
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.	Features 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	28
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.....	36
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 merging roles.....	41
3.13	Ability to create scenarios from D365 module menus.....	42
3.14	Snapshots based performance and scalability enhancements	43
3.15	Improved "Create role wizard" based on a grid framework	45
3.16	Accessing Security Explorer from all D365 FOE forms	45
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	Security and compliance studio 10.0.34.39	56
4.2	Security and compliance studio 10.0.32.38	56
4.3	Security and compliance studio 10.0.31.37	57
4.4	Security and compliance studio 10.0.29.36	57
4.5	Security and compliance studio 10.0.28.34	57
4.6	Security and compliance studio 10.0.27.33	58
4.7	Security and compliance studio 10.0.26.32	58
4.8	Security and compliance studio 10.0.26.31	58
4.9	Security and compliance studio 10.0.25.30	58
4.10	Security and compliance studio 10.0.24.29	58
4.11	Security and compliance studio 10.0.22.27	58
4.12	Security and compliance studio 10.0.18.1	58
4.13	Security and compliance studio 10.0.12.5	59
4.14	Security and compliance studio 10.0.12.4	59
4.15	Security and compliance studio 10.0.12.3	59
4.16	Security and compliance studio 10.0.12.2	59
4.17	Security and compliance studio 10.0.12.1	59
4.18	Security and compliance studio 10.0.10.1	59
4.19	Security and compliance studio 10.0.6.11	59
4.20	Security and compliance studio 10.0.6.10	59
4.21	Security and compliance studio 10.0.6.9	60
4.22	Security and compliance studio 10.0.6.8	60
4.23	Security and compliance studio 10.0.6.7	60
4.24	Security and compliance studio 10.0.6.6	60
4.25	Security and compliance studio 10.0.6.5	60
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	Deprecated features older versions	64
6.	Known issues	65

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.

This is summarized in the following table.

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

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

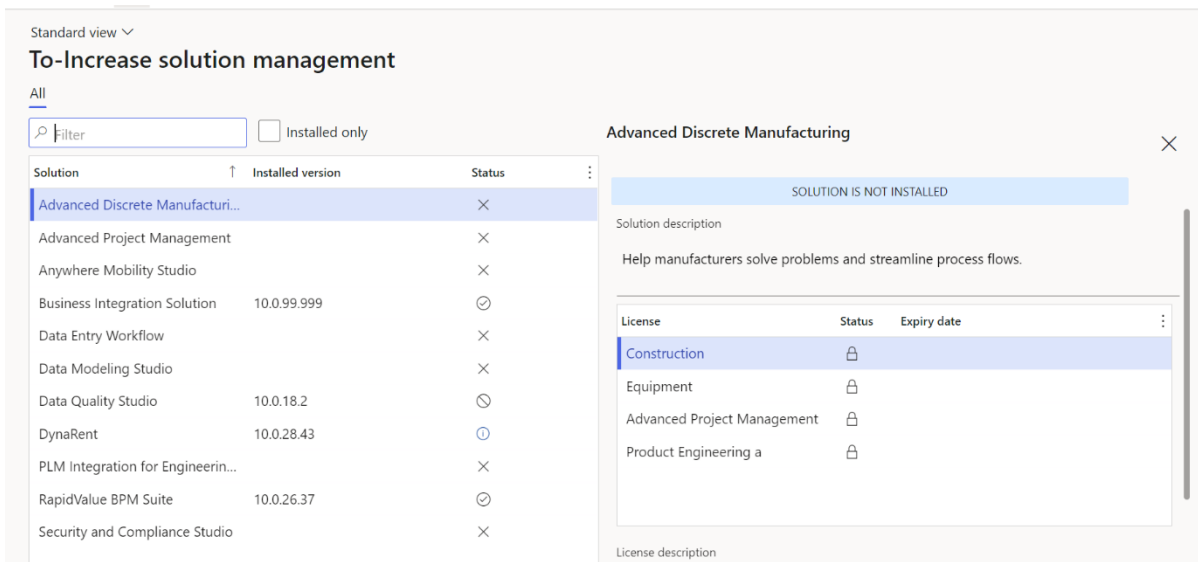
1.5 Common features

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.



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.

The screenshot shows a feedback form titled 'To-Increase would love your feedback!'. The form asks for a rating from 1 to 5 and a text box for additional insights. It includes a 'Submit' button and a 'Cancel' button.

To-Increase would love your feedback!

Please rate your experience in using the All solutions screen.

5 - Excellent

4

3

2

1 - Poor

Please tell us why you chose the rating. Additional insights would help us improve our products further.

Thank you for providing us feedback!

Your privacy is important to us. To protect your privacy, please don't include any personal information.

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 be 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 further 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 explorer 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.

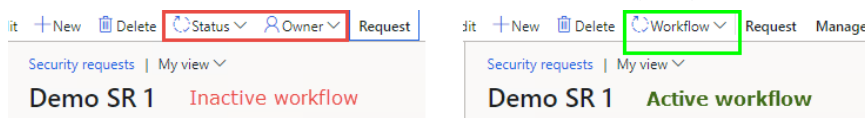
3.1 Security requests enhancements and workflow

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.

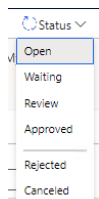
One of the greatest enhancements brought to you is the automated process that will create security requests once it is approved.

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.



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



Security types

- a) General

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

Security requests | My view ▼

Demo SR 1

General

Request	Type	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	Type	Origin	Area
Demo SR 1	Create user	User requests	WHS

Status

Priority	Status	Owner
Normal	Open	Admin

Create users

User ID	User name	Email	Company
newUser1	newUser1	newUser1@to-increase.com	DAI

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 view

Demo SR 1

Demo SR 1 Assign role to user User requests

Status

Priority: Normal Status: Open Owner: Admin

Assign roles to user

USER

User ID: Admin User name: Admin Email: fmihoc@toincrease.onmicro... Company: USMF

ROLES

+ Add Remove

Role name	Description	Role AOT name
Auditor	Manages and reviews aud...	AUDITPOLICYMANAGER

COMPANIES

+ Add Remove

Company	Company accounts
CNMF	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.

Security requests | My view

Demo SR 1

Request: Demo SR 1 Type: Remove role from user Origin: User requests

Status

Priority: Normal Status: Open Owner: Admin

Remove roles from user

USER

User ID: Admin User name: Admin Email: fmihoc@toincrease.onmicro... Company: USMF

ROLES

+ Add Remove

Role name	Description	Role AOT name
Lease clerk	The lease clerk role has ac...	ASSETLEASECLERKROLE
View lease	View of lease roles	ASSETLEASELEASEVIEW

e) Disable user

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

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

Security requests | My view ▾

Demo SR 1

General

Request: Demo SR 1 Type: **Disable user** Origin: User requests Area: WHS

Status

Priority: Normal Status: Open Owner: Admin

Disable users

Add Remove

<input type="checkbox"/>	User ID	User name
<input type="checkbox"/>	BrunoD	BrunoD

Description

f) Enable user

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

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

Security requests | My view ▾

Demo SR 1

General

Request: Demo SR 1 Type: **Enable user** Origin: User requests Area: WHS

Status

Priority: Normal Status: Open Owner: Admin

Enable users

Add Remove

<input type="checkbox"/>	User ID	User name
<input type="checkbox"/>	JanetS	Janet Schor

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.

Security requests | My view ▼

Demo SR 1

General

Request: Demo SR 1 Type: **Delete user** Origin: User requests Area: WHS

Status

Priority: Normal Status: Open Owner: Admin

Delete users

Add + Remove -

	User ID	User name	Email
<input type="radio"/>	CASSIE	CASSIE	CASSIE@contosoax7.onm...
<input type="radio"/>	cdsauroruser	Auroraus...	Auroruser01@capintegr...

Description

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.

Save + New + Delete + Status ▼ + Owner ▼ | **Request** Manage Options +

Priority: High priority, Normal, Low View: Related record

Security requests | My view ▼

Demo SR 1

General

Request: Demo SR 1 Type: **Delete user** Origin: User requests Area: WHS

Status

Priority: Normal Status: Open Owner: Admin

Create role

ROLE

[Upload task recording](#)

Role name: SCS_DemoRole1 Description: Demo purposes Scenario: [skRecordingForCSReplicate.axtr](#)

SCENARIO DETAILS

<input type="radio"/>	Step number	Securable object	Securable type	Access level	Description	File name	Child scenario	Remark
<input type="radio"/>	1	salestablelistpage	Display	Full control	Go to Accounts receivabl...	TaskRecordingForCSRepli...		
	2	DefaultDashboard	Display	Full control	Close the page.	TaskRecordingForCSRepli...		Additional securable object found in the task recording
	5	salestablelistpage	Display	Full control	Go to All sales orders.	TaskRecordingForCSRepli...		
	7	SalesTableDetails	Display	Full control	In the list, click the link in ...	TaskRecordingForCSRepli...		Additional securable object found in the task recording
	9	SalesLineCopy	Display	Full control	Click From line.	TaskRecordingForCSRepli...		
	13	InventTrans	Display	Full control	Click Transactions.	TaskRecordingForCSRepli...		

Description

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.

Modify role

ROLE

Role name	Description	Role AOT name
View lease	View of lease roles	ASSETLEASEVIEW

SCENARIO DETAILS

Step number	Securable object	Securable type	Access level	Description	File name	Child scenario	Remark
1	salestablelistpage	Display	Full control	Go to Accounts receivable > Orders > A...	DemoTx recording.axtr		
3	SalesTableDetails	Display	Full control	In the list, click the link in the selected r...	DemoTx recording.axtr		Additional securable object found in the task recording
5	SalesCopyAllLines	Display	Full control	Click From all.	DemoTx recording.axtr		
8	InventReserve	Display	Full control	Click Reservation.	DemoTx recording.axtr		
10	MCROrderNotes	Display	Full control	Click Notes.	DemoTx recording.axtr		
13	InventTransferOrderCreat...	Action	Full control	Click Transfer order.	DemoTx recording.axtr		

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**.

Lock roles

Role name	Name
Applicant anonymous (external)	ANONYMOUSAPPLICANT

k) Unlock role

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

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

Security requests | My view

Demo SR 1

General

Request: Demo SR 1 | Type: **Unlock role** | Origin: User requests | Area: WHS

Status

Priority: Normal | Status: Open | Owner: Admin

Unlock roles

Role name	Name
Warehouse worker	WMSWAREHOUSEWORKER

Description

l) Delete role

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

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

Security requests | My view

Demo SR 1

General

Request: Demo SR 1 | Type: **Delete role** | Origin: User requests | Area: WHS

Status

Priority: Normal | Status: Open | Owner: Admin

Delete role

Role name	Description	Role AOT name
SCS_RoleTest_2		6DEC7811-E0C5-42C5-94...
SCS_RoleTest1		82B6FA62-0C74-46CC-8D...

Description

m) Create rule

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

Security requests | My view

Demo SR 1

General

Request: Demo SR 1 | Type: **Create rule** | Origin: User requests | Area: WHS

Status

Priority: Normal | Status: Open | Owner: Admin

Enhanced SoD rules

Name	Type	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	AdvancedLedger...	Menu item display	Create	BankChequeCompanyL...	Menu item display	Full control	4/28/2022 10:43:44...	12/31/2154 11:59:5...	<input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/>

Description

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.

Security requests | My view ▾

Demo SR 1

General

Request: Demo SR 1 | Type: **Resolve conflict** | Origin: User requests | Area: WHS

Status

Priority: Normal | Status: Open | Owner: Admin

Enhanced SoD conflicts

+ Add Remove

Rule name	Type	User ID	First	Role	Second	New role	Resolution	Override reason	Role to remove
Duty test1	Duty	APRIL	Approve budget plans	Budget clerk	A parameter that is used t...	Budget manager	Exclude		Existing role
<input checked="" type="checkbox"/> Test 1	Duty	EMMAH	PrintMgmtSetupUI/Main	Sales clerk	ProjActivity	Sales representative	Override	Demo purpos	Existing role

Description

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.

Security requests | My view ▾

Demo SR 1

General

Request: Demo SR 1 | Type: **Delete rule** | Origin: User requests | Area: WHS

Status

Priority: Normal | Status: Open | Owner: Admin

Delete enhanced SoD rules

+ Add Remove

Name	Type	Effective from	Effective to	First	First securable object type	First access level	Second	Second securable object type	Second access level
<input checked="" type="checkbox"/> SoD Test 1 - do not use	Entry point	4/20/2021 12:11:46 PM	12/31/2154 11:59:59 PM	DSMAuditLog	Menu item display	View	DSMAssetClassification	Menu item display	View
Duty test1	Duty	11/25/2021 2:00:45 PM	12/31/2154 11:59:59 PM	Approve budget plans		No access	A parameter that is used t...		No access

Description

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.

Security requests | My view ▼

Demo SR 1

General

Request: Demo SR 1 Type: Add stand-in Origin: User requests Area: WHS

Status

Priority: Normal Status: Open Owner: Admin

Create stand-in

+ Add Remove

<input type="checkbox"/>	<input type="checkbox"/>	User ID	Stand-in	From date	To date	Copy assigned organizations
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Admin	ALICIA	4/28/2022	4/30/2022	<input checked="" type="checkbox"/>

Description

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.

Security requests | My view ▼

Demo SR 1

General

Request: Demo SR 1 Type: Cancel stand-in Origin: User requests Area: WHS

Status

Priority: Normal Status: Open Owner: Admin

Remove stand-in

+ Add Remove

<input type="checkbox"/>	<input type="checkbox"/>	User ID	Stand-in	From date	To date	Copy assigned organizati...
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Admin	ALICIA	4/28/2022	4/30/2022	<input type="checkbox"/>

Description

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.

Security requests | My view ▾

Demo SR 1

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 | Area: AssetLease | Mitigation: Test | Status: Initial

Category: Strategic | Inherent risk: Very low | Residual risk: Very low | Response: Ignore

SOD RULES

+ Add Remove

Name	Organization Risk
Test 1	Dmeo business risk

Description

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

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.

