

Release Notes for Security and Compliance Studio 10.0.42.46

Release Notes

Author: Ankit Bhadana, Product Owner

Table of Contents

1.	Introdu	iction	7
1.1 1.2 1.3 1.4 1.5 1.6	Audien Produc Deliver Commo	e ce t release information ables on features ate renewal	7 7 8 9
2.	What's	New in Security and Compliance Studio 10.0.42.46	.12
2.1 2.2 2.3	period. Include	to raise security request to enable user and allocate roles for a specific ""No. of access" on View access entry points page ource record and Generate report feature for Sensitive data log	. 15
3.	Feature	es introduced in last few releases of Security and Compliance Studio	. 18
3.1	Versior	10.0.41.45	. 23
	3.1.1 3.1.2 3.1.3 3.1.4 3.1.5	Security user role data Ability to raise stand-in requests for other users Batch-job to clean audit logs Ability to activate and deactivate Sensitive data setup Ability to select dimension and financial tag field using Table security recording	. 24 . 25 . 27
3.2	Versior 3.2.1 3.2.2	10.0.40.44 Release Organization assignment for security request Continuous user action logging	. 28
3.3	Versior 3.3.1 3.3.2 3.3.3 3.3.4	10.0.39.43 Release User audit log for sensitive data Securable tree view Security request history track Enhanced SoD predefined list	. 31 . 34 . 37
3.4	Versior	10.0.37.42 and Older	. 40

3.4.1	Segregation of duties sets	40
3.4.2	Security requests enhancements and workflow	41
3.4.3	Export security explorer objects to excel in a de-normalized format	52
3.4.4	Merge security scenarios and match role	53
3.4.5	Mark any Security Role as Active/Inactive	53
3.4.6	Recording steps to scenario.	54
3.4.7	Override permission based on scenarios	54
3.4.8	Option to mark, track and audit security objects providing access to	
	sensitive data	55
3.4.9	Option to create a duty from Matched Privileges grid in Match roles form	
		63
3.4.10	Option to import and export data using Data Entities in Security and	
	Compliance Studio	63
3.4.11	Option to compare Security Snapshots stored in the security setup	64
3.4.12	Enhanced Audit log capability to capture all the changes from	
	development space (AOT) as well into Audit Log	68
3.4.13	Option to create one or more privileges and also one or more duties	
	while merging roles	69
3.4.14	Ability to create scenarios from D365 module menus	70
3.4.15	Snapshots based performance and scalability enhancements	71
3.4.16	Improved "Create role wizard" based on a grid framework	73
3.4.17	Accessing Security Explorer from all D365 FOE forms	73
3.4.18	Option to create duties and SOD compliance check as well while	
	merging roles	74
3.4.19	Importing New Users while Synchronizing the group users with the Active	
	Directory group members	75
3.4.20	Uptake RapidValue BPM Suite Scenarios directly as SCS Security	
	Scenarios	75
3.4.21	Enhanced Segregation of Duties	77
3.4.22	Organization risk Register	78
3.4.23	AAD related SoD Validations across SCS	79
3.4.24	Security Explorer displaying Tables, Service operations and Data Entities	
	entry point's type	79
3.4.25	Performance Optimization	79
3.4.26	A new "Share" workspace	79
3.4.27	AAD groups' information in D365FO	80
3.4.28	Verify SoD rules in Stand in	81
3.4.29	Chart to give an overview of the number of users and their last logging	
	details	81
3.4.30	Asset classification User Interface	82
3.4.31	A List page with Workflow delegation details	83
3.4.32	User groups – combined two tabs in one	83
3.4.33	New export/import role functionality	
3.4.34	License count changes	
	-	
Bug fix	es	

4.

4.1	Security and compliance studio 10.0.42.46	87
4.2	Security and compliance studio 10.0.41.45	87
4.3	Security and compliance studio 10.0.40.44	88
4.4	Security and compliance studio 10.0.39.43	88
4.5	Security and compliance studio 10.0.37.42	88
4.6	Security and compliance studio 10.0.36.41	89
4.7	Security and compliance studio 10.0.36.40	89
4.8	Security and compliance studio 10.0.34.39	90
4.9	Security and compliance studio 10.0.32.38	
4.10	Security and compliance studio 10.0.31.37	
4.11	Security and compliance studio 10.0.29.36	
4.12	Security and compliance studio 10.0.28.34	
4.13	Security and compliance studio 10.0.27.33	
4.14	Security and compliance studio 10.0.26.32	
4.15	Security and compliance studio 10.0.26.31	
4.16	Security and compliance studio 10.0.25.30	
4.17	Security and compliance studio 10.0.24.29	
4.18	Security and compliance studio 10.0.22.27	
4.19	Security and compliance studio 10.0.18.1	
4.20	Security and compliance studio 10.0.12.5	
4.21	Security and compliance studio 10.0.12.4	
4.22	Security and compliance studio 10.0.12.3	
4.23	Security and compliance studio 10.0.12.2	
4.24	Security and compliance studio 10.0.12.1	
4.25	Security and compliance studio 10.0.10.1	
4.26	Security and compliance studio 10.0.6.11	
4.27	Security and compliance studio 10.0.6.10	
4.28	Security and compliance studio 10.0.6.9	
4.29	Security and compliance studio 10.0.6.8	
4.20	Security and compliance studio 10.0.6.7	
4.30	Security and compliance studio 10.0.6.6	
4.31	Security and compliance studio 10.0.6.5	
4.32	Security and compliance studio 10.0.6.4	
4.34	Security and compliance studio 10.0.6.3	
4.35	Security and compliance studio 10.0.6.2	
4.35	Security and compliance studio 10.0.6.1	
4.30	Security and compliance studio 10.0.3.3	
4.37	Security and compliance studio 10.0.3.2	
4.38	Security and compliance studio 10.0.3.2	
4.39		
4.40 4.41	Security and compliance studio 10.0.1.3	
4.41 4.42	Security and compliance studio 10.0.1.2	
	Security and compliance studio 10.0.1.1	
4.43	Security and compliance studio 81.3.2.1	
4.44	Security and compliance studio 81.3.1.1	
4.45	Security and compliance studio 81.2.1.1	
4.46	Security and compliance studio 81.1.2.1	9/

4.47 4.48 4.49	Security and compliance studio 81.1.1.1 Security and compliance studio 81.20.3.1 Security and compliance studio 81.20.2.2 *(This build was created as the earlier	
	deployable package had some issues)	97
4.50	Security and compliance studio 81.20.2.1	97
4.51	Security and compliance studio 81.20.1.1	97
4.52	Security and compliance studio 1804.15.2.1	97
4.53	Security and compliance studio 1804.15.1.1	98
4.54	Security and compliance studio 1712.12.1.1	98
5.	Changed or deprecated features	99
5.1	Deprecated features 10.0.31.37	
5.2	Deprecated features older versions	99
6. Know	vn issues	100

Document Information

Title	Release Notes for Security and Compliance Studio 10.0.42.46
Subtitle (Subject)	Release Notes
Solution Suite	GRC; Security and Compliance Studio
Category	Release Notes
Author	Ankit Bhadana
Published Date	1/31/2025
Status	Final
Comments	Security and Compliance Studio Release Notes

© Copyright STAEDEAN B.V. 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 STAEDEAN B.V. STAEDEAN 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 **Release Notes for Security and Compliance Studio 10.0.42.46** release from Staedean. This release is compatible with the version of Microsoft Dynamics 365 for Finance and Operations, **10.0.39 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

Release Notes for Security and Compliance Studio 10.0.42.46 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 Staedean 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.

Release date	Staedean Version No.	Minimum required D365 version	Validated against D365 version	Compatible with D365 version
05/04/2024	10.0.39.43	10.0.36	10.0.39	10.0.36 and above
02/07/2024	10.0.40.44	10.0.36	10.0.40	10.0.36 and above
10/11/2024	10.0.41.45	10.0.36	10.0.41	10.0.36 and above
31/01/2025	10.0.42.46	10.0.39	10.0.42	10.0.39 and above

This is summarized in the following table.

In case of an Error, Staedean may provide a Hotfix on a reasonable efforts basis in a way it considers appropriate in its discretion. Staedean 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 - Staedean

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	Release Notes for Security and Compliance Studio 10.0.42.46 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</i> <i>Studio 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</i> <i>Security 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</i> <i>Studio documentation</i> BPM library. This library contains a comprehensive set of task guides that document how to use <i>Security and Compliance Studio</i> for your BPM activities. This documentation is provided in U.S. English only.
Authentication assets	A Staedean 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

Staedean 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.

P Filter	Installed only		Advanced Discrete Manufacturing	
Solution	↑ Installed version	Status	:	
Advanced Discrete Manufa	cturi	×	SOLUTION IS NOT INST	ALLED
Advanced Project Manager	nent	×	Solution description	
Anywhere Mobility Studio		×	Help manufacturers solve problems and streaml	ine process flows.
Business Integration Solution	on 10.0.99.999	\oslash		
Data Entry Workflow		×		piry date
Data Modeling Studio		×	Construction	
Data Quality Studio	10.0.18.2	\otimes	Equipment 🔒	
DynaRent	10.0.28.43	()	Advanced Project Management	
PLM Integration for Engine	erin	×	Product Engineering a	
RapidValue BPM Suite	10.0.26.37	\oslash		
Security and Compliance St	tudio	×		

On all Staedean 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 would love your feedback!
Please rate your experience in using the All solutions screen.
5 - Excellent
4
3
<u>2</u>
🔵 1 - Poor
Please tell us why you chose the rating. Additional insights would help us improve our products further.
Thank you for providing us feedback!
Your privacy is important to us. To protect your privacy, please don't include any personal information.

Below is the list of changes in common library in Jan-2025 release:

#	Issue	Description			
1 Deprecation fix		This will ensure that the STAEDEAN License team can generate and upload license files to Azure Blob Storage without any impact. Additionally, customers will be able to retrieve their license files from Azure Blob Storage seamlessly.			
2	Enumeration translation fix	This will ensure that customers do not encounter any issues while using the 'Populate Enumeration Translations' process.			
3	Solution management batch job issue	This will ensure that customers do not experience any issues while performing deployments or maintenance mode activities.			
4	To hide the 'Used' column in Solution management	This will ensure that no confusion is caused to customers due to the accuracy of the Used column data.			
5	In-App feedback - tenant fix	This will ensure that the In-App feedback does not automatically pop up for STAEDEAN users.			



1.6 Certificate renewal

The security certificate, that expires every 3 years, ensures that our customers have valid Staedean 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 Staedean 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 10.0.42.46

2.1 Ability to raise security request to enable user and allocate roles for a specific period

These enhancements focus on enabling or disabling users for specific periods and allocating or removing roles for specific periods. Following security request types has been enhanced to achieve this feature:

Create User:

• Two new fields, named "From Date" and "To Date" have been introduced to specify the period during which the user will be active.

Create users	\frown
User name User ID Email Company From date To date Image: Company Image: Company	
Add 🗎 Remove	
Role name Description Role AOT name From date To date	:
We didn't find anything to show here.	

- Additionally, two field named "From date" and "To date" will be added in the Roles grid as well. If admin need to specify a date for a specific period then admin can specify the period in the From date and To date field.
- Users will be created but only activated during the specified period. For example, if the period is from June 1, 2025, to June 10, 2025, the user will be active only during these dates.
- This enhancement allows pre-scheduled activations, ensuring users are only active when needed, enhancing security and resource management.

Disable User:

• Two new fields, named "From Date" and "To Date," have been introduced to specify the period during which the user will be disabled.

Disable users				^
Add 🛍 Remove				
User ID	↑ User name	From date	To date	
		We didn't find anything to	o show here.	

- Users will be disabled during the specified period without deleting their accounts or revoking permissions. They will be re-enabled after the period ends.
- This enhancement manages temporary suspensions or ensures users cannot access the system during specific periods, such as vacations or security breaches.

Enable User:

• Two new fields, named "From Date" and "To Date," have been introduced to specify the period during which the user will be enabled.

Enabl	e users				\frown
Add	🕅 Remove				
0	User ID	1 User name	From date	To date	:
			We didn't find anything to sho	w here.	

- Users will be enabled during the specified period, and will be disabled after the "To date".
- This enhancement controls the reactivation of user accounts, ensuring users can only access the system during approved periods.

Assign Role to User:

• Two new columns, named "From Date" and "To Date," have been introduced to specify the period during which the role will be assigned.

ROLES					
Add 🗐 Remov	2				
O Role name	Description	Role AOT name	From date	To date	:
		We didn't find anything) to show here.		

- Roles will be assigned to users only for the specified period. For instance, if the date range for role is specified from January 5, 2025, to January 8, 2025, then the role will be assigned only during these dates and will be revoked after "To date".
- This enhancement ensures permissions are granted only when required, reducing the risk of unauthorized access and improving compliance with security policies.

Remove Role from User:

• Two new fields, named "From Date" and "To Date," have been introduced to specify the period during which the role will be removed.

ROLE	;					-	
Add	🗓 Remove						
0	Role name	Description	Role AOT name	From date	To date		:
			We didn't find anything to show here.				

- Roles will be removed from users only for the specified period and reallocated after the period ends.
- This enhancement allows temporary revocation of access without permanently altering user roles, useful for temporary projects or leaves of absence.

A batch job will run every morning to allocate or deallocate roles based on the specified periods, however this is possible to modify the schedule of the batch job. The name of the batch job is *Implement approve security requests*.

If a request is approved within the specified period, the changes will take effect immediately without waiting for the next batch job execution. This enhancement ensures timely updates to user roles and statuses, maintaining the integrity and security of the system.

These enhancements aim to provide more flexibility and control over user management and role assignments within the Security and Compliance Studio, ensuring that security policies are enforced effectively and efficiently.



2.2 Include "No. of access" on View access entry points page

This enhancement provides more detailed insights into user activity and entry point usage. A new column named "Number of Access" has been introduced on the "View accessed entry points" popup of the security explorer page. This column shows how many times each entry point has been accessed by the user. The data is displayed in descending order, with the most frequently accessed entry points at the top. This allows users to quickly identify which entry points are most and least used by the selected user.

/iew access	ed entry points								
Show enabled	users only								
JSERS		ENTRY POINTS PERMITTED		ENTRY POINTS ACCESSED					
D	∀↑ Name	Entry point (AOT name)	Type	Menu item name	Menu item label	Menu item type	Last accessed on	No. of access \downarrow	
\$COBA	\$COBA	AbbreviationsEntity	DataEntity	DQSDataPolicy	Data policy	Display	12/26/2024 12:12:37 PM	74	
aabdi	Anouar Abdi (AABDI.TI)	AbbreviationsEntity	DataEntity	DewWorkflowWizard	Workflow wizard	Display	12/19/2024 11:12:40 AM	72	
ab		AccountingDistBankStatement	Menu item display	DQSDataPolicyListPage	Data quality policies	Display	12/26/2024 12:11:54 PM	46	
abachhu	Anusha Bachhu	AccountingDistCustFreeInvoice	Menu item display	DewWorkflowTemplateListPage	Data entry workflo	Display	12/23/2024 10:30:05 AM	36	
abachhu testing	abachhu	AccountingDistCustInvJour	Menu item display	DewWorkflowWorkspace	Data entry workflo	Display	12/27/2024 11:07:34 AM	31	
abachhu1	abachhu test	AccountingDistMarkupTransInv	Menu item display	DewWorkflowTemplatePreview	Data entry workflows	Display	12/27/2024 11:07:37 AM	31	
abachhutest	abachhu test	AccountingDistMarkupTransInv	Menu item display	LogisticsPostalAddressGridFor		Display	12/26/2024 11:18:04 AM	26	
abcde	abcd test	AccountingDistMarkupTransPO	Menu item display	DQSQualityAssessmentHistory	Quality assessment	Display	12/24/2024 10:40:15 AM	25	
abhadana	Ankit Rhadana	AccountingDistMarkupTransReg		DSMSecurityRequests	Security requests	Display	12/27/2024 12:00:20 PM	24	

This enhancement provides a clearer picture of entry point usage, helping to identify frequently and rarely used entry points. System administrators can use this information to modify roles or permissions based on actual usage patterns, enhancing security and resource management.

2.3 Open source record and Generate report feature for Sensitive data log

In the previous version, we introduced the sensitive data setup feature, allowing users to specify which fields in each table are sensitive. Once the setup is activated, the application captures audit logs whenever the values of these fields are modified. This information is accessible under the inquiry section on the sensitive data log page, where users can filter details by individual user or table.

This enhancement will allow the user to navigate to the source record which has been modified and generate a report of the sensitive data logs.

• **Open source record**: A new "Open Source Record" button has been introduced. This button allows users to navigate directly to the selected record in the log grid.

Clean-up sensitive data log	Generate report Open source re	ecord 😳 Options 🔎						🛛 🔍 🔍 🖉	
insitive data log									
tandard view ~									
ATE RANGE									
rom date To date									
DITIONAL FILTER OPTIONS									
er ID Table n	ame 🗸								
Record identifier	Secondary identifier	Form name	Form label	Table label	Modified table	Event created by	Sensitive data setup name	Sensitive data setup description	
000021	abtest customer	CustTable	Customers	Customers	CustTable	abhadana	AB_CustDataCheck		
test213	test213	SysUserManagement	Users	User Information	UserInfo	amartyniuk	Vishnu Test user	Logging	
anm	DEL	SysUserManagement	Users	User Information	UserInfo	amartyniuk	Vishnu Test user	Logging	
		CustGroup	Customer groups	Customer groups	CustGroup	Vijay	testing for bug	test	
10001		custoroup							
	Test 10001	CustGroup	Customer groups	Customer groups	CustGroup	Vijay	testing for bug	test	

If the record has been deleted or is linked to other records that cannot be accessed directly, the application will prompt an error message indicating that the record does not exist or cannot be opened.

