DOKUMENTATION
PROXESS ADMINISTRATOR CONSOLE

Stand: PROXESS 10 Release 2020R2

Inhaltsverzeichnis

Copyright-Hinweis, Haftungshinweis

Konventionen in dieser Dokumentation

Ein Hinweis für Benutzerinnen:
Wegen der besseren Lesbarkeit verzichten wir in dieser Dokumentation auf die ausdrückliche Anrede von Benutzern und Benutzerinnen. Wir möchten aber ausdrücklich darauf hinweisen, dass mit Benutzern stets Frauen und Männer gemeint sind.

Hervorhebungen im Text

In dieser Dokumentation werden Hervorhebungen folgendermaßen verwendet:

Fett	bezeichnet Menübefehle, Schaltflächen, Feldnamen, Optionen und Programmgruppen. Beispiele: der Befehl Neu, im Feld Name
"Anführungszeichen"	bezeichnen Menütitel, Ordnernamen und Dialogfelder. Beispiele: das Menü "Benutzer", der Ordner "Smartcards", das Dialogfeld "Passwort festlegen"
GROSSBUCHSTABEN	bezeichnen Menütitel, Ordnernamen und Dialogfelder. Beispiele: das Menü "Benutzer", der Ordner "Smartcards", das Dialogfeld "Passwort festlegen"
(Klammern)	zeigen an, dass ein Platzhalterzeichen gemeint ist. Beispiele: (%) (_) im Rahmen der PROXESS-Suche

Tipps

	zeigen Ihnen besonders komfortable Möglichkeiten der Bedienung oder nützliche Zusatzinformationen. Tipps werden immer wie dieser Absatz dargestellt.

Warnhinweise

	finden Sie bei Aktionen, die einen erheblichen Mehraufwand an Arbeit verursachen könnten oder sogar Datenverluste oder sonstige materielle Schäden zur Folge haben könnten. Warnhinweise werden durch dieses Symbol gekennzeichnet: **Warnhinweise sollten Sie besonders aufmerksam lesen, bevor Sie weiterarbeiten.**

Organisationsanalyse als Voraussetzung

Vor der Einrichtung eines PROXESS-Systems müssen Sie einige organisatorische Fragen klären. Idealerweise haben Sie im Vorfeld eine Organisationsanalyse durchgeführt und die untenstehenden Fragen beantwortet:

Als Administrator benötigen Sie folgende Informationen für die Systemeinrichtung:

Welche Archivdatenbanken werden benötigt?
Welche Dokumenttypen werden in den jeweiligen Archivdatenbanken benötigt?
Welche Indexfelder werden in jeder Archivdatenbank benötigt?
Welche Indexfelder sollen verschlüsselt werden?
Welche Indexfelder sollen Pflichtfelder werden?
Sollen einige Indexfelder mit einer Validierungsregel versehen werden?
Sollen bestimmte Suchen über Suchbedingungen fest eingegeben werden?
Welche Felder sollen mit einem dynamischen Suchkriterium verknüpft werden?
Welche Dateitypen sollen archiviert werden und mit welchen Anwendungsprogrammen zum Bearbeiten, Ansehen und Drucken werden diese von den Anwendern aufgerufen?
Werden Dateivorlagen in Verbindung mit bestimmten Anwendungsprogrammen (z. B. Winword) benötigt?
Auf welchen Speichermedien und wie lange sollen Dokumente archiviert werden?

Für die Arbeit des PROXESS Supervisors in der PROXESS Administrator Console ist es notwendig zu wissen:

Welche Benutzer und Gruppen werden benötigt?
Welche Rechte auf Datenbanken und Dokumenttypen erhalten die Benutzer und Gruppen?
Welche Datenbanken sollen als Hochsicherheitsdatenbanken verschlüsselt werden?
Welche Benutzer sollen als Datenbank-Bereichsadministrator eingesetzt werden?

Erst auf Basis dieser Informationen können Sie die Konfiguration und Einrichtung von PROXESS vornehmen.

Was ist die PROXESS Administrator Console?

Die PROXESS Administrator Console dient der zentralen Systemadministration.

Diese Aufgaben können Sie mit der PROXESS Administrator Console durchführen:

- Benutzerverwaltung und Rechteverwaltung
- Verwaltung von Smartcards für Supervisor
- Erstellung und Aktivierung des Systemzertifkates und der Supervisorzertifikate
- Datenbanksignierung, Feld- und Dateiverschlüsselung
- Verwaltung und Konfiguration von Archivdatenbanken
- Einrichten von Feldern, Dokumenttypen und Dateitypen
- Einrichtung der Index- und Suchmasken
- Konfiguration von Validierungsregeln, Vorlagedateien sowie Such- und Sortierkriterien

Die PROXESS Administrator Console wird als "Snap-In" der Microsoft Management Console (MMC) bereitgestellt.

siehe auch:
Inbetriebnahme des Systems - Schritt für Schritt
Organisationsanalyse
Vor der ersten Anmeldung

Systemeinrichtung bei Betrieb im OEM-Modus

Bei einem Systembetrieb im OEM Modus muss kein Systemzertifkat beantragt werden. Die Einrichtung von Hochsicherheitsdatenbanken mit einer speziellen Datei- und Feldverschlüsselung stehen nicht zur Verfügung. Im OEM-Modus werden diese Zertifikatsoptionen zwar angezeigt, haben aber keine Verwendung.

Nach der Installation im OEM-Modus steht das System sofort betriebsbereit mit einer Standarddatenbank zur Verfügung.

Welcher Modus verwendet wird, hängt davon ab, wie der PROXESS professional Setupsatz installiert wird. Hier kann entweder der Zertifikatsmodus oder der OEM-Modus aktiviert werden. **Es ist nachträglich nicht möglich vom Zertifikatmodus in den OEM-Modus zu wechseln oder umgekehrt.**

Systemeinrichtung bei Betrieb im Zertifikatsmodus

	Welcher Modus verwendet wird, hängt davon ab, wie der PROXESS professional Setupsatz installiert wird. Hier kann entweder der Zertifikatsmodus oder der OEM-Modus aktiviert werden. **Es ist nachträglich nicht möglich vom Zertifikatmodus in den OEM-Modus zu wechseln oder umgekehrt.**

Wenn Sie **PROXESS im Modus mit Sicherheitszertifikat** installiert haben, müssen vor dem ersten Systemstart und dem ersten Arbeiten mit PROXESS einige vorbereitende Schritte in der PROXESS Administrator Console ausgeführt werden.

NACH Installation der Software und VOR der ersten Anmeldung müssen Sie:

einmalig ein PROXESS Systemzertifikat für Ihr System beantragen, aktivieren und installieren

Ihre erste Supervisor Smartcard vorbereiten und erstellen

Ihre individuelle PROXESS-Systemlizenz (erstellt von der PROXESS GmbH) einspielen

die Datenbanksignierung initialisieren

Wie die Schritte im einzelnen ausgeführt werden, erfahren Sie, wenn Sie den eingetragenen Links in der Tabelle folgen.

1. Schritt: PROXESS Software installieren	einmalig	
2. Schritt: Systemzertifikat beantragen	einmalig	==> Online-Übermittlung des Antrags an die PROXESS GmbH ==> PROXESS schickt die signierte Datei an den Antragsteller zurück

3. Schritt: Systemzertifikat aktivieren und installieren Aktivierung / Installation	einmalig	
4. Schritt: Erste Supervisor Smartcard erstellen Vorbereitung / Erstellung	einmalig	==> Übertragung der Daten aus dem Supervisorzertifikats an PROXESS ==> Erstellung und Übermittlung der Lizenzdateien durch PROXESS
5. Schritt: Lizenzdateien einspielen	einmalig	==> 1. PROXESS-Systemstart durch den Supervisor
6. Schritt: Datenbanksignierung initialisieren	einmalig	==> **Das System ist nun freigeschaltet!** ==> Benutzeranmeldung und weitere Administration sind jetzt möglich

7. Schritt: Weitere Supervisor Smartcards erstellen Vorbereitung / Erstellung / Zuweisung	jederzeit im lfd. Betrieb	Wir empfehlen Ihnen, dass Sie Sie sicherheitshalber mindestens eine weitere Superivsor-Smartcard erstellen.

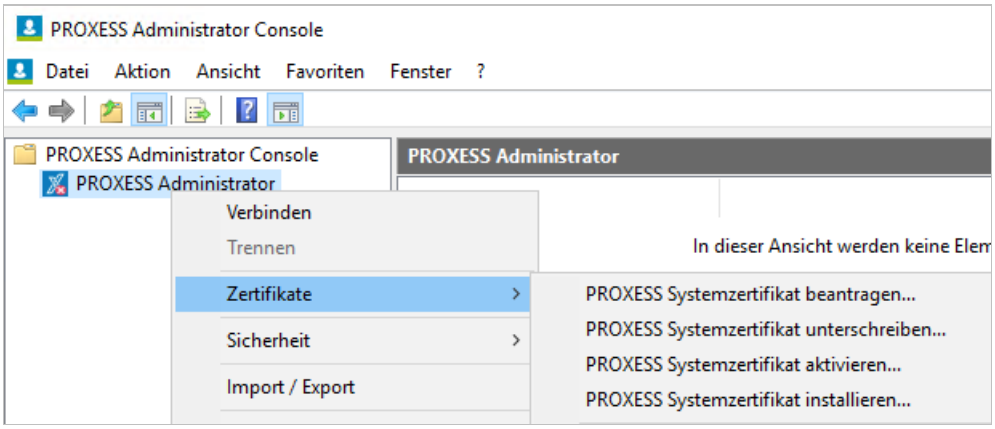


Abb.: Notwendige Schritte für das PROXESS Systemzertifikat

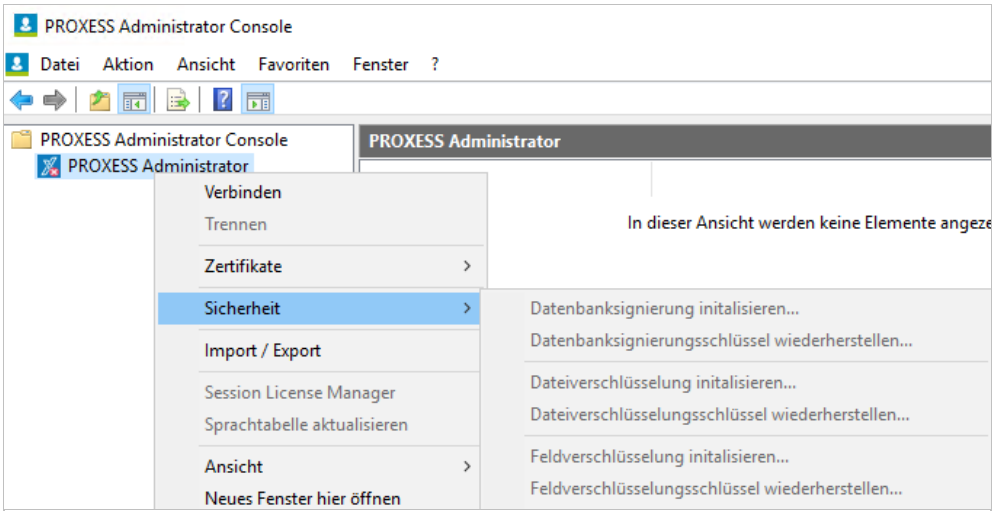


Abb.: Funktionen zur notwendige Datenbanksignierung und für die optionale Verschlüsselung für Hochsicherheitsdatenbanken

Administratorkategorien im Überblick

PROXESS trennt die administrativen Bereiche der Zugriffrechtevewaltung durch einen PROXESS Supervisor von der technischen Administration durch den PROXESS Administrator. Der PROXESS-Supervisor ist zuständig für das "Wer?" des Archivzugriffs und der PROXESS Administrator für das "Was?". Dabei können alle Aufgaben des Administrators auch durch den Supervisor durchgeführt werden. Um den Supervisor zu entlasten, kann er für bestimmte Datenbanken die sogenannten Datenbank-Bereichsadministratoren ernennen. Dies können dann in Ihren eigenen Datenbankbereichen die Benutzerzugriffsrechteverwaltung übernehmen.
Die Rechte in der Übersicht:

Supervisor	**Datenbank-Bereichsadministrator**	**Administrator**
• Systeminitialisierung • Benutzerverwaltung • Zugriffsrechteverwaltung • Verschlüsselung von Feldinhalten oder Dateien	• wird vom Supervisor ernannt • Verwaltung von Zugriffsrechten, Zurücksetzen von Passwörtern, Benutzersperrung im eigenen Datenbankbereich	• Anlegen neuer Archivdatenbanken • Verwaltung von Feldern, Dokumenttypen und Dateitypen • Verwaltung von Dokumentmasken • Verwaltung von Validierungsregeln, Vorlagedateien sowie Such- und Sortierkriterien • Systemadministration (Erstellen und Verwalten externer Speichermedien, Cacheverwaltung, externe SQL-DB-Administration etc.)

Supervisor

PROXESS trennt die administrativen Bereiche der Zugriffsrechteverwaltung durch einen PROXESS Supervisor von der technischen Administration durch den PROXESS Administrator. Der PROXESS Supervisor ist zuständig für das "Wer?" des Archivzugriffs (Benutzer- und Gruppenberechtigungen), der PROXESS Administrator für das "Was?" (Datenbankfelder, Dokumenttypen, Thesauren etc.). Dabei können alle Aufgaben des PROXESS Administrators auch durch den PROXESS Supervisor ausgeführt werden. Der Supervisor authentifiziert sich immer mit Smartcard und PIN am System.

Das Sicherheitskonzept von PROXESS sieht die Geschäftsführung eines Unternehmens in der Rolle des Supervisors, der sich über eine persönliche Smartcard zur Administration sicherheitsrelevanter Funktionen am System authentifiziert. Zu diesen Funktionen/Berechtigungen gehört u. a., die Verschlüsselung von Feldinhalten oder Dateien zu aktivieren, sowie Benutzer- und Gruppenberechtigungen einzurichten bzw. zu ändern.

Soll ein Mitarbeiter erweiterte administrative Aufgaben und die Verwaltung von Zugriffsrechten bestimmter Bereiche übernehmen, so kann der Supervisor ihm diese Rolle übertragen. So kann zum Beispiel der Personalleiter die Verwaltung von Zugriffsrechten für die Datenbank "Personal" übernehmen (Datenbank-Bereichsadministrator). Bei Bedarf ist es dem Supervisor auf diese Weise auch möglich, den ursprünglichen PROXESS-Administrator wieder mit jeglichen Rechten auszustatten. Somit ist ein Systembetrieb "wie gewohnt" möglich.

Supervisor ist jeder registrierte Benutzer in PROXESS, der Mitglied der Gruppe "SUPERVISORS" ist und dem eine gültige Supervisor Smartcard zugewiesen ist.

Siehe auch:
Benutzerverwaltung - Konzept und Überblick
Zugriffsrechte - Konzept und Überblick

PROXESS Administrator - Aufgaben und Rechte

PROXESS Administratoren sind alle Mitglieder der PROXESS-Benutzergruppe "Admin". Administratoren melden sich mit PROXESS- Benutzerkurznamen und Kennwort am System an. Die Anmeldung einen Windows-Active-Directory-Benutzers ist in der PROXESS Admin Console nicht möglich.

Administratoraufgaben sind:

- Anlage neuer Archivdatenbanken
- Konfiguration von Feldern, Dokumenttypen und Dateitypen (inkl. Verschlüsselungsoptionen auf Feld- und Dateiebene)
- Erstellung und Konfiguration von Dokumentmasken
- Konfiguration von Validierungsregeln, Sortierkriterien, Thesauren, etc.
- Systemadministration (Erstellen und Verwalten externer Speichermedien, Cacheverwaltung, externe SQL-Datenbankadministration etc.)

Die Aufgabe der Benutzerverwaltung und die Vergabe von Zugriffsrechten auf Datenbanken und Dokumenttypen nimmt der Supervisor bzw. der vom Supervisor ernannte Datenbank-Bereichsadministrator vor. Administrator ist jeder Benutzer, der Mitglied der Gruppe "Administratoren" ist.

Mit der Neuanlage einer Datenbank erhält der Administrator automatisch Zugriffsrecht auf diese Datenbank. Das Zugriffsrecht wird benötigt um oben genannte administrative Aufgaben ausführen zu können. Das Zugriffsrecht auf die Datenbank gewährt allerdings nicht automatisch den Zugriff auf die Dokumente dieser Datenbank. Hierzu müssen gesonderte Zugriffsberechtigungen auf Dokumenttypebene vergeben werden.

Was darf der Administrator nicht?
Die Vergabe von Zugriffsrechten auf Datenbanken und Dokumenttypen erfolgt durch den Supervisor oder den Datenbank-Bereichsadministrator. Der Administrator kann die Rechte nur sehen, aber nicht erteilen oder entziehen.

Siehe auch:

Zugriffsrechte - Konzept und Überblick

Datenbank-Bereichsadministrator

Ein Datenbank-Bereichsadministrator kann vom Supervisor mit Supervisorprivilegien ausgestattet werden. **Der Supervisor erteilt dem Datenbank-Bereichsadministrator das Verwaltungsrecht für eine oder mehrere Datenbanken.**

Das Verwaltungsrecht für eine Datenbank ermöglicht es, in dieser Datenbank anderen PROXESS-Benutzern Zugriffsrechte auf Dokumente zu erteilen oder zu entziehen. Darüber hinaus kann der Bereichsadministrator für Benutzer mit Zugriffsrecht auf "seine" Datenbank Kennwörter festlegen und zurücksetzen, Benutzerkonten sperren und entsperren.

Als Bereichsadministrator für eine Datenbank, erscheinen nur die Datenbanken in der Anzeige, die vom Supervisor freigeschaltet wurden. Bereichsadministratoren können sich alle bestehende Benutzer- und Gruppenzugehörigkeiten anzeigen lassen, jedoch nur eingeschränkt Änderungen vornehmen. So kann der Datenbank-Bereichsadministrator nur dann Benutzern und Gruppen Zugriffsrecht auf die von ihm verwaltete Datenbank erteilen, wenn diese Benutzer und Gruppen keine Zugriffsrechte auf andere Datenbanken besitzen, die er nicht selbst auch verwaltet. Genauso können nur diejenigen Benutzer in eine Gruppe mit Zugriffsrecht auf die verwaltete Datenbank aufgenommen werden, die keine Zugriffsrechte auf andere Datenbanken besitzen. Verwaltet ein Datenbankbereichs-Administrator mehrere Datenbanken, so kann er innerhalb seines Verwaltungsbereichs Benutzer und Gruppen frei zuordnen und Zugriffsrechte erteilen.

Mit dieser Regelung soll verhindert werden, dass Bereichsadministratoren ihre Befugnisse missbrauchen können und sich durch Kennwortänderung mit einem anderen Benutzerlogin Zugang zu einem Archiv verschaffen, für das sie keinen Zugriff erhalten haben. Gleichzeitig soll dabei der Supervisor von täglichen Routineaufgaben der Benutzerverwaltung wie "Passwort zurücksetzen" entlastet werden.

Neben dem grundsätzlichen Zugriff auf eine Archivdatenbank ist der Datenbank-Bereichsadministrator dafür verantwortlich, innerhalb seines Verwaltungsbereiches von einer oder mehreren Datenbanken die entsprechenden Dokumenttyprechte zu vergeben.

Siehe auch:

Benutzerverwaltung - Konzept und Überblick

Zugriffsrechte - Konzept und Überblick

Datenbankrechte verwalten

Dokumenttyprechte verwalten

Anmeldung

Nach dem ersten Start der PROXESS Administrator Console erscheint der PROXESS Anmeldedialog.
Bei allen weiteren Starts verbinden Sie sich über den Menüpunkt Aktion/Verbinden mit dem bereits eingetragenen PROXESS System (alternativ über das Kontextmenü).

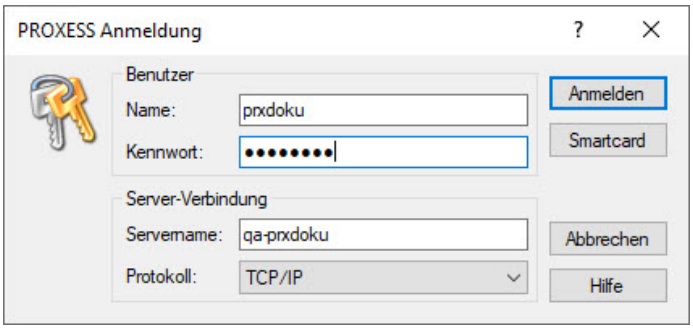


Abbildung: Anmeldemaske der PROXESS Administrator Console

In der PROXESS Administrator Console haben Sie zwei Anmeldemöglichkeiten: Die Anmeldung über Smartcard und die Anmeldung mit Benutzername und Kennwort. Die Anmeldung mit einem Windows-Active-Directory Benutzerkonto ist nicht möglich. Je nach gewählter Anmeldeform und Ihrem Benutzerprofil werden Sie mit unterschiedlichen Rechten zur Ausführung von Funktionen innerhalb der PROXESS Administrator Console ausgestattet.

1. Möglichkeit: Anmeldung mit Smartcard und PIN-Eingabe

Die Anmeldung über Smartcard mit PIN-Eingabe ist ausschließlich PROXESS-Benutzern mit Supervisorprivilegien vorbehalten.

Stellen Sie sicher, dass die Eingaben für die Server-Verbindung korrekt sind (siehe Tabelle). Schließen Sie den Smartcard-Reader an Ihren Rechner an und wählen Sie den Befehl **Smartcard**. Auf dem Bildschirm erscheint ein Aktionsfenster des Smartcard-Readers. Gleichzeitig werden Sie in der Anzeige des Smartcard-Readers aufgefordert, eine gültige Supervisor-PIN einzugeben und mit ENTER zu bestätigen.

Eine Eingabe von Benutzername und Kennwort ist bei der Anmeldung über Smartcard nicht notwendig.

2. Möglichkeit: Anmeldung mit Benutzername und Kennwort

Anwender, Administratoren und Datenbank-Bereichsadministratoren melden sich mit Benutzername und Kennwort an. Die Anmeldung über Benutzername mit Kennwort beinhaltet keine Supervisorprivilegien.

Name	In diesem Feld geben Sie Ihren Benutzernamen ein oder übernehmen Sie den Namen, der noch von der vorherigen Sitzung eingestellt ist. Bei der ersten Anmeldung verwenden Sie den Benutzernamen, der bei der Installation angelegt worden ist. Das Programm speichert den eingestellten Benutzernamen, so dass Sie ihn bei der nächsten Anmeldung direkt übernehmen können.
Kennwort	Hier geben Sie Ihr Kennwort ein. Bei der ersten Anmeldung verwenden Sie das Kennwort, das bei der Installation angelegt worden ist. Die Änderung von Kennwörtern innerhalb der PROXESS Administrator Console kann nur durch den Supervisor erfolgen. Die Änderung des eigenen Passwortes ist z. B. im Programm "PROXESS" oder "PROXESS Administrator" möglich.

Servername	Hier geben Sie den Namen des gewünschten PROXESS-Servers ein. Die Syntax hängt von dem Netzwerk ab, in dem Sie PROXESS installiert haben. Die PROXESS Administrator Console speichert den PROXESS-Servernamen, so dass Sie ihn bei der nächsten Anmeldung direkt übernehmen können.
Protokoll	Hier wählen Sie das Netzwerkprotokoll für die Verbindung zum Server aus. Beachten Sie, dass die Auswahlmöglichkeit der Protokollsequenz von den installierten Netzwerk-Komponenten abhängt. Wenn PROXESS Server und das vorliegende Modul auf einem Rechner installiert sind, wählen Sie die Einstellung "Lokaler Server".

Die PROXESS Server-Verbindung wird gespeichert. Sie brauchen sie nur anzupassen, wenn sich an den Einstellungen etwas geändert hat bzw. wenn Sie mit einem anderen Server arbeiten wollen.

Geben Sie Ihre Anmeldedaten ein und wählen Sie den Befehl **Anmelden**.

Direkt nach der Anmeldung sind Sie mit der Datenbank der letzten Session verbunden:

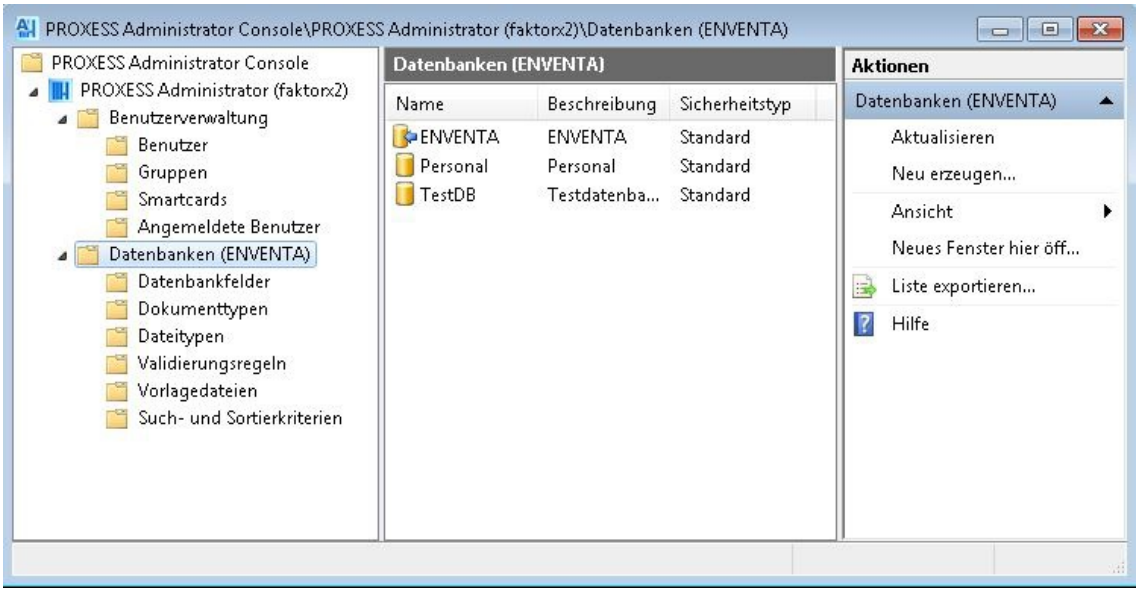


Abb: Dialog nach erfolgreicher Anmeldung

---

siehe auch:

Kennwort ändern

Datenbank verbinden

Zur Verwaltung einer Datenbank müssen Sie sich zuvor mit dieser Datenbank verbinden.

