

ORTEC Workforce Scheduling 7

Implementierungshandbuch Access Control

August 2026 - Public

ORTEC

Copyright

© Copyright 2026 ORTEC.
Alle Rechte vorbehalten.

Kein Teil dieser Veröffentlichung darf ohne ausdrückliche Genehmigung von ORTEC oder einem mit ORTEC verbundenen Unternehmen in irgendeiner Form oder zu irgendeinem Zweck vervielfältigt oder übertragen werden.

ORTEC Workforce Scheduling 7 und andere in dieser Veröffentlichung verwendete Marken, Handelsnamen, Dienstleistungsmarken, Logos und sonstige Kennzeichen von ORTEC B.V. sind durch niederländisches Recht und andere anwendbare Rechtsvorschriften geschützt. Jede unbefugte Nutzung oder Vervielfältigung ist strengstens untersagt.

Alle anderen genannten Produkt- und Dienstleistungsnamen sind Marken der jeweiligen Unternehmen.

Inhaltsverzeichnis

1 Einführung 1

2 Zugangskontrolle 2

3 Erste Schritte 3

4 Benutzerverwaltung 4

5 Verwaltung von Benutzergruppen 7

6 Berechtigungen 12

6.1 Berechtigungen finden 14

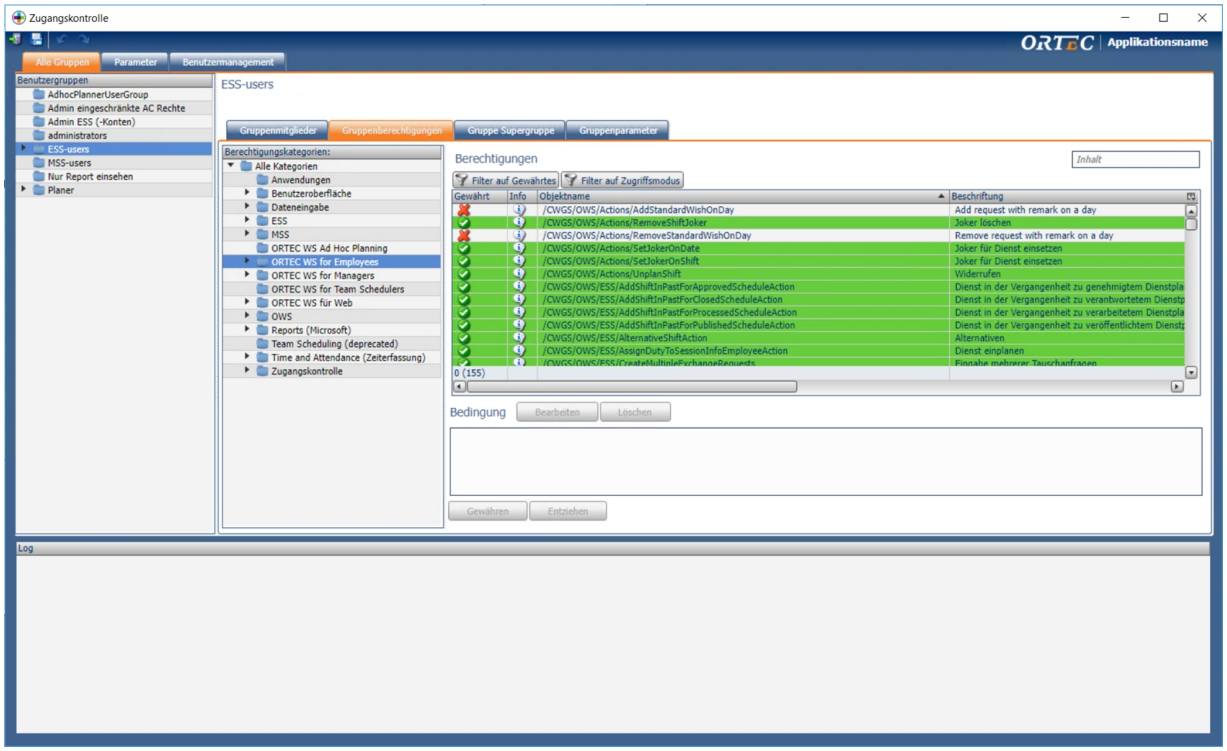
7 Rechenschaftspflicht 24

1 Einführung

Access Control ist die Anwendung für Benutzerauthentifizierung, Berechtigungen und Verantwortlichkeit in ORTEC Workforce Scheduling (ORTEC WS).

- **Authentifizierung**: zur Bestätigung der Identität eines Benutzers.
- **Berechtigungen**: um festzulegen, ob ein Benutzer Zugang zu bestimmten Teilen des Systems hat.
- **Rechenschaftspflicht**: Nachvollziehbarkeit, welche Teile des Systems von welchem Benutzer genutzt wurden.

Zur Verwaltung der Benutzerauthentifizierung und -berechtigungen steht eine gesicherte Webanwendung zur Verfügung.



Diese Dokumentation ist für Benutzer von Access Control gedacht. Bitte beachten Sie, dass möglicherweise nicht alle in diesem Handbuch beschriebenen Berechtigungen auf Ihr System zutreffen. Welche Funktionen in Ihrem System zur Verfügung stehen, hängt von der Systemkonfiguration für Ihr Unternehmen und den Ihnen erteilten Berechtigungen ab.

© 2026, Alle Rechte vorbehalten

2 Zugangskontrolle

ORTEC WS Benutzer benötigen Berechtigungen, um die verschiedenen Anwendungen zu nutzen. Unter Zugangskontrolle versteht man die Vergabe von Berechtigungen an Benutzer zur Nutzung bestimmter Anwendungen, zur Nutzung bestimmter Funktionen oder zum Lesen oder Bearbeiten von Informationen für eine bestimmte Dienstplangruppe.

Die Zugangskontrolle protokolliert auch die Anmeldesitzungen für jede Anwendung, diese Informationen können für Auditing-Zwecke verwendet werden.

Die Zutrittskontrolle bietet die folgenden Hauptfunktionen:

- Verwalten Sie Benutzer.
- Verwalten Sie Benutzergruppen.
- Konfigurieren Sie Berechtigungen für Benutzergruppen.



Es ist auch möglich, Berechtigungen für die Anwendung Access Control selbst zu vergeben.

© 2026, Alle Rechte vorbehalten

3 Erste Schritte

ORTEC WS Access Control ist über das Intranet Ihrer Organisation verfügbar. Sie benötigen die Webadresse, einen Benutzernamen und ein Passwort, bevor Sie die Anwendung nutzen können.

Verwendung

Einloggen

1. Rufen Sie die **Webadresse der Zugangskontrolle** auf.
2. Wählen Sie eine **Sprache**.
3. Geben Sie Ihren **Benutzernamen** ein.
4. Geben Sie Ihr **Passwort** ein.
5. Drücken Sie die Entertaste oder klicken Sie auf **Anmelden**.

> Bei der Vergabe eines Kennworts kann der Applikationsexperte die Option auswählen, dass das Kennwort bei der ersten Anmeldung geändert werden muss. In diesem Fall wird die Seite Passwort ändern angezeigt, nachdem Sie zum ersten Mal auf Anmelden geklickt haben.