• **Generate report**: A new "Generate Report" button has been introduced on Sensitive data log page. When clicked, a pop-up allows users to select the sensitive data setup name and the period for which they want to generate the report.

Clean-up sensitive data lo	g Generate report Open source re	cord 😳 Options 🔎						🗞 🔕 👂 🛇
ensitive data log								
tandard view								
ATE RANGE								
m date To d								
2/1/2024 🗐 12/	/26/2024							
DDITIONAL FILTER OPTIONS								
ser ID Tabl	le name							
Record identifier	Secondary identifier	Form name	Form label	Table label	Modified table	Event created by	Sensitive data setup name	Sensitive data setup description
000021	abtest customer	CustTable	Customers	Customers	CustTable	abhadana	AB_CustDataCheck	
	test213	SysUserManagement	Users	User Information	UserInfo	amartyniuk	Vishnu Test user	Logging
test213								
test213 anm	DEL	SysUserManagement	Users	User Information	UserInfo	amartyniuk	Vishnu Test user	Logging
	DEL	SysUserManagement CustGroup	Users Customer groups	User Information Customer groups	Userinfo CustGroup	amartyniuk Vijay	Vishnu Test user testing for bug	Logging test
anm	DEL Test 10001							

Users can also specify a schedule for generating reports frequently. Once the schedule is defined, or if the report is generated immediately, the application will process the report in the background.

Users can continue working while the report is being generated.

To access the generated reports, users can go to the security management page of the SCS Workspace and click on the "Share" button.

In the "Logs" fast tab under the "Save" section, users can view and download the latest reports in Excel format. These reports include details such as setup name, table name, form name, form label, record identifier, and updated fields.

Generate report		?
Parameters		^
SENSITIVE DATA SETUP Sensitive data setup name	~	
DATES		
From date	To date	
12/1/2024	12/27/2024	
Run in the background		^
Recurrence Alerts		
Batch processing	Task description	
No No	Generate report	
	Batch group	
	Private No	
	Critical Job	
	No No	
	Monitoring category	
	Undefined 🗸	
Start date: 12/27/2024 (12:25:14	pm) (GMT) Coordinated Universal Time	
	OK	Cancel

Security and complia	nce file share						
 Summary 							
∧ Share							
Task recording	T Upload 🛓 Download 🗎 De	elete 🔿 Refresh 🛛 Vi	ew 🗸				
Images	File name	File types	∀ Size	Created date and time	Ļ	Downloads	:
Exported role	AB_CustDataCheck-01122024-2	Sensitive data log	4.40 KB	12/26/2024 11:19:39 AM		1	
Logs	AB_CustDataCheck-01122024-2	Sensitive data log	4.40 KB	12/26/2024 11:13:18 AM		1	
	AB_CustDataCheck-01122024-0	Sensitive data log	1.20 KB	12/4/2024 7:23:42 AM		1	
	Test User_Testrecordidentifie	Sensitive data log	103.30 KB	12/4/2024 6:32:51 AM		3	
	Testrecordidentifier-0111202	Sensitive data log	57.80 KB	12/4/2024 6:30:56 AM		1	
	Testrecordidentifier-0111202	Sensitive data log	57.80 KB	12/4/2024 6:28:20 AM		1	
				-			

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

Some important features from the last few releases include 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. **Problem:** 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. 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.

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 Version 10.0.41.45

3.1.1 Security user role data

This enhancement will allow the user to view a holistic view of all the roles, privileges, entry points allocated to the role and the user allocated to the roles.

On the *Enquires* section of the Security and compliance studio, a new option named Security user role data has been added. On clicking this option, the application will navigate the user to the page that will populate the list of roles, privileges allocated to roles, entry points, access rights and users who are allocated to that role.

Simple viev	w 😳 Options 🔎							⊗	0 👂	U
urity user role	e data									
andard	view ~									
Filter										
)	Privilege name	Privilege identifier	Entry point name	Entry point (AOT name)	Securable object type	Access right	User ID	Name	Enabled	
	Maintain accountant information	AccountantInformationMaintain	AccountantPostalAddressNew BR			Full control	abtest	AB Test	true	-
	Maintain accountant information	AccountantinformationMaintain	AccountantPostalAddressNew_BR	-		Full control	test applyorg1	test	true	
	Maintain accountant information	AccountantInformationMaintain	AccountantPostalAddressNew_BR	-		Full control	test applyorg1	test	true	
	Maintain accountant information	AccountantInformationMaintain	AccountantPostalAddressNew_BR	-		Full control	test applyorg1	test	true	
	Access compensation managem		HcmWorkerListPage Employees	HcmWorkerListPage Employees		Full control	abachhutest	abachhu test	true	
	Access compensation managem		HcmWorkerListPage_Employees	HcmWorkerListPage_Employees		Full control	abtest	AB Test	true	
	Access compensation managem		HcmWorkerListPage_Employees	HcmWorkerListPage_Employees		Full control	test applyorg1	test	true	
	Access compensation managem		HcmWorkerListPage_Employees		Menu item display	Full control	test applyorg1	test	true	
	Access compensation managem		HcmWorkerListPage_Employees		Menu item display	Full control	test applyorg1	test	true	
	Access compensation managem		HRMCompEventEmpl_Created	HRMCompEventEmpl_Created	Menu item display	Full control	abachhutest	abachhu test	true	
	Access compensation managem		HRMCompEventEmpl_Created	HRMCompEventEmpl_Created	Menu item display	Full control	abtest	AB Test	true	
	Access compensation managem		HRMCompEventEmpl_Created	HRMCompEventEmpl_Created	Menu item display	Full control		test	true	
			HRMCompEventEmpl_Created	HRMCompEventEmpl_Created	Menu item display	Full control	test applyorg1	test	true	
	Access compensation managem				Menu item display		test applyorg1	test	true	
	Access compensation managem Access expiring certificates in pe		HRMCompEventEmpl_Created	HRMCompEventEmpl_Created		Full control View	test applyorg1 NANCY	NANCY		
					Menu item display	View	NANCY	NANCY	true	
	Access expiring certificates in pe	MssExpiringCertificateRecordsVi BatchAbort	MssMyTeamWithExpiringCertific BatchAbort	MssMyTeamWithExpiringCertific BatchAbort	Menu item display				true	
					Menu item action	Full control	NANCY	NANCY	true	
	Accept a request for quotation	PurchRFQFormLetter_AcceptPro		FormletterService.postRequestF	Service operation	Full control	NANCY	NANCY	true	
	Accept a request for quotation	PurchRFQFormLetter_AcceptPro		FormletterService.postRequestF	Service operation	Full control	NANCY	NANCY	true	
	Accept a request for quotation	PurchRFQFormLetter_AcceptPro	PurchRFQEditLines	PurchRFQEditLines	Menu item display	Full control	NANCY	NANCY	true	

There are two types of views available for the data populated on the page:

- Simple view: In simple view, application populates the following data: Role Name, Company accounts ID, Level, Duty name, Privileges name, Entry point name, Securable object type, Access right, User ID, Name, Enabled and Email.
- Advances view: In advanced view, application populates the following additional information: Role identifier, Duty identifier, Privilege identifier, Entry point (AOT Name),

Application also allows the user to export the data in Excel format using the standard *Open in Microsoft office* feature on F&SCM.



3.1.2 Ability to raise stand-in requests for other users

As per the current implementation of security requests, application allows the user to raise the standin request for the logged-in user only. This enhancement will allow the user to raise stand-in requests for other users as well.

This enhancement will allow the logged-in user to select the user, for which the stand-in request is needed to be raised, using the drop-down menu.

General							
Request		Туре	Origin		Area		
Stand-in_0	310	Add stand-in	Security and com	pliance studio \checkmark	~		
Status	ID	↑ Туре	Name	Email	Provider	Enabled	
Priority	\$COBA	Claims user	\$COBA	1			
Normal	aabdi	Claims user	Anouar Abdi (AABDI.TI)			~	
	ab	Claims user			·	~	
Create sta	abachhu	Claims user	Anusha Bachhu			~	
+ Add [abachhu1	Claims user	Claims user chhu Anush58test				
0 3	abachhutest	Claims user	abachhu test			~	

Once the stand-in request is approved, the stand-in user will be able to perform the activities for the user for the specified period.



3.1.3 Batch-job to clean audit logs

This enhancement will allow the authorized user to create batch jobs to clean-up the audit logs captured over the period.

On the *Parameter* page of Security & Compliance studio, a new fast tab named *Logs* has been added.

Security and compliance studio parameters									
General	Logs setup for security and compliance studio								
License count	RETENTION DAYS								
Data migration	Audit log retention period (In days)								
Enhanced SoD rules	Sensitive data log retention period (In								
Number sequences	1								
Logs	LOGS								
	Enable continuous user logging								
	No No								

This page will allow the user to specify the audit logs retention period and sensitive data log retention period in *Audit log retention period (In days)* and *Sensitive data log retention period (In days)* fields respectively.

On the Audit log page (Under the *Enquiries* section), a new option; named *Clean-up audit log*, has been introduced in the action pane. On clicking this button, a new pop-up will appear that will allow the user to specify the audit log clean-up batch job.

The Audit log retention period (In days) specified on the job is populated from the Security and compliance studio parameter page. When the job is executed, application will delete the logs which are older than the days specified in the Audit log retention period (In days) field.

Users can either run the job by clicking on the OK button or can schedule a batch job to delete the audit logs as per the defined scheduled.

Parameters		
Audit log retention period (In days) 5 NOTE: to change the retention days plea to Security and Compliance Studio -> Se		
Run in the background		^
Recurrence Alerts		
Batch processing	Task description	
No No	Clean-up audit log	
	Batch group	
	Private	
	No No	
	Critical Job	
	No No	
	Monitoring category	
	Undefined \checkmark	
Start date: 10/3/2024 (06:42:47 am) (GM	T) Coordinated Universal Time	
		OK Cancel

Similar to Audit log, application will also allow the user to schedule a batch job for the Sensitive data logs as well. On the action pane of the *Sensitive data logs* page, a new option *Clean-up sensitive data log* has been added. On clicking *Clean-up sensitive data log*, application will prompt a pop-up that will allow the user to either schedule a batch job to clean up sensitive data logs or clean the logs right away.

Clean-up sensitive data l	og	
Parameters		$\widehat{}$
Sensitive data log retention period 1 NOTE: to change the retention days to Security and Compliance Studio -	please navigate	
Run in the background		
Recurrence Alerts		
Batch processing	Task description	
No No	Clean-up sensitive data log	
	Batch group	
	Private	
	No No	
	Critical Job	
	No No	
	Monitoring category	
	Undefined 🗸	
Start date: 10/3/2024 (07:03:28 am) ((GMT) Coordinated Universal Time	
	ок	Cancel

The Sensitive data log retention period (In days) specified on the job is populated from the Security and compliance studio parameter page. When the job is executed, the application will delete the logs which are older than the days specified in the Sensitive data log retention period (In days) field.

Users can either run the job by clicking on the OK button or can schedule a batch job to delete the audit logs as per the defined scheduled.



3.1.4 Ability to activate and deactivate Sensitive data setup

As per the current implementation of Sensitive data setup, application starts capturing the sensitive data logs as soon as the sensitive data setup is configured.

This enhancement will allow the user to activate and deactivate the sensitive data setup in the application

A new button named Activate has been added on the Sensitive data setup page.

← 😑 🖫 Save → New 🗊 Delete	Activate Sensitive data condi	tion setup 😳 Options	R	
✓ Vendor	standard view ∽ Sensitive data setu	ıp		
VendorDataLogs	Name	Created by	Created date and time	Active status
10/3/2024 8:08:20 AM	VendorDataLogs	abhadana	10/3/2024 08:08:20 AM	Inactive 🗸
	Description General + Add In Delete Field pick	cker		
	C Table name	Reference field name	Field label	Observation
	VendTable	✓ CreditMax	✓ Credit limit	
	VendTable	CreditRating	Credit rating	

Application will not capture any sensitive data logs for the setup only if the setup is Active.

For an active setup, the user will be able to view a button named *Deactivate*, that will allow the user to deactivate sensitive data log setup.

← = + New 🗊 Delete Deactiv	vate Sensitive data condition setup	C Options		
	standard view ∽ Sensitive data setup)		
VendorDataLogs 10/3/2024 8:08:20 AM	Name VendorDataLogs Description	Created by abhadana	Created date and time 10/3/2024 08:08:20 AM	Active statusActive
	General			
	+ Add 🛍 Delete 🛛 Field picke	er		
	Table name	Reference field name	Field label	Observation
	VendTable	CreditMax	Credit limit	
	VendTable	CreditRating	Credit rating	

As soon as a sensitive data setup is Deactivated, application will stop capturing the sensitive data setup logs.

3.1.5 Ability to select dimension and financial tag field using Table security recording



This enhancement will allow the user to select the dimension field and the financial tag field on Journal voucher page using Table security recording.

ournal voucher 00459 : WFGenJrn					ß	Remove 🗌 Stop recording	
Standard view ~					C	Field name	:
isplay journal lines					C		
All						LedgerDimension	
List General Invoice Payment Payment fee Fixed assets Remittance History							
+ New 🗊 Delete Voucher Financial dimensions 🗸 Tax Functions 🗸							
O Date Voucher Company Account type Account	Financial tags	Description	Debit	Credit Offset company Offset acr			
Date Voucher Company Account type Account 12/11/2017 + JE000001 + usmf + Ledger + 600150-001-022-008-Ac	-	Description + Misc Expense +	Debit 1,20 <mark>1+</mark> 1	Credit Offset company Offset acr			

3.2 Version 10.0.40.44 Release

3.2.1 Organization assignment for security request

In the current version of Security and Compliance Studio, when submitting a request to create a new user or assign a role, the application permits the selection of companies to be allocated to the user.

This enhancement will enable users to choose whether to allocate companies from a legal entity list or from the organization hierarchies set up in the application.

The "Assign roles to user" and "Create user" sections have been updated to allow users to decide if they want to:

- Assign all organizations: This option enables users to request allocation of all organizations for which the request is made.
- Assign a specific organization: This option allows users to select from either the legal entity or the organization hierarchies available in the application.

COMPANIES						
SELECT ORGANIZATIONS Assign organization Assign all organization Assing specific organizations Available organisation nodes: Select organisation hierarchy (All legal entities)]					
Name	Company Î	:	+	Company	Company accounts	:
Contoso Entertainment System	USMF		+		() () () () () () () () () () () () () (
Contoso Group	GLCO		=			
Contoso Italy	ITCO		Ĩ		We didn't find anything to show here.	
Contoso Orange Juice	USP2					
Contoso Process Industry	USPI					
Contoso Retail	GLRT					

Once the security request is approved, the user for which the security request is approved, will be granted permission to selected legal entities.

3.2.2 Continuous user action logging

On the Security Explorer page of Security and compliance studio, a new option, named View accessed entry points, has been introduced on the toolbar.

← OCreate snapsh	ot Refresh licenses 🖄 I	Reset p	ins Advanced view Show joined	Vie	ew accessed entry points Export to E	xcel	Options				8	0 (P 🕐 🗖
Standard view \vee													
Security explorer: full view													
USERS			ROLES		DUTIES		PRIVILEGES		ENTRY POINTS				
HP Pin users			-🛱 Pin role		-⇔ Pin duty		-t¤ Pin privilege		- Pin entry point and permissions				
User	Name		Role name 1 :		Duty name 1 :		Privilege name		Entry point (AOT name) 1 T	lype		Acc	cess right
-			AAC_Hotfixtest		A parameter that is used to gro		testpriv1		AadWorkerIntegrationEntity	DataEntity		Vie	BW
-			abcde		 Access benefit management wo 		TestSoDAccess12		AadWorkerIntegrationEntity	DataEntity		Ful	II control
-			Accountant		 Access benefits workspace 		SCS_testexcludeentry (tables)		■□ AbatementCertificate_IN	Menu item display		Ful	Il control
•			Accounting manager		Access employee development		 SCS_testhotfix1 (display) 		■ ○ AbatementPeriodicCertificate_IN	Menu item action		Cre	eate
-			Accounting supervisor		Access expense management w		 Sensitive Data Role (display) 		AbatementPeriodicCertificate_IN	Menu item action		Ful	II control
-			 Accounts payable centralized pa. 		Access the leave and absence te		SCS_testbug (action)		AbbreviationCodeImport_RU	Menu item action		Cre	eate
-			Accounts payable clerk		Access workforce management		testprivreg		AbbreviationCodeImport_RU	Menu item action		Ful	II control
•			Accounts payable manager		Access workforce management		SCS_ABDemo_1812 (action)		■ ③ AbbreviationsEntity	DataEntity		Vie	2W
•		1	 Accounts payable payments clerk 	1	 Accounting manager (display) 	1	 SCS_rolewithpriv (display) 	1	AbbreviationsEntity	DataEntity		Ful	Il control

This feature allows to view the entry points permitted to a user and the entry points accessed by the selected user.



