2-Controlware Inc.
228 E45th St, #9E
NY 10017
United States of America

+1(332) 253 6739
www.2-controlware.com
sales@2-controlware.com

Authorizations in Business Central

How to approach designing, managing, and monitoring authorizations?

Whitepaper

2-Controlware Inc.

Table of Contents

1 Introduction: Who Are We?

2-Controlware is the specialist in authorization management for Microsoft Dynamics 365 Business Central. We develop user-friendly software solutions that help organizations to stay in control of permissions, internal controls, and information security.

Our roots lie with the IT audit firm 2-Control, with whom we continue to work closely. While 2-Control focuses on independent IT audits and advisory services, our focus is entirely on developing, delivering, and supporting authorization software. Operating from the same office, we work as one close-knit team, each with our own specialization. Our software and services are the result of more than twenty years of experience in IT auditing, Microsoft Dynamics 365, and hands-on expertise in developing authorization solutions.

With a personal approach, we help organizations stay continuously ‘in control.’

2 The Theory Behind Permissions

Assigning the right permissions to users in Business Central is a challenging and complex process. Doing this correctly requires a deep understanding of both Business Central and the organizational roles and responsibilities. In addition, the functionality for assigning permissions to users in standard Business Central is quite complex. Manual processes are inefficient and error-prone, and the absence of a structured approach hinders progress.

This whitepaper will take a closer look at how to set up permissions in Business Central efficiently, how to safeguard the quality, and how 2-Controlware supports organizations in overcoming these challenges.

2.1 What are Permissions?

Permissions, also known as authorizations or access rights, determine which users or groups of users have access to functionality and data within a system. In the case of Business Central, permissions are essential to define who can view or edit business information. This helps protect company data and ensures that users only have access to the information relevant to their organizational role.

2.2 The Importance of Setting Up Permissions

Permissions are set up to ensure that the actions users can perform in Business Central align with their organizational tasks and responsibilities. This means that rights to perform functions and access data should be granted, while rights to other functions and data should be restricted. Examples include restricting configuration settings (object), adding an extra approval step for payments (system), controlling whether or not employees can record hours (setting), or limiting users to only work with specific document types such as purchase orders (extension).

In short, a carefully designed permissions setup not only protects your data, but also supports the reliability and manageability of business processes.

2.3 Permissions in Business Central

Permissions are essential for defining who can view or manage which objects in Business Central. A well-structured permissions setup ensures that users only have access to the functionality and data relevant to their role within the organization. This is crucial for protecting sensitive information, keeping processes manageable, and preventing errors or unauthorized actions.
The authorization model in Business Central consists of four interconnected components:

- **Licenses (entitlements):** Define, at a high level, which modules and functionality a user can access.
- **Permission sets (object-level permissions):** Control access to specific objects, such as tables, pages, or reports, and define which actions (read, modify, delete, execute) are allowed.
- **User-specific application controls:** Additional settings, often configured per user, that influence specific actions in processes (such as posting periods or approval limits).
- **Profiles (roles):** The visual configuration of the user interface, designed to provide users with quick access to the relevant menus and functions. While these are not a hard security measure, they improve clarity and user-friendliness.

In the following sections, we will take a closer look at each of these components: how they work, how they are managed, and what possibilities they offer within Business Central.

2.3.1 *Licenses (Entitlements)*

Licenses (referred to by Microsoft as entitlements) form the first layer of permissions. They define which functionality and modules a user can access. If a user has a limited license, their access is restricted to the functionality available under that license.

The licensing structure of Business Central is designed to be flexible, allowing companies to choose the appropriate level of access and functionality that best fits their needs. Below are the main license types in Business Central:

1. **Essentials License:** Provides access to the core functionality of Business Central, supporting most standard business processes.
2. **Premium License:** Includes all features of the Essentials License, plus advanced functionality for organizations with more complex requirements.
3. **Team Members License:** Intended for users who require only basic functionality, primarily for viewing data and performing simple tasks.
4. **Device License:** Designed for shared devices rather than individual users.
5. **Microsoft 365 License:** Also referred to as the “read-only” license, offering users viewing rights only.

