

INHALTSVERZEICHNIS

Benutzer, Gruppen und Zugriffsrechte	2
Möglichkeiten	2
Administrationsbereich	2
Benutzerverwaltung	3
Zugriffsrechte	4
Benutzergruppen	7

BENUTZER, GRUPPEN UND ZUGRIFFSRECHTE

Die INTex PLUS Lösungen unterstützen umfassende Sicherheit. Das geht beim Hosting in zertifizierten deutschen Rechenzentren los, setzt sich bei der SSL-verschlüsselten Übertragung aller Daten fort und findet seine logische Vollendung in der Einrichtung von Passwort-geschützten Benutzerkonten und einer detaillierten Zugriffsrechte-Steuerung.

Durch die dezidierten Benutzerkonten erst ist es möglich, a) bestimmten Benutzern nur bestimmte Rechte einzuräumen, etwa das Löschen von Datensätzen zu verwehren und b) festzuhalten, wer welchen Datensatz wie und wann zuletzt geändert hat. Der Betrieb etwa eines Forums wäre ohne Kennung, wer was wann geschrieben hat, undenkbar. Aber auch bei der Arbeitszeiterfassung ist es von entscheidender Bedeutung nachhalten zu können, wer welchen Arbeitszeiteintrag vorgenommen hat.

INTex PLUS Lösungen unterstützen zwar auch die gemeinsame Nutzung eines User-Accounts durch mehrere Benutzer, Sie geben aber als Betreiber damit viele Möglichkeiten der Prüfung von Dateneinträgen und der Kontrolle Ihres Systems auf, weil Aktivitäten in der Datenbank nicht mehr eindeutig bestimmten Benutzern zuzuordnen sind.

MÖGLICHKEITEN

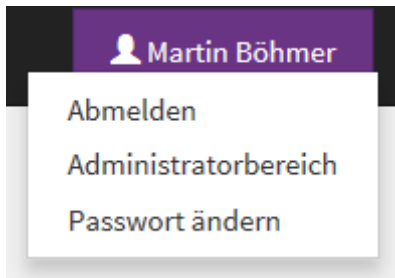
Und das sind die grundsätzlichen Möglichkeiten:

- Definition von Benutzerkonten durch den Administrator mit Zuordnung der Benutzer zu Zugriffsrechte-Gruppen. Die Benutzer können sich Passwörter vergeben und ändern und bei Bedarf auch wieder vom System abrufen.
- Anlage von Zugriffsrechte-Gruppen. Diese fassen vordefinierte Zugriffsrechte zu einem Set zusammen und werden wahlweise einem oder mehreren Benutzern zugeordnet. Ein Benutzer kann auch Teil mehrerer Zugriffsrechte-Gruppen sein. Der Administrator hat immer vollen Zugriff.
- Drei Zugriffsrechte-Gruppen sind fest vordefiniert:
 - *Administrator*: Der Administrator hat alle Rechte in allen Modulen über alle Benutzer hinweg.
 - *Standard*: Eine Vorgabe von Zugriffsrechten für neue Benutzer ohne Zuweisung spezifischer Rechte.
 - *Gast*: Ein reiner Lese-Zugriff.
- Zwei weitere Zugriffsrechte sind optional, d.h. Sie können diese Rechtegruppen auch löschen oder umbenennen:
 - Benutzer: Zugriffsrechte des Standard-Benutzers gemäß den Vorgaben von INTex.
 - Demo: Zugriffsrechte des Demo-Benutzers aus unserer Online-Demo.
- Beschreibung von Zugriffsrechten für die Rechte-Gruppen in mehreren Unterteilungen:
 - Unterscheidung der Zugriffsrechte nach Modul/Datentabelle/Menüpunkt
 - Zugriffsrecht *Hinzufügen*: Der Benutzer darf Daten eintragen oder nicht
 - Zugriffsrecht *Ändern*: Der Benutzer darf vorhandene Daten ändern oder nicht
 - Zugriffsrecht *Löschen*: Der Benutzer darf vorhandene Daten löschen oder nicht
 - Zugriffsrecht *Anzeigen*: Der Benutzer darf Daten sehen oder nicht. Ohne dieses Zugriffsrecht sind Hinzufügen, Ändern und Löschen unmöglich.
 - Zugriffsrecht *Drucken/Exportieren*: Der Benutzer darf vorhandene Daten drucken und/oder exportieren oder nicht
 - Zugriffsrecht *Importieren*: Der Benutzer darf neue Daten per Import hinzufügen.

