Installation and User Manual

Installation and User Manual

Confidential Data Protection

Confidential Data Protection is a Business Central extension that helps you protect your sensitive and confidential data from unauthorized access. It allows you to designate specific users as **SUPER administrator**, specify which tables contain confidential data, mark G/L accounts as "Confidential", generate restricted permission sets, resolve confidentiality-violating permission set assignments, and get better insights into permission sets.

Why Confidential Data Protection?

In many businesses, there is certain data that should not be exposed to all users, such as financial transactions, budgets, salaries, contracts, etc. **However, by default, Business Central does not provide a way to restrict access to this data based on the content of the records**. For example, if a user has the permission assigned to view the **G/L Entry** table, they will be able to see all the entries in that table, regardless of the **G/L account(s)** they are related to. However, many users would not be able to perform their daily tasks without this table permission, and it is common for users to have this permission.

This poses a serious risk for your business, as it can compromise your **data security**, **privacy**, and **compliance**. Moreover, it can affect your users' productivity and performance, as they will have to deal with a lot of irrelevant and distracting information.

Confidential Data Protection solves this problem by enabling you to define which data should be treated confidentially, and who can access that data, at a more granular level. It also helps you to manage your permission sets more efficiently and effectively, by providing you with tools to monitor and resolve any issues related to data confidentiality.

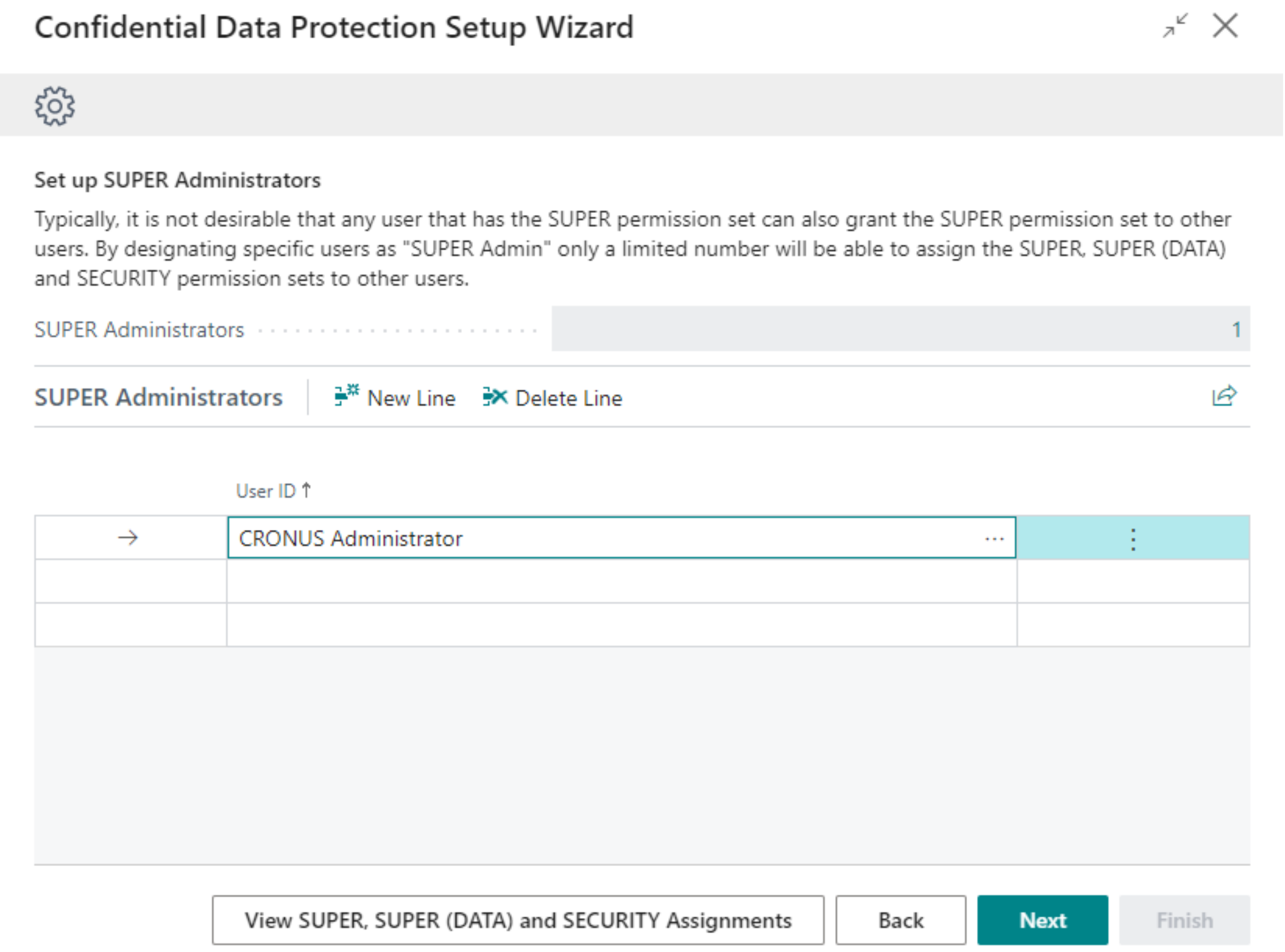
How Confidential Data Protection Works

Confidential Data Protection works by adding a layer of security and control over your data and permission sets.

The extension achieves this by adding the following features to your Business Central environment:

- **SUPER Administrators**

This feature allows you to designate specific users as SUPER administrators, who will be the only users able to assign the **SUPER**, **SUPER (DATA)** and **SECURITY** permission sets to other users. This way, you can limit the number of users who have and can grant full access to your system and data.



Confidential Data Protection Setup Wizard

Set up SUPER Administrators

Typically, it is not desirable that any user that has the SUPER permission set can also grant the SUPER permission set to other users. By designating specific users as "SUPER Admin" only a limited number will be able to assign the SUPER, SUPER (DATA) and SECURITY permission sets to other users.

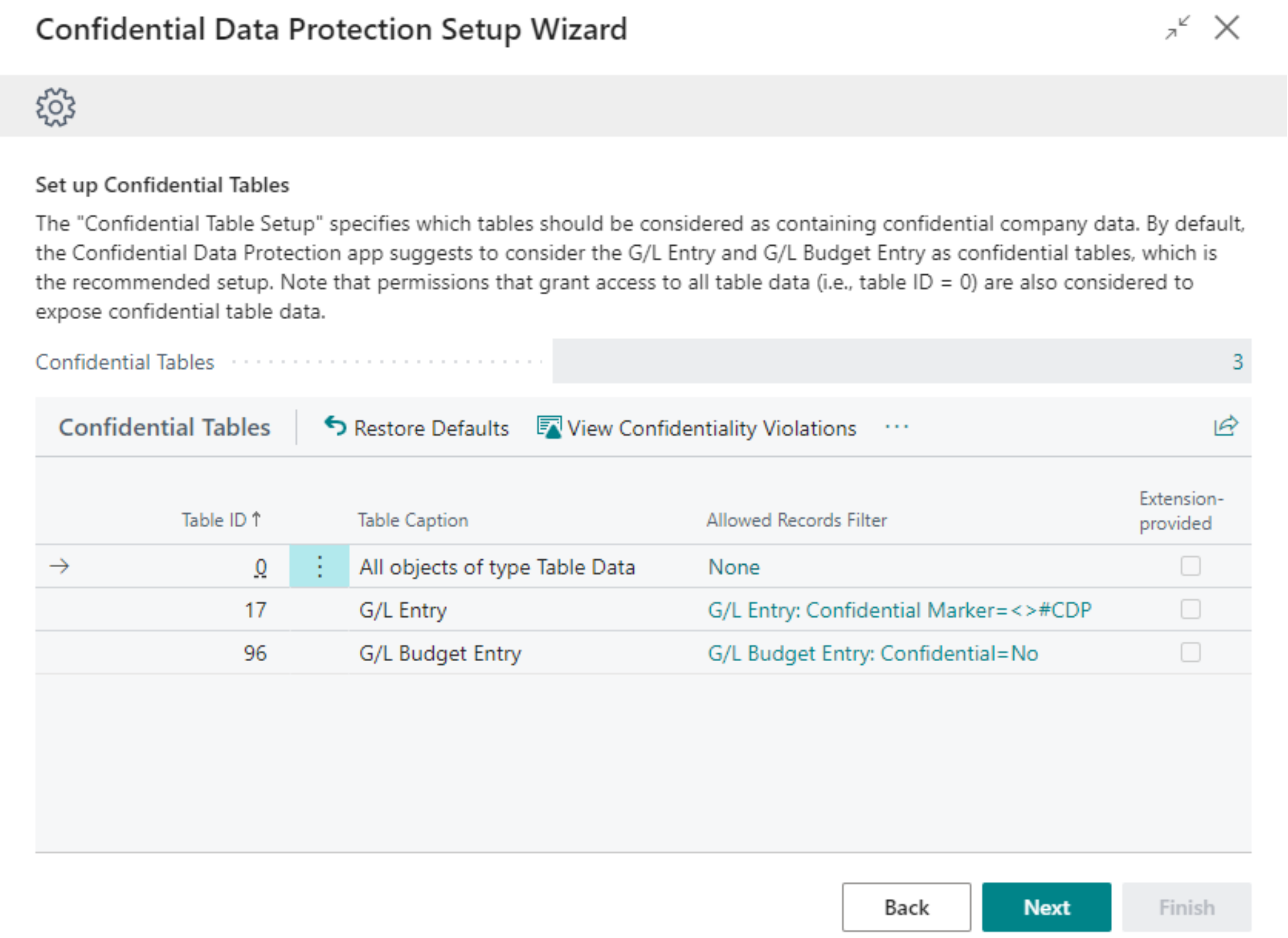
SUPER Administrators: 1

User ID ↑
CRONUS Administrator

Set up SUPER administrators in your Business Central environment to limit the number of users that have and can grant full access to your system and data.

- Confidential Tables

This feature allows you to specify which tables in your Business Central environment contain confidential data. By default, the extension suggests to consider the **G/L Entry** and **G/L Budget** Entry tables as confidential, which is the recommended setup. However, you can also add or remove other tables as needed.



Confidential Data Protection Setup Wizard

Set up Confidential Tables

The "Confidential Table Setup" specifies which tables should be considered as containing confidential company data. By default, the Confidential Data Protection app suggests to consider the G/L Entry and G/L Budget Entry as confidential tables, which is the recommended setup. Note that permissions that grant access to all table data (i.e., table ID = 0) are also considered to expose confidential table data.

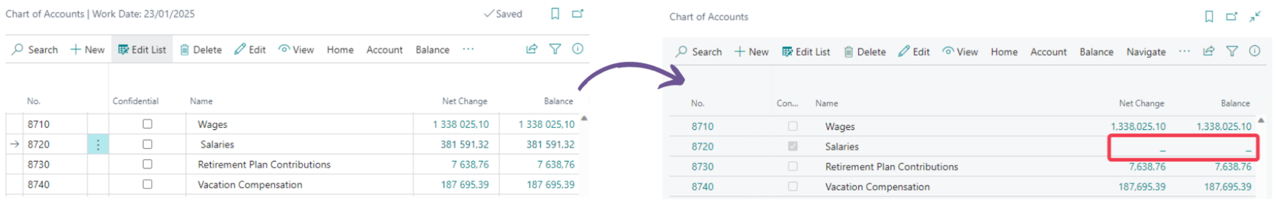
Confidential Tables: 3

Table ID ↑	Table Caption	Allowed Records Filter	Extension-provided
0	All objects of type Table Data	None	□
17	G/L Entry	G/L Entry: Confidential Marker=<>#CDP	□
96	G/L Budget Entry	G/L Budget Entry: Confidential=No	□

Set up tables that should be considered as containing confidential data and should be treated and protected accordingly.

- **Confidential G/L Accounts**

  This feature allows you to mark certain G/L accounts as "Confidential", so that the related G/L data for these accounts will not be exposed to users who have access to the **G/L Entry** table. Instead, only users who have explicit permission to view these accounts will be able to see the entries for those accounts.



No.	Confidential	Name	Net Change	Balance
8710	□	Wages	1 338 025,10	1 338 025,10
8720	□	Salaries	381 591,32	381 591,32
8730	□	Retirement Plan Contributions	7 638,76	7 638,76
8740	□	Vacation Compensation	187 695,39	187 695,39

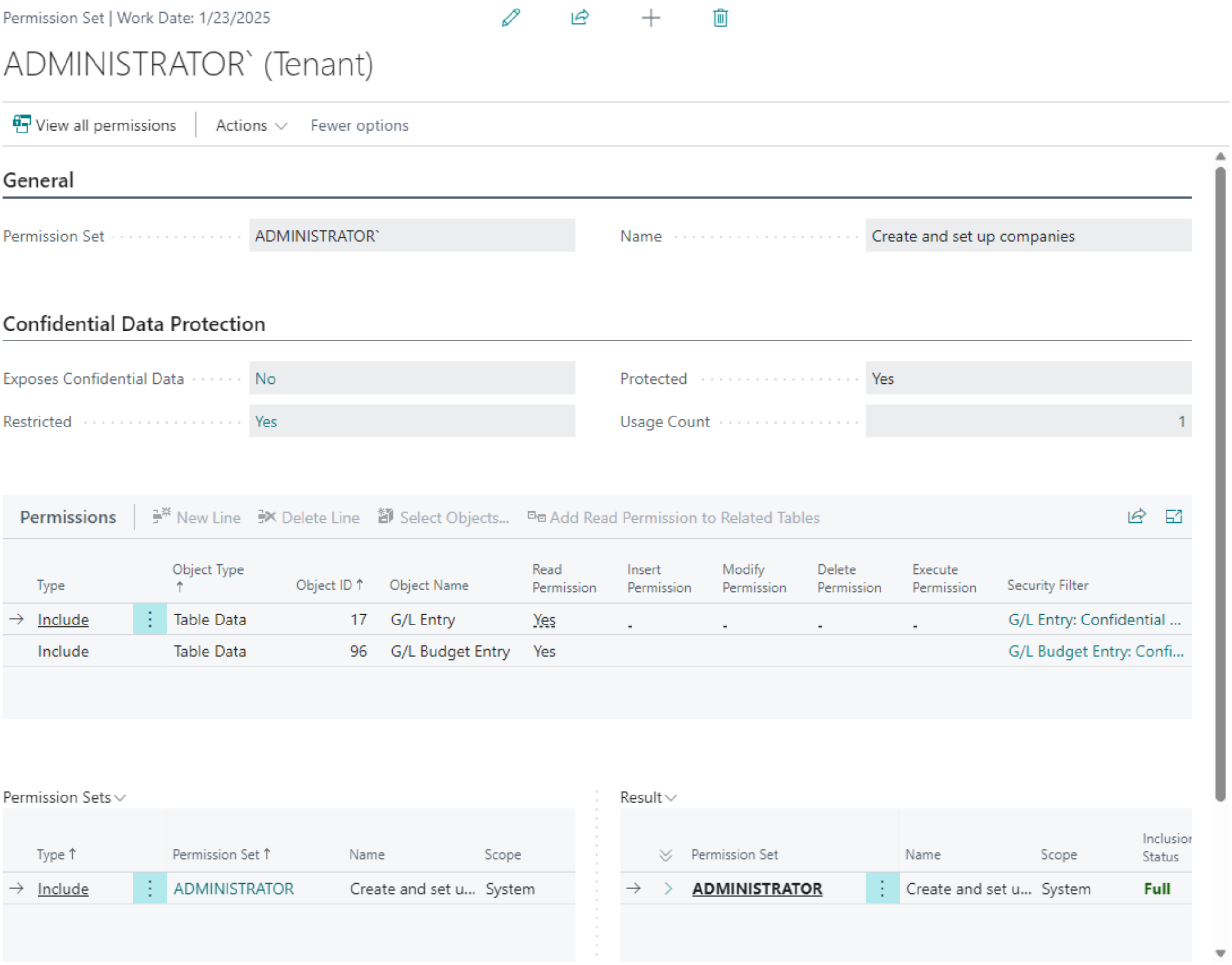
No.	Con...	Name	Net Change	Balance
8710	□	Wages	1,338,025.10	1,338,025.10
8720	☑	Salaries	_	_
8730	□	Retirement Plan Contributions	7,638.76	7,638.76
8740	□	Vacation Compensation	187,695.39	187,695.39

Protect G/L data for G/L accounts that relate to confidential data by marking specific G/L accounts as "Confidential". This way users will not have access to the G/L data related to that G/L account, not even from calculated flowfields.

- **Restricted Permission Sets**

The **Confidential Data Protection** extension includes a feature which automatically protects your Business Central environment against **confidentiality-violating** permission set assignments. To achieve this the extension automatically generates **Restricted** permission sets, which are permission sets that exclude access to confidential table data.

For example, if you have a permission set that grants access to the **G/L Entry** table and attempt to assign it to a user or group of users, the extension automatically provides and assigns a restricted permission set that will only grant access to the entries of non-confidential **G/L accounts** instead. You can also assign these restricted permission sets yourself directly to your users, who do not need to see confidential data.



Permission Set | Work Date: 1/23/2025

ADMINISTRATOR` (Tenant)

General

Permission Set	ADMINISTRATOR`	Name	Create and set up companies

Confidential Data Protection

Exposes Confidential Data	No	Protected	Yes
Restricted	Yes	Usage Count	1

Permissions

Type	Object Type ↑	Object ID ↑	Object Name	Read Permission	Insert Permission	Modify Permission	Delete Permission	Execute Permission	Security Filter
Include	Table Data	17	G/L Entry	Yes	.	.	.	.	G/L Entry: Confidential ...
Include	Table Data	96	G/L Budget Entry	Yes					G/L Budget Entry: Confi...

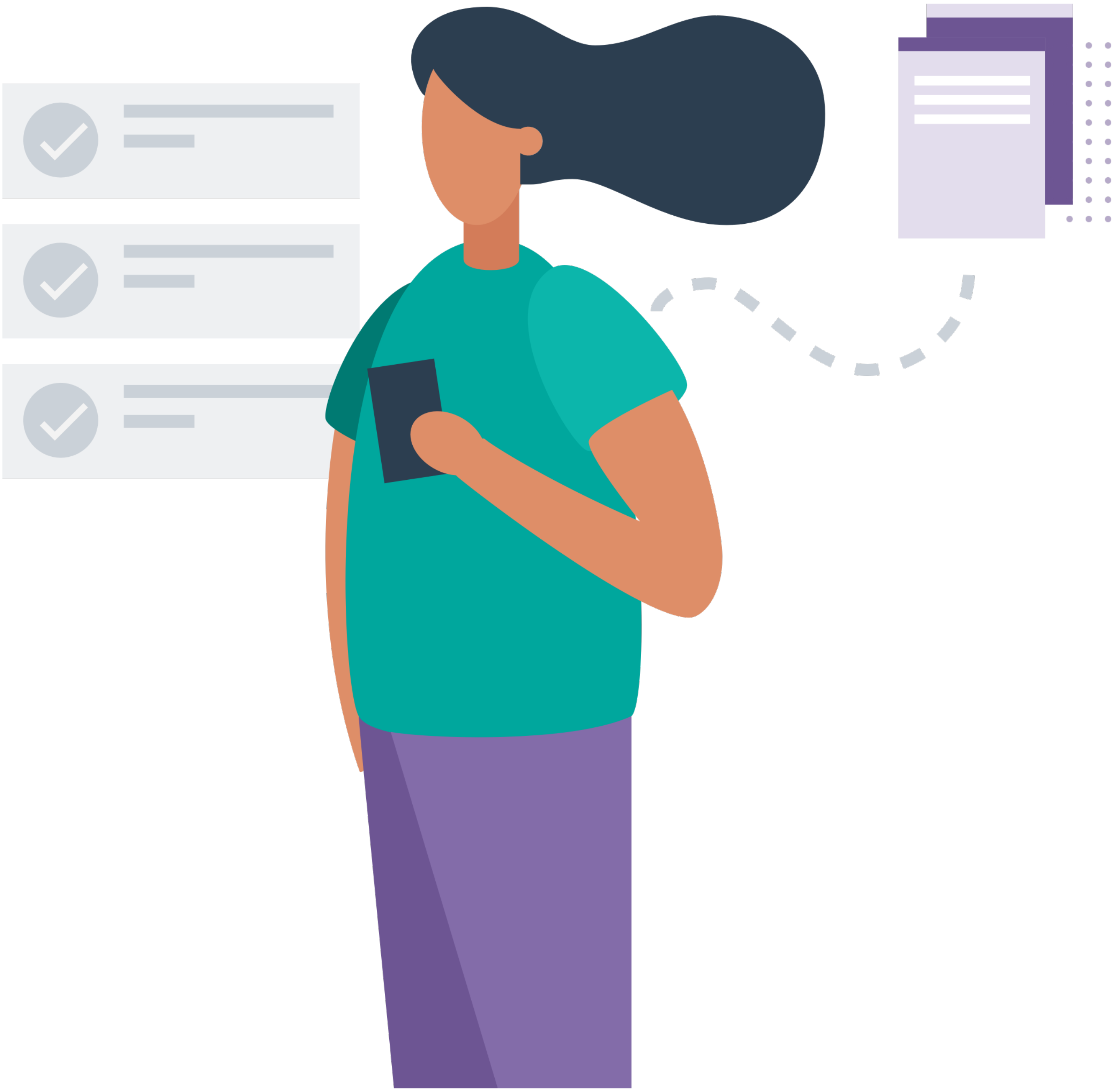
Permission Sets

Type ↑	Permission Set ↑	Name	Scope
Include	ADMINISTRATOR	Create and set u...	System

Result

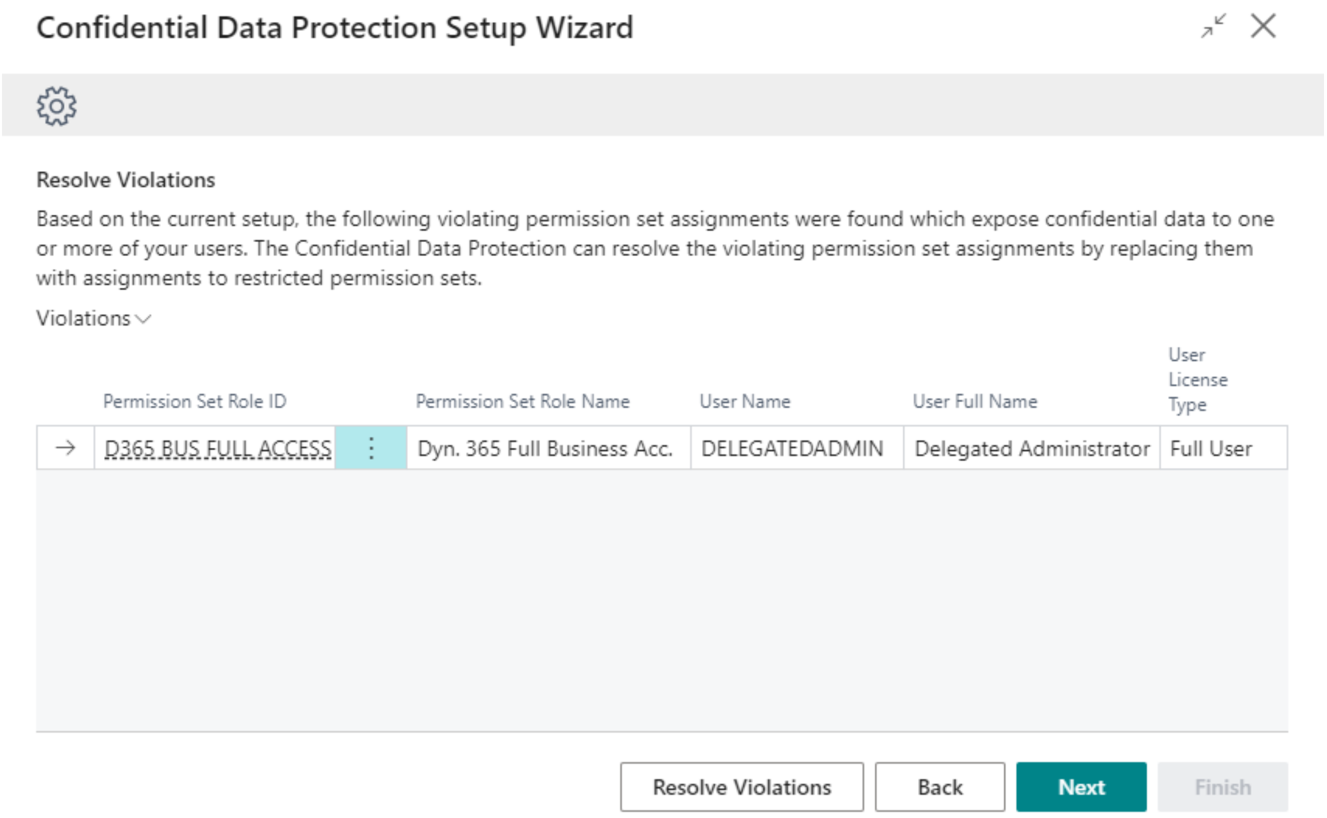
Permission Set	Name	Scope	Inclusion Status
ADMINISTRATOR	Create and set u...	System	Full

The extension automatically protects you against attempts to create confidentiality-violating permission set assignments. This is achieved by automatically generating "restricted" permission sets and assigning these permission sets instead.



- **Confidentiality Violation Resolution**

  This feature allows you to identify and resolve any permission set assignments that violate your data confidentiality rules. For example, if you have a user who has been assigned a permission set that grants access to a confidential table or a confidential G/L account, the **Confidential Data Protection** extension helps you to identify and fix this issue by replacing the **confidentiality-violating** permission set assignment.



Confidential Data Protection Setup Wizard

Resolve Violations

Based on the current setup, the following violating permission set assignments were found which expose confidential data to one or more of your users. The Confidential Data Protection can resolve the violating permission set assignments by replacing them with assignments to restricted permission sets.

Violations

	Permission Set Role ID	Permission Set Role Name	User Name	User Full Name	User License Type
→	D365 BUS FULL ACCESS	Dyn. 365 Full Business Acc.	DELEGATEDADMIN	Delegated Administrator	Full User

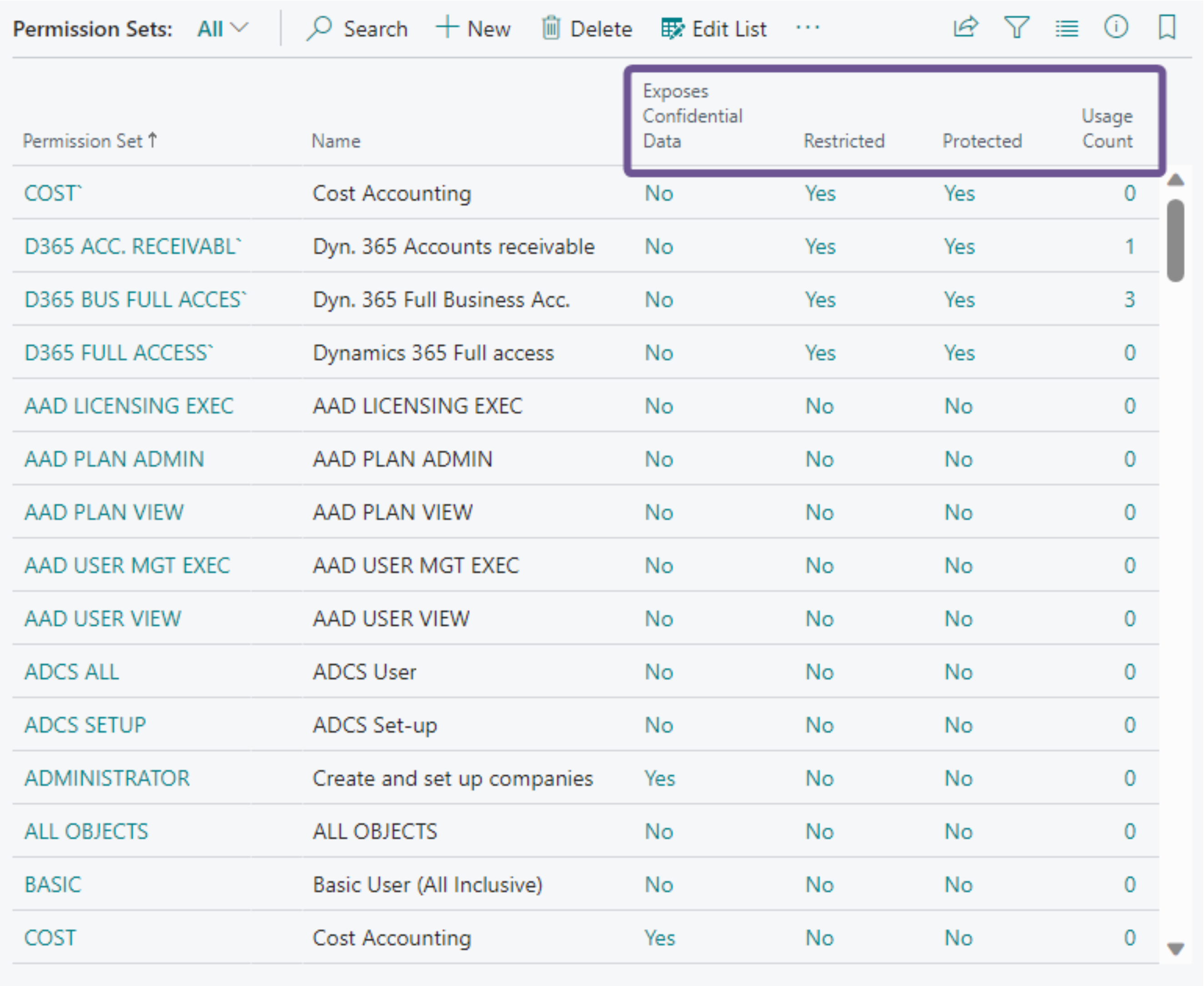
Identify and resolve confidentiality-violating permission set assignments.

- **Permission Set Insights**

  This feature allows you to get better insights into your permission sets and their properties and usages.

  - Easily find out the number of users and/or groups of users that have been assigned a certain permission set.
  - Easily find out which permission sets expose confidential table data, and for which confidential tables these permission sets expose confidential data.
  - Easily find out which restricted permission sets have been generated by the **Confidential Data Protection** extension, and for what reason.

  On the **Permission Sets** page you will also have new fields at your disposal that you can use to filter and sort.



Permission Set ↑	Name	Exposes Confidential Data	Restricted	Protected	Usage Count
COST`	Cost Accounting	No	Yes	Yes	0
D365 ACC. RECEIVABL`	Dyn. 365 Accounts receivable	No	Yes	Yes	1
D365 BUS FULL ACCES`	Dyn. 365 Full Business Acc.	No	Yes	Yes	3
D365 FULL ACCESS`	Dynamics 365 Full access	No	Yes	Yes	0
AAD LICENSING EXEC	AAD LICENSING EXEC	No	No	No	0
AAD PLAN ADMIN	AAD PLAN ADMIN	No	No	No	0
AAD PLAN VIEW	AAD PLAN VIEW	No	No	No	0
AAD USER MGT EXEC	AAD USER MGT EXEC	No	No	No	0
AAD USER VIEW	AAD USER VIEW	No	No	No	0
ADCS ALL	ADCS User	No	No	No	0
ADCS SETUP	ADCS Set-up	No	No	No	0
ADMINISTRATOR	Create and set up companies	Yes	No	No	0
ALL OBJECTS	ALL OBJECTS	No	No	No	0
BASIC	Basic User (All Inclusive)	No	No	No	0
COST	Cost Accounting	Yes	No	No	0

Get better insights into your permission sets, and their properties and usages.

How to Get Started

To get started with the **Confidential Data Protection** extension, you need to install the extension in your Business Central environment from **Microsoft AppSource**. Please note that you can try out the **Confidential Data Protection** extension completely for **free**

by installing it directly from Microsoft AppSource in one of your Business Central **Sandbox** environments; **no trial period, no obligations**!

In our online **Installation Manual** you can find all the instructions you need to install the extension and configure permissions. Then it is just a matter of opening the **Confidential Data Protection Setup Wizard** page and following the steps, as described in the **Setup** section of the installation manual.

For more detailed information about the **Confidential Data Protection** extension, and its features, please check out our **User Manual**.

Contact and Support

We hope you (will) enjoy using the **Confidential Data Protection** extension to help make your business more secure.

If you have any questions or feedback that you would like to share with us, please feel free to reach out to our **Support** team.

Last update: September 5, 2023

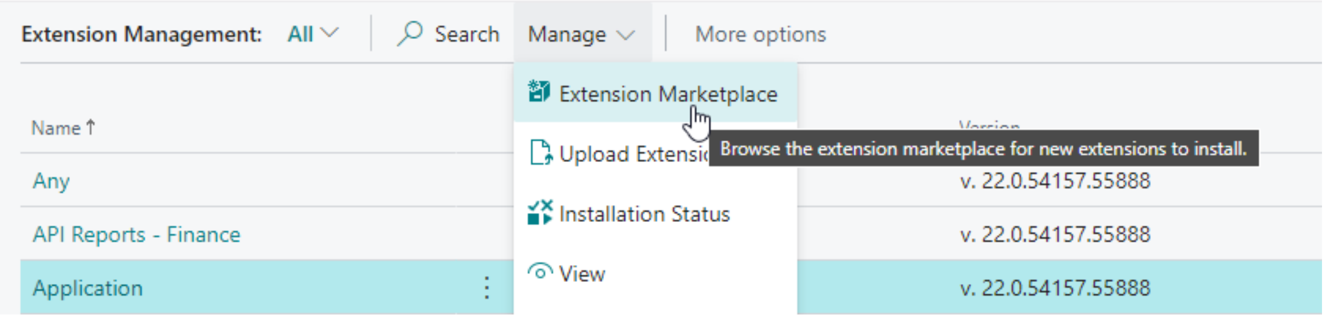
Installing the Extension

The **Confidential Data Protection** extension can be installed for Microsoft Dynamics 365 Business Central (online) or Microsoft Dynamics 365 Business Central on-premises. The installation instructions for both can be found in the following sections.

Microsoft Dynamics 365 Business Central (online)

For Microsoft Dynamics 365 Business Central online, the **Confidential Data Protection** extension can be installed from the **Extension Marketplace (AppSource)**. To install the extension, please follow the following steps:

1. In Microsoft Dynamics 365 Business Central, go to **Setup & Extensions | Extensions** (or, use the *Tell Me* search feature to search for and open the **Extension Management** page).
2. Open the **Extension Marketplace** (AppSource) via: **Manage | Extension Marketplace**



Browse the extension marketplace for new extensions to install.