Passwort ändern

Es könnte sein, dass Ihr Applikationsexperte Sie dazu zwingt, Ihr Kennwort bei der ersten Anmeldung zu ändern. Sie werden automatisch zur Seite 'Kennwort ändern' weitergeleitet, wenn Sie zum ersten Mal auf 'Anmelden' klicken. Sie können Ihr Passwort jederzeit ändern, indem Sie bei der Anmeldung **Passwort ändern** wählen.

1. Wählen Sie **Passwort ändern**, wenn Sie sich bei der Anwendung anmelden.
2. Geben Sie Ihr **aktuelles Passwort** ein.
3. Geben Sie ein **neues Passwort** ein.
4. Geben Sie das neue Kennwort erneut in das Feld **Neues Kennwort bestätigen** ein.
5. Klicken Sie auf **Übernehmen**, um Ihr Passwort zu ändern und die Anmeldung abzuschließen.

© 2026, Alle Rechte vorbehalten

4 Benutzerverwaltung

Um einem Benutzer Berechtigungen zu erteilen, muss zunächst ein Benutzer in der Anwendung Access Control erstellt werden.

Für einen Benutzer können der Benutzername, der vollständige Name und eine Beschreibung eingegeben werden. Es ist möglich, einen Benutzer daran zu hindern, sich bei einer beliebigen Anwendung anzumelden, indem ein Benutzerkonto deaktiviert wird.

Für jeden Benutzer kann die Authentifizierungsmethode angegeben werden, die verwendet wird, um zu bestätigen, dass das angegebene Passwort für den Benutzer gültig ist.

In der Benutzerverwaltung kann das Passwort eines Benutzers geändert werden oder ein Benutzer kann gezwungen werden, sein Passwort zu ändern.

Verwendung

Einen neuen Benutzer anlegen

1. Klicken Sie auf die Registerkarte **Benutzermanagement**.
2. Klicken Sie im Bereich **Dateimanagement** auf **Benutzer hinzufügen**.
3. Geben Sie auf der Registerkarte **Allgemein** Werte für die (erforderlichen) Felder ein.
4. Auf der Registerkarte **Benutzergruppen** weisen Sie dem Benutzer eine Benutzergruppe zu.

   Weitere Informationen über Benutzergruppen finden Sie unter "Verwaltung von Benutzergruppen" auf Seite 7.

5. Wenn alle erforderlichen Felder ausgefüllt sind, klicken Sie auf **OK** oder **Speichern**.

   Nicht ausgefüllte Pflichtfelder sind farblich markiert , die Registerkarten, bei denen nicht alle Pflichtfelder ausgefüllt sind, sind mit  gekennzeichnet.

Einen Benutzer suchen

1. Klicken Sie auf die Registerkarte **Benutzerverwaltung**.
2. Klicken Sie im Bereich Dateimanagement auf **Benutzer auflisten** .

© 2026, Alle Rechte vorbehalten

3. Finden Sie den Benutzer durch:
   - Geben Sie im Abschnitt **Benutzer suchen** den Text (z. B. einen Teil des Benutzernamens) ein, nach dem Sie suchen möchten, und klicken Sie dann auf **Suchen**.

     Diese Aktion führt eine Volltextsuche in allen in der Ergebnisliste angezeigten Spalten durch, z. B. Benutzername, vollständiger Name, Beschreibung usw.

   - Klicken Sie auf eine **Spaltenüberschrift**, um die Ergebnisse in der Tabelle zu sortieren.
   - Drücken Sie die **Umschalttaste** und klicken Sie dann auf eine **Spaltenüberschrift**, um die Ergebnisse auf der Grundlage der ausgewählten Spalte zu gruppieren.

Deaktivieren eines Benutzers

Die Deaktivierung eines Benutzers verhindert, dass er sich bei einer Anwendung anmeldet.

1. Klicken Sie auf die Registerkarte **Benutzerverwaltung**.
2. Klicken Sie im Bereich Dateimanagement auf **Benutzer auflisten** .
3. Wählen Sie im Abschnitt **Ergebnisse** einen Benutzer aus.
4. Klicken Sie mit der rechten Maustaste auf den ausgewählten Benutzer, und klicken Sie dann auf **Benutzer bearbeiten** .
5. Deaktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Konto aktiviert**.
6. klicken Sie auf **OK** oder **Speichern**.

Passwortbeschränkungen für die Comtec-Authentifizierungsmethode festlegen

1. Starten Sie auf dem **Application Server** die **System Configuration**.
2. Geben Sie Ihren **Benutzernamen** ein.
3. Geben Sie Ihr **Passwort** ein.
4. Drücken Sie die **Eingabetaste** oder klicken Sie auf **OK**.
5. Klicken Sie auf der Registerkarte **Configuration** im Abschnitt **Settings Management** auf **Settings Manager**.
6. Wählen Sie in der Kategorie **CUASFW** die Option **ComtecAuthentication**.
   - Die Mindestlänge eines Passworts kann mit der Einstellung MinimumPasswordLength festgelegt werden (Standardwert 8).
   - Wenn ein Benutzer sein Passwort ändern soll, weil sein aktuelles Passwort kürzer als die Mindestlänge ist, kann die Einstellung ForcePasswordChangeIfTooShort (Standard: True) aktiviert werden.

© 2026, Alle Rechte vorbehalten

Herunterladen der Zugangsdaten (Credential Files) für einen Benutzer

Zugangsdaten können von einer ORTEC WS-Anwendung verwendet werden, um sich gegenüber einer anderen ORTEC WS-Anwendung zu identifizieren.

1. Klicken Sie auf die Registerkarte **Benutzerverwaltung**.
2. Suchen Sie den Benutzer, für den Sie die Zugangsdaten herunterladen möchten
   - Klicken Sie im Abschnitt Dateimanagement auf **Benutzer auflisten**  oder
   - Geben Sie im Abschnitt **Benutzer suchen** den Text ein, nach dem Sie suchen möchten, und klicken Sie dann auf **Suchen**.
     Mit dieser Aktion wird eine Volltextsuche in allen in der Ergebnisliste angezeigten Spalten durchgeführt.
3. Wählen Sie im Abschnitt **Ergebnisse** einen Benutzer aus.
4. Klicken Sie mit der rechten Maustaste auf den ausgewählten Benutzer, und klicken Sie dann auf **Zugangsdaten herunterladen** .
5. Geben Sie im Fenster 'Zugangsdaten herunterladen' das **Passwort** des Benutzers ein und klicken Sie auf **OK**.
6. Klicken Sie im Fenster zum Herunterladen der Datei auf **Speichern** und geben Sie einen **Speicherort** für die Datei an.
7. Klicken Sie auf **Speichern** und dann auf **Schließen**.

© 2026, Alle Rechte vorbehalten

5 Verwaltung von Benutzergruppen

Benutzer, die dieselben Berechtigungen haben, können in Benutzergruppen zusammengefasst werden. Daher müssen die Berechtigungen für Benutzergruppen und nicht für einzelne Benutzer erteilt werden.

Außerdem kann eine Benutzergruppe Berechtigungen von anderen Benutzergruppen erben. Mit dieser Funktionalität ist es möglich, eine Benutzergruppenhierarchie zu erstellen.

Von einer anderen Benutzergruppe geerbte Berechtigungen können **nicht** entzogen werden. Es können nur zusätzliche Genehmigungen erteilt werden.

Eine Dienstplangruppe kann einer Benutzergruppe zugewiesen werden, um anzugeben, dass die gewährten oder geerbten Berechtigungen in dieser Benutzergruppe nur für die ausgewählte Dienstplangruppe und die zu dieser Dienstplangruppe gehörenden Dienstplangruppen gelten.

