

Release Notes for Security and Compliance Studio 10.0.40.44

Release Notes

Author: Ankit Bhadana, Product Owner

Table of Contents

1.	Introduction				
1.1 1.2	Audien	e ce	7		
1.3		t release information			
1.4		ables			
1.5		on features			
1.6	Certific	ate renewal	10		
2.	What's	New in Security and Compliance Studio 10.0.40.44	11		
2.1	-	zation assignment for security request			
2.2	Continu	uous user action logging	12		
3.	Feature	es introduced in last few releases of Security and Compliance Studio	14		
3.1	Versior	10.0.39.43 Release			
	3.1.1	User audit log for sensitive data	19		
	3.1.2	Securable tree view	21		
	3.1.3	Security request history track	24		
	3.1.4	Enhanced SoD predefined list	25		
3.2	Versior	10.0.37.42 and Older	27		
	3.2.1	Segregation of duties sets	27		
	3.2.2	Security requests enhancements and workflow			
	3.2.3	Export security explorer objects to excel in a de-normalized format			
	3.2.4	Merge security scenarios and match role			
	3.2.5	Mark any Security Role as Active/Inactive			
	3.2.6	Recording steps to scenario.	41		
	3.2.7	Override permission based on scenarios	41		
	3.2.8	Option to mark, track and audit security objects providing access to	40		
	3.2.9	sensitive data Option to create a duty from Matched Privileges grid in Match roles form			
			50		
	3.2.10	Option to import and export data using Data Entities in Security and Compliance Studio			
	3.2.11	Option to compare Security Snapshots stored in the security setup			
	0.2.11	option to compare occurry onaponoto stored in the security setup			

	3.2.12	Enhanced Audit log capability to capture all the changes from development space (AOT) as well into Audit Log	55
	3.2.13	Option to create one or more privileges and also one or more duties	
		while merging roles.	
	3.2.14	Ability to create scenarios from D365 module menus	
	3.2.15	Snapshots based performance and scalability enhancements	
	3.2.16	Improved "Create role wizard" based on a grid framework	
	3.2.17	Accessing Security Explorer from all D365 FOE forms	60
	3.2.18	Option to create duties and SOD compliance check as well while merging roles.	61
	3.2.19	Importing New Users while Synchronizing the group users with the Active Directory group members	62
	3.2.20	Uptake RapidValue BPM Suite Scenarios directly as SCS Security	
	0.0.01	Scenarios	
	3.2.21	Enhanced Segregation of Duties	
	3.2.22	Organization risk Register	
	3.2.24	Security Explorer displaying Tables, Service operations and Data Entities entry point's type	66
	3.2.25	Performance Optimization	66
	3.2.26	A new "Share" workspace	66
	3.2.27	AAD groups' information in D365FO	67
	3.2.28	Verify SoD rules in Stand in	68
	3.2.29	Chart to give an overview of number of users and their last logging details	68
	3.2.30	Asset classification User Interface	
	3.2.31	A List page with Workflow delegation details	
	3.2.31	User groups – combined two tabs in one	
	3.2.32	New export/import role functionality	
	3.2.33	License count changes	
	3.2.34		
4.	Bug fix	es	74
4.1		y and compliance studio 10.0.40.44	
4.2		y and compliance studio 10.0.39.43	
4.3		y and compliance studio 10.0.37.42	
4.4		y and compliance studio 10.0.36.41	
4.5		y and compliance studio 10.0.36.40	
4.6		y and compliance studio 10.0.34.39	
4.7		y and compliance studio 10.0.32.38	
4.8		y and compliance studio 10.0.31.37	
4.9		y and compliance studio 10.0.29.36	
4.10		y and compliance studio 10.0.28.34	
4.11		y and compliance studio 10.0.27.33	
4.12		y and compliance studio 10.0.26.32	
4.13	Securit	y and compliance studio 10.0.26.31	

4.14	Security and compliance studio 10.0.25.30	
4.15	Security and compliance studio 10.0.24.29	79
4.16	Security and compliance studio 10.0.22.27	79
4.17	Security and compliance studio 10.0.18.1	
4.18	Security and compliance studio 10.0.12.5	79
4.19	Security and compliance studio 10.0.12.4	
4.20	Security and compliance studio 10.0.12.3	79
4.21	Security and compliance studio 10.0.12.2	79
4.22	Security and compliance studio 10.0.12.1	79
4.23	Security and compliance studio 10.0.10.1	80
4.24	Security and compliance studio 10.0.6.11	80
4.25	Security and compliance studio 10.0.6.10	
4.26	Security and compliance studio 10.0.6.9	
4.27	Security and compliance studio 10.0.6.8	80
4.28	Security and compliance studio 10.0.6.7	80
4.29	Security and compliance studio 10.0.6.6	81
4.30	Security and compliance studio 10.0.6.5	81
4.31	Security and compliance studio 10.0.6.4	81
4.32	Security and compliance studio 10.0.6.3	81
4.33	Security and compliance studio 10.0.6.2	81
4.34	Security and compliance studio 10.0.6.1	81
4.35	Security and compliance studio 10.0.3.3	82
4.36	Security and compliance studio 10.0.3.2	82
4.37	Security and compliance studio 10.0.3.1	82
4.38	Security and compliance studio 10.0.1.3	
4.39	Security and compliance studio 10.0.1.2	82
4.40	Security and compliance studio 10.0.1.1	82
4.41	Security and compliance studio 81.3.2.1	82
4.42	Security and compliance studio 81.3.1.1	82
4.43	Security and compliance studio 81.2.1.1	82
4.44	Security and compliance studio 81.1.2.1	83
4.45	Security and compliance studio 81.1.1.1	83
4.46	Security and compliance studio 81.20.3.1	83
4.47	Security and compliance studio 81.20.2.2 *(This build was created as the earlier	
	deployable package had some issues)	83
4.48	Security and compliance studio 81.20.2.1	83
4.49	Security and compliance studio 81.20.1.1	83
4.50	Security and compliance studio 1804.15.2.1	83
4.51	Security and compliance studio 1804.15.1.1	84
4.52	Security and compliance studio 1712.12.1.1	84
5.	Changed or deprecated features	85
5.1	Deprecated features 10.0.31.37	85
5.2	Deprecated features older versions	
0.2		

Document Information

Title	Release Notes for Security and Compliance Studio 10.0.40.44
Subtitle (Subject)	Release Notes
Solution Suite	GRC; Security and Compliance Studio
Category	Release Notes
Author	Ankit Bhadana
Published Date	7/12/2024
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 10.0.40.44** release from Staedean. This release is compatible with the version of Microsoft Dynamics 365 for Finance and Operations, **10.0.36 or later**.

1.2 Audience

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

1.3 Product release information

Release Notes for Security and Compliance Studio 10.0.40.44 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	

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 10.0.40.44 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 Manufact	uring	
Solution	↑ Installed version	Status	:		
Advanced Discrete Manufactur	i	×		UTION IS NOT INSTALLED	
Advanced Project Managemen	t	×	Solution description		
Anywhere Mobility Studio		\times	Help manufacturers solve probl	lems and streamline process flows.	
Business Integration Solution	10.0.99.999	\odot			
Data Entry Workflow		×	License	Status Expiry date	
Data Modeling Studio		×	Construction	A	
Data Quality Studio	10.0.18.2	\otimes	Equipment	8	
DynaRent	10.0.28.43	0	Advanced Project Managemen	it 🗛	
PLM Integration for Engineerin		×	Product Engineering a		
RapidValue BPM Suite	10.0.26.37	\odot			
Security and Compliance Studi		×			

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	
○ 2	
🔵 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, pleas don't include any personal information.	e

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 10.0.40.44

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 1	:	+	Company	Company accounts	:
Contoso Entertainment System	USMF		+			
Contoso Group	GLCO					
Contoso Italy	ITCO				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.



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.

← Oreate snap	oshot Refresh licenses 🖄 Re	eset p	ins Advanced view Show joined	Vi	ew accessed entry points Export to Ex	cel	© Options			<	8	0	0	0 ¤
Standard view 🗸														
Security exp	olorer: full view													
USERS			ROLES		DUTIES	F	PRIVILEGES		ENTRY POINTS					
HP Pin users			-🛱 Pin role		H⊐ Pin duty		-t¤ Pin privilege		- Pin entry point and permissions					
User	Name		Role name 1 :		Duty name 1 :		Privilege name		Entry point (AOT name) î T	ype		A	Access ri	ight
•			AAC_Hotfixtest		A parameter that is used to gro		testpriv1		AadWorkerIntegrationEntity	DataEntity		١	∕iew	
•			abcde		 Access benefit management wo 		TestSoDAccess12		AadWorkerIntegrationEntity	DataEntity		F	ull con	ntrol
•			Accountant		 Access benefits workspace 		SCS_testexcludeentry (tables)		AbatementCertificate_IN	/lenu item display		F	ull con	ntrol
•			Accounting manager		Access employee development		SCS_testhotfix1 (display)		AbatementPeriodicCertificate_IN	fenu item action		(Create	
•			Accounting supervisor		Access expense management w		 Sensitive Data Role (display) 		AbatementPeriodicCertificate_IN	lenu item action		F	ull con	ıtrol
•			 Accounts payable centralized pa. 		Access the leave and absence te		SCS_testbug (action)		■ C AbbreviationCodeImport_RU M	lenu item action		0	Create	
•			Accounts payable clerk		Access workforce management		testprivreg		■ C) AbbreviationCodeImport_RU M	lenu item action		F	ull con	ntrol
•			Accounts payable manager		Access workforce management		SCS_ABDemo_1812 (action)		■⊡- AbbreviationsEntity E	DataEntity		\	∕iew	
•			Accounts payable payments clerk	1	 Accounting manager (display) 	1	 SCS_rolewithpriv (display) 	1	■G- AbbreviationsEntity	DataEntity		F	ull con	ntrol

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

Filter Show enal	essed entry points									
ERS				ENTRY POINTS PERMITTED			ENTRY POINTS ACCESSED			
)	⊽† Name	Enabled		Entry point (AOT name) î	Туре	Access right	Menu item name	Menu item label	Menu item type	Last accessed on
SCOBA	SCOBA	false		AbbreviationsEntity	DataEntity	View	DSMUserAccessedEntryPointsL	View accessed entry points	Display	7/2/2024 10:44:30
		true		AbbreviationsEntity	DataEntity	Full contro	DSMSecurityLicenseTypeExplore	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:
		true		AccountingDistMarkupTransPO	Menu item display	View	DQSDataPolicy	Data policy	Display	6/28/2024 10:33:
		true	1	AccountingDistMarkupTransReq	Menu item display	View	DQSDataPolicyListPage	Data quality policies	Display	6/28/2024 10:33:
		true		AccountingDistPurchReqTable	Menu item display	View	DewWorkflowWizard	Workflow wizard	Display	6/28/2024 6:21:0
		true		AccountingDistPurchTable	Menu item display	View	DewWorkflowStepOpenPart	Open tasks assigned to me	Display	6/28/2024 6:20:5
		true		AccountingDistribution	Table	No access	DewWorkflowTemplatePreview	Data entry workflows	Display	6/28/2024 6:15:5
		true		AccountingDistributionOrderSu	Menu item display	View	DewWorkflowWorkspace	Data entry workflow workspace	Display	6/28/2024 6:15:5
		true		AccountingDistributions	Menu item display	View	DewWorkflowWizardFieldCRDr	Change request	Display	6/27/2024 10:50:
		true		AccountingDistributionsDocum	Menu item display	View	DewWorkflowTemplateNewVer	Create new version	Display	6/27/2024 10:30:
		true		AccountingDistTaxTransTmp	Menu item display	View	DQSParameters	Data quality studio parameters	Display	6/27/2024 8:52:5
		true		AccountingDistTaxVendPackSlip	Menu item display	View	VendTableListPage	All vendors	Display	6/26/2024 9:39:0

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 lo	ogs for entry points accessed	Options 🔎			4	» ۵	1	P 0	- C
	Personalise Po	age options Sh	are							
			ate a custom alert \smile							
Add t	to workspace V Advand Record		hage my alerts							
	Record									
										~
User co	ontinuous log									
Star	ndard view ~									
ADDIT	ONAL INFO TO INCLUDE	DA	TE RANGE							
User ID	Entr	y point Fro	om date To date							
	~	~ 7,	/4/2024 🛅 7/4/2024	<u></u>						
0	User ID	Menu item name	Menu item label	Menu item type	Last accessed on	\\ \\				:
\bigcirc	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 p	oints 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 🗸	
Start date: 7/4/2024 (11:46:00 am) (G	iMT) 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. Features introduced in last few releases of Security and Compliance Studio

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

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

- Option to import and export data using Data Entities in Security and Compliance Studio. In this release we have added some data entities currently supported for Security and Compliance Studio. The approach has been to enable data entities for all tables where relevant in Security and Compliance Studio in order to provide import and export capabilities.
- Option to compare Security Snapshots stored in the security setup. Building upon what we already have implemented in the fall release (security snapshots) we have gone furthered and added the possibility of comparing the existing security snapshots. Snapshot comparison feature allows security officers and administrators to do a detailed comparative analysis between any two security snapshots for all security objects in D365 FOE setup i.e. Users, roles, duties, privileges. Both single record compare and full compare options for the selected snapshots are supported along with multiple views. The comparison option will allow the user to see what modifications had occurred in the security setup since the last changes. The users can keep track of the changes, comprehend and analyze them in order to strengthen the security further.