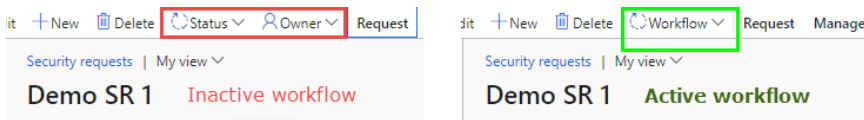
Security Requests workflow configuration

My view ▾

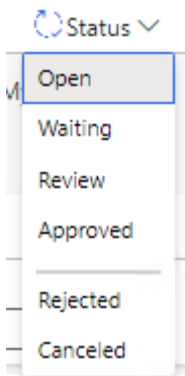
Filter

Status	Default	ID	Name	Association	Type	Instances	Active vers...
<input type="radio"/>	✓	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.



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:

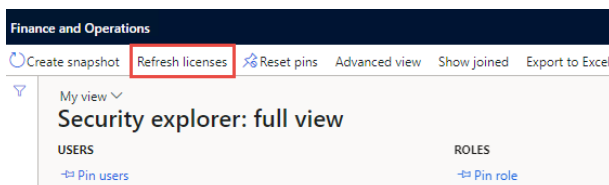
- Approve – set the status to **Approved** and the request will be automatically created.
- Reject – set the status to **Reject** and decline the request.
- Require more information from the user and set the status to **Rejected** or back to **Open**.

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:

- Navigate to **Security and Compliance Studio module -> Inquires ->** and open **Security explorer** form and here run the “Refresh licenses” batch job option and wait to finish.



- After the “Refresh licenses” job finished navigate to **Security and Compliance Studio module -> Setup ->** and open the **Parameters** form.

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

Security and compliance studio parameters

General setup for the purchased licenses

[Open admin.microsoft.com](https://open.admin.microsoft.com)

LICENSE PARAMETERS INPUT

License	No of licenses
Activity users	150
EAM	20
Finance	10
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.

License optimization

Summary

Merge roles | Security explorer

License

Usage

All users | Full users | Activity users | Team members | Scenarios

License type	Actual use...	Licensed users c...	Remaining us...
Finance	11	10	-1
HR	10	60	50
ProjectOperations	4	67	63
Retail	15	55	40
SCM	29	18	-11
Activity users	12	150	138
Team members	16	76	60
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 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.

Security explorer: full view

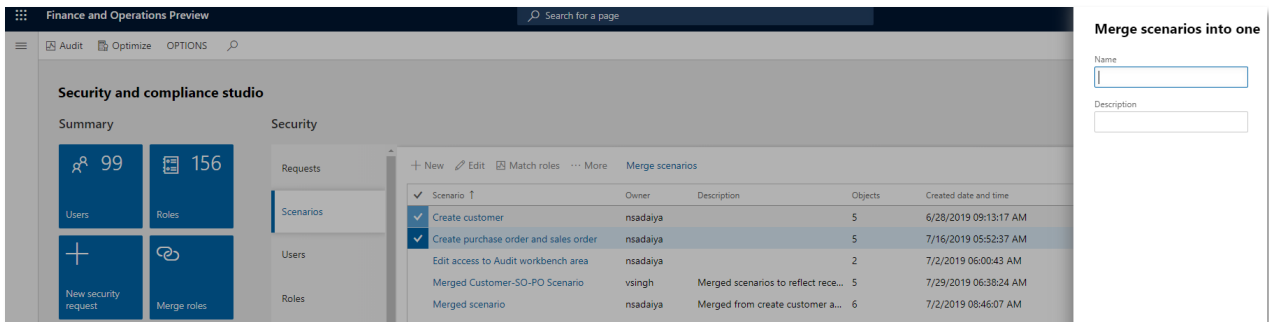
USERS | ACCOUNTANT | DUTIES | PRIVILEGES | ENTRY POINTS

User ID	Name	Role name	Duty name	Privilege name	Entry point (AOT name)
OSCAR	OSCAR	Accountant	Configure electronic fiscal d	@ApplicationSuite_Localizati	AbatementCertificate_IN
RetailServiceAccount	RetailService	Accounting manager	Enable bank management c	@ApplicationSuite_Localizati	AbatementPeriodicCertificate_IN
STAN	STAN	Accounting supervisor	Enable electronic document	Account number enhanced	Accountant_BR
		Accounts payable centralize	Enable escheatment proces	account reference -ViewLed	Accountant_BR
		Accounts payable clerk	Enable EU sales list proces	AccountingSourceExplorerV	AccountantElectronicAddressEdi...
		Accounts payable manager	Enable financial reports gen	Action class settings mainta	AccountantElectronicAddressEdi...
		Accounts payable payment	Enable fixed assets proces	Action class settings view	AccountantElectronicAddressNe...
		Accounts payable positive	Enable Intrastat proces	Action populate records tas	AccountantElectronicAddressNe...

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

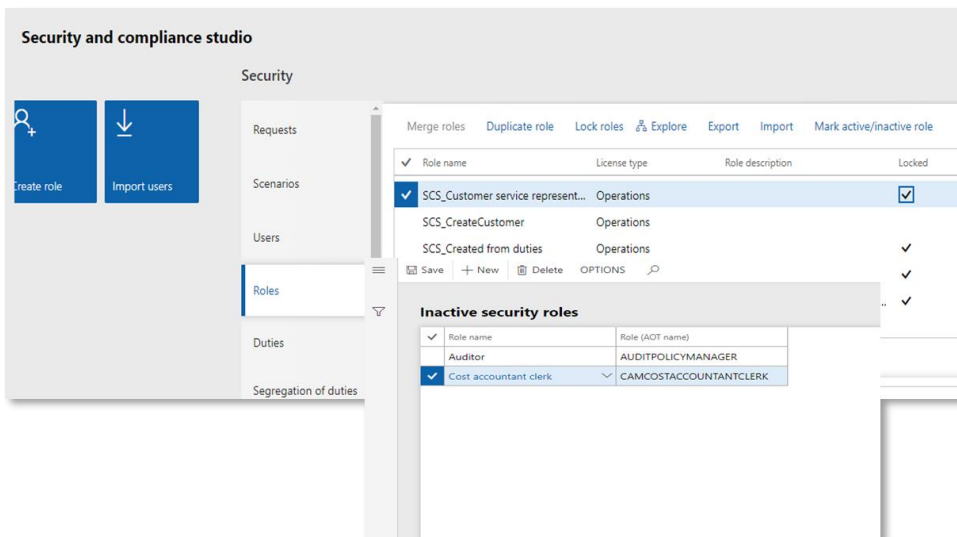
3.3 Merge security scenarios and match role

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.



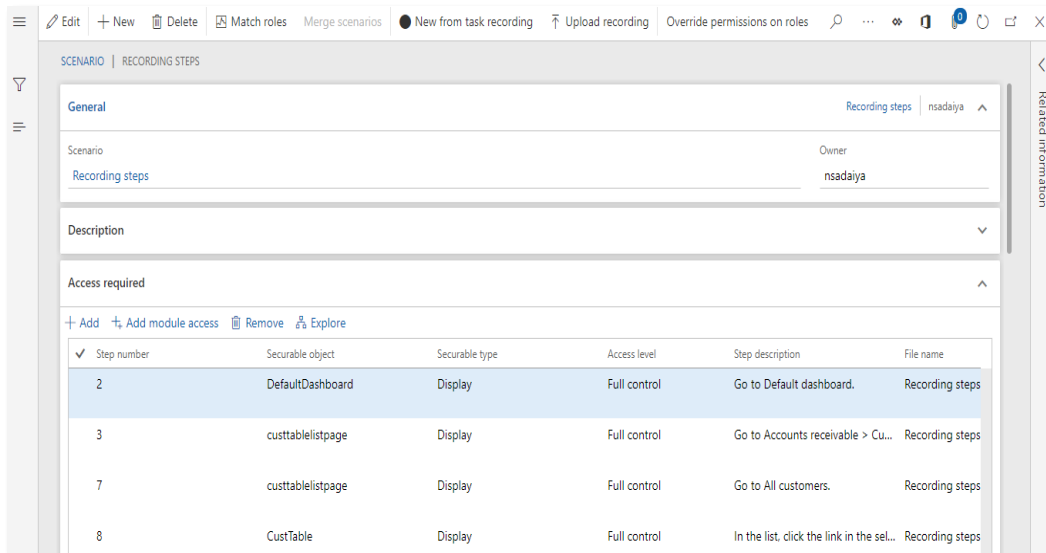
3.4 Mark any Security Role as Active/Inactive

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.



3.5 Recording steps to scenario.

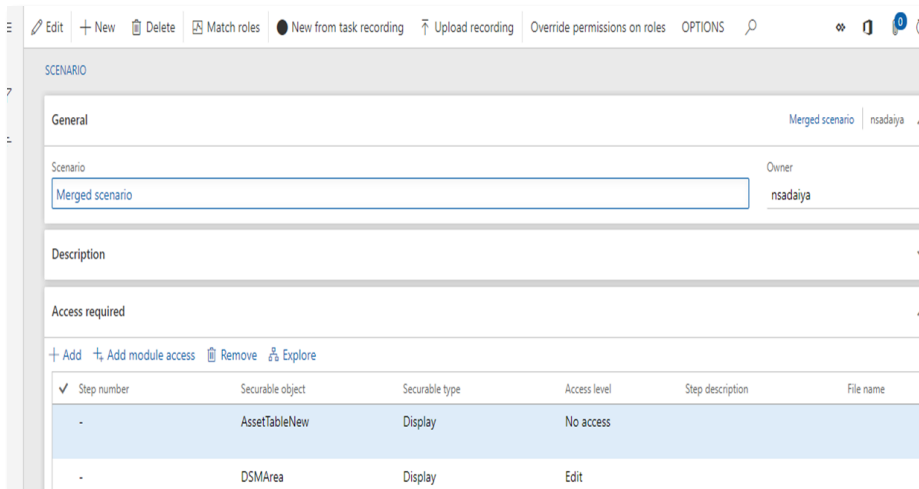
You can now record Business process steps along with entry points while creating a security scenario for more information.

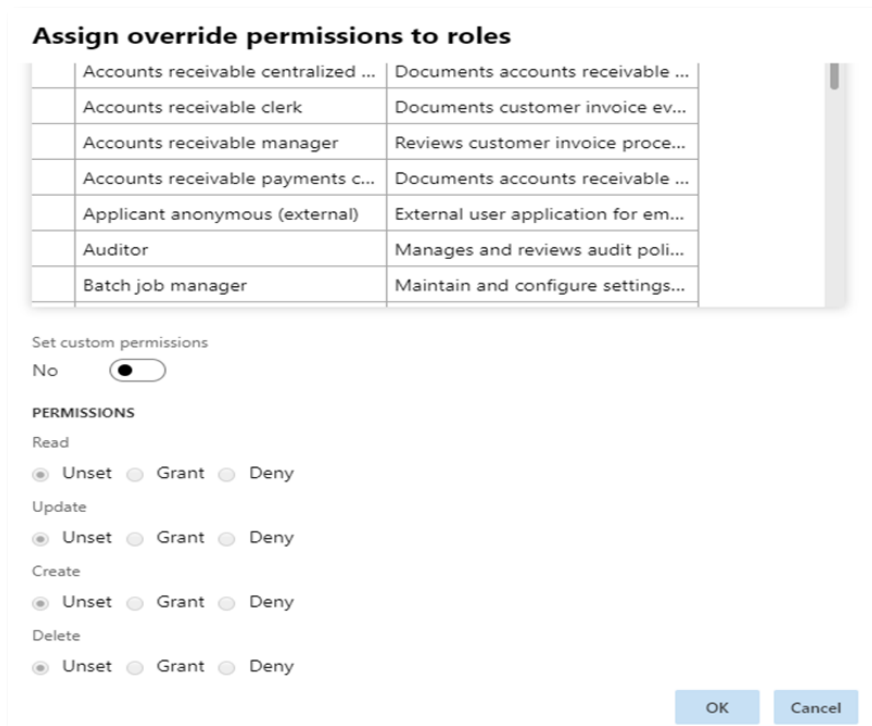


Useful in optimizing the license cost while creating a new security role. If an entry point is increasing the license cost, recorded steps will help to decide whether access is required or not.

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.





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**

Date and time	Event created by	Event type	Company	Description
10/19/2019 06:34:33 AM	atayyala	Duty undone sensitive data access	*	Duty 'Import ZIP/postal codes' a...
10/19/2019 06:33:40 AM	atayyala	Duty given sensitive data access	*	Duty 'AT_007 (display)' is given ...
10/19/2019 06:15:51 AM	atayyala	Duty undone sensitive data access	*	Duty 'AT_007 (display)' access to...
10/19/2019 05:54:21 AM	atayyala	Role given sensitive data access	*	Role 'AT_007' is given access to ...
10/19/2019 05:14:22 AM	atayyala	Role undone sensitive data access	*	Role 'AT_007' access to sensitive...
10/19/2019 11:35:12 AM	naadaya	Endpoint given sensitive data access	*	Endpoint 'AbatementCertificat...
10/19/2019 11:34:40 AM	naadaya	Endpoint given sensitive data access	*	Endpoint 'AccountingDistCust...
10/19/2019 11:34:19 AM	naadaya	Endpoint given sensitive data access	*	Endpoint 'AccountingDistBank...
10/19/2019 11:09:40 AM	naadaya	Role undone sensitive data access	*	Role 'Accounting supervisor' acc...

Sensitive data access reasons form

It will load Default data for sensitive reason.

Sensitive data access reason

You can specify sensitive data reason type as sensitive or highly sensitive.

Reason	Type
Address: hereunder residential	Sensitive
Area of work	Sensitive
Benefits	Sensitive
Biometric data	Highly sensitive

- **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.