Benutzergruppen 'Berechtigungen' und 'Dienstplangruppe'

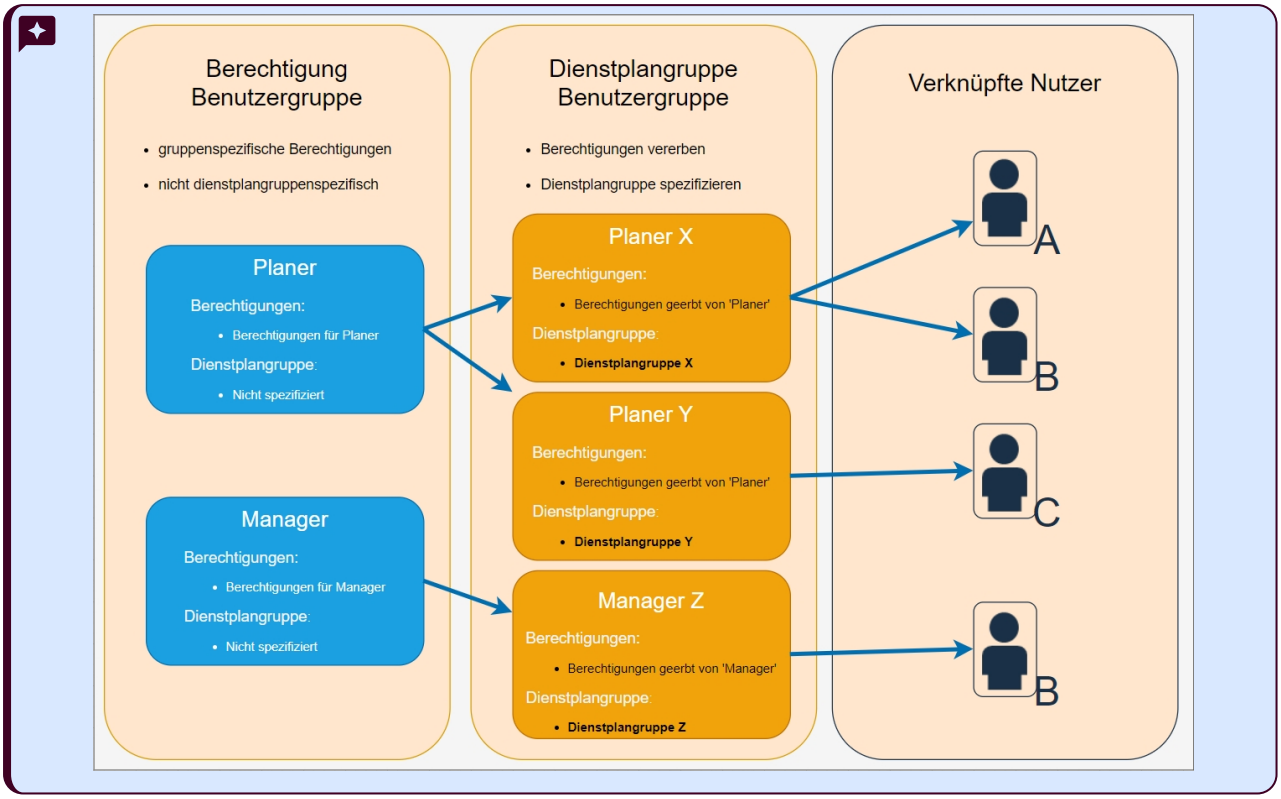
Um zu vermeiden, dass allen Gruppen Berechtigungen zugewiesen werden müssen, empfiehlt es sich, eine Benutzergruppe zu verwenden, die ausschließlich für die Erteilung von Berechtigungen zuständig ist, wir nennen dies eine 'Berechtigungs-Benutzergruppe'. Erstellen Sie dann eine oder mehrere Benutzergruppen, die die Berechtigungen der Benutzergruppe 'Berechtigung' erben, und geben Sie die Dienstplangruppe an, für die sie gelten sollen; wir nennen dies eine 'Dienstplangruppen-Benutzergruppe'. Mit dieser Konfiguration ist es einfacher, Berechtigungen zu erteilen oder zu entziehen.

Nachdem die Benutzergruppen konfiguriert wurden, werden die Benutzer einer oder mehreren Benutzergruppen zugewiesen, um die konfigurierten Berechtigungen in ORTEC WS-Anwendungen zu erhalten.

Beispiel

Die Benutzer A und B sind Planer für die Dienstplangruppe X, Benutzer B ist auch Manager der Dienstplangruppe Y und Benutzer C ist Planer für die Dienstplangruppe Z. Dies lässt sich am besten mit der folgenden Konfiguration konfigurieren:

© 2026, Alle Rechte vorbehalten



Nachdem die Berechtigungen einer Benutzergruppe wie gewünscht konfiguriert wurden, ist es möglich, die einer Benutzergruppe gewährten Berechtigungen zu sichern. Diese Sicherung kann zur Wiederherstellung von Berechtigungen in anderen Umgebungen oder als Vorlage für eine neue Benutzergruppe in der aktuellen Umgebung verwendet werden.

Verwendung

Erstellen Sie eine neue Benutzergruppe

Bei der Vergabe von Berechtigungen für eine bestimmte Benutzergruppe (z.B. Planer, Manager, etc.) muss eine neue Benutzergruppe in Access Control angelegt werden.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Klicken Sie im Abschnitt **Benutzergruppen** mit der rechten Maustaste und dann auf **Neue Benutzergruppe erstellen**.
3. Geben Sie den Namen der neuen Benutzergruppe ein.
4. Klicken Sie auf **OK**.

© 2026, Alle Rechte vorbehalten

Festlegen einer Dienstplangruppe für eine Benutzergruppe

Für eine Benutzergruppe kann eine Dienstplangruppe angegeben werden, um festzulegen, für welche Dienstplangruppen die Berechtigungen erteilt werden.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt **Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie mit der rechten Maustaste auf den Gruppenparameter der Dienstplangruppe im Abschnitt Gruppenparameter und dann auf **Wert einstellen**.
4. Geben Sie im Abschnitt **Parameter eingeben** den Namen der Dienstplangruppe ein, nach der Sie suchen möchten, und klicken Sie dann auf **Suche**.

   > Mit dieser Aktion wird eine Volltextsuche in den Namen aller Dienstplangruppen durchgeführt.

5. Wählen Sie im Abschnitt **Ergebnisse** eine Dienstplangruppe aus und klicken Sie auf **OK**.

   > Wenn eine Dienstplangruppe ausgewählt wird, die keine Untergruppe ist, werden alle für die Benutzergruppe festgelegten Berechtigungen allen Untergruppen gewährt.

Hinzufügen eines Benutzers zu einer Benutzergruppe

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt **Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenmitglieder**.
4. Optional können Sie im Abschnitt **Parameter** den Benutzernamen (oder einen Teil davon) eingeben
5. Klicken Sie auf **Suche**. Nur Benutzer, die nicht der ausgewählten Benutzergruppe zugeordnet sind, werden unten aufgeführt.
6. Wählen Sie einen oder mehrere Benutzer aus, die der ausgewählten Benutzergruppe zugeordnet werden sollen.
7. Klicken Sie auf **Benutzer auswählen** , um den/die ausgewählten Benutzer zu der ausgewählten Benutzergruppe hinzuzufügen. Die zugewiesenen Benutzer werden im rechten Fensterbereich aufgelistet.

