

Author: DGV Team

Security and Compliance Studio 10.0.34.39

Release Notes

Contents

1.	Introduction	6
1.1	Purpose	6
1.2	Audience	6
1.3	Product release information	6
1.4	Deliverables	7
1.5	Common features	7
1.6	Certificate renewal	8
2.	What's New in Security and Compliance Studio 10.0.34.39	.10
2.1	Dynamic snapshot	10
3. Featu	res introduced in last few releases of Security and Compliance Studio	.11
3.1	Security requests enhancements and workflow	14
3.2	Export security explorer objects to excel in a de-normalized format	25
3.3	Merge security scenarios and match role	26
3.4	Mark any Security Role as Active/Inactive	26
3.5	Recording steps to scenario	26
3.6	Override permission based on scenarios	27
3.7	Option to mark, track and audit security objects providing access to sensitive data	
3.8	Option to create a duty from Matched Privileges grid in Match roles form	35
3.9	Option to import and export data using Data Entities in Security and Compliance	
	Studio	
3.10	Option to compare Security Snapshots stored in the security setup	37
3.11	Enhanced Audit log capability to capture all the changes from development space	
	(AOT) as well into Audit Log	41
3.12	Option to create one or more privileges and also one or more duties while	11
2 1 2	merging roles.	
3.13	Ability to create scenarios from D365 module menus	
3.14	Snapshots based performance and scalability enhancements	
3.15	Improved "Create role wizard" based on a grid framework	
3.16	Accessing Security Explorer from all D365 FOE forms	
3.17	Option to create duties and SOD compliance check as well while merging roles	46

3.18	Importing New Users while Synchronizing the group users with the Active	
	Directory group members	47
3.19	Uptake RapidValue BPM Suite Scenarios directly as SCS Security Scenarios	47
3.20	Enhanced Segregation of Duties	49
3.21	Organization risk Register	50
3.22	AAD related SoD Validations across SCS	50
3.23	Security Explorer displaying Tables, Service operations and Data Entities entry	
	point's type	51
3.24	Performance Optimization	51
3.25	A new "Share" workspace	51
3.26	AAD groups' information in D365FO	52
3.27	Verify SoD rules in Stand in	53
3.28	Chart to give an overview of number of users and their last logging details	53
3.29	Asset classification User Interface	54
3.30	A List page with Workflow delegation details	55
3.31	User groups – combined two tabs in one	55
4.	Bug fixes	56
4 1		FC
4.1	Security and compliance studio 10.0.34.39	
4.2	Security and compliance studio 10.0.32.38	
4.3	Security and compliance studio 10.0.31.37	
4.4	Security and compliance studio 10.0.29.36	
4.5	Security and compliance studio 10.0.28.34	
4.6	Security and compliance studio 10.0.27.33	
4.7	Security and compliance studio 10.0.26.32	
4.8	Security and compliance studio 10.0.26.31	
4.9	Security and compliance studio 10.0.25.30	
4.10	Security and compliance studio 10.0.24.29	
4.11	Security and compliance studio 10.0.22.27	
4.12	Security and compliance studio 10.0.18.1	
4.13	Security and compliance studio 10.0.12.5	
4.14	Security and compliance studio 10.0.12.4	
4.15	Security and compliance studio 10.0.12.3	
4.16	Security and compliance studio 10.0.12.2	
4.17	Security and compliance studio 10.0.12.1	
4.18	Security and compliance studio 10.0.10.1	
4.19	Security and compliance studio 10.0.6.11	
4.20	Security and compliance studio 10.0.6.10	
4.21	Security and compliance studio 10.0.6.9	
4.22	Security and compliance studio 10.0.6.8	60
4.23	Security and compliance studio 10.0.6.7	
4.24	Security and compliance studio 10.0.6.6	
4.25	Security and compliance studio 10.0.6.5	
4.26	Security and compliance studio 10.0.6.4	60
4.27	Security and compliance studio 10.0.6.3	61

4.28	Security and compliance studio 10.0.6.2	61
4.29	Security and compliance studio 10.0.6.1	61
4.30	Security and compliance studio 10.0.3.3	61
4.31	Security and compliance studio 10.0.3.2	61
4.32	Security and compliance studio 10.0.3.1	61
4.33	Security and compliance studio 10.0.1.3	61
4.34	Security and compliance studio 10.0.1.2	61
4.35	Security and compliance studio 10.0.1.1	62
4.36	Security and compliance studio 81.3.2.1	62
4.37	Security and compliance studio 81.3.1.1	62
4.38	Security and compliance studio 81.2.1.1	62
4.39	Security and compliance studio 81.1.2.1	62
4.40	Security and compliance studio 81.1.1.1	62
4.41	Security and compliance studio 81.20.3.1	62
4.42	Security and compliance studio $81.20.2.2$ *(This build was created as the earlier	
	deployable package had some issues)	62
4.43	Security and compliance studio 81.20.2.1	63
4.44	Security and compliance studio 81.20.1.1	63
4.45	Security and compliance studio 1804.15.2.1	63
4.46	Security and compliance studio 1804.15.1.1	63
4.47	Security and compliance studio 1712.12.1.1	63
5.	Changed or deprecated features	64
5.1	Deprecated features 10.0.31.37	64
5.2	·	
J.Z	Deprecated features older versions	04
J.Z	Deprecated features older versions	04

Document Information

Title	Security and Compliance Studio 10.0.34.39
Subtitle (Subject)	Release Notes
Solution Suite	GRC; Security and Compliance Studio
Category	Release Notes
Author	SCS Team
Published Date	7/5/2023
Status	Final

© Copyright To-Increase 2023. All rights reserved.

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

1. Introduction

1.1 Purpose

This document highlights new features and enhancements that ship in the new **Security and Compliance Studio 10.0.34.39** release from To-Increase. This release is compatible with the version of Microsoft Dynamics 365 for Finance and Operations, **10.0.27 or later**.

1.2 Audience

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

1.3 Product release information

Security and Compliance Studio 10.0.34.39 for Dynamics 365 Finance and Dynamics 365 Supply Chain Management (10.0) is built upon D365 version [Minimum GA version required]. Since Microsoft maintains a no breaking changes policy, the fact that this release is built on this version means that it can be applied to an environment running on D365 version [Minimum GA version required] or any later version and the application should compile without any issues. However, as we have only functionally validated this version against D365 version [latest GA version], we recommend applying our TI product release on that MS version as well. If you deviate from this (and thus apply the release to a different version), we recommend performing a more thorough round of testing before applying the release to a production environment.

Release date [TI-Product]	[TI-Version number]	Minimum required D365 version	Validated against D365 version	Compatible with D365 version
03/04/2023	10.0.32.38	10.0.29	10.0.32	10.0.29 and above
05/07/2023	10.0.34.39	10.0.32	10.0.34	10.0.32 and above

This is summarized in the following table.

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

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

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

1.4 Deliverables

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

Deliverable	Description
Solution package	Security and Compliance Studio is delivered as a Microsoft Dynamics Lifecycle Services (LCS) solution package.
Software deployable package	Security and Compliance Studio 10.0.34.39 and SCS-fix deployment issue
Release notes	This document is provided with the Security and Compliance Studio product deliverables.
Implementation methodology	The solution package contains a <i>Security and Compliance Studio</i> <i>implementation methodology</i> that provides detailed step-by-step instructions on how to install, learn, and implement Security and Compliance Studio.
Getting started BPM library	The solution package includes a <i>Getting started with the Security</i> <i>and Compliance Studio</i> BPM library. This library contains a number of task guides that showcase some of the key capabilities of Security and Compliance Studio.
Documentation BPM library	The solution package includes a <i>Security and Compliance Studio</i> <i>documentation</i> BPM library. This library contains a comprehensive set of task guides that document how to use <i>Security and</i> <i>Compliance Studio</i> for your BPM activities. This documentation is provided in U.S. English only.
Authentication assets	A To-Increase security certificate is provided to allow trusted installation of the provided model files and ISV license files.
Process data package	The solution package provides a simple Security and Compliance Studio <i>demo</i> process data package that can help you get started from LCS.

1.5 Common features

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

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

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

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

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

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

	!
To-Increase would love your feedback!	!
Please rate your experience in using the All solutions screer	n.
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!	
Thank you for providing us feedback!	
Thank you for providing us feedback!	
Thank you for providing us feedback! Your privacy is important to us. To protect your privacy, pleadon't include any personal information.	ase

1.6 Certificate renewal

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

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

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

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

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

Click here for more information on the Solution Management Workspace.

2. What's New in Security and Compliance Studio 10.0.34.39

2.1 Dynamic snapshot

We got a lot of feedback and learnings related to the security snapshot. A lot of features are depending 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.

- When changes to security configurations are published, they will automatically be added to the current snapshot and available in the "Security explorer" form.
- Creating or modifying roles using the Security and Compliance wizards the changes will also be automatically added to the current snapshot and available in the "Security explorer" form.
- Importing roles using the Security and Compliance import/export functionality will also be automatically added to the current snapshot and available in the "Security explorer" form.
- Assign users to roles changes will also be captured into the dynamic snapshot and the changes will be automatically added to the current snapshot and available in the "Security explorer" form.

Match roles will no longer require you to create a new snapshot in order to find and display matched roles after security configuration changes.