Haben Sie sich bereit erfolgreich am PROXESS-Server angemeldet, so werden Sie automatisch wieder mit der Datenbank Ihrer letzten Session verbunden. Möchten Sie eine andere Datenbank verwalten, müssen Sie sich erst mit dieser Datenbank verbinden.

Schritt für Schritt:

Selektieren Sie die Datenbank, mit der Sie sich verbinden möchten.

Wählen Sie im Menü "Aktion" (alternativ über das Kontextmenü) die Funktion "Verbinden".

Die aktuell verbundene Datenbank erkennen Sie am blauen Pfeilsymbol.

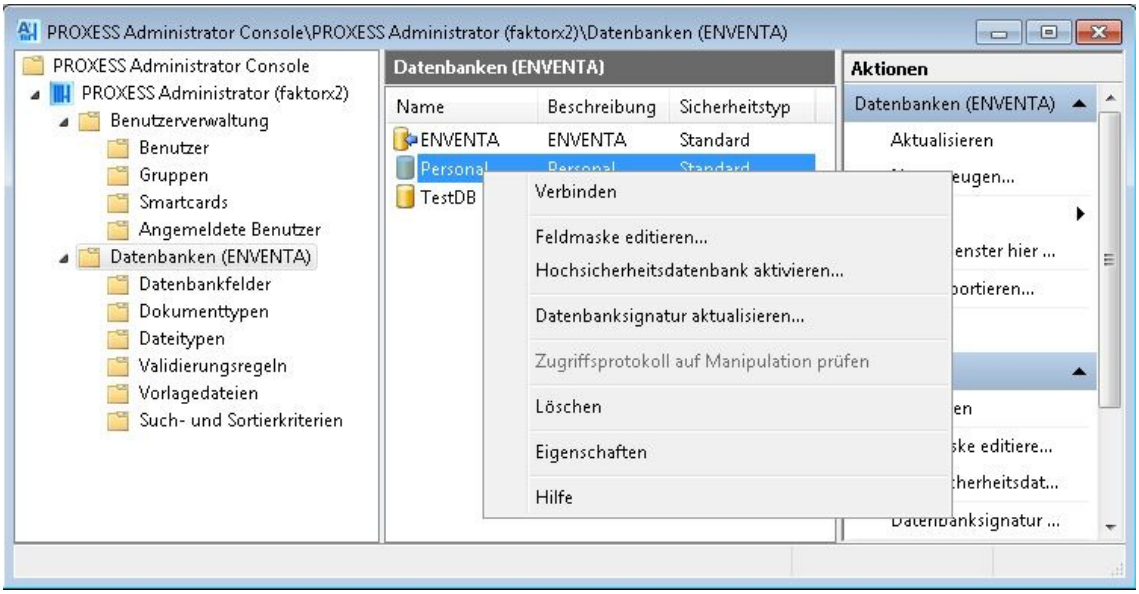


Abb.: Verbinden mit der Datenbank "Personal"

Supervisor-Kennwort zurücksetzen (OEM-Modus)

Wird PROXESS im OEM-Modus betrieben, kann das Supervisor-Kennwort von PROXESS zurückgesetzt werden.

Das Zurücksetzen des Supervisor-Kennworts steht im Betrieb mit Zertifikatsmodus NICHT zur Verfügung.

Falls Sie das Supervisors-Passwort vergessen haben, gibt es die Möglichkeit dieses durch die PROXESS GmbH zurückzusetzen.

Schritt für Schritt:

Bitte fordern Sie bei PROXESS ein Einmalpasswort an. Das Einmalpasswort wird von der PROXESS GmbH ausgestellt.

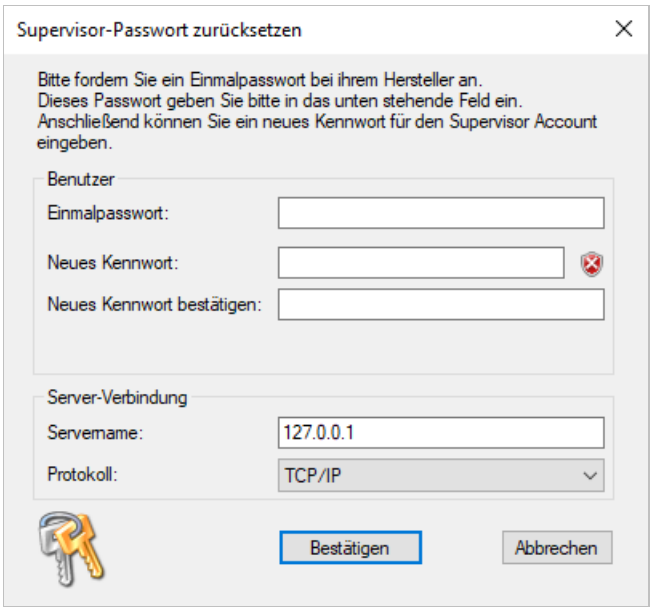
Wählen Sie im Menüpunkt "Sicherheit" den Befehl **Supervisor-Passwort zurücksetzen**.

Geben Sie hier das **Einmalpasswort** ein.

Nun können Sie selbst ein **neues Kennwort** für den Suervisor-Account vergeben unter Einhaltung der Kennwortrichtlinie.

Bestätigen Sie die Eingabe Ihres neuen Kennworts.

Unten geben Sie bitte Ihre PROXESS-Serververbindungsdaten an.



Zertifikate - Konzept und Übersicht

Vor dem ersten PROXESS-Systemstart muss ein einmaliger Zertifizierungsprozess durchgeführt werden. Zudem erstellen Sie die erste PROXESS-Supervisor Smartcard des Systems. Die notwendigen Schritte des Zertifizierungsprozesses führen Sie mit Hilfe der PROXESS Administrator Console durch. In diesem Zuge entstehen verschiedene Zertifikatsdateien und Zertifikatsdokumente. Diese sind für den sicheren laufenden Betrieb des Systems, für einen Systemumzug auf neue Hardware oder zur Wiederherstellung eines Systems nach Hardwareausfall notwendig. (siehe: Inbetriebnahme des Systems - Schritt für Schritt)

Folgende Dokumente und Dateien entstehen im Zuge des Zertifizierungsprozesses:

- **Request-Datei des PROXESS Systemzertifikates (.req):** Datei, die als Zertifikatsantrag an die PROXESS GmbH gesendet wird (Beispiel: proxess_Musterfirma_GmbH_SN2012c4fd.req)
- **PROXESS Systemzertifikatsantrag**: Ausdruck, der bei der Beantragung des PROXESS Systemzertifikats entsteht
- **privater Schlüssel (.pvk)**: Datei, die bei der Beantragung des PROXESS Systemzertifikats entsteht (Beispiel: proxess_Musterfirma_GmbH_SN2012c4fd.pvk)
- **PROXESS-Systemzertifikat (.cer):** Datei, die entsteht, wenn die PROXESS GmbH das Systemzertifikat gegengezeichnet hat (Beispiel: proxess_Musterfirma_GmbH_SN2012c4fd.cer)
- **PROXESS Systemzertifikat (.pfx):** Datei, die bei der Aktivierung des Systemzertifikats entsteht (Beispiel: proxess_Musterfirma_GmbH_SN2012c4fd.pfx)

Bei der Erstellung von PROXESS Supervisor Smartcards entstehen ebenfalls Zertifikatsdateien und Dokumente:

- **PROXESS Supervisorzertifikat (.pfx)**: (Beispiel: proxess-sv_Musterfirma_GmbH_SN0f4898a9.pfx)
- **PROXESS Supervisorzertifkat**: Ausdruck des PROXESS Supervisorzertifikats
- **Datei mit individuellen Smartcarddaten (.dmp):** Diese Datei wird an die PROXESS GmbH gesendet und in die individuelle Kundenlizenz eingearbeitet. Dieser Schritt ist nur für die erste PROXESS Supervisor Smartcard notwendig (Beispiel: proxess-sv_Musterfirma_GmbH_SN0f4898a9.dmp)

Warnhinweis:

	Ohne diese Dateien und Dokumente ist die spätere Erstellung zusätzlicher Smartcards für die Administration nicht möglich. Für diese Dateien und Dokumente muss ferner sichergestellt werden, dass Sie nicht in Hände Dritter gelangen, da hierdurch die Sicherheit der archivierten Dokumente nicht mehr gewährleistet werden kann. Die Dateien (.pvk, .cer, .pfx) sollten auf einen gesonderten Datenträger (z. B. Memory Stick, CD/DVD übertragen und an einem sichern Ort (Safe oder Notar) aufbewahrt werden. Die Lesbarkeit der Datenträger ist dabei sicherzustellen. Die PROXESS GmbH ist ausdrücklich nicht in der Lage, gültige Duplikate der Smartcard zu erstellen. Ohne vorgenannte Dateien und Dokumente ist die spätere Erstellung zusätzlicher Smartcards auch für die PROXESS GmbH nicht möglich.

Siehe auch:
Inbetriebnahme des Systems - Schritt für Schritt

Lizenzdateien

PROXESS benötigt zwei Lizenzdateien. Sie erhalten diese Lizenzdateien per E-Mail von der PROXESS GmbH, nachdem Sie den PROXESS Zertifizierungsprozess durchlaufen haben und im Rahmen der Erstellung der ersten PROXESS Supervisor Smartcard die Datei mit der Endung *.dmp* per Online-Formular (https://www.PROXESS.de/lizenzantrag.html) an PROXESS übertragen haben.

Sie erhalten zwei Dateien:

Lizenz.txt	**LizenzSec.txt**
LizenzSec.txt	**Kunden-Lizenzdatei**: Angaben des Zertifizierungsantrags und der ersten Supervisor Smartcard, Eintrag der Hochsicherheits-Datenbanken

Beide Dateien müssen sich im angegebenen Lizenzverzeichnis befinden. Die Angaben zum gültigen Lizenzverzeichnis werden im Programm "PROXESS Registry Setup" und "PROXESS Storage Manager Explorer" vorgenommen. In der Standardeinstellung ist dies das Arbeitsverzeichnis des PROXESS-Servers (z. B. C:\Programme\PROXESS\LizenzSigned.txt und C:\Programme\PROXESS\LizenzSec.txt).
Werden keine Angaben vorgenommen, greift PROXESS auf dieses Verzeichnis zurück.

Nach dem Einspielen der Lizenzdateien können Sie die Datenbanksignierung aktivieren.

Siehe auch:
Inbetriebnahme von PROXESS - Schritt für Schritt

PROXESS Supervisor Smartcard vorbereiten

Voraussetzungen:

- Sie haben bereits den Zertifizierungsprozess durchgeführt
- Sie haben eine gültige Systemzertikatsdatei (pfx-Datei) (siehe PROXESS Systemzertifikat aktivieren)

Schritt für Schritt:

Verbinden Sie den PROXESS Smartcard Reader per USB-Schnittstelle mit dem Computer

Legen Sie eine neue "leere" Smartcard in den Reader ein.

Starten Sie über Start/Programme das Programm Gemalto Classic Client Toolbox.

Wählen Sie im Menü "Card-Contents" den Befehl **Certificates.**

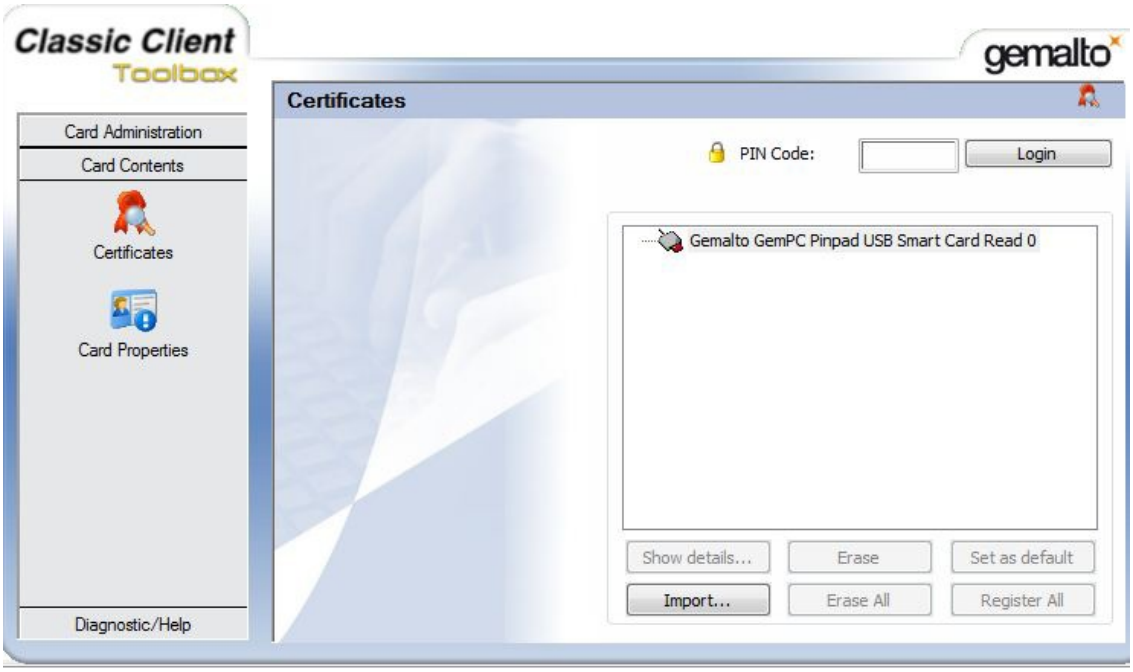


Abb.: Dialogfenster der Gemalto Classic Client Toolbox zum Import der Schlüsseldatei (.pfx).

Wählen Sie in der Auswahl "Import/Import from File" den Befehl **Open.**

Wählen Sie aus dem von Ihnen bereits gewählten Ablageverzeichnis die Datei mit der Endung .pfx aus, die Sie im Rahmen des Zertifizierungsprozesses im Menüpunkt "PROXESS Systemzertifikat aktivieren" erstellt haben.

Geben Sie im folgenden Dialog das Kennwort Ihres PROXESS Systemzertikatsantrages ein. (Das Kennwort finden Sie auf dem Ausdruck Ihres PROXESS Systemzertikatsantrags.)

Bestätigen Sie die Eingabe mit dem Befehl **Verify**.

Nach erfolgreicher Prüfung wird das zu importierende Zertifikat in der Auswahlliste angezeigt.

Wählen Sie das Zertifikat aus und geben Sie die PIN der eingelegten Smartcard ein. (Diese lautet im Auslieferungszustand: 1234).

Die Standard PIN sollten Sie im späteren Verlauf im Programm Gemalto Classic Client Toolbox im Menü "PIN Management" in eine individuelle PIN ändern (siehe PIN Verwaltung der PROXESS Supervisor Smartcards).

Bestätigen Sie Eingaben mit dem Befehl **Import**. Sie erhalten eine Bestätigung, dass das Zertifikat erfolgreich importiert wurde.

Der importierte Schlüssel wird nun im Menü "Certificates" angezeigt und ist Ihrem PROXESS-Systemzertifikat zugeordnet.

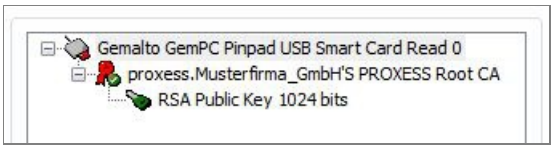


Abb.: Anzeige nach erfolgreicher Übertragung im Menü "Certificates"

Nun können Sie eine PROXESS Supervisor Smartcard erstellen.

Siehe auch:

PIN-Verwaltung der PROXESS Supervisor Smartcards

Inbetriebnahme des Systems - Schritt für Schritt

PROXESS Supervisor Smartcard erstellen

Voraussetzungen:

- Für diese Aktion benötigen Sie Supervisorprivilegien.
- Verbinden Sie den PROXESS Smartcard Reader per USB-Schnittstelle mit Ihrem Computer
- Sie benötigen eine vorbereitete Smartcard. Wie Sie eine Smartcard vorbereiten, erfahren Sie im Kapitel "PROXESS Supervisor Smartcard vorbereiten".

Schritt-für-Schritt:

Starten Sie die PROXESS Administrator Console und markieren Sie im Konsolenstamm den Knotenpunkt PROXESS Administrator ("Servername").

Wählen Sie entweder im Menü "Aktion" oder über das Kontextmenü oder über das Aktionspanel rechts den Menüpunkt"Zertifikate" und wählen Sie den Befehl **PROXESS Supervisorzertifikat erstellen**.

Wählen Sie ein Ablageverzeichnis für die Erstellung der Zertifikatsdateien aus, sowie einen Drucker zum Ausdruck Ihres PROXESS Supervisorzertikates.

Bestätigen Sie Ihre Eingaben mit dem Befehl **Erstellen**.

Im gewählten Ablageverzeichnis entstehen folgende Dateien:

proxess-sv_Musterfirma_GmbH_SN0f4898a9.pfx	Ergebnisdatei der Aktivierung des PROXESS Supervisorzertifikates.
proxess-sv_Musterfirma_GmbH_SN0f4898a9.dmp	Datei mit individuellen Smartcarddaten. Diese Datei wird später an die PROXESS GmbH gesendet und in die individuelle Kundenlizenz eingearbeitet. Dieser Schritt ist nur für die erste PROXESS Supervisor Smartcard notwendig.

Warnhinweis

	**Wählen Sie ein sicheres Ablageverzeichnis aus, sowie einen sicheren (lokalen) Drucker um unbefugten Zugriff zu vermeiden. Bei unbefugter Verwendung dieser Dokumente wird das PROXESS System potentiell unsicher. Bewahren Sie das entstehende PROXESS Supervisorzertifikat und die entstehenden Dateien an einem sicheren Ort auf.**

Während der Erstellung der Dateien werden Sie zur Eingabe Ihrer PIN aufgefordert. Achten Sie auf die Anzeige Ihres Smartcard Readers. (Die PIN lautet im Auslieferungszustand: 1234). Diese Standard PIN sollten Sie im späteren Verlauf im Programm Gemalto Classic Client Toolbox im Menü "PIN Management" in eine individuelle PIN ändern (siehe "PIN Verwaltung der PROXESS Supervisor Smartcards").

Starten Sie über Start/Programme/ das Programm Gemalto Classic Client Toolbox.

Wählen Sie im Menü "Card-Contents" den Befehl **Certificates**.

Wählen Sie in der Auswahl "Import/Import from File" den Befehl **Open**.

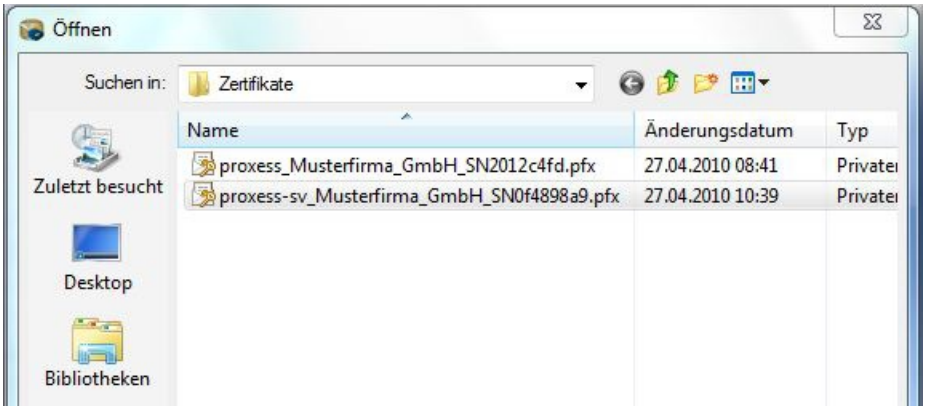


Abb.: Auswahl des PROXESS Supervisorzertikates für den Import (Beispielnamen)

Sie erkennen das PROXESS Supervisorzertifikat am Dateinamen "proxess-**sv**_SN<Seriennummer>.pfx.

Wählen Sie die das PROXESS Supervisorzertifikat aus und bestätigen Sie Ihre Auswahl mit dem Befehl **Import**.

Im folgenden Dialog müssen Sie nun das Kennwort Ihres PROXESS Supervisorzertifikates eintragen. Das Kennwort finden Sie auf dem Ausdruck Ihres PROXESS Supervisorzertifikates.

Nach erfolgreicher Prüfung wird Ihr Zertifikat in der Auswahlliste angeboten.

Wählen Sie das Zertifkat aus und starten Sie den Import mit dem Befehl **Import**. Sie erhalten eine Bestätigung, dass das Zertifikat erfolgreich importiert wurde.

Kontrolle: Der importierte Schlüssel wird jetzt im Menü "Certificates" angezeigt und ist Ihrem Supervisorzertifikat zugeordnet.

PROXESS Systemzertifikat aktivieren

Sobald Sie die gegengezeichnete Datei des Zertifikatsantrages (cer-Datei) von der PROXESS GmbH erhalten haben, können Sie Ihr Zertifikat aktivieren. Aktivierung heißt, dass Sie die Teile Ihres Zertfikates (pvk-Datei und cer-Datei) vom System zu einem funktionsfähigen Zertifikat (pfx-Datei) zusammensetzen lassen.

Schritt-für-Schritt:
Starten Sie die PROXESS Administrator Console und markieren Sie im Konsolenstamm den Zweig "PROXESS Administrator". Klicken Sie im Menü "Aktionen" auf "Zertifikate" und wählen Sie den Befehl **PROXESS Systemzertifikat aktivieren**.

Es erscheint folgendes Dialogfenster:

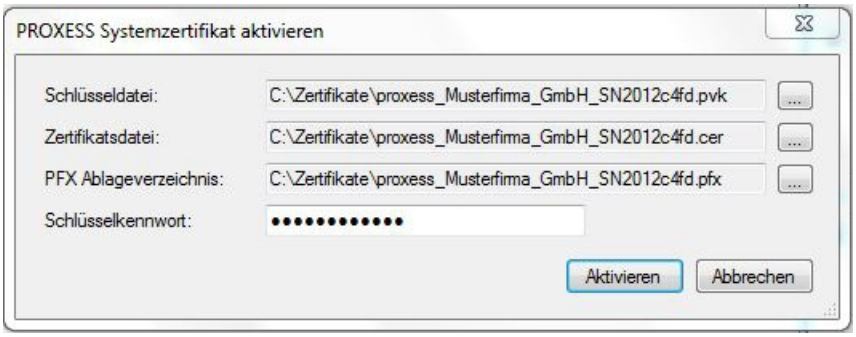


Abb: Dialogfeld zum Aktivieren des PROXESS Systemzertifikates

Wählen Sie zunächst den Speicherort der privaten Schlüssel-Datei (pvk-Datei) aus. Liegen alle notwendigen Dateien in einem Verzeichnis, so werden die Angaben zum PFX Ablageverzeichnis automatisch eingetragen.

In der Zeile Zertifikatsdatei geben Sie den Speicherort für Ihre von PROXESS gegengezeichnete cer-Datei an und wählen den Befehl **Aktivieren**. Sie erhalten eine Bestätigung, dass die Aktivierung erfolgreich durchgeführt wurde.

Verzeichnisinhalt nach erfolgreicher Aktivierung:

proxess_Musterfirma_GmbH_SN2012c4fd.req*	Request-Datei des PROXESS Systemzertifikates. Diese Datei wurde im vorangegangenen Schritt "PROXESS-Systemzertifikat beantragen" an die PROXESS GmbH gesendet.
proxess_Musterfirma_GmbH_SN2012c4fd.pvk*	Private Schlüsseldatei. Diese Datei ist das zentrale kryptographische Geheimnis zur Erstellung der Superivsor-Smartcards und muss daher sicher aufbewahrt werden.
proxess_Musterfirma_GmbH_SN2012c4fd.cer*	Individuelles PROXESS Systemzertifikat. Diese Datei hat die PROXESS GmbH an Sie übermittelt.
proxess_Musterfirma_GmbH_SN2012c4fd.pfx*	Ergebnisdatei der Aktivierung. Dies ist die Basisdatei zur Erstellung von Supervisor-Smartcards und muss daher sicher aufbewahrt werden.

* Beispieldateinamen

Warnhinweis

	**Durch unbefugte Verwendung der rot markierten Dateien (.pvk und .pfx), können sich Dritte Zugang zum System verschaffen. Verwahren Sie diese Dateien daher an einem sicheren Ort auf.**

Im nächsten Schritt können Sie das PROXESS Systemzertifikat installieren.