   > Es ist auch möglich, Benutzergruppenzuordnungen über das Dateneingabefenster des Dateimanagement zu pflegen, das über die Registerkarte **Benutzermanagement** zugänglich ist.

© 2026, Alle Rechte vorbehalten

Entfernen eines Benutzers aus einer Benutzergruppe

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im **Abschnitt Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenmitglieder**. Im rechten Fensterbereich werden die Benutzer aufgelistet, die der ausgewählten Benutzergruppe zugeordnet sind.
4. Wählen Sie einen oder mehrere Benutzer aus, die aus der Benutzergruppe entfernt werden sollen.
5. Klicken Sie auf **Benutzer entfernen** , um den/die ausgewählten Benutzer aus der Benutzergruppe zu entfernen.

> Es ist auch möglich, Benutzergruppenzuordnungen über das Dateneingabefenster des Dateimanagement zu pflegen, das über die Registerkarte **Benutzermanagement** zugänglich ist.

Umbenennen einer Benutzergruppe

Wenn eine Benutzergruppe einen falschen Namen hat, kann die Benutzergruppe umbenannt werden.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Klicken Sie im Abschnitt **Benutzergruppen** mit der rechten Maustaste auf die Benutzergruppe, und klicken Sie dann auf **Gruppe umbenennen**.
3. Geben Sie den neuen Namen der neuen Benutzergruppe ein.
4. Klicken Sie auf **OK**.

Löschen einer Benutzergruppe

Wenn eine Benutzergruppe nicht mehr verwendet wird, kann die Benutzergruppe gelöscht werden, allerdings nur, wenn der Benutzergruppe keine Benutzer mehr zugeordnet sind.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Klicken Sie mit der rechten Maustaste auf die ausgewählte Benutzergruppe im Abschnitt **Benutzergruppen** und dann auf **Benutzergruppe löschen**.
3. Klicken Sie in dem angezeigten Bestätigungsfenster auf **OK**, um das Löschen der Benutzergruppe zu bestätigen.

Erstellen einer Sicherungskopie der Benutzergruppenberechtigungen

Nachdem die Berechtigungen einer Benutzergruppe wie gewünscht konfiguriert wurden, ist es möglich, die einer Benutzergruppe gewährten Berechtigungen zu sichern.

© 2026, Alle Rechte vorbehalten

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Klicken Sie im Abschnitt **Benutzergruppen** mit der rechten Maustaste auf die Benutzergruppe, und klicken Sie dann auf **Gruppe nach XML exportieren**.
3. Klicken Sie im Fenster zum Herunterladen der Datei auf **Speichern** und geben Sie einen Speicherort für die Datei an.
4. Klicken Sie auf **Speichern** und dann auf **Schließen**.

> Die Sicherungsdatei für eine Benutzergruppe enthält die Berechtigungen, die der Benutzergruppe direkt gewährt werden (nicht die geerbten Berechtigungen) und die Benutzergruppen, von denen sie erbt.

Sicherung der Benutzergruppenberechtigungen wiederherstellen

Eine Sicherungskopie einer Benutzergruppe kann importiert werden, um die Definition der gewährten Berechtigungen und der Benutzergruppe, von der sie abstammt, in der Datei wiederherzustellen.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Klicken Sie im Abschnitt **Benutzergruppen** mit der rechten Maustaste und dann auf **Gruppen importieren**.
3. Klicken Sie im Fenster Gruppen importieren auf **Upload** und wählen Sie die zu importierende Benutzergruppendatei aus.
4. Aktivieren Sie das Kontrollkästchen **Nicht importierte Berechtigungen entfernen**, wenn der Benutzergruppe derzeit gewährte Berechtigungen entzogen werden sollen.
5. Klicken Sie auf **OK** und dann auf **Schließen**.

> Der in der Sicherungsdatei definierte Benutzergruppenname und die Benutzergruppenvererbung legen fest, in welche Benutzergruppe die Berechtigungen importiert werden und von welchen Benutzergruppen sie geerbt werden. Falls der Name der Benutzergruppe bereits existiert, wird diese Benutzergruppe mit den importierten Daten angepasst. Andernfalls wird eine neue Benutzergruppe erstellt.
> Die Datei kann in Editoren wie Notepad oder einem anderen XML-Editor bearbeitet werden, um eine Datei zu erhalten, die in eine andere Umgebung oder als Vorlage für eine neue Benutzergruppe importiert werden kann.

```
<?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>
```


© 2026, Alle Rechte vorbehalten

6 Berechtigungen

Berechtigungen werden für Benutzergruppen erteilt, nicht für einzelne Benutzer.

Nachdem die Berechtigungen einer Benutzergruppe wie gewünscht konfiguriert wurden, ist es möglich, die einer Benutzergruppe gewährten Berechtigungen zu sichern. Diese Sicherung kann zur Wiederherstellung von Berechtigungen in anderen Umgebungen oder als Vorlage für eine neue Benutzergruppe in der aktuellen Umgebung verwendet werden.

Verwendung

Die Hintergrundfarbe zeigt an, ob eine Genehmigung erteilt wurde:

- Grün für erteilte Berechtigungen.
- Helleres Grün für geerbte Berechtigungen.
- Keine Hintergrundfarbe für Berechtigungen, die weder erteilt noch geerbt werden.

Erteilen einer Berechtigung für eine Benutzergruppe

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt **Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenberechtigungen**.
4. Wählen Sie im Abschnitt **Berechtigungen** die Berechtigung(en) aus, die erteilt werden soll(en).

   > Weitere Informationen zum Auffinden von Berechtigungen finden Sie unter "Berechtigungen finden" auf Seite 14.

5. Klicken Sie auf **Gewähren**, um die Berechtigung für die ausgewählte Benutzergruppe zu gewähren.

Entziehen einer Berechtigung für eine Benutzergruppe

Wenn eine Berechtigung erteilt wurde, aber die Benutzergruppe diese Berechtigung nicht mehr haben darf, kann sie entzogen werden.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt **Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenberechtigungen**.
4. Wählen Sie im Abschnitt **Berechtigungen** die zu entziehende(n) Berechtigung(en) aus.

© 2026, Alle Rechte vorbehalten

5. Klicken Sie auf **Entziehen**, um der ausgewählten Benutzergruppe die Berechtigung zu entziehen.

Filterberechtigungen für eine Benutzergruppe

Um nur die gewährten, geerbten oder weder gewährten noch geerbten Berechtigungen anzuzeigen, kann die Filterfunktion verwendet werden.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt **Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenberechtigungen**.
4. Klicken Sie auf den Button **Filter auf Gewährtes** und wählen Sie die zu filternden Optionen aus:
   - **(Alle auswählen)**
     Zeigt alle Berechtigungen an.
   - **Gewährt**
     Zeigt die Berechtigungen an, die der ausgewählten Benutzergruppe direkt gewährt werden.
   - **Geerbt**
     Zeigt die Berechtigungen, die von anderen Benutzergruppen geerbt werden.
   - **Weder gewährt noch geerbt**
     Zeigt die Berechtigungen an, die der ausgewählten Benutzergruppe weder direkt gewährt noch von anderen Benutzergruppen geerbt werden.
5. Klicken Sie auf **OK**, um den Filter auf die angezeigten Berechtigungen anzuwenden.

