



Release Notes for Security and Compliance Studio 10.0.44.48

Release Notes

Author: Ankit Bhadana, Product Owner



Table of Contents

1.	Introduction	7
1.1	Purpose.....	7
1.2	Audience	7
1.3	Product release information	7
1.4	Deliverables	8
1.5	Common features.....	9
1.6	Certificate renewal	11
2.	What's New in Security and Compliance Studio 10.0.44.48	12
2.1	Securable Tree View – User-Based Security Object Analysis	12
2.2	Merge Role – Filtering and Sorting Enhancements for Role Selection Grids	13
2.3	Security Explorer – Filter Sensitive Data Access Objects by Security Reason	14
2.4	Security Explorer – View Access Details Enhancement	15
2.5	Sensitive Data Setup – Library	16
3.	Features introduced in last few releases of Security and Compliance Studio	17
3.1	Version 10.0.43.47	22
3.1.1	Select roles for Stand-in request.....	22
3.1.2	Import/Export of sensitive data setup.....	23
3.1.3	Security compliance	25
3.2	Version 10.0.42.46.....	27
3.2.1	Ability to raise security request to enable user and allocate roles for a specific period	27
3.2.2	Include “No. of access” on View access entry points page	30
3.2.3	Open source record and Generate report feature for Sensitive data log	31
3.3	Version 10.0.41.45	32
3.3.1	Security user role data.....	32
3.3.2	Ability to raise stand-in requests for other users	34
3.3.3	Batch-job to clean audit logs	35
3.3.4	Ability to activate and deactivate Sensitive data setup	37
3.3.5	Ability to select dimension and financial tag field using Table security recording	37



3.4	Version 10.0.40.44 Release	38
3.4.1	Organization assignment for security request.....	38
3.4.2	Continuous user action logging	39
3.5	Version 10.0.39.43 Release	41
3.5.1	User audit log for sensitive data	41
3.5.2	Securable tree view	44
3.5.3	Security request history track	47
3.5.4	Enhanced SoD predefined list.....	48
3.6	Version 10.0.37.42 and Older	50
3.6.1	Segregation of duties sets	50
3.6.2	Security requests enhancements and workflow	51
3.6.3	Export security explorer objects to excel in a de-normalized format	62
3.6.4	Merge security scenarios and match role	63
3.6.5	Mark any Security Role as Active/Inactive.....	63
3.6.6	Recording steps to scenario.	64
3.6.7	Override permission based on scenarios	64
3.6.8	Option to mark, track and audit security objects providing access to sensitive data.....	65
3.6.9	Option to create a duty from Matched Privileges grid in Match roles form	73
3.6.10	Option to import and export data using Data Entities in Security and Compliance Studio	73
3.6.11	Option to compare Security Snapshots stored in the security setup	74
3.6.12	Enhanced Audit log capability to capture all the changes from development space (AOT) as well into Audit Log.....	78
3.6.13	Option to create one or more privileges and also one or more duties while merging roles.	79
3.6.14	Ability to create scenarios from D365 module menus	80
3.6.15	Snapshots based performance and scalability enhancements	81
3.6.16	Improved “Create role wizard” based on a grid framework.....	83
3.6.17	Accessing Security Explorer from all D365 FOE forms.....	83
3.6.18	Option to create duties and SOD compliance check as well while merging roles.	84
3.6.19	Importing New Users while Synchronizing the group users with the Active Directory group members.....	85
3.6.20	Uptake RapidValue BPM Suite Scenarios directly as SCS Security Scenarios	85
3.6.21	Enhanced Segregation of Duties	87
3.6.22	Organization risk Register	88
3.6.23	AAD related SoD Validations across SCS	89
3.6.24	Security Explorer displaying Tables, Service operations and Data Entities entry point’s type	89



3.6.25	Performance Optimization	89
3.6.26	A new “Share” workspace	89
3.6.27	AAD groups’ information in D365FO	90
3.6.28	Verify SoD rules in Stand in	91
3.6.29	Chart to give an overview of the number of users and their last logging details	91
3.6.30	Asset classification User Interface	92
3.6.31	A List page with Workflow delegation details	93
3.6.32	User groups – combined two tabs in one	93
3.6.33	New export/import role functionality.....	94
3.6.34	License count changes.....	94

4. Bug fixes 97

4.1	Security and compliance studio 10.0.44.48	97
4.2	Security and compliance studio 10.0.43.47	97
4.3	Security and compliance studio 10.0.42.46	97
4.4	Security and compliance studio 10.0.41.45	98
4.5	Security and compliance studio 10.0.40.44	98
4.6	Security and compliance studio 10.0.39.43	98
4.7	Security and compliance studio 10.0.37.42	99
4.8	Security and compliance studio 10.0.36.41	100
4.9	Security and compliance studio 10.0.36.40	100
4.10	Security and compliance studio 10.0.34.39	100
4.11	Security and compliance studio 10.0.32.38	101
4.12	Security and compliance studio 10.0.31.37	102
4.13	Security and compliance studio 10.0.29.36	102
4.14	Security and compliance studio 10.0.28.34	102
4.15	Security and compliance studio 10.0.27.33	103
4.16	Security and compliance studio 10.0.26.32	103
4.17	Security and compliance studio 10.0.26.31	103
4.18	Security and compliance studio 10.0.25.30	103
4.19	Security and compliance studio 10.0.24.29	103
4.20	Security and compliance studio 10.0.22.27	103
4.21	Security and compliance studio 10.0.18.1	103
4.22	Security and compliance studio 10.0.12.5	103
4.23	Security and compliance studio 10.0.12.4	103
4.24	Security and compliance studio 10.0.12.3	104
4.25	Security and compliance studio 10.0.12.2	104
4.26	Security and compliance studio 10.0.12.1	104
4.27	Security and compliance studio 10.0.10.1	104
4.28	Security and compliance studio 10.0.6.11	104
4.29	Security and compliance studio 10.0.6.10	104
4.30	Security and compliance studio 10.0.6.9	104
4.31	Security and compliance studio 10.0.6.8	105
4.32	Security and compliance studio 10.0.6.7	105

4.33	Security and compliance studio 10.0.6.6	105
4.34	Security and compliance studio 10.0.6.5	105
4.35	Security and compliance studio 10.0.6.4	105
4.36	Security and compliance studio 10.0.6.3	106
4.37	Security and compliance studio 10.0.6.2	106
4.38	Security and compliance studio 10.0.6.1	106
4.39	Security and compliance studio 10.0.3.3	106
4.40	Security and compliance studio 10.0.3.2	106
4.41	Security and compliance studio 10.0.3.1	106
4.42	Security and compliance studio 10.0.1.3	106
4.43	Security and compliance studio 10.0.1.2	106
4.44	Security and compliance studio 10.0.1.1	107
4.45	Security and compliance studio 81.3.2.1	107
4.46	Security and compliance studio 81.3.1.1	107
4.47	Security and compliance studio 81.2.1.1	107
4.48	Security and compliance studio 81.1.2.1	107
4.49	Security and compliance studio 81.1.1.1	107
4.50	Security and compliance studio 81.20.3.1	107
4.51	Security and compliance studio 81.20.2.2 *(This build was created as the earlier deployable package had some issues).....	107
4.52	Security and compliance studio 81.20.2.1	108
4.53	Security and compliance studio 81.20.1.1	108
4.54	Security and compliance studio 1804.15.2.1	108
4.55	Security and compliance studio 1804.15.1.1	108
4.56	Security and compliance studio 1712.12.1.1	108
5.	Changed or deprecated features	109
5.1	Deprecated features 10.0.31.37	109
5.2	Deprecated features older versions	109
6.	Known issues	110



Document Information

Title	Release Notes for Security and Compliance Studio 10.0.44.48
Subtitle (Subject)	Release Notes
Solution Suite	GRC; Security and Compliance Studio
Category	Release Notes
Author	Ankit Bhadana
Published Date	6/4/2025
Status	Final
Comments	Security and Compliance Studio Release Notes

© Copyright STAEDEAN B.V. All rights reserved.

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



1. Introduction

1.1 Purpose

This document highlights new features and enhancements that ship in the new **Release Notes for Security and Compliance Studio 10.0.44.48** release from Staedean. This release is compatible with the version of Microsoft Dynamics 365 for Finance and Operations, **10.0.41 or later**.

1.2 Audience

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

1.3 Product release information

Release Notes for Security and Compliance Studio 10.0.44.48 for Dynamics 365 Finance and Dynamics 365 Supply Chain Management (10.0.44) is built upon D365 version 10.0.41. 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 10.0.41 or any later version and the application should compile without any issues. However, as we have only functionally validated this version against D365 version 10.0.44, we recommend applying our Staedean product release on that MS version as well. If you deviate from this (and thus apply the release to a different version), we recommend performing a more thorough round of testing before applying the release to a production environment.

This is summarized in the following table.

Release date	Staedean Version No.	Minimum required D365 version	Validated against D365 version	Compatible with D365 version
05/04/2024	10.0.39.43	10.0.36	10.0.39	10.0.36 and above
02/07/2024	10.0.40.44	10.0.36	10.0.40	10.0.36 and above
10/11/2024	10.0.41.45	10.0.36	10.0.41	10.0.36 and above
31/01/2025	10.0.42.46	10.0.39	10.0.42	10.0.39 and above
25/03/2025	10.0.43.47	10.0.40	10.0.43	10.0.40 and above
04/06/2025	10.0.44.48	10.0.41	10.0.44	10.0.41 and above

In case of an Error, Staedean may provide a Hotfix on a reasonable efforts basis in a way it considers appropriate in its discretion. Staedean cannot be obliged to provide Hotfixes if Client has not deployed



the latest Release or the Release second to the latest Release and/or is not using a supported version of Microsoft Dynamics.

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

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

1.4 Deliverables

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

Deliverable	Description
Solution package	Security and Compliance Studio is delivered as a Microsoft Dynamics Lifecycle Services (LCS) solution package.
Software package deployable	Release Notes for Security and Compliance Studio 10.0.44.48 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 library BPM	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 Staedean security certificate is provided to allow trusted installation of the provided model files and ISV license files.
Process data package	The solution package provides a simple Security and Compliance Studio <i>demo</i> process data package that can help you get started from LCS.



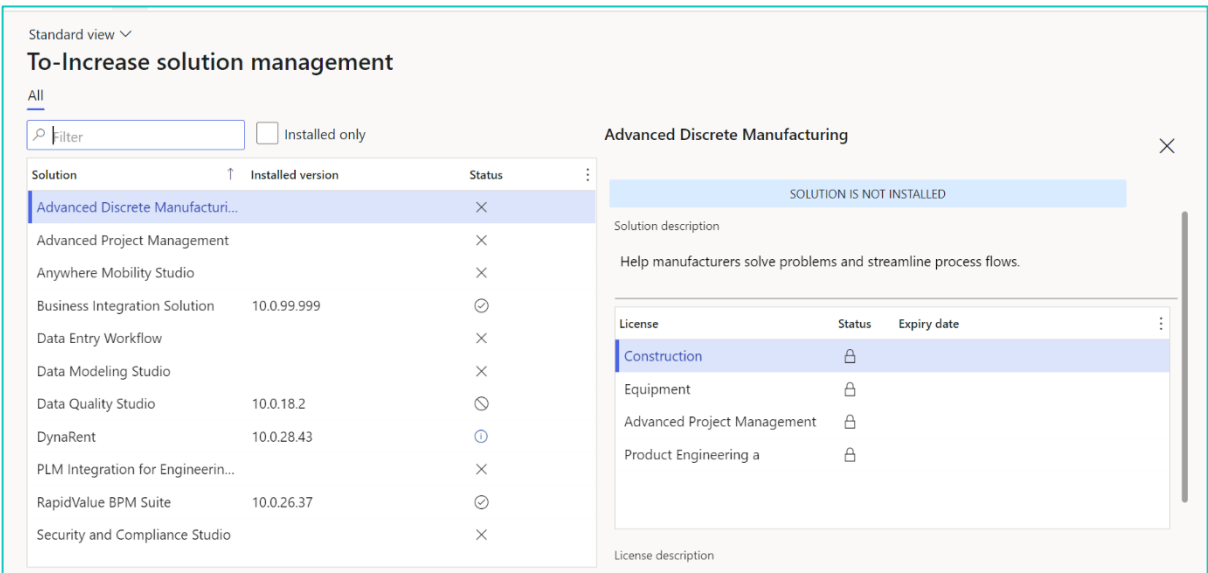
1.5 Common features

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

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

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

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



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



?

To-Increase would love your feedback!

Please rate your experience in using the All solutions screen.

☐ 5 - Excellent

☐ 4

☐ 3

☐ 2

☐ 1 - Poor

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

Thank you for providing us feedback!

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

SubmitCancel

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

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



1.6 Certificate renewal

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

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

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

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

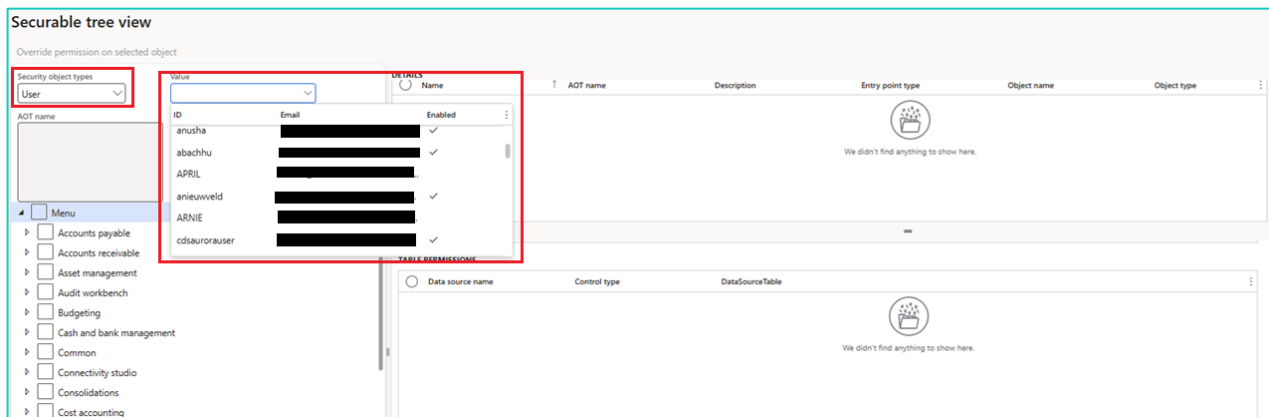
Step 3: Validate the licenses for correctness and completeness and click import

Click [here](#) for more information on the Solution Management Workspace.

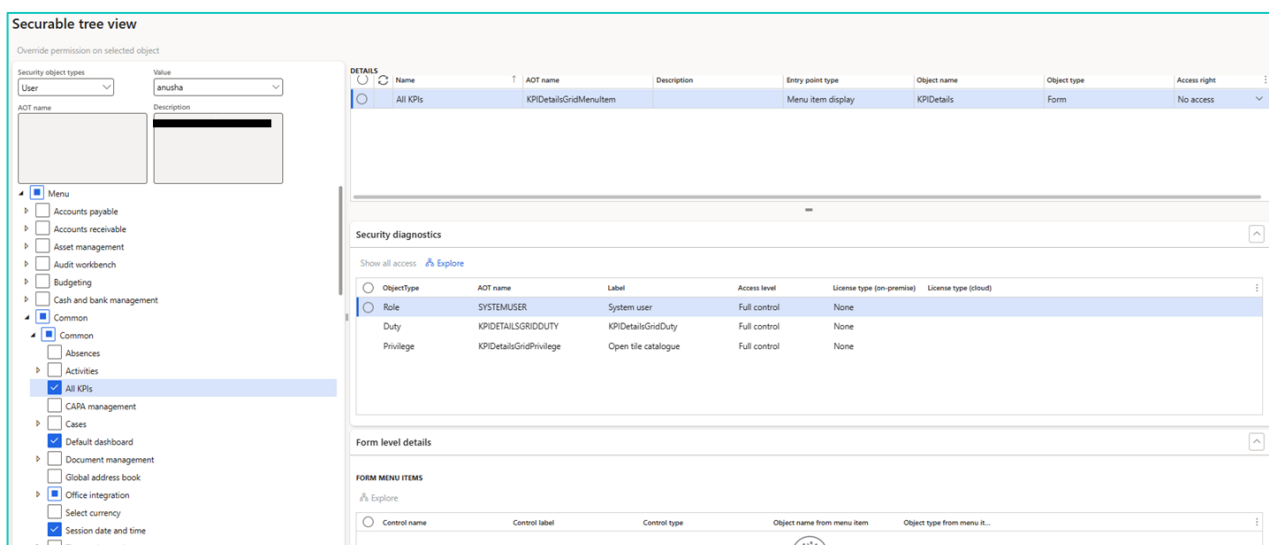
2. What's New in Security and Compliance Studio 10.0.44.48

2.1 Securable Tree View – User-Based Security Object Analysis

This enhancement will allow the user to analyse security access from an end-user perspective by introducing a new "Users" option in the Security Object Type dropdown on the Securable Tree View page. When this option is selected, the Values dropdown is dynamically populated with the list of users configured in the application.



Once a user is selected, the application automatically identifies and displays all menu objects assigned to the user through their roles within the tree view structure. This visual representation provides clear insights into the user's access across the application modules.





Additionally, in the Details → Security Diagnostic section, the Form Level diagnostics grid displays:

- Triple Permissions (Read, Update, Create) based on the user's role permissions
- Form Controls that require explicit access permissions

This user-centric enhancement improves security visibility, simplifies compliance auditing, and supports the enforcement of least-privilege access policies.

Note:

- If a user has System Administration role allocated, then the objects related to that role are not marked. However, if there is any object which is common for System Administration role and any other role allocated to that user, then that object is marked.
- Application may take some time to load the objects for the selected user depending on the roles allocated to the selected user.

2.2 Merge Role – Filtering and Sorting Enhancements for Role Selection Grids

This enhancement will allow the user to filter and sort roles within the Available Roles and Selected Roles grids on the Merge Role page. Previously, these grids only displayed static lists—Available Roles showing all roles in the system, and Selected Roles listing the roles chosen for merging—without any capability for filtering or sorting.

The screenshot shows the 'Merge roles' page. On the left is a sidebar with a progress indicator: 'Select roles' (active), 'Privilege settings', 'Permissions set', and 'Completed'. The main area is divided into two sections. The top section, 'Select or enter the role to merge to.', contains a 'TARGET ROLE' section with a 'Name' dropdown and a 'Lock target role?' toggle set to 'Yes'. Below this is the 'Select the roles to merge from.' section. This section contains two grids: 'AVAILABLE ROLES' and 'SELECTED ROLES'. The 'AVAILABLE ROLES' grid is highlighted with a red box and shows a header with 'Role name' and a dropdown menu. Below the header are sorting options: 'Sort A to Z' and 'Sort Z to A'. There is also a filter section with the label 'Role name begins with' and a text input field. Below the input field are 'Apply' and 'Clear' buttons. The 'SELECTED ROLES' grid is currently empty, showing a message 'We didn't find anything to show here.' with a folder icon. Arrows indicate the flow of roles between the two grids.

With this update, both grids now support the standard filtering and sorting functionality provided by Microsoft Dynamics 365. Users can apply filters directly within the grid headers to narrow down role selections based on specific criteria and sort the role data in ascending or descending order for improved navigation and usability.

This enhancement significantly improves the user experience when managing large volumes of roles, enabling more efficient and accurate role selection during merge operations.

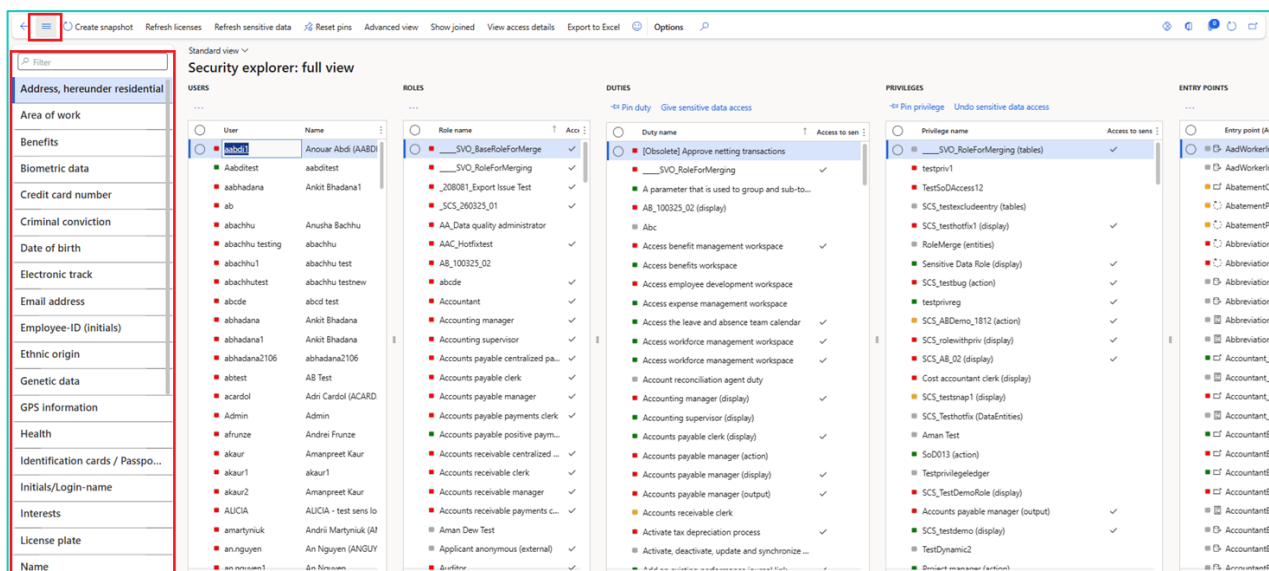
2.3 Security Explorer – Filter Sensitive Data Access Objects by Security Reason

This enhancement will allow the user to filter sensitive data access objects based on Security Reason within the **Manage Sensitive Data Access** page of the Security Audit workspace in the Security and Compliance Studio application.

When the user clicks on the “Manage Sensitive Data Access” option in the Summary section, the application navigates to an enhanced Security Explorer page. This page allows the user to view objects—such as roles, duties, privileges, and entry points—as having access to sensitive data. While allowing an object as sensitive data access, the application prompts a popup where the user must provide a Security Reason and a description.

