2CONTROLWARE

Autorisaties in Business Central

Hoe pak je het ontwerpen, beheren en controleren van autorisaties echt aan?

Whitepaper

2-Controlware B.V.

Table of contents

Introductie: Wie zijn wij?

2-Controlware is de specialist in autorisatiebeheer voor Microsoft Dynamics 365 Business Central. Wij ontwikkelen gebruiksvriendelijke softwareoplossingen die organisaties helpen om grip te houden op toegangsrechten, interne beheersing en informatiebeveiliging.

Onze oorsprong ligt bij IT-auditbedrijf 2-Control, waarmee we nog altijd nauw samenwerken. Waar 2-Control zich richt op onafhankelijke IT-audits en adviesdiensten, ligt onze focus volledig op het ontwikkelen, leveren en ondersteunen van autorisatiesoftware. Vanuit hetzelfde kantoor opereren we als één hecht team met ieder een eigen specialisatie. Onze software en dienstverlening zijn het resultaat van meer dan twintig jaar ervaring in IT-auditing en praktijkervaring in het ontwikkelen van autorisatieoplossingen.

Met een persoonlijke aanpak helpen wij organisaties om blijvend ‘in control’ te zijn.

Hoofdstuk 1: De theorie achter autorisaties

Het toekennen van de juiste rechten aan gebruikers in Business Central is een uitdagend en complex proces. Het correct toekennen van rechten vereist een diepgaand begrip van zowel Business Central als de organisatorische rollen en verantwoordelijkheden. Daarnaast is de functionaliteit voor het aan gebruikers toekennen van benodigde rechten erg complex in standaard Business Central. Handmatige processen zijn inefficiënt en foutgevoelig, en de afwezigheid van een gestructureerde aanpak remt de vooruitgang.

Deze whitepaper zal dieper ingaan op hoe je autorisaties binnen Business Central efficiënt inricht, de kwaliteit bewaakt en hoe 2-Controlware organisaties helpt bij deze uitdagingen.

1.1. Wat zijn autorisaties?

Autorisaties, ook wel bekend als toegangsrechten of permissies, bepalen welke gebruikers of groepen gebruikers toegang hebben tot functionaliteit en gegevens binnen een systeem. In het geval van Business Central, zijn autorisaties essentieel om te bepalen wie welke bedrijfsinformatie mag zien of bewerken. Dit helpt bij de bescherming van bedrijfsgegevens en zorgt dat gebruikers alleen toegang hebben tot de informatie die relevant is voor hun functie.

1.2. Het belang van autorisaties inrichten

Autorisaties worden ingericht om te zorgen dat de handelingen die gebruikers in Business Central kunnen uitvoeren aansluiten op hun organisatorische taken en bevoegdheden. Dit houdt in dat rechten voor het uitvoeren van functies en gegevens dienen te worden toegekend, en dat de rechten voor overige functies en gegevens dienen te worden beperkt. Denk hierbij aan het beperken van instellingen (object), het inbrengen van een extra controle op betalingen (systeem), het wel of niet schrijven van uren (instelling) of het uitsluitend toestaan van het documenttype inkooporders

(extensie). Kortom: een zorgvuldige autorisatie-inrichting beschermt niet alleen je gegevens, maar ondersteunt ook de betrouwbaarheid en beheersbaarheid van de processen.

1.3. Autorisaties in Business Central

Autorisaties zijn essentieel om te bepalen wie welke objecten kan zien of beheren in Business Central. Een goede autorisatie-inrichting zorgt ervoor dat gebruikers alleen toegang hebben tot de functionaliteit en gegevens die passen bij hun rol binnen de organisatie. Dit is belangrijk voor het beschermen van gevoelige informatie, het beheersbaar houden van processen en het voorkomen van fouten of ongewenste handelingen. Binnen Business Central is het autorisatiemodel opgebouwd uit vier samenhangende onderdelen:

- **Licenties (entitlements):**

Bepalen op hoofdlijnen tot welke modules en functionaliteit een gebruiker toegang heeft.

- **Machtigingensets (objectautorisaties):**

Regelen toegang tot specifieke objecten, zoals tabellen, pagina's of rapporten, en bepalen welke acties (lezen, schrijven, uitvoeren) zijn toegestaan.

- **Gebruikersspecifieke applicatiecontroles:**

Aanvullende instellingen, vaak per gebruiker in te richten, die specifieke acties op processen beïnvloeden (zoals boekingsperiodes of goedkeuringslimieten).

- **Profielen (rollen):**

Visuele inrichting van de gebruikersinterface, bedoeld om gebruikers snel toegang te geven tot de relevante menu's en functies. Deze vormen geen harde beveiliging, maar helpen wel bij overzicht en gebruiksvriendelijkheid.

In de volgende paragrafen gaan we dieper in op elk van deze onderdelen: hoe ze werken, hoe je ze beheert en wat de mogelijkheden zijn binnen Business Central.