Erstellen einer Sicherungskopie der Benutzergruppenberechtigungen

Nachdem die Berechtigungen einer Benutzergruppe wie gewünscht konfiguriert wurden, ist es möglich, die einer Benutzergruppe gewährten Berechtigungen zu sichern.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Klicken Sie im Abschnitt **Benutzergruppen** mit der rechten Maustaste auf die Benutzergruppe, und klicken Sie dann auf **Gruppe nach XML exportieren**.
3. Klicken Sie im Fenster zum Herunterladen der Datei auf **Speichern** und geben Sie einen Speicherort für die Datei an.
4. Klicken Sie auf **Speichern** und dann auf **Schließen**.

> Die Sicherungsdatei für eine Benutzergruppe enthält die Berechtigungen, die der Benutzergruppe direkt gewährt werden (nicht die geerbten Berechtigungen) und die Benutzergruppen, von denen sie erbt.

© 2026, Alle Rechte vorbehalten

Sicherung der Benutzergruppenberechtigungen wiederherstellen

Eine Sicherungskopie einer Benutzergruppe kann importiert werden, um die Definition der gewährten Berechtigungen und der Benutzergruppe, von der sie erbt, in der Datei wiederherzustellen.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Klicken Sie im Abschnitt **Benutzergruppen** mit der rechten Maustaste und dann auf **Gruppen importieren**.
3. Klicken Sie im Fenster Gruppen importieren auf **Upload** und wählen Sie die zu importierende Benutzergruppendatei aus.
4. Aktivieren Sie das Kontrollkästchen **Nicht importierte Berechtigungen entfernen**, wenn der Benutzergruppe derzeit gewährte Berechtigungen entzogen werden sollen.
5. Klicken Sie auf **OK** und dann auf **Schließen**.

Der in der Sicherungsdatei definierte Benutzergruppenname und die Benutzergruppenvererbung legen fest, in welche Benutzergruppe die Berechtigungen importiert werden und von welchen Benutzergruppen sie geerbt werden. Falls der Name der Benutzergruppe bereits existiert, wird diese Benutzergruppe mit den importierten Daten angepasst, andernfalls wird eine neue Benutzergruppe angelegt.
Die Datei kann in Editoren wie Notepad oder einem anderen XML-Editor bearbeitet werden, um eine Datei zu erhalten, die in eine andere Umgebung oder als Vorlage für eine neue Benutzergruppe importiert werden kann.

```
<?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>
```

6.1 Berechtigungen finden

Jede Berechtigung bezieht sich auf ein bestimmtes Objekt und auf die Art des Zugriffs darauf (Zugriffsmodus).

Objekte

- Anwendungen (wie die Client-Anwendung, die System Configuration oder die Anwendung Access Control)
- Menüaktionen in Anwendungen
- Dateneinheiten

© 2026, Alle Rechte vorbehalten

Zugriffsmodus

Zum Starten von Anwendungen und zur Verwendung von Menüaktionen gibt es den Zugriffsmodus:

Ausführen

In diesem Modus kann der Benutzer eine Anwendung starten oder eine Menüaktion verwenden.

Für Dateneinheiten gibt es die folgenden Zugriffsmodi:

Erstellen

Dieser Modus ermöglicht es dem Benutzer, eine Dateneinheit zu erstellen.

Lesen

Dieser Modus ermöglicht es dem Benutzer, die Details einer Dateneinheit zu sehen.

Update

Dieser Modus ermöglicht es dem Benutzer, die Details einer Dateneinheit zu aktualisieren.

Löschen

Dieser Modus ermöglicht es dem Benutzer, eine Dateneinheit zu löschen.

Auflisten

Dieser Modus ermöglicht es dem Benutzer, eine Listenübersicht der Dateneinheiten abzurufen.

Berechtigungen können durch die Suche nach Teilen des Berechtigungsnamens oder nach anderen in den Berechtigungsspalten angezeigten Informationen gefunden werden. Mit der Filterfunktion können Sie herausfinden, welche Berechtigungen der ausgewählten Benutzergruppe gewährt, geerbt oder weder gewährt noch geerbt werden.

Die Berechtigungen sind in verschiedene Kategorien eingeteilt. Die meisten Kategorien entsprechen der Einteilung der Menüaktionen in der Client-Anwendung. In den folgenden Abschnitten werden die bemerkenswerten Kategorien beschrieben.



Es ist möglich, dass eine Berechtigung in mehreren Anwendungen verwendet wird, daher kann eine Berechtigung in mehreren Kategorien angezeigt werden.
In Access Control sind zahlreiche Berechtigungen für zukünftige Zwecke verfügbar. Sie werden in den Anwendungen noch nicht geprüft.

© 2026, Alle Rechte vorbehalten

Verwendung

Filter auf Zugriffsmodus

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt **Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenberechtigungen**.
4. Klicken Sie auf den Button **Filter auf Zugriffsmodus** und wählen Sie die zu filternden Zugriffsmodi aus.

> Der Filter wird in Echtzeit auf die angezeigten Berechtigungen angewandt, es ist nicht erforderlich, auf OK zu klicken, um den Filter anzuwenden.

Freitextfilter

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt **Benutzergruppen** die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenberechtigungen**.
4. Geben Sie im Feld **Inhalt** oben rechts auf der Seite einen Text ein, um einen Freitextfilter anzuwenden.

> Diese Aktion führt eine Volltextsuche in allen in der Ergebnisliste angezeigten Spalten durch, z. B. Benutzername, vollständiger Name, Beschreibung.

Erteilte Berechtigungen für eine Benutzergruppefiltern

Um nur die gewährten, geerbten oder weder gewährten noch geerbten Berechtigungen anzuzeigen, kann die Filterfunktion verwendet werden.

1. Klicken Sie auf die Registerkarte **Alle Gruppen**.
2. Wählen Sie im Abschnitt Benutzergruppen die Benutzergruppe aus.
3. Klicken Sie auf die Registerkarte **Gruppenberechtigungen**.
4. Klicken Sie auf den Button **Filter auf Gewährtes** und wählen Sie die zu filternden Optionen aus:
   - **Alle auswählen**
     Zeigt alle Berechtigungen an.
   - **Gewährt**
     Zeigt die Berechtigungen an, die der ausgewählten Benutzergruppe direkt gewährt werden.
   - **Geerbt**
     Zeigt die Berechtigungen, die von anderen Benutzergruppen geerbt werden.
   - **weder gewährt noch geerbt**
     Zeigt die Berechtigungen an, die der ausgewählten Benutzergruppe