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.

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.

3.1 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 Delete Ostatus ∧ Owner ∧ 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.

	$\circlearrowright Status \lor$
vŀ	Open
	Waiting
	Review
	Approved
_	Rejected
ż	Canceled

Security types a) General

05 July 2023, © To-increase 14

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.

Request	Туре	Origin	Area
Demo SR 1	General	User requests	WHS
Status			
Priority	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
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.

Security requests My vi		
Demo SR 1	ew v	
Demo SR 1	Assign role to user	✓ User requests
Status		
Priority	Status	Owner
Normal 🗸	Open	Admin
Assign roles to user		
USER		
User ID	User name Email	Company
Admin	Admin fmihoc@toincreas	e.onmicros USMF
ROLES		
Add 🗎 Remove		
○ ○ Role name	Description	Role AOT name
 Auditor 	Manages and reviews aud	AUDITPOLICYMANAGER ~
COMPANIES		
+ Add 🗊 Remove		
◯ Company C	Company accounts	
CNMF V C	Contoso Entertainment China	

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.

equest Demo SR 1		Type Remove role from user	Origin User requests	
tatus				
riority Normal V]	Status Open	Owner Admin	
emove roles from use	r			
ISER				
lser ID	User name	Email	Company	
Admin	Admin	fmihoc@toincrease.onm	icros USMF	
OLES Add 🗻 Remove				
O C Role name		Description	Role AOT name	-
0		The lease clerk role has ac	ASSETLEASECLERKROLE ~	
 Lease clerk 				

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.

ieneral					
Request Demo SR 1		Type Disable user	$\overline{}$	Origin User requests	Area WHS
Status					
Priority Normal V		Status Open		Owner Admin	
Disable users					
Add 🗎 Remove	User na	me			
O BrunoD	Bruno				

f) Enable user

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

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

Security requests My view ~ Demo SR 1			
General			
Request Demo SR 1	Type Enable user	Origin User requests 🗸 🗸	Area WHS
Status			
Priority Normal	Status Open	Owner Admin	
Enable users			
Add In Remove	User name		
JanetS	Janet Schor		
L			
Description			

g) Delete user

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

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

Request Demo SR		Туре		Origin	Area
		Del	ete user 🗸 🗸	User requests 🗸	WH
Status		_			
Priority		Statu	IS	Owner	
Normal	\sim	Ope	en	Admin	
Delete use	arc				1
	Remove				-
	User ID 1	User name	Email		
	CASSIE	CASSIE	CASSIE@contosoax7.onm		
-	cdsaurorauser	Auroraus	Aurorauser01@capintegr		
			- 1 5		

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.

Convrite room	uests My view 🗸						
Demo							
	SICT						
General							
Request		Туре	Origin	Area WHS	~		
Demo SR 1	1	Delete user	User requests	WHS	~		
Status							
Priority		Status	Owner				
Normal	\sim	Open	Admin				
Create role							
ROLE	e Isk recording						
ROLE Upload tas	isk recording	Description	Scenario				
ROLE Upload tas Role name SCS_Demo	isk recording	Description Demo purposes	Scenario skRecordingForCSReplicat	e.axtr			
ROLE Upload tas Role name SCS_Demo SCENARIO E	oRole1	Demo purposes			File name	Child scenario	Î Remark
ROLE Upload tas Role name SCS_Demo SCENARIO E	isk recording	Demo purposes t Securable type	skRecordingForCSReplicat	Description	File name TaskRecordingForCSRepli		Î Remark
ROLE Upload tas Role name SCS_Demo SCENARIO D	oRole1 DETAILS number Securable object	Demo purposes t Securable type ige Display	skRecordingForCSReplicat	Description			1 Remark Additional securable object found in the task recording
ROLE Upload tas Role name SCS_Demo SCENARIO D	sk recording ORole1 DETAILS number Securable object 1 salestablelistpa	Demo purposes t Securable type ge Display ard Display	skRecordingForCSReplicat Access level Full control	Description Go to Accounts receivabl	TaskRecordingForCSRepli		Additional securable object
ROLE Upload tas Role name SCS_Demo SCENARIO D	oRole1 DETAILS number Securable object 1 salestablelistpa 2 DefaultDashbo	Demo purposes t Securable type ge Display ard Display ge Display	skRecordingForCSReplicat Access level Full control Full control	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli		Additional securable object
ROLE Upload tas Role name SCS_Demo SCENARIO D	sk recording oRole1 DETAILS number Securable object 1 salestablelistpa 2 DefaultDashbo 5 salestablelistpa	Demo purposes t Securable type ge Display ard Display ge Display	skRecordingForCSReplicat Access level Full control Full control Full control	Description Go to Accounts receivabl Close the page. Go to All sales orders.	TaskRecordingForCSRepli TaskRecordingForCSRepli TaskRecordingForCSRepli		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 Request Demo Si	o SR 1	e odify role	Origin Vser requests	Area WHS	~			
Status	_							
Priority Normal		tus pen	Owner Admin					
Modify r	ole							
ROLE								
	e 🗎 Remove							
0 0		scription w of lease roles	Role AOT name ASSETLEASELEASEVIEW					
	O DETAILS							
Upload	O DETAILS task recording							
Upload Scenario								
Upload Scenario Demo1x	task recording k recording.axtr p number Securable object	Securable type	Access level	Description	File name	Child scenario	Î Rema	rk
Upload Scenario Demo1x	task recording	Securable type Display	Access level Full control	Description Go to Accounts receivable > Orders > A		Child scenario	Î Rema	rk
Upload Scenario Demo1x	task recording k recording.axtr p number Securable object				Demo1x recording.axtr	Child scenario	Addit	ional securable object
Upload Scenario Demo1x	t task recording k recording.axtr ep number Securable object 1 salestablelistpage	Display	Full control	Go to Accounts receivable > Orders > A	Demo1x recording.axtr	Child scenario	Addit	ional securable object
Upload Scenario Demo1x	I task recording recording axtr pnumber 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	Addit	rk ional securable object in the task recording
Upload Scenario Demo1x	task recording attr crecording axtr prinumber 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	Addit	ional securable object

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*.

re +New	🗎 Delete 🙁 Status 🗸	Q Owner ∽ Request	Manage C	options 🔎		
Security re	equests My view 🗸					
Demo	5 SR 1					
General						
Request Demo SF	R 1	Type Lock role	\sim	Origin User requests	\sim	Area WHS V
Status						
Priority	\sim	Status Open		Owner Admin		
Lock role						
+ Add	Remove					
00	Role name		Name			
	Applicant anonymous (exte	ernal) 🗸 🗸	ANONYMOU	SAPPLICANT		

k) Unlock role

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

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

quest lemo SR 1	Type Unlock role	Origin User requests	Area WHS
atus	Unlock role	User requests V	WID
riority Normal V	Status Open	Owner Admin	
Jnlock roles			
Add Remove	Name		
	V WMSWAREHOUSEWORKER		

I) Delete role

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

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

e	-	quests My view ∽ • SR 1					
Gene	eral						
Requ Dem		R1	Type Delete role	$\overline{}$	Origin User requests	\checkmark	Area WHS
Statu	IS						
Priori Nor		\sim	Status Open		Owner Admin		
Delet		le I Remove					
							-
0		Role name	Description	Role AOT	name	Î	
0		Role name SCS_RoleTest_2	Description	Role AOT 6DEC781	name 11-E0C5-42C5-94		

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 ∽ IOSR1										
l.										
sR 1	Type Create rule			Area WHS	\sim					
al 🗸	Status Open									
ed SoD rules										
i 🗊 Remove										
C Name 1	Туре	First	First securable object type	First access level	Second	Second securable object type	Second access level	Effective from	Effective to	Enabled
Create demo rule 2 from	Entry point V	AdvancedLedger $ \smallsetminus $	Menu item display 🛛 🗸	Create ~	BankChequeCompanyI $\scriptstyle{\smallsetminus}$	Menu item display 🛛 🗸	Full control V	4/28/2022 10:43:44 🖽 💿	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	
	o SR 1	o SR 1 SR 1 SR 1 Status open ed SoD rules Remove Name 1 Type	o SR 1	o SR 1 SR 1 Status Status Status Status Status Status Status Owner Admin Status Owner Admin Status Create rule Status Owner Admin Status Creater vile Status Owner Admin Status Owner Admin Status Owner Admin Status Owner Admin Status Owner Admin Status Owner Admin Status Owner Admin Status Status Owner Admin Status Status Owner Admin Status Statu	o o SR 1 Type Origin Area SR 1 Create rule VIEWHS Status Owner ad SoD rules Remove Name 1 Type First securable object type First access level Create demo rule 2 from Entry point V AdvancedLedger Menu item display Create V	o o SR 1	o SR 1 SR 1 Status Overer Area WHS WHS WHS Status Owner Admin d Status Owner Admin Create demo rule 2 from _ Entry point _ AdvancedLedger ~ Menu item display ~ Create _ BankChequeCompanyL ~ Menu item display ~	o o SR 1 SR 1 SR 1 Status Origin Area WHS WHS Owner Admin Status Owner Admin Status Owner Admin Status Copen Status Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Comer Status Copen Status Comer Status Copen Status Copen Status Copen Status Comer Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status Copen Status S	in o SR 1 SR 1 Create rule Status Owner Atria User requests WHS WHS WHS Create full Create full	o SR1 SR1 SR1 SR1 Status Origin Area WHS WHS WHS WHS WHS

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.

