ORTEC Workforce Scheduling 7

Implementatiehandleiding Access Control

juli 2025

PUBLIEK

ORTEC

Gepubliceerd: juli 01, 2025

Versie: 2025.2

Inhoudsopgave

1 Access Control (Toegangscontrole) 1

2 Aan de slag 2
- 2.1 Inloggen 2
- 2.2 Wijzig wachtwoord 2
- 2.3 SSO-toegangscontrole 2

3 Gebruikersbeheer 3
- 3.1 Gebruiker toevoegen 3
- 3.2 Gebruiker zoeken 3
- 3.3 Gebruikersaccount uitschakelen 4
- 3.4 Authenticatiebestand downloaden voor gebruiker 4
- 3.5 Wachtwoordbeperkingen instellen voor de Comtec-verificatiemethode 4

4 Beheer gebruikersgroepen 5
- 4.1 Gebruikersgroephiërarchie 5
- 4.2 Nieuwe gebruikersgroep aanmaken 6
- 4.3 Selecteer een roostergroep voor een gebruikersgroep 6
- 4.4 Voeg een gebruiker aan een gebruikersgroep toe 7
- 4.5 Een gebruiker uit de gebruikersgroep verwijderen 7
- 4.6 Hernoemen van een gebruikersgroep 8
- 4.7 Verwijderen van een gebruikersgroep 8
- 4.8 Een back-up maken van alle gebruikersgroep permissies 8
- 4.9 Herstel groepspermissies van de back-up 8

5 Permissies 10
- 5.1 Permissies verlenen 10
- 5.2 Permissies intrekken 11
- 5.3 Filter op verleend 11
- 5.4 Filteren op toegangsmodus 11
- 5.5 Vrije tekst filter 12
- 5.6 Access Control / Toegangscontrole 12
- 5.7 Applicaties 12
- 5.8 Databeheer 13
- 5.9 ORTEC WS Ad Hoc Planning 15
- 5.10 ORTEC WS for Employees 15
- 5.11 ORTEC WS for Managers 15
- 5.12 ORTEC WS for Team Schedulers 15
- 5.13 ORTEC WS for Web 15
- 5.14 Rapporten (Microsoft) 15
- 5.15 Tijdregistratie 15
- 5.16 Gebruikersinterface 16

6 Verantwoording 17

1 Access Control (Toegangscontrole)

De **Access Control (Toegangscontrole)** web applicatie wordt gebruikt voor gebruikersauthenticatie, permissies en verantwoording in **ORTEC Workforce Scheduling (ORTEC WS)**.

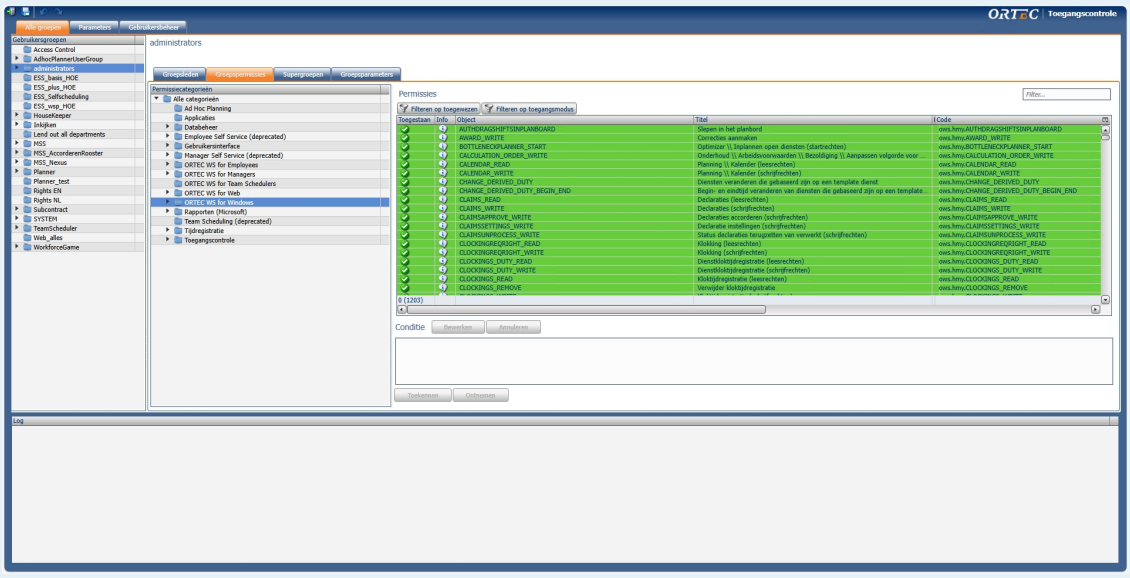
- **Authenticatie**: om de identiteit van de gebruiker te bevestigen.
- **Permissies**: om te bepalen welke gebruiker of gebruikersgroep toegang heeft tot welke delen van het systeem.

  - Niet alle permissies zijn mogelijk van toepassing op jouw systeem. Dit hangt af van de systeemconfiguratie van jouw organisatie en de permissies die aan je zijn toegekend.
  - Het is ook mogelijk om permissies toe te kennen voor de **Access Control** applicatie zelf.

- **Verantwoording**: om bij te houden wie welke delen van het systeem heeft gebruikt. Deze informatie kan worden gebruikt voor auditdoeleinden.

Voorbeeld

Access Control applicatie.



2 Aan de slag

De **ORTEC WS** webapplicatie **Access Control** is beschikbaar via het intranet van je organisatie. Je hebt het webadres, een gebruikersnaam en een wachtwoord nodig voordat je de applicatie kunt gaan gebruiken.