Security explorer: full view

USERS: SCOBA, Admin, ALICIA, APRIL, ARNIE, atayyala, axrunner, BENJAMIN, BRAD, BROOKE

ROLES: Accounts payable, Accounts receivable, Applicant anonym, AT_007

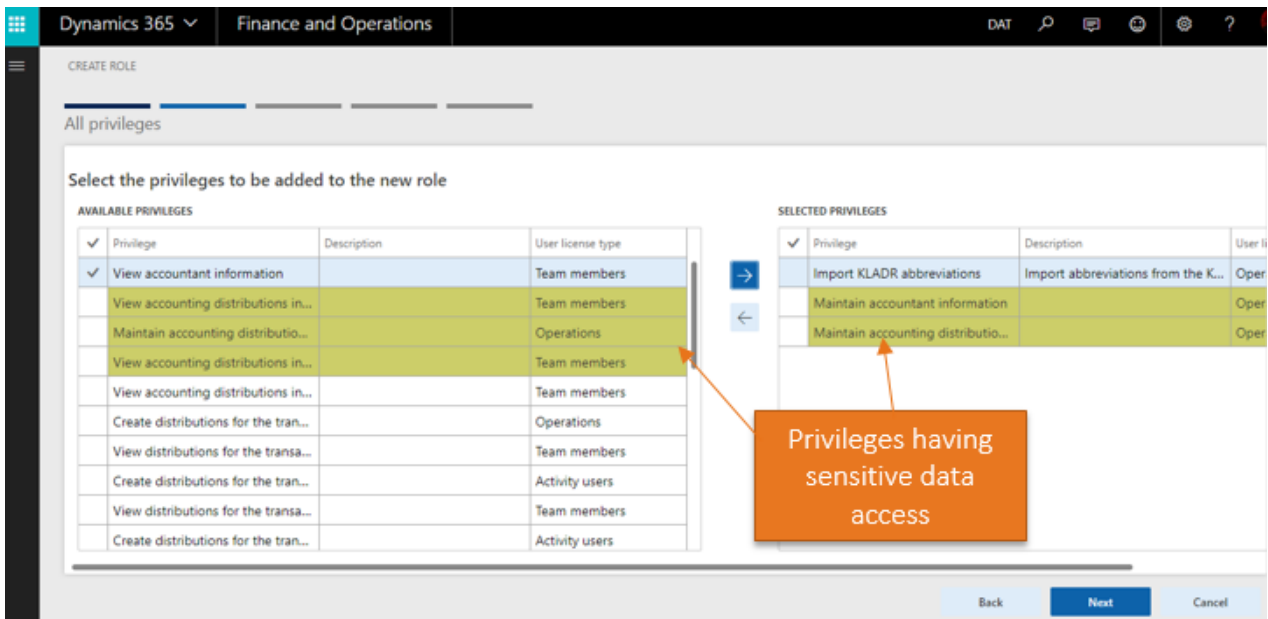
DUTIES: A parameter that is used to gro..., Access benefits workspace, Access expense management w..., Access workforce management ..., Activate tax depreciation process, Activate, deactivate, update and..., Add an existing performance jo..., Add custom fields, Application document entities, Approve absences

PRIVILEGES: A param, Accept, Access, Access c, Access e, Access r, Access v, Account, account

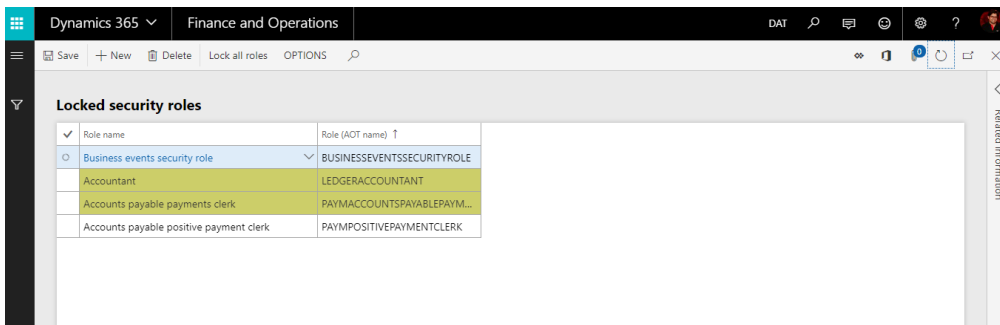
ENTRY POINTS: Abaten, Abaten, Abaten, Abbrev, Accour, Accour, Accour, Accour, Accour

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

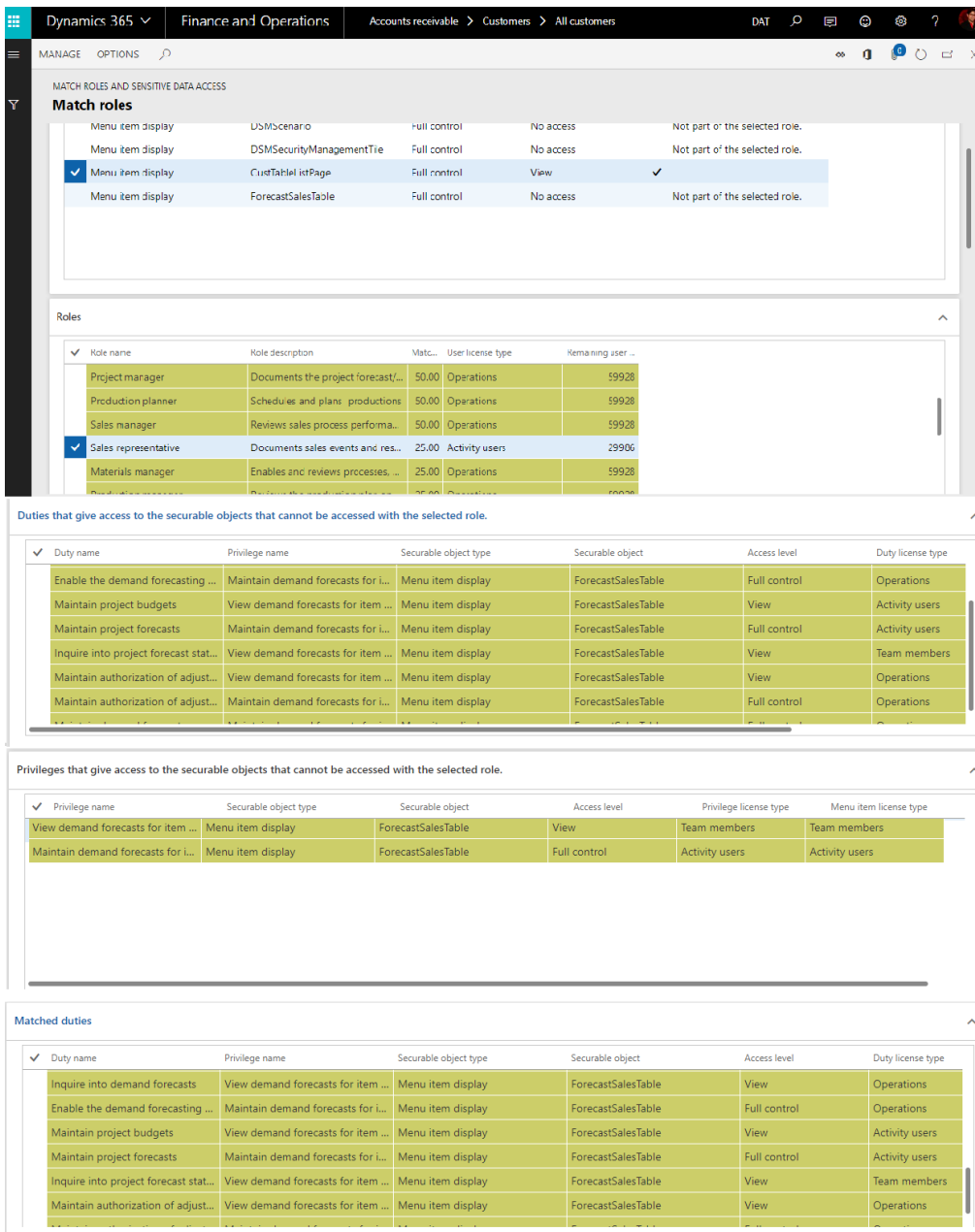
- **Undo access to sensitive data** - You can unset sensitive data access to a securable object. If you unset sensitive data access to a securable object, then automatically all securable objects which are related to it lose access to sensitive data.
- **Sensitive data access inheritance**- Please refer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



- 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.

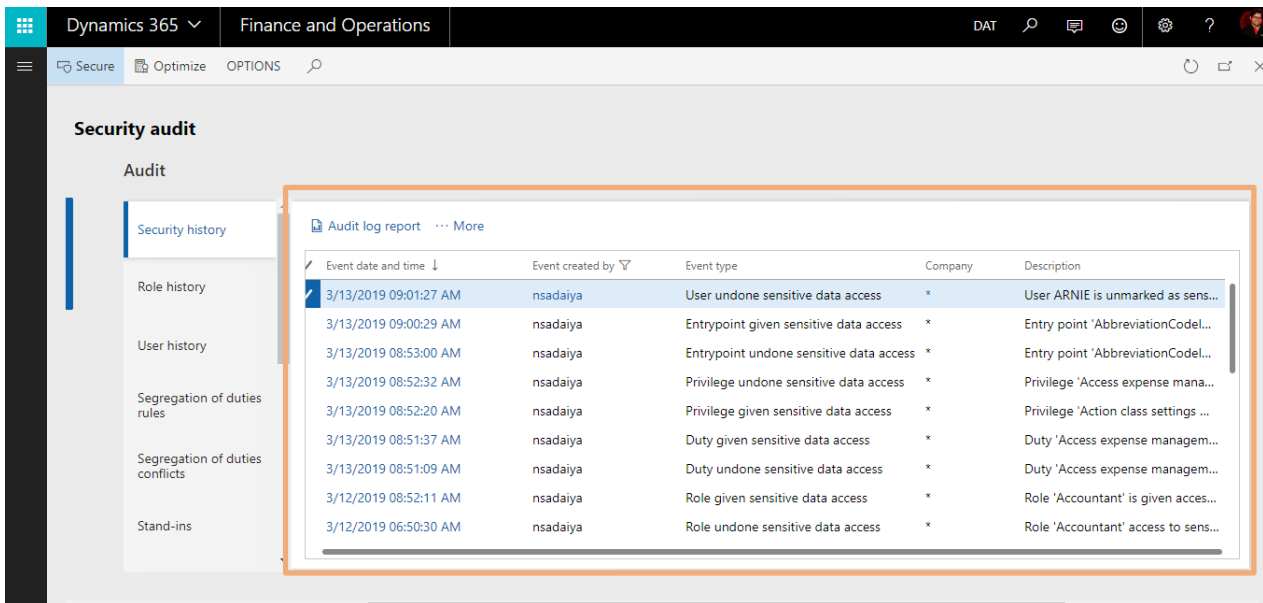


- Audit log enhancements to capture all changes to security objects providing sensitive data access

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.

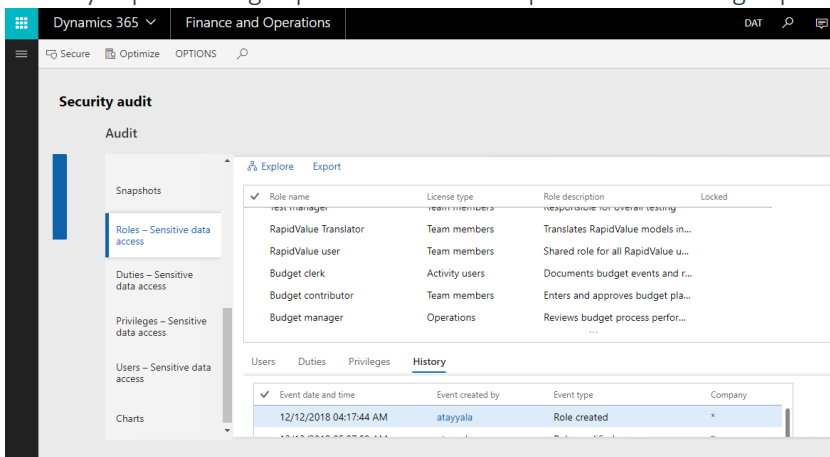
Event types are as mentioned below:

- 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.



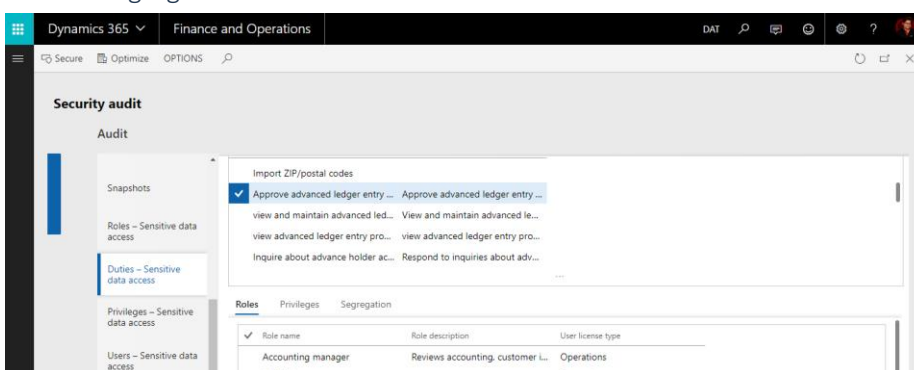
- Sensitive data access forms
 - Roles - Sensitive data access

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



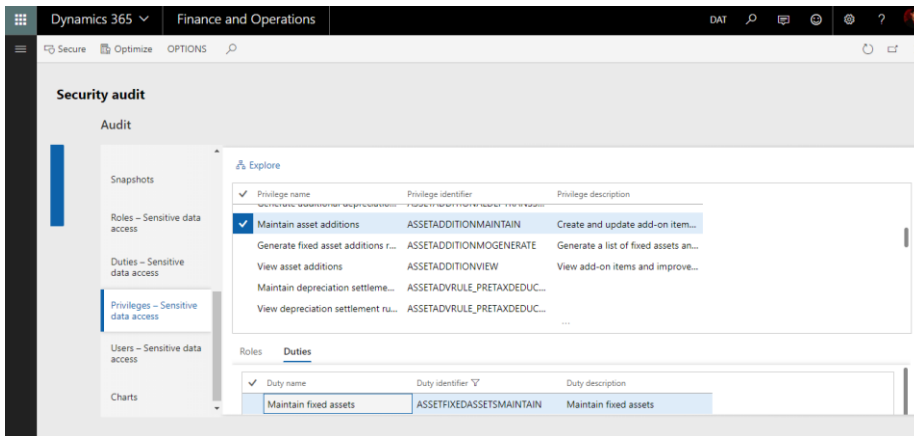
- Duties - Sensitive data access

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.



