remove			
○ C Name 1	Туре	First First securable object ty	pe First access level
Demo Sod rules sets	Segregation security sets ~	Tralaalala	No access

3. Navigate to 'Security and Compliance Studio -> Setup -> and open Enhanced SoD rules' form. Here you will find the new set of rules created as a parent-child hierarchy that can be expanded.

hanced SoD rules					Enha	nced SoD rules				
tandard view	,				Sta	ndard view~				
Filter					₽ Fi	lter				
Name	î Туре	Effective from	Effective to	Enabled	0	Name	î Type	Effective from	Effective to	Enabled
) 🗸 test	Segregation security sets	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~	0	∨ test	Segregation security sets			~
test4	Entry point	6/29/2023 10:46:24 AM	12/31/2154 11:59:59 PM			test_01	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~
testsodentry	Entry point	6/7/2023 10:01:46 AM	12/31/2154 11:59:59 PM			test_02	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~
testsodpriv	Privilege	6/7/2023 9:59:38 AM	12/31/2154 11:59:59 PM			test_03	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	$\checkmark$
						test_04	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~
						test_05	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~
						test_06	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~
						test4	Entry point	6/29/2023 10:46:24 AM	12/31/2154 11:59:59 PM	
						testsodentry	Entry point	6/7/2023 10:01:46 AM	12/31/2154 11:59:59 PM	
						testsodpriv	Privilege	6/7/2023 9:59:38 AM	12/31/2154 11:59:59 PM	

A predefine list of SoD examples will be available as excel sheet to be imported in system if desired. This will help you in starting the security setup for your environment 😊

## 3.2 Security requests enhancements and workflow

Security requests functionality has been introduced to new exciting features that will help your organization to better handle user requests. The form has been enhanced and for a better control we also introduced the workflow component that will allow you to review/approve/deny/reject the security requests.

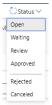
One of the greatest enhancements brought to you is the automated process that will create security requests once it is approved.

#### I. Security requests enhancements:

- 1) **Security types** has been added. This will allow you to select what kind of request to do want to create. For each of the types there will be a new tab where the user will add the required data.
- 2) Security workflow. Navigate to Security and Compliance Studio -> Setup -> and open Security Requests workflow configuration form. Click new and this will open the workflow editor. Here you can create your own approval workflow and then activate it. The 'workflow' button will be available on the form. After the user creates a security requests he can submit it to approval.

it +New	jit +New
Security requests   My view ∽	Security requests   My view 🗡
Demo SR 1 Inactive workflow	Demo SR 1 Active workflow

**Note**: when the workflow is <u>not activated</u> you can review/approve/reject/etc the security request by using the *Status* button.



#### Security types

a) General

The 'general' security type is used for requests that cannot be handled by the defined types below and cannot be an automated process, but rather an action that some supervisor user needs to do 'manually'. The request will be created and the details field will be used to describe the request.

1	General		
	General	User requests	WHS
	Status	Owner	
	Open	Admin	

#### b) Create user

A new tab will be made visible. Here the required information for creating a new role will be available to fill in. When the request will be approved the user will be automatically created and it will be available in the System administration -> Users form.

Security requests   My view ∽ Demo SR 1			
General			
Request Demo SR 1	Type Create user	Origin User requests 🗸 🗸	Area WHS V
Status			
Priority Normal	Status Open	Owner Admin	
Create users			
User ID newUser1	User name newUser1	Email newUser1@to-increase.com	Company DAT V
Description			
Details			

#### c) Assign role to user

A new tab will be made visible. In this tab there will be an option to select roles that are desired to be assigned to the user. You can select an existing user from the UserId lookup and all other user information will be automatically filled in.

For each selected role there is also the possibility of selecting a specific company. If not company is selected, the role will be added for all companies.

Demo SR	1		] [	Assi	gn role to user	$\sim$	User requests	
Status			_					
Priority Normal	~	)		tatu Ope			Owner Admin	
Assign rol	les to user							
USER				_			_	
User ID Admin		User na			mail fmihoc@toincreas		Company	
ROLES					tomercus	cromeros	00111	
Add 🗎	Remove							L
00	Role name		Descript	tion		Role AOT name	e :	
0	Auditor		Manage	es a	nd reviews aud	AUDITPOLICY	MANAGER 🗸	
COMPANI + Add	ES III Remove							L
+ Add	Remove	Company	accounts	s				+

#### d) Remove role from user

A new tab will be made visible and in this tab that will be addressed to the user who created the security request. You can select an existing user from the UserId lookup and all other user information will be automatically filled in. A list of all the roles currently assign to the user will be available to choose from.

When the request is approved all the selected roles will be removed from the user.

Request Demo SF	۱ 1		Type Remove role from user	Origin V User reques	its
Status					
Priority Normal	$\sim$		Status Open	Owner Admin	
Remove r	oles from user				
USER					
User ID		User name	Email	Company	
Admin		Admin	fmihoc@toincrease.onm	icros USMF	
ROLES	Remove				
00	Role name		Description	Role AOT name	
0	Lease clerk		The lease clerk role has ac	ASSETLEASECLERKROL	E 🗸
$\cup$			View of lease roles	ASSETLEASELEASEVIEV	

#### e) Disable user

A new tab will be made visible and in this tab a list of all enabled users in the system will be available to choose from using the 'Add' button.

When the request is approved all the selected users will be disabled.

Security requests   My view ~ Demo SR 1			
General			
Request Demo SR 1	Type Disable user	Origin User requests	Area WHS
Status			
Priority Normal	Status Open	Owner Admin	
Disable users			
Add I Remove	User name	-	
O BrunoD	BrunoD		
Description			

#### f) Enable user

A new tab will be made visible and in this tab a list of all disabled users in the system will be available to choose from using the 'Add' button.

When the request is approved all the selected users will be enabled.

Security requests   My view ~ Demo SR 1			
General			
Request Demo SR 1	Type Enable user	Origin User requests 🗸 🗸	Area WHS
Status			
Priority Normal	Status Open	Owner Admin	
Enable users			
Add 🔟 Remove			
-	er name net Schor		
Janets Ja			
Description			

#### g) Delete user

A new tab will be made visible and in this tab the option of deleted an existing user will be available. Using the 'Add' button a selection can be made from a list with all the users in the system.

When the security request is approved the selected users will be deleted from the system.

General					
Request Demo S	R 1	Type Del	e lete user 🗸 🗸	Origin User requests 🗸	Are
Status					
Priority Normal	$\checkmark$	State Op		Owner Admin	
Delete u	sers				
	Remove				
0 0	User ID 1	User name	Email		
0	CASSIE	CASSIE	CASSIE@contosoax7.onm		
	cdsaurorauser	Auroraus	Aurorauser01@capintegr		I .
	cusaurorauser	Autoraus	Autorausero r@capintegr		

#### h) Create role

A new tab will be made visible. On this tab there will be an option to create a role based on a task recording. The task recording will be uploaded in the system, a scenario will be automatically created and it will be added on the form along with all the menu items detected.

When the security request is approved the role will be created based on the scenario's securable objects and the selected access level.

Security reque	uests   My view ∽ SR 1							
General								
Request Demo SR 1	1	Type Delete user	Origin User requests	Area WHS	$\checkmark$			
Status								
Priority Normal	$\sim$	Status Open	Owner Admin					
Create role ROLE Upload task								
ROLE Upload task Role name SCS_DemoR SCENARIO DI	ik recording iRole1 DETAILS	Description Demo purposes	Scenario					
ROLE Upload task Role name SCS_DemoF SCENARIO DI O Step nu	ik recording Role1 DETAILS number Securable obje	Demo purposes	skRecordingForCSReplicat	Description	File name TaskBargedingEor/SBanli	Child scenario	Î Remark	
ROLE Upload task Role name SCS_DemoR SCENARIO DI	ik recording iRole1 DETAILS	Demo purposes	skRecordingForCSReplicat	Description	File name TaskRecordingForCSRepli	Child scenario	Î Remark	
ROLE Upload task Role name SCS_DemoF SCENARIO DI O Step nu	ik recording Role1 DETAILS number Securable obje	Demo purposes tt Securable type age Display	skRecordingForCSReplicat	Description		Child scenario	Remark Additional securable object found in the task recording	
ROLE Upload task Role name SCS_DemoF SCENARIO DI O Step nu	Role1 DETAILS 1 salestablelistp	Demo purposes tt Securable type age Display bard Display	skRecordingForCSReplicat	Description Go to Accounts receivabl	TaskRecordingForCSRepli	Child scenario	Additional securable object	
ROLE Upload task Role name SCS_DemoF SCENARIO DI	ik recording iRole1 DETAILS number Securable obje 1 salestablelistp 2 DefaultDashb	Demo purposes           ct         Securable type age           age         Display           bard         Display           age         Display	skRecordingForCSReplicat	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli TaskRecordingForCSRepli	Child scenario	Additional securable object	
ROLE Upload task Role name SCS_DemoF SCENARIO DI	ik recording iRole1 DETAILS number Securable obje 1 salestablelistp 2 DefaultDashb 5 salestablelistp	Demo purposes           ct         Securable type           age         Display           bard         Display           age         Display           age         Display	skRecordingForCSReplicat Access level Full control Full control Full control	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli TaskRecordingForCSRepli TaskRecordingForCSRepli	Child scenario	Additional securable object found in the task recording Additional securable object	

#### i) Modify role

A new tab will be made visible. On this tab there will be an option to modify one or more existing roles based on a task recording. The task recording will be uploaded in the system, a scenario will be automatically created and it will be added on the form along with all the menu items detected.

When the security request is approved the role will be modified based on the scenario's securable objects and the selected access level. If the securable objects exist on the role they will be updated with the selected access level, or they will be added if do not exists.

	equests   My view ∽							
	o SR 1							
Request		ype Modify role	Origin	Area WHS	$\sim$			
Demo S		Modify role	User requests	V WHS	~			
Status								
Priority	-	itatus	Owner					
Normal	$\sim$	Open	Admin					
Modify n	ala							
	01e							
ROLE	e 🗐 Remove							
-		Description	Role AOT name 1					
0	View lease	/iew of lease roles	ASSETLEASELEASEVIEW					
Upload Scenario	O DETAILS task recording							
Upload Scenario Demo1x	task recording							
Upload Scenario Demo1x	task recording recording.axtr p number Securable object	Securable type	Access level	Description	File name	Child scenario	î	Remark
Upload Scenario Demo1x	task recording	Securable type Display	Access level Full control	Go to Accounts receivable > Orders > A	Demo1x recording.axtr	Child scenario	Î	Remark
Upload Scenario Demo1x	task recording recording.axtr p number Securable object 1 salestablelistpage 3 SalesTableDetails				Demo1x recording.axtr	Child scenario	Ť	Additional securable obje
Upload Scenario Demo1x	task recording crecording.axtr p number Securable object 1 salestablelistpage	Display	Full control	Go to Accounts receivable > Orders > A	Demo1x recording.axtr	Child scenario	Î	Additional securable obje
Upload Scenario Demo1x	task recording recording.axtr p number Securable object 1 salestablelistpage 3 SalesTableDetails	Display Display	Full control	Go to Accounts receivable > Orders > A In the list, click the link in the selected r	Demo1x recording.axtr	Child scenario	t	Additional securable obje
Upload Scenario Demo1x	task recording crecording.axtr p number Securable object 1 salestablelistpage 3 SalesTableDetails 5 SalesCopyAllLines	Display Display Display	Full control Full control Full control	Go to Accounts receivable > Orders > A In the list, click the link in the selected r Click From all.	Demo1x recording.axtr Demo1x recording.axtr Demo1x recording.axtr	Child scenario	t	Remark Additional securable obje found in the task recordin

#### j) Lock role

A new tab will be visible and an option to lock roles will be presented. Roles can be chosen from a list of all unlocked roles available in the system.

When the security request is approved the role(s) will be locked and can be found in the *Security* and *Compliance Studio -> Inactive security roles*.

e Tivew	🗏 Delete 🛛 📿 Status 🗸	✓ Q Owner ✓ Request	Manage O	ptions >>		
Security re	equests   My view 🗸					
Demo	SR 1					
Denne	5 51(1					
General						
Request		Туре		Origin	Area	
Demo Si	R 1	Lock role	~	User requests	WHS	$\sim$
Status		6				
Priority		Status		Owner		
Normal	$\sim$	Open		Admin		
Lock role						
+ Add	🗊 Remove					
+ Add	Remove		Name			
+ Add	🗊 Remove	external]	Name ANONYMOU			
+ Add	Remove	external] v				
+ Add	Remove	external] v				
+ Add	Remove	external]				
+ Add	Remove	external] v				
+ Add	Remove	external] ~				

#### k) Unlock role

A new tab will be visible and an option to unlock roles will be presented. Roles can be chosen from a list of all unlocked roles available in the system.

When the security request is approved the role(s) will be unlocked and removed from the *Security* and *Compliance Studio -> Inactive security roles*.

Security requests   My view ~ Demo SR 1			
General			
Request Demo SR 1	Type Unlock role V	Origin User requests 🗸 🗸	Area WHS V
Status			
Priority Normal	Status Open	Owner Admin	
Unlock roles			
+ Add 🗊 Remove			
O C Role name	Name		
✓ Warehouse worker ✓	WMSWAREHOUSEWORKER		

Description

#### I) Delete role

A new tab will be visible and an option to delete roles from the system will be available. Roles can be chosen from a list of all existing in the system.

When the security request is approved the role(s) will be permanently deleted from the system.

Gene	eral						
Requ Der	iest no Sf	R1	Type Delete role	$\sim$	Origin User requests	$\sim$	Area WHS
Statu	us						
Prior Nor		$\sim$	Status Open		Owner Admin		
Dele	te ro	le					
Add	d role	🗊 Remove					
0	С	Role name	Description	Role AOT	name î		
0		SCS_RoleTest_2		6DEC781	1-E0C5-42C5-94		
		SCS_RoleTest1		82B6FA6	2-0C74-46CC-8D		

#### m) Create rule

A new tab will be visible. In here enhanced sods can be defined. Once the security request is approved all the rules will be automatically created. They can be found under *Security and Compliance Studio -> Security -> Enhanced SoD -> Enhanced SoD rules* form.

uest mo SR 1 tus		Type Create rule	Viii Us	gin ser requests V	Area						
						~					
rity											
irmal	~	Status Open	Ow	mer dmin							
anced SoD rule	les										
Add 🗐 Remov											
) C Name	Ť	Туре	First	First securable object type	First access level	Second	Second securable object type	Second access level	Effective from	Effective to	Enabled
Create d	demo rule 2 from	Entry point V	AdvancedLedger 🗠	🗸 Menu item display 🛛 🗸	Create $\checkmark$	BankChequeCompanyl $\vee$	Menu item display 🛛 🗸	Full control $~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	4/28/2022 10:43:44 🖽 ⊙	12/31/2154 11:59:5 🖽 💿	
Create d	demo rule from SR	Duty	Maintain Absorption.		No access	Import ZIP/postal codes		No access	4/28/2022 10:43:06 AM	5/26/2022 11:59:59 PM	<b>V</b>

#### n) Resolve conflict

A new tab will be visible. In here there will be the possibility of selecting which conflict(s) are wished to be resolved and how. The resolution type can be set and the override reason can be filled in. Once the security request is approved all the conflicts will be resolved. They can be found under *Security and Compliance Studio -> Security -> Enhanced SoD -> Enhanced SoD conflicts* form.

Reque Dem	est o SR 1	Type Resolve conflict		Origin User requests	Area WHS	$\sim$				
itatu	s									
riorit Norn		Status Open		Owner Admin						
nhar	nced SoD conflicts									
+ Ac	dd 🗐 Remove									
0	C Rule name	Туре	User ID	First	Role	Second	New role	Resolution	Override reason	Role to remove
	Duty test1	Duty	APRIL	Approve budget plans	Budget clerk	A parameter that is used t	Budget manager	Exclude		Existing role
0	Test 1	∨ Duty	EMMAH	PrintMgmtSetupUIMain	Sales clerk	ProjActivity	Sales representative	Override	<ul> <li>Demo purpose</li> </ul>	Existing role

#### o) Delete rule

A new tab will be visible. Here the user can select what rules to be deleted from the system.

Once the security request is approved all the rules will be deleted. They will be removed from the *Security and Compliance Studio -> Security -> Enhanced SoD* form.

Der		ests ∣ Myview ∽ SR 1									
Gene	al										
Reque Dem	st o SR 1		Type Delete rule	Origin User req	uests 🗸	Area WHS	~				
Statu	5										
Priorit Norr		~	Status Open	Owner Admin							
Delet	e enha	nced SoD rules									
		Remove									
	C N	ame î	Туре	Effective from	Effective to	First	First securable object type	First access level	Second	Second securable object type	Second access leve
	So	oD Test 1 - do not use 🗸 🗸	Entry point	4/20/2021 12:11:46 PM	12/31/2154 11:59:59 PM	DSMAuditLog	Menu item display	View	DSMAssetClassification	Menu item display	View
	D	uty test1	Duty	11/25/2021 2:00:45 PM	12/31/2154 11:59:59 PM	Approve budget plans		No access	A parameter that is used t		No access

#### p) Add stand-in

A new tab will be visible and in here the user who created the request can set up a stand-in for a specific period of time.