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

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

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

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



- Option to create duties and SOD compliance check as well while merging roles. "Merge role" feature now comes with an option to create duties along with the privileges. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.).
- Importing New Users while Synchronizing the group users with the Active Directory group members. We added a new small feature to our Azure AD group synchronization job. On the dialog of the Synchronize the group users with the Active Directory group members, we introduced a new parameter to import users.
- Licensing changes To help our customers we have implemented new licensing changes within SCS. Microsoft has taken a commercial decision last year to split the license to Finance, SCM, and project, for more details you can have a look at Microsoft's new licensing guide. These changes left customers confusing about how they can be compliant with new license changes. That's why we have decided to build this feature, now customers can see a new license type field in SCS forms such as security explorer, match roles, license optimization workspace, etc.
- Uptake RapidValue Scenarios directly as SCS Security Scenarios Customers can now directly upload the RapidValue Scenario task guides per security roles (Procedure activities which include flows across multiple roles) as a Security scenario in Security and Compliance Studio. This will be very useful where both RapidValue BPM Suite and Security and Complicate Studio are implemented. You might be aware that now in RapidValue, you can have Business process hierarchy with its linked task guides exported from RapidValue to a user defined local Windows folder. Export logic takes care of both the modeling techniques where customer is using Flow-Activity way of modeling and also the Scenario" Procedure Activity" way of capturing flow variations.
- Enhanced Segregation Of Duties In standard D365FSC, we can only define SoD rules at duty level which is rarely useful. In SCS, with this release user can now define SoD rulesets at any level (Duty, Privilege or Entry Point) in the security hierarchy in D365FSC. This makes this feature more practical and extremely useful for customers seeking better regulatory compliance like ISO 27001 section 6.1.2, SOX Control 404 and in general much improved security design better equipped to prevent frauds.
- **Organization Risk Register** All Organizational risks can be now mapped in SCS "*Integrated risk Management workspace*". They may be financial risks related to SoD violations or can be related to any other organizational strategy or operational aspect. This feature will evolve in coming quarters in a full-fledged "Risk Management" capabilities within SCS enabling Organizations to register, assess, monitor, mitigate and close it.
- AAD related SoD Validations across SCS SCS now ensures that SoD violation checks also consider Security roles acquired by a user from being associated within an AAD. This is applicable all across SCS features. This helps in better handling of internal controls.
- Security Explorer displaying Tables, Service operations and Data Entities entry point's type Security expirer has been enhanced to now include also the following entry point's type: Tables, Service Operations and Data Entities.
- **Performance Optimization** Significant performance improvement in the following programs: Create snapshot; Security Explorer pinning, Match roles and Marking a record as sensitive.



- A new "Share" Workspace A new workspace "Security and compliance file share" is added to manage task recording and images being used at various places in security & compliance studio.
- **AAD groups' information in D365FO-** In standard D365FO, we cannot check what all the users added to AAD groups and we have to login to azure portal. Now in SCS, we can check what all the users added to AAD groups in D365FO itself along with all related audit tracking for AAD groups in SCS itself.
- Verify SoD rules in Stand in You can now use "Validate Sod rules " functionality while defining new stand-ins in SCS to know in advance, if there will be any SoD violation when security roles of user will be assigned to stand in user.
- Chart to give an overview of number of users and their last logging details- SCS now comes with a chart to categorize all users with their login details and time series analytics. This helps a lot in both compliance needs and optimizing license costs to deactivate or remove users based on an organization's security policy.
- Asset classification User Interface SCS provides user interface, which shows all the fields with their asset classification. Chart to get the overview of different asset classification and how many field has the same asset classification. Asset classification is a table field property, classifying type of data it contains. Tagging a column helps easily marking data in scope for GDPR/GxP and many other such compliance regulations.
- A List page with delegation details This one is a UI improvements to make it easier for SCS administrators to manage and track "*Workflow Delegations*". Every user has to login by himself to delegate work flow to other user, in D365FO. Now using SCS, administrator can delegate workflow to any user for a particular time period.
- User groups combined two tabs in one This one is a UI improvements to make it easier for SCS administrators to manage a simplified standard user group's form. Users who are outside the organization hierarchy for budget planning must work with budget plans, you can assign budget plans to user groups. You can also set up restrictions for journal posting that are based on user groups. Users can be added to different groups using same tab. Also in SCS now a list of added users to different groups can be exported to excel using list tab.
- **Dynamic snapshot** We got a lot of feedback and learnings related to the security snapshot. A lot of features depend on having actual data in the snapshot. New changes in the snapshot framework have been introduced where the snapshot no longer requires to updated via a batch job after security changes have been made.

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

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

• New export/import role functionality

- 1. **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 10.0.39.43 Release

3.1.1 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:

	e MO recording .	Created by Admin		date and time Secu 24 08:58:58 AM Op	urity record status	Owner		
De	scription)			
_	•						I	
	neral							
	Add 🔟 Delete Field picker							
0		Reference field na	me	Field label	displayObservat	ion		
	LogisticsLocation	Description		Name or description				
	HcmWorkerTitle	OriginalHireDate		Original hire date	Table 'HcmWor	kerTitle' is dat	effective or supports	inheritance ar
	DirPerson	✓ NameAlias	~	Search name				
_								
Qu	ery							
Ec	dit query							
0	Query name	Table name						
	DirPerson 🗸	DirPersonStaging						
Use	ers							
Use								
+	Add 间 Delete	Name		uatwork Alias	natworkDomoir			
+	Add 🗊 Delete	Name		ietworkAlias	networkDomain		creace com	
+	Add Delete Oldete Oldete Image: Second se	✓ fmihoc	f	mihoc@to-increase.com	https://sts.wind	dows.net/to-in	crease.com	
+	Add 🗊 Delete		f		https://sts.wind .com https://sts.wind	dows.net/to-in dows.net/	crease.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:

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

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

This means that the selected table is part of an exception and cannot be used to validate the data against it, so we need to create a table mapping that will be replacing the original table in the validation process.

The mapping table should be a staging table or a child table that has the field(s) in question (the fields we are trying to mark as sensitive).

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

	С	Main table 1	Staging tab	le				
		DirPartyTable	DirPartyTableAttachmentsStaging					
2		DirPerson	DirPerson	Staging				
	٦	DirPersonName	DirPerson	NameHistoricalStaging				
		LogisticsPostalAddress	LogisticsP	ostalAddressElectronicContactV2Staging				
+,	Add	🗊 Delete 🛛 🗍 Generate ma	apping					
+			apping) ↑	Stanning table field				
+/		Delete Generate ma Main table field AnniversaryDay	apping	Stagging table field AnniversaryDay				
+ 1		Main table field	apping) ↑					
+		Main table field AnniversaryDay	apping) ↑	AnniversaryDay				
+,00		Main table field AnniversaryDay AnniversaryMonth	apping) ↑	AnniversaryDay AnniversaryMonth				
+		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".

standard view	~								
	date /2/2024 🗎	3							
DITIONAL FILTER OPTION	s								
ser ID Ta	ble name								
V[~							
Table label	Modifie	d table	Description	Event created by	Sensitive data setup name	Event date			
Addresses	Logistic	csPostalAddress		Admin	Test from scratch	11/2/2023 12:44:54	1 PM		
Position details	HcmPo	sitionDetail		Admin	HCMPositionDetail	11/2/2023 12:44:37	7 PM		
Customers	CustTab	ble		Admin	Custtable - credit	11/2/2023 12:34:58	3 PM		
Customers	CustTab	ble		Admin	Custtable - credit	11/2/2023 12:15:53	8 PM		
Customers	CustTak	ble		Admin	Custtable - credit	11/2/2023 10:19:55	5 AM		
Order lines	SalesLir	ne		Admin	InventDim	10/30/2023 11:47:2	26 AM		
Position details	HcmPo	sitionDetail		Admin	HCMPositionDetail	10/30/2023 11:31:1	I0 AM		
Position details	HcmPo	sitionDetail		Admin	HCMPositionDetail	10/26/2023 12:13:1	17 PM		
Position details	HcmPo	sitionDetail		Admin	Position - test	10/11/2023 7:03:43	3 AM		
Addresses	Logistic	sPostalAddress		Admin	Test worker address	10/10/2023 9:23:45	5 AM		
Addresses	Logistic	csPostalAddress		Admin	Test worker address	10/10/2023 9:23:31	I AM		
User Information	UserInf	ò		Admin	User data	8/10/2023 10:36:58	3 AM		
User Information	UserInf	o		Admin	User data	8/10/2023 10:36:40	D AM		
Vendors	VendTa	ble		Admin	Vendor table	8/10/2023 10:31:55	5 AM		
Global address book	DirPart	yTable		Admin	Vendor table	8/10/2023 10:31:24	1 AM		
User Information	UserInf	o		Admin	User data	8/10/2023 10:12:12	2 AM		
User Information	UserInf	io .		Admin	User data	8/10/2023 10:08:32	2 AM		
TAILS								=	
	Field label	Event type	Value from		Value to	Form	name	Form label	Created date and time
Reference field name			413 Oak Street TEST		413 Oak Street TDEMO1	Lee's	sticsPostalAddress	Manage addresses	10/10/2023 9:23:31 AN

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.

3.1.2 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	N								
Override permission on selected	object								
Security object types	Value	DETAILS							
Role 🗸	Budget contributor	🖧 Explore							
AOT name	Description	O C 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	O General ledger parameters	LedgerHarameters		Menu item display	Leogerrarameters	Form	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	ient	O Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor		View	Team members	Team members	
Common		Duty	BUDGETBUDGETPROCESSPOLICIESINQUIRE	Inquire into budget process polic		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	Control label Co	ontrol type	Object nam	e from menu item	Object type from men	u item	
Allocations		 LedgerOppositeSignUpdate 	F	ormBuildFunctionButtonControl	LedgerOpp	oositeSignUpdate	Action		
Calendars		EximParameters_IN	F	ormBuildFunctionButtonControl	EximParam	eters_IN	Display		
Chart of accounts									
Currencies									
Deferrals									
Deferrals setup									
Financial report setup									
Financial reports setup	-	TABLE PERMISSIONS							
Inquiries and reports Journal entries		O Data source name	Control type	DataSourceTable					
		LedgerParameters	Data source	LedgerParameters					
 Journal setup Ledger setup 		TaxParameters	Data source	TaxParameters					
Advance adjustment p	scholder								
Cash control configur		NumberSequenceReference	Data source	NumberSequenceReference	e				
Cash control contigur		AssetParameters	Data source	AssetParameters					
Check voucher series	And a	InventDimSetupGrid	Data source	InventDimSetupGrid					
Date intervals		CustParameters	Data source	CustParameters					
Financial reporting set	10	FORM CONTROLS							
Fiscal calendars	an fe	O Control name	Control type	Object name from menu	item Okiest	type from menu item	Needed permissions		
General ledger param	atarc		FormBuildFunctionButtonControl				Manual		
INPC rates		O UpdateDelimiter	FormsultaFunctionsuttonControl	DimensionsiegmentSepi	aratorDataUpda Action		manual		
Ledger									
Ledger calendars									
Matrix report									
Period allocation cate	pories								

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 🖧 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
	n 🖧 Explore		
how access based on selection	م المعرفة AOT name	Label	Access le
how access based on selection		Label Auditor	Access le View
how access based on selection	AOT name		
how access based on selection ObjectType Role	AOT name AUDITPOLICYMANAGER	Auditor	View
how access based on selection ObjectType Role Role	AOT name AUDITPOLICYMANAGER BUDGETBUDGETCLERK	Auditor Budget clerk	View View
Role Role	AOT name AUDITPOLICYMANAGER BUDGETBUDGETCLERK BUDGETBUDGETCONTRIBUTOR	Auditor Budget clerk Budget contributor	View View

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

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

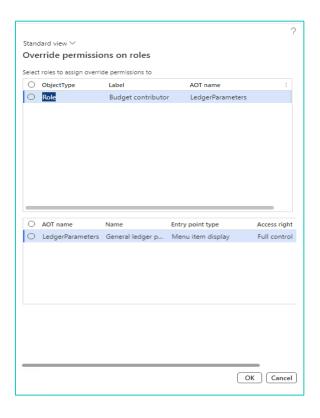
On form level there are multiple options/buttons that are opening other forms. Here these forms are displayed so you will know that if you want to provide full access to a form you need to provide access to the forms that are opening from the buttons available on that form.