1.3.1. Licenties (entitlements)

Licenties (door Microsoft ook wel entitlements genoemd) zijn de eerste laag van autorisaties. Ze bepalen welke functionaliteit en modules gebruikers kunnen benaderen. Als een gebruiker een beperkte licentie heeft, kan hij maximaal de functionaliteit bereiken die deze licentie beschikbaar stelt. De licentiestructuur van Business Central is ontworpen om flexibel te zijn, zodat bedrijven kunnen kiezen voor de juiste mate van toegang en functionaliteit die ze nodig hebben. Hieronder zijn de belangrijkste typen licenties in Business Central op een rijtje gezet:

Belangrijkste licenties Business Central:

1. **Essentials License:** Biedt toegang tot de kernfunctionaliteit van Business Central, die de meeste bedrijfsprocessen ondersteunen.
2. **Premium License:** Omvat alle functies van de Essentials licentie, plus extra geavanceerde functionaliteit voor bedrijven met complexere behoeften
3. **Team Members License:** Bedoeld voor gebruikers die basisfuncties nodig hebben en voornamelijk gegevens moeten raadplegen en eenvoudige taken moeten uitvoeren.
4. **Device License:** Bedoeld voor apparaten in plaats van individuele gebruikers.
5. **MS 365 License:** Ook wel de ‘alleen-lezen’ licentie genoemd, biedt enkel leesrechten aan gebruikers.

De werking van licenties verschilt tussen SaaS-omgevingen (cloud) en on-premise omgevingen. In de SaaS-omgevingen bepaalt Microsoft op basis van je licentie (entitlement) welke functionaliteit je mag gebruiken. Als er nieuwe objecten bijkomen via een extensie, worden deze automatisch aan je licentie

toegevoegd. Je mag echter alleen die functies gebruiken die expliciet zijn toegestaan in jouw licentie. Objecten buiten jouw entitlement zijn dan wel zichtbaar, maar je kunt ze alleen indirect gebruiken (bijvoorbeeld via een goedgekeurde actie), niet direct openen of bewerken.
Voor een on-premise omgeving werkt dit precies andersom. Hier heb je standaard geen toegang tot objecten, tenzij die expliciet in je licentie zijn opgenomen. Als er via de installatie van een extensie nieuwe objecten bijkomen, moet je licentie handmatig worden uitgebreid om deze toegankelijk te maken.

Kortom: in de SaaS-omgeving (cloud) krijg je automatisch toegang tot nieuwe objecten maar ben je functioneel beperkt door je licentie (entitlement). In on-premise omgevingen krijg je alleen toegang als dit vooraf expliciet is toegekend in je licentie.

1.3.2. Machtigingensets

Hoewel licenties bepalen welke objecten in Business Central technisch benaderbaar zijn, is dit in de praktijk veel te ruim. Niet elke gebruiker heeft toegang nodig tot alle objecten binnen de licentie. Om autorisaties nauwkeuriger af te stemmen op de rol en verantwoordelijkheden van de gebruiker, worden machtigingensets ingezet. Hiermee kun je de objecten binnen een licentie beperken tot enkel die onderdelen die relevant zijn voor een specifieke gebruiker of groep gebruikers. In hoofdstuk 2 gaan wij verder in op het inrichten van deze machtigingensets.

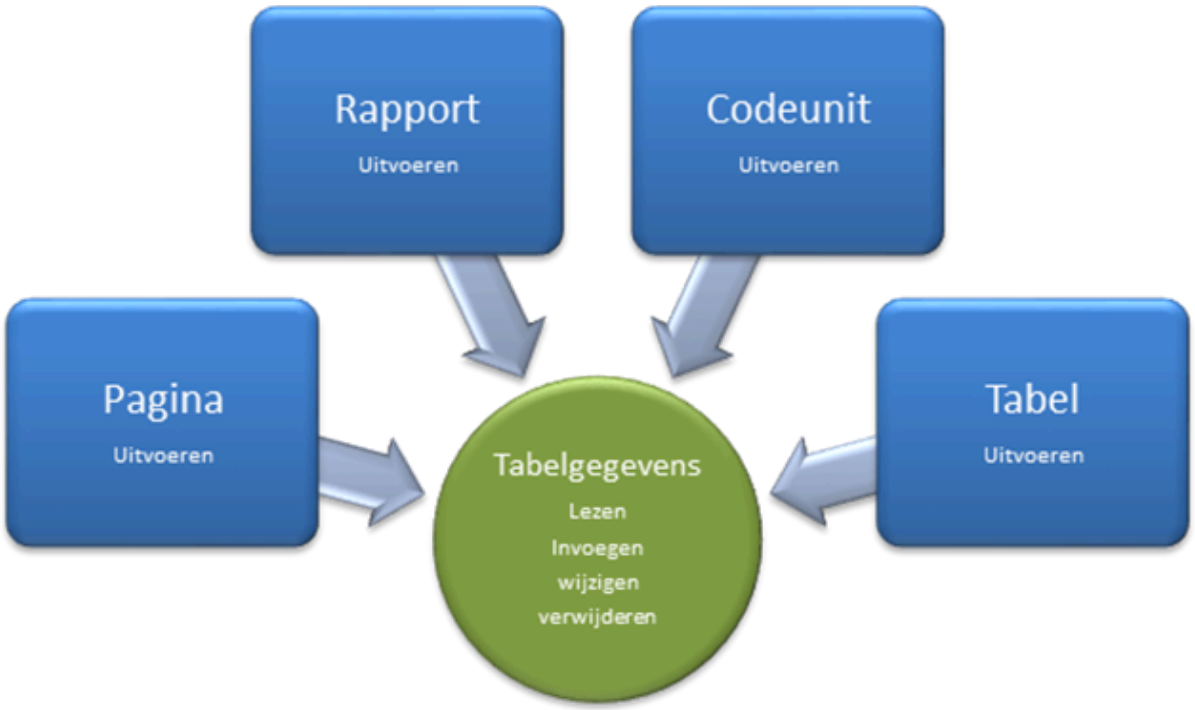
Machtigingensets vormen dus het middel waarmee gebruikers deze toegangsrechten krijgen. Elke gebruiker krijgt toegang tot objecten via één of meerdere van deze sets. Business Central kent hierbij **drie typen machtigingensets:**