Once the security request is approved the stand-in will be created and it can be found under *Security and Compliance Studio -> Security -> Stand-in* form.

Stand-in From date To date Copy assigned organizations	emo SR 1 Add stand-in VUser requests WHS atus ority Status Owner formal Open Admin eate stand-in Add I Remove O O User ID Stand-in From date To date Copy assigned organizations	eneral								
Status     Owner       Open     Admin	atus iority Status Owner Iormal Open Addmin  Add  Remove  User ID Stand-in From date To date Copy assigned organizations	equest		1.5						
Ve Admin Ve Stand-in From date Copy assigned organizations	iority Status Owner Normal ✓ Open Admin  reate stand-in  Add  Remove  O O User ID Stand-in From date To date Copy assigned organizations	Jemo SR 1	Add stand	d-in		User reques	sts	<u> </u>	WHS	
Ve Admin Ve Stand-in From date Copy assigned organizations	Normal     Open     Admin       reate stand-in       - Add      Remove       O     O User ID     Stand-in       From date     To date     Copy assigned organizations	itatus								
Ve Stand-in From date To date Copy assigned organizations	reate stand-in - Add  Remove User ID Stand-in From date To date Copy assigned organizations	riority	Status			Owner				
Stand-in From date To date Copy assigned organizations	Add         Image: Remove           ○         User ID         Stand-in         From date         To date         Copy assigned organizations	Normal 🗸	Open			Admin				
Stand-in From date To date Copy assigned organizations	Add         Image: Remove           ○         User ID         Stand-in         From date         To date         Copy assigned organizations									
Stand-in From date To date Copy assigned organizations	O C User ID Stand-in From date To date Copy assigned organizations						_			_
		reate stand-in								
ALICIA ~ 4/28/2022 III 4/30/2022 III	Admin ALICIA ~ 4/28/2022 III 4/30/2022 III	Create stand-in + Add I Remove								
		+ Add 🗊 Remove	Stand-in	From date	To	o date	_	Copy assigned organiz	zations	7
		Add I Remove					63		zations	
		Add I Remove					63		zations	
		Add I Remove							zations	
		Add I Remove							rations	
		Add I Remove					•		zations	
		Add I Remove					ā		zations	

#### q) Cancel stand-in

A new tab will be visible and in here the user who created the request can cancel one or more stand-ins available.

Once the security request is approved the selected stand-in(s) will be cancelled.

Gene	eral											
Requ				Туре					Origin		Area	
Dem	no SF	R 1		Cancel st	and-ir	n	$\sim$		User requ	ests	✓ WHS	
Statu	IS											
Priori	ity			Status					Owner			
Nor	mal	$\sim$		Open					Admin			
		stand-in i Remove										
0		User ID	Stand	-in	Fre	om date		To da	te		Copy assigned organizati	-
		Admin	ALICI	Α ,	~ 4/	28/2022		4/30	/2022			

#### r) Create business risk

A new tab will be visible and all the information required to create a business risk will be presented to the user. Additionally, enhanced sods can be assigned to the created business risk.

As soon as the security request is approved the business risk will be created and the selected sod rules will be linked to it. The created business risk can be found under *Security and Compliance Studio -> Workspaces -> Integrated risk management* workspace.

General			
Request Demo SR 1	Type Cancel stand-in	Origin User requests	Area WHS
Status			
Priority Normal V	Status Open	Owner Admin	
Create business risk BUSINESS RISK			
Name Dmeo business risk Category Strategic	Area AssetLease Inherent risk Very Jow	Mitigation Test Residual risk Very low	Status Initial V Response
SOD RULES + Add I Remove	Very low 🗸	very low V	Ignore 🗸
○         Name           ☑         Test 1	<ul> <li>↑ Organization Risk</li> <li>✓ Dmeo business risk </li> </ul>	:	

Description

**Note**: if the type of the request is changed all the information from the current tab will be deleted. A popup message will be available to inform the user that all data related to the current type will be removed.

Switching type from 'AssignUserRole' will remove all data specific to it. Are you sure want to continue?



#### II. Security requests workflow

Activating the security request workflow requires to navigation to **Security and Compliance Studio -> Security -> Security request workflow configuration** form.

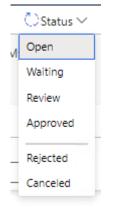
A new workflow will need to be created by using the "New" button. This will open the standard workflow editor where the workflow approval design will be created. Once it is done it will appear in the form and it will be activated.

Security Requests		nfiguration				
₽ Filter						
O Status	Default	ID	Name	Association	Туре	Instances Active vers
0	~	000247	Security Requests workflow	Organization-wide	DSMSecurityRequestWorkflowType	0 2.0.0.0

Activating the security request form will replace the "Status" and "Owner" buttons with the "workflow" option from where the request can be submitted to approval. From here the standard workflow framework will kick in and do the rest, based on the workflow design.

it	+New	📋 Delete	$\odot$ Status $\sim$	$\otimes$ Owner $\smallsetminus$	Request	dit	$+_{New}$	🗓 Delete	<sup>(</sup> )Workflow ∨	Request	Manage
	Security r	equests   1	My view ∽				Security n	equests   N	∕ly view ∽		
	Dem	o SR 1	Inactiv	e workflo	w		Demo	o SR 1	Active w	orkflow	,

If the workflow is not activated the approval can be done manually by the owner of the request using the "status" button.



Once the "created by" user finishes the filling in all the necessary information on the Security Request it will select the **owner** (the person designated to review and take suitable action) and it will change the status to **Waiting.** In this moment only the owner of the request can take action.

When the owner will start looking into the request(s) it will set the status to **Review**.

As soon as the owner decided what action to take he can do the following:

- Approve set the status to **Approved** and the request will be automatically created.
- Reject set the status to **Reject** and decline the request.
- Require more information from the user and set the status to **Rejected** or back to **Open**.

#### Licensing framework update

Microsoft has taken some decisions during the last releases and introduced multiple licenses like Finance, SCM, EAM, Operations, Retail, HR, Activity and Team members. For more details, you can have a look at Microsoft's new licensing guide. These changes left customers confusing about how they can be compliant with new license changes. That's why we have managed during the past releases to keep up with them and redesign the SCS licensing framework to be compliant with the new changes.

#### Steps required after update to SCS 10.0.24.20:

a) Navigate to Security and Compliance Studio module -> Inquires -> and open Security explorer form and here run the <u>"Refresh licenses"</u> batch job option and wait to finish.

Fina	nce and Operati	ons				
ÖC	reate snapshot	Refresh licenses	\land Reset pins	Advanced view	Show joined	Export to Excel
V	<sup>My view</sup> ∽ Securit	ty explore	r: full vie	w		
	USERS				ROLES	
	⊣¤ Pin users				⊣¤ Pin role	

b) After the "Refresh licenses" job finished navigate to Security and Compliance Studio module -> Setup -> and open the Parameters form.

On the License count tab there will be a new grid that will display all the licenses detected on the system. This grid has been design to store and save the data related to acquired licenses, details that you can get from your Microsoft admin page: https://admin.microsoft.com/

Security and compliance studio parame	ters
---------------------------------------	------

General	General setup for the purchased	licenses
License count	Open admin.microsoft.com	
Data migration	O C License ↑	No of licenses
bata migration	<ul> <li>Activity users</li> </ul>	15 <b>0</b>
Enhanced SoD rules	EAM	20
	Finance	10
Number sequences	HR	60
	OPERATIONS	90
	ProjectOperations	67
	Retail	55
	SCM	18
	Team members	76

c) Navigate to License optimization workspace and here you can find the updated information related to number of used licenses in your system.

Summary	License				
ල <u>සි</u>	Usage	O License type	Actual use Lic	ensed users c R	Remaining us
		Finance	11	10	-1
Security	All users	HR	10	60	50
Merge roles explorer	Full users	ProjectOperations	4	67	63
		Retail	15	55	40
	Activity users	SCM	29	18	-11
	Team members	Activity users	12	150	138
	realitimenibers	Team members	16	76	60
	Scenarios	EAM	0	20	20
		OPERATIONS	0	90	90

### 

**NOTE:** In this release, we made updates to comply with Microsoft changes around the new License SKUs for Dynamics 365 subscriptions. Although we tested all standard security and some custom security objects, we would not know if all scenarios for customizations on security will be reflected correctly. In case the license SKUs are not displayed correctly, we would need your feedback to improve the complex logic.

## 3.3 Export security explorer objects to excel in a denormalized format

You can now export securable objects in a "De-normalized form" from security explorer. All Securable objects related to a particular role/user/duty/privilege/entry points can be exported into an Excel sheet for further analysis.

SERS		ACCOUNTANT	DUTIES	PRIVILEGES	ENTRY POINTS	
🖙 Pin users		🕫 Unpin role	-t⊐ Pin duty	🖙 Pin privilege	-s= Pin entry point	
User ID.	Name	Role name 1	Duty name 1	Privilege name 1	Entry point (AOT name) 1	
OSCAR	OSCAR	Accountant	Configure electronic fiscal	a	al 🧧 🖂 AbatementCertificate_IN	
RetailServiceAccount	RetailService	<ul> <li>Accounting manager</li> </ul>	Enable bank management	p  @ApplicationSuite_Localiz	al 🗧 🔿 AbatementPeriodicCertificate_IN	
STAN	STAN	<ul> <li>Accounting supervisor</li> </ul>	Enable electronic document	Account number enhanced	d 🖂 Accountant_BR	
		<ul> <li>Accounts payable centraliz</li> </ul>	e Enable escheatment proce	s: account reference -ViewLe	d  C Accountant_BR	
		<ul> <li>Accounts payable clerk</li> </ul>	Enable EU sales list process	AccountingSourceExplorer	V 📑 AccountantElectronicAddressEdi.	Privilege name
		Accounts payable manager	Enable financial reports ge	n 🛢 Action class settings maint	a 🗉 🖂 AccountantElectronicAddressEdi	@ApplicationSuite_LocalizationRTax25RegisterProfitEntityMain
		<ul> <li>Accounts payable payment</li> </ul>	Enable fixed assets process	Action class settings view	AccountantElectronicAddressNe.	@ApplicationSuite_LocalizationRTax25RegisterProfitEntityView
		Accounts payable positive	Enable Intrastat process	Action populate records ta	s 🔹 🖾 AccountantElectronicAddressNe	Account number enhanced preview
			Enable escheatr	nent processing for sta	ale-dated accounts payable payme	nts account reference - ViewLedgerShowReferences:
			Enable EU sales	list process		AccountingSourceExplorerView
			Enable financial	reports generator		Action class settings maintain
			Enable fixed ass	ets process		Action class settings view
			Enable Intrastat	process		Action populate records task maintain
			Enable receipt e	electronic fiscal docum	ent process	Add category criterion group
			Enable sales tax			Add category criterion group vendor rating
	1		Enable tax accou			Add components from purchase order

## 3.4 Merge security scenarios and match role

You can now merge more than one scenario into one new scenario if required by business and change in organization setup. This feature is very useful in combining more than one scenario then create a role which can perform all the business process recorded in the scenarios.

	Finance and Operati	ions Preview		D Search for a page						
=	🖪 Audit 🛛 🗟 Optimize	Merge scenarios into one								
		Name								
	Security and o		Description							
	Summary	Security						bachpion		
	<sub>x</sub> ~ 99	156	Requests	+ New 🖉 Edit 🛛 Match roles \cdots More						
				✓ Scenario ↑	Owner	Description	Objects	Created date and time		
	Users	Roles	Scenarios	✓ Create customer	nsadaiya		5	6/28/2019 09:13:17 AM		
				Create purchase order and sales order	nsadaiya		5	7/16/2019 05:52:37 AM		
	+	ତ	Users	Edit access to Audit workbench area	nsadaiya		2	7/2/2019 06:00:43 AM		
	New security			Merged Customer-SO-PO Scenario	vsingh	Merged scenarios to reflect rece	5	7/29/2019 06:38:24 AM		
	request	Merge roles	Roles	Merged scenario	nsadaiya Merged from create customer a		6	7/2/2019 08:46:07 AM		
							-			

## 3.5 Mark any Security Role as Active/Inactive

Mark any security role as "Inactive". Once the role is inactive, it cannot be assigned to any user in SCS. This feature is very useful in limiting the number of security roles that can be assigned to users. Also if you want to preserve a set of roles that should not be updated like standard Microsoft security roles for reference. With SCS, it is useful in helping prevent update standard MS roles by mistake.

+ ⊻	Requests	î	Merge roles	Duplicate role	Lock role	es 윦 Explore	Export Import	Mark active/inactive role			
	Scenarios		✓ Role name		Licen	se type	Role description	Locked			
ite role Import users	Scenanos		✓ SCS_Customer service represent Operations								
			SCS_Create	Customer	Ope	rations					
			SCS_Created from duties Operations								
			E Save + New Delete OPTIONS O								
	Roles			☑ Inactive security roles							
	Duties			Role name		Role (AOT name)					
	Duties		Audito	or		AUDITPOLICYN	MANAGER				
	Segregation of duties		✓ Cost a	ccountant clerk	$\sim$	CAMCOSTACO	OUNTANTCLERK				

## 3.6 Recording steps to scenario.

You can now record Business process steps along with entry points while creating a security scenario for more information.

≡	Ø E	dit + New	📋 Delete	Match roles	Merge scenarios	New from task recording	→ Upload recording	Override permissions on roles	ه م	• 0 🖡	U	ď	×	
7 =	SCENARIO   RECORDING STEPS													
		General		Recording st	eps nsadaiy	• ^		Related information						
		Scenario							Owner				dinfor	
		Recording step	nsadaiya			matio								
		Description			~		2							
		Access required												
	+ Add 🔸 Add module access 🗊 Remove 🖧 Explore													
		✓ Step number		Secu	rable object	Securable type	Access level	Step description		File name				
		2		Defa	aultDashboard	Display	Full contro	ol Go to Default da	ashboard.	Recording s	teps			
					tablelistpage	Display	Full contro	Go to Accounts	receivable > Cu	Recording s	teps			
					tablelistpage	Display	Full contro	Go to All custon	Go to All customers.					
		8		Cust	Table	Display	Full contro	In the list, click t	he link in the sel	Recording s	teps			

Useful in optimizing the license cost while creating a new security role. If an entry point is increasing the license cost, recorded steps will help to decide whether access is required or not.

## 3.7 Override permission based on scenarios

You can now override permission on existing roles based on your recording or a security scenario. This helps security administrators to deny access to some entry points on a particular role. Customized permission can also be set for other access types. Very useful if you want to merge roles and just exclude limited entry points.

Edit + New	🗊 Delete	\Lambda Match roles	New from task recording	$\overline{\uparrow}$ Upload recording	Override permissions on roles	OPTIONS	<u>م</u>	0	0	
SCENARIO										
General							М	erged scenar	io   r	sad
Scenario							Owner			
Merged scenar	rio						nsada	iya		
Description										
Access required	4								_	
Access required		ess 🗊 Remove a	읊 Explore							
Access required	d module acce			iecurable type	Access level	Step descripti	ion		File na	me
Access required	d module acce	Securab	ble object S	iecurable type Display	Access level No access	Step descript	ion		File na	me

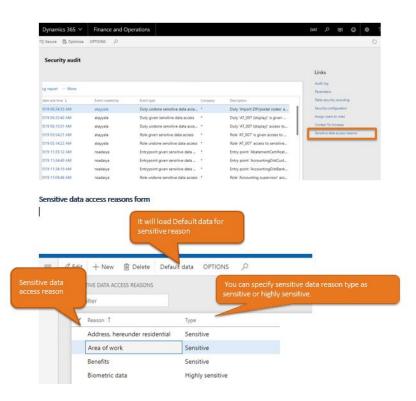
Accounts receivable centralized	Documents accounts receivable	·	
Accounts receivable clerk	Documents customer invoice ev		
Accounts receivable manager	Reviews customer invoice proce		
Accounts receivable payments c	Documents accounts receivable		
Applicant anonymous (external)	External user application for em		
Auditor	Manages and reviews audit poli		
Batch job manager	Maintain and configure settings		
No • PERMISSIONS Read			
PERMISSIONS			
©ERMISSIONS Read Unset Grant Deny Update Unset Grant Deny			
©ERMISSIONS Read Unset Grant Deny Update Unset Grant Deny Create			
PERMISSIONS Read Unset Grant Deny Jpdate Unset Grant Deny Create Unset Grant Deny			

## 3.8 Option to mark, track and audit security objects providing access to sensitive data

Specific definition of sensitive data might be different for different industries or countries. An organization can define specific definition for sensitive data as per their industry, country and policies. For some organizations, sensitive data might be any data that is related to finance, human resource or personal. It is up to an organization to define sensitive data. SCS helps in defining and managing the security objects access to sensitive data. In D365FO we assign security roles to users. Security roles grant access to perform business operations, it might provide access to sensitive data as well. In SCS we can specify which role, duty, privilege or entry point provides access to sensitive data.