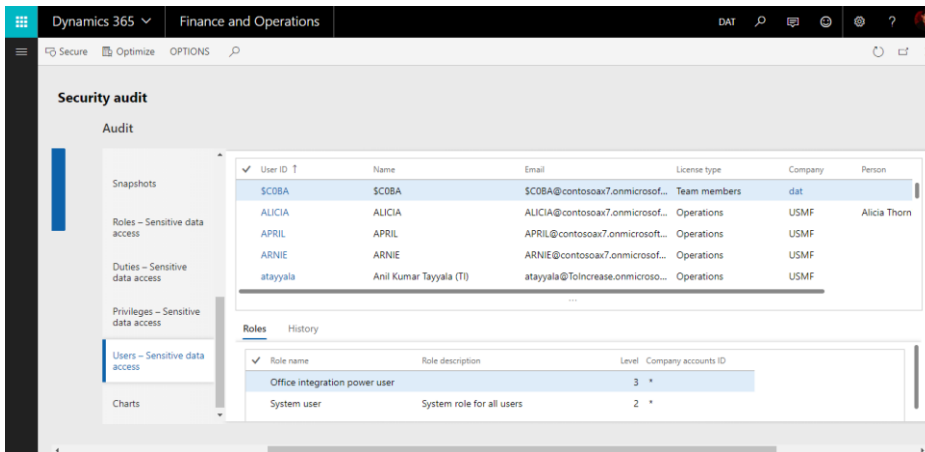
- Privileges - Sensitive data access

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.



- 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 use history which contained changed events of the user.



- Charts

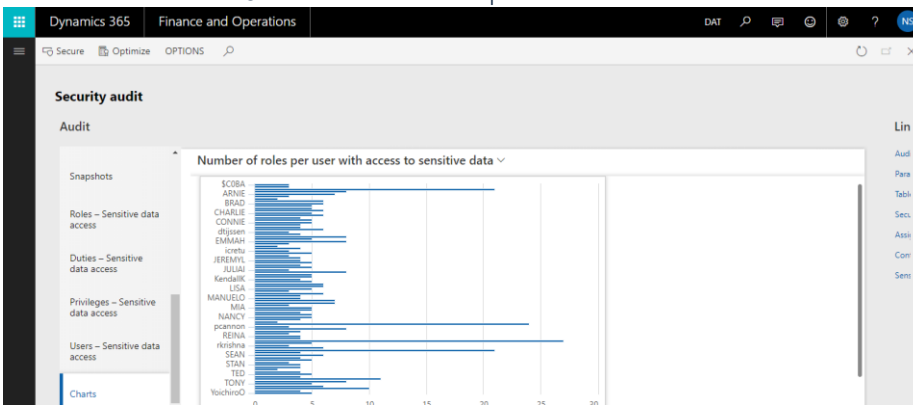
- Number of security objects with access to sensitive data



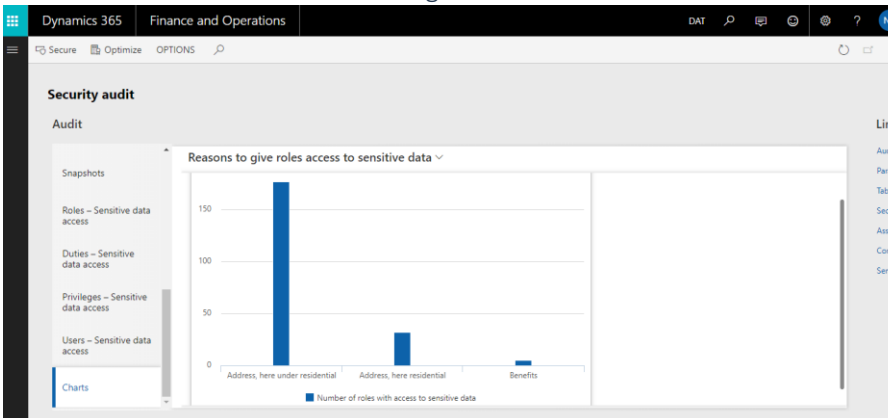
- Number of users with access to sensitive data per organization



o Number of roles per user with access to sensitive data

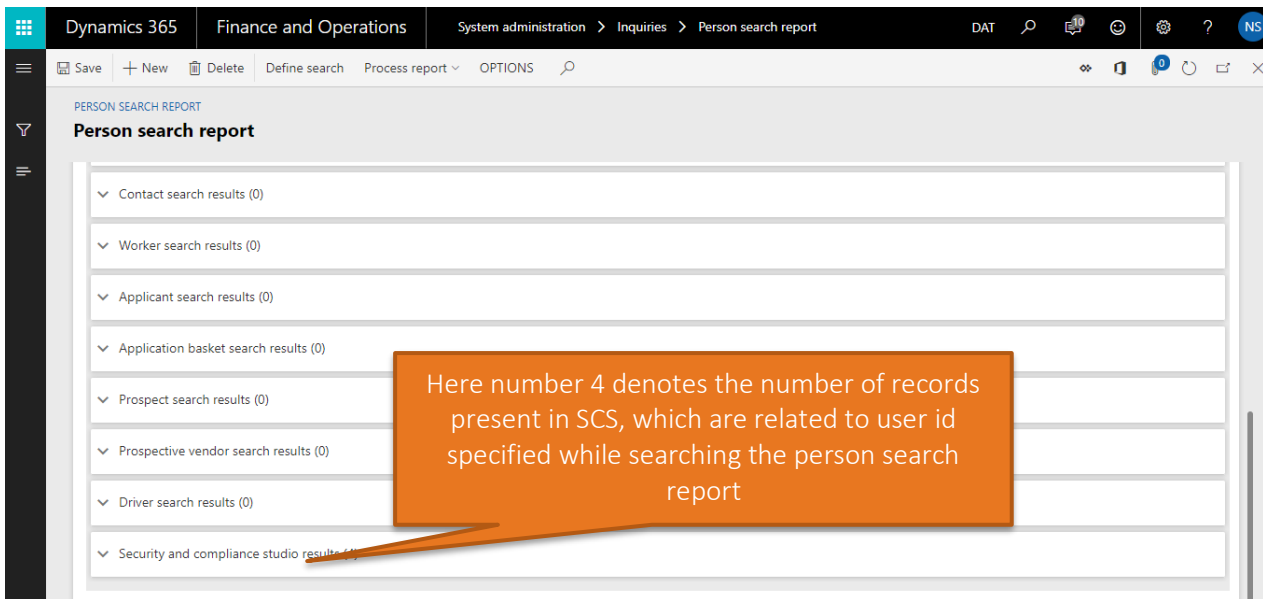


o Reasons to give roles access to sensitive data



- Person search report extension

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



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.

^ Security and compliance studio results (4)

SECURITY REQUESTS						
Include	Owner	Request	Description	Type	Status	
<input checked="" type="checkbox"/>	nsadaiya	Add accountant role		General	Open	

STAND-IN							
Include	Stand-in	User ID	From date	To date	Copy assigned organizations	Closed	
<input checked="" type="checkbox"/>	ALICIA	nsadaiya	3/14/2019	3/30/2019	true	No	

SCENARIOS				
Include	Scenario	Description	Owner	Created date and time
<input checked="" type="checkbox"/>	Match roles and sensitive data a...		nsadaiya	3/12/2019 05:53:05 AM

TABLE SECURITY RECORDINGS					
Include	Owner	Name	Description	Created date and time	
<input checked="" type="checkbox"/>	nsadaiya	Customer table recording		3/14/2019 11:51:19 AM	

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

Enter the new duty name and the description.

Create duty

Parameters

Duty name <input type="text" value="SCS"/>	Description <input type="text"/>
---	-------------------------------------

Security objects that are included into the new duty

<input type="text" value="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.

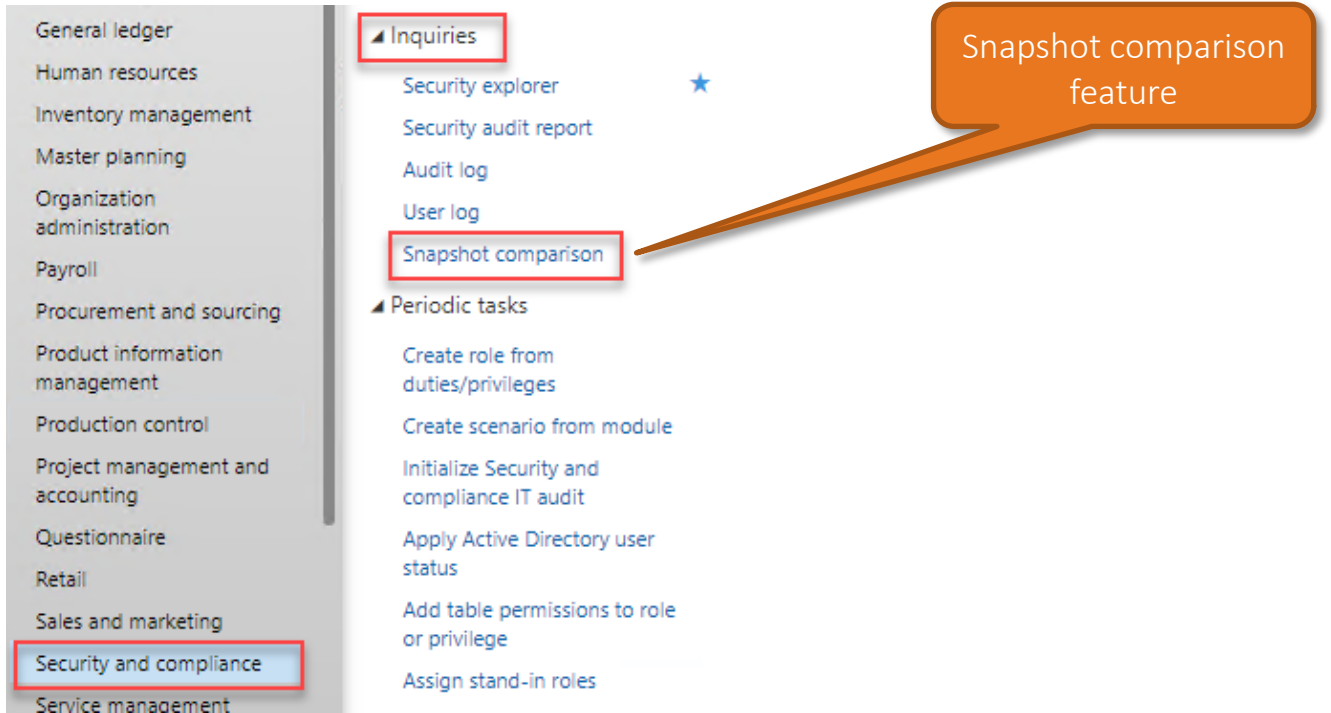


Fig 1. Snapshot comparison path

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

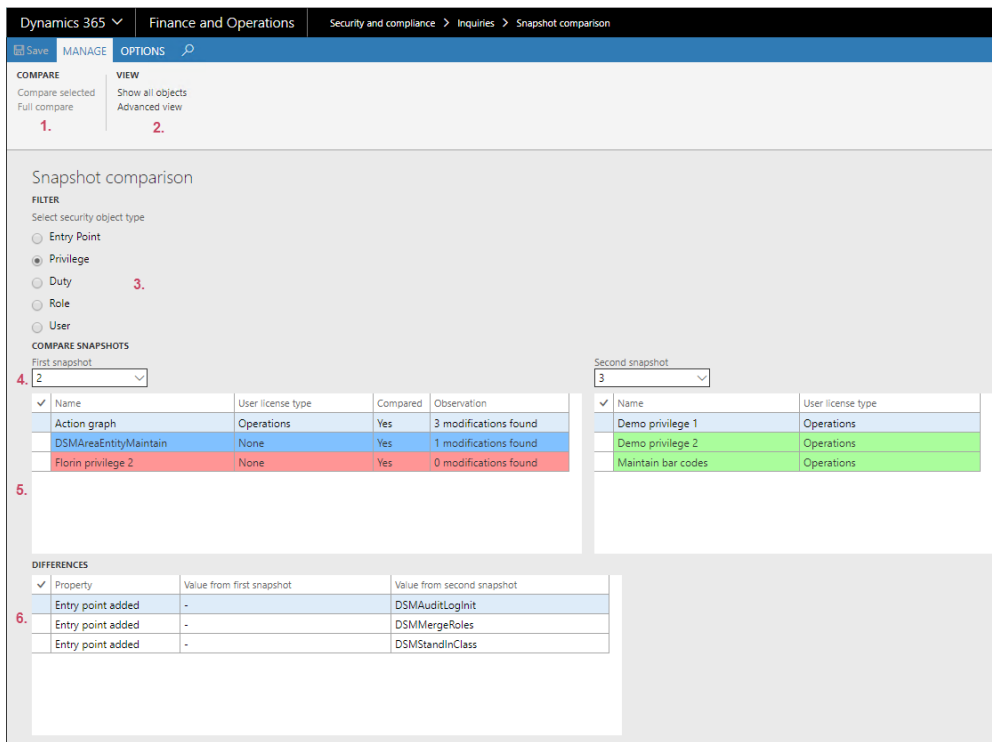


Fig 2. Snapshot comparison form

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)