Previously, although the grid displayed objects along with their assigned Security Reasons, there was no way to filter the list based on these reasons.

With this enhancement, A hamburger icon has been added to the top-left corner of the screen. Clicking this icon opens a panel displaying a list of configured Security Reasons. Upon selecting a Security Reason, the application filters the grid to display only those objects associated with the selected reason.



All other functionalities, such as pinning by role, duty, or user, remain unchanged. This enhancement improves the precision and usability of sensitive data access reviews by enabling quick filtering based on Security Reason.



2.4 Security Explorer – View Access Details Enhancement

This enhancement will allow the user to benefit from a redesigned "View Access Details" experience on the Security Explorer page. The existing button “View Accessed Entry Points” has been renamed to "View Access Details" for improved clarity. The existing functionality of the button remains unchanged.

A new dropdown labelled "Security Object" has been added to the View Access Details page, allowing users to choose from:

- 1. Roles
- 2. Duties
- 3. Privileges
- 4. Entry Points

Based on the selection, corresponding access grids are displayed alongside a persistent Users Grid, which always shows all users with their ID, Name, and Enabled status. This grid supports sorting and filtering and remains visible when switching between security objects.

View access details

☐ Show enabled users only

Security object

Roles

ID	Name	Enabled
SC08A	SC08A	false
aabd1	Anouar Abdi (AABDI.TI)	true
Aabditest	aabditest	true
aabhadana	Ankit Bhadana1	true
ab	test add	true
abachhu	Anusha Bachhu	true
abachhu testing	abachhu	true
abachhu1	abachhu test	false
abachhutest	abachhu testnew	false
abcode	abcode test	true
abhadana	Ankit Bhadana	true
abhadana1	Ankit Bhadana	true
abhadana2106	abhadana2106	false
abtest	AB Test	false
acarbol	Adin Cardol (ACARD.TI)	true

ROLES ALLOCATED

Role AOT name	Role name
COLLECTIONLETTERCOLLECTIO...	Collections manager
DEWDATAENTRYWORKFLOWU...	Data entry workflow user
FLOWPOWERUSERROLE	Power Automate administrator
OFFICEINTEGRATIONPOWERUS...	Office integration power user
PAYMACCOUNTSRECEIVABLECE...	Accounts receivable centralized ...
PAYMACCOUNTSRECEIVABLEPRA...	Accounts receivable payments c...
-SYSADMIN-	System administrator
SYSTEMUSER	System user

ROLES ACCESS

Role identifier	Role name	Last accessed on	N
DEWDATAENTRYWORKFLOWUS...	Data entry workflow user	12/6/2024 7:19:11 AM	
DEWDATAENTRYWORKFLOWM...	Data entry workflow manager	12/6/2024 7:01:06 AM	

When a user is selected, the application displays access history derived from the entry points accessed by that user. Roles, duties, or privileges shown in the respective accessed grids are inferred based on entry point relationships. For example, if an entry point is linked to two roles, both roles will appear in the Roles Accessed grid if that entry point was accessed by the user.

All access grids support filtering and sorting, and depending upon Security object selected, the Role, Duty, or Privilege access grids are automatically sorted by last access date/time and number of accesses in descending order. A loading indicator is shown while data is being fetched, and appropriate error messages are displayed in case of data retrieval issues.



2.5 Sensitive Data Setup – Library

In this released, we have created sensitive data setup configuration for the following modules:

- Account Payable
- Account Receivable
- Human Resources
- Product Management

These standard configuration files (XML files) can be imported in the application using the Import feature available on the Sensitive Data Setup page. Once imported, user will be able to activate the setup, and application will start capturing the logs for the activated setup.

Note: Please make sure to specify the users who will be able to view the sensitive data logs for the setup.

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



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

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

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

- **Option to import and export data using Data Entities in Security and Compliance Studio.** In this release we have added some data entities currently supported for Security and Compliance Studio. The approach has been to enable data entities for all tables where relevant in Security and Compliance Studio in order to provide import and export capabilities.
- **Option to compare Security Snapshots stored in the security setup.** Building upon what we already have implemented in the fall release (security snapshots) we have gone furthered and added the possibility of comparing the existing security snapshots. Snapshot comparison feature allows security officers and administrators to do a detailed comparative analysis between any two security snapshots for all security objects in D365 FOE setup i.e. Users, roles, duties, privileges. Both single record compare and full compare options for the selected snapshots are supported along with multiple views. The comparison option will allow the user to see what modifications had occurred in the security setup since the last changes. The users can keep track of the changes, comprehend and analyze them in order to strengthen the security further.
- **Enhanced Audit log capability to capture all the changes from development space (AOT) as well into Audit Log**
This release enhances the audit log feature within Security and Compliance studio in order to capture and register the changes made directly on the security objects from the development space (visual studio). Now, when a new snapshot is created; automatically the new snapshot will be compared with the last one. In this way all the changes made in security configuration will be captured in the Audit log.
This comes as a solution of capturing all the changes no matter if they took place in the *UI (user interface)* or directly into *development space (in Visual Studio)*.
- **Option to create one or more privileges and also one or more duties while merging roles.** “Merge role” feature now comes with an option to create only one merged privilege for all entry point types in addition to the existing options to create multiple privileges and one or more duties. Previously you can split up entry points in separate privileges and duties by entry point type. Now you can create also only one privilege for the merged roles.
- **Ability to create scenarios from D365 module menus.** You can now model security scenarios for D365 modules. “Add module access” feature helps you to create a new scenario based on the complete list of a module menu items with a desired level of access types. This is of great help when you desire to have a security role providing you access to all or most of one module features.
- **Snapshots based performance and scalability enhancements.** The entire functionality for Rebuild Data, Security Explorer and Match Roles revolves around the security objects (roles, duties, privileges and entry points) and the associations between them (duties assigned to role; privileges assigned to each duty, etc.). All of these are kept in standard code that was preserved, externally, into a DLL. Using this DLL for multiple scopes in Security and Compliance Studio end up with a performance issues on the above mentioned business logics/functionalities. We now have created a structure of tables to keep the data related to each security object and the association between them and easily access it directly from tables and also much faster. This has led to drastic improvement in the “Match roles” and “Rebuild data” programs performance.
- **Improved “Create role wizard” based on a grid framework.** “Create role wizard” is now based on a new grid framework making it a great user experience. This wizard helps you to create a new security role based on duties and privileges with letting you know the license type before role creation.
- **Accessing Security Explorer from all D365 FOE forms.** This release comes with Security and compliance studio security explorer embedded in all D365 FOE forms. This provides a very useful way to analyze users and associated security objects (roles, duties, privileges, entry points) that have access to that D365 FOE form.



- **Option to create duties and SOD compliance check as well while merging roles.** “Merge role” feature now comes with an option to create duties along with the privileges. Previously you can split up entry points in separate privileges by entry point type. Now you can create and associate duties as well for the different entry point type (action, display, output etc.).
- **Importing New Users while Synchronizing the group users with the Active Directory group members.** We added a new small feature to our Azure AD group synchronization job. On the dialog of the Synchronize the group users with the Active Directory group members, we introduced a new parameter to import users.
- **Licensing changes** – To help our customers we have implemented new licensing changes within SCS. Microsoft has taken a commercial decision last year to split the license to Finance, SCM, and project, for more details you can have a look at Microsoft's new licensing guide. These changes left customers confusing about how they can be compliant with new license changes. That's why we have decided to build this feature, now customers can see a new license type field in SCS forms such as security explorer, match roles, license optimization workspace, etc.
- **Uptake RapidValue Scenarios directly as SCS Security Scenarios** – Customers can now directly upload the RapidValue Scenario task guides per security roles (Procedure activities which include flows across multiple roles) as a Security scenario in Security and Compliance Studio. This will be very useful where both RapidValue BPM Suite and Security and Complicate Studio are implemented. You might be aware that now in RapidValue, you can have Business process hierarchy with its linked task guides exported from RapidValue to a user defined local Windows folder. Export logic takes care of both the modeling techniques where customer is using Flow-Activity way of modeling and also the Scenario" Procedure Activity" way of capturing flow variations.
- **Enhanced Segregation Of Duties** – In standard D365FSC, we can only define SoD rules at duty level which is rarely useful. In SCS, with this release user can now define SoD rulesets at any level (Duty, Privilege or Entry Point) in the security hierarchy in D365FSC. This makes this feature more practical and extremely useful for customers seeking better regulatory compliance like ISO 27001 section 6.1.2, SOX Control 404 and in general much improved security design better equipped to prevent frauds.
- **Organization Risk Register**– All Organizational risks can be now mapped in SCS “*Integrated risk Management workspace*”. They may be financial risks related to SoD violations or can be related to any other organizational strategy or operational aspect. This feature will evolve in coming quarters in a full-fledged “Risk Management” capabilities within SCS enabling Organizations to register, assess, monitor, mitigate and close it.
- **AAD related SoD Validations across SCS** – SCS now ensures that SoD violation checks also consider Security roles acquired by a user from being associated within an AAD. This is applicable all across SCS features. This helps in better handling of internal controls.
- **Security Explorer displaying Tables, Service operations and Data Entities entry point's type** - Security 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.
- **Dynamic snapshot** - We got a lot of feedback and learnings related to the security snapshot. A lot of features depend on having actual data in the snapshot. New changes in the snapshot framework have been introduced where the snapshot no longer requires to updated via a batch job after security changes have been made.

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

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

- **New export/import role functionality**
 1. **Problem:** For a couple of years, we have discovered and reported to Microsoft a standard bug that for AOT Privileges the node ‘FormControlOverrides’ is not readable from code and that is affecting, for example, the current SCS Export / Import functionality.
 2. **Issue that is generated by the bug explained:** When exporting a role using SCS Export function the XML file generated does not contain the entries under the ‘FormControlOverrides’ from AOT Privileges.
After the SCS Import function runs, the content from the XML file is applied to the target environment. Since the ‘FormControlOverrides’ node is empty in the XML file, the



algorithm interprets it as a change (entries removed from node by user) therefore it will override the privilege in target environment and the entries will be removed.

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

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

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

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

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

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

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

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

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

3.1 Version 10.0.43.47

3.1.1 Select roles for Stand-in request

This enhancement will allow the user to select the roles that must be allocated to a stand-in user. Previously, when a stand-in request was created and approved, the delegate user would automatically inherit all roles assigned to the primary user for the specified period. However, there was no option to control or limit which roles were allocated. This resulted in unnecessary access being granted, which could pose security risks and administrative challenges.

With this enhancement, users now can selectively assign roles to a stand-in user rather than granting full access to all roles by default. A new feature has been introduced within the "Create Stand-in Request" workflow, allowing users to specify the exact roles that should be assigned to the delegate user. This improvement ensures that only the necessary permissions are granted during the delegation period, enhancing security and providing better control over role management.

General

Request

209367_3

Type

Add stand-in

Origin

User requests

Area

Status

Priority

Normal

Security record status

Open

Owner

abhadana

Create stand-in

+ Add

Remove

Assign roles

User ID

Stand-in

From date

↑ To date

Copy assigned organizations

abhadana2106

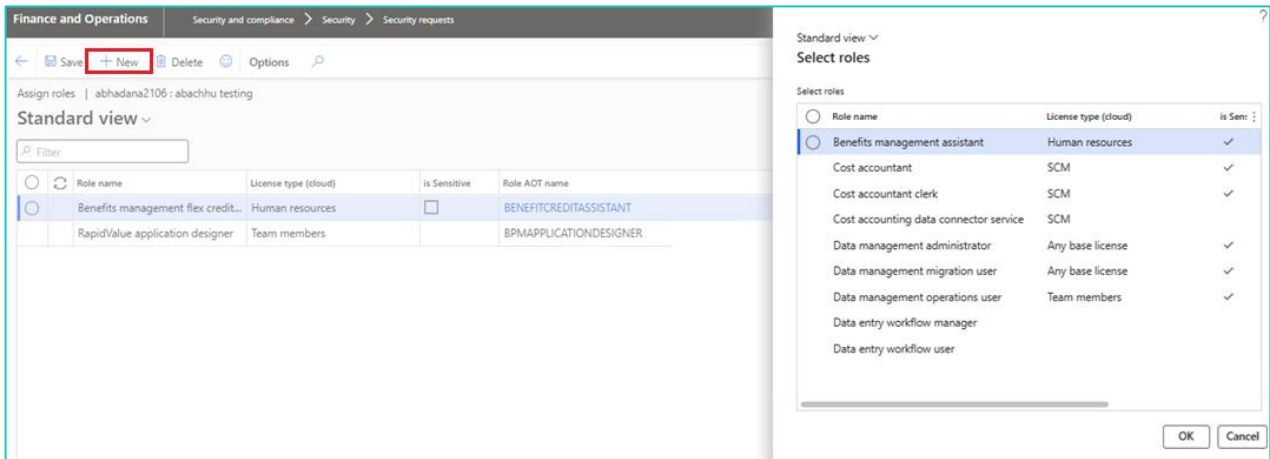
abachhu testing

3/7/2025

3/7/2025

A new "Assign Role" button has been added to the stand-in request form, enabling users to choose roles that should be allocated to the delegate user for the specified period. Upon clicking this button, the system presents a pop-up containing a list of roles currently assigned to the primary user but not yet allocated to the delegate.

The user can then select one or more roles from this list and submit the request for approval. Any roles already assigned to the delegate will not be displayed in the selection list, ensuring that only unallocated roles are available for assignment.



Once the request is approved, the system automatically grants the selected roles to the delegate user when the stand-in period begins. This ensures that the delegate has the required access for the specified time frame. At the end of the stand-in period, the system revokes the assigned roles from the delegate user, returning them to their previous state. This process eliminates the need for manual intervention, reducing administrative overhead while ensuring compliance with security policies.

This enhancement improves security by enforcing the principle of least privilege, ensuring that delegate users receive only the access necessary for their role during the delegation period. Additionally, it enhances the user experience by providing a more flexible and controlled approach to role assignment. The new workflow simplifies delegation management, making it easier for users to request and manage stand-in access without unnecessary permissions being granted.

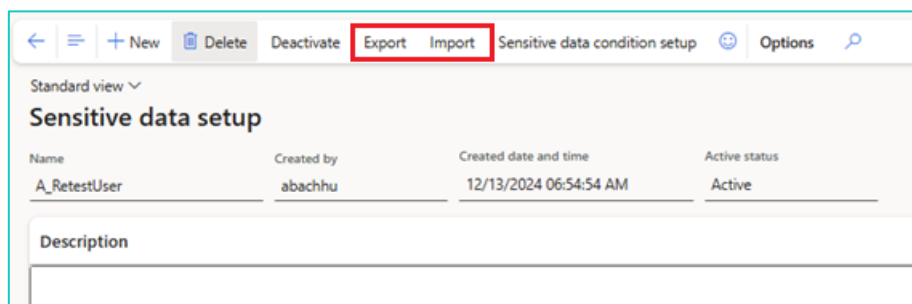
3.1.2 Import/Export of sensitive data setup

This release introduces a new feature within the Sensitive Data Setup module of the Security & Compliance System (SCS), enabling users to import and export sensitive data setup configurations between different environments.

With the new import and export functionality, users can now seamlessly export a setup from one environment and import it into another without manual reconfiguration.

Two new buttons have been introduced on the Sensitive data setup page:

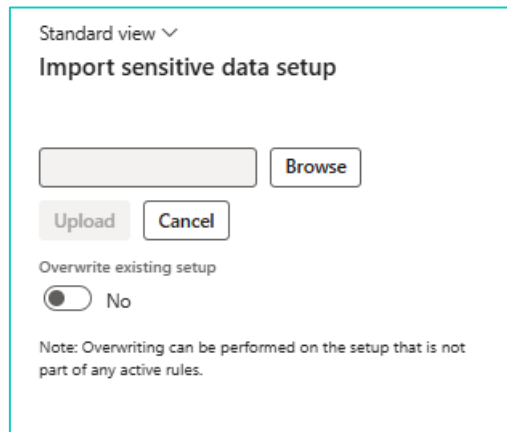
- Export and
- Import





On clicking the *Export* button, the system generates an XML file containing the complete configuration, which can be downloaded and stored locally. To replicate the setup in a different environment, users can simply import the XML file into the target system, ensuring that the setup remains identical across environments.

On clicking the Import button, application will prompt a pop-up to select the import file.



The image shows a dialog box titled "Import sensitive data setup". At the top left, it says "Standard view" with a downward arrow. Below the title is a text input field followed by a "Browse" button. Underneath are "Upload" and "Cancel" buttons. A toggle switch is labeled "Overwrite existing setup" and is currently set to "No". At the bottom, a note states: "Note: Overwriting can be performed on the setup that is not part of any active rules."

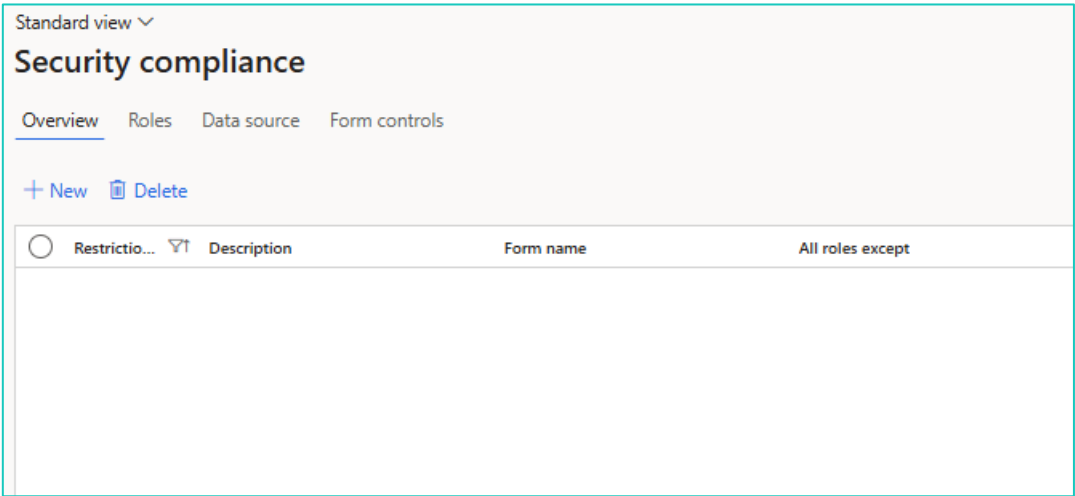
During the import process, if the setup already exists in the target environment, the system provides an option to overwrite the existing setup. This is particularly useful when making updates to an existing setup while maintaining consistency across environments. If the overwrite option is selected, the imported setup replaces the previous version, ensuring that all configurations remain up to date. However, there is a limitation to this functionality—overwrite can only be performed on setups that are not active. This restriction ensures that no disruptions occur in environments where the setup is currently in use.

Additionally, the system automatically handles discrepancies that may arise due to differences in environment-specific configurations. For example, if a user is assigned to the sensitive data setup in the source environment but does not exist in the target environment, the system will still complete the import successfully while omitting the missing user. This prevents errors and allows for a smooth transition between environments.

3.1.3 Security compliance

A new feature named *Security Compliance* has been introduced in the Security & Compliance Studio. This feature enables users to define and enforce security restrictions on forms based on user roles and field values. It enhances security controls by allowing organizations to specify role-based restrictions that limit user access to certain functionalities, making data handling more secure and reducing unauthorized modifications.

With this feature, users can create security rules that either revoke or modify access permissions based on predefined conditions. This feature supports conditions that enable or disable specific fields, button group, or button within forms, helping organizations enforce strict data access policies across different modules.

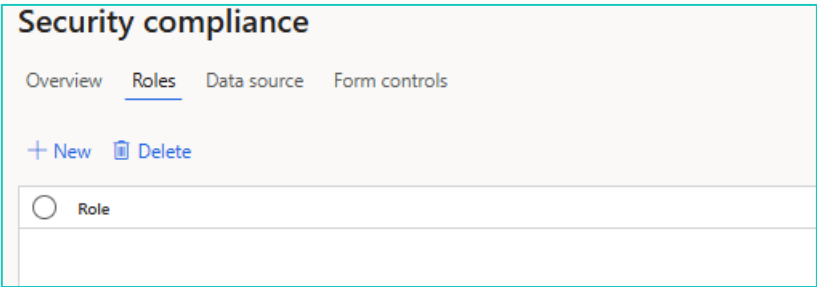


There are four tabs on *Security Compliance* tab.

Overview: This tab has the following information:

- **Restriction Code:** This field will allow the user to specify the code for the role.
- **Description:** This field will allow the user to describe the restriction.
- **Form Name:** This field will allow the user to select the form on which the restriction rule will be applied.
- **All roles except:** This field is a checkbox field. If the checkbox field is checked, then the restriction will be applicable for all the roles except the one specified in the Roles tab. Or else if the checkbox is unchecked, then the restriction will be applicable for all the roles specified in the Roles tab.

Roles: The Roles tab allows users to specify roles for the security restriction.





Data Source: The Data Source Tab allows users to define restrictions at the table level and configure access rules for specific data fields within forms. This tab has following fields:

- Data Source: Users need to specify form name in this field.
- Table Name: This will be auto populated.
- Access Level: User will need to select access level from this drop-down field. This drop-down will have following access levels:
 - Default: the default table access set for the role will not be modified (e.g. if the role has Read access to the form, it will still have Read access).
 - Disable selected: The fields selected in the Fields table will be disabled (i.e. equal to the current logic).
 - Disable all except: All the table fields will be disabled, except those listed in the Fields table.
 - Read: The default access to the selected table will be modified to Read access (i.e. equal to the previous “Disable all” logic)
 - Edit: the default access to the selected table will be modified to Edit access.
 - Create: the default access to the selected table will be modified to Create access.
- If the selected access level is Disable selected or disable all except, then application must allow the user to select the fields in the Datasource Fields table.

Security compliance

Overview

Roles

Data source

Form controls

+ New

Delete

Query

Flush cache

<input type="radio"/> Data source	Table name	Access level	Cache	
<div><div></div><div>We didn't find anything to show here.</div></div>				

DATASOURCE FIELDS

+ New

Delete

<input type="radio"/> Field name	Field label	
<div><div></div><div>We didn't find anything to show here.</div></div>		

Form Control: The Form Control Tab extends security restrictions to buttons or button group on the forms. This feature is particularly useful for controlling form-level security by disabling or enabling specific buttons based on user roles.

User will need to select the following information on the tab:



- Control Name: In this field, user will need to specify the control name. The drop-down will automatically populate the list of controls that includes action pane, button groups and individual buttons.
- Data Source: This will be auto populated based on the selected form.