The way licenses work differs between SaaS environments (cloud) and on-premises environments. In SaaS environments, Microsoft determines (based on your license / entitlement) which functionality you are allowed to use. When new objects are added through an extension, they are automatically included in your license. However, you are only permitted to use those functions explicitly allowed within your license. Objects outside your entitlement may still be visible, but you can only access them indirectly (for example, through an approved action), not by opening or editing them directly.

In an on-premises environment, the logic works the other way around. By default, you do not have access to any objects unless they are explicitly included in your license. When new objects are added through the installation of an extension, your license must be manually updated to make these accessible.

In short: in a SaaS (cloud) environment, you automatically gain access to new objects but are functionally restricted by your license (entitlement). In on-premises environments, you only gain access if it has been explicitly granted in your license beforehand.

2.3.2 *Permission Sets*

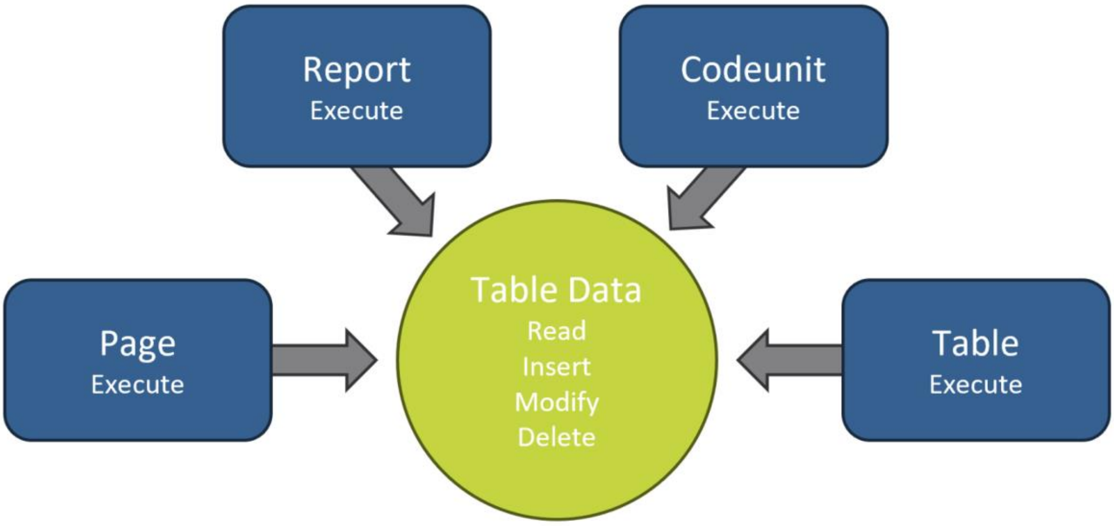
While licenses determine which objects in Business Central are technically accessible, this scope is far too broad in practice. Not every user needs access to all objects within a license. To align permissions more closely with user’s role and responsibilities, permission sets are used. These allow you to restrict the objects within a license to only those components that are relevant to a specific user or group of users. In Chapter 2, we will explore in more detail how to configure these permission sets.

Permission sets are therefore the mechanism by which users are granted access rights. Each user gains access to objects through one or more of these sets. Business Central distinguishes three types of permission sets:

1. **System sets**: delivered by default and not customizable.
2. **Extension sets** : provided through apps or extensions and also not customizable.
3. **Custom sets**: created and managed by the application administrator of the organization, offering flexibility to tailor permissions to organizational needs.