1. Systeemsets (die standaard meegeleverd worden en niet aanpasbaar zijn)
2. Extensiesets (die met apps of uitbreidingen meekomen en ook niet aanpasbaar zijn)
3. Zelf gedefinieerde sets, die door functioneel beheerders kunnen worden

ingericht en aangepast.

De technische structuur van Business Central bestaat uit verschillende objecttypen zoals tabellen, pagina's, rapporten en code-units. Voor elk objecttype wordt binnen een machtigingenset vastgelegd welke specifieke acties een gebruiker mag uitvoeren. Bij tabelgegevens gaat het om lezen, invoegen, wijzigen en verwijderen, terwijl bij andere objecttypen het alleen gaat om uitvoeringsrechten. Een belangrijk onderscheid binnen deze acties betreft **directe versus indirecte** rechten:

- Een *direct recht* betekent dat de gebruiker de actie zelfstandig op de lijst of kaart mag uitvoeren.
- Een *indirect recht* houdt in dat de gebruiker alleen toegang tot het object krijgt als onderdeel van een andere toegestane actie. Een typisch voorbeeld: een gebruiker mag geen grootboekposten direct invoegen, maar wél via een factuur boeken. Omdat het boeken van een factuur automatisch leidt tot het invoegen van grootboekposten, is het indirecte recht op dat moment voldoende.



Een specifieke uitdaging doet zich voor wanneer één tabel meerdere soorten gegevens bevat. Een voorbeeld hiervan zijn de tabellen Verkoopkop (36) en Verkoopregel (37), waarin verschillende typen verkoopdocumenten worden opgeslagen zoals offertes, orders, facturen en creditnota's. Wanneer een gebruiker rechten krijgt op deze tabellen, krijgt hij automatisch toegang tot alle typen documenten binnen die tabellen. Om dit te beperken, kun je via machtigingensets rechten geven op specifieke pagina's, bijvoorbeeld alleen de pagina voor verkoopfacturen. Dit heeft echter beperkingen: het is lastig om gebruikers dan wel leesrechten maar geen bewerkrechten te geven of bepaalde documenttypen volledig af te schermen.

Om die reden biedt de Compliance **Field Security** app van 2-Controlware een waardevolle aanvulling. Deze app maakt het mogelijk om binnen machtigingensets met filters te werken, bijvoorbeeld op Documenttype. Hierdoor kun je gedetailleerd instellen welke typen verkoopdocumenten een gebruiker mag zien of bewerken, zelfs binnen één en dezelfde tabel. *Bezoek onze website voor uitgebreide informatie over de Compliance Field Security app*.

1.3.3. Geautomatiseerde controles

Het derde onderdeel van de autorisaties van gebruikers binnen Business Central zijn de 'per gebruiker specifiek in te richten controles'. Bijvoorbeeld: toegestane perioden van boeken op basis van de gebruikersinstellingen, toegestane magazijnwerknemers, limieten via gebruikersinstellingen voor goedkeuring en gebruikers bij werkstromen.

Naast de standaardinstellingen in Business Central worden vaak aanvullende gebruikersspecifieke applicatiecontroles toegevoegd via extensies (apps). Denk bijvoorbeeld aan apps die aanvullende workflow-instellingen of goedkeuringsregels bevatten die je per gebruiker moet instellen. Ook deze instellingen vallen onder het handmatige beheer dat functioneel beheerders veel tijd kost.

Binnen standaard Business Central worden deze instellingen handmatig ingericht per gebruiker én per administratie. Dit is arbeidsintensief, vooral bij het in-, door- en uitstroomproces van medewerkers. Functioneel beheerders zijn daardoor veel tijd kwijt aan het instellen en bijhouden van deze instellingen.

Om dit proces te vereenvoudigen heeft 2-Controlware de **User Templates module** ontwikkelt in de **Authorization Box**. Met deze module kunnen de instellingen die anders handmatig per gebruiker in Business Central ingevuld moeten worden, geautomatiseerd worden door de logica te koppelen aan functie van de gebruikers. Daarnaast kun je ook gebruikersinstellingen, medewerkersgegevens en toegang tot apps en portalen koppelen aan rollen. Via deze wijze kan alles wat in een tabel in Business Central staat via een autorisatieverzoek worden ingevuld.

1.3.4. Profielen (rollen)

In Business Central kan een gebruiker zelf een profiel kiezen via de persoonlijke instellingen. Dit profiel bepaalt wat je allemaal te zien krijgt in Business Central en wordt ook wel zachte beveiliging genoemd. Het profiel bepaalt wat je ziet, maar niet wat je daadwerkelijk mag doen, maar is geen harde beperking op rechten. Zo kan een gebruiker bijvoorbeeld:
-Een verborgen pagina openen door de juiste naam in te typen in de zoekfunctie.
-Een directe URL gebruiken om alsnog bij een pagina te komen.
-Verborgen velden en acties weer zichtbaar maken via personaliseren of design (bijvoorbeeld in een pre-productieomgeving).