 Filter Show enal only 	bled users										
SERS				ENTRY POINTS PERMITTED			1	ENTRY POINTS ACCESSED			
D	\∀† Name	Enabled		Entry point (AOT name) î	Туре	Access right		Menu item name	Menu item label	Menu item type	Last accessed on
\$C0BA	SCOBA	false		AbbreviationsEntity	DataEntity	View		DSMUserAccessedEntryPointsL	View accessed entry points	Display	7/2/2024 10:44:30
		true		AbbreviationsEntity	DataEntity	Full contro		DSMSecurityLicenseTypeExplorer	Security explorer	Display	7/2/2024 10:42:25
		true		AccountingDistCustFreeInvoice	Menu item display	View		DSMSecurityRequests	Security requests	Display	7/2/2024 10:42:19
		true		AccountingDistCustInvJour	Menu item display	View		HcmTaskList		Display	7/2/2024 10:42:09
		false		AccountingDistMarkupTransInv	Menu item display	View		DSMSecRequestSelectRoles	Add	Display	7/2/2024 6:53:33
		true		AccountingDistMarkupTransInv	Menu item display	Full contro		DewWorkflowTemplateListPage	Data entry workflow templates	Display	6/28/2024 11:27:0
		true		AccountingDistMarkupTransPO	Menu item display	View		DQSDataPolicy	Data policy	Display	6/28/2024 10:33:1
		true	1	AccountingDistMarkupTransReq	Menu item display	View	r.	DQSDataPolicyListPage	Data quality policies	Display	6/28/2024 10:33:0
		true		AccountingDistPurchReqTable	Menu item display	View		DewWorkflowWizard	Workflow wizard	Display	6/28/2024 6:21:01
		true		AccountingDistPurchTable	Menu item display	View		DewWorkflowStepOpenPart	Open tasks assigned to me	Display	6/28/2024 6:20:53
		true		AccountingDistribution	Table	No access		DewWorkflowTemplatePreview	Data entry workflows	Display	6/28/2024 6:15:54
		true		AccountingDistributionOrderSu	Menu item display	View		DewWorkflowWorkspace	Data entry workflow workspace	Display	6/28/2024 6:15:53
		true		AccountingDistributions	Menu item display	View		DewWorkflowWizardFieldCRDr	Change request	Display	6/27/2024 10:50:0
		true		AccountingDistributionsDocum	Menu item display	View		DewWorkflowTemplateNewVer	Create new version	Display	6/27/2024 10:30:2
		true		AccountingDistTaxTransTmp	Menu item display	View		DQSParameters	Data quality studio parameters	Display	6/27/2024 8:52:50
		true		AccountingDistTaxVendPackSlip	Menu item display	View		VendTableListPage	All vendors	Display	6/26/2024 9:39:00

The admin user can adjust the licenses assigned to a selected user based on the entry points they have accessed.

Additionally, A batch job has also been added on the 'User continuous log' page that will allow the user to clean the audit logs older than the specified period.

(←)	Reset filters Clean up	logs for entry points accessed 😳	Options 🔎				⊗	٥	p	U	ы
	to workspace \checkmark Advan	ity diagnostics Get a link ∽ Cre	a re ate a custom alert ∽ nage my alerts								~
Star	ontinuous log ndard view ~ IONAL INFO TO INCLUDE En 	try point Fr	ATE RANGE To date om date To date /4/2024 To date								
0	User ID	Menu item name	Menu item label	Menu item type	Last accessed on	\\$↑					
\circ	pp	DQSDataQualityPolicyLogCleanup	Clean-up logs	Action	7/4/2024 5:06:22 AM						
	pp	VendTableListPage	All vendors	Display	7/4/2024 5:06:35 AM						
	SainathR	DewWorkflowTemplateListPage	Data entry workflow templates	Display	7/4/2024 5:06:36 AM						- 11
	pp	HcmTaskList		Display	7/4/2024 5:06:49 AM						
	Marius.Rusu	SysEmailHistory	Email history	Display	7/4/2024 8:05:19 AM						

This batch job has been placed on the User continuous log page as the data-source for user continuous logs and entry point logs is the same.

Clean up logs for entry poi	ints accessed	
Parameters		^
Retention days		
Run in the background		\frown
Recurrence Alerts		
Batch processing	Task description	
No No	Clean up logs for entry points a	
	Batch group	
	Private	
	No No	
	Critical Job	
	No No	
	Monitoring category	
	Undefined \checkmark	
Start date: 7/4/2024 (11:46:00 am) (GM	T) Coordinated Universal Time	
	ОК	Cancel

This batch job allows the user to specify the retention period. Once the batch job is executed, application will delete the logs which are older than the specified no. of days.

3.3 Version 10.0.39.43 Release

3.3.1 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.

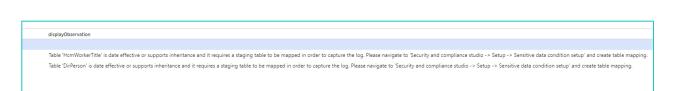
This new form can be found under *Security and Compliance Studio -> Inquires -> Sensitive data setup*. Please refer to the screenshot below:

	reco	ording . Standard	view \sim									
Ser	nsit	tive data se	tup									
Name				ted by	Created	date and time	Security r	record status	Owner			
		ording .	\neg	min)		24 08:58:58 AM	Open					
Dee	riptic											
Desc	npuc	011								•		
Gen	eral											
+4	dd	🗊 Delete 🛛 Field pick	er									
С	Table	e name		Reference field name	•	Field label		displayObservat	tion			
	-	isticsLocation		Description		Name or description						
		WorkerTitle		OriginalHireDateTin		Original hire date		Table 'HcmWor	rkerTitle' is dat	effective or	supports	inheritance a
	DirPe	erson	~	NameAlias	~	Search name						
							1					
Que	· .						1					
Edi	t quei											
Edi	t quei Quer	ry name		ole name								
Edi	t quei Quer			ole name PersonStaging								
Edi	t quei Quer	ry name										
Edi	t quei Quer	ry name										
Edi	t quei Quer	ry name										
Edi	t quei Quer	ry name										
Edi	t quei Quer	ry name										
Edi	Quer DirPe	ry name										
User	t quei Quer DirPe	erson										
Edi	t quer Quer DirPe	ing Delete	∼ Din	PersonStaging		networkAlias		networkDomai	n			
User	t quer Quer DirPe	erson	∼ Din			networkAlias fmihoc@to-increase.com		networkDomaii https://sts.win		Icrease.com		
Edi	t quer Quer DirPe	In Delete User ID	 Dir 	PersonStaging	f		osoft.com	https://sts.win	dows.net/to-in	Icrease.com		
Edi	t quer Quer DirPe	Delete User ID fmihoc	V Dir	PersonStaging Name fmihoc	f	fmihoc@to-increase.com		https://sts.win	dows.net/to-in dows.net/	Icrease.com		

This page has three sections:

- 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:



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 1	Staging tab	le				
	_	DirPartyTable	DirPartyTableAttachmentsStaging					
)		DirPerson	DirPerson	Staging				
		DirPersonName	DirPerson	NameHistoricalStaging				
		LogisticsPostalAddress	LogisticsP	ostalAddressElectronicContactV2Staging				
+	Add) 🗊 Delete) (Generate ma	apping					
+	Add		apping	Stagging table field				
+ 0			apping) ↑	Stagging table field AnniversaryDay				
+		Main table field	apping) ↑					
+		Main table field AnniversaryDay	apping) ↑	AnniversaryDay				
+ 0		Main table field AnniversaryDay AnniversaryMonth	apping) ↑	AnniversaryDay AnniversaryMonth				
+ C		Main table field AnniversaryDay AnniversaryMonth AnniversaryYear	apping) ↑	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".

-		

tandard view 🗸									
TE RANGE									
m date To d		_							
(1/2023 💼 4/		1							
DITIONAL FILTER OPTIONS									
er ID Tab	e name	\sim							
							\		
Table label	Modifie	d table	Description	Event created by	Sensitive data setup name	Event date	<u></u>		
Addresses	Logisti	csPostalAddress		Admin	Test from scratch	11/2/2023 12:44:54 PM	Л		
Position details	HcmPositionDetail			Admin	HCMPositionDetail	11/2/2023 12:44:37 PM	Л		
Customers	CustTable			Admin	Custtable - credit	11/2/2023 12:34:58 PM	Л		
Customers	CustTable			Admin	Custtable - credit	11/2/2023 12:15:53 PM	Л		
Customers	CustTable			Admin	Custtable - credit	11/2/2023 10:19:55 AM	4		
Order lines	SalesLine			Admin	InventDim	10/30/2023 11:47:26 4	10/30/2023 11:47:26 AM		
Position details	HcmPositionDetail			Admin	HCMPositionDetail	10/30/2023 11:31:10 A	M		
Position details	HcmPositionDetail			Admin	HCMPositionDetail	10/26/2023 12:13:17 PM			
Position details	HcmPositionDetail			Admin	Position - test	10/11/2023 7:03:43 AM			
Addresses	LogisticsPostalAddress			Admin	Test worker address	10/10/2023 9:23:45 AM	10/10/2023 9:23:45 AM		
Addresses	Logisti	csPostalAddress		Admin	Test worker address	10/10/2023 9:23:31 AM	10/10/2023 9:23:31 AM		
User Information	UserInf	o		Admin	User data	8/10/2023 10:36:58 AM	A		
User Information	UserInfo			Admin	User data	8/10/2023 10:36:40 AM	A		
Vendors	VendTable			Admin	Vendor table	8/10/2023 10:31:55 AM	4		
Global address book	DirPartyTable			Admin	Vendor table	8/10/2023 10:31:24 AM	A		
User Information	UserInf	o		Admin	User data	8/10/2023 10:12:12 AM	8/10/2023 10:12:12 AM		
User Information	UserInf	o		Admin	User data	8/10/2023 10:08:32 AM	4		
AILS								=	
	Field label	Event type	Value from		Value to	Form na	ne	Form label	Created date and time
Reference field name		Record modified	413 Oak Street TEST		413 Oak Street TDEMO1	Logistic	sPostalAddress	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.

3.3.2 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.



My view 🗠									
Securable tree view	v								
Override permission on selected									
Security object types	Value	DETAILS							
Role 🗸	Budget contributor	🖧 Explore							
AOT name	Description	○ ② Name	1 AOT name	Description	Entry point type	Object name	Object type	Access right	
BUDGETBUDGETCONTRIBUTO	Enters and approves budget	O General ledger parameters	LedgerParameters		Menu item display	LedgerParameters	Form	View	
R	plan requests	C deneral redger parameters	ceugerrarameters		menu nem unspray	beogenarameters	Point	VIEW	
🔺 🔳 Menu							-		
Accounts payable		Security diagnostics							
Accounts receivable		Security diagnostics							
Asset management		Show all access 🖓 Explore							
Audit workbench		O ObjectType	AOT name	Label		Access level	License type (on-premise)	License type (cloud)	
Budgeting									
Cash and bank manager	ent	O Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor		View	Team members	Team members	
Common	I	Duty	BUDGETBUDGETPROCESSPOLICIESINQUIRE	Inquire into budget process polici	ties	View	Team members	Team members	
Consolidations		Privilege	LedgerParametersView	View general ledger parameters		View	Team members	Team members	
Cost accounting									
Cost management									
Credit and collections									
Demo data									
Expense management		Form level details							
Fiscal books		Form level details							
Fixed assets		FORM MENU ITEMS							
Fixed assets (Russia)		A Explore							
Fleet management									
4 🔳 General ledger		Control name		ontrol type	Object nar	me from menu item	Object type from men	u item	
Allocations		 LedgerOppositeSignUpdate 	F	ormBuildFunctionButtonControl	LedgerOp	opositeSignUpdate	Action		
Calendars		EximParameters_IN	F	ormBuildFunctionButtonControl	EximParan	meters_IN	Display		
Chart of accounts Currencies									
Currencies Deferrals									
Deferrals setup									
Deterrals setup Financial report setup									
Financial report setup Financial reports setup	I								
Inquiries and reports	-	TABLE PERMISSIONS							
Inquiries and reports Journal entries		O Data source name	Control type	DataSourceTable					
Journal entries Journal setup		LedgerParameters	Data source	LedgerParameters					
Journal setup Ledger setup		TaxParameters	Data source	TaxParameters					
Advance adjustment p	acamator	NumberSequenceReference	Data source	NumberSequenceReference					
Cash control configure					E				
Cash position paramet		AssetParameters	Data source	AssetParameters					
Check voucher series		InventDimSetupGrid	Data source	InventDimSetupGrid					
Date intervals		CustParameters	Data source	CustParameters					
Financial reporting set	10	FORM CONTROLS							
Fiscal calendars	-	O Control name	Control type	Object name from menu it	item Ohier	ct type from menu item	Needed permissions	V	
General ledger param	ters	O UpdateDelimiter	FormBuildFunctionButtonControl				Manual		
INPC rates		Opdatebeimiter	FormsultaFunctionsuttonControl	I DimensionSegmentSepa	aratoripataupda Actio	20	manual		
Ledger									
Ledger calendars									
Matrix report									
Period allocation cate	ories								

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)

how all access 器 Explore			
ObjectType	AOT name	Label	Access lev
) Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor	View
Duty	BUDGETBUDGETPROCESSPOLICIESINQUIRE	Inquire into budget process policies	View
Privilege	LedgerParametersView	View general ledger parameters	View
curity diagnostics	on 🖧 Explore		
how access based on selection	ውስ 🖧 Explore AOT name	Label	Access le
how access based on selection		Label Auditor	Access lev View
how access based on selection ObjectType	AOT name		
how access based on selection ObjectType Role	AOT name AUDITPOLICYMANAGER	Auditor	View
how access based on selecti ObjectType Role Role	AOT name AUDITPOLICYMANAGER BUDGETBUDGETCLERK	Auditor Budget clerk	View View
how access based on selecti ObjectType 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.

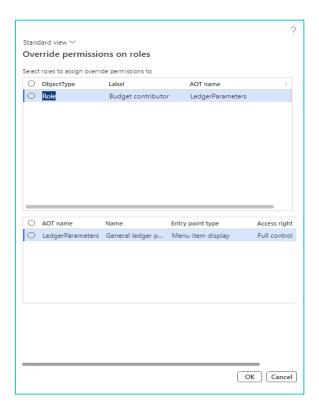
On form level there are multiple options/buttons that are opening other forms. Here these forms are displayed so you will know that if you want to provide full access to a form you need to provide access to the forms that are opening from the buttons available on that form.

- 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 permission' 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.

^{My view ∽} Securable tree viev	N								
Override permission on selected	object								
Security object types Role	Funde .	DETAILS ஃ Explo	re						
AOT name	Description	00	Name î	AOT name	Description	Entry point type	Object name	Object type	Access right
BUDGETBUDGETCONTRIBUTO	Enters and approves budget	•	General ledger parameters	LedgerParameters		Menu item display	LedgerParameters	Form	Full control 🛛 👻
R P Expense management Fiscal books	plan requests						_		

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.



3.3.3 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.

Security history	Audit log report Open securi	ity request history ···· M	ore			
Role history	P Filter					
User history	 Event date and time 3/13/2024 12:03:05 PM 	Event created by Admin	Event type Duty created	Company *	Description Duty DutyUniqueProjectTest1 created	Security request referen
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
	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
2	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.

pen request details juest odify role e	Area Created by	Created date a 4/3/2024 07:		End date	Owner					
curity request details ipen request details quest lodify role pe lodify role	Area			End date						
ipen request details quest lodify role pe				End date	-					
quest Iodify role				End date						
fodify role pe				End date						
pe	Created by	4/3/2024 07:					Security record status	Scenario	Description	
			14:10 AM		Admin		Completed			
loaity role	Admin	Start date		Origin	Priority Normal		Modified by Admin			
	Norm			User requests	Normai		Admin			
orkflow approval history										
pen workflow approval details										
itance ID	Workflow ID	Status		Document	Document type		Workflow	Version	Submitting user	Company accounts ID
00001	000014	Completed		Quotation: QN0000002, Ci	ity Sales quotatio	n	Review project quotations	1.0.0.0	JUNE	ussi
			Message	Comment	Created date and time					
Workflow St	ubmission	000001: Quotation: QN00	Submitted by: JUNE		1/1/2016 8:35:13 PM	JUNE				
Workflow C	reation	000001: Quotation: QN00			1/1/2016 8:35:29 PM	JUNE				
Approval Cr	reation	Project Quotation Approv	PSAProjQuotationTemp	plate	1/1/2016 8:35:34 PM	JUNE				
Approval A	uto complete condition	Project Quotation Approv	Auto-completion	A	1/1/2016 8:35:42 PM	JUNE				
			condition: Project							
Approval Ci	ompletion	Project Quotation Approv			1/1/2016 8:35:44 PM	JUNE				
Workflow C	ompletion	000001: Quotation: QN00			1/1/2016 8:35:49 PM	JUNE				
idit log details										
Event date and time D	escription		Event type	Reference Comp	any Event created	by i				
) 3/11/2024 1:01:46 PM D	uty Landed cost agent (dis	play) was created from Overri.	Duty created	0 *	Admin	1				
3/11/2024 1:01:53 PM Pr	rivilege Landed cost agent	(display) was created from Ov	Privilege created	0 *	Admin					
3/11/2024 1:01:54 PM R	ole Landed cost agent was	modified from Override perm	ni Role modified	0 *	Admin					
3/11/2024 1:01:54 PM D	uty Landed cost agent (dis	play) was created from Overri	 Duty created 	0 *	Admin					
		or operations master was mod		0 *	Admin					
3/11/2024 1:01:55 PM D	uty Maintain receipt operat	tions was modified from Over	rr Duty modified	0 -	Admin					
Reference description	Name		Reference type	Refere	nce table type					
Duty Landed cost agent (display	y) wa Landed cost agen	nt (display)	Duty	Duty						

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

3.3.4 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 <u>package</u> file type needs to be added.