Je kunt ook **Access Control** openen binnen de **OWS-client**. Voor meer informatie, zie "SSO-toegangscontrole" op pagina 2.

2.1 Inloggen

1. Ga naar het webadres van **Access Control**.
2. Selecteer een **Taal**.
3. Vul jouw **Gebruikersnaam** in.
4. Vul jouw **Wachtwoord** in.
5. Druk op Enter of klik op **Inloggen**.

2.2 Wijzig wachtwoord

De Applicatiebeheerder kan gebruikers verplichten hun wachtwoord te wijzigen bij hun eerste aanmelding door die optie te selecteren bij het uitgeven van een wachtwoord. In dat geval wordt de pagina **Wachtwoord wijzigen** weergegeven nadat je voor de eerste keer bent ingelogd.

Je kunt je wachtwoord ook op elk gewenst moment als volgt wijzigen:

1. Schakel het selectievakje **Wachtwoord wijzigen** in wanneer je je aanmeldt bij de applicatie.
2. Vul jouw **Huidig wachtwoord** in.
3. Vul jouw **Nieuw wachtwoord** in.
4. Vul opnieuw jouw wachtwoord in, in het veld **Bevestig nieuw wachtwoord.**
5. Klik **Toepassen** om je wachtwoord te wijzigen en in te loggen.

2.3 SSO-toegangscontrole

Een ORTEC consultant of een Applicatiebeheerder kan het openen van **Toegangscontrole** met single sign-on (SSO) binnen de **OWS Client** mogelijk maken:

1. Klik in de **OWS Client** met je rechtermuisknop op een lege plek in de menubalk.
2. Selecteer **Customize**.
3. Selecteer op het tabblad **Commando's** de categorie **Onderhoud**.
4. Sleep de opdracht **Toegangscontrole** naar een menu. Bijvoorbeeld het menu **Onderhoud**.

3 Gebruikersbeheer

Om het delen en onderhouden van permissies te vereenvoudigen, wordt geadviseerd om individuele gebruikers toe te voegen aan gebruikersgroepen. Indien nodig kan een individueel gebruikersaccount worden uitgeschakeld om de toegang te beperken.

Geef per gebruiker de verificatiemethode op die wordt gebruikt om de geldigheid van het wachtwoord van elke gebruiker te bevestigen.

3.1 Gebruiker toevoegen

1. Klik op de tab **Gebruikersbeheer**.
2. Klik in de **Data beheer** sectie op **Gebruiker toevoegen**.
3. Vul op de tab **Algemeen** de (vereiste) velden in.

   Verplichte velden die niet zijn ingevuld, hebben een kleurmarkering  , de tabbladen waarvoor niet alle verplichte velden zijn ingevuld, zijn gemarkeerd  .

4. Voeg op het tabblad **Gebruikersgroep**en de gebruiker toe aan een of meer gebruikersgroepen.
   - Klik op de knop **Toevoegen**.
   - Zoek de juiste gebruikersgroep(en).
   - Selecteer gebruikersgroep(en). Als je meerdere gebruikersgroepen tegelijk wilt selecteren, houdt je de Ctrl- of Shift-toets ingedrukt.
   - Klik op **OK.**
5. Klik op **OK.**

3.2 Gebruiker zoeken

1. Klik op de tab **Gebruikersbeheer**.
2. Klik in het gedeelte **Data beheer** op **Gebruiker zoeken**.

   Of klik op **Gebruikerslijst tonen**. Filter in de rechterbovenhoek de gebruikerslijst.

3. Typ in het gedeelte **Gebruiker zoeken** de tekst (bijvoorbeeld een deel van een gebruikersnaam) waarnaar je wilt zoeken.
4. Klik op **Zoek**.
   Hiermee wordt in volledige tekst gezocht in alle kolommen die in de resultatenlijst worden weergegeven, bijv. Gebruikersnaam, Naam voluit, Omschrijving.

   - Om de getoonde kolommen te beheren, klik je - in de kolomkop rechtsboven - **op Configureer grid kolommen**.
   - Om de resultaten te sorteren, klik je op een **kolomkop**.
   - Als je de resultaten wilt groeperen, druk je op de **Shift-toets** + een **kolomkop** om de resultaten in het raster te groeperen op basis van de geselecteerde kolom.

3.3 Gebruikersaccount uitschakelen

Een uitgeschakeld gebruikersaccount heeft geen toegang tot het systeem.

1. Klik op de tab **Gebruikersbeheer**.
2. Zoek het gebruikersaccount dat je wilt uitschakelen.
3. Klik met de rechtermuisknop op de geselecteerde gebruiker en klik op **Gebruiker aanpassen**.
4. Deselecteer het **Account actief** selectievakje op de tab **Algemeen**.
5. Klik op **OK.**

3.4 Authenticatiebestand downloaden voor gebruiker

Authenticatiebestanden kunnen worden gebruikt door een **ORTEC WS** applicatie om zichzelf te identificeren bij een andere **ORTEC WS** applicatie.

1. Klik op de tab **Gebruikersbeheer**.
2. Vind de gebruiker waarvan je het authenticatiebestand wilt downloaden.
3. Klik met de rechtermuisknop op de geselecteerde gebruiker en klik op **Authenticatiebestand downloaden**.
4. In het **Authenticatiebestand downloaden** venster vul je het wachtwoord van de gebruiker in. Klik vervolgens op **OK**.
5. Klik op **Opslaan** in het download venster en kies een **locatie** waar het bestand moet worden opgeslagen.
6. Klik op **Opslaan** en daarna **Sluiten**.