Security compliance

Overview Roles Data source Form controls

+ New Delete

	Control name	Data source
<input checked="" type="checkbox"/>	[ButtonGroup:ButtonGroupForecast]	▼

3.2 Version 10.0.42.46

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

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

Create User:

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

Create users

User name User ID Email Company

From date To date

12/27/2024 12/31/2154

ROLES

Add Remove

Role name	Description	Role AOT name	From date	To date
We didn't find anything to show here.				

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

Disable User:



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

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

Enable User:


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

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

Assign Role to User:

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




ROLES				
Add Remove				
<input type="radio"/> Role name	Description	Role AOT name	From date	To date
<div> We didn't find anything to show here.</div>				

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

Remove Role from User:

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

ROLES				
Add Remove				
<input type="radio"/> Role name	Description	Role AOT name	From date	To date
<div> We didn't find anything to show here.</div>				

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

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

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

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



3.2.2 Include “No. of access” on View access entry points page

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

aa8di - Anouar Abdi (AABDI.T) | Standard view

View accessed entry points

Filter

Show enabled users only

USERS		ENTRY POINTS PERMITTED		ENTRY POINTS ACCESSED					
ID	Name	Entry point (AOT name)	Type	Menu item name	Menu item label	Menu item type	Last accessed on	No. of access	
SC0BA	SC0BA	AbbreviationsEntity	DataEntity	DQSDatapolicy	Data policy	Display	12/26/2024 12:12:37 PM	74	
aa8di	Anouar Abdi (AABDI.T)	AbbreviationsEntity	DataEntity	DewWorkflowWizard	Workflow wizard	Display	12/19/2024 11:12:40 AM	72	
ab		AccountingDistBankStatement	Menu item display	DQSDatapolicyListPage	Data quality policies	Display	12/26/2024 12:11:54 PM	46	
abachhu	Anusha Bachhu	AccountingDistCustFreeInvoice	Menu item display	DewWorkflowTemplateListPage	Data entry workflo...	Display	12/23/2024 10:30:05 AM	36	
abachhu testing	abachhu	AccountingDistCustInvoicr	Menu item display	DewWorkflowWorkspace	Data entry workflo...	Display	12/27/2024 11:07:34 AM	31	
abachhu1	abachhu test	AccountingDistMarkupTransinv	Menu item display	DewWorkflowTemplatePreview...	Data entry workflows	Display	12/27/2024 11:07:37 AM	31	
abachhutest	abachhu test	AccountingDistMarkupTransinv	Menu item display	LogisticsPostalAddressGridFor...		Display	12/26/2024 11:18:04 AM	26	
abode	abod test	AccountingDistMarkupTransPO	Menu item display	DQSDQualityAssessmentHistory	Quality assessment...	Display	12/24/2024 10:40:15 AM	25	
abachhu2	abachhu test	AccountingDistMarkupTransPO	Menu item display	DQSDQualityAssessmentHistory	Quality assessment...	Display	12/27/2024 11:07:37 AM	24	

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

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

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

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

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

The screenshot shows the 'Sensitive data log' page with the 'Open source record' button highlighted in the top navigation bar. The page displays a table of sensitive data logs with columns: Record identifier, Secondary identifier, Form name, Form label, Table label, Modified table, Event created by, Sensitive data setup name, and Sensitive data setup description. The table contains several rows of data, including records for 'abtest customer', 'test213', 'anm', '10001', and 'Guest'.

Record identifier	Secondary identifier	Form name	Form label	Table label	Modified table	Event created by	Sensitive data setup name	Sensitive data setup description
000021	abtest customer	CustTable	Customers	Customers	CustTable	abhadana	AB_CustDataCheck	
test213	test213	SysUserManagement	Users	User information	Userinfo	amartyniuk	Vishnu Test user	Logging
anm	DEL	SysUserManagement	Users	User information	Userinfo	amartyniuk	Vishnu Test user	Logging
10001		CustGroup	Customer groups	Customer groups	CustGroup	Vijay	testing for bug	test
10001	Test 10001	CustGroup	Customer groups	Customer groups	CustGroup	Vijay	testing for bug	test
Guest		SysUserManagement	Users	User information	Userinfo	abachhu	Vishnu Test user	Logging

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

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

The screenshot shows the 'Sensitive data log' page with the 'Generate report' button highlighted in the top navigation bar. The page displays a table of sensitive data logs with columns: Record identifier, Secondary identifier, Form name, Form label, Table label, Modified table, Event created by, Sensitive data setup name, and Sensitive data setup description. The table contains several rows of data, including records for 'abtest customer', 'test213', 'anm', '10001', and 'Guest'.

Record identifier	Secondary identifier	Form name	Form label	Table label	Modified table	Event created by	Sensitive data setup name	Sensitive data setup description
000021	abtest customer	CustTable	Customers	Customers	CustTable	abhadana	AB_CustDataCheck	
test213	test213	SysUserManagement	Users	User information	Userinfo	amartyniuk	Vishnu Test user	Logging
anm	DEL	SysUserManagement	Users	User information	Userinfo	amartyniuk	Vishnu Test user	Logging
10001		CustGroup	Customer groups	Customer groups	CustGroup	Vijay	testing for bug	test
10001	Test 10001	CustGroup	Customer groups	Customer groups	CustGroup	Vijay	testing for bug	test
Guest		SysUserManagement	Users	User information	Userinfo	abachhu	Vishnu Test user	Logging

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

Users can continue working while the report is being generated.

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

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

Generate report

Parameters

SENSITIVE DATA SETUP

Sensitive data setup name

DATES

From date

12/1/2024

To date

12/27/2024

Run in the background

Recurrence

Alerts

Batch processing

No

Task description

Generate report

Batch group

Private

No

Critical Job

No

Monitoring category

Undefined

Start date: 12/27/2024 (12:25:14 pm) (GMT) Coordinated Universal Time

OK

Cancel

Security and compliance file share

Summary

Share

Task recording	Upload	Download	Delete	Refresh	View
Images					
Exported role					
Logs					
	File name	File types	Size	Created date and time	Downloads
	AB_CustDataCheck-01122024-2...	Sensitive data log	4.40 KB	12/26/2024 11:19:39 AM	1
	AB_CustDataCheck-01122024-2...	Sensitive data log	4.40 KB	12/26/2024 11:13:18 AM	1
	AB_CustDataCheck-01122024-0...	Sensitive data log	1.20 KB	12/4/2024 7:23:42 AM	1
	Test User_Testrecordidentifie...	Sensitive data log	103.30 KB	12/4/2024 6:32:51 AM	3
	TestrecordIdentifier-0111202...	Sensitive data log	57.80 KB	12/4/2024 6:30:56 AM	1
	TestrecordIdentifier-0111202...	Sensitive data log	57.80 KB	12/4/2024 6:28:20 AM	1

3.3 Version 10.0.41.45

3.3.1 Security user role data

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

On the *Enquires* section of the Security and compliance studio, a new option named Security user role data has been added. On clicking this option, the application will navigate the user to the page

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

32

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

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

General

Request

Stand-in_0310

Type

Add stand-in

Origin

Security and compliance studio

Area

Status	ID	Type	Name	Email	Provider	Enabled
Priority	\$COBA	Claims user	\$COBA			
Normal	aabdi	Claims user	Anouar Abdi (AABDI.TI)			✓
	ab	Claims user				✓
Create status	abachhu	Claims user	Anusha Bachhu			✓
+ Add	abachhu1	Claims user	Bachhu AnushS8test			
	abachhutest	Claims user	abachhu test			✓

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



3.3.3 Batch-job to clean audit logs

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

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

Security and compliance studio parameters

General

License count

Data migration

Enhanced SoD rules

Number sequences

Logs

Logs setup for security and compliance studio

RETENTION DAYS

Audit log retention period (In days)

5

Sensitive data log retention period (In ...)

1

LOGS

Enable continuous user logging

☐ No

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

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

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

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

Clean-up audit log

Parameters

Audit log retention period (In days)

5

NOTE: to change the retention days please navigate to Security and Compliance Studio -> Setup -> Parameters

Run in the background

Recurrence Alerts

Batch processing

☐ No

Task description

Clean-up audit log

Batch group

Private

☐ No

Critical Job

☐ No

Monitoring category

Undefined

Start date: 10/3/2024 (06:42:47 am) (GMT) Coordinated Universal Time

OK Cancel



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

Clean-up sensitive data log

Parameters

Sensitive data log retention period (In ...

1

NOTE: to change the retention days please navigate to Security and Compliance Studio -> Setup -> Parameters

Run in the background

Recurrence Alerts

Batch processing

No

Task description

Clean-up sensitive data log

Batch group

Private

No

Critical Job

No

Monitoring category

Undefined

Start date: 10/3/2024 (07:03:28 am) (GMT) Coordinated Universal Time

OK

Cancel

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

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



3.3.4 Ability to activate and deactivate Sensitive data setup

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

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

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

The screenshot shows the 'Sensitive data setup' page. The top navigation bar includes a back arrow, a menu icon, and buttons for 'Save', '+ New', 'Delete', and 'Activate' (highlighted with a red box). The page title is 'Sensitive data condition setup'. Below the navigation bar, there is a search bar with 'Vendor' entered. The main content area shows the 'Sensitive data setup' form. The 'Name' field is 'VendorDataLogs', 'Created by' is 'abhadana', 'Created date and time' is '10/3/2024 08:08:20 AM', and 'Active status' is 'Inactive'. The 'Description' field is empty. The 'General' section has a table with columns 'Table name', 'Reference field name', 'Field label', and 'Observation'. The table contains two rows: 'VendTable' with 'CreditMax' and 'Credit limit', and 'VendTable' with 'CreditRating' and 'Credit rating'. The 'Activate' button is highlighted with a red box.

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

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

The screenshot shows the 'Sensitive data setup' page. The top navigation bar includes a back arrow, a menu icon, and buttons for '+ New', 'Delete', and 'Deactivate' (highlighted with a red box). The page title is 'Sensitive data condition setup'. Below the navigation bar, there is a search bar with 'Vendor' entered. The main content area shows the 'Sensitive data setup' form. The 'Name' field is 'VendorDataLogs', 'Created by' is 'abhadana', 'Created date and time' is '10/3/2024 08:08:20 AM', and 'Active status' is 'Active'. The 'Description' field is empty. The 'General' section has a table with columns 'Table name', 'Reference field name', 'Field label', and 'Observation'. The table contains two rows: 'VendTable' with 'CreditMax' and 'Credit limit', and 'VendTable' with 'CreditRating' and 'Credit rating'. The 'Deactivate' button is highlighted with a red box.

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

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



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

3.4 Version 10.0.40.44 Release

3.4.1 Organization assignment for security request

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

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

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

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

COMPANIES

SELECT ORGANIZATIONS

Assign organization

☐ Assign all organization

☒ Assigning specific organizations

Available organisation nodes:

Select organisation hierarchy

(All legal entities) ▾

Name	Company	↑	⋮
Contoso Entertainment System ...	USMF		
Contoso Group	GLCO		
Contoso Italy	ITCO		
Contoso Orange Juice	USP2		
Contoso Process Industry	USPI		
Contoso Retail	GLRT		

Company

Company accounts

⋮

We didn't find anything to show here.

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

3.4.2 Continuous user action logging

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

←

↺

Create snapshot

Refresh licenses

↺

Reset pins

Advanced view

Show joined

View accessed entry points

Export to Excel

⚙️

Options

🔍

Standard view ▾

Security explorer: full view

Pin users

User	Name
■	
■	
■	
■	
■	
■	
■	
■	
■	
■	

Pin role

Role name
■ AAC_Hotfixtest
■ abcde
■ Accountant
■ Accounting manager
■ Accounting supervisor
■ Accounts payable centralized pa...
■ Accounts payable clerk
■ Accounts payable manager
■ Accounts payable payments clerk

Pin duty

Duty name
■ A parameter that is used to gro...
■ Access benefit management wo...
■ Access benefits workspace
■ Access employee development ...
■ Access expense management w...
■ Access the leave and absence te...
■ Access workforce management ...
■ Access workforce management ...
■ Accounting manager (display)

Pin privilege

Privilege name
■ testpriv1
■ TestSoDAccess12
■ SCS_testexcludentry (tables)
■ SCS_testhotfix1 (display)
■ Sensitive Data Role (display)
■ SCS_testbug (action)
■ testprivreg
■ SCS_ABDemo_1812 (action)
■ SCS_rolewithpriv (display)

Pin entry point and permissions

Entry point (AOT name)	Type	Access right
■ AadWorkerIntegrationEntity	DataEntity	View
■ AadWorkerIntegrationEntity	DataEntity	Full control
■ AbatementCertificate_IN	Menu item display	Full control
■ AbatementPeriodicCertificate_IN	Menu item action	Create
■ AbatementPeriodicCertificate_IN	Menu item action	Full control
■ AbbreviationCodeImport_RU	Menu item action	Create
■ AbbreviationCodeImport_RU	Menu item action	Full control
■ AbbreviationsEntity	DataEntity	View
■ AbbreviationsEntity	DataEntity	Full control

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

View accessed entry points

☐ Show enabled users only

ID	Name	Enabled
SC0BA	SC0BA	false
		true
		true
		true
		false
		true
		true
		true
		true
		true
		true
		true
		true
		true
		true
		true
		true
		true
		true
		true
		true

Entry point (AOT name)	Type	Access right
AbbreviationsEntity	DataEntity	View
AbbreviationsEntity	DataEntity	Full control
AccountingDistCustFreeInvoice	Menu item display	View
AccountingDistCustInvJour	Menu item display	View
AccountingDistMarkupTransInv	Menu item display	View
AccountingDistMarkupTransInv	Menu item display	Full control
AccountingDistMarkupTransPO	Menu item display	View
AccountingDistMarkupTransReq	Menu item display	View
AccountingDistPurchReqTable	Menu item display	View
AccountingDistPurchTable	Menu item display	View
AccountingDistribution	Table	No access
AccountingDistributionOrderSu...	Menu item display	View
AccountingDistributions	Menu item display	View
AccountingDistributionsDocum...	Menu item display	View
AccountingDistTaxTransImp	Menu item display	View
AccountingDistTaxVendPackSlip...	Menu item display	View

Menu item name	Menu item label	Menu item type	Last accessed on
DSMUserAccessedEntryPointsL...	View accessed entry points	Display	7/2/2024 10:44:30 AM
DSMSecurityLicenseTypeExplor...	Security explorer	Display	7/2/2024 10:42:25 AM
DSMSecurityRequests	Security requests	Display	7/2/2024 10:42:19 AM
HcmTaskList		Display	7/2/2024 10:42:09 AM
DSMSecRequestSelectRoles	Add	Display	7/2/2024 6:53:33 AM
DewWorkflowTemplateListPage	Data entry workflow templates	Display	6/28/2024 11:27:01 AM
DQSDDataPolicy	Data policy	Display	6/28/2024 10:33:12 AM
DQSDDataPolicyListPage	Data quality policies	Display	6/28/2024 10:33:09 AM
DewWorkflowWizard	Workflow wizard	Display	6/28/2024 6:21:01 AM
DewWorkflowStepOpenPart	Open tasks assigned to me	Display	6/28/2024 6:20:53 AM
DewWorkflowTemplatePreview...	Data entry workflows	Display	6/28/2024 6:15:54 AM
DewWorkflowWorkspace	Data entry workflow workspace	Display	6/28/2024 6:15:53 AM
DewWorkflowWizardFieldCRDr...	Change request	Display	6/27/2024 10:50:00 AM
DewWorkflowTemplateNewVer...	Create new version	Display	6/27/2024 10:30:20 AM
DQSDParameters	Data quality studio parameters	Display	6/27/2024 8:52:50 AM
VendTableListPage	All vendors	Display	6/26/2024 9:39:00 AM

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

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

Reset filters

Clean up logs for entry points accessed

Options

Personalise

Personalise this page

Add to workspace

Page options

Security diagnostics

Advanced filter or sort

Record info

Share

Get a link

Create a custom alert

Manage my alerts

User continuous log

Standard view

ADDITIONAL INFO TO INCLUDE

User ID

Entry point

DATE RANGE

From date

To date

User ID	Menu item name	Menu item label	Menu item type	Last accessed on
pp	DQSDDataQualityPolicyLogCleanup	Clean-up logs	Action	7/4/2024 5:06:22 AM
pp	VendTableListPage	All vendors	Display	7/4/2024 5:06:35 AM
SainathR	DewWorkflowTemplateListPage	Data entry workflow templates	Display	7/4/2024 5:06:36 AM
pp	HcmTaskList		Display	7/4/2024 5:06:49 AM
Marius.Rusu	SysEmailHistory	Email history	Display	7/4/2024 8:05:19 AM

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



Clean up logs for entry points accessed

Parameters

Retention days

Run in the background

Recurrence Alerts

Batch processing
☒ No

Task description

Batch group

Private
☒ No

Critical Job
☒ No

Monitoring category

Start date: 7/4/2024 (11:46:00 am) (GMT) Coordinated Universal Time

OK

Cancel

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

3.5 Version 10.0.39.43 Release

3.5.1 User audit log for sensitive data

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

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

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

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

41

DEMO recording . | Standard view

Sensitive data setup

Name
DEMO recording .

Created by
Admin

Created date and time
4/2/2024 08:58:58 AM

Security record status
Open

Owner

Description

General

+ Add
Delete
Field picker

Table name	Reference field name	Field label	displayObservation
LogisticsLocation	Description	Name or description	
HcmWorkerTitle	OriginalHireDateTime	Original hire date	Table 'HcmWorkerTitle' is date effective or supports inheritance and
DirPerson	NameAlias	Search name	

Query

Edit query

Query name	Table name
DirPerson	DirPersonStaging

Users

+ Add
Delete

User ID	Name	networkAlias	networkDomain
fmihoc	fmihoc	fmihoc@to-increase.com	https://sts.windows.net/to-increase.com
icretu	icretu	icretu@toincrease.onmicrosoft.com	https://sts.windows.net/
Admin	Admin	fmihoc@toincrease.onmicrosoft.c...	https://sts.windows.net/

This page has three sections:

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

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



displayObservation

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

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

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

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

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

Standard view

Condition staging setup

	Main table	Staging table
	DirPartyTable	DirPartyTableAttachmentsStaging
<input checked="" type="checkbox"/>	DirPerson	DirPersonStaging
	DirPersonName	DirPersonNameHistoricalStaging
	LogisticsPostalAddress	LogisticsPostalAddressElectronicContactV2Staging

+ Add

Delete

Generate mapping

	Main table field	Staging table field
<input checked="" type="checkbox"/>	AnniversaryDay	AnniversaryDay
	AnniversaryMonth	AnniversaryMonth
	AnniversaryYear	AnniversaryYear
	BirthDay	BirthDay
	BirthMonth	BirthMonth
	BirthYear	BirthYear

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

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

After the mapping is completed the message from the Observation will be removed.

Now, when editing the fields from the Sensitive data setup will be capture under a log.

The new log can be seen opening the “Security and Compliance studio -> Inquiries -> Sensitive data log”.

Options

Sensitive data log

Standard view

DATE RANGE

From date 3/1/2023 To date 4/2/2024

ADDITIONAL FILTER OPTIONS

User ID Table name

Table label	Modified table	Description	Event created by	Sensitive data setup name	Event date
Addresses	LogisticsPostalAddress		Admin	Test from scratch	11/2/2023 12:44:54 PM
Position details	HcmPositionDetail		Admin	HCMPositionDetail	11/2/2023 12:44:37 PM
Customers	CustTable		Admin	Custtable - credit	11/2/2023 12:34:58 PM
Customers	CustTable		Admin	Custtable - credit	11/2/2023 12:15:53 PM
Customers	CustTable		Admin	Custtable - credit	11/2/2023 10:19:55 AM
Order lines	SalesLine		Admin	InventDim	10/30/2023 11:47:26 AM
Position details	HcmPositionDetail		Admin	HCMPositionDetail	10/30/2023 11:31:10 AM
Position details	HcmPositionDetail		Admin	HCMPositionDetail	10/26/2023 12:13:17 PM
Position details	HcmPositionDetail		Admin	Position - test	10/11/2023 7:03:43 AM
Addresses	LogisticsPostalAddress		Admin	Test worker address	10/10/2023 9:23:45 AM
Addresses	LogisticsPostalAddress		Admin	Test worker address	10/10/2023 9:23:31 AM
User Information	UserInfo		Admin	User data	8/10/2023 10:36:58 AM
User Information	UserInfo		Admin	User data	8/10/2023 10:36:40 AM
Vendors	VendTable		Admin	Vendor table	8/10/2023 10:31:55 AM
Global address book	DirPartyTable		Admin	Vendor table	8/10/2023 10:31:24 AM
User Information	UserInfo		Admin	User data	8/10/2023 10:12:12 AM
User Information	UserInfo		Admin	User data	8/10/2023 10:08:32 AM

DETAILS

Reference field name	Field label	Event type	Value from	Value to	Form name	Form label	Created date and time
Street	Street	Record modified	413 Oak Street TEST	413 Oak Street TDEMO1	LogisticsPostalAddress	Manage addresses	10/10/2023 9:23:31 AM

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

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

3.5.2 Securable tree view

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

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

My view 'v'

Securable tree view

Override permission on selected object

Security object types
Role
Value
Budget contributor

AOT name
BUDGETBUDGETCONTRIBUTOR
Description
Enters and approves budget plan requests

- Menu
- Accounts payable
- Accounts receivable
- Asset management
- Audit workbench
- Budgeting
- Cash and bank management
- Common
- Consolidations
- Cost accounting
- Cost management
- Credit and collections
- Demo data
- Expense management
- Fiscal books
- Fixed assets
- Fixed assets (Russia)
- Fleet management
- General ledger
- Allocations
- Calendars
- Chart of accounts
- Currencies
- Deferrals
- Deferrals setup
- Financial report setup
- Financial reporting setup
- Inquiries and reports
- Journal entries
- Journal setup
- Ledger setup
- Advance adjustment parameters
- Cash control configuration
- Cash position parameters
- Check voucher series
- Date intervals
- Financial reporting setup
- Fiscal calendars
- General ledger parameters
- INIC rates
- Ledger
- Ledger calendars
- Matrix report
- Period allocation categories
- Revenue automation

DETAILS

Explore

Name	AOT name	Description	Entry point type	Object name	Object type	Access right
General ledger parameters	LedgerParameters		Menu item display	LedgerParameters	Form	View

Security diagnostics

Show all access Explore

ObjectType	AOT name	Label	Access level	License type (on-premise)	License type (cloud)
Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor	View	Team members	Team members
Duty	BUDGETBUDGETPROCESSPOLICIESINQUIRE	Inquire into budget process policies	View	Team members	Team members
Privilege	LedgerParametersView	View general ledger parameters	View	Team members	Team members

Form level details

FORM MENU ITEMS

Explore

Control name	Control label	Control type	Object name from menu item	Object type from menu item
LedgerOppositeSignUpdate		FormBuildFunctionButtonControl	LedgerOppositeSignUpdate	Action
EximParameters_IN		FormBuildFunctionButtonControl	EximParameters_IN	Display

TABLE PERMISSIONS

Data source name	Control type	DataSourceTable
LedgerParameters	Data source	LedgerParameters
TaxParameters	Data source	TaxParameters
NumberSequenceReference	Data source	NumberSequenceReference
AssetParameters	Data source	AssetParameters
InventDimSetupGrid	Data source	InventDimSetupGrid
CustParameters	Data source	CustParameters

FORM CONTROLS

Control name	Control type	Object name from menu item	Object type from menu item	Needed permissions
UpdateDelimiter	FormBuildFunctionButtonControl	DimensionSegmentSeparatorDataUpdate...	Action	Manual

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

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

This page contains the following section:

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

Object type	AOT name	Label	Access level
Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor	View
Duty	BUDGETBUDGETPROCESSPOLICIESINQUIRE	Inquire into budget process policies	View
Privilege	LedgerParametersView	View general ledger parameters	View

Object type	AOT name	Label	Access level
Role	AUDITPOLICYMANAGER	Auditor	View
Role	BUDGETBUDGETCLERK	Budget clerk	View
Role	BUDGETBUDGETCONTRIBUTOR	Budget contributor	View
Role	BUDGETBUDGETMANAGER	Budget manager	View
Role	COMPANYCHIEFFINANCIALOFFICER	Chief financial officer	View
Role	INVENTCOSTACCOUNTANT	Inventory accountant	View

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

- **Form level details:** This section it’s divided into three grids as follows:
 - a) **Form menu items:** if the selected entry point (from Details grid) is form type it will display all the other menu items that are found on the form’s level.
On form level there are multiple options/buttons that are opening other forms. Here these forms are displayed so you will know that if you want to provide full access to a form you need to provide access to the forms that are opening from the buttons available on that form.
 - b) **Table permissions:** it will display all the tables behind the datasources of the selected entry point on the Details grid.
 - c) **Form Controls:** some form control require ‘manual permission’ that is set on the form’s properties by the developer/Microsoft. These controls require the specific access in order to access them.