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

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

^{My view ∽} Securable tree viev	N								
Override permission on selected	object								
Security object types Role	Funde .	DETAILS ஃ Explo							
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.



3.1.3 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.

curity request h	vendor master was modifie	Standard view 🗠								
ecurity request n	istory									
	,									
ecurity request details										
Open request details										
equest	Area	Created date a		End date	Owner		Security record status	Scenario	Description	
lodify role		4/3/2024 07	:14:10 AM		Admin		Completed			
pe /lodify role	Created by Admin	Start date		Origin	Priority		Modified by			
riodity role	Addition			User requests	Normal		Admin			
orkflow approval history										
Open workflow approval details	1									
stance ID	Workflow ID	Status		Document	Document type		Workflow	Version	Submitting user	Company accounts ID
100001	000014	Completed		Quotation: QN0000002, City	/ Sales quotation	1	Review project quotations	1.0.0.0	JUNE	ussi
Context	Action	Name	Message	Comment	Created date and time	User				
Workflow	Submission	000001: Quotation: QN00	Submitted by: JUNE		1/1/2016 8:35:13 PM	JUNE				
Workflow	Creation	000001: Quotation: QN00	Workflow 000014 PSAProjQuotationTem	plate	1/1/2016 8:35:29 PM	JUNE				
Approval	Creation	Project Quotation Approv			1/1/2016 8:35:34 PM	JUNE				
Approval	Auto complete condition	Project Quotation Approv	Auto-completion condition: Project		1/1/2016 8:35:42 PM	JUNE				
Approval	Completion	Project Quotation Approv			1/1/2016 8:35:44 PM	JUNE				
Workflow	Completion	000001: Quotation: QN00			1/1/2016 8:35:49 PM	JUNE				
udit log details										
Event date and time	Description		Event type	Reference Compa	ny Event created b	w 1				
3/11/2024 1:01:46 PM		splay) was created from Overri		0 *	Admin					
3/11/2024 1:01:53 PM		t (display) was created from O		0 -	Admin					
3/11/2024 1:01:54 PM		s modified from Override pern		0 *	Admin					
3/11/2024 1:01:54 PM	Duty Landed cost agent (di	splay) was created from Overri	Duty created	0 *	Admin					
3/11/2024 1:01:54 PM	Duty Inquire into products	for operations master was mo	d Duty modified	0 *	Admin					
3/11/2024 101:34 PW	Duty Maintain receipt oper	ations was modified from Ove	rr Duty modified	0 *	Admin					
3/11/2024 1:01:55 PM					te table type					
	Name		Reference type	Reterent						

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

3.1.4 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.

Impor	t /	AX : Operations My view ~				
DE	MC) import				
Impo	ort					
Grou	p nar	ne Description	Da	ata project ope	ration type	Project categor
DEN	/IO in	nport		mport		Project
Selec	ted	entities				
(+ A	dd fi	$[e \checkmark] +$ Add template \checkmark 🗊 Remove entity Open in E	cel Reseque	nce∨ Sort b	oy ∽ Disable	e 🗠 Entity attribute
0	С	Entity	View map	Executi 1	Level in ex	Sequence
0		Segregation security sets	L)	1	1	1
		Segregation security set lines	L)	1	1	2
		Enhanced SoD rules	L.	1	1	3

Import the file and the result should look like this:

ntity 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.



3.2 Version 10.0.37.42 and Older

3.2.1 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 \mid My view \sim				
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				
O C Name	1 Туре	First Fir	st securable object type	First access level
 Demo Sod rules sets 	Segregation security sets	🗸 Tralaalalal 🗸 🗸		No access
	L			



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.

3.2.2 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 ı Delete ◯Status > 80mmer > Request	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	
	Waiting	
	Review	
	Approved	
	Rejected	
	Canceled	

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

c) Assign role to user

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

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



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	
- Saudilli					
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.

Security 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	
Description	

f) Enable user

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

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

Security requests My view ~ Demo SR 1			
General			
Request Demo SR 1	Type	Origin User requests ∽	Area WHS
Status			
Priority Normal	Status Open	Owner Admin	
Enable users			
Add 🛍 Remove			
○ ○ User ID ↑ ○ JanetS	User name 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 Demo SR 1 tatus		Type Del	ete user 🗸 🗸	Origin User requests V	Area
		Del	ete user 🗸 🗸 🗸	User requests V	W/H
tatus					
		_			
riority		Statu		Owner	
Normal	\sim	Ope	en	Admin	
elete users	5				
Add 间 Re	emove				-
000	ser ID 1	User name	Email		-
	ASSIE	CASSIE	CASSIE@contosoax7.onm		
	dsaurorauser	Auroraus	Aurorauser01@capintegr		

h) Create role

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

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

Security req	uests My view 🗸						
Demo	SR 1						
General							
Request		Trans	Origin	Area			
Demo SR	1	Type Delete user	User requests	WHS	\sim		
Status							
Priority	\sim	Status	Owner Admin				
Normal	~	Open	Admin				
Create role ROLE Upload ta:	: sk recording						
ROLE Upload ta: Role name	sk recording	Description	Scenario	ie avtr			
ROLE Upload ta:	sk recording oRole1	Description Demo purposes	Scenario Scenario SkRecordingForCSReplica	ie axtr			
ROLE Upload ta: Role name SCS_Demo SCENARIO	sk recording oRole1	Demo purposes		ie.axtr Description	File name	Child scenario	↑ Remark
ROLE Upload ta: Role name SCS_Demo SCENARIO	sk recording oRole1 DETAILS	Demo purposes t Securable type	skRecordingForCSReplica	Description	File name TaskRecordingForCSRepli		[†] Remark
ROLE Upload ta: Role name SCS_Demo SCENARIO	sk recording oRole1 DETAILS number Securable objec	Demo purposes t Securable type age Display	skRecordingForCSReplica	Description			Remark Additional securable object found in the task recording
ROLE Upload ta: Role name SCS_Demo SCENARIO	sk recording pRole1 DETAILS number Securable object 1 salestablelistpr	Demo purposes t Securable type ige Display ard Display	skRecordingForCSReplica Access level Full control	Description Go to Accounts receivabl	TaskRecordingForCSRepli		Additional securable object
ROLE Upload ta: Role name SCS_Demo SCENARIO	sk recording DROIe1 DETAILS number Securable object 1 salestablelistpr 2 DefaultDashbc	Demo purposes t Securable type age Display aard Display age Display	skRecordingForCSReplica Access level Full control Full control	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli TaskRecordingForCSRepli		Additional securable object
ROLE Upload ta: Role name SCS_Demo SCENARIO	sk recording pRole1 DETAILS number Securable objec 1 salestablelistp; 2 DefaultDashbc 5 salestablelistp;	Demo purposes t Securable type nge Display ard Display nge Display nge Display nge Display	skRecordingForCSReplica Access level Full control Full control Full control Full control	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli TaskRecordingForCSRepli TaskRecordingForCSRepli		Additional securable object found in the task recording Additional securable object

i) Modify role

A new tab will be made visible. On this tab there will be an option to modify one or more existing roles based on a task recording. The task recording will be uploaded in the system, a

scenario will be automatically created and it will be added on the form along with all the menu items detected.

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

Demo	equests My view ∽ SR 1						
Request		уре	Origin	Area			
Demo Si	R1	Modify role	User requests	WHS	~		
Status							
Priority Normal		itatus Open	Owner Admin				
Modify re	ole						
ROLE							
Add role	e 🗊 Remove						
_	Role name	Description F	Role AOT name 1				
0	View lease	View of lease roles	ASSETLEASELEASEVIEW				
	O DETAILS						
Upload Scenario Demo1x	task recording						
Upload Scenario Demo1x	task recording recording.axtr p number Securable object	Securable type	Access level	Description	File name	Child scenario	† Remark
Upload Scenario Demo1x	task recording	Securable type Display	Access level Full control	Description Go to Accounts receivable > Orders > A		Child scenario	Î Remark
Upload Scenario Demo1x	task recording recording.axtr p number Securable object				Demo1x recording.axtr	Child scenario	Remark Additional securable obje found in the task recordin
Upload Scenario Demo1x	task recording recording.axtr p 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	recording.axtr p number Securable object 1 salestablelistpage 3 SalesTableDetails	Display Display	Full control	Go to Accounts receivable > Orders > A In the list, click the link in the selected r	Demo1x recording.axtr Demo1x recording.axtr	Child scenario	Additional securable obje
Upload Scenario Demo1x	task recording recording.axtr p number Securable object 1 salestablelistpage 3 SalesTableDetails 5 SalesCopyAllLines	Display Display Display	Full control Full control Full control	Go to Accounts receivable > Orders > A In the list, click the link in the selected r Click From all.	Demo1x recording.axtr Demo1x recording.axtr Demo1x recording.axtr	Child scenario	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.**

Gener			Туре	_	Origin		Area
Dem	o SR	81	Lock role	\sim	User requests	\checkmark	WHS
Priorit	у	~	Status Open		Owner Admin		
				_			
-							
0	9		ernal) v		USAPPLICANT		
	Reque Dem Status Priorit Norn Lock I + Ac	Request Demo SF Status Priority Normal Lock role: + Add O O	Request Demo SR 1 Status Priority Normal Lock roles Add Remove R	Request Type Lock role Priority Status Normal Cock roles Add Remove C Role name	Request Type Lock role Vana Control Co	Request Type Origin User requests Priority Status Owner Admin Lock roles + Add Remove O 2 Role name Name	Request Type Origin User requests ✓ Status Priority Status Owner Admin Lock roles + Add ® Remove O 2 Role name Name

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	Type Unlock role V	Origin User requests 🗸 🗸	Area WHS
itatus			
Priority Normal V	Status Open	Owner Admin	
Jnlock roles			
+ Add 🗊 Remove			
○ C Role name	Name		
 Warehouse worker 	WMSWAREHOUSEWORKER		

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	Ch.h.u	
Priority Normal	Status Open	Owner Admin
Delete role		
Add role 🔟 Remove		
○ C Role name	Description	Role AOT name
SCS_RoleTest_2		6DEC7811-E0C5-42C5-94
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										
Jem	O SK I										
General											
Request Demo S		Type Create rule	Origi Use	in r requests ->	Area WHS	\checkmark					
Status											
Priority Normal	I ~	Status Open	Own Adr								
	ed SoD rules										
	Remove										
		Туре	First		First access level	Second	Second securable object type			Effective to	Enabled
0	Create demo rule 2 from		AdvancedLedger $ \sim $		Create ~	BankChequeCompanyI \vee	Menu item display 🛛 🗸	Full control ~		12/31/2154 11:59:5 🖽 💿	_
	Create demo rule from SR	Duty	Maintain Absorption		No access	Import ZIP/postal codes		No access	4/28/2022 10:43:06 AM	5/26/2022 11:59:59 PM	

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.

	requests My view ∽ no SR 1									
Genera	al									
Reques Demo		Type Resolve conflict		rigin User requests	Area WHS	~				
Status										
Priority Norm		Status Open		wner Admin						
	ced SoD conflicts									
	d 🗊 Remove	Туре	User ID	First	Role	Second	New role	Resolution	Override reason	Role to remove
	Duty test1	Duty	APRIL	Approve budget plans	Budget clerk			Exclude		Existing role
	Test 1 V	Duty	EMMAH	PrintMgmtSetupUIMain	Sales clerk	ProjActivity	Sales representative	Override ~	Demo purpose	Existing role

o) Delete rule

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

Once the security request is approved all the rules will be deleted. They will be removed from

_		-		-							
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				
itatus	5										
Priorit			Status	Owner							
nont											
Norm											
Norm		\checkmark	Open	Admin							
	nal	ed SoD rules									
Delete	nal	ed SoD rules									
Delete + Ad	nal e enhanc	ed 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 Ə Nam	ed 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 d 🗊 Re O Nam SoD	end SoD rules emove ne 1	Open Type	Effective from						Menu item display	View
Delete	e enhanc d 🗊 Re O 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 d 🗊 Re O 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 d 🗊 Re O 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 d 🗊 Re O 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	<i>\</i> ∨						
General								
Request Demo S	iR 1	Type Add stand-	in		Drigin User requests	\checkmark	Area WHS	\sim
Status Priority Normal	\checkmark	Status Open)wner Admin			
Create st	tand-in							
	User ID	Stand-in	From date	To dat	e	Copy assigned organi	zations	
0	Admin	ALICIA ~	4/28/2022	₪ 4/30/	2022 📾			
Descript								

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.

eneral								
equest			Туре			Origin		Area
Demo S	R 1		Cancel sta	nd-in	\sim	User requ	ests	✓ WHS
tatus								
riority			Status			Owner		
Normal	\sim		Open			Admin		
	stand-in Remove User ID	Stand	in	From date		To date		Copy assigned organizati
	Admin	 ALICI 		4/28/2022	Ø	4/30/2022	6	

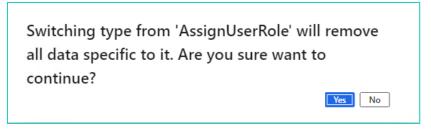
r) Create business risk

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

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

General			
Request Demo SR 1	Type Cancel stand-in	Origin User requests	Area WHS
Status			
Priority Normal	Status Open	Owner Admin	
Create business risk			
BUSINESS RISK Name Dmeo business risk Category	Area AssetLease	Mitigation Test Residual risk	Status Initial V
Strategic V SOD RULES	Very low	Very low	Ignore V
+ Add I Remove	Organization Risk		
✓ Test 1	✓ Dmeo business risk		

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.