Gener	ral									
Reque:	st o SR 1	Type Resolve conflict		Drigin User requests	Area WHS	\checkmark				
itatus	5									
Priorit; Norm	nal 🗸	Status Open		Owner Admin						
	d 🗊 Remove									
	C Rule name	Туре	User ID	First	Role	Second	New role	Resolution	Override reason	Role to remov
	Duty test1	Duty	APRIL	Approve budget plans	Budget clerk	A parameter that is used t	Budget manager	Exclude		Existing role
		 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 the *Security and Compliance Studio -> Security -> Enhanced SoD* form.

General Request Demo S	R 1	Type Delete rule	Origin V User req	uests 🗸	Area WHS	~				
Status										
Priority Normal	\checkmark	Status Open	Owner Admin							
	nhanced SoD rules									
	Remove									
00		Туре	Effective from	Effective to	First	First securable object type	First access level		Second securable object type	
	SoD Test 1 - do not use 🚿		4/20/2021 12:11:46 PM	12/31/2154 11:59:59 PM	DSMAuditLog	Menu item display	View	DSMAssetClassification	Menu item display	View
0		Duty	11/25/2021 2:00:45 PM	12/31/2154 11:59:59 PM	Approve budget plans		No access	A parameter that is used t		No access
0	Duty test1									

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.

General					
Request Demo S		Type Add stand-	in V	Origin User requests	Area WHS
Status					
Priority Normal	I ~	Status Open		Owner Admin	
Create s					
+ Add	🗊 Remove	Stand-in	From date	To date	Copy assigned organizations
0 3	User ID				
00	Output See See See See See See See See See Se	ALICIA ~	4/28/2022	4/30/2022 📾	

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.

equest Demo S	R 1		Type	cel stan	id-in	\sim	Origin User req	uests	Area WHS
Status									
Priority Normal	~	-	Statu	-			Owner Admin		
Remove	stand-in								
	Remove User ID		Stand-in		From date		To date		Copy assigned organizati
\bigcirc	Admin	~	ALICIA	~	4/28/2022	6	4/30/2022	0	
0	Admin	~	ALICIA	~	4/28/2022		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 Strategic \checkmark SOD RULES	Area AssetLease Inherent risk Very Iow	Mitigation Test Residual risk Very Iow	Status Initial V Response Ignore V
+ Add in Remove	 ↑ Organization Risk : ✓ Dmeo business risk 		

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

Switching type from 'AssignUserRole' will remove
all data specific to it. Are you sure want to
continue?
Yes No

II. Security requests workflow

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

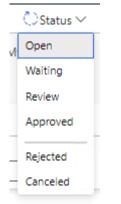
A new workflow will need to be created by using the "New" button. This will open the standard workflow editor where the workflow approval design will be created. Once it is done it will appear in the form and it will be activated.

Security Reques		onfiguration				
O Status	Default	ID	Name	Association	Туре	Instances Active vers
0	~	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	\circlearrowright Status \checkmark	ROwner∨	Request	dit	$+_{New}$	🗓 Delete	\bigcirc Workflow \checkmark	Request	Manage
	Security re	equests N	∕ly view ∨				Security re	equests N	∕ly view ∨		
	Demo	5 SR 1	Inactiv	e workflov	N		Demo	5 SR 1	Active we	orkflow	/

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



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

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

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

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

Licensing framework update

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

Steps required after update to SCS 10.0.24.20:

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



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 cor	mpliance studio parameters	
General	General setup for the purchased	licenses
License count	Open admin.microsoft.com LICENSE PARAMETERS INPUT	
Data migration	O C License ↑	No of licenses
	 Activity users 	15d
Enhanced SoD rules	EAM	20
	Finance	10
Number sequences	HR	60
	OPERATIONS	90
	ProjectOperations	67
	Retail	55
	SCM	18
	Team members	76

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

icense op	timizatio	n				
Summary		License				
ଦ୍ଧ	ቆ	Usage	O License type	Actual use	Licensed users c	Remaining us
			Finance	11	10	-1
	Security	All users	HR	10	60	50
Merge roles	explorer	Full users	ProjectOperations	4	67	63
			Retail	15	55	40
		Activity users	SCM	29	18	-11
		Team members	Activity users	12	150	138
		learn 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 Export security explorer objects to excel in a denormalized format

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

JSERS	ull view	ACCOUNTANT	DUTIES	PRIVILEGES	ENTRY POINTS
-s= Pin users		xê Unpin role	-⇔ Pin duty	🖘 Pin privilege	-s= Pin entry point
User ID	Name	Role name 1	Duty name 1	Privilege name 1	Entry point (AOT name) 1
OSCAR	OSCAR	Accountant	Configure electronic fiscal	d	a 😑 🖃 AbatementCertificate_IN
RetailServiceAccount STAN	RetailService STAN	Accounting manager Accounting supervisor Accounts payable centraliz Accounts payable centraliz Accounts payable derk Accounts payable payment Accounts payable payment Accounts payable payment	Enable EU sales list process Enable financial reports ge Enable fixed assets process	Account number enhances account reference -ViewLes AccountingSourceExplores n Action class settings main	d C Accountant_BR d Accountant_BR V AccountantElectronicAddress AccountantElectronicAddress C AccountantElectronicAddress

<u> </u>		<u> </u>	U U U U U U U U U U U U U U U U U U U	
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

3.3 Merge security scenarios and match role

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

Finance and Operat	ions Preview		D Search for a pag					Merge scenarios into or
🖪 Audit 🛛 🖺 Optimiz	e OPTIONS 🔎							Name
Security and	compliance stud	io						Description
Summary		Security						
_x ~ 99	99 📰 156 Requests		+ New ⊘ Edit ⊡ Match roles ···· More Merge scenarios					
			✓ 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	
Manu an anni ta i			Merged Customer-SO-PO Scenario	vsingh	Merged scenarios to reflect rece	5	7/29/2019 06:38:24 AM	
New security request	Merge roles	Roles	Merged scenario	nsadaiya	Merged from create customer a	6	7/2/2019 08:46:07 AM	

3.4 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.

ate role Import users Scenarios SCS_Customer service represent Operations SCS_Create Customer expresent Operations SCS_Create Customer Operations SCS_Created from duties Operations SCS_Created from duties Operations P P P P P P P P P P P P P P P P P P P	este role Import urere Scenarios	Role description Locked
Users SCS_Customer service represent Operations Users SCS_Created from duties SCS_Created from duties Operations Roles Save + New @ Delete OPTIONS P Duties Materiane Role Auditor AUDITPOLICYMANAGER Costs accountant clerk CANCOSTACCOUNTANTCLERK	✓ SCS_Customer service represent Operations	
Users Operations V SCS_Created from duties Operations V Roles Duties Duties CSS_Created from duties Operations V Inactive security roles V Cost accountant clerk V Cost accoun		
Roles Inactive security roles ✓ Duties ✓ Role name Role (AOT name) Auditor Auditro Auditro Cost accountant clerk ✓ Cost accountant clerk	Users	
Roles Roles Inactive security roles V Duties Rele name Rele (ADT name) Auditor AUDITPOLICYMANAGER Cost accountant clerk Cost accountant clerk		
Duties Inactive security roles Duties		
Auditor AUDITPOLICYMANAGER	□ Inactive security roles	. •
Cost accountant clerk CAMCOSTACCOUNTANTCLERK	Duties Role name Role (AOT	iame)
Segregation of duties	Segregation of duties	TACCOUNTANTCLERK

3.5 Recording steps to scenario.

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

	Edit + New	🗊 Delete	Match roles Merge scenarios	New from task recording	$\overline{\uparrow}$ Upload recording Ov	erride permissions on roles $, ho \cdots$	∞ 1 ₽ ७	С
7	SCENARIO RECO	RDING STEPS						
	General					Recording	steps nsadaiya 🔨	
	Scenario Recording steps	s				Owner nsadaiya		
	Description						~	
	Access required						^	
	+ Add 🕂 Add	d module acces	ss 🛍 Remove 🖧 Explore					
	✓ Step number	er	Securable object	Securable type	Access level	Step description	File name	
	2		DefaultDashboard	Display	Full control	Go to Default dashboard.	Recording steps	
	3		custtablelistpage	Display	Full control	Go to Accounts receivable > Cu	. Recording steps	
	7		custtablelistpage	Display	Full control	Go to All customers.	Recording steps	
	8		CustTable	Display	Full control	In the list, click the link in the sel	Recording steps	

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.

3.6 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.