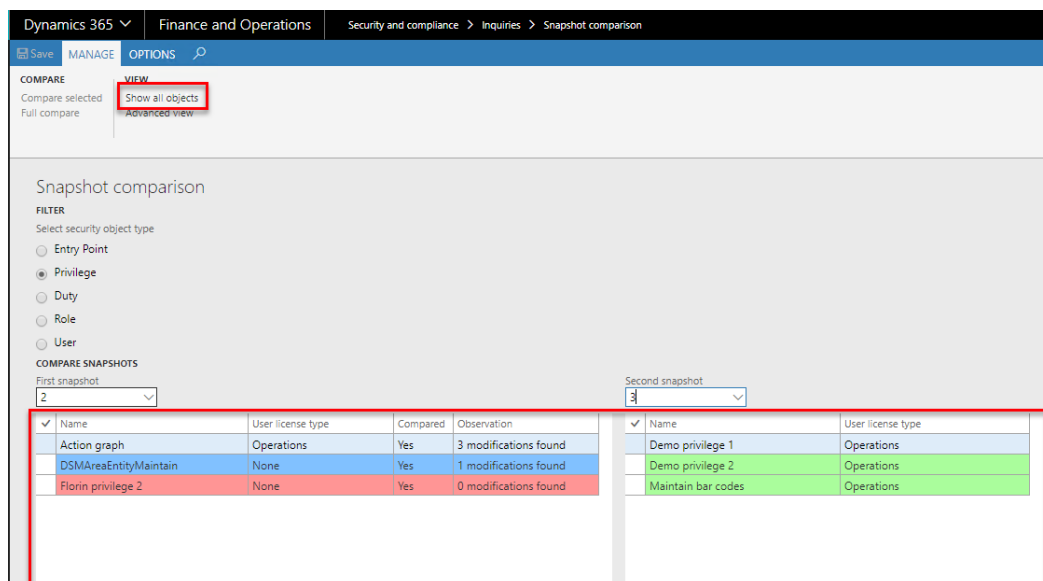


Fig. 3 See a list of the modified objects

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)

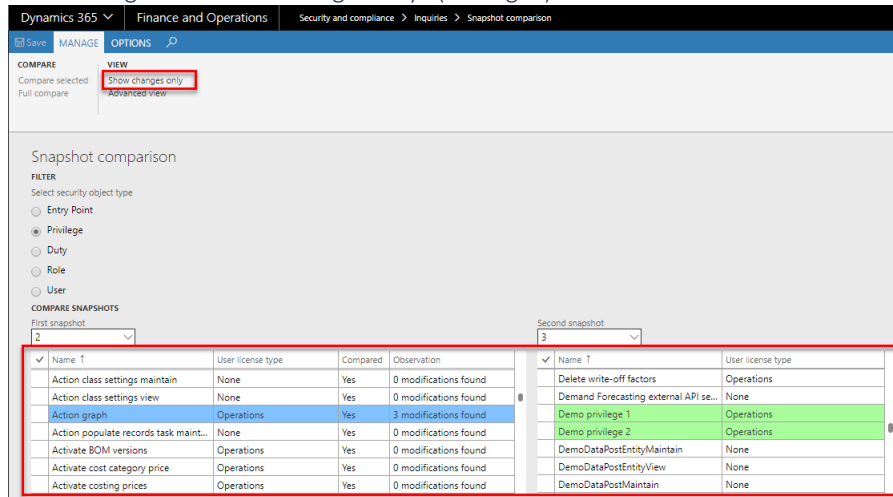


Fig 4. See a list of all objects from selected snapshots

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)

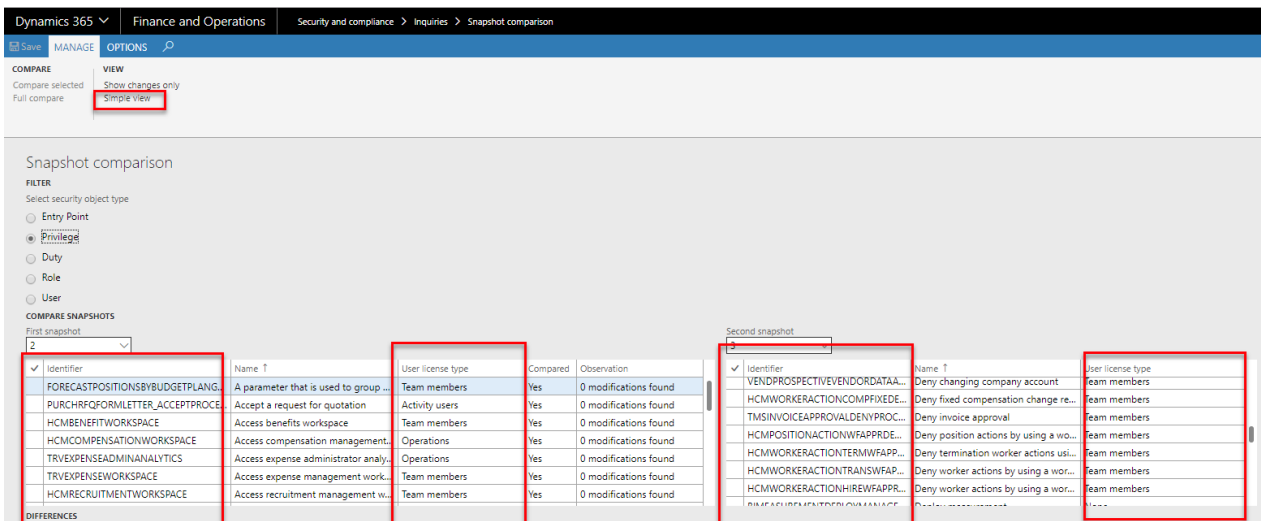


Fig 5. Advanced view

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)

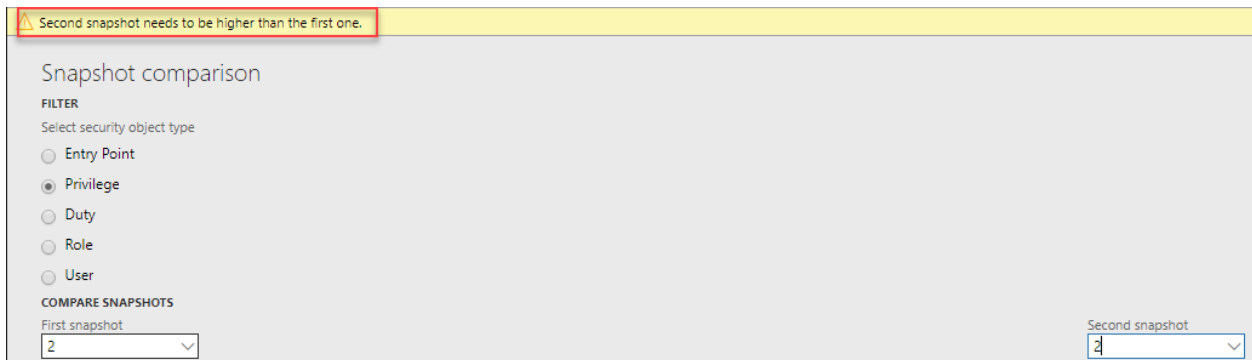


Fig. 6 snapshot selection restriction

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:

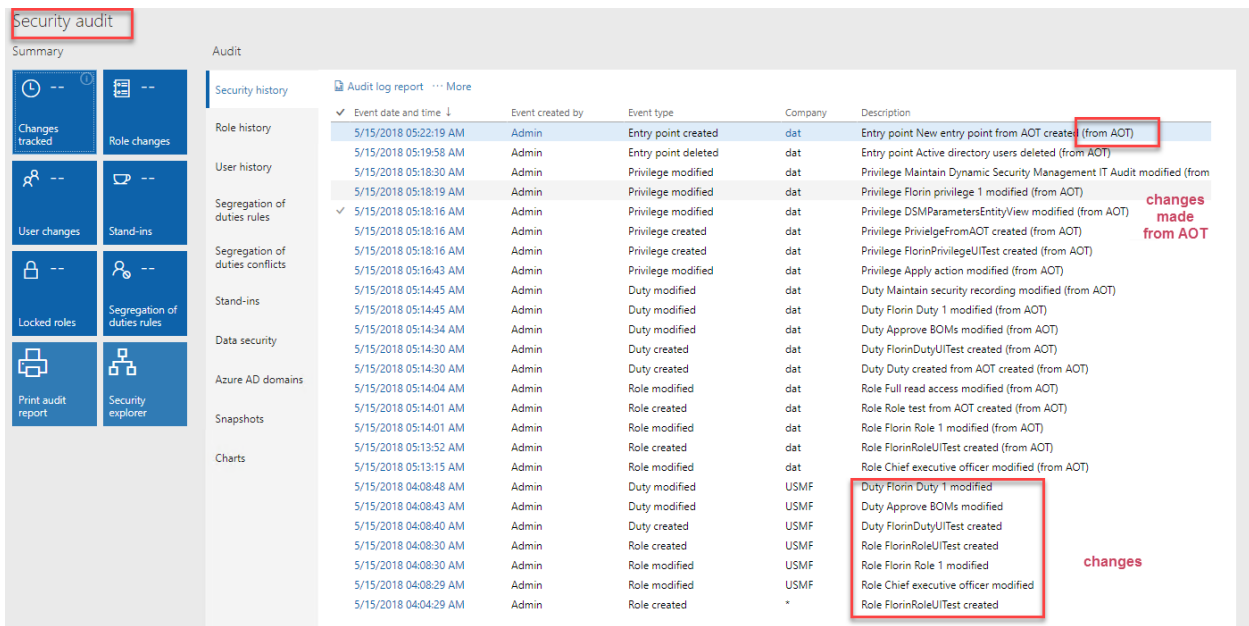
Property	Value from first snapshot	Value from second snapshot
Duty added	-	View sales

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.



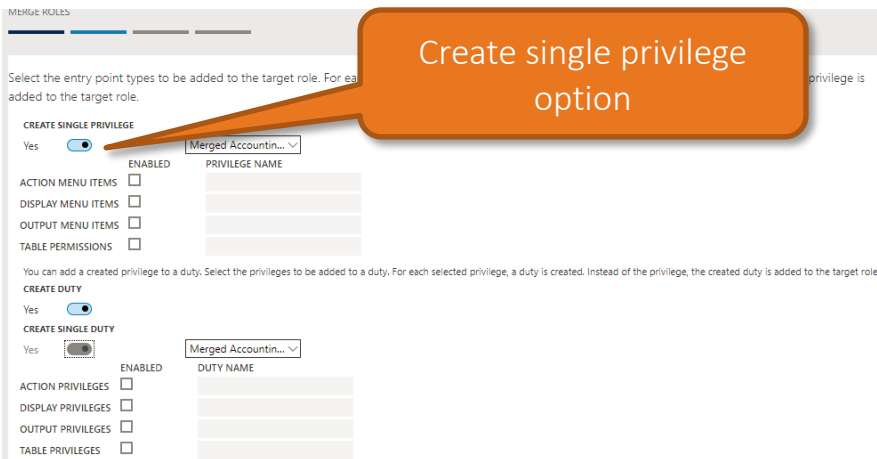
New Events types that will be used to track changes done directly to permissions from Development environment:

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).

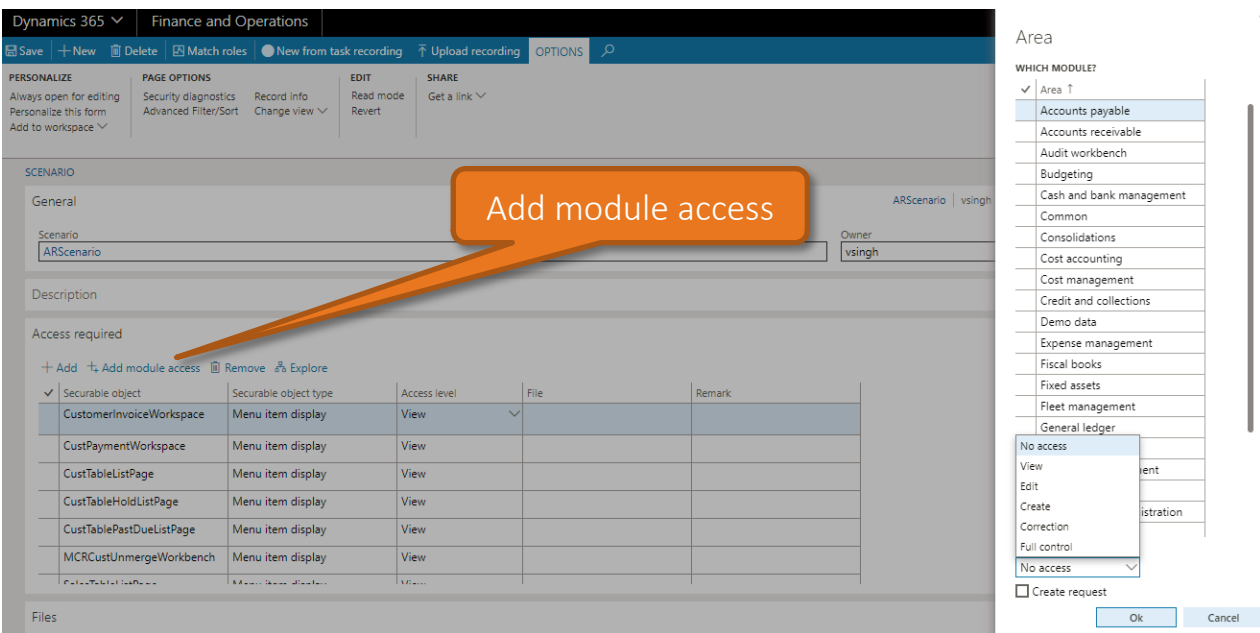
3.12 Option to create one or more privileges and also one or more duties while merging roles.

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.



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.



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.