Name ↑	Version
Any	v. 22.0.54157.55888
API Reports - Finance	v. 22.0.54157.55888
Application	v. 22.0.54157.55888

3. In the page that opens, search for the extension name, "**Confidential Data Protection**", and select it.
4. Please take note of the **End-User License Agreement** and **Privacy Statement**.
5. Choose **FREE TRIAL**, enter your details, and follow the additional steps shown on the **Extension Installation** page that will open in Microsoft Dynamics 365 Business Central.

Microsoft Dynamics 365 Business Central on-premises

For Microsoft Dynamics 365 Business Central on-premises, the extension can be installed using the **Business Central Administration Shell**. Please follow the instructions that can be found on the How to: Publish and Install an Extension v2.0 - Business Central | Microsoft Docs page. If you are upgrading from a previous version, then please see Upgrading Extensions - Business Central | Microsoft Docs for instructions on how to perform an upgrade with the cmdlets of the **Business Central Administration Shell**.

Prerequisites

- Your Business Central license should include the "Apportunix Suite" ISV module.

This ISV module can be added to the license through PartnerSource Business Center by an **Apportunix** reseller.

- Download the latest .app files for the extension and the required libraries ("System Library" and "Monet") for your version of Microsoft Dynamics 365 Business Central.

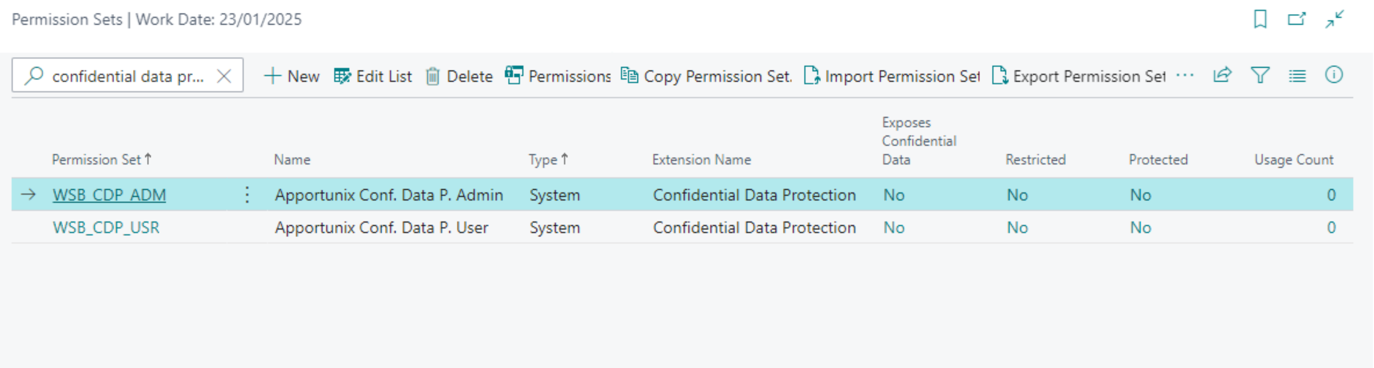
Instructions

1. Download and install the latest (compatible) version of the "System Library" app.
2. Download and install the latest (compatible) version of the "Monet" app.
3. Download and install the latest (compatible) version of the app.

Last update: September 4, 2023

Permission Configuration

After the *Confidential Data Protection* extension has been installed, new permission sets for the extension are added to your Business Central environment.



Permission Sets | Work Date: 23/01/2025

Permission Set ↑	Name	Type ↑	Extension Name	Exposes Confidential Data	Restricted	Protected	Usage Count
WSB_CDP_ADM	Apportunix Conf. Data P. Admin	System	Confidential Data Protection	No	No	No	0
WSB_CDP_USR	Apportunix Conf. Data P. User	System	Confidential Data Protection	No	No	No	0

Info

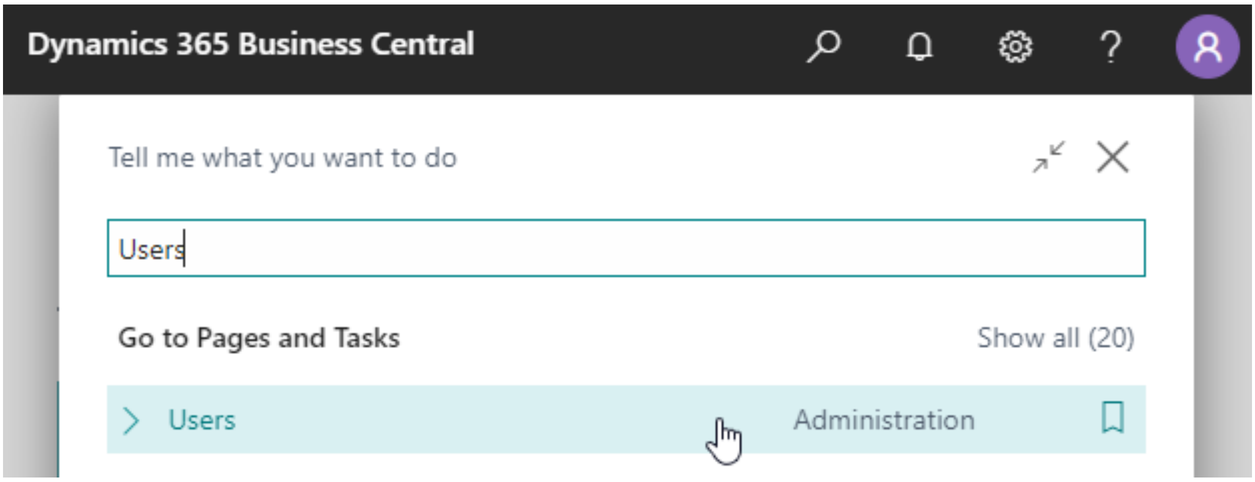
The following permission sets are available:

- `Apportunix Conf. Data P. Admin` - A permission set for a manager or administrator that allows to edit configurations and setup of the extension.
- `Apportunix Conf. Data P. User` - A permission set for users, i.e., allows for using Business Central with the extension installed.

The permission sets should be assigned to relevant users or groups of users.

To assign the permission set to users:

1. Use the **Tell Me** search feature ('magnifying glass icon in the top right corner') to search for and open the **Users** page.



2. Select the user that you want to assign permission to.

   Any permission sets that are already assigned to the user are displayed in the **Permission Sets** factbox.
3. Choose the **Edit** action to open the **User Card** page.
4. On the **User Permission Sets** FastTab, on a new line, fill in the Permission Set field with the permission set for the **Confidential Data Protection** extension.

For more information, please refer to Dynamics 365 Business Central documentation page, Managing Users and Permissions on Microsoft Learn.

Last update: September 5, 2023

License Activation

Important

You can use the extension for **free** in your Business Central **Sandbox** environment. For **Sandbox** environments, you can skip the instructions in this section of the installation manual. Please find more information on the licensing and pricing on our website.

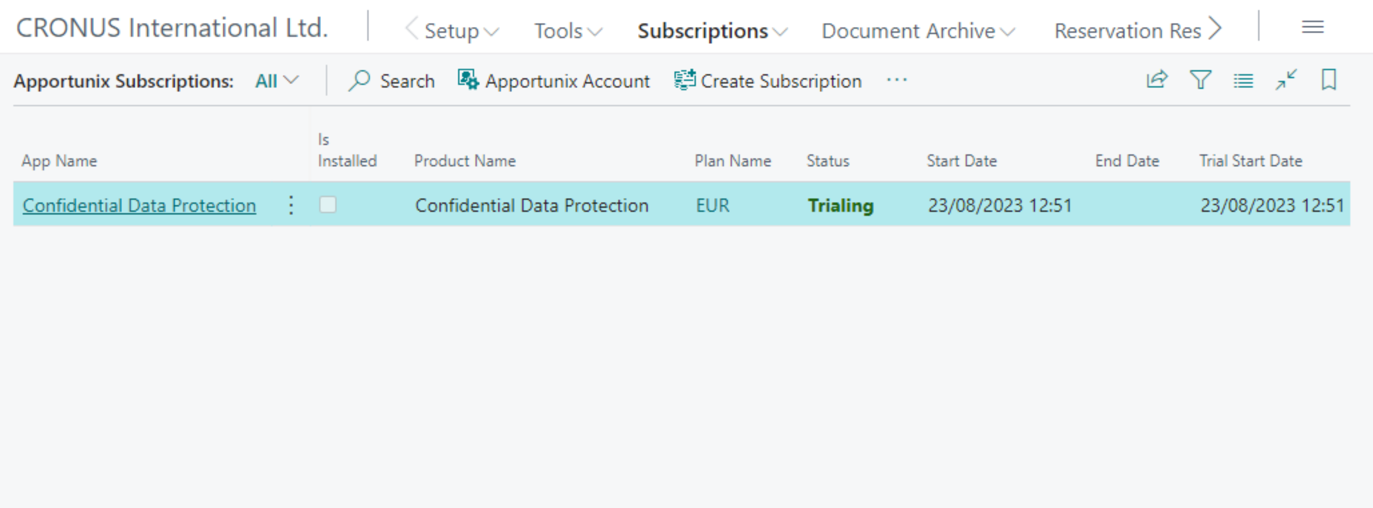
To activate **Confidential Data Protection** for a **Production** environment, please start a subscription via the **Apportunix Subscriptions** page as described in this chapter.

A subscription in a **Production** environment includes a free **trial period**.

This extension can be used for free, without limitations, in one or more of your Dynamics 365 Business Central **Sandbox** environments. When you use features of the extension that would require a subscription for use in one of your **Production** environments, a notification will be displayed that informs you that you are using such a feature.

To use all the features of the extension in a **Production** environment, you can start a free trial subscription that will automatically change to a paid subscription after the trial period ends. You can cancel your subscription at any time you like, and will be able to use the features of the extension until the current invoicing period ends.

To manage your subscriptions, you can use the **Apportunix Subscriptions** page. On this page you can start or cancel subscriptions for Apportunix extensions and view or update the payment methods that are used for your subscriptions.



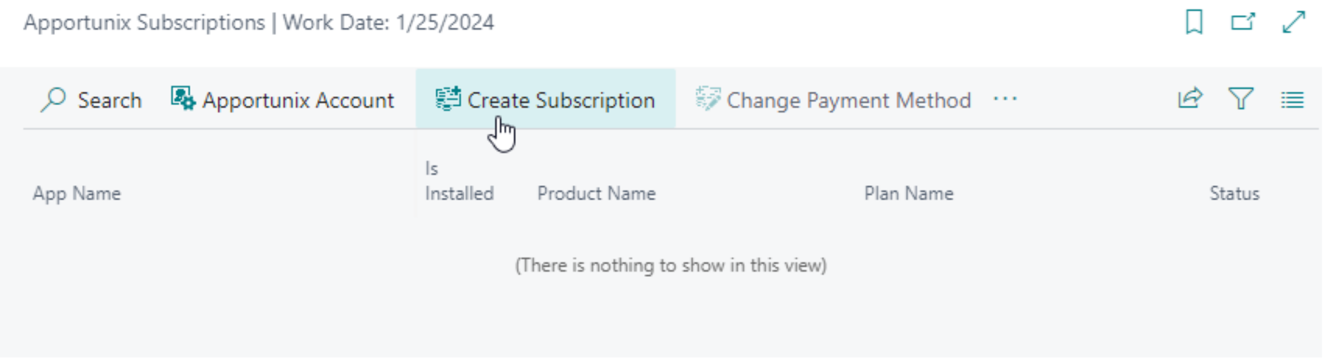
App Name	Is Installed	Product Name	Plan Name	Status	Start Date	End Date	Trial Start Date
Confidential Data Protection	□	Confidential Data Protection	EUR	Trialing	23/08/2023 12:51		23/08/2023 12:51

Please note that your payments are handled safely, in a PCI-compliant manner, in cooperation with our payment provider **Stripe**. For more information, please feel free to contact us by visiting the Contact page on our website.

Create a Subscription

To set up a subscription for the **Confidential Data Protection** extension, in a **Production** environment, please follow these steps:

1. Open the Apportunix Subscriptions page in your Business Central environment.
2. Invoke the **Create Subscription** action, which will open the **Create Subscription** wizard.

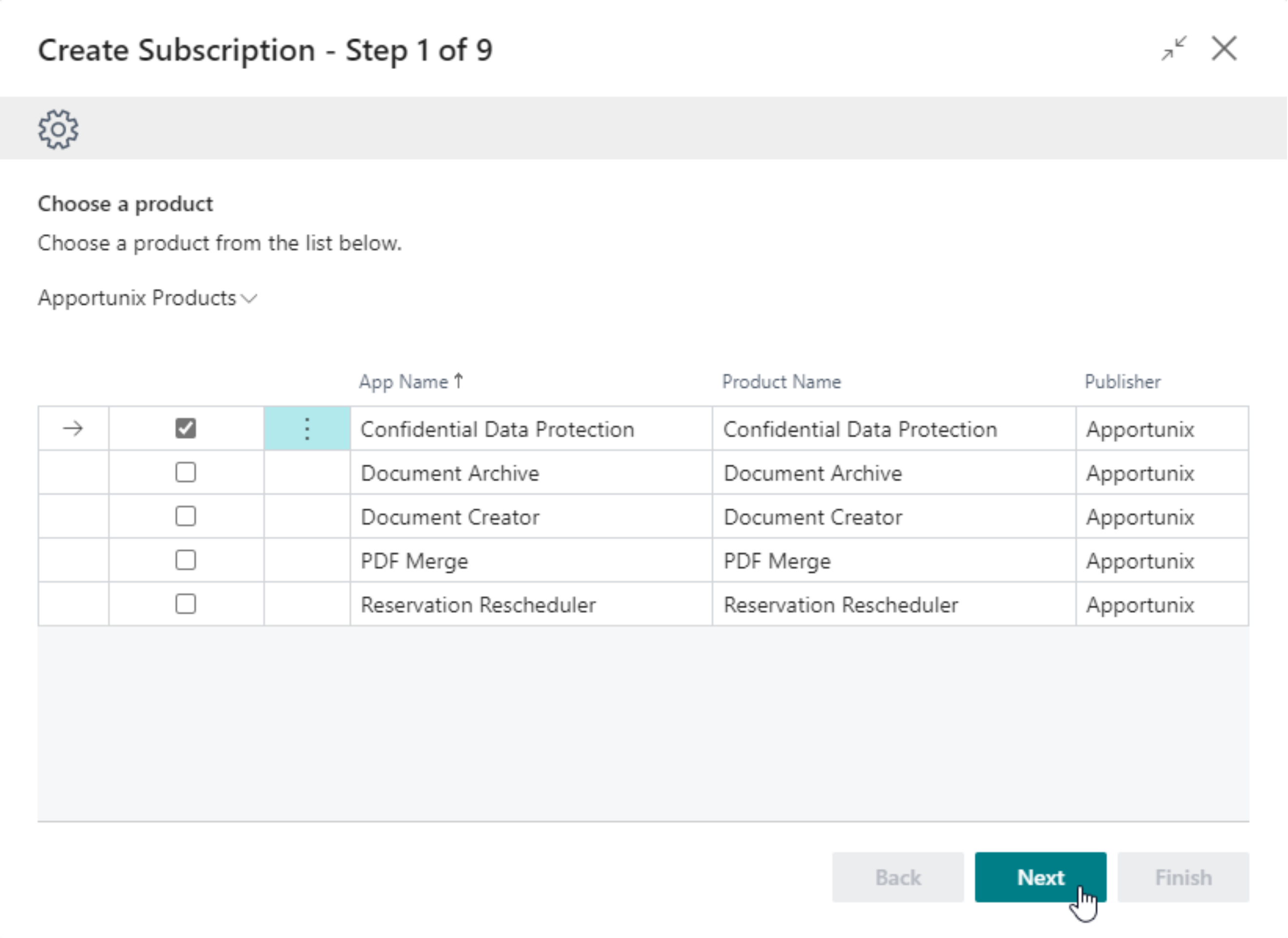


Apportunix Subscriptions | Work Date: 1/25/2024

App Name	Is Installed	Product Name	Plan Name	Status

(There is nothing to show in this view)

3. In the **Create Subscription** wizard, select the product for the **Confidential Data Protection** extension. Then, choose **Next**.



Create Subscription - Step 1 of 9

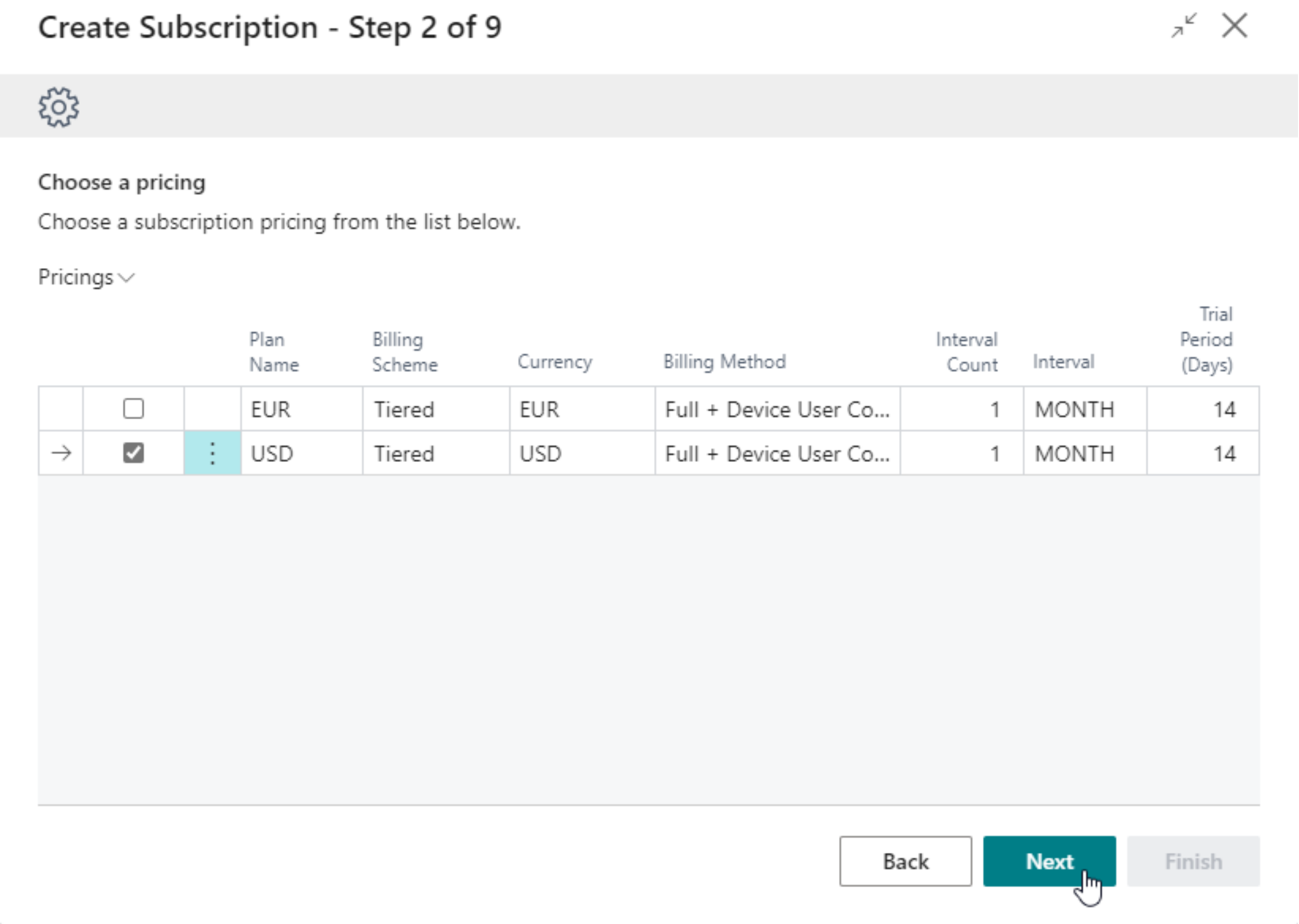
Choose a product

Choose a product from the list below.

Apportunix Products

			App Name ↑	Product Name	Publisher
→	☑	⋮	Confidential Data Protection	Confidential Data Protection	Apportunix
	☐		Document Archive	Document Archive	Apportunix
	☐		Document Creator	Document Creator	Apportunix
	☐		PDF Merge	PDF Merge	Apportunix
	☐		Reservation Rescheduler	Reservation Rescheduler	Apportunix

4. Next, select the plan/pricing for the product that applies for you. Choose **Next**.



Create Subscription - Step 2 of 9

Choose a pricing

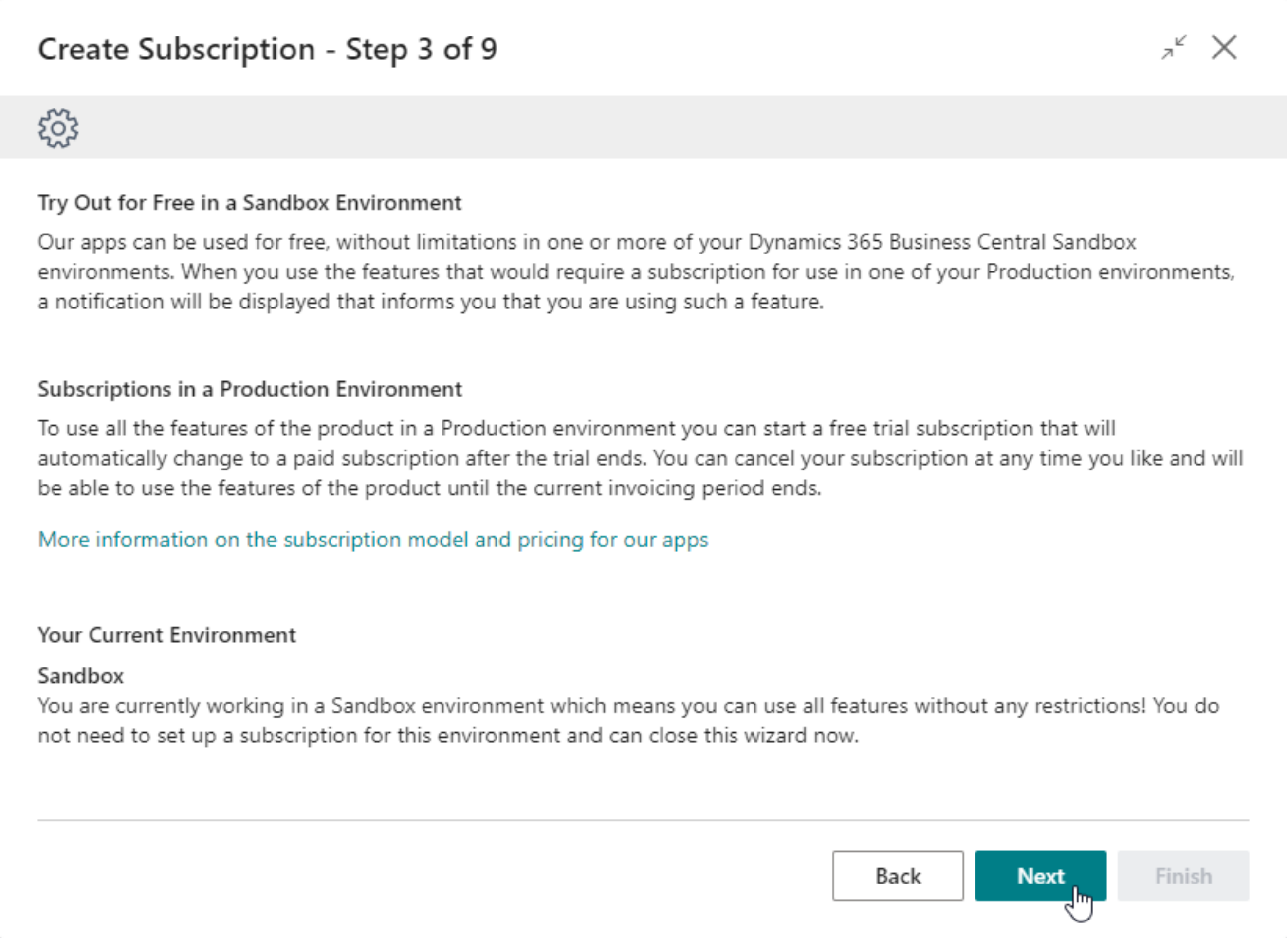
Choose a subscription pricing from the list below.

Pricings

			Plan Name	Billing Scheme	Currency	Billing Method	Interval Count	Interval	Trial Period (Days)
	☐		EUR	Tiered	EUR	Full + Device User Co...	1	MONTH	14
→	☑	⋮	USD	Tiered	USD	Full + Device User Co...	1	MONTH	14

Note: You can find more information about a plan, using the **View** action.

5. Take note of the information in the next step. Note that you only need a subscription for **Production** environments. You can use the extension for free in a **Sandbox** environment.



Create Subscription - Step 3 of 9

Try Out for Free in a Sandbox Environment

Our apps can be used for free, without limitations in one or more of your Dynamics 365 Business Central Sandbox environments. When you use the features that would require a subscription for use in one of your Production environments, a notification will be displayed that informs you that you are using such a feature.

Subscriptions in a Production Environment

To use all the features of the product in a Production environment you can start a free trial subscription that will automatically change to a paid subscription after the trial ends. You can cancel your subscription at any time you like and will be able to use the features of the product until the current invoicing period ends.

More information on the subscription model and pricing for our apps

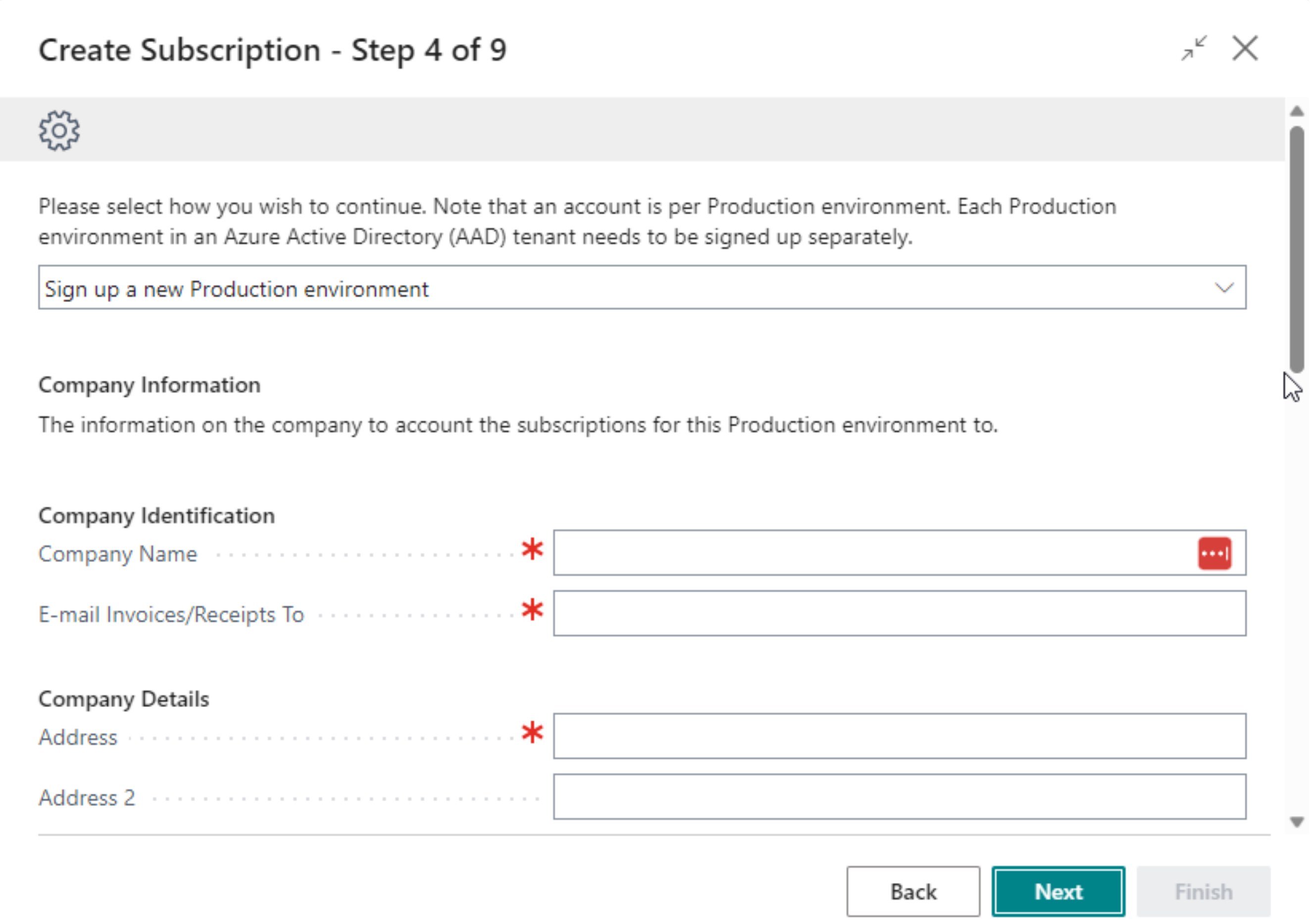
Your Current Environment

Sandbox

You are currently working in a Sandbox environment which means you can use all features without any restrictions! You do not need to set up a subscription for this environment and can close this wizard now.

If you are in a **Production** environment and wish to create a subscription, choose **Next**.

6. Enter your company information. Make sure to enter a correct **Tax ID** and **Tax ID Type** combination.



Create Subscription - Step 4 of 9

Please select how you wish to continue. Note that an account is per Production environment. Each Production environment in an Azure Active Directory (AAD) tenant needs to be signed up separately.

Sign up a new Production environment

Company Information

The information on the company to account the subscriptions for this Production environment to.

Company Identification

Company Name *

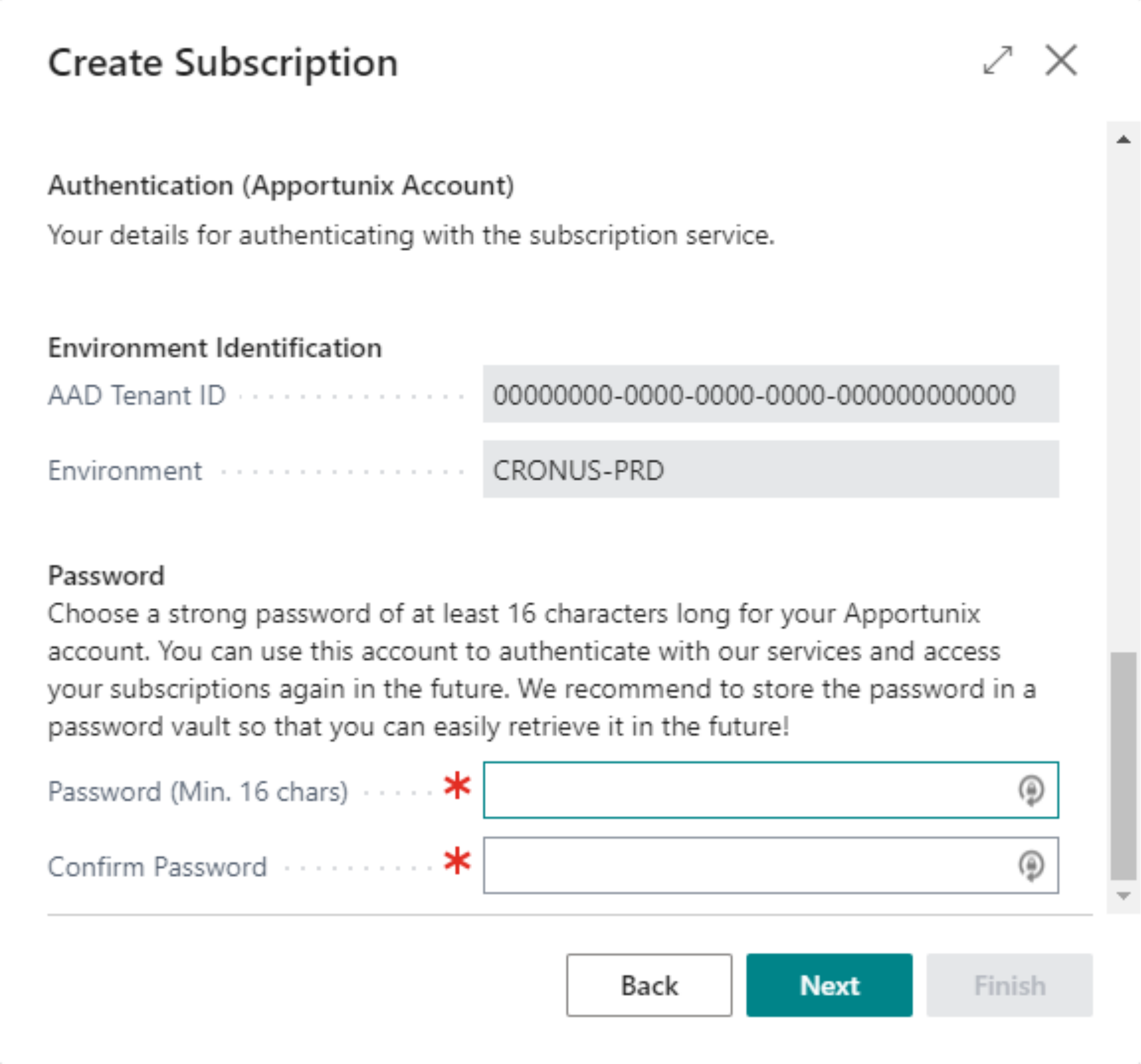
E-mail Invoices/Receipts To *

Company Details

Address *

Address 2

7. Also, choose a strong password and store/remember it well, as you will need it if you want to make any changes at a later time.



Create Subscription

Authentication (Apportunix Account)

Your details for authenticating with the subscription service.