Import AX: Operations My view ~ DEMO import					
Import 1					
Group name Desc DEMO import	ription	Data p	roject operation type rt	Project category Project	\checkmark
Selected entities + Add file \checkmark + Add template \checkmark in Rem	ove entity Open	in Excel Resequence	✓ Sort by ✓ Disable ✓	Entity attribute	
Add file JOB DETAILS Source data format Package 2 UPLOAD IMPORT FILES Upload data file Close	d 3	View map Executi	î Level in ex	Sequence Obsolete	Source

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

	AX : Operations My view ∽				
1C) import				
t					
			Data project operation type		
			1	-	-
0		_	Executi	Level in ex	Sequence
	Segregation security sets	L)	1	1	1
	Segregation security set lines	I.	1	1	2
	Enhanced SoD rules	I.	1	1	3
	t Dim ed e d fil	name Description Dimport ed entities d file > + Add template > Remove entity Open in Ex Entity Segregation security sets Segregation security set lines	t name Description Da Dimport II ed entities d file > + Add template > II Remove entity Open in Excel Resequen C Entity View map Segregation security sets Segregation security set lines	t name Description Data project ope import Import ed entities d file > + Add template >> Impore entity Open in Excel Resequence >> Sort b C Entity View map Executi ↑ Segregation security sets Import 1 Segregation security set lines Import 1	t name Description Data project operation type Import ed entities d file > + Add template > Remove entity Open in Excel Resequence > Sort by > Disable C Entity View map Executi Level in ex Segregation security sets E 1 1 1

Import the file and the result should look like this:

Entity processing status								
View staging data 🛛 🖓 Filter 🗠						1		
C Entity		Status	Pending	In staging	Created	Updated	Tota	
Segregation security sets	~	Succeeded	0	41	41	0	41	
Segregation security set lines	~	Succeeded	0	435	435	0	43	
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.



3.4 Version 10.0.37.42 and Older

3.4.1 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.

Filter Talaalalal	Standard view V Segregation Segregation security set	security sets	
	Tralaalalal	Traslalaa	
rat2	Segregation security	set lines	
	+ Add 🗊 Remove		
	 Securable object 	Securable object	t type Access level
	 Accountant_BR 	Menu item dis	play View
	ACOJournalPos	t_BR Menu item act	tion View
	AdvanceAdjust	mentPara Menu item dis	play Full control
	AssetChangeGr	oup Menu item act	tion 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 Security and compliance st 🗸	Area	\sim
Status	-			
Priority Normal	Security record status Open	Owner Admin		
Enhanced SoD rules				
+ Add 🗊 Remove				
○ C Name	î Туре	First First see	urable object type	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.

	rd view~					Sta	nced SoD rules				
Filter	me	î Type	Effective from	Effective to	Enabled	P Fil	Name	î Type	Effective from	Effective to	Enabled
∨ tes	t	Segregation security sets	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~	0	∨ test	Segregation security sets	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	~
tes	t4	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	~
tes	tsodentry	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	~
tes	tsodpriv	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	~
							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.

3.4.2 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 🛍 Delete ◯Workflow 🗸 Request Manage
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.

	\bigcirc Status \checkmark	
1	Open	L
	Waiting	L
	Review	L
	Approved	L
	Rejected	
	Canceled	L

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.

			A
lequest	Туре	Origin	Area
Demo SR 1	General	User requests	WHS
tatus			
riority	Status	Owner	
Normal	Open	Admin	
Description			

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 V	Area WHS V
Status			
Priority Normal	Status Open	Owner Admin	
Create users			
User ID newUser1	User name newUser1	Email newUser1@to-increase.com	Company
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.



itatus Priority Normal				
	~	Status Open		Owner Admin
ssign roles to user				
ISER Iser ID Admin OLES Add I Remove	User nam		ncrease.onmicros	Company USMF
○ C Role name	D	escription	Role AOT nam	ne :
O Auditor	N	lanages and reviews	aud AUDITPOLIC	YMANAGER ~
COMPANIES + Add I Remove				
○ C Company	Company a	counts		

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.

lequest Demo S	iR 1		Type Remove role from user	Origin User requests	
tatus					
riority Normal	~]	Status Open	Owner Admin	
lemove	roles from user	-			
ISER					-
lser ID		User name	Email	Company	
Admin		Admin	fmihoc@toincrease.onm	nicros USMF	
- Southing					
OLES					
OLES] Remove				
OLES			Description	Role AOT name	
OLES				Role AOT name : ASSETLEASECLERKROLE ×	

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.

ecurity requests My view ∽	
Demo SR 1	
General	
Request Type	Origin Area
Demo SR 1 Disable user V	User requests VWHS
Status	_
Priority Status	Owner
Normal V Open	Admin
Disable users	
Add 📵 Remove	
O C User ID ↑ User name	
O BrunoD BrunoD	

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.

Demo	oguests My vi SR 1	ew 🗸			
General					
Request Demo S	R 1		Type Enable user	Origin User requests V	Area WHS
Status					
Priority Normal	\sim		Status Open	Owner Admin	
Enable u	sers				
Add 🗎	Remove				
00	User ID	Î	User name		
0	JanetS		Janet Schor		

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.



equest		Туре		Origin	Area
Demo SR 1			lete user 🗸 🗸	User requests 🗸 🗸	WH
tatus		_			
riority		Statu		Owner	
Normal	\sim	Op	en	Admin	
elete u	sers				1
Add 间	l Remove				+
	User ID 1	User name	Email		-
0	CASSIE	CASSIE	CASSIE@contosoax7.onm		
<u> </u>	cdsaurorauser	Auroraus	Aurorauser01@capintegr		
		/ taroraa.sm	/ aronadsero re capinegi m		

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.

C	uests My view 🗸									
Demo										
Demo	31 1									
General										
Request		Туре			rigin	Area				
Demo SR	1	Delete	user	U	Jser requests	V WHS	\sim			
Status										
Priority		Status		Ov	wner					
Normal	\sim	Open		Δ						
Create role ROLE Upload ta	e Isk recording				Admin					
ROLE	sk recording	Description	2585	Scenario		axtr				
ROLE Upload ta Role name	sk recording oRole1	Description	3565	Scenario	4dmin gForCSReplicate	axtr				
ROLE Upload ta Role name SCS_Demo SCENARIO	sk recording oRole1 DETAILS number Securable obj	Description	oses Securable type	Scenario		Description	File name	Child scenario	Î Remark	
ROLE Upload ta Role name SCS_Demo SCENARIO	oRole1 DETAILS	Description		Scenario skRecording	gForCSReplicate	Description	File name TaskRecordingForCSRepli		Î Remark	
ROLE Upload ta Role name SCS_Demo SCENARIO O Step	sk recording oRole1 DETAILS number Securable obj	Description Demo purpt	Securable type	Scenario skRecording Acco Full	gForCSReplicate	Description			Remark Additional secura found in the task	
ROLE Upload ta Role name SCS_Demo SCENARIO O Step	sk recording oRole1 DETAILS number Securable obj 1 salestablelist	Description Demo purple ect page	Securable type Display	Scenario skRecording Acco Full Full	gForCSReplicate cess level Il control	Description Go to Accounts receivabl	TaskRecordingForCSRepli		Additional secura	
ROLE Upload ta Role name SCS_Demo SCENARIO O Step	sk recording oRole1 DETAILS number Securable obj- 1 salestablelist 2 DefaultDasht	Description Description Demo purps ext page page	Securable type Display Display	Scenario SkRecording SkRecording Full Full	gForCSReplicate cess level Il control Il control	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli TaskRecordingForCSRepli		Additional secura	recording ble object
ROLE Upload ta Role name SCS_Demo SCENARIO O Step	sk recording oRole1 DETAILS number Securable obj 1 salestablelist 2 DefaultDasht 5 salestablelist	Description Demo purps ect page page tails	Securable type Display Display Display	Scenario skRecording Full Full Full	gForCSReplicate cess level Il control Il control Il control	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli TaskRecordingForCSRepli TaskRecordingForCSRepli		Additional secura found in the task Additional secura	recording ble 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.

Demo	equests My view ∽ ⊃ SR 1						
Request		lype	Origin	Area			
Demo S	R 1	Modify role	User requests	WHS	~		
Status							
Priority Normal	\sim	Status Open	Owner Admin				
Modify r	role						
ROLE							
Add role	e 间 Remove						
_	Role name	Description R	Role AOT name 1				
0	View lease	View of lease roles	ASSETLEASELEASEVIEW				
	O DETAILS						
Upload Scenario Demo1x	i task recording × recording.axtr						
Upload Scenario Demo1x	t task recording x recording.axtr p number Securable object	Securable type	Access level	Description	File name	Child scenario	Î Remark
Upload Scenario Demo1x	i task recording x recording.axtr	Securable type Display	Access level Full control	Description Go to Accounts receivable > Orders > A		Child scenario	Î Remark
Upload Scenario Demo1x	t task recording x recording.axtr p number Securable object				Demo1x recording.axtr	Child scenario	Remark Additional securable obje found in the task recordin
Upload Scenario Demo1x	t task recording k recording.axtr tp number Securable object 1 salestablelistpage	Display	Full control	Go to Accounts receivable > Orders > A	Demo1x recording.axtr	Child scenario	Additional securable obje
Upload Scenario Demo1x	t task recording execording.axtr pp 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 Demo1x recording.axtr	Child scenario	Additional securable obje
Upload Scenario Demo1x	k recording.axtr promber 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	Additional securable obje

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.**

Gene			Туре	_	Origin	Area
	no SR	1	Lock role	\sim	User requests V	WHS ~
Statu	s					
Priori	-	\sim	Status Open		Owner Admin	
Lock	roles					
+ A	dd [🗊 Remove				
0	9	Role name		Name		
		Applicant anonymous (exte	ernal)	ANONYMOUS	SAPPLICANT	

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.**

Request Demo SR 1	1	Type Unlock role	Origin User requests V	Area WHS	
Status					
Priority Normal	\sim	Status Open	Owner Admin]	
Jnlock role	25				
0 0 r	Remove Role name Narehouse worker V	Name WMSWAREHOUSEWORKER			
0 0 r	Role name				
_	Role name				
0 0 r	Role name				

l) 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.

Security requests My view ∽ Demo SR 1		
General		
Request Demo SR 1	Type Delete role	Origin Area User requests V WHS
Status Priority Normal	Status Open	Owner Admin
Delete role		
Add role 🗊 Remove	Description	Role AOT name ↑ 6DEC7811-E0C5-42C5-94
SCS_RoleTest_2 SCS_RoleTest1		82B6FA62-0C74-46CC-8D
Description		

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.

	requests ∣ My view ∽ oSR1										
Demo	OSKI										
General											
Request Demo S	5R 1	Type Create rule	→ Origi Use	n r requests ->	Area WHS	\checkmark					
Status											
Priority Normal		Status Open	Owne								
	ed SoD rules										
	Remove										
02	Name 1	Туре	First	First securable object type	First access level	Second	Second securable object type	Second access level	Effective from	Effective to	Enabled
					-						
0	Create demo rule 2 from Create demo rule from SR		AdvancedLedger ∨ Maintain Absorption		Create ~ No access	BankChequeCompanyI ~ Import ZIP/postal codes	1.2		4/28/2022 10:43:44 ₪ ⊙ 4/28/2022 10:43:06 AM	12/31/2154 11:59:5 🖽 💿 5/26/2022 11:59:59 PM	
0											
0											
0											

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.

	ity requests ∣ My view ∨ mo SR 1									
Gene	eral									
Requ	est no SR 1	Type Resolve conflict		rigin User requests 🔊 🔨	Area WHS	\checkmark				
Statu	Status									
Prior Nor	·	Status Open		wner Admin						
Enha	nced SoD conflicts									
	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
	Test 1 V	Duty	EMMAH	PrintMgmtSetupUIMain	Sales clerk	ProjActivity	Sales representative	Override \vee	Demo purpose	Existing role
Desc	ription									

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

		-	and	-			-				
ecurity	y reques	ts Myview ∽									
Den	no Sl	R 1									
Gener	al										
Reque: Demo	st o SR 1		Type Delete rule	Origin V User req	uests 🗸	Area WHS	\checkmark				
tatus											
Priorit			Status	Owner							
nont											
Norm		~									
Norm		\sim	Open	Admin							
	hal	ced SoD rules									
Delete	hal	ed SoD rules									
Delete + Ad	nal e enhanc	eed SoD rules			Effective to	First	First securable object type	First access level	Second	Second securable object type	Second acces
Delete + Ad	e enhanc Id 🗊 Re 📿 Nam	eed SoD rules	Open Type	Admin	Effective to 12/31/2154 11:59:59 PM	First DSMAuditLog	First securable object type Menu item display	First access level View	Second DSMAssetClassification	Second securable object type Menu item display	Second acces View
+ Ad	e enhanc Id 🗊 Re C Nam SoD	emove 1	Open Type	Effective from						Menu item display	View
Delete	e enhanc Id 🗊 Re C Nam SoD	emove ne 1) Test 1 - do not use	Open Type Entry point	Effective from 4/20/2021 12:11:46 PM	12/31/2154 11:59:59 PM	DSMAuditLog		View	DSMAssetClassification	Menu item display	
Delete	e enhanc Id 🗊 Re C Nam SoD	emove ne 1) Test 1 - do not use	Open Type Entry point	Effective from 4/20/2021 12:11:46 PM	12/31/2154 11:59:59 PM	DSMAuditLog		View	DSMAssetClassification	Menu item display	View
Delete	e enhanc Id 🗊 Re C Nam SoD	emove ne 1) Test 1 - do not use	Open Type Entry point	Effective from 4/20/2021 12:11:46 PM	12/31/2154 11:59:59 PM	DSMAuditLog		View	DSMAssetClassification	Menu item display	View
Delete	e enhanc Id 🗊 Re C Nam SoD	emove ne 1) Test 1 - do not use	Open Type Entry point	Effective from 4/20/2021 12:11:46 PM	12/31/2154 11:59:59 PM	DSMAuditLog		View	DSMAssetClassification	Menu item display	View

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.

-	equests My view ` SR 1	~					
General							
Request Demo S	R 1	Type Add stand-	in 🗸	Origin User requests	\checkmark	Area WHS	\sim
Status Priority Normal	\checkmark	Status Open		Owner Admin			
Create st	and-in Remove						
	User ID	Stand-in	From date	To date	Copy assigned organi	zations	
0	Admin	ALICIA ~	4/28/2022	4/30/2022 📾			
Descripti							

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.

ener	al										
eques					уре			Origin			Area
Demo SR 1				Cancel stand-in 🗸		User requ	ests	~	WHS		
tatus											
riority	/			S	itatus			Owner			
Vorm	nal	\sim	·	[Open			Admin			
		tand-in									
		User ID		Stand-in		From date		To date		Copy assigned organiz	ati
0		Admin	~	ALICIA	~	4/28/2022	1	4/30/2022			

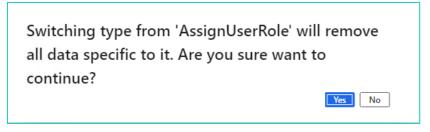
r) Create business risk

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 V	Area WHS
Status			
Priority Normal V	Status Open	Owner Admin	
Create business risk			
BUSINESS RISK Name Dmeo business risk	Area AssetLease	Mitigation Test	Status
Category Strategic V	Inherent risk	Residual risk	Response
SOD RULES + Add I Remove			<u> </u>
○ ○ Name ✓ Test 1	Organization Risk : Dreeo business risk		
	Diffeo busiless lisk		

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



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.

My view	Security Requests workflow configuration My view ~									
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 OStatus Owner Request	Jit +New ı́Delete ◯Workflow > Request Manage
Security requests My view ~	Security requests My view 🗠
Demo SR 1 Inactive workflow	Demo SR 1 Active workflow

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

	\circlearrowright Status \lor								
N	Open								
	Waiting								
	Review								
	Approved								
	Rejected								
	Canceled								
		I							

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.



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: <u>https://admin.microsoft.com/</u>

Security and complia	ance	e s	tudio parame	ter	5				
General	Gen	era	I setup for the pur	chas	ed licenses				
License count									
Data migration	0	С	License	Î	No of licenses				
bata migration	0		Activity users		15d				
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.

immary	License						
と 品	Usage	O License type	Actual use I	Licensed users c	users c Remaining us		
		Finance	11	10	-1		
Security	All users	HR	10	60	50		
lerge 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		
	rean members	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.

3.4.3 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.

Greate snapshot 🛛 🕉 Reset j	oins Advanced v	ew Show joined Export to Exce	N OPTIONS ,O			» () 👂
Security explorer: fo	ull view	ACCOUNTANT	DUTIES	PRIVILEGES	ENTRY POINTS	
-t= Pin users		st Unpin role	-t⊐ Pin duty	Havitzets	+ 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	d @ApplicationSuite_Localiz	a 😑 🖂 Abatemen	tCertificate_IN
RetailServiceAccount STAN	RetailService STAN	Accounting manager Accounting supervisor Accounts payable centralize Accounts payable cierk Accounts payable cierk Accounts payable manager Accounts payable manager	Enable EU sales list proces Enable financial reports ge	Account number enhanced account reference -ViewLe AccountingSourceExplorer AccountingSourceExplorer Action class settings maint	d 🖬 Accountan d I T Accountan V I Accountan ta I T Accountan	-

User ID	Name 🗸	Role name 🔹	Duty name	Privilege name
OSCAR	OSCAR	Accountant	Configure electronic fiscal document	@ApplicationSuite_LocalizationRTax25RegisterProfitEntityMaintain
RetailServiceAccount	RetailServiceAccount		Enable bank management process	@ApplicationSuite_LocalizationRTax25RegisterProfitEntityView
STAN	STAN		Enable electronic document exchange	Account number enhanced preview
			Enable escheatment processing for stale-dated accounts payable payments	account reference - ViewLedgerShowReferences:
			Enable EU sales list process	AccountingSourceExplorerView
			Enable financial reports generator	Action class settings maintain
			Enable fixed assets process	Action class settings view
			Enable Intrastat process	Action populate records task maintain
			Enable receipt electronic fiscal document process	Add category criterion group
			Enable sales taxes process	Add category criterion group vendor rating
			Enable tax accounting process	Add components from purchase order

3.4.4 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 Operat	ions Preview		D Search for a page					Merge scenarios into one
=	🖪 Audit 🛛 🛗 Optimiz	e OPTIONS 🔎							<u> </u>
									Name
	Security and	compliance studi	o						Description
	Summary Security								Description
	9 00 5T 1EC			<u>.</u>					
	_۶ ۴ 99	156	Requests	+ New 🖉 Edit 🖾 Match roles … More	Merge scenar	ios			
				✓ 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	

3.4.5 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.