Following specific features have been developed in SCS in this release:

• Set up sensitive data access reasons



• Give access to sensitive data- You can mark sensitive data access to a securable object that you feel provides access to sensitive information. If you grant sensitive data access to a securable object, then automatically all securable objects which are related to it are marked as providing access to sensitive data.

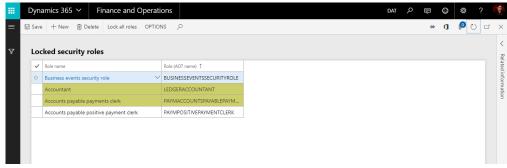
=	🖔 Create snapshot 🛛 🖒 Rese	et pins Advanced view Show joined	options $P$	× ⊐ () 🍳 D ↔
Y	Security explorer: USERS -□ Pin users ···	full view ROLES -≒ Pin role ····	DUTIES -⊏⊐ Pin duty Give sensitive data access	PRIVILEGES ENTRY POINTS -t⊐ Pin privilege ··· -t⊐ Pin entry point ···
	✓ Pin User ID	✓ Pin Role name ↑	✓ Pin Duty name ↑ Access to sensiti	✓ Pin Privilege ✓ Pin Entry po
	\$C0BA	Accounts payable	<ul> <li>A parameter that is used to gro</li> </ul>	A param 🖂 Abatem
	<ul> <li>Admin</li> </ul>	Accounts payable	Access benefits workspace	Accept : 🗾 🖬 🖬 Abatem
	ALICIA	Accounts payable	Access expense management w	Access t 🍵 💍 Abatem
	APRIL	<ul> <li>Accounts receivabl</li> </ul>	Access workforce management 🗸	<ul> <li>Access c</li> <li>Abbrev</li> </ul>
	ARNIE	: Accounts receivabl	Activate tax depreciation process 🗸	: Access 🤄 🖂 Accoun
	<ul> <li>atayyala</li> </ul>	<ul> <li>Accounts receivable</li> </ul>	<ul> <li>Activate, deactivate, update and</li> </ul>	Access 🤅 🗖 Accoun
	axrunner	<ul> <li>Accounts receivable</li> </ul>	Add an existing performance jo	Access r 🔹 🗹 Accoun
	BENJAMIN	Applicant anonyme	<ul> <li>Add custom fields</li> </ul>	Access v 🔹 🗖 Accoun
	BRAD	<ul> <li>AT_</li> </ul>	<ul> <li>Application document entities</li> </ul>	Account 🖂 Account
	BROOKE	AT 007	Approve absences 🗸	account 🔹 🗹 Account

For example, if you grant sensitive data access to a privilege, then related users, roles, privileges, and entry points also are marked as providing access to sensitive data.

- Undo access to sensitive data You can unset sensitive data access to a securable object. If you unset sensitive data access to a securable object, then automatically all securable objects which are related to it lose access to sensitive data.
- **Sensitive data access inheritance** Please refer to the Product Documentation for more details on this topic.
- Use of sensitive data access Once an organization define sensitive data access to securable objects, we can use this information while creating, locking and matching roles.
  - Create Role Wizard When you are creating a new role using create role wizard. It is important to know that whether newly created role will have access to sensitive data.

CREATE	EROLE						
All or	ivileges						
Airpi	mieges						
Sele	ct the privileges to be addee	d to the new role					
AVAI	LABLE PRIVILEGES				SELEC	TED PRIVILEGES	
~	Privilege	Description	User license type		~	Privilege	Description
~	View accountant information		Team members	$\rightarrow$		Import KLADR abbreviations	Import abbreviations from the K
	View accounting distributions in		Team members	÷		Maintain accountant information	
	Maintain accounting distributio		Operations	÷		Maintain accounting distributio	
	View accounting distributions in		Team members	M		Ţ	
	View accounting distributions in		Team members				
	Create distributions for the tran		Operations			at the set of the state of	
	View distributions for the transa		Team members			rivileges having	
	Create distributions for the tran		Activity users			sensitive data	
	View distributions for the transa		Team members			access	
	Create distributions for the tran		Activity users				

• Locked Roles - Security roles having access to sensitive data is highlighted in locked roles form



• Match Roles - In the "Match Roles" form, security objects having access to sensitive data will be highlighted in all the grids.

bynan		e and Operations Acco	unts receiv	able 🗲 Custome	ers 🗲 Al	customers	DA	πP	ē	® 7
/ANAGE	OPTIONS D								∞ <b>()</b>	P 0 ⊑
	ROLES AND SENSITIVE DATA ACCES	is								
Wato	Menu item display	USMScenario	Full co		No acce		Not part of the selec			
	Menu item display		Full co		No acce		Not part of the selec			
	Menu item display	DSMSecurityManagementTie CustTablel istPage	Full co		View			teu role.		
	Menu item display	ForecastSalesTable	Full co		No acce		Not part of the selec	ted role		
	were remaisplay	1 Of Casual Calabi	- un co		NO BUCE		Not part of the select	ited fole.		
Roles										^
~	Role name	Role description	Matc	User license type		Remaining user				
Ē	Project manager	Documents the project forecas:		Operations		59928				
	Production planner	Schedules and plans productio				59928				
	Sales manager	Reviews sales process performa				59928				
	Sales representative	Documents sales events and re		Activity users		29986				1
	Materials manager	Enables and reviews processes,		Operations		59928				
	Materials manager	chables and reviews processes,	25.00	operations		55520				
	e the demand forecasting	Privilege name Maintain demand forecasts for i	. Menu ite	e object type em display		Securable object	e Ful	ess level		Duty license type Operations
Mainta	ain project budgets	View demand forecasts for item	. Menu ite	em display		ForecastSalesTable	e Vie	w		Activity users
Mainta	ain project forecasts	Maintain demand forecasts for i	Menu it	em display		ForecastSalesTable	e Ful	l control		Activity users
Inquir	e into project forecast stat	View demand forecasts for item	. Menu it	em display		ForecastSalesTable	e Vie	w		Team members
Mainta	ain authorization of adjust	View demand forecasts for item	. Menu ite	em display		ForecastSalesTable	e Vie	w		Operations
Mainta	ain authorization of adjust	Maintain demand forecasts for i	Menu ite	em display		ForecastSalesTable	e Ful	l control		Operations
eges tha Privileg		le objects that cannot be accessed	I with the s			Access level	Privilege licens	e type	Menu item	license type
ew dema	and forecasts for item Me		precastSale	sTable	Vie	W	Team members		Team member	rs
	lemand forecasts for i Me	enu item display Fo	precastSale	sTable	Ful	l control	Activity users		Activity users	
aintain d										
aintain d ned dutie Duty na	25	Privilege name	Securable	object type		Securable object	Acce	-ss level		Duty license type
ned dutie Duty na	25	Privilege name View demand forecasts for item		object type m display		Securable object				Duty license type
ned dutie Duty na Inquire	es me		Menu ite				Viev		C	
Duty na	es me into demand forecasts	View demand forecasts for item	Menu ite Menu ite	m display		ForecastSalesTable	View Full	v control	( (	Operations
Duty na Duty na Inquire Enable Mainta	es me into demand forecasts the demand forecasting	View demand forecasts for item Maintain demand forecasts for i	Menu ite Menu ite Menu ite	m display m display		ForecastSalesTable ForecastSalesTable	View Full View	v control	) () ()	Operations Operations
Duty na Duty na Inquire Enable Mainta Mainta	es me e into demand forecasts the demand forecasting ini project budgets	View demand forecasts for item Maintain demand forecasts for i View demand forecasts for item	Menu ite Menu ite Menu ite Menu ite	em display em display em display		ForecastSalesTable ForecastSalesTable ForecastSalesTable	View Full View Full	v control v control	0 0 4 4	Operations Operations Activity users

- Walle
- Audit log enhancements to capture all changes to security objects providing sensitive data access

If we give/undo sensitive data access to a securable object such as role, privilege, duty or entry point, then this event is captured in audit log. The audit log contains the event details like event type and event description.

Event types are as mentioned below:

- Role given sensitive data access/ Role undo sensitive data access.
- Duty given sensitive data access/ Duty undo sensitive data access.
- Privilege given sensitive data access/ Privilege undo sensitive data access.
- Entry point undo sensitive data access/ Entry point undo sensitive data access.
- Below is the image of audit log.

e 🖪 Optimize OPTIONS	Q				(
rity audit					
Audit					
Security history	🔒 Audit log report 🛛 … More				
	✓ Event date and time ↓	Event created by $oldsymbol{\nabla}$	Event type	Company	Description
Role history	/ 3/13/2019 09:01:27 AM	nsadaiya	User undone sensitive data access	*	User ARNIE is unmarked as s
	3/13/2019 09:00:29 AM	nsadaiya	Entrypoint given sensitive data access	*	Entry point 'AbbreviationCod
User history	3/13/2019 08:53:00 AM	nsadaiya	Entrypoint undone sensitive data access	*	Entry point 'AbbreviationCod
	3/13/2019 08:52:32 AM	nsadaiya	Privilege undone sensitive data access	*	Privilege 'Access expense ma
Segregation of duties rules	3/13/2019 08:52:20 AM	nsadaiya	Privilege given sensitive data access	*	Privilege 'Action class setting
	3/13/2019 08:51:37 AM	nsadaiya	Duty given sensitive data access	*	Duty 'Access expense manag
Segregation of duties conflicts	3/13/2019 08:51:09 AM	nsadaiya	Duty undone sensitive data access	*	Duty 'Access expense manag
	3/12/2019 08:52:11 AM	nsadaiya	Role given sensitive data access	*	Role 'Accountant' is given ac
Stand-ins	3/12/2019 06:50:30 AM	nsadaiya	Role undone sensitive data access	*	Role 'Accountant' access to s

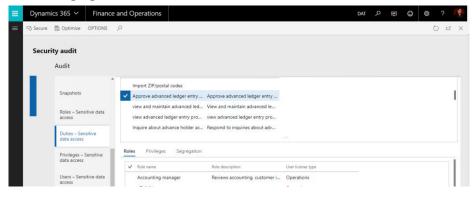
- Sensitive data access forms
  - o Roles Sensitive data access

It shows all the roles which have access to sensitive data. It also shows all the user, duties and privileges related to role. You can also see role history which contained changed events of the role. You can go to security explore using explore button and export the role using Export button.

(	Dynam	ics 365 🗸	Finance	and Operations			DAT 🔎 🗊
5	Secure	🔂 Optimize	OPTIONS	P			
	Secur	ity audit					
		Audit					
			1	🖧 Explore Export			
		Snapshots		✓ Role name	License type	Role description	Locked
		Roles – Sens	sitive data	RapidValue Translator	Team members	Translates RapidValue models i	n
		access		RapidValue user	Team members	Shared role for all RapidValue u	i
		Duties – Sen data access	nsitive	Budget clerk	Activity users	Documents budget events and	f
		uata accesa		Budget contributor	Team members	Enters and approves budget pl	a
		Privileges – data access		Budget manager	Operations	Reviews budget process perfor	
		Users – Sens access	sitive data	Users Duties Privileges	History		
		00000		✓ Event date and time	Event created by	Event type	Company
		Charts		12/12/2018 04:17:44 AM	atayyala	Role created	×
						• · · · ·	

o Duties - Sensitive data access

It shows all the duties which have access to sensitive data. It also shows all the roles, privileges and SoD related to duty. You can go to security explore using "explore" button and you can create SoD rule using "Create segregation of duties rule" button.



o Privileges - Sensitive data access

It shows all the privileges which have access to sensitive data. It also shows all the roles, duties related to privilege. You can go to security explore using "explore" button.

	Dynam	ics 365 🗸	Finance	and Operations				DAT	Q	<li>I</li>	٢	٢	?	And a
=	Secure	🖪 Optimize	OPTIONS	Q								Ċ	) 🗆	×
	Secur	<b>ity audit</b> Audit												
		Snapshots	<sup>^</sup>	룹 Explore										
				Privilege name		Privilege identifier	Privilege description							
		Roles – Sensi access	itive data	✓ Maintain asset ad	Iditions	ASSETADDITIONMAINTAIN	Create and update add-on item							.1
				Generate fixed as	set additions r	ASSETADDITIONMOGENERATE	Generate a list of fixed assets an							41
		Duties – Sen: data access	sitive	View asset addition	ons	ASSETADDITIONVIEW	View add-on items and improve							
		1.1.1.1		Maintain deprecia	ation settleme	ASSETADVRULE_PRETAXDEDUC								
		Privileges – S data access	Sensitive	View depreciation	n settlement ru	ASSETADVRULE_PRETAXDEDUC								
		Users – Sensi access	itive data	Roles Duties										
				✓ Duty name		Duty identifier 🏹	Duty description							Ш
		Charts		Maintain fixed	assets	ASSETFIXEDASSETSMAINTAIN	Maintain fixed assets							Ш

o Users - Sensitive data access

It shows all the users which have access to sensitive data. It also shows all the role related to user. You can also user history which contained changed events of the user.

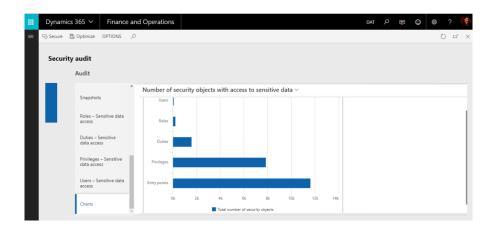
	Dynamics 365 🗸 🛛 Fir	nance and Operations			DAT	ı م	₽ 😳	۲		A.
=	ි Secure 🗓 Optimize OPTIC	ons ,o						Ö	ď	×
	Security audit Audit									
		•								
	Snapshots	✓ User ID ↑	Name	Email	License type		Company	Person		
		\$C0BA	SCOBA	\$C0BA@contosoax7.onmicrosof			dat			41
	Roles – Sensitive da	ALICIA	ALICIA	ALICIA@contosoax7.onmicrosof	Operations		USMF	Alicia	Thorn	
	access	APRIL	APRIL	APRIL@contosoax7.onmicrosoft	Operations		USMF			
	Duties – Sensitive	ARNIE	ARNIE	ARNIE@contosoax7.onmicrosof	Operations		USMF			
	data access	atayyala	Anil Kumar Tayyala (TI)	atayyala@ToIncrease.onmicroso	Operations		USMF			
	Privileges – Sensitiv									
	data access	Roles History								
	Users – Sensitive da access	Role name	Role description	Level Comp	any accounts ID					
		Office integra	tion power user	3 *						ш
	Charts	System user	System role for all users	2 *						ч
	4									

Charts

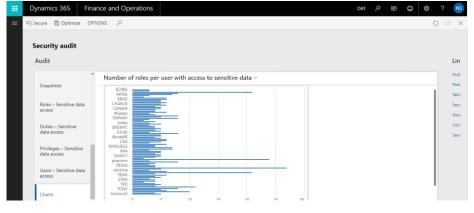
o Number of security objects with access to sensitive data



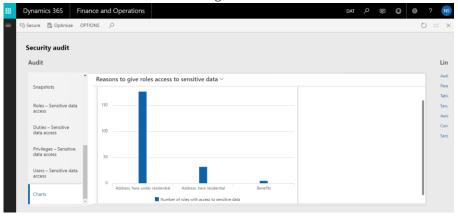
• Number of users with access to sensitive data per organization



#### o Number of roles per user with access to sensitive data



o Reasons to give roles access to sensitive data

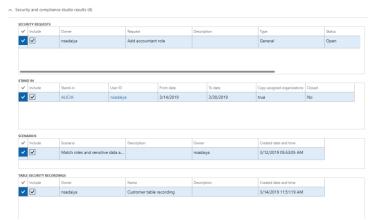


#### • Person search report extension

On the standard Person search report form a new SCS tab is added. For more details on person search report please refer https://docs.microsoft.com/en-us/dynamics365/unified-operations/dev-itpro/gdpr/gdpr-person-search-report. You can find person search report at System administration > Inquires > person search report. Below image is a screen shot of the person search report.

	Dy	nar	nics 365	Fina	ance and Op	erations		:	Syste	em ad	dminist	tration	n 🔪 li	Inquirie	ies >	Person	n search	h repor	t		DAT	Q	Ę	0	٢	ŝ	?		NS
≡	🔛 Sa	ve	+ New	🗊 Delete	Define search	Process r	repo	eport ~	~ 0	OPTIO	NS	Q												↔	٥	p	Ü	ď	×
7			I SEARCH REP O <b>n searc</b>	ort h repor	t																								
=		~	Contact se	arch results	(0)																							1	
		~	Worker sea	arch results	(0)																							1	
		~	Applicant	search resul	ts (0)																							1	
		~	Application	n basket sea	arch results (0)																							1	
		~	Prospect s	earch result	s (0)		ŀ													of n o us									
		~	Prospectiv	e vendor se	arch results (0)															on se		Г						1	L
		~	Driver sear	ch results ((	0)										re	port	t											1	L
		~	Security ar	nd complian	ice studio r <u>esulte</u>	-																							

When you expand SCS results tab, you can see all the records present in SCS, which are related to user id specified while searching the report. In below image we have used user id as nsadaiya.



Please refer to the product documentation *User and Training Guide - Security and Compliance Studio* – available on request and *Documentation BPM libraries* available with the deployable package of the latest SCS release.