Siehe auch:

PROXESS Systemzertifikat beantragen

PROXESS Systemzertifikat installieren

PROXESS Systemzertifikat beantragen

Zu Beginn des Zertifizierungsprozesses erstellen Sie einen Systemzertifikatsantrag, den Sie an die PROXESS GmbH schicken müssen. Während der Erstellung des Systemzertifikatantrages werden zwei Dateien erzeugt. Die Datei mit der Endung **req** beinhaltet den Zertifizierungsantrag. Die Datei mit der Dateiendung **pvk** enthält einen privaten Schlüssel. Dieser beinhaltet das zentrale kryptographische Geheimnis der Smartcard-Erstellung und darf nicht in die Hände Dritter, auch nicht in die von der PROXESS GmbH gelangen. Zudem wird der Antrag als Papierausdruck ausgegeben.

Schritt für Schritt:
Starten Sie die PROXESS Administrator Console und markieren Sie im Konsolenstamm den Zweig "PROXESS Administrator". Klicken Sie im Menü "Aktionen" auf "Zertifikate" und wählen Sie den Befehl **PROXESS Systemzertifikat beantragen**.

Geben Sie im folgenden Dialogfenster Ihre Firmendaten ein:

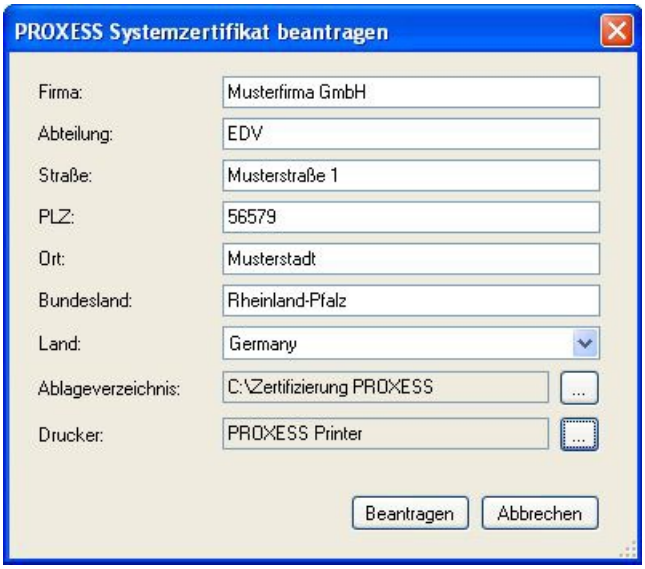


Abb.: Dialogfeld zur Beantragung eines PROXESS-Systemzertifikates

Ablageverzeichnis	Mit dem Antrag werden zwei Dateien erzeugt: - Die Datei mit der Endung req beinhaltet den Zertifizierungsantrag. - Die Datei mit der Dateiendung pvk enthält einen privaten Schlüssel. Beide Dateien werden in dem hier angegebenen Verzeichnis abgelegt. Aus Sicherheitsgründen empfiehlt der Hersteller ein geschütztes lokales Verzeichnis.
Drucker	Wählen Sie einen Drucker für den Ausdruck des Systemzertifikatsantrages aus. Aus Sicherheitsgründen empfiehlt der Hersteller einen lokalen Drucker.

Warnhinweis

	Der Ausdruck des PROXESS Systemzertifikatsantrages enthält ein Kennwort, das strengster Geheimhaltung unterliegt. Unbefugte könnten sich durch seine Kenntnis Zugang zu geschützten Archivdaten verschaffen. Bitte halten Sie diesen Antrag unter Verschluss und bewahren Sie ihn an einem sicheren Ort auf. Für den Ausdruck empfiehlt die PROXESS GmbH die Nutzung eines lokalen Druckers.

Bestätigen Sie Ihre Eingaben durch Anklicken der Schaftfläche **Beantragen.**

Im folgenden Dialogfenster werden Sie aufgefordert Ihren privaten Schlüssel durch die Eingabe des Kennwortes aus dem Systemzertifizierungsantrages zu sichern. Dieses Kennwort finden Sie auf dem Ausdruck des Systemzertifizierungsantrages.

Abbildung: Eingabedialog für Kennwort des privaten Schlüssels

Bestätigen Sie Ihre Eingabe mit **OK**. Der geschützte Systemzertifizierungsantrag wird nun erstellt und in dem oben angegebenen Ablageverzeichnis gespeichert.
Sie erhalten eine Bestätigung, dass der Vorgang erfolgreich durchgeführt wurde.

Übermitteln Sie den erzeugten Systemzertifizierungsantrag (**req**-Datei) an PROXESS per Online- Formular: https://www.PROXESS.de/zertifikatsantrag.html.

Nach kurzer Bearbeitungszeit erhalten Sie von PROXESS per E-Mail das digital gegengezeichnete PROXESS-Systemzertifikat (Datei mit der Endung **cer**). Dieses ist ausschließlich in Verbindung mit Ihrem bereits erzeugten privaten Schlüssel verwendbar und kann daher sicher per E-Mail übertragen werden.

Nun können Sie das PROXESS Systemzertifikat aktivieren.

Siehe auch:

PROXESS Systemzertifikat aktivieren

PROXESS Systemzertifikat installieren

Für diesen Schritt benötigen Sie Ihr PROXESS-Systemzertifikat (pfx-Datei). Hierfür müssen zuvor die Schritte "PROXESS Systemzertifikat beantragen" und "PROXESS Systemzertifikat aktivieren" durchgeführt worden sein. Mit dem Befehl "PROXESS Systemzertifikat installieren" geben Sie Ihrem PROXESS System die pfx-Datei als gültige Zertifikatsdatei bekannt.

Schritt-für-Schritt:
Starten Sie die PROXESS Administrator Console und markieren Sie im Konsolenstamm den Zweig "PROXESS Administrator". Klicken Sie im Menü "Aktion" auf "Zertifikate" und wählen Sie den Befehl **PROXESS Systemzertifikat installieren**.

Es erscheint folgendes Dialogfenster:

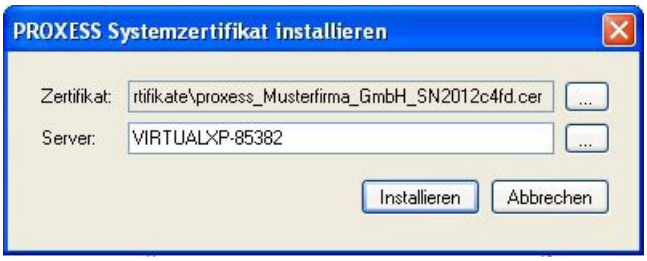


Abb: Dialogfeld zum Installieren des PROXESS Systemzertifikates

Als Zertifikat wählen Sie Ihr PROXESS-Systemzertifikat aus. Dieses haben Sie im Rahmen des Schrittes "PROXESS-Systemzertifikat beantragen" an die PROXESS GmbH übertragen und von dort digital gegengezeichnet per E-Mail wieder erhalten.

Im Feld "Server" tragen Sie bitte die IP-Adressen bzw. den Namen Ihres PROXESS-Servers ein. Bei einem verteilten System ist dies der Rechner, auf dem der PROXESS Document Manager installiert ist.

Bestätigen Sie Ihre Eingaben durch Anklicken der Schaltfläche **Installieren**.

Sie erhalten eine Bestätigung, dass die Aktion erfolgreich durchgeführt wurde.

Im nächsten Schritt können Sie eine Supervisor-Smartcard vorbereiten und erstellen.

Siehe auch:
PROXESS Supervisor Smartcard vorbereiten

PROXESS Supervisor Smartcard erstellen

Sicherheitsfunktionen - Konzept und Überblick

Das PROXESS-Sicherheitskonzept umfasst vier Hauptfunktionen:

Supervisor-Authentifizierung mittels Smartcard und PIN: Supervisorprivilegien benötigen Sie für die Vergabe von Berechtigungen, für die Delegation von Verwaltungstätigkeiten sowie für die Aktivierung weiterer optionaler Sicherheitsfunktionen.
Datenbanksignierung: PROXESS bildet eine Signatur über relevante Datenbankfelder und bietet so Schutz vor Manipulationen der Datenbankeinträge. Diese Funktion ist für die PROXESS Verwaltungsdatenbank verbindlich und für einzelne PROXESS Archivdatenbanken optional.
Feldverschlüsselung: Einzelne Felder einer Datenbank werden verschlüsselt gespeichert (optional).
Dateiverschlüsselung: Dateien eines Dokumenttyps werden verschlüsselt gespeichert (optional).

Sie können sich für einen Systembetrieb mit oder ohne Sicherheitsfunktionen entscheiden. Dies hängt von Ihrem Sicherheitsbedürfnis bzw. von der Schutzwürdigkeit der archivierten Dokumente ab. Beispielsweise sind personenbezogene Dokumente wie Gehaltsabrechnungen oder Bewerbungsunterlagen sensible Informationen und damit schutzwürdiger als Wareneingangsrechnungen einzustufen.

Systembetrieb ohne Sicherheitsfunktionen

Wenn Sie sich für einen Systembetrieb ohne Sicherheitsfunktionen entscheiden, müssen nur zwei Standardsicherheitsfunktionen aktiviert und genutzt werden.

Hierzu gehört die Anmeldung über Smartcard und PIN des Supervisors. Diese ist notwendig, um die Benutzer- und Zugriffsrechteverwaltung durchzuführen bzw. um Bereichsadministratoren für die weitere Benutzer- und Zugriffsrechteverwaltung in diesem Bereich zu ernennen. So kann der Supervisor (in der Regel ein Mitglied der Geschäftsleitung) beispielsweise den Personalleiter als Bereichsadministrator für das Personalarchiv ernennen. Konkret erhält der Personalleiter für die Archivdatenbank "Personal" Verwaltungsrechte.

Die Datenbanksignierung ist die zweite notwendige Bedingung auch für einen Systembetrieb ohne Sicherheitsfunktionen. Sie bewirkt eine Signierung der PROXESS-Verwaltungsdatenbank in der zugrundeliegenden SQL-Datenbank. Diese Verwaltungsdaten werden in der sogenannten PROXESS DB gespeichert. Hierzu zählen unter anderem auch Benutzerverwaltungsdaten. Durch die Signierung der zugehörigen Datensätze werden manipulative Eingriffe über die SQL-Ebene transparent.

Beispiel: Wird ein PROXESS Benutzer, ohne Zugriff auf die Archivdatenbank "Personal" per SQL-Befehl zum Mitglied einer Gruppe , die Zugriffsrechte auf die Archivdatenbank "Personal" besitzt, erkennt das System die Manipulation und sperrt das Benutzerkonto.

Systembetrieb mit Sicherheitsfunktionen

Entscheiden Sie sich für einen Systembetrieb mit Sicherheitsfunktionen, werden in PROXESS zusätzliche Sicherheitsfunktionen angeboten.

Aktivieren Sie eine PROXESS-Archivdatenbank als Hochsicherheitsdatenbank, bewirkt dies zunächst die Verschlüsselung der in der Volltextdatenbank gespeicherten Beziehungen zu PROXESS Dokumenten. Desweiteren wird so die Voraussetzung geschaffen, dass SQL-Feldinhalte und Inhalte der in PROXESS archivierten Dateien verschlüsselt werden können. Eine tatsächliche Verschlüsselung von SQL-Feldinhalten findet allerdings erst dann statt, wenn dies im Programm PROXESSS Administrator auf Datenbankebene konfiguriert wird.

Weitere Voraussetzungen für die Konfiguration von Feldern oder Dateien als verschlüsselt ist die Initialisierung der

Datei- und Feldverschlüsselung. **Bei der Initialisierung der Datei- und Feldverschlüsselung werden Kennwörter für den Verschlüsselungsalgorithmus erzeugt und ausgedruckt. Diese Kennwörter benötigen Sie zwingend im Rahmen einer Systemwiederherstellung oder eines Hardwarewechsels. Ohne Kennwörter können die verschlüsselten Daten und Dateien nicht wieder lesbar gemacht werden.**

In beiden Fällen erhalten Sie von der PROXESS GmbH vor der Inbetriebnahme des Systems eine Erklärung, in der Sie auf die Wichtigkeit der Zertifikats- und Verschlüsselungskennwörter hingewiesen werden. Diese Erklärung ist vor Inbetriebnahme des Systems unterschrieben an die PROXESS GmbH zurückzugeben.

Die Tabelle fasst die Ausführungen nochmals zusammen:

Sicherheitsfunktion	Systembetrieb ohne Sicherheitsfunktionen	Systembetrieb mit Sicherheitsfunktionen	Wirkung
Anmeldung über Smartcard und PIN	ja	ja	notwendig um Benutzerverwaltung und Zugriffsrechteverwaltung durchzuführen
Signierung der PROXESS Verwaltungsdatenbank	ja	ja	Metadatenschutz für Benutzerverwaltung Konsistenzprüfung der Benutzerdaten
Hochsicherheitsdatenbank	nein	ja	Voraussetzung für Verschlüsselung von Standardfeldern und Dateiverschlüsselung pro Dokumenttyp in dieser Datenbank Aktivierung der Volltext-DB-Verschlüsselung Eintrag in Lizenz notwendig
Dateiverschlüsselung	nein	ja	dient dem Schutz der Dokumentdatensätze in der SQL-DB Konfiguration pro Standardfeld nur in Hochsicherheits-DB´s möglich

Feldverschlüsselung	nein	ja	dient dem Schutz der PROXESS-Dateiinhalte Konfiguration pro Dokumenttyp nur in Hochsicherheitsdabenbanken möglich

---

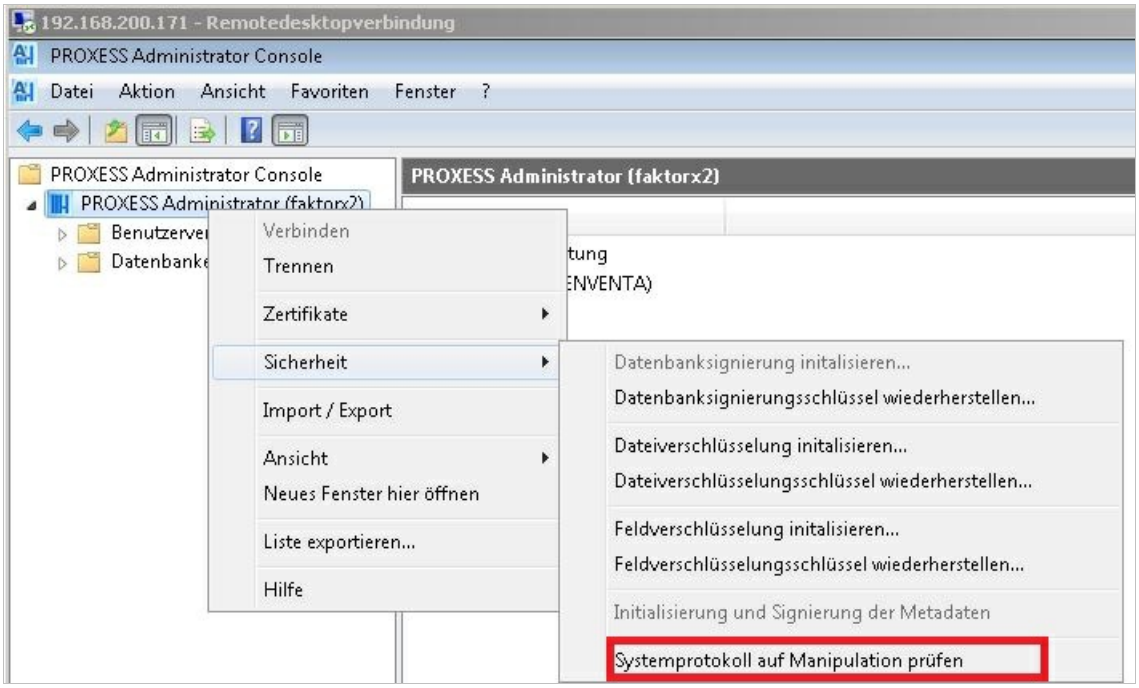
Siehe auch:

Protokollierung

Inbetriebnahme des Systems- Schritt für Schritt-Anleitung

Systemprotokoll

Das Systemprotokoll sollte regelmäßig auf Manipulationen geprüft werden:



Untenstehende Liste gibt einen Überblick über alle PROXESS-Ereignisse, die im Systemprotokoll erfasst werden. Mit Hilfe von mitgelieferten SQL-Skripten können Sie Auswertungen des Protokolls vornehmen. (siehe: Datenbanksicherheit (Protokollierung).

SQL-Tabelle: SystemMetaLog
SQL-Datenbank: PROXESS MasterDB
Funktion: alle Konfigurationsereignisse protokollieren

Event	Event ID	Erläuterung
eDBCREATE	1	Datenbank: Neu anlegen
eDBUPDATE	2	Datenbank: Beschreibung ändern
eDBDELETE	3	Datenbank: Löschen
eDBRGRANT	4	Datenbank: Rechte vergeben
eDBRREVOKE	5	Datenbank: Rechte entziehen
eDBRREMOVE	6	Datenbank: Rechte löschen
eDBPURGE	7	Datenbank: Löschverhalten konfigurieren

eDBLOG	8	Datenbank: Ereignisprotokoll aktivieren
eDTCREATE	9	Dokumenttyp: Neu anlegen
eDTUPDATE	10	Dokumenttyp: Eigenschaften ändern
eDTDELETE	11	Dokumenttyp: Löschen
eDTRGRANT	12	Dokumenttyp Rechte vergeben
eDTRREVOKE	13	Dokumenttyp: Rechte entziehen
eDTRREMOVE	14	Dokumenttyp Rechte löschen
eDT_FIELDNEW	15	Dokumenttyp: Feld neu anlegen
eDT_FIELDUPDATE	16	Dokumenttyp: Feld Eigenschaften ändern
eDT_FIELDDELETE	17	Dokumenttyp: Löschen
eDT_DEL_KFT	18	Dokumenttyp Aufbewahrungsfrist: Ausnahme für einen Dateityp löschen
eFTCREATE	19	Dateityp: Neu anlegen
eFTUPDATE	20	Dateityp: Eigenschaften ändern
eFTDELETE	21	Dateityp: Löschen
eFT_FILEASSIGN	22	Dateityp: Verknüpfung zu Vorlagedatei erstellen
eFT_FILEREMOVE	23	Dateityp: Verknüpfung zu Vorlagedatei entfernen
eEDCREATE	24	Editor: neu anlegen
eEDUPDATE	25	Editor: Eigenschaften ändern
eEDDELETE	26	Editor: löschen
eFIELDCREATE	27	Feld: Neu anlegen
eFIELDUPDATE	28	Feld: Eigenschaften ändern
eFIELDDELETE	29	Feld: Löschen
eUDISABLE	30	Benutzer: Sperren/Entsperren

eUG_ASSIGN	31	Benutzer: Einer Gruppe zuweisen
eUG_REMOVE	32	Benutzer: Aus seiner Gruppe entfernen
eUNEW	33	Benutzer: Neu anlegen
eUMODIFY	34	Benutzer: Eigenschaften ändern
eUDELETE	35	Benutzer: Löschen
eUPASSCHANGE	36	Benutzer: Kennwort vom Administrator geändert
eUMY_PASSCHANGE	37	Benutzer: Ändert sein Kennwort selbst
eGNEW	38	Gruppe: Neu anlegen
eGMODIFY	39	Gruppe: Eigenschaften ändern
eGDELETE	40	Gruppe: Löschen
eVRNEW	41	Validierungsregel: Neu anlegen
eVRUPDATE	42	Validierungsregel: Eigenschaften ändern
eVRDELETE	43	Validierungsregel: Löschen
eVRASSIGN	44	Validierungsregel: Feldverknüpfung erstellen
eVRCANCEL	45	Validierungsregel: Feldverknüfung aufheben
eVRTHES	46	NICHT belegt
eCERTNEW	47	Zertifikat: Neu anlegen
eCERTUPDATE	48	Zertifikat: Eigenschaften ändern
eALLGRANT	49	Bulk Rechte (der Admin-Gruppe alle Rechte geben)
eMASTERKEY	50	Masterkey: Neu anlegen
eSIGNDOCS	51	Signieren: Hochsicherheitsdatenbank
eSIGNMETA	52	Signieren: Metadaten
ePROFILENEW	53	Profil: Neu anlegen
ePROFILEDELETE	54	Profil: Löschen

ePROFILEUPDATE	55	Profil: Eigenschaften ändern

Das Protokoll selbst ist durch mitgeführte Hashwerte und eine Verknüpfung des betreffenden Protokolleintrages auf seinen jeweiligen Vorgänger und Nachfolger vor Manipulation gesichert.

---

siehe auch:

Datenbankprotokollierung (Sicherheit)l

Dateiverschlüsselung

Dateiverschlüsselung in PROXESS bedeutet, dass die Inhalte der in PROXESS archivierten Dateien verschlüsselt werden. Die Dateiverschlüsselung muss zuvor durch den Supervisor in der PROXESS Administrator Console initialisiert werden. Die Initialisierung der Dateiverschlüsselung ist ein einmaliger Vorgang und kann nicht rückgängig gemacht werden. Ob Sie die Dateiverschlüsselung initialisieren hängt davon ab, ob Sie sich für einen Systembetrieb mit Sicherheitsoptionen oder für einen Systembetrieb ohne Sicherheitsoptionen entschieden haben.

Erst nach der Initialisierung kann die Dateiverschlüsselung über die Eigenschaften eines Dokumenttyps gesteuert werden. Diese Einstellung wird im Programm PROXESS Administrator vorgenommen. Die Dateiverschlüsselung für Dokumenttypen kann nur in den PROXESS Datenbanken eingestellt werden, die zuvor als Hochsicherheitsdatenbank aktiviert wurden.

Das Setzen der Option "Dateiverschlüsselung" für einen Dokumenttyp im Programm PROXESS Administrator bewirkt keine rückwirkende Verschlüsselung bereits archivierter Dateien dieses Dokumenttyps. Erst ab dem Zeitpunkt, ab dem der Administrator für einen Dokumenttyp die Dateiverschlüsselung aktiviert hat, werden die Dateien verschlüsselt.

Dateiverschlüsselung initialisieren

Verbinden Sie sich als Supervisor mit Ihrer Smartcard mit dem eingetragenen "PROXESS Administrator".
Wählen Sie im Menü "Aktion/Sicherheit" den Befehl **Dateiverschlüsselung initialisieren**.

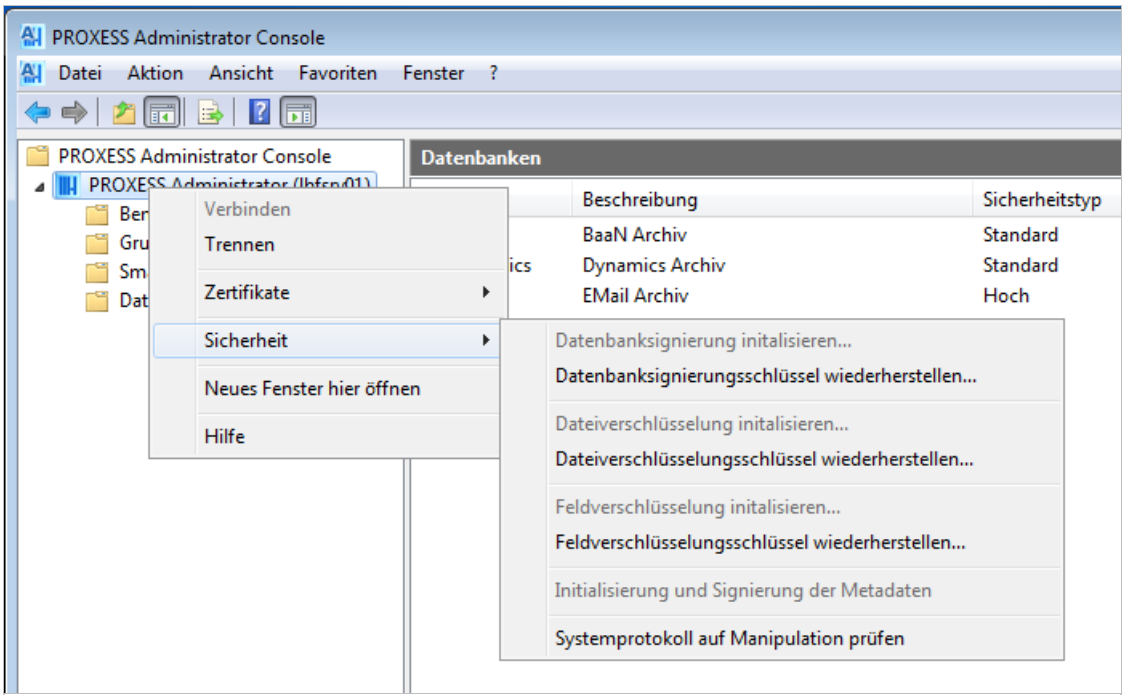


Abb.: Menü "Aktion/Sicherheit"

Wählen Sie einen Drucker für den Ausdruck "PROXESS Hauptschlüssel-Dateiverschlüsselung" aus. Wählen Sie aus Sicherheitsgründen einen lokalen Drucker oder nicht öffentlich zugänglichen Drucker aus. (Wählen Sie keinen PDF-Drucker o.a. aus, da die Gefahr besteht, dass Ihre Kennwort-Datei versehentlich überschrieben wird.)
Bestätigen Sie Ihre Auswahl mit dem Befehl **Initialisieren**.
Ihre Änderungen werden erst nach einem **Neustart des PROXESS-Systems** wirksam.