3.5 Wachtwoordbeperkingen instellen voor de Comtec-verificatiemethode

1. Start **ORTEC System Configuration** op de **applicatie server**.
2. Voer je **Gebruikersnaam** in.
3. Vul je **Wachtwoord** in.
4. Druk op Enter of klik op **OK.**
5. Klik op de tab **Configuration**, klik in de sectie **Settings Management** op **Settings Manager**.
6. Klik op de categorie **CUASFW** en selecteer **ComtecAuthentication**.
    - De minimaal vereiste lengte voor een wachtwoord kan met de instelling MinimumPasswordLength (standaard 8) worden ingesteld.
    - Wanneer een gebruiker het wachtwoord moet wijzigen omdat de minimale vereiste lengte van het wachtwoord niet overeenkomt, kan deze instelling EnforcePasswordRequirementsDuringLogin worden gebruikt (standaard: True).

4 Beheer gebruikersgroepen

Gebruikers die dezelfde permissies delen kunnen samengevoegd worden in gebruikersgroepen. Permissies worden toegekend aan gebruikersgroepen; niet aan individuele gebruikers. Voor meer informatie over permissies, zie "Permissies" op pagina 10.

4.1 Gebruikersgroephiërarchie

Een gebruikersgroep kan permissies erven van andere gebruikersgroepen, waardoor je een gebruikersgroephiërarchie kunt vormen. Een roostergroep kan bijvoorbeeld worden toegewezen aan een gebruikersgroep om ervoor te zorgen dat alle toegekende en geërfde permissies alleen gelden voor deze roostergroep en alle onderliggende roostergroepen.

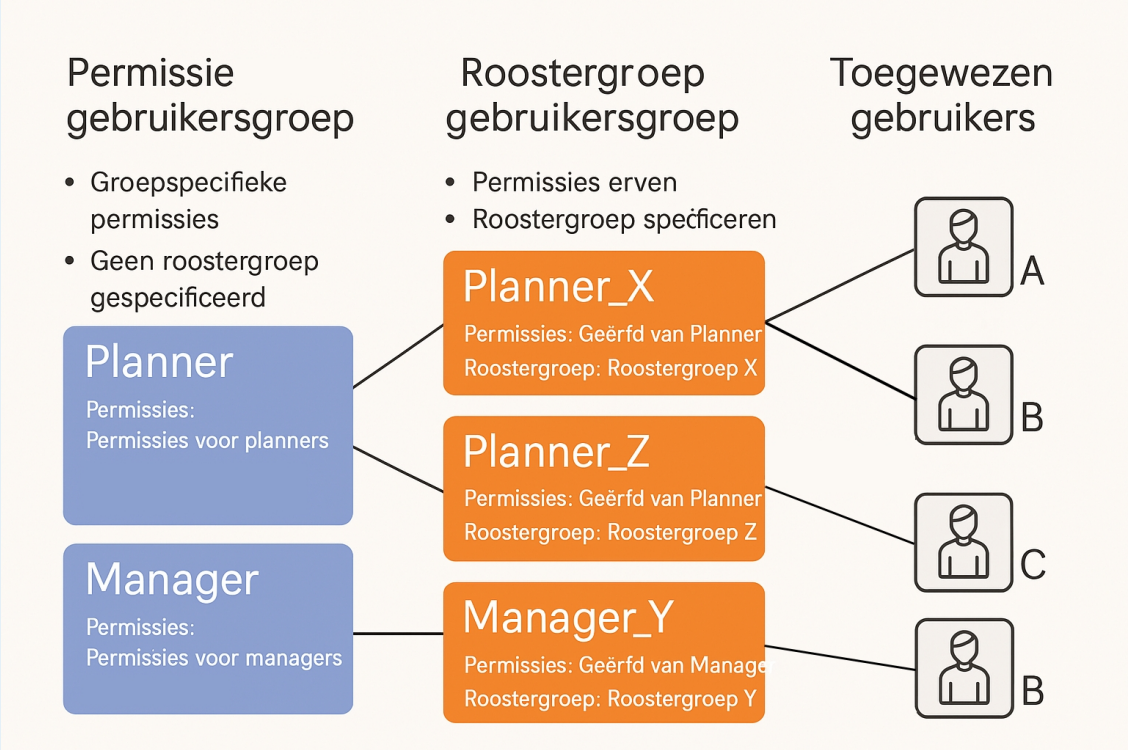
> Permissies die zijn geërfd van een andere gebruikersgroep, kunnen **niet** worden ontnomen. Alleen extra permissies kunnen worden toegekend.

Om te voorkomen dat voor elke gebruikersgroep permissies moeten worden ingeregeld, is het aan te raden om één gebruikersgroep aan te maken die uitsluitend wordt gebruikt voor permissies. We noemen dit een **Permissie gebruikersgroep**. Creëer vervolgens een gebruikersgroep die de permissies erft van de 'Permissie gebruikersgroep' en definieer vervolgens voor welke roostergroep (en) deze permissies gelden. We noemen dit een **Roostergroep gebruikersgroep**. Door zo te configureren is het makkelijker om permissies toe te kennen of te ontnemen.

Nadat de gebruikersgroepen zijn geconfigureerd, zullen gebruikers moeten worden toegekend aan één of meerdere gebruikersgroepen om gebruik te maken van de geconfigureerde permissies in de **ORTEC WS** applicaties.