Hoewel de profielen in het rollencentrum dus geen echte bevoegdheden van gebruikers ontneemt, is het wel een goede eerste defensielijn in het voorkomen van ongeautoriseerde handelingen.

Binnen standaard Business Central kan aan iedere gebruiker een profiel worden toegekend met het gebruikersconfiguratie scherm. Deze handeling

kan in de **Authorization Box** van 2-Controlware geautomatiseerd worden door het profiel te koppelen aan een organisatierol, of door een profiel aan een gebruiker te koppelen in een autorisatieverzoek in de **Authorization Box**. *Ga naar onze website voor alles wat u wilt weten over onze Authorization Box.*

Hoofdstuk 2: Van theorie naar praktijk: Autorisaties inrichten, hoe begin je daaraan?

Het zorgvuldig inrichten van autorisaties in Business Central is essentieel om te zorgen dat gebruikers alleen toegang hebben tot de functies en gegevens die passen bij hun rol. Dit beperkt niet alleen beveiligingsrisico's, maar helpt ook om fouten en inefficiëntie te beperken. In dit hoofdstuk beschrijven we het stapsgewijze proces waarmee een betrouwbare autorisatiestructuur wordt ontworpen, getest en geïmplementeerd. We bespreken hoe je begint met het opstellen van een autorisatieraamwerk, hoe machtigingensets worden opgenomen en opgeschoond, hoe je deze test, en hoe je uiteindelijk live gaat met de nieuwe inrichting. Tot slot lichten we toe hoe het beheer van autorisaties het beste georganiseerd kan worden.

2.1. Stap 1: Stel het autorisatieraamwerk op

De eerste stap is het opstellen van een helder autorisatieraamwerk. Daarbij proberen we zo dicht mogelijk aan te sluiten bij de organisatorische functies van de Business Central-gebruikers. Hierdoor ontstaat geen onduidelijkheid bij de indiensttreding van nieuwe medewerkers over welke rechten zij zouden moeten krijgen.

We starten met het opstellen van een organigram waarin alle afdelingen worden opgenomen die met Business Central werken. Onder elke afdeling benoemen we de functies die daarin actief zijn. Vervolgens wordt per functie geïnventariseerd welke gebruikers toegang nodig hebben tot Business Central en wat zij daarbinnen moeten kunnen doen. Deze inventarisatie gebeurt vaak op basis van een kerngebruiker per functie, die toelicht welke taken in Business Central worden uitgevoerd. Op basis van deze input wordt een overzichtelijke matrix opgesteld, waarin taken per functie worden gekoppeld. Deze matrix wordt ter goedkeuring voorgelegd aan de

verantwoordelijke(n) van het autorisatieproject.

2.2. Stap 2: Neem de taken op van een functie

In een vervolgsessie worden de taken uit de autorisatiematrix verder uitgewerkt. Elke taak krijgt een eigen machtigingenset, zodat een modulaire inrichting ontstaat. Met 'opnemen' bedoelen we het vastleggen van alle objecten (zoals tabellen en pagina's) die een gebruiker nodig heeft voor het kunnen uitvoeren van een taak.

Dit opnameproces kan worden uitgevoerd met de standaardfunctionaliteit van Business Central: machtigingen registreren. Hierbij maak je door te klikken op de relevantie functies binnen Business Central een machtigingenset aan. Alle objecten die worden aangeraakt tijdens deze sessie worden automatisch toegevoegd aan de set, inclusief lees-, schrijf- en uitvoerrechten.

2.3. Stap 3: Schoon de machtigingensets op

Na het opnemen is de taak-gerelateerde machtigingenset ("taakset") nog niet klaar voor gebruik. Om de set overzichtelijk en beheersbaar te houden moet deze worden opgeschoond, zodat alleen de relevante rechten voor de specifieke taak overblijven. Alle overige "algemene" rechten dienen te worden toegekend via basissets, zoals:

- Eén basisset voor algemene leesrechten.
- Eén basisset voor basis wijzigingsrechten.

Het opschonen kan handmatig of via de functie "machtigingensets uitsluiten". De nieuwere versies van Business Central ondersteunen ook dynamische uitsluiting, waarbij wijzigingen in de basisset automatisch worden doorgevoerd in de taaksets.

De standaard recorder van Business Central helpt bij het vastleggen van deze informatie, maar heeft als nadeel dat je alleen je eigen gebruikerssessie kunt

opnemen en niet automatisch kunt opschonen. Daarom hebben wij de **Advanced Permissions Recorder** ontwikkeld, die gratis beschikbaar is via AppSource. Met deze recorder kun je via andere gebruikerssessies opnemen, bepaal je vooraf welke acties (lezen, invoegen, wijzigen, verwijderen en/of uitvoeren) van welke typen objecten worden opgenomen en hoe de set automatisch wordt opgeschoond. *Op zoek naar meer details over de Advanced Permissions Recorder? Kijk op onze website.*