Environment Identification

AAD Tenant ID: 00000000-0000-0000-0000-000000000000

Environment: CRONUS-PRD

Password

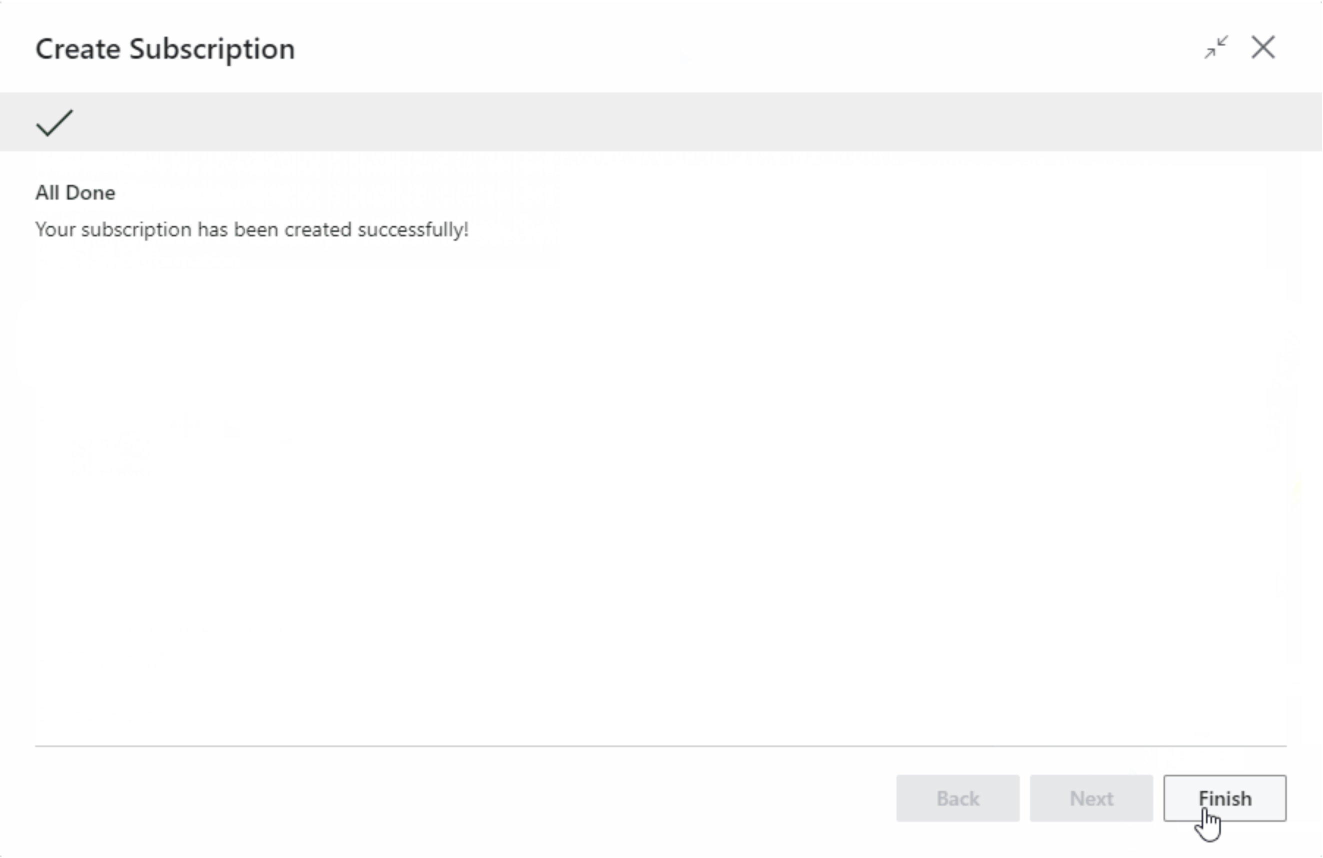
Choose a strong password of at least 16 characters long for your Apportunix account. You can use this account to authenticate with our services and access your subscriptions again in the future. We recommend to store the password in a password vault so that you can easily retrieve it in the future!

Password (Min. 16 chars) *

Confirm Password *

8. Follow and finish the remainder of the wizard.

   When you are done you will be met with the final step of the wizard that informs you that the subscription was set up successfully and you are ready to go.



Create Subscription

All Done

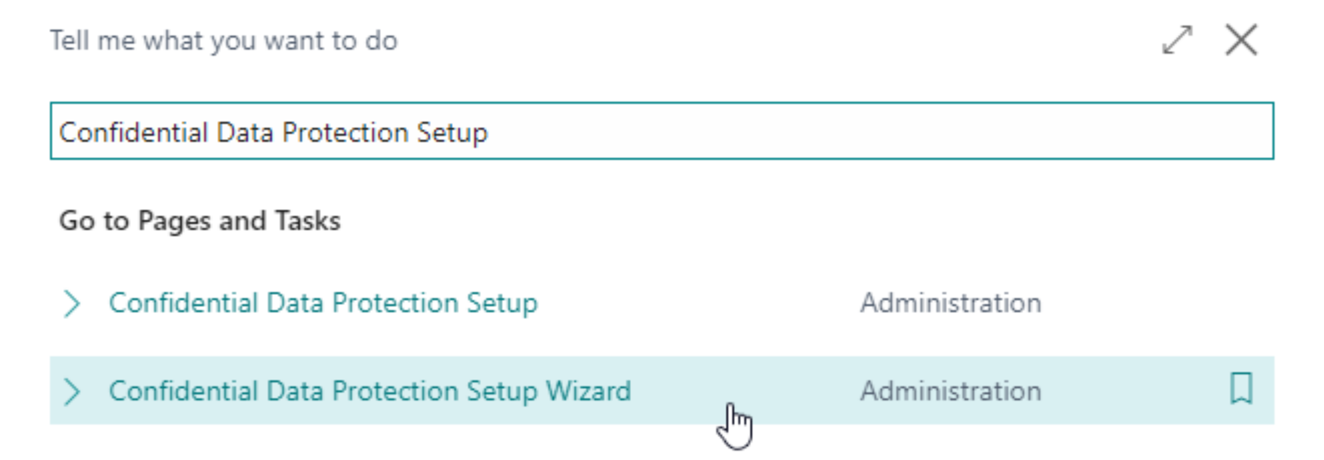
Your subscription has been created successfully!

Last update: September 7, 2023

Setup

Confidential Data Protection has an integrated setup wizard to assist you with the initial configuration of the extension. It is recommended to use the setup wizard page to set up the extension.

1. Search for and open the **Confidential Data Protection Setup Wizard** page using the **Tell Me** search feature.



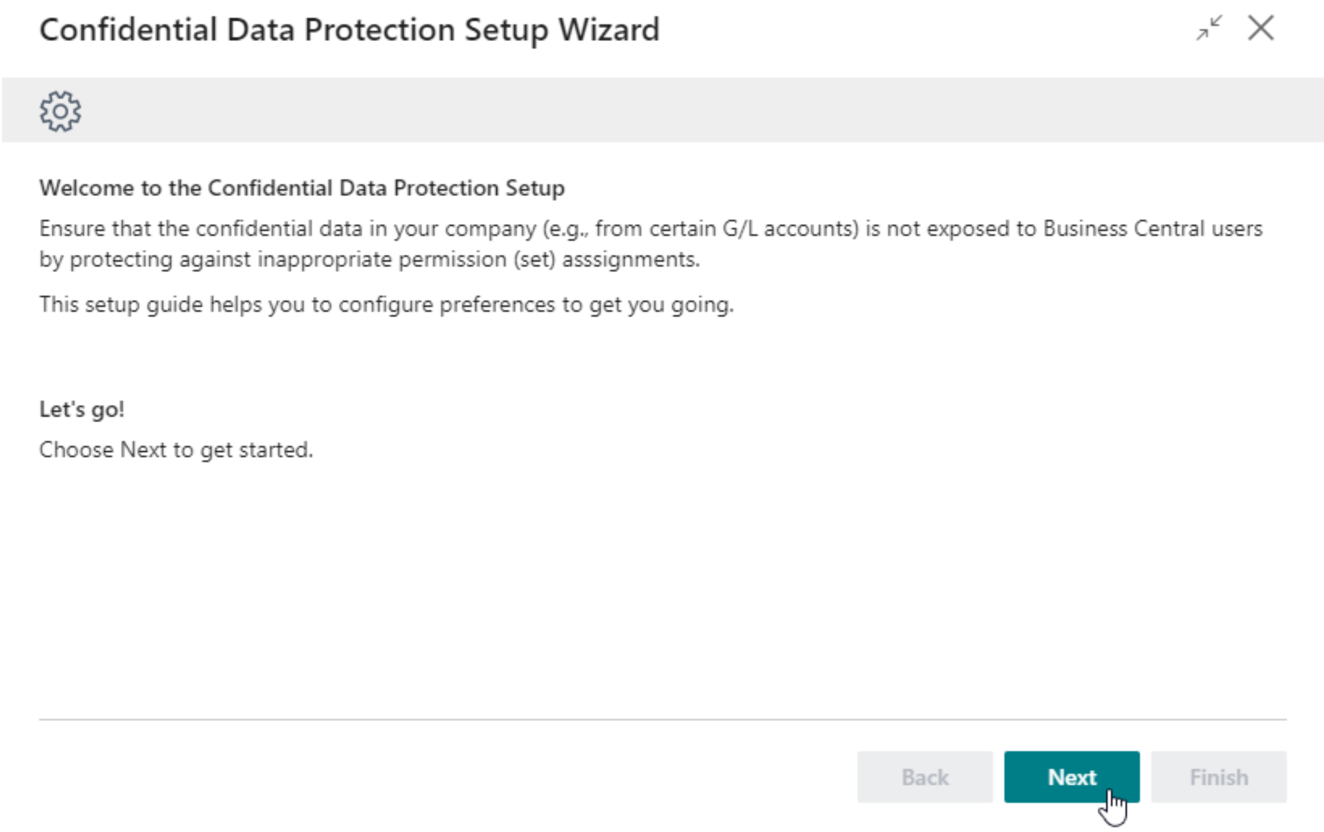
Tell me what you want to do

Confidential Data Protection Setup

Go to Pages and Tasks

Confidential Data Protection Setup	Administration
Confidential Data Protection Setup Wizard	Administration

2. Read the introduction and click on **Next** to move on to the next step.



Confidential Data Protection Setup Wizard

Welcome to the Confidential Data Protection Setup

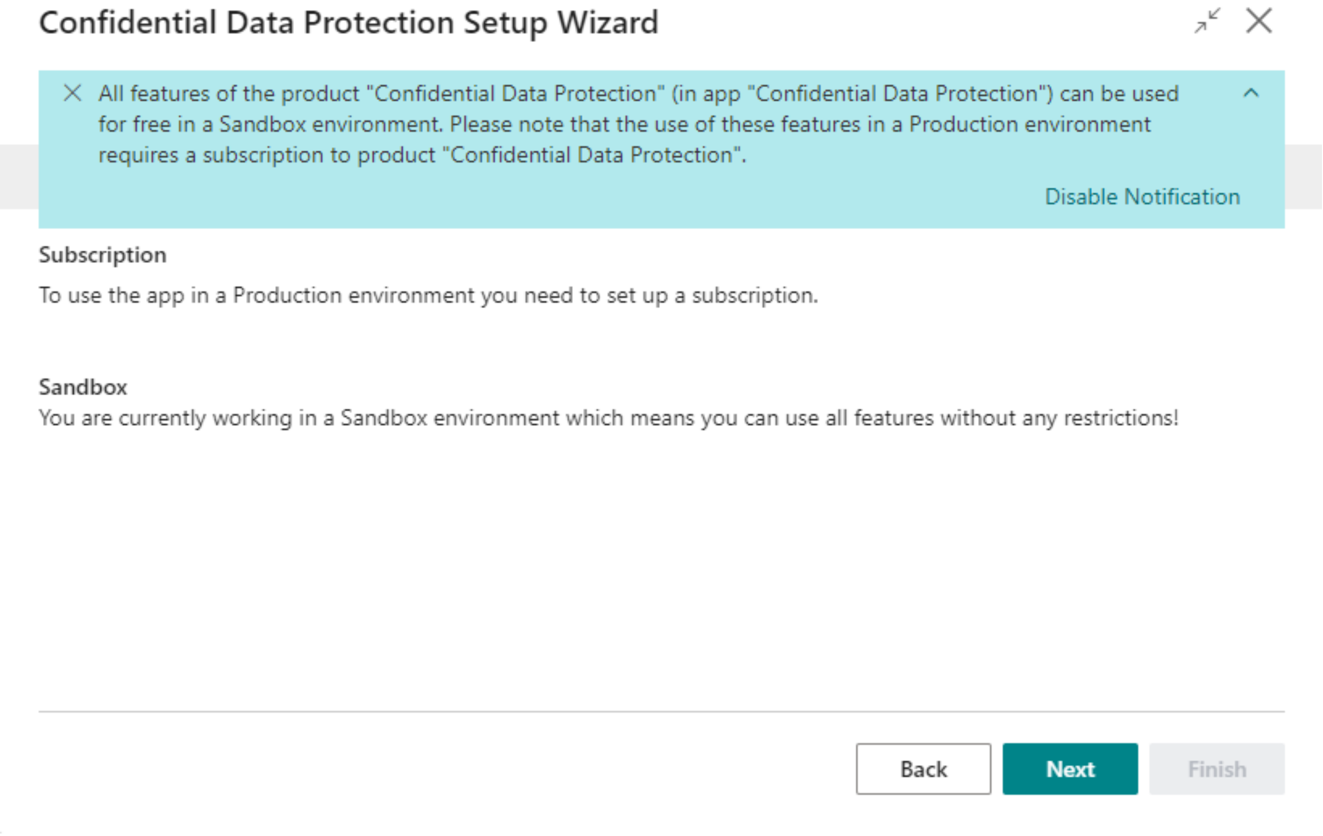
Ensure that the confidential data in your company (e.g., from certain G/L accounts) is not exposed to Business Central users by protecting against inappropriate permission (set) assignments.

This setup guide helps you to configure preferences to get you going.

Let's go!

Choose Next to get started.

3. Read the information about the extension being free-to-use in **Sandbox** environments and requiring a subscription in **Production** environments and choose **Next** to move on to the next step.



Confidential Data Protection Setup Wizard

All features of the product "Confidential Data Protection" (in app "Confidential Data Protection") can be used for free in a Sandbox environment. Please note that the use of these features in a Production environment requires a subscription to product "Confidential Data Protection".

Subscription

To use the app in a Production environment you need to set up a subscription.

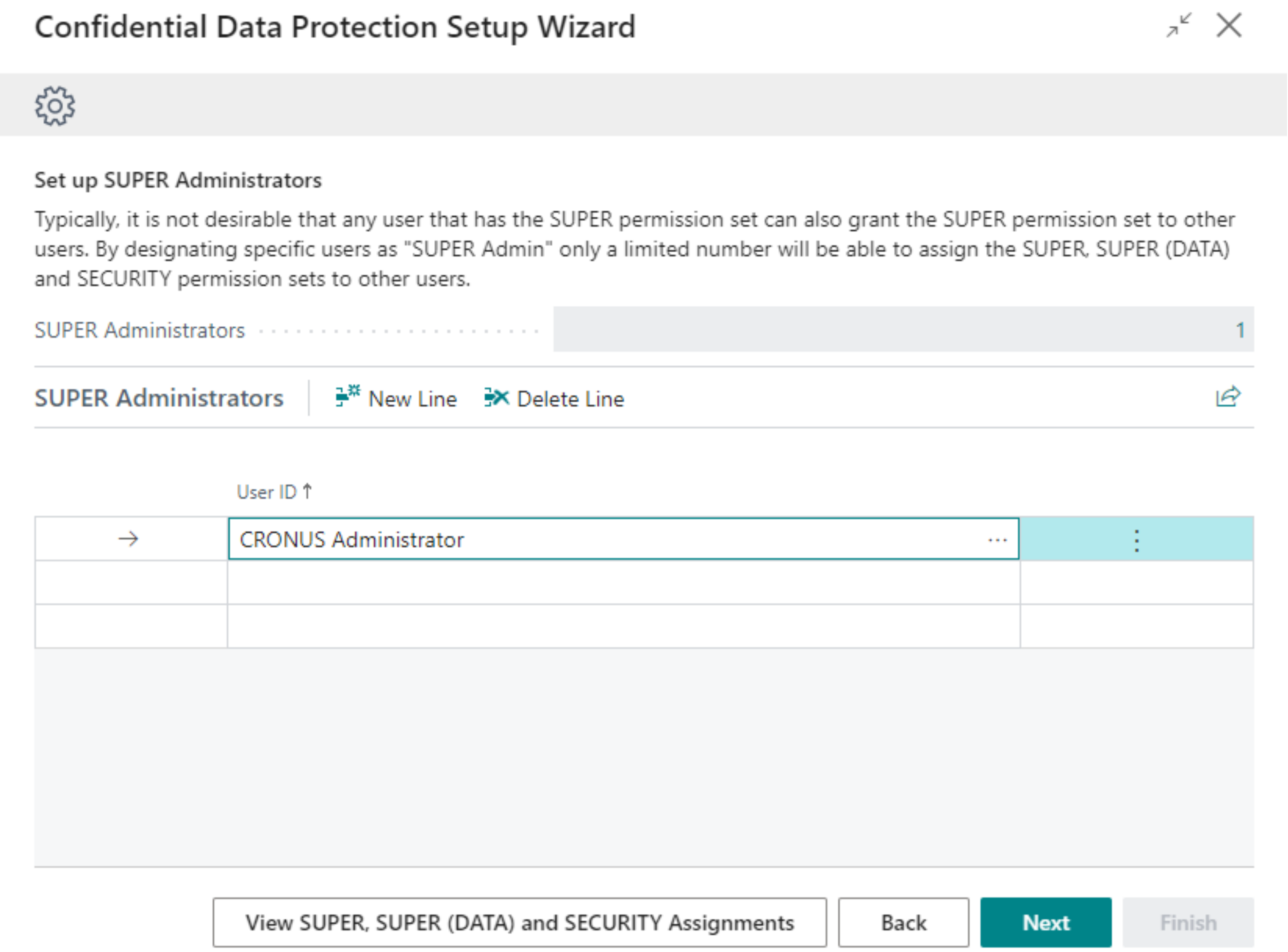
Sandbox

You are currently working in a Sandbox environment which means you can use all features without any restrictions!

4. SUPER Administrators

The **Set up Super Administrators** step of the setup wizard allows you to assign SUPER administrators for your Business Central environment.

A **SUPER administrator** is a user that is allowed to assign the **SUPER**, **SUPER (DATA)** and **SECURITY** permission set to users in your Business Central environment. Please find more information about these special permission sets in the Special permission sets section on Microsoft Learn.



Set up SUPER Administrators

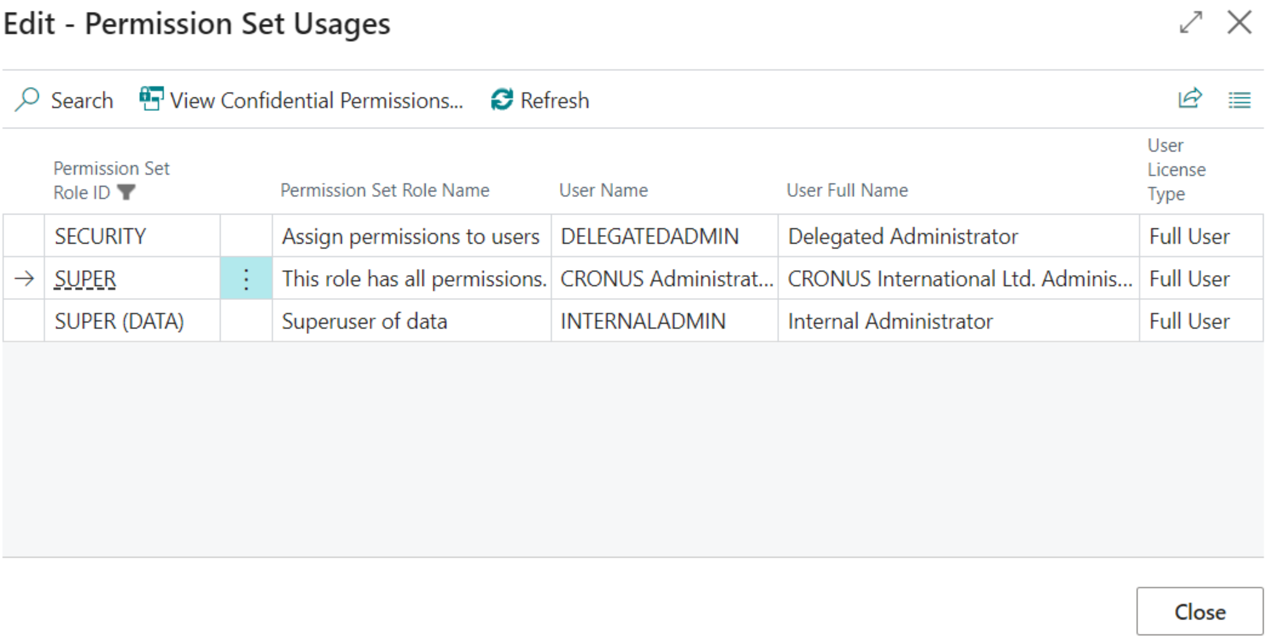
Typically, it is not desirable that any user that has the SUPER permission set can also grant the SUPER permission set to other users. By designating specific users as "SUPER Admin" only a limited number will be able to assign the SUPER, SUPER (DATA) and SECURITY permission sets to other users.

SUPER Administrators: 1

User ID ↑
CRONUS Administrator

You can configure zero, one or multiple SUPER administrators. If no SUPER administrators have been configured, then any user that has the **SUPER** permission set assigned will be able to assign the permission sets to other users, like would normally be the case.

Note that you can use the **View SUPER, SUPER (DATA) and SECURITY Assignments** action in this step to view the users that currently have the SUPER, SUPER (DATA) and/or SECURITY permission sets assigned.



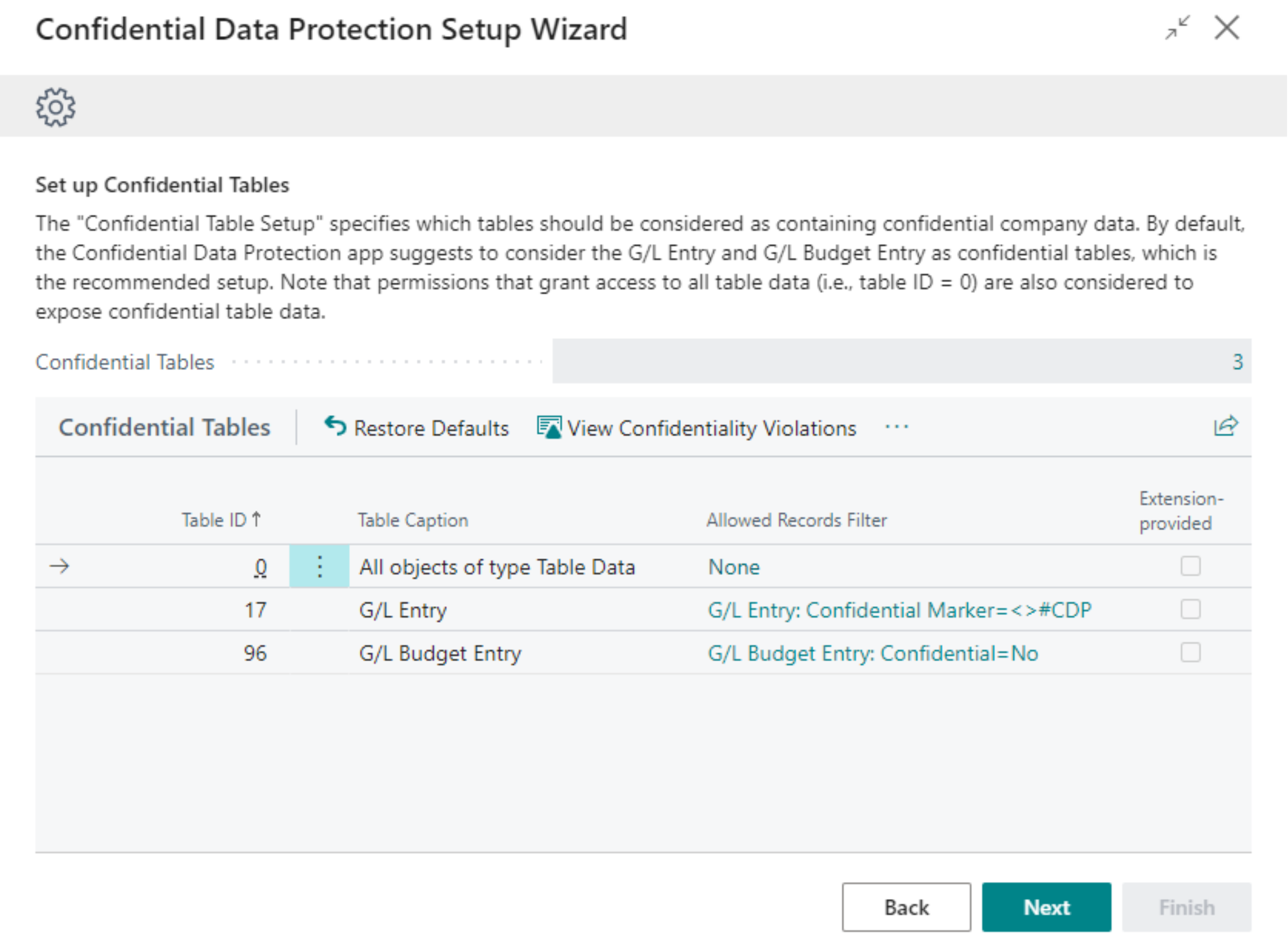
Edit - Permission Set Usages

	Permission Set Role ID		Permission Set Role Name	User Name	User Full Name	User License Type
	SECURITY		Assign permissions to users	DELEGATEDADMIN	Delegated Administrator	Full User
→	SUPER	⋮	This role has all permissions.	CRONUS Administrat...	CRONUS International Ltd. Adminis...	Full User
	SUPER (DATA)		Superuser of data	INTERNALADMIN	Internal Administrator	Full User

After configuring the SUPER administrators for your Business Central environment, choose **Next** to move on to the next step.

5. Confidential Tables Setup

In the **Set up Confidential Tables** step you can view which tables are considered to contain confidential data by the **Confidential Data Protection** extension.



Confidential Data Protection Setup Wizard

Set up Confidential Tables

The "Confidential Table Setup" specifies which tables should be considered as containing confidential company data. By default, the Confidential Data Protection app suggests to consider the G/L Entry and G/L Budget Entry as confidential tables, which is the recommended setup. Note that permissions that grant access to all table data (i.e., table ID = 0) are also considered to expose confidential table data.

Confidential Tables: 3

Confidential Tables | Restore Defaults | View Confidentiality Violations

	Table ID ↑	Table Caption	Allowed Records Filter	Extension-provided
→	0	All objects of type Table Data	None	□
	17	G/L Entry	G/L Entry: Confidential Marker=<>#CDP	□
	96	G/L Budget Entry	G/L Budget Entry: Confidential=No	□

By default, the **G/L Entry** table and **G/L Budget Entry** tables are considered to contain confidential data (and they are part of the recommended default setup). This means that **Table Data Direct Read** permission assignments for these tables are considered confidentiality-violating permission assignments as they would grant users access to confidential data in Business Central.

For tables where only some records contain confidential data, the **Allowed Records Filter** field is used to specify which records are allowed to be accessed by users, i.e., which records in the table are non-confidential.

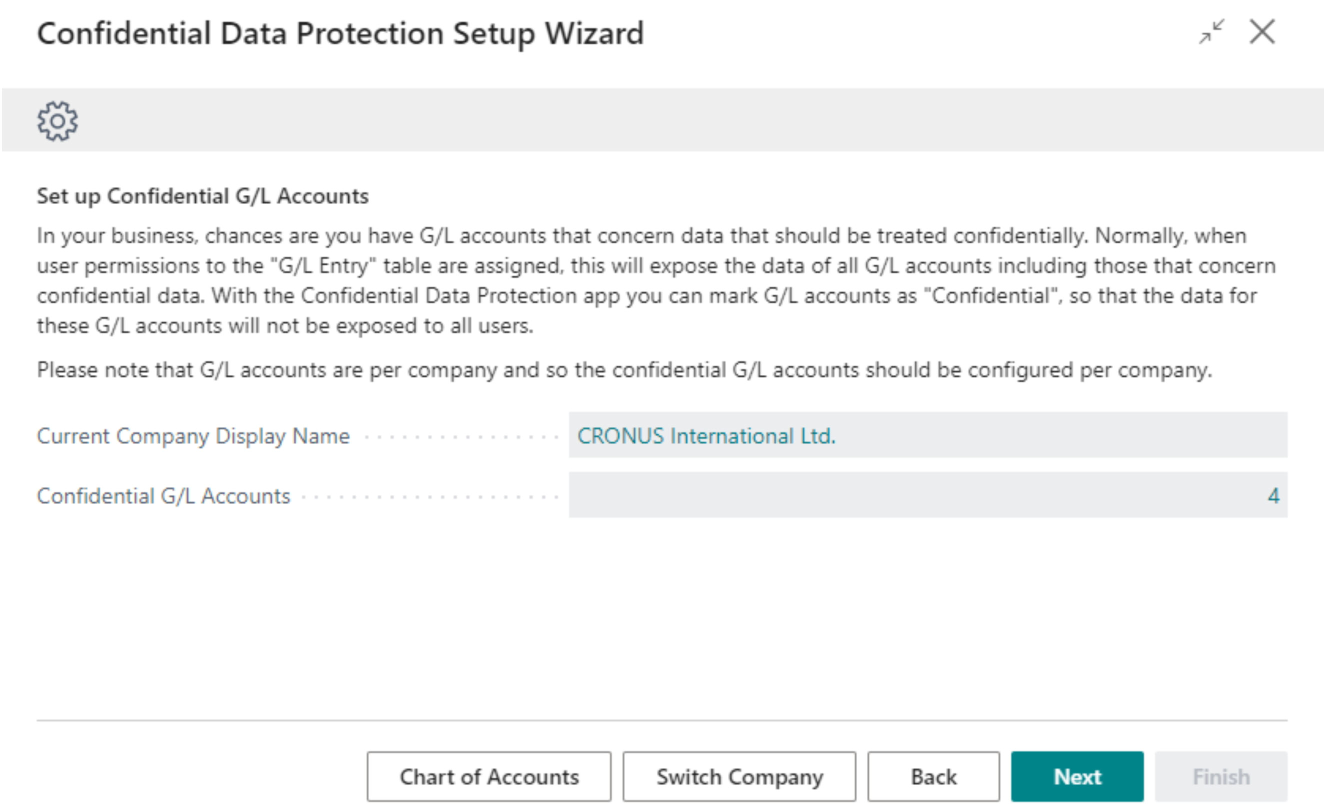
Note that permission assignments that grant access to all table data (i.e., a permission assignment for table ID = 0) are always considered to expose confidential table data.

For more detailed information, please see the Confidential Tables Setup section in the user manual.

Choose **Next** to move on to the next step.

6. Confidential G/L Accounts

In the **Set up Confidential G/L Accounts** step you can configure your preferences for access to G/L account/entry data. With the **Confidential Data Protection** extension installed, you can mark specific G/L accounts as **Confidential** for those G/L accounts where the related G/L entries contain confidential data.



Set up Confidential G/L Accounts

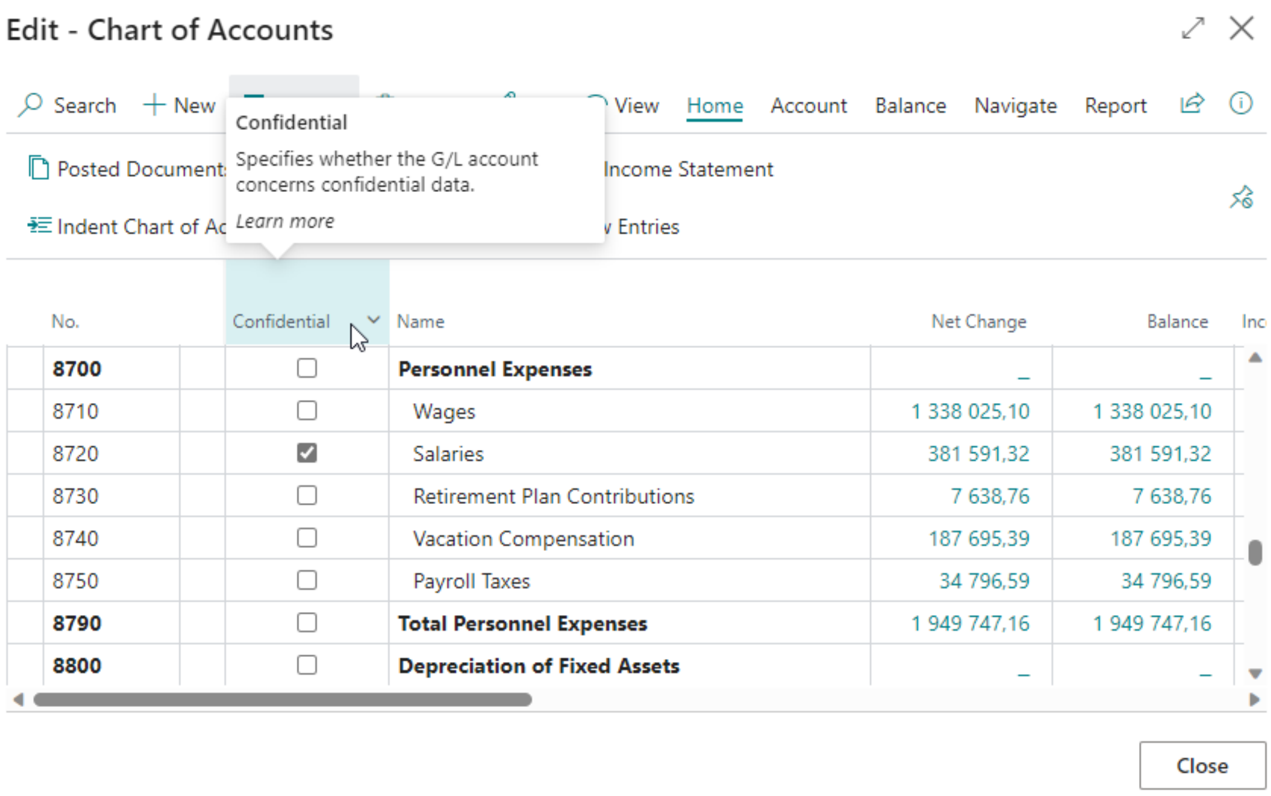
In your business, chances are you have G/L accounts that concern data that should be treated confidentially. Normally, when user permissions to the "G/L Entry" table are assigned, this will expose the data of all G/L accounts including those that concern confidential data. With the Confidential Data Protection app you can mark G/L accounts as "Confidential", so that the data for these G/L accounts will not be exposed to all users.

Please note that G/L accounts are per company and so the confidential G/L accounts should be configured per company.

Current Company Display Name: CRONUS International Ltd.

Confidential G/L Accounts: 4

The Confidential G/L Accounts field will display the number of G/L accounts that have been marked as **Confidential**. By drilling down on the field, you can open the **Chart of Accounts** page and use the **Confidential** field to mark G/L accounts that contain confidential data.



Confidential

Specifies whether the G/L account concerns confidential data.