Voorbeeld

Gebruikers A en B zijn planners voor roostergroep X, Gebruiker B is ook manager van roostergroep Y en gebruiker C is planner voor roostergroep Z. Dit kan het best geconfigureerd worden via de onderstaande configuratie:



4.2 Nieuwe gebruikersgroep aanmaken

Om permissies toe te kennen aan een specifieke groep gebruikers (zoals Planners, Managers, enz.), maak je een nieuwe gebruikersgroep aan.

1. Klik op de tab **Alle groepen**.
2. Klik met de rechtermuisknop in de **Gebruikersgroepen** sectie op **Nieuwe gebruikersgroep**.
3. Voer de naam van de nieuwe gebruikersgroep in.
4. Klik op **OK**.

4.3 Selecteer een roostergroep voor een gebruikersgroep

Specificeer een roostergroep voor een gebruikersgroep om permissies alleen aan die roostergroep toe te kennen.

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepsparameters**.

4. Klik met de rechtermuisknop op department (roostergroep) in de tabel en klik vervolgens op **Waarde zetten**.

   Wanneer er geen 'department' parameter is, maak er dan eerst een aan via de **Parameters** tab.

5. In de **Invoerparameters** sectie, typ je in het veld Naam de naam van de roostergroep die je wilt vinden en klik op **Zoek**.

   Deze actie voert een zoekactie uit in de namen van alle roostergroepen.

6. In de **Resultaten** sectie, selecteer je een roostergroep en klik op **OK**.

   Als een tussenliggende (lege) roostergroep is geselecteerd, zullen alle toegekende permissies worden toegekend aan de onderliggende roostergroepen.

4.4 Voeg een gebruiker aan een gebruikersgroep toe

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepsleden**.
4. Klik op **Gebruiker toevoegen**.
5. Eventueel voer je in de **Invoerparameters** sectie (een deel van) de naam van de gebruiker in.
6. Klik op **Zoek**. Alleen gebruikers die niet aan de geselecteerde gebruikersgroep zijn toegewezen, worden weergegeven.
7. Selecteer één of meerdere gebruikers (met de Ctrl-toets) om toe te voegen aan de geselecteerde gebruikersgroep.
8. Klik op **OK**.

   Het is ook mogelijk om de toewijzing van gebruikersgroepen te beheren vanuit Data beheer, dat toegankelijk is via het tabblad Gebruikersbeheer.

4.5 Een gebruiker uit de gebruikersgroep verwijderen

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepsleden**. In het rechterdeel, worden de toegekende gebruikers van de geselecteerde groep weergegeven.
4. Selecteer één of meer gebruikers (met de Ctrl-toets) om deze te verwijderen uit de gebruikersgroep.
5. Klik op de knop 'Verwijderen'.

   Het is ook mogelijk om de toewijzing van gebruikersgroepen te beheren vanuit Data beheer, dat toegankelijk is via het tabblad Gebruikersbeheer.

4.6 Hernoemen van een gebruikersgroep

1. Klik op de tab **Alle groepen**.
2. Klik met de rechtermuisknop op de betreffende groep en selecteer **Hernoem groep** in de **Gebruikersgroepen** sectie.
3. Vul de naam van de nieuwe gebruikersgroep in.
4. Klik op **OK**.

4.7 Verwijderen van een gebruikersgroep

Verwijder een gebruikersgroep alleen als er geen gebruikers aan zijn toegewezen.

1. Klik op de tab **Alle groepen**.
2. Klik met de rechtermuisknop op de betreffende groep en selecteer **Groep verwijderen** in de **Gebruikersgroepen** sectie.
3. Klik op **OK**.

4.8 Een back-up maken van alle gebruikersgroep permissies

Maak een back-up van de permissies die aan een gebruikersgroep zijn toegekend. De back-up kan gebruikt worden om permissies te importeren in andere omgevingen of als template voor een nieuwe gebruikersgroep in de huidige omgeving.

1. Klik op de tab **Alle groepen**.
2. Klik met de rechtermuisknop op de Gebruikersgroep in de sectie **Gebruikersgroepen** en klik dan op **Exporteer groep naar XML**.
3. Klik op **Opslaan** in het Download bestand venster en kies een locatie waar het bestand moet worden opgeslagen.
4. Klik op **Opslaan** en daarna **Sluiten**.

> Het back-up bestand van een gebruikersgroep bevat de permissies die direct gekoppeld zijn aan de gebruikersgroep (niet de geërfde permissies) en de geërfde gebruikersgroepen.

4.9 Herstel groepspermissies van de back-up

Een back-up van een gebruikersgroep kan worden teruggezet om de definitie van toegewezen permissies en de gebruikersgroep waarvan geërfd wordt te herstellen.

1. Klik op de tab **Alle groepen**.
2. Klik met de rechtermuisknop in de sectie **Gebruikersgroep** op **Importeer groepen**.
3. Klik op **Upload** in het Importeer groepen venster en selecteer het gebruikersgroep bestand dat geïmporteerd moet worden.
4. Om de momenteel toegekende permissies van de gebruikersgroep in te trekken, selecteer je het selectievakje Niet geïmporteerde permissies verwijderen.