		Security					
R_	$\overline{\mathbf{h}}$	Requests	Î	rge roles Duplicate role Lock	roles 🖧 Explore	Export Import	Mark active/inactive role
		Scenarios		Role name	License type	Role description	Locked
reate role	Import users	Scenarios		SCS_Customer service represent	Operations		\checkmark
		Users		SCS_CreateCustomer	Operations		
				-	Operations		~
		Roles	=	Save + New 🗊 Delete OP	TIONS D		~
		in the second se	7	Inactive security roles			🗸
		Duties		✓ Role name	Role (AOT name)		
				Auditor	AUDITPOLICYMAN		
		Segregation of duties		Cost accountant clerk		JTANTCLERK	

3.4.6 Recording steps to scenario.

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

≡	0	idit + New	🗓 Delete	🗄 Match roles	Merge scenarios	New from task recording	↑ Upload recording	Override permissions on roles	، م <u>ر</u>	» ()	p	Ü	ď	Х
7	S	CENARIO REC	ORDING STEPS											<
v ≕		General							Recording s	teps n	sadaiya	^		Related information
-		Scenario							Owner					d info
		Recording ste	ps						nsadaiya				L	matio
		Description										~	1	2
		Access require	d									^		
		+ Add ++ Ad	d module acc	ess 🗊 Remove	යි Explore									
		✓ Step numb	ier	Secur	able object	Securable type	Access level	Step description		File nan	ne			
		2		Defa	ultDashboard	Display	Full contro	ol Go to Default da	ashboard.	Record	ding ste	ips		
		3		custt	ablelistpage	Display	Full contro	Go to Accounts	receivable > Cu	Record	ding ste	ps		
		7		custt	ablelistpage	Display	Full contro	Go to All custon	ners.	Record	ding ste	ps		
		8		Cust	able	Display	Full contro	ol In the list, click t	he link in the sel	Record	ding ste	ps		

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.

3.4.7 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.

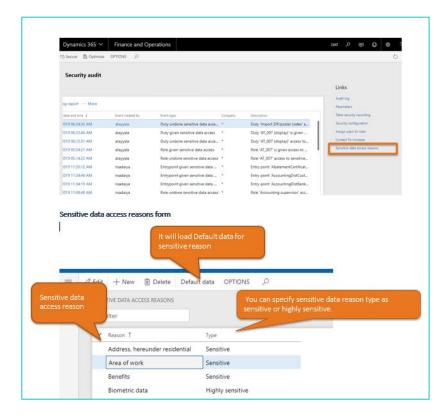
Edit 🕂 New 🗊 Delete	Match roles New from task rec	ording ↑ Upload recording	Override permissions on roles	OPTIONS /	0	•	1
SCENARIO							
General					Merged	scenario	nsa
Scenario					Owner		
Merged scenario					nsadaiya		
Description							
Access required							
+ Add + Add module ac	ccess 🛍 Remove යයි Explore						
✓ Step number	Securable object	Securable type	Access level	Step description		File	name
	AssetTableNew	Display	No access				
•	DSMArea	Display	Edit				
		ne to rolee					
	rride permissio		counts receivable				
Accounts re	eceivable centralized	Documents ac	counts receivable	_		I	
Accounts re Accounts re	eceivable centralized eceivable clerk	Documents ac	stomer invoice ev	·		l	
Accounts re Accounts re Accounts re	eceivable centralized eceivable clerk eceivable manager	Documents ac Documents cu Reviews custor	stomer invoice ev mer invoice proce			I	
Accounts re Accounts re Accounts re Accounts re	eceivable centralized eceivable clerk eceivable manager eceivable payments c	Documents ac Documents cu Reviews custor Documents ac	stomer invoice ev mer invoice proce counts receivable	·		I	
Accounts re Accounts re Accounts re Accounts re Accounts re	eceivable centralized eceivable clerk eceivable manager	Documents ac Documents cu Reviews custor Documents ac External user a	stomer invoice ev mer invoice proce counts receivable application for em	·		1	
Accounts re Accounts re Accounts re Accounts re Accounts re Applicant a Auditor	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external)	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····		1	
Accounts re Accounts re Accounts re Accounts re Accounts re	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external)	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable application for em	····			
Accounts re Accounts re Accounts re Accounts re Accounts re Applicant a Auditor	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····		•	
Accounts re Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····		•	
Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n et custom permiss o	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····		•	
Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n et custom permiss o	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····			
Accounts re Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····			
Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n et custom permiss o	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····			
Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n et custom permiss o C C C C C C C C C C C C C C C C C C	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager iions	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····		•	
Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n et custom permiss o et custom permiss o et custom permiss o unset of for end	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager iions	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····			
Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n et custom permiss o ERMISSIONS ead Unset Gre pdate Unset Gre	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager iions ant Deny ant Deny	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····			
Accounts re Accounts re Accounts re Accounts re Accounts re Applicant a Auditor Batch job n Batch job n et custom permiss o ERMISSIONS ead Unset Gre pdate Unset Gre reate	eceivable centralized eceivable clerk eceivable manager eceivable payments c anonymous (external) manager iions ant Deny ant Deny	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable opplication for em reviews audit poli	····			

3.4.8 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 snapsho	it 🧏 Reset pin	s Advanced	l view Show joined	OPTIONS	Q					00	۹ (0 O	с х
7	USERS		ROLES		DUTIES				PRIVILEGES			ENTRY PO		
	⊣¤ Pin users ···		⊣¤ Pin role		-⇔ Pin (luty	Give sensitive data access		-⇔ Pin privi	lege		HH PIN 6	entry poir	nt ···
	V Pin U	lser ID	✓ Pin	Role name 1	✓ Pin		Duty name ↑	Access to sensiti	✓ Pin	Privilege		✓ Pin	1	Entry po
	S	COBA		Accounts payable	~		A parameter that is used to gro			A param			-	🗹 Abaten
	• A	dmin					Access benefits workspace			Accept a			• •	🗈 Abaten
	• A	LICIA	-	Accounts payable			Access expense management w			Access Ł			• 0) Abaten
	• A	PRIL		Accounts receivabl			Access workforce management	~		Access (• 0) Abbrev
	• A	RNIE .	- 1	Accounts receivabl			Activate tax depreciation process	~		Access e			C	⊴ Accour
	 at 	tayyala 🛛 🔋					Activate, deactivate, update and			Access e			C	∃ Accour
	 a) 	xrunner					Add an existing performance jo			Access r			• •	⊐ Accour
	 B 	ENJAMIN	-				Add custom fields			Access v			• •	∃ Accour
	 B 	RAD					Application document entities			Account			C	∃ Accour
	 B 	ROOKE		AT_ AT_007			Approve absences	~		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.

	Dyr	nan	nics 365 🗸 🛛 Finance ar	nd Operations				DAT	ç	Ę	٢	۲	?
=	CRE	EATE I	ROLE										
	_												
	All	priv	vileges										
	Se	lect	t the privileges to be added	to the new role									
			ABLE PRIVILEGES				SELEC	TED PRIVILEGES					
		~	Privilege	Description	User license type		~	Privilege	Descript	ion			User I
		~	View accountant information		Team members	\rightarrow		Import KLADR abbreviations	Import	abbrevi	ations fr	om the K	. Oper
			View accounting distributions in		Team members	\leftarrow		Maintain accountant information					Oper
			Maintain accounting distributio		Operations	~		Maintain accounting distributio					Oper
			View accounting distributions in		Team members			T					
			View accounting distributions in		Team members								
			Create distributions for the tran		Operations		0	rivilação having					
			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		_						
	-										_		
								Back		Next		Cance	el .

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

)	yna	imics 365 🗸	Finance and Operat	ions		DAT	Q	Ð	٢
s	ave	+ New 🗊 De	elete Lock all roles OPTIC	ns ,0				*	đ
	Loc	ked security r	oles						
	~	Role name		Role (AOT name) 1					
	0	Business events sec	urity role 🛛 🗸 🗸	BUSINESSEVENTSSECURITYROLE					
		Accountant		LEDGERACCOUNTANT					
		Accounts payable p	ayments clerk	PAYMACCOUNTSPAYABLEPAYM					
		Accounts payable p	ositive payment clerk	PAYMPOSITIVEPAYMENTCLERK					

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

Dynan	mics 365 ∨ Finar	nce and Operations Acc	ounts receivable > Custom	ers > All customers		Dat ,0	Ē	()	3 ?	4
/ANAGE	OPTIONS D						~	a 🖗	0 5	×
MATCH	ROLES AND SENSITIVE DATA ACC	IESS								
Mate	ch roles									
	Menu item display	DSMScenario	Full control	No access	Not part of the se					
	Menu item display	DSMSecurityManagementTie		No access	Not part of the se	lected role.				
~	Menu item display	CustTableI istPage	Full control	View	✓					L.
	Menu item display	ForecastSalesTable	Full control	No access	Not part of the se	lected role.				L
L										l
Roles									^	
~	Role name	Role description	Matc User license type	Remaining user						
	Project manager	Documents the project foreca	st/ 50.00 Operations	59928						
	Production planner	Schedules and plans product	ions 50.00 Operations	59928					- 1	
	Sales manager	Reviews sales process perform	na 50.00 Operations	59928						
~	Sales representative	Documents sales events and r	es 25.00 Activity users	29986					-	
	Materials manager	Enables and reviews processe	s, 25.00 Operations	59928						
	Decision and the second second	Destance also see also at a set of a		0000						
s that gi	ive access to the securable	e objects that cannot be accessed w	ith the selected role.							^
Duty na	ame	Privilege name	Securable object type	Securable object	t A	ccess level		Duty li	cense type	
Enable	e the demand forecasting .	Maintain demand forecasts for i.	Menu item display	ForecastSales	Table F	ull control		Opera	ations	
	ain project budgets	View demand forecasts for item		ForecastSales	Table \	/iew		Activi	ty users	
Mainta	ain project forecasts	Maintain demand forecasts for i.	Menu item display	ForecastSales	Table F	ull control		Activi	ty users	
	e into project forecast stat			ForecastSales		/iew			members	
	ain authorization of adjust		Menu item display	ForecastSales	Table \	/iew		Opera	ations	
	ain authorization of adjust			ForecastSales		ull control		Opera		
	an an a'			e	÷					•
eges that	t give access to the secura	able objects that cannot be accesse	d with the selected role.							^
Privileo		Securable object type	Securable object	Access level	Privilege lice		Manu	item license		
	and forecasts for item N		orecastSalesTable	View	Team member		Team me		e type	-
	lemand forecasts for i N		orecastSalesTable	Full control	Activity users		Activity u			
u	remandrioreceato for fini in	reno nem display	or coastoales lable	Tur control	Picturey deels		, activity u			
									_	
ed dutie	es									^
Duty na	me	Privilege name	Securable object type	Securable object	: A	ccess level		Duty lic	ense type	
Inquire	into demand forecasts	View demand forecasts for item .	Menu item display	ForecastSales	lable V	iew		Opera	tions	
and the second sec	the demand forecasting	. Maintain demand forecasts for i	. Menu item display	ForecastSales		ull control		Opera		
Enable	in project budgets	View demand forecasts for item .		ForecastSales		iew			y users	
		in the second for the second s	a construction of the second	. er ceutoures						
Mainta		Maintain demand forecasts for i	Menu item display	ForecastSales1	Table E	ull control		Activit	v users	
Mainta Mainta	in project forecasts	Maintain demand forecasts for i	Menu item display	ForecastSales		ull control			y users	
Mainta Mainta Inquire		View demand forecasts for item .	Menu item display Menu item display Menu item display	ForecastSales ForecastSales ForecastSales	Fable V	ull control iew iew			members	

• 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.

	ce and Operations			DAT	> ■ ⊕
e 🖸 Optimize OPTIONS	Q				
urity audit					
Audit					
Security history	🔓 Audit log report 🛛 … More				
-	✓ Event date and time ↓	Event created by $ abla$	Event type	Company	Description
Role history	/ 3/13/2019 09:01:27 AM	nsadaiya	User undone sensitive data access	*	User ARNIE is unmarked as
	3/13/2019 09:00:29 AM	nsadaiya	Entrypoint given sensitive data access	*	Entry point 'AbbreviationCo
User history	3/13/2019 08:53:00 AM	nsadaiya	Entrypoint undone sensitive data access	*	Entry point 'AbbreviationCo
	3/13/2019 08:52:32 AM	nsadaiya	Privilege undone sensitive data access	*	Privilege 'Access expense m
Segregation of duties rules	3/13/2019 08:52:20 AM	nsadaiya	Privilege given sensitive data access	*	Privilege 'Action class settin
	3/13/2019 08:51:37 AM	nsadaiya	Duty given sensitive data access	*	Duty 'Access expense mana
Segregation of duties conflicts	3/13/2019 08:51:09 AM	nsadaiya	Duty undone sensitive data access	*	Duty 'Access expense mana
	3/12/2019 08:52:11 AM	nsadaiya	Role given sensitive data access	*	Role 'Accountant' is given a
		nsadaiya	Role undone sensitive data access	*	Role 'Accountant' access to

- Sensitive data access forms
 - 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	nics 365 🗸	Finance	e and Operations					DAT	Q	Đ
=	G Secure	🚯 Optimize	OPTIONS	Q							
	Secu	ity audit									
		Audit									
		Snapshots		Role name		License type	Role description	Locked			
		Roles – Sens access	sitive data	RapidValue Trans RapidValue user	lator	Team members Team members	Translates RapidValue m Shared role for all Rapid				
		Duties – Sen data access	nsitive	Budget clerk Budget contribut	or	Activity users Team members	Documents budget ever Enters and approves bu				
		Privileges – data access	Sensitive	Budget manager		Operations	Reviews budget process	perfor			
		Users – Sens access	sitive data	Users Duties	Privileges	History					
		Charts		12/12/2018 04	:17:44 AM	Event created by atayyala	Event type Role created	Company *	/	ų.	
							A. 100 1	-			

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.

III Dy	ynamics 365 V Finance	and Operations			DAT	م	Đ	٢	۲	?	4
≡ © S	ecure 🖺 Optimize OPTIONS	Q							C) 11	×
s	ecurity audit Audit										
	A Snapshots Roles - Sensitive data access Duties - Sensitive data access	Import ZIP/postal codes Approve advanced ledger entry view and maintain advanced ledg view advanced ledger entry pro Inquire about advance holder ac	view advanced ledger entry pro							1	[
	Privileges – Sensitive data access Users – Sensitive data access	Roles Privileges Segregation ✓ Role name Accounting manager	Role description Reviews accounting, customer i	User license type Operations							

• 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.

	Dynamie	cs 365 🗸 🛛 Financ	and Operations	DAT ,	j C	٢	۲	?	6
=	C Secure	Doptimize OPTIONS	م				(0	۲ X
		ty audit Audit							
		Snapshots	🖧 Explore						
			Privilege name Privilege identifier Privilege description Construct or procession						
		Roles – Sensitive data access	Maintain asset additions ASSETADDITIONMAINTAIN Create and update add-on item						
			Generate fixed asset additions r ASSETADDITIONMOGENERATE Generate a list of fixed assets an						
		Duties – Sensitive data access	View asset additions ASSETADDITIONVIEW View add-on items and improve						
		Privileges – Sensitive data access	Maintain depreciation settleme ASSETAD/RULE_PRETAXDEDUC View depreciation settlement ru ASSETAD/RULE_PRETAXDEDUC						
		Users – Sensitive data access	Roles Duties						_
			✓ Duty name Duty identifier ♡ Duty description	_					
		Charts	Maintain fixed assets ASSETFIXEDASSETSMAINTAIN Maintain fixed assets						

• 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.

Dynar	mics 365 🗸 🛛 Finance	and Operations			DAT 🔎		© ?
Secure	Optimize OPTIONS	<u>م</u>					0 5
Secu	rity audit						
	Audit						
	•	✓ User ID ↑	Name	Email	License type	Company	Person
	Snapshots	\$C0BA	\$COBA	\$C0BA@contosoax7.onmicrosof	Team members	dat	
	Roles – Sensitive data	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 – Sensitive						
	data access	Roles History					
	Users – Sensitive data access	✓ Role name	Role description	Level Comp	any accounts ID		
	access	Office integration	power user	3 *			
	Charts	System user	System role for all	users 2 *			

- Charts
 - o Number of security objects with access to sensitive data

	Dynamics	s 365 ∨ Finance ar	nd Operations								DAT	Q, T	¢	9 6	≥ ?	(ÿ)
=	🗟 Secure [ြာ Optimize OPTIONS ၂၀													0	c ×
	Security	y audit Audit														
		Snapshots	Number of se	curity obj	ects with a	ccess to :	ensitive	data \vee								
		snapsnots	Users													
		Roles – Sensitive data access	Roles													
		Duties – Sensitive data access	Duties													
		Privileges – Sensitive data access	Privileges													
		Users – Sensitive data access	Entry points													
		Charts	Ok	2k	4k	6k mber of securi	8k ty objects	10k	12k	14k						

o Number of users with access to sensitive data per organization



o Number of roles per user with access to sensitive data

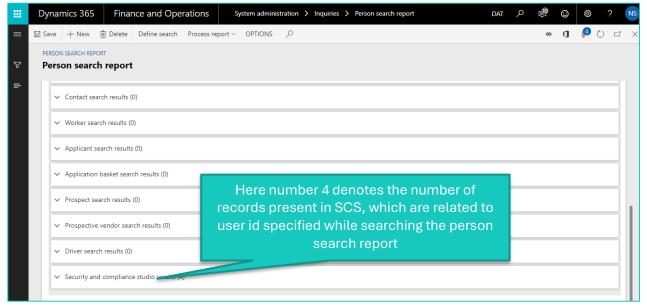
	Dynamics 365 Fi	inance and Operations DAT P (2) (2) (2) (2)	NS
≡	ං Secure 🔂 Optimize ර	۵ C anotted	×
	Security audit Audit	u	in
	Snapshots	Number of roles per user with access to sensitive data \checkmark	udi ara
	Roles – Sensitive data access	BAD CHARLE St	ablı ecu ssiş
	Duties – Sensitive data access	icretu JREMVY	oni ens
	Privileges – Sensitive data access	MANUELO MANOY PRINA	
	Users – Sensitive data access	Nishna	
	Charts	TONY	

o Reasons to give roles access to sensitive data

ynamics 365 Finan	nce and Operations DAT , P 👳	© @ ? (
Secure 📴 Optimize OPTIC	Q and	0 🖬
Security audit		
Audit		U
	Reasons to give roles access to sensitive data $\!$	A
Snapshots		Pa Ta
Roles – Sensitive data access	150	Si A
Duties – Sensitive data access	100	c
Privileges – Sensitive data access	50	
Users – Sensitive data access		
Charts	Address, here under residential Address, here residential Benefits Number of roles with 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/devitpro/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.