ADMINISTRATIONSBEREICH

Alle Änderungen und Einstellungen an Benutzer- und Zugriffsrechten kann ausschließlich ein ins System eingeloggter Administrator im *Administrationsbereich* vornehmen – im Demo-Modus ist dieser Bereich daher

nicht zugänglich. Der Administrator gelangt über den Benutzer-Schalter rechts oben und den Befehl „Administratorbereich“ in diesen Bereich.



Das Hauptmenü weist nun die Einträge *Zugriffsrechte*, *Benutzergruppen* und *Benutzerverwaltung* auf. Sie befinden sich zunächst bei den Zugriffsrechten.

INTex Hausverwaltung | Zugriffsrechte | Benutzergruppen | Benutzerverwaltung

Home / Zugriffsrechte

Speichern Anzeige: Alle Tabellen | Sortierung: Wie im Menü

[Gruppe hinzufügen](#) [Berechtigungen kopieren von...](#)

<Administrator> <Standard> <Gast> **Benutzer** Demo

Suche nach	Hinzufügen	Ändern	Löschen	Anzeigen	Drucken/Exportieren	Importieren	Administrator Modus (Zugriff auf alle Datensätze)
Alles aufklappen	■	■	■	■	■	■	■
Abrechnungen (8) ▶							
Gebäude (11) ▶							
Inventar (11) ▶							
Aufträge (7) ▶							
Adressen (8) ▶							
Organizer (15) ▶							
Einstellungen (4) ▶							
Nicht gelistete Tabellen (26) ▶							

Wechseln Sie für die Ersteinrichtung zunächst über das schwarz unterlegte Menü oben in den Bereich *Benutzerverwaltung*.

BENUTZERVERWALTUNG

In der *Benutzerverwaltung* sehen Sie die in Ihrer Lizenz verfügbaren Benutzer. In der Regel können Sie keine Benutzer anlegen und löschen, da die Lizenz ja eine vordefinierte Benutzerzahl mit sich bringt. Sie können aber die Benutzer voll inhaltlich ändern und mit anderen Rechten versehen als dies im Auslieferungszustand vorgesehen war.

Benutzerverwaltung

Anzeige von 1 - 20 aus 3 20 ▾

<input type="checkbox"/>	Name	Bild	Email	Benutzername
<input type="checkbox"/>	Martin Böhmer		MB@intex-publishing.de	admin
<input type="checkbox"/>	Demo		demo@demo.de	demo
<input type="checkbox"/>	Tester		test@test.de	test

Um einen Benutzer zu verändern, klicken Sie auf das Stift-Symbol. In der *Ändern*-Maske haben Sie die Möglichkeit, jeden Benutzer mit einem Klartextnamen oder – wenn gewünscht – Pseudonym, einem Bild oder Avatar und einem System-Benutzernamen zu versehen. Die Email-Adresse dient dem Versenden eines Passwort-Ändern-Links an den Benutzer, denn nicht nur Sie als Admin, sondern auch der Benutzer selbst kann das Passwort ändern.

Benutzer, Ändern [admin]

Name *

Bild Behalten Löschen Aktualisieren

Email *

Benutzername *

Passwort *

Mit *Speichern* übernehmen Sie die Änderungen.

ZUGRIFFSRECHTE

Im eingangs schon gesehenen Modul *Zugriffsrechte* bestimmen Sie für die Vorgabe-Benutzerrechte *Administrator*, *Standard* und *Gast* sowie alle weitere Gruppen die Zugriffsrechte detailliert nach Rechten für *Hinzufügen*, *Ändern*, *Löschen*, *Anzeigen*, *Drucken/Exportieren* und *Importieren*.

Über die Registerkarten oben legen Sie fest, welche Rechtegruppe Sie bearbeiten – achten Sie also darauf, nicht versehentlich dem Gast die Rechte des Admins zu gewähren oder den Admin so zu beschneiden, dass er seinen Aufgaben nicht mehr nachkommen kann.

Sie sollten sich für die Definition der Zugriffsrechte ruhig Zeit nehmen und einen Plan machen – nehmen Sie dabei ein Organigramm oder eine Personalliste Ihrer Firma zur Hilfe und verwenden Sie vielleicht eine Excel-Tabelle als Planungshilfe. Besser etwas zu viel geplant, als dass später die Praktikantin die Daten aller Key Accounts löschen kann. Denken Sie daran, nicht nur böswillige Aktivitäten gar nicht erst zu erlauben, sondern auch Datenverlust durch versehentliches Tun oder sinnentfremdete Fehlbedienung zu verhindern.

Wenn der Plan steht, legen Sie mit „Gruppe hinzufügen“ zunächst alle benötigten Gruppen an oder löschen unbenötigte Gruppen bzw. benennen diese nach Ihren Bedürfnissen um.