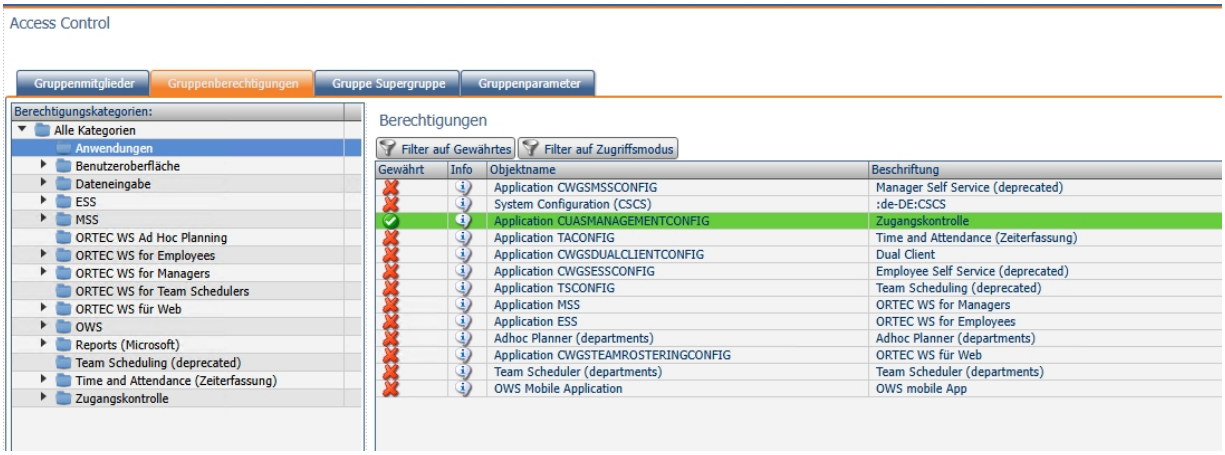
© 2026, Alle Rechte vorbehalten

weder direkt gewährt noch von anderen Benutzergruppen geerbt werden.

5. Klicken Sie auf **OK**, um den Filter auf die angezeigten Berechtigungen anzuwenden.

6.1.1 Anwendungen

Die Kategorie Anwendungen enthält die Anmeldeberechtigungen für die meisten Anwendungen von ORTEC WS. Die folgenden Anwendungsberechtigungen sind verfügbar:



6.1.2 Benutzeroberfläche

Die Kategorie Benutzeroberfläche enthält allgemeine Berechtigungen für die Benutzeroberflächen der Anwendungen.

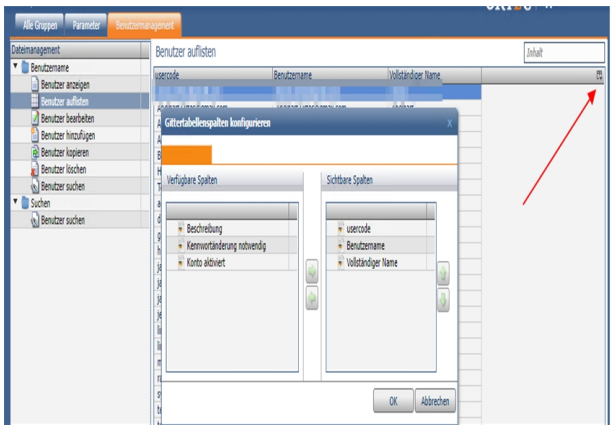
Für die webbasierten Anwendungen sind die folgenden Berechtigungen erwähnenswert:

- **Einstellungen speichern**
  Mit dieser Berechtigung werden die zuletzt verwendeten Einstellungen der Benutzeroberfläche gespeichert (beim Abmelden), so dass sie bei der nächsten Anmeldung des Benutzers verwendet werden. Einige Beispiele für Einstellungen der Benutzeroberfläche, die gespeichert werden, sind 'Filter', 'Letzte aktive Registerkarte', 'Zuletzt geöffneter Dienstplan', 'Größenänderung von Zellen', 'Manuell konfigurierte Spalten', 'Größe und Position von Popup-Fenstern (wie MS Reporting-Fenster)'

© 2026, Alle Rechte vorbehalten

Es ist möglich, dass eine Anwendung so implementiert ist, dass nicht alle Einstellungen der Benutzeroberfläche gespeichert werden (z. B. ORTEC WS Employee Self Service öffnet immer auf der Startseite).

- **Dienstplan > Dienstplanspalten konfigurieren**
  Mit diesem Recht kann der Benutzer konfigurieren, welche Spalten in den Listenübersichten sichtbar sind.



6.1.3 Dateneingabe

Die Kategorie 'Dateneingabe' enthält die Berechtigungen für Dateneinheiten. Wenn in einer Anwendung ein Standarddateneingabefenster verwendet wird, sind die entsprechenden Berechtigungen in dieser Kategorie zu finden.

Handlungsberechtigungen

Für jede Dateneinheit gibt es einige Hauptberechtigungen, wie z.B. das Erstellen, Anzeigen oder Löschen der Dateneinheit. Diese Berechtigungen werden als Aktionsberechtigungen bezeichnet und sind in der Kategorie Dateneingabe \ <Datenentität> \ Aktionen mit den folgenden Zugriffsmodi zu finden:

Erstellen

Ermöglicht es dem Benutzer, eine neue Instanz der Dateneinheit zu erstellen. Bei einigen Datenentitäten ermöglicht diese Berechtigung auch die Erstellung einer Kopie einer Datenentität.

Lesen

Ermöglicht es dem Benutzer, die Details einer Dateneinheit zu sehen.

Update

Ermöglicht es dem Benutzer, die Details einer Dateneinheit zu aktualisieren.

© 2026, Alle Rechte vorbehalten

Löschen

Ermöglicht es dem Benutzer, eine Dateneinheit zu löschen.

Auflisten

Ermöglicht es dem Benutzer, eine Listenübersicht über die Dateneinheiten abzurufen.

Forumlarberechtigungen

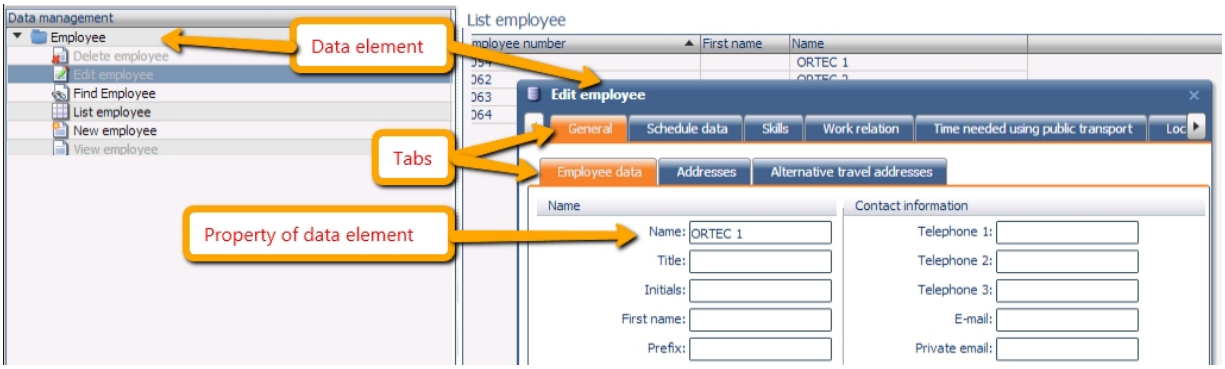
In Access Control sind auch Berechtigungen für das Datenentitätsfenster selbst verfügbar, z. B. das Verbot, eine bestimmte Eigenschaft der Datenentität zu ändern oder eine ganze Registerkarte anzuzeigen. Diese Berechtigungen werden als Formularberechtigungen bezeichnet und befinden sich in der Kategorie Dateneingabe \ Dienst \ Formular.