Learn more

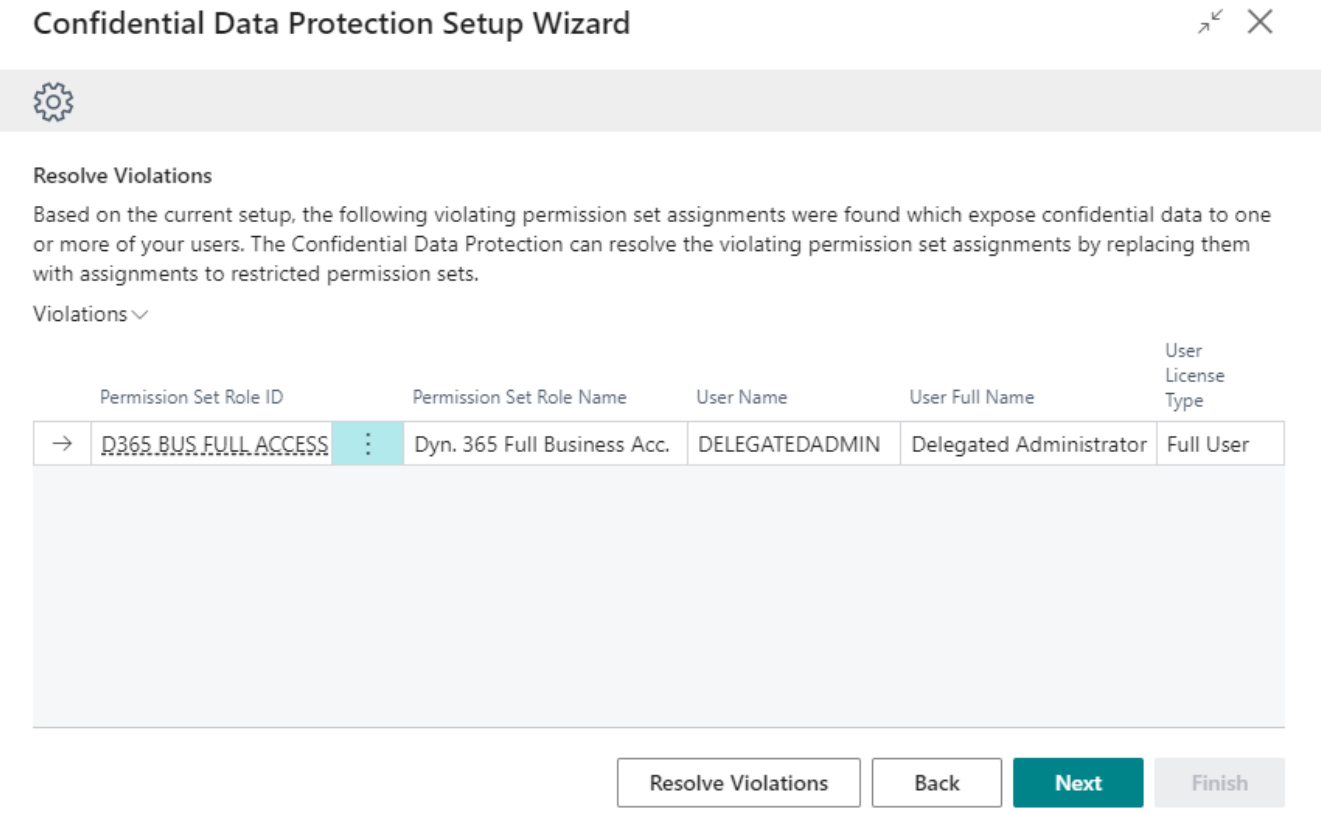
No.	Confidential	Name	Net Change	Balance
8700	☐	**Personnel Expenses**	_	_
8710	☐	Wages	1 338 025,10	1 338 025,10
8720	☑	Salaries	381 591,32	381 591,32
8730	☐	Retirement Plan Contributions	7 638,76	7 638,76
8740	☐	Vacation Compensation	187 695,39	187 695,39
8750	☐	Payroll Taxes	34 796,59	34 796,59
8790	☐	**Total Personnel Expenses**	1 949 747,16	1 949 747,16
8800	☐	**Depreciation of Fixed Assets**	_	_

For more detailed information, please see the Confidential G/L Accounts section in the user manual.

After configuring G/L accounts as **confidential** G/L accounts to preferences, choose **Next** to move on to the next step.

7. Identify and Resolve Violations

Based on your setup in the previous step, the **Resolve Violations** step will show you the identified confidentiality-violating permission (set) assignments, and help you to get these violations resolved.



Confidential Data Protection Setup Wizard

Resolve Violations

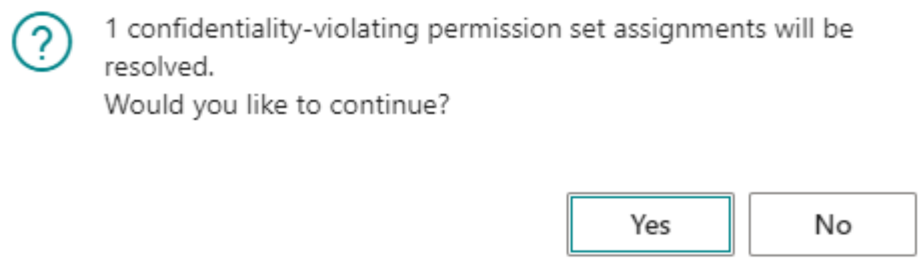
Based on the current setup, the following violating permission set assignments were found which expose confidential data to one or more of your users. The Confidential Data Protection can resolve the violating permission set assignments by replacing them with assignments to restricted permission sets.

Violations

	Permission Set Role ID	Permission Set Role Name	User Name	User Full Name	User License Type
→	D365 BUS FULL ACCESS	Dyn. 365 Full Business Acc.	DELEGATEDADMIN	Delegated Administrator	Full User

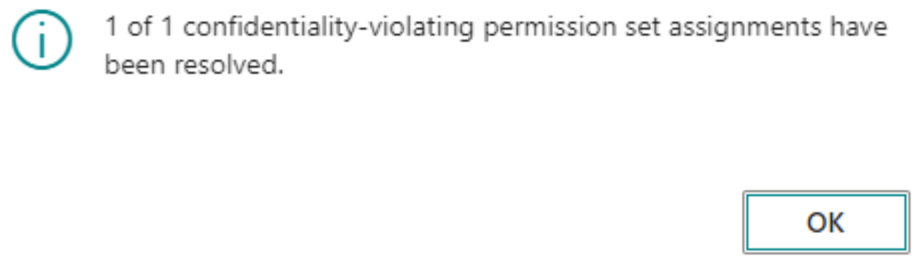
When you first open this step of the wizard the listpart page will show you the confidentiality-violating permission (set) assignments, i.e., assignments of a permission set that grants access to confidential table data to users.

Invoke the **Resolve Violations** actions to resolve the identified violations. After you invoke the action, you will first get a confirmation dialog which prompts you to confirm the action.



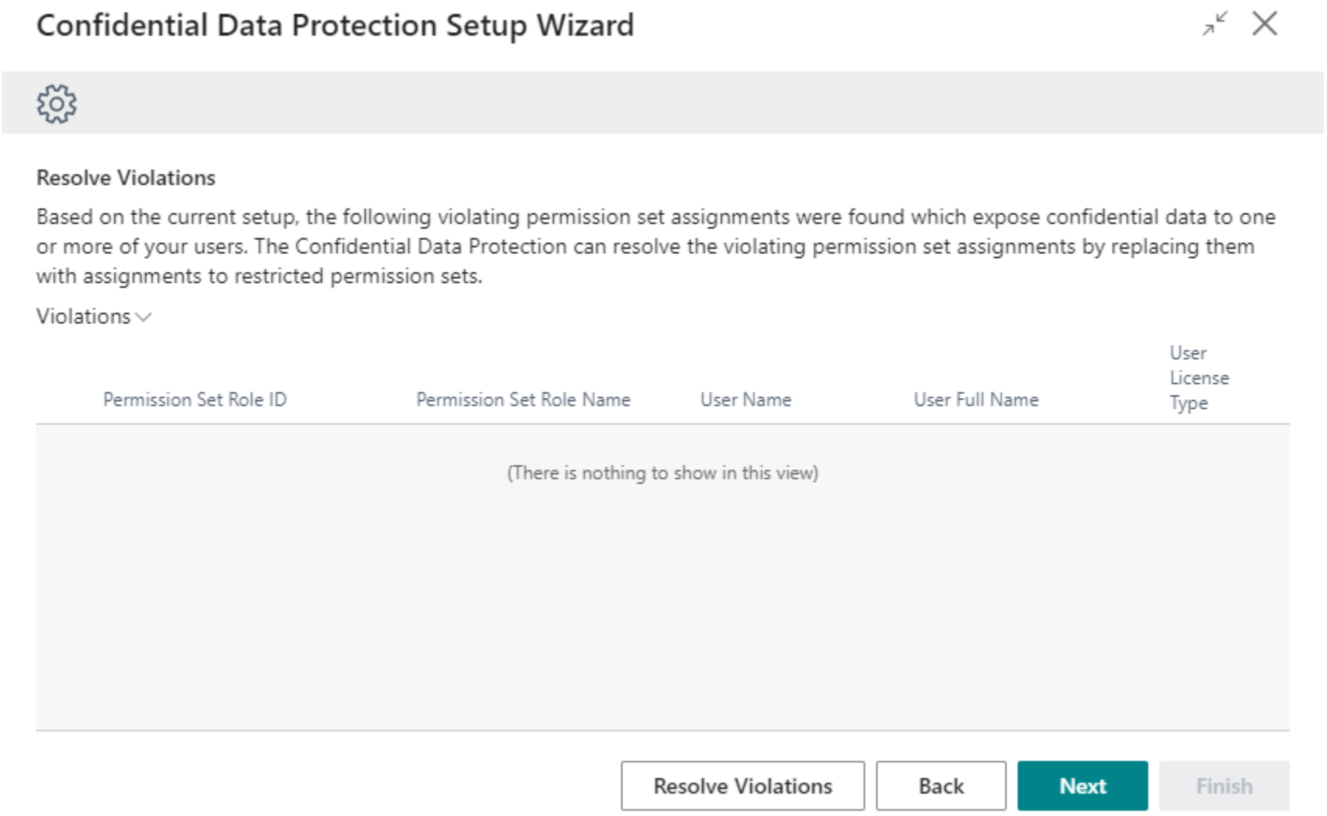
1 confidentiality-violating permission set assignments will be resolved.
Would you like to continue?

Choose **Yes** to allow the **Confidential Data Protection** extension to resolve the violations. During this action, each confidentiality-violating permission set assigned to users (or groups of users) will be replaced by a new, restricted permission set, derived from the original permission set, but without exposing confidential data.



1 of 1 confidentiality-violating permission set assignments have been resolved.

After the action has completed and the page is refreshed, all confidentiality-violating permission set assignments will have been resolved.



Confidential Data Protection Setup Wizard

Resolve Violations

Based on the current setup, the following violating permission set assignments were found which expose confidential data to one or more of your users. The Confidential Data Protection can resolve the violating permission set assignments by replacing them with assignments to restricted permission sets.

Violations

Permission Set Role ID	Permission Set Role Name	User Name	User Full Name	User License Type

(There is nothing to show in this view)

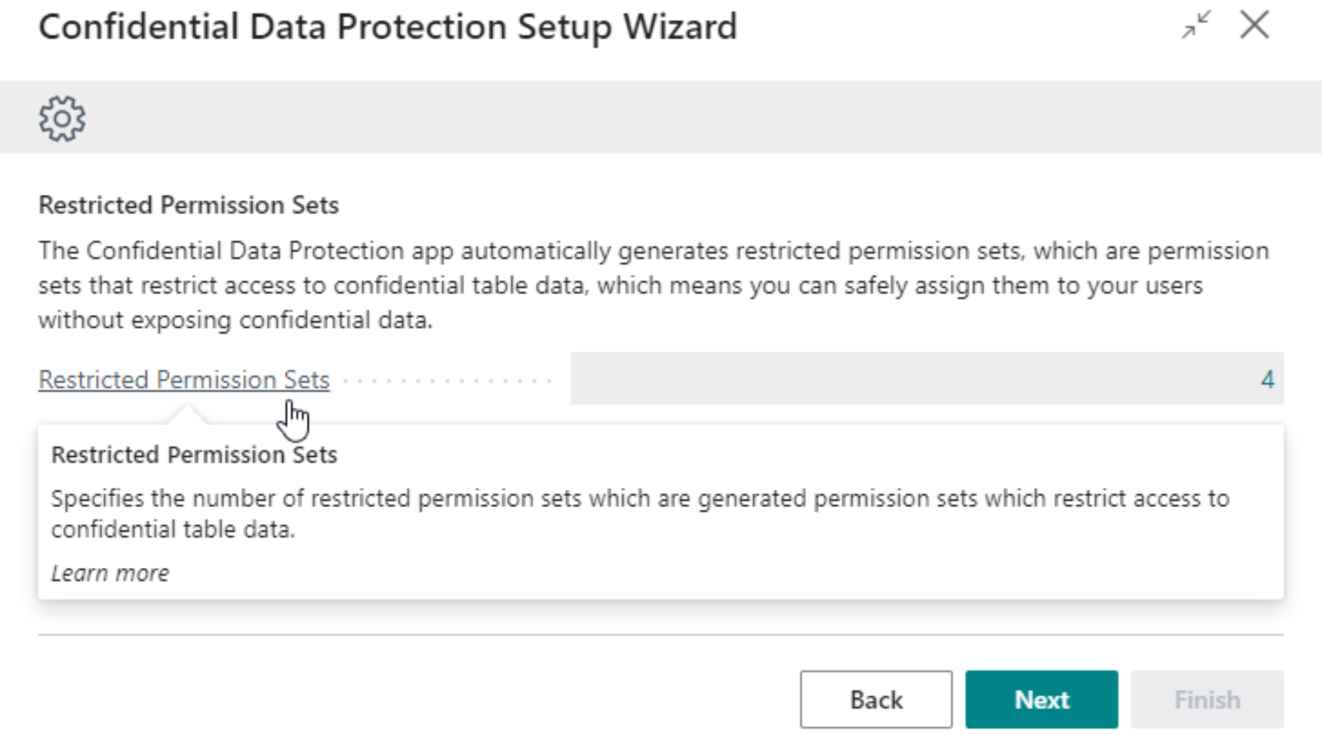
For more information, please also see the Identify and Resolve Violations section in the user manual.

Choose **Next** to move on to the next step of the wizard.

8. Restricted Permission Sets

The **Confidential Data Protection** extension automatically generates **Restricted Permission Sets**, which are permission sets in which the access that would be granted to confidential tables has been restricted, making them safe to assign to users without exposing confidential data.

The **Restricted Permission Sets** field displays the total number of restricted permission sets.



Confidential Data Protection Setup Wizard

Restricted Permission Sets

The Confidential Data Protection app automatically generates restricted permission sets, which are permission sets that restrict access to confidential table data, which means you can safely assign them to your users without exposing confidential data.

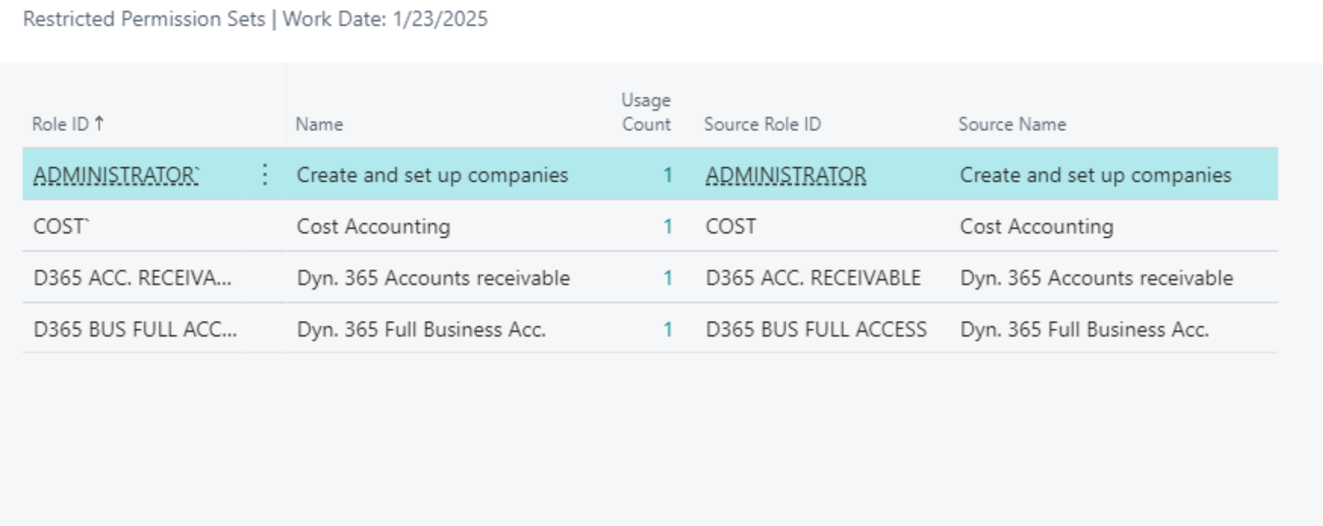
Restricted Permission Sets: 4

Restricted Permission Sets

Specifies the number of restricted permission sets which are generated permission sets which restrict access to confidential table data.

Learn more

You can drilldown on this field which will open the **Restricted Permission Sets** page where you can view all restricted permission sets in your Business Central environment. On this page you can also view the **Confidential** (source) permission set that the **Restricted** permission set was derived from, if any, and how many times the permission set is used/assigned.



Restricted Permission Sets | Work Date: 1/23/2025

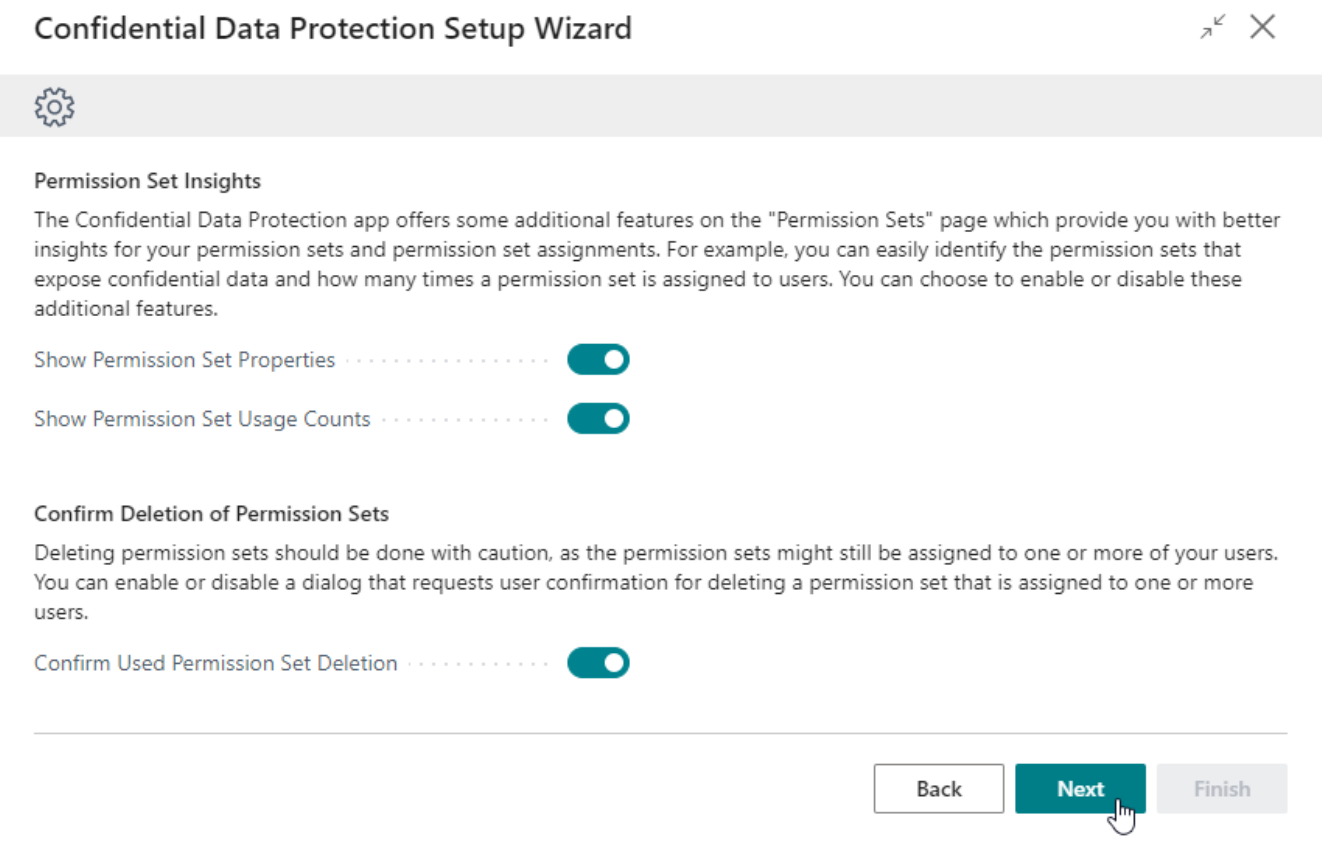
Role ID ↑	Name	Usage Count	Source Role ID	Source Name
ADMINISTRATOR`	Create and set up companies	1	ADMINISTRATOR	Create and set up companies
COST`	Cost Accounting	1	COST	Cost Accounting
D365 ACC. RECEIVA...	Dyn. 365 Accounts receivable	1	D365 ACC. RECEIVABLE	Dyn. 365 Accounts receivable
D365 BUS FULL ACC...	Dyn. 365 Full Business Acc.	1	D365 BUS FULL ACCESS	Dyn. 365 Full Business Acc.

For more detailed information, please see the Restricted Permission Sets section in the user manual.

Choose **Next** to move on to the next step of the wizard.

9. Additional Properties on the Permission Sets Page

In the next step of the setup wizard page you will find some more setup options that you can use to configure additional preferences.



Confidential Data Protection Setup Wizard

Permission Set Insights

The Confidential Data Protection app offers some additional features on the "Permission Sets" page which provide you with better insights for your permission sets and permission set assignments. For example, you can easily identify the permission sets that expose confidential data and how many times a permission set is assigned to users. You can choose to enable or disable these additional features.

Show Permission Set Properties ●

Show Permission Set Usage Counts ●

Confirm Deletion of Permission Sets

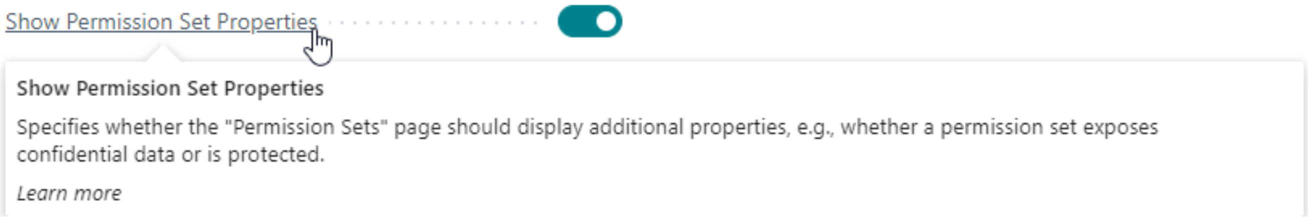
Deleting permission sets should be done with caution, as the permission sets might still be assigned to one or more of your users. You can enable or disable a dialog that requests user confirmation for deleting a permission set that is assigned to one or more users.

Confirm Used Permission Set Deletion ●

In the **Permission Set Insights** tab you will find feature toggles that can be used to enable/display or disable/hide additional properties on the **Permission Sets** page. These properties can provide you with additional insights into properties and usage/assignments of permission sets.

Show Permission Set Properties

The Show Permission Set Properties field can be used to specify whether the **Permission Sets** page should calculate and show additional fields which describe properties of the permission sets that are used by the **Confidential Data Protection** extension.



Show Permission Set Properties

Show Permission Set Properties

Specifies whether the "Permission Sets" page should display additional properties, e.g., whether a permission set exposes confidential data or is protected.

Learn more

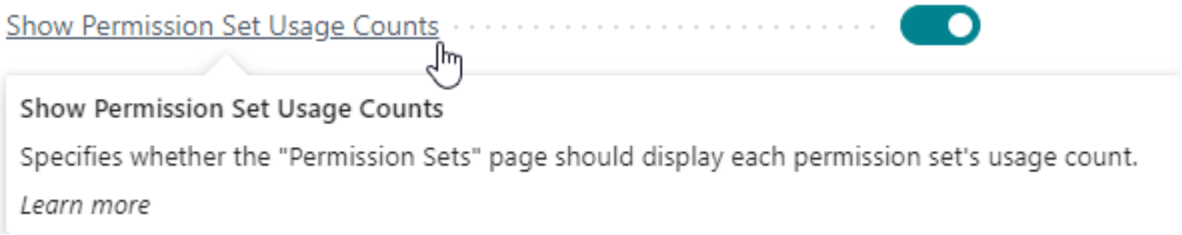
The fields that are added to the **Permission Sets** page when this setting is enabled, are as follows:

- Exposes Confidential Data - Specifies whether the permission set exposes confidential data when it would be assigned.
- Restricted - Specifies whether the permission set is a restricted permission set, i.e., a permission set for which the access that would be granted to confidential tables has been restricted, making them safe to assign to users without exposing confidential data.
- Protected - Specifies whether the permission set is protected against being edited/modified by a user.

Note that you can also sort and filter on these fields/properties.

Show Permission Set Usage Counts

The Show Permission Set Usage Counts field can be used to configure whether or not the **Permission Sets** page should calculate and show the **Usage Count** field which specifies the number of usages/assignments of each permission set. This provides you with better insights into whether permission sets are used or not.

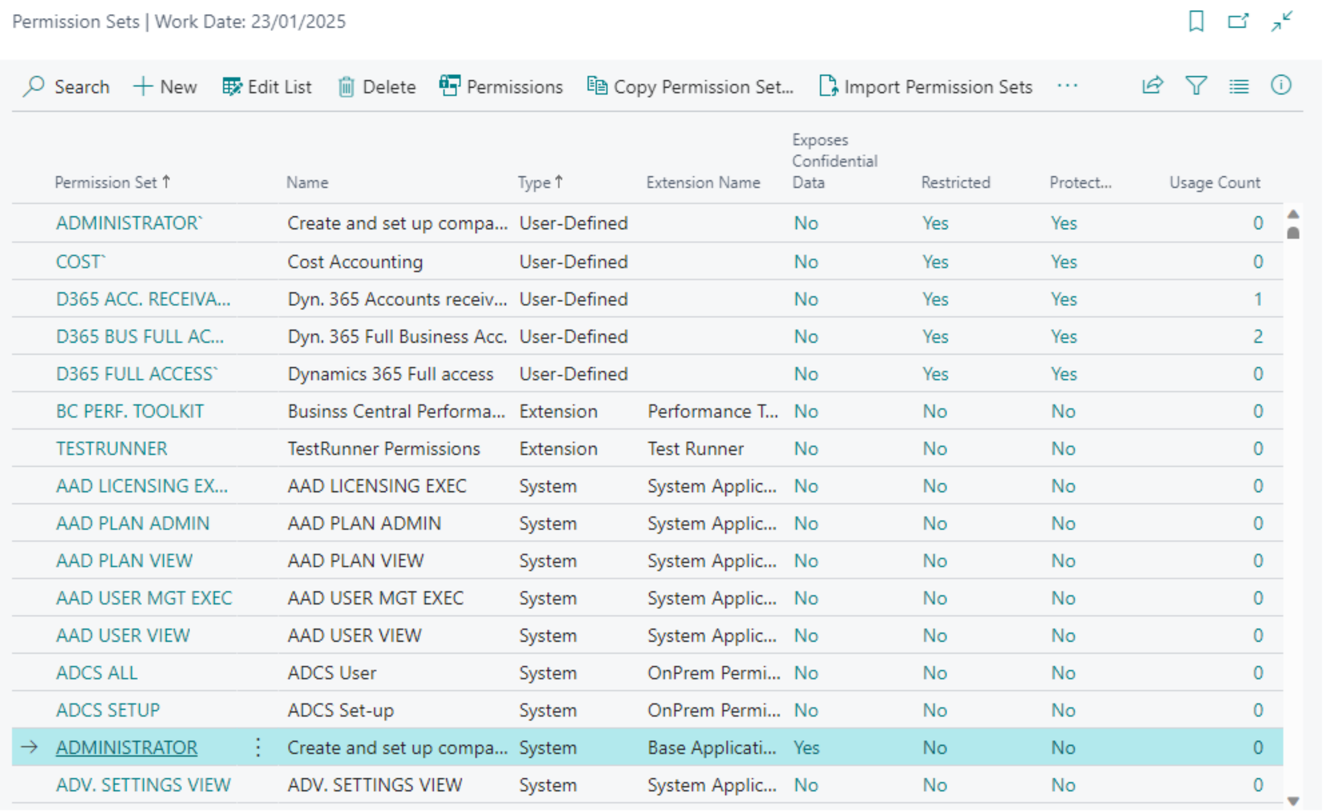


Show Permission Set Usage Counts

Show Permission Set Usage Counts

Specifies whether the "Permission Sets" page should display each permission set's usage count.

Learn more



Permission Sets | Work Date: 23/01/2025

Permission Set ↑	Name	Type ↑	Extension Name	Exposes Confidential Data	Restricted	Protect...	Usage Count
ADMINISTRATOR`	Create and set up compa...	User-Defined		No	Yes	Yes	0
COST`	Cost Accounting	User-Defined		No	Yes	Yes	0
D365 ACC. RECEIVA...	Dyn. 365 Accounts receiv...	User-Defined		No	Yes	Yes	1
D365 BUS FULL AC...	Dyn. 365 Full Business Acc.	User-Defined		No	Yes	Yes	2
D365 FULL ACCESS`	Dynamics 365 Full access	User-Defined		No	Yes	Yes	0
BC PERF. TOOLKIT	Businss Central Performa...	Extension	Performance T...	No	No	No	0
TESTRUNNER	TestRunner Permissions	Extension	Test Runner	No	No	No	0
AAD LICENSING EX...	AAD LICENSING EXEC	System	System Applic...	No	No	No	0
AAD PLAN ADMIN	AAD PLAN ADMIN	System	System Applic...	No	No	No	0
AAD PLAN VIEW	AAD PLAN VIEW	System	System Applic...	No	No	No	0
AAD USER MGT EXEC	AAD USER MGT EXEC	System	System Applic...	No	No	No	0
AAD USER VIEW	AAD USER VIEW	System	System Applic...	No	No	No	0
ADCS ALL	ADCS User	System	OnPrem Permi...	No	No	No	0
ADCS SETUP	ADCS Set-up	System	OnPrem Permi...	No	No	No	0
→ ADMINISTRATOR	Create and set up compa...	System	Base Applicati...	Yes	No	No	0
ADV. SETTINGS VIEW	ADV. SETTINGS VIEW	System	System Applic...	No	No	No	0

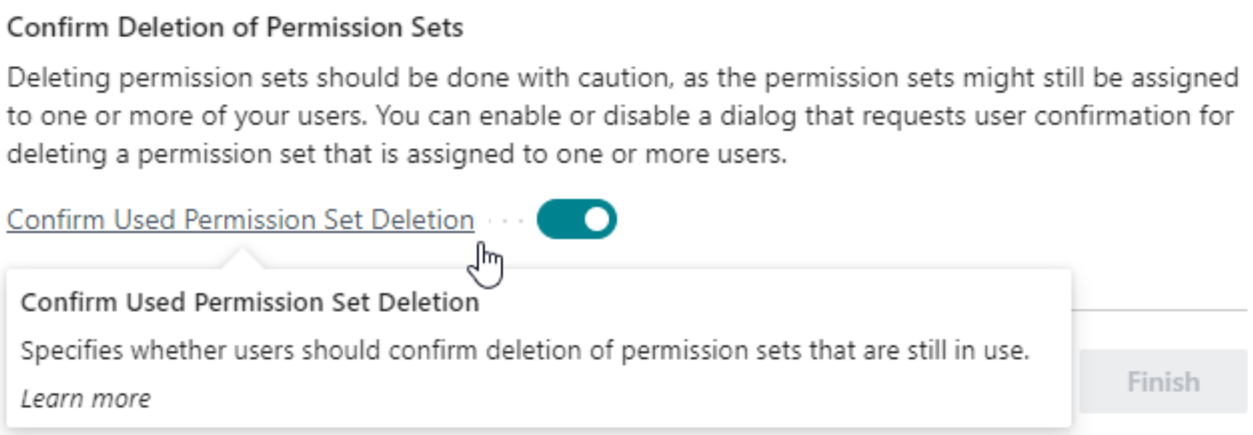
Note that you can also sort and filter on the **Usage Count** field on the **Permission Sets** page.

For more information, please see the Permission Set Insights section of the user manual.

10. Confirm Deletion of Permission Sets

Deleting permission sets should be done with caution, as the permission sets might still be assigned to one or more of your users or groups of users.

In the **Confirm Deletion of Permission Sets** tab you can use the **Confirm used Permission Set Deletion** field to specify whether a confirmation dialog should be shown when a user attempts to delete a permission set. This prompts for user confirmation, making the user aware that the permission set that they are attempting to delete is still assigned to one or more users, or groups of users.



Confirm Deletion of Permission Sets

Deleting permission sets should be done with caution, as the permission sets might still be assigned to one or more of your users. You can enable or disable a dialog that requests user confirmation for deleting a permission set that is assigned to one or more users.