## 3.9 Option to create a duty from Matched Privileges grid in Match roles form

You can now create a duty from selecting one or more privileges in the Match roles form to design a security role matching the user work scenario at the least license cost.

The SCS *Create duty from privileges* functionality helps you to select multiple privileges from the *Matched Privileges* grid on the Match Roles form and create a duty. This is very useful feature to help you evaluate the privileges that provide complete access to a recorded security scenario at the least license cost and create a new duty and eventually a role if required..

Select one or more privileges on the Matched Privileges grid.

Matched privileges

~	Privilege name	Securable object type	Securable object	Access level	Privilege license type	Menu item license type
	MergeRoleTest	Menu item display	VendTable	Full control	Activity users	Team members
	Maintain vendors	Menu item display	VendTable	Full control	Activity users	Team members
~	Maintain retail vendors	Menu item display	VendTable	Full control	Team members	Team members
~	Accountant_reduced (display)	Menu item display	VendInvoiceJournal_Action	View	Team members	Team members

#### Click on the Create Duty button as shown below.

MATCHING	CREATE ROLE		CREATE DUTY	SEGREGATION OF DUTIES	VIEW	ASSIGN TO USER
Match roles Find matched entry points Reset data	Create role Create role from privileges	Create role from duties Duplicate role	Create duty from privileges	Create SOD	Simple Advanced	Assign users to role

Enter the new duty name and the description.

Create duty

Parameters	
Duty name SCS	Description

Security objects that are included into the new duty

,∽ Filter		
Object type	Label	
Privilege	Accountant_reduced (display)	
Privilege	Maintain retail vendors	

The new duty is now in place and you can assign it to a security role and user to end users in D365.

# 3.10 Option to import and export data using Data Entities in Security and Compliance Studio

Data entity provides conceptual abstraction and encapsulation (de-normalized view) of underlying table schemas to represent key data concepts and functionalities. A data entity encapsulates a business concept into a format that makes development and integration easier. Below table holds the data entities currently supported for Security and Compliance Studio. The approach has been to enable data entities for all tables in SCS in order to provide import and export capabilities where relevant.

Notes:

• See comments column for additional info when relevant.

Entity Name	Category	Create	Modify/Update	Import	Export	Comments
Scenario	Master	Yes	Yes	Yes	Yes	
File store	Reference	Yes	Yes	Yes	Yes	Reference data for "Scenarios"
Stand-in	Master	Yes	Yes	Yes	Yes	Can be or not reference to "Security requests"
Locked Roles	Master	Yes	Yes	Yes	Yes	Can be or not reference to "Security requests"
SOD	Master	Yes	Yes	Yes	Yes	This is standard entity and can be reference to "Security requests"
Table security recording	Master	Yes	Yes	Yes	Yes	Can be or not reference to "Security requests"
Security Requests	Master	Yes	Yes	Yes	Yes	
SCS Parameters	Parameter	Yes	Yes	Yes	Yes	

# 3.11 Option to compare Security Snapshots stored in the security setup

Snapshot comparison feature allows security officers and administrators to do a detailed comparative analysis between any two security snapshots for all security objects in D365 FOE setup i.e. Users, roles, duties, privileges. Both single record compare and full compare options for the selected snapshots are supported along with multiple views. The comparison option will allow the user to see what modifications had occurred in the security setup since the last changes. The users can keep track of the changes, comprehend and analyze them in order to improve and strengthen the security.



The form that will open will show like this (see Fig. 2) and below a short description of it.

Dyna	Dynamics 365 V Finance and Operations Security and compliance > Inquiries > Snapshot comparison								
🔚 Save	MANAGE	OPTIONS	Q						
COMPA Compa Full cor 1.	re selected npare	VIEW Show all objec Advanced view 2.							
FILT Sele O O O CON	apshot Ci ere Entry Point Privilege Duty Role User IPARE SNAPSHO snapshot	ct type 3.	n				Seco 3	nd snapshot	
~	Name		User licens		ompared	Observation	~	Name	User license type
	Action graph		Operation	s Ye	s	3 modifications found		Demo privilege 1	Operations
	DSMAreaEnt	ityMaintain	None	Ye	s	1 modifications found		Demo privilege 2	Operations
	Florin privile	ge 2	None	Ye	s	0 modifications found		Maintain bar codes	Operations
5.									
	ERENCES								
~	Property		Value from first snapsh	ot		m second snapshot	_		
6.	Entry point a		-			ditLogInit	_		
0.	Entry point a		-			rgeRoles	_		
_	Entry point a	dded	-		DSMSta	ndInClass			

Fig 2. Snapshot comparison form

#### Legend:

#### 1. COMPARE button group - contains two buttons:

- a) Compare selected: will run a comparison only for the selected records from the first grid.
- b) Full compare: will run a full comparison between the two selected snapshots

#### 2. VIEW button group – contains three buttons:

#### a) Show changes only:

- i. when clicked will display only the objects that have been changed (deleted, modified or newly created);
- ii. label will be changed to "Show all objects" (see Fig. 3)

Dyna	amics 365 🗸	Finance and	Operations Security a	nd compliand	e > Inquiries > Snapshot con	nparison		
🔚 Save	MANAGE OF	TIONS 🔎						
COMPA Compa Full con	re selected Sho	w all objects anced view						
FILT Sele O O O COP	apshot com er er er et security object ty Entry Point Privilege Duty Role User Werr ENAPSHOTS t snapshot					Secc	nd snapshot	
~	Name		User license type	Compared	Observation	~	Name	User license type
	Action graph		Operations	Yes	3 modifications found		Demo privilege 1	Operations
	DSMAreaEntityN		None	Yes	1 modifications found		Demo privilege 2	Operations
	Florin privilege 2		None	Yes	0 modifications found		Maintain bar codes	Operations

Fig. 3 See a list of the modified objects

#### b) Show all objects:

i. when clicked will display all the objects from both of the selected snapshots

ii. label will be changed to "Show changes only" (see Fig. 4)

ynamics 365 🗸	Finance and C	perations Security a	nd complianc	e > Inquiries > Snapshot co	mpar	son		
ave MANAGE C	PTIONS 🔎							
mpare selected St	ew ow changes only tvanced view							
Snapshot co FILTER Select security object Entry Point Privilege Duty Role User	ype							
COMPARE SNAPSHOT	-						nd snapshot	
COMPARE SNAPSHOT		User license type	Compared	Observation		3		User license type
COMPARE SNAPSHOT	$\overline{}$	User license type	Compared Yes	Observation 0 modifications found		3	~	User license type Operations
COMPARE SNAPSHOT	v tings maintain			0 modifications found		3	Name 1	Operations
COMPARE SNAPSHOT: First snapshot 2 V Name 1 Action class set	v tings maintain	None	Yes	0 modifications found	1	3	Name 1 Delete write-off factors	Operations
COMPARE SNAPSHOT: First snapshot 2 V Name 1 Action class set Action class set Action graph	v tings maintain	None None	Yes Yes	0 modifications found 0 modifications found	1	3	Name 1 Delete write-off factors Demand Forecasting external API se	Operations None
COMPARE SNAPSHOT: First snapshot 2 V Name 1 Action class set Action class set Action graph	tings maintain tings view e records task maint	None Operations	Yes Yes Yes	0 modifications found 0 modifications found 3 modifications found	1	3	Name 1 Delete write-off factors Demand Forecasting external API se Demo privilege 1	Operations None Operations
COMPARE SNAPSHOT: First snapshot 2 V Name 1 Action class set Action class set Action graph Action populat	tings maintain tings view e records task maint ersions	None None Operations None	Yes Yes Yes Yes	0 modifications found 0 modifications found 3 modifications found 0 modifications found	1	3	Name 1 Delete write-off factors Demand Forecasting external API se Demo privilege 1 Demo privilege 2	Operations Operations Operations

Fig 4. See a list of all objects from selected snapshots

c) Simple view: - When clicked some fields will be hidden (this is the default view when the form is opened) and the label will be changed to "Advanced view". (See Fig. 4 as by default the form is in Simple view)

d) Advanced view: - when clicked, the "identifier" and "User license type" fields will be visible and the label will be changed to "Simple view" (see Fig 5)

Dyna	amics 365 Y Finance and Ope	erations Security and compliance	> Inquiries > Snapshot con	nparison						
Save										
OMPAI										
	re selected Show changes only npare Simple view									
Sn	apshot comparison									
Sele	ct security object type									
	Entry Point									
•	Privilege									
	Duty									
	Role									
0	User									
~	IPARE SNAPSHOTS									
First	snapshot						Second snapshot			
2	~			1		- F	3 V	1		_
~	Identifier	Name 1	User license type	Compared	Observation		✓ Identifier		Jser license type	
	FORECASTPOSITIONSBYBUDGETPLANG.	A parameter that is used to group	Team members	Yes	0 modifications found		VENDPROSPECTIVEVENDORDATAA		Team members	
	PURCHRFQFORMLETTER_ACCEPTPROCE	Accept a request for quotation	Activity users	Yes	0 modifications found		HCMWORKERACTIONCOMPFIXEDE		Team members	
					0 modifications found		TMSINVOICEAPPROVALDENYPROC	Denv invoice approva	leam members	_
_	HCMBENEFITWORKSPACE	Access benefits workspace	Team members	Yes	0 modifications found					_
	HCMBENEFITWORKSPACE HCMCOMPENSATIONWORKSPACE	Access benefits workspace Access compensation management.	Team members Operations	Yes Yes	0 modifications found 0 modifications found		HCMPOSITIONACTIONWFAPPRDE	Deny position actions by using a wo	Team members	
			Operations	-	-		HCMPOSITIONACTIONWFAPPRDE HCMWORKERACTIONTERMWFAPP	Deny position actions by using a wo Deny termination worker actions usi	Team members Team members	-
	HCMCOMPENSATIONWORKSPACE	Access compensation management.	Operations Operations	Yes	0 modifications found		HCMPOSITIONACTIONWFAPPRDE HCMWORKERACTIONTERMWFAPP HCMWORKERACTIONTRANSWFAP	Deny position actions by using a wo Deny termination worker actions usi Deny worker actions by using a wor	Team members Team members Team members	
	HCMCOMPENSATIONWORKSPACE TRVEXPENSEADMINANALYTICS	Access compensation management. Access expense administrator analy.	Operations Operations	Yes Yes	0 modifications found 0 modifications found	_	HCMPOSITIONACTIONWFAPPRDE HCMWORKERACTIONTERMWFAPP HCMWORKERACTIONTRANSWFAP	Deny position actions by using a wo Deny termination worker actions usi Deny worker actions by using a wor	Team members Team members	

Fig 5. Advanced view

- 3. Filter group contains one radio button control:
- a) Select security object type: select the security object type to be displayed in the grids below.
- 4. Compare snapshots group contains two drop downs to select the snapshots to compare
  - a) First snapshot : select the snapshot that will be compared
  - b) Second snapshots: select the snapshots that first snapshot will be compared with **Observation**:
    - i. Second snapshot will be disabled until first snapshot will be selected
    - ii. Second snapshot cannot be lower or equal with first snapshot (see fig. 6)

Second snapshot needs to be higher than the first one.	
Snapshot comparison	
FILTER	
Select security object type	
Entry Point	
Privilege	
Duty	
O Role	
🔿 User	
COMPARE SNAPSHOTS	
First snapshot	

Fig. 6 snapshot selection restriction

- **5.** Grid group contains two grids. One for each snapshot selection:
  - a) Left grid: shows the records associated with the value from First snapshot dropdown. Observations:
    - i. In column **Compared** you will see if the record was already compared or not.
    - ii. in column **Observation** you will see how many changes were detected

Colour legend:

Colour	Definition
Red	The records exist in first snapshot, but not the second one -> the security object was deleted.
Blue	The records exist in both snapshot but changes were detected -> the security object was modified.

b) Right grid: shows the records associated with the value from Second snapshot dropdown.

Colour legend:

Colour	Definition			
Green	The record exists only in the second snapshot ->			
	the security object was newly created.			

6. Details group – contains one grid where the differences will be displayed.

a) Difference grid: shows the differences for the selected record (from first grid) in comparison with the second one. Here you can see what was modified. The old value, the new value and the property that was changed.

E.g.: 1) the license type for a role has changed from "Team members" to "Operations" it will display the following:

Property	Value from first snapshot	Value from second snapshot
UserLicType	Team members	Operations

2) A new duty was added to the selected role:

Property	Value from first snapshot	Value from second snapshot
Duty added	-	View sales

3) A new duty was removed to the selected role:

Property	Value from first snapshot	Value from second snapshot
Duty removed	Maintain sales	-

## 3.12 Enhanced Audit log capability to capture all the changes from development space (AOT) as well into Audit Log.

The Audit log will have a larger spectrum and will capture all of the changes from security configuration. Beside the Audit log we will also include a visualization of the changes, of the comparison so the user can analyze.

ecurity aud	ait							
ummary		Audit						
• <sup>(1)</sup>	<b>:</b>	Security history	🗋 Audit log report 🛛 🗥 More					
			✓ Event date and time ↓	Event created by	Event type	Company	Description	
Thanges racked	Role changes	Role history	5/15/2018 05:22:19 AM	Admin	Entry point created	dat	Entry point New entry point from AOT created (fro	om AOT)
			5/15/2018 05:19:58 AM	Admin	Entry point deleted	dat	Entry point Active directory users deleted (from AC	T)
x <sup>8</sup>	□	User history	5/15/2018 05:18:30 AM	Admin	Privilege modified	dat	Privilege Maintain Dynamic Security Management	IT Audit modified (from
<u> </u>		Segregation of	5/15/2018 05:18:19 AM	Admin	Privilege modified	dat	Privilege Florin privilege 1 modified (from AOT)	changes
		duties rules	5/15/2018 05:18:16 AM	Admin	Privilege modified	dat	Privilege DSMParametersEntityView modified (fror	<sup>m AOT)</sup> made
Jser changes	Stand-ins		5/15/2018 05:18:16 AM	Admin	Privilege created	dat	Privilege PrivielgeFromAOT created (from AOT)	from AOT
		Segregation of	5/15/2018 05:18:16 AM	Admin	Privilege created	dat	Privilege FlorinPrivilegeUITest created (from AOT)	
台	ዶ。	duties conflicts	5/15/2018 05:16:43 AM	Admin	Privilege modified	dat	Privilege Apply action modified (from AOT)	
			5/15/2018 05:14:45 AM	Admin	Duty modified	dat	Duty Maintain security recording modified (from A	AOT)
	Segregation of	Stand-ins	5/15/2018 05:14:45 AM	Admin	Duty modified	dat	Duty Florin Duty 1 modified (from AOT)	
ocked roles	duties rules		5/15/2018 05:14:34 AM	Admin	Duty modified	dat	Duty Approve BOMs modified (from AOT)	
		Data security	5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty FlorinDutyUITest created (from AOT)	
÷	格		5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty Duty created from AOT created (from AOT)	
		Azure AD domains	5/15/2018 05:14:04 AM	Admin	Role modified	dat	Role Full read access modified (from AOT)	
Print audit report	Security explorer		5/15/2018 05:14:01 AM	Admin	Role created	dat	Role Role test from AOT created (from AOT)	
-p		Snapshots	5/15/2018 05:14:01 AM	Admin	Role modified	dat	Role Florin Role 1 modified (from AOT)	
		1.1.1.1	5/15/2018 05:13:52 AM	Admin	Role created	dat	Role FlorinRoleUITest created (from AOT)	
		Charts	5/15/2018 05:13:15 AM	Admin	Role modified	dat	Role Chief executive officer modified (from AOT)	
			5/15/2018 04:08:48 AM	Admin	Duty modified	USMF	Duty Florin Duty 1 modified	
			5/15/2018 04:08:43 AM	Admin	Duty modified	USMF	Duty Approve BOMs modified	
			5/15/2018 04:08:40 AM	Admin	Duty created	USMF	Duty FlorinDutyUITest created	
			5/15/2018 04:08:30 AM	Admin	Role created	USMF	Role FlorinRoleUITest created	
			5/15/2018 04:08:30 AM	Admin	Role modified	USMF	Role Florin Role 1 modified Ch	nanges
			5/15/2018 04:08:29 AM	Admin	Role modified	USMF	Role Chief executive officer modified	
			5/15/2018 04:04:29 AM	Admin	Role created	*	Role FlorinRoleUITest created	

New Events types that will be used to track changes done directly to permissions from Development environment:

Event name	Status
Entry point deleted	New
Entry point modified	New
Entry point created	New

This comes as a solution of capturing all the changes no matter if they took place in the UI (user interface) or directly into development space (in Visual Studio).

## 3.13 Option to create one or more privileges and also one or more duties while merging roles.

You now have an option to create duties along with the privileges while using the "Merge roles" feature. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.). In addition you are also warned of possible SOD violations while you select the roles to be merged.