Ξ	🖉 Edit	+ New 🗊	Delete	A Match roles	New from task recording	↑ Upload recording	Override permissions on roles	OPTIONS	Q		0	1	p	Ċ
7	SCENARI	10												
-	Gener	al								Merged s	cenario	nsa	ıdaiya	/
	Scenari Merg	io Jed scenario								Owner nsadaiya				
	Descri	iption												`
	Acces	s required												/
	+ Add	d 🕂 Add mo	dule acce	ss 🛍 Remove a	윰 Explore									
	v	Step number		Securab	ole object S	ecurable type	Access level	Step descripti	on		Fi	le name	2	
		-		AssetTa	ableNew D	Display	No access							
				DSMA	rea C	Display	Edit							

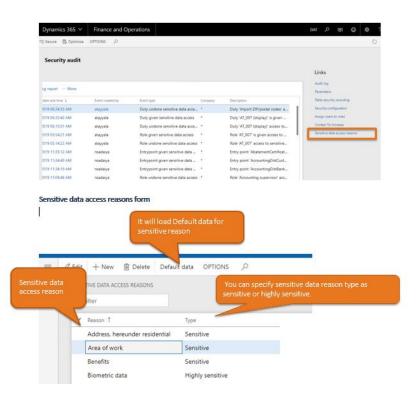
Accounts receivable centralized	Documents accounts receivable		- H
Accounts receivable clerk	Documents customer invoice ev		-
Accounts receivable manager	Reviews customer invoice proce		
Accounts receivable payments c	Documents accounts receivable		
Applicant anonymous (external)	External user application for em		
Auditor	Manages and reviews audit poli		
Batch job manager	Maintain and configure settings	,	
Set custom permissions No e PERMISSIONS Read			
No PERMISSIONS Read Unset Grant Deny Update Unset Grant Deny Create			
No PERMISSIONS Read Unset Grant Deny Update Unset Grant Deny Create Unset Grant Deny			
No PERMISSIONS Read Unset Grant Deny Update Unset Grant Deny Create			

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

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

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

• Set up sensitive data access reasons



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

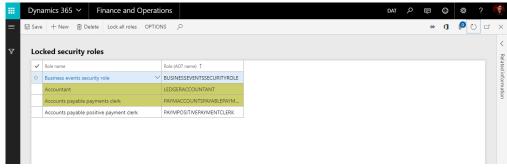
=	🕐 Create snapshot 🛛 🖒 R	eset pins Advanced view Show joined	OPTIONS ,O	× 🗅 🗘 📦 🕽 🗰
7	Security explore	r: full view	DUTIES	PRIVILEGES ENTRY POINTS
	-⇔ Pin users ····	⊣¤ Pin role	-ta Pin duty Give sensitive data access	-⇔ Pin privilege ···· =⇔ Pin entry point ····
	✓ Pin User ID	✓ Pin Role name ↑	✓ Pin Duty name ↑ Access to sensiti.	🗸 Pin Privilege 🗸 Pin Entry po
	\$C0BA	Accounts payable	 A parameter that is used to gro 	A param 🖂 Abater
	 Admin 	 Accounts payable 	Access benefits workspace	Accept : 🗧 🖂 Abater
	ALICIA	Accounts payable	Access expense management w	Access t 🔹 💍 Abater
	APRIL	 Accounts receivabl 	Access workforce management 🗸	 Access c Abbrev
	ARNIE	Accounts receivabl	 Activate tax depreciation process 	Access e 🖂 Accourt
	 atayyala 	 Accounts receivabl 	Activate, deactivate, update and	Access e 🖂 Accou
	axrunner	 Accounts receivabl 	Add an existing performance jo	Access r 🔹 🗖 Accou
	BENJAMIN	Applicant anonym	 Add custom fields 	Access v 🔳 🖾 Accourt
	BRAD	 AT_ 	 Application document entities 	Account 🗅 Accourt
	BROOKE	AT 007	Approve absences 🗸	account 🔹 🗹 Accourt

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

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

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

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



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

		e and Operations Acc								I @ O ⊑
ANAGE	OPTIONS D								~ (I (₽ () ⊏
	ROLES AND SENSITIVE DATA ACCES	s								
Mate	ch roles Menu item display	USMScenario	Full co		No acces		Not part of the			
	Menu item display	DSMScenario			No acces		Not part of the			
	Menu item display	CustTableListPage	Full co		View	s •		selected role.		
Ě	Menu item display	ForecastSalesTable	Full co		No acces	-	Not part of the			
	Menu ken uspay	TORCASSAESTADIE	Tur co		No acces		Not part of the	selected tole.		
Roles										
×	Role name	Role description	Matc	User license type		Remaining user				
	Project manager	Documents the project foreca	ist/ 50.00	Operations		59928				
	Production planner	Schedules and plans product	tions 50.00	Operations		59928				1
	Sales manager	Reviews sales process perform	na 50.00	Operations		59928				
~	Sales representative	Documents sales events and r	res 25.00	Activity users		29986				
	Materials manager	Enables and reviews processe	s, 25.00	Operations		59928				
Duty n Enable	e the demand forecasting	Privilege name Maintain demand forecasts for i		e object type em display		Securable object	e	Access level Full control		Duty license type Operations
Maint	tain project budgets	View demand forecasts for item	Menu it	em display		ForecastSalesTable	e	View		Activity users
Maint	tain project forecasts	Maintain demand forecasts for i	Menu it	em display		ForecastSalesTable	e	Full control		Activity users
Inquir	re into project forecast stat	View demand forecasts for item	Menu it	em display		ForecastSalesTable	e	View		Team members
Maint	tain authorization of adjust	View demand forecasts for item	Menu it	em display		ForecastSalesTable	e	View		Operations
14-1-1	tain authorization of adjust	Maintain demand forecasts for i.	Menu ite	em display		ForecastSalesTable	e	Full control		Operations
Maint		And the second second								o
		le objects that cannot be accesse	d with the s	selected role.						
eges tha	at give access to the securab	le objects that cannot be accesse Securable object type	ed with the s			Access level	Privilege	icense type	Menu iter	m license type
eges tha Privileg	at give access to the securab	Securable object type		e object	Vie		Privilege I		Menu iter Team memb	
eges tha Privileg	at give access to the securab ge name and forecasts for item Me	Securable object type nu item display	Securable	e object sTable				ers		ers
eges tha Privileg ew dema aintain c	at give access to the securab ge name and forecasts for item Me demand forecasts for i Me	Securable object type nu item display	Securable ForecastSale:	e object sTable		w	Team memb	ers	Team memb	ers
eges tha Privileg ew dema aintain c	at give access to the securab ge name and forecasts for item Me demand forecasts for i Me	Securable object type nu item display	Securable ForecastSale:	e object sTable	Full	w	Team memb	ers	Team memb	ers
eges tha Privileç ew dema aintain o aintain o Duty na	at give access to the securab gename and forecasts for item Me demand forecasts for i Me	Securable object type nu item display F nu item display F Privilege name	Securable ForecastSale: ForecastSale	object type	Full	w control Securable object	Team memb	ars and a second	Team memb	ers s
eges tha Privileg ew dem: aintain o aintain o duti	at give access to the securab ge name and forecasts for item Me demand forecasts for i Me es es e into demand forecasts	Securable object type nu item display	Securable ForecastSale: ForecastSale: Securable Menu ite	object type m display	Full	w control Securable object ForecastSalesTable	Team memb Activity user	Access level View	Team memb	ers s Duty license type Operations
eges tha Privileg ew dem: aintain o aintain o duti Duty na Inquire Enable	at give access to the securab ge name and forecasts for item Me demand forecasts for i Me eles e into demand forecasts e the demand forecasting	Securable object type nu item display F nu item display F Privilege name View demand forecasts for item . Maintain demand forecasts for item .	Securable corecastSale: corecastSale: Securable Menu ite Menu ite	object type m display	Full	w control Securable object ForecastSalesTable ForecastSalesTable	Team memb Activity user	s Access level View Full control	Team memb	ers s Duty license type Operations Operations
eges tha Privileges ew dema aintain o aintain o uty na Inquire Enable Mainta	at give access to the securab ge name and forecasts for item Me demand forecasts for i Me es es e into demand forecasts	Securable object type nu item display	Securable corecastSale: corecastSale: Securable Menu ite Menu ite Menu ite	object type m display	Full	w control Securable object ForecastSalesTable	Team memb Activity user	Access level View	Team memb	ers s Duty license type Operations

Maintain

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

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

Event types are as mentioned below:

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

e 🛱 Optimize OPTIONS	<u>م</u>				
urity audit					
Audit					
Security history	🔒 Audit log report 🛛 … More				
-	✓ Event date and time ↓	Event created by 🍸	Event type	Company	Description
Role history	/ 3/13/2019 09:01:27 AM	nsadaiya	User undone sensitive data access	*	User ARNIE is unmarked as s
	3/13/2019 09:00:29 AM	nsadaiya	Entrypoint given sensitive data access	×	Entry point '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 setting
	3/13/2019 08:51:37 AM	nsadaiya	Duty given sensitive data access	*	Duty 'Access expense manag
Segregation of duties conflicts	3/13/2019 08:51:09 AM	nsadaiya	Duty undone sensitive data access	*	Duty 'Access expense manag
	3/12/2019 08:52:11 AM	nsadaiya	Role given sensitive data access	*	Role 'Accountant' is given a
Stand-ins	3/12/2019 06:50:30 AM	nsadaiya	Role undone sensitive data access	*	Role 'Accountant' access to :

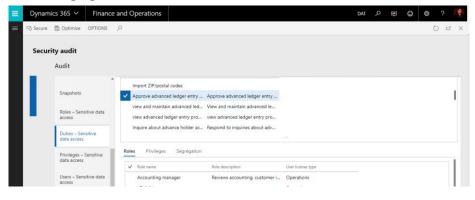
- Sensitive data access forms
 - o Roles Sensitive data access