The technical structure of Business Central is composed of different object types such as tables, pages, reports, and codeunits. Within a permission set, the specific actions a user is allowed to perform on each object type are defined. For table data, this includes read, insert, modify, and delete, while for other object types the focus is typically on execution rights.
An important distinction within these actions lies in direct versus indirect permissions:

1. **Direct** permission means the user can perform the action independently of a list or card.
2. **Indirect** permission means the user only gains access to an object as part of another permitted action. A typical example: a user may not insert general ledger entries directly but can do so indirectly when posting an invoice. Since posting an invoice automatically creates ledger entries, indirect permission is sufficient in this scenario.



A specific challenge arises when a single table contains multiple types of data. An example of this can be found in the Sales Header (36) and Sales Line (37) tables, where different types of sales documents are stored, such as quotes, orders, invoices, and creditnotas. When a user is granted permissions on these tables, they automatically gain access to all document types within them. To limit this, you can assign permissions at the page level through permission sets, for example, granting access only to the sales invoice page.

However, this approach has its limitations: it becomes difficult to allow users read-only rights without edit rights, or to completely restrict access to certain document types. For this reason, 2-Controlware's **Compliance Field Security app** provides valuable enhancement. This app enables the use of filters within permission sets, such as filtering by document type. With this, you can define in detail which types of sales documents a user may view or edit, even within a single table. *Visite our website for more information about the Compliance Field Security app.*

2.3.3 *Automated Controls*

The third component of user permissions within Business Central consists of user-specific configurable controls. Examples include:

- Permitted posting periods based on user settings.
- Allowed warehouse employees.
- Approval limits defined through user settings.
- User assignments within workflows.

In addition to the standard settings in Business Central, organizations often implement additional user-specific application controls via extensions (apps). Examples include apps that introduce supplementary workflow configurations or approval rules that need to be set up per user. These configurations also fall under manual administration, which can be time-consuming for functional administrators.

In standard Business Central, these settings must be configured manually for each user and for each company. This is labor-intensive, especially during employee onboarding, role changes, and offboarding. As a result, functional administrators spend a significant amount of time setting up and maintaining these configurations.

To simplify this process, 2-Controlware has developed the **User Templates** **module** within the **Authorization Box**. With this module, settings that would otherwise need to be entered manually per user in Business Central can be automated by linking the logic to the user's role or function. In addition, user settings, employee data, and access to apps and portals can also be tied to roles. In this way, everything stored in a Business Central table can be configured through an authorization request.

2.3.4 *Profiles (roles)*

In Business Central, a user can select a profile through their personal settings. This profile determines what the user sees in Business Central and is often referred to as soft security. A profile controls the visibility of menus and features but does not impose any hard restrictions on permissions. For example, a user can still:

- Open a hidden page by typing its name into the search function.
- Access a page directly by using its URL.
- Reveal hidden fields and actions through personalization or design (for example, in a pre-production environment).

Although profiles in the Role Center do not actually revoke a user's underlying permissions, they do serve as a useful first line of defense in preventing unauthorized actions.

In standard Business Central, each user can be assigned a profile via the User Configuration screen. Within 2-Controlware's **Authorization Box**, this process can be automated by linking profiles to organizational roles, or by assigning a profile to a user through an authorization request in the Authorization Box. *Visit our website to learn more about the Authorization Box.*

3 From Theory to Practice: How to Set Up Permissions

Carefully structuring permissions in Business Central is essential to ensure that users only have access to the functions and data relevant to their role. This not only reduces security risks but also helps prevent errors and inefficiencies. In this chapter, we describe the step-by-step process for designing, testing, and implementing a reliable permissions framework. We explain how to start with defining a permissions framework, how to build and clean up permission sets, how to test them, and how to go live with the new structure. Finally, we outline best practices for organizing ongoing permissions management.

3.1 Step 1: Define the Permissions Framework

The first step is to define a clear permissions framework, closely aligned with the organizational functions of Business Central users. This prevents uncertainty when new employees join the organization about which permissions they should be granted.

First, we create an organizational chart that includes all departments working with Business Central. Under each department, the relevant job functions are listed, and for each function we determine which users require access to Business Central and what actions they need to perform within it. This assessment is often carried out in consultation with a key user per role, who explains which tasks are performed in Business Central. Based on this input, a clear matrix is created that maps tasks to roles, which gets submitted to the project stakeholders responsible for authorization for approval.