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.

SECUR	RITY REQUESTS									
~	Include	Owner		Request		Descript	tion	Туре		Status
~	✓	nsadaiya		Add accountant	role			General		Open
STAN	D IN									
~	Include	Stand-in	User ID		From date		To date	Copy assigned organizations	Closed	
~	 Image: A set of the set of the	ALICIA					2/20/2010	true	No	
		AUCIA	nsadaiy	a	3/14/2019		3/30/2019	ute	NO	
	ARIOS	AUCIA	nsadaiy	a	3/14/2019		3/30/2019	uue	NO	
		AUCIA	nsadaiy	Description	3/14/2019	Owner	3/30/2019	Created date and time	NO	
SCEN	ARIOS				3/14/2019	Owner nsadaij			NO	
scen⊎ ✓	ARIOS Include	Scenario Match roles and sensitive			3/14/2019			Created date and time	NO	
scen⊎ ✓	AREOS Include	Scenario Match roles and sensitive			3/14/2019		ya	Created date and time	NO	
SCENU V TABLE	ARBOS Include	Scenario Match roles and sensitive		Description		nsadaij	ya	Created date and time 3/12/2019 05:53:05 AM	NO	



3.4.9 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.

Mate	ched 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.

SCS		Description
acurity objects t	hat are include	ad into the new duty
	hat are include	ed into the new duty
,∽ Filter		ed into the new duty
r	hat are include	ed into the new duty
,∽ Filter	Label	ed into the new duty ant_reduced (display)

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

3.4.10 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	

3.4.11 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.

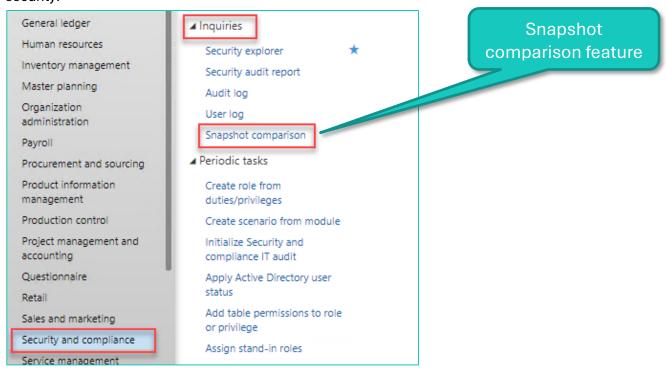




Fig 1. Snapshot comparison path

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

Dyr	namics 365 🗸 🛛 Finar	nce and Operations Se	curity and compliant	ce > Inquiries > Snapshot co	mpariso	n	
🗟 Sav	MANAGE OPTIONS	م					
Full o	ARE VIEW vare selected Show all object Advanced view 1. 2.						
	napshot compariso TER Entry Point Privilege Duty 3. Role User WERRSMORSHOTS st snapshot	n			Se 3	cond snapshot	
	/ Name	User license type	Compared	Observation		Name	User license type
	Action graph	Operations	Yes	3 modifications found		Demo privilege 1	Operations
	DSMAreaEntityMaintain	None	Yes	1 modifications found		Demo privilege 2	Operations
	Florin privilege 2	None	Yes	0 modifications found		Maintain bar codes	Operations
5.							
	FFERENCES	Value from first snapshot		om second snapshot			
-	Property	value from first snapshot				-	
6.	Entry point added Entry point added	-		uditLogInit ergeRoles			
-	Entry point added			andInClass			
		1					

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)

IPARE VIEW Appare selected compare Advanced view							
Snapshot comparison							
FILTER Select security object type							
Entry Point							
Privilege							
Duty							
🗇 Role							
-							
🔵 User							
COMPARE SNAPSHOTS				Serie	and snanshot		
				Seco 3	ond snapshot		
COMPARE SNAPSHOTS	User license type	Compared	Observation			User license type	
COMPARE SNAPSHOTS	User license type Operations	Compared Yes	Observation 3 modifications found	3		User license type Operations	
COMPARE SNAPSHOTS First snapshot 2 Name				3	Name		
COMPARE SNAPSHOTS First snapshot 2 V Name Action graph	Operations	Yes	3 modifications found	3	Name Demo privilege 1	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

Dynamics 365 🗸 🗌	Finance and C	perations Security	and compliant	ce 🔰 Inquiries 🗲 Snapshot c	ompa	irison		
ave MANAGE OPT	ions 🔎							
MPARE VIEW npare selected Show	changes only nced view							
Snapshot comp FILTER Select security object type Entry Point Privilege								
Duty Role User COMPARE SNAPSHOTS First snapshot 2	7					Seco 3	nd snapshot	
Role User COMPARE SNAPSHOTS First snapshot]	User license type	Compared	Observation		3		User license type
Role User COMPARE SNAPSHOTS First snapshot 2		User license type None	Compared Yes	Observation 0 modifications found		3	~	User license type Operations
Role User COMPARE SNAPSHOTS First snapshot 2 V Name 1	gs maintain					3	Name î	
Role User COMPARE SNAPSHOTS First snapshot 2 V Name 1 Action class setting	gs maintain	None	Yes	0 modifications found		3	Name 1 Delete write-off factors	Operations
Role User COMPARE SNAPSHOTS First snapshot 2 V Name 1 Action class setting Action class setting	gs maintain gs view	None	Yes Yes	0 modifications found 0 modifications found	0	3	Name T Delete write-off factors Demand Forecasting external API se	Operations None
Role User compare snapshot 2 V Name 1 Action class setting Action graph	gs maintain gs view cords task maint	None None Operations	Yes Yes Yes	0 modifications found 0 modifications found 3 modifications found		3	Name 1 Delete write-off factors Demand Forecasting external API se Demo privilege 1	Operations None Operations
Role User compare snapshot 2 Name 1 Action class setting Action class setting Action praph Action populate re	gs maintain gs view ecords task maint ions	None None Operations None	Yes Yes Yes Yes	0 modifications found 0 modifications found 3 modifications found 0 modifications found		3	Name 1 Delete write-off factors Demand Forecasting external API se Demo privilege 1 Demo privilege 2	Operations Operations Operations Operations

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

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)

Dynamics 365 ✓ Finance and Ope	erations Security and compliance	e > Inquiries > Snapshot com	parison				
Save MANAGE OPTIONS	· · · · ·						
COMPARE VIEW Compare selected Show changes only Full compare Simple view							
Snapshot comparison FITER Sect searthy abject type Entry Point Privilege Duty Role User COMPARE SNAPSHOTS First magnot			1		Second snapshot		
✓ Identifier	Name 1	User license type	Compared	Observation	✓ Identifier	Name 1	User license type
FORECASTPOSITIONSBYBUDGETPLANG.	A parameter that is used to group	Team members	Yes	0 modifications found	VENDPROSPECTIVEVENDORDATAA		leam members
PURCHRFQFORMLETTER_ACCEPTPROCE.	Accept a request for quotation	Activity users	Yes	0 modifications found		Deny fixed compensation change re	Team members
HCMBENEFITWORKSPACE	Access benefits workspace	Team members	Yes	0 modifications found	TMSINVOICEAPPROVALDENYPROC		Team members
HCMCOMPENSATIONWORKSPACE	Access compensation management.	Operations	Yes	0 modifications found			eam members
TRVEXPENSEADMINANALYTICS	Access expense administrator analy.	Operations	Yes	0 modifications found		· ·	Feam members
TRVEXPENSEWORKSPACE	Access expense management work	Team members	Yes	0 modifications found			Feam members
HCMRECRUITMENTWORKSPACE	Access recruitment management w	Team members	Yes	0 modifications found	HCMWORKERACTIONHIREWFAPPR	Deny worker actions by using a wor	Feam members
DIFFERENCES					I DIMENSIOPMENTDEDI OVMANIACE	DI	

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
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	-

3.4.12 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 au	udit	Audit							
Summary		Audit							
• •	2 =-	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 of	created (from AOT)	
IUCKCU	Noie changes		5/15/2018 05:19:58 AM	Admin	Entry point deleted	dat	Entry point Active directory users delete	ed (from AOT)	
x ²	D	User history	5/15/2018 05:18:30 AM	Admin	Privilege modified	dat	Privilege Maintain Dynamic Security Ma	anagement IT Audit modified (from	
× <u></u>	<u> </u>		5/15/2018 05:18:19 AM	Admin	Privilege modified	dat	Privilege Florin privilege 1 modified (fro	om AOT) changes	
		Segregation of duties rules	✓ 5/15/2018 05:18:16 AM	Admin	Privilege modified	dat	Privilege DSMParametersEntityView mo	odified (from AOT) made	
User changes	Stand-ins		5/15/2018 05:18:16 AM	Admin	Privilege created	dat	Privilege PrivielgeFromAOT created (fro		
		Segregation of	5/15/2018 05:18:16 AM	Admin	Privilege created	dat	Privilege FlorinPrivilegeUITest created (f	from AOT)	
A	Ro	duties conflicts	5/15/2018 05:16:43 AM	Admin	Privilege modified	dat	Privilege Apply action modified (from A	(OT)	
		Stand-ins	5/15/2018 05:14:45 AM	Admin	Duty modified	dat	Duty Maintain security recording modified (from 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 AC	от)	
	D	Data security	5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty FlorinDutyUITest created (from AC	(TC	
₿	格	Azure AD domains	5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty Duty created from AOT created (fr	rom AOT)	
		Azure AD domains	5/15/2018 05:14:04 AM	Admin	Role modified	dat	Role Full read access modified (from AC	ЭТ)	
Print audit report	Security explorer		5/15/2018 05:14:01 AM	Admin	Role created	dat	Role Role test from AOT created (from a	AOT)	
		Snapshots	5/15/2018 05:14:01 AM	Admin	Role modified	dat	Role Florin Role 1 modified (from AOT)		
		Charts	5/15/2018 05:13:52 AM	Admin	Role created	dat	Role FlorinRoleUITest created (from AO	T)	
		Charts	5/15/2018 05:13:15 AM	Admin	Role modified	dat	Role Chief executive officer modified (fr	rom 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	changes	
			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).

3.4.13 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.

Select the entry point types to be added to the target role. For eadded to the target role.	Create single privilege option	privilege is
CREATE SINGLE PRIVILEGE		
Yes Merged Accountin V		
ACTION MENU ITEMS		
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 duty. For each selected privilege, a duty is created. Instead of the privilege, the created duty is added	i to the target role.
CREATE DUTY		
Yes 💿		
CREATE SINGLE DUTY		
Yes Merged Accountin V		
ENABLED DUTY NAME		
ACTION PRIVILEGES		
DISPLAY PRIVILEGES		
OUTPUT PRIVILEGES		
TABLE PRIVILEGES		



3.4.14 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.

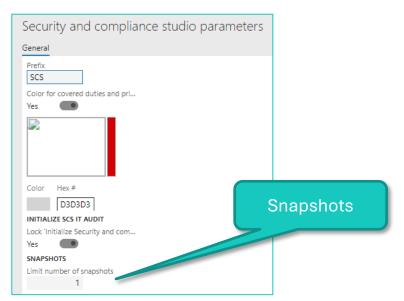
Dynam	ics 365 🗸 🛛 Finance and	Operations								1
Save	+ New 📋 Delete 🛛 Match ı	oles New from tas	sk recording	OPTIONS P			Ar	ea		
PERSONAL	ZE PAGE OPTIONS		EDIT SHARE				WH	ICH MODULE?		
	en for editing Security diagnosti	cs Record info	Read mode Get a link V				\checkmark	Area î		
		ort Change view 🗸	Revert					Accounts payable		
Add to wo	rkspace 🗸							Accounts receivable	e	
								Audit workbench		
SCENA	RIO							Budgeting		
Gene	eral			Add mod	ile	ARScenario vsingh		Cash and bank mar	nagement	
				/ laa moa		Owner		Common		
Scer	ario Scenario					vsingh		Consolidations		
								Cost accounting		
Desc	ription							Cost management Credit and collection		
								Demo data	ons	
Acce	ss required							Expense managem	ant	
	Add + Add module access							Fiscal books	ent	
								Fixed assets		
~	Securable object	Securable object type		File	Remark			Fleet management		
	CustomerInvoiceWorkspace	Menu item display	View 🗸					General ledger		
	CustPaymentWorkspace	Menu item display	View				No	access		
	CustTableListPage	Menu item display	View				Vie	2W	ent	
	-		View				Ed	it		
	CustTableHoldListPage	Menu item display						eate	istration	
	CustTablePastDueListPage	Menu item display	View					rrection		1
	MCRCustUnmergeWorkbench	Menu item display	View					ll control		
	COLUMN CONTRACT	NALING SECTION	A/:					access V]	
							Ц	Create request		
Files								0	lk	Cancel

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.

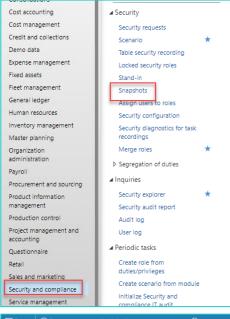
ATCHIN	IG	CREATE ROLE			SEGREGATION	OF DUT	IES VIEW	ASSIG	N TO USER	
		te role from dutie licate role			Simple Assig Advanced		gn users to role			
	^{ENARIO} tch roles									
Secu	rable objects									
~	Securable object type Se		ecurable object		Required access N		Maximum access on role		Remark	
	Menu item display Cu		CustomerInvoiceWorkspace		View		View			
	Menu item display Cu		CustPaymentWorkspace		View		View			
	Security roles match degree			dro o	liew	Full control		~		
	Security	rotes mai	cnue	gree	/iew	V	iew	~		
_	Menu item display Cu		ustic ige		√iew	View		~	/	
	Menu item display M		MCRCustUnme h		View	w Noac			Not part of the selected role	
	Menu item display Sa		SalesTableListPage		View	View		~		
Role	s									
~	Role name	R	ole descriptio	n	Match de	gree 1	User license type		Remaining user lice	
	Accounts receivable manager		Reviews customer invoice pro		o 72.81		Operations		59933	
	Accounting manager		Reviews accounting, custome		68.66		Operations		59933	
	Accounts receivable clerk		Documents customer invoice		68.66		o Operations		59933	
	Accountant		Documents accounting event		60.37		Operations		59933	
	Accounting supervisor		Reviews accounting process p		57.14 C		Operations		59933	
	Collections manager		Reviews collections process p		53.92 (Operations		59933	
	concetions manage	er R	eviews colle	ctions process p.		33.92	operations			

3.4.15 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 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.



 \blacksquare Save \bigcirc Set up automatic deletion OPTIONS \checkmark

Snapshots

♀ Filter					
Version	Name	Description	Created by	Created date and time	Protected
1	Generated from batch, version 1 on 2/13/2018 03:55:37 am	Automatically create from batch job on 2/13/2018	Admin	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.

STAEDEAN confidential and proprietary information for internal user only, No unauthorized distribution permitted, © STAEDEAN



"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'.

3.4.16 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.

CREATE ROLE												
All 1 2												
All duties												
Select duties to be add	led to the ne	ew role										
AVAILABLE DUTIES		- Tone						FIF	CTED DUTIES			
✓ Duty		Description		User license type		٦	[Descrip	tion	User license type
Maintain Absorptio	n Casta	Description		Operations			\rightarrow	*	Inquire into Absorption Cost		2001	Team members
							7				ad as formulation of south a	
Import ZIP/postal c				Operations	-1		\leftarrow		Inquire into purchase agreen	Kespo	nd to inquiries about p	Team members
Approve advanced	-		lvanced ledger ent	· · /				-				
view and maintain a	advanced I	View and m	naintain advanced I	Team members	_							
view advanced ledg	er entry p	view advan	ced ledger entry p	Team members	R	lol	eli	İC	ense type			
					b	oet	ore	Ð	you finish			
CREATE ROLE												
					-							
Summary												
Review the selected role setup	. Click Finish to	create the rol										
The resulting role will have the u	iser license type	Operations										
Role name	Role description											
SCS_NewRole	SCS_NewRole											
Selected privileges									Selected duties			
Privilege name	Description		License type.						Duty name		Description	License type.
Import KLADR abbreviations View accounting distributions	Import abbreviat	tions from th	Operations Team Members						Inquire into Abso		Respond to inquiries about p	Team Members Team Members
view accounting distributions	l		learn Mempers						Inquire into purc	ase agreem	Respond to inquiries about p	learn intempers

3.4.17 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.