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

Name	AOT name	Description	Entry point type	Object name	Object type	Access right
General ledger parameters	LedgerParameters	Menu item display	Form	LedgerParameters	Form	Full control

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



Standard view

Override permissions on roles

Select roles to assign override permissions to

<input type="radio"/> ObjectType	Label	AOT name	
<input checked="" type="radio"/> Role	Budget contributor	LedgerParameters	

<input type="radio"/> AOT name	Name	Entry point type	Access right
<input checked="" type="radio"/> LedgerParameters	General ledger p...	Menu item display	Full control

OKCancel

3.5.3 Security request history track

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

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

The new column will display the name of the 'Security Request' if the audit trails was generated by one.

A new button was added, and it will be enabled when a record with 'Security request' has been selected.

Audit

Security history

Audit log report

Open security request history

More

Filter

Event date and time	Event created by	Event type	Company	Description	Security request reference
3/13/2024 12:03:05 PM	Admin	Duty created	*	Duty DutyUniqueProjectTest1 created	
3/13/2024 12:03:04 PM	Admin	Role created	*	Role RoleUniqueProjTest1 created	
3/12/2024 10:53:41 AM	Admin	Role modified	*	Role Purchasing agent modified	
3/12/2024 10:53:41 AM	Admin	Duty modified	*	Duty Approve request for quotations modified	
3/11/2024 1:02:57 PM	Admin	Role unlocked	*	Role Warehouse worker unlocked	Unlock role
3/11/2024 1:02:57 PM	Admin	Stand-in rule created	*	Stand-in rule for user "I" has been created	Add stand-in
3/11/2024 1:02:45 PM	Admin	Stand-in rule deleted	*	Stand-in rule for user 'Lola' has been deleted	Cancel stand-in
3/11/2024 1:01:58 PM	Admin	Duty modified	*	Duty Inquire into vendor master was modified from Override permissions on roles	Modify role
3/11/2024 1:01:58 PM	Admin	Duty modified	*	Duty Maintain vendor invoices was modified from Override permissions on roles	Modify role
3/11/2024 1:01:57 PM	Admin	Duty modified	*	Duty Maintain product receipt was modified from Override permissions on roles	Modify role
3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty Inquire into voyage costs was modified from Override permissions on roles	Modify role
3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_CostedProcessDuty was modified from Override permissions on roles	Modify role
3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_DocReceivedProcessDuty was modified from Override permissions on roles	Modify role
3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_InTransitProcessDuty was modified from Override permissions on roles	Modify role
3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdate_ReadyForCostingProcessDuty was modified from Override permissions on roles	Modify role
3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty ITMUpdateFolio_DocReceivedProcessDuty was modified from Override permissions on roles	Modify role
3/11/2024 1:01:56 PM	Admin	Duty modified	*	Duty Maintain cost estimates was modified from Override permissions on roles	Modify role

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

Duty modified : Duty Inquire into vendor master was modified | Standard view

Security request history

Open request details

Request	Area	Created date and time	End date	Owner	Security record status	Scenario	Description
Modify role		4/3/2024 07:14:10 AM		Admin	Completed		
Type	Created by	Start date	Origin	Priority	Modified by		
Modify role	Admin		User requests	Normal	Admin		

Open workflow approval details

Instance ID	Workflow ID	Status	Document	Document type	Workflow	Version	Submitting user	Company accounts ID
000001	000014	Completed	Quotation: QN000000002_City...	Sales quotation	Review project quotations	1.0.0.0	JUNE	user

Context	Action	Name	Message	Comment	Created date and time	User
Workflow	Submission	000001: Quotation: QN00...	Submitted by: JUNE		1/1/2016 8:35:13 PM	JUNE
Workflow	Creation	000001: Quotation: QN00...	Workflow 000014	PSAProjectQuotationTemplate	1/1/2016 8:35:29 PM	JUNE
Approval	Creation	Project Quotation Approv...			1/1/2016 8:35:34 PM	JUNE
Approval	Auto complete condition ...	Project Quotation Approv...	Auto-completion condition: Project		1/1/2016 8:35:42 PM	JUNE
Approval	Completion	Project Quotation Approv...			1/1/2016 8:35:44 PM	JUNE
Workflow	Completion	000001: Quotation: QN00...			1/1/2016 8:35:49 PM	JUNE

Audit log details

Event date and time	Description	Event type	Reference	Company	Event created by
3/11/2024 1:01:46 PM	Duty Landed cost agent (display) was created from Over...	Duty created	0 *	Admin	Admin
3/11/2024 1:01:53 PM	Privilege Landed cost agent (display) was created from Ov...	Privilege created	0 *	Admin	Admin
3/11/2024 1:01:54 PM	Role Landed cost agent was modified from Override perm...	Role modified	0 *	Admin	Admin
3/11/2024 1:01:54 PM	Duty Landed cost agent (display) was created from Over...	Duty created	0 *	Admin	Admin
3/11/2024 1:01:54 PM	Duty Inquire into products for operations master was mod...	Duty modified	0 *	Admin	Admin
3/11/2024 1:01:55 PM	Duty Maintain receipt operations was modified from Over...	Duty modified	0 *	Admin	Admin

Reference description	Name	Reference type	Reference table type
Duty Landed cost agent (display) wa...	Landed cost agent (display)	Duty	Duty

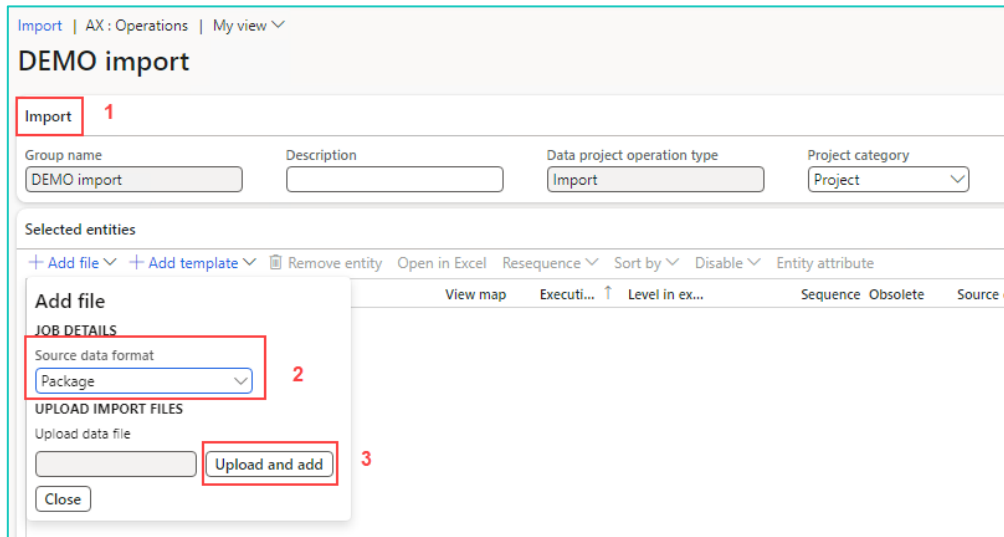
Of course, for in deep analysis options like ‘Open request details’ and ‘Open workflow approval details’ are available.

3.5.4 Enhanced SoD predefined list

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

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

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



Import | AX : Operations | My view

DEMO import

Import 1

Group name: DEMO import Description: Data project operation type: Import Project category: Project

Selected entities

+ Add file + Add template Remove entity Open in Excel Resequence Sort by Disable Entity attribute

Add file

JOB DETAILS

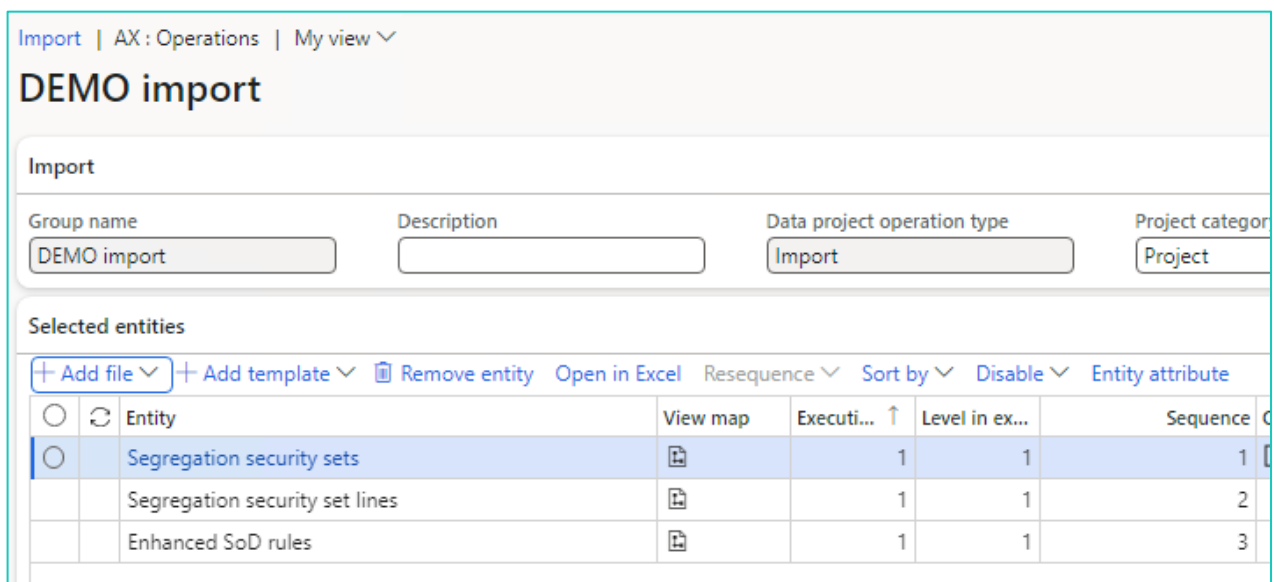
Source data format: Package 2

UPLOAD IMPORT FILES

Upload data file: Upload and add 3

Close

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



Import | AX : Operations | My view

DEMO import

Import

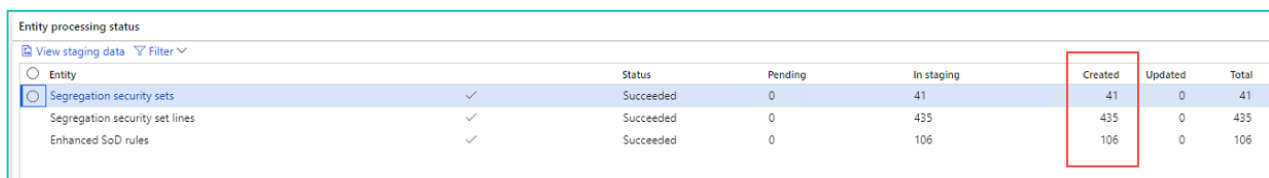
Group name: DEMO import Description: Data project operation type: Import Project category: Project

Selected entities

+ Add file + Add template Remove entity Open in Excel Resequence Sort by Disable Entity attribute

	Entity	View map	Executi...	Level in ex...	Sequence
<input type="radio"/>	Segregation security sets		1	1	1
<input type="radio"/>	Segregation security set lines		1	1	2
<input type="radio"/>	Enhanced SoD rules		1	1	3

Import the file and the result should look like this:



Entity processing status

View staging data Filter

	Status	Pending	In staging	Created	Updated	Total
<input type="radio"/> Entity						
<input checked="" type="radio"/> Segregation security sets	Succeeded	0	41	41	0	41
Segregation security set lines	Succeeded	0	435	435	0	435
Enhanced SoD rules	Succeeded	0	106	106	0	106

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

The rules should be 106.

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



3.6 Version 10.0.37.42 and Older

3.6.1 Segregation of duties sets

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

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

Securable object	Securable object type	Access level
Accountant_BR	Menu item display	View
ACJournalPost_BR	Menu item action	View
AdvanceAdjustmentPara...	Menu item display	Full control
AssetChangeGroup	Menu item action	Correction

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

Name	Type	First	First securable object type	First access level
Demo Sod rules sets	Segregation security sets	Tralaalalal		No access

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

Name	Type	Effective from	Effective to	Enabled
test	Segregation security sets	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test4	Entry point	6/29/2023 10:46:24 AM	12/31/2154 11:59:59 PM	✓
testsodentry	Entry point	6/7/2023 10:01:46 AM	12/31/2154 11:59:59 PM	✓
testsodpriv	Privilege	6/7/2023 9:59:38 AM	12/31/2154 11:59:59 PM	✓

Name	Type	Effective from	Effective to	Enabled
test	Segregation security sets	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test_01	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test_02	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test_03	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test_04	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test_05	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test_06	Entry point	7/26/2023 7:09:36 AM	12/31/2154 11:59:59 PM	✓
test4	Entry point	6/29/2023 10:46:24 AM	12/31/2154 11:59:59 PM	✓
testsodentry	Entry point	6/7/2023 10:01:46 AM	12/31/2154 11:59:59 PM	✓
testsodpriv	Privilege	6/7/2023 9:59:38 AM	12/31/2154 11:59:59 PM	✓

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

3.6.2 Security requests enhancements and workflow

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

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

I. Security requests enhancements:

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

Status	Owner	Request
Demo SR 1	Inactive workflow	

Status	Owner	Request
Demo SR 1	Active workflow	

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

Status
Open
Waiting
Review
Approved
Rejected
Canceled

Security types

a) General

The 'general' security type is used for requests that cannot be handled by the defined types below and cannot be an automated process, but rather an action that some supervisor user



needs to do ‘manually’. The request will be created and the details field will be used to describe the request.

Security requests | My view

Demo SR 1

General

Request

Demo SR 1

Type

General

Origin

User requests

Area

WHS

Status

Priority

Normal

Status

Open

Owner

Admin

Description

b) Create user

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

Security requests | My view

Demo SR 1

General

Request

Demo SR 1

Type

Create user

Origin

User requests

Area

WHS

Status

Priority

Normal

Status

Open

Owner

Admin

Create users

User ID

newUser1

User name

newUser1

Email

newUser1@to-increase.com

Company

DAT

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

Request: Demo SR 1 | Type: Assign role to user | Origin: User requests

Status: Priority: Normal | Status: Open | Owner: Admin

Assign roles to user

USER

User ID: Admin | User name: Admin | Email: fmihoc@toincrease.onmicos... | 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.onmicos... | 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

	User ID	User name
<input checked="" type="radio"/>	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

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

Description

g) Delete user

A new tab will be made visible and in this tab the option of deleting 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 checked="" type="radio"/>	CASSIE	CASSIE	CASSIE@contosoax7.onm...
<input type="radio"/>	cdsaurorauruser	Aurorauser...	Aurorauser01@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

[Upload task recording](#)

Role name: SCS_DemoRole1 Description: Demo purposes Scenario: skRecordingForCSReplicate.xtr

SCENARIO DETAILS

	Step number	Securable object	Securable type	Access level	Description	File name	Child scenario	Remark
<input checked="" type="radio"/>	1	salestablelistpage	Display	Full control	Go to Accounts receivabl...	TaskRecordingForCSRepli...		
<input type="radio"/>	2	DefaultDashboard	Display	Full control	Close the page.	TaskRecordingForCSRepli...		Additional securable object found in the task recording
<input type="radio"/>	5	salestablelistpage	Display	Full control	Go to All sales orders.	TaskRecordingForCSRepli...		
<input type="radio"/>	7	SalesTableDetails	Display	Full control	In the list, click the link in ...	TaskRecordingForCSRepli...		Additional securable object found in the task recording
<input type="radio"/>	9	SalesLineCopy	Display	Full control	Click From line.	TaskRecordingForCSRepli...		
<input type="radio"/>	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...	Demo1x recording.axtr		
3	SalesTableDetails	Display	Full control	In the list, click the link in the selected r...	Demo1x recording.axtr		Additional securable object found in the task recording
5	SalesCopyAllLines	Display	Full control	Click From all.	Demo1x recording.axtr		
8	InventReserve	Display	Full control	Click Reservation.	Demo1x recording.axtr		
10	MCROrderNotes	Display	Full control	Click Notes.	Demo1x recording.axtr		
13	InventTransferOrderCreat...	Action	Full control	Click Transfer order.	Demo1x 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

Description

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

+ Add | Remove

<input type="radio"/>	<input type="radio"/>	Role name	Name
<input checked="" type="radio"/>	<input type="radio"/>	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

Add role | Remove

<input type="radio"/>	<input type="radio"/>	Role name	Description	Role AOT name
<input type="radio"/>	<input type="radio"/>	SCS_RoleTest_2		6DEC7811-E0C5-42C5-94...
<input type="radio"/>	<input type="radio"/>	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
<input checked="" type="radio"/>	Create demo rule 2 from ...	Entry point	AdvancedLedger...	Menu item display	Create	BankChequeCompany...	Menu item display	Full control	4/28/2022 10:43:44...	12/31/2154 11:59:5...	<input checked="" type="checkbox"/>
<input type="radio"/>	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

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

	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="radio"/>	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	DSMAuditClassification	Menu item display	View
<input type="radio"/>	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.

The screenshot shows the 'Security requests' interface for 'Demo SR 1'. The 'General' section includes fields for Request (Demo SR 1), Type (Add stand-in), Origin (User requests), and Area (WHS). The 'Status' section shows Priority (Normal), Status (Open), and Owner (Admin). A 'Create stand-in' table is highlighted with a blue border, containing one row with User ID 'Admin', Stand-in 'ALICIA', From date '4/28/2022', To date '4/30/2022', and Copy assigned organizations checked. Below the table is a 'Description' field.

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

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.

The screenshot shows the 'Security requests' interface for 'Demo SR 1'. The 'General' section includes fields for Request (Demo SR 1), Type (Cancel stand-in), Origin (User requests), and Area (WHS). The 'Status' section shows Priority (Normal), Status (Open), and Owner (Admin). A 'Remove stand-in' table is highlighted with a blue border, containing one row with User ID 'Admin', Stand-in 'ALICIA', From date '4/28/2022', To date '4/30/2022', and Copy assigned organizations unchecked. Below the table is a 'Description' field.

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

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
<input checked="" type="checkbox"/>	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.

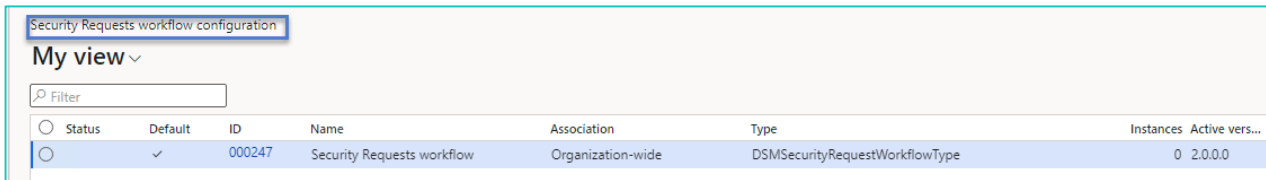
Switching type from 'AssignUserRole' will remove all data specific to it. Are you sure want to continue?

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.



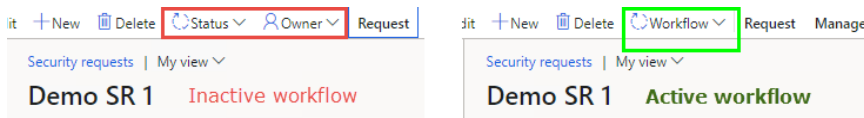
Security Requests workflow configuration

My view ▾

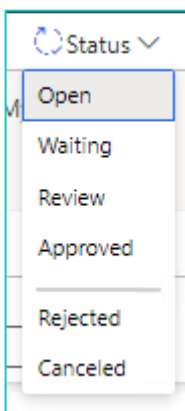
Filter

Status	Default	ID	Name	Association	Type	Instances	Active vers...
○	✓	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:

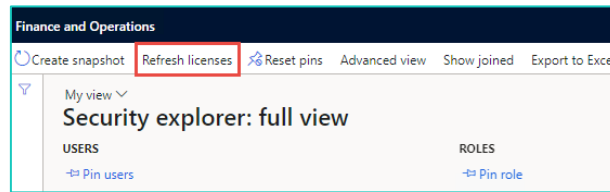
- Approve – set the status to **Approved** and the request will be automatically created.
- Reject – set the status to **Reject** and decline the request.
- Require more information from the user and set the status to **Rejected** or back to **Open**.