Confirm Used Permission Set Deletion ● On

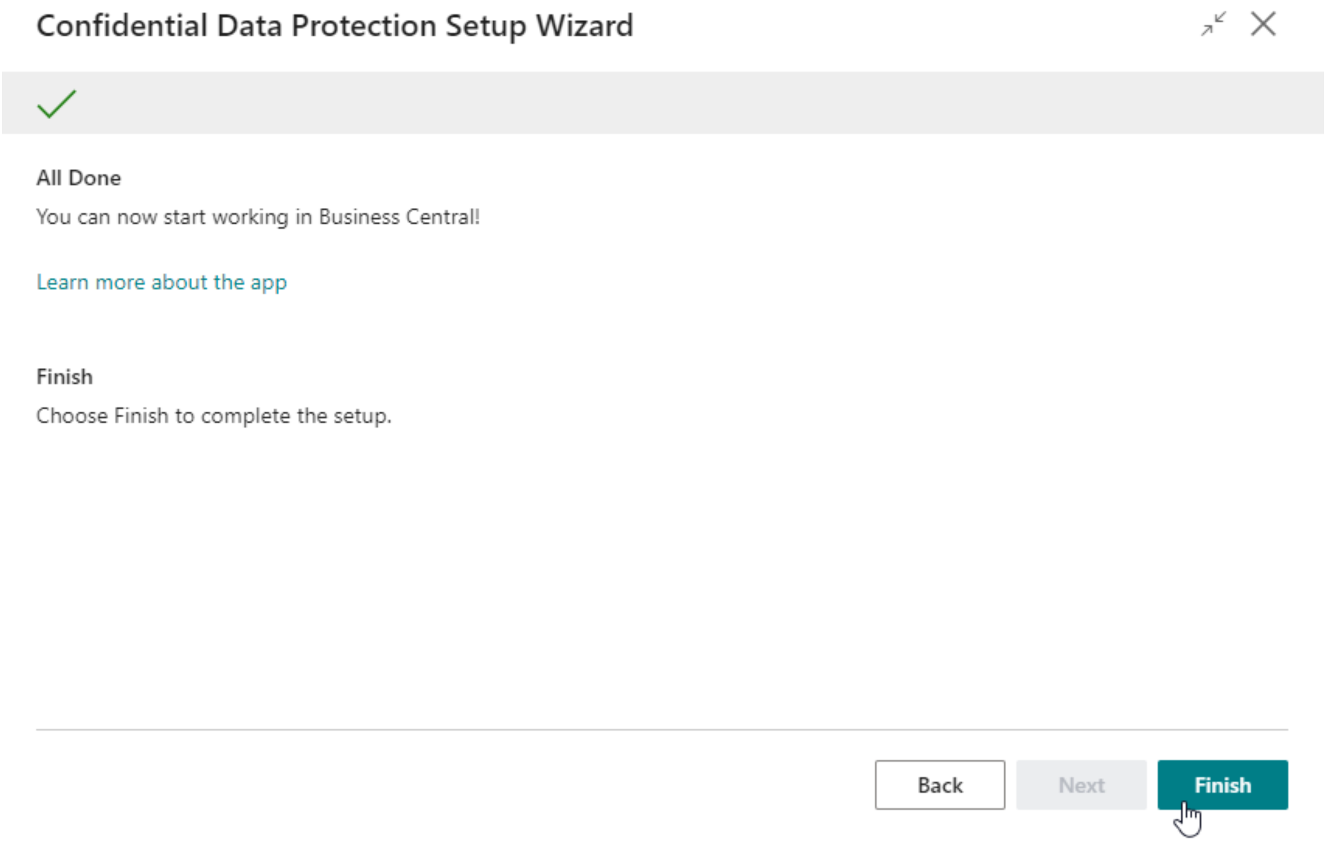
Confirm Used Permission Set Deletion

Specifies whether users should confirm deletion of permission sets that are still in use.

Learn more

When you are done setting your preferences, choose **Next** to move on to the next and final step of the setup wizard page.

11. Click on **Finish** to finish the setup and start using Confidential Data Protection.



Confidential Data Protection Setup Wizard

✓

All Done

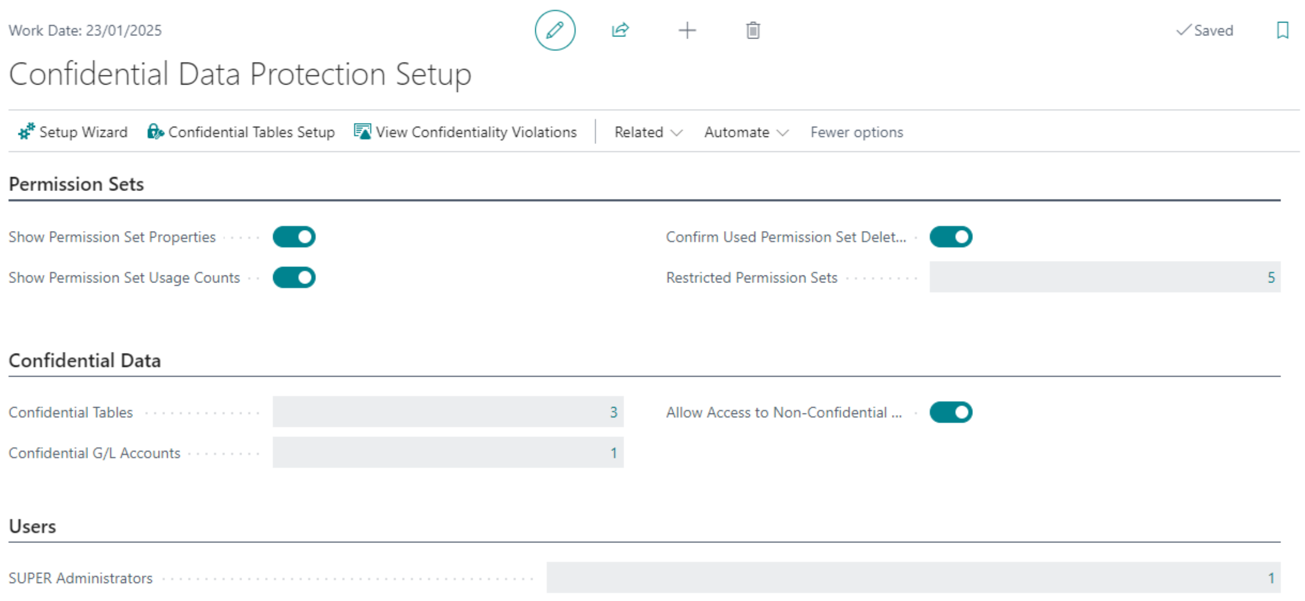
You can now start working in Business Central!

Learn more about the app

Finish

Choose Finish to complete the setup.

Please note that you can always open the **Confidential Data Protection Setup** page to edit the settings of the extension later if you would like to make any changes.



Work Date: 23/01/2025

Confidential Data Protection Setup

Permission Sets

Show Permission Set Properties ●
Show Permission Set Usage Counts ●
Confirm Used Permission Set Delet... ●
Restricted Permission Sets 5

Confidential Data

Confidential Tables 3
Confidential G/L Accounts 1
Allow Access to Non-Confidential ... ●

Users

SUPER Administrators 1

Alternatively, you can step through the **Confidential Data Protection Setup Wizard** page again to edit the settings.

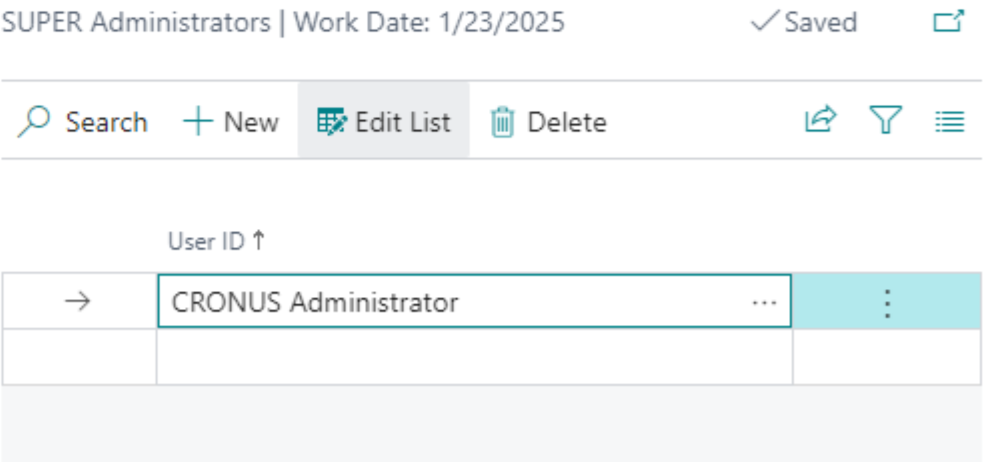
Apportunix Confidential Data Protection is now configured and is ready to be used.

Last update: January 16, 2024

SUPER Administrators

With the **Confidential Data Protection** extension installed, you can designate users as **SUPER administrators** on the **SUPER Administrators** page.

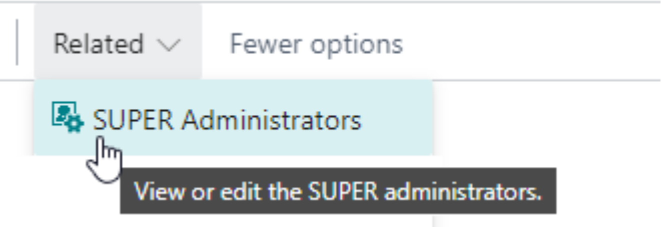
A **SUPER administrator** is the only type of user that will be allowed to assign the **SUPER**, **SUPER (DATA)**, and **SECURITY** permission sets to users in Business Central. Please find more information about these special permission sets in the Special permission sets section on Microsoft Learn.



User ID ↑
CRONUS Administrator

Note

You can open the **SUPER Administrators** page using the **SUPER Administrators** action on the **Confidential Data Protection Setup** page.



You can configure zero, one, or multiple **SUPER administrators**.

If no **SUPER administrators** have been configured, then any user that has the **SUPER** permission set assigned will be able to assign the earlier mentioned permission sets to other users, like would normally be the case (in other words, in this scenario, all users that have the **SUPER** permission set assigned will be considered to be SUPER administrators).

If there are **SUPER administrators** configured, then any users that only have the **SUPER** permission set assigned will **NOT** be able to assign the **SUPER**, **SUPER (DATA)**, and **SECURITY** permission sets to other users.

Rules for granting and revoking the SUPER Administrator role

The following rules and restrictions apply for granting and revoking the **SUPER Administrator** role:

- A user needs to have the **SUPER** permission set assigned for it to be allowed to grant SUPER administrator privileges to that user.
- If the current user does not have the **SUPER** permission set assigned, then the current user will **NOT** be allowed to grant nor revoke the **SUPER Administrator** role.
- If there are no SUPER administrator users, the current user has the **SUPER** permission set assigned, and the current user tries to grant the **SUPER Administrator** role, then this is allowed.
- If there are already SUPER administrator users, the current user has the **SUPER** permission set assigned, but is not designated as a SUPER administrator, then the current user will **NOT** be allowed to grant or revoke the **SUPER Administrator** role to or from user.
- It is always allowed to revoke the **SUPER Administrator** role from a user that does not have the **SUPER** permission set assigned.
- A user that has the **SUPER Administrator** role can grant and/or revoke the **SUPER Administrator** role to/from users.
- It is not allowed to revoke the **SUPER** permission set from a user that has the **SUPER Administrator** role. If you would like to revoke permissions from a user with the **SUPER Administrator** role, then the role should first be revoked from the user.

Last update: September 22, 2023

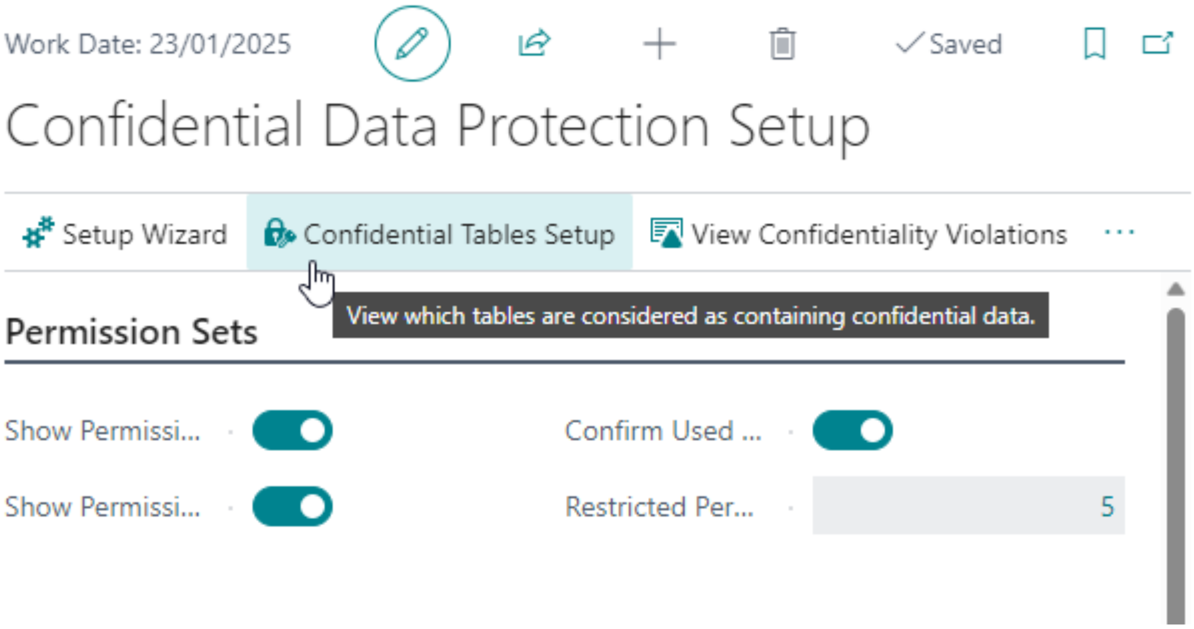
Confidential Tables Setup

With the **Confidential Data Protection** extension you can protect your confidential data from being exposed to Business Central users in your company that should not have access to this data.

Confidential Tables Setup Page

The extension allows you to specify the tables that have data that should not be directly accessible to all Business Central users. On the **Confidential Tables Setup** page you can find which tables are considered as containing confidential data.

As an administrator you can view the setup by opening this page using the **Confidential Tables Setup** action on the **Confidential Data Protection Setup** page.


Work Date: 23/01/2025
✓Saved
Confidential Data Protection Setup
Setup Wizard
Confidential Tables Setup
View Confidentiality Violations
···
View which tables are considered as containing confidential data.
Permission Sets
Show Permissi...
Show Permissi...
Confirm Used ...
Restricted Per...
5

By default, the **G/L Entry** table and **G/L Budget Entry** tables are considered to contain confidential tables (N.B. when no extensions or customizations have been applied). This means that **Table Data Direct Read** permission assignments for these tables are considered confidentiality-violating permission assignments as they would grant users access to confidential data in Business Central.

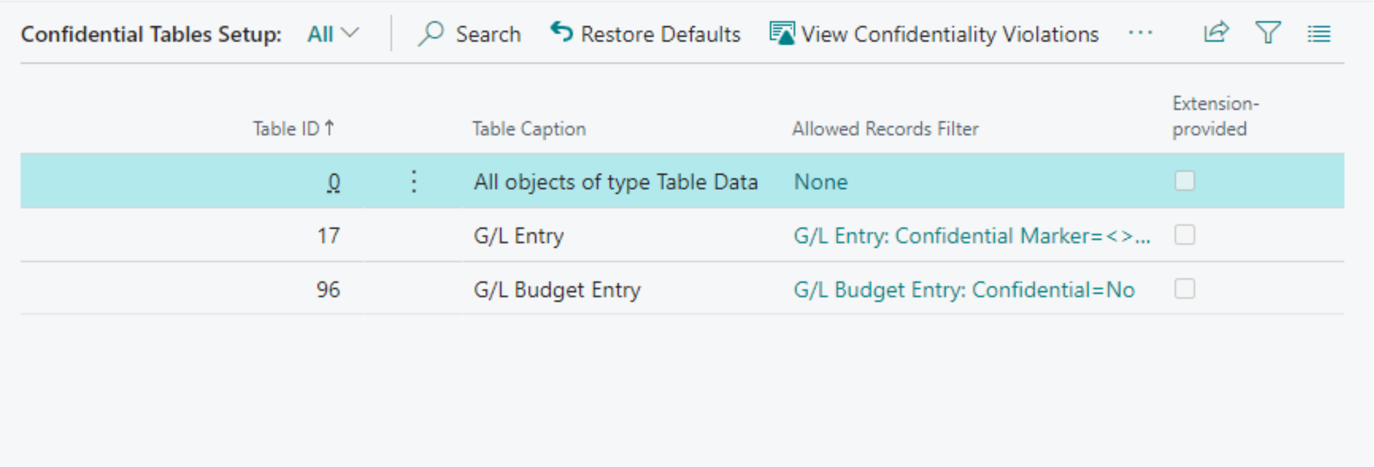

Confidential Tables Setup: All
Search
Restore Defaults
View Confidentiality Violations
···

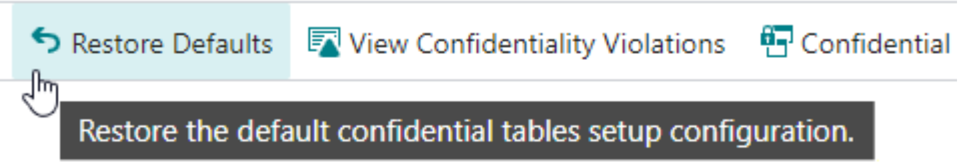
Table ID ↑	Table Caption	Allowed Records Filter	Extension-provided
0	All objects of type Table Data	None	□
17	G/L Entry	G/L Entry: Confidential Marker=<>...	□
96	G/L Budget Entry	G/L Budget Entry: Confidential=No	□

For tables where only some records contain confidential data, the **Allowed Records Filter** field is used to specify which records are allowed to be accessed by users, i.e., which records in the table are non-confidential.

Important

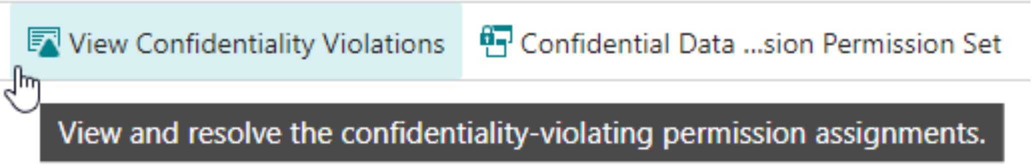
Note that permission assignments that grant access to all table data (i.e., a permission assignment for table ID = 0) are always considered to expose confidential table data.

The **Restore Defaults** action on the **Confidential Tables Setup** page can be used to easily apply the default confidential tables setup (e.g., when extensions to the defaults have been added or removed).



Restore the default confidential tables setup configuration.

The **View Confidentiality Violations** action can be used to identify and resolve confidentiality-violating permission set assignments to users based on the **Confidential Tables Setup** configuration. For more information on how you can use this action, please see the **Identify and Resolve Violations** section in the user manual.


View Confidentiality Violations
Confidential Data ...sion Permission Set

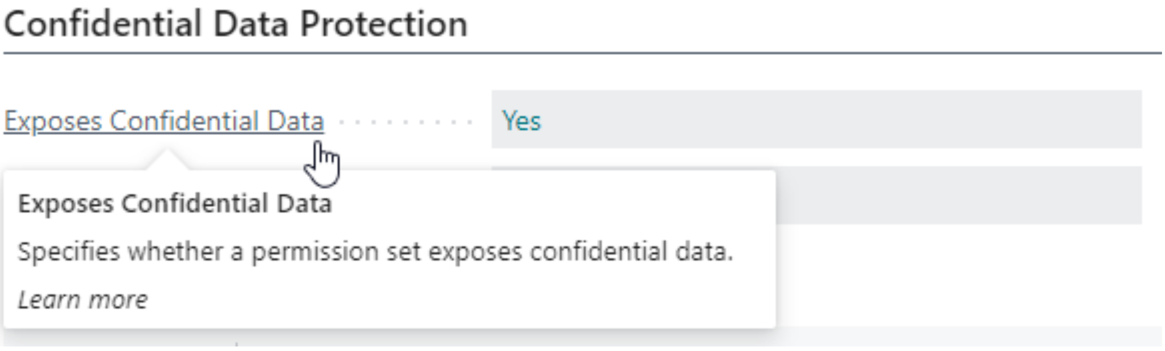
View and resolve the confidentiality-violating permission assignments.

Confidential Permission Sets

Based on the **Confidential Table Setup** configuration, the **Confidential Data Protection** extension can identify which permission set pose a risk to exposing confidential data to your Business Central users.

A permission set is considered as exposing confidential data when one of the effective permissions of the permission set grant **TableData Direct Read** permissions for a table that has been configured on the Confidential Table Setup page.

The **Confidential Data Protection** tab on the **Permission Set** card page contains an **Exposes Confidential Data** field which specifies whether the permission set exposes confidential data through one of its effective permissions.



Confidential Data Protection

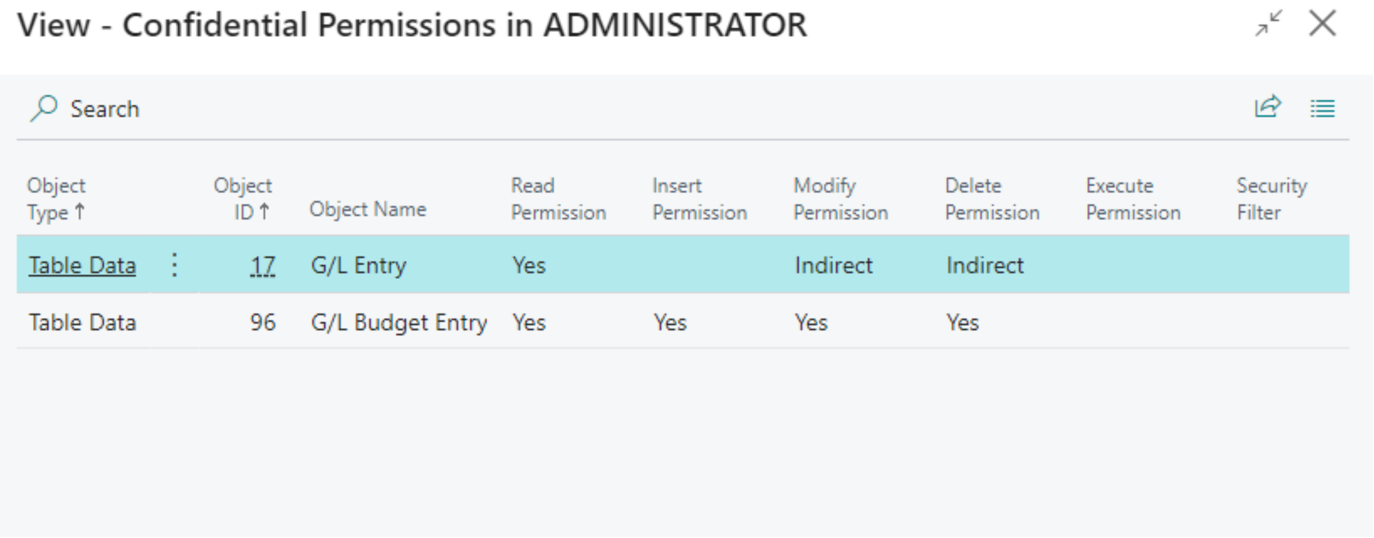
Exposes Confidential Data: Yes

Exposes Confidential Data

Specifies whether a permission set exposes confidential data.

Learn more

By drilling down on the field value (i.e., by clicking on **Yes**), you can see which effective permissions the **Confidential Data Protection** extension identified as exposing confidential data.

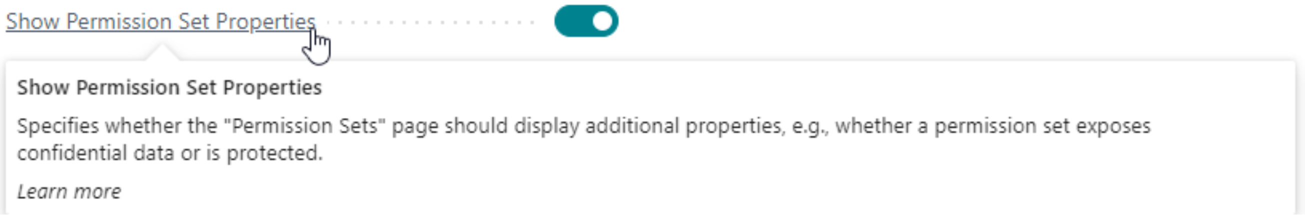


View - Confidential Permissions in ADMINISTRATOR

Object Type ↑	Object ID ↑	Object Name	Read Permission	Insert Permission	Modify Permission	Delete Permission	Execute Permission	Security Filter
Table Data	17	G/L Entry	Yes		Indirect	Indirect		
Table Data	96	G/L Budget Entry	Yes	Yes	Yes	Yes		

Tip

If you have enabled the Show Permission Set Properties setting on the **Confidential Data Protection Setup** page, then a **Exposes confidential Data** field will be available on the **Permission Sets** page which specifies for each permission set whether it exposes confidential data through one of its effective permissions. Note that you can also sort and filter the list page on this field.

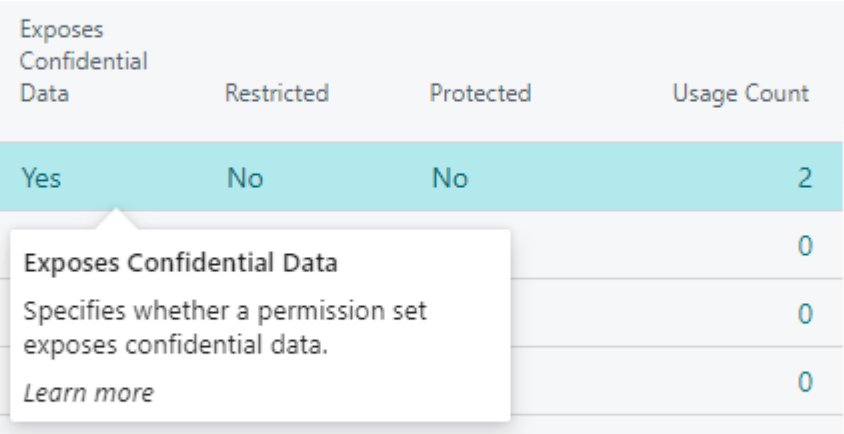


Show Permission Set Properties

Show Permission Set Properties

Specifies whether the "Permission Sets" page should display additional properties, e.g., whether a permission set exposes confidential data or is protected.

Learn more



Exposes Confidential Data	Restricted	Protected	Usage Count
Yes	No	No	2
			0
			0
			0

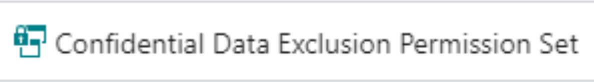
Exposes Confidential Data

Specifies whether a permission set exposes confidential data.

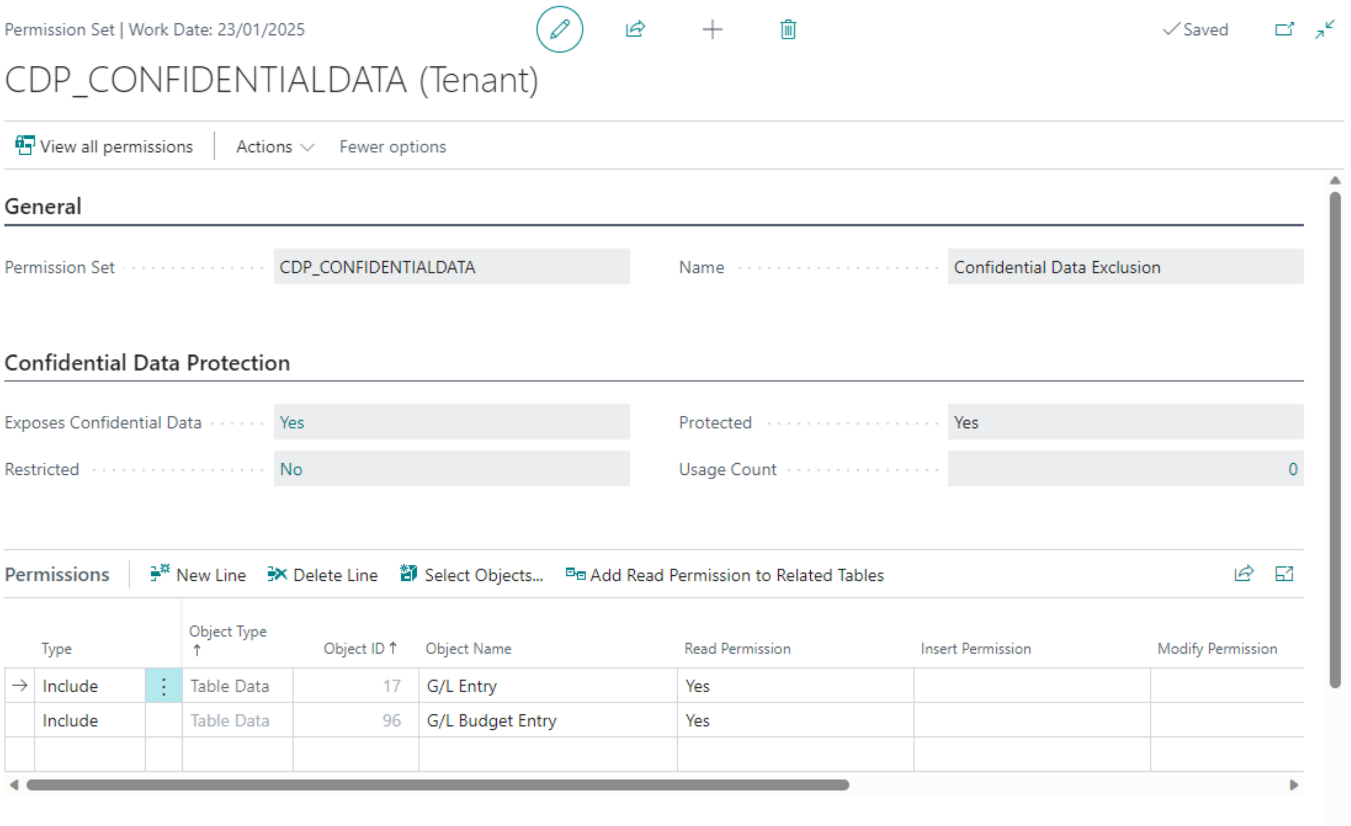
Learn more

Confidential Data Exclusion Permission Set

From the **Confidential Tables Setup** configuration, a **Confidential Data Exclusion** permission set is generated and updated automatically whenever the configuration is changed by an administrator. You can view this permission set by invoking the **Confidential Data Exclusion Permission Set** action on the Confidential Tables Setup page.



The **Confidential Data Exclusion** permission set is used to exclude **Table Data Direct Read** permission assignments from permission sets that expose confidential data (according to how this is defined on the **Confidential Table Setup** page).



CDP_CONFIDENTIALDATA (Tenant)

General

Permission Set	CDP_CONFIDENTIALDATA	Name	Confidential Data Exclusion

Confidential Data Protection

Exposes Confidential Data	Yes	Protected	Yes
Restricted	No	Usage Count	0

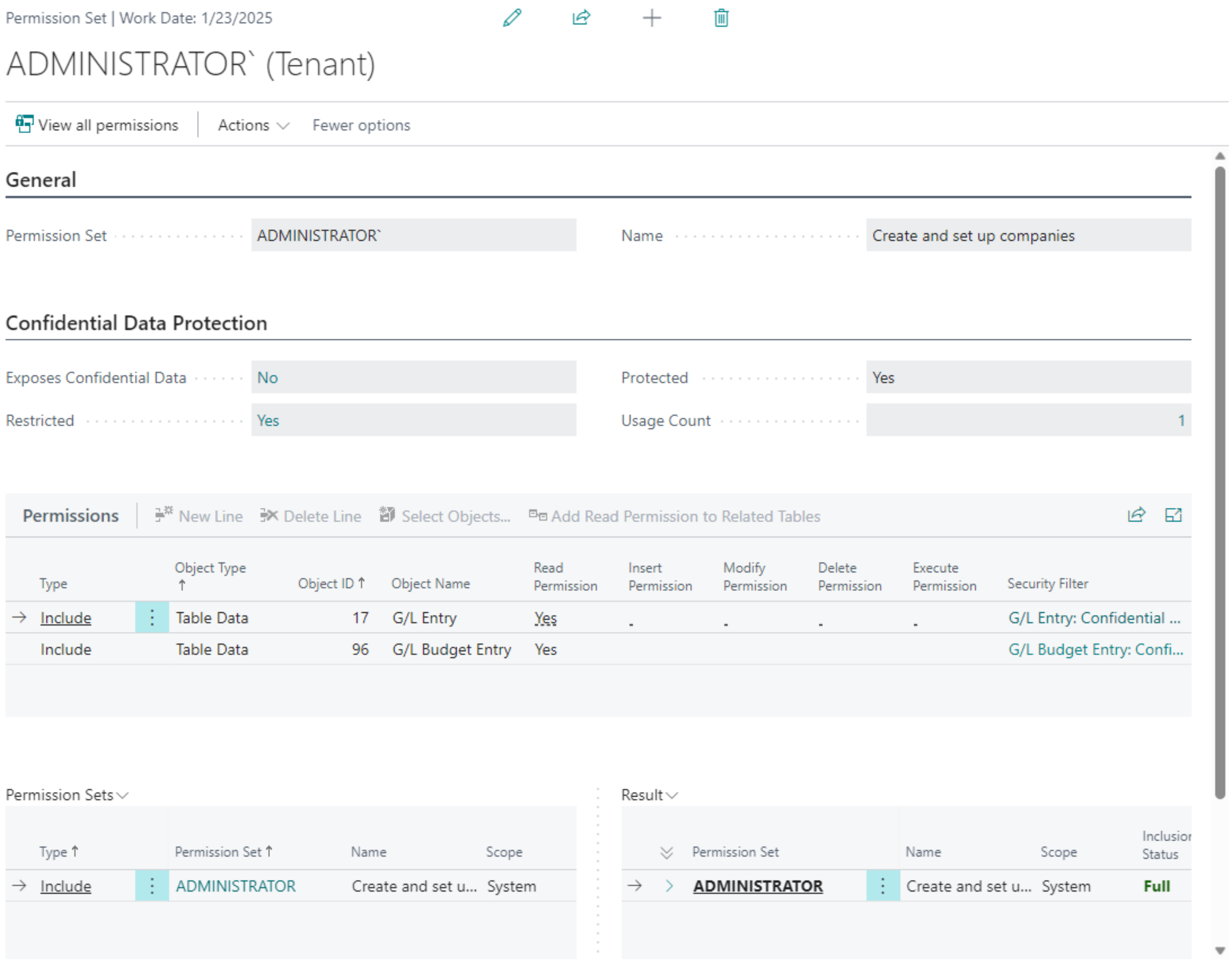
Permissions

Type	Object Type ↑	Object ID ↑	Object Name	Read Permission	Insert Permission	Modify Permission
Include	Table Data	17	G/L Entry	Yes		
Include	Table Data	96	G/L Budget Entry	Yes		

Restricted Permission Sets

If a permission set is assigned to a user or group of users (i.e., a security group) which would expose confidential data to users, then a **Restricted** permission set will be generated automatically and the permission set assignment will be replaced automatically with an assignment of the newly generated, restricted permission set.