2.4. Stap 4: Testen en go-live

Zodra alle taken zijn opgenomen en de machtigingensets zijn opgeschoond, is het tijd om te testen. Advies is te beginnen met een *(1) interne kwaliteitscontrole*. Hierbij kent de autorisatiebeheerder de machtigingensets individueel toe aan zichzelf en voert alle taken één voor één uit met representatieve data. Zo wordt gecontroleerd of elke set op zichzelf correct functioneert. Vervolgens is het advies om kerngebruikers *(2) detailtests* te laten uitvoeren. Zij krijgen de eerder geïnventariseerde taken opnieuw toegewezen, maar nu als afzonderlijke machtigingensets en controleren of een taak losstaand van andere machtigingenset uitgevoerd kan worden. Wanneer alle machtigingensets zijn getest en uitvolgende foutmeldingen zijn verwerkt, kunnen we door naar de *(3) acceptatietesten*. Bij de acceptatietesten worden alle machtigingensets die onder een functie komen tegelijk toegekend aan de kerngebruiker en worden opnieuw gecontroleerd. Na deze test moeten alle openstaande problemen zijn opgelost, zodat de machtigingensets van de testomgeving overgezet kunnen worden naar de productieomgeving.

Hierna is het tijd voor de livegang. De machtigingensets worden vanuit de testomgeving geëxporteerd. Dit kan op twee manieren:

1. Via de machtigingensetpagina: exporteren als .xml.
2. Via configuratiepakketten: exporteer tabellen 2000000165 (Permission Set) en 2000000166 (Permission Set Object).[1]

[1] Let op: deze tabellen zijn niet zichtbaar in de standaardlijst, maar kunnen handmatig worden ingevoerd. Tabellen 2000000004 en 2000000005 bevatten systeemmachtigingensets en zijn alleen exporteerbaar, niet importeerbaar.

Afhankelijk van de organisatie kan gekozen worden voor gefaseerde livegang (per afdeling of gebruikersgroep) of een Big Bang (in één keer voor de gehele organisatie). In beide gevallen worden de nieuwe machtigingensets geïmporteerd en vervangen ze de oude toewijzingen bij de gebruikers.
De manier waarop de sets worden toegekend aan gebruikers hangt af van de gekozen structuur. Als alleen met losse machtigingensets wordt gewerkt, moet voor elke gebruiker handmatig op de gebruikerskaart in Business Central worden aangegeven welke sets van toepassing zijn. Vanaf Business Central 2025 zijn deze groepen vervangen door beveiligingsgroepen, aangemaakt in Azure/Entra, waaraan vervolgens in Business Central machtigingensets kunnen worden gekoppeld.

Voor organisaties die een gestructureerd en geautomatiseerd proces zoeken, biedt de **Authorization Box** van 2-Controlware een geïntegreerde oplossing. Door een digitaal organigram te maken met afdelingen en organisatierollen, ontstaat een duidelijk overzicht van wie welke rechten heeft of zou moeten krijgen. Het voordeel hiervan is de extra veiligheid die wordt aangeboden door het inrichten van goedkeuringen voor autorisatieverzoeken. Zo kijken er altijd vier ogen mee bij het toekennen van (kritische) bevoegdheden. Deze goedkeuringsprocessen kun je ook instellen voor wijzigingen in de autorisatiestructuur zelf, zoals het toevoegen van een machtigingenset aan een rol.

2.5. Stap 5: Machtigingensets onderhouden

Na implementatie moet het beheer van de autorisaties goed worden ingericht. De persoon die verantwoordelijk is voor het uitgeven van machtigingensets moet begrijpen hoe de inrichting werkt en hoe foutmeldingen kunnen worden opgelost. Voorbeeld: Een gebruiker kan geen facturen meer boeken. Controleer eerst of dit recht volgens de designmatrix is toegestaan. Zo ja, dan ontbreekt er waarschijnlijk een machtigingenset of is deze niet correct gekoppeld. Zo nee, overleg dan met de leidinggevende of het recht alsnog toegekend mag worden.

Hoofdstuk 3: Controleren en beoordelen van autorisaties

Een succesvolle implementatie van autorisaties is het begin van effectief autorisatiebeheer. Zodra autorisaties live zijn, begint het proces van beheren en bewaken. Dit is essentieel voor zowel de bedrijfscontinuïteit als compliance-doeleinden. Effectieve controle van autorisaties bestaat uit drie complementaire benaderingen.

3.1. Proactieve controle

Na de livegang is het belangrijk om de autorisaties proactief te blijven controleren in Business Central. Met de standaard functionaliteit is dit uitdagend maar niet onmogelijk, mits je weet welke objecten kritisch zijn en welke combinaties potentiële conflicten kunnen veroorzaken.

De meest eenvoudige, maar ook de meest intensieve, oplossing is om per gebruiker de effectieve machtigingen te beoordelen. Dit is een functie bovenaan de gebruikerskaart die alle object-autorisaties uit machtigingensets en groepen op gebruikersniveau samenvat.

Een alternatieve benadering is het gebruik van Excel om verschillende exports te combineren. Hiervoor zijn tabellen zoals Access Control (2000000053), AllObjWithCaption (2000000058), Tenant Permission (2000000165) en Tenant Permission Set (2000000166) noodzakelijk. Door objecten in machtigingensets te koppelen aan gebruikers, kun je beoordelen of kritische objecten zijn toegewezen en of potentiële conflicten bestaan. Let op dat je niet alle tabellen middels configuratiepakketten kunt exporteren omdat dit systeemtabellen zijn. Wat je hiervoor kunt doen is de URL aanpassen in Business Central om de tabel naar voren te halen. Je vervangt dan alles na ‘page=xxxx’ met ‘table=xxxx’.