Warnhinweis

	**Bewahren Sie den entstehenden Ausdruck "PROXESS Hauptschlüssel - Dateiverschlüsselung" sicher auf. Dieser Ausdruck enthält ein Schlüsselkennwort für den Algorithmus der Dateiverschlüsselung. Ohne dieses Kennwort ist es nicht möglich, verschlüsselte Dateien zum Beispiel nach einem Austausch der Hardware, wieder zu entschlüsseln und wieder im Originalformat anzuzeigen. Geht der Hauptschlüssel-Dateiverschlüsselung verloren, so entsteht Datenverlust!**

Dateiverschlüsselung wiederherstellen

Die Wiederherstellung der Dateiverschlüsselung ist z. B. nach einem Austausch der Systemhardware notwendig.

Verbinden Sie sich als Supervisor mit Smartcard mit dem eingetragenen "PROXESS Administrator".
Wählen Sie im Menü "Aktionen/Sicherheit" den Befehl **Dateiverschlüsselung wiederherstellen**.
Geben Sie das Kennwort des Ausdrucks "PROXESS Hauptschlüssel - Dateiverschlüsselung" ein.
Bestätigen Sie Ihre Eingabe dem Befehl **Wiederherstellen**.
Ihre Änderungen werden erst nach einem **Neustart des PROXESS-Systems** wirksam.

Siehe auch:

Hochsicherheitsdatenbank aktivieren

Datenbanksicherheit (Protokollierung)

Zugriffsprotokoll

In diesem Protokoll werden alle Zugriffe auf archivierte Dokumente und Dateien erfasst. Im Protokoll werden PROXESS-Benutzername, Uhrzeit und Datum und die Art des Zugriffs festgehalten. Bei der Art des Zugriffs wird unterschieden in "Anlegen", „Lesen“, „Ändern“ oder „Löschen“. Das Protokoll kann durch den Supervisor oder Datenbankverwalter pro Datenbank aktiviert/deaktiviert werden.

Das Protokoll selbst ist durch mitgeführte Hashwerte und eine Verknüpfung des betreffenden Protokolleintrages auf seinen jeweiligen Vorgänger und Nachfolger vor Manipulation gesichert.

Zugriffsprotokoll aktivieren und einrichten

Verbinden Sie sich als Supervisor oder Datenbank-Bereichsadministrator mit dem System.

Wählen Sie die gewünschte Datenbank aus.

Wählen Sie im Menü Aktion den Menüpunkt "Eigenschaften" (alternativ über das Kontextmenü).

Nun wählen Sie den Reiter "Sicherheit":

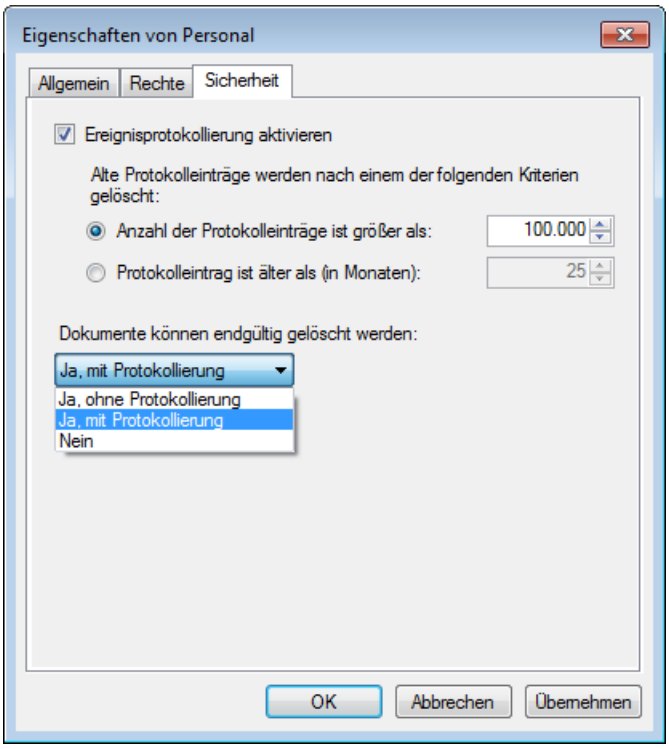


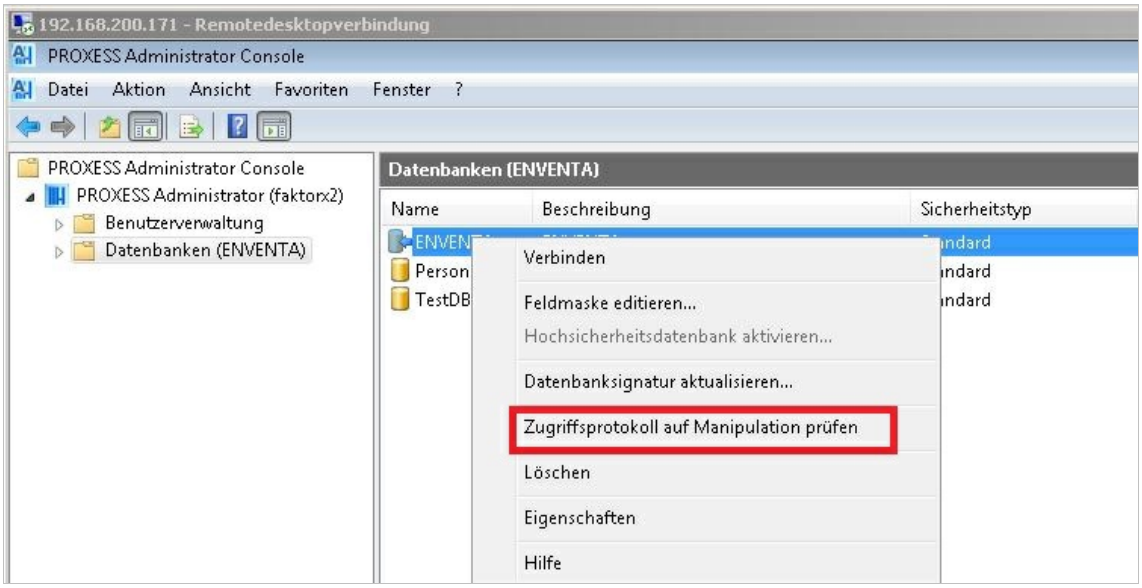
Abb: Einstellungen zur Protokollierung auf Datenbankebene am Beispiel der DB "Personal"

Mögliche Einstellungen der Zugriffsprotokollierung.

Ereignisprotokollierung aktivieren	Aktivieren/Deaktivieren Sie hier die Protokollierung von Benutzerzugriffen auf die Dokumente für die ausgewählte Datenbank. Standardmäßig ist die Protokollierung nicht aktiviert.

Protokolleinträge löschen	Aus Performancegründen können Sie entweder mengenabhängig oder zeitabhängig ältere Protokolleinträge automatisch löschen lassen. Hier sind Werte zwischen 100.000 und 1.000.000 erlaubt. Hier sind Werte ab 25 Monaten erlaubt.

Die Konsistenz des Protokolls sollte regelmäßig durch den Supervisor oder Datenbankverwalter geprüft werden:



Statistische Auswertungen der Zugriffsprotokollierung:

Über die mitgelieferte PROXESS Report Console können Sie Benutzerzugriffe auf Dokumente und Dateien filtern und darstellen. Basis der Auswertungen ist das hier aktivierte PROXESS-Zugriffsprotokoll.
Die Auswertungen können als xls- oder csv-Datei exportiert werden. Weitere Informationen finden Sie in der Moduldokumentation der PROXESS Report Console.

Beispiele für betriebswirtschaftliche und organisatorische Auswertungen:

- Anzahl der Dokumentzugriffe je Benutzergruppe mit dem Ziel einer Kostenumlage der PROXESS DMS-Kosten.
- Zeitraumbezogene Statistik der Dokumentzugriffe je Benutzergruppe, für bestimmte durchgeführten Aktionen etc.
- Häufigkeit von Zugriffen/Änderungen bezogen auf einen bestimmten Dokumenttyp (z. B. Kaufverträge).

Protokollierung von Löschvorgängen

Benutzer mit Löschberechtigung können archivierte Dokumente zwar zur Löschung markieren, aber aus Sicherheitsgründen nicht endgültig aus dem System entfernen. Die vorgemerkten Dokumente können in PROXESS erst durch einen PROXESS-Administrator endgültig gelöscht oder wiederhergestellt werden, Um den unterschiedlichen gesetzlichen Vorgaben verschiedener Dokumenttypen zur Aufbewahrung und zur Vernichtung von Unternehmensdokumenten (z. B. bei Personaldokumenten) Rechnung zu tragen, können Sie für jede Archivdatenbank Einstellungen zum Löschverhalten und der Protokollierung des Löschvorgangs treffen.

Konfiguration zur Löschprotokollierung:

Verbinden Sie sich als Supervisor oder Datenbank-Bereichsadministrator mit dem System, wählen Sie die gewünschte Datenbank aus. Wählen Sie im Menü Aktion den Menüpunkt "Eigenschaften" (alternativ über das Kontextmenü). Nun wählen Sie den Reiter "Sicherheit" (siehe Abb. oben):

Mögliche Einstellungen zur Protokollierung des Löschvorgangs:

Dokumente endgültig löschen....	
Nein **Ja, mit Protokollierung** **Ja, ohne Protokollierung (Standardeinstellung)**	Es ist keine endgültige Löschung von Dokumenten möglich. Alle Dokumente werden mit der Möglichkeit der Wiederherstellung im System vorgehalten. Vom Benutzer gelöschte Dokumente können allerdings nicht gesucht werden und werden damit bei einer Recherche nicht mehr angezeigt. Dokumente, die vom Administrator endgültig gelöscht werden, werden im Löschprotokoll vermerkt. Der Löscheintrag beinhaltet den ausführenden PROXESS-Benutzer, den Zeitpunkt der Löschung sowie alle Inhalte des Dokuments zum Zeitpunkt der Löschung. Eine endgültige Löschung von Dokumenten durch den Administrator ist möglich, es werden keine Einträge über Dokumentinhalte im Löschprotokoll vorgenommen.

	Das Löschprotokoll finden Sie als SQL-Tabelle "LogInfo" in der jeweiligen Datenbank und kann über herkömmliche SQL-Tools eingesehen werden.

Systemprotokollierung

Änderungen an Metadaten und zentralen Einstellungen werden in einem zentralen Systemprotokoll festgehalten. Zu den im Systemprotokoll protokollierten Vorgängen gehören unter anderem das Anlegen oder Löschen von Feldern, Dokumenttypen oder von Benutzern und Gruppen. Eine Liste aller im Systemprotokoll erfassten Ereignisse ist im Kapitel Liste der Log-Events im Systemprotokoll aufgeführt.

Ebenso wie beim Zugriffsprotokoll sind die Protokolleinträge durch Hashwerte und eine Verknüpfung auf Vorgänger und Nachfolger vor Manipulation gesichert. Über die Systemprotokollierung können manipulative Zugriffe an den Systemeinstellungen sichtbar gemacht werden. Das Systemprotokoll kann nicht deaktiviert werden.

Eine Überprüfung/Auswertung des Systemprotokolls sollten Sie regelmäßig vornehmen, um manipulative Eingriffe zu erkennen, Verbinden Sie sich hierzu mit dem System als Supervisor. Wählen Sie Ihr PROXESS-System aus und wählen Sie im Menü Aktion/Sicherheit die Funktion: Systemprotokoll auf Manipulation prüfen.

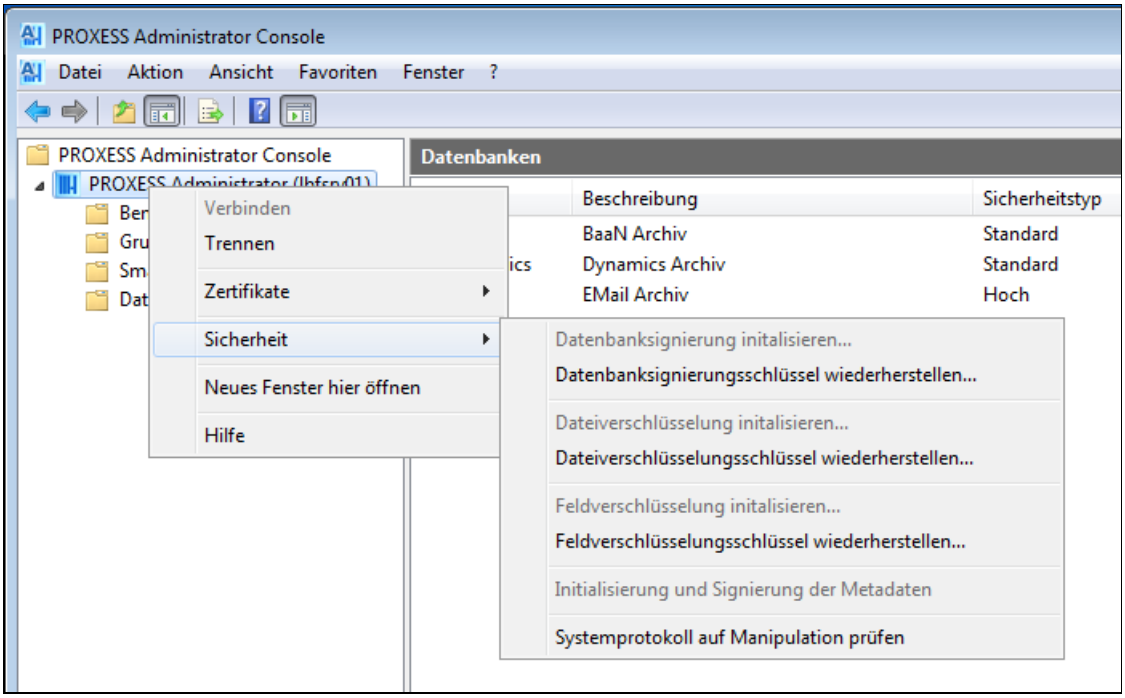


Abb: Menü Sicherheit

Statistische Auswertungen der Systemprotokollierung:

Im Programmumfang werden SQL-Skripte mitgeliefert, mit Hilfe derer Sie Auswertungen zu den Änderungen an den PROXESS-Systemeinstellungen durchführen können. Über diese Auswertungen können Sie Konfigurationsänderungen bezogen auf Datenbanken, Dokumenttypen etc. nachvollziehen. Die Abfrageergebnisse können unter anderem als CSV-Datei gespeichert werden.

Beispiele zu möglichen Auswertungen:

- Welcher Benutzer hat welchen Benutzern oder Gruppen welche Rechte auf eine bestimmte Datenbank zugewiesen?
- Welcher Benutzer hat welche anderen Benutzer wann in eine bestimmte Gruppe aufgenommen?
- Welcher Benutzer hat in einer bestimmten Datenbank welche Dokumenttyprechte an wen vergeben?

a) gefiltert für einen bestimmten Dokumenttyp
b) zusätzlich gefiltert für nur eine bestimmte Gruppe

siehe auch:
Liste der Log-Events im Systemprotokoll

Datenbanksignierung (Verwaltungsdatenbank)

Mit der Signierung der Verwaltungsdatenbank werden Metadaten wie Verwaltungsdaten von Benutzern, Gruppen und Rechten vor unberechtigten Zugriffen von außen (z. B. über externe SQL-Tools) geschützt. Wird zum Beispiel die Gruppenzugehörigkeit eines Benutzers über einen externes SQL-Befehl manipulativ verändert, erkennt das PROXESS-System diese Manipulation und sperrt das betroffene Benutzerkonto. Die Datenbanksignierung macht somit unberechtigte Zugriffe und Manipulationen an den Verwaltungsdaten sichtbar.

Die Initialisierung der Datenbanksignierung ist Voraussetzung für den Betrieb von PROXESS. Sie muss auch dann initialisiert werden, wenn Sie keine weiteren Verschlüsselungsoptionen, also einen Systembetrieb ohne Sicherheitsfunktionen, wählen möchten. Ist die Datenbanksignierung noch nicht initialisiert worden, können sich auch keine Benutzer am System anmelden bzw. mit einer Datenbank verbinden.

Für die nachstehend beschriebenen Funktionen "Datenbanksignierung initialisieren", "Datenbanksignierung wiederherstellen" und "Initialisierung und Signierung der Metadaten" benötigen Sie Supervisorprivilegien.

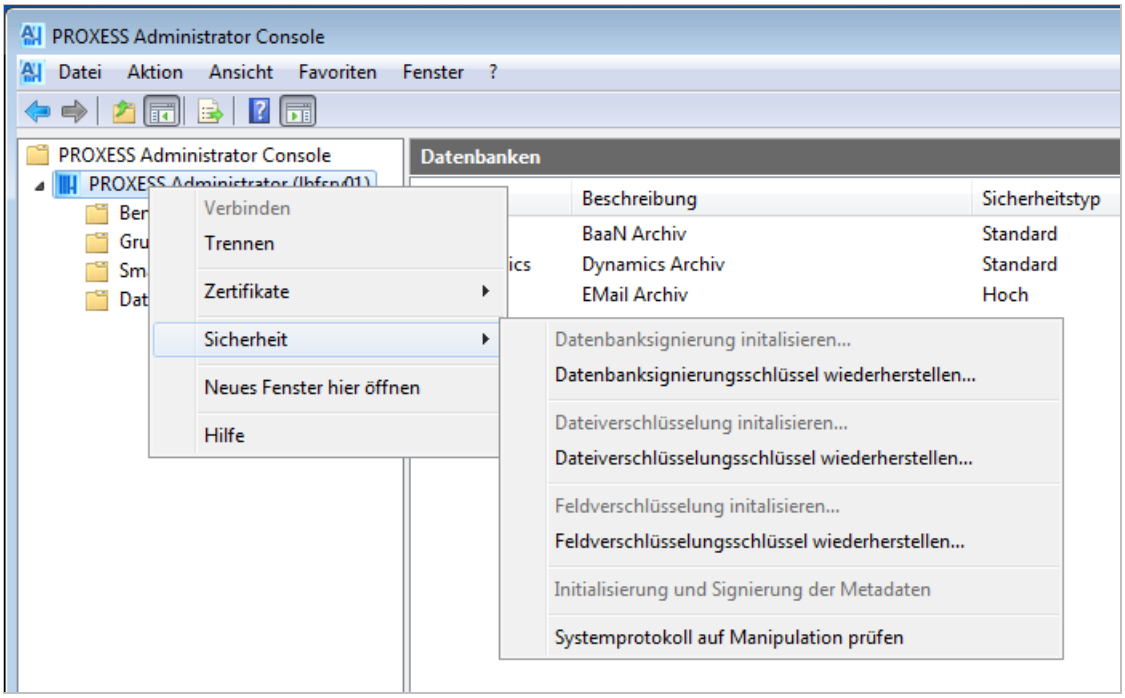


Abb.: Menü "Aktion/Sicherheit"

Datenbanksignierung initialisieren

Wählen Sie einen Drucker für den Ausdruck "PROXESS Hauptschlüssel - Datenbanksignierungsschlüssel" aus. Wählen Sie aus Sicherheitsgründen einen lokalen Drucker oder nicht öffentlich zugänglichen Drucker aus. (Wählen Sie keinen PDF-Drucker o. ä. aus, da die Gefahr besteht, dass Ihre Kennwort-Datei versehentlich überschrieben wird.)
Bestätigen Sie Ihre Auswahl mit dem Befehl **Initialisieren**.
Ihre Änderungen werden erst nach einem **Neustart des PROXESS-Systems** wirksam.

Warnhinweis

	**Bewahren Sie den entstehenden Ausdruck "PROXESS Hauptschlüssel - Datenbanksignierung" sicher auf. Dieser Ausdruck enthält ein Schlüsselkennwort, das für eine eventuelle Wiederherstellung der Datenbanksignierung z. B. nach einem Austausch der Hardware notwendig ist. Ohne dieses Kennwort ist es nicht möglich, das System durch den Anwender selbstständig wieder in Betrieb zu nehmen. Die Datenbanksignierung muss dann kostenpflichtig durch die PROXESS GmbH neu initialisiert werden.**

Datenbanksignierung wiederherstellen

Die Wiederherstellung der Datenbanksignierung ist z. B. nach einem Austausch der Systemhardware notwendig.

Verbinden Sie sich als Supervisor mit Smartcard mit dem eingetragenen "PROXESS Administrator".
Wählen Sie im Menü "Aktionen/Sicherheit" den Befehl **Datenbanksignierung wiederherstellen**.
Geben Sie das Kennwort des Ausdrucks "PROXESS Hauptschlüssel - Datenbanksignierungsschlüssel" ein.
Bestätigen Sie Ihre Eingabe dem Befehl **Wiederherstellen**.
Ihre Änderungen werden erst nach einem **Neustart des PROXESS-Systems** wirksam.

Initialisierung und Signierung der Metadaten

Diese Funktion benötigen Sie nur bei einem Update von PROXESS 5.0 auf PROXESS 5^{+}. Mit dem Befehl werden neue Datenbankfelder der Verwaltungsdatenbank in die Datenbanksignierung mit aufgenommen. Bei einer Neuinstallation von PROXESS 5^{+} müssen Sie diesen Befehl nicht ausführen.

Siehe auch:
Hochsicherheitsdatenbank aktivieren

Feldverschlüsselung

Feldverschlüsselung in PROXESS bedeutet, dass einzelne Datenbankfeldinhalte einer in PROXESS als Hochsicherheitsdatenbank aktivierten Archivdatenbank verschlüsselt werden. Datenbankfeldinhalte sind die eingetragenen Suchkriterien eines Dokumentes. Bei einer Personaldatenbank können dies z. B. die Personalnummer und der Name eines Mitarbeiters sein. Möchten Sie solche Informationen besonders schützen, so aktivieren Sie für diese Felder die Feldverschlüsselung. Diese Einstellung nehmen Sie im Programm PROXESS Administrator vor.

Vorab muss die Feldverschlüsselung zunächst durch den Supervisor in der PROXESS Administrator Console initialisiert werden. Die Initialisierung der Feldverschlüsselung ist ein einmaliger Vorgang und kann nicht rückgängig gemacht werden. Ob Sie die Feldverschlüsselung initialisieren hängt davon ab, ob Sie sich für einen Systembetrieb mit Sicherheitsoptionen oder für einen Systembetrieb ohne Sicherheitsoptionen entschieden haben.

Nach der Initialisierung kann die Feldverschlüsselung über die Eigenschaften eines PROXESS-Standardfeldes im Programm PROXESS Administrator gesteuert werden. Das Setzen der Eigenschaft "Verschlüsselt" für einen Standardfeld im PROXESS Administrator bewirkt keine rückwirkende Verschlüsselung bereits eingetragener und archivierter Feldinhalte. Es können nur Standardfelder von Hochsicherheitsdatenbanken verschlüsselt werden.

Feldverschlüsselung initialisieren

Verbinden Sie sich im der PROXESS Administrator Console als Supervisor mit Ihrer Smartcard mit dem eingetragenen "PROXESS Administrator".
Wählen Sie im Menü "Aktion/Sicherheit" den Befehl **Feldverschlüsselung initialisieren**.

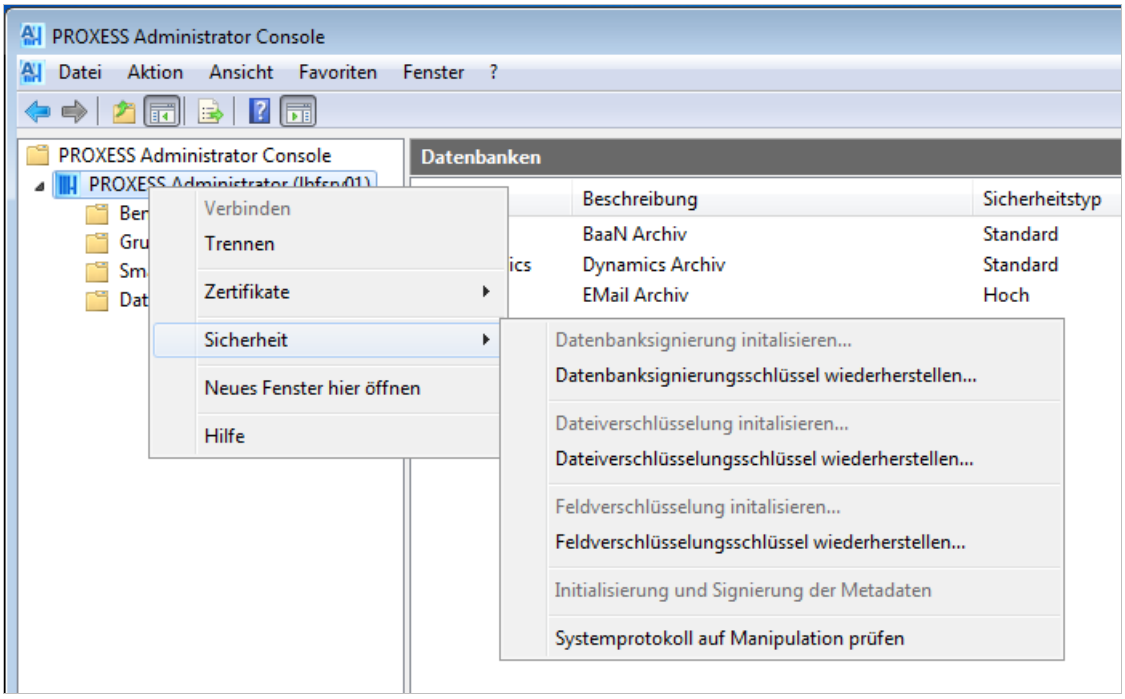


Abb.: Menü "Aktion/Sicherheit"

Wählen Sie einen Drucker für den Ausdruck "PROXESS Hauptschlüssel-Feldverschlüsselung" aus. Wählen Sie aus Sicherheitsgründen einen lokalen Drucker oder nicht öffentlich zugänglichen Drucker aus. (Wählen Sie keinen PDF-Drucker o. ä. aus, da die Gefahr besteht, dass Ihre Kennwort-Datei versehentlich überschrieben wird.)
Bestätigen Sie Ihre Auswahl mit dem Befehl **Initialisieren**.
Ihre Änderungen werden erst nach einem **Neustart des PROXESS-Systems** wirksam.