Den Administrator dürften Sie zumindest für den Anfang nicht ändern müssen, weil dieser ja Zugriffsrechte auf alles haben soll und darauf ist er werksseitig bereits eingestellt.

Das Zugriffs-Set „Standard“ muss nicht direkt Benutzern zugeordnet werden, sondern kann auch lediglich als Vorgabe für weitere Rechte-Sets dienen („Berechtigungen kopieren von...“).

Der *Gast* ist ab Werk als reiner Lese-Zugriff konzipiert, einen reinen Gastzugang ohne Login mit Benutzername und Passwort haben wir aber aus Sicherheitsgründen im Standard nicht freigeschaltet. Sie können jedoch die Gastrechte jederzeit einem Benutzer zuordnen, etwa einem Betriebsprüfer.

Das Zugriffs-Set „Benutzer“ ist in der Werkseinstellung die Definition für den normalen Anwender – dies sollten Sie daher nur mit Vorsicht und Bedacht ändern, um nicht Ihre Anwender versehentlich von wichtigen Funktionen auszusperrern und damit von ihrer Arbeit abzuhalten.

Den Demo-Zugang können Sie in Ihren Einstellungen löschen – die ausgelieferte Vollversion der INtex PLUS Lösung hat ja ohnehin keinen Demo-Benutzer mehr.

Inventar (11) ▼						
<input type="checkbox"/> Inventar (Inventar)	■	■	■	■	■	■
<input checked="" type="checkbox"/> Inventar Bilder (Inventar Bilder)				■	■	
<input checked="" type="checkbox"/> Finanzbericht (Finanzbericht)				■	■	
<input checked="" type="checkbox"/> Mengenbericht (Mengenbericht)				■	■	
<input checked="" type="checkbox"/> Inventar Diagramme (Inventar Diagramme)				■		
<input checked="" type="checkbox"/> Inventar Etiketten (Inventar Etiketten)				■	■	
<input checked="" type="checkbox"/> Inventar Datenblatt (Inventar Datenblatt)				■	■	
<input type="checkbox"/> Inventar Stapelverarbeitung (Inventar Stapelverarbeitung)		■	■	■		
<input type="checkbox"/> Sets (Sets)	■	■	■	■		
<input type="checkbox"/> Schlagwoerter (Schlagwoerter)	■	■	■	■		
<input type="checkbox"/> Klassifikationen Inventar (Klassifikationen Inventar)	■	■	■	■	■	■

Was ein Benutzer mit dem oben aktivierten Benutzerrecht darf und was nicht, sehen Sie an den farbigen Quadraten.

- Schwarz = Administrator-Zugriff
- Grau = Teilweiser Zugriff gewährt
- Rot = Zugriff in der jeweiligen Zugriffsart (Hinzufügen, Ändern etc.) verwehrt
- Grün = Zugriff in der jeweiligen Zugriffsart gewährt

Achtung: Beachten Sie, dass die Rechte *Hinzufügen, Ändern, Löschen, Drucken/Exportieren* und *Importieren* unbedingt mit dem Recht *Anzeigen* kombiniert werden müssen, um Sinn zu machen. Wie wollen Sie sonst Daten löschen, die Sie nicht sehen können?

Durch einfaches Anklicken der Kästchen setzen Sie ganze Spalten (Zugriffsrechte-Art), Zeilen (Module) oder Zellen (einzelne Zugriffsrechte-Art für ein Modul) auf an oder aus. Änderungen werden durch eine gelbe Markierung hervorgehoben.



Die Änderungen werden aber erst wirklich übernommen, wenn Sie oben links auf „Speichern“ klicken. Noch haben Sie also die Möglichkeit, versehentliche Änderungen mit „Zurücksetzen“ zurückzunehmen.

Gehen Sie in Ruhe durch Auf- und Zuklappen der Module alle Bereiche der INTex PLUS Lösung durch und entscheiden Sie, welche Zugriffsrechte sinnvoll sind und Sie gewähren möchten.