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

ARSCENARIO
Match roles

Securable objects

Securable object type	Securable object	Required access	Maximum access on role	...	Remark
Menu item display	CustomerInvoiceWorkspace	View	View		✓
Menu item display	CustPaymentWorkspace	View	View		✓
Menu item display		View	Full control		✓
Menu item display		View	View		✓
Menu item display	MRCustUnm...	View	No access		Not part of the selected role.
Menu item display	SalesTableListPage	View	View		✓

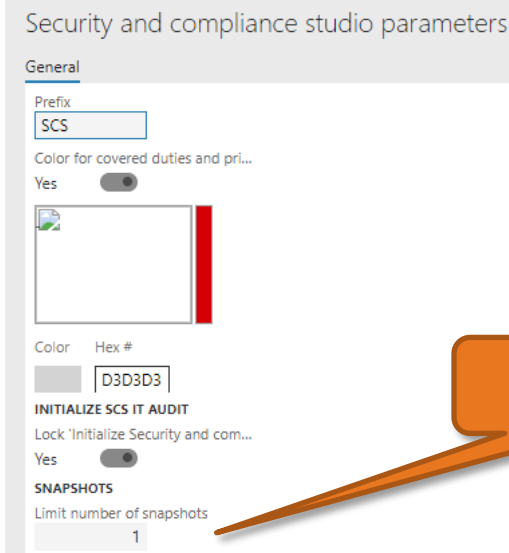
Security roles match degree

Roles

Role name	Role description	Match degree ↑	User license type	Remaining user lice...
Accounts receivable manager	Reviews customer invoice pro...	72.81	Operations	59933
Accounting manager	Reviews accounting, custome...	68.66	Operations	59933
Accounts receivable clerk	Documents customer invoice ...	68.66	Operations	59933
Accountant	Documents accounting event...	60.37	Operations	59933
Accounting supervisor	Reviews accounting process p...	57.14	Operations	59933
Collections manager	Reviews collections process p...	53.92	Operations	59933
Accounts receivable payments cle...	Documents accounts receivab...	50.23	Operations	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 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.

Version	Name	Description	Created by	Created date and time	Protected
1	Generated from batch, version 1 on 2/13/2018 03:55:37 am	Automatically create from batch job on 2/13/2018	Admin	2/13/2018 03:55:37 AM	<input checked="" type="checkbox"/>
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	<input type="checkbox"/>
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	<input type="checkbox"/>
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	<input type="checkbox"/>

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

- "-1" (negative one) value will used to store unlimited number of snapshots. This will also pop-up two warnings to inform the user.
- "0" (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.

CREATE ROLE
All duties

Select duties to be added to the new role

AVAILABLE DUTIES			SELECTED DUTIES		
✓ Duty	Description	User license type	✓ Duty	Description	User license type
<input checked="" type="checkbox"/> Maintain Absorption Costs		Operations	<input checked="" type="checkbox"/> Inquire into Absorption Costs		Team members
<input type="checkbox"/> Import ZIP/postal codes		Operations	<input checked="" type="checkbox"/> Inquire into purchase agreem...	Respond to inquiries about p...	Team members
<input type="checkbox"/> Approve advanced ledger ent...	Approve advanced ledger ent...	Operations			
<input type="checkbox"/> view and maintain advanced l...	View and maintain advanced l...	Team members			
<input type="checkbox"/> view advanced ledger entry p...	view advanced ledger entry p...	Team members			

CREATE ROLE
Summary

Review the selected role setup. Click Finish to create the role.
The resulting role will have the user license type **Operations**

Role name: SCS_NewRole | Role description: SCS_NewRole

Privilege name	Description	License type
Import KLADR abbreviations	Import abbreviations from th...	Operations
View accounting distributions...		Team Members

Duty name	Description	License type
Inquire into Absorption Costs		Team Members
Inquire into purchase agreem...	Respond to inquiries about p...	Team Members

Role license type before you finish

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.

Security diagnostics

This is the list of security objects that grant the active security entry point.

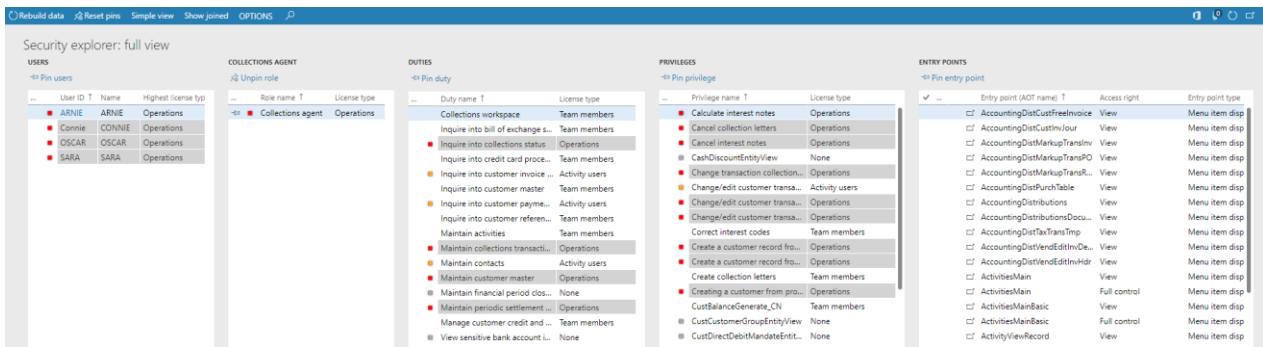
[Add roles to user](#) [Show object identifiers](#) [Explore](#)

Filter

✓ Object type	Label
Role	SCSCollections agent
Role	Auditor
<input checked="" type="checkbox"/> Role	Collections agent
Role	Collections manager
Role	Chief executive officer

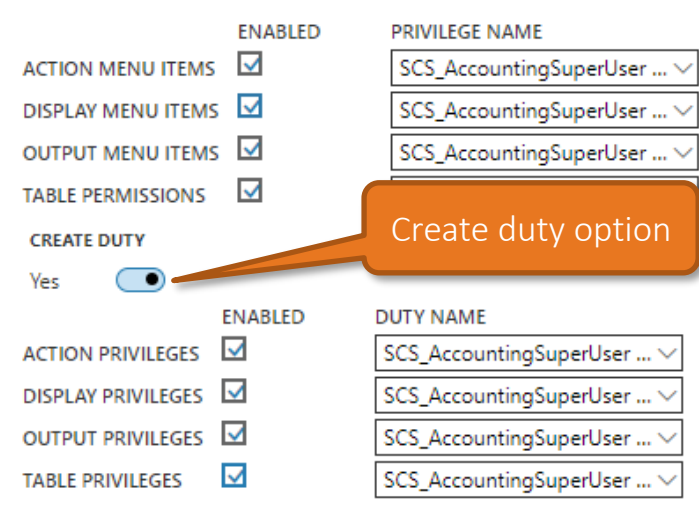
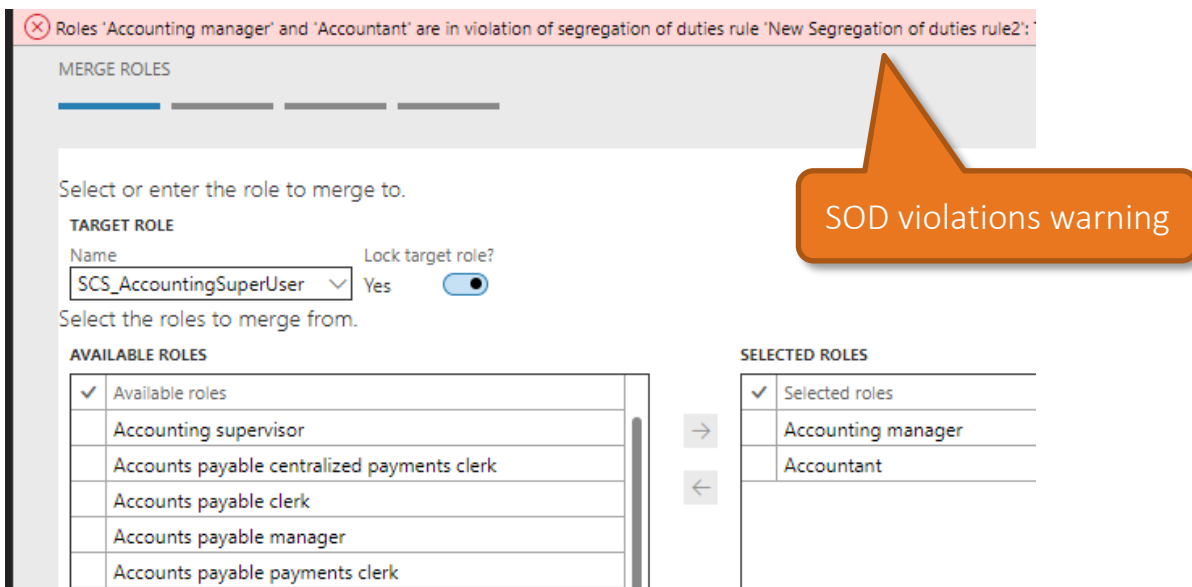
Security explorer icon on all D365FOE forms

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



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

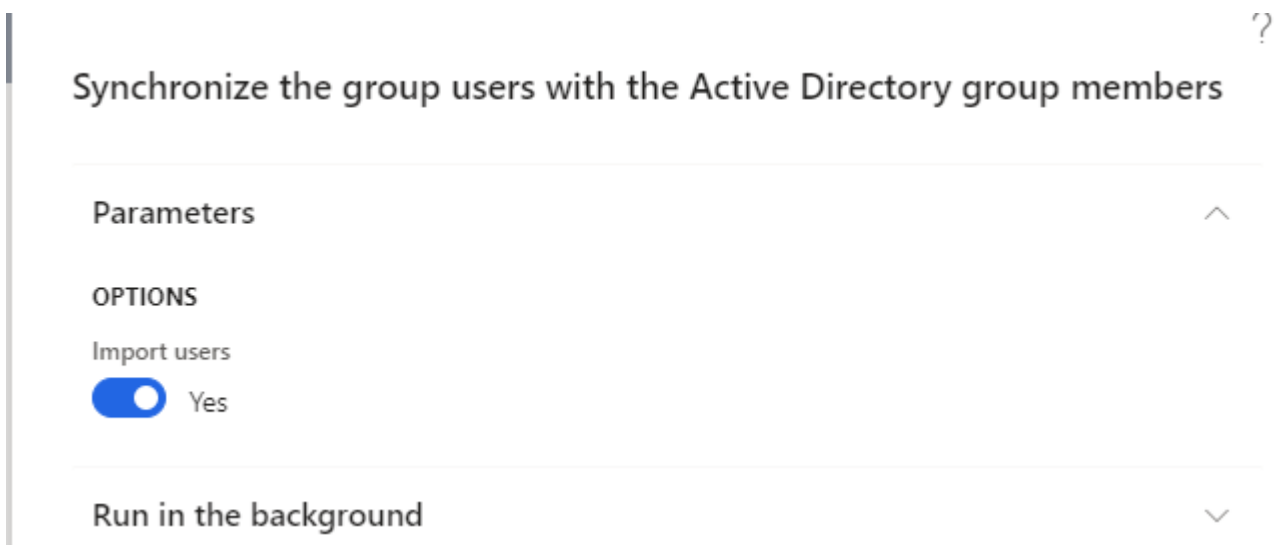
You now have an option to create duties along with the privileges while using the “Merge roles” feature. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.).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



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.

Modeling

Overview

Business strategy

Business processes

Activities

Roles

Organizations

People

Applications

References

Statistics

My tasks

My feedback

Charts

Edit Hierarchy Design LCS Publish DevOps Browse Get link

Hierarchy

- Process specification
- Scope statement
- Process verification
- Gap analysis
- 1.2 Services Master data
 - 1.2.1 Create Bom
 - 1.2.1.2 Create Formula
 - VS3.2.5 Create Formula Scenario
 - Define Co or By Products Scenario
 - 1.2.1.3 Create Route
 - 1.2.1.4 Product Change Case
 - 1.2.1.5 Process a case
 - 1.2.1.6 Create Production Resources
 - 1.2.2 Manage Item Data
- 1.3 Sell Products
- 1.4 Manage Projects
- 1.5 Material and Resource Planning
- 1.6 Purchase Products and Services
- 1.7 Production Control
- 1.8 Manage Quality
- 1.9 Manage Warehousing and Logistics
- 1.10 Service Management
- 2.0 Finance and Supporting Processes
- 10.0 Retail - Operating Processes
- 20.0 Retail - Finance and Supporting Processes

1.0 Operating processes > 1.2 Manage Product and Services Master data > 1.2.1.2 Create Formula

1.2.1.2 Create Formula

The Production Manager defines an item's Formula consisting of formula lines that identify the components to produce the item. Each Formula line minimally identifies a component, a required quantity, and the warehouse source of the component. The Production Manager approves and activates the item's Formula version after completing definition.

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

Business process designer

Hierarchy List

Define Co/By Products Scenario

+ New Delete Filter Up Down Tools Details Strategy Flow Activities Procedure Preview

- Columbus Solution
 - 1.0 Operating processes
 - 1.1 Sales and Marketing
 - 1.1.1 Marketing
 - 1.1.2 Sales and Marketing reports
 - 1.2 Manage Product & Services Master data
 - 1.2.1 Manage Engineering
 - 1.2.1.1 Create Bom
 - 1.2.1.2 Create Formula
 - Create Formula Scenario
 - Define Co/By Products Scenario
 - 1.2.1.3 Create Route
 - 1.2.1.4 Product Change Case
 - 1.2.1.5 Process a case
 - 1.2.1.6 Create Production Resources
 - 1.2.2 Manage Item Data
 - 1.3 Sell Products
 - 1.4 Manage Projects
 - 1.5 Material and Resource Planning

Define Co/By Products Scenario

The Production Manager defines an item's Formula consisting of formula lines that identify the components to produce the item. An item may require multiple Formula versions to reflect planned changes in the Formula, variations between sites producing the same item, or alternate Formulas. Each Formula line minimally identifies a component, a required quantity, and the warehouse source of the component. The production manager approves and activates the item's Formula version after completing definition.

Scenario 2 - Define Co/By Products

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.