MERGE ROLES Select the entry point types to be added to the target role. For ea added to the target role.	Create single privilege option
CREATE SINGLE PRIVILEGE	
Yes Merged Accountin V	
ENABLED PRIVILEGE NAME	
DISPLAY MENU ITEMS	
OUTPUT MENU ITEMS	
TABLE PERMISSIONS	
You can add a created privilege to a duty. Select the privileges to be added to a du CREATE DUTY	uty. For each selected privilege, a duty is created. Instead of the privilege, the created duty is added to the target role
Yes 💿	
CREATE SINGLE DUTY	
Yes Merged Accountin V	
ENABLED DUTY NAME	
ACTION PRIVILEGES	
DISPLAY PRIVILEGES	
OUTPUT PRIVILEGES	
TABLE PRIVILEGES	

#### 3.14 Ability to create scenarios from D365 module menus

"Add module access" feature helps you to create a new scenario based on the complete list of a module menu items with a desired level of access types. This is of great help when you desire to have a security role providing you access to all or most of one module features. You can also select the access type for the module security objects- No access, View, Edit, Create, Correction and Full control.

ALIZE PAGE OPTIONS	F	DIT SHARE				WH	HICH MODULE?	
open for editing Security diagnost		lead mode Get a link V				~	∕ Area î	
alize this form Advanced Filter/S		levert					Accounts paya	able
workspace 🗸							Accounts rece	ivable
							Audit workber	nch
ENARIO							Budgeting	
ieneral			dd mod	ule access	ARScena	rio   vsingh	Cash and ban	k management
		F	add mod	ule access			Common	
Scenario ARScenario					Owner vsingh		Consolidation	-
Anaceriano					vsingn		Cost accounti	-
lossription							Cost manager	
escription							Credit and col	
Description							Credit and col Demo data	lections
ccess required							Credit and col Demo data Expense mana	lections
	Remove 🖧 Explore						Credit and col Demo data Expense mana Fiscal books	lections
ccess required	Remove 🖧 Explore Securable object type	Access level	File	Remark			Credit and col Demo data Expense mana Fiscal books Fixed assets	lections Igement
Access required		Access level View	File	Remark			Credit and col Demo data Expense mana Fiscal books Fixed assets Fleet manager	lections Igement ment
<ul> <li>ccess required</li> <li>+ Add t Add module access </li> <li>Securable object</li> <li>Customer/invoiceWorkspace</li> </ul>	Securable object type Menu item display	View		Remark			Credit and col Demo data Expense mana Fiscal books Fixed assets Fleet manager General ledge	lections Igement ment
<ul> <li>cccess required</li> <li>+ Add ↑, Add module access ⓐ</li> <li>✓ Securable object</li> <li>CustomerinvoiceWorkspace</li> <li>CustPaymentWorkspace</li> </ul>	Securable object type Menu item display Menu item display	View View		Remark			Credit and col Demo data Expense mana Fiscal books Fixed assets Fleet manager	igement ment r
<ul> <li>ccess required</li> <li>+ Add t Add module access </li> <li>Securable object</li> <li>Customer/invoiceWorkspace</li> </ul>	Securable object type Menu item display	View		Remark			Credit and col Demo data Expense mana Fiscal books Fixed assets Fleet manager General ledge o access iew	lections Igement ment
<ul> <li>cccess required</li> <li>+ Add ↑, Add module access ⓐ</li> <li>✓ Securable object</li> <li>CustomerinvoiceWorkspace</li> <li>CustPaymentWorkspace</li> </ul>	Securable object type Menu item display Menu item display	View View		Remark		Vie	Credit and col Demo data Expense mana Fiscal books Fixed assets Fleet manager General ledge o access iew	r
ccess required     + Add ↑, Add module access      Securable object     CustomerinvoiceWorkspace     CustPaymentWorkspace     CustTableListPage	Securable object type Menu item display Menu item display Menu item display	View View View		Remark		Vie Ed Cr	Credit and col Demo data Expense mana Fiscal books Fixed assets Fleet manager General ledge o access lew dit	igement ment r
<ul> <li>cccess required</li> <li>+ Add + Add module access </li> <li>✓ Securable object</li> <li>Customer/invoiceWorkspace</li> <li>CustRaymentWorkspace</li> <li>CustTableListPage</li> <li>CustTableHoldListPage</li> </ul>	Securable object type Menu item display Menu item display Menu item display Menu item display	View View View View		Remark		Vii Ed Cr	Credit and col Demo data Expense mana Fiscal books Fixed assets Fleet manager General ledge o access lew dit reate	r

You can also create an associated security request in the same step to ensure proper tracking. You can then run match roles from the same form to find out the best matching role at the least license cost.

			CECOECATION OF I		
CHIN chire		Create role from du	SEGREGATION OF I	Simple	ASSIGN TO USER Assian users to role
	tched entry points Create role fro		create SOD	Advanced	Assign users to role
et da					
	ENARIO				
Ma	tch roles				
_					
ecu	urable objects				
~	Securable object type	Securable object	Required access	Maximum access on ro	ole Remark
	Menu item display	CustomerInvoiceWorkspace	View	View	✓
Menu item display C		CustPaymentWorkspace	View	View	✓
	Coourity roles r	natah dagraa	liew	Full control	$\checkmark$
	Security roles r	natch degree	liew	View	$\checkmark$
_	ivienu item display	CUSIN THE	View	View	$\checkmark$
	Menu item display	MCRCustUnm th	View	No access	Not part of the selected role
	Menu item display	SalesTableListPage	View	View	✓
Role	S				
~	Role name	Role description	Match degree	1 User license type	Remaining user lice
	Accounts receivable manager	Reviews customer invoice p	ro 72.	31 Operations	59933
	Accounting manager	Reviews accounting, custon	ne 68.0	56 Operations	59933
	Accounts receivable clerk	Documents customer invoid	.e 68.0	66 Operations	59933
	Accountant	Documents accounting eve	nt 60.	37 Operations	59933
	Accountant				
	Accounting supervisor	Reviews accounting process	s p 57.	14 Operations	59933
		Reviews accounting process Reviews collections process	·	14 Operations 92 Operations	59933 59933

# 3.15 Snapshots based performance and scalability enhancements

A Snapshot means a version of the current security configuration setup. The entire functionality for Rebuild Data, Security Explorer and Match Roles revolves around the security objects (roles, duties, privileges and entry points) and the associations between them (duties assigned to role; privileges assigned to each duty, etc.). All of these are kept in standard code that was preserved, externally, into a DLL. Using this DLL for multiple scopes in Security and Compliance Studio end up with a performance on the above mentioned business logics/functionalities. As a response, our solution was to create a structure of tables to keep the data related to each security object and the association between them and easily access it directly from tables and also much faster. This was important to support security analysis of scenarios with very high number of security objects. This has led to drastic improvement in the "Match roles" and "Rebuild data" programs performance. For example analyzing scenarios with 200 objects takes a minute.

Security and compliance studio parameters	
General	
Prefix SCS	
Color for covered duties and pri Yes	
Color Hex #	
D3D3D3	Snapshots
INITIALIZE SCS IT AUDIT	
Lock 'Initialize Security and com	
Yes 💽	
SNAPSHOTS	
Limit number of snapshots	
1	

Security administrator can decide on the number of snapshots to be stored as per company policy. You can also lock a snapshot if you don't want it to be deleted by checking on the *Protected* check box.

accounting					
st accounting	▲ Security				
management	Security requests				
dit and collections	Scenario	*			
mo data	Table security recording				
pense management	Locked security roles				
ixed assets	Stand-in				
leet management	Snapshots				
eneral ledger	Assign users to roles				
luman resources	Security configuration				
nventory managemen	Security diagnostics for task				
laster planning	recordings				
Organization	Merge roles 💙	*			
administration	Segregation of duties				
Payroll	⊿ Inquiries				
Procurement and sour Product information	cing	*			
roduct information nanagement	Security audit report				
Production control	Audit log				
Project management a accounting					
Questionnaire	Periodic tasks				
Retail	Create role from				
ales and marketing	duties/privileges				
Security and complian	ce Create scenario from module				
	Initialize Security and				

1	Generated from batch, version 1 on 2/13/2018 03:55:37 am	Automatically create from batch job on 2/13/2018		2/13/2018 03:55:37 AM	
2	Generated from batch, version 2 on 2/13/2018 05:56:11 am	Automatically create from batch job on 2/13/2018	vsingh	2/13/2018 05:56:11 AM	
3	Generated from batch, version 3 on 2/13/2018 06:11:50 am	Automatically create from batch job on 2/13/2018	vsingh	2/13/2018 06:11:50 AM	
4	Generated from batch, version 4 on 2/28/2018 08:31:23 am	Automatically create from batch job on 2/28/2018	vsingh	2/28/2018 08:31:23 AM	

A batch program need to be set up for automatic deletion of the snapshots based on the parameter

settings. "Set up automatic deletion"

This feature also lays the foundation for further enhancements in Audit Workspace to capture, compare and visualize Snapshots of the complete D365 FOE data log.

"Limit number of snapshots" parameter functionality has been change as following

a) "-1" (negative one) value will used to store unlimited number of snapshots. This will also pop-up two warnings to inform the user.

b) "0" (zero) value will not keep any snapshot versions except the ones marked as 'protected'.

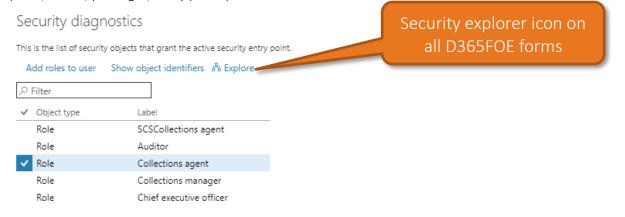
# 3.16 Improved "Create role wizard" based on a grid framework

Create role wizard" is now based on a new grid framework making it a great user experience. This wizard helps you to create a new security role based on duties and privileges with letting you know the license type before role creation.

CRE	ATE ROLE											
A IL	duties											
All	auties											
Sele	ect duties to be add	ded to the ne	ew role									
AV.	AILABLE DUTIES							SELE	CTED DUTIES			
~	/ Duty		Description		User license type			~	Duty	Descrip	tion	User license type
	Maintain Absorptio	on Costs			Operations		$\rightarrow$		Inquire into Absorption Costs			Team members
	Import ZIP/postal c	odes			Operations				Inquire into purchase agreem	Respor	nd to inquiries about p	Team members
	Approve advanced	ledger ent	Approve ad	dvanced ledger ent	Operations		$\leftarrow$					
	view and maintain a	advanced I	View and n	naintain advanced I	Team members							
	view advanced ledg	ger entry p	view advan	ced ledger entry p	Team members	R	ole	lic	ense type			
						b	petor	^e	you finish			
CREA	TE ROLE											
Sum	mary					_	_					
Revie	ew the selected role setup	o. Click Finish to	create the role	e.								
The	e resulting role will have the u	user license type	Operations									
	name	Role description										
SC	S_NewRole	SCS_NewRole										
Sele	cted privileges								Selected duties			
Priv	vilege name	Description		License type.					Duty name		Description	License type.
Im	port KLADR abbreviations	Import abbreviat	tions from th	Operations					Inquire into Absorpti			Team Members
	w accounting distributions			Team Members							Respond to inquiries about p	Team Members

#### 3.17 Accessing Security Explorer from all D365 FOE forms

You can now access the Security and compliance studio security explorer embedded in all D365 FOE forms from security diagnostics. This provides a very useful way to analyze users and associated security objects (roles, duties, privileges, entry points) that have access to that D365 FOE form.



Clicking on the icon will provide you a 360 degree view of that object type.

ERS	2 - 1			COULTC	TIONS AGENT		DUTIES			PRIVIL			ENTRY POINT			
Pin	users			s≊ Ung	in role		-8ª Pin (	duty		-es Pin	privilege		-t= Pin entry	point		
	User ID 1	Name	Highest license typ		Role name 1	License type		Duty name 1	License type		Privilege name 1	License type	×	Entry point (AOT name) 1	Access right	Entry point ty
	ARNIE	ARNIE	Operations	-10 .	Collections agent	Operations		Collections workspace	Team members		Calculate interest notes	Operations		□ AccountingDistCustFreeInvoice	View	Menu item
	Connie	CONNIE	Operations					Inquire into bill of exchange s	Team members		Cancel collection letters	Operations		☐ AccountingDistCustInvJour	View	Menu item
	OSCAR	OSCAR	Operations					Inquire into collections status	Operations		Cancel interest notes	Operations		☐ AccountingDistMarkupTransInv	View	Menu item
•	SARA	SARA	Operations					Inquire into credit card proce	Team members		CashDiscountEntityView	None		☐ AccountingDistMarkupTransPO	View	Menu item
								Inquire into customer invoice	Activity users		Change transaction collection	Operations		☐ AccountingDistMarkupTransR	View	Menu item
								Inquire into customer master	Team members		Change/edit customer transa	Activity users		☐ AccountingDistPurchTable	View	Menu item
								Inquire into customer payme	Activity users		Change/edit customer transa	Operations		☐ AccountingDistributions	View	Menu item
								Inquire into customer referen	Team members		Change/edit customer transa	Operations		□ AccountingDistributionsDocu	View	Menu item
								Maintain activities	Team members		Correct interest codes	Team members		☐ AccountingDistTaxTransTmp	View	Menu item
								Maintain collections transacti	Operations		Create a customer record fro	Operations		☐ AccountingDistVendEditInvDe	View	Menu item
								Maintain contacts	Activity users		Create a customer record fro	Operations		☐ AccountingDistVendEditInvHdr	View	Menu item
								Maintain customer master	Operations		Create collection letters	Team members			View	Menu item
								Maintain financial period clos	None		Creating a customer from pro	Operations		□ ActivitiesMain	Full control	Menu item
								Maintain periodic settlement	Operations		CustBalanceGenerate_CN	Team members		☐ ActivitiesMainBasic	View	Menu item
								Manage customer credit and	Team members		CustCustomerGroupEntityView	None		□' ActivitiesMainBasic	Full control	Menu item
								View sensitive bank account i	None		CustDirectDebitMandateEntit	None		Activity/ViewRecord	View	Menu item

## 3.18 Option to create duties and SOD compliance check as well while merging roles.

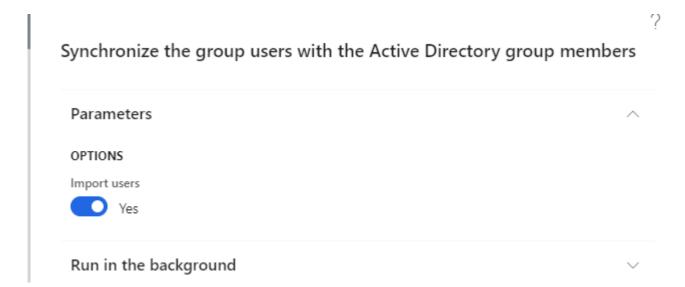
You now have an option to create duties along with the privileges while using the "Merge roles" feature. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.). In addition you are also warned of possible SOD violations while you select the roles to be merged.

🛞 Roles 'Accounting manager' and 'Accountan	nt' are in violation of segregation of duties r	ule 'New Segregation of duties rule2':
MERGE ROLES		
Select or enter the role to merge to TARGET ROLE Name SCS_AccountingSuperUser V Yes	o. c target role?	SOD violations warning
Select the roles to merge from.		
AVAILABLE ROLES		SELECTED ROLES
✓ Available roles		✓ Selected roles
Accounting supervisor	$\rightarrow$	Accounting manager
Accounts payable centralized pay		Accountant
Accounts payable clerk		
Accounts payable manager		
Accounts payable payments clerk		
ACTION MENU ITEMS  DISPLAY MENU ITEMS  OUTPUT MENU ITEMS  TABLE PERMISSIONS  CREATE DUTY	PRIVILEGE NAME SCS_AccountingSuperUser SCS_AccountingSuperUser SCS_AccountingSuperUser Create duty option	
Yes		
	JTY NAME	
	CS_AccountingSuperUser ∨	
	CS_AccountingSuperUser ∨	
	CS_AccountingSuperUser $\lor$	
TABLE PRIVILEGES S	CS_AccountingSuperUser $\lor$	

## 3.19 Importing New Users while Synchronizing the group users with the Active Directory group members

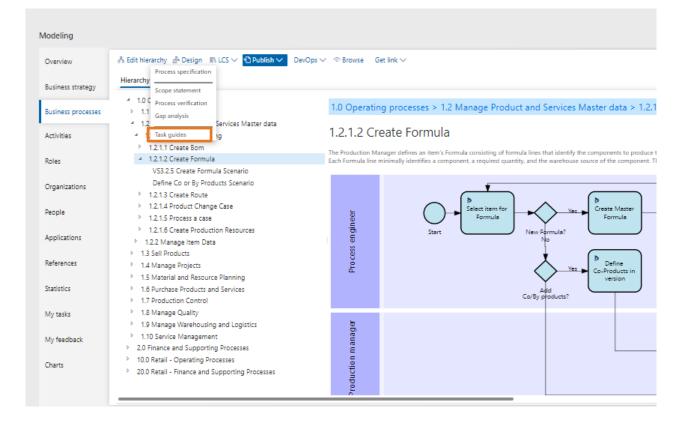
This is very useful for offline analysis and drill down of the required security setup in a company or department. We added a new small feature to our Azure AD group synchronization job. On the dialog of the Synchronize the group users with the Active Directory group members, we introduced a new parameter to import users. When enabled, it will not only synchronize the Azure AD group member information but will also look for users which are not a user in Dynamics 365. The user will be added to the application together with the group information. The default login company and language will be copied from the Group settings.