Security diagn	ostics		Security explorer icon
This is the list of security	objects that grant the active security entry po	int.	on all D365FOE forms
Add roles to user	Show object identifiers 🖧 Explore		
,⊃ Filter			
✓ Object type	Label		
Role	SCSCollections agent		
Role	Auditor		
✓ Role	Collections agent		
Role	Collections manager		
Role	Chief executive officer		

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



ebuild o	lata 🕺	Reset pins	Simple	e view Show join	ed OPT	tions 🔎												000
Secu	rity ev	plorer:	full vi	iew														
USERS	ny cz	spiorer.	i cani vi		COLLEC	TIONS AGENT		DUT	165		PRIVI	ILEGES			ENTRY POL	NTS		
-ta Pin	LIGATE				st Hee	pin role			Pin duty			in privilege			-t= Pin en	to point		
					74 019													
		D Î Name		ghest license typ		Role name 1	License type		Duty name 1	License type		Privilege		License type	✓	Entry point (AOT name) 1	Access right	Entry point type
	ARNIE			perations	-12 .	 Collections ager 	t Operations		Collections workspace	Team members			e interest notes	Operations		□ AccountingDistCustFreeInvoice		Menu item dis
	Conni			perations					Inquire into bill of exchange s.	Team members		 Cancel ci 	ollection letters	Operations		AccountingDistCustInvJour	View	Menu item di
	OSCA	R OSCA	R Op	perations					 Inquire into collections status 	Operations		 Cancel in 	nterest notes	Operations		☐ AccountingDistMarkupTransInv	View	Menu item di
	SARA	SARA	Op	perations					Inquire into credit card proce-	 Team members 		CashDisc	countEntityView	None		☐ AccountingDistMarkupTransPO	View	Menu item di
									Inquire into customer invoice	Activity users		Change t	transaction collection.	Operations		AccountingDistMarkupTransR	View	Menu item di
									Inquire into customer master	Team members		Change/	edit customer transa	. Activity users		☐ AccountingDistPurchTable	View	Menu item di
									 Inquire into customer payme 	Activity users		Change/	edit customer transa	. Operations		AccountingDistributions	View	Menu item di
									Inquire into customer referen.			Change/	edit customer transa	Operations		☐ AccountingDistributionsDocu	View	Menu item di
									Maintain activities	Team members		Correct i	nterest codes	Team members		AccountingDistTaxTransTmp	View	Menu item di
									 Maintain collections transacti. 	_ Operations		Create a	customer record fro	Operations		☐ AccountingDistVendEditInvDe	View	Menu item di
									 Maintain contacts 	Activity users		Create a	customer record fro	Operations		AccountingDistVendEditInvHdr	View	Menu item d
									 Maintain customer master 	Operations		Create cr	ollection letters	Team members		□ ActivitiesMain	View	Menu item d
									 Maintain financial period clos. 			Creating	a customer from pro.	Operations		□ ActivitiesMain	Full control	Menu item d
									 Maintain periodic settlement . 				nceGenerate_CN	Team members		ActivitiesMainBasic	View	Menu item d
									Manage customer credit and .				tomerGroupEntityView			□ ActivitiesMainBasic	Full control	Menu item di
									 View sensitive bank account i. 				ctDebitMandateEntit.			□ Activity/ViewRecord	View	Menu item di

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

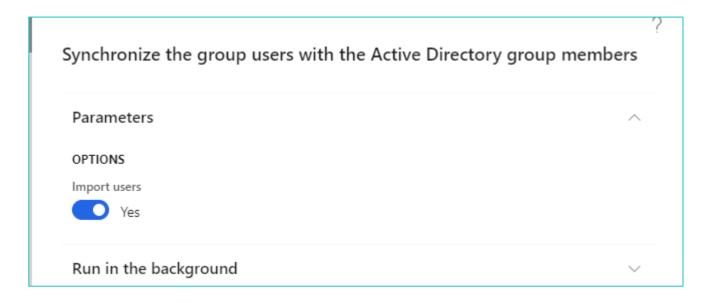
You now have an option to create duties along with the privileges while using the "Merge roles" feature. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.).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

🛞 Roles 'Accounting manager' and 'Accoun	tant' are in violation of segrega	tion of duties	rule '	New Segregation of duties rule2':	
MERGE ROLES					
	to. ock target role? es			SOD viola	tions
Select the roles to merge from.					
AVAILABLE ROLES			SEL	ECTED ROLES	
✓ Available roles			~	Selected roles	
Accounting supervisor		\rightarrow		Accounting manager	
Accounts payable centralized p	ayments clerk			Accountant	
Accounts payable clerk					
Accounts payable manager					
Accounts payable payments cle	erk				
ENABLED	PRIVILEGE NAME				
ACTION MENU ITEMS	SCS_AccountingSuperU	ser 🗸			
DISPLAY MENU ITEMS	SCS_AccountingSuperU	ser 🗸			
OUTPUT MENU ITEMS	SCS_AccountingSuperU				
CREATE DUTY	Create duty	′ (
Yes					
ENABLED	DUTY NAME				
ACTION PRIVILEGES	SCS_AccountingSuperUse	er 🗸			
DISPLAY PRIVILEGES	SCS_AccountingSuperUse				
	SCS_AccountingSuperUse				
TABLE PRIVILEGES	SCS_AccountingSuperUse				



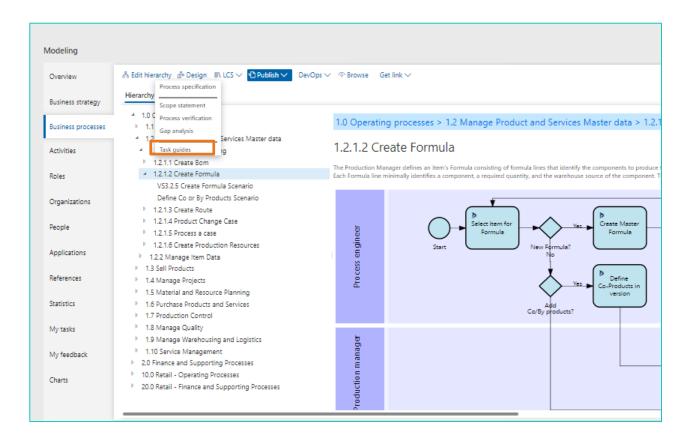
This is very useful for offline analysis and drill down of the required security setup in a company or department. We added a new small feature to our Azure AD group synchronization job. On the dialog of the Synchronize the group users with the Active Directory group members, we introduced a new parameter 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.



3.4.20 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.

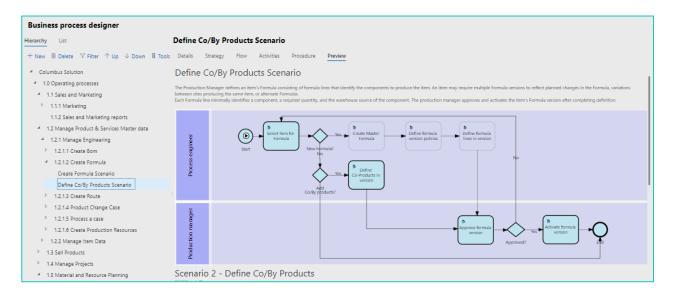


Figure: Scenario-Procedure activity based modelling



the	e left pane, select steps. In the right pane	select or create the activity to link as sub a	ctivity to the selecte	ed steps.		Flow activities Activities
9	Unlink sub activities					
~		Step	Exists in flow	Sub activity	Title	
	1.1	Go to Product information man		Select item for Formula		es an item's Formula consisting of formula lines that identify the components to produce the item. An ite
	1.2	In the list, find and select the de		Select item for Formula		entifies a component, a required quantity, and the warehouse source of the component. The production
	2.1	Click Formula versions.		Define Co-Products in version		T
	2.2	On the Action Pane, click Formu		Define Co-Products in version		Select item for set yes - Create Master - Define formula
	2.3	Click Co-products.		Define Co-Products in version		Select item for Formula
	2.4	Click New.		Define Co-Products in version		Start New Formula?
	2.5	In the list, mark the selected row.		Define Co-Products in version		
	2.6	In the Item number field, enter		Define Co-Products in version		Yes Co-Products in version
	2.7	In the Production type field, sele		Define Co-Products in version		Add Co/By products?
	2.8	In the Warehouse field, type a v		Define Co-Products in version		Co/ey products?
	2.9	In the Quantity field, enter a nu		Define Co-Products in version		
	2.10	In the By-product cost allocatio		Define Co-Products in version		
	2.11	Click Save.		Define Co-Products in version		
	2.12	Click New.		Define Co-Products in version		
	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	In the Co. product cost allocatio		Dafine Co. Products in version		

Figure: Scenario-Procedure activity based modelling 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 mana	agement		
Summary		Security	
_.	343	Requests	+ New C Edit 🖸 Match roles … More Merge scenarios Upload RV scenario
Users F	Roles	Scenarios	Scenario î 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.

3.4.21 Enhanced Segregation of Duties

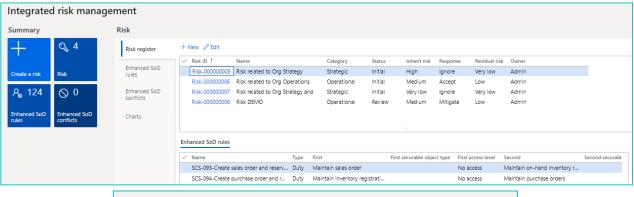
In standard D365FSC, we can only define SoD rules at duty level which is rarely useful. In SCS, with this release users can now define SoD rulesets at any level (Duty, Privilege or Entry Point) in the security hierarchy in D365FSC. This makes this feature more practical and extremely useful for customers 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 fraud.



	✓ Name ↑	Туре	First	First securab	le object type	First access level	Second
Enhanced SoD rules	Demo rule for Entry points	Entry point	AccountingDistVe	endEditInvHdr Menu item	display	Create	AdvancedLedgerEntryDateDr
	Match role test - ep 1	Entry point	AuditPolicyCaseG	iroup Menu item	display	Full control	ACOJournalPost_BR
nhanced SoD	Match roles test - duty	Duty	Maintain Absorpt	tion Costs		No access	Maintain audit policies
onflicts	Match roles test - duty 2	Duty	Maintain audit po	olicies		No access	Maintain Absorption Costs
harts	Match roles test - ep 2	Entry point	ACOJournalPost_	BR Menu item a	action	Full control	AuditPolicyCaseGroup
and to	Match roles test - ep 3	Entry point	DSMSecurityRequ	uestPriorityH Menu item a	action	Correction	ACOJournalPost_BR
	Match roles test - ep 4	Entry point	DSMMultiSelectR	loleSetup Menu item	display	Full control	DSMSecurityRequestPriorityH.
	Match roles test - priv 1	Privilege	Maintain case gro	ouping criteria		No access	Maintain Absorption Costs
	Match roles test - priv 2	Privilege	Maintain Absorpt	tion Costs		No access	Maintain case grouping criteri
	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	Ignore	Very low	Admin

3.4.22 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" capability within SCS enabling Organizations to register, assess, monitor, mitigate and close it.







3.4.23 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 with better handling of internal controls.

3.4.24 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



3.4.25 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.

3.4.26 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

Security I	managemen	t					
Summary		Security					
_ജ ^മ 109	E 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
			Purchase order form access	Modify user	Normal	Open	Admin
	ଚ	Users	Create role for vendor access	General	Normal	Completed	Admin
			Add accountant role	Assign role to user	High	Completed	Admin
New security		Groups	Credit note on purchase order	General	Normal	Open	Admin
request	Merge roles		Customer	General	Normal	Approved	Admin
		Roles	Provide customer access	General	High	Open	abahlman
品	Ę		Create Customer Permission required for Eric	Create role	Normal	Open	vsingh
		Duties	something	Add stand-in	High	Waiting	andre.adcalavon
Security explorer	Security configuration		SCS	General	Normal	Open	abahlman
explorer	conliguration	Segregation of duties rules	Customer access	General	Normal	Approved	nsadaiya
0			Customer_full_access	General	Normal	Approved	nsadaiya
\frown	⊻	Segregation of duties conflicts					
Create role	Import users	Stand-ins					

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

3.4.27 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.

Security a	ind complian	ce studio					
Summary		Security					
_ജ ം 87	362	Requests	Edit Import groups Sy	nchronize More			
Users	Roles	Scenarios	AAD group id SCSUser SCSUser1	AAD group name SCS-TEST0365 SCS-TSTGROUP1			
+	୍ଦ	Users	SCSUser2	SCS-TSTGROUP1			
New security request	Merge roles	AAD groups					
ቆ	ស៊ែះ	Roles Duties					
Security explorer	Security configuration	Segregation of	Users				
0		duties rules	✓ ID ↑ ♥	Name	Email		Enabled
×,	⊻	Segregation of duties conflicts	vsingh	Vivek Singh		ase.onmicros	true
Create role	Import users	Stand-ins		_			

urity								
Requests	+ New 🖉 Edit	+ Import 음 Explore	··· More					
	✓ User ID ↑ Nam	ne Email		License type	С	ompany	Person	
Scenarios	TRICIA	TRICIA	TRI			Operations		USS
	VINCE	VINCE	VIN			Operations		USN
Users	✓ vsingh	Vivek Singh	vsir			Operations		USN
	Wayne	Wayne	Wa		÷	Operations		USM
AAD groups	voichiroo	VOICHIROO	voichu	roomcontosoay / onm	icro	Onerations		11551
Roles	Roles History	Login date and time	AAD group					
	 AAD group id 	AAD group na	me					
Duties	SCSUser	SCS-TEST036	55					
Segregation of duties rules	SCSUser1	SCS-TSTGRC	UUP1					

3.4.28 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 a compliance perspective to be aware of any SoD violation proactively.

			OAssign stand-in roles	Validate So		tions 🔎	
	Stan	d-in					
	2	Filter					
	~	User ID ↑	Stand-in	From	date	To date	Copy assigned organizations
	\checkmark	ALICIA	APRIL	12/13	/2018	12/13/2018	0 🗸
		APRIL	dtijssen	1/19/	2019	1/20/2019	\checkmark
		atayyala	acardol	10/21	/2019	10/31/2019	\checkmark
		BENJAMIN	CHARLIE	10/3/	2019	10/11/2019	
		CHARLIE	BENJAMIN	10/3/	2019	10/17/2019	
		dtijssen	Admin	1/21/	2019	1/22/2019	\checkmark
		JACOB	JEREMYL	10/22	/2019	10/31/2019	
		JACOB	nsadaiya	10/22	/2019	10/24/2019	\checkmark
		nsadaiya	ALICIA	3/14/	2019	3/30/2019	\checkmark
		OSCAR	JULIA	10/22	/2019	10/31/2019	\checkmark
		🔋 Delete 🛛 💍 Assign stand-in	n roles Validate SoD rules Options	Q			
+	New						
		R's roles to JULIA are in violation of S	oD rules: 'SCS-083-Release production order and	I move inventory': The role	Accounts receivable payment	its clerk' contains duty 'Maintain customer p	payments' and the role 'Accountant' contains duty 'Enable bank manageme
gnmen Star	nd-in	R's roles to JULIA are in violation of S	ioD rules: 'SCS-083-Release production order and	d move inventory': The role	'Accounts receivable paymen	its clerk' contains duty 'Maintain customer p	bayments' and the role 'Accountant' contains duty 'Enable bank manageme
gnmen Star	t of OSCA	R's roles to JULIA are in violation of S	ioD rules: 'SCS-083-Release production order and	d move inventory': The role	'Accounts receivable paymer	its clerk' contains duty 'Maintain customer p	sayments' and the role 'Accountant' contains duty 'Enable bank manageme
gnmen Star	nd-in P Filter	D ↑ Stand-in	From date	To date	Copy assigned	ts clerk' contains duty 'Maintain customer p	ayments' and the role 'Accountant' contains duty 'Enable bank manageme
star	nd-in P Filter V User II ALICI.	D T Stand-in A APRIL	From date 12/13/2018	To date 12/13/2018	Copy assigned	ts clerk' contains duty 'Maintain customer p	ayments' and the role 'Accountant' contains duty Trable bank manageme
star	nd-in P Filter V User II ALICI. APRIL	D † Stand-in A APRIL - dtijssen	From date 12/13/2018 1/19/2019	To date 12/13/2018 1/20/2019	Copy assigned	ts clerk' contains duty 'Maintain customer y	ayments' and the role 'Accountant' contains duty Trable bank manageme
gnmen Star	nd-in P Filter V User II ALICI.	D † Stand-in A APRIL - dtijssen ala acardol	From date 12/13/2018	To date 12/13/2018	Copy assigned	ts clerk' contains duty "Maintain customer j	ayments' and the role 'Accountant' contains duty Trable bank manageme
gnmen Star	nd-in P Filter V User II ALICI. APRIL atayy	D T Stand-in A APRIL - dtijssen ala acardol AMIN CHARLIE	From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019	To date 12/13/2018 1/20/2019 10/31/2019	Copy assigned	ts clerk' contains duty "Maintain customer j	ayments' and the role 'Accountant' contains duty Trable bank manageme
star	nd-in P Filter V User II ALICI. APRIL atayy BENJ/	D T Stand-in A APRIL - dtijsen ala acardol AMIN CHARLIE LIE BENJAMIN	From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019	To date 12/13/2018 1/20/2019 10/31/2019 10/11/2019	Copy assigned	ts clerk' contains duty "Maintain customer j	ayments' and the role 'Accountant' contains duty Trable bank manageme
gnmen Star	nd-in Filter User II ALICI. APRIL atayy BENJ/ CHAF	D 7 Stand-In A APRIL - dtijssen ala acardol AMIN CHARLIE ULE BENJAMIN en Admin	From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019 4 10/3/2019	To date 12/13/2018 1/20/2019 10/31/2019 10/11/2019 10/11/2019 10/17/2019	Copy assigned	ts clerk' contains duty 'Maintain customer j	ayments' and the role 'Accountant' contains duty 'Enable bank manageme
gnmen Star	tt of OSCA nd-in Filter User II ALICI. APRIL atayy BENJ CHAF dtijss	D T Stand-In A APRIL - dtijssen ala acardol AMIN CHARLIE BENJAMIN en Admin B JEREMYL	From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019 1/21/2019 1/21/2019	To date 12/13/2018 1/20/2019 10/31/2019 10/11/2019 10/17/2019 1/22/2019	Copy assigned	ts clerk' contains duty 'Maintain customer j	ayments' and the role 'Accountant' contains duty 'Enable bank manageme