Security Reques		onfiguration				
O Status	Default	ID	Name	Association	Туре	Instances Active vers
0	\checkmark	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 AOwner 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.

	\bigcirc Status \checkmark	
Л	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 param	eters	5
	General	Gen	era	I setup for the p	urchas	ed licenses
	License count	Open	adı	min.microsoft.com		
		LICEN	SE F	ARAMETERS INPUT		
	Data migration	0	С	License	1	No of licenses
		\circ		Activity users		15 d
	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				
る 品	Usage	O License type	Actual use I	Licensed 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
	ream 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.

3.2.3 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.

Create snapshot 🧏 Reset ;	pins Advanced v	iew Show joined Export to Exce	I OPTIONS O		∞ () () ∞
Security explorer: f	ull view				
SERS		ACCOUNTANT	DUTIES	PRIVILEGES	ENTRY POINTS
🕫 Pin users		x8 Unpin role	-⇔ Pin duty	🖙 Pin privilege	-sa Pin entry point
User ID	Name	Role name T	Duty name 1	Privilege name 1	Entry point (AOT name) 1
OSCAR	OSCAR	Accountant	Configure electronic fiscal	d	a 😑 🖂 AbatementCertificate_IN
RetailServiceAccount	RetailService	 Accounting manager 	Enable bank management	ç	al 🧧 🔅 AbatementPeriodicCertificate
STAN	STAN	 Accounting supervisor 	Enable electronic documer	Account number enhanced	Accountant_BR
		 Accounts payable centralize 	e Enable escheatment proce	s: account reference -ViewLee	d 🔳 🖂 Accountant_BR
		 Accounts payable clerk 	Enable EU sales list proces	AccountingSourceExplorer	V 🖆 AccountantElectronicAddress
		Accounts payable manager	Enable financial reports ge	n 🖷 Action class settings maint.	a 🗉 🖂 AccountantElectronicAddress
		Accounts payable payments	Enable fixed assets process	Action class settings view	AccountantElectronicAddress
		Accounts payable positive p	Enable Intrastat process	Action populate records ta	s 🔹 🖂 AccountantElectronicAddress

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

3.2.4 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		O Search for a page	2				Merge scenarios into one
=	🖪 Audit 🛛 🔀 Optimiz	e OPTIONS 🔎							5
									Name
	Security and	compliance stud	io						Description
	Summary		Security						
	۶ ^۹ 99	156	Requests	+ New 🖉 Edit 🖸 Match roles … More	Merge scena	rios			
				✓ 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	

3.2.5 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.

	\downarrow	Security	1	Merge	roles Duplicate role	Lock rol	es 🖧 Explore	Export Import	Mark active/inactive role
7		nequests	Ŀ		e name		ise type	Role description	Locked
ate role	Import users	Scenarios		✓ scs	5_Customer service represe	ent Ope	rations		\checkmark
		Users		SCS	5_CreateCustomer 5_Created from duties	Ope	rations rations		~
		Roles			e + New 🗈 Delete		is ,0		. *
		Duties		~	020070000000		Role (AOT name)		
		Segregation of duties		~	Auditor Cost accountant clerk	~	AUDITPOLICYM	the second s	

3.2.6 Recording steps to scenario.

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

≡	Ø 6	idit + New	🗊 Delete	Match roles	Merge scenarios	New from task recording	↑ Upload recording	Override permissions on roles	، در	» ()	p	Ü	ď	Х
7	S	CENARIO REC	CORDING STEPS											<
¥ ≡		General							Recording s	teps n	sadaiya	^		Related information
_		Scenario							Owner					d info
		Recording ste	eps						nsadaiya				L	rmatic
		Description										~	1	ă
		Description										·	U.	
		Access require	ed									^		
		+ Add ++ Ad	dd module acc	ess 🗊 Remove	යි Explore									
		✓ Step num	ber	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	eps		
		3		custt	ablelistpage	Display	Full contro	Go to Accounts	receivable > Cu	Record	ding ste	eps		
		7		custt	tablelistpage	Display	Full contro	Go to All custon	ners.	Record	ding ste	eps		
		8		Cust	Table	Display	Full contro	In the list, click t	he link in the sel	Record	ding ste	eps		

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.

3.2.7 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.

Scenario Owner Merged scenario nsadaiya Description Access required + Add +, Add module access @ Remove & Explore Step description ✓ Step number Securable type Access level Step description ✓ Step number Securable type Access level Step description File network ✓ Step number Securable type Access level Step description File network • DSMArea Display No access Step description File network • DSMArea Display Edit Step description File network Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable clerk Documents customer invoice proce Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Documents accounts receivable	General Merged scenario Ourner Merged scenario nsadaiya nsadaiya Description nsadaiya nsadaiya Access required - - + Add t, Add module access @ Remove ♣ Explore - - ✓ Step number Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description ✓ Step number Display No access - - - - DSMArea Display Edit - - Step description File name - - - - DSMArea Display Edit - - - DSMArea Documents accounts receivable - - Accounts receivable clerk Documents customer invoice ev - - Accounts receivable manager Reviews customer invoice proce - -	Edit 🕂 New 🗊 Delete	Match roles New from task record	rding ↑ Upload recording	Override permissions on roles	OPTIONS &	0	0	0
Scenario Owner Merged scenario nsadaiya Description Access required + Add +1, Add module access @ Remove & Explore Securable object Securable type ✓ Step number Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description File ne ✓ Step number Securable object Securable type Access level Step description File ne • DSMArea Display No access Securable type Access level Step description Securable contralized Display Edit Securable type Access level Step description Accounts receivable centralized Documents accounts receivable Documents customer invoice ev Image: Counts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Documents accounts receivable Image: Counts receivable payments c	Senario Ourrer nadajya Description Access required + Add t, Add module access @ Remove & Explore ✓ Step number Securable object Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description ✓ Step number Access level Step description Securable object Securable type Access level Step description Access level Step description Access level Step description Securable object Securable type Access level Step description Securable object Descurable type Access level Description Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents accounts receivable Accounts receivable payments c Documents accounts receiva	SCENARIO							
Merged scenario nsadaiya Description Access required + Add +, Add module access @ Remove & Explore Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access Step description • DSMArea Display No access Securable cype • DSMArea Display Edit	Merged scenario nsadaiya Description Access required + Add +, Add module access @ Remove ♣ Explore ✓ Step number Securable object Securable object Securable type Access twel Step description File name . AssetTableNew Display No access . DSMArea Display Edit . Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli	General					Merged	scenario	nsa
Merged scenario nsadaiya Description Access required + Add t, Add module access @ Remove & Explore Access level Step description ✓ Step number Securable object Securable type Access level Step description ✓ Step number Securable object Securable type Access level Step description File not securable object ✓ Step number Securable object Securable type Access level Step description File not securable object AssetTableNew Display No access No access Edit AssetTableNew Display Edit Edit Edit Edit Accounts receivable centralized Documents accounts receivable Edit Edit Edit Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Edit Accounts receivable manager Reviews customer invoice proce Documents accounts receivable Edit	Merged scenario nsadaiya Description Access required + Add +, Add module access @ Remove ♣ Explore ✓ Step number Securable object Securable object Securable type Access twel Step description File name . AssetTableNew Display No access . DSMArea Display Edit . Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli	Scenario					Owner		
Access required + Add t, Add module access @ Remove & Explore ✓ Securable type Access level Step description File reference ✓ Securable type Access Step description File reference ✓ Securable type Access Step description File reference ✓ Securable type Access Step description File reference AssetTableNew Display No access Step description File reference Sessign oveerride permissions to roles Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Documents accounts receivable Documents accounts receivable	Access required + Add t, Add module access								
Access required + Add t, Add module access @ Remove & Explore ✓ Securable type Access level Step description File reference ✓ Securable type Access Step description File reference ✓ Securable type Access Step description File reference ✓ Securable type Access Step description File reference AssetTableNew Display No access Step description File reference Sessign oveerride permissions to roles Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Documents accounts receivable Documents accounts receivable	Access required + Add t, Add module access								_
+ Add +, Add module access Remove Aspectable object Securable type Access level Step description File ne	Add th, Add module access Remove status type Securable type Access level Step description File name ✓ Step number AssetTableNew Display No access DSMArea Display Edit DSMArea Display Edit Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli	Description							
✓ Step number Securable object Securable type Access level Step description File na - AssetTableNew Display No access .	✓ Step number Securable object Securable type Access level Step description File name · AssetTableNew Display No access · DSMArea Display Edit ssign override permissions to roles Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli	Access required							
✓ Step number Securable object Securable type Access level Step description File na - AssetTableNew Display No access .	✓ Step number Securable object Securable type Access level Step description File name · AssetTableNew Display No access · DSMArea Display Edit ssign override permissions to roles Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli	+ Add + Add module acce	ess 🗎 Remove 🖧 Explore						
DSMArea Display Edit Accounts receivable centralized Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable	DSMArea Display Edit Set of the permissions to roles Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli			Securable type	Access level	Step description		Fil	e name
Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable	ssign override permissions to roles Accounts receivable centralized Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor		AssetTableNew	Display	No access				
Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable	ssign override permissions to roles Accounts receivable centralized Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor								
Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable	Accounts receivable centralized Documents accounts receivable Accounts receivable clerk Documents customer invoice ev Accounts receivable manager Reviews customer invoice proce Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli		DSMArea	Display	Edit				
Accounts receivable payments c Documents accounts receivable	Accounts receivable payments c Documents accounts receivable Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli	_	-		counts receivable	•		I	
	Applicant anonymous (external) External user application for em Auditor Manages and reviews audit poli	Accounts re	ceivable centralized	Documents ac				I	
Applicant energy (automal) External user explication for en	Auditor Manages and reviews audit poli	Accounts re Accounts re	ceivable centralized ceivable clerk	Documents ac	stomer invoice ev	/		I	
Applicant anonymous (external) External user application for em		Accounts re Accounts re Accounts re	ceivable centralized ceivable clerk ceivable manager	Documents ac Documents cu Reviews custor	stomer invoice ev mer invoice proce	·		I	
Auditor Manages and reviews audit poli	Batch job manager Maintain and configure settings	Accounts re Accounts re Accounts re Accounts re	ceivable centralized ceivable clerk ceivable manager ceivable payments c	Documents ac Documents cu Reviews custor Documents ac	stomer invoice ev mer invoice proce counts receivable	/ 2		I	
Batch job manager Maintain and configure settings		Accounts re Accounts re Accounts re Accounts re Accounts re Applicant ar	ceivable centralized ceivable clerk ceivable manager ceivable payments c	Documents ac Documents cu Reviews custor Documents ac External user a	stomer invoice ev mer invoice proce counts receivable pplication for em	/ 2		I	
t custom permissions		Accounts re Accounts re Accounts re Accounts re Applicant ar Auditor Batch job m	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external)	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			
		Accounts re- Accounts re- Accounts re- Accounts re- Applicant ar Auditor Batch job m	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external)	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·		1	
•		Accounts re Accounts re Accounts re Accounts re Applicant ar Auditor Batch job m	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external)	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			
	RMISSIONS	Accounts re- Accounts re- Accounts re- Accounts re- Applicant ar Auditor Batch job m et custom permission o	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external)	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			
o CRMISSIONS tad 0 Unset Grant Deny	RMISSIONS ad Unset O Grant O Deny	Accounts re- Accounts re- Accounts re- Accounts re- Applicant ar Auditor Batch job m et custom permission o • Co Co Co Co Co Co Co Co Co Co Co Co Co	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external) manager	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			
o CRMISSIONS ead Unset Grant Deny pdate	RMISSIONS ad Unset Grant Deny idate	Accounts re- Accounts re- Accounts re- Accounts re- Applicant ar Auditor Batch job m et custom permission o • et custom permission	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external) aanager ons	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			
o CRMISSIONS ead 0 Unset Grant Deny pdate 0 Unset Grant Deny	RMISSIONS ad Unset Grant Deny idate Unset Grant Deny	Accounts re- Accounts re- Accounts re- Accounts re- Accounts re- Applicant ar Auditor Batch job m et custom permission o • CRMISSIONS ead Unset Gra pdate Unset Gra	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external) aanager ons	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			
et custom permissions o ERMISSIONS ead Unset Grant Deny pdate Unset Grant Deny reate Unset Grant Deny	RMISSIONS ad Unset Grant Deny odate Unset Grant Deny eate	Accounts re- Accounts re- Accounts re- Accounts re- Applicant ar Auditor Batch job m et custom permission o • et custom permission o • et custom servission o • et custom servison o • e	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external) manager ons ant Deny	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			
o Grant Deny pdate Unset Grant Deny pdate Unset Grant Deny reate	RMISSIONS ad Unset Grant Deny date Unset Grant Deny eate Unset Grant Deny	Accounts re- Accounts re- Accounts re- Accounts re- Applicant ar Auditor Batch job m at custom permission o • CRMISSIONS Bad O Unset Gra podate O Unset Gra	ceivable centralized ceivable clerk ceivable manager ceivable payments c nonymous (external) manager ons ant Deny	Documents ac Documents cu Reviews custor Documents ac External user a Manages and	stomer invoice ev mer invoice proce counts receivable pplication for em reviews audit poli	·			