By introducing this feature, the creation of users, assigning roles and check for possible Segregation of Duties with our enhanced SoD features can be fully automated with information from Azure Active Directory.



## 3.20 Uptake RapidValue BPM Suite Scenarios directly as SCS Security Scenarios

Customers can now directly upload the RapidValue Scenario task guides per security roles (Procedure activities which include flows across multiple roles) as a Security scenario in Security and Compliance Studio. This will be very useful where both RapidValue BPM Suite and Security and Complicate Studio are implemented. You might be aware that now in RapidValue, you can have Business process hierarchy with its linked task guides exported from RapidValue to Share Workspace. Export logic takes care of both the modeling techniques where customer is using Flow-Activity way of modeling and also the Scenario" Procedure Activity" way of capturing flow variations.



If the customer is predominantly using Scenarios (Procedure Activity) based modeling; following logic applies.

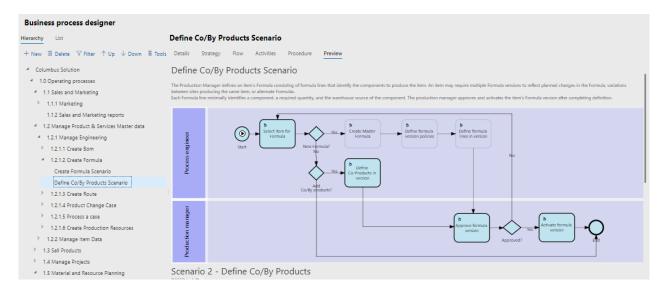


Figure: Scenario-Procedure activity based modeling

#### Manage sub activities for Scenario 2 - Define Co/By Products

In the left pane, select steps. In the right pane, select or create the activity to link as sub activity to the selected steps. Flow activities Activities Unlink sub activities  $\checkmark$ Exists in flow Sub activity Title Go to Product information man... Select item for Fo ing of formula lines that identify the components to produce the item. An item may *n* ired quantity, and the warehouse source of the component. The production manager 1.2 In the list, find and select the de... Select item for Formula 2.1 Click Formula versions. Define Co-Products in version On the Action Pane, click Formu... Define Co-Products in version 2.2 2.3 Click Co-products. Define Co-Products in version 2.4 Click New Define Co-Products in version 2.5 Define Co-Products in version In the list, mark the selected row. 2.6 In the Item number field, enter ... Define Co-Products in version 2.7 In the Production type field, sele... Define Co-Products in version 2.8 In the Warehouse field, type a v.. Define Co-Products in version 2.9 In the Quantity field, enter a nu... Define Co-Products in version In the By-product cost allocatio... Define Co-Products in version 2.10 2.11 Click Save Define Co-Products in version 2.12 Click New Define Co-Products in versior 2.13 In the list, mark the selected row. Define Co-Products in version 2.14 In the Item number field, enter ... Define Co-Products in version 5/2018 09:17:48 am 2.15 In the Quantity field, enter a nu... Define Co-Products in version 2.16 oduct cost allocatio Dafina Co. Broducts in varsion

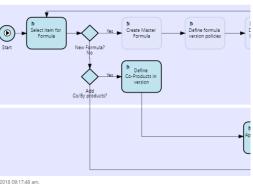


Figure: Scenario-Procedure activity based modeling with recorded steps linked to flow activities

In the example shown above, for the scenario attached to the business process node, Define Co/By Products Scenario, exporting the task guides will create at the lowest level, two folders one each for Production Manager and Process Engineer with the respective task guides.

These can be uploaded in SCS using the SCS (Upload RV Scenario) Button in Scenarios tabbed list in the Security Management Workspace

Security ma	nagement		
Summary		Security	
<sub>.</sub>	<b>343</b>	Requests	+ New 🖉 Edit 🗵 Match roles … More Merge scenarios Upload RV scenario
Users	Roles	Scenarios	✓         Scenario ↑         Owner         Objects         Created date and time           123         nsadaiya         68         7/1/2020 05:01:19 AM

This makes it easier to create right "Security Role" using Match roles feature in SCS based on role definitions in RapidValue.

#### Enhanced Segregation of Duties 3.21

In standard D365FSC, we can only define SoD rules at duty level which is rarely useful. In SCS, with this release user can now define SoD rulesets at any level (Duty, Privilege or Entry Point) in the security hierarchy in D365FSC. This makes this feature more practical and extremely useful for customers seeking better regulatory compliance like ISO 27001 section 6.1.2, SOX Control 404 and in general much improved security design better equipped to prevent frauds.

	✓ Name ↑	Type	First	First securi	able object type	First access level	Second
nhanced SoD ules	Demo rule for Entry point	s Entry point	AccountingDist	tVendEditInvHdr Menu iten	n display	Create	AdvancedLedgerEntryDateDr
	Match role test - ep 1	Entry point	AuditPolicyCase	eGroup Menu iten	n display	Full control	ACOJournalPost_BR
hanced SoD	Match roles test - duty	Duty	Maintain Absor	rption Costs		No access	Maintain audit policies
nflicts	Match roles test - duty 2	Duty	Maintain audit	policies		No access	Maintain Absorption Costs
narts	Match roles test - ep 2	Entry point	ACOJournalPos	it_BR Menu iten	n action	Full control	AuditPolicyCaseGroup
iui ta	Match roles test - ep 3	Entry point	DSMSecurityRe	questPriorityH Menu iten	n action	Correction	ACOJournalPost_BR
	Match roles test - ep 4	Entry point	DSMMultiSelec	tRoleSetup Menu iten	n display	Full control	DSMSecurityRequestPriorityH
	Match roles test - priv 1	Privilege	Maintain case <u>c</u>	grouping criteria		No access	Maintain Absorption Costs
	Match roles test - priv 2	Privilege	Maintain Absor	rption Costs		No access	Maintain case grouping criter
	Risk						
	✓ Risk ID	Category	Status	Inherit risk	Response	Residual risk	Owner
	Risk-00000006	Operational	Initial	Medium	Accept	Low	Admin
	Risk-00000007	Strategic	Initial	Very low	lanore	Very low	Admin

### 3.22 Organization risk Register

All Organizational risks can be now mapped in SCS "Integrated risk Management workspace". They may be financial risks related to SoD violations or can be related to any other organizational strategy or operational aspect. This feature will evolve in coming quarters in a full-fledged "Risk Management" capabilities within SCS enabling Organizations to register, assess, monitor, mitigate and close it. Integrated risk management

Summary	Risk					
		+ New ∥Edit				
	Risk register		ategory Status Ir	nherit risk Response	Residual risk Owner	
Create a risk Risk	Enhanced SoD			ligh Ignore	Very low Admin	
Create a risk Risk	rules			Vedium Accept	Low Admin	
ു 124 🚫 0	Enhanced SoD conflicts	Risk-000000007 Risk related to Org Strategy and St	itrategic Initial V	/ery low Ignore	Very low Admin	
	connicts	Risk-00000008 Risk DEMO O	Operational Review N	Medium Mitigate	Low Admin	
Enhanced SoD Enhanced So rules conflicts	OD Charts					
		Enhanced SoD rules				
		✓ Name Type First	First sec	urable object type First a	ccess level Second	Second securable
			in sales order	No ao		
		SCS-094-Create purchase order and r Duty Maintai	in inventory registrati	No ac	ccess Maintain purchase order	s
Risk						
Risk register	Organization Risk	/				
Enhanced SoD						
rules						
Enhanced SoD						
conflicts						
Charts						
		Initial Accepted Review Monito	or Expire			
		inda Accepted Review Montu	or <u>copre</u>			

## 3.23 AAD related SoD Validations across SCS

SCS now ensures that SoD violation checks also consider Security roles acquired by a user from being associated within an AAD. This is applicable all across SCS features. This helps in better handling of internal controls.

## 3.24 Security Explorer displaying Tables, Service operations and Data Entities entry point's type

Security explorer has been enhanced to now include also the following entry point's type: Tables, Service Operations and Data Entities. The complete list of entry point types are listed below:

- Menu item display
- Menu item action'
- Menu item output
- Table
- Data entity
- Service operation

ENTRY POINTS	
H⊐ Pin entry point a	and permissions
Туре	Access right
Table	No access
Service operation	No access
Service operation	Full control
Menu item display	View
Table	View
Menu item display	Full control
DataEntity	View
DataEntity	Full control

#### 3.25 Performance Optimization

Performance improvement across the application have been implemented in this release to improve user experience. Following programs have been positively impacted by the changes:

- Create snapshot,
- Security Explorer pinning,
- Match roles and
- Marking a record as sensitive.

Changes have been made in both indexes and the logic to improve the customer experience when working on these forms.

### 3.26 A new "Share" workspace

A new workspace "Security and compliance file share" is added to manage task recording and images. You can upload new task recordings and add them to scenarios (refer Add files to scenario). All the task recordings added to different scenarios will be listed in this workspace, you can also delete the task recordings which are no longer used in any scenario. Images can also be uploaded and added to the security request.

For viewing "Security and compliance file share ", go to Security management workspace and click on Share

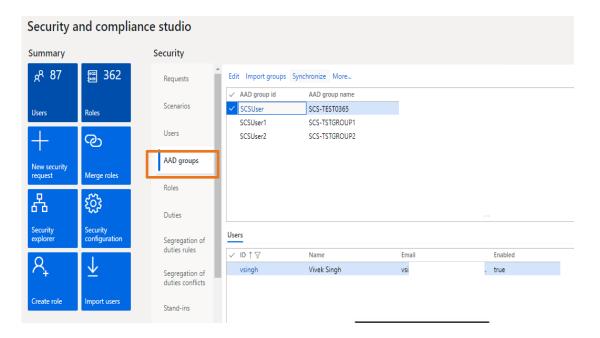
ecurity i	management						
ummary		Security					
<sub>я</sub> я 109	<b>:</b> 190	Requests	+ New 🖉 Edit \cdots See more				
			✓ Request	Туре	Priority	Status	Owner
Users	Roles	Scenarios	Provide access to customer and Project activity form	General	Normal	Approved	JOHN
55015	THE S		Purchase order form access	Modify user	Normal	Open	Admin
	୍ଷ	Users	Create role for vendor access	General	Normal	Completed	Admin
	-0		Add accountant role	Assign role to user	High	Completed	Admin
lew security		Groups	Credit note on purchase order	General	Normal	Open	Admin
equest	Merge roles		Customer	General	Normal	Approved	Admin
	~	Roles	Provide customer access	General	High	Open	abahlman
8	र्द्धेः		Create Customer Permission required for Eric	Create role	Normal	Open	vsingh
		Duties	something	Add stand-in	High	Waiting	andre.adcalavon
ecurity xplorer	Security configuration		SCS	General	Normal	Open	abahlman
хрютет	configuration	Segregation of duties rules	Customer access	General	Normal	Approved	nsadaiya
Ą			Customer_full_access	General	Normal	Approved	nsadaiya
$\rightarrow$	$\underline{\mathbf{v}}$	Segregation of					

More details are mentioned in the "User and training manual".

## 3.27 AAD groups' information in D365FO

In standard D365FO, we cannot check what all the users added to AAD groups and we have to login to azure portal. Now in SCS, we can check what all the users added to AAD groups in D365FO itself along with all related audit tracking for AAD groups in SCS itself.

If a role is assigned to a group then all the users added in the group also get access to that role, SCS captures this important information in various SCS forms and in audit log.



		+↓ Import 路 Explore	··· More			
	✓ User ID ↑ Nam	ne Email	License ty	pe	Company	Person
Scenarios	TRICIA	TRICIA	TRIC		Operations	USS
	VINCE	VINCE	VIN		. Operations	USN
Users	✓ vsingh	Vivek Singh	vsin		Operations	USN
	Wayne	Wayne	Way		Operations	USM
AAD groups	voichiroo	VOICHIROO	voic		Onerations	1155
Roles	Roles History	Login date and time	AAD groups			
Duties	✓ AAD group id SCSUser	AAD group na				
		SCS-TEST036				

#### 3.28 Verify SoD rules in Stand in

You can now use "Validate Sod rules " functionality while defining new stand-ins in SCS to know in advance, if there will be any SoD violation when security roles of user will be assigned to stand in user. This is important from compliance perspective to be aware of any SoD violation proactively.

	+New [	🗓 Delete 🛛 🖒	Assign stand-in ro	oles Validate S	oD rules	Options 🔎	
	Stand-in						
	₽ Filter						
	🗸 User ID	1	Stand-in	From	date	To date	Copy assigned organizations
	ALICIA		APRIL	12/1	3/2018	12/13/2018	0 🗸
	APRIL		dtijssen	1/19	/2019	1/20/2019	$\checkmark$
	atayya	la	acardol	10/2	1/2019	10/31/2019	$\checkmark$
	BENJA	MIN	CHARLIE	10/3	/2019	10/11/2019	
	CHARL	IE.	BENJAMIN	10/3	/2019	10/17/2019	
	dtijsse	n	Admin	1/21	/2019	1/22/2019	$\checkmark$
	JACOB		JEREMYL	10/2	2/2019	10/31/2019	
	JACOB		nsadaiya	10/2	2/2019	10/24/2019	$\checkmark$
	nsadai	ya	ALICIA	3/14	/2019	3/30/2019	$\checkmark$
	OSCAR	ł	JULIA	10/2	2/2019	10/31/2019	$\checkmark$
ssignmen			Validate SoD rules Optio		e 'Accounts receivable p	ayments clerk' contains duty 'Maintain customer p	ayments' and the role 'Accountant' contains duty 'Enable bank managemen
signmen	nt of OSCAR's roles to JULI				e 'Accounts receivable p	ayments clerk' contains duty 'Maintain customer p	syments' and the role "Accountant" contains duty "Inable bank managemen
ssignmen Star	nt of OSCAR's roles to JULI nd-in P Filter V User ID 1	A are in violation of SoD rules Stand-in	: 'SCS-083-Release production ord From date	er and move inventory': The rol To date	Copy assigned		syments' and the role "Accountant" contains duty "Inable bank managemen
signmen Star	nd-in Pilter User ID ALICIA	A are in violation of SoD rules Stand-in APRIL	: 'SCS-083-Release production ord From date 12/13/2018	er and move inventory': The rol To date 12/13/2018	Copy assigned		syments' and the role "Accountant" contains duty "Trable bank managemen
signmen Star	nd-in P Filter V User ID T ALICIA APRIL	A are in violation of SoD rules Stand-in APRIL dtijssen	SCS-083-Release production ord From date 12/13/2018 1/19/2019	er and move inventory': The rol To date 12/13/2018 1/20/2019	Copy assigned		syments' and the role "Accountant" contains duty "Inable bank managemen
signmen Star	nd-in Pilter User ID ALICIA	A are in violation of SoD rules Stand-in APRIL	: 'SCS-083-Release production ord From date 12/13/2018	er and move inventory': The rol To date 12/13/2018	Copy assigned		syments' and the role 'Accountant' contains duty 'Inable bank managemen
signmen Star	nd-in P Filter User ID T ALICIA APRIL atayyala	A are in violation of SoD rules Stand-in APRIL dtijssen acardol	* \$2\$-083-Release production and From date 12/13/2018 1/19/2019 10/21/2019	er and move inventory). The rol To date 12/13/2018 1/20/2019 10/31/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Enable bank managemen
signmen Star	nt of OSCAR's roles to JULIA nd-in 2 Filter 2 User ID T ALICIA APRIL atayyala BENJAMIN	A are in violation of SoD rules Stand-in APRIL dtijssen acardol CHARLIE	*\$C\$-083-Release production and From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019	er and move inventory'. The rol To date 12/13/2018 1/20/2019 10/31/2019 10/11/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Trable bank managemen
signmen Star	nd-in D <sup>2</sup> Filter 2 Filter AUCIA APRIL atayyala BENJAMIN CHARUE	A are in violation of 5oD rules Stand-in APRIL dtijsen acardol CHARLIE BENJAMIN	*SC5-083-Release production and From date 12/13/2018 1/19/2019 10/3/2019 10/3/2019	er and move inventory'. The rol To date 12/13/2018 1/20/2019 10/31/2019 10/11/2019 10/17/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Enable bank managemen
ssignmen Star	nd -in OF Filter V User ID 1 ALICIA APRIL ATV APRIL ATV ALICIA APRIL ALICIA APRIL CHARLIE dtjissen	Stand-in Stand-in APRIL dtijssen acardol CHARLIE BENJAMIN Admin	* SCI-083-Release production and From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019 10/3/2019 1/21/2019	er and move inventory). The rol To date 12/13/2018 1/20/2019 10/11/2019 10/11/2019 10/17/2019 1/22/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Enable bank managemen

# 3.29 Chart to give an overview of number of users and their last logging details

SCS now comes with a chart to categorize all users with their login details and time series analytics .This helps a lot in both compliance needs and optimizing license costs to deactivate or remove users based on an organization's security policy.