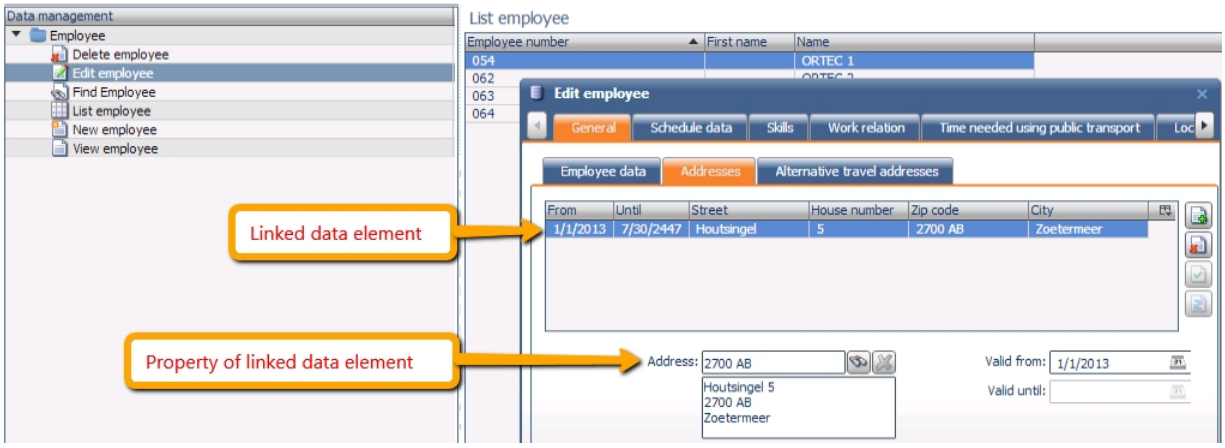
> Formularberechtigungen haben in den meisten Formularen in ORTEC WS for Windows noch keine Auswirkungen. Sie sind in Access Control für zukünftige Zwecke verfügbar.

Ein Dateneingabefenster für eine Dateneinheit (wie einen Benutzer, eine Adresse oder eine Dienst) besteht aus den folgenden Teilen:

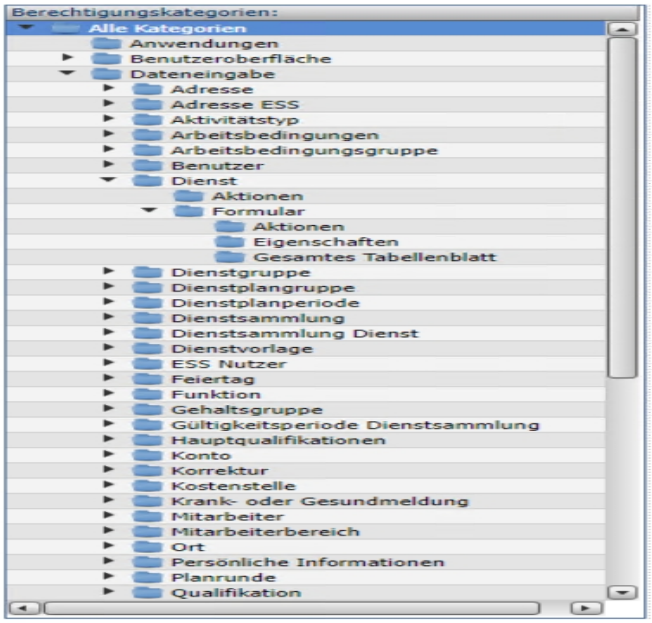
- **Registerkarte**
  Eine Registerkarte kann eines (oder eine Kombination aus) der folgenden Elemente enthalten
  - **Eigenschaften der Datenentität**
    Dies sind die Eigenschaften der Dateneinheit (wie der Benutzername oder der vollständige Name eines Benutzers).
  - **Verknüpfte Dateneinheit**
    Dies sind andere Datenentitäten, die mit der Hauptdatenentität verknüpft sind (wie die zugewiesene Benutzergruppe eines Benutzers).
    - **Eigenschaften der verknüpften Datenentität**
      Dies sind die Eigenschaften der verknüpften Dateneinheiten.
  - **Registerkarte(n)**
    Eine Registerkarte kann auch innerhalb einer Registerkarte definiert werden .

© 2026, Alle Rechte vorbehalten



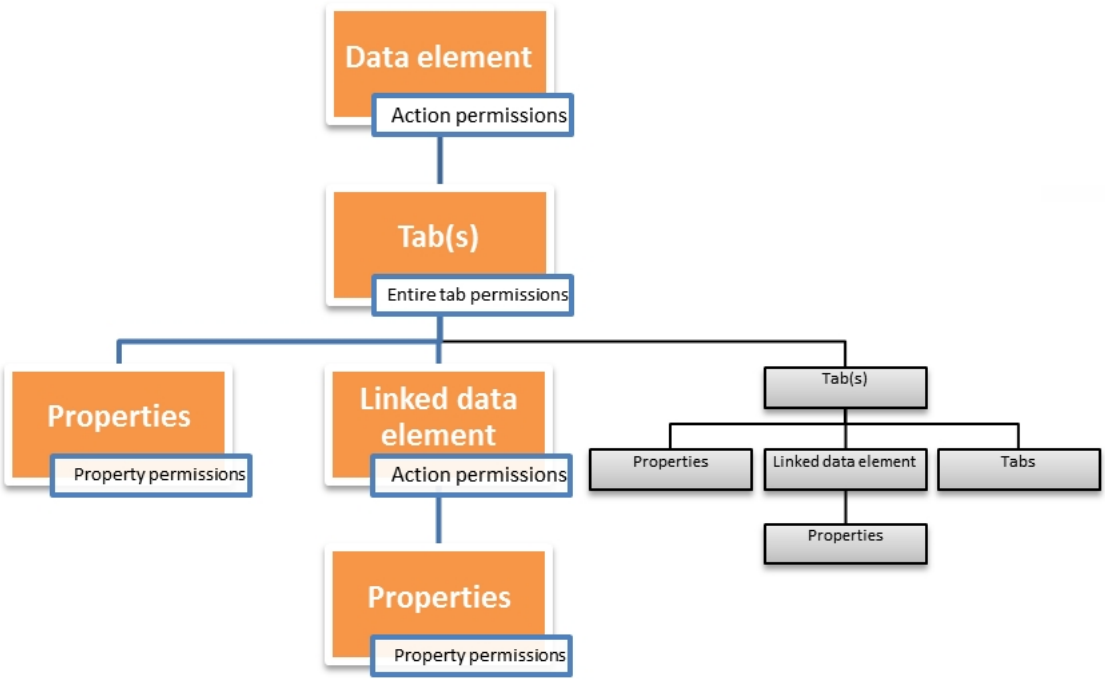


Die verschiedenen Teile eines Dateneingabefensters werden in Access Control als Kategorien festgelegt.



© 2026, Alle Rechte vorbehalten

Es gilt die folgende Berechtigungshierarchie :



Berechtigungen für die gesamte Registerkarte
Die folgenden Berechtigungen können für die Registerkarte erteilt werden:

- **Erstellen**
  Derzeit wird diese Berechtigung in den Anwendungen nicht genutzt. Sie wird in einer späteren Version entfernt werden.
- **Lesen**
  Diese Berechtigung gibt an, ob die Registerkarte für den Benutzer sichtbar ist.
- **Bearbeiten**
  Mit dieser Berechtigung kann der Benutzer die in den Komponenten auf der Registerkarte und allen darunter liegenden Registerkarten angezeigten Informationen aktualisieren.

Berechtigungen für Merkmale
Die folgenden Berechtigungen können für die auf der Registerkarte angezeigten (verknüpften) Datenentitätsmerkmale gewährt werden.