3.2 Step 2: Record the Tasks of each Role

In follow-up sessions, the tasks from the permissions matrix are further detailed. Each task is recorded to a permission set, creating a modular setup. By “recording,” we mean capturing all objects (such as tables and pages) that a user needs to perform a task. This recording process can be carried out with the standard functionality of Business Central: recording permissions. By clicking through the relevant functions in Business Central, you generate a permission set. All objects that are touched during this session are automatically added to the set, including reading, writing, and executing permissions.

3.3 Step 3: Clean Up the Permission Sets

After recording, the task-related permission set (“task set”) is not yet ready for use. To keep the set clear and manageable, it must be cleaned up so that only the relevant permissions for the specific task remain. All other “general” rights should be granted through base sets, such as:

- One base set for general read permissions.
- One base set for basic modification permissions.

The cleanup can be performed manually or by using the exclude permission sets function. The more recent versions of Business Central also support dynamic exclusion, where changes in a base set are automatically reflected in the task sets. The standard recorder in Business Central helps capture this information, but it has limitations: it only allows you to record your own user session and does not provide automatic cleanup. That is why we developed the Advanced Permissions Recorder, available via AppSource. With this recorder, you can capture sessions from other users, predefine which actions (read, insert, modify, delete, and/or execute) on which object types should be recorded, and apply automatic cleanup to the resulting set.

Want to learn more about the Advanced Permissions Recorder? Visit our website for detailed information.

3.4 Step 4: Test the Permission Sets

Once all tasks have been recorded and the permission sets cleaned up, it is time to test. We recommend starting with an **(1) internal quality check**. In this phase, the authorization administrator assigns the permission sets individually to themselves and executes all tasks one by one using representative data. This verifies whether each set works correctly on its own. Next, we advise involving key users in **(2) detailed testing**. They are reassigned the tasks identified earlier, but now as separate permission sets, and they check whether each task can be performed independently of the other sets. When all permission sets have been tested and resulting errors have been resolved, the process moves on to **(3) acceptance testing**. In this phase, all permission sets linked to a role are assigned together to a key user, who validates them as a group. After acceptance testing, all outstanding issues should be resolved, allowing the tested permission sets to be transferred to the production environment.

3.5 Step 5: Go-live

Once testing is complete, it is time to go live. Permission sets are exported from the test environment, which can be done in two ways:

- Via the permission set page: export as an .xml file.
- Via configuration packages: export tables 2000000165 (Permission Set) and 2000000166 (Permission Set Object).[1]

Depending on the organization, the go-live can follow a phased approach (per department or user group) or a Big Bang (all users at once). In both cases, the new permission sets are imported and replace the old assignments at the user level.

The way sets are assigned to users depends on the chosen structure. If only standalone permission sets are used, each user must be manually assigned the relevant sets via their user card in Business Central. As of Business Central 2025, however, these have been replaced by security groups created in Azure/Entra, to which permission sets can then be linked in Business Central.
For organizations seeking a structured and automated process,

2-Controlware's **Authorization Box** offers an integrated solution. By creating a digital organizational chart with departments and roles, organizations gain a clear overview of who has (or should have) what permissions. A major advantage of this approach is the added security provided by approval workflows for authorization requests. This ensures that at least two people (four-eyes principle) review the assignment of critical permissions. These approval workflows can also be applied to changes in the authorization structure itself, such as adding a permission set to a role.

3.6 Step 6: Maintain the Permission Sets

After implementation, it is crucial to properly organize the ongoing management of permissions. The person responsible for assigning permission sets must understand how the setup works and how to troubleshoot potential issues.

For example: a user can no longer post invoices. The first step is to check whether this right is allowed according to the design matrix. If yes, the issue is likely caused by a missing permission set or an incorrect assignment. If no, the matter should be discussed with the user's manager to decide whether the right should be granted after all.