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.



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

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

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 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.

3.6.3 Export security explorer objects to excel in a de-normalized format

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

Create snapshot Reset pins Advanced view Show joined Export to Excel OPTIONS

Security explorer: full view

USERS		ACCOUNTANT	DUTIES	PRIVILEGES	ENTRY POINTS
Pin users		Unpin role	Pin duty	Pin privilege	Pin entry point
User ID	Name	Role name	Duty name	Privilege name	Entry point (AOT name)
OSCAR	OSCAR	Accountant	Configure electronic fiscal document	@ApplicationSuite_LocalizationRTax25RegisterProfitEntityMaintain	AbatementCertificate_IN
RetailServiceAccount	RetailService	Accounting manager	Enable bank management process	@ApplicationSuite_LocalizationRTax25RegisterProfitEntityView	AbatementPeriodicCertificate_IN
STAN	STAN	Accounting supervisor	Enable electronic document exchange	Account number enhanced preview	Accountant_BR
		Accounts payable centralize	Enable escheatment processing for stale-dated accounts payable payments	account reference -ViewLedgerShowReferences:	Accountant_BR
		Accounts payable clerk	Enable EU sales list process	AccountingSourceExplorerView	AccountantElectronicAddressEdit
		Accounts payable manager	Enable financial reports generator	Action class settings maintain	AccountantElectronicAddressEdit
		Accounts payable payments	Enable fixed assets process	Action class settings view	AccountantElectronicAddressEdit
		Accounts payable positive	Enable Intrastat process	Action populate records task maintain	AccountantElectronicAddressEdit
			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	

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

3.6.4 Merge security scenarios and match role

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

Finance and Operations Preview Search for a page

Security and compliance studio

Summary: 99 Users, 156 Roles

Security: Requests, Scenarios, Users, Roles

Actions: + New, Edit, Match roles, More, Merge scenarios

Scenario	Owner	Description	Objects	Created date and time
✓ Create customer	nsadaiya		5	6/28/2019 09:13:17 AM
✓ Create purchase order and sales order	nsadaiya		5	7/16/2019 05:52:37 AM
Edit access to Audit workbench area	nsadaiya		2	7/2/2019 06:00:43 AM
Merged Customer-SO-PO Scenario	vsingh	Merged scenarios to reflect rece...	5	7/29/2019 06:38:24 AM
Merged scenario	nsadaiya	Merged from create customer a...	6	7/2/2019 08:46:07 AM

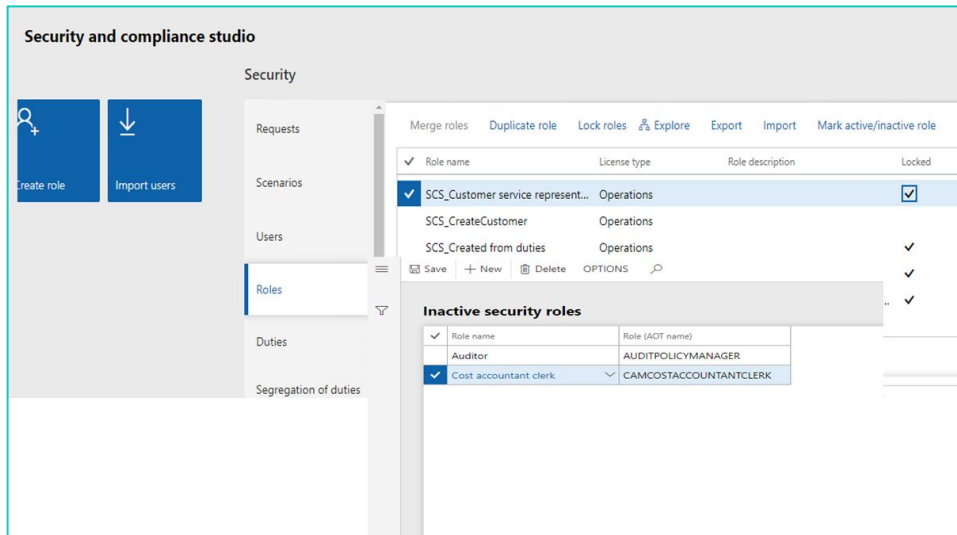
Merge scenarios into one

Name:

Description:

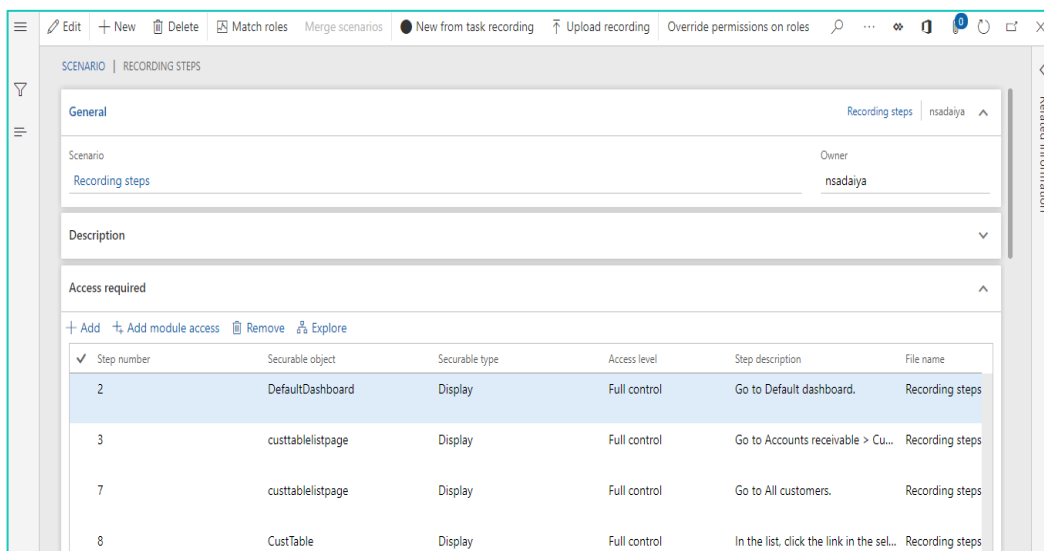
3.6.5 Mark any Security Role as Active/Inactive

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



3.6.6 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.

3.6.7 Override permission based on scenarios

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

SCENARIO

General

Merged scenario | nsadaiya

Scenario: Merged scenario | Owner: nsadaiya

Description

Access required

+ Add + Add module access - Remove - Explore

Step number	Securable object	Securable type	Access level	Step description	File name
-	AssetTableNew	Display	No access		
-	DSMArea	Display	Edit		

Assign override permissions to roles

Accounts receivable centralized ...	Documents accounts receivable ...
Accounts receivable clerk	Documents customer invoice ev...
Accounts receivable manager	Reviews customer invoice proce...
Accounts receivable payments c...	Documents accounts receivable ...
Applicant anonymous (external)	External user application for em...
Auditor	Manages and reviews audit poli...
Batch job manager	Maintain and configure settings...

Set custom permissions
No ☒

PERMISSIONS

Read
☒ Unset ☐ Grant ☐ Deny

Update
☒ Unset ☐ Grant ☐ Deny

Create
☒ Unset ☐ Grant ☐ Deny

Delete
☒ Unset ☐ Grant ☐ Deny

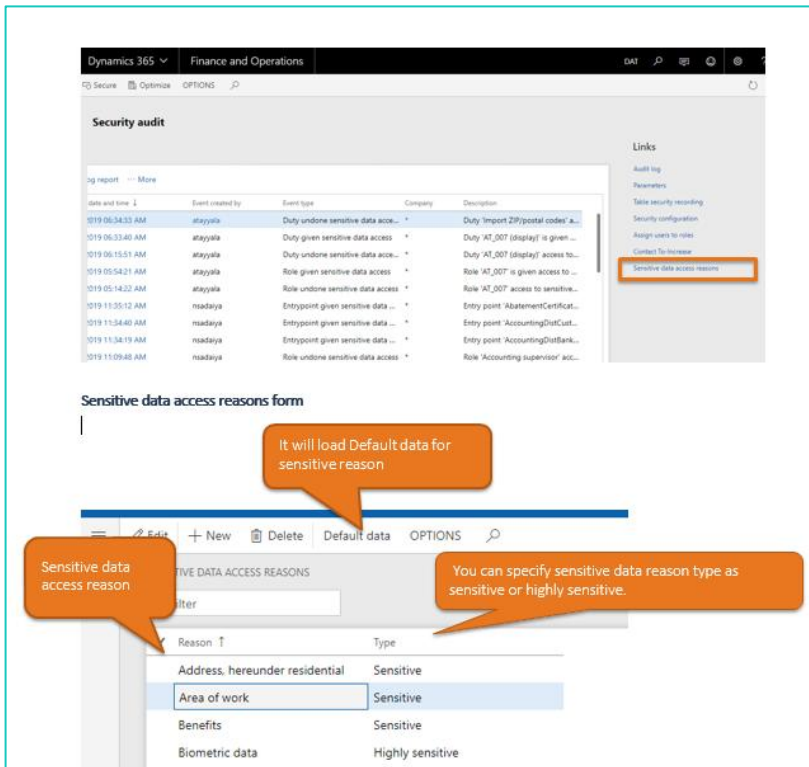
OK Cancel

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

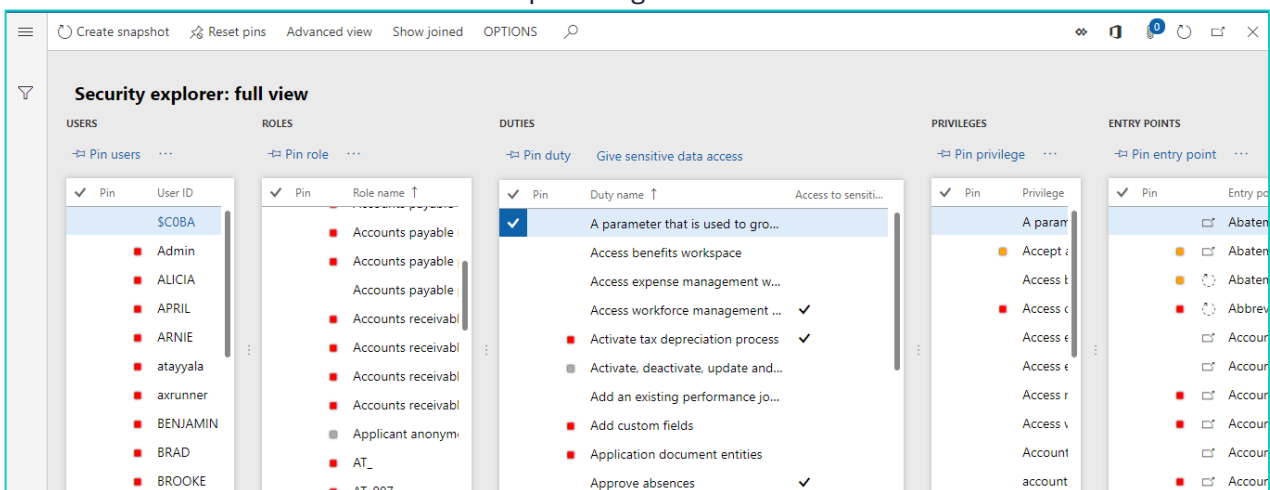
Specific definition of sensitive data might be different for different industries or countries. An organization can define specific definition for sensitive data as per their industry, country and policies. For some organizations, sensitive data might be any data that is related to finance, human resource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

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

- **Set up sensitive data access reasons**



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



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

- **Undo access to sensitive data** - You can unset sensitive data access to a securable object. If you unset sensitive data access to a securable object, then automatically all securable objects which are related to it lose access to sensitive data.
- **Sensitive data access inheritance-** Please refer to the Product Documentation for more details on this topic.

- **Use of sensitive data access** - Once an organization define sensitive data access to securable objects, we can use this information while creating, locking and matching roles.
 - Create Role Wizard - When you are creating a new role using create role wizard. It is important to know that whether newly created role will have access to sensitive data.

CREATE ROLE

All privileges

Select the privileges to be added to the new role

AVAILABLE PRIVILEGES	SELECTED PRIVILEGES
Privilege	Privilege
<input checked="" type="checkbox"/> View accountant information	<input checked="" type="checkbox"/> Import KLADR abbreviations
<input type="checkbox"/> View accounting distributions in...	<input type="checkbox"/> Maintain accountant information
<input type="checkbox"/> Maintain accounting distributio...	<input type="checkbox"/> Maintain accounting distributio...
<input type="checkbox"/> View accounting distributions in...	
<input type="checkbox"/> View accounting distributions in...	
<input type="checkbox"/> Create distributions for the tran...	
<input type="checkbox"/> View distributions for the transa...	
<input type="checkbox"/> Create distributions for the tran...	
<input type="checkbox"/> View distributions for the transa...	
<input type="checkbox"/> Create distributions for the tran...	

Privileges having sensitive data access

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

Locked security roles

Role name	Role (AOT name)
<input checked="" type="radio"/> Business events security role	BUSINESSEVENTSSECURITYROLE
<input type="radio"/> Accountant	LEDGERACCOUNTANT
<input type="radio"/> Accounts payable payments clerk	PAYMACCOUNTSPAYABLEPAYM...
<input type="radio"/> Accounts payable positive payment clerk	PAYMPOSITIVEPAYMENTCLERK

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

Dynamics 365 Finance and Operations Accounts receivable > Customers > All customers

MATCH ROLES AND SENSITIVE DATA ACCESS

Match roles

Menu item display	DSMSscenario	Full control	No access	Not part of the selected role.
Menu item display	DSMSecurityManagementTie	Full control	No access	Not part of the selected role.
✓ Menu item display	CureTabletKitPage	Full control	View	✓
Menu item display	ForecastSalesTable	Full control	No access	Not part of the selected role.

Roles

Role name	Role description	Matc...	User license type	Remaining user ...
Project manager	Documents the project forecast/...	50.00	Operations	59928
Production planner	Schedules and plans productions	50.00	Operations	59928
Sales manager	Reviews sales process performa...	50.00	Operations	59928
✓ Sales representative	Documents sales events and res...	25.00	Activity users	29906
Materials manager	Enables and reviews processes...	25.00	Operations	59928

Duties that give access to the securable objects that cannot be accessed with the selected role.

Duty name	Privilege name	Securable object type	Securable object	Access level	Duty license type
Enable the demand forecasting ...	Maintain demand forecasts for i...	Menu item display	ForecastSalesTable	Full control	Operations
Maintain project budgets	View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Activity users
Maintain project forecasts	Maintain demand forecasts for i...	Menu item display	ForecastSalesTable	Full control	Activity users
Inquire into project forecast stat...	View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Team members
Maintain authorization of adjust...	View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Operations
Maintain authorization of adjust...	Maintain demand forecasts for i...	Menu item display	ForecastSalesTable	Full control	Operations

Privileges that give access to the securable objects that cannot be accessed with the selected role.

Privilege name	Securable object type	Securable object	Access level	Privilege license type	Menu item license type
View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Team members	Team members
Maintain demand forecasts for i...	Menu item display	ForecastSalesTable	Full control	Activity users	Activity users

Matched duties

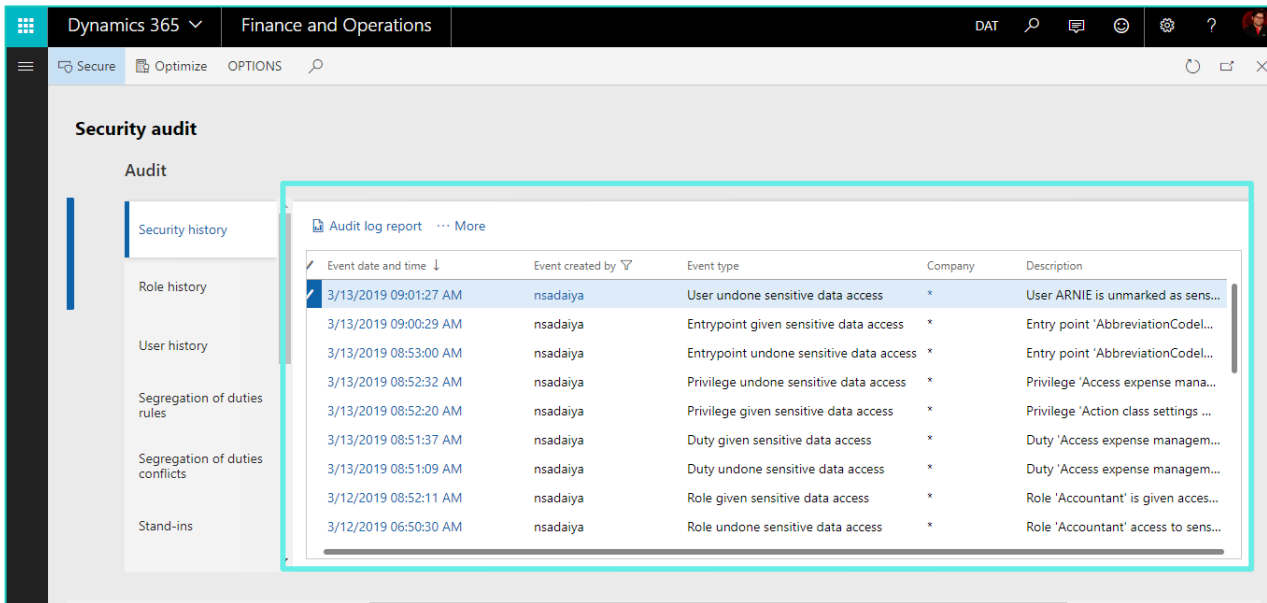
Duty name	Privilege name	Securable object type	Securable object	Access level	Duty license type
Inquire into demand forecasts	View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Operations
Enable the demand forecasting ...	Maintain demand forecasts for i...	Menu item display	ForecastSalesTable	Full control	Operations
Maintain project budgets	View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Activity users
Maintain project forecasts	Maintain demand forecasts for i...	Menu item display	ForecastSalesTable	Full control	Activity users
Inquire into project forecast stat...	View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Team members
Maintain authorization of adjust...	View demand forecasts for item ...	Menu item display	ForecastSalesTable	View	Operations

- 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.



Security audit

Audit

Security history

Role history

User history

Segregation of duties rules

Segregation of duties conflicts

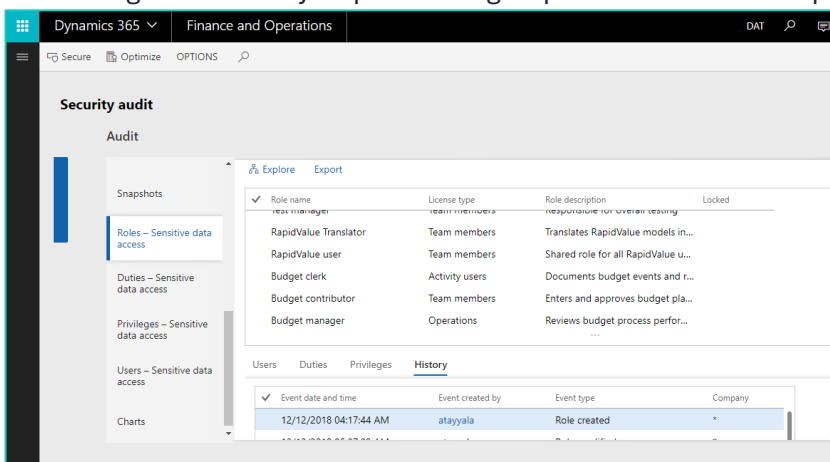
Stand-ins

Audit log report ... More

Event date and time ↓	Event created by	Event type	Company	Description
3/13/2019 09:01:27 AM	nsadaiya	User undone sensitive data access	*	User ARNIE is unmarked as sens...
3/13/2019 09:00:29 AM	nsadaiya	Entrypoint given sensitive data access	*	Entry point 'AbbreviationCodel...
3/13/2019 08:53:00 AM	nsadaiya	Entrypoint undone sensitive data access	*	Entry point 'AbbreviationCodel...
3/13/2019 08:52:32 AM	nsadaiya	Privilege undone sensitive data access	*	Privilege 'Access expense mana...
3/13/2019 08:52:20 AM	nsadaiya	Privilege given sensitive data access	*	Privilege 'Action class settings ...
3/13/2019 08:51:37 AM	nsadaiya	Duty given sensitive data access	*	Duty 'Access expense managem...
3/13/2019 08:51:09 AM	nsadaiya	Duty undone sensitive data access	*	Duty 'Access expense managem...
3/12/2019 08:52:11 AM	nsadaiya	Role given sensitive data access	*	Role 'Accountant' is given acces...
3/12/2019 06:50:30 AM	nsadaiya	Role undone sensitive data access	*	Role 'Accountant' access to sens...

- 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.



Security audit

Audit

Explore Export

Role name License type Role description Locked

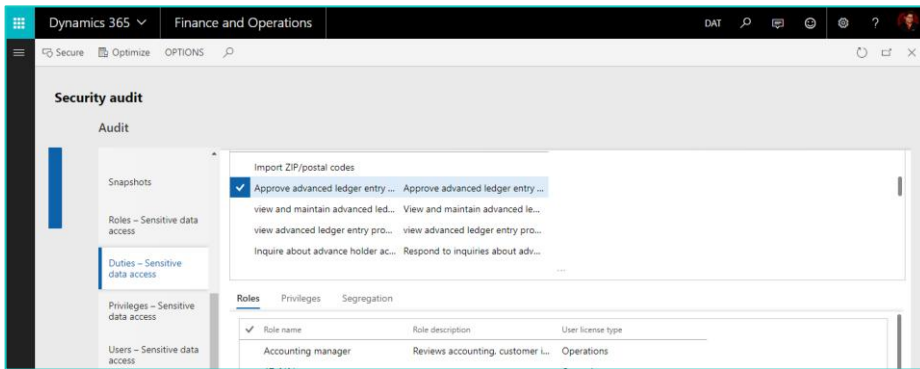
✓ RapidValue Translator	Team members	Translates RapidValue models in...	
RapidValue user	Team members	Shared role for all RapidValue u...	
Budget clerk	Activity users	Documents budget events and r...	
Budget contributor	Team members	Enters and approves budget pla...	
Budget manager	Operations	Reviews budget process perfor...	