- **Erstellen**
  Diese Berechtigung ist erforderlich, um einen Wert für ein Merkmal einzugeben, wenn eine neue (verknüpfte) Dateneinheit durch eine Erstellungsaktion erstellt wird.
- **Lesen**
  Diese Berechtigung ist erforderlich, um den Wert eines Merkmals lesen zu können.

© 2026, Alle Rechte vorbehalten

> Die Leseberechtigungen für ein Merkmal werden nicht auf die in der Listenübersicht einer (verknüpften) Dateneinheit angezeigten Spalten angewendet.

- **Update**
  Diese Genehmigung ist erforderlich, um den Wert eines Merkmals verändern zu können.

6.1.4 Zugangskontrolle

Die Kategorie Zugangskontrolle (Access Control) enthält Berechtigungen, die für die Anwendung Zugangskontrolle relevant sind.

Für die Webschnittstelle der Zugangskontrolle (Access Control) sind die folgenden Berechtigungen erwähnenswert:

- Die Kategorie **Zugangskontrolle (Access Control) \ Aktionen** enthält Berechtigungen für alle Aktionen, die in der Anwendung Access Control ausgeführt werden können.
- Die Kategorie **Zugangskontrolle (Access Control) \ Authentifizierung** enthält derzeit nur die Berechtigung, die es dem Benutzer erlaubt, das Kennwort von anderen Benutzern als dem eigenen zu ändern.

Berechtigungen zur Benutzerverwaltung in Access Control finden Sie in der Kategorie **Dateneingabe** (Dateneinheit **Benutzer**).

> Siehe "Dateneingabe " auf Seite 18 für weitere Informationen darüber, wie die Berechtigungen für Dateneinheiten gehandhabt werden.

6.1.5 ORTEC WS for Employees

Die Kategorie ORTEC WS for Employees enthält die für die Anwendung ORTEC WS for Employees relevanten Berechtigungen.

Die Kategorien, die unter der Kategorie ORTEC WS for Employees zu finden sind, entsprechen den verschiedenen Arbeitsbereichen, die in ORTEC WS for Employees verfügbar sind.

6.1.6 ORTEC WS for Manager

Die Kategorie ORTEC WS for Manager enthält die für die Anwendung ORTEC WS for Manager relevanten Berechtigungen.

© 2026, Alle Rechte vorbehalten

Die Kategorien unter der Kategorie ORTEC WS for Manager entsprechen den verschiedenen Arbeitsbereichen, die in ORTEC WS for Manager zur Verfügung stehen.

6.1.7 Reports (Microsoft)

Die Kategorie Reports (Microsoft) enthält Berechtigungen für MS-Reports, falls diese in den verschiedenen Anwendungen verfügbar sind.

> Berechtigungen werden für Reports registriert, die in ORTEC WS System Configuration hochgeladen werden, und zwar durch die Post Installation 'MS-Reports hochladen'.

© 2026, Alle Rechte vorbehalten

7 Rechenschaftspflicht

Die Anwendung 'Zugangskontrolle (Access Control)' verfolgt, welcher Benutzer auf welche Teile des Systems zugegriffen hat. Diese Protokollierungssätze sind von der Anwendung aus nicht zugänglich, sondern nur von den Datenbanktabellen. Auf diese Tabellen kann nur ein Benutzer zugreifen, der direkten Zugriff auf die Datenbank hat und über grundlegende SQL-Kenntnisse verfügt.

Diese Informationen werden 366 Tage lang gespeichert.

Die Tabelle **acLoginSession** enthält Informationen über die Benutzer, die gerade auf eine Anwendung zugreifen, und zwar die folgenden Informationen

- **id_user**
  Die Kennung des Benutzers, der auf das System zugegriffen hat.

  Informationen über den Benutzer (z. B. den Benutzernamen) finden Sie in der Datenbanktabelle **[user]**.

- **created_datetime**
  Der Zeitstempel, wann sich der Benutzer bei einer Anwendung angemeldet hat.
- **Anwendung**
  Die Anwendung, auf die der Benutzer zugreift.

Die Tabelle **acLoginSessionLog** enthält Informationen über die Benutzer, die auf eine Anwendung zugegriffen haben, die folgenden Informationen sind verfügbar:

- **userName**
  Der Benutzer, der auf das System zugegriffen hat.
- **LogDatetime**
  Der Zeitstempel des Ereignisses, das beim Zugriff auf eine Anwendung auftritt.
- **eventType**
  Die folgenden Arten von Ereignissen werden protokolliert
  - login: Der Benutzer hat sich bei der Anwendung angemeldet
  - logout: Der Benutzer hat sich bei der Anwendung abgemeldet
  - invalidate: Der Benutzer wurde gezwungen, sich bei der Anwendung abzumelden
  - expired: Der Benutzer ist seit einer bestimmten Zeit (ca. 30 Minuten) nicht mehr aktiv gewesen.

© 2026, Alle Rechte vorbehalten

> Dies gilt nur für die Webanwendungen.

    - validationFailed: Eine Anwendung hat festgestellt, dass die Anmeldesitzung des Benutzers nicht mehr gültig ist.
- **eventData**
  Zusätzliche Informationen zum Ereignis; die Art der Informationen hängt von der Art des Ereignisses ab.
- **Anwendung**
  Die Anwendung, auf die der Benutzer zugegriffen hat.

Die Tabelle **acFailedLoginLog** enthält Informationen über die fehlgeschlagenen Anmeldeversuche für eine Anwendung, wobei die folgenden Informationen zur Verfügung stehen:

- **userName**
  Der Benutzer, der auf das System zugegriffen hat.
- **LogDatetime**

  Der Zeitstempel des Ereignisses, das beim Zugriff auf eine Anwendung auftritt.

- **eventType**

  Die folgenden Arten von fehlgeschlagenen Anmeldeversuchen werden protokolliert

    - UserDoesNotExist: Der eingegebene Benutzername ist in der Anwendung nicht bekannt.
    - UserAccountDisabled: Das Kontrollkästchen **Enabled** ist für das Benutzerdatenelement nicht gesetzt.
    - IncorrectPassword: Das eingegebene Passwort ist falsch.
    - AuthenticationProviderNotSupported: Der verwendete Authentifizierungsanbieter wird nicht mehr unterstützt.
    - AccessDenied: Der Benutzer hat keine Berechtigung zum Zugriff auf die Anwendung.
    - PasswordChangeRequired: Der Benutzer wird gezwungen, sein Passwort zu ändern.

      > Dieses Ereignis kann nur für den Comtec-Authentifizierungsanbieter auftreten.

    - AnErrorHasOccured: Alle anderen Fehler, die während des Anmeldeversuchs auftreten.

© 2026, Alle Rechte vorbehalten

- **eventData**
  Zusätzliche Informationen zum Ereignis; die Art der Informationen hängt von der Art des Ereignisses ab.
- **Anwendung**
  Die Anwendung, auf die der Benutzer zugegriffen hat.

© 2026, Alle Rechte vorbehalten

Kontaktinformationen

Für weitere Informationen wenden Sie sich bitte an ORTEC, entweder über Ihren bestehenden ORTEC-Ansprechpartner oder über die entsprechenden Kontaktdaten auf www.ortec.com.

Auf unserer Website finden Sie Fallstudien, Whitepapers, Broschüren, Demos und vieles mehr.