[Unlink sub activities](#)

✓		Step	Exists in flow	Sub activity	Title
	1.1	Go to Product information man...	<input type="checkbox"/>	Select item for Formula	
	1.2	In the list, find and select the de...	<input type="checkbox"/>	Select item for Formula	
	2.1	Click Formula versions.	<input type="checkbox"/>	Define Co-Products in version	
	2.2	On the Action Pane, click Formu...	<input type="checkbox"/>	Define Co-Products in version	
	2.3	Click Co-products.	<input type="checkbox"/>	Define Co-Products in version	
	2.4	Click New.	<input type="checkbox"/>	Define Co-Products in version	
	2.5	In the list, mark the selected row.	<input type="checkbox"/>	Define Co-Products in version	
	2.6	In the Item number field, enter ...	<input type="checkbox"/>	Define Co-Products in version	
	2.7	In the Production type field, sele...	<input type="checkbox"/>	Define Co-Products in version	
	2.8	In the Warehouse field, type a v...	<input type="checkbox"/>	Define Co-Products in version	
	2.9	In the Quantity field, enter a nu...	<input type="checkbox"/>	Define Co-Products in version	
	2.10	In the By-product cost allocatio...	<input type="checkbox"/>	Define Co-Products in version	
	2.11	Click Save.	<input type="checkbox"/>	Define Co-Products in version	
	2.12	Click New.	<input type="checkbox"/>	Define Co-Products in version	
	2.13	In the list, mark the selected row.	<input type="checkbox"/>	Define Co-Products in version	
	2.14	In the Item number field, enter ...	<input type="checkbox"/>	Define Co-Products in version	
	2.15	In the Quantity field, enter a nu...	<input type="checkbox"/>	Define Co-Products in version	
	2.16	In the Co-product cost allocatio...	<input type="checkbox"/>	Define Co-Products in version	

Flow activities Activities

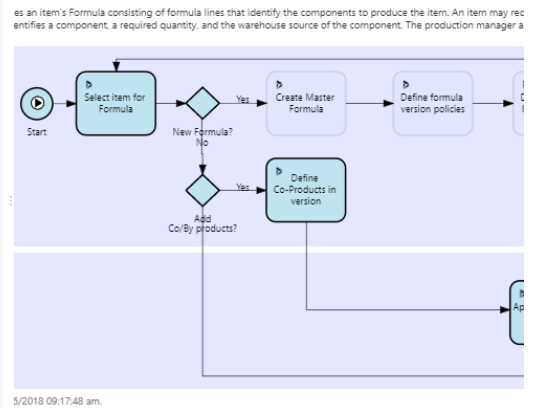


Figure: Scenario-Procedure activity based modeling with recorded steps linked to flow activities

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

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	First securable object type	First access level	Second
Demo rule for Entry points	Entry point	AccountingDistVendEditInvHdr	Menu item display	Create	AdvancedLedgerEntryDateDr...
Match role test - ep 1	Entry point	AuditPolicyCaseGroup	Menu item display	Full control	ACJournalPost_BR
Match roles test - duty	Duty	Maintain Absorption Costs		No access	Maintain audit policies
Match roles test - duty 2	Duty	Maintain audit policies		No access	Maintain Absorption Costs
Match roles test - ep 2	Entry point	ACJournalPost_BR	Menu item action	Full control	AuditPolicyCaseGroup
Match roles test - ep 3	Entry point	DSMSecurityRequestPriorityH...	Menu item action	Correction	ACJournalPost_BR
Match roles test - ep 4	Entry point	DSMMultiSelectRoleSetup	Menu item display	Full control	DSMSecurityRequestPriorityH...
Match roles test - priv 1	Privilege	Maintain case grouping criteria		No access	Maintain Absorption Costs
Match roles test - priv 2	Privilege	Maintain Absorption Costs		No access	Maintain case grouping criteria

Risk ID	Category	Status	Inherit risk	Response	Residual risk	Owner
Risk-000000006	Operational	Initial	Medium	Accept	Low	Admin
Risk-000000007	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

+
Create a risk

4
Risk

124
Enhanced SoD rules

0
Enhanced SoD conflicts

Risk

Risk register

Enhanced SoD rules

Enhanced SoD conflicts

Charts

+ New Edit

Risk ID	Name	Category	Status	Inherit risk	Response	Residual risk	Owner
Risk-000000005	Risk related to Org Strategy	Strategic	Initial	High	Ignore	Very low	Admin
Risk-000000006	Risk related to Org Operations	Operational	Initial	Medium	Accept	Low	Admin
Risk-000000007	Risk related to Org Strategy and	Strategic	Initial	Very low	Ignore	Very low	Admin
Risk-000000008	Risk DEMO	Operational	Review	Medium	Mitigate	Low	Admin

Enhanced SoD rules

Name	Type	First	First securable object type	First access level	Second	Second securabl
SCS-093-Create sales order and reserv...	Duty	Maintain sales order		No access	Maintain on-hand inventory r...	
SCS-094-Create purchase order and r...	Duty	Maintain inventory registrati...		No access	Maintain purchase orders	

Risk


Risk register

Enhanced SoD rules

Enhanced SoD conflicts

Charts

Organization Risk



■ Initial
■ Accepted
■ Review
■ Monitor
■ Expire

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 permissions	
Type	Access right
Table	No access
Service operation	No access
Service operation	Full control
Menu item display	View
Table	View
Menu item display	Full control
DataEntity	View
DataEntity	Full control

3.24 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:

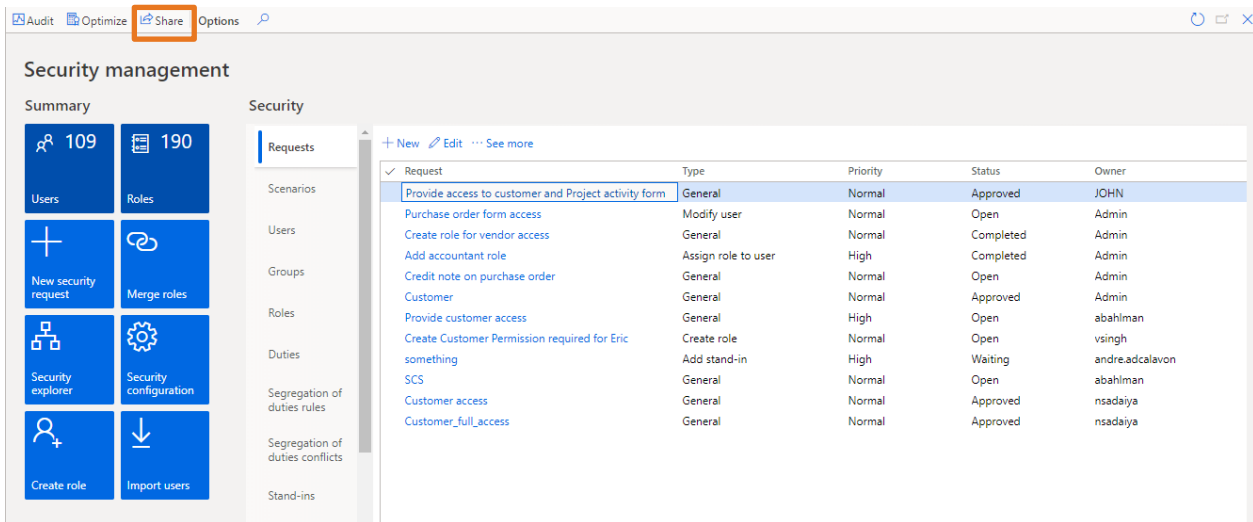
- Create snapshot,
- Security Explorer pinning,
- Match roles and
- Marking a record as sensitive.

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

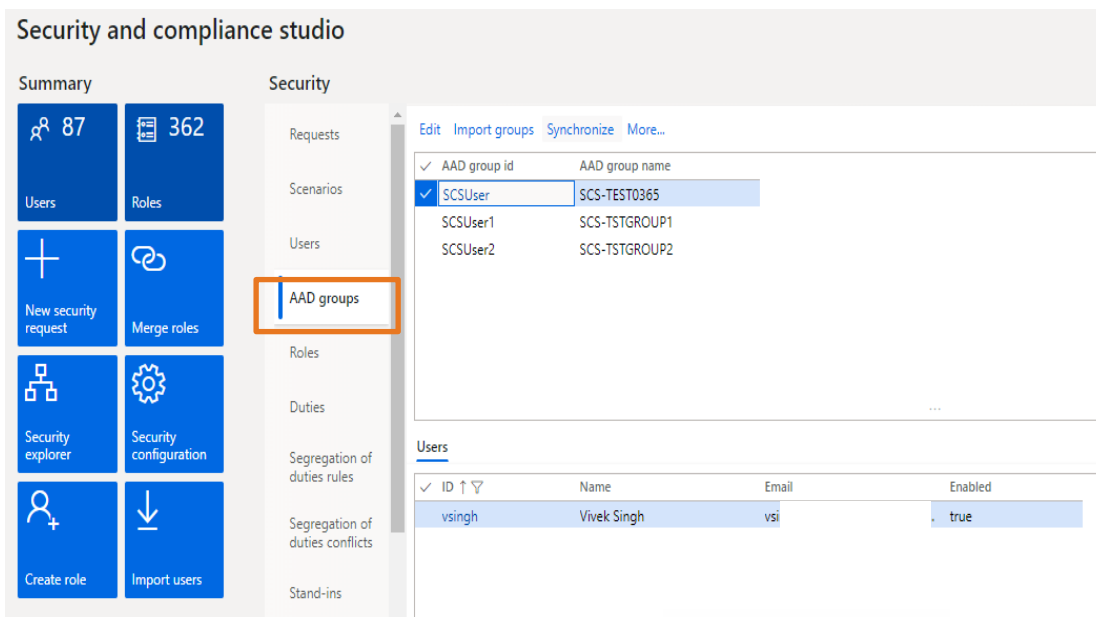


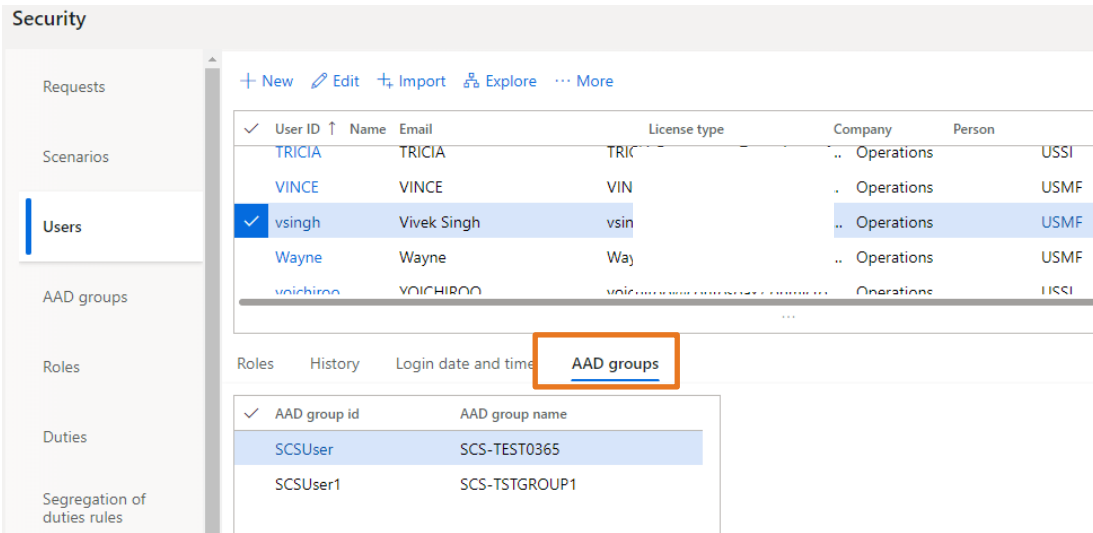
More details are mentioned in the “User and training manual”.

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.

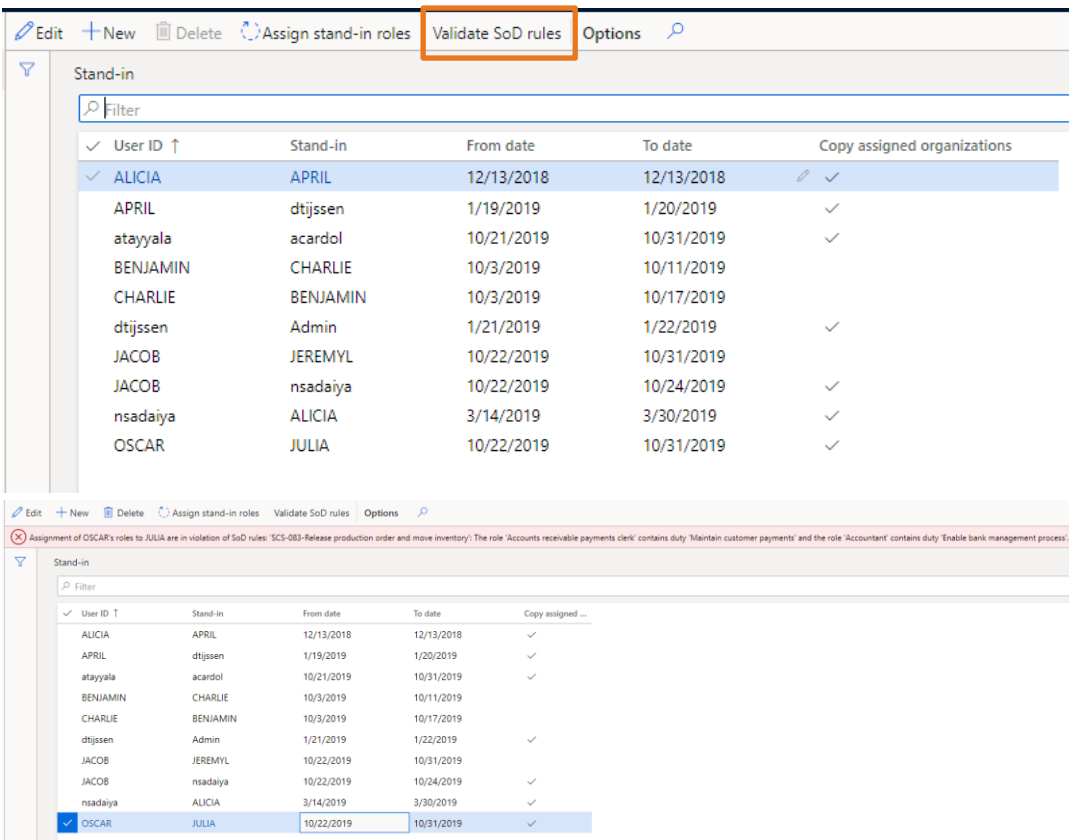
If a role is assigned to a group then all the users added in the group also get access to that role, SCS captures this important information in various SCS forms and in audit log.