Users Duties Privileges **History**

Event date and time	Event created by	Event type	Company
12/12/2018 04:17:44 AM	atayyala	Role created	*

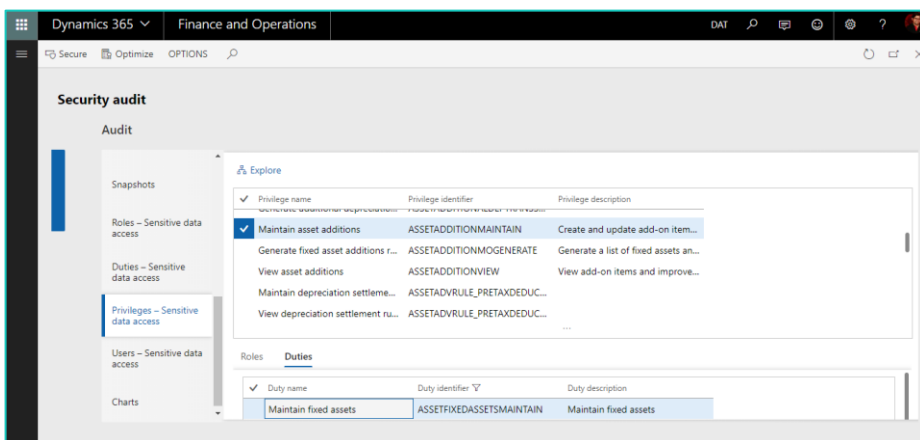
- Duties - Sensitive data access

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.



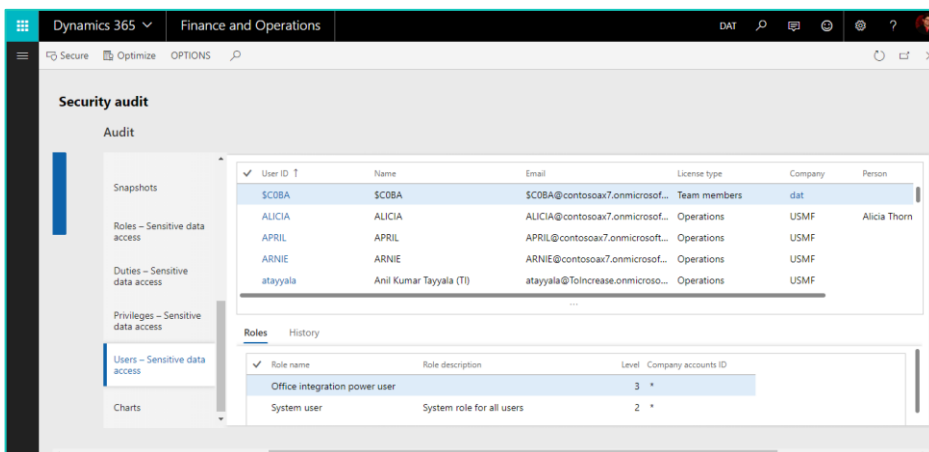
- Privileges - Sensitive data access

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 user history which contained changed events of the user.



- Charts

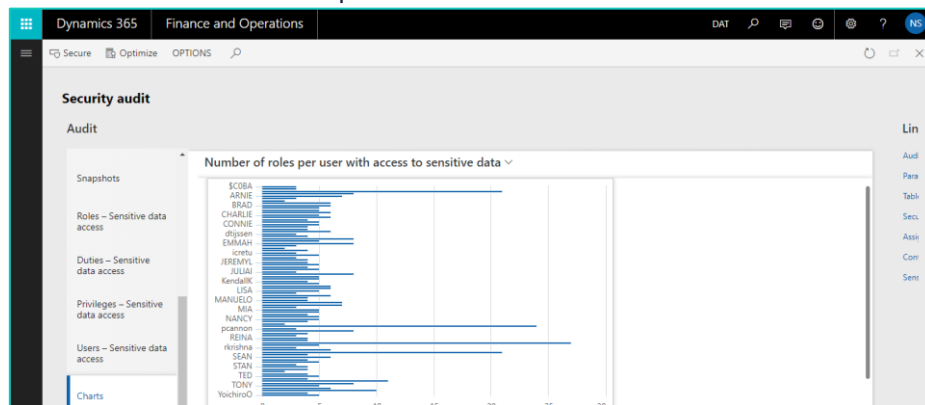
- Number of security objects with access to sensitive data



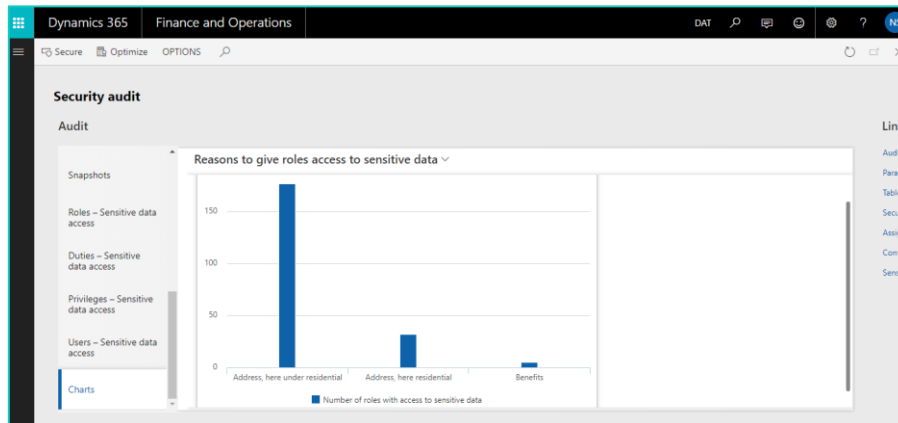
- Number of users with access to sensitive data per organization



- Number of roles per user with access to sensitive data



- 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.

PERSON SEARCH REPORT

Person search report

- Contact search results (0)
- Worker search results (0)
- Applicant search results (0)
- Application basket search results (0)
- Prospect search results (0)
- Prospective vendor search results (0)
- Driver search results (0)
- Security and compliance studio results (4)

Here number 4 denotes the number of records present in SCS, which are related to user id specified while searching 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)

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

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

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

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.

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

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

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

Select one or more privileges on the *Matched Privileges* grid.

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

Click on the Create Duty button as shown below.

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

Enter the new duty name and the description.

Create duty

Parameters

Duty name

SCS

Description

Security objects that are included into the new duty

Filter

Object type	Label
Privilege	Accountant_reduced (display)
Privilege	Maintain retail vendors

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

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

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

Notes:

- See comments column for additional info when relevant.



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

3.6.11 Option to compare Security Snapshots stored in the security setup

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

The screenshot shows the D365 FOE navigation pane with the following structure:

- General ledger
- Human resources
- Inventory management
- Master planning
- Organization administration
- Payroll
- Procurement and sourcing
- Product information management
- Production control
- Project management and accounting
- Questionnaire
- Retail
- Sales and marketing
- Security and compliance** (highlighted with a red box)
- Service management

Under the 'Security and compliance' section, the 'Inquiries' sub-section is expanded, showing the following options:

- Security explorer
- Security audit report
- Audit log
- User log
- Snapshot comparison** (highlighted with a red box and a callout bubble pointing to it with the text 'Snapshot comparison feature')

Below the 'Inquiries' section, the 'Periodic tasks' sub-section is also visible, containing options like 'Create role from duties/privileges', 'Create scenario from module', 'Initialize Security and compliance IT audit', 'Apply Active Directory user status', 'Add table permissions to role or privilege', and 'Assign stand-in roles'.

Fig 1. Snapshot comparison path

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

Snapshot comparison

FILTER
Select security object type

☐ Entry Point

☒ Privilege

☐ Duty

☐ Role

☐ User

COMPARE SNAPSHOTS

First snapshot: 2

Second snapshot: 3

Name	User license type	Compared	Observation
Action graph	Operations	Yes	3 modifications found
DSMAreaEntityMaintain	None	Yes	1 modifications found
Florin privilege 2	None	Yes	0 modifications found

Name	User license type
Demo privilege 1	Operations
Demo privilege 2	Operations
Maintain bar codes	Operations

DIFFERENCES

Property	Value from first snapshot	Value from second snapshot
Entry point added	-	DSMAuditLogInit
Entry point added	-	DSMMergeRoles
Entry point added	-	DSMStandInClass

Fig 2. Snapshot comparison form

Legend:

1. COMPARE button group – contains two buttons:

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

2. VIEW button group – contains three buttons:

a) Show changes only:

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

COMPARISON

Compare selected
Full compare

VIEW

Show all objects
Advanced view

Snapshot comparison

FILTER

Select security object type

☐ Entry Point

☒ Privilege

☐ Duty

☐ Role

☐ User

COMPARE SNAPSHOTS

First snapshot: 2

Second snapshot: 3

Name	User license type	Compared	Observation
Action graph	Operations	Yes	3 modifications found
DSMAreaEntityMaintain	None	Yes	1 modifications found
Florin privilege 2	None	Yes	0 modifications found

Name	User license type
Demo privilege 1	Operations
Demo privilege 2	Operations
Maintain bar codes	Operations

Fig. 3 See a list of the modified objects

b) Show all objects:

- when clicked will display all the objects from both of the selected snapshots
- label will be changed to “Show changes only” (see Fig. 4)

COMPARISON

Compare selected
Full compare

VIEW

Show changes only
Advanced view

Snapshot comparison

FILTER

Select security object type

☐ Entry Point

☒ Privilege

☐ Duty

☐ Role

☐ User

COMPARE SNAPSHOTS

First snapshot: 2

Second snapshot: 3

Name	User license type	Compared	Observation
Action class settings maintain	None	Yes	0 modifications found
Action class settings view	None	Yes	0 modifications found
Action graph	Operations	Yes	3 modifications found
Action populate records task maint...	None	Yes	0 modifications found
Activate BOM versions	Operations	Yes	0 modifications found
Activate cost category price	Operations	Yes	0 modifications found
Activate costing prices	Operations	Yes	0 modifications found

Name	User license type
Delete write-off factors	Operations
Demand Forecasting external API se...	None
Demo privilege 1	Operations
Demo privilege 2	Operations
DemoDataPostEntityMaintain	None
DemoDataPostEntityView	None
DemoDataPostMaintain	None

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)

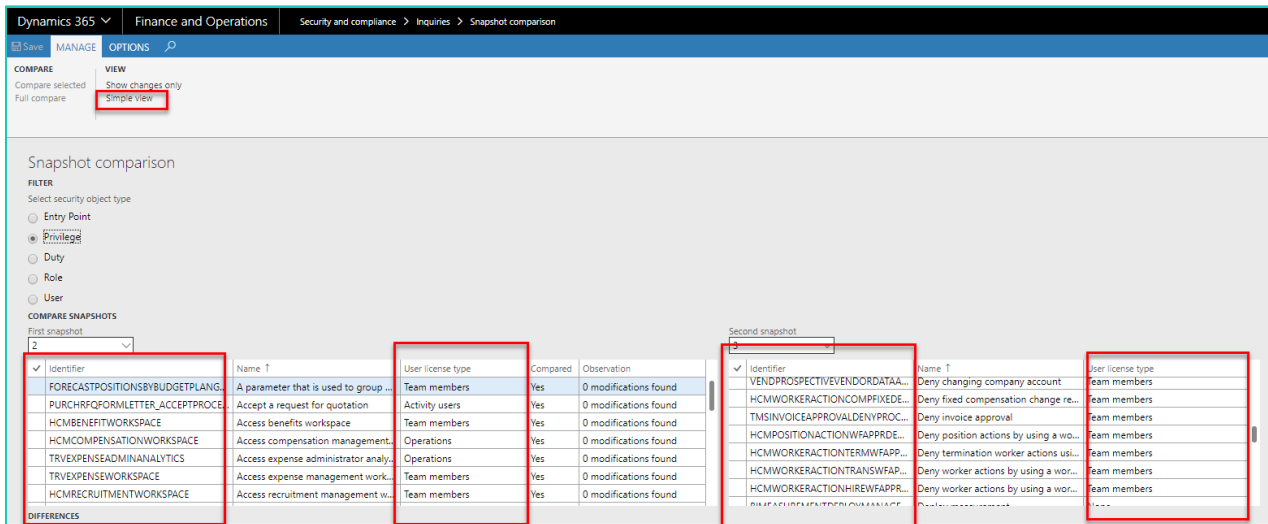


Fig 5. Advanced view

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)

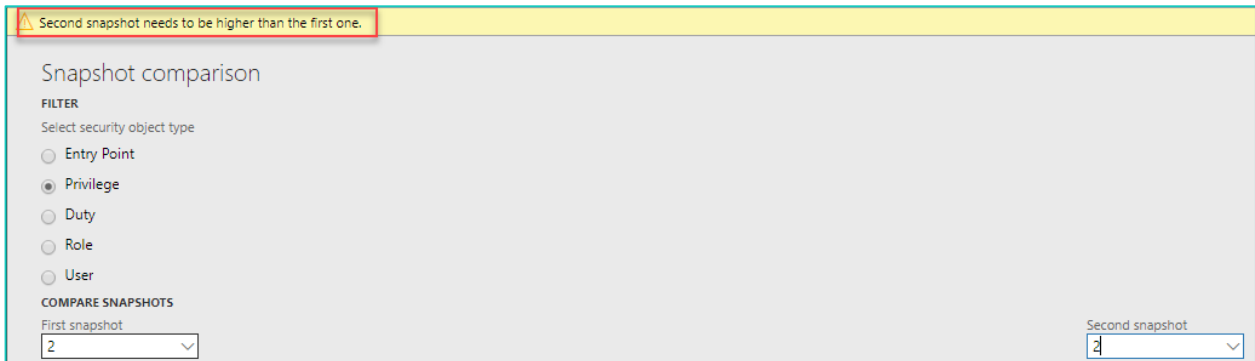


Fig. 6 snapshot selection restriction

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	-

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

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

Security audit

Summary

Audit

Security history

Audit log report

Event date and time	Event created by	Event type	Company	Description
5/15/2018 05:22:19 AM	Admin	Entry point created	dat	Entry point New entry point from AOT created (from AOT)
5/15/2018 05:19:58 AM	Admin	Entry point deleted	dat	Entry point Active directory users deleted (from AOT)
5/15/2018 05:18:30 AM	Admin	Privilege modified	dat	Privilege Maintain Dynamic Security Management IT Audit modified (from AOT)
5/15/2018 05:18:19 AM	Admin	Privilege modified	dat	Privilege Florin privilege 1 modified (from AOT)
5/15/2018 05:18:16 AM	Admin	Privilege modified	dat	Privilege DSMPParametersEntityView modified (from AOT)
5/15/2018 05:18:16 AM	Admin	Privilege created	dat	Privilege PrivilegeFromAOT created (from AOT)
5/15/2018 05:18:16 AM	Admin	Privilege created	dat	Privilege FlorinPrivilegeUITest created (from AOT)
5/15/2018 05:16:43 AM	Admin	Privilege modified	dat	Privilege Apply action modified (from AOT)
5/15/2018 05:14:45 AM	Admin	Duty modified	dat	Duty Maintain security recording modified (from AOT)
5/15/2018 05:14:45 AM	Admin	Duty modified	dat	Duty Florin Duty 1 modified (from AOT)
5/15/2018 05:14:34 AM	Admin	Duty modified	dat	Duty Approve BOMs modified (from AOT)
5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty FlorinDutyUITest created (from AOT)
5/15/2018 05:14:30 AM	Admin	Duty created	dat	Duty Duty created from AOT created (from AOT)
5/15/2018 05:14:04 AM	Admin	Role modified	dat	Role Full read access modified (from AOT)
5/15/2018 05:14:01 AM	Admin	Role created	dat	Role Role test from AOT created (from AOT)
5/15/2018 05:14:01 AM	Admin	Role modified	dat	Role Florin Role 1 modified (from AOT)
5/15/2018 05:13:52 AM	Admin	Role created	dat	Role FlorinRoleUITest created (from AOT)
5/15/2018 05:13:15 AM	Admin	Role modified	dat	Role Chief executive officer modified (from AOT)
5/15/2018 04:08:48 AM	Admin	Duty modified	USMF	Duty Florin Duty 1 modified
5/15/2018 04:08:43 AM	Admin	Duty modified	USMF	Duty Approve BOMs modified
5/15/2018 04:08:40 AM	Admin	Duty created	USMF	Duty FlorinDutyUITest created
5/15/2018 04:08:30 AM	Admin	Role created	USMF	Role FlorinRoleUITest created
5/15/2018 04:08:30 AM	Admin	Role modified	USMF	Role Florin Role 1 modified
5/15/2018 04:08:29 AM	Admin	Role modified	USMF	Role Chief executive officer modified
5/15/2018 04:04:29 AM	Admin	Role created	*	Role FlorinRoleUITest created

changes made from AOT

changes

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).

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

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

MERGE ROLES

Select the entry point types to be added to the target role. For each selected entry point type, a privilege is added to the target role.

CREATE SINGLE PRIVILEGE

Yes ☒ Merged Accountin...

ENABLED

PRIVILEGE NAME

ACTION MENU ITEMS ☐

DISPLAY MENU ITEMS ☐

OUTPUT MENU ITEMS ☐

TABLE PERMISSIONS ☐

You can add a created privilege to a duty. Select the privileges to be added to a duty. For each selected privilege, a duty is created. Instead of the privilege, the created duty is added to the target role.

CREATE DUTY

Yes ☒ Merged Accountin...

ENABLED

DUTY NAME

ACTION PRIVILEGES ☐

DISPLAY PRIVILEGES ☐

OUTPUT PRIVILEGES ☐

TABLE PRIVILEGES ☐

Create single privilege option



3.6.14 Ability to create scenarios from D365 module menus

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

Add module

Area

WHICH MODULE?

- ☒ Area 1
- ☐ Accounts payable
- ☐ Accounts receivable
- ☐ Audit workbench
- ☐ Budgeting
- ☐ Cash and bank management
- ☐ Common
- ☐ Consolidations
- ☐ Cost accounting
- ☐ Cost management
- ☐ Credit and collections
- ☐ Demo data
- ☐ Expense management
- ☐ Fiscal books
- ☐ Fixed assets
- ☐ Fleet management
- ☐ General ledger

Access required

+ Add + Add module access Remove Explore

Securable object	Securable object type	Access level	File	Remark
CustomerInvoiceWorkspace	Menu item display	View		
CustPaymentWorkspace	Menu item display	View		
CustTableListPage	Menu item display	View		
CustTableHoldListPage	Menu item display	View		
CustTablePastDueListPage	Menu item display	View		
MCRCustUnmergeWorkbench	Menu item display	View		

Files

Area 1

No access

View

Edit

Create

Correction

Full control

No access

☐ Create request

Ok Cancel

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

MATCHING	CREATE ROLE		SEGREGATION OF DUTIES	VIEW	ASSIGN TO USER
Match roles Find matched entry points Reset data	Create role Create role from privileges	Create role from duties Duplicate role	Create 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	✓	
			View	Full control	✓	
			View	View	✓	
	Menu item display	Cust...	View	View	✓	
	Menu item display	MCRCustUnm...	View	No access		Not part of the selected role.
	Menu item display	SalesTableListPage	View	View	✓	

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

3.6.15 Snapshots based performance and scalability enhancements

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

Security and compliance studio parameters

General

Prefix
SCS

Color for covered duties and pri...
Yes ☐

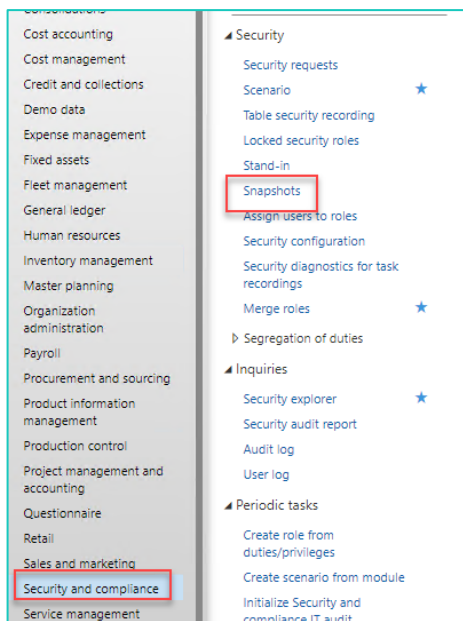
Color Hex #
D3D3D3

INITIALIZE SCS IT AUDIT
Lock 'Initialize Security and com...
Yes ☐

SNAPSHOTS
Limit number of snapshots
1

Snapshots

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.



Save | Set up automatic deletion | OPTIONS

Snapshots

Filter

Version	Name	Description	Created by	Created date and time	Protected
1	Generated from batch, version 1 on 2/13/2018 03:55:37 am	Automatically create from batch job on 2/13/2018	Admin	2/13/2018 03:55:37 AM	<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” [Set up automatic deletion](#)

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



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

- a) "-1" (negative one) value will used to store unlimited number of snapshots. This will also pop-up two warnings to inform the user.
- b) "0" (zero) value will not keep any snapshot versions except the ones marked as 'protected'.