A **Restricted** permission set is a permission set in which the access that would be granted to confidential tables has been restricted, making them safe to assign to users without exposing confidential data. If an attempt is made to assign a permission set that would expose confidential data to users, then a restricted permission set will be generated which **includes** the original permission set and **excludes** the **Confidential Data Exclusion** permission set. The restricted permission set is then assigned to the user instead of the confidential permission set.



Permission Set | Work Date: 1/23/2025

ADMINISTRATOR` (Tenant)

General

Permission Set	ADMINISTRATOR`	Name	Create and set up companies

Confidential Data Protection

Exposes Confidential Data	No	Protected	Yes
Restricted	Yes	Usage Count	1

Permissions

Type	Object Type ↑	Object ID ↑	Object Name	Read Permission	Insert Permission	Modify Permission	Delete Permission	Execute Permission	Security Filter
Include	Table Data	17	G/L Entry	Yes	-	-	-	-	G/L Entry: Confidential ...
Include	Table Data	96	G/L Budget Entry	Yes					G/L Budget Entry: Confi...

Permission Sets

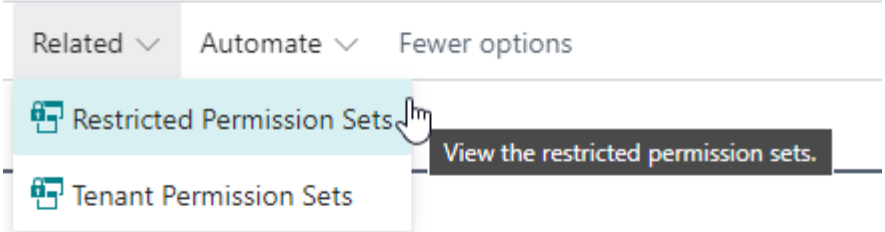
Type ↑	Permission Set ↑	Name	Scope
Include	ADMINISTRATOR	Create and set u...	System

Result

Permission Set	Name	Scope	Inclusion Status
ADMINISTRATOR	Create and set u...	System	Full

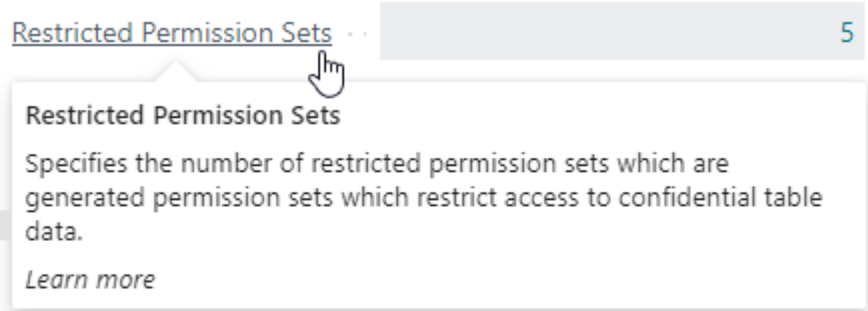
Tip

1. You can open an overview of all Restricted permission sets by invoking the **Restricted Permission Sets** action on the Confidential Data Protection Setup page.



View the restricted permission sets.

Or, using the drilldown of the **Restricted Permission Sets** field on the **Confidential Data Protection Setup** page.



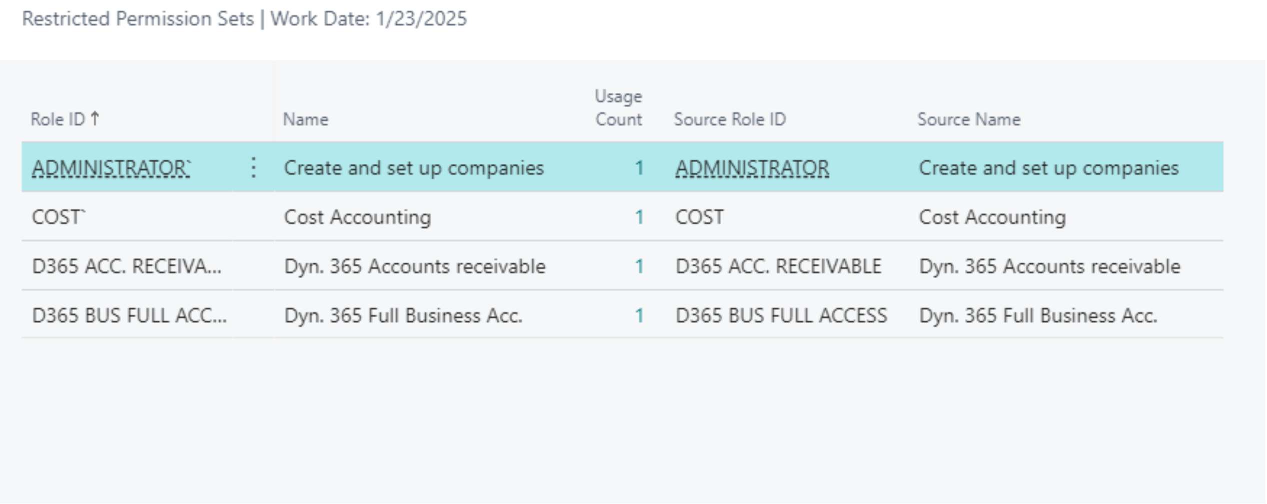
Restricted Permission Sets 5

Restricted Permission Sets

Specifies the number of restricted permission sets which are generated permission sets which restrict access to confidential table data.

Learn more

This will open a page where you can view all restricted permission sets in your Business Central environment.

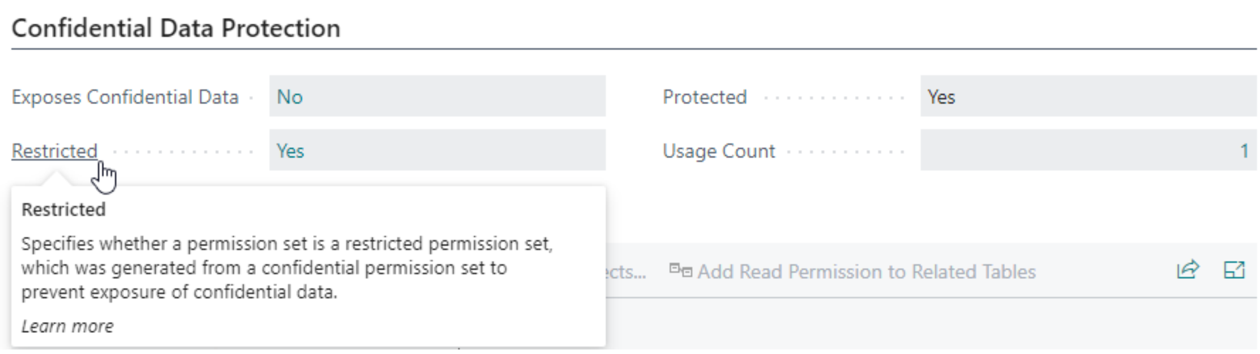


Restricted Permission Sets | Work Date: 1/23/2025

Role ID ↑	Name	Usage Count	Source Role ID	Source Name
ADMINISTRATOR`	Create and set up companies	1	ADMINISTRATOR	Create and set up companies
COST`	Cost Accounting	1	COST	Cost Accounting
D365 ACC. RECEIVA...	Dyn. 365 Accounts receivable	1	D365 ACC. RECEIVABLE	Dyn. 365 Accounts receivable
D365 BUS FULL ACC...	Dyn. 365 Full Business Acc.	1	D365 BUS FULL ACCESS	Dyn. 365 Full Business Acc.

On this page you can also view the Confidential (source) permission set that the Restricted permission set was derived from, if any, and how many times the permission set is used/assigned.

2. The **Confidential Data Protection** tab on the **Permission Set** card page also shows whether a permission set is a restricted permission set.



Confidential Data Protection

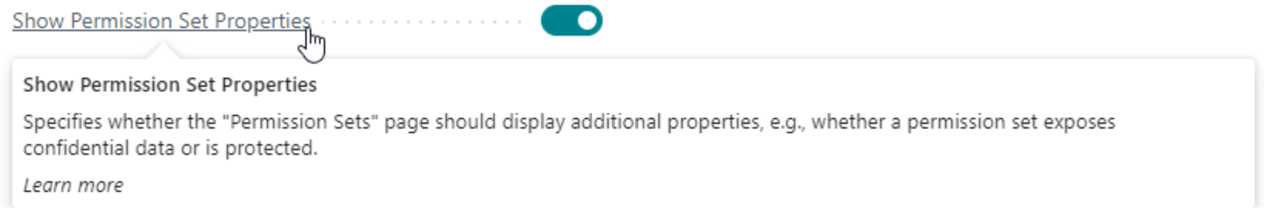
Exposes Confidential Data	No	Protected	Yes
Restricted	Yes	Usage Count	1

Restricted

Specifies whether a permission set is a restricted permission set, which was generated from a confidential permission set to prevent exposure of confidential data.

Learn more

3. If you have enabled the **Show Permission Set Properties** setting on the **Confidential Data Protection Setup** page, then a **Restricted** field will be available on the **Permission Sets** page which specifies for each permission set whether it is a restricted permission set.

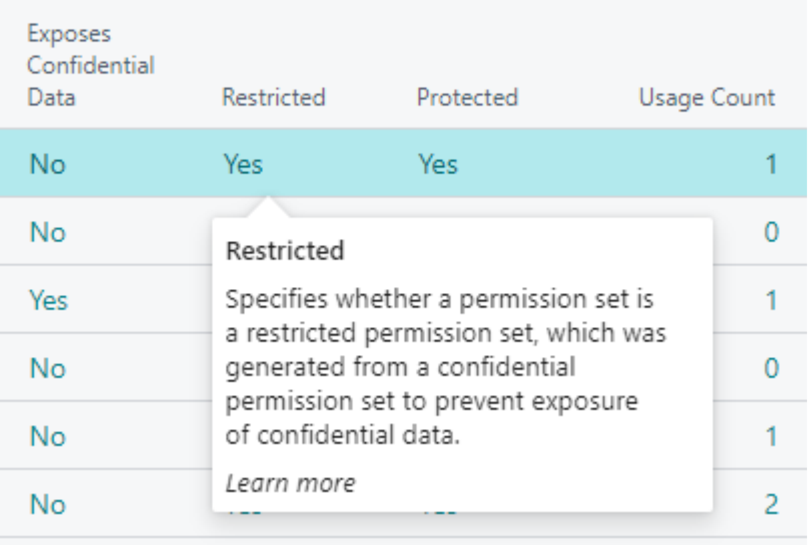


Show Permission Set Properties

Show Permission Set Properties

Specifies whether the "Permission Sets" page should display additional properties, e.g., whether a permission set exposes confidential data or is protected.

Learn more



Exposes Confidential Data	Restricted	Protected	Usage Count
No	Yes	Yes	1
No			0
Yes			1
No			0
No			1
No			2

Restricted

Specifies whether a permission set is a restricted permission set, which was generated from a confidential permission set to prevent exposure of confidential data.

Learn more

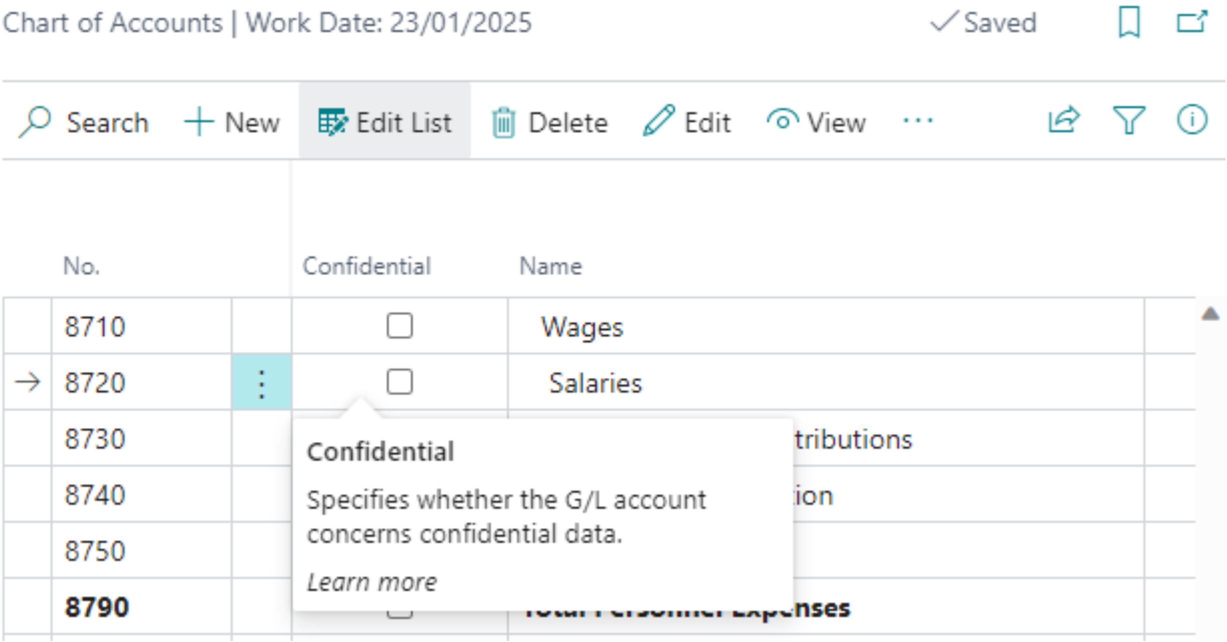
Note that you can also sort and filter the list page on this field.

Last update: September 22, 2023

Confidential G/L Accounts

In your business, chances are you have G/L accounts that concern data that should be treated confidentially. Normally, when user permissions to the **"G/L Entry"** table are assigned, this will expose the data of all G/L accounts, including those that concern confidential data. With the **Confidential Data Protection** extension you can mark G/L accounts as **Confidential**, so that the related G/L data for these G/L accounts will not be exposed to users.

To protect confidential G/L data, first of all, open the **Chart of Accounts** or **Chart of Accounts Overview** page. On the page you will find all **G/L Accounts** in your Business Central company, and a new **Confidential** field, which specifies whether the data related to that **G/L Account** should be treated confidentially and not be exposed to all users.



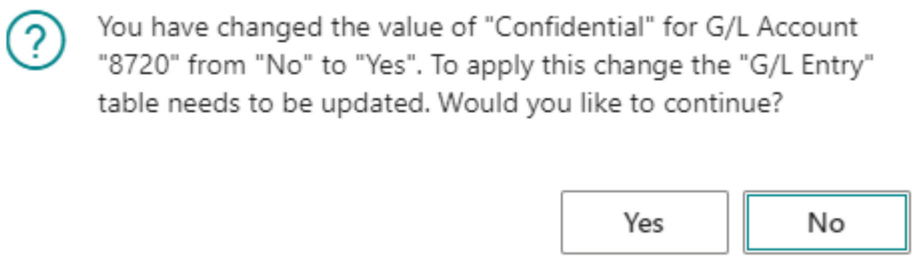
No.	Confidential	Name
8710	□	Wages
8720	□	Salaries
8730		tributions
8740		ion
8750		
8790	□	**Total Personnel Expenses**

Confidential

Specifies whether the G/L account concerns confidential data.

Learn more

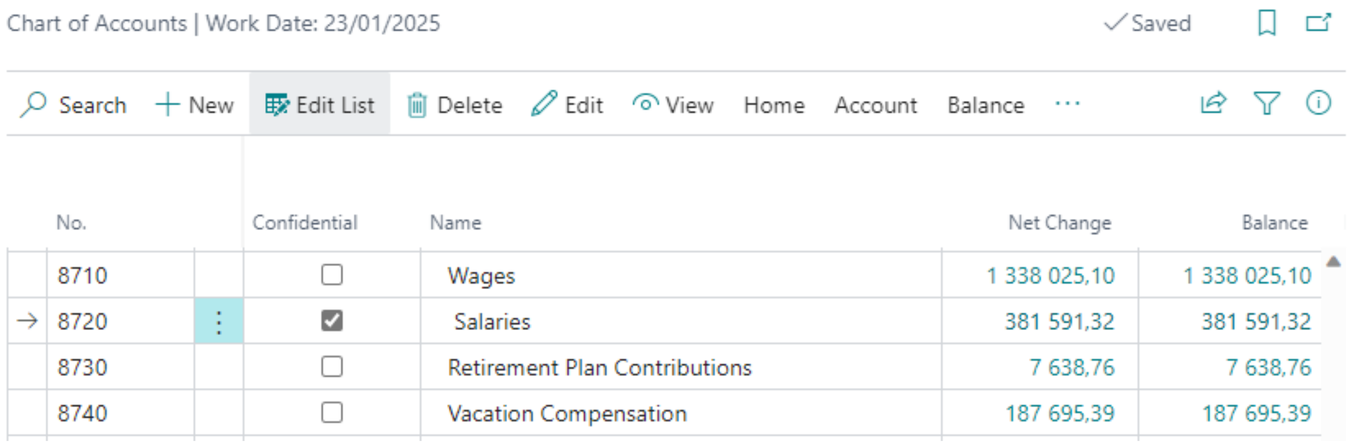
Identify the G/L accounts that you would like to protect (for instance, account 8720: "Salaries"), and enable the **Confidential** field to mark the G/L account as confidential.


You have changed the value of "Confidential" for G/L Account "8720" from "No" to "Yes". To apply this change the "G/L Entry" table needs to be updated. Would you like to continue?

A confirmation dialog will be shown that you prompts you to confirm the change and informs you that the G/L Entry table will be updated accordingly. Choose **Yes** to confirm the change and a progress dialog will be displayed.

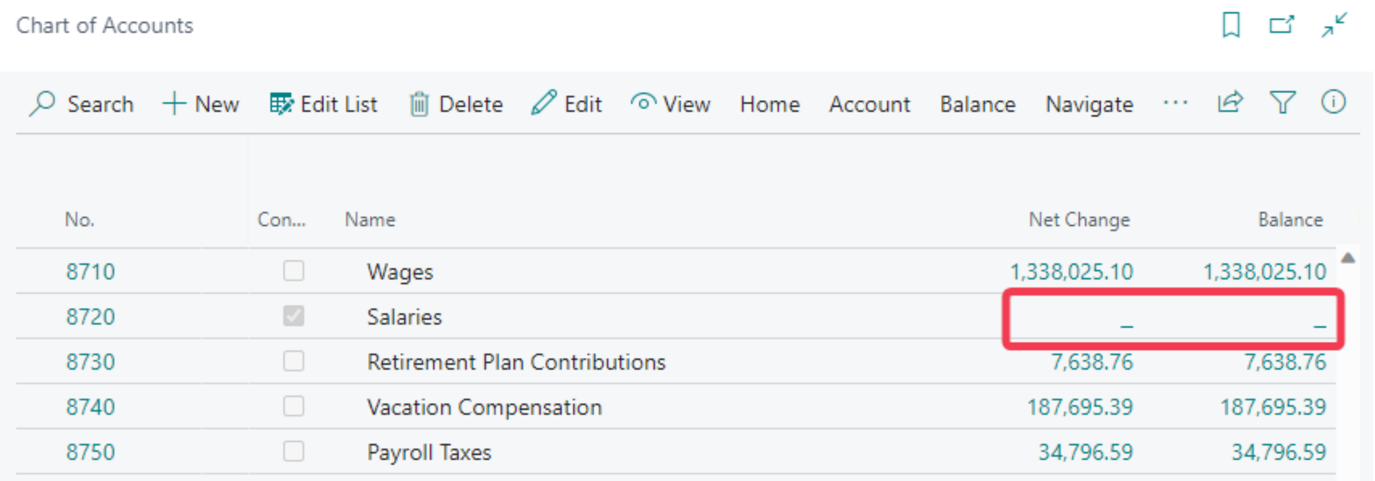
After the change has been applied, users will have to refresh the page to see changes take effect.

If you are logged in with a user account that has the **SUPER** permission set assigned, you will still be able to see the G/L data related to the confidential G/L account.



No.	Confidential	Name	Net Change	Balance
8710	□	Wages	1 338 025,10	1 338 025,10
8720	☑	Salaries	381 591,32	381 591,32
8730	□	Retirement Plan Contributions	7 638,76	7 638,76
8740	□	Vacation Compensation	187 695,39	187 695,39

On the other hand, users with restricted access (i.e., a user that does not have the **SUPER** or **SUPER (DATA)** permission set assigned), will no longer be able to see the G/L data related to the confidential G/L account in your company, nor see the values of flowfields that use the confidential G/L data for their calculations.



No.	Con...	Name	Net Change	Balance
8710	□	Wages	1,338,025.10	1,338,025.10
8720	☑	Salaries	_	_
8730	□	Retirement Plan Contributions	7,638.76	7,638.76
8740	□	Vacation Compensation	187,695.39	187,695.39
8750	□	Payroll Taxes	34,796.59	34,796.59

Info

The **G/L Entry** records that are considered as relating to a confidential **G/L Account** are records for which one of the followings applies:

- The "**G/L Account No.**" field contains the "**No.**" of a confidential **G/L Account**.
- The "**Bal. Account Type**" is "**G/L Account**" and the "**Bal. Account No.**" field contains the "**No.**" of a confidential **G/L Account**.

The **G/L Budget Entry** records that are considered as relating to a confidential **G/L Account** are records for which the "**G/L Account No.**" field contains the "**No.**" of a confidential **G/L Account**.

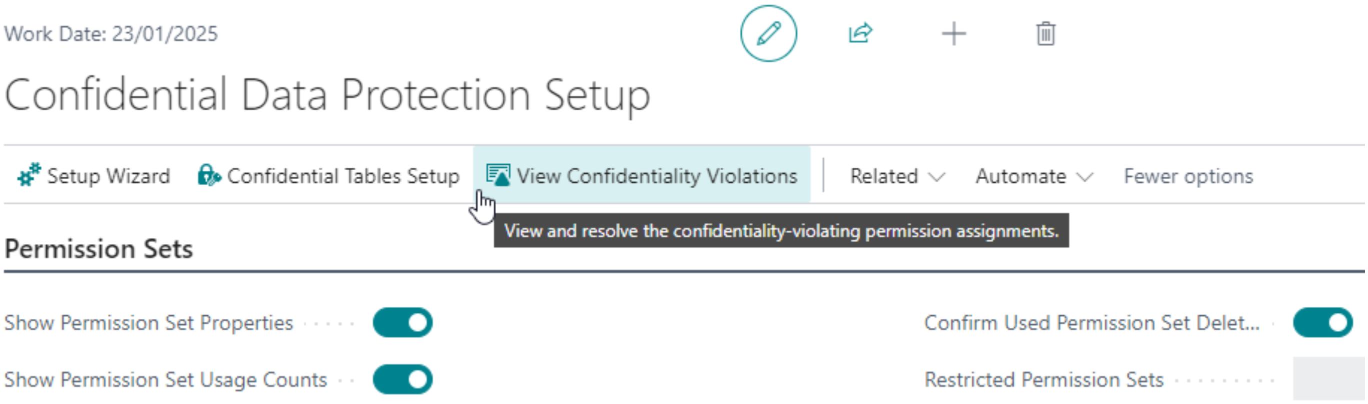
Last update: September 22, 2023

Identify and Resolve Violations

With the Confidential Table Setup configuration in place, the **Confidential Data Protection** can identify and resolve confidentiality-violating permission set assignments in your Business Central environment.

Identify Confidentiality Violations

Using the **View Confidentiality Violations** action on the **Confidential Data Protection Setup** page you can open an overview of the confidentiality-violating permission set assignments that have been identified by the **Confidential Data Protection** extension.


Work Date: 23/01/2025

Confidential Data Protection Setup

View and resolve the confidentiality-violating permission assignments.

Permission Sets

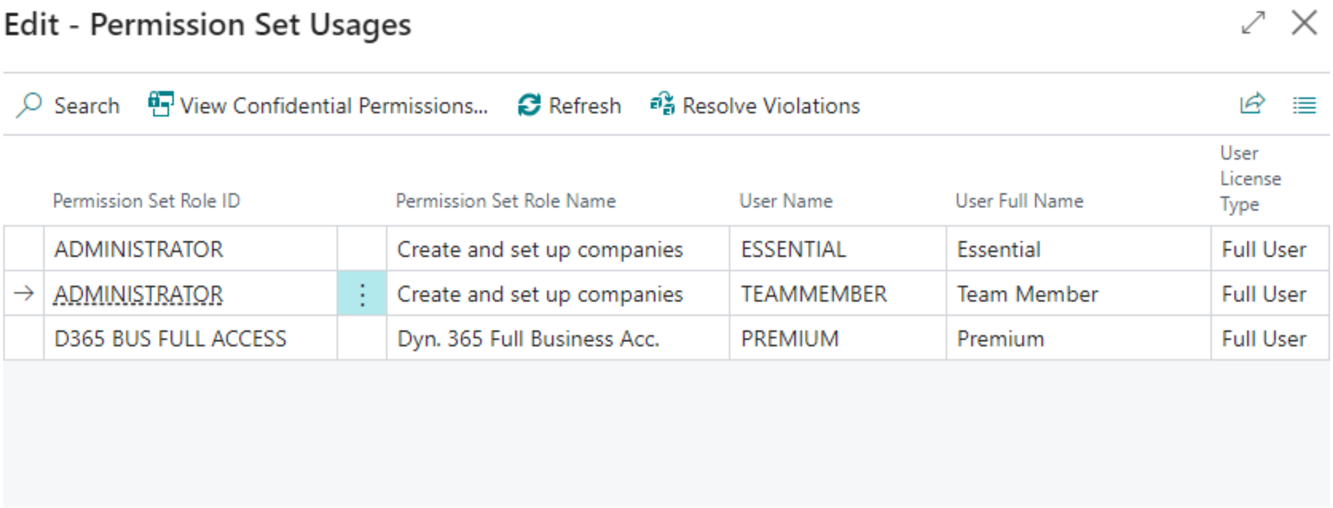
Show Permission Set Properties: on

Show Permission Set Usage Counts: on

Confirm Used Permission Set Delet...: on

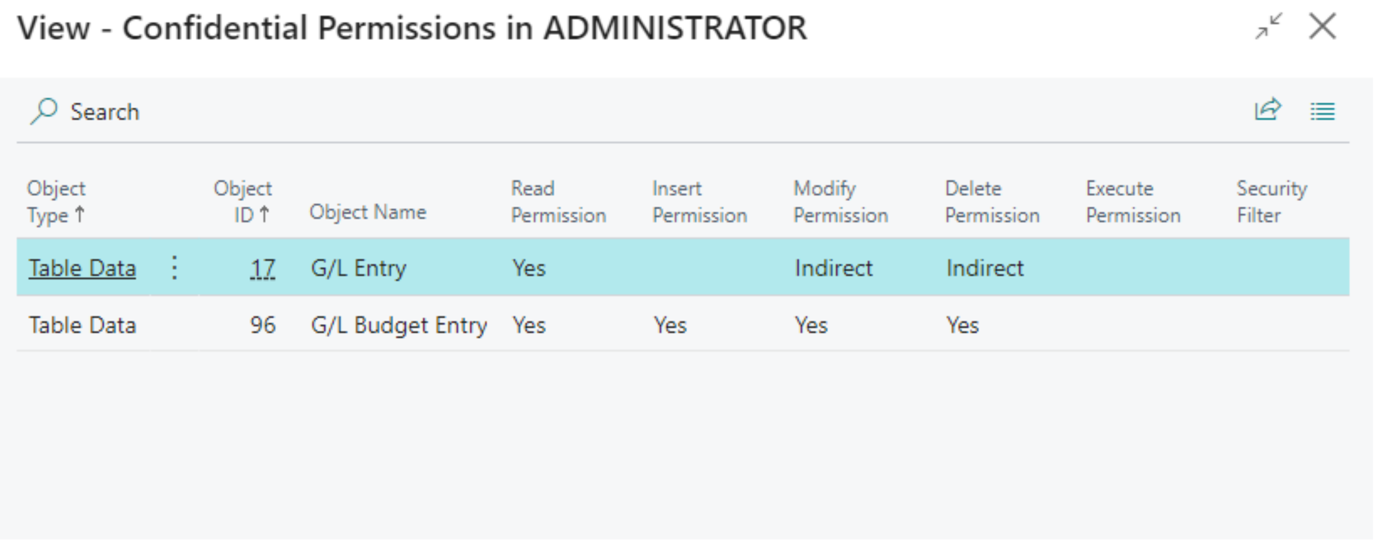
Restricted Permission Sets

On the page that opens, you can view the permission set assignments that expose confidential data to users in your Business Central environment. You can see which confidential permission sets have been assigned to users, and to which users or groups of users they have been assigned.


Edit - Permission Set Usages

Permission Set Role ID	Permission Set Role Name	User Name	User Full Name	User License Type
ADMINISTRATOR	Create and set up companies	ESSENTIAL	Essential	Full User
ADMINISTRATOR	Create and set up companies	TEAMMEMBER	Team Member	Full User
D365 BUS FULL ACCESS	Dyn. 365 Full Business Acc.	PREMIUM	Premium	Full User

You can invoke the **View Confidential Permissions...** action to view the permissions in the permission set that expose confidential data to users.

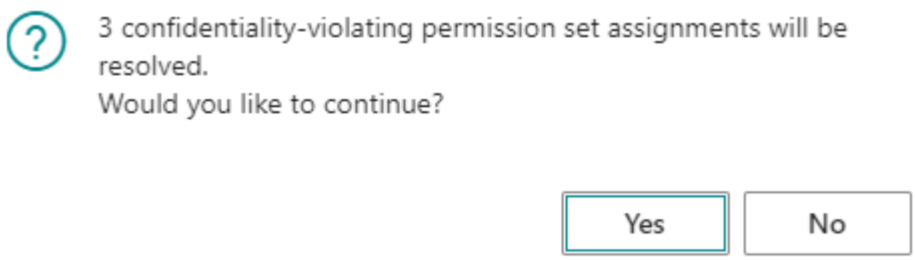


View - Confidential Permissions in ADMINISTRATOR

Object Type ↑	Object ID ↑	Object Name	Read Permission	Insert Permission	Modify Permission	Delete Permission	Execute Permission	Security Filter
Table Data	17	G/L Entry	Yes		Indirect	Indirect		
Table Data	96	G/L Budget Entry	Yes	Yes	Yes	Yes		

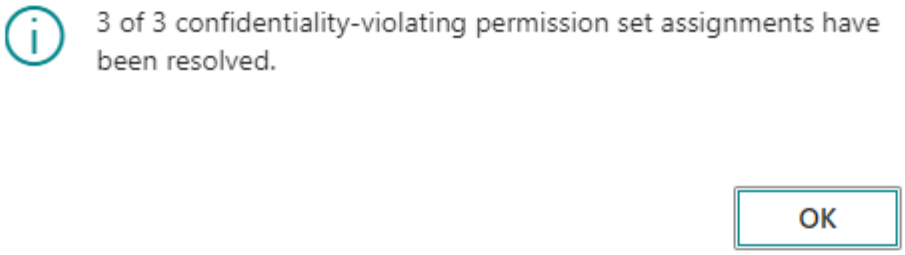
Resolve Confidentiality Violations

To resolve the identified violations you can invoke the **Resolve Violations** action. After you invoke the action, you will first get a confirmation dialog.



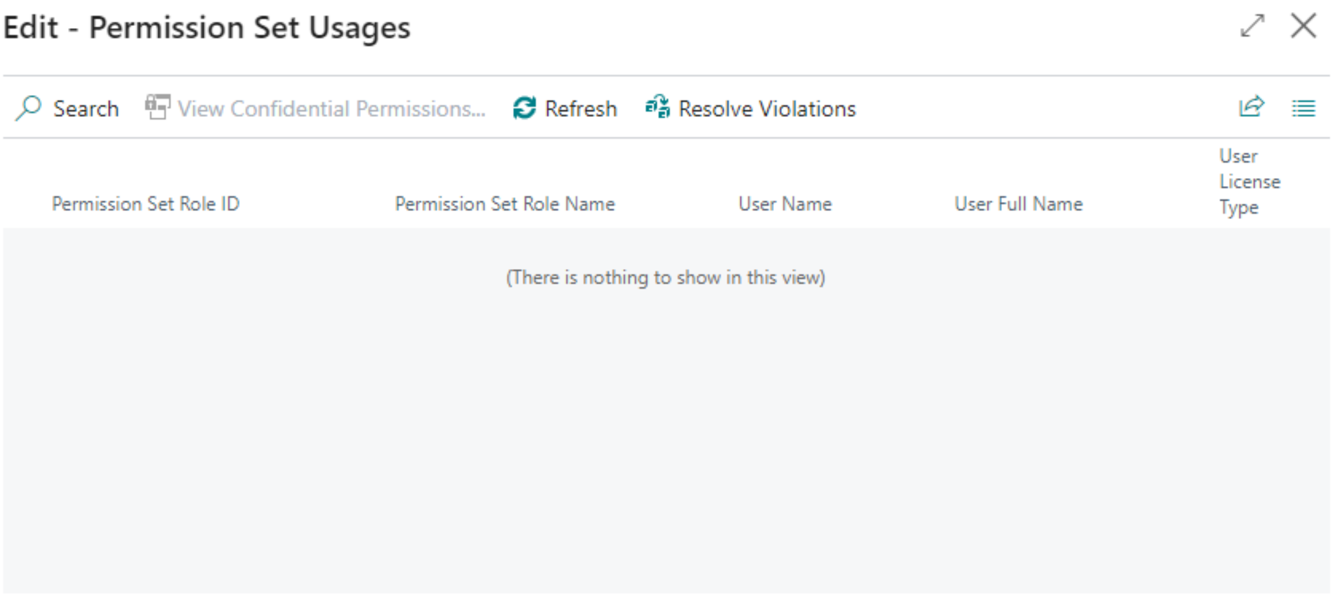
3 confidentiality-violating permission set assignments will be resolved.
Would you like to continue?

Choose **Yes** to let the **Confidential Data Protection** extension resolve the violations. Each confidentiality-violating permission set assignment to users or groups of users will be replaced by assigning a new, restricted permission set, derived from the original permission set.



3 of 3 confidentiality-violating permission set assignments have been resolved.