	Security							
ዶ 103  📰 175	Requests							
		✓ User ID ↑	Name	Email		License type	Company	Person
sers Roles	Scenarios	abahlman	Ard Bahlman	ab		Operations	DAT	
	L.	acardol	Adri Cardol	aci		Activity users	DAT	
- ©	Users	andre.adcalavon	André Arnaud de Calavon	an	.com	Operations	DAT	
	AAD groups	atayyala	Anil Kumar Tayyala (ATAYY.TI)	ata		Team members	dat	
lew security equest Merge roles	And groups	dvschie evhofwegen	David van Schie (DVSCH.TI) Eric van Hofwegen	dv	1	Operations Operations	dat DAT	
	Roles	nsadaiya	Nitish Sadaiya (NSADA.TI)	evi ns		Operations	usmf	
음 🐯		Pradeep.Bapna	Pradeep Kumar Bapna	Pra	om	Operations	DAT	
10 VXV	Duties	SCS-TSTGroup1	SCS-TSTGROUP1			Operations	DAT	
ecurity Security xplorer configuration		SCS-TSTGroup2	SCS-TSTGROUP2			Operations	DAT	
xplorer configuration	Segregation of duties rules	✓ vsingh	Vivek Singh (VSING.TI)	vsi		Operations	dat	
eate role Import users	duties conflicts Stand-ins Data security Snapshots History Charts	Roles History Log Last login date and time 11/6/2019 07:48:42 AM	AAD groups Days since last login onlin 0 0.00					
User's last log < 1 mo 1 to 3 mo	in							
> 3 mo Never Io								

#### 3.30 Asset classification User Interface

In standard D365FO there is no user interface in D365FO to know asset classification property set on different table fields. SCS now provides user interface, which shows all the fields with their asset classification. You have a chart to get the overview of different asset classification and how many field has the same asset classification. Asset classification is a table field property, classifying type of data it contains. Tagging a column helps easily marking data in scope for GDPR/GxP and many other such compliance regulations.

	cation		Asset classification
Tables			
PFilter			
Table name	Table label	Table ID	
Accountant_BR		6799	
AccountantLogisticsLoc	ation	1315	
AccountantLogisticsLoc	ationR	6664	
AccountingDistribTmp0	OrderLi	4548	
AccountingDistribution	EventT	6373	
AccountingDistribution	Tmp	97	
AccountingDistribution	TmpA	2882	
Asset classification info			Access Control Data Customer Content ECustomerContent
<ul> <li>Field name</li> </ul>	Field label	Asset classification	End User Identifiable Information End User Identifiable Information (EUII) End User Pseudonymous Identifiers Information (EUPI)
CNPJNum_BR		Customer Content	Extension ANil Object Metadata Organization Identifiable Information (Oll
CPFNum_BR		Customer Content	

#### 3.31 A List page with Workflow delegation details

This one is a UI improvements to make it easier for SCS administrators to manage and track "*Workflow Delegations*". Every user has to login by himself to delegate work flow to other user, in D365FO. Now using SCS, administrator can delegate workflow to any user for a particular time period.

Workflow delegation history list page is also there for tracking. You can reach here from the Security and Compliance Module > Inquiries > Workflow delegation and >Workflow delegation history

≡	🖉 Ed	dit +New 🛍 Delete Options 🔎						* <b>(</b> ]	♥ ♡ □ ×
ŵ	7	P Filter	Workflow delegation						
☆	-	40504	Notifications						
L)		\$0F81	Line item workflow notification t Individual	Send notifications in email	Send notifications to Action C Yes				
0:		Adri Cardol (ACARD.TI)							
		Admin	Delegation						^
		Anil Kumar Tayyala (TI)	+ Add  Remove Delegation  Active  Scope Name	/ Delegate	Start date/time $\uparrow \bigtriangledown$	End date/time 🏹	Enabled		
		BENJAMIN			We didn't find anything to show	here.			
		CHARLIE							
		Daiva Greiciune	Comment						
		Dirk Tijssen (DTIJS.TI)							
		Flavin Mikas							

#### 3.32 User groups – combined two tabs in one

This one is a UI improvements to make it easier for SCS administrators to manage a simplified standard user group's form. Users who are outside the organization hierarchy for budget planning must work with budget plans, you can assign budget plans to user groups. You can also set up restrictions for journal posting that are based on user groups. Users can be added to different groups using same tab. Also in SCS now a list of added users to different groups can be exported to excel using list tab.

Users can be added to different groups using same tab.

	+New 🗓 Delete 🛛 O	Options 🔎				
7	Users groups					
	Users groups	•				
	Setup List					
	✓ Group ↑ User gro	oup name				
	Approvers Project	journal approvers gro				
	<ul> <li>Originat Project j</li> </ul>	journal originator gro				
	OverBu Over bu	dget processing user				
	TestGro TestGro	up1				
	TestGro TestGro	up2				
	Name	Filter				
	REMAINING USERS	Filter		SELECTED USERS		
		60504				
	\$0F81	\$0F81		Admin	Admin	
	\$5E39	Anil Kumar Tayyala (A.		atayyala	Anil Kumar Tayyala (TI)	
	acardol	Adri Cardol (ACARD.TI	) (~	axrunner	axrunner	
	BENJAMIN	BENJAMIN				
	CHARLIE	CHARLIE				
	dgre	Daiva Greiciune				
	dtijssen	Dirk Tijssen (DTIJS.TI)				

You can reach here from the Security and Compliance Module > Inquiries > User groups

#### 3.33 New export/import role functionality

#### a) <u>Problem</u>:

For a couple of years, we have discovered and reported to Microsoft a standard bug that for AOT Privileges the node 'FormControlOverrides' is not readable from code and that is affecting, for example, the current SCS Export / Import functionality.

#### b) Issue that is generated by the bug explained:

When exporting a role using SCS Export function the XML file generated does not contain the entries under the 'FormControlOverrides' from AOT Privileges.

After the SCS Import function runs, the content from the XML file is applied to the target environment. Since the 'FormControlOverrides' node is empty in the XML file, the algorithm interprets it as a change (entries removed from node by user) therefor it will override the privilege in target environment and the entries will be removed.

#### <u>c)</u> <u>Solution:</u>

Since the only framework that was exporting the 'FormControlOverrides' is the standard 'Export' from Security Configuration form (which exports only the customizations and all of them) we decided to use that and make it more practical for the end user, where now, with the new functionality you can export the customizations for a selection of roles.

The 'Export role configuration' / 'Import role configuration' can be found on *Security and Compliance - Security management workspace -> Roles tab* 

8 135 🔚 242	<del> </del>   ල		ß	ស៊្វ	0					
	T (6)	, ц	50	2025	$\frown$	$\underline{+}$				
ers Roles	New security request Merge		ecurity explorer	Security configuration	Create role	Import users				
rity										
quests	Merge roles Duplicate	role Lock role	es க் Explore	Export Import [	Define active/inacti	ve role Export	role configuration Impo	ort role cor	figuration	
	Merge roles Duplicate	role Lock role	es 💑 Explore	Export Import [ f License type	Define active/inacti		role configuration Impo	Locked	figuration Inactive	Has configuration
cenarios			es க் Explore			loud) Ro				Has configuration
sers	O Role name	curity role	es	1 License type	License type (cl	loud) Ro				Has configuration
sers roups	Role name Business events see	curity role ewer	es के Explore	License type     Operations	License type (cl	loud) Ro				Has configuration
equests cenarios sers roups o <b>les</b>	O Role name Business events see Business events vie	curity role ewer	es 💑 Explore	License type     Operations     None	License type (cl	loud) Ro ces Ro	le description			Has configuration
sers roups	Role name Business events see Business events vie BusinessConnector	curity role ewer r Role	es 💑 Explore	License type     Operations     None     None	License type (cl	loud) Ro ces R D	e description	Locked		

A new column has been introduced to show all the roles that due have customizations and can be exported. The 'Export role configuration' button will be enabled when a record marked as 'Has configuration' is selected.

NOTE: This is working the same as standard security configuration export, except the fact that you can export them per roles.

#### 3.34 License count changes

New options have been added in the *Security and Compliance Studio -> Setup -> Parameters* form, under License count tab.

For all cloud licenses (Finance, Commerce, HR, Project operations, SCM) a new input option has been added called '- attached license' (E.g. Finance – attach license) where the user can add the number of attached licenses that have been bought, not only the base number.

eneral	General setup for the purchased lice	nses		
icense count	Open admin.microsoft.com	Open admin.microsoft.com		
ata migration	LICENSE PARAMETERS INPUT			
nhanced SoD rules	○ C License	Î	No of licenses	
nhanced SoD rules	<ul> <li>Activity users</li> </ul>		150	
lumber sequences	Commerce		12	
	Commerce - attached license		3	
	Finance		10	
	Finance - attached license		5	
	Human resouces		10	
	Human resouces - attached license		5	
	Operations		0	
	Project operations		60	
	Project operations - attached license	1	30	
	SCM		18	
	SCM - attached license		9	
	Team members		76	

These changes will reflect in the 'License optimization' workspace on the 'Usage' tab.

#### License optimization

∽ Summary						
△ License						
Usage All users Full users	Based on your actual subscription, The licensed users and remaining li	The actual count is a total of required base and attach licenses. In case one of base the licenses is required, the count is listed in 'Any base license'. Based on your actual subscription, you can use this information to verify your compliance. The licensed users and remaining licenses might be incorrect in case there are users requiring more than one license. The Dynamics 365 user interface is not aware of assigned licenses in Entra ID.				
Activity users	C License type	√↑ Actual users count	Base license users count	Attach license users count	Remaining users count	:
Team members	<ul> <li>Activity users</li> </ul>	3	150	0	147	
Scenarios	Any base license	10	0	0	-10	
Sections	Commerce	30	12	3	-15	
	Finance	35	10	5	-20	
	Human resouces	4	10	5	11	
	Project operations	18	60	30	72	
	SCM	47	18	9	-20	
	Team members	30	76	0	46	

The new license calculation formula will now: (Base license + Attached license) – Actual user count.

In order to separate the 'cloud license' from 'On premise' licenses we added the "View on premise" / "View cloud license" button that can toggle this view.

Full users	The Dynamics 365 user interface i	is not aware of assigned licenses in Entr	a ID.	Cloud licen	se view	
	View on premise licenses					
Activity users	<ul> <li>License type</li> </ul>	√↑ Actual users count	Base license users count	Attach license users count	Remaining users count	
Team members	<ul> <li>Activity users</li> </ul>	3	150	0	147	
Scenarios	Any base license	10	0	0	-10	
	Commerce	30	12	3	-15	
	Finance	35	10	5	-20	
	Human resouces	4	10	5	11	
	Project operations	18	60	30	72	
	SCM	47	18	9	-20	
	Team members	30	76	0	46	
		ired base and attach licenses. In case on you can use this information to verify		the count is listed in 'Any base license'.		
All users	The licensed users and remaining	licenses might be incorrect in case ther is not aware of assigned licenses in Entr		ne license.		
All users	The licensed users and remaining The Dynamics 365 user interface i			Attach license users count	Remaining users count	
All users full users Activity users	The licensed users and remaining The Dynamics 365 user interface in View cloud licenses	is not aware of assigned licenses in Entr	a ID.		Remaining users count	
Usage All users Full users Activity users Team members Scenarios	The licensed users and remaining The Dynamics 365 user interface i View cloud licenses	is not aware of assigned licenses in Entr	a ID. Base license users count	Attach license users count		

## 4. Bug fixes

### 4.1 Security and compliance studio 10.0.39.43

ID	Description	Observation
183994	CS00232323   German labels in modul SCS are missing or incorrectly translated	German label was not correctly translated. Fixed now.
179439	CS00227272   Publishing unpublished objects can take hours.	Performance improved.
185793	Duty pinning is fetching incorrect roles	Pinning down a duty was also bringing roles that were added directly to the privileges of the selected duty. Fixed: pinning down a duty will show only roles where the duty is assigned.
185794	License suggestion not showing on all levels	Incorrect license suggestion on role level when Project Operation license was present. Fixed.
183138	Menu item actions not available on entry point table - Security explorer	Menu items action not showing any more on Security Explorer. Fixed.

### 4.2 Security and compliance studio 10.0.37.42

function in Security and Compliance Studio modifies std. objects.node populated are having an issue Export/Import functionality due to a standard bug. All entries from this r cannot get pass into the XML file, th at the import step the node will get overridden and all entries are remo the object from the XML file). <b>175967</b> CS00227144   Deviation in standard role after import of custom role.overridden and all entries are remo the object from the XML file). <b>&amp;</b> As a fix we introduced a new function called : "Export role customizations". For more deta please see WHAT'S NEW SECTION. <b>176711</b> CS00227886   Manage access on roles to multiple organisations is not working in 'NL'Using a different language than EN- making 'System administrator' role for organization assignation, which correct since it is an all-organization <b>180975</b> CS00227833   'Any base license' rolesIncorrect license count.	ID	Description	Observation
role after import of custom role. the object from the XML file). As a fix we introduced a new function called : "Export role customizations". For more deta please see WHAT'S NEW SECTION. CS00227886   Manage access on roles to multiple organisations is not working in 'NL' 180975 CS00227833   'Any base license' roles CS00227833   'Any base license' roles		function in Security and Compliance Studio modifies std. objects.	AOT privileges with 'FormControlOverrides' node populated are having an issue on SCS Export/Import functionality due to a MS standard bug. All entries from this node cannot get pass into the XML file, therefore at the import step the node will get
176711called : "Export role customizations role customizations". For more deta please see WHAT'S NEW SECTION.CS00227886   Manage access on roles to multiple organisations is not working in 'NL'Using a different language than EN- making 'System administrator' role for organization assignation, which correct since it is an all-organization180975CS00227833   'Any base license' rolesIncorrect license count.		·	- · ·
Please see WHAT'S NEW SECTION.         CS00227886   Manage access on roles to multiple organisations is not working in 'NL'       Using a different language than EN- making 'System administrator' role for organization assignation, which correct since it is an all-organization         180975       CS00227833   'Any base license' roles			called : "Export role customizations / Import
roles to multiple organisations is not working in 'NL' for organization assignation, which correct since it is an all-organization CS00227833   'Any base license' roles Incorrect license count.	176711		
	180975	roles to multiple organisations is not	Using a different language than EN-US was making 'System administrator' role available for organization assignation, which is not correct since it is an all-organizations role.
<b>180707</b> 'SCM' licensesparameters license count system.	&	are counted in both 'Finance' and 'SCM' licenses	New options have been added to the SCS parameters license count system. For more details please see WHAT'S NEW

	CS00227738   wrong count of used licenses for role	
176445	Internal   Description of the Security request should not be editable after it had been submitted to the workflow	Some form sections from 'Security requests' were still editable after it was submitted. Fixed now.
179815	Internal   Align licensing details with MSFT changes (Read overrides to Team members)	Align with new change from MS where if a securable object (role, duty or privilege) it's view only than the license should be 'Team members', always.

### 4.3 Security and compliance studio 10.0.36.41

ID Description	Observation
CS00227639   Cannot import roles. Error: "Cannot create a record in Roles (DSMRolesTable)."	This is most likely an issue where the role was initially deleted and imported again. A Dynamic Snapshot feature is generating the error, probably due to incorrect data. To fix the issue at short notice, we added a parameter in the Security and Compliance Studio where the Dynamic snapshot feature can be switched on and off. In case the feature is disabled, the snapshot versions should be created regularly to have all information in Security and Compliance Studio up to date. E.g. the Security Explorer is dependent on actual snapshot information.

### 4.4 Security and compliance studio 10.0.36.40

ID	Description	Observation
169675	Internal   Security request should not be editable after it had been submitted to the workflow	After submission the security request remains available for editing. Fixed.
171641	Internal   Error publishing selection - security configuration	Publishing objects in security configuration was throwing an error. Roles created via 'Merge role wizard' can encounter a problem if there are entities involved. In some special cases entities were added under the 'tables' node, which is not correct and the roles become corrupted.
172461	CS00226211   Task recorder saving to security failing - DSM 10.0.32.38	Recording and saving a scenario using D365FO in different language than English was generating an error. Now it's fixed.
173892	CS00226365   Dead lock error while publishing role changes	Dead lock error while publishing huge amount on objects in security configuration.

rvation

### 4.5 Security and compliance studio 10.0.34.39

Obser	Description
Ot	Description

169679	CS00225097   Unwanted records created in log	Running a full comparison of two snapshots was generating some false audit log for standard privileges. This has been identified and fixed.
169725	CS00225236   Match role functionality is not showing any role, duty, or privilege	Creating a scenario based on a task recording file that was recorded in a different user language than English was causing the matching to fail.
170823	CS00225405   privilege not shown when matching roles via a scenario	Duties or privileges that were not linked to any role were not shown up in Match Roles functionality. Now these objects will be visible.
171005	Internal   Data entity support for user and user role details for security requests.	New data entities added for 'Security requests'.