Warnhinweis

	**Bewahren Sie den entstehenden Ausdruck "PROXESS Hauptschlüssel - Feldverschlüsselung" sicher auf. Dieser Ausdruck enthält ein Schlüsselkennwort für den Algorithmus der Feldverschlüsselung. Ohne dieses Kennwort ist es nicht möglich, verschlüsselte Feldwerte zum Beispiel nach einem Austausch der Hardware, wieder zu entschlüsseln und wieder im Originalformat anzuzeigen. Geht der Hauptschlüssel-Feldverschlüsselung verloren, so entsteht Datenverlust!**

Feldverschlüsselung wiederherstellen

Die Wiederherstellung der Feldverschlüsselung ist z. B. nach einem Austausch der Systemhardware notwendig.

Verbinden Sie sich als Supervisor mit Smartcard mit dem eingetragenen "PROXESS Administrator".
Wählen Sie im Menü "Aktionen/Sicherheit" den Befehl **Feldverschlüsselung wiederherstellen**.
Geben Sie das Kennwort des Ausdrucks "PROXESS Hauptschlüssel - Feldverschlüsselung" ein.
Bestätigen Sie Ihre Eingabe dem Befehl **Wiederherstellen**.
Ihre Änderungen werden erst nach einem **Neustart des PROXESS-Systems** wirksam.

Siehe auch:

Hochsicherheitsdatenbank aktivieren

Hochsicherheitsdatenbank aktivieren

In den Dokumentdatensätzen einer PROXESS Archivdatenbank werden zum einen inhaltliche Informationen über das archivierte Dokument (Inhalte der Dokumentfelder) als auch Verwaltungsinformationen des archivierten Dokuments wie Lebensdauer, Aufbewahrungsfrist und Speichermedium eingetragen. Möchte man diese Informationen besonders schützen, so empfiehlt sich die Aktivierung einer Datenbank als Hochsicherheitsdatenbank.

Durch die Aktivierung als Hochsicherheitsdatenbank werden die Dokumentdatensätze dieser PROXESS Archivdatenbank in der zugrundeliegenden SQL-Datenbank signiert. Manipulative Eingriffe von außen, also über die SQL-Ebene können so durch das PROXESS-System erkannt werden und dem Benutzer angezeigt werden.

Beispiel: Wird ein Dokument via SQL-Befehl einem anderen Dokumenttyp zugeordnet, so wird die Anzeige und Bearbeitung des betroffenen Dokuments mit einem Warnhinweis gesperrt. Nur ein Supervisor kann diese Sperrung wieder aufheben.

Die korrespondierenden Einträge in der Volltextdatenbank werden ebenfalls durch Verschlüsselung vor unberechtigten Zugriffen geschützt.

Bevor Sie eine Datenbank als Hochsicherheitsdatenbank aktivieren können, müssen diese Voraussetzungen erfüllt sein:

- Die Datenbanksignierung muss bereits initialisiert worden sein (siehe Datenbanksignierung).
- Die gewünschte Datenbank muss als Hochsicherheitsdatenbank in der aktiven PROXESS-Lizenzdatei eingetragen sein.
- Dieser Eintrag kann nur durch den Hersteller (PROXESS) erfolgen. Wenden Sie sich im Bedarfsfall an Ihren Vertriebspartner oder direkt an die PROXESS GmbH.

Die Aktivierung einer Datenbank als Hochsicherheitsdatenbank ist ein einmaliger Vorgang und kann nicht rückgängig gemacht werden. Führen Sie die Aktivierung zu einem Zeitpunkt durch, zu dem bereits mit dem System gearbeitet wurde und bereits Dokumente in dieser Datenbank gespeichert wurden, werden diese nachträglich signiert. Je nach der Anzahl bestehender Dokumente kann diese nachträgliche Signierung längere Zeit in Anspruch nehmen. Sie erhalten vor dem Start der Signierung einen Hinweis über die Anzahl der bestehenden Dokumente.

Schritt-für-Schritt-Anleitung

Verbinden Sie sich als Supervisor mit Smartcard mit dem eingetragenen "PROXESS Administrator".

Markieren Sie die Datenbank, die Sie als Hochsicherheitsdatenbank aktivieren möchten. Sie müssen dabei nicht mit der Datenbank verbunden sein.

Wählen Sie im Menü "Aktion" (alternativ über das Kontextmenü) die Funktion "Hochsicherheitsdatenbank aktivieren".

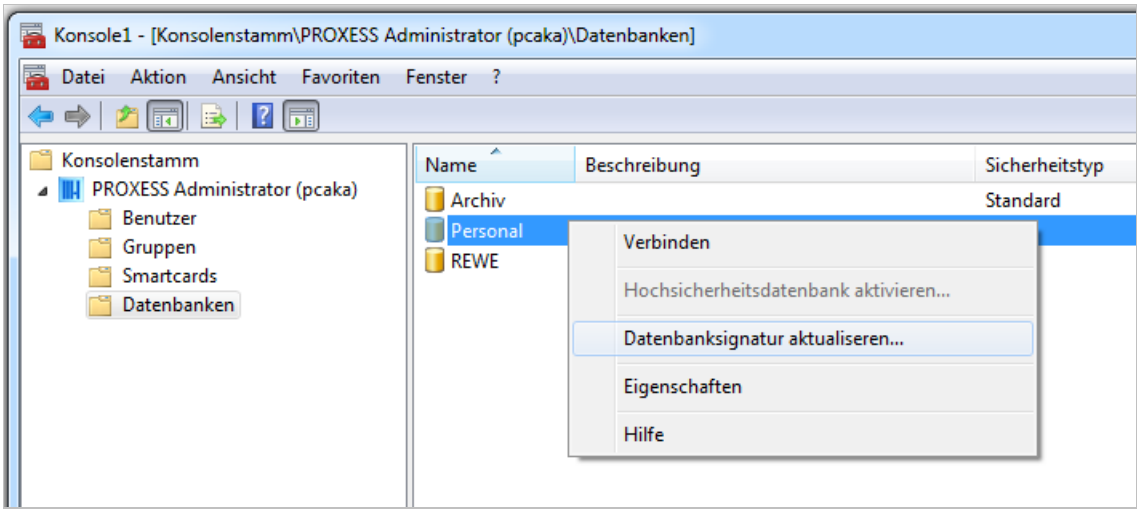


Abb.: Aktivierung der Datenbank "Personal" als Hochsicherheitsdatenbank

Es erscheint eine Meldung, wieviele Dokumente in dieser Datenbank nachsigniert werden müssen. Da gelöschte Dokumente in PROXESS nicht endgültig gelöscht werden, werden auch diese Datensätze nachsigniert und mitgezählt. Starten Sie den Vorgang mit dem Befehl **Ja**.

Haben Sie eine Datenbank erfolgreich als Hochsicherheitsdatenbank aktiviert, so wird der Menüpunkt "Hochsicherheitsdatenbank aktivieren" deaktiviert. Der Sicherheitstypus der Datenbank erhält den Status "Hoch".

Aktive Schnittstelle festlegen

Ab Version PROXESS 8.0 wird der Unicode-Zeichensatz unterstützt. Aus Gründen der Abwärtskompatibilität kann auch weiterhin der ältere Codepage-Zeichensatz verwendet werden. Mit der Funktion **Aktive Schnittstelle festlegen** bestimmen Sie, welcher Zeichensatz in der Kommunikation zwischen PROXESS Server und PROXESS Clients verwendet werden soll.

Schritt-für-Schritt:
Verbinden Sie sich in der PROXESS Administrator Console als Supervisor mit Ihrer Smartcard mit dem eingetragenen "PROXESS Administrator".
Wählen Sie im Menü "Aktion/Sicherheit" den Befehl **Aktive Schnittstelle festlegen** (alternativ das Kontextmenü).

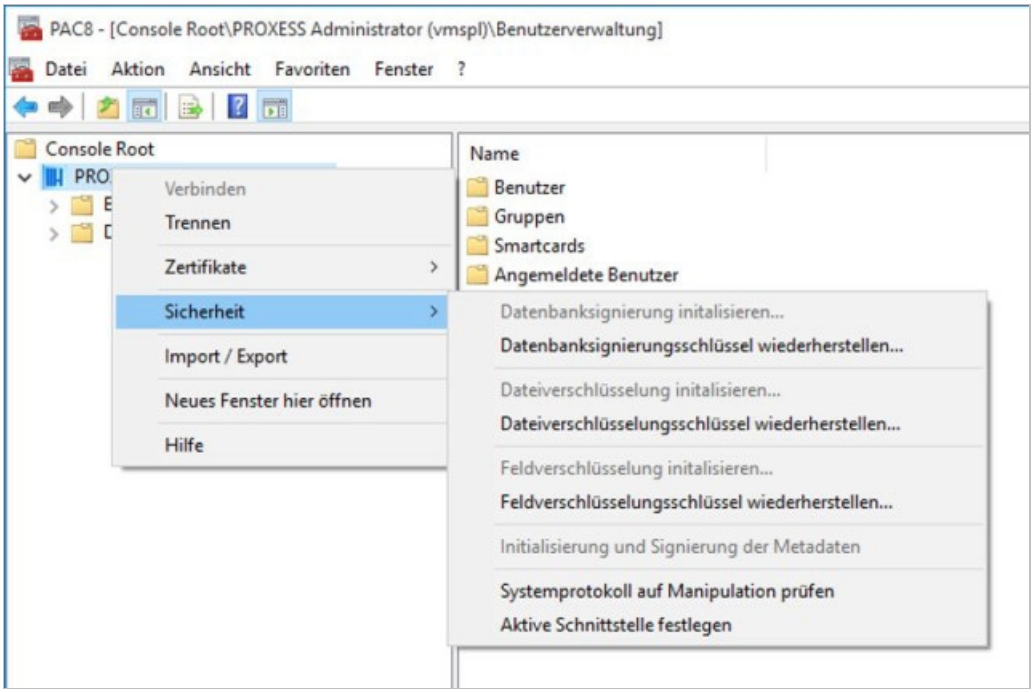


Abb.: Kontextmenü Server/Sicherheit

Sie haben folgende Einstellungsmöglichkeiten.

nur Codepage-basiert	Der Codepage-Zeichensatz deckt die Schriftzeichen der meisten europäischen Sprachen ab. Wenn diese Einstellung aktiv ist, dann können sich nur PROXESS Clients bis zur Version 5^{+} R2 am PROXESS Server anmelden.
nur Unicode-basiert	Der Unicode-Zeichensatz umfasst die Schriftzeichen aller weltweit bekannten Sprachen. Er wird ab Version PROXESS 8.0 unterstützt. Wenn diese Einstellung aktiv ist, dann können sich nur PROXESS Clients ab der Version PROXESS 8.0 am PROXESS Server anmelden.

Beide	Bei dieser Einstellung können sich PROXESS Clients aller PROXESS Versionen anmelden.  **Verwenden Sie diese Einstellung nur temporär z. .B. in einer Umstellungsphase von einer älteren PROXESS-Version auf PROXESS 8.0.** **Sind beide Schnittstellen aktiviert kann es zu unbeabsichtigen Überschreibungen von Dokumenten mit dem alten Codepage-Schriftsatz kommen.** Unbekannte Zeichen werden dann mit sogenannten Ersetzungszeichen wie "?" zurückgeschrieben. Diese Dokumente werden dadurch unleserlich. Um diese Überschreibungen nachvollziehen zu können, sollten Sie während der Umstellungsphase die Dokumenten-Historie im PROXESS Administrator aktivieren.

Metadaten importieren/exportieren

	Für diese Funktion müssen Sie als Supervisor angemeldet sein.

Sie können Metadaten in eine Datei (XML-Format) exportieren und aus einer Datei bzw. aus einem System in eine andere Datenbank/ein anderes System importieren. So sparen Sie sich als Systemadministrator bei der Einrichtung eine Menge manueller Arbeit zum Beispiel wenn mehrere Datenbanken einen ähnlichen Aufbau haben.

Diese Metadaten können exportiert/importiert werden:

- Benutzer
- Gruppen
- Datenbankfelder
- Dokumenttypen
- Dateitypen
- Vorlagedateien
- Validierungsregeln
- Such- und Sortierkriterien

Schritt für Schritt:

Wählen Sie den Zweig Ihres PROXESS-Systems aus und wählen Sie im Kontextmenü den Befehl **Import/Export.**

Öffnen Sie das Menü "**Datei**".

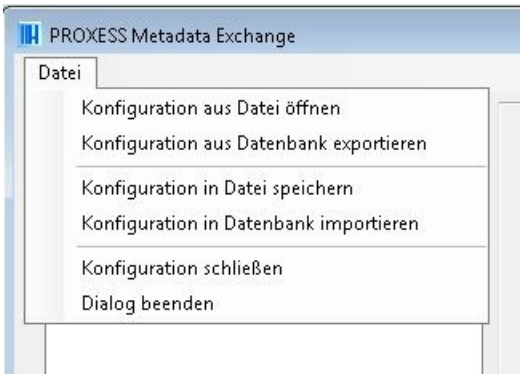


Abb.: Funktionsüberblick für den PROXESS Metadata Exchange Dialog

Je nachdem ob Sie importieren oder exportieren möchten, stehen folgende Funktionen zur Verfügung.

Konfiguration aus Datei öffnen	Hiermit öffnen Sie eine vorhandene PMX-Datei ((PROXESS Metadata Exchange) über das Explorer-Menü. Nutzen Sie diese Funktion, wenn Sie Metadaten importieren möchten.

Konfiguration aus Datenbank exportieren	Wählen Sie die gewünschte Datenbank aus. Alle Metadaten werden ausgelesen. Das Auslesen der aktuellen Metadaten sehen Sie rechts im Fenster "Protokoll". (siehe Abbildung unten).
Konfiguration in Datei speichern	Mit diesem Befehl speichern Sie die oben ausgewählten Werte in einer PMX-Datei. Vorher entscheiden Sie im linken Fensterbereich "Metadaten", welche Metadaten in die Exportdatei geschrieben werden.
Konfiguration in Datenbank importieren	Wählen Sie hier die gewünschte Datenbank für den Import. In diesem Dialog können Sie gleichzeitig auch eine neue Datenbank erstellen lassen. Wählen Sie zudem in diesem Dialog aus, welche Metadaten importiert werden sollen. (siehe Abbbildung unten)
Konfiguration schließen	Hiermit erhalten Sie wieder ein leeres Dialogfenster.
Dialog beenden	Hier schließen Sie das Fenster.

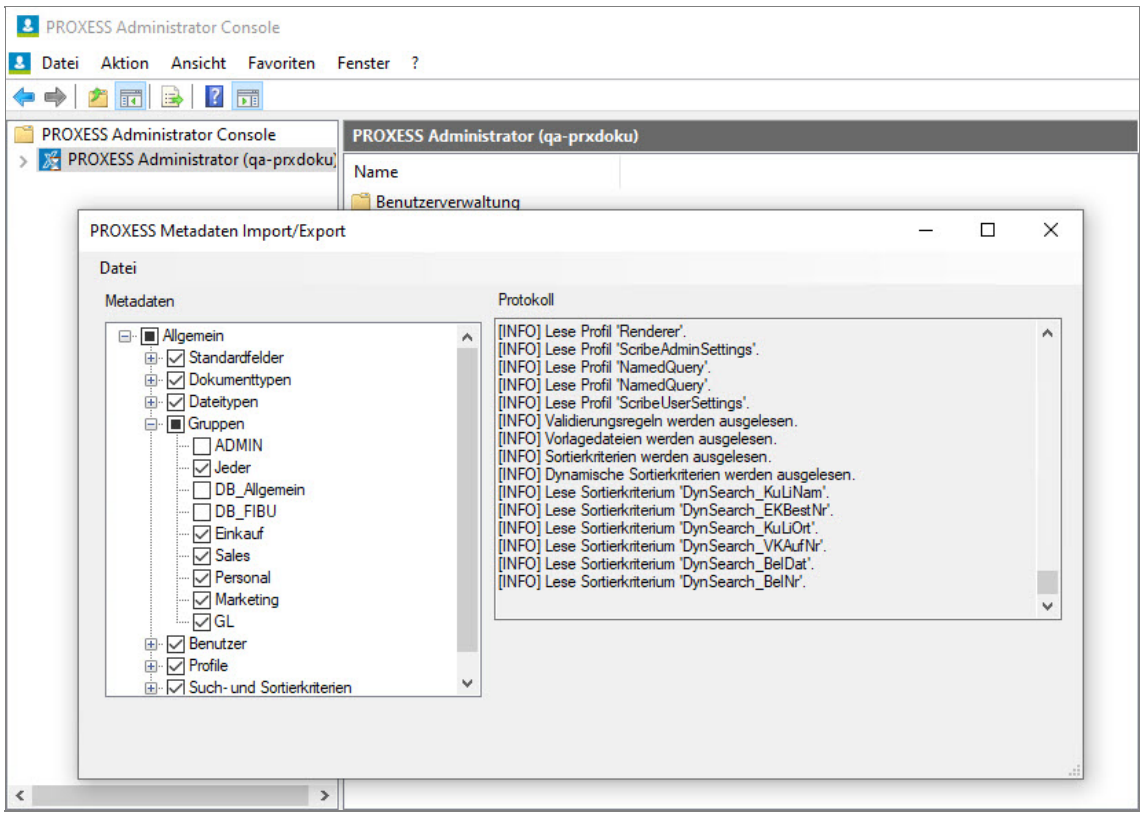


Abb.: Auslesen und Konfigurieren der Metadatendatei für den Export

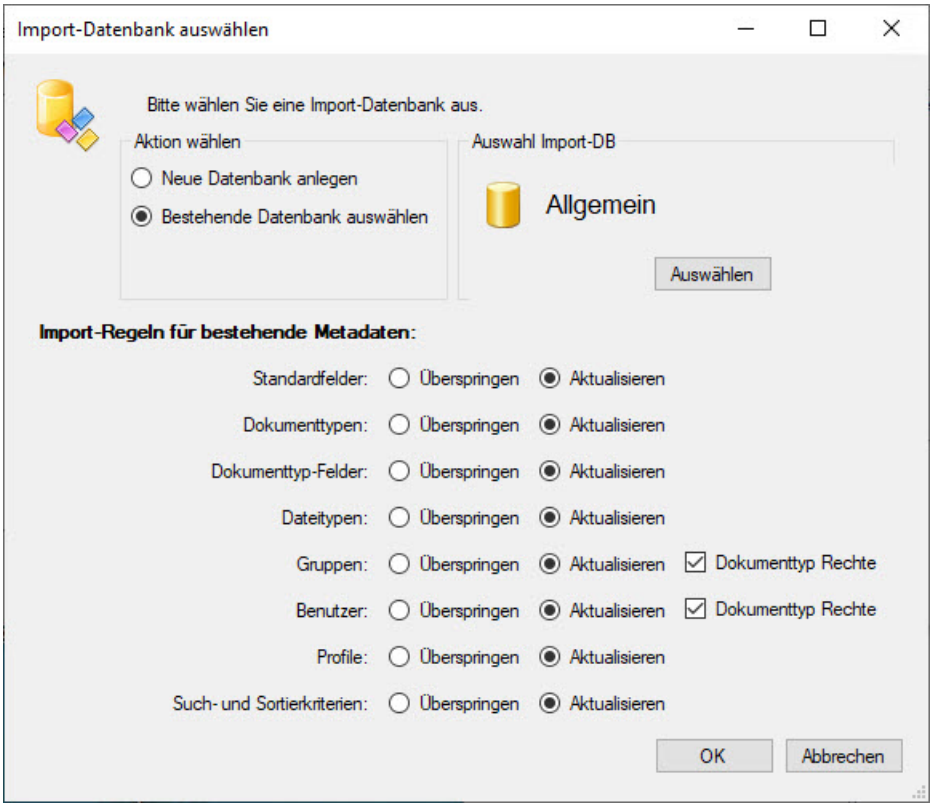


Abb.: Konfigurationsdialog für den Import von Metadaten

Neue Datenbank anlegen

Für diese Funktion benötigen Sie Supervisorprivilegien.

Wählen Sie den Knotenpunkt Datenbanken aus uns wählen Sie im Aktionspanel oder über das Kontextmenü die Funktion **Neu erzeugen...**

Nun können Sie für die neue Datenbank (für das neue Archiv) einen Namen und eine Beschreibung vergeben.

Name	Name der Datenbank, der auch in der SQL-Datenbank verwendet wird. Geben Sie hier eine Bezeichnung mit maximal 8 Zeichen ein. Das erste Zeichen muss ein Buchstabe sein. Schlüsselwörter, die von der Datenbank für interne Zwecke reserviert sind, können Sie nicht verwenden. Einmal gespeichert, kann der Name nicht mehr geändert werden.
Beschreibung	Beschreibung oder Erläuterung der Datenbank. Diese kann jederzeit wieder geändert werden.
In DBMS erzeugen	Hier können Sie sich mit dem Datenbank Management System (DBMS) verbinden (siehe Dialogfenster unten), um die PROXESS-Datenbank im zugrundeliegenden SQL-Datenbanksystem physisch anzulegen. Sind PROXESS-Datenbankmanager und PROXESS Administrator Console auf einem Rechner installiert, so werden die SQL-Verbindungseinstellungen bereits in den Dialog übernommen.
Anlegen	**Sie können die Datenbank in der PROXESS Administrator Console erst dann anlegen, wenn die neue Datenbank als SQL-Datenbank bereits angelegt wurde.**
Abbrechen	Hiermit verlassen Sie den Dialog, ohne die Eingaben zu speichern.

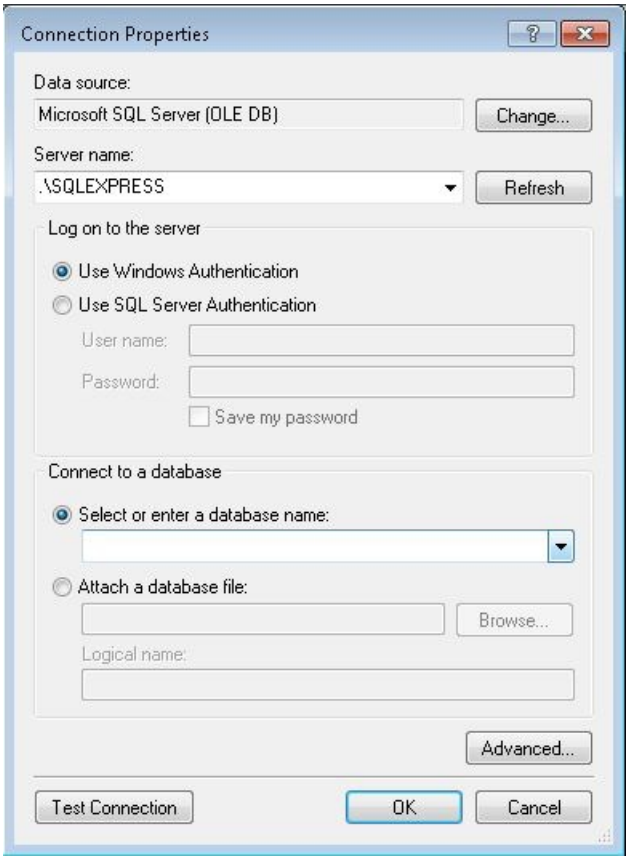


Abb.: Verbindungsdialog des DBMS

Allgemeine Datenbankeigenschaften

Markieren Sie im Konsolenstamm der PROXESS Administrator Console den Zweig "Datenbanken.
Markieren Sie die zu verwaltende Datenbank und wählen Sie im Kontextmenü ("rechte Maustaste") den Befehl **Eigenschaften** und den Reiter **Allgemein**.

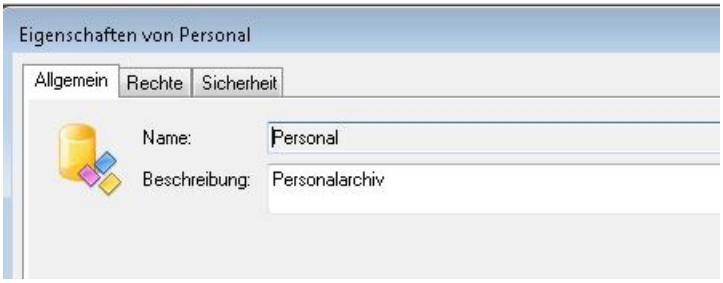


Abb.: Allgemeine Datenbankeigenschaften der Datenbank "Personal"

Hier können Sie die **Beschreibung** für die Datenbank verändern.

