



Your people. Our priority®

Managing Payroll NOW Access in Business Central

Controlling Access to Payroll NOW Screens

Microsoft Dynamics 365 Business Central

Table of Contents

Overview	3
Microsoft Documentation References	3
Built-In Payroll Permission Sets	3
Creating a Permission Set	4
Payroll View Only Configuration	4
Payroll Full Processing Configuration	5
Assigning Permission Sets to Users	6
Payroll Users Setup	6
Licensing Considerations	8

Overview

Permission Sets in Microsoft Dynamics 365 Business Central control what users can see and do within the system. This article explains how to configure payroll-specific security roles to control access to Payroll NOW screens while maintaining data integrity.

Permission Sets allow administrators to define granular access at the object level—specifying whether a user can read, insert, modify, delete, or execute specific tables, pages, and reports. By creating custom Permission Sets tailored to payroll roles, you can ensure that users only have access to the functionality they need.

Microsoft Documentation References

For additional background on Permission Sets in Business Central, refer to the following Microsoft documentation:

- **Define Granular Permissions**

<https://learn.microsoft.com/dynamics365/business-central/ui-define-granular-permissions>

- **Special Permission Sets (SUPER, SECURITY)**

<https://learn.microsoft.com/dynamics365/business-central/dev-itpro/administration/administration-special-permission-sets>

- **Entitlements Overview**

<https://learn.microsoft.com/dynamics365/business-central/dev-itpro/developer/devenv-entitlements-and-permissionsets-overview>

Built-In Payroll Permission Sets

Before creating custom Permission Sets, be aware that Payroll NOW ships with two built-in permission sets that cover common access scenarios:

Permission Set	Description
IDPN PAYROLL NOW	The standard Payroll NOW permission set. Grants the permissions needed to access and operate Payroll NOW pages, tables, and reports. Assign this to any user who needs to work within Payroll NOW.

USPY PRIMO PAYDAY

The Primo Payday permission set. Provides permissions for Primo Payday functionality within Business Central. Assign this to users who require access to Primo Payday features.

These built-in sets provide a starting point. You can assign them directly to users, or use them as a reference when creating custom Permission Sets with more granular control.

Creating a Permission Set

To create a new Permission Set for payroll access:

- Search for “Permission Sets” in the BC search bar.
- Click **+ New** to create a new Permission Set.
- Enter a descriptive code (e.g., **PAYROLL-VIEW** for view-only access or **PAYROLL-FULL** for full processing access).
- Click **Permissions** to open the permission lines and configure object-level access.

Note: Permission Sets created here are user-defined and will not be overwritten by system updates. Microsoft distinguishes between system-defined and user-defined Permission Sets. For payroll security, always create user-defined sets so they persist through upgrades.

Payroll View Only Configuration

A View Only Permission Set allows users to see payroll data without making changes. This is appropriate for managers, auditors, or HR staff who need visibility but should not modify payroll records.

Permission Line Settings

Permission	Setting	Description
Read	Yes	Allows the user to view records in employee and payroll setup tables.
Insert	Blank	User cannot create new records.
Modify	Blank	User cannot change existing records.

Delete	Blank	User cannot remove records.
Execute	Yes	Allows the user to open and navigate payroll pages and run reports.

Objects to Include

Add the following object types to the Permission Set with Read and Execute access:

- Payroll Employee tables
- Payroll Setup tables
- Payroll Company tables
- Payroll pages (Employee Card, Payroll Setup, Reports, etc.)
- Related dimension and ledger tables (Read only)

Payroll Full Processing Configuration

A Full Processing Permission Set grants the access needed to run payroll end-to-end. This includes everything in the View Only set, plus the ability to create, modify, and process payroll transactions.

Permission Line Settings

Permission	Setting	Description
Read	Yes	View all payroll data including employee records, setup, and history.
Insert	Yes	Create new payroll documents, hours entries, and employee records.
Modify	Yes	Edit existing payroll records, employee information, and setup.
Delete	Yes	Remove payroll records where applicable (e.g., unposted documents).
Execute	Yes	Open pages, run payroll processing, and generate reports.

Ledger Table Access

For ledger tables (e.g., G/L Entry, Payroll Ledger Entry), set Insert to **Indirect** rather than Yes. Indirect access means the user cannot manually insert records into the ledger, but the system can insert records

on the user's behalf during payroll posting. This protects ledger integrity while allowing normal payroll processing.