[1] *These tables are not visible in the standard list but can be entered manually. Tables 2000000004 and 2000000005 contain system permission sets and can only be exported, not imported*.

4 Monitoring and Reviewing Permissions

A successful implementation of permissions is only the beginning of effective authorization management. Once permissions are in production, the process of maintaining and monitoring begins. This is essential both for business continuity and for compliance purposes. Effective monitoring of permissions consists of three complementary approaches.

4.1 Proactive Monitoring

After go-live, it is important to proactively monitor permissions in Business Central. Using the standard functionality, this is challenging but not impossible, provided you know which objects are critical and which combinations may create potential conflicts.

The simplest, but also most labor-intensive, method is to review each user’s effective permissions. This feature, available at the top of the user card, summarizes all object-level permissions from permission sets and groups assigned to the user.

An alternative approach is to use Excel to combine different exports. For this, you need tables such as Access Control (2000000053), AllObjWithCaption (2000000058), Tenant Permission (2000000165), and Tenant Permission Set (2000000166). By linking objects in permission sets to users, you can assess whether critical objects are assigned and whether potential conflicts exist. Note, however, that not all tables can be exported using configuration packages since some are system tables. A workaround is to modify the URL in Business Central to display the table directly: replace everything after page=xxxx with table=xxxx.

For a significant simplification of this process, 2-Controlware’s **Continuous Monitoring module** within the **Authorization Box** offers an integrated solution. This module retrieves all relevant authorization data via a web service and presents it in clear dashboards. This allows administrators to quickly gain insight into who has which permissions, at the user, permission set, and organizational role levels.

An additional benefit of this module is the review system, which enables permissions to be evaluated and approvals to be documented for compliance and reporting purposes. The system tracks when permissions have changed since the last review, ensuring administrators immediately see where renewed checks are required. This not only improves security but also strengthens audit readiness and compliance documentation.

4.2 Reactive Monitoring

In addition to checking access rights (“who has which permissions?”), it is also valuable to monitor actual activity (“who did what?”).

In Business Central, you can enable change log entries on critical tables and review them periodically to identify unauthorized modifications. A limitation of this approach is that intervention is only possible after a change has already taken place, meaning corrective action rather than prevention.

For a reliable change log, it is crucial that not everyone has the ability to change the log settings and thereby (temporarily) disable the logging of tables. When reviewing the change log, administrators should also verify who has modification rights on the Change Log Setup (402). While individual records in the log cannot easily be deleted, in theory the entire log could be cleared if someone acted maliciously.

Logging changes always involve a trade-off between security and performance. For every logged table, Business Central needs to write the data twice: once to the table itself and once to the log. If too many tables are logged, the system performance can be significantly impacted. Our recommendation is to always enable logging for configuration settings, master data, and only the process data that you want to use for insights.

4.3 Periodic Evaluation

Once permissions are configured and in use, periodic evaluation is essential. Over time, for example, when an audit is approaching, you will want to confirm that the configuration is still correct and aligned with organizational needs.

A more detailed explanation of these evaluation processes will be provided in Chapter 4.

5 How to Keep Permissions Up to Date?

The effectiveness of authorization management depends heavily on broader organizational processes. Without clear procedures for requesting, modifying, and revoking permissions, even the most technically sound authorization setup will fall short in practice. The following processes form the backbone of sustainable authorization management and ensure that the carefully designed permission structure continues to function as intended.

5.1 Employee Lifecycle: Onboarding, Role Changes, and Offboarding

Throughout the entire lifecycle of an employee, from onboarding, to internal transfers, to eventual offboarding, authorization processes are a critical part of personnel management and organizational policy.