3.6.16 Improved “Create role wizard” based on a grid framework

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

CREATE ROLE

All duties

Select duties to be added to the new role

✓	Duty	Description	User license type
<input checked="" type="checkbox"/>	Maintain Absorption Costs		Operations
<input type="checkbox"/>	Import ZIP/postal codes		Operations
<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

✓	Duty	Description	User license type
<input checked="" type="checkbox"/>	Inquire into Absorption Costs		Team members
<input checked="" type="checkbox"/>	Inquire into purchase agreem...	Respond to inquiries about p...	Team members

Role license type before you finish

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	Role description
SCS_NewRole	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

3.6.17 Accessing Security Explorer from all D365 FOE forms

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

Security diagnostics

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

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

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

Rebuild data... Reset pins... Sample view... Show journal... OPTIONS... 1 2 3 4

Security explorer: full view

USERS
Pin users

User ID	Name	Highest license type
ARNE	ARNE	Operations
CONNIE	CONNIE	Operations
OSCAR	OSCAR	Operations
SARA	SARA	Operations

COLLECTIONS AGENT
Unpin role

Role name	License type
Collections agent	Operations

DUTIES
Pin duty

Duty name	License type
Collections workspace	Team members
Inquire into bill of exchange ...	Team members
Inquire into collections statu...	Operations
Inquire into credit card proc...	Team members
Inquire into customer invoice ...	Activity users
Inquire into customer master	Team members
Inquire into customer payme...	Activity users
Inquire into customer referen...	Team members
Maintain activities	Team members
Maintain collections transact...	Operations
Maintain contacts	Activity users
Maintain customer master	Operations
Maintain financial period clos...	None
Maintain periodic settlement ...	Operations
Manage customer credit and ...	Team members
View sensitive bank account ...	None

PRIVILEGES
Pin privilege

Privilege name	License type
Calculate interest notes	Operations
Cancel collection letters	Operations
Cancel interest notes	Operations
CashDiscountEntry/View	None
Change transaction collection...	Operations
Change/edit customer transa...	Activity users
Change/edit customer transa...	Operations
Change/edit customer transa...	Operations
Correct interest codes	Team members
Create a customer record fro...	Operations
Create a customer record fro...	Operations
Create collection letters	Team members
Create a customer from pin...	Operations
CustBalanceGenerate_CN	Team members
CustCustomerGroupEntry/View	None
CustDirectDebitMandateRet...	None

ENTRY POINTS
Pin entry point

Entry point (AOT name)	T	Access right	Entry point type
AccountingDistCustfreeInvoice	View	Menu item disp	
AccountingDistCustInquiry	View	Menu item disp	
AccountingDistMarkupTransDiv	View	Menu item disp	
AccountingDistMarkupTransPO	View	Menu item disp	
AccountingDistMarkupTransR...	View	Menu item disp	
AccountingDistPurchTable	View	Menu item disp	
AccountingDistributions	View	Menu item disp	
AccountingDistributionsDocu...	View	Menu item disp	
AccountingDistVendEditInHd...	View	Menu item disp	
AccountingDistVendEditInDe...	View	Menu item disp	
ActivitiesMain	View	Menu item disp	
ActivitiesMain	Full control	Menu item disp	
ActivitiesMainBasic	View	Menu item disp	
ActivitiesMainBasic	Full control	Menu item disp	
ActivityViewRecord	View	Menu item disp	

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

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

Roles 'Accounting manager' and 'Accountant' are in violation of segregation of duties rule 'New Segregation of duties rule2':

MERGE ROLES

Select or enter the role to merge to.

TARGET ROLE

Name: Lock target role? ☒ Yes

Select the roles to merge from.

AVAILABLE ROLES

Available roles
Accounting supervisor
Accounts payable centralized payments clerk
Accounts payable clerk
Accounts payable manager
Accounts payable payments clerk

SELECTED ROLES

Selected roles
Accounting manager
Accountant

SOD violations

ENABLED

ACTION MENU ITEMS ☒

DISPLAY MENU ITEMS ☒

OUTPUT MENU ITEMS ☒

TABLE PERMISSIONS ☒

CREATE DUTY

Yes ☒

PRIVILEGE NAME

DUTY NAME

Create duty



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

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

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

Synchronize the group users with the Active Directory group members

Parameters

OPTIONS

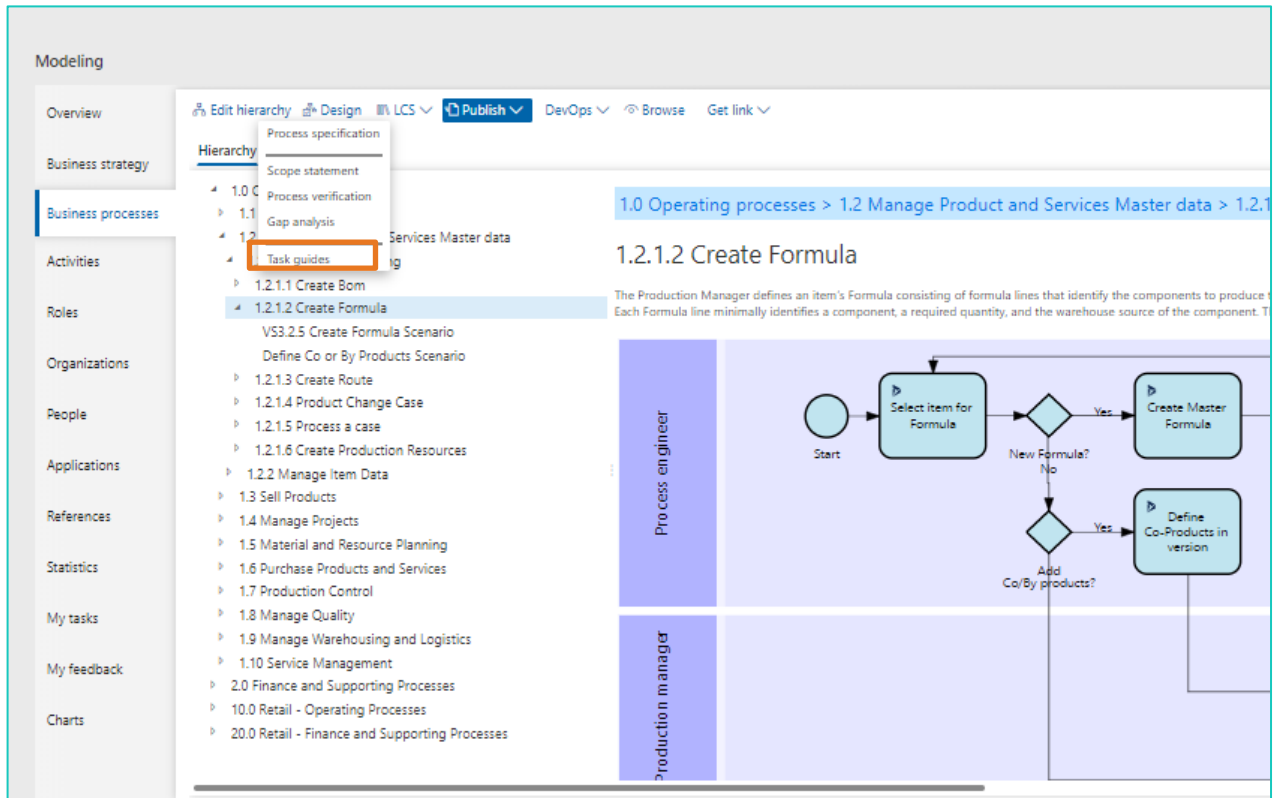
Import users

☒ Yes

Run in the background

3.6.20 Uptake RapidValue BPM Suite Scenarios directly as SCS Security Scenarios

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



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

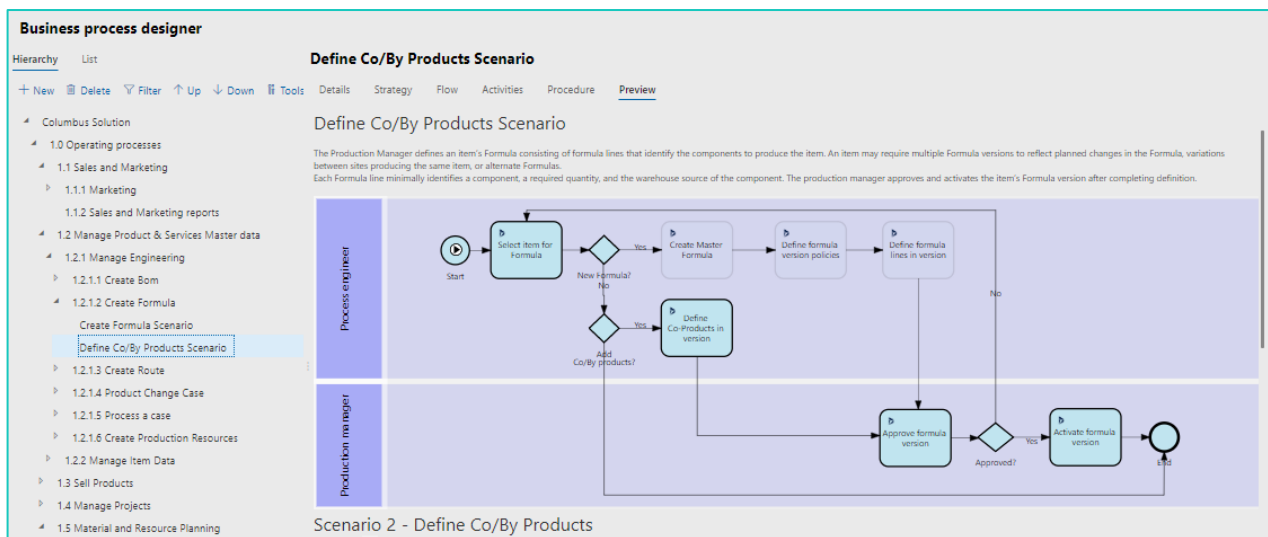


Figure: Scenario-Procedure activity based modelling

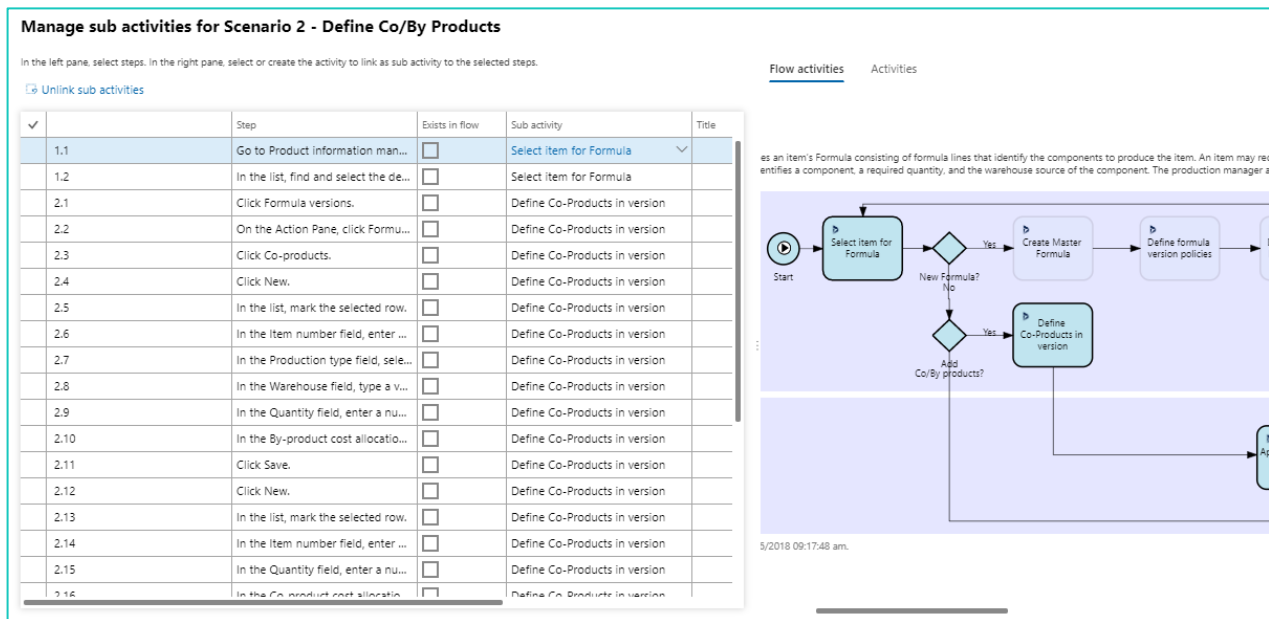
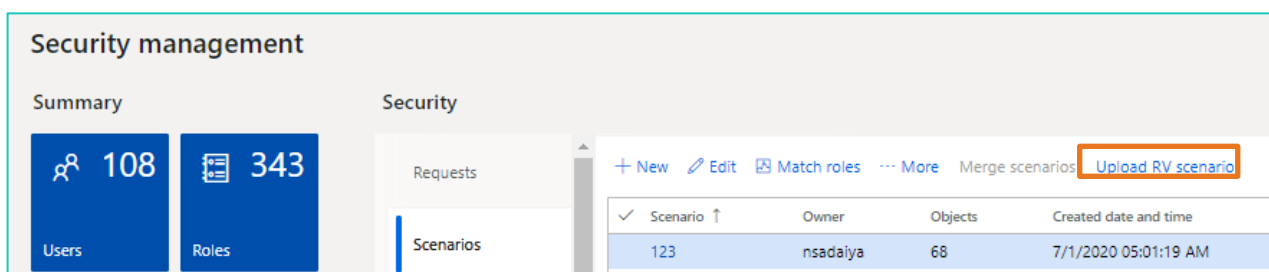


Figure: Scenario-Procedure activity based modelling with recorded steps linked to flow activities

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

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



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

3.6.21 Enhanced Segregation of Duties

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

Risk register						
+ New Edit Validate duties and roles Verify compliance of user-role assignments						
Enhanced SoD rules	✓ 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	ACOLedgerPost_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	ACOLedgerPost_BR	Menu item action	Full control	AuditPolicyCaseGroup
	Match roles test - ep 3	Entry point	DSMSecurityRequestPriorityH...	Menu item action	Correction	ACOLedgerPost_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						
✓ 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

3.6.22 Organization risk Register

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

Integrated risk management

+
Create a risk

4
Risk

124
Enhanced SoD rules

0
Enhanced SoD conflicts

Risk

Risk register

+ New

Edit

Enhanced SoD rules

✓ 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 conflicts

Charts

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...

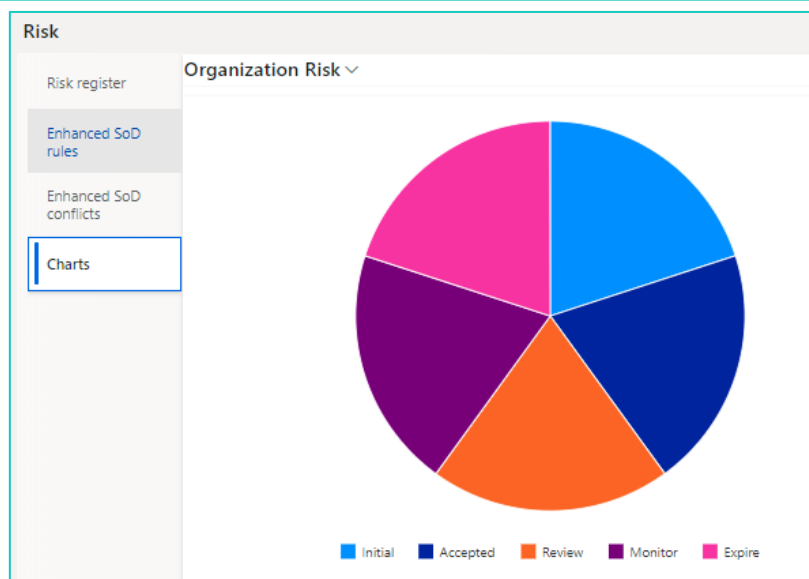
SCS-094-Create purchase order and r...

Duty

Maintain inventory registrati...

No access

Maintain purchase orders





3.6.23 AAD related SoD Validations across SCS

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

3.6.24 Security Explorer displaying Tables, Service operations and Data Entities entry point’s type

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

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

ENTRY POINTS	
Pin entry point and permissions	
Type	Access right
Table	No access
Service operation	No access
Service operation	Full contro
Menu item display	View
Table	View
Menu item display	Full control
DataEntity	View
DataEntity	Full control

3.6.25 Performance Optimization

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

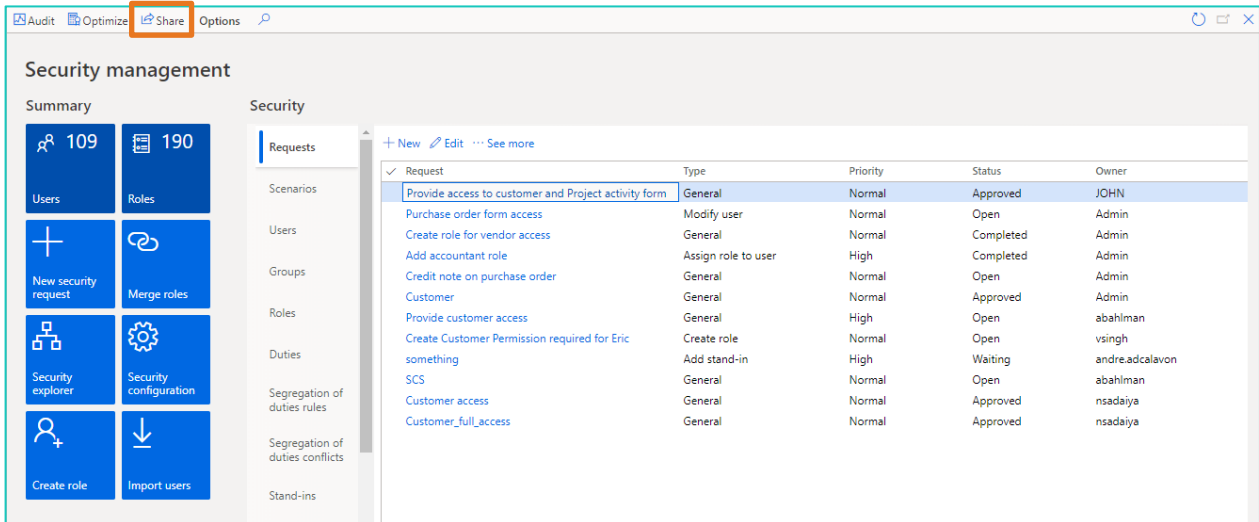
- Create snapshot,
- Security Explorer pinning,
- Match roles and
- Marking a record as sensitive.

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

3.6.26 A new “Share” workspace

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

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

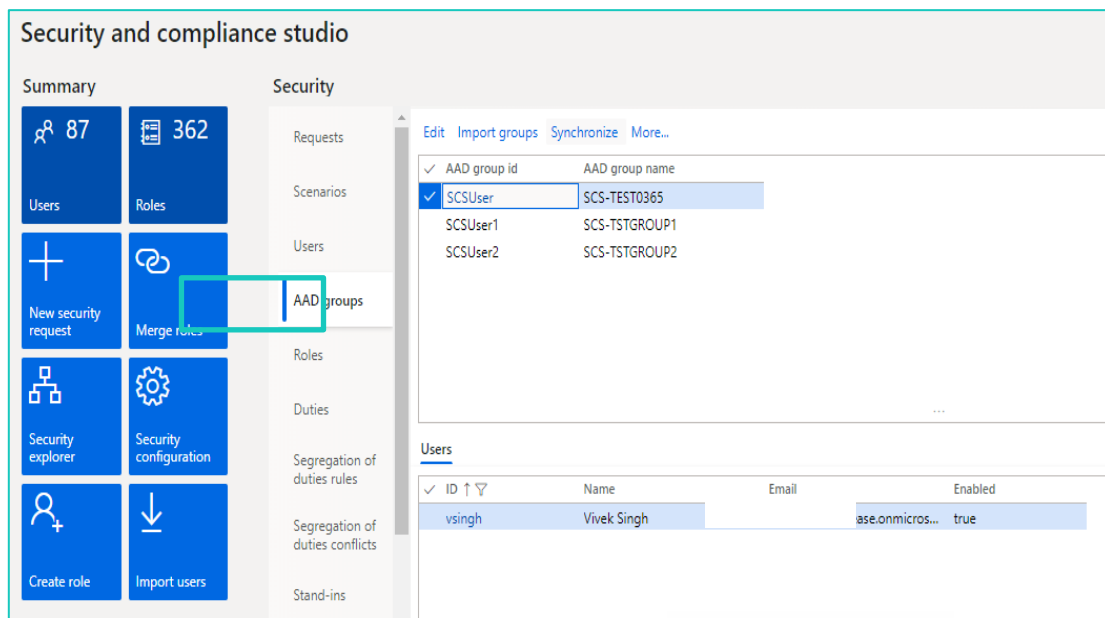


More details are mentioned in the “User and training manual”.

3.6.27 AAD groups’ information in D365FO

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

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



Security						
Requests	+ New Edit Import Explore More					
Scenarios						
Users						
AAD groups						
Roles						
Duties						
Segregation of duties rules						

✓ User ID ↑	Name	Email	License type	Company	Person
TRICIA	TRICIA	TRICIA	TRI	Operations	USSI
VINCE	VINCE	VINCE	VIN	Operations	USMF
vsingh	Vivek Singh	vsir	Operations	USMF	
Wayne	Wayne	Wa	Operations	USMF	
vaichiroo	VOICHIROO	vaichiroo@contoso.com	Operations	USSI	

✓ AAD group id	AAD group name
SCSUser	SCS-TEST0365
SCSUser1	SCS-TSTGROUP1

3.6.28 Verify SoD rules in Stand in

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

Edit	+ New	Delete	Assign stand-in roles	Validate SoD rules	Options
------	-------	--------	-----------------------	--------------------	---------

✓ User ID ↑	Stand-in	From date	To date	Copy assigned organizations
ALICIA	APRIL	12/13/2018	12/13/2018	✓
APRIL	dtijssen	1/19/2019	1/20/2019	✓
atayyala	acardol	10/21/2019	10/31/2019	✓
BENJAMIN	CHARLIE	10/3/2019	10/11/2019	
CHARLIE	BENJAMIN	10/3/2019	10/17/2019	
dtijssen	Admin	1/21/2019	1/22/2019	✓
JACOB	JEREMY	10/22/2019	10/31/2019	
JACOB	nsadaiya	10/22/2019	10/24/2019	✓
nsadaiya	ALICIA	3/14/2019	3/30/2019	✓
OSCAR	JULIA	10/22/2019	10/31/2019	✓

Assignment of OSCAR's roles to JULIA are in violation of SoD rules: 'SCS-083-Release production order and move inventory'. The role 'Accounts receivable payments clerk' contains duty 'Maintain customer payments' and the role 'Accountant' contains duty 'Enable bank management process'.