Important: Setting ledger tables to Insert = Indirect is a best practice. Direct insert access to ledger tables bypasses normal posting routines and could result in unbalanced entries. Only grant Direct insert on ledger tables if specifically required.

Assigning Permission Sets to Users

Once Permission Sets have been created, they must be assigned to individual users:

- Search for "Users" in the BC search bar.
- Open the user card for the user you want to configure.
- Scroll down to the **User Permission Sets** section.
- Add the appropriate payroll Permission Set (e.g., PAYROLL-VIEW or PAYROLL-FULL).
- If restricted access is required, **remove the SUPER permission set** from the user. SUPER overrides all other Permission Sets and grants unrestricted access to everything in BC.

Best Practices for Payroll Security:

- Always test Permission Sets with a non-admin user account before rolling out to production.
- Document which Permission Sets are assigned to each role in your organization.
- Review Permission Set assignments periodically, especially after staff changes.
- Use the "Effective Permissions" page in BC to verify what a specific user can access.
- Keep SUPER limited to system administrators only.

Payroll Users Setup

In addition to BC Permission Sets, Payroll NOW has its own user-level security settings on the **Payroll Users Setup** page. These settings work alongside Permission Sets to provide fine-grained control over what each user can do within payroll.

Payroll Setup >> Payroll Users Setup

Payroll Setup

Payroll Users Setup New Line Delete Line

User ID ↑	Payroll Reversal Allowed	Employ... Personal Info Visible	Payroll Journal Batch Name	Payroll Journal Document Nos.	Manual Hours Batch Name	Manual Piece Rate Batch Name	PTO Journal Batch Name	PTO Journal Document Nos.	Hours Approval Admini...	Receiver of Auto-run Reports	Enter Hours Detail Allowed	Enter Piece Rate Entries Allowed	Employ... Change Admini...	Allow User to See G/L Records Genera... from Payroll
→ BCDEMOUSER	☒	☒	DEFAULT	PAYROLL-JN			DEFAULT	PAYROLL-PT	☒	☒	☒	☒	☒	☐
DEMOBC	☒	☒	DEFAULT	PAYROLL-JN			DEFAULT	PAYROLL-PT	☒	☒	☒	☒	☒	☐

Key settings on this page include:

- **Employee Personal Info Visible** — When unchecked, sensitive information such as Social Security Numbers will be masked. Even if a user has read access through their Permission Set, this setting controls whether they can see the actual data.
- **Payroll Reversal Allowed** — Controls whether the user can reverse posted payroll documents.
- **Hours Approval Admin** — Determines if the user can approve hours entries.
- **Hours Detail Allowed** — Controls access to the Hours Detail entry screen.
- **Employee Change Admin** — Determines if the user can make changes to employee records.
- **Enter Piece Rate Entries Allowed** — Controls access to piece rate entry.
- **Receiver of Auto-run Reports** — Designates the user as a recipient of automated report output.
- **Allow User to See G/L Records Generated from Payroll** — Controls visibility of GL entries created by payroll posting.

Important: Permission Sets and Payroll Users Setup work together. A user may have read access to a payroll page through their Permission Set, but the Payroll Users Setup controls what data is visible or what actions are allowed on that page. Always configure both to achieve the desired level of access.

Licensing Considerations

The user's Business Central license type also determines what they can access, independent of Permission Sets. Key points to be aware of:

- **SUPER permission set** — Only a full (Premium or Essentials) license with administrator rights will honor SUPER. Users on limited or team member licenses cannot be granted full SUPER access regardless of their Permission Set assignments.
- **Team Member licenses** — Have inherent restrictions on what objects they can access. Even if a Permission Set grants access to a page, the license entitlement must also allow it. Team Member licenses are typically limited to read access on most tables.
- **Entitlements** — Business Central enforces entitlements at the license level before evaluating Permission Sets. If a user's license does not include entitlement to a particular object, no Permission Set can grant access to it.

Tip: When troubleshooting access issues, check the user's license type first. If the license does not support the required access level, upgrading the license is the only resolution—Permission Sets alone cannot override license entitlements.

Questions / Resources

If you have questions or comments please email support@integrity-data.com.

Last Review: 02/2026

Key Words: Permission Sets, Payroll Security, Read Only Access, Payroll Processing