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.



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 and compliance studio

Summary

- Users: 103
- Roles: 175
- New security request
- Merge roles
- Security explorer
- Security configuration
- Create role
- Import users

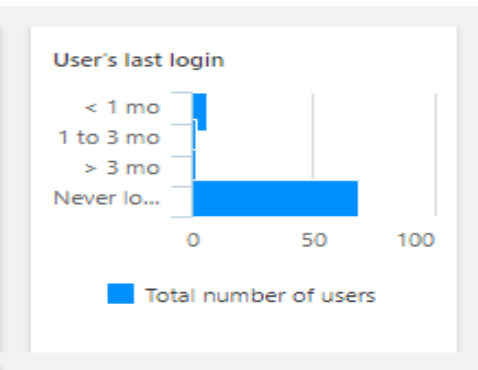
Security

- Requests
- Scenarios
- Users
- AAD groups
- Roles
- Duties
- Segregation of duties rules
- Segregation of duties conflicts
- Stand-ins
- Data security
- Snapshots
- History
- Charts

User ID	Name	Email	License type	Company	Person
abahlman	Ard Bahlman	ab	Operations	DAT	
acardol	Adri Cardol	ac	Activity users	DAT	
andre.adcalavon	André Arnaud de Calavon	an	.com	Operations	DAT
atayjala	Anil Kumar Teyjala (ATAYY.TI)	at		Team members	dat
dvschie	David van Schie (DVSC.H.TI)	dv		Operations	dat
evhofwegen	Éric van Hofwegen	evi	1	Operations	DAT
nsadaiya	Nitish Sadaiya (NSADA.TI)	ns		Operations	usmf
Pradeep Bapna	Pradeep Kumar Bapna	Pri	om	Operations	DAT
SCS-TSTGroup1	SCS-TSTGROUP1			Operations	DAT
SCS-TSTGroup2	SCS-TSTGROUP2			Operations	DAT
vsingh	Vivek Singh (VSING.TI)	vsi		Operations	dat

Login date and time

Last login date and time	Days since last login	onlineTime	Type
11/6/2019 07:48:42 AM	0	0:00:00	Logon



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.

Rebuild asset classification | Asset classification chart | Options

Asset classification

Tables

Table name	Table label	Table ID
Accountant_BR		6799
AccountantLogisticsLocation_...		1315
AccountantLogisticsLocationR...		6664
AccountingDistribTmpOrderLi...		4548
AccountingDistributionEventT...		6373
AccountingDistributionTmp		97
AccountingDistributionTmpA...		2882

Asset classification info

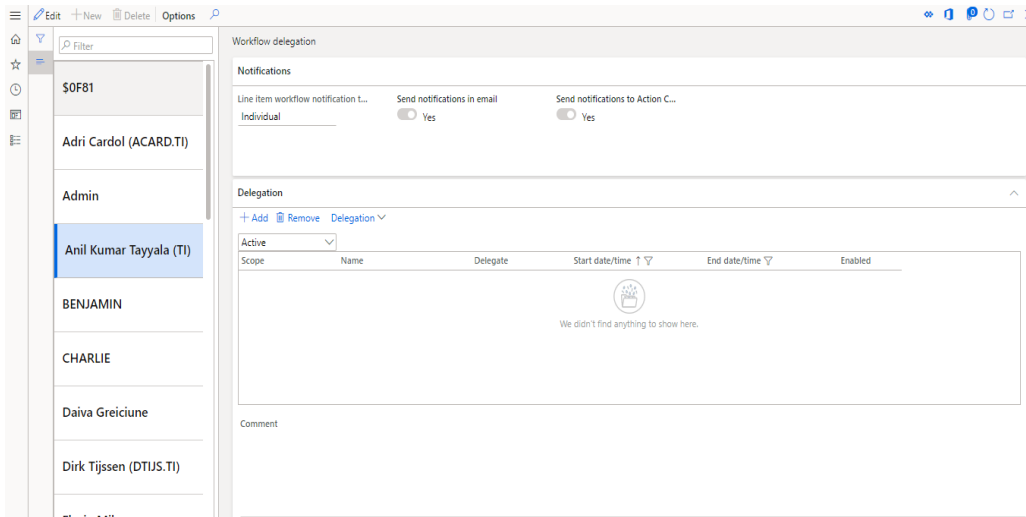
Field name	Field label	Asset classification
CNP/Num_BR		Customer Content
CPFNum_BR		Customer Content

Asset classification

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.

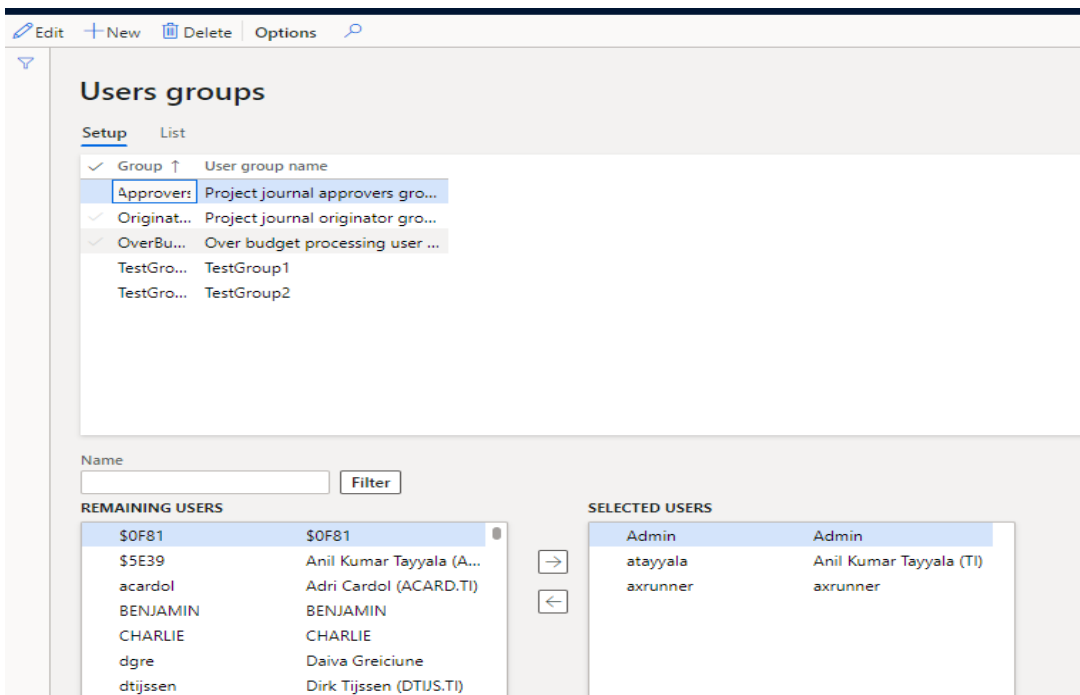
Workflow delegation history list page is also there for tracking. You can reach here from the Security and Compliance Module > Inquiries > Workflow delegation and >Workflow delegation history



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.



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

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

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

4.3 Security and compliance studio 10.0.31.37

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

4.4 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.	Enhanced 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
145372	CS00221370 Incorrect user security log in SCS	Now shows the correct log items
146730	CS00221689 Issue with Licensing framework	If snapshot is in queue and due to start in the upcoming 30 mins, the refresh license job cannot be set to start.

147973	CS00221859 The "Copy security setup" functionality on users also copies disabled roles	Disabled users are not copied anymore.
144053	CS00212605 New license type	Changes made to license display and calculation. The security explorer now shows recommendations for the base and attach licenses.

4.6 Security and compliance studio 10.0.27.33

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

4.7 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
144620	CS00218247 No security change logging when importing security roles while running in 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
140147	CS00208677 Table securable objects shown as a menu item display in the securable 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
124416	CS00164486 - User security log does not work when a data management import has been 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
115373	CS00144263-Enhanced SoD not showing display menu items when setting up, only 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
81072	Purchased license count setup: License information is now stored at admin.Microsoft.com. SCS now provides an option to administrator to setup the purchased license value in SCS. Purchased license value is used in license optimization workspace.
86619	CS00080538 – Security Explorer- No colored icon for “Tem Member” license type.
86627	CS00079152 – Apply Active Directory User Status – Authentication Method

4.30 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-POY5 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.	

4.43 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 ENRYPPOINTNAME failed because one or more objects access this column.

```
ALTER TABLE DSMSECURITYENRYPPOINTPRIVASSOCIATION ALTER COLUMN ENRYPPOINTNAME NVARCHAR(255) NOT NULL;
```

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

Steps:

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

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

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

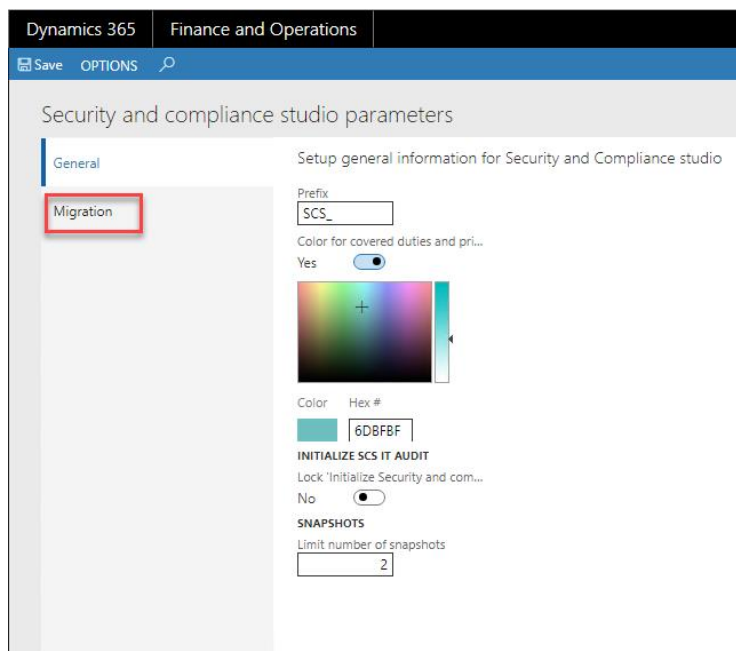


Fig. 1 New tab in SCS Parameters form

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

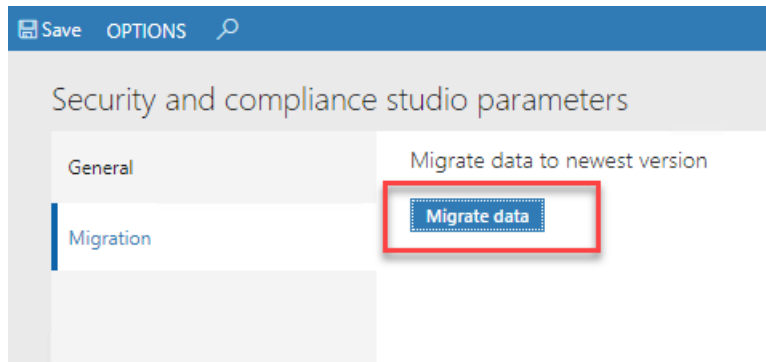


Fig. 2 "Migrate data" button on SCS Parameters form

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

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

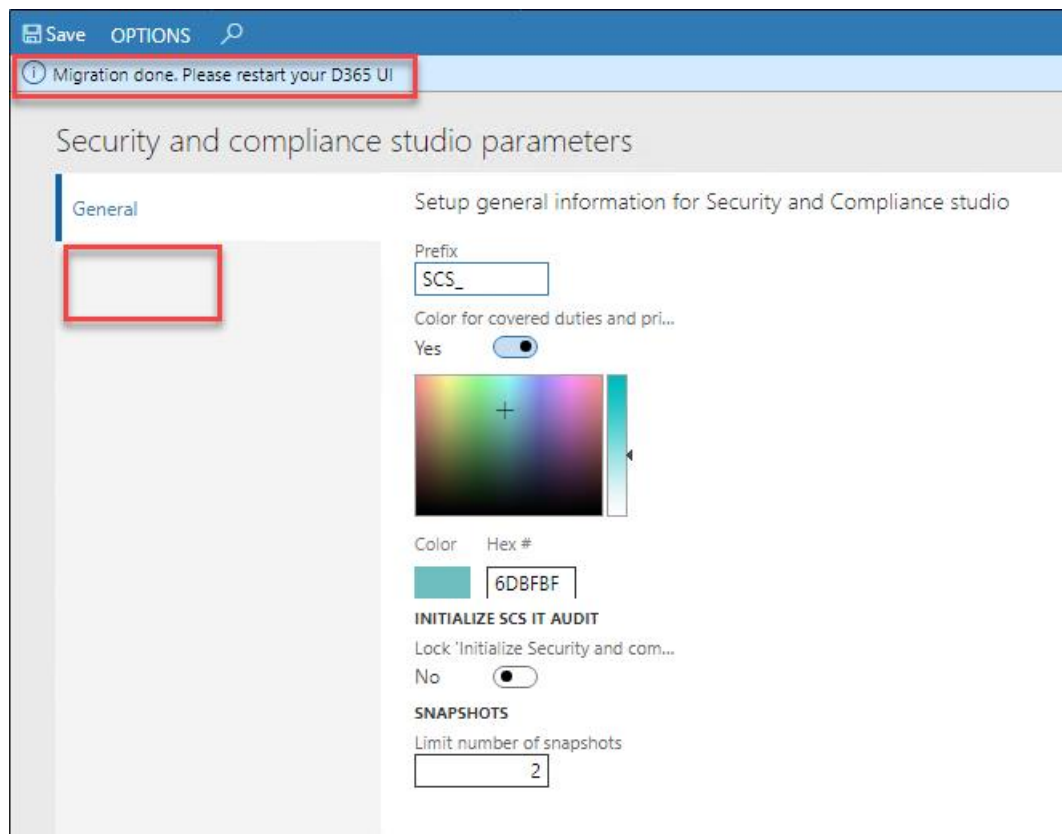


Fig. 3 "Migration" tab not available anymore after moving data