Folgende Hinweise sind wichtig:

- Wer nichts anzeigen kann, wird komplett von einem Modul ausgesperrt, kann also folgerichtig auch nichts ändern, löschen oder hinzufügen. Vor allem bei gelegentlichen Mitarbeitern, Praktikanten etc. sollten Sie intensiv darüber nachdenken, ob der Zugriff zu einem Modul überhaupt gewährt werden muss. Ein weiteres Modul hinterher „aufschließen“ geht schnell, verlorene oder gar gestohlene Daten lassen sich nicht mehr zurückholen.
- Durch das Verwehren des Anzeige-Rechts können Sie für Anfänger unter den Anwendern auch die Oberfläche der INTex PLUS Lösung klar, aufgeräumt und übersichtlich halten. Module nämlich, auf die kein Anzeigen-Zugriffsrecht besteht, erscheinen erst gar nicht im Eingangsbildschirm und Menü.
- Einem Betriebsprüfer brauchen und sollten Sie nur einen reinen Lese-Zugriff gewähren und das auch nur auf Module, die für die Betriebsprüfung und steuerliche Fragen relevant sind. Im Team-Chat etwa hat der Prüfer nichts zu suchen.
- Mit dem Löschen-Recht sollten Sie äußerst vorsichtig umgehen. Bei GOBD relevanten Datentabellen ist ein Löschen von Datensätzen schon ab Werk überhaupt nicht vorgesehen, weil die Finanzverwaltung das nicht toleriert. Hier müssen etwa Storno-Buchungen dafür sorgen, dass fehlerhafte Buchungen wertmäßig korrigiert werden. Aber auch das Löschen von Kundenadressen ist nicht sonderlich sinnvoll, selbst wenn der Kunde etwa Pleite gegangen ist. Schließlich hängen an der Kundenadresse ja auch die Auftragshistorie und andere Vorgänge, die ohne Adresse nicht mehr nachvollziehbar sind. Im Zweifel also besser kein Löschrrecht einräumen.
- Das Importieren von Daten erweist sich in der Praxis immer schnell als kompliziert und den normalen Anwender überfordernd. Da versehentlich oder falsch importierte Daten dann auch noch wieder gelöscht werden müssen, sollten Sie sich als Administrator das Importieren-Recht vorbehalten, es sei denn, Ihre Anwender sind „fit“ oder importieren immer gleiche Ausgangsdaten wie Kontoauszüge, wo dann in der Regel nichts schiefgehen kann.
- Das Drucken und Exportieren von Daten sollte ebenfalls gut überlegt sein. Schließlich kann auf diesem Wege ein Mitarbeiter schnell die Umsatzdaten aller Key Accounts auf einen USB Stick ziehen und mitnehmen – selbst wenn Ihre Daten nicht so interessant sind wie bei Schweizer Banken, sollten Sie hier Vorsicht walten lassen. Natürlich können Sie umgekehrt nicht verhindern, dass etwa Rechnungen gedruckt werden müssen. Deshalb haben wir in der Software aber schon explizite Druck-Daten in eigene Module ausgelagert.

BENUTZERGRUPPEN

Über die *Benutzergruppen* können Sie als Administrator die verschiedenen Benutzer Ihres Teams in der Regel *einer* Zugriffsrechte-Gruppe zuordnen und damit als Co-Admin, Benutzer, Prüfer (Gast) etc. klassifizieren. Sie haben aber auch die Möglichkeit, einem Benutzer mehrere Zugriffsrechte zuzuordnen.

Praktisch erfolgt die Zuordnung über Klick auf die Farbfelder mit anschließendem „Speichern“.

Benutzer	Benutzername	E-mail	<Aministrator>	Benutzer	Demo
Suche nach			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> admin	Martin Böhmer	MB@intex-publishing.de	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> test	Tester	test@test.de	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> demo	Demo	demo@demo.de	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Die Vergabe mehrerer Zugriffsrechte an einen Benutzer macht dann Sinn, wenn Sie die Zugriffsrechte sehr kleinteilig und modular aufgesplittet haben. Sie könnten ja etwa statt einem Zugriffsrecht „Benutzer“ für jedes Modul ein getrenntes Benutzerrecht anlegen, etwa „Benutzer Adressen“, „Benutzer Organizer“, „Benutzer Korrespondenz“. Soll dann ein Benutzer Zugriff auf alle Module haben, müssten Sie die drei genannten Zugriffsrechte gleichzeitig aktivieren.

Achten Sie aber dringend darauf, dem Anwender keine widersprüchlichen Zugriffsrechte zu vergeben. Die Software ist so ausgelegt, dass bei sich widersprechenden Zugriffsrechten das jeweilige Recht gewährt wird. Wenn der Anwender also wegen Recht A beispielsweise Adressen nicht sehen darf, dank Recht B aber schon, dann greift das großzügigere Recht B. Wenngleich dies technisch so funktioniert, sollten Sie in der Regel auf solche „Konstruktionen“ verzichten, denn im Zweifel verlieren Sie dabei am Ende den Überblick. Und die ganzen Zugriffsrechte und Benutzergruppe nützen letztlich nichts, wenn Sie selbst die Kontrolle darüber verlieren.