Der **Name** der Datenbank kann nicht verändert werden, da er mit dem Datenbanknamen zugrundeliegenden SQL-Datenbank übereinstimmen muss.

---

siehe auch:
Datenbankrechte verwalten

Datenbanksicherheit (Protokollierung)

Datenbank löschen

Falls Sie eine Datenbank nicht mehr benötigen, z. B. eine Testdatenbank, können Sie diese wieder löschen. Dies ist nur möglich, wenn kein Benutzer mehr mit dieser Datenbank verbunden ist. Es erscheint eine Warnung, die Sie bestätigen müssen, um tatsächlich zu löschen.

Schritt für Schritt:

Wählen Sie den Zweig "Datenbanken" im linken Teilfenster.

Markieren Sie in der Datenbankliste in der Mitte die Datenbank, die Sie löschen möchten.

Wählen Sie im Menü "Aktion" (alternativ über das Kontextmenü) die Funktion "Löschen".

Beachten und bestätigen Sie die Warnmeldung, wenn Sie die Datenbank tatsächlich löschen möchten.

Warnhinweis

	Eine gelöschte Datenbank ist nicht wiederherstellbar. Alle Dokumente, die in dieser Datenbank gespeichert sind, werden ebenfalls unwiederbringlich gelöscht.

Datenbanksignatur aktualisieren

Hier handelt es sich um eine interne Verwaltungsfunktion, die notwendig wird, wenn aufgrund von Wartungsarbeiten über SQL-Tools Änderungen an den PROXESS-Datenbanktabellen vorgenommen wurden (z. B. nachträglich ein Feld verlängert wird). Ein solcher Eingriff erfordert eine Aktualisierung der Datenbanksignatur der betroffenen Dokumente. Nur so sind die Dokumente weiterhin für den Anwender anzeigbar.

Warnhinweis

	Führen Sie diese Wartungsarbeiten immer in Verbindung mit Ihrem PROXESS Servicepartner durch. Bei fehlerhafter Ausführung werden die betroffenen Dokumente nicht mehr im System angezeigt bzw. Datenbankeinträge werden verfälscht.

Schritt für Schritt-Anleitung:

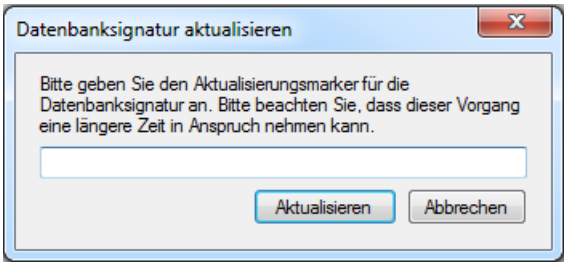
Lassen Sie im Rahmen der Wartungsarbeiten über den SQL-Befehl die Spalte "Datahash" mit einem beliebigen Eintrag markieren (z.B. Update).

Verbinden Sie sich in der PROXESS Administrator Console mit Supervisorprivilegien mit dem eingetragenen "PROXESS Administrator".

Wählen Sie die betroffene Datenbank aus.

Wählen Sie im Menü "Aktionen den Befehl **Datenbanksignatur aktualisieren** (alternativ über das Kontextmenü der gewählten Datenbank).

Es öffnet sich folgendes Dialogfenster:



Geben Sie hier den oben verwendeten Markierungseintrag (z.B. "Update") ein.

Wählen Sie den Befehl **Aktualisieren.**

Siehe auch:

Datenbanksignierung

Sicherheitsfunktionen - Konzept und Überblick

Datenbankrechte verwalten

Damit ein Benutzer in einem Teilarchiv, also in einer Datenbank arbeiten , d.h. recherchieren kann oder Dokumente hinzufügen kann, benötigt er Zugriffsrechte auf diese Datenbank. Nachdem er ein grundsätzliches Zugriffsrecht für eine Datenbank erhalten hat, sind zusätzlich noch Zugriffsrechte auf die Dokumenttypen dieser Datenbank notwendig (siehe Dokumenttyprechte verwalten).

Hinweis

	Zur Verwaltung von Datenbankrechten müssen Sie als Supervisor angemeldet sein. Als Datenbank-Bereichsadministrator oder als (System-)Administrator sehen Sie nur die Datenbanken in der Anzeige, die für Sie vom Supervisor bereits freigeschaltet wurden. Sie können sich bestehende Benutzer- und Gruppenrechte anzeigen lassen, jedoch keine Änderungen vornehmen.

Markieren Sie im Konsolenstamm der PROXESS Administrator Console den Zweig "Datenbanken.
Markieren Sie die zu verwaltende Datenbank und wählen Sie im Kontextmenü ("rechte Maustaste") den Befehl **Eigenschaften** und den Reiter **Rechte**.

Es erscheint folgendes Dialogfenster:

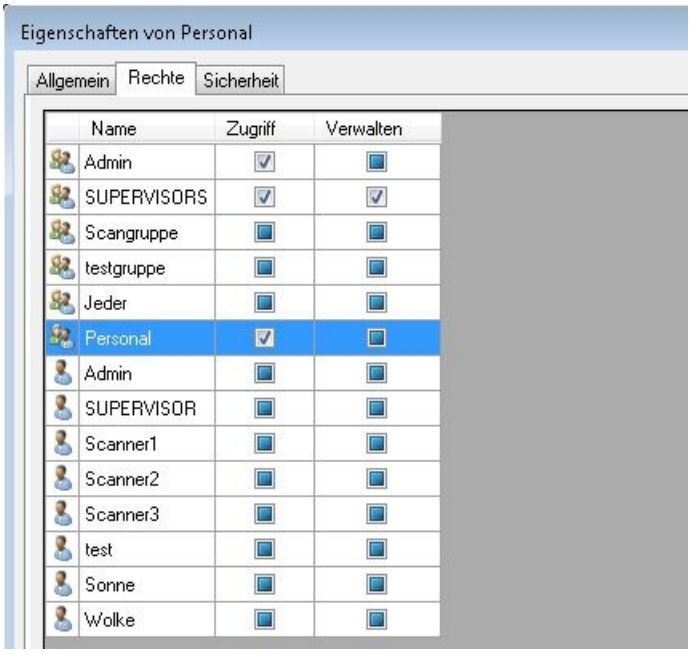


Abb.: Datenbankrechte der Datenbank "Personal"

In der Titelleiste sehen Sie den Namen der gewählten Datenbank. In der Tabelle sind alle bestehenden Benutzer und Gruppen aufgeführt.

Diese zwei Datenbankrechte werden unterschieden:

Zugriff ermöglicht es, eine Verbindung mit der Datenbank aufzubauen. Für den erfolgreichen Zugriff auf archivierte Dokumente wird zusätzlich das Zugriffsrecht auf Dokumenttypen benötigt.

Verwalten	ermöglicht es, innerhalb dieser Datenbank anderen PROXESS-Benutzern Zugriffsrechte zu erteilen oder zu entziehen. Erhält ein Benutzer das Verwaltungsrecht für eine Datenbank, so wird er zum Datenbank-Bereichsadministrator.

Es gibt drei Zustände bei der Rechtevergabe:

Häkchen gesetzt	Recht erteilt
grünes Kästchen (bzw. ausgegrautes Häkchen im klassischen Windows-Design)	Recht nicht erteilt (= Standardeinstellung). Evtl. hat ein Benutzer aber über seine Gruppenzugehörigkeit entsprechende Rechte.
leeres Kästchen	Recht explizit entzogen (= verbieten). Das sogenannte "Verbieten" für Einzelbenutzer überstimmt das Recht, das der Benutzer aufgrund seiner Gruppenzugehörigkeit besitzt.

Der Gruppe der SUPERVISORS und den Supervisoren selbst kann kein Recht erteilt oder entzogen werden. Supervisoren haben per se Zugriff und Verwaltungsrecht auf alle Datenbanken.

Administratoren erhalten automatisch ein Zugriffsrecht auf die Datenbanken, die sie im Programm PROXESS Administrator angelegt haben. Damit werden dem Administrator die notwendigen Verwaltungsaufgaben, wie die Anlage von Dokumenttypen und Feldern in dieser Datenbank ermöglicht. Das Zugriffsrecht auf eine Datenbank allein ermöglicht noch nicht den Zugriff auf archivierte Dokumente dieser Datenbank. Hierfür sind zusätzlich Zugriffsrechte auf Dokumenttypebene und auf Dokumentebene notwendig. Administratoren erhalten zudem kein Verwaltungsrecht für die angelegten Datenbanken, d. h. sie können keine Benutzerrechte erteilen.

Durch Klicken auf ein Kästchen aktivieren Sie die verschiedenen Zustände. Erst mit dem Befehl **OK** oder **Übernehmen** werden alle gewählten Datenbankrechte wirksam.

Siehe auch:

Zugriffsrechte - Konzept und Überblick

Datenbank-Bereichsadministrator

Datenbankfeld anlegen

Mit den Datenbankfeldern legen Sie die Such- und Indexfelder für ein Archiv fest. Es ist unbedingt zu empfehlen, die diese Felder vorab in einem Organisationsgespräch festzulegen.

Schritt für Schritt:

Um ein neues Feld anzulegen, verbinden Sie sich mit der gewünschten Datenbank und wählen Sie im linken Teilfenster den **Knotenpunkt Datenbankfelder** unter Datenbank.

Haben Sie für eine Datenbank noch keine Felder angelegt, so sehen Sie zunächst die beiden **PROXESS-Kernfelder Doc Des und DocsDocTypeName.** Die beiden Felder DocDes (Dokumentname) und DocsDocTypeName (Dokumenttyp) sind in jeder Datenbank immer automatisch vorhanden. Sie können diesen beiden Feldern einen anderen Namen vergeben, alle anderen Eigenschaften sind jedoch festgelegt und nicht veränderbar.

Im Aktionspanel rechts (alternativ über das Kontextmenü) wählen Sie den Befehl **Neu.**

Es erscheint folgendes Dialogfenster:

Abb.: Anlegen eines neuen Datenbankfeldes "Nachname"

Feldname	Hier vergeben Sie einen Namen für das neue Feld. Dieser Name muss den Anforderungen der zugrundeliegenden SQL-Datenbank entsprechen. Verwenden Sie Zeichen, die in der SQL-Datenbank nicht erlaubt sind, so färbt sich der Eintrag rot und kann nicht gespeichert werden. So können Sie zum Beispiel bestimmte Schlüsselwörter, die für datenbankinterne Zwecke reserviert sind, nicht verwenden. Später können Sie noch einen sprechenden Feldnamen für die Anwendermaske ergänzen.
Datentyp	Hier wählen Sie einen Datentyp aus. Welche Datentypen zur Auswahl stehen, hängt von der verwendeten Datenbank bzw. der Schnittstelle ab. Bei Microsoft SQL Server stehen Ihnen z. B. die Typen STRING (alpanumerische Zeichen), INTEGER (natürliche Zahl), DATETIME (Datum und Uhrzeit) und DOUBLE (Fließkommazahl) zur Verfügung. Der Datentyp kann nachträglich nicht mehr geändert werden.
Feldlänge	Wenn Sie als Datentyp STRING ausgewählt haben, legen Sie zusätzlich die maximale Feldlänge fest. Diese kann zwischen 1 und 255 Zeichen betragen. Mehr als die hier definierte Anzahl von Zeichen kann der Benutzer dann in diesem Feld nicht eingeben. Die Feldlänge kann wie der Datentyp nachträglich nicht mehr geändert werden.

Feste Länge	Diese Option kann nur gewählt werden für Felder vom Typ STRING. Hiermit definieren Sie eine feste Feldlänge für den jeweiligen Datenbankeintrag. Nicht genutzte Zeichen werden dann ggfs. durch Leerzeichen aufgefüllt. Durch die feste Länge kann geringfügig Speicherplatz in der Datenbank optimiert werden. Für aktuelle Datenbanken ist dieser Vorteil jedoch vernachlässigbar, so dass der Hersteller empfiehlt, diese Option nicht zu aktivieren.
Verschlüsselt	Aktivieren Sie das Kontrollkästchen, um Feldinhalte dieses Merkmalsfeldes in der SQL-Datenbank verschlüsseln zu lassen. Die Aktivierung ist nur möglich, wenn Ihr Supervisor diese Datenbank vorab als Hochsicherheitsdatenbank in der PROXESS Administrator Console aktiviert hat. Die Aktivierung der Feldverschlüsselung können Sie als Mitglied der Administratorgruppe auch ohne Supervisorprivilegien vornehmen.(siehe Hinweis unten), Verschlüsselte Felder werden mit diesem Symbol gekennzeichnet: **Warnhinweis** Verschlüsselte Felder führen zu bestimmten Einschränkungen: Zum einen sind nur noch exakte Gleichheitssuchen möglich (also keine "%-Suchen" mehr), zum anderen kann sich die Performance des Systems verschlechtern. Dies ist abhängig von der Menge der zu verschlüsselnden Daten und Ihrer eingesetzten Hardware.
Anlegen	Hiermit legen Sie ein neues Feld mit den eingegebenen Daten an. Einmal gespeichert können diese Eigenschaften nicht mehr geändert werden. Sie können aber die für den Benutzer sichtbaren Eigenschaften konfigurieren.

Tipp

	In PROXESS werden bestimmte **Kernfelder** automatisch generiert und in der Dokumentmaske mit angezeigt. Hierzu zählen der Benutzer, der das Dokument erstellt hat., das Datum der Erstellung und das Datum der letzten Änderung am Dokument . Diese Felder werden im PROXESS Client in der Dokumentmaske im Register Kernfelder angezeigt. Auch die Archivierungsfrist des Dokuments wird dort automatisch angezeigt.

siehe auch:
PROXESS Metadata Exchange

Datenbankfeld Eigenschaften

Verbinden Sie sich mit der gewünschten Datenbank. Wählen Sie im linken Teilfenster den Knotenpunkt Datenbankfelder. Im mittleren Teilfenster sehen Sie eine Liste der vorhandenen Datenbankfelder.
Markieren Sie das gewünschte Feld und wählen Sie im Aktionspanel rechts (alternativ über das Kontextmenü) den Befehl **Eigenschaften**.

Es öffnet sich folgender Dialog:

Abb.: Eigenschaften des Datenbankfeldes "Niederlassung"

Allgemeine Einstellungen	
Feldname in Datenbank	Der Feldname in der Datenbank wurde beim Anlegen des Feldes vergeben (siehe: Datenbankfeld anlegen). Er kann nachträglich nicht mehr verändert werden.
Validierungsregel	Hier sehen Sie, ob eine Validierungsregel mit dem Feld verknüpft ist.
Anzeigename	Name des Feldes auf der Such- und Indexmaske
Feld-Beschreibung	Zusätzliche Information für den Benutzer in der Statuszeile
Indexiert	Dieses Kontrollkästchen dient der Information, ob ein bestimmtes Feld - zur Beschleunigung der Suche - in der Datenbank indexiert ist oder nicht. Die Felder **Dokumenttitel** und **Dokumenttyp** sind bereits automatisch indexiert. Sie können einen Index bei der Konfiguration von Dynamischen Sortierkriterien anlegen. Wenn Sie ein Feld aus einem anderen Grund indizieren wollen, können Sie dies direkt in der Datenbank tun. Detaillierte Hinweise zur Indexierung finden Sie in der Dokumentation zu ihrer SQL- Datenbank.
Sichtbar	Ist die Option aktiviert, so ist dieses Feld in der Standardmaske für den Anwender sichtbar.
Pflichtfeld	Aktivieren Sie das Kontrollkästchen, um ein Feld als Pflichtfeld zu definieren. Der Benutzer kann dann in der Anwendung seine Eingaben nicht eher speichern, bis er auch das Pflichtfeld ausgefüllt hat. Pflichtfelder sollten nur für besonders wichtige Daten, z. B. Rechnungsnummer, angelegt werden, die für die Bearbeitung und Suche von Dokumenten unverzichtbar sind.
Verschlüsselt	Die Aktivierung dieser Option ist nur möglich, wenn Ihr Supervisor diese Datenbank vorab als Hochsicherheitsdatenbank aktiviert hat. Die Aktivierung der Feldverschlüsselung können Sie als ein Mitglied der Administratorgruppe vornehmen.

Datenbankfeld löschen

Die Organisationsanalyse sollte gewährleisten, dass nur die benötigten Datenbankfelder mit den gewünschten Eigenschaften angelegt werden. Falls ein Feld irrtümlich angelegt wurde oder einen falschen Namen in der Datenbank, einen falschen Datentyp oder eine falsche Länge bekommen hat, können Sie es notfalls auch wieder löschen.

Schritt-für-Schritt:

Verbinden Sie sich mit der gewünschten Datenbank.

Wählen Sie den Eintrag "Datenbankfelder".

Nun werden im mittleren Teilfenster alle Datenbankfelder angezeigt.

Wählen Sie das zu löschenden Feld aus.

Wählen Sie den Befehl **Löschen** über das Kontextmenü.

Warnhinweis

Da das Löschen des Feldes bedeutet, dass eventuell schon gespeicherte Daten ebenfalls gelöscht werden, erscheint eine Sicherheitsabfrage, die Sie bestätigen müssen, um wirklich zu löschen.

Dokumenttyp anlegen

Gleichartige Dokumente werden in PROXESS in Form von Dokumenttypen zusammengefasst. Beispiele hierfür sind: Eingangsrechnung, Ausgangsrechnung, Lieferschein, Auftragsbestätigung, Anschreiben, Vertrag, Bestellung etc. Mit einem Dokumenttyp werden eine Reihe von Eigenschaften festgelegt, wie z. B. Zugriffsrechte und Aufbewahrungsfristen und -medium und auch die jeweilige Indexierungsmaske. Die Festlegung Ihrer unternehmensbezogenen Dokumenttypen sollten Sie in einer Organisationsanalyse vorab analysiert haben. Viele Dokumenttypen ergeben sich dabei aus den integrierten ERP- und FIBU-Systemen in Ihrem Unternehmen.

Schritt für Schritt

Verbinden Sie sich mit der gewünschten Datenbank.

Wählen Sie den Knotenpunkt Dokumenttyp aus.

Wählen Sie im Kontextmenü (oder im Aktionspanel rechts) den Befehl **Neu.**

Es erscheint folgendes Dialogfenster:

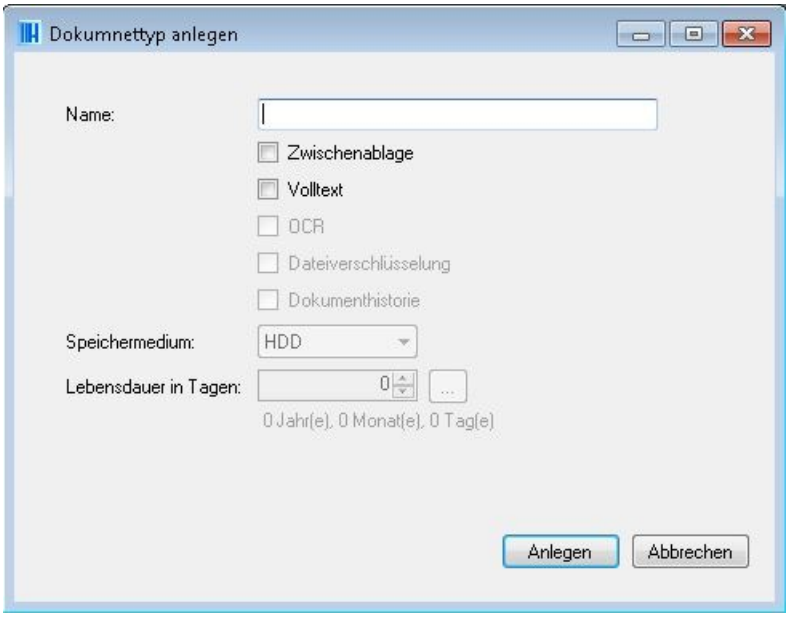


Abb.: Anlegen eines neuen Dokumenttyps

Vergeben Sie nun einen Namen für den Dokumenttyp. Welche Dokumenttypen Sie anlegen und mit welchen Eigenschaften, sollten Sie vorab in einer Organisationsanalyse festgelegt haben.

Entscheiden Sie ob der Dokumenttyp eine Zwischenablage sein soll und ob er über die Volltextsuche recherchiert werden kann.

Erläuterungen zu den Eigenschaften finden Sie im nächsten Kapitel unter: Eigenschaften von Dokumenttypen

Eigenschaften von Dokumenttypen

Gleichartige Dokumente werden in PROXESS in Form von Dokumenttypen zusammengefasst. Beispiele hierfür sind: Eingangsrechnung, Ausgangsrechnung, Lieferschein, Auftragsbestätigung, Anschreiben, Vertrag, Bestellung etc. Mit einem Dokumenttyp werden eine Reihe von Eigenschaften festgelegt, wie z. B. Zugriffsrechte und Aufbewahrungsfristen und -medium und auch die jeweilige Indexierungsmaske. Die Festlegung Ihrer unternehmensbezogenen Dokumenttypen sollten Sie in einer Organisationsanalyse vorab analysiert haben. Viele Dokumenttypen ergeben sich dabei aus den integrierten ERP- und FIBU-Systemen in Ihrem Unternehmen.

Schritt für Schritt:

Wählen Sie die gewünschte Datenbank und den gewünschten Dokumentyp aus. Über einen Doppelklick öffnet sich das Eigenschaften-Fenster des Dokumenttyps.

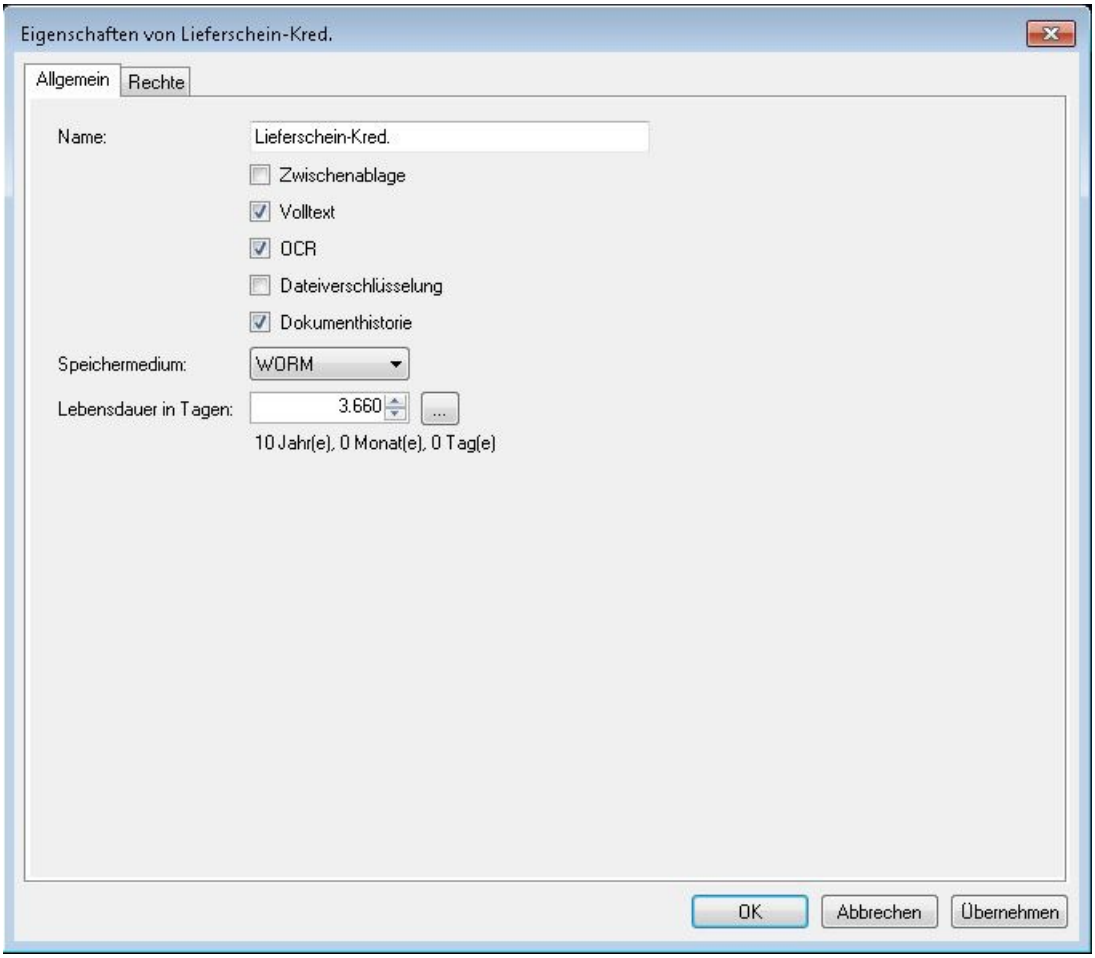


Abb.: Eigenschaften eines Dokumenttyps bestimmen (hier: Lieferschein-Kred.)

Name	Hier geben Sie den Namen/die Bezeichnung des Dokumenttyps an.

<table>
<tr><td>Zwischenablage</td><td>
Der Dokumenttyp kann hier als Zwischenablage angelegt werden. Zwischenablagen sind änderbare Dokumenttypen. Dokumente in Zwischenablagen erfordern in der Regel noch einer Nachbearbeitung und werden später einem endgültigen Dokumenttyp zugeordnet.