Voor een aanzienlijke vereenvoudiging van dit proces biedt de **Continuous Monitoring module** in de **Authorization Box** van 2-Controlware een geïntegreerde

oplossing. Deze module haalt via een web-service alle relevante autorisatiedata op en presenteert deze in overzichtelijke dashboards. Hierdoor kunnen beheerders snel inzicht krijgen in wie welke rechten heeft, op gebruikers-, machtigingenset- en organisatierol-niveau.
Een extra voordeel van deze module is het beoordelingssysteem, waarmee autorisaties kunnen worden geëvalueerd en beoordelingen worden vastgelegd voor compliance en rapportage. Het systeem houdt bij wanneer autorisaties zijn gewijzigd sinds de laatste beoordeling, zodat beheerders direct zien waar hernieuwde controle nodig is. Dit zorgt niet alleen voor betere beveiliging, maar ondersteunt ook de documentatie voor audits en compliance-controles.

3.2. Reactieve monitoring

Naast het controleren van toegangsrechten ('wie heeft welke rechten?') is het ook waardevol om te blijven monitoren wat er daadwerkelijk is gebeurd ('wie heeft wat gedaan?').

In Business Central kun je wijzigingslogposten activeren op kritische tabellen en deze periodiek beoordelen om ongeautoriseerde wijzigingen te identificeren. Een beperking van deze aanpak is dat je pas kunt ingrijpen nadat een wijziging heeft plaatsgevonden, waardoor alleen herstelwerkzaamheden mogelijk zijn.

Voor een betrouwbare log is het essentieel dat niet iedereen de log-instellingen kan aanpassen en daarmee het loggen van tabellen (tijdelijk) kan uitschakelen. Daarom moet bij het controleren van de log ook worden nagegaan wie wijzigingsrechten heeft op de Change Log Setup (402). Hoewel individuele regels uit de log niet zomaar verwijderd kunnen worden, bestaat theoretisch de mogelijkheid dat de gehele log wordt opgeschoond als iemand kwaadwillig is.

Bij het loggen van wijzigingen is het altijd een afweging tussen veiligheid en continuïteit. Bij elke gelogde tabel moet Business Central de data tweemaal

wegschrijven: eenmaal in de tabel zelf en eenmaal naar de log. Als veel tabellen gelogd worden kan het systeem dus erg traag worden. Wij adviseren om logging wel altijd te activeren op instellingen, stamgegevens en op procesdata die je wilt gebruiken voor inzicht.

3.3. Periodieke evaluatie

Wanneer autorisaties eenmaal zijn ingesteld en in gebruik zijn genomen, is periodieke evaluatie essentieel. Na verloop van tijd, bijvoorbeeld wanneer een accountantscontrole nadert, wil je weten of de inrichting nog steeds correct is. Een preciezer verloop van deze processen wordt uitgelegd in hoofdstuk 4.

Hoofdstuk 4: Hoe kun je ervoor zorgen dat de autorisaties up-to-date blijven?

De effectiviteit van autorisatiebeheer staat of valt bij de bredere organisatieprocessen. Zonder duidelijke procedures voor het aanvragen, wijzigen en intrekken van rechten schiet zelfs de technisch perfecte autorisatie-inrichting in de praktijk tekort. De volgende processen vormen de ruggengraat van duurzaam autorisatiebeheer en zorgen ervoor dat de zorgvuldig opgebouwde autorisatiestructuur daadwerkelijk blijft functioneren zoals bedoeld.

4.1. Instroom, doorstroom en uitstroom van medewerkers

Gedurende de gehele levenscyclus van een medewerker (van indiensttreding tot functiewijzigingen en uiteindelijk uitdiensttreding) vormen autorisatieprocessen een belangrijk onderdeel van het personeelsbeheer en organisatiebeleid.

Bij indiensttreding is het belangrijk dat autorisaties zorgvuldig worden ingesteld op basis van de specifieke rol van de nieuwe medewerker. Dit betekent dat alleen relevante modules en gegevens toegankelijk zijn, zodat de gebruiker efficiënt kan werken zonder onnodige blootstelling aan gevoelige informatie.

Bij een functiewijziging moeten de toegangsrechten opnieuw worden beoordeeld en aangepast in samenhang met hun nieuwe verantwoordelijkheden. Dit houdt in dat nieuwe rechten worden toegekend indien nodig, terwijl verouderde rechten worden ingetrokken om ongeautoriseerde toegang tot niet-relevante gegevens te voorkomen.

Bij uitdiensttreding moeten alle toegangsrechten worden ingetrokken en het account worden gedeactiveerd om de veiligheid van het systeem te

waarborgen. Dit omvat het verwijderen van machtigingensets en een beveiligingscontrole om te verzekeren dat er geen ongeautoriseerde toegangspunten achterblijven. Daarnaast kunnen de door de gebruiker beheerde gegevens worden gearchiveerd en gedocumenteerd voor audit- en compliance-doeleinden.