#### 4.6 Security and compliance studio 10.0.32.38

ID	Description	Observation
160423	CS00223035   Meaning of any unique license	In specific scenarios the license suggestion from Security Explorer was not correct. Calculating licenses has been improved. <sup>1</sup>
163925	CS00223817   AD user status sync	Microsoft users like 'PowerPlatformApp' which are used specifically by the system to operate different frameworks were disabled. Issue has been fixed.
144592	Internal   Error when downloading file	Some files were throwing a 'Record for ID – {xxx.xxx.xx.xx.xx} not found'. Error was due to connection to temp blob. Issue has been fixed.
161013	Internal   License calculation not working correctly - 'Activity' license shouldn't be included	Some activity users were displaying incorrect license. Issue fixed. <sup>1</sup>
162939	Internal   Implement new form pattern for vertically scrolling workspaces	Applying new form patterns to the workspaces. They are now displayed vertical
164224	Internal   Review licenses on the menu items	Security and Compliance Studio's menu items have been reviewed and the user licenses have been updated accordingly
165288	Internal   Merge role wizard -> entity permissions set wrong on merged role	Permissions at entity level were not set correctly when roles were created/modified using 'Merge role' wizard. Issue has been fixed.

<sup>1</sup> Based on support feedback from our customers, we improved the licensing suggestions. Both to get more accurate information, but also we improved the suggestion text. To get the new code working, a new security snapshot should be created first, before running the License updates. Due to ongoing updates and possible bugs from Microsoft, there might be some suggestions wrongly interpreted. In case you find any inconsistent suggestions, please contact To-Increase support, so we can review, improve and contact Microsoft to get better suggestions in future releases.

## 4.7 Security and compliance studio 10.0.31.37

158243deleted; only headers remained. This issue has been fixed.Internal   A user without system administrator rights can create users and grant the system admin roleThere were two places where a security administrator or other custom roles could assign the security role to a user; including himself. When importing users and during the copty security setup, we restricted now the option to copy the system administrato role in case a user is not assigned to the system administrator role.160517CS00222903   Can't create a snapshotWhen the snapshot creation got interrupted by e.g. an environment restart or shutdown some orphaned records could cause an error: "Cannot create a record in Privilege – duty link (DSMSecurityPrivDutyAssociationHistory). The record already exists." When starting the snapshot creation, the	ID	Description	Observation
administrator rights can create users and grant the system admin role administrator or other custom roles could assign the security role to a user; including himself. When importing users and during the copy security setup, we restricted now the option to copy the system administrato role in case a user is not assigned to the system administrator role. CS00222903   Can't create a snapshot CS00222903   Can't create a snapshot CS0022903   Can't create a snapshot CS002904   Can't create a s	158243		was not respecting the setting for number of snapshots to keep. Snapshot details were deleted; only headers remained. This issue
by e.g. an environment restart or shutdown some orphaned records could cause an error: "Cannot create a record in Privilege – duty link (DSMSecurityPrivDutyAssociationHistory). The record already exists." When starting the snapshot creation, the	160517	administrator rights can create users and	administrator or other custom roles could assign the security role to a user; including himself. When importing users and during the copy security setup, we restricted now the option to copy the system administrator role in case a user is not assigned to the
records will be cleaned up to prevent the duplicate record error.	159501	CS00222903   Can't create a snapshot	error: "Cannot create a record in Privilege – duty link (DSMSecurityPrivDutyAssociationHistory). The record already exists." When starting the snapshot creation, the records will be cleaned up to prevent the

## 4.8 Security and compliance studio 10.0.29.36

ID	Description	Observation	
with AD group members batch runs into information when ar		Enchanced error handle to provide more information when an user fails to be imported from azure groups.	
151835	Internal   Data source fields not Changes over the data source fields ar		

#### 4.9 Security and compliance studio 10.0.28.34

ID	Description	Observation
145372	CS00221370   Incorrect user security log in SCS	Now shows the correct log items
146730	CS00221689   Issue with Licensing framework	If snapshot is in queue and due to start in the upcoming 30 mins, the refresh license job cannot be set to start.
147973	CS00221859   The "Copy security setup" functionality on users also copies disabled roles	Disabled users are not copied anymore.
144053	CS00212605   New license type	Changes made to license display and calculation. The security explorer now shows recommendations for the base and attach licenses.

#### 4.10 Security and compliance studio 10.0.27.33

ID	Description
	CS00221640   SCS user log does not record user role changes when using "Copy security
146434	setup". This has been fixed now.

#### 4.11 Security and compliance studio 10.0.26.32

ID	Description
143052	CS00214823   Security and Compliance Studio 10.0.22.27 (isv)
144943	CS00220293   Add multiple selections to the enhanced SOD
145090	CS00220439   Changing operations license type on read only objects for SCS tool

#### 4.12 Security and compliance studio 10.0.26.31

ID	Description
	CS00218247   No security change logging when importing security roles while running in
144620	background

### 4.13 Security and compliance studio 10.0.25.30

10	C	Description	
1	24413	CS00164201	SCS - Role Export / Import Generating New AOT Name

#### 4.14 Security and compliance studio 10.0.24.29

ID	Description	
140218	CS00208843   Rename of Group in Azure is not complete in D365	
	CS00208677   Table securable objects shown as a menu item display in the securable	
140147	objects grid when the matching role functionality is used.	

#### 4.15 Security and compliance studio 10.0.22.27

ID	Description
124414	CS00162740   SCS - Unable To Add Alert (Workflow Delegation History)

#### 4.16 Security and compliance studio 10.0.18.1

ID	Description
	No external bug has been reported in the last release!We dont list down the internal bugs fixed in the release notes.

#### 4.17 Security and compliance studio 10.0.12.5

ID	Description
124417	CS00162914   Security request on the user does not open the specific security request.

#### 4.18 Security and compliance studio 10.0.12.4

ID	Description
	CS00164486 - User security log does not work when a data management import has been
124416	used

### 4.19 Security and compliance studio 10.0.12.3

ID	Description
	No external bug has been reported in the last release ! We dont list down the internal bugs fixed in the release notes.

#### 4.20 Security and compliance studio 10.0.12.2

ID	Description
121625	CS00155216 - Amended Master Roles Not Removing Privileges During Export / Import Into New Sys

#### 4.21 Security and compliance studio 10.0.12.1

	ID	Description
	119466	CS00150048-New User Import - Assign Organisations Based on Existing User Not Working
Γ	119596	CS00150823-Apply Active Directory Status - Using AAD Email Address Not UPN/Alias

## 4.22 Security and compliance studio 10.0.10.1

ID	Description
	CS00144263-Enhanced SoD not showing display menu items when setting up, only
115373	action/output

## 4.23 Security and compliance studio 10.0.6.11

ID	Description
109266	CS00130218-Alert rule on SCS audit log table email contains no further information
113069	CS00140037-SCS Parameter - Warning Dialogue Spelling Mistake

#### 4.24 Security and compliance studio 10.0.6.10

ID	Description
108559	CS00128698-DSM Tables growing rapidly (V10.0.6.6)
108471	CS00128399-Export and import of security scenarios fails
108836	CS00129465-TI SCS Parameters Data Entity Missing Fields

#### 4.25 Security and compliance studio 10.0.6.9

ID	Description
103912	CS00121877-Blank securable objects on certain task recordings
104104	CS00121887-When importing security scenarios, in some cases file relations is lost

#### 4.26 Security and compliance studio 10.0.6.8

ID	Description
99355	CS00107517-SCS Role Export - Not Including "Form Controls"

#### 4.27 Security and compliance studio 10.0.6.7

ID	Description
87380	CS00080500: Sensitive Access Users Not Showing on Form
100873	CS00111593-Security Snapshot Will Not Run In Batch Mode
100974	CS00111816-"Corrupted Data Batch Fix" Doesn't Remove SCS Parameters
100323	CS00111058-Create the batch job for role import and export
101229	CS00112112-SCS Periodic AAD Sync Disabled Admin Account
	CS00114631- cannot create snapshots. It throws an error "Cannot create a record in License
101712	roles for user (DSMSecurityRoleUserAssociationHistory). The record already exists.
101897	CS00114717-SCS Role Export Not Including Sub Roles
101957	CS00115222-"Migrate scenario data" batch job throws error
100837	CS00109162-Asset Classification - Re-Running "Rebuild asset classification" periodic job
100836	CS00111408-Sensitive Data Access Configuration Lost During Application Update

#### 4.28 Security and compliance studio 10.0.6.6

ID	Description
100323	CS00111058-Unable To Import Security Roles

## 4.29 Security and compliance studio 10.0.6.5

ID	Description
84033	CS00106681-SCS parameters page should be independent of the company
98372	CS00104154-Entity "task recording step" is marked as obsolete
99360	CS00107418-Import Roles - Name is already in use
99496	CS00106272-Security administrator are able to add System administrator to own user

#### 4.30 Security and compliance studio 10.0.6.4

ID	Description
97753	CS00102923: DSMAOTMenuItemsTable.AOTName Limited to 60 characters
98176	CS00103892-New indexes introduced in SCS 10.6.3 is causing environments to not update
97110	CS00101145: FW: Issue in SCS for customer DFDS Group on renaming scenarios

#### 4.31 Security and compliance studio 10.0.6.3

ID	Description
95300	CS00097146: Entities are being added as table permissions rather than entities on Merge role
95306	CS00097144: Form controls being created with the incorrect table name

95373 CS00090408: Sensitive Data Access Hex Colour Using Incorrect Parameter

#### 4.32 Security and compliance studio 10.0.6.2

ID	Description
91326	CS00089115: Remove excess entry points only gives grant to Delete and not Read Update Create
48279	CS00089476: SCS - Data Management Template

#### 4.33 Security and compliance studio 10.0.6.1

ID	Description
	Purchased license count setup: License information is now stored at admin.Microsoft.com.
	SCS now provides an option to administrator to setup the purchased license value in SCS.
81072	Purchased license value is used in license optimization workspace.
86619	CS00080538 – Security Explorer- No colored icon for "Tem Member" license type.
86627	CS00079152 – Apply Active Directory User Status – Authentication Method

#### 4.34 Security and compliance studio 10.0.3.3

ID	Description
83602	<ul> <li>Standard Import user menu item is not visible if SCS license expired.</li> </ul>

#### 4.35 Security and compliance studio 10.0.3.2

ID	Description
77956	CS00069693 – License Count Data Source.

### 4.36 Security and compliance studio 10.0.3.1

ID	Description
77954	CS00070995 – Pin privilege is not working properly.
77957	CS00069700 – SCS-Table recording issue.

#### 4.37 Security and compliance studio 10.0.1.3

ID	Description
	No external bug has been reported in the last release ! We dont list down the internal bugs
	fixed in the release notes.

#### 4.38 Security and compliance studio 10.0.1.2

ID [	Description
	No external bug has been reported in the last release ! We dont list down the internal bugs fixed in the release notes.

#### 4.39 Security and compliance studio 10.0.1.1

ID	Description
	No external bug has been reported in the last release ! We dont list down the internal bugs fixed in the release notes.

#### 4.40 Security and compliance studio 81.3.2.1

ID	Description
68669	TI-12573-X5J6 - Merger role functionality is assigning the higher level of access if read.
70101	TI-12768-F2K5 - Cannot import security object having name more than 30 characters.
71286	TI-12922-K0V1 - Security setup to GOLD at EQIN.

#### 4.41 Security and compliance studio 81.3.1.1

ID	Description
68926	TI-12597-S1R0 Merger role functionality is assigning the higher level of access if read.

#### 4.42 Security and compliance studio 81.2.1.1

ID	Description
67975	TI-12427-X2X7 Issue with security role export
68381	TI-12526-Q4F4 'Not part of current AOT configuration'

#### 4.43 Security and compliance studio 81.1.2.1

ID	Description
67640	TI-12373-Q2R9 Add securable objects outside privileges to a new privilege
66654	TI-12213-S8Q4 Add table permissions to role or privilege

#### 4.44 Security and compliance studio 81.1.1.1

ID	Description	
67640	TI-12373-Q2R9 Add securable objects outside privileges to a new privilege	
66654	TI-12213-S8Q4 Add table permissions to role or privilege	

#### 4.45 Security and compliance studio 81.20.3.1

ID	Description	
67267	TI-12287-S1G1 Matched control is not part of privilege	

4.46 Security and compliance studio 81.20.2.2 \*(This build was created as the earlier deployable package had some issues)

ID	Description	
66652	TI-12204-S3M9 Audit log duplicate records as coming from AOT	
66653	TI-12205-P0Y5 User audit log not working properly	
66654	TI-12213-S8Q4 Add table permissions to role or privilege	
66533	TI-12179-C0V4 Error on security role import.	
	Note: For Bug 66533 and BUG 66652 requires immediately after installation running of the "Clean Demo Data" batch program and thereafter creating a snapshot.	

#### 4.47 Security and compliance studio 81.20.2.1

ID	Description
66652	TI-12204-S3M9 Audit log duplicate records as coming from AOT

66653	TI-12205-P0Y5 User audit log not working properly	
66654	TI-12213-S8Q4 Add table permissions to role or privilege	
66533	TI-12179-C0V4 Error on security role import.	
	Note: For Bug 66533 and BUG 66652 requires immediately after installation running of the	
"Clean Demo Data" batch program and thereafter creating a snapshot.		

#### 4.48 Security and compliance studio 81.20.1.1

ID	Description
	No external bug has been reported in the last release ! We dont list down the internal bugs fixed in the release notes.
	ince in the release notes.

### 4.49 Security and compliance studio 1804.15.2.1

ID	Description	
61572	TI-11605-D4L0 Creating new role with exact access level not working	
62494	TI-11720-N4Y4 SCS Installation issue	
	Note: Bug 62494 requires the one time running of a job to update the data model changes. Instructions for the same are given in the known issues section.	

## 4.50 Security and compliance studio 1804.15.1.1

ID	Description
	No external bug has been reported in the last release ! We dont list down the internal bugs fixed in the release notes.

#### 4.51 Security and compliance studio 1712.12.1.1

	ID	Description
Γ		No external bug has been reported in the last release ! We dont list down the internal bugs
		fixed in the release notes.

## 5. Changed or deprecated features

### 5.1 Deprecated features 10.0.31.37

Feature	Notes
Create role from duties/privileges	The functionality was broken and is now replaced with the new Security role wizard which has more enhanced features; also for updating roles instead of only creating new security roles. See also the what's new section in this document.

### 5.2 Deprecated features older versions

Feature	Notes
License model	A single license enables the full functionality of Security and Compliance Studio, as opposed to separate security and audit licenses used in Dynamic Security Management on AX 2012.
Security Tree	The security and license type explorer tree has been replaced with a list based Security explorer form which provides list based insight into user, role, duty, privilege and entry point relationships.
Active Directory Users overview	The AD group related features has been deprecated in D365 for Finance and Operations because those are no longer relevant.
AD group membership information	The AD group related features has been deprecated in D365 for Finance and Operations because those are no longer relevant.

## 6. Known issues

- In case you are using Microsoft demo data; first "Clean DEMO data base" as the current DEMO database from Microsoft is coming with some corrupt security data. Few privileges and duties have been deleted from AOT, but still exist in the table. So now the table has the record and the privilege/duty does not exist in AOT and this causes errors. This job will clean up this corrupt data so that you don't get any error while working on Security and compliance studio. Path: Security and Compliance -> Periodic Tasks -> Clean DEMO database.
- 2. Bug 62494 requires the one time running of a batch program to update the data model changes. Instructions are as below:

For the users that are trying to update Security and Compliance Studio to the update 15 and encountered the following error, below are the steps needed in order to not lose any data from production environments:

"ALTER TABLE ALTER COLUMN ENTRYPOINTNAME failed because one or more objects access this column.

ALTER TABLE DSMSECURITYENTRYPOINTPRIVASSOCIATION ALTER COLUMN ENTRYPOINTNAME NVARCHAR(255) NOT NULL;

UPDATE SQLDICTIONARY SET STRSIZE = 255, RIGHTJUSTIFY = 0, FIELDTYPE = 0 WHERE NAME = 'EntryPointName' AND TABLEID = 19484"

#### Steps:

#### 1. Navigate to Security and Compliance Studio -> Security -> and open Parameters form.

On this form a new tab called "Migration" will be available (see figure 1)

\*NOTE: this option will be available only if you have data into the

"DSMSecurityEntryPointPrivAssociation" table (the table from the error above).

Dynamics 365	Finance and Operations
Save OPTIONS	۹
Security and	compliance studio parameters
General	Setup general information for Security and Compliance studio Prefix SCS Color for covered duties and pri Yes Color Hex # Color Hex # GDBFBF INITIALIZE SCS IT AUDIT Lock 'Initialize Security and com No SNAPSHOTS
	Limit number of snapshots

#### Fig. 1 New tab in SCS Parameters form

2. On this tab a new button is available and it's called "Migrate data". Click this button in order to move data (see figure 2)

Save OPTIONS 🔎	
Security and compliance studio parameters	
General	Migrate data to newest version
Migration	Migrate data

Fig. 2 "Migrate data" button on SCS Parameters form

3. The process of moving data will start and it will take few seconds / minutes, depending of the amount of data that you have.

After the process is finished a message to restart the D365 user interface will be displayed and the "Migration" tab will not be available anymore (see figure 3)

Bave OPTIONS ₽	
(1) Migration done. Please restart your D365 UI	
Security and compliance	studio parameters
General	Setup general information for Security and Compliance studio  Prefix SCS_ Color for covered duties and pri Yes  F  Color Hex #  Color Hex #  Color Hex #  Color Hex #  Color Color Color Color Hex #  Color

Fig. 3 "Migration" tab not available anymore after moving data