Beispiel:
Ein Beispiel für eine Zwischenablage ist der Barcorde-Pool oder auch ein allgemeiner Scan-Pool. Beim Barcode-Scannen mit dem PROXESS Scan Link werden die gescannten Dokumente zunächst mit dem erkannten Barcode in einem Dokumenttyp "Barcode-Pool" archiviert.. Nach der endgültigen Indexierung z. B. über die ERP-Daten werden sie dann ihrem endgültigen Dokumenttyp (z.B. Lieferschein) zugeordnet.

Warnhinweis
<table><tr><td></td><td>Eine Zwischenablage erstellen Sie genauso wie einen normalen Dokumenttyp. Das bedeutet, dass im Standard alle Indexfelder in der Indexierungsmaske angezeigt werden. Wenn Benutzer in der Zwischenablage in diese Felder Informationen eintragen, kann es vorkommen, dass diese Informationen später unsichtbar sind, wenn der Dokumenttyp gewechselt wird. Um solche Bearbeitungsfehler zu vermeiden, reduzieren Sie am besten die sichtbaren Felder für Zwischenablagen auf das absolute Minimum. Bei gescannter Eingangspost z. B. genügt in der Regel die Barcodenummer.</td></tr></table>
</td></tr>
<tr><td>Volltext</td><td>
Hiermit wird die Volltextrecherche für den Dokumenttyp aktiviert.
d.h.
1.) Die Einträge der Indexfelder sind über die Volltextsuche recherchierbar.
2.) Dateiinhalte, die mit diesem Dokumenttyp gespeichert werden können nun für die Volltextsuche aktiviert werden. Damit die Dateiinhalte auch recherchierbar sind, muss zusätzlich der jeweilige Dateityp für die Volltextrecherche aktiviert werden.
</td></tr>
<tr><td>OCR</td><td>
Der Dokumenttyp wird im PROXESS User zur OCR-Bearbeitung freigeschaltet.
Alle Dateien mit diesem Dokumenttyp können Sie dann über die integrierte Texterkennung bearbeitet werden. Für die Bearbeitung großer Belegmengen bietet PROXESS Schnittstellen zu weiterer OCR- bzw. ICR-Software an.
</td></tr>
<tr><td>Dateiverschlüsselung</td><td>
Hier können Dokumenttypen zur Verschlüsselung aktiviert werden.
Dateien, die mit diesem Dokumenttyp archiviert werden, werden vom System verschlüsselt. Die Aktivierung von Dokumenttypen zur Dateiverschlüsselung ist nur in Hochsicherheitsdatenbanken möglich. Die Aktivierung als Hochsicherheitsdatenbank erfolgt vorab über die PROXESS Administrator Console mit Supervisorprivilegien. Ein verschlüsselter Dokumenttyp verhält sich für Anwender im System genauso wie ein normaler Dokumenttyp.
</td></tr>
</table>

Dokumenthistorie	Hier können Sie die Dokumenthistorie aktivieren. In der Dokumenthistorie werden alle Änderungen an Merkmalsfeldern (Indexfeldern) eines Dokuments in Form einer "Verlaufsakte" protokolliert. Zum Anzeigen der Dokumenthistorie benötigt der Benutzer das Recht "Bearbeiten" für diesen Dokumenttyp. Die Dokumenthistorie ergänzt die Funktion "Versionierung", in der Änderungen an den archivierten Dateien aufgelistet werden. Bei einer nachträglichen Aktivierung der Option werden alle Änderungen ab dem Zeitpunkt der Aktivierung protokolliert. Standard-Einstellung für Zwischenablagen: deaktiviert Standard-Einstellung für Dokumenttypen: aktiviert
Speichermedium	Dokumente können auf verschiedenen Medien (z. B. Festplatte, WORM, DVD) archiviert werden. Welches Medium Sie wählen können, hängt von der vorhandenen Hardware ab, aber auch von der benötigten Archivierungsdauer der Dokumente. Dokumente mit identischer Lebensdauer und Speichermedium werden auf ein gemeinsames Volume geschrieben. (siehe hierzu die Dokumentation des Storage Manager Explorers). **Tipp**  Die Standardeinstellungen für Speichermedien sind an den Dokumenttyp gebunden. Da Dokumente aber manchmal aus verschiedenen Dateien bestehen, kann es sinnvoll sein, Abweichungswerte abhängig vom Dateityp zu definieren. Auf diese Weise können Sie zum Beispiel steuern, dass Notizdateien zum eigentlichen Beleg auf ein kurzlebigeres Medium gespeichert werden.
Lebensdauer in Tagen	Für viele Dokumentarten gibt es gesetzliche Vorschriften, wie lange diese Dokumente archiviert werden müssen. Für andere Dokumentarten gibt es unternehmensspezifische Regelungen. Die Lebensdauer und damit die Archivierungsfrist eines Dokumenttyps können Sie hier definieren. Dokumente mit derselben Lebensdauer und demselben Speichermedium werden organisatorisch zusammen aufbewahrt und auf ein gemeinsames Volume geschrieben. (siehe hierzu die Dokumentation des Storage Manager Explorers). **Dokumente mit abgelaufener Lebensdauer werden übrigens nicht automatisch gelöscht, sondern können durch den Administrator über den PROXESS Windows Client/Sortierkriterien regelmäßig abgefragt und dort zum endgültigen Löschen markiert werden.**

siehe auch:

Dokumenttyprechte verwalten

Dokumenttyprechte verwalten

Dokumenttypen bilden das organisatorische Rückgrat einer PROXESS Archivdatenbank. Jedes archivierte Dokument muss einem Dokumenttyp zugeordnet werden. Dokumenttypen werden im Programm "PROXESS Administrator" erstellt und konfiguriert.

Voraussetzungen für die Rechtevergabe:
Eine notwendige Voraussetzung, dass ein Benutzer in PROXESS überhaupt Dokumente eines bestimmten Dokumenttyps sehen und damit arbeiten kann, ist das Zugriffsrecht auf diesen Dokumenttyp.

	Auf neu angelegte Dokumenttypen erhalten Gruppen und Benutzer systemseitig keine automatischen Zugriffsrechte. Eine initiale Rechtezuweisung durch den Supervisor oder Bereichsadministrator ist daher zwingend notwendig, um Benutzern und Gruppen ein Arbeiten mit dem Dokumenttyp zu ermöglichen.

Zur Verwaltung von Dokumenttyprechten, markieren Sie im Konsolenstamm den Eintrag für Ihr PROXESS-System und wählen Sie die Aktion **Verbinden.** Melden Sie sich als Supervisor mit Smartcard und PIN an.

Lassen Sie sich über Doppelklick auf den Zweig alle Datenbanken des verbundenen PROXESS Systems anzeigen.

Verbinden Sie sich mit der gewünschten Datenbank, indem Sie die gewünschte Datenbank markieren und im Menü "Aktionen" den Befehl **Verbinden** wählen.

Tipp

	Zur Information wird die jeweils aktive, verbundene Datenbank im linken Teilfenster im Zweig Datenbanken in Klammern angezeigt.

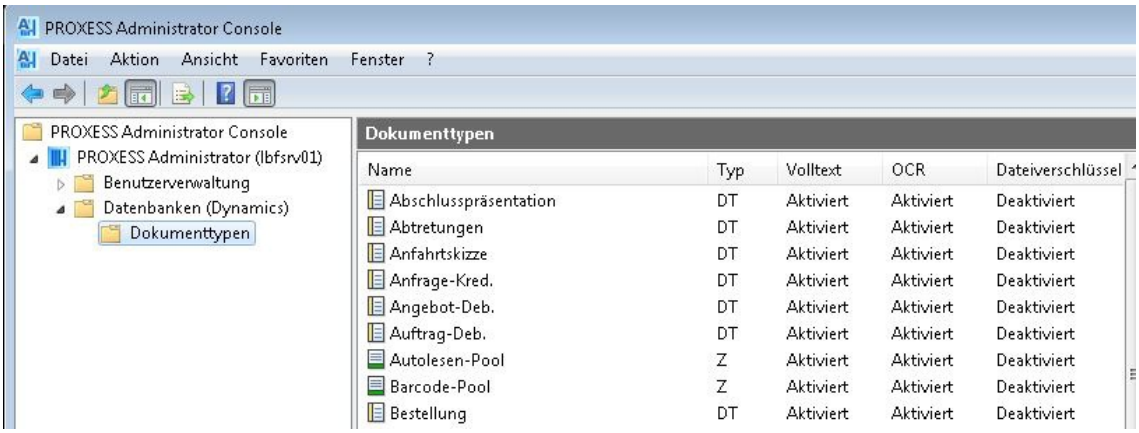


Abb.: Verbunden mit der Datenbank "Dynamics"

Erst nach dem erfolgreichen Verbinden mit einer Datenbank, werden die in dieser Datenbank verfügbaren Dokumenttypen und die bestehenden Dokumenttyprechte "geladen" und können nun verwaltet werden.

1. Möglichkeit: Dokumenttyprechte über den Dokumenttyp vergeben

Wählen Sie den Knoten "Dokumenttypen".

Durch Doppelklick auf den gewünschten Dokumenttyp öffnet sich folgender Dialog:

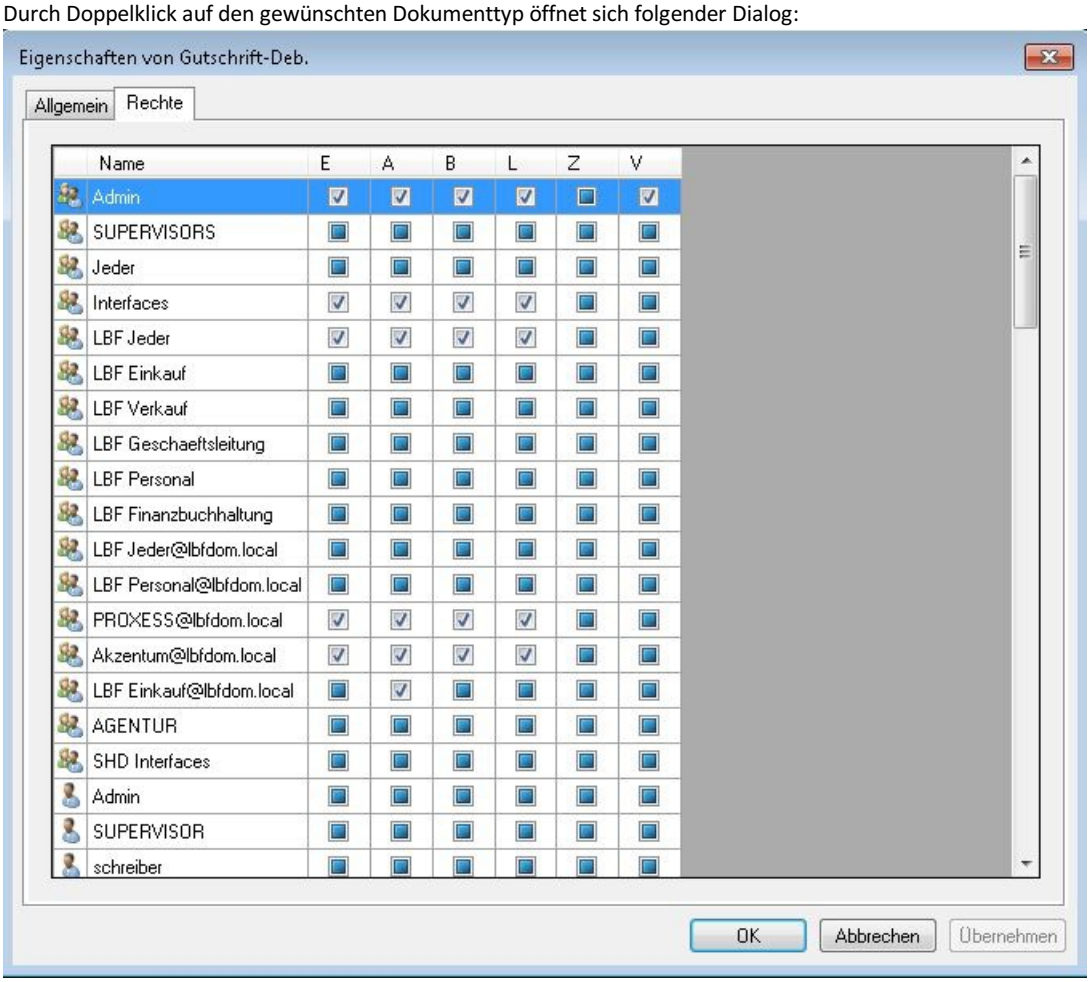


Abb: Übersicht aller Rechte auf den Doktyp "Gutschrift-Deb"

Auf Dokumenttypebene wird zwischen sechs verschiedenen Aktionsrechten unterschieden:

Anlegen (E)	Ist das Kontrollkästchen aktiviert, erhält der Benutzer das Recht, neue Dokumente dieses Typs anzulegen.
Ansehen (A)	Ist das Kontrollkästchen aktiviert, hat der Benutzer/die Gruppe das Recht, Dokumente dieses Typs anzusehen. Dies ist die Voraussetzung dafür, dass er Dokumente diesen Typs bei einer Recherche überhaupt findet und in seiner Ergebnisliste angezeigt werden.
Bearbeiten (B)	Ist das Kontrollkästchen aktiviert, hat der Benutzer das Recht, Dokumente dieses Typs zu bearbeiten. Er kann dann sowohl Merkmalsfeldern als auch alle Dateien dieses Dokumentes verändern.
Löschen (L)	Ist das Kontrollkästchen aktiviert, erhält der Benutzer das Recht, Dokumente mit diesem Dokumenttyp zu löschen. Löschen ist nur eine Korrekturmöglichkeit und nicht die Regel in der Archivierung. Das Löschrecht sollte daher sehr restriktiv eingesetzt werden. **Wichtiger Hinweis: Gelöschte Dokumente kann der PROXESS-Benutzer nicht wiederherstellen.**

Dokumente verrechten (Z)	Ist das Kontrollkästchen aktiviert, hat der Benutzer das Recht, für einzelne Dokumente dieses Typs selbst Rechte zu vergeben. Das hat Vorteile für die Bearbeitung von Vorgängen, die durch die Hände mehrerer Benutzer gehen. Ein Abteilungsleiter, der z. B. einem Sachbearbeiter Einsicht in eine vertrauliche Aktennotiz gewähren möchte, kann dies tun, ohne dass dieser Benutzer grundsätzlich für den Dokumenttyp Aktennotiz freigegeben werden muß. Oder umgekehrt: Soll das vertrauliche Dokument nur einem ganz kleinen Personenkreis zugänglich sein, kann der Grant User anderen, die für den Dokumenttyp zugelassen sind, den Zugriff auf dieses Dokument verwehren. Benutzer mit diesem Recht können also die von Ihnen angelegte Rechtestruktur erweitern oder einschränken, sodass ein Überblick über die effektiv gültigen Rechte an einem Dokument nur im Dokumentfenster von PROXESS möglich ist.
Dokumenttyp verrechten (V)	Ist das Kontrollkästchen aktiviert, kann der Benutzer für diesen Dokumenttyp die Aktionsrechte Anlegen, Ansehen etc. an andere Benutzer vergeben. Nur Supervisoren und Datenbank-Bereichsadministratoren können dieses Recht vergeben. Diese Option ist sinnvoll, wenn das Unternehmen nur ein Datenbankarchiv eingerichtet hat und daher auf Datenbankebene keine rechtliche Differenzierung vornehmen kann. In der Regel ist dies bei kleineren PROXESS-Systemen der Fall.

Die Aktionsrechte bauen aufeinander auf. Sie können Benutzern z. B. nur das Recht zum Ansehen zuweisen. Wollen Sie das Recht zum Löschen zuweisen, ist das Recht zum Ansehen Voraussetzung hierfür und muss ebenfalls vergeben werden.

Rechtszustände:

Häkchen gesetzt	Recht erteilt
grünes Kästchen (bzw. ausgegrautes Häkchen im klassischen Windows-Design)	Recht nicht erteilt (= Standardeinstellung). Evtl. hat ein Benutzer aber über seine Gruppenzugehörigkeit entsprechende Rechte.
leeres Kästchen	Recht explizit entzogen (= verbieten). Das sogenannte "Verbieten" für Einzelbenutzer überstimmt das Recht, das der Benutzer aufgrund seiner Gruppenzugehörigkeit besitzt.

Klicken Sie auf die Kästchen um den jeweiligen Rechtszustand zu verändern.

2. Möglichkeit: Dokumenttyprechte über die Gruppe/den Benutzers ändern:

Wählen Sie den Knoten "Benutzerverwaltung".

Markieren sie den Zweig Gruppen. (Alternativ können Sie die Rechte ebenso auf Benutzerebene vergeben. In diesem Fall markieren Sie den Zweig Benutzer.)

Wählen Sie im mittleren Teilfenster die gewünschte Gruppe, deren Rechte Sie verwalten möchten aus und wählen Sie im Menü "Aktionen" den Befehl **Eigenschaften**. Wählen Sie den Reiter **Rechte**.

Abb.: Dialogfeld zur Rechteverwaltung für die Gruppe "Personalabteilung" in der Datenbank "Personal"

Gehen Sie wie nun wieder wie unter "1. Möglichkeit: Dokumenttyprechte über den Dokumenttyp vergeben" beschrieben vor.

Tipp

	Möchten Sie für mehrere Dokumenttypen/mehrere Benutzer oder Gruppen die gleichen Rechte vergeben, so können Sie sich die Arbeit erleichtern. Markieren Sie die entsprechenden Dokumenttypen bzw. Gruppen oder Benutzer und wählen Sie im Kontextmenü den Befehl **Rechte mehrfach setzen**. Setzen Sie die gewünschten Rechte wie gewohnt und bestätigen Sie Ihre Eingaben mit **Übernehmen**.

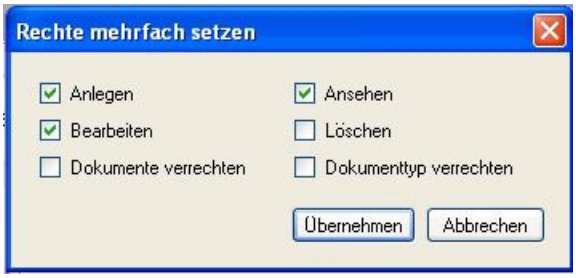


Abb: Gleichzeitiges Bearbeiten der Rechte für mehrere Dokumenttypen./merhrerer Benutzer oder Gruppen

Siehe auch:

Zugriffsrechte - Kon

Dateityp anlegen

Archivierten Dateien werden in PROXESS einem Dateityp zugeordnet. Dateitypen sind gekennzeichnet durch einen Namen und eine Erweiterung. Mit jedem Dateityp können Anwendungsprogramme bestimmt werden, mit denen der Benutzer in PROXESS die archivierte Datei dieses Dateityps ansieht und bearbeitet. Gängige Beispiele für Dateitypen sind Scanning, Word-Datei oder COLD-Datei.

Schritt für Schritt:

Verbinden Sie sich mit der gewünschten Datenbank.

Wählen Sie in der Datenbank den Zweig "Dateityp" aus.

Wählen Sie über das Kontextmenü den Befehl **Neu**.

Es öffnet sich folgendes Dialogfenster:

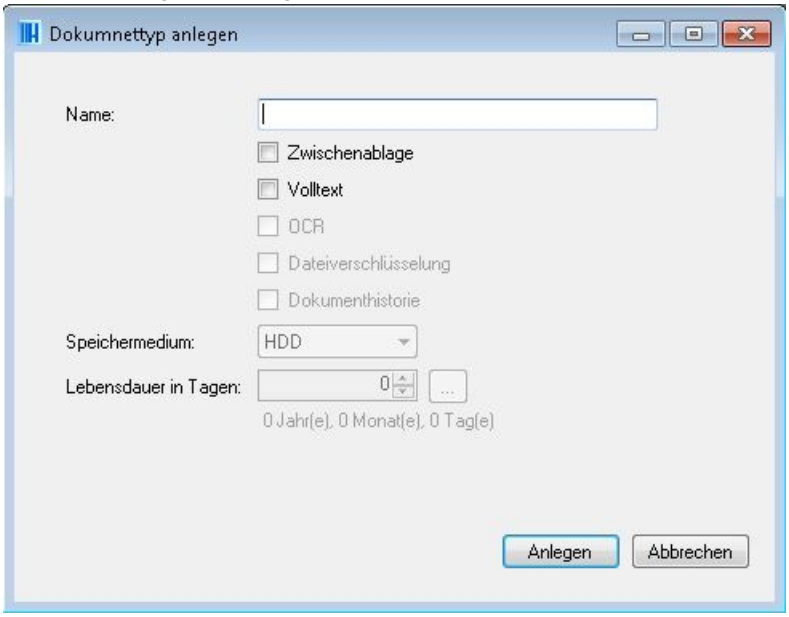


Abb.: Dialogfenster, um einen neuen Dateityp anzulegen

Wählen Sie nun einen Namen für den Dateityp und die Erweiterung.

Erläuterungen zu den Eigenschaften eines Dateityps:

Name	Hier können Sie den Namen des Dateityps ändern. Die Änderung wird auch für Dateien gültig, die bereits in PROXESS archiviert sind.
Erweiterung	Diese Dateierweiterung korrespondiert in der Regel mit der gewohnten Dateierweiterung der gewünschten Dateityp-Anwendung zum Bearbeiten der Datei.

Universeller Dateityp	Wird diese Option gewählt, wird beim Anlegen einer Datei durch den Benutzer aus der Dateiendung das jeweils passende Anwendungsprogramm aus der lokalen Registry herausgelesen und, falls dort ein Eintrag vorhanden ist, der Datei automatisch die korrekte Dateiendung anfügt. Diese Option ist zum Beispiel dann sehr nützlich, wenn beim Import aus dem Windows-Explorer unterschiedliche Datein ausgewählt und importiert werden.
Volltextrecherche aktivieren	Hier wird der Dateityp für die Volltextrecherche aktiviert und freigeschaltet. Voraussetzung. (siehe auch: Eigenschaften von Dokumenttypen)
OCR aktivieren	Hier aktivieren Sie den Dateityp für die OCR-Funktion.
für OCR-Lesen	Hier können Sie den Dateityp für die OCR-Texterkennung aktivieren. Die Erkennungsvorgang muss allerdings im PROXESS Client manuell angestoßen werden. Beispiel: Sie aktivieren den Dateityp "Scanning" für das OCR-Lesen.
für OCR-Ergebnis	Hier können Sie den Dateityp für die Ausgabe von erkanntem OCR-Text aktivieren. Beispiel: Sie aktivieren den Dateityp "Textdatei" für das OCR-Ergebnis, so wird der erkannte Text in eben diesem Dateityp abgespeichert.

---

siehe auch:

Dateityp mit Anwendung verknüpfen

Dateityp mit Vorlagedatei verknüpfen

Eigenschaften von Dateitypen

Dateitypen sind gekennzeichnet durch einen Titel und eine Erweiterung. Damit verbunden sind Anwendungsprogramme, mit denen der Benutzer in PROXESS den jeweilige Dateityp ansieht und bearbeitet. Beispiele für Dateitypen sind Scanning oder Word-Datei oder COLD-Datei.

Per Doppelklick auf den Dateityp erreichen Sie das jeweilige Eigenschaftenfenster:

Abb.: Eigenschaften des Dateityps "PDF"

Name	Hier können Sie den Namen des Dateityps ändern. Die Änderung wird auch für Dateien gültig, die bereits in PROXESS archiviert sind.
Erweiterung	Diese Dateierweiterung korrespondiert in der Regel mit der gewohnten Dateierweiterung der gewünschten Dateityp-Anwendung zum Bearbeiten der Datei.
Universeller Dateityp	Wird diese Option gewählt, wird beim Anlegen einer Datei durch den Benutzer aus der Dateiendung das jeweils passende Anwendungsprogramm aus der lokalen Registry herausgelesen und, falls dort ein Eintrag vorhanden ist, der Datei automatisch die korrekte Dateiendung anfügt. Diese Option ist zum Beispiel dann sehr nützlich, wenn beim Import aus dem Windows-Explorer unterschiedliche Datein ausgewählt und importiert werden.
Volltextrecherche aktivieren	Hier wird der Dateityp für die Volltextrecherche aktiviert und freigeschaltet. Voraussetzung. (siehe auch: Eigenschaften von Dokumenttypen)
OCR aktivieren	Hier aktivieren Sie den Dateityp für die OCR-Funktion.