5. Klik op **OK**, en daarna **Sluiten**.

De naam van de gebruikersgroep en de overname van de gebruikersgroep die in het back-upbestand zijn gedefinieerd, bepaalt naar welke gebruikersgroep de permissies worden geïmporteerd en van welke gebruikersgroepen de rechten worden overgenomen. In het geval dat de groep naam al bestaat zullen hierin gegevens worden geïmporteerd. Indien de naam niet bestaat, zal er een nieuwe groep worden aangemaakt.
Het bestand kan met elke XML editor of Notepad worden aangepast, zodat het in een andere omgeving kan worden ingelezen of kan worden gebruikt als een sjabloon voor een nieuwe gebruikersgroep.

```
<?xml version="1.0" encoding="utf-8" ?>
- <userGroups>
  - <userGroup name="Test_User_group_2">
    - <parentUserGroups>
        <parentUserGroup name="Test_User_group" />
      </parentUserGroups>
    - <userGroupPermissions>
        <userGroupPermission acObjectCode="gui.application.cwgs.CUASMANAGEMENTCONFIG" accessMode="Execute" condition="" />
      </userGroupPermissions>
    </userGroup>
  </userGroups>
```

5 Permissies

Permissies worden verleend aan gebruikersgroepen en niet aan individuele gebruikers. Gebruikers die dezelfde rechten delen, worden ingedeeld in gebruikersgroepen.

Zie "Beheer gebruikersgroepen" op pagina 5 voor meer informatie over gebruikersgroepen. Daar vindt je ook meer informatie over:

- Overgenomen permissies en hoe je er het beste mee kunt werken in een hiërarchie van gebruikersgroepen.
- Back-up maken en herstellen van rechten voor gebruikersgroepen.

Permissies zijn gegroepeerd in categorieën. Het merendeel van de categorieën komen overeen met de manier waarop de menu acties in de client-applicatie zijn gecategoriseerd.

- Het is mogelijk dat een permissie wordt gebruikt in meerdere applicaties, daarom kan een permissie worden getoond in meerdere categorieën.
- Sommige permissies zijn beschikbaar voor toekomstige doeleinden en worden nog niet gebruikt in de applicaties.
- Sommige categorieën zijn afgeschaft. Dit zijn **Employee Self Service**, **Manager Self Service**, **ORTEC WS voor Windows** en **Team Scheduling**.

Toegangsmodi

Elke permissie heeft betrekking op een zeker object en de toegang tot het object (toegangsmodus). Objecten kunnen toepassingen zijn (zoals de clienttoepassing, de systeemconfiguratie of de toepassing voor toegangscontrole), menuacties of gegevensentiteiten.

Voor het starten van applicaties en het gebruik van menu-acties is er de toegangsmodus **Uitvoeren**. Voor gegevens zijn er de volgende toegangsmodi:

- **Aanmaken**
  Deze modus geeft de gebruiker de mogelijkheid een data entiteit te maken.
- **Lezen**
  Met deze modus kan de gebruiker de details zien van een data entiteit.
- **Bewerken**
  Met deze modus kan de gebruiker de details van een data entiteit aanpassen.
- **Verwijderen**
  Met deze modus kan de gebruiker een data entiteit verwijderen.
- **Lijst**
  Deze modus stelt de gebruiker in staat om een lijst met data entiteiten te raadplegen.

5.1 Permissies verlenen

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepspermissies.**
4. Selecteer de permissie(s) in de sectie **Permissies** om deze toe te kennen.
5. Klik op **Toekennen** om de permissie toe te kennen aan de geselecteerde gebruikersgroep.

De achtergrondkleur geeft aan of een permissie is toegewezen:

- Groen voor toegewezen permissies.
- Licht groen voor geërfde permissies.
- Geen achtergrond kleur bij de permissies geeft aan dat deze niet zijn toegewezen en/of geërfd.

5.2 Permissies intrekken

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepspermissies.**
4. Selecteer de permissie(s) in de sectie **Permissies** om deze te ontnemen.
5. Klik op **Ontnemen** om de permissie(s) in te trekken voor de geselecteerde gebruikersgroep.

5.3 Filter op verleend

Als je alleen permissies wilt weergeven die zijn verleend, overgenomen of niet zijn verleend of overgeërfd, gebruik je de functie **Filteren op verleend**.

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepspermissies.**
4. Klik op de knop **Filteren op toegewezen** en selecteer de opties om te filteren:
   - **(Alles selecteren)**
     Toont alle permissies.
   - **Toegewezen**
     Toont alle permissies die direct zijn toegewezen aan de geselecteerde gebruikersgroep.
   - **Geërfd**
     Toon alle permissies die zijn geërfd van andere gebruikersgroepen.
   - **Niet toegewezen en niet geërfd**
     Toont de permissies die niet direct toegewezen en niet geërfd zijn aan de geselecteerde gebruikersgroep van andere gebruikersgroepen.
5. Klik op **OK** om het filter toe te passen op de weergegeven permissies.

5.4 Filteren op toegangsmodus

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepspermissies.**
4. Klik op de knop **Filteren op toegangsmodus** en selecteer de modus waarop gefilterd moet worden.

   Het filter wordt in realtime toegepast op de getoonde permissies, het is niet nodig om op OK te klikken om het filter toe te passen.

5.5 Vrije tekst filter

1. Klik op de tab **Alle groepen**.
2. Selecteer in de sectie **Gebruikersgroepen** de betreffende gebruikersgroep.
3. Klik op de tab **Groepspermissies.**
4. Typ in het vak **Filter...** in de rechterbovenhoek van de pagina een tekst om een vrije-tekstfilter toe te passen.

> Met deze actie wordt een volledige tekstzoekopdracht uitgevoerd in alle kolommen die in de resultatenlijst worden weergegeven, bijvoorbeeld Gebruikersnaam, Naam voluit, Omschrijving.