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

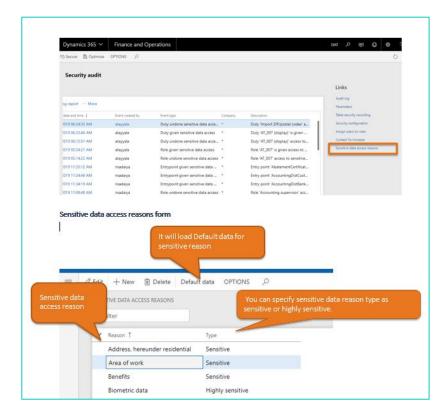
ОК

Cancel

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

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

• Set up sensitive data access reasons



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

=	🖔 Create snapshot	🔊 Reset pins 🛛 Advance	d view Show joined O	PTIONS ,O				0	•	J 🖗	0 O	с х
V	Security expl users -⇔ Pin users …	lorer: full view ROLES -⇔ Pin role		DUTIES -⇔ Pin duty	Give sensitive data access		PRIVILEGES -⊐ Pin privile	ge ···		ENTRY POI ⊣⊐ Pin e	INTS entry poin	nt ···
	✓ Pin User	ID 🗸 Pin	Role name 1	✓ Pin	Duty name 1	Access to sensiti	✓ Pin	Privilege		✓ Pin		Entry po
	\$COE	ЗА	Accounts payable	~	A parameter that is used to gro			A param				3 Abaten
	Adm				Access benefits workspace		•	Accept a			• •	3 Abaten
	ALIC		Accounts payable		Access expense management w			Access Ł			• C) Abaten
	APRI	ι .	Accounts receivabl		Access workforce management	✓		Access c			• 0) Abbrev
	ARN		Accounts receivabl		Activate tax depreciation process	✓		Access e				1 Accour
	 atayy 	yala	Accounts receivabl		Activate, deactivate, update and			Access e				f Accour
	axrui	nner	Accounts receivabl		Add an existing performance jo			Access r			• •	f Accour
	BENJ	JAMIN	Applicant anonym		Add custom fields			Access v			• •	f Accour
	BRAI	D	AT_		Application document entities			Account				f Accour
	BRO	OKE	AT 007		Approve absences	~		account			• •	1 Accour

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	۵	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.

_	mics 365 ∨ Finar	ace and Operations Ac	counts receivable > Custom	hers > All customers		DAT ,O	ġ	© (9 ? 9	a.
/ANAGE	OPTIONS D						**	a 🕻	0	×
MATCH F	ROLES AND SENSITIVE DATA ACC	ESS								
Matc	ch roles									
	Menu item display	DSMScenario	Full control	No access		art of the selected role.				
	Menu item display	DSMSecurityManagementTie		No access		art of the selected role.				
~	Menu item display	CustTablel istPage	Full control	View	✓					
	Menu item display	ForecastSalesTable	Full control	No access	Not p	art of the selected role.				L
L										
Roles									^	
~	Role name	Role description	Matc User license type	Remaining use	er					
	Project manager	Documents the project forec	ast/ 50.00 Operations	599	928					
	Production planner	Schedules and plans produc	tions 50.00 Operations	599	928				1	
	Sales manager	Reviews sales process perfor	ma 50.00 Operations	599	928					
~	Sales representative	Documents sales events and	res 25.00 Activity users	299	986				-	
	Materials manager	Enables and reviews processe	es, 25.00 Operations	599	928					
	Bardination account	Builden also and a second second second			0.00					
s that giv	ve access to the securable	objects that cannot be accessed v	with the selected role.							^
Duty na	ame	Privilege name	Securable object type	Securable of	bject	Access level		Duty I	license type	
Enable	e the demand forecasting	Maintain demand forecasts for i	i Menu item display	ForecastS	alesTable	Full control		Oper	ations	
	ain project budgets	View demand forecasts for item		ForecastS	alesTable	View			ity users	
Mainta	ain project forecasts	Maintain demand forecasts for i	i Menu item display	ForecastS	alesTable	Full control			ity users	
	e into project forecast stat.			ForecastS		View			members	
	ain authorization of adjust.			ForecastS		View			ations	
	ain authorization of adjust.			ForecastS		Full control			ations	
		And the second second				e 11 - 1 - 1		0		•
eges that	t give access to the secura	ble objects that cannot be accesse	ed with the selected role.							^
Privilege	e name	Securable object type	Securable object	Access leve		Privilege license type	Meni	item licens	se tyne	
	and forecasts for item N		ForecastSalesTable	View		m members	Team me			-
	lemand forecasts for i N		ForecastSalesTable	Full control	Act	ivity users	Activity u	sers		
aintain de	15									^
aintain de		Privilege name	Securable object type	Securable of	bject	Access level		Duty li	cense type	^
ed dutie		Privilege name View demand forecasts for item		Securable of ForecastSz		Access level View		Duty li Opera		^
ed dutie Duty nar	me		Menu item display		lesTable				ations	^
ed dutie Duty nar Inquire Enable	me e into demand forecasts	View demand forecasts for item	Menu item display	ForecastSa	elesTable elesTable	View		Opera Opera	ations	^
ed dutie Duty nar Inquire Enable Maintai	me : into demand forecasts : the demand forecasting	View demand forecasts for item Maintain demand forecasts for i	 Menu item display Menu item display Menu item display 	ForecastSa ForecastSa	ilesTable ilesTable ilesTable	View Full control		Opera Opera Activi	ations	~
ed dutie Duty nar Inquire Enable Maintai Maintai	me = into demand forecasts = the demand forecasting sin project budgets	View demand forecasts for item Maintain demand forecasts for i. View demand forecasts for item Maintain demand forecasts for i.	 Menu item display Menu item display Menu item display Menu item display 	ForecastSa ForecastSa ForecastSa	ilesTable ilesTable ilesTable ilesTable	View Full control View		Opera Opera Activi Activi	ations ations ty users	

• 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	<u>م</u>							
	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 – Sensitive data 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 Dyn	namics 365 🗸 🛛 Finance	and Operations			DAT	م	¢.	٢	۲	?	4
🚍 🖓 Sec	cure 🖺 Optimize OPTIONS	Q							C) []	×
Se	curity audit Audit										
	A Snapshots Roles – Sensitive data access Duties – Sensitive data access	Import ZIP/postal codes Approve advanced ledger entry view and maintain advanced ledger entry pro Inquire about advance holder ac	view advanced ledger entry pro							1	I
	Privileges – Sensitive data access Users – Sensitive data access	Roles Privileges Segregation ✓ Role name Accounting manager	Role description Reviews accounting, customer L.	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.

	Dynamics 365 V Financ	e and Operations		DAT ,O	Ē	٢	۵	?	64
=	Secure Doptimize OPTIONS	<u>م</u>					(ບ ⊏	3 >
	Security audit Audit								
	Snapshots	a Explore							
	Roles – Sensitive data access	Privilege name Privilege identifier users of the second sec	Privilege description Create and update add-on item						
	Duties – Sensitive data access	Generate fixed asset additions r ASSETADDITIONMOGENERATE View asset additions ASSETADDITIONVIEW	Generate a list of fixed assets an View add-on items and improve						1
	Privileges – Sensitive data access	Maintain depreciation settleme ASSETADVRULE_PRETAXDEDUC View depreciation settlement ru ASSETADVRULE_PRETAXDEDUC							
	Users – Sensitive data access	Roles Duties							
	Charts	✓ Duty name Duty identifier ♥ Maintain fixed assets ASSETFIXEDASSETSMAINTAIN	Duty description 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.

G Secure	Doptimize OPTIONS	2							0 🗆
Secu	rity audit								
	Audit								
		~	User ID 1	Name	E	mail	License type	Company	Person
	Snapshots		\$COBA	\$C0BA	S	COBA@contosoax7.onmicrosof	Team members	dat	
	Roles – Sensitive data		ALICIA	ALICIA	A	ALICIA@contosoax7.onmicrosof	Operations	USMF	Alicia Thor
ac	access		APRIL	APRIL	A	APRIL@contosoax7.onmicrosoft	Operations	USMF	
	Duties – Sensitive		ARNIE	ARNIE	A	ARNIE@contosoax7.onmicrosof	Operations	USMF	
	data access		atayyala	Anil Kumar Ta	yyala (TI) a	tayyala@ToIncrease.onmicroso	Operations	USMF	
	Privileges – Sensitive	1.7							
	data access	Ro	es History						
	Users – Sensitive data		Role name	Ro	le description	Level Compa	any accounts ID		
	access		Office integratio	n power user		3 *			
	Charts		System user	Sy	stem role for all users	2 *			

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

	Dynamics	s 365 🗸 🛛 Finance a	nd Operations								DAT	Q	Ð	٢	۵	?	1
≡	🗟 Secure [ر Optimize OPTIONS)												Ċ) 다	×
	Security	y audit Audit															
		Snapshots	Number of secu	rity objec	ts with ac	cess to s	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 Total numi	6k ber of securit	8k y objects	10k	12k	14k							I
					Total num	per of securit	y objects										

o Number of users with access to sensitive data per organization



o Number of roles per user with access to sensitive data

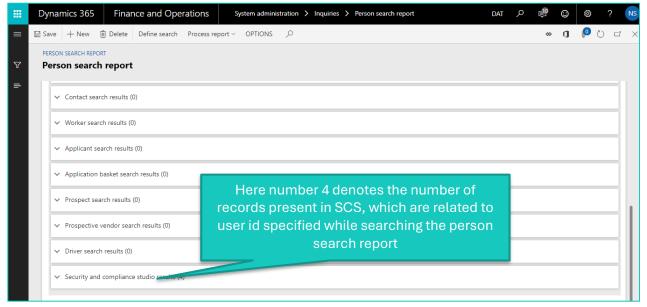
	Dynamics 365	Finance and Operations DAT P 🖾 🎯 ? 🖪	5
≡	🕞 Secure 🛛 Dptimize	OPTIONS A C	×
	Security audit Audit	Lir	
	Snapshots	Number of roles per user with access to sensitive data \lor Autors Scotta	
	Roles – Sensitive dat access	CONNE dtjisen EMMAH	
	Duties – Sensitive data access	iontu Cor JRIMIN ALLA ALLA Sent	
	Privileges – Sensitive data access		
	Users – Sensitive dat access		
	Charts	Voidhro0 0 5 10 15 20 25 20	

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	

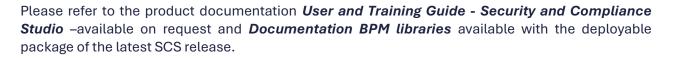
• Person search report extension

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/dev-itpro/gdpr/gdpr-person-search-report. You can find person search report at System administration > Inquires > person search report. Below image is a screen shot of the person search report.