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

	Dynam	ics 365 🗸	Finance	e and Operations			dat 🔎 戻
≣	G Secure	🛐 Optimize	OPTIONS	Q			
	Secur	ity audit					
		Audit					
			-	🖧 Explore Export			
		Snapshots		Role name rest manager	License type	Role description	Locked
		Roles – Sens	itive data	RapidValue Translator	Team members	Translates RapidValue models	in
		access		RapidValue user	Team members	Shared role for all RapidValue	u
		Duties – Sen data access	sitive	Budget clerk	Activity users	Documents budget events and	r
		uata accesa		Budget contributor	Team members	a	
		Privileges – S data access	Sensitive	Budget manager	Operations	Reviews budget process perfo	
		Users – Sens access	iitive data	Users Duties Privileges	History		
				 Event date and time 	Event created by	Event type	Company
		Charts		12/12/2018 04:17:44 AM	atayyala	Role created	*
					1	A. 1. 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.



o Privileges - Sensitive data access

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

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

o Users - Sensitive data access

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

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

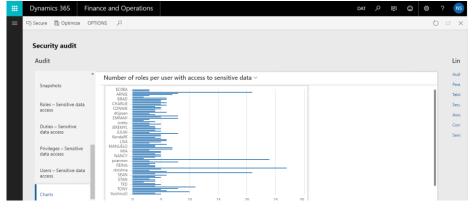
- Charts
 - o Number of security objects with access to sensitive data



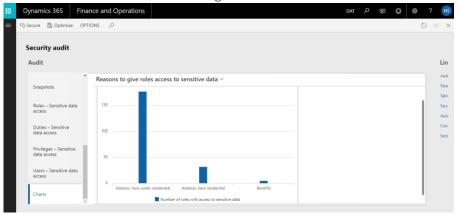
• Number of users with access to sensitive data per organization



o Number of roles per user with access to sensitive data



o Reasons to give roles access to sensitive data

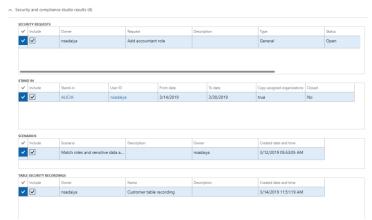


• Person search report extension

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

	Dy	mar	nics 365	Fina	nce and Ope	erations		Syste	em adm	ninistrati	tion >	Inquir	iries >	Person :	search re	eport		DAT	Q	1 9	٢	6	,	?	NS
≡	🔛 Sa	ave	+ New	🗊 Delete	Define search	Process re	eport	ort ~ C	OPTION	is ,C	Ø									*	٥	ø	Q	ď	×
7			N SEARCH REP ON Searc	ort h report	t																				
=		~	Contact se	arch results	(0)																			٦	
		~	Worker sea	arch results (0)																			٦	
		~	Applicant	earch result	s (0)																			٦	
		~	Application	n basket sea	rch results (0)																			٦	
		~	Prospect s	earch results	(0)												er of I to u								
		~	Prospectiv	e vendor sea	arch results (0)												son s								L
		~	Driver sear	ch results (0)								re	port										1	
		~	Security ar	id compliant	ce studio r <u>esulta f</u>																				

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



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

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

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

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

Select one or more privileges on the Matched Privileges grid.

Matched privileges

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

Click on the Create Duty button as shown below.

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

Enter the new duty name and the description.

Create duty

Parameters	
Duty name SCS	Description

Security objects that are included into the new duty

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

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

3.9 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	

3.10 Option to compare Security Snapshots stored in the security setup

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



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

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

Fig 2. Snapshot comparison form

Legend:

1. COMPARE button group - contains two buttons:

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

2. VIEW button group – contains three buttons:

a) Show changes only:

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

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

Fig. 3 See a list of the modified objects

b) Show all objects:

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

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

Dynamics 365 Y Finance and Operations Security and compliance > Inquiries > Snapshot comparison									
	MANAGE OPTIONS P								
npare com	selected Show changes only								
FILTEI Selec P P R R	t security object type ntry Point rivilege luty ole					Sec	nd snapshot		
First s									
First s	Name 1	User license type	Compared	Observation		3	Name 1	User license type	_
2	Name î	User license type	Compared Yes	Observation 0 modifications found		3		User license type Operations	
²irst s 2 ✓	~					3	Name 1	Operations	
First s 2 ✓	Name 1 Action class settings maintain	None	Yes	0 modifications found	•	3	Name 1 Delete write-off factors	Operations	
2 ✓	Name 1 Action class settings maintain Action class settings view	None None	Yes Yes	0 modifications found 0 modifications found	•	3	Name 1 Delete write-off factors Demand Forecasting external API se	Operations None	
2	Name 1 Action class settings maintain Action class settings view Action graph	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	
First s	Name 1 Action class settings maintain Action class settings view Action graph Action populate records task maint	None None Operations None	Yes Yes Yes Yes	0 modifications found 0 modifications found 3 modifications found 0 modifications found	•	3	Name 1 Delete write-off factors Demand Forecasting external API se Demo privilege 1 Demo privilege 2	Operations Operations Operations	

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)

ynamics 365 🗸 🔰 Finance and Op	erations Security and compliance	Inquiries > Snapshot comp	parison											
ave MANAGE OPTIONS 🔎														
MPARE VIEW														
npare selected Show changes only compare Simple view														
Snapshot comparison														
FILTER Select security object type														
Entry Point														
Privilege														
Duty														
🔾 Role														
User														
User COMPARE SNAPSHOTS First snapshot						Second snapshot								
COMPARE SNAPSHOTS						Second snapshot								
OMPARE SNAPSHOTS irst snapshot 2	Name 1	User license type	Compared	Observation		S → Jecrificerse type								
MPARE SNAPSHOTS st snapshot			Compared Yes	Observation 0 modifications found	_,[Identifier VENDEROSPECTIVEVENDORDATAA Deny changing company account eam members								
Identifier	A parameter that is used to group	Team members				Venterfiler Name 1 Just Ticense type VENDPROSPECTIVEVENDORDATAA. Deny changing company account Eam members HCMWORKERACTIONCOMPFIXEDE Deny fixed compensation change re Eam members								
MPARE SNAPSHOTS ist snapshot 2 / Identifier FORECASTPOSITIONS8YBUDGETPLANG.	A parameter that is used to group	Team members Activity users	Yes	0 modifications found		V Identifier Derr license type VENDPROSPECTIVEVENDORDATAA Deny changing company account Eam members HCNWORKERACTIONCOMPTIXEDE Deny invoice approval Eam members TMSINVOICEAPPROVALDENYPROC Deny invoice approval Eam members								
OMPARE SNAPSHOTS Stats snapshot 2 V Identifier FORECASTPOSITIONS8V8UDGETPLANG PURCHRFQFORMLETTER_ACCEPTPROCE	A parameter that is used to group Accept a request for quotation	Team members Activity users Team members	Yes Yes	0 modifications found 0 modifications found	1	Verifier Name 1 Jer license type VENDPROSPECTIVEVENDORDATAL Deny changing company account Eam members HCMWORKERACTIONCOMFPRIZEDE Deny invoice approval Eam members TMSINVOICEAPPROVALDENVPROC Deny invoice approval Eam members HCMPOSTIONACTIONVPAPROE Deny isosition actions by using a w Eam members								
COMPARE SNAPSHOTS Virit Snapphot 2 Virit Snapphot FORECASTPOSITIONSBYBUDGETPLANG, PURCHREGORMLETTER_ACCEPTPROCE HCMBENEFITWORKSPACE	A parameter that is used to group Accept a request for quotation Access benefits workspace	Team members Activity users Team members Operations	Yes Yes Yes	0 modifications found 0 modifications found 0 modifications found		Name 1 Just license type VENDROSPECTIVEVENDORDATA. Deny changing company account 6am members HCMWORKERACTIONCOMPTIXEDE. Deny fixed compensation change re 6am members TMSINVOICEAPPROVALDEN/RROC Deny position actions by using a wa feam members HCMWORKERACTIONCACTION/NERPRED Deny position actions by using a wa feam members HCMWORKERACTIONTERNIWRAPP Deny position actions using a wa feam members								
OMPARE SNAPSHOTS Inst snapshot 2 Cleentifier FORECASTPOSITIONSBYBUDGETPLANG, PURCHREPTERAGONILETTERACCEPTPROCE HCMBENETPHINORSPACE HCMCOMPENSATIONWORKSPACE	A parameter that is used to group Accept a request for quotation Access benefits workspace Access compensation management.	Team members Activity users Team members Operations Operations	Yes Yes Yes Yes	0 modifications found 0 modifications found 0 modifications found 0 modifications found		Name 1 Der license type VeNDPROSPECTIVEVENDORDATAA. Deny changing company account eam members HCMWORKERACTIONCOMPFIXEDE. Deny invoice approval Eam members HCMWORKERACTIONTKAMSWFAP. Deny position actions by using a wor. HCMWORKERACTIONTRAMSWFAP. Deny worker actions by using a wor. Eam members								
Commerce Sharehords First snapshot V locatifier FORECASTOSTITONSBYBUDGETPLANG, PURCHREQFORMLETTER, ACCEPTRACCE HCMEENEFTWORKSBACE HCMCONFENSATIONWORKSPACE TWVEPKISEADMINANALITICS	A parameter that is used to group Accept a request for quotation Access benefits workspace Access compensation management Access expense administrator analy	Team members Activity users Team members Operations Operations Team members	Yes Yes Yes Yes Yes	0 modifications found 0 modifications found 0 modifications found 0 modifications found 0 modifications found		Name 1 Just license type VENDROSPECTIVEVENDORDATA. Deny changing company account 6am members HCMWORKERACTIONCOMPTIXEDE. Deny fixed compensation change re 6am members TMSINVOICEAPPROVALDEN/RROC Deny position actions by using a wa feam members HCMWORKERACTIONCACTION/NERPRED Deny position actions by using a wa feam members HCMWORKERACTIONTERNIWRAPP Deny position actions using a wa feam members								

Fig 5. Advanced view

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

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

Fig. 6 snapshot selection restriction

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

Colour legend:

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

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

Colour legend:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.13 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.