- **Onboarding:** When an employee joins, permissions must be carefully assigned based on their specific role. This ensures that only the relevant modules and data are accessible, allowing the user to work efficiently without unnecessary exposure to sensitive information.
- **Role Changes:** When responsibilities shift, access rights must be reassessed and adjusted accordingly. This involves granting new rights where required and revoking outdated rights to prevent unauthorized access to data no longer relevant to the role.
- **Offboarding:** When an employee leaves the organization, all access rights must be revoked and the account deactivated to safeguard system security. This includes removing linked permission sets and performing a security check to ensure no unauthorized access points remain. Additionally, data managed by the employee may be archived and documented for audit and compliance purposes.

Manually processing these personnel changes in permissions is often error-prone. 2-Controlware's **Authorization Box** simplifies these processes by grouping permission sets under organizational roles, rather than assigning them individually to each user. Based on authorization requests for onboarding, role changes, and/or offboarding, with optional approval workflows, permissions in Business Central are automatically adjusted and logged at the right time. The **Authorization Box** not only saves time but also enforces traceability.

5.2 Incident Management

Incident management related to permissions is an important part of the broader IT service processes within an organization. When users experience issues with their access rights, a fast and efficient resolution is essential, not only from a technical perspective but also operationally, to avoid disruption of business activities.

The process starts with the reporting and classification of the incident by the user. The IT team then analyzes the issue by reviewing log files and user profiles to identify the root cause. Based on this analysis, permissions may be adjusted, for example, by updating rights, modifying roles, or granting temporary access.

After the incident has been resolved, the user is informed about the corrective measures taken, and all changes are documented to ensure compliance with audit and regulatory requirements.

5.3 Change Management

When changes occur in Business Central, such as software updates or the introduction of new functionality, it is important to take the existing permission structure into account. This ensures that users consistently retain the correct level of access without compromising security.

The change process begins with an impact analysis to determine which users and functions will be affected. Based on this analysis, a change plan is drawn up and test scenarios are developed to assess the impact on permissions.

The changes are first implemented in a controlled test environment and subjected to security checks. After implementation, user feedback is collected to quickly resolve any issues. All changes are thoroughly documented to meet compliance requirements and serve as a reference for future adjustments.

6 Best Practices for Effective Authorization Management

After understanding the theoretical foundation of permissions, the practical setup, the evaluation of the implementation, and the establishment of management processes, we arrive at our best practices. In this chapter, we share the expertise we have gained through more than twenty years of experience with authorization management across hundreds of Business Central environments.

6.1 Modular Design for Detailed Permissions

An effective authorization structure is built on a modular approach. This means that a separate permission set is created for each specific task. These permission sets are deliberately kept small, ensuring that users have exactly the rights they need to perform their tasks, no more and no less. In this approach, two types of rights are kept outside the task-specific permission sets:

1. Read rights, which are defined separately.
2. Basic rights, which form a general baseline.

Read rights are typically divided into two categories:

1. General read rights (pages and reports accessible to all users).
2. Financial read rights (pages and reports specifically for finance and management).

A general baseline set contains rights that everyone needs, such as login rights and access to object types that are not part of task-specific permission sets. As a result, a task-specific permission set will only contain table data objects with the options insert, modify, or delete.

Because the modular approach may result in a large number of permission sets, a clear naming convention is strongly recommended. One suggested structure is: [company abbreviation]-[department abbreviation]-[task]

For example: 2C-PUR-ORDER for the permission set that allows users to create purchase orders. To further organize permission sets, they can be grouped into security groups. These groups are created in Azure AD/Entra, where users are also assigned. It is advisable to align these security groups as closely as possible with the HR organizational chart to reduce the risk of incorrectly assigned permission sets for new users.

6.2 Segregation of Duties

For optimal segregation of duties, certain splits within permission sets are consistently maintained. For operational tasks, there is always a distinction between creating, receiving, and posting documents. *For example, creating a purchase order, posting a purchase receipt, and posting a purchase invoice are each set up as separate permission sets.*

In addition, there are several configuration tables for which we create specific permission sets per department. *For instance, there may be a permission set for financial settings, one for project settings, and one for production settings.* The management of master data is also separated into its own permission sets, such as managing items, customers, vendors, and vendor bank accounts.