5.6 Access Control / Toegangscontrole

De Toegangscontrole categorie bevat permissies die relevant zijn voor de Access Control applicatie.

De volgende permissies zijn het vermelden waard:

- De **Toegangscontrole \ Acties** categorie bevat permissies die relevant zijn voor de Access Control applicatie.
- De **Toegangscontrole \ Authenticatie** categorie bevat momenteel alleen de permissie waarmee de gebruiker het wachtwoord van andere gebruikers kan wijzigen.

Permissies voor gebruikersbeheer in Access Control zijn te vinden in de categorie **Databeheer \ Gebruiker**.

5.7 Applicaties

De categorie **Applicaties** bevat de inlogrechten voor de meeste applicaties van **ORTEC WS**. De volgende applicatie permissies zijn beschikbaar:

- :en-US:CSCS
- Toegangscontrole
- Adhoc Planner (roostergroepen)
- Duale client
  De webapplicatie die in de **ORTEC WS WS for Windows** applicatie wordt gebruikt om webvensters beschikbaar te maken in de applicatie.
- Employee Self Service (deprecated)
- Employee Self Service App
- Manager Self Service (deprecated)
- ORTEC WS for Employees
- ORTEC WS for Managers
- ORTEC WS for Web
- Team Scheduler (roostergroepen)
- Team Scheduling (deprecated)
- Tijdregistratie

5.8 Databeheer

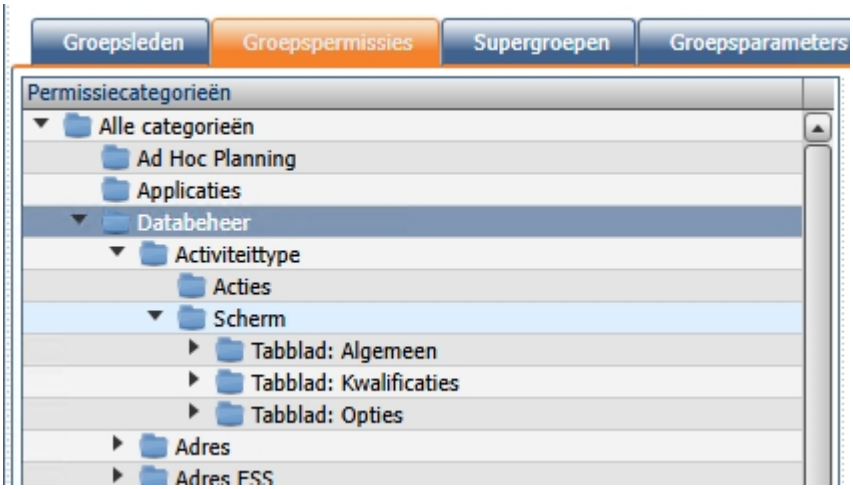
De categorie **Databeheer** bevat de permissies voor gegevensentiteiten. Wanneer een standaard gegevensinvoer venster is gebruikt in een applicatie, kunnen de relevante permissies in deze categorie worden gevonden.

Actie permissies

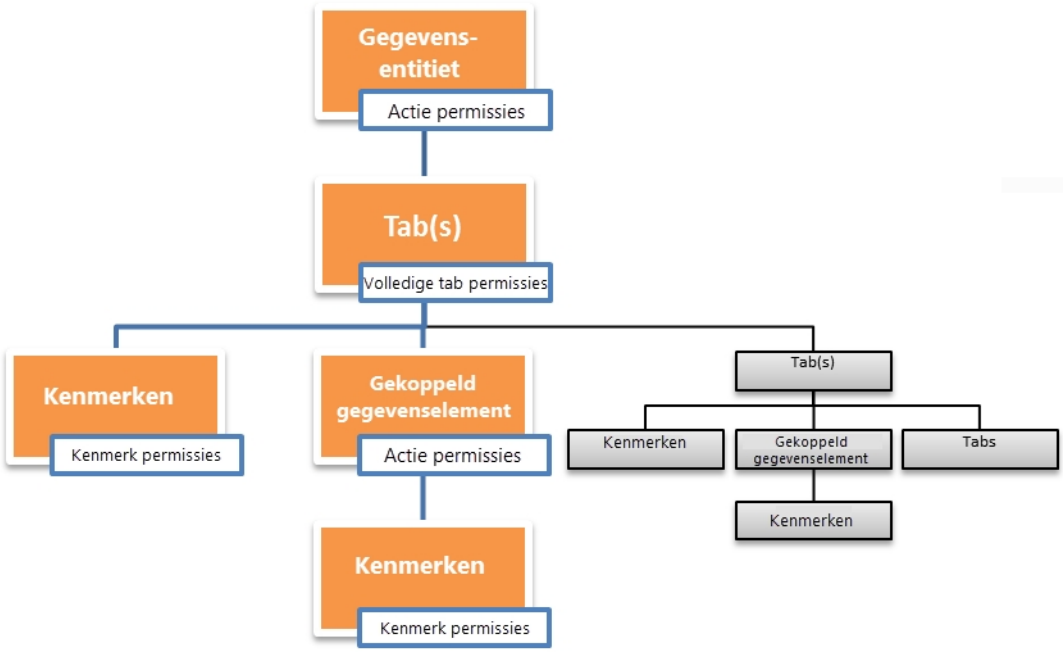
De actie permissies zijn te vinden in de categorieën **Databeheer \ <Gegevensentiteit> \ Acties**. Dit zijn meestal Aanmaken, Lezen, Bewerken, Verwijderen en Lijst. Voor meer informatie, zie "Permissies" op pagina 10.