IZE PAGE OPTIONS	EL EL	DIT SHARE				WHICH MODULE?	
en for editing Security diagnost		ead mode Get a link 🗸				✓ Area î	
e this form Advanced Filter/S		evert				Accounts pa	ayable
orkspace 🗸						Accounts re	ceivable
						Audit workb	bench
RIO						Budgeting	
eral		Δ	ham bh	ule access	ARScenario vsingh	Cash and ba	ank management
		A	la mou	ale access		Common	
nario IScenario					Owner vsingh	Consolidatio	ons
scenario					vsingn	Cost accoun	-
cription						Cost manag	
Inpuon						Credit and c	ollections
ess required						Demo data	
						Expense ma	2
Add 🕂 Add module access 📋	Remove S Explore					Fiscal books	
Add 14 Add module access @	nemore an explore					Fixed assets	
Securable object	Securable object type	Access level	File	Remark			
		Access level		Remark	_	Fleet manag	gement
Securable object CustomerInvoiceWorkspace	Securable object type Menu item display	View		Remark		Fleet manag General ledg	gement
Securable object CustomerInvoiceWorkspace CustPaymentWorkspace	Securable object type Menu item display Menu item display	View View		Remark		Fleet manag General ledg No access	ger
Securable object CustomerInvoiceWorkspace	Securable object type Menu item display	View		Remark		Fleet manag General ledg No access View	gement
Securable object CustomerInvoiceWorkspace CustPaymentWorkspace	Securable object type Menu item display Menu item display	View View		Remark		Fleet manag General ledg No access	ger
Securable object CustomerInvoiceWorkspace CustPaymentWorkspace CustTableListPage	Securable object type Menu item display Menu item display Menu item display	View View View		Remark		Fleet manag General ledg No access View Edit	ger
Securable object Customer/nvoiceWorkspace CustPaymentWorkspace CustTableListPage CustTableHoldListPage	Securable object type Menu item display Menu item display Menu item display Menu item display	View View View View View		Remark		Fleet manag General ledg No access View Edit Create	ger jent

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

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

3.14 Snapshots based performance and scalability enhancements

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

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

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

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

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

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

settings. "Set up automatic deletion"

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

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

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

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

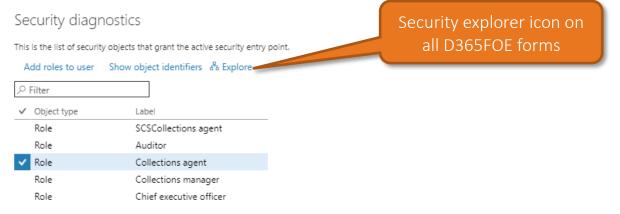
3.15 Improved "Create role wizard" based on a grid framework

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	duties											
Se	ect duties	to be added to the	e new role									
AVAILABLE DUTIES SELECTED DUTIES												
•	/ Duty		Description		User license type			~	Duty	Descript	tion	User license type
	Maintai	in Absorption Costs			Operations		\rightarrow		Inquire into Absorption Costs			Team members
IE	Import	ZIP/postal codes			Operations				Inquire into purchase agreem	Respon	id to inquiries about p	Team members
IE	Approv	e advanced ledger ent	Approve a	dvanced ledger ent	Operations		\leftarrow					
view and maintain advanced I View and maintain advanced I Team members												
	view advanced ledger entry p view advanced ledger entry p Team members Role license type											
						he	for	P	you finish			
CRE	TE ROLE					200			yourningh			
Sur	mary					_	-	-		·		
		ted role setup. Click Finish		e.								
	e resulting rol e name	e will have the user license ty Role descript										
	S_NewRole	SCS_NewR										
Sele	cted privileg	les							Selected duties			
_	vilege name	Description		License type.					Duty name		Description	License type.
	port KLADR a		eviations from th	Operations					Inquire into Absorptio			Team Members
V	ew accounting	distributions		Team Members					Inquire into purchase	agreem	Respond to inquiries about p	Team Members

3.16 Accessing Security Explorer from all D365 FOE forms

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



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

SERS	rity exp			COLLECTIONS AGENT		DUTIES		PRIVI			ENTRY POIN			
^a Pin	users			焓 Unpin role		-ta Pin duty		-ei pi	n privilege		-t= Pin entr	y point		
	User ID 1	Name	Highest license typ	Role name 1	License type	Duty name 1	License type		Privilege name 1	License type	×	Entry point (AOT name) 1	Access right	Entry point t
	ARNIE	ARNIE	Operations	🕫 🗧 Collections agent	Operations	Collections workspace	Team members		 Calculate interest notes 	Operations		□ AccountingDistCustFreeInvoice	View	Menu item
•	Connie	CONNIE	Operations			Inquire into bill of exchange	ge s Team members		Cancel collection letters	Operations		AccountingDistCustInvJour	View	Menu item
•	OSCAR	OSCAR	Operations			 Inquire into collections sta 	atus Operations		 Cancel interest notes 	Operations		□ AccountingDistMarkupTransInv	View	Menu item
•	SARA	SARA	Operations			Inquire into credit card pr	oce Team members		CashDiscountEntityView	None		□ AccountingDistMarkupTransPO	View	Menu item
						Inquire into customer invo	pice Activity users		 Change transaction collection. 	Operations		☐ AccountingDistMarkupTransR	View	Menu item
						Inquire into customer mas	ster Team members		Change/edit customer transa	Activity users		□ AccountingDistPurchTable	View	Menu item
						Inquire into customer pay	me Activity users		 Change/edit customer transa 	Operations		□ AccountingDistributions	View	Menu item
						Inquire into customer refe	ren Team members		 Change/edit customer transa 	Operations		□ AccountingDistributionsDocu	View	Menu item
						Maintain activities	Team members		Correct interest codes	Team members		☐ AccountingDistTaxTransTmp	View	Menu item
						 Maintain collections trans 	acti Operations		 Create a customer record fro 	Operations		□ AccountingDistVendEditInvDe	View	Menu item
						 Maintain contacts 	Activity users		 Create a customer record fro 	Operations		☐ AccountingDistVendEditInvHdr	View	Menu item
						 Maintain customer master 	r Operations		Create collection letters	Team members		☐ ActivitiesMain	View	Menu item
						Maintain financial period	clos None		 Creating a customer from pro. 	Operations	·	□ ActivitiesMain	Full control	Menu item
						 Maintain periodic settlem 	ent Operations		CustBalanceGenerate_CN	Team members		□ ActivitiesMainBasic	View	Menu item
						Manage customer credit a	and Team members		CustCustomerGroupEntityView	None		□ ActivitiesMainBasic	Full control	Menu item
						View sensitive bank account	int i None		CustDirectDebitMandateEntit.	None		☐ Activity/ViewRecord	View	Menu item

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

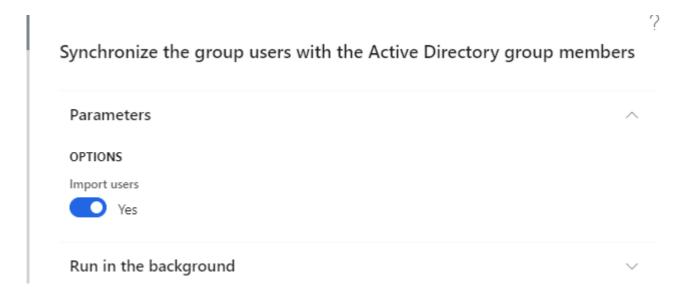
You now have an option to create duties along with the privileges while using the "Merge roles" feature. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.).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

Roles 'Accounting manager' and 'Accour	ntant' are in violation of segregation of (duties rule 'New Segregation of duties rule2':
MERGE ROLES		
	e to. ock target role? Yes	SOD violations warning
Select the roles to merge from.		
AVAILABLE ROLES		SELECTED ROLES
✓ Available roles		✓ Selected roles
Accounting supervisor	1	\rightarrow Accounting manager
Accounts payable centralized	payments clerk	← Accountant
Accounts payable clerk		~
Accounts payable manager		
Accounts payable payments cl	erk	
ENABLED ACTION MENU ITEMS DISPLAY MENU ITEMS OUTPUT MENU ITEMS TABLE PERMISSIONS CREATE DUTY	PRIVILEGE NAME SCS_AccountingSuperUser \ SCS_AccountingSuperUser \ SCS_AccountingSuperUser \ Create duty option	
Yes 💽		
ENABLED	DUTY NAME	7
ACTION PRIVILEGES	SCS_AccountingSuperUser ∨	
DISPLAY PRIVILEGES	SCS_AccountingSuperUser \lor	
OUTPUT PRIVILEGES	SCS_AccountingSuperUser \lor	*
TABLE PRIVILEGES	SCS_AccountingSuperUser \lor	