6.3 Include vs. Exclude

The method described above is what we call an “include approach,” where specific permissions are explicitly defined for what a user is allowed to do. This approach offers the highest degree of certainty that users only have access to exactly what they need.

An alternative approach is the “exclude approach,” in which a broad range of permissions is initially granted, and only the rights that a user should not have are restricted. The advantage of this method is that it requires less effort to set up. By focusing only on identifying the core tables needed for performing a task, you reduce the biggest risks of improper access while still limiting users’ exposure to unnecessary functionality.

7 Conclusion and Next Steps

Effectively managing permissions in Microsoft Dynamics 365 Business Central is a complex but vital task for every organization. As outlined in this whitepaper, a structured approach is the foundation for safeguarding data security and compliance. From carefully setting up licenses, permission sets, user-specific controls, and profiles, to implementing robust management processes for employee onboarding, internal transfers, offboarding, incident handling, and change management, each step contributes to a sustainable authorization structure.

The application of best practices, such as a modular design of permission sets and the implementation of strict segregation of duties, is essential to managing complexity and minimizing risks. While the standard functionality of Business Central provides a foundation, practical experience shows that manual processes are both time-consuming and error-prone.

At 2-Controlware, we understand the challenges involved in managing permissions in Business Central. With more than twenty years of experience in IT auditing and the development of specialized software solutions, we are the partner that helps you stay in control.

The **Authorization Box** from 2-Controlware is your integrated solution for:

- **Simplified process management:** Automate the assignment and adjustment of permissions during onboarding, role changes, and offboarding, including approval workflows, to save time and enforce traceability.
- **Proactive control and monitoring:** Gain instant insight into who has which permissions at the user, permission set, and organizational role levels through clear dashboards. Evaluate authorizations, document reviews for compliance, and immediately identify where renewed checks are required.
- Advanced configuration: Use the power of modular permission sets and implement detailed access controls, even at field level, with our **Compliance Field Security app.**
- Data integrity assurance: Ensure the accuracy of your data with our **Compliance Field Validation app**, enforcing mandatory fields and specific formats.

Take the next step toward effortless control and data security in Business Central. Visit our website to learn more about the **Authorization Box**, the **Advanced Permissions Recorder**, and our Compliance apps, or contact us directly for a personalized demonstration and discover how 2-Controlware can help your organization maintain lasting control over permissions.

Extra information

Discover 2-Controlware. Below you will find more detailed information about our products, quick scans for your organization, links to our social media channels, and much more. Each of these resources is designed to help you optimize your IT environment and improve your business. Explore the links below to discover what 2-Controlware can do for you.

- ✓ **Wiki page**
  More information about our apps.

- ✓ **Wiki page for the Authorization Box**
  More information about our Authorization Box.

- ✓ **"Is your Dynamics application fraud proof?" - Checklist**
  Gain insight into which areas of your Dynamics environment are already safeguarded against fraud and which ones may still require additional attention.

- ✓ **Blogs**
  Stay up to date with our latest discoveries and insights. By sharing our expertise, we aim to give you a deeper understanding of permissions.

- ✓ **AppSource**
  Download our apps via Microsoft AppSource.

- ✓ **LinkedIn**
  Follow us on LinkedIn for more updates about our products and knowledge shares.

- ✓ **YouTube**
  Follow us on YouTube and check out our explanation videos on our apps and Authorization Box.

2CONTROLWARE

Software Solutions for Microsoft Dynamics

Europe
2-Controlware B.V.
Haagsemarkt 1, 4813 BA
Breda, The Netherlands
sales@2-controlware.com

USA
2-Controlware Inc.
228 E45th St, #9E
NY 10017
United States of America
sales@2-controlware.com

Contact
Europe: +31(0)765019470
USA: +1(332) 253 6739
sales@2-controlware.com
www.2-controlware.com