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		Description		Type General		Status
~	✓	nsadaiya		Add accountant	idd accountant role					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	title	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	



3.2.9 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
\checkmark	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 CREA	EATE ROLE	 CREATE DUTY	SEGREGATION OF DUTIES	VIEW	ASSIGN TO USER
	eate role Cr eate role from privileges Du	Create duty from privileges	Create SOD	Simple Advanced	Assign users to role

Enter the new duty name and the description.

arameters		
Duty name SCS		Description
Security objects t	hat are includ	led into the new duty
Security objects t	hat are includ	led into the new duty
	hat are includ	led into the new duty
,∕P Filter	Label	led into the new duty tant_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.

3.2.10 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	

3.2.11 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.

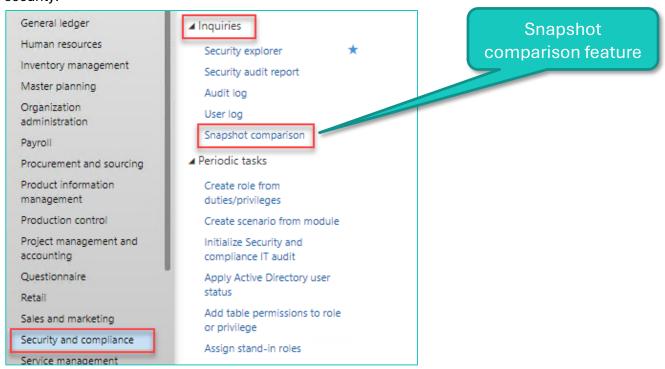




Fig 1. Snapshot comparison path

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

Dy	namics 365 💊	Finance and	Operations Security	and complian	ce > Inquiries > Snapshot co	mpariso	n	
层 Sa	ve MANAGE	OPTIONS P						
Full o	pare selected	VIEW Show all objects Advanced view 2.						
	inapshot co Itter Elect security objec Entry Point Privilege Duty Role User OMPARE SAAPSHO omprare SAAPSHO 2	ttype 3.				Se	icand snapshot	
	✓ Name		User license type	Compared	Observation	•	✓ Name	User license type
	Action graph		Operations	Yes	3 modifications found		Demo privilege 1	Operations
	DSMAreaEnti	tyMaintain	None	Yes	1 modifications found		Demo privilege 2	Operations
	Florin privileg	e 2	None	Yes	0 modifications found		Maintain bar codes	Operations
5.	IFFERENCES							
	Property	Value fre	m first snapshot	Volue fi	rom second snapshot			
	Entry point ac		in macanopanoc		uditLogInit		-	
6.	Entry point ac Entry point ac				ergeRoles			
	Entry point ac				andInClass		-	
		I						

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

ynamics 365 🗸 🛛 Finan	ce and Operations Secur	ty and complian	ce > Inquiries > Snapshot o	ompa	irison		
ave MANAGE OPTIONS ,							
MPARE VIEW Impare selected I compare Advanced view							
Snapshot compariso FILTER Select security object type Entry Point Privilege Duty	n						
Role User COMPARE SNAPSHOTS First snapshot 2					Seco	ind snapshot	
User COMPARE SNAPSHOTS First snapshot	User license type	Compared	Observation				User license type
User COMPARE SNAPSHOTS First snapshot 2		Compared Yes	Observation 0 modifications found	-	3	~	User license type Operations
User COMPARE SNAPSHOTS First snapshot 2 V Name 1					3	Name î	
User COMPARE SNAPSHOTS First snapshot 2 V Name 1 Action class settings mainta	in None	Yes	0 modifications found		3	Name 1 Delete write-off factors	Operations
User COMPARE SNAPSHOTS First snapshot 2 V Name 1 Action class settings mainta Action class settings view	in None None Operations	Yes Yes	0 modifications found 0 modifications found	-	3	Name T Delete write-off factors Demand Forecasting external API se	Operations None
User COMPARE SNAPSHOTS First snapshot 2 Name 1 Action class settings mainta Action class settings view Action graph	in 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
User COMPARE SNAPSHOTS First snapshot 2 V Name 1 Action class settings mainta Action class settings view Action populate records tas	iin None None Operations k maint None Operations	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 None 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 Op	erations Security and compliance	e > Inquiries > Snapshot.com	parison				
Save MANAGE OPTIONS P							
COMPARE VIEW Show changes only Full compare Simple view							
Snapshot comparison FILTR Select security ebject type © Entry Point © Drivilegg © Duty © Role © User COMPARE SNAPSHOTS First regenerat [2]			1		Second snapshot	1	
✓ Identifier	Name 1	User license type		Observation	Vendprospectivevendordataa	Name 1	Jser license type Team members
FORECASTPOSITIONSBYBUDGETPLANG.		Team members	Yes	0 modifications found		Deny changing company account Deny fixed compensation change re	Feam members
PURCHRFQFORMLETTER_ACCEPTPROCE		Activity users	Yes	0 modifications found	TMSINVOICEAPPROVALDENYPROC		Team members
HCMBENEFITWORKSPACE	Access benefits workspace	Team members	Yes	0 modifications found			Feam members
HCMCOMPENSATIONWORKSPACE	Access compensation management.	Operations	Yes	0 modifications found			Feam members
TRVEXPENSEADMINANALYTICS	Access expense administrator analy.		Yes	0 modifications found		- /	Team members
TRVEXPENSEWORKSPACE	Access expense management work	Team members	Yes	0 modifications found		Deny worker actions by using a wor	Feam members
HCMRECRUITMENTWORKSPACE	Access recruitment management w	Team members	Yes	0 modifications found	DIMEASUDEMENTDEDLOVAAANAGE	Denty worker actions by using a work.	N
DIFFERENCES							

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	-		

3.2.12 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.

iecurity au ummary	udit	Audit						
summary		Addit						
• •	2 =-	Security history	📓 Audit log report 🛛 … More					
			✓ Event date and time ↓	Event created by	Event type	Company	Description	
Changes tracked	Role changes	Role history	5/15/2018 05:22:19 AM	Admin	Entry point created	dat	Entry point New entry point from AOT of	reated (from AOT)
IIdekeu			5/15/2018 05:19:58 AM	Admin	Entry point deleted	dat	Entry point Active directory users delete	ed (from AOT)
x ⁸	D	User history	5/15/2018 05:18:30 AM	Admin	Privilege modified	dat	Privilege Maintain Dynamic Security Ma	nagement IT Audit modified (from
×	<u>~</u>		5/15/2018 05:18:19 AM	Admin	Privilege modified	dat	Privilege Florin privilege 1 modified (fro	m AOT) changes
		Segregation of duties rules	✓ 5/15/2018 05:18:16 AM	Admin	Privilege modified	dat	Privilege DSMParametersEntityView mo	dified (from AOT) made
User changes	Stand-ins	dutes fores	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 (1	rom AOT)
A	Ro	duties conflicts	5/15/2018 05:16:43 AM	Admin	Privilege modified	dat	Privilege Apply action modified (from A	OT)
			5/15/2018 05:14:45 AM	Admin	Duty modified	dat	Duty Maintain security recording modif	ied (from AOT)
	Segregation of	Stand-ins	5/15/2018 05:14:45 AM	Admin	Duty modified	dat	Duty Florin Duty 1 modified (from AOT)	
Locked roles	duties rules		5/15/2018 05:14:34 AM	Admin	Duty modified	dat	Duty Approve BOMs modified (from AC	סד)
		Data security	5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty FlorinDutyUITest created (from AC	T)
÷	옮		5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty Duty created from AOT created (fr	om AOT)
		Azure AD domains	5/15/2018 05:14:04 AM	Admin	Role modified	dat	Role Full read access modified (from AC)T)
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)	
			5/15/2018 05:13:52 AM	Admin	Role created	dat	Role FlorinRoleUITest created (from AO	D)
		Charts	5/15/2018 05:13:15 AM	Admin	Role modified	dat	Role Chief executive officer modified (fr	om 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).

3.2.13 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		



3.2.14 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.

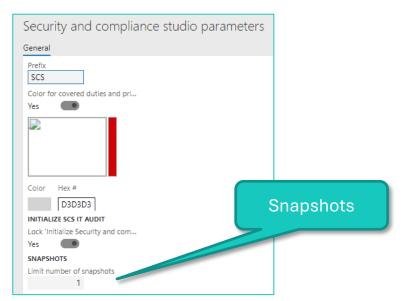
Dynam	ics 365 🗸 🛛 Finance and	d Operations						
🗟 Save	+New 💼 Delete 🛛 Match r	oles 🛛 🔵 New from tasl	k recording ☐ Upload recording	OPTIONS D			Area	
PERSONAL	IZE PAGE OPTIONS		EDIT SHARE				WHICH MODULE?	
	en for editing Security diagnosti	cs Record info	Read mode Get a link 🗸				✓ Area î	
		ort Change view 🗸	Revert				Accounts payable	
Add to wa	rkspace 🗸						Accounts receivab	le
							Audit workbench	
SCENA	RIO						Budgeting	
Gen	eral			Add modu	ile	ARScenario vsingh	Cash and bank ma	anagement
				/ aa moac	100		Common	
							Consolidations	
	Sections					(singh	Cost accounting	
Desc	ription						Cost managemen	
Dest							Credit and collect	ons
Acce	ss required						Demo data	
							Expense manager Fiscal books	ient
+	Add 🕂 Add module access 🔳	Remove 🚓 Explore					Fixed assets	
~	Securable object	Securable object type	Access level	File	Remark		Fixed assets Fleet managemen	
	CustomerInvoiceWorkspace	Menu item display	View 🗸				General ledger	<u> </u>
	CustPaymentWorkspace	Menu item display	View			_	No access	· ·
			No				View	lent
							Edit	
	CustTableHoldListPage	Menu item display	View				Create	istration
	CustTablePastDueListPage	Menu item display	View				Correction Full control	
	ARScenario Owner View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item display View CustTableHoldListPage Menu item displa							_
	CalasTablel intDeas		View			_	No access	/
							Create request	
Files								Ok 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.

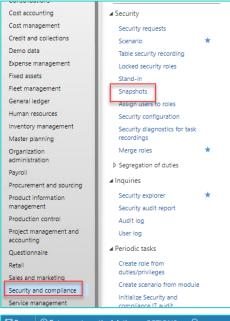
ATCHIN	IG	CREATE ROLE			SEGREGATION	OF DUT	IES VIEW	ASSIG	N TO USER	
Match roles Create role Find matched entry points Create role from privileges Reset data			Create role from duties Create SOD eges Duplicate role			Simple Advanced		Assign users to role		
	^{ENARIO} tch roles									
Secu	irable objects									
~	Securable object type	e Secur	able object		Required access	M	laximum access on r	ole	Remark	
	Menu item display	Custo	omerInvoiceV	Vorkspace	View	٧	iew	~		
	Menu item display	Cust	PavmentWorl	kspace	View	V	iew	~		
	Coourity	roloo mot	ob do	dro o	liew	F	ull control	~		
	Security	roles mat	cnue	gree	/iew	V	iew	~		
	Menu item display	Cust	0	qe	√iew	V	iew	~		
	Menu item display	MCR	CustUnme	the state	View	N	lo access		Not part of the selected rol	
	Menu item display	Sales	SalesTableListPage		View V		View			
Role	s									
~	Role name	R	ole descriptio	n	Match de	gree 1	User license type		Remaining user lice	
	Accounts receivable	e manager 🛛 R	leviews custo	mer invoice pro	o 72.81		1 Operations		59933	
	Accounting manag	er R	eviews accou	unting, custome.		68.66	Operations		59933	
	Accounts receivable	e clerk 🛛 🛛	Documents customer invoice .		68.66		Operations		59933	
	Accountant	C	Documents accounting event			60.37	Operations		59933	
	Accounting supervi	sor R	leviews accou	unting process p		57.14	Operations		59933	
	Collections manager		ons manager Reviews collections process p.		53.92 Operations			59933		
	concetions manage	er R	eviews colleg	ctions process p.		33.92	operations			

3.2.15 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.



"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'.