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

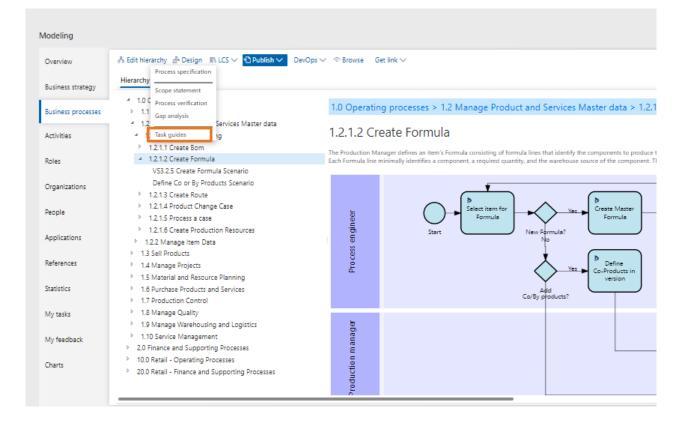
This is very useful for offline analysis and drill down of the required security setup in a company or department. We added a new small feature to our Azure AD group synchronization job. On the dialog of the Synchronize the group users with the Active Directory group members, we introduced a new parameter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

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



3.19 Uptake RapidValue BPM Suite Scenarios directly as SCS Security Scenarios

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



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

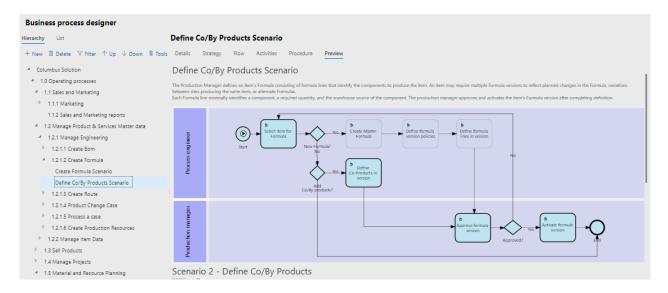


Figure: Scenario-Procedure activity based modeling

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

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

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

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

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

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

3.20 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 ↑	Type	First	Firs	t securable object type	First access level	Second
nhanced SoD ules	Demo rule for Entry	points Entry point	AccountingDist	tVendEditInvHdr Me	nu item display	Create	AdvancedLedgerEntryDateDr
	Match role test - ep	Entry point	AuditPolicyCase	eGroup Me	nu item display	Full control	ACOJournalPost_BR
hanced SoD	Match roles test - du	ty Duty	Maintain Absor	rption Costs		No access	Maintain audit policies
onflicts	Match roles test - du	ty 2 Duty	Maintain audit	policies		No access	Maintain Absorption Costs
harts	Match roles test - ep	2 Entry point	ACOJournalPos	st_BR Me	nu item action	Full control	AuditPolicyCaseGroup
iui ta	Match roles test - ep	3 Entry point	DSMSecurityRe	equestPriorityH Me	nu item action	Correction	ACOJournalPost_BR
	Match roles test - ep	4 Entry point	DSMMultiSelec	tRoleSetup Me	nu item display	Full control	DSMSecurityRequestPriorityH
	Match roles test - pri	v 1 Privilege	Maintain case <u>c</u>	grouping criteria		No access	Maintain Absorption Costs
	Match roles test - pri	v 2 Privilege	Maintain Absor	rption Costs		No access	Maintain case grouping criteri
	Risk						
	✓ Risk ID	Category	Status	Inherit risk	Response	Residual risk	Owner
	Risk-00000006	Operational	Initial	Medium	Accept	Low	Admin
	Risk-00000007	Strategic	Initial	Very low	Ignore	Very low	Admin

3.21 Organization risk Register

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

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

3.22 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.

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

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

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

	ENTRY POINTS						
	- Pin entry point and permission						
	Туре	Access right					
	Table	No access					
	Service operation	No access					
C	Service operation	Full control					
	Menu item display	View					
	Table	View					
	Menu item display	Full control					
C	DataEntity	View					
	DataEntity	Full control					

3.24 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.

3.25 A new "Share" workspace

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

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

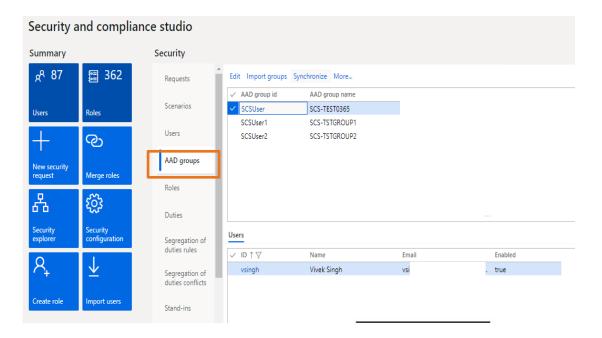
ecurity i	management						
ummary		Security					
_я я 109	: 190	Requests	+ New 🖉 Edit \cdots See more				
			✓ Request	Туре	Priority	Status	Owner
Users	Roles	Scenarios	Provide access to customer and Project activity form	General	Normal	Approved	JOHN
55015	THE S		Purchase order form access	Modify user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

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

3.26 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.



		··· More			
✓ User ID ↑ Nam	e Email	License type		Company	Person
TRICIA	TRICIA	TRIC		Operations	USS
VINCE	VINCE	VIN		. Operations	USN
✓ vsingh	Vivek Singh	vsin		Operations	USN
Wayne	Wayne	Way		Operations	USN
voichiroo	VOICHIROO	voic		Onerations	2211
Roles History	Login date and time	AAD groups			
✓ AAD group id	AAD group na	ne			
SCSUser	SCS-TEST036	5			
	TRICIA VINCE Vince Vaina Vayne Vaichiron Roles History	TRICIA TRICIA VINCE VINCE vsingh Vivek Singh Wayne Wayne voichirco VOICHIROO Roles History Login date and time ✓ AAD group id	TRICIA TRICIA TRIC VINCE VINCE VIN vsingh Vivek Singh vsin Wayne Wayne Way voichiroo VOICHIBOO voichiroo Roles History Login date and time AAD groups	TRICIA TRICIA TRIC VINCE VINCE VIN vsingh Vivek Singh vsin Wayne Wayne Way voichiroo VOICHIBOO voic Roles History Login date and time AAD groups	TRICIA TRIC Operations VINCE VINCE VIN Operations vsingh Vivek Singh vsin Operations Wayne Wayne Way Operations voichiroo VOICHIROO voic