Personeelswijzigingen handmatig verwerken in autorisaties is vaak omslachtig en foutgevoelig. De **Authorization Box** van 2-Controlware vereenvoudigt deze processen door machtigingensets te groeperen onder een organisatierol, in plaats van ze handmatig toe te moeten kennen aan elke gebruiker. Op basis van autorisatieverzoeken voor de indiensttreding, functiewijziging en/of uitdiensttreding, met eventuele goedkeuringsflows, worden de rechten in Business Central automatisch op de juiste momenten aangepast en gelogd. De **Authorization Box** bespaart hiermee niet alleen tijd, maar forceert hiermee ook een tracering.

4.2. Incidentenbeheer

Incidentenbeheer rond autorisaties vormt een belangrijk onderdeel van de bredere IT-serviceprocessen binnen de organisatie. Wanneer gebruikers problemen ondervinden met hun toegangsrechten, is een snelle en efficiënte afhandeling niet alleen technisch maar ook operationeel noodzakelijk om bedrijfsactiviteiten niet te verstoren.

Het proces begint met het melden en classificeren van het incident door de gebruiker. Het IT-team analyseert vervolgens het probleem door logbestanden en gebruikersprofielen te controleren en de oorzaak te achterhalen. Op basis hiervan worden de toegangsrechten aangepast, bijvoorbeeld door rechten bij te werken, rollen te wijzigen of tijdelijke toegang te verlenen.

Na het oplossen van het incident wordt de gebruiker geïnformeerd over de genomen maatregelen en worden alle wijzigingen gedocumenteerd voor naleving van compliance- en auditvereisten.

4.3. Wijzigingen beheer

Bij wijzigingen in Business Central, zoals software-updates of nieuwe functionaliteit, is het cruciaal om rekening te houden met de bestaande autorisatiestructuur. Dit garandeert dat gebruikers continu de juist toegang behouden zonder de beveiliging in gevaar te brengen.

Het wijzigingsproces start met een impactanalyse om te bepalen welke gebruikers en functies worden beïnvloed. Op basis hiervan worden een wijzigingsplan opgesteld en testscenario's ontwikkeld om de impact op autorisaties te toetsen. De wijzigingen worden eerst in een gecontroleerde testomgeving doorgevoerd en onderworpen aan beveiligingscontroles. Na implementatie wordt gebruikersfeedback verzameld om eventuele knelpunten snel op te lossen. Alle wijzigingen worden zorgvuldig gedocumenteerd om te voldoen aan compliance-vereisten en als referentie voor toekomstige aanpassingen.

Hoofdstuk 5: Best practices voor effectief autorisatiebeheer

Na het begrijpen van de theoretische basis van autorisaties, het praktisch inrichten ervan, het evalueren van de implementatie en het opzetten van beheerprocessen, komen we bij onze best practices. In dit hoofdstuk delen we de expertise die we hebben opgebouwd tijdens meer dan twintig jaar ervaring met autorisatiebeheer in honderden Business Central-omgevingen.

5.1. Modulaire opbouw voor een verfijnde inrichting

Een effectieve autorisatie-inrichting is gebaseerd op een modulaire aanpak. Dit betekent dat voor iedere specifieke taak een afzonderlijke machtigingenset wordt gebouwd. Deze machtigingensets worden bewust klein gehouden, zodat gebruikers precies die rechten hebben die ze nodig hebben voor hun taken: niet meer en niet minder.

Bij deze aanpak worden twee soorten rechten buiten de machtigingenset gehouden: (1) leesrechten die worden apart gedefinieerd en (2) basis-rechten. Leesrechten worden doorgaans opgesplitst in twee categorieën: algemene leesrechten (pagina's en rapporten voor iedereen) en financiële leesrechten (pagina's en rapporten specifiek voor administratie en directie). Een algemene basis-set bevat rechten die iedereen nodig heeft, zoals inlogrechten en toegang tot objecttypes die geen onderdeel zijn van specifieke taak-machtigingensets. Een specifieke taak-machtigingenset bevat hierdoor enkel het objecttype tabelgegevens met de opties invoegen, wijzigen of verwijderen.

Door het potentieel grote aantal machtigingensets is een duidelijke naamgevingsconventie aan te raden. Een aanbevolen structuur is: [bedrijfsafkorting]-[afdelingsafkorting]-[taak]. Bijvoorbeeld: 2C-INK-ORDER voor de machtigingenset om inkooporders aan te maken.

Om machtigingensets verder te structureren, kunnen ze worden gebundeld in beveiligingsgroepen. Deze beveiligingsgroepen worden aangemaakt in Azure AD/Entra, waar ook gebruikers aan worden gekoppeld. Het is aan te raden om deze beveiligingsgroepen zo veel mogelijk af te stemmen op het HR-organigram om het risico op verkeerd toegekende machtigingensets bij nieuwe gebruikers te verminderen.

5.2. Segregation of Duties

Voor een optimale functiescheiding worden bepaalde splitsingen in machtigingensets consequent aangehouden. Voor operationele taken wordt altijd onderscheid gemaakt tussen aanmaken, ontvangen en boeken van documenten. Bijvoorbeeld: inkooporder aanmaken, inkoopontvangst boeken, en inkoopfactuur boeken worden als aparte machtigingensets ingericht.