3.2.16 Improved "Create role wizard" based on a grid framework

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

CRE	ATE ROLE												
-													
All	All duties												
Sel	ect duties to be add	ed to the n	ew role										
	AILABLE DUTIES							SELI	ECTED DUTIES				
5	/ Duty		Description		User license type			~	Duty		Descript	ion	User license type
	Maintain Absorptio	n Costs			Operations		\rightarrow		Inquire into Abso	orption Costs			Team members
	Import ZIP/postal co	odes			Operations				Inquire into pure	chase agreem	Respon	d to inquiries about p	Team members
	Approve advanced	edger ent	Approve ad	lvanced ledger ent	Operations		\leftarrow						
	view and maintain a	dvanced I	View and m	naintain advanced I	Team members								
	view advanced ledg	er entry p	view advan	ced ledger entry p	Team members	R	ole	lic	ense ty	vpe			
									-				
						b	etoi	e	you fin	ish			
CREA	TE ROLE												
Sun	imary					_							
Reut	ew the selected role setup	Click Finish to	create the role										
	ew the selected role setup e resulting role will have the u	Г											
	e name	Role description	operation										
SC	S_NewRole	SCS_NewRole											
	cted privileges			њ I						elected duties			
_	vilege name port KLADR abbreviations	Description	tions from th	License type. Operations					_	Duty name Inquire into Absorption		Description	License type. Team Members
	ew accounting distributions	pore apprevia	and a second state	Team Members						1 State 1 Stat		Respond to inquiries about p	Team Members

3.2.17 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 diagr	nostics		Security explorer icon
This is the list of securit	ty 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.



lebuild	l data	🕫 Res	et pins – Si	imple view Show joi	ned Ol	PTIONS ,P													0 9 0
Secu	urity	explo	orer: ful	ll view															
USERS	s				cours	CTIONS AGENT			DUTI	165		PRIVI	ILEG	ES		ENTRY POIN	(TS		
-ta Pi	in user	rs			x≩ U	npin role			-64 (Pin duty		-to p	Pin p	rivilege		-t= Pin ent	ry point		
	Us	ser ID 1	Name	Highest license typ		Role name 1		License type		Duty name 1	License type			Privilege name 1	License type	×	Entry point (AOT name) 1	Access right	Entry point type
	 A5 	RNIE	ARNIE	Operations	-63	 Collections a 	gent	Operations		Collections workspace	Team members			Calculate interest notes	Operations		☐ AccountingDistCustFreeInvoice	View	Menu item dis
	• Co	onnie	CONNIE	Operations						Inquire into bill of exchange s.	Team members		•	Cancel collection letters	Operations		C AccountingDistCustInvJour	View	Menu item di
	• 09	SCAR	OSCAR	Operations						Inquire into collections status			•	Cancel interest notes	Operations		☐ AccountingDistMarkupTransInv	View	Menu item di
	. SA	ARA	SARA	Operations						Inquire into credit card proce-	Team members			CashDiscountEntityView	None		□ AccountingDistMarkupTransPO	View	Menu item di
										Inquire into customer invoice	Activity users		•	Change transaction collection	Operations		AccountingDistMarkupTransR	View	Menu item d
										Inquire into customer master	Team members		•	Change/edit customer transa	Activity users		□ AccountingDistPurchTable	View	Menu item d
										Inquire into customer payme	Activity users		•	Change/edit customer transa	Operations		AccountingDistributions	View	Menu item d
										Inquire into customer referen.	. Team members		•	Change/edit customer transa	Operations		□ AccountingDistributionsDocu	View	Menu item d
										Maintain activities	Team members			Correct interest codes	Team members		AccountingDistTaxTransTmp	View	Menu item d
										 Maintain collections transacti. 	Operations		•	Create a customer record fro	Operations		☐ AccountingDistVendEditInvDe	View	Menu item d
										 Maintain contacts 	Activity users		•	Create a customer record fro	Operations		AccountingDistVendEditInvHdr	View	Menu item d
										 Maintain customer master 	Operations			Create collection letters	Team members		□ ActivitiesMain	View	Menu item d
										Maintain financial period clos.	None		•	Creating a customer from pro	Operations		□ ActivitiesMain	Full control	Menu item d
										Maintain periodic settlement .	Operations			CustBalanceGenerate_CN	Team members		□ ActivitiesMainBasic	View	Menu item di
										Manage customer credit and .	Team members			CustCustomerGroupEntityView	None		□ ActivitiesMainBasic	Full control	Menu item d
										View sensitive bank account i.	None			CustDirectDebitMandateEntit	None		□ ActivityViewRecord	View	Menu item di

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

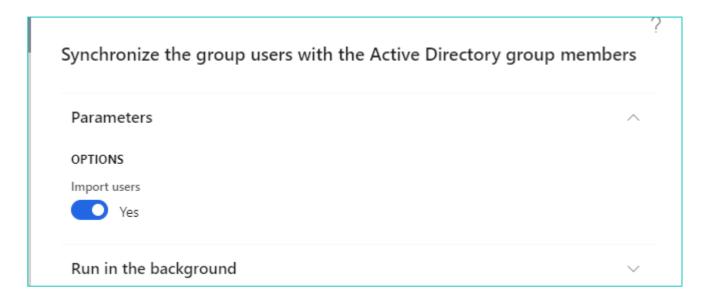
You now have an option to create duties along with the privileges while using the "Merge roles" feature. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.).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

Roles 'Accounting manager' and 'Accountant'	are in violation of segrega	tion of du	ities r	ule 'l	New Segregation of duties rule2':	
MERGE ROLES						
Select or enter the role to merge to. TARGET ROLE Name Lock ta SCS_AccountingSuperUser V Yes	irget role?				SOD violat	tions
Select the roles to merge from.						
AVAILABLE ROLES				SELE	ECTED ROLES	
✓ Available roles				~	Selected roles	
Accounting supervisor			\rightarrow		Accounting manager	
Accounts payable centralized payme	ents clerk		\leftarrow		Accountant	
Accounts payable clerk		11. 1				
Accounts payable manager						
Accounts payable payments clerk						
ENABLED PRI	VILEGE NAME					
ACTION MENU ITEMS	CS_AccountingSuperU	ser 🗸]			
DISPLAY MENU ITEMS	CS_AccountingSuperU	ser ∨	j			
	CS_AccountingSuperU	ser ∨]			
TABLE PERMISSIONS						
CREATE DUTY	Create duty					
Yes						
ENABLED DUT	Y NAME					
ACTION PRIVILEGES 🔽 SCS	_AccountingSuperUse	r∨				
DISPLAY PRIVILEGES 🗹 SCS	_AccountingSuperUse	er 🗸				
OUTPUT PRIVILEGES 🗹 SCS	_AccountingSuperUse	er 🗸				
	_AccountingSuperUse					



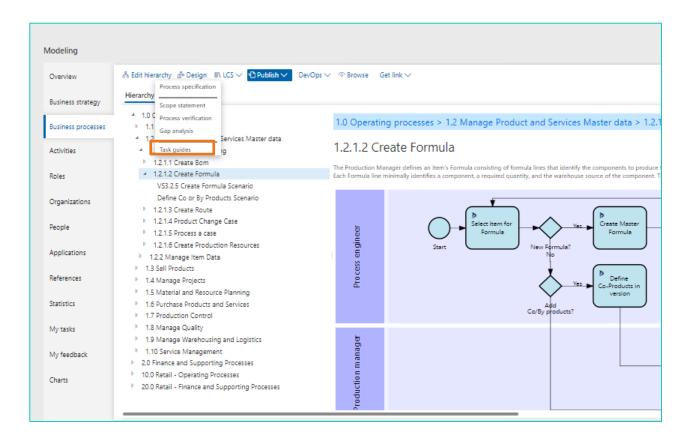
This is very useful for offline analysis and drill down of the required security setup in a company or department. We added a new small feature to our Azure AD group synchronization job. On the dialog of the Synchronize the group users with the Active Directory group members, we introduced a new parameter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



3.2.20 Uptake RapidValue BPM Suite Scenarios directly as SCS Security Scenarios

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



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

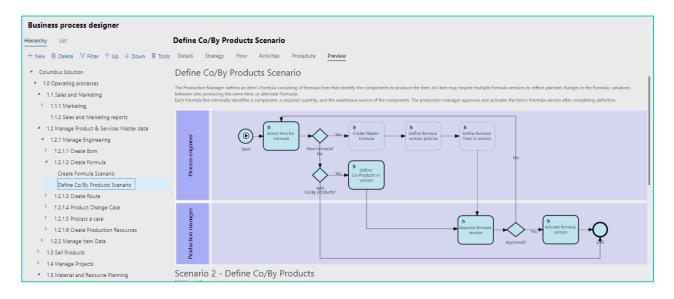


Figure: Scenario-Procedure activity based modeling



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		r
	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 modeling with recorded steps linked to flow activities

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

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

Security 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.

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

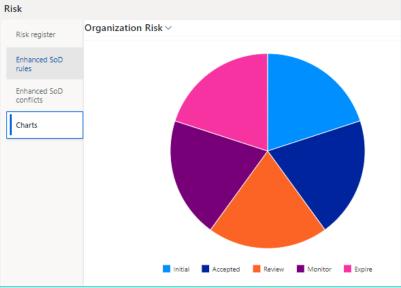


	✓ Name ↑	Туре	First		First securable object type	First access level	Second
Enhanced SoD rules	Demo rule for Entry points	Entry point	AccountingDistV	/endEditInvHdr	Menu item display	Create	AdvancedLedgerEntryDateDr
	Match role test - ep 1	Entry point	AuditPolicyCase	Group	Menu item display	Full control	ACOJournalPost_BR
inhanced SoD	Match roles test - duty	Duty	Maintain Absorp	otion Costs		No access	Maintain audit policies
conflicts	Match roles test - duty 2	Duty	Maintain audit p	olicies		No access	Maintain Absorption Costs
Charts	Match roles test - ep 2	Entry point	ACOJournalPost	BR	Menu item action	Full control	AuditPolicyCaseGroup
churca	Match roles test - ep 3	Entry point	DSMSecurityReq	questPriorityH	Menu item action	Correction	ACOJournalPost_BR
	Match roles test - ep 4	Entry point	DSMMultiSelecti	RoleSetup	Menu item display	Full control	DSMSecurityRequestPriorityH.
	Match roles test - priv 1	Privilege	Maintain case gr	rouping criteria		No access	Maintain Absorption Costs
	Match roles test - priv 2	Privilege	Maintain Absorp	otion Costs		No access	Maintain case grouping criteria
	Risk						
	✓ Risk ID	Category	Status	Inherit ris	ik Response	Residual risk	Owner
	Risk-00000006	Operational	Initial	Medium	Accept	Low	Admin
	Risk-00000007	Strategic	Initial	Very low	Ignore	Very low	Admin

3.2.22 Organization risk Register

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

Summary		Risk											
+	Q 4	Risk register	+ N	lew 🖉 Edit									
			~	Risk ID 1	Name		Category	Status	Inherit risk	Response	Residual ris	k Owner	
Create a risk	Risk	Enhanced SoD rules		Risk-000000005	Risk related to Org St	rategy	Strategic	Initial	High	Ignore	Very low	Admin	
				Risk-000000006	Risk related to Org O	perations	Operational	Initial	Medium	Accept	Low	Admin	
ጼ 124	$\bigotimes 0$	Enhanced SoD		Risk-00000007	Risk related to Org St	rategy an	d Strategic	Initial	Very low	Ignore	Very low	Admin	
	Ŭ	conflicts		Risk-00000008	Risk DEMO		Operational	Review	Medium	Mitigate	Low	Admin	
Enhanced SoD rules	Enhanced SoD conflicts	Charts											
			Enh	anced SoD rules									
			~	Name		Туре	First	1	First securable object	ct type F	irst access level	Second	Second securab
				SCS-093-Create s	ales order and reserv	Duty	Maintain sales order			N	lo access	Maintain on-hand inventory r	
				SCS-094-Create p	ourchase order and r	Duty	Maintain inventory regi	strati		N	lo access	Maintain purchase orders	





3.2.23 AAD related SoD Validations across SCS

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

3.2.24 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



3.2.25 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.