3.27 Verify SoD rules in Stand in

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

	+New [🗓 Delete 🛛 🖒	Assign stand-in ro	oles Validate S	oD rules	Options 🔎	
	Stand-in						
	P Filter						
	🗸 User ID	1	Stand-in	From	date	To date	Copy assigned organizations
	ALICIA		APRIL	12/1	3/2018	12/13/2018	0 🗸
	APRIL		dtijssen	1/19	/2019	1/20/2019	\checkmark
	atayya	la	acardol	10/2	1/2019	10/31/2019	\checkmark
	BENJA	MIN	CHARLIE	10/3	/2019	10/11/2019	
	CHARL	IE.	BENJAMIN	10/3	/2019	10/17/2019	
	dtijsse	n	Admin	1/21	/2019	1/22/2019	\checkmark
	JACOB		JEREMYL	10/2	2/2019	10/31/2019	
	JACOB		nsadaiya	10/2	2/2019	10/24/2019	\checkmark
	nsadai	ya	ALICIA	3/14	/2019	3/30/2019	\checkmark
	OSCAR	ł	JULIA	10/2	2/2019	10/31/2019	\checkmark
ssignmen			Validate SoD rules Optio		e 'Accounts receivable p	ayments clerk' contains duty 'Maintain customer p	ayments' and the role 'Accountant' contains duty 'Enable bank managemen
signmen	nt of OSCAR's roles to JULI				e 'Accounts receivable p	ayments clerk' contains duty 'Maintain customer p	syments' and the role "Accountant" contains duty "Inable bank managemen
ssignmen Star	nt of OSCAR's roles to JULI nd-in P Filter V User ID 1	A are in violation of SoD rules Stand-in	: 'SCS-083-Release production ord From date	er and move inventory': The rol To date	Copy assigned		syments' and the role "Accountant" contains duty "Inable bank managemen
signmen Star	nd-in Pilter User ID ALICIA	A are in violation of SoD rules Stand-in APRIL	: 'SCS-083-Release production ord From date 12/13/2018	er and move inventory': The rol To date 12/13/2018	Copy assigned		syments' and the role "Accountant" contains duty "Trable bank managemen
signmen Star	nd-in P Filter V User ID T ALICIA APRIL	A are in violation of SoD rules Stand-in APRIL dtijssen	SCS-083-Release production ord From date 12/13/2018 1/19/2019	er and move inventory': The rol To date 12/13/2018 1/20/2019	Copy assigned		syments' and the role "Accountant" contains duty "Inable bank managemen
signmen Star	nd-in Pilter User ID ALICIA	A are in violation of SoD rules Stand-in APRIL	: 'SCS-083-Release production ord From date 12/13/2018	er and move inventory': The rol To date 12/13/2018	Copy assigned		syments' and the role 'Accountant' contains duty 'Inable bank managemen
signmen Star	nd-in P Filter User ID T ALICIA APRIL atayyala	A are in violation of SoD rules Stand-in APRIL dtijssen acardol	* \$2\$-083-Release production and From date 12/13/2018 1/19/2019 10/21/2019	er and move inventory). The rol To date 12/13/2018 1/20/2019 10/31/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Enable bank managemen
signmen Star	nt of OSCAR's roles to JULIA nd-in 2 Filter 2 User ID T ALICIA APRIL atayyala BENJAMIN	A are in violation of SoD rules Stand-in APRIL dtijssen acardol CHARLIE	* \$25-083-Release production and From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019	er and move inventory'. The rol To date 12/13/2018 1/20/2019 10/31/2019 10/11/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Trable bank managemen
signmen Star	nd-in D ² Filter 2 Filter AUCIA APRIL atayyala BENJAMIN CHARUE	A are in violation of 5oD rules Stand-in APRIL dtijsen acardol CHARLIE BENJAMIN	*SC5-083-Release production and From date 12/13/2018 1/19/2019 10/3/2019 10/3/2019	er and move inventory' The rol To date 12/13/2018 1/20/2019 10/31/2019 10/11/2019 10/17/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Enable bank managemen
ssignmen Star	nd -in OF Filter V User ID 1 ALICIA APRIL ATV APRIL ATV ALICIA APRIL ALICIA APRIL CHARLIE dtjissen	Stand-in Stand-in APRIL dtijssen acardol CHARLIE BENJAMIN Admin	* SCI-083-Release production and From date 12/13/2018 1/19/2019 10/21/2019 10/3/2019 10/3/2019 1/21/2019	er and move inventory). The rol To date 12/13/2018 1/20/2019 10/11/2019 10/11/2019 10/17/2019 1/22/2019	Copy assigned		ayments' and the role 'Accountant' contains duty 'Enable bank managemen

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

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

	Security							
ዶ 103 📰 175	Requests							
		✓ User ID ↑	Name	Email		License type	Company	Person
sers Roles	Scenarios	abahlman	Ard Bahlman	ab		Operations	DAT	
	L.	acardol	Adri Cardol	aci		Activity users	DAT	
- ©	Users	andre.adcalavon	André Arnaud de Calavon	an	.com	Operations	DAT	
	AAD groups	atayyala	Anil Kumar Tayyala (ATAYY.TI)	ata		Team members	dat	
lew security equest Merge roles	And groups	dvschie evhofwegen	David van Schie (DVSCH.TI) Eric van Hofwegen	dv	1	Operations Operations	dat DAT	
	Roles	nsadaiya	Nitish Sadaiya (NSADA.TI)	evi ns		Operations	usmf	
음 🐯		Pradeep.Bapna	Pradeep Kumar Bapna	Pra	om	Operations	DAT	
10 VXV	Duties	SCS-TSTGroup1	SCS-TSTGROUP1			Operations	DAT	
ecurity Security xplorer configuration		SCS-TSTGroup2	SCS-TSTGROUP2			Operations	DAT	
xplorer configuration	Segregation of duties rules	✓ vsingh	Vivek Singh (VSING.TI)	vsi		Operations	dat	
eate role Import users	duties conflicts Stand-ins Data security Snapshots History Charts	Roles History Log Last login date and time 11/6/2019 07:48:42 AM	AAD groups Days since last login onlin 0 0.000					
User's last log < 1 mo 1 to 3 mo	in							
> 3 mo Never Io								

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

3.30 A List page with Workflow delegation details

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

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

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

3.31 User groups – combined two tabs in one

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

Users can be added to different groups using same tab.

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

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

4. Bug fixes

4.1 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'.

4.2 Security and compliance studio 10.0.32.38

	eccarrey and compliance sea	
ID	Description	Observation
	CS00223035 Meaning of any unique	In specific scenarios the license suggestion
	license	from Security Explorer was not correct.
160423		Calculating licenses has been improved. ¹
	CS00223817 AD user status sync	Microsoft users like 'PowerPlatformApp'
		which are used specifically by the system to
		operate different frameworks were disabled.
163925		Issue has been fixed.
	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
144592		fixed.
	Internal License calculation not working	Some activity users were displaying incorrect
	correctly - 'Activity' license shouldn't be	license.
161013	included	Issue fixed. ¹
	Internal Implement new form pattern for	Applying new form patterns to the
162939	vertically scrolling workspaces	workspaces. They are now displayed vertical
	Internal Review licenses on the menu	Security and Compliance Studio's menu
	items	items have been reviewed and the user
164224		licenses have been updated accordingly
	Internal Merge role wizard -> entity	Permissions at entity level were not set
	permissions set wrong on merged role	correctly when roles were created/modified
		using 'Merge role' wizard.
165288		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 To-Increase support, so we can review, improve and contact Microsoft to get better suggestions in future releases.

4.3	Security and compliance st	udio 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.

4.3 Security and compliance studio 10.0.31.37

4.4 Security and compliance studio 10.0.29.36

ID	Description	Observation
153855	Internal Synchronize the group users with AD group members batch runs into error when Import roles parameter is activated.	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.

4.5 Security and compliance studio 10.0.28.34

ID	Description	Observation
	CS00221370 Incorrect user security log	Now shows the correct log items
145372	in SCS	
	CS00221689 Issue with Licensing	If snapshot is in queue and due to start in the
	framework	upcoming 30 mins, the refresh license job
146730		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.

4.6 Security and compliance studio 10.0.27.33

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

4.7 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

4.8 Security and compliance studio 10.0.26.31

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

4.9 Security and compliance studio 10.0.25.30

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

4.10 Security and compliance studio 10.0.24.29

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

4.11 Security and compliance studio 10.0.22.27

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

4.12 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.

4.13 Security and compliance studio 10.0.12.5

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

4.14 Security and compliance studio 10.0.12.4

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

4.15 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.

4.16 Security and compliance studio 10.0.12.2

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

4.17 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

4.18 Security and compliance studio 10.0.10.1

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

4.19 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

4.20 Security and compliance studio 10.0.6.10

ID	Description
108559	CS00128698-DSM Tables growing rapidly (V10.0.6.6)
108471	CS00128399-Export and import of security scenarios fails

108836 CS00129465-TI SCS Parameters Data Entity Missing Fields

4.21 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

4.22 Security and compliance studio 10.0.6.8

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

4.23 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

4.24 Security and compliance studio 10.0.6.6

ID	Description
100323	CS00111058-Unable To Import Security Roles

4.25 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

4.26 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

4.27 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

4.28 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

4.29 Security and compliance studio 10.0.6.1

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

4.30 Security and compliance studio 10.0.3.3

ID	Description
83602	 Standard Import user menu item is not visible if SCS license expired.

4.31 Security and compliance studio 10.0.3.2

ID	Description
77956	CS00069693 – License Count Data Source.

4.32 Security and compliance studio 10.0.3.1

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

4.33 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.

4.34 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.

4.35 Security and compliance studio 10.0.1.1

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

4.36 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.

4.37 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.

4.38 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'

4.39 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

4.40 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

4.41 Security and compliance studio 81.20.3.1

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

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

ID	Description
66652	TI-12204-S3M9 Audit log duplicate records as coming from AOT
66653	TI-12205-P0Y5 User audit log not working properly

66654	4 TI-12213-S8Q4 Add table permissions to role or privilege	
66533	5533 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.		

4.43 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.	

4.44 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.

4.45 Security and compliance studio 1804.15.2.1

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

4.46 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.

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

5.2 Deprecated features older versions

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

6. Known issues

- 1. The license recommendations provided in the security explorer form might show incorrect recommendations in case of custom roles. We are working on a solution where the information is easy to read and understand.
- 2. 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.
- 3. Bug 62494 requires the one time running of a batch program to update the data model changes. Instructions are as below:

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

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

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

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

Steps:

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

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

*NOTE: this option will be available only if you have data into the "DSMSecurityEntryPointPrivAssociation" table (the table from the error above).

Dynamics 365	Finance and Operations	
Save OPTIONS	م	
Security and	d compliance studio pai	ameters
General	Setup gene Prefix	ral information for Security and Compliance studio
Migration	SCS_	red duties and pri
	Yes +	
	Color Hex	* IFBF
	INITIALIZE SC Lock 'Initialize	IT AUDIT Security and com
	No (SNAPSHOTS	D
	Limit number	of snapshots

Fig. 1 New tab in SCS Parameters form

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

```	0 /		
🗟 S	ave OPTIONS 🔎		
Security and compliance studio parameters			
	General	Migrate data to newest version	
	Migration	Migrate data	

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

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

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

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

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