3.4.29 Chart to give an overview of the 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.

ummary		Security							
_ജ ^{മ,} 103	a 175	Requests							
			✓ User ID ↑	Name	Email		License type	Company	Person
Users	Roles	Scenarios	abahlman	Ard Bahlman	al		Operations	DAT	
1		Users	acardol andre.adcalavon	Adri Cardol André Arnaud de Calavon	a: ai	t.com	Activity users Operations	DAT	
	ତ		atayyala	Anil Kumar Tayyala (ATAYY.TI)	at	LCOM	Team members	dat	
New security		AAD groups	dvschie	David van Schie (DVSCH.TI)	d		Operations	dat	
request	Merge roles		evhofwegen	Eric van Hofwegen	e	m	Operations	DAT	
	<u>~</u> ~	Roles	nsadaiya	Nitish Sadaiya (NSADA.TI)	n:		Operations	usmf	
8	ૼૢૼૺૺ૱	Duties	Pradeep.Bapna	Pradeep Kumar Bapna	Pi	com	Operations	DAT	
Security	Security	Duties	SCS-TSTGroup1 SCS-TSTGroup2	SCS-TSTGROUP1 SCS-TSTGROUP2			Operations Operations	DAT DAT	
Security explorer	configuration	Segregation of	vsingh	Vivek Singh (VSING.TI)	V		Operations	dat	
8.	$\overline{\mathbf{h}}$	duties rules							
\frown_{+}	$\underline{\mathbf{v}}$	Segregation of duties conflicts							
		uuties connicts							
Create role	Import users	Stand-ins							
		Data security	Roles History Log	in date and time AAD groups					
		Snapshots			Time Total	e			
		Snapshots	Last login date and time 11/6/2019 07:48:42 AM	Days since last login online 0 0:00		e gon			
		Snapshots History	Last login date and time	Days since last login online					
		History	Last login date and time	Days since last login online					
			Last login date and time	Days since last login online					
			Last login date and time	Days since last login online					
Use	er's last log	History Charts	Last login date and time	Days since last login online					
		History Charts	Last login date and time	Days since last login online					
	< 1 mo	History Charts	Last login date and time	Days since last login online					
		History Charts	Last login date and time	Days since last login online					
1 te	< 1 mo o 3 mo	History Charts	Last login date and time	Days since last login online					
- 1 to 2	< 1 mo o 3 mo > 3 mo	History Charts	Last login date and time	Days since last login online					
- 1 to 2	< 1 mo o 3 mo	History Charts	Last login date and time	Days since last login online					
- 1 to 2	< 1 mo o 3 mo > 3 mo ver Io	History Charts	Last login date and time 11/6/2019 07/48/42 AM	Days since last login online					
- 1 to 2	< 1 mo o 3 mo > 3 mo	History Charts	Last login date and time	Days since last login online					
- 1 to 2	< 1 mo o 3 mo > 3 mo ver lo	History Charts	Last login date and time 11/6/2019 07/48/42 AM	Days since last login online					

3.4.30 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 a 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 fields have 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.

Asset classifi Tables	cation		Asset classification			
Pilter						
Table name	Table label	Table ID				
Accountant_BR		6799				
AccountantLogisticsLocation AccountantLogisticsLocationR		1315				
		6664				
AccountingDistribTmp	DrderLi	4548				
AccountingDistribution	EventT	6373				
AccountingDistribution	Tmp	97				
AccountingDistributionTmpA		2882				
Asset classification info			Access Control Data Customer Content CustomerContent			
✓ Field name	Field label	Asset classification	End User Pseudonymous Identifiers End User Pseudonymous Information (EUPI)			
CNPJNum_BR		Customer Content	 Extension ANil Object Metadata Organization Identifiable Information (OII) System Metadata System Metadata 			
CPFNum_BR		Customer Content				



3.4.31 A List page with Workflow delegation details

This one is a UI improvement to make it easier for SCS administrators to manage and track "*Workflow Delegations*". Every user has to login by himself to delegate workflow to other user, in D365FO. Now using SCS, administrators 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

≡	🖉 Ec	dit +New 🛍 Delete Options 🖇	0					• 1 ₽0 ¤ ×
ŵ	Y	₽ Filter	Workflow delegation					
☆	=		Notifications					
٩		\$0F81	Line item workflow notification t	Send notifications in email	Send notifications to Action C			
		Adri Cardol (ACARD.TI)	Individual	Yes Yes	Yes			
		Admin	Delegation					^
		Anil Kumar Tayyala (TI)	+ Add Remove Delegation Active Scope Name	Delegate	Start date/time $\uparrow \heartsuit$	End date/time \heartsuit	Enabled	
		BENJAMIN			We didn't find anything to show	here.		
		CHARLIE						
		Daiva Greiciune	Comment					
		Dirk Tijssen (DTIJS.TI)						
		Florin Milhoo						

3.4.32 User groups – combined two tabs in one

This one is a UI improvement 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.

🖉 Edit	+New 🗓 Delete 🛛	Options 🔎				
₽	Users groups Setup List	5				
	Approvers Project Originat Project					
	Name REMAINING USERS	Filter		SELECTED USERS		
	\$0F81	\$0F81		Admin	Admin	1
	\$5E39	Anil Kumar Tayyala (A	\rightarrow	atayyala	Anil Kumar Tayyala (TI)	
	acardol	Adri Cardol (ACARD.TI)	F	axrunner	axrunner	
	BENJAMIN	BENJAMIN				
	CHARLIE	CHARLIE				
	dgre	Daiva Greiciune				
	dtijssen	Dirk Tijssen (DTIJS.TI)				



3.4.33 New export/import role functionality

a) Problem:

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.

c) 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

Security management						
Summary						
_x A 135 24	2 十 ② 品	ស៊្ល	ନ୍ ↓			
Users Roles	New security request Merge roles explorer	Security	Create role Impo	rt users		
Security						
Requests	Merge roles Duplicate role Lock roles តឹង Explore	e Export Import De	efine active/inactive role	Export role configuration Import role configurati	on	
Scenarios	O Role name	↑ License type	License type (cloud)	Role description Locked Inactiv	e Has configuration	
Users	Business events security role	Operations	Human resouces			
Groups	Business events viewer	None				
Roles	BusinessConnector Role	None		Role Used to Decide if us		
Roles	Buying agent	Activity users	Activity users	Documents purchase eve	\checkmark	
Duties	Chief executive officer	Activity users	Activity users	Reviews the financial and	~	
Segregation of duties rules	Chief financial officer	Activity users	Activity users	Reviews the financial perf	~	
Segregation of duties conflic	Collections agent	Operations	Finance	Documents collections ev		
Stand-inc						

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.

3.4.34 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.

^{My view} ∽ Security and cor	pliance studio param	eters	
General	General setup for the pu	urchased licenses	
License count	Open admin.microsoft.com		
Data migration	LICENSE PARAMETERS INPUT		
	O C License	Ť	No of licenses
Enhanced SoD rules	 Activity users 		150
Number sequences	Commerce		12
	Commerce - attached	license	3
	Finance		10
	Finance - attached lice	ense	5
	Human resouces		10
	Human resouces - atta	ached license	5
	Operations		0
	Project operations		60
	Project operations - a	ttached license	30
	SCM		18
	SCM - attached licens	e	9
	Team members		76

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

Summary			License optimization						
′ Summary									
License									
Usage			n case one of base the licenses is require	d, the count is listed in 'Any base lie	iense'.				
All users	The licensed users and remainin	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 356 user interface is not aware of assigned licenses in Entra ID.							
Full users	View on premise								
Activity users	 License type 	☆↑ Actual users con	Int Base license users count	Attach license users count	Remaining users count				
Team members	 Activity users 		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				

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.



ull users uctivity users eam members cenarios	View on premise licenses Ucense type Activity users Any base license Commerce	Vî A	ctual users count 3	Base license users count	Cloud licen		
eam members	 Activity users Any base license Commerce 	Vî A		Base license users count	Attach license users count		
	Any base license Commerce		3		Actach neense asers count	Remaining users count	
cenarios	Commerce			150	0	147	
			10	0	0	-10	
			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	
Isage	The actual count is a total of rec Based on your actual subscription				the count is listed in 'Any base license'.		
All users	The licensed users and remaining	ng licenses might b	e incorrect in case the	ere are users requiring more than or	ne license.		
ull users	The Dynamics 365 user interface View cloud licenses	e is not aware of as	signed licenses in Ent	ira iD.			
ctivity users	 License type 	Vî A	ctual users count	Base license users count	Attach license users count	Remaining users count	
eam members	 Activity users 		3	150	0	147	
cenarios	Operations		0	0	0	0	
centros	Team members		30	76	0	46	



4. Bug fixes

4.1 Security and compliance studio 10.0.42.46

ID	Description	Observation
208801	CS00235313 Audit log showing	This fix will ensure that in the audit logs the
	incorrect information when copying	company name for which the role is being
	assigned roles to users	allocated to the user should populate.
209542	CS00235288 User security log is not	This bug fix will ensure that the application
	complete	must capture the security logs for the
		changes made using the IAM solutions.
210322	CS00235322 Sensitive data log	This fix will ensure that the application
		generates the sensitive logs for all the
		changes made in sensitive data fields
		specified in Sensitive data setup.
210548	CS00235500 Audit log bug - audit log	This fix will ensure that the application must
	not correctly populated when changing	capture the audit log whenever a role is
	organization ass	allocated or deallocated for an organization.
205241	CS00234809 Cleanup of table	This bug fix will ensure that user is able to
	DSMSECURITYPRIVDUTYASSOCIATION	clean the table
	HISTORY	DSMSECURITYPRIVDUTYASSOCIATIONHIST
		ORY successfully.

4.2 Security and compliance studio 10.0.41.45

ID	Description	Observation
198394	CS00234215 Problem in the D365 process might be caused by the SCS module	This bug fix will ensure that D365 processes must not be impacted by 'Continuous User Logging' feature of Security and Compliance Studio.
195568	CS00233677 Security roles for Security compliance studio	This enhancement will ensure that a user with a Security request user role should be able to manage the security requests, which includes Create New Request, Submit the request, Reject the request or approve the request.
202709	CS00234369 - Approved Enhanced Sod Rules still stuck on approved after removing the related roles from the user	This enhancement will ensure that once a role is removed for a user profile, the SoD conflicts, related to that role, must be removed from the Enhanced SoD conflicts page of SCS application.



4.3 Security and compliance studio 10.0.40.44

ID	Description	Observation
179803	License recommendation incorrect in case of both HR and PO roles	This bug fix will ensure that HR license should appear as an attached license and not base license.
195135	CS00233715 SCS version10.0.39.43 causes a lot of objects in garbage collection	Memory consumption issue that leads to slow performances got fixed. Garbage collection is working correctly.

4.4 Security and compliance studio 10.0.39.43

ID	Description	Observation
183994	CS00232323 German labels in module 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.

4.5 Security and compliance studio 10.0.37.42

ID	De	scription	Observation
175967		CS00227225 Export/Import	AOT privileges with
		function in Security and Compliance	'FormControlOverrides' node populated
&		Studio modifies std. objects.	are having an issue on SCS Export/Import
			functionality due to a MS standard bug. All
176711		&	entries from this node cannot get pass into
			the XML file, therefore at the import step
		CS00227144 Deviation in standard	the node will get overridden and all entries
		role after import of custom role.	are removed (as the object from the XML
			file).
			As a fix we introduced a new functionality
			called : "Export role customizations /

		Import role customizations". For more details please see WHAT'S NEW SECTION.
180975	CS00227886 Manage access on roles to multiple organisations is not working in 'NL'	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.
180707 & 180696	CS00227833 'Any base license' roles are counted in both 'Finance' and 'SCM' licenses &	Incorrect license count. New options have been added to the SCS parameters license count system. For more details please see WHAT'S NEW SECTION.
	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.

4.6 Security and compliance studio 10.0.36.41

ID	Description	Observation
180210	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.

4.7 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.

4.8 Security and compliance studio 10.0.34.39

ID	Description	Observation
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'.

4.9 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. ¹
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. ¹

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.

¹ 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 Staedean support, so we can review, improve and contact Microsoft to get better suggestions in future releases.

4.10 Security and compliance studio 10.0.31.37

ID	Description	Observation
158243	Internal Snapshot deletion not working properly	In specific scenarios the snapshot deletion was not respecting the setting for number of snapshots to keep. Snapshot details were deleted; only headers remained. This issue has been fixed.
160517	Internal A user without system administrator rights can create users and grant the system admin role	There 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 copy security setup, we restricted now the option to copy the system administrator role in case a user is not assigned to the system administrator role.
159501	CS00222903 Can't create a snapshot	When 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 records will be cleaned up to prevent the duplicate record error.

4.11 Security and compliance studio 10.0.29.36

ID Description Observation

153855	Internal Synchronize the group users	Enhanced error handle to provide more
	with AD group members batch runs into	information when an user fails to be imported
	error when Import roles parameter is	from azure groups.
	activated.	
151835	Internal Data source fields not	Changes over the data source fields are not
	recognized during direct role import	detected during direct role import.

Security and compliance studio 10.0.28.34 4.12

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.

Security and compliance studio 10.0.27.33 4.13

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

Security and compliance studio 10.0.26.32 4.14

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

Security and compliance studio 10.0.26.31 4.15

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

Security and compliance studio 10.0.25.30 4.16

ID	Description
124413	CS00164201 SCS - Role Export / Import Generating New AOT Name

Security and compliance studio 10.0.24.29 4.17 ID

Description



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

4.18 Security and compliance studio 10.0.22.27

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

4.19 Security and compliance studio 10.0.18.1

ID	Description
	No external bug has been reported in the last release ! We don't list down the internal
	bugs fixed in the release notes.

4.20 Security and compliance studio 10.0.12.5

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

4.21 Security and compliance studio 10.0.12.4

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

4.22 Security and compliance studio 10.0.12.3

ID	Description
	No external bug has been reported in the last release ! We don't list down the internal
	bugs fixed in the release notes.

4.23 Security and compliance studio 10.0.12.2

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

4.24 Security and compliance studio 10.0.12.1

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



4.25 Security and compliance studio 10.0.10.1

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

4.26 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

4.27 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-Staedean SCS Parameters Data Entity Missing Fields

4.28 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

4.29 Security and compliance studio 10.0.6.8

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

4.30 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
101712	CS00114631- cannot create snapshots. It throws an error "Cannot create a record in License 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

4.31 Security and compliance studio 10.0.6.6

ID	Description
100323	CS00111058-Unable To Import Security Roles

4.32 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

4.33 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

4.34 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

4.35 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

4.36 Security and compliance studio 10.0.6.1

ID	Description
81072	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.
	Purchased license value is used in license optimization workspace.
86619	CS00080538 – Security Explorer- No colored icon for "Team Member" license type.



86627	CS00079152 – Apply Active Directory User Status – Authentication Method
-------	---

4.37 Security and compliance studio 10.0.3.3

Ш	D	Description
8	3602	– Standard Import user menu item is not visible if SCS license expired.

4.38 Security and compliance studio 10.0.3.2

ID	Description
77956	CS00069693 – License Count Data Source.

4.39 Security and compliance studio 10.0.3.1

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

4.40 Security and compliance studio 10.0.1.3

ID	Description
	No external bug has been reported in the last release ! We don't list down the internal
	bugs fixed in the release notes.

4.41 Security and compliance studio 10.0.1.2

ID	Description
	No external bug has been reported in the last release ! We don't list down the internal
	bugs fixed in the release notes.

4.42 Security and compliance studio 10.0.1.1

ID	Description
	No external bug has been reported in the last release ! We don't list down the internal
	bugs fixed in the release notes.

4.43 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.

4.44 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.

4.45 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'

4.46 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

4.47 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

4.48 Security and compliance studio 81.20.3.1

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

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

Description	
TI-12204-S3M9 Audit log duplicate records as coming from AOT	
TI-12205-P0Y5 User audit log not working properly	
TI-12213-S8Q4 Add table permissions to role or privilege	
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.	

4.50 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.	

4.51 Security and compliance studio 81.20.1.1

ID	Description
	No external bug has been reported in the last release ! We don't list down the internal
	bugs fixed in the release notes.

4.52 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

4.53 Security and compliance studio 1804.15.1.1

ID	Description
	No external bug has been reported in the last release ! We don't list down the internal
	bugs fixed in the release notes.

4.54 Security and compliance studio 1712.12.1.1

ID	Description		
	No external bug has been reported in the last release ! We don't 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 duties/privi	role leges	from	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.



- 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).

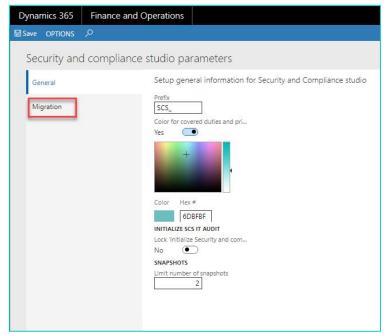


Fig. 1 New tab in SCS Parameters form

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)

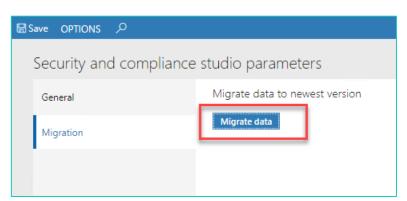


Fig. 2 "Migrate data" button on SCS Parameters form

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 ₽	
() Migration done. Please restart your D365 UI	
Security and compliance s	tudio parameters
General	Setup general information for Security and Compliance studio Prefix SCS_ Color for covered duties and pri Yes Color for covered duties and pri Yes Color Hex # Color Support Suppor

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