✓ User ID ↑	Stand-in	From date	To date	Copy assigned ...
ALICIA	APRIL	12/13/2018	12/13/2018	✓
APRIL	dtijssen	1/19/2019	1/20/2019	✓
atayyala	acardol	10/21/2019	10/31/2019	✓
BENJAMIN	CHARLIE	10/3/2019	10/11/2019	
CHARLIE	BENJAMIN	10/3/2019	10/17/2019	
dtijssen	Admin	1/21/2019	1/22/2019	✓
JACOB	JEREMY	10/22/2019	10/31/2019	
JACOB	nsadaiya	10/22/2019	10/24/2019	✓
nsadaiya	ALICIA	3/14/2019	3/30/2019	✓
OSCAR	JULIA	10/22/2019	10/31/2019	✓

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

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

Security and compliance studio

Summary

103

Users

175

Roles

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	al	Operations	DAT	
acardol	Adri Cardol	ai	Activity users	DAT	
andre.adcalavon	André Amaud de Calavon	ai	Operations	DAT	
atayyala	Anil Kumar Tayyala (ATAYY.TI)	ai	Team members	dat	
dvschie	David van Schie (DVSCH.TI)	di	Operations	dat	
evhofwegen	Eric van Hofwegen	ei	Operations	DAT	
nsadaiya	Nitish Sadaiya (NSADA.TI)	ni	Operations	usmf	
Pradeep.Bapna	Pradeep Kumar Bapna	Pi	Operations	DAT	
SCS-TSTGroup1	SCS-TSTGROUP1		Operations	DAT	
SCS-TSTGroup2	SCS-TSTGROUP2		Operations	DAT	
vsingh	Vivek Singh (VSING.TI)	vi	Operations	dat	

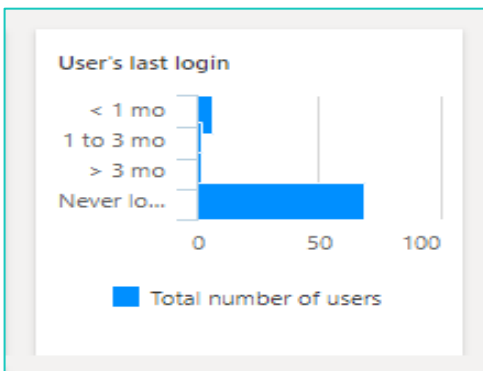
Roles

History

Login date and time

AAD groups

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



3.6.30 Asset classification User Interface

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

Rebuild asset classification

Asset classification chart

Options

Asset classification

Tables

Filter

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
CNPNum_BR		Customer Content
CPFNum_BR		Customer Content

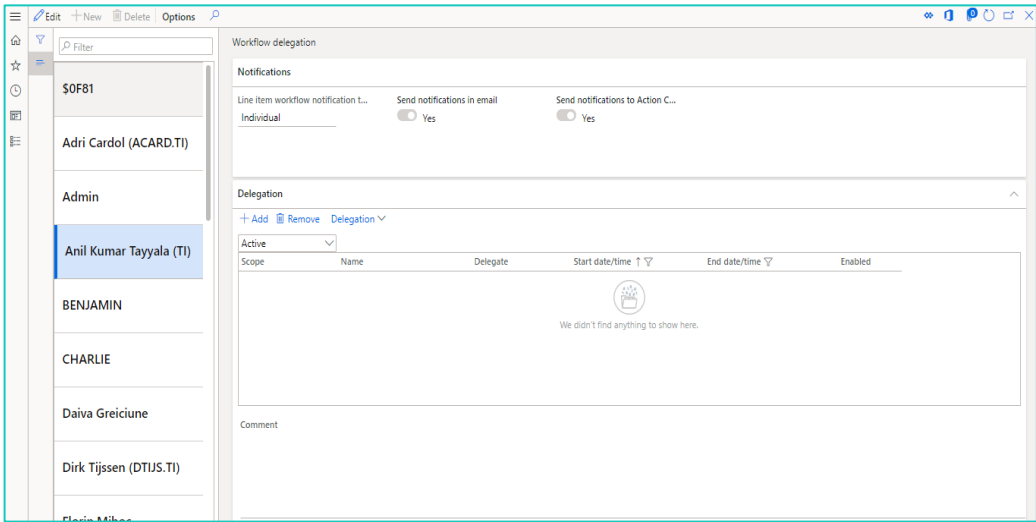
Asset classification

Asset Classification
Access Control Data
Customer Content
CustomerContent
End User Identifiable Information (EUI)
End User Pseudonymous Identifiers
End User Pseudonymous Information (EUP)
Extension Attrib
Object Metadata
Organization Identifiable Information (OI)
System Metadata



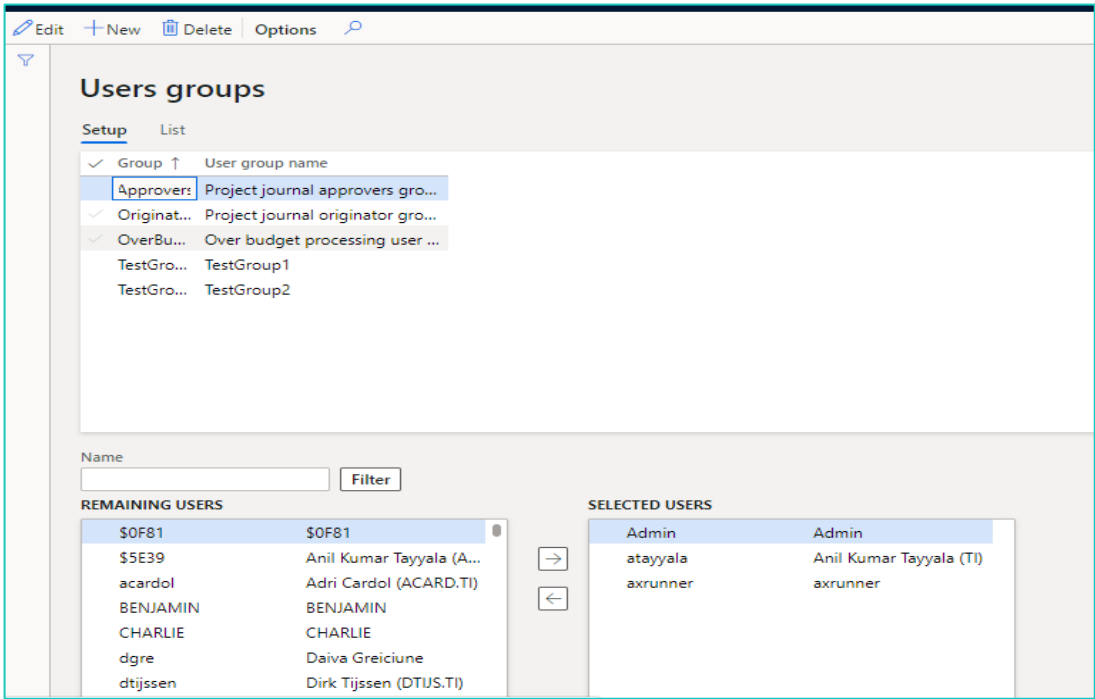
3.6.31 A List page with Workflow delegation details

This one is a UI improvement to make it easier for SCS administrators to manage and track “Workflow Delegations”. Every user has to login by himself to delegate workflow to other user, in D365FO. Now using SCS, administrators can delegate workflow to any user for a particular time period. Workflow delegation history list page is also there for tracking. You can reach here from the Security and Compliance Module > Inquiries > Workflow delegation and >Workflow delegation history



3.6.32 User groups – combined two tabs in one

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





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

3.6.33 New export/import role functionality

a) Problem:

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

b) Issue that is generated by the bug explained:

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

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

c) Solution:

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

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

Security management

Summary

Users 135 Roles 242

New security request Merge roles Security explorer Security configuration Create role Import users

Security

Requests Scenarios Users Groups Roles Duties Segregation of duties rules Segregation of duties conflicts Stand-ins

Merge roles Duplicate role Lock roles Explore Export Import Define active/inactive role Export role configuration Import role configuration

Role name	License type	License type (cloud)	Role description	Locked	Inactive	Has configuration
Business events security role	Operations	Human resouces				
Business events viewer	None					
BusinessConnector Role	None		Role Used to Decide if us...			
Buying agent	Activity users	Activity users	Documents purchase eve...			✓
Chief executive officer	Activity users	Activity users	Reviews the financial and ...			✓
Chief financial officer	Activity users	Activity users	Reviews the financial perf...			✓
Collections agent	Operations	Finance	Documents collections ev...			

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

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

3.6.34 License count changes

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



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

My view ▾

Security and compliance studio parameters

General

License count

Data migration

Enhanced SoD rules

Number sequences

General setup for the purchased licenses

[Open admin.microsoft.com](#)

LICENSE PARAMETERS INPUT

<input type="radio"/>	License	No of licenses
<input checked="" type="radio"/>	Activity users	150
	Commerce	12
	Commerce - attached license	3
	Finance	10
	Finance - attached license	5
	Human resouces	10
	Human resouces - attached license	5
	Operations	0
	Project operations	60
	Project operations - attached license	30
	SCM	18
	SCM - attached license	9
	Team members	76

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

License optimization

Summary

License

Usage

All users

Full users

Activity users

Team members

Scenarios

The actual count is a total of required base and attach licenses. In case one of base the licenses is required, the count is listed in 'Any base license'.
Based on your actual subscription, you can use this information to verify your compliance.
The licensed users and remaining licenses might be incorrect in case there are users requiring more than one license.
The Dynamics 365 user interface is not aware of assigned licenses in Entra ID.

[View on premise](#)

<input type="radio"/>	License type	Actual users count	Base license users count	Attach license users count	Remaining users count
<input checked="" type="radio"/>	Activity users	3	150	0	147
	Any base license	10	0	0	-10
	Commerce	30	12	3	-15
	Finance	35	10	5	-20
	Human resouces	4	10	5	11
	Project operations	18	60	30	72
	SCM	47	18	9	-20
	Team members	30	76	0	46

The new license calculation formula will now: (Base license + Attached license) – Actual user count.
In order to separate the ‘cloud license’ from ‘On premise’ licenses we added the “View on premise” / “View cloud license” button that can toggle this view.



Usage

All users

Full users

Activity users

Team members

Scenarios

The actual count is a total of required base and attach licenses. In case one of base the licenses is required, the count is listed in 'Any base license'.
Based on your actual subscription, you can use this information to verify your compliance.
The licensed users and remaining licenses might be incorrect in case there are users requiring more than one license.
The Dynamics 365 user interface is not aware of assigned licenses in Entra ID.

View on premise licenses

Cloud license view

<input type="radio"/> License type	Actual users count	Base license users count	Attach license users count	Remaining users count
<input checked="" type="radio"/> Activity users	3	150	0	147
Any base license	10	0	0	-10
Commerce	30	12	3	-15
Finance	35	10	5	-20
Human resouces	4	10	5	11
Project operations	18	60	30	72
SCM	47	18	9	-20
Team members	30	76	0	46

Usage

All users

Full users

Activity users

Team members

Scenarios

The actual count is a total of required base and attach licenses. In case one of base the licenses is required, the count is listed in 'Any base license'.
Based on your actual subscription, you can use this information to verify your compliance.
The licensed users and remaining licenses might be incorrect in case there are users requiring more than one license.
The Dynamics 365 user interface is not aware of assigned licenses in Entra ID.

View cloud licenses

On premise view

<input type="radio"/> License type	Actual users count	Base license users count	Attach license users count	Remaining users count
<input checked="" type="radio"/> Activity users	3	150	0	147
Operations	0	0	0	0
Team members	30	76	0	46



4. Bug fixes

4.1 Security and compliance studio 10.0.44.48

ID	Description	Observation
209310	CS00235328 Organization hierarchy assignment not functioning correctly	This fix will ensure that user is able to use the “Add with Child” functionality of standard Organization Hierarchy feature of Dynamics 365 F&SCM.
220879	CS00236855 STAEDEAN SCS ISV Deployment	This fix will ensure that user is able to successfully save a security scenario.
219780	CS00236707 FW: Case CS00236071 has been closed	This fix will ensure that user is able to successfully save a security scenario.

4.2 Security and compliance studio 10.0.43.47

ID	Description	Observation
201660	CS00234102 Deleting a security request that has been submitted to workflow	This fix will ensure that user should be able to delete only an open security request and not the completed security request.

4.3 Security and compliance studio 10.0.42.46

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



205241	CS00234809 Cleanup of table DSMSECURITYPRIVDUTYASSOCIATION HISTORY	This bug fix will ensure that user is able to clean the table DSMSECURITYPRIVDUTYASSOCIATIONHISTORY successfully.
--------	--	---

4.4 Security and compliance studio 10.0.41.45

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

4.5 Security and compliance studio 10.0.40.44

ID	Description	Observation
179803	License recommendation incorrect in case of both HR and PO roles	This bug fix will ensure that HR license should appear as an attached license and not base license.
195135	CS00233715 SCS version 10.0.39.43 causes a lot of objects in garbage collection	Memory consumption issue that leads to slow performances got fixed. Garbage collection is working correctly.

4.6 Security and compliance studio 10.0.39.43

ID	Description	Observation
183994	CS00232323 German labels in module SCS are missing or incorrectly translated	German label was not correctly translated. Fixed now.



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

4.7 Security and compliance studio 10.0.37.42

ID	Description	Observation
175967 & 176711	CS00227225 Export/Import function in Security and Compliance Studio modifies std. objects. & CS00227144 Deviation in standard role after import of custom role.	AOT privileges with 'FormControlOverrides' node populated are having an issue on SCS Export/Import functionality due to a MS standard bug. All entries from this node cannot get pass into the XML file, therefore at the import step the node will get overridden and all entries are removed (as the object from the XML file). As a fix we introduced a new functionality called : "Export role customizations / Import role customizations". For more details please see WHAT'S NEW SECTION .
180975	CS00227886 Manage access on roles to multiple organisations is not working in 'NL'	Using a different language than EN-US was making 'System administrator' role available for organization assignation, which is not correct since it is an all-organizations role.
180707 & 180696	CS00227833 'Any base license' roles are counted in both 'Finance' and 'SCM' licenses & CS00227738 wrong count of used licenses for role	Incorrect license count. New options have been added to the SCS parameters license count system. For more details please see WHAT'S NEW SECTION .
176445	Internal Description of the Security request should not be editable after it had been submitted to the workflow	Some form sections from 'Security requests' were still editable after it was submitted. Fixed now.
179815	Internal Align licensing details with MSFT changes (Read overrides to Team members)	Align with new change from MS where if a securable object (role, duty or privilege)



		it's view only than the license should be 'Team members', always.
--	--	---

4.8 Security and compliance studio 10.0.36.41

ID	Description	Observation
180210	CS00227639 Cannot import roles. Error: "Cannot create a record in Roles (DSMRolesTable)."	This is most likely an issue where the role was initially deleted and imported again. A Dynamic Snapshot feature is generating the error, probably due to incorrect data. To fix the issue at short notice, we added a parameter in the Security and Compliance Studio where the Dynamic snapshot feature can be switched on and off. In case the feature is disabled, the snapshot versions should be created regularly to have all information in Security and Compliance Studio up to date. E.g. the Security Explorer is dependent on actual snapshot information.

4.9 Security and compliance studio 10.0.36.40

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

4.10 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'.

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



4.12 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.

4.13 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 recognized during direct role import	Changes over the data source fields are not detected during direct role import.

4.14 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.



4.15 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.

4.16 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

4.17 Security and compliance studio 10.0.26.31

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

4.18 Security and compliance studio 10.0.25.30

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

4.19 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.

4.20 Security and compliance studio 10.0.22.27

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

4.21 Security and compliance studio 10.0.18.1

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

4.22 Security and compliance studio 10.0.12.5

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

4.23 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
--------	--

4.24 Security and compliance studio 10.0.12.3

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

4.25 Security and compliance studio 10.0.12.2

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

4.26 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

4.27 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

4.28 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

4.29 Security and compliance studio 10.0.6.10

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

4.30 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

4.31 Security and compliance studio 10.0.6.8

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

4.32 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

4.33 Security and compliance studio 10.0.6.6

ID	Description
100323	CS00111058-Unable To Import Security Roles

4.34 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

4.35 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



4.36 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

4.37 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

4.38 Security and compliance studio 10.0.6.1

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

4.39 Security and compliance studio 10.0.3.3

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

4.40 Security and compliance studio 10.0.3.2

ID	Description
77956	CS00069693 – License Count Data Source.

4.41 Security and compliance studio 10.0.3.1

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

4.42 Security and compliance studio 10.0.1.3

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

4.43 Security and compliance studio 10.0.1.2

ID	Description
----	-------------



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

4.44 Security and compliance studio 10.0.1.1

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

4.45 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.

4.46 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.

4.47 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'

4.48 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

4.49 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

4.50 Security and compliance studio 81.20.3.1

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

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

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



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

4.52 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.

4.53 Security and compliance studio 81.20.1.1

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

4.54 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.

4.55 Security and compliance studio 1804.15.1.1

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

4.56 Security and compliance studio 1712.12.1.1

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



5. Changed or deprecated features

5.1 Deprecated features 10.0.31.37

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

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

“ALTER TABLE ALTER COLUMN ENTRYPPOINTNAME failed because one or more objects access this column.

```
ALTER TABLE DSMSECURITYENTRYPPOINTPRIVASSOCIATION ALTER COLUMN ENTRYPPOINTNAME 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).

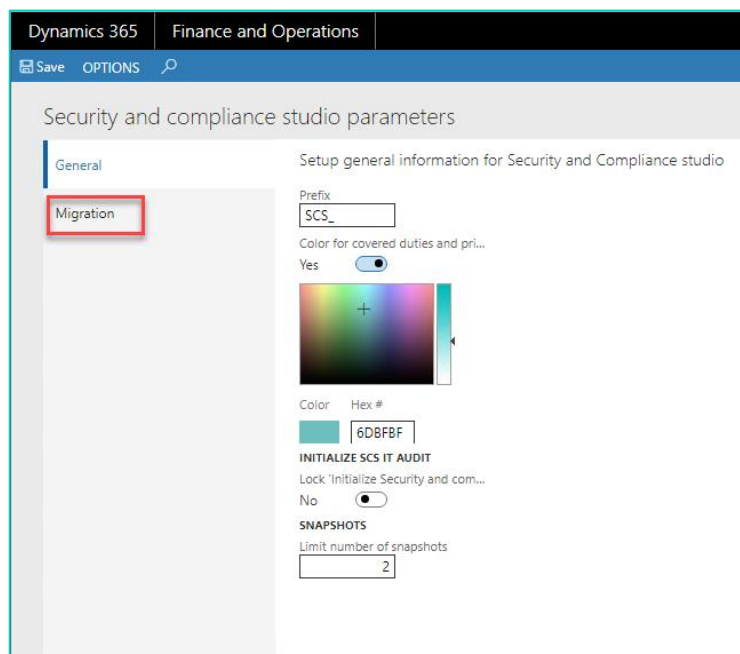


Fig. 1 New tab in SCS Parameters form

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)

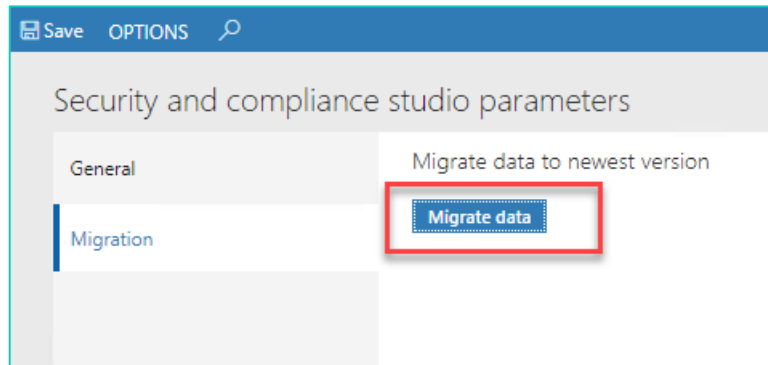


Fig. 2 “Migrate data” button on SCS Parameters form

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)

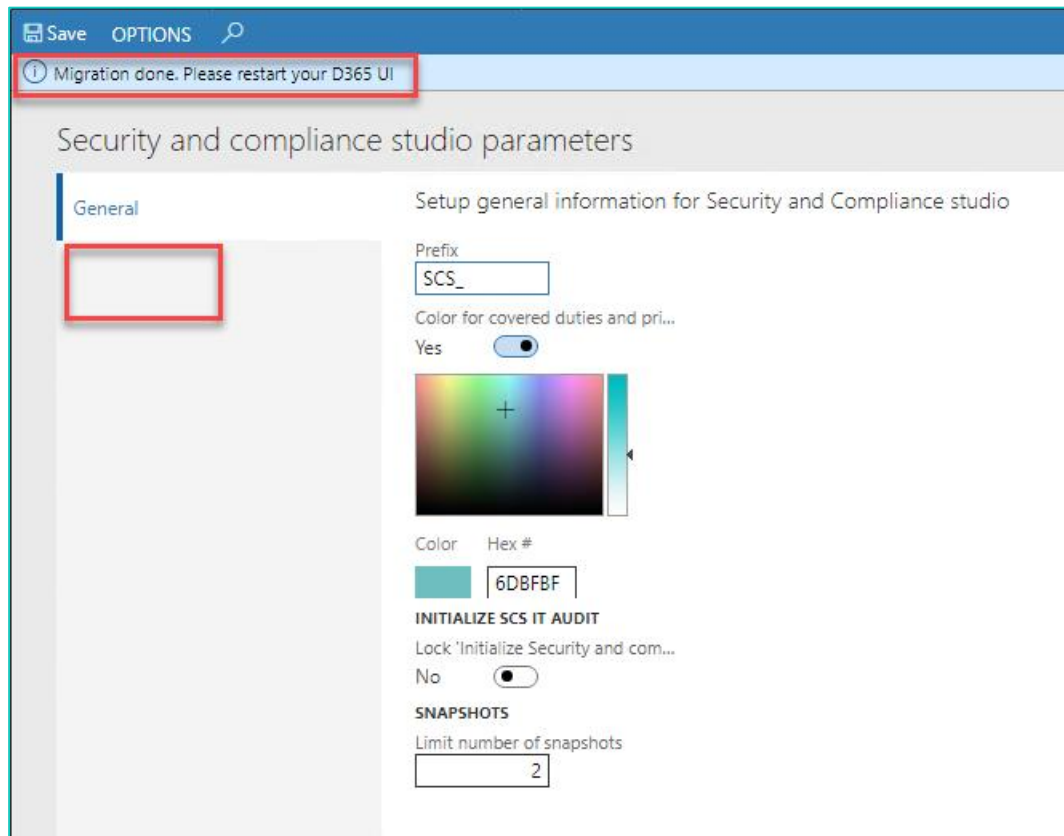


Fig. 3 “Migration” tab not available anymore after moving data