Scherm permissies

Scherm permissies zijn voor de vensters van de gegevensentiteit, zoals het verbieden om een bepaalde eigenschap van de gegevensentiteit te wijzigen of om een heel tabblad weer te geven. De scherm permissies zijn te vinden in de categorieën **Databeheer \ <Gegevensentiteit> \ Scherm**.



De volgende permissiehiërarchie is van toepassing:



Permissies voor volledige tabbladen

De volgende permissies kunnen worden toegewezen aan de tab:

- **Aanmaken**
  Deze permissie is momenteel niet in gebruik in de applicaties. Zal worden verwijderd in een toekomstige versie.
- **Lezen**
  Deze permissie bepaalt of de tab zichtbaar is voor de gebruiker.
- **Bewerken**
  Deze permissie maakt het mogelijk voor de gebruiker om de informatie van deze en elke onderliggende tab te wijzigen.

Permissies voor kenmerken

De volgende permissies kunnen toegewezen worden aan de (gekoppelde) data entiteit eigenschappen die in de tab worden getoond.

- **Aanmaken**
  Deze permissie is vereist om een waarde voor een kenmerk toe te kennen wanneer een (gekoppeld) data entiteit is gecreëerd door een 'creëren actie'.
- **Lezen**
  Deze permissie is vereist om de waarde van een kenmerk te bekijken.

  > De leesrechten voor een kenmerk worden niet toegepast op de kolommen die worden weergegeven in het lijstoverzicht van een (gekoppelde) gegevensentiteit.

- **Bewerken**
  Deze permissie is vereist om de waarde van een kenmerk te kunnen wijzigen.

5.9 ORTEC WS Ad Hoc Planning

De categorie **ORTEC WS Ad Hoc Planning** bevat een permissie die relevant is voor de **ORTEC WS Ad Hoc Planning** applicatie.

5.10 ORTEC WS for Employees

De categorie **ORTEC WS fo Employees** bevat de permissies die relevant zijn voor de applicatie **ORTEC WS for Employees**.

De categorieën in de categorie **ORTEC WS for Employees** komen overeen met de verschillende werkplekken die beschikbaar zijn in **ORTEC WS for Employees**.

5.11 ORTEC WS for Managers

De categorie **ORTEC WS for Managers** bevat de permissies die relevant zijn voor de **ORTEC WS for Managers** applicatie.

De categorieën in de categorie **ORTEC WS for Managers** komen overeen met de verschillende werkplekken die beschikbaar zijn **inORTEC WS for Managers**.

5.12 ORTEC WS for Team Schedulers

De categorie **ORTEC WS for Team Schedulers** bevat permissies die relevant zijn voor de **ORTEC WS for Team Schedulers** applicatie.

5.13 ORTEC WS for Web

De categorie **ORTEC WS for Web** bevat permissies die relevant zijn voor de **ORTEC WS for Web-applicatie**.

5.14 Rapporten (Microsoft)

De categorie **Rapporten (Microsoft)** bevat permissies voor MS-rapporten voor het geval deze beschikbaar zijn in de verschillende applicaties.

> Permissies worden geregistreerd voor rapporten die worden geüpload in **ORTEC WS Systeemconfiguratie**, via de stap 'Upload MS Reporting' na installatie.

5.15 Tijdregistratie

De categorie **Tijdregistratie** bevat permissies die relevant zijn voor de module **Tijdregistratie**.

5.16 Gebruikersinterface

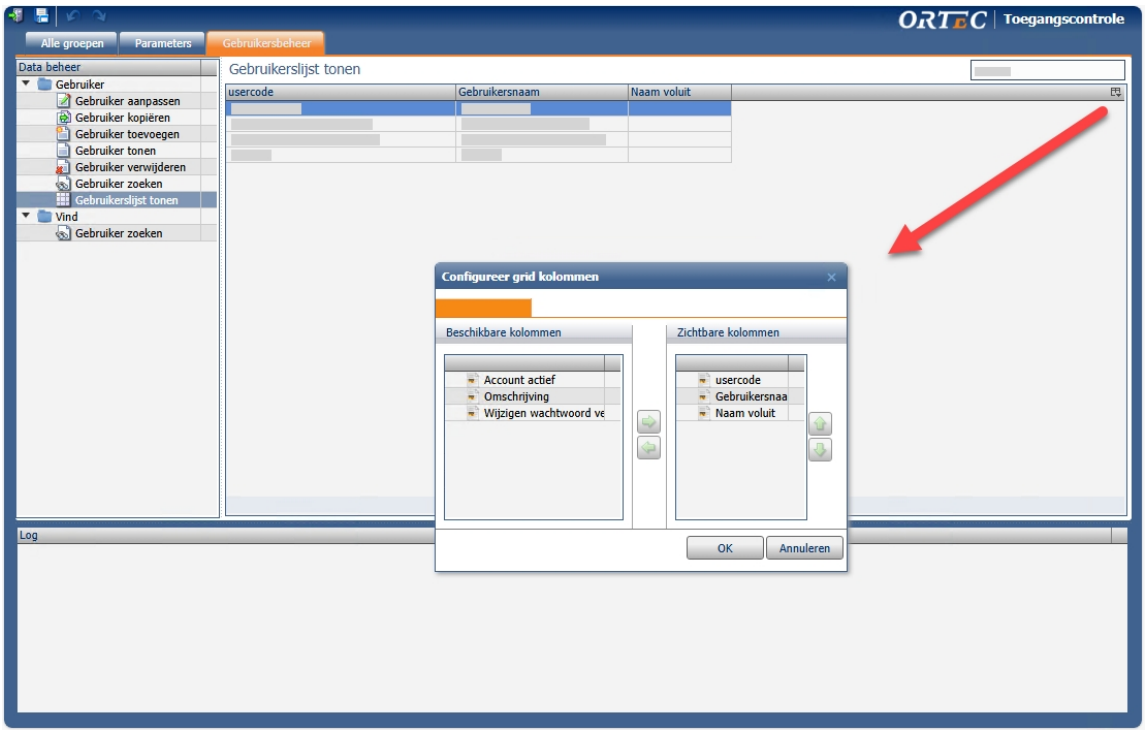
De categorie **Gebruikersinterface** bevat algemene permissies voor de gebruikersinterfaces van de applicaties.