3.2.26 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 ı	managemen	t					
Summary		Security					
_ജ ^{മ,} 109	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
<u> </u>	ര	Users	Create role for vendor access	General	Normal	Completed	Admin
	-65		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	٤Õ		Create Customer Permission required for Eric	Create role	Normal	Open	vsingh
	~~	Duties	something	Add stand-in	High	Waiting	andre.adcalavon
Security	Security		SCS	General	Normal	Open	abahlman
explorer	configuration	Segregation of duties rules	Customer access	General	Normal	Approved	nsadaiya
0		dates rates	Customer_full_access	General	Normal	Approved	nsadaiya
\sim	⊻	Segregation of duties conflicts					
Create role	Import users	Stand-ins					

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

3.2.27 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		_			

curity								
Requests	▲ + New 🖉 Edit	+ Import 음 Explore	··· More					
	✓ User ID ↑ Na	me Email	l	License type	C	ompany	Person	
Scenarios	TRICIA	TRICIA	TRI			Operations		USSI
	VINCE	VINCE	VIN			Operations		USM
Users	🗸 vsingh	Vivek Singh	vsir			Operations		USM
	Wayne	Wayne	Wa		÷	Operations		USM
AAD groups	voichiroo	VOICHIROO	voichu	roo@contosoay / onn		Onerations		11551
Roles	Roles History	Login date and time	AAD group	os				
	 AAD group id 	AAD group na	ime					
Duties	SCSUser	SCS-TEST03	65					
Segregation of duties rules	SCSUser1	SCS-TSTGRC)UP1					

3.2.28 Verify SoD rules in Stand in

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

			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

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

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

ummary		Security							
_ኛ 103	175	Requests							
			✓ User ID ↑	Name	Email		License type	Company	Person
sers	Roles	Scenarios	abahlman	Ard Bahlman	ai		Operations	DAT	
		Users	acardol	Adri Cardol	a		Activity users	DAT	
<u>+-</u>	ତ	Users	andre.adcalavon	André Arnaud de Calavon	a	't.com	Operations Team members	DAT	
		AAD groups	atayyala dvschie	Anil Kumar Tayyala (ATAYY.TI) David van Schie (DVSCH.TI)	at di		Operations	dat dat	
ew security quest	Merge roles	5 1	evhofwegen	Eric van Hofwegen	e	m	Operations	DAT	
		Roles	nsadaiya	Nitish Sadaiya (NSADA.TI)	n:		Operations	usmf	
8	र्छेः		Pradeep.Bapna	Pradeep Kumar Bapna	Pi	com	Operations	DAT	
		Duties	SCS-TSTGroup1	SCS-TSTGROUP1			Operations	DAT	
ecurity plorer	Security configuration	Segregation of	SCS-TSTGroup2	SCS-TSTGROUP2			Operations	DAT	
		duties rules	✓ vsingh	Vivek Singh (VSING.TI)	V		Operations	dat	
S ^T	\downarrow	Segregation of							
T		duties conflicts							
eate role	Import users								
		Stand-ins							
		Data security							
		Data security	Roles History Log	in date and time AAD groups					
		Snapshots	Last login date and time	Days since last login online	Time Type				
			11/6/2019 07:48:42 AM	0:00	:00 Logon				
		History							
		Charts							
		Charts		1					
Use	er's last log								
	_								
	< 1 mo								
	_								
1 to	< 1 mo								
1 to	< 1 mo o 3 mo ⊳ 3 mo								
1 to	< 1 mo o 3 mo								
1 te	< 1 mo o 3 mo > 3 mo ver Io	in	100						
1 te	< 1 mo o 3 mo ⊳ 3 mo		100						
1 te	< 1 mo o 3 mo > 3 mo ver Io 0	in							

3.2.30 Asset classification User Interface

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

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



3.2.31 A List page with Workflow delegation details

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

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

≡	🖉 Ec	dit +New 🛍 Delete Options 🗸	D					* ()	0 ⊡ ×
ଜ	7	₽ Filter	Workflow delegation						
☆ ©	-	\$0F81	Notifications						
Ē			Line item workflow notification t Individual	Send notifications in email Yes	Send notifications to Action C Yes				
8:		Adri Cardol (ACARD.TI)							
		Admin	Delegation						^
		Anil Kumar Tayyala (TI)	+ Add Remove Delegation Active Scope Name	Delegate	Start date/time $\uparrow \bigtriangledown$	End date/time \heartsuit	Enabled		
		BENJAMIN			We didn't find anything to show	here.			
		CHARLIE							
		Daiva Greiciune	Comment						
		Dirk Tijssen (DTIJS.TI)							
		Clorin Milaco							

3.2.32 User groups – combined two tabs in one

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

Users can be added to different groups using same tab.

🖉 Edit	+New 🗓 Delete 🛛 Op	tions 🔎								
7	Users groups Setup List									
	 Originat Project jo 	urnal approvers gro urnal originator gro get processing user p1								
	Name REMAINING USERS	Filter		SELECTED USERS						
	\$0F81	\$0F81	1	Admin	Admin]				
	\$5E39	Anil Kumar Tayyala (A	\rightarrow	atayyala	Anil Kumar Tayyala (TI)					
	acardol BENJAMIN CHARLIE	Adri Cardol (ACARD.TI) BENJAMIN CHARLIE	←	axrunner	axrunner					
	dgre	Daiva Greiciune								
	dtijssen	Dirk Tijssen (DTIJS.TI)								

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

3.2.33 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

	ent								
ummary									
k ^R 135 🔚 242	+	ତ	品	٤Õ	R_	\downarrow			
Users Roles	New security request	Merge roles	Security explorer	Security configuration	Create role	Import users			
ecurity									
Requests	Merge roles D	Duplicate role Loo	ck roles 🖧 Explore	Export Import [Define active/inactiv	ve role Export role configuration Imp	ort role con	figuration	
Requests Scenarios	Merge roles D		ck roles 🖧 Explore	Export Import [Define active/inactiv		ort role con Locked	figuration Inactive	Has configuration
	O Role name					loud) Role description		-	Has configuration
Scenarios Users	O Role name Business e			1 License type	License type (cle	loud) Role description		-	Has configuration
Scenarios Users Groups	O Role name Business e Business e	events security role		License type Operations	License type (cle	loud) Role description	Locked	-	Has configuration
Scenarios Users	O Role name Business e Business e	events security role events viewer onnector Role		License type Operations None	License type (cle	loud) Role description	Locked	-	Has configuration
Scenarios Users Groups	Role name Business e Business C Buying age	events security role events viewer onnector Role		License type Operations None None	License type (cle Human resouc	Role description	Locked	-	
Scenarios Users Groups Roles	Role name Business e Business e BusinessC Buying age Chief exec	events security role events viewer onnector Role ent		↑ License type Operations None Activity users	License type (cle Human resouc	Role description ces Role Used to Decide if us Documents purchase eve	Locked	-	~

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

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

3.2.34 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	nplianc	e studio pa	arameters					
General	Ger	General setup for the purchased licenses						
License count	Ope	admin.microsoft.c	iom					
Data migration	LICE	ISE PARAMETERS II	NPUT					
5	0	C License		î	No of licenses			
Enhanced SoD rules	0	Activity users			150			
Number sequences		Commerce			12			
		Commerce -	attached license		3			
		Finance			10			
		Finance - atta	ached license		5			
		Human resou	ices	_	10			
		Human resou	uces - attached license		5			
		Operations		-	0			
		Project opera	itions		60			
		Project opera	ations - attached licens	e	30			
		SCM			18			
		SCM - attach	ed license		9			
		Team membe	ers		76			

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

License optimiza	ation					
 Summary 						
License						
Usage		uired base and attach licenses. In case o n, you can use this information to verify		he count is listed in 'Any base lic	ense'.	
All users	The licensed users and remaining	licenses might be incorrect in case the is not aware of assigned licenses in Enti	re are users requiring more than one	e license.		
Full users	View on premise	-				
Activity users	 License type 	√↑ Actual users count	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	
occitatios	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.



Jsage	The actual count is a total of required base and attach licenses. In case one of base the licenses is required, the count is listed in 'Any base license'. Based on your actual subscription, you can use this information to verify your compliance. The licensed users and remaining licenses might be incorrect in case there are users requiring more than one license.						
kii users	The Dynamics 365 user interfac				Cloud licen		
ull users	View on premise licenses				Cloud licen	se view	
Activity users	O License type	7t	Actual users count	Base license users count	Attach license users count	Remaining users count	
feam members	 Activity users 		3	150	0	147	
cenarios	Any base license		10	0	0	-10	
centarios	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	
Jsage	The actual count is a total of re Based on your actual subscript				, the count is listed in 'Any base license'.		
All users				your compliance. re are users requiring more than o	ine license.		
ull users	The Dynamics 365 user interfac	te is not aware	e of assigned licenses in Ent	ra ID.			
-ull users	View cloud licenses						
Activity users	 License type 	71	Actual users count	Base license users count	Attach license users count	Remaining users count	
eam members	 Activity users 		3	150	0	147	
	Operations		0	0	0	0	
cenarios			30	76	0	46	
cenarios	Team members		30	70	•	40	



4. Bug fixes

4.1 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 lead to slow performances got fixed. Garbage collection is working correctly.

4.2 Security and compliance studio 10.0.39.43

ID	Description	Observation
183994	CS00232323 German labels in modul SCS are missing or incorrectly translated	-
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.

4.3 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
			the node will get overridden and all entries

	CS00227144 Deviation in standard 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	CS00227833 'Any base license'	Incorrect license count.
& 180696	roles are counted in both 'Finance' and 'SCM' licenses &	New options have been added to the SCS parameters license count system. For more details please see WHAT'S NEW 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.

4.4 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.

4.5 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.

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

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
172461	CS00226211 Task recorder saving to security failing - DSM 10.0.32.38	corrupted. 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.

4.6 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'.

4.7 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.
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.

4.8 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.



4.9 Security and compliance studio 10.0.29.36

ID	Description	Observation
153855		Enchanced error handle to provide more information when an user fails to be imported from azure groups.
151835	Internal Data source fields not recognised during direct role import	Changes over the data source fields are not detected during direct role import.

4.10 Security and compliance studio 10.0.28.34

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

4.11 Security and compliance studio 10.0.27.33

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

4.12 Security and compliance studio 10.0.26.32

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

4.13 Security and compliance studio 10.0.26.31

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

4.14 Security and compliance studio 10.0.25.30

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



4.15 Security and compliance studio 10.0.24.29

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.

4.16 Security and compliance studio 10.0.22.27

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

4.17 Security and compliance studio 10.0.18.1

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

4.18 Security and compliance studio 10.0.12.5

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

4.19 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

4.20 Security and compliance studio 10.0.12.3

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

4.21 Security and compliance studio 10.0.12.2

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

4.22 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



4.23 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

4.24 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

4.25 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

4.26 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

4.27 Security and compliance studio 10.0.6.8

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

4.28 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

4.29 Security and compliance studio 10.0.6.6

ID	Description
100323	CS00111058-Unable To Import Security Roles

4.30 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

4.31 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

4.32 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

4.33 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

4.34 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 "Tem Member" license type.



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

4.35 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.

4.36 Security and compliance studio 10.0.3.2

ID	Description
77956	CS00069693 – License Count Data Source.

4.37 Security and compliance studio 10.0.3.1

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

4.38 Security and compliance studio 10.0.1.3

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

4.39 Security and compliance studio 10.0.1.2

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

4.40 Security and compliance studio 10.0.1.1

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

4.41 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.

4.42 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.

4.43 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'

4.44 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	

4.45 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	

4.46 Security and compliance studio 81.20.3.1

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

4.47 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.		

4.48 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.		

4.49 Security and compliance studio 81.20.1.1

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

4.50 Security and compliance studio 1804.15.2.1

ID Description



61572	II-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 mode	
	changes. Instructions for the same are given in the known issues section.	

4.51 Security and compliance studio 1804.15.1.1

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

4.52 Security and compliance studio 1712.12.1.1

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

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).

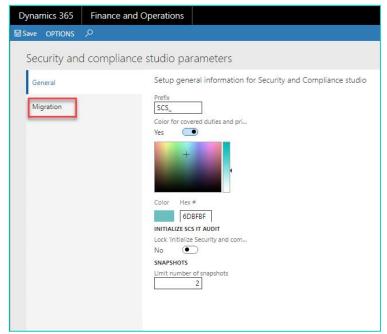


Fig. 1 New tab in SCS Parameters form

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)

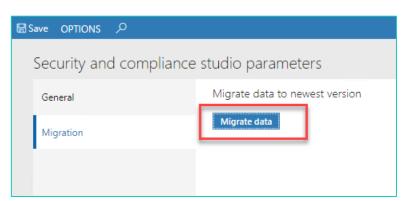


Fig. 2 "Migrate data" button on SCS Parameters form

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)

■Save OPTIONS ク	
() Migration done. Please restart your D365 UI	
Security and compliance st	udio parameters
General	Setup general information for Security and Compliance studio Prefix SCS_ Color for covered duties and pri Yes + + Color Hex # GDBFBF INITIALIZE SCS IT AUDIT Lock 'Initialize Security and com No SNAPSHOTS Limit number of snapshots 2

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