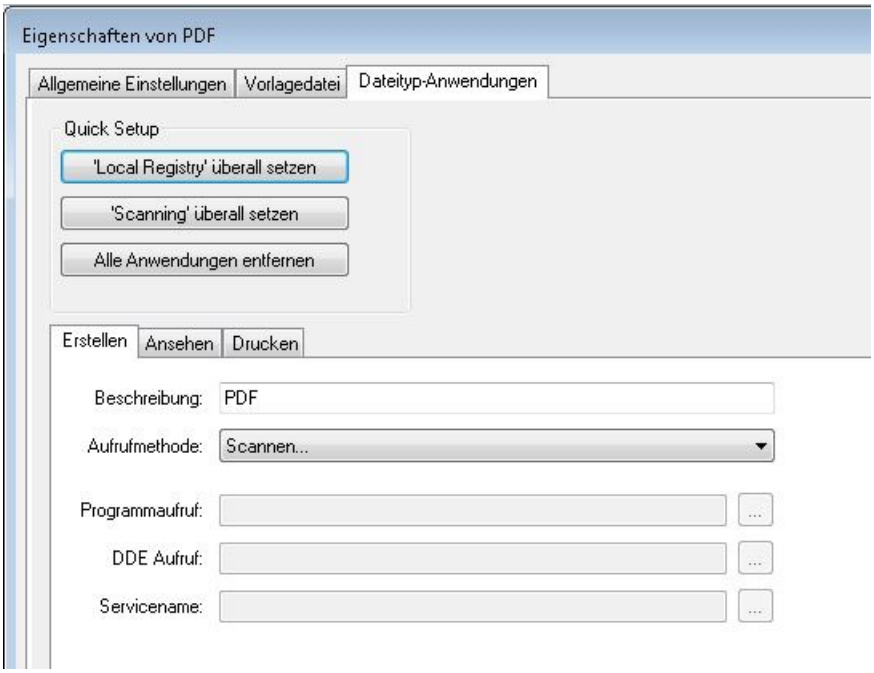
für OCR-Lesen	Hier können Sie den Dateityp für die OCR-Texterkennung aktivieren. Die Erkennungsvorgang muss allerdings im PROXESS Client manuell angestoßen werden. Beispiel: Sie aktivieren den Dateityp "Scanning" für das OCR-Lesen.
für OCR-Ergebnis	Hier können Sie den Dateityp für die Ausgabe von erkanntem OCR-Text aktivieren. Beispiel: Sie aktivieren den Dateityp "Textdatei" für das OCR-Ergebnis, so wird der erkannte Text in eben diesem Dateityp abgespeichert.

Dateityp mit Anwendung verknüpfen

Damit PROXESS zum Erstellen, Ansehen und Drucken von Dateien die richtige Anwendung für einen gewählten Dateityp startet, verbinden Sie jeden Dateityp mit einer Anwendung also einem Programm.

Per Doppelklick auf den Dateityp erreichen Sie das Eigenschaftenfenster.

Wählen Sie hier das Register "Dateityp-Anwendungen".



Über das **Quick-Setup** können Sie die gängigen Einstellungen mit einem einzigen Klick für "Erstellen", "Ansehen" und "Drucken" von Dateien setzen.

Folgende Aufrufmethoden können Sie für die drei Funktionen **Erstellen, Ansehen und Drucken** auswählen:

Programmaufruf	Hier können Sie manuell den Programmaufruf für die Applikation (z. B. Winword) hinterlegen, die sich beim Erstellen, Ansehen oder Drucken öffnen soll. Falls Sie auf ihrem Arbeitsplatz, ein Programm installiert haben, das mit der Dateinamenerweiterung dieses Dateityps verknüpft ist, wird automatisch die Syntax für den Programmaufruf aus der Systemregistrierung eingefügt.
DDE	Diese Möglichkeit gilt für alle DDE-fähigen Programme, z. B. für Microsoft Word oder Excel. Falls Sie auf Ihrem Rechner ein Programm installiert haben, das mit der Dateinamenerweiterung dieses Dateityps verknüpft ist, wird automatisch die Syntax für den DDE-Aufruf aus der Systemregistrierung eingefügt.

<table>
<tr><td>Lokale Registry</td><td>Die Option Lokale Registry dient zum schnellen, automatischen Einbinden von Applikationen. Sie bewirkt, dass auf jedem Client-Rechner in der Systemregistrierung nach einem Programm für die Dateinamenerweiterung dieses Dateityps gesucht wird.

Diese Methode ist sinnvoll bei sehr unterschiedlich installierten Rechnern. Ein weiterer Vorteil: Sie brauchen die korrekte Aufrufmethode nicht zu ermitteln, sondern nutzen bereits vorhandene Systeminformationen.

Wenn Sie die Option Lokale Registry nutzen, müssen Sie die Eingabefelder nicht ausfüllen.

Tipp
<table><tr><td>  </td><td>Für den universellen Dateitypen ist dies die korrekte Einstellung</td></tr></table></td></tr>
<tr><td>Scannen</td><td>Für gescannte Dokumente genügt es, die Option Scannen zu aktivieren, da für den Aufruf die PROXESS-eigenen DLLs benutzt werden. Die Eingabefelder bleiben leer.</td></tr>
<tr><td>Diaclip</td><td>Die Option Diaclip aktivieren Sie für das PROXESS-Modul Diaclip. Zusätzlich tragen Sie im Feld Programmaufruf einen oder mehrere Parameter ein. Die korrekte Syntax:
App=notepad.exe %1 Tiff=\\<Server>\<Path>\<Filename>.TIF XOffset=0 YOffset=0 FontWidth=144 FontHeight=240 LineHeight=240 CountLines=1 MaxLines=72
wird vom System automatisch eingetragen, sodass Sie nur die zutreffenden Werte ergänzen müssen. (siehe auch: Parameter für Diaclip)</td></tr>
</table>

Universeller Dateityp

Der universelle Dateityp erleichtert den Import von Dateien z. B. aus dem Windows Explorer.

Wird beim Import einer Datei über den PROXESS Windows Client der Universelle Dateityp gewählt, so wird automatisch anhand der Dateiendung im Windows Explorer das passende Programm aus der lokalen Registry ausgelesen.

So müssen nicht sämtliche, möglichen Dateitypen separat angelegt und konfiguriert werden.

Daher empfiehlt es sich grundsätzlich, einen universellen Dateityp anzulegen.

Schritt für Schritt:

Verbinden Sie sich mit der gewünschten Datenbank.

Markieren Sie im Zweig **Datenbank verwalten** den Knotenpunkt **Dateitypen.**

Wählen Sie nun über das Kontextmenü den Befehl **Neu**.

Es erscheint der Dialog "Dateityp anlegen":

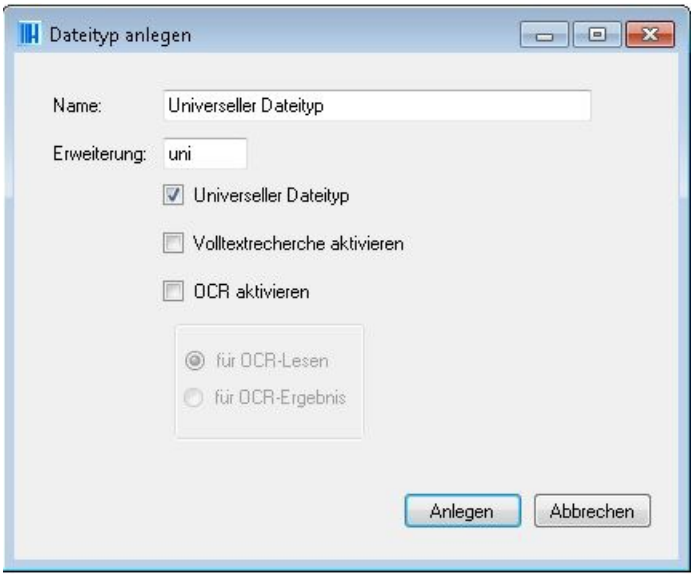


Abb.: Dialogfenster zum Anlegen eines universellen Dateityps

Prinzipiell können Sie jeden beliebigen Namen und jede beliebige Erweiterung verwenden. Wir empfehlen Ihnen die obenstehenden Einträge.

Aktivieren Sie die Eigenschaft **Universeller Dateityp**.

Bestätigen Sie Ihre Eingaben mit dem Befehl **Anlegen**.

Standardmaske einrichten

Mit dem sogenannten **Feldmasken-Editor** legen Sie die Position und Größe der Indexfelder in der Such- und Indexierungsmaske für den Windows-Anwender fest. Im ersten Schritt wird eine Standardmaske für die gesamte Datenbank, also das gesamte Archiv, festgelegt. Hiervon abweichend können Sie danach dokumenttypabhängige Masken einrichten (siehe: Dokumenttymaske einrichten).

Tipp

	Bevor Sie die Standardmaske einrichten, vergewissern Sie sich, dass bereits alle notwendigen Felder angelegt sind (siehe: Datenbankfeld anlegen).

Um den Feldmasken-Editor für die Standardmaske aufzurufen, markieren Sie die gewünschte Datenbank und wählen über das Kontextmenü den Befehl **Feldmaske editieren** (alternativ über das Aktionspanel rechts)**.**

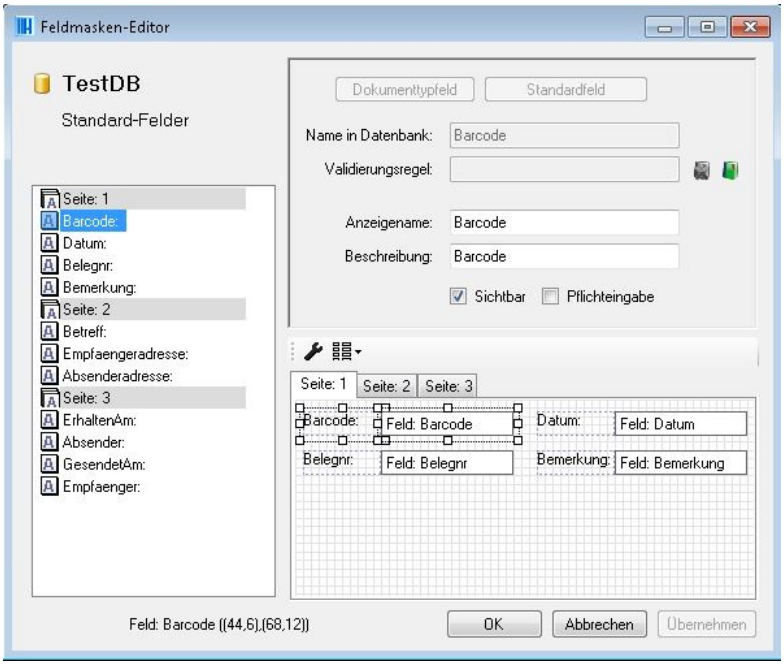


Abb.: Feldmasken-Editior für die Standardmaske der Datenbank TestDB

Im linken Teilfenster sehen Sie die Liste der vorhandenen Felder und deren Aufteilung auf die Seitenregister in der Maske. Die Reihenfolge der Felder in der Liste bestimmt auch deren Tabulatorposition für den Anwender.

Im rechten oberen Teilfenster finden Sie einige Feldeigenschaften:

Dokumenttypfeld/Standardfeld	Diese Option ist für die Standardmaske deaktiviert.
Name in Datenbank	Name des Feldes in der zugrundeliegenen SQL-Datenbank. Der Name entspricht dem Feldnamen, den Sie beim Anlegen des Feldes vergeben haben und kann nachträglich nicht mehr geändert werden.
Validierungsregel	Zeigt die zugewiesene Validierungsregel für das Feld an. Hier können Sie dem Feld eine Validierungsregel zuweisen oder entfernen (siehe auch: Validierungsregel einen Datenbankfeld zuordnen)
Anzeigename	Feldname, der in der Suchmaske angezeigt wird. Dieser wurde bei der Feldanlage vergeben und kann jederzeit geändert werden.
Beschreibung	Eine kurze Beschreibung für das Feld, die im Windows-Client in der Statuszeile angezeigt wird.
Sichtbar	Felder können zur besseren Übersicht ausgeblendet werden. Dies macht zum Beispiel dann Sinn, wenn bestimmte Felder nur bei einem einzelnen Dokumenttyp verwendet werden.
Pflichteingabe	Hier können Sie das Feld zu einem "Muss"-Feld für die Indexierung machen.

Im **rechten unteren Teilfenster** werden die Felder mit Position und Größe in der Maske dargestellt.

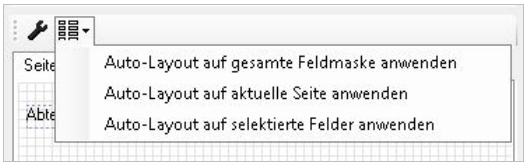
Am unteren Dialograng wird das aktuell markierte Feld mit seinen Koordinaten auf der Maske angezeigt.

Seitenposition und Tabulatorposition ändern:
Markieren Sie das Feld in der Liste und schieben Sie es per Drag & Drop an die gewünschte Stelle. Dabei ist es möglich mehrere Felder gleichzeitig zu markieren.

Neue Seite einrichten und Felder auf dieser Seite positionieren
Eine neue Seite erstellen Sie über das Kontextmenü innerhalb der Feldliste. Felder können Sie entweder per Drag & Drop auf diese Seite ziehen oder über das Kontextmenü auf diese Seite stellen.

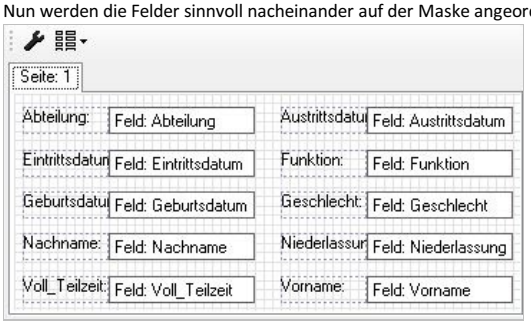
Felder auf eine andere Seite verschieben
1. Markieren Sie das Feld und wählen Sie im Kontextmenü den Befehl **Verschieben nach...**
2. Markieren Sie das Feld in der Auswahlliste links und verschieben es **per Drag & Drop innerhalb der Auswahlliste**
3. Markieren Sie das Feld in der Auswahlliste links und ziehen es per **Drag & Drop auf den Tab-Reiter der neuen Seite**

Maskeneinrichtung mit der Auto-Layout-Funktion
Alle angelegten Felder stehen in der Liste links. Auf der Maske werden diese Felder zunächst alle übereinandergelegt. Nutzen Sie daher die Autolayout-Funktion für einen ersten Maskenaufbau:



Wählen Sie **Auto-Layout auf gesamte Feldmaske anwenden**.

Nun werden die Felder sinnvoll nacheinander auf der Maske angeordnet:



Dokumenttypmaske einrichten

Innerhalb einer Datenbank werden unterschiedlichste Dokumenttypen archiviert. Die Anforderungen an die Indexierung können dabei völlig unterschiedlich sein. So sind zum Beispiel bei einer Eingangsrechnung Indexfelder wie Belegnummer und Lieferantenadresse interessant, bei einer E-Mail aber Felder wie Absender, Betreff und Empfänger. Im Dokumenttyp "Barcode-Pool" wird in der Regel nur ein Feld Barcode benötigt.

Um diesen unterschiedlichen Anforderungen gerecht zu werden, können Sie die Indexierungs- und die Suchmasken pro Dokumenttyp definieren. Ausgangsbasis ist hierbei immer die Standardmaske, die Sie vorab als Grundlage festgelegt haben sollten (siehe: Standardmaske einrichten).

Tipp

	Führen Sie vorab eine Organisationsanalyse für Ihr Unternehmen durch und legen Sie hierbei fest, welche Dokumenttypen und welche Indexfelder Sie für jeden Dokumenttyp benötigen. Ihr PROXESS-Projektpartner unterstützt Sie dabei.

Schritt für Schritt:

Markieren Sie den gewünschten Dokumenttyp und wählen Sie im Kontextmenü die Funktion **Feldmaske editieren.**

Es öffnet sich der Feldmasken-Editor:

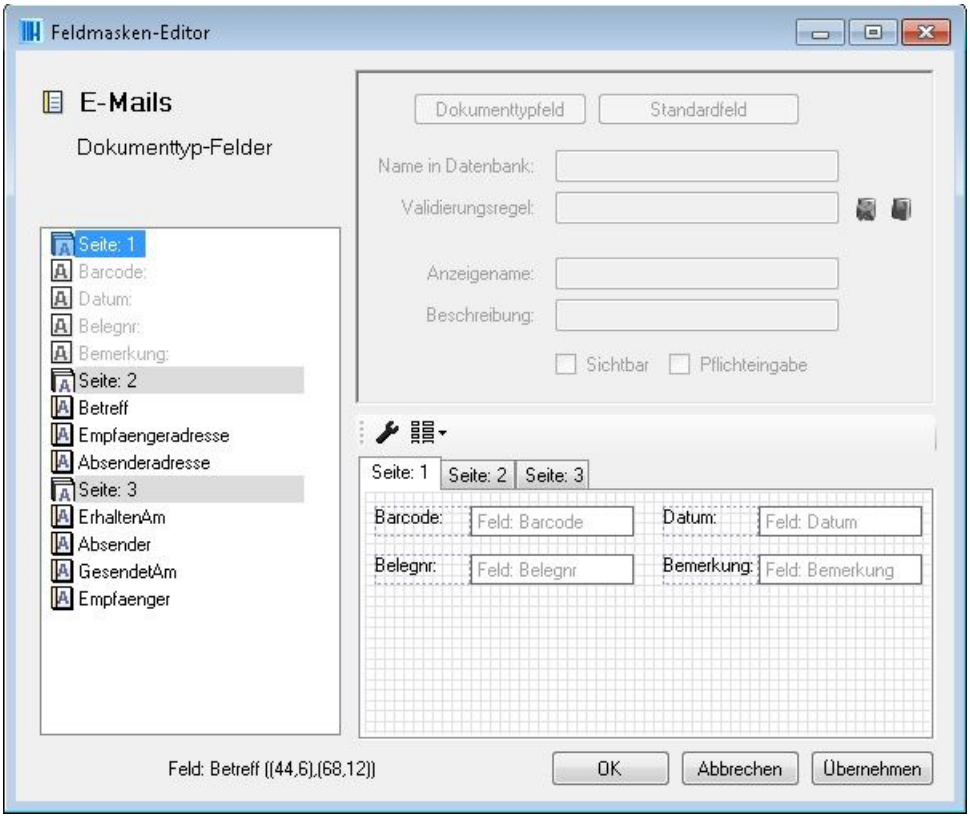


Abb.: Feldmaskeneditor für den Dokumenttyp "E-Mails"

Zunächst sind alle Felder in der Liste ausgegraut. Ausgegraute Felder sind Standardfelder und haben Standardeigenschaften.

Markieren Sie jetzt die Felder, die Sie in Dokumenttypfelder umwandeln möchten, und wählen Sie den Button **Dokumenttypfeld**. Nun werden diese Felder schwarz angezeigt und sind jetzt editierbar. Das bedeutet, Sie können den Anzeigenamen, die hinterlegte Validierungsregel und die Position auf der Maske verändern. Außerdem können

Sie das Feld ausblenden oder als Pflichtfeld definieren.

Ändern Sie nun für jedes Feld die Eigenschaften und die Position auf der Feldmaske, wie gewünscht.
(siehe hierzu die Erklärungen in Standardfeldmaske einrichten)

Beispiele für den Dokumenttyp **E-Mails:**
Markieren Sie "Seite 1" in der Liste und wählen Sie den Befehl **Seite löschen** über das Kontextmenü. Nun werden alle Felder von Seite 1 und von Seite 2 automatisch auf einer Seite zusammengefasst.
Wandeln Sie das Feld Barcode zum Dokumenttypfeld um und deaktivieren Sie die Funktion "Sichtbar". Nun erscheint das Feld nicht mehr auf der Maske.
Über die Funktion **AutoLayout** im Kontextmenü einer Seite können Sie die Felder auf der Seite wieder ausrichten.

Tastatursteuerung zum Anpassen der Feldmaske

Es ist möglich, die Felder mit Hilfe der Cursor-Tasten genau auf der jeweiligen Seite zu positionieren.

Markieren Sie hierzu ein oder mehrere Felder.

Folgende Kombinationen werden in Verbindung mit den Cursor-Tasten unterstützt:

Nur Cursor-Taste	Die selektierten Elemente werden um 1 Größeneinheit (ca. 1,5 Pixel) in die gewünschte Richtung verschoben.
Strg + Cursor-Tasten	Die selektierten Elemente werden um 2 Größeneinheiten in die gewünschte Richtung verschoben.
Alt + Cursor-Tasten	Die selektierten Elemente werden um 4 Größeneinheiten in die gewünschte Richtung verschoben.
Shift + Cursor-Tasten	Die Größe der selektierten Elemente wird vergrößert bzw. verkleinert durch Verschiebung des rechten bzw. unteren Randes der Elemente. Die Größe wird um 1 Größeneinheiten verändert.
Shift + Strg + Cursor-Tasten	Die Größe der selektierten Elemente wird um 2 Größeneinheiten verändert.
Shift + Alt + Cursor-Tasten	Die Größe der selektierten Elemente wird um 4 Größeneinheiten verändert.

Was sind Suchkriterien?

Suchkriterien ermöglichen dem Benutzer in PROXESS einen zusätzlichen Suchweg, den Sie hier für ihn vorbereiten. Der Sinn dieses Suchwegs besteht darin, dem Benutzer etwas Vertrautes, eine Art hierarchische Ablagestruktur, zur Verfügung zu stellen; vergleichbar einem Karteikasten.

Dazu haben Sie zwei Möglichkeiten:

Statisches Suchkriterium
Sie definieren das gewünschte Suchkriterium manuell und hinterlegen eine **SQL-Abfrage** an die relationale Datenbank.

Dynamisches Suchkriterium
Hier geben Sie lediglich das Feld an, das ausgewertet werden soll. In Abhängigkeit der archivierte Dokumente baut sich der Suchzweig automatisch auf.

Über die Erweiterte Suche kann der Benutzer auch mehrere Suchkriterien in einer Abfage kombinieren.

Statisches Sortier- und Suchkriterum

Bei einem statischen Suchkriterum definieren das gewünschte Suchkriterium manuell und hinterlegen eine **SQL-Abfrage** an die relationale Datenbank.

Schritt-für Schritt:

Verbinden Sie sich mit der gewünschten Datenbank und wählen Sie unter Datenbank den Zweig Suchkriterien.

Wählen Sie über das Kontextmenü den Befehl **Neues statisches Kriterium..**

Es erscheint dieses Dialogfenster:

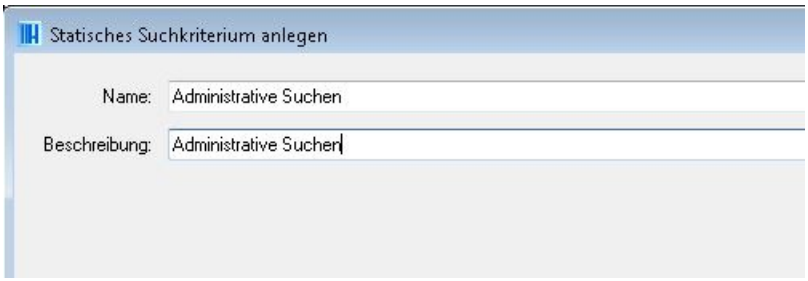


Abb.: Neues Statisches Suchkriterium anlegen

Geben Sie einen Namen und (optional) eine Beschreibung für das neue Suchkriterium an.

Wählen Sie den Befehl **Anlegen**.

Das neue statische Sortierkriterium erscheint nun in der Liste.

Um verschiedene statische Suchkriterien mit einer SQL-Suchbedingung zu definieren, öffnen Sie das Sortierkriterium nun per Doppelklick.

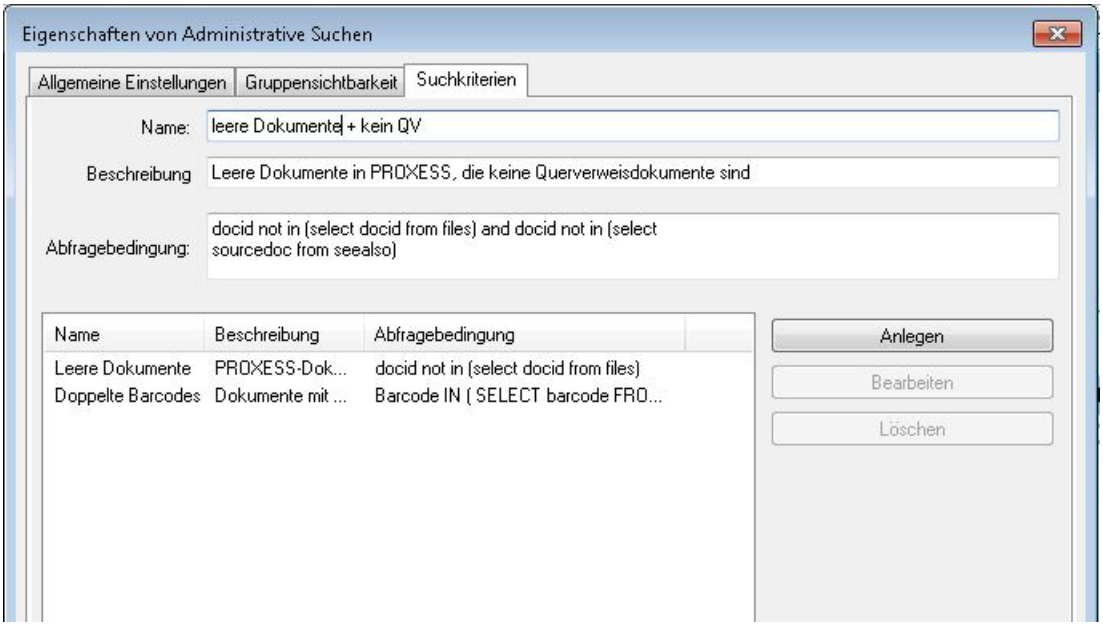


Abb.: Statische Suchkriterien mittels SQL-Abfrage definieren

Im obenstehenden Dialog finden Sie bereits einige Beispiele für SQL-Suchbedingungen. Weitere Beispiele finden Sie im Thema Beispiele für