De volgende permissies voor de web-based interfaces zijn het noemen waard:

- **Instellingen opslaan**
  Met deze permissie worden de laatst gebruikte gebruiker interface instellingen opgeslagen (bij het uitloggen). Deze instellingen zullen worden gebruikt als de gebruiker zich de volgende keer aanmeldt. Enkele voorbeelden van gebruikers interface-instellingen die worden opgeslagen zijn 'filters', 'laatst geopende tab', 'laatst geopende rooster', 'het formaat van vensters', 'handmatig geconfigureerde kolommen in een venster', 'de grootte en de positie van de pop-up vensters (zoals MS Reporting vensters)'.

  > Het kan zijn dat een applicatie zo is geïmplementeerd dat niet alle instellingen van de gebruikersinterface worden opgeslagen.

- **Configureer grid kolommen**
  Met deze permissie kan de gebruiker configureren welke kolommen zichtbaar zijn in de lijst met overzichten.



6 Verantwoording

De applicatie **Access Control** houdt bij welke delen van het systeem door welke gebruiker zijn geopend. Deze logboekgegevens zijn niet toegankelijk vanuit de applicatie maar uitsluitend vanuit de database tabellen. Deze tabellen zijn uitsluitend toegankelijk voor een gebruiker die toegang heeft tot de database en beschikt over voldoende basis SQL kennis.

> De logboekgegevens worden 366 dagen bewaard.

De **acLoginSession** tabel bevat informatie over de gebruikers die momenteel de applicatie gebruiken, de volgende informatie is beschikbaar:

- **id_user**
  De id van de gebruiker die de applicatie heeft gebruikt.

  > Informatie over de gebruiker (bijvoorbeeld de gebruikersnaam) is te vinden in de databasetabel **[gebruiker].**

- **created_datetime**
  De tijd en datum van wanneer de gebruiker is ingelogd in de applicatie.
- **application**
  De applicatie die de gebruiker gebruikt.

De **acFailedLoginLog** tabel bevat informatie over de mislukte inlog pogingen voor een applicatie. De volgende informatie is beschikbaar:

- **userName**
  De gebruiker die de applicatie heeft gebruikt.
- **LogDatetime**
  De datum en tijd van de gebeurtenis die voorkomt wanneer wordt ingelogd op een applicatie.
- **eventType**
  De volgende typen gebeurtenissen worden vastgelegd.
  - login: De gebruiker heeft ingelogd in de applicatie
  - logout: De gebruiker heeft uitgelogd uit de applicatie
  - Invalidate: De gebruiker is gedwongen om uit te loggen uit de applicatie.
  - expired:De gebruiker is gedurende een bepaalde periode (ongeveer 30 minuten) niet actief geweest

    > Dit geldt alleen voor de webapplicaties.

  - validationFailed: Een applicatie heeft geconstateerd dat de login sessie van de gebruiker niet meer geldig is.
- **eventData**
  Aanvullende informatie over de gebeurtenis. Het type informatie is afhankelijk van het type gebeurtenis.
- **application**
  De applicatie die de gebruiker gebruikt.

De **acFailedLoginLog** tabel bevat informatie over de mislukte inlog pogingen voor een applicatie. De volgende informatie is beschikbaar:

- **userName**
  De gebruiker die de applicatie heeft gebruikt.
- **LogDatetime**
  De datum en tijd van de gebeurtenis die voorkomt wanneer wordt ingelogd op een applicatie.
- **eventType**
  De volgende soorten van mislukte login pogingen worden vastgelegd.
  - UserDoesNotExist: De ingevoerde gebruikersnaam is niet bekend in de applicatie.
  - UserAccountDisabled: Het **Enabled** selectievakje is niet aangevinkt voor het data element gebruiker.
  - IncorrectPassword: Het ingevoerde wachtwoord is onjuist.
  - AuthenticationProviderNotSupported: De gebruikte authenticatie provider wordt niet meer ondersteund.
  - AccessDenied: De gebruiker heeft geen permissie om de applicatie te gebruiken.
  - PasswordChangeRequired: De gebruiker is verplicht zijn/haar wachtwoord te wijzigen.

    Deze gebeurtenis kan alleen plaatsvinden voor de authenticatieprovider van Comtec.

  - AnErrorHasOccured: Elke andere gebeurtenis die voorkomt tijdens een login poging.
- **eventData**
  Aanvullende informatie over de gebeurtenis. Het type informatie is afhankelijk van het type gebeurtenis.
- **application**
  De applicatie die de gebruiker gebruikt.

Contactgegevens

Neem voor meer informatie contact op met ORTEC, hetzij via jouw ORTEC contactpersoon, hetzij via de contactgegevens op www.ortec.com.

Onze website biedt casestudies, white papers, brochures, demo's en nog veel meer.