Hiernaast zijn er ook diverse instellingen-tabellen waar wij per afdeling een specifieke machtigingenset voor maken. *Bijvoorbeeld een machtigingenset voor financiële instellingen, voor projectinstellingen en voor productie-instellingen.* Tot slot krijgen het beheren van stamgegevens ook hun eigen machtigingenset. *Bijvoorbeeld beheren van artikelen, klanten, leveranciers en de bankrekening leveranciers.*

5.3. Include vs. exclude benadering

De hierboven beschreven methode noemen wij een "include inrichting", waarbij specifiek wordt benoemd welke wijzigrechten een gebruiker mag hebben. Deze aanpak biedt de meeste zekerheid dat gebruikers alleen toegang hebben tot precies wat ze nodig hebben. Een alternatieve aanpak is de "exclude inrichting", waarbij een groot deel van de rechten wordt opengesteld en alleen wordt beperkt wat een gebruiker niet mag doen.
Het voordeel van deze methode is dat het niet zo intensief is om in te richten, door alleen de “kern” tabellen te identificeren die nodig zijn bij het uitvoeren van een taak haal je aan de ene kant de grootste aanpassingsrisico’s er uit en aan de andere kant krijgen gebruikers niet zo

snel foutmeldingen op achterliggende tabellen. Het nadeel van deze aanpak is wel dat je alleen beveiligd wat je expliciet benoemt. Alles wat je niet benoemd of wat later wordt toegevoegd, staat in deze aanpak automatisch open voor alle gebruikers.

Hoofdstuk 6: Conclusie en volgende stappen

Het doeltreffend beheren van autorisaties in Microsoft Dynamics 365 Business Central is een complexe, maar belangrijke taak voor elke organisatie. Zoals we in deze whitepaper hebben uiteengezet, vormt een gestructureerde aanpak de basis voor het waarborgen van databeveiliging en compliance. Van het zorgvuldig inrichten van licenties, machtigingensets, gebruikersspecifieke controles en profielen tot het implementeren van robuuste beheerprocessen voor instroom, doorstroom en uitstroom van medewerkers, incidenten en wijzigingen beheer, elke stap draagt bij aan een duurzame autorisatiestructuur.

De toepassing van best practices, zoals een modulaire opbouw van machtigingensets en de implementatie van strikte functiescheiding (Segregation of Duties), is essentieel om de complexiteit te beheersen en risico's te minimaliseren. Hoewel standaard Business Central functionaliteiten hiervoor een basis bieden, tonen de praktijkervaringen aan dat handmatige processen arbeidsintensief en foutgevoelig zijn.

Bij 2-Controlware begrijpen we de uitdagingen die komen kijken bij autorisatiebeheer in Business Central. Met meer dan twintig jaar ervaring in IT-auditing en de ontwikkeling van gespecialiseerde softwareoplossingen, zijn wij de partner die u helpt "in control" te blijven.

De **Authorization Box** van 2-Controlware is uw geïntegreerde oplossing voor:

- **Vereenvoudigd procesbeheer:** Automatiseer de toekenning en aanpassing van rechten bij in-, door- en uitstroom, inclusief goedkeuringsflows, om tijd te besparen en tracering te forceren.
- **Proactieve controle en monitoring:** Krijg snel inzicht in wie welke rechten heeft op gebruikers-, machtigingenset- en organisatierol-niveau via overzichtelijke dashboards. Beoordeel autorisaties, leg beoordelingen vast voor compliance en identificeer direct waar hernieuwde controle

nodig is.

- **Geavanceerde inrichting:** Benut de kracht van modulaire machtigingensets en implementeer verfijnde toegangscontroles, zelfs tot op veldniveau, met onze Compliance **Field Security** app.
- **Data-integriteit waarborgen:** Met onze **Field Validation** app verzekert u de nauwkeurigheid van uw data door bijvoorbeeld verplichte velden of specifieke formaten af te dwingen.

Neem de volgende stap naar moeiteloze controle en databeveiliging in Business Central.

Bezoek onze website voor meer informatie over de **Authorization Box** , de **Advanced Permissions Recorder** , en onze Compliance apps. Of neem direct contact met ons op voor een persoonlijke demonstratie en ontdek hoe 2-Controlware uw organisatie kan helpen om blijvend grip te houden op autorisaties.

Extra informatie

Ontdek 2-Controlware. Onderstaand vindt u meer gedetailleerde informatie over onze producten, quick scans voor uw organisaties, links naar onze sociale media en nog veel meer. Elk van deze bronnen is ontworpen om u te helpen uw IT-omgeving te optimaliseren en uw bedrijf te verbeteren. Ontdek via onderstaande links wat 2-Controlware voor u kan betekenen.

- **Wiki page**
  Meer informatie over onze apps.

- **Wiki page for the Authorization Box**
  Meer informatie over onze Authorization Box

- **"Is your Dynamics application fraud proof?" - Checklist**
  Krijg inzicht in welke punten al fraudebestendig zijn en welke mogelijk nog onvoldoende aandacht krijgen in je Dynamics aanvraag.

- **Blogs**
  Blijf op de hoogte van onze laatste ontdekkingen en inzichten. Door onze kennis te delen, hopen we je een beter inzicht te geven in autorisaties.

- **AppSource**
  Download al onze apps via Microsoft AppSource.

Volg ons via Social media

Wil je regelmatig updates ontvangen? Volg ons dan!

2CONTROLWARE

Address:

2-Controlware B.V.

Haagsemarkt 1

4813 BA Breda

The Netherlands

sales@2-controlware.com

Contact Us :

P : +31(0)765019470

W : www.2-controlware.com