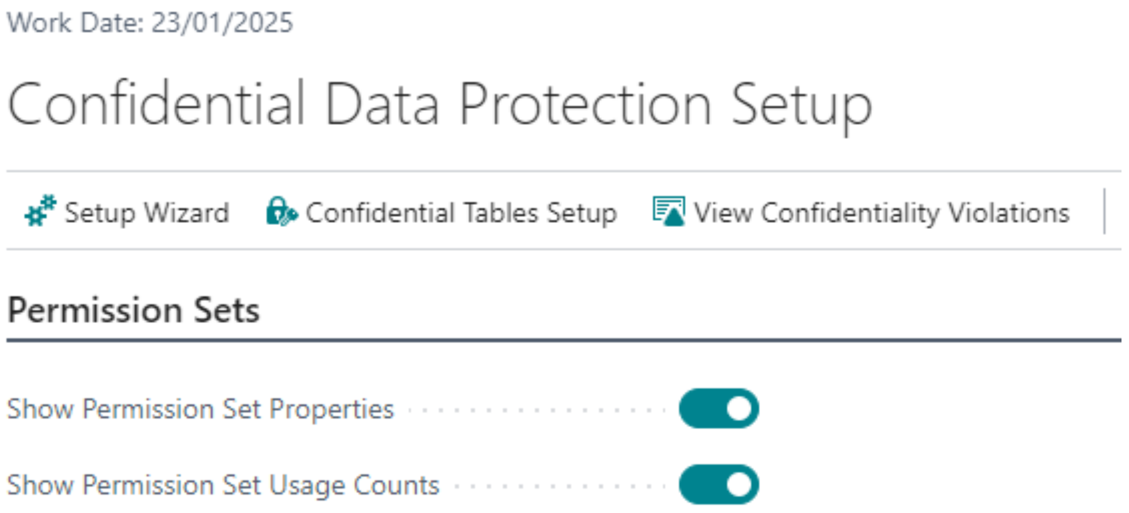
After the action has completed and the page is refreshed, all confidentiality-violating permission set assignments will have been resolved.



Last update: September 12, 2023

Additional Permission Set Insights

The **Confidential Data Protection** extension also offers some additional insights into the properties and usage/assignments of permission sets.



Work Date: 23/01/2025

Confidential Data Protection Setup

Permission Sets

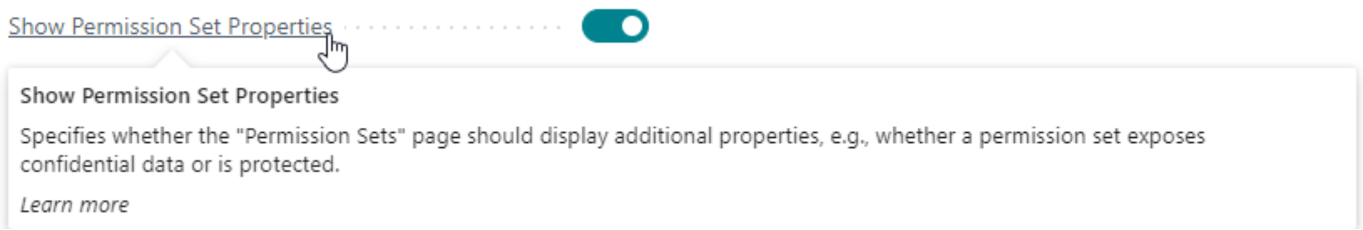
Show Permission Set Properties ● On

Show Permission Set Usage Counts ● On

In the **Permission Sets** tab of the **Confidential Data Protection Setup** page you will find feature toggles that can be used to enable/display or disable/hide these additional properties on the **Permission Sets** page.

Show Permission Set Properties

The **Show Permission Set Properties** field can be used to specify whether the **Permission Sets** page should calculate and show additional fields which describe properties of the permission sets that are used by the **Confidential Data Protection** extension.



Show Permission Set Properties ● On

Show Permission Set Properties

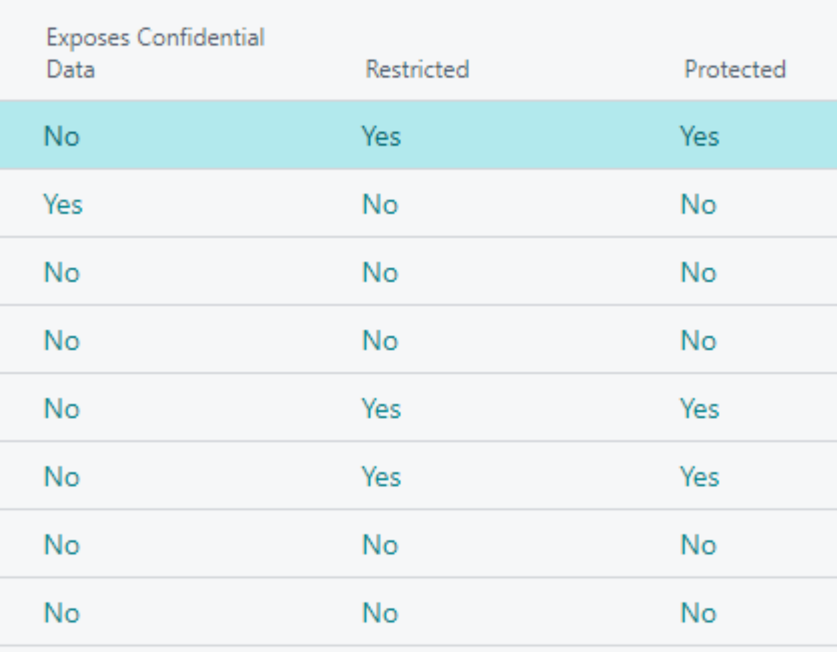
Specifies whether the "Permission Sets" page should display additional properties, e.g., whether a permission set exposes confidential data or is protected.

Learn more

The fields that are added to the **Permission Sets** page when this setting is enabled, are as follows :

- Exposes Confidential Data - Specifies whether the permission set exposes confidential data when it is assigned.

- **Restricted** - Specifies whether the permission set is a restricted permission set, i.e. a permission set in which access to confidential tables has been restricted, making them safe to assign to users.
- **Protected** - Specifies whether the permission set is protected against being edited/modified by a user.



Exposes Confidential Data	Restricted	Protected
No	Yes	Yes
Yes	No	No
No	No	No
No	No	No
No	Yes	Yes
No	Yes	Yes
No	No	No
No	No	No

Protected permission sets

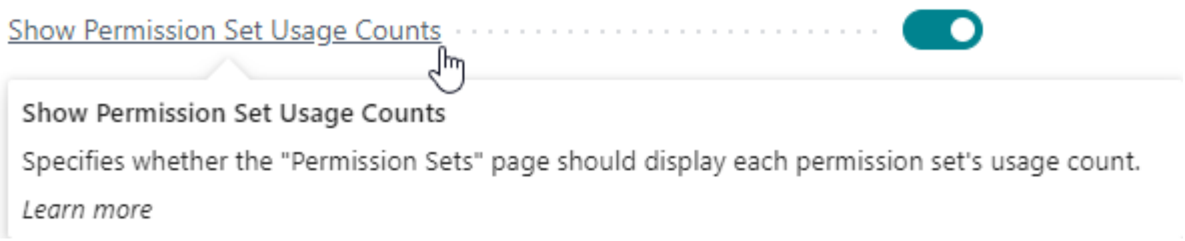
The permission sets that will automatically be marked as **Protected** (protected against being edited/modified) by the **Confidential Data Protection** extension are:

- The **Confidential Data Exclusion** permission set is a protected permission set. It can only be modified by a **SUPER administrator** user via the **Confidential Tables Setup** page.
- A **Restricted** permission set is also a protected permission set. A restricted permission set is a permission set that is automatically generated to restrict access to confidential data, and therefore cannot be edited directly by users.

Note that you can also sort and filter on these fields/properties.

Show Permission Set Usage Counts

The **Show Permission Set Usage Counts** field can be used to configure whether or not the **Permission Sets** page should calculate and show the **Usage Count** field, which specifies the number of usages/assignments of each permission set. This provides you with better insights into which permission sets are assigned to users and to how many users the permission sets are assigned.

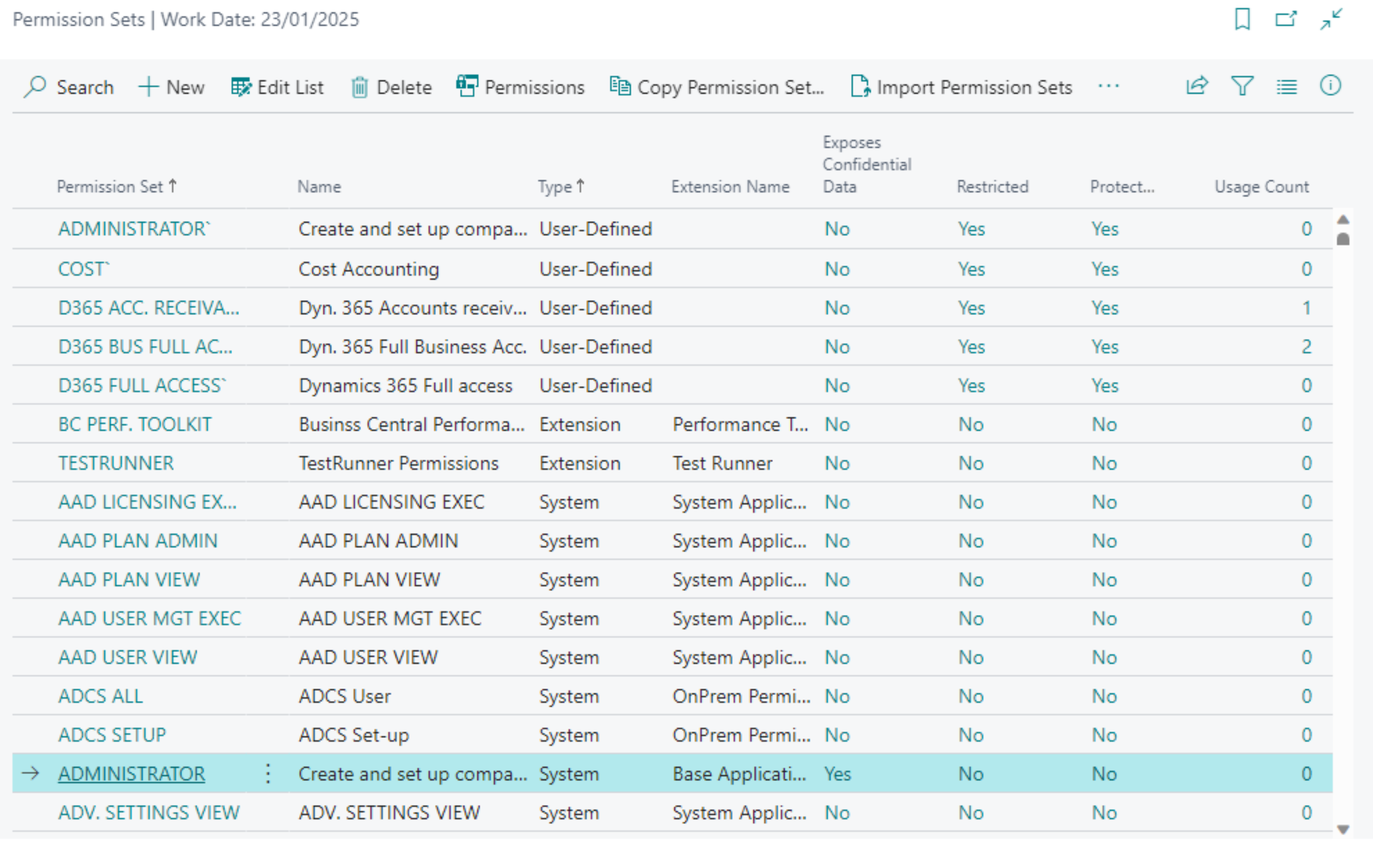


Show Permission Set Usage Counts

Show Permission Set Usage Counts

Specifies whether the "Permission Sets" page should display each permission set's usage count.

Learn more



Permission Sets | Work Date: 23/01/2025

Permission Set ↑	Name	Type ↑	Extension Name	Exposes Confidential Data	Restricted	Protect...	Usage Count
ADMINISTRATOR`	Create and set up compa...	User-Defined		No	Yes	Yes	0
COST`	Cost Accounting	User-Defined		No	Yes	Yes	0
D365 ACC. RECEIVA...	Dyn. 365 Accounts receiv...	User-Defined		No	Yes	Yes	1
D365 BUS FULL AC...	Dyn. 365 Full Business Acc.	User-Defined		No	Yes	Yes	2
D365 FULL ACCESS`	Dynamics 365 Full access	User-Defined		No	Yes	Yes	0
BC PERF. TOOLKIT	Businss Central Performa...	Extension	Performance T...	No	No	No	0
TESTRUNNER	TestRunner Permissions	Extension	Test Runner	No	No	No	0
AAD LICENSING EX...	AAD LICENSING EXEC	System	System Applic...	No	No	No	0
AAD PLAN ADMIN	AAD PLAN ADMIN	System	System Applic...	No	No	No	0
AAD PLAN VIEW	AAD PLAN VIEW	System	System Applic...	No	No	No	0
AAD USER MGT EXEC	AAD USER MGT EXEC	System	System Applic...	No	No	No	0
AAD USER VIEW	AAD USER VIEW	System	System Applic...	No	No	No	0
ADCS ALL	ADCS User	System	OnPrem Permi...	No	No	No	0
ADCS SETUP	ADCS Set-up	System	OnPrem Permi...	No	No	No	0
→ ADMINISTRATOR	Create and set up compa...	System	Base Applicati...	Yes	No	No	0
ADV. SETTINGS VIEW	ADV. SETTINGS VIEW	System	System Applic...	No	No	No	0

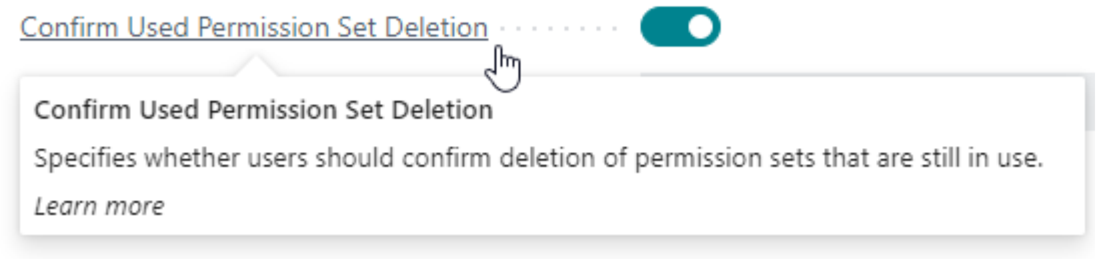
Note that you can also sort and filter on the **Usage Count** field on the **Permission Sets** page.

Last update: September 12, 2023

Confirm Permission Set Deletion

Deleting permission sets should be done with caution, as the permission sets might still be assigned to one or more of your users or groups of users.

On the **Confidential Data Protection Setup** page you can use the **Confirm used Permission Set Deletion** field to specify if a confirmation dialog should be shown when a user attempts to delete a permission set that is still assigned to users or groups of users.



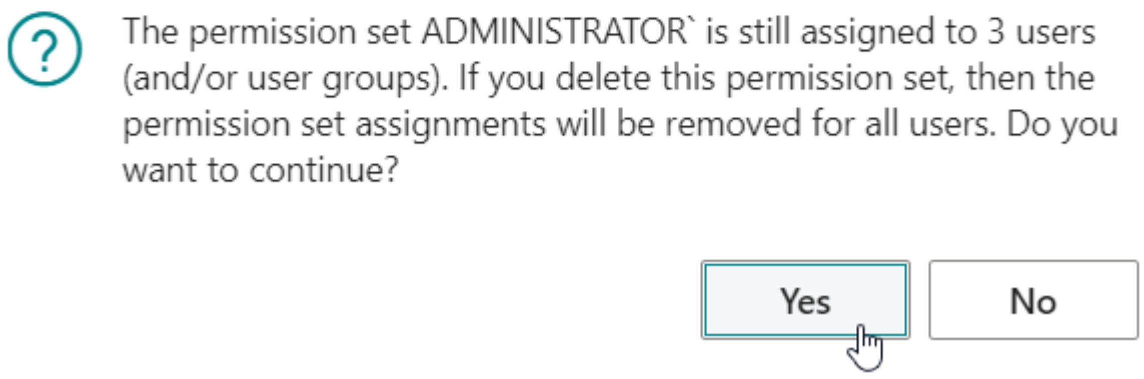
Confirm Used Permission Set Deletion

Confirm Used Permission Set Deletion

Specifies whether users should confirm deletion of permission sets that are still in use.

Learn more

When this setting is enabled, the user will be prompted for confirmation, making the user aware that the permission set that they are attempting to delete is still assigned to one or more users or groups of users.



The permission set ADMINISTRATOR` is still assigned to 3 users (and/or user groups). If you delete this permission set, then the permission set assignments will be removed for all users. Do you want to continue?

If the permission set is not in use (i.e., not assigned to any user or group of users), the confirmation dialog will not be shown.

Last update: September 12, 2023

API Reference Introduction

In this reference documentation you can find an overview of all the objects that make up the public Application Programming Interface (API) of the latest version of the **Confidential Data Protection** extension for Microsoft Dynamics 365 Business Central.

This documentation is intended as a reference for Business Central extension developers who would like to use the exposed functionality in their own extensions.

Codeunit WSB_CDPConfEntryProtection

Implements protection of confidential entries in confidential data tables using security filters. For example, you can create permission sets that allows one to grant users read permissions to G/L entries without exposing confidential G/L data, i.e., by excluding access to G/L entries that relate to G/L accounts that are marked as "Confidential".

Properties

Name	Value
Access	Public

Methods

wgFncCreateSecurityFilterRestrictedPermissionSets:Integer

Creates permission sets which can be used to grant filtered permissions, for example, a permission set to grant access to G/L entries related to non-confidential G/L accounts.

Returns

Type	Description
`Integer`	The number of new permission sets that were created.

wgFncGetSecurityFilterRestrictedPermissionSetRoleID(Integer):Code[20]

Retrieves the role ID of the permission set that grants security filter restricted read access to the specified table.

Parameters

Type	Name	Description
`Integer`	`pTableID`	The ID of the table object to get a security-filtered permission set role ID for.

Returns

Type	Description
`Code[20]`	Role ID of the permission set.

wlEvpOnAfterGetBuiltInConfidentialSecurityFilterValuesForTable(Integer, Text@, Text@, Boolean@)

Allows to apply protection of confidential entries for additional tables.

Parameters

Type	Name	Description
`Integer`	`pTableNo`	The ID of the table.
`Text`	`vSecurityFilterFieldName`	The Security Filter Field Name
`Text`	`vSecurityFilter`	The Security Filter
`Boolean`	`vSecurityFilterApplied`	Whether a security filter was applied/found.

wlEvpOnUpdateGLEntryConfidentialDataProtection(G/L Entry@, Boolean@)

Allows to apply additional protection of G/L Entries for reasons other than Confidential G/L Account. Important note: This event will not be triggered for G/L Entry records that are already considered 'confidential' by the Confidential Data Protection extension and thus cannot be used to override Confidential Data Protection.

Parameters

Type	Name	Description
`Record "G/L Entry"`	`vRecGLEntry`	The G/L Entry record.
`Boolean`	`vIsHandled`	Set this to true if your extension handled the confidential assignment.

Codeunit WSB_CDPConfidentialPermSetMgt

Implements functionality related to exposure of confidential data by permission sets.

Properties

Name	Value
Access	Public

Methods

wgFncConfidentialDataExclusionPermissionSetExists:Boolean

Returns whether the "Confidential Data Exclusion" permission set exists.

Returns

Type	Description
`Boolean`	true iff the "Confidential Data Exclusion" permission exists.

wgFncGetConfidentialDataExclusionPermissionSet(Tenant Permission Set@)

Gets the "Confidential Data Exclusion" (tenant) permission set (and creates it if it does not exist yet).

Parameters

Type	Name	Description
`Record "Tenant Permission Set"`	`vRecTenantPermissionSet`	The "Confidential Data Exclusion" (tenant) permission set

wgFncGetConfidentialPermissionSets(Permission Set Buffer@)

Retrieves the confidential permission sets in a buffer table.

Parameters

Type	Name	Description
`Record "Permission Set Buffer" temporary`	`vRecTempPermissionSetBuffer`	

wgFncGetConfidentialTableObjectIDs(List[Integer]@)

Gets the object IDs (as a list) of the tables that are considered as containing confidential data.

Parameters

Type	Name	Description
`List`	`vConfidentialTableObjectIDs`	The confidential table object IDs in a list.

wgFncGetConfidentialTableObjectIDs(Boolean, List[Integer]@)

Gets the object IDs (as a list) of the tables that are considered as containing confidential data.

Parameters

Type	Name	Description
`Boolean`	`pFullyConfidentialOnly`	Whether to only include that the tables were all records are confidential.
`List`	`vConfidentialTableObjectIDs`	The confidential table object IDs in a list.

wgFncGetConfidentialTableObjectIDsFilter:Text

Gets a filter string with the object IDs of the tables that are considered as containing confidential data.

Returns

Type	Description
`Text`	The filter string.

wgFncGetConfidentialTableObjectIDsFilter(Boolean):Text

Gets a filter string with the object IDs of the tables that are considered as containing confidential data.

Parameters

Type	Name	Description
`Boolean`	`pFullyConfidentialOnly`	Whether to only include that the tables were all records are confidential.

Returns

Type	Description
`Text`	The filter string.

wgFncGetDefaultConfidentialTableObjectIDs(List[Integer]@)

Gets the object IDs of the tables that are considered as containing confidential data by default.

Parameters

Type	Name	Description
`List`	`vConfidentialTableObjectIDs`	The default confidential table object IDs in a list.

wgFncGetDefaultConfidentialTableObjectIDs(List[Integer]@, Boolean)

Gets the object IDs of the tables that are considered as containing confidential data by default.

Parameters

Type	Name	Description
`List`	`vConfidentialTableObjectIDs`	The default confidential table object IDs in a list.
`Boolean`	`pIncludeExtensionChanges`	Specifies whether to include changes to the defaults applied by extensions.

wgFncIsConfidentialDataExclusionPermissionSet(Tenant Permission Set):Boolean

Returns whether the (tenant) permission set is the "Confidential Data Exclusion" permission set.

Parameters

Type	Name	Description
`Record "Tenant Permission Set"`	`pRecTenantPermissionSet`	The tenant permission set to check.

Returns

Type	Description
`Boolean`	true if the permission set is the "Confidential Data Exclusion" permission set.

wgFncIsConfidentialDataExclusionPermissionSet(Guid, Code[20]):Boolean

Returns whether the permission set with specified role ID and app ID is the "Confidential Data Exclusion" permission set.

Parameters

Type	Name	Description
`Guid`	`pAppID`	The app ID of the permission set.
`Code[20]`	`pRoleID`	The role ID of the permission set.

Returns

Type	Description
`Boolean`	true if the permission set is the "Confidential Data Exclusion" permission set.

wgFncIsConfidentialTableSetupCustomized:Boolean

Returns whether the "Confidential Tables Setup" has been customized, i.e., is different from the default due to changes to the setup by an administrator in the client.

Returns

Type	Description
`Boolean`	true if the Confidential Tables Setup has been customized.

wgFncIsConfidentialTableSetupExtended:Boolean

Returns whether the "Confidential Tables Setup" has been extended, i.e., is different from the default by changes from one or more extensions.

Returns

Type	Description
`Boolean`	true if the Confidential Tables Setup has been extended.

wgFncIsPermissionSetConfidential(Guid, Code[20]):Boolean

Returns whether the permission set with specified role ID and app ID exposes confidential data.

Parameters

Type	Name	Description
`Guid`	`pAppID`	The app ID of the permission set.
`Code[20]`	`pRoleID`	The role ID of the permission set.

Returns

Type	Description
`Boolean`	true if the permission set exposes confidential data.

wgFncIsPermissionSetWithFullyConfidentialTables(Guid, Code[20]):Boolean

Returns whether the permission set with specified role ID and app ID exposes confidential data of tables where all records are confidential.

Parameters

Type	Name	Description
`Guid`	`pAppID`	The app ID of the permission set.
`Code[20]`	`pRoleID`	The role ID of the permission set.

Returns

Type	Description
`Boolean`	true if the permission set exposes confidential data of tables where all records are confidential.

wgFncIsTenantPermissionExcludingConfidentialDataTable(Tenant Permission):Boolean

Returns whether the tenant permission excludes confidential data.

Parameters

Type	Name	Description
`Record "Tenant Permission"`	`pRecTenantPermission`	The tenant permission.

Returns

Type	Description
`Boolean`	true if the tenant permission excludes confidential data.

wgFncIsTenantPermissionExcludingConfidentialDataTable(Tenant Permission, Boolean):Boolean

Returns whether the tenant permission excludes confidential data.

Parameters

Type	Name	Description
`Record "Tenant Permission"`	`pRecTenantPermission`	The tenant permission.
`Boolean`	`pFullyConfidentialOnly`	Whether to only include that the tables were all records are confidential.

Returns

Type	Description
`Boolean`	true if the tenant permission excludes confidential data.

wgFncIsTenantPermissionForConfidentialTable(Tenant Permission):Boolean

Returns whether the tenant permission is related to confidential data.

Parameters

Type	Name	Description
`Record "Tenant Permission"`	`pRecTenantPermission`	The tenant permission.

Returns

Type	Description
`Boolean`	true if the tenant permission is related to confidential data.

wgFncIsTenantPermissionForConfidentialTable(Tenant Permission, Boolean):Boolean

Returns whether the tenant permission is related to confidential data.

Parameters

Type	Name	Description
`Record "Tenant Permission"`	`pRecTenantPermission`	The tenant permission.
`Boolean`	`pFullyConfidentialOnly`	Whether to only include that the tables were all records are confidential.

Returns

Type	Description
`Boolean`	true if the tenant permission is related to confidential data.

wgFncIsTenantPermissionIncludingConfidentialDataTable(Tenant Permission):Boolean

Returns whether the tenant permission includes/exposes confidential data.

Parameters

Type	Name	Description
`Record "Tenant Permission"`	`pRecTenantPermission`	The tenant permission.

Returns

Type	Description
`Boolean`	true if the tenant permission includes/exposes confidential data.

wgFncIsTenantPermissionIncludingConfidentialDataTable(Tenant Permission, Boolean):Boolean

Returns whether the tenant permission includes/exposes confidential data.

Parameters

Type	Name	Description
`Record "Tenant Permission"`	`pRecTenantPermission`	The tenant permission.
`Boolean`	`pFullyConfidentialOnly`	Whether to only include that the tables were all records are confidential.

Returns

Type	Description
`Boolean`	true if the tenant permission includes/exposes confidential data.

wgFncRestoreConfidentialTableSetupDefaults

Restores the default configuration in the Confidential Table Setup table.

wgFncSetConfidentialTableFiltersOnExpandedPermission(Guid, Code[20], Expanded Permission@)

Applies filters on a "Expanded Permission" record to only get the permissions that expose confidential table data for a permission set with specified role ID and app ID.

Parameters

Type	Name	Description
`Guid`	`pAppID`	The app ID of the permission set to get the confidential permissions for.
`Code[20]`	`pRoleID`	The role ID of the permission set to get the confidential permissions for.
`Record "Expanded Permission"`	`vRecExpandedPermission`	The "Expanded Permission" record to apply the filters to.

wgFncSetConfidentialTableFiltersOnExpandedPermission(Guid, Code[20], Boolean, Expanded Permission@)

Applies filters on a "Expanded Permission" record to only get the permissions that expose confidential table data for a permission set with specified role ID and app ID.

Parameters

Type	Name	Description
`Guid`	`pAppID`	The app ID of the permission set to get the confidential permissions for.
`Code[20]`	`pRoleID`	The role ID of the permission set to get the confidential permissions for.
`Record "Expanded Permission"`	`vRecExpandedPermission`	The "Expanded Permission" record to apply the filters to.
`Boolean`	`pFullyConfidentialOnly`	Whether to only include that the tables were all records are confidential.

wgFncSetConfidentialTableFiltersOnExpandedPermission(Expanded Permission@)

Applies filters on a "Expanded Permission" record to only get the permissions that expose confidential table data.

Parameters

Type	Name	Description
`Record "Expanded Permission"`	`vRecExpandedPermission`	The "Expanded Permission" record to apply the filters to.

wgFncSetConfidentialTableFiltersOnExpandedPermission(Expanded Permission@, Boolean)

Applies filters on a "Expanded Permission" record to only get the permissions that expose confidential table data.

Parameters

Type	Name	Description
`Record "Expanded Permission"`	`vRecExpandedPermission`	The "Expanded Permission" record to apply the filters to.
`Boolean`	`pFullyConfidentialOnly`	Whether to only include that the tables were all records are confidential.

wgFncViewConfidentialDataExclusionPermissionSet

Opens a page to view the confidential data exclusion permission set.

wgFncViewConfidentialPermissionsInPermissionSets

Opens a page to view the details of all TableData Direct Read permissions in confidential permission sets.

wgFncViewConfidentialPermissionsOfPermissionSet(Guid, Code[20])

Opens a page to view the confidential permissions exposed by a permission set.

Parameters

Type	Name	Description
`Guid`	`pAppID`	The app ID of the permission set.
`Code[20]`	`pRoleID`	The role ID of the permission set.

wlEvpOnAfterGetDefaultConfidentialTableObjectIDs(Dictionary[Integer, Boolean]@)

Allows to adjust which confidential tables should be considered confidential. Please note that it is not possible to remove table object ID = 0 (All table data) via an event subscriber to this event publisher.

Parameters

Type	Name	Description
`Dictionary`	`vConfidentialTableObjectIDSet`	The set of table object IDs of the confidential tables.

IExpClnAfterGetDefaultConfidentialTableObjectIDs(Dictionary[Integer, Boolean]@)

Codeunit WSB_CDPInternalPermSetMgt

Exposes procedures to help with identifying internal permissions (SUPER, SUPER (DATA) and SECURITY).

Properties

Name	Value
Access	Public

Methods

wgFncGetInternalPermissionSetRoleIDs:List[Code]

Gets the role IDs of the internal permission sets as a list.

Returns

Type	Description
`List`	The list of role IDs of the internal permission sets.

wgFncGetSuperPermissionSetRoleID:Code[20]

Gets the role ID of the SUPER permission set.

Returns

Type	Description
`Code[20]`	The role ID of the SUPER permission set.

wgFncIsInternalPermissionSet(Code[20]):Boolean

Checks whether the permission set with specified role ID is an internal permission set (SUPER, SUPER (DATA) or SECURITY).

Parameters

Type	Name	Description
`Code[20]`	`pRoleID`	The role ID of the permission set.

Returns

Type	Description
`Boolean`	true iff the permission set is an internal permission set.

Codeunit WSB_CDPPermSetRestriction

Implements functionality for restricting permission sets to prevent exposure of confidential data.

Properties

Name	Value
Access	Public

Methods

wgFncIsPermissionSetRestricted(Option, Guid, Code[20]):Boolean

Returns whether the permission set with specified scope, app ID and role ID is a restricted permission set.

Parameters

Type	Name	Description
`Option`	`pScope`	The scope of the permission set.
`Guid`	`pAppID`	The app ID of the permission set.
`Code[20]`	`pRoleID`	The role ID of the permission set.

Returns

Type	Description
`Boolean`	true if the permission set is a restricted permission set.

Codeunit WSB_CDPPermissionSetAssignment

Implements functionality to protect against permission assignments that would expose confidential data.

Properties

Name	Value
Access	Public

Methods

wgFncVerifyCurrentUserCanAssignInternalPermissionSet

Verifies that the current user is a user which can assign the SUPER permission set. Throws an error if the current user is not allowed to assign the SUPER permission set.

Codeunit WSB_CDPPermissionSetLookup

Provides procedures to conveniently look up permission sets.

Properties

Name	Value
Access	Public

Methods

wgFncLookupPermissionSets(Boolean, Aggregate Permission Set, Aggregate Permission Set@):Boolean

Opens the "Lookup Permission Set" page to select permission sets. If the user clicks on "OK" to close the page, the selected permission set(s) will be returned.

Parameters

Type	Name	Description
`Boolean`	`pAllowMultiselect`	Whether to allow multi-select.
`Record "Aggregate Permission Set"`	`pRecSelectedAggregatePermissionSet`	The permission set the user had selected before opening the page.
`Record "Aggregate Permission Set" temporary`	`vRecTempAggregatePermissionSet`	The selected permission set(s).

Returns

Type	Description
`Boolean`	true iff the user selected permission set(s) and pressed "OK".

wgFncLookupPermissionSets(Boolean, Aggregate Permission Set@):Boolean

Opens the "Lookup Permission Set" page to select permission sets. If the user clicks on "OK" to close the page, the selected permission set(s) will be returned.

Parameters

Type	Name	Description
`Boolean`	`pAllowMultiselect`	Whether to allow multi-select.
`Record "Aggregate Permission Set" temporary`	`vRecTempAggregatePermissionSet`	The selected permission set(s).

Returns

Type	Description
`Boolean`	true iff the user selected permission set(s) and pressed "OK".

wgFncMultiselectAccessControlPermissionSetLookup(Access Control):Boolean

Opens the permission set lookup page, allowing for multi-select. When the user clicks "OK", the selected permission sets are assigned to the user.

Parameters

Type	Name	Description
`Record "Access Control"`	`pRecAccessControl`	The selected access control ('user permission set assignment') record which specifies the "User Security ID".

Returns

Type	Description
`Boolean`	true iff user permission sets were assigned.

Codeunit WSB_CDPPermissionSetProtection

Implements permission set protection, preventing users from editing specific permission sets.

Properties

Name	Value
Access	Public

Methods

wgFncIsPermissionSetProtected(Option, Guid, Code[20]):Boolean

Returns whether the permission set with specified scope, app ID and role ID is a protected permission set.

Parameters

Type	Name	Description
`Option`	`pScope`	The scope of the permission set.
`Guid`	`pAppID`	The app ID of the permission set.
`Code[20]`	`pRoleID`	The role ID of the permission set.

Returns

Type	Description
`Boolean`	true if the permission set is a protected permission set.

wlEvpOnAfterIsPermissionSetProtected(Option, Guid, Code[20], Boolean@)

Allows to implement *additional* conditions under which permission sets should be protected.

Parameters

Type	Name	Description
`Option`	`pScope`	The scope for the permission set
`Guid`	`pAppID`	The app ID of the permission set.
`Code[20]`	`pRoleID`	The role ID of the permission set.
`Boolean`	`vResult`	Set this parameter to true in your extension if the permission with specified parameters should be protected.

Codeunit WSB_CDPPermissionSetUsage

Exposes procedures to get insights into the usage/assignments of permission sets.

Properties

Name	Value
Access	Public

Methods

wgFncGetAllPermissionSetUsages(WSB_CDPPermSetUsage@)

Retrieves all permission set usages and stores them in a temporary record set.

Parameters

Type	Name	Description
`Record "WSB_CDPPermSetUsage" temporary`	`vRecTempWSB_CDPPermSetUsage`	A temporary record set in which all permission set usages are stored.

wgFncGetPermissionSetUsages(Permission Set Buffer, WSB_CDPPermSetUsage@)

Retrieve the usages of a permission set and stores them in a temporary record set.

Parameters

Type	Name	Description
`Record "Permission Set Buffer" temporary`	`pRecTempPermissionSetBuffer`	The permission set.
`Record "WSB_CDPPermSetUsage" temporary`	`vRecTempWSB_CDPPermSetUsage`	A temporary record set in which all permission set usages are stored.

wgFncGetPermissionSetUsageCount(Permission Set Buffer):Integer

Gets the total usage count of the permission set.

Parameters

Type	Name	Description
`Record "Permission Set Buffer" temporary`	`pRecTempPermissionSetBuffer`	Permission set

Returns

Type	Description
`Integer`	The number of times the permission set is referenced in permission set assignments.

wgFncSetAccessControlPermissionSetUsageFilters(Permission Set Buffer, Access Control@)

Filters the "Access Control" table record to usages of a permission set.

Parameters

Type	Name	Description
`Record "Permission Set Buffer" temporary`	`pRecTempPermissionSetBuffer`	Permission set
`Record "Access Control"`	`vRecAccessControl`	The "Access Control" table record to filter.

wgFncSetUserGroupPermissionSetUsageFilters(Permission Set Buffer, User Group Permission Set@)

Obsolete

User Groups are deprecated. This procedure will be removed when user groups are no longer available. Use wgFncGetPermissionSetAccessControlUsages instead. 1.0.0.0

Filters the "User Group Permission Set" table record to usages of a permission set.

Parameters

Type	Name	Description
`Record "Permission Set Buffer" temporary`	`pRecTempPermissionSetBuffer`	Permission set
`Record "User Group Permission Set"`	`vRecUserGroupPermissionSet`	The "User Group Permission Set" table record to filter.

wgFncViewPermissionSetUsages(Permission Set Buffer)

Opens a page to view the usages of a permission set.

Parameters

Type	Name	Description
`Record "Permission Set Buffer" temporary`	`pRecTempPermissionSetBuffer`	The permission set.

wgFncViewInternalPermissionSetUsages

Opens a page to view the usages of the SUPER, SUPER (DATA) and SECURITY permission sets.

wgFncViewSUPERPermissionSetUsages

Opens a page to view the usages of the SUPER permission set.

Codeunit WSB_CDPPermissionViolation

Exposes procedures to identify and resolve confidentiality-violating permission assignments.

Properties

Name	Value
Access	Public

Methods

OnRun

Resolves the confidentiality-violating permission assignments in the environment.

wgFncGetConfidentialPermissionAssignmentViolations(WSB_CDPPermSetUsage@)

Retrieves the confidentiality-violating permission assignments.

Parameters

Type	Name	Description
`Record "WSB_CDPPermSetUsage" temporary`	`vRecTempWSB_CDPViolation`	Temporary record set to store the violations in.

wgFncGetConfidentialPermissionAssignmentViolationsCount:Integer

Retrieves the number of confidentiality-violating permission assignments.

Returns

Type	Description
`Integer`	The number of violations found.

wgFncInitJobQueueEntry(Job Queue Entry@):Boolean

Initializes a job queue entry that periodically resolves the confidentiality-violating permission assignments.

Parameters

Type	Name	Description
`Record "Job Queue Entry"`	`vRecJobQueueEntry`	The job queue entry.

Returns

Type	Description
`Boolean`	true iff the job queue entry was successfully set up.

wgFncResolveConfidentialPermissionAssignmentViolations

Resolves the confidentiality-violating permission assignments.

wgFncResolveConfidentialPermissionAssignmentViolations(Boolean)

Resolves the confidentiality-violating permission assignments.

Parameters

Type	Name	Description
`Boolean`	`pConfirm`	Whether to request confirmation from the user before making any changes.

wgFncViewConfidentialPermissionSetAssignmentViolations

Opens a page to view the confidentiality-violating permission assignments.

Codeunit WSB_CDPSuperAdminMgt

Implements the "SUPER Admin" functionality.

Properties

Name	Value
Access	Public

Methods

wgFncIsCurrentUserSuper:Boolean

Gets whether the current user is SUPER.

Returns

Type	Description
`Boolean`	true iff the current user is SUPER.

wgFncIsCurrentUserSuperAdmin:Boolean

Gets whether the current user is a "SUPER Admin".

Returns

Type	Description
`Boolean`	true iff the current user is a "SUPER Admin".

wgFncIsUserSuper(Code[50]):Boolean

Gets whether or not the specified user is a SUPER user.

Parameters

Type	Name	Description
`Code[50]`	`pUserID`	The user ID of the user to check

Returns

Type	Description
`Boolean`	true iff the specified user is SUPER.

wgFncIsUserSuperAdmin(Code[50]):Boolean

Gets whether the specified user is a "SUPER Admin".

Parameters

Type	Name	Description
`Code[50]`	`pUserID`	The User ID of the user to check.

Returns

Type	Description
`Boolean`	true iff the specified user is a "SUPER Admin".

wgFncSuperAdminUsersExists:Boolean

Gets whether any SUPER admin user exists in this environment/database.

Returns

Type	Description
`Boolean`	true iff any SUPER admin user exists.

wgFncVerifyCurrentUserIsSuper

Verifies that the current user is a user that has the SUPER permission set. Throws an error if the current user does not have the SUPER permission set.

wgFncVerifyUserIsSuper(Code[50])

Verifies that the specified user is a user that has the SUPER permission set. Throws an error if the specified user does not have the SUPER permission set.

Parameters

Type	Name	Description
`Code[50]`	`pUserID`	The user ID of the user to check.

PageExtension WSB_ApportunixRoleCenterCDP

A page extension which adds navigation action for the "Confidential Data Protection" extension to the "Apportunix Rolecenter".

PageExtension WSB_ChartOfAccountsCDP

A page extension for the "Chart of Accounts" page that adds the "Confidential" field.

PageExtension WSB_ChartOfAccountsOverviewCDP

A page extension for the "Chart of Accounts Overview" page that adds the "Confidential" field.

PageExtension WSB_GLAccountCardCDP

A page extension for the "G/L Account Card" page that adds the "Confidential" field.

PageExtension WSB_LookupPermissionSetCDP

A page extension for the "Lookup Permission Set" page that adds additional fields.

PageExtension WSB_PermissionSetCDP

A page extension for the "Permission Set" page that adds additional fields.

PageExtension WSB_PermissionSetsCDP

A page extension for the "Permission Sets" page that adds additional fields.

PageExtension WSB_UserSubformCDP

A page extension for the "User subform" page (i.e., User Permission Set assignments).

PageExtension WSB_UsersCDP

A page extension for the "Users" page.

Page WSB_CDPConfTableSetupPart

A listpart page where one can view the tables which should be considered as containing confidential data. Customizing the Confidential Table Setup configuration is supported, but disabled in the initial version of the extension. Extending the Confidential Table Setup configuration is supported and enabled though.

Properties

Name	Value
ApplicationArea	#All
Caption	Confidential Tables
DeleteAllowed	False
Editable	False
Extensible	False
InsertAllowed	False
ModifyAllowed	False
PageType	ListPart
SourceTable	70257897

Page WSB_CDPConfidentialTableSetup

A list page where one can view the tables which should be considered as containing confidential data. Customizing the Confidential Table Setup configuration is supported, but disabled in the initial version of the extension. Extending the Confidential Table Setup configuration is supported and enabled though.

Properties

Name	Value
ApplicationArea	#All
Caption	Confidential Tables Setup
DeleteAllowed	False
Editable	False
Extensible	False
InsertAllowed	False
ModifyAllowed	False
PageType	List
SourceTable	70257897
UsageCategory	None

Page WSB_CDPExpandedPermissions

A list page to view all permissions in the environment.

Properties

Name	Value
ApplicationArea	#All
Caption	Expanded Permissions
Editable	False
Extensible	False
PageType	List
SourceTable	2000000254
UsageCategory	None

Page WSB_CDPPermSetUsageListPart

A listpart page to view permission set usages by users or user groups.

Properties

Name	Value
ApplicationArea	#All
Caption	Permission Set Usages
DeleteAllowed	False
InsertAllowed	False
ModifyAllowed	False
PageType	ListPart
SourceTable	70257899
SourceTableTemporary	True

Methods

wgFncRefresh

Updates the permission set usages with the most recent state.

wgFncSetConfidentialAssignmentViolationsOnly(Boolean)

Allows one to set whether the permission set usages should only include confidentiality-violating permission set assignments.

Parameters

Type	Name	Description
`Boolean`	`pConfidentialAssignmentViolationsOnly`	Whether to restrict to confidentiality-violating assignments.

Page WSB_CDPPermSetUsages

A page to view permission set usages by users or user groups.

Properties

Name	Value
ApplicationArea	#All
Caption	Permission Set Usages
DeleteAllowed	False
InsertAllowed	False
ModifyAllowed	False
PageType	List
SourceTable	70257899
SourceTableTemporary	True
UsageCategory	None

Methods

wgFncRefresh

Updates the permission set usages with the most recent state.

wgFncSetConfidentialAssignmentViolationsOnly(Boolean)

Allows one to set whether the permission set usages should only include confidentiality-violating permission set assignments.

Parameters

Type	Name	Description
`Boolean`	`pConfidentialAssignmentViolationsOnly`	Whether to restrict to confidentiality-violating assignments.

wgFncSetPermissionSet(Permission Set Buffer)

Allows one to set a single permission set to show the usages for.

Parameters

Type	Name	Description
`Record "Permission Set Buffer" temporary`	`pRecTempPermSetBuffer`	The permission set.

wgFncSetPermissionSetFilters(WSB_CDPPermSetUsage@)

Allows one to set filters to limit the usages that should be shown.

Parameters

Type	Name	Description
`Record "WSB_CDPPermSetUsage"`	`vRecWSB_CDPPermSetUsage`	The record that specifies the filters to apply.

Page WSB_CDPResolvedViolationLog

A list page to view the confidentiality-violating permission assignments resolved by the Confidential Data Protection extension.

Properties

Name	Value
ApplicationArea	#All
Caption	Resolved Violation Log
DeleteAllowed	False
Editable	False
InsertAllowed	False
ModifyAllowed	False
PageType	List
SourceTable	70257901
SourceTableView	sorting(ResolvedDateTime) order(descending)
UsageCategory	None

Fields

ID	Type	Name	Description
	``	`EntryNo`	Entry No. of the resolved confidentiality-violating permission assignment.
	``	`ResolvedDateTime`	The date and time at which the violation was resolved.

ID	Type	Name	Description
	``	`UserSecurityID`	Security ID of the user using the permission set.
	``	`UserName[50]`	Name of the user using the permission set.
	``	`UserFullName[80]`	Full name of the user using the permission set.
	``	`UserLicenseType`	License Type of the user using the permission set.
	``	`UserGroupCode[20]`	Code of the user group using the permission set.
	``	`UserGroupName[50]`	Name of the user group using the permission set.
	``	`PermissionSetScope`	Scope of the permission set.
	``	`AppID`	ID of the app that the permission set comes from.
	``	`RoleID[20]`	Role ID of the permission set.
	``	`RoleName[30]`	Role Name of the permission set.
	``	`CompanyName[30]`	Name of the company for which the permission set assignment applies.

Page WSB_CDPRestrictedPermSets

A list page for viewing all restricted permission sets.

Properties

Name	Value
ApplicationArea	#All
Caption	Restricted Permission Sets
DeleteAllowed	False
Editable	False
InsertAllowed	False
ModifyAllowed	False
PageType	List
SourceTable	70257895
UsageCategory	None

Page WSB_CDPSetup

A page to view and edit settings for the Apportunix Confidential Data Protection app.

Properties

Name	Value
AccessByPermission	tabledata WSB_CDPSetup = M
ApplicationArea	#All
Caption	Confidential Data Protection Setup
DeleteAllowed	False
InsertAllowed	False
ModifyAllowed	True
PageType	Card
SourceTable	70257898
UsageCategory	Administration

Fields

ID	Type	Name	Description
	``	`PrimaryKey[10]`	A setup primary key field.
	``	`SuperAdminCount`	Specifies the number of users designated as SUPER administrators.
	``	`ConfidentialTableCount`	Specifies the number of tables that are set-up to be considered as containing confidential data.

ID	Type	Name	Description
	``	`ConfidentialGLAccountCount`	Specifies the number of G/L Accounts that are set-up to be considered as concerning confidential data.
	``	`RestrictedPermissionSetCount`	Specifies the number of restricted permission sets which are generated permission sets which restrict access to confidential table data.
	``	`ShowPermissionSetProperties`	Specifies whether the "Permission Sets" page should display additional properties, e.g., whether a permission set exposes confidential data or is protected.
	``	`ShowPermissionSetUsageCounts`	Specifies whether the "Permission Sets" page should display each permission set's usage count.
	``	`ConfirmUsedPermSetDeletion`	Specifies whether users should confirm deletion of permission sets that are still in use.

Page WSB_CDPSetupWizard

A setup wizard page to configure the Apportunix Confidential Data Protection app.

Properties

Name	Value
AccessByPermission	tabledata WSB_CDPSetup = M
ApplicationArea	#All
Caption	Confidential Data Protection Setup Wizard
DeleteAllowed	False
InsertAllowed	False
ModifyAllowed	True
PageType	NavigatePage
SourceTable	70257898
UsageCategory	Administration

Methods

wlEvpOnBeforeFinish

Allows one to perform additional actions when a user clicks on Finish in the setup wizard page.

Page WSB_CDPSuperAdministrators

A list page that allows you to easily set-up the preferred users as SUPER administrators.

Properties

Name	Value
ApplicationArea	#All
Caption	SUPER Administrators
DeleteAllowed	True
Extensible	False
InsertAllowed	True
ModifyAllowed	True
PageType	List
SourceTable	70257900
UsageCategory	None

Page WSB_CDPSuperAdministratorsPart

A listpart page that allows you to easily set-up the preferred users as SUPER administrators.

Properties

Name	Value
ApplicationArea	#All
Caption	SUPER Administrators
DeleteAllowed	True
Extensible	False
InsertAllowed	True
ModifyAllowed	True
PageType	ListPart
SourceTable	70257900

Page WSB_CDPTenantPermissionSets

A list page for viewing all tenant permission sets.

Properties

Name	Value
ApplicationArea	#All
Caption	Tenant Permission Sets
DeleteAllowed	True
Extensible	False
InsertAllowed	False
ModifyAllowed	False
PageType	List
SourceTable	2000000165
UsageCategory	None

PermissionSet WSB_CDP_ADM

A permission set that grants administrator priviliges for the Apportunix Confidential Data Protection app.

Properties

Name	Value
Access	Public
Assignable	1
Caption	Apportunix Conf. Data P. Admin
IncludedPermissionSets	WSB_CDP_USR

PermissionSet WSB_CDP_USR

A permission set that allows one to use the features of the Apportunix Confidential Data Protection app.

Properties

Name	Value
Access	Public
Assignable	1
Caption	Apportunix Conf. Data P. User
IncludedPermissionSets	#e0f70cf530044fd79ec00efe161a6f20#WSB_MON

TableExtension WSB_GLAccountCDP

A table extension for the "G/L Account" table which adds the "Confidential" field.

TableExtension WSB_GLBudgetEntryCDP

A table extension for the "G/L Budget Entry" table which adds the "Confidential" field.

TableExtension WSB_GLEntryCDP

A table extension for the "G/L Entry" table.

TableExtension WSB_PermissionSetBufferCDP

A table extension for the "Permission Set Buffer" table which adds additional fields.

Table WSB_CDPPermSetUsage

A temporary table to store permission set usages.

Properties

Name	Value
Access	Public
Caption	Permission Set Usage
Extensible	False
TableType	Temporary

Fields

ID	Type	Name	Description
1	`Integer`	`EntryNo`	Entry no. for the permission set usage.
10	`Guid`	`UserSecurityID`	Security ID of the user using the permission set.
	``	`UserName[50]`	Name of the user using the permission set.
	``	`UserFullName[80]`	Full name of the user using the permission set.
13	`Option`	`UserLicenseType`	License Type of the user using the permission set.
	``	`UserGroupCode[20]`	Code of the user group using the permission set.
	``	`UserGroupName[50]`	Name of the user group using the permission set.
30	`Option`	`PermissionSetScope`	Scope of the permission set.
31	`Guid`	`AppID`	ID of the app that the permission set comes from.

ID	Type	Name	Description
	``	`RoleID[20]`	Role ID of the permission set.
	``	`RoleName[30]`	Role Name of the permission set.
	``	`CompanyName[30]`	Name of the company for which the permission set assignment applies.

Table WSB_CDPRestrictedPermissionSet

Stores which (tenant) permission sets are restricted permission sets.

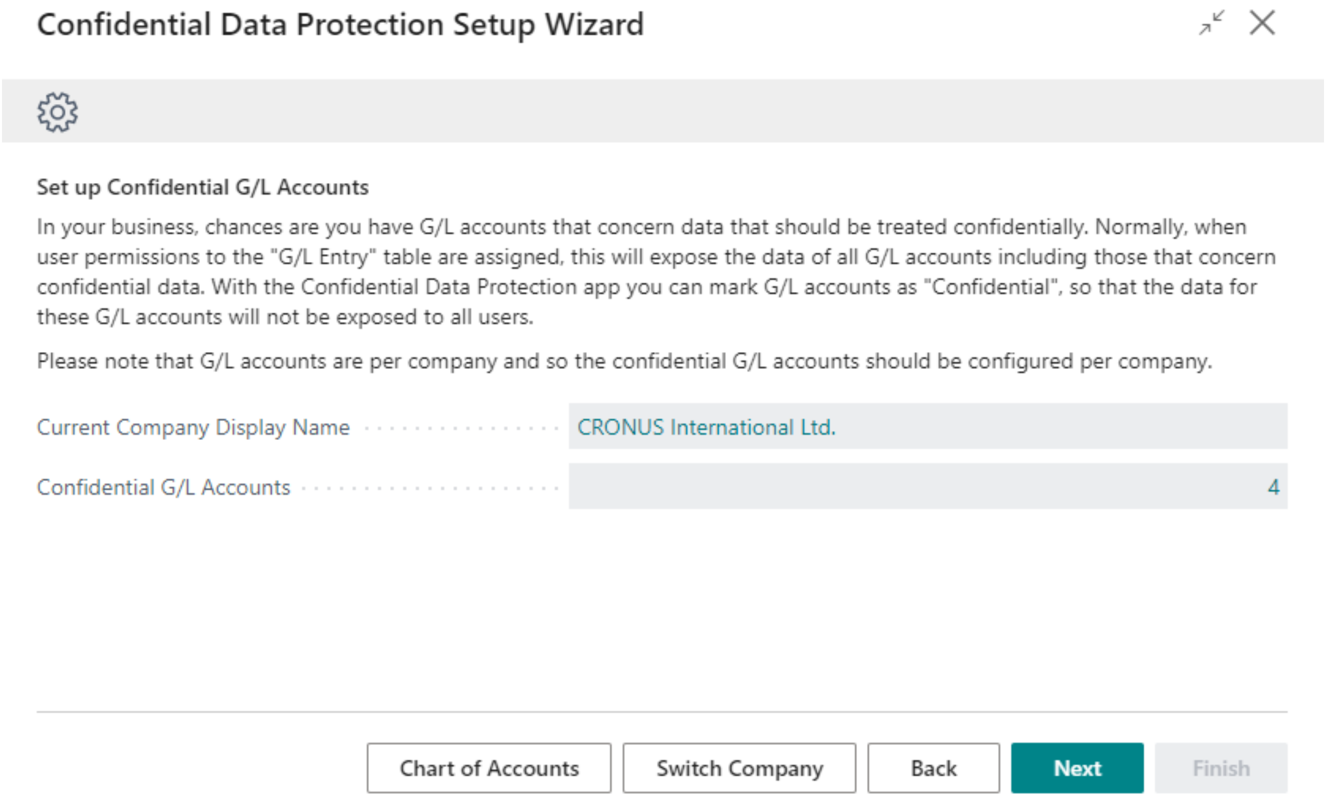
Properties

Name	Value
Access	Internal
Caption	Restricted Permission Set
DataClassification	SystemMetadata
DataPerCompany	False
DrillDownPageId	WSB_CDPRestrictedPermSets
LookupPageId	WSB_CDPRestrictedPermSets
ReplicateData	False

Changelog

1.8.0.0 2024-01-29

- Improved the **Confidential G/L Accounts** step on the **Confidential Data Protection Setup Wizard** page for setting up confidential G/L accounts **per company**.



Confidential Data Protection Setup Wizard

Set up Confidential G/L Accounts

In your business, chances are you have G/L accounts that concern data that should be treated confidentially. Normally, when user permissions to the "G/L Entry" table are assigned, this will expose the data of all G/L accounts including those that concern confidential data. With the Confidential Data Protection app you can mark G/L accounts as "Confidential", so that the data for these G/L accounts will not be exposed to all users.

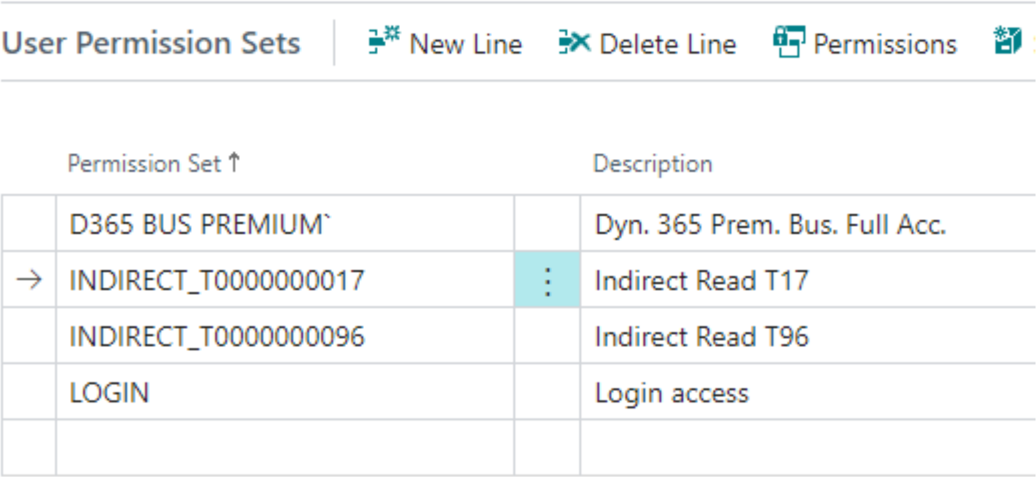
Please note that G/L accounts are per company and so the confidential G/L accounts should be configured per company.

Current Company Display Name: CRONUS International Ltd.

Confidential G/L Accounts: 4

  - A new text has been added to make the user aware that G/L accounts should be marked for each company.
  - A **Current Company Display Name** field has been added. Drilling down on this field opens the **User Settings** page so that the user can easily switch to a different company if needed.
  - A **Chart of Accounts** action has been added so that the user can easily open the **Chart of Accounts** page for marking G/L accounts as confidential.
  - A **Switch Company** action has been added which opens the **User Settings** page so that the user can easily switch to a different company if needed.
- When an attempt is made to assign a permission set that exposes confidential data by granting direct read access, then Confidential Data Protection restricts the permission set assignments by replacing it with a permission set to which security-filters are applied for the relevant tables containing confidential data. However, this could cause issues in very special scenarios when codeunits would only require indirect read access to a confidential table. Therefore now the extension will also automatically grant **full indirect read**

access next to the restricted/security-filtered direct read access by assigning a permission set for each relevant confidential table.

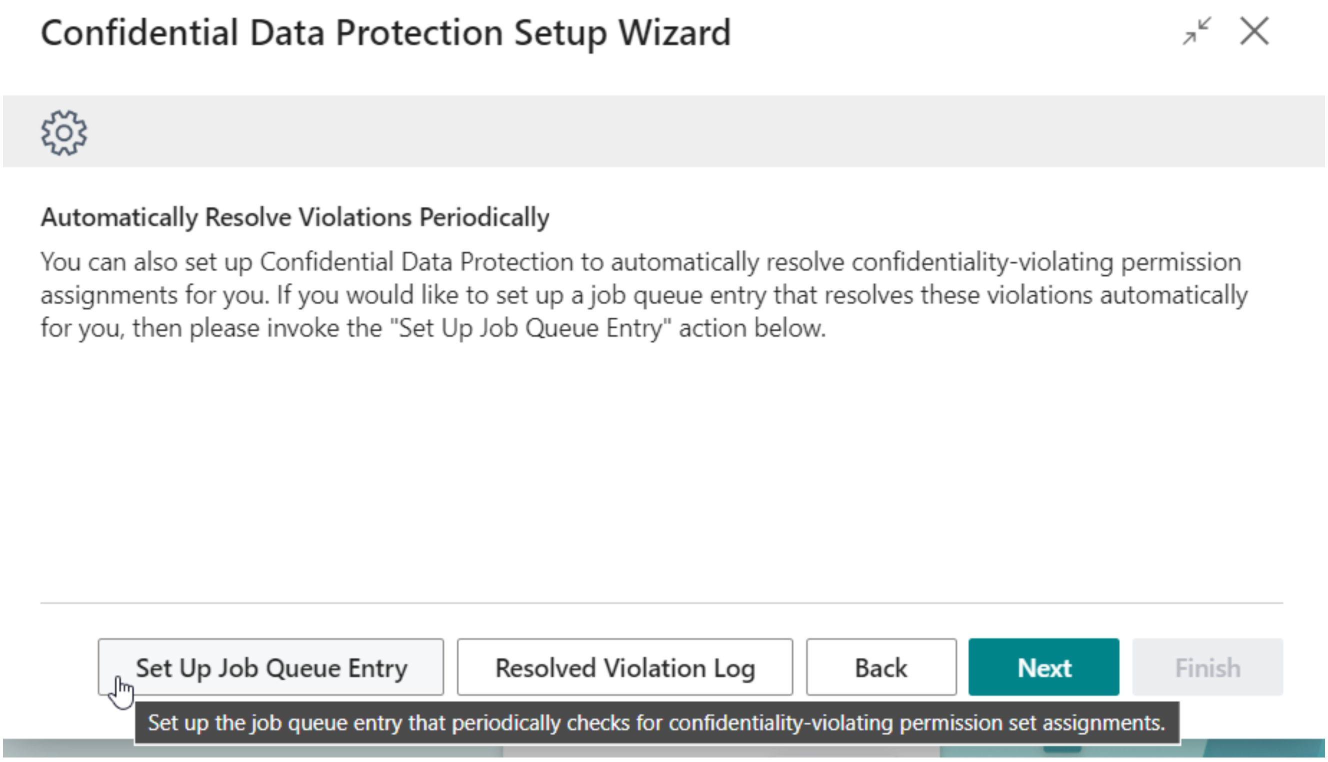


	Permission Set ↑		Description
	D365 BUS PREMIUM`		Dyn. 365 Prem. Bus. Full Acc.
→	INDIRECT_T0000000017	⋮	Indirect Read T17
	INDIRECT_T0000000096		Indirect Read T96
	LOGIN		Login access

- When a permission set that exposes confidential data is assigned to a user that has **SUPER** or **SUPER (DATA)** access (for the same company(!)), then this assignment is no longer restricted as the user will not get *more* access to confidential data (as the user already has full data access for the entire company or environment).
- Add missing tooltip for **Extension-provided** field
- Applied bold styling to **Exposes Confidential Data** field values on the **User Subform** page for records with value **Yes**.
- Fix clearing confidential marker

1.6.0.0 2024-01-11

- A new **Automatically Resolve Violations Periodically** step has been added to the **Confidential Data Protection Setup Wizard** page.



Confidential Data Protection Setup Wizard

Automatically Resolve Violations Periodically

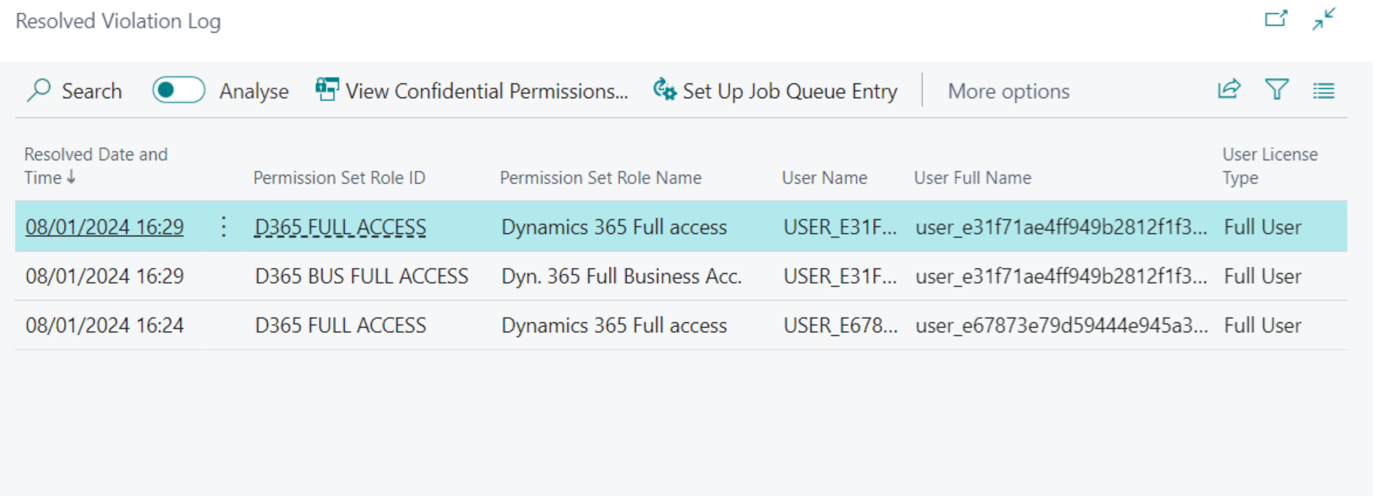
You can also set up Confidential Data Protection to automatically resolve confidentiality-violating permission assignments for you. If you would like to set up a job queue entry that resolves these violations automatically for you, then please invoke the "Set Up Job Queue Entry" action below.

Set Up Job Queue Entry
Resolved Violation Log
Back
Next
Finish
Set up the job queue entry that periodically checks for confidentiality-violating permission set assignments.

In this step the user is informed about the possibility to set up a job queue entry to periodically resolve confidentiality-violating permission set assignments. The action **Set Up Job Queue Entry** will set up a job queue entry which can be edited to the user's preference. The **default** is set to resolve violations in the background every **180 minutes**.

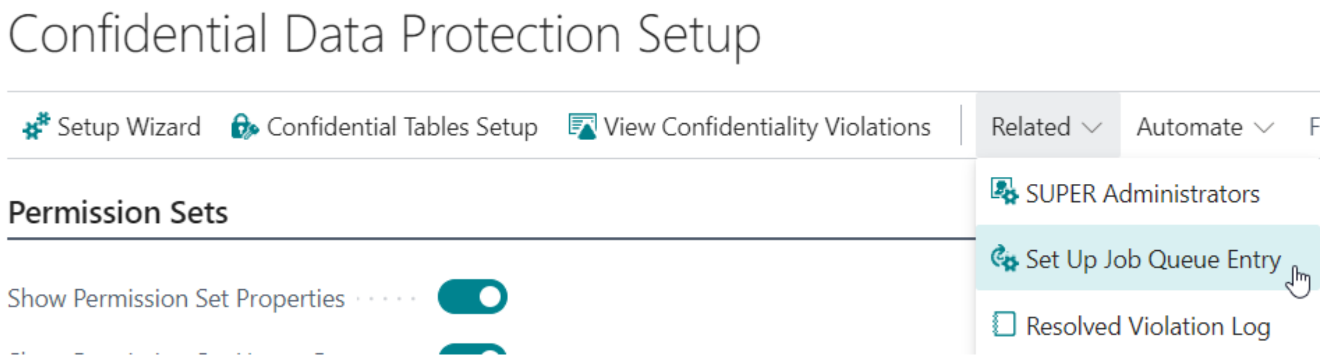
If the user tries to continue the wizard without setting up a job queue entry by clicking on the **Next** button, a dialog is shown to let the user choose to set up the job queue entry (recommended) or continue without setting up a job queue entry.

- The **Confidential Data Protection** extension now keeps a log of confidentiality-violating permission set assignments that were resolved. You can view the log entries by using the **Resolved Violation Log** action on the **Confidential Data Protection Setup (Wizard)** page.



Resolved Date and Time ↓	Permission Set Role ID	Permission Set Role Name	User Name	User Full Name	User License Type
08/01/2024 16:29	D365 FULL ACCESS	Dynamics 365 Full access	USER_E31F...	user_e31f71ae4ff949b2812f1f3...	Full User
08/01/2024 16:29	D365 BUS FULL ACCESS	Dyn. 365 Full Business Acc.	USER_E31F...	user_e31f71ae4ff949b2812f1f3...	Full User
08/01/2024 16:24	D365 FULL ACCESS	Dynamics 365 Full access	USER_E678...	user_e67873e79d59444e945a3...	Full User

- New actions have been added to the **Confidential Data Protection Setup** card page


Confidential Data Protection Setup
Setup Wizard
Confidential Tables Setup
View Confidentiality Violations
Related
Automate
F
Permission Sets
Show Permission Set Properties
SUPER Administrators
Set Up Job Queue Entry
Resolved Violation Log

  - **Set Up Job Queue Entry** - Set up the job queue entry that periodically checks for confidentiality-violating permission set assignments.
  - **Resolved Violation Log** - View the log of the confidentiality-violating permission assignments resolved by the Confidential Data Protection extension.

1.4.0.0 2023-12-01

- Handle warning about obsoleted/to-be-removed permission set `WSB_MON` (User permission set for the *Monet* library app).
- Ensure that procedure `wgFncGetConfidentialTableObjectIDs` does not tamper with the state/flag of an in-progress creation of the *Confidential Data Exclusion* permission set.

1.2.0.0 2023-11-10

- Added **Exposes Confidential Data** page field to the **User Subform** page that shows the permission sets of a user on the **User** card page. This field shows whether the permission set that the user has access to exposes confidential table data to the user.

- Directly resolve confidentiality violations introduced after applying updates to license configurations of users to the **Update Users from Microsoft 365** action instead of preventing them with an error.
- Update error message that is displayed to a user when the system attempts to assign permission sets that expose confidential data to the user on first login due to confidentiality-violating license configurations.
- Account for G/L entry no. increment during sales doc. post. In the situation that the latest G/L entry at the time relates to a confidential G/L account, then the security filters prevented determining the next entry no. when users that do not have access to the confidential G/L account data would post sales documents which generate G/L entries.

1.0.0.0 2023-10-02

Initial version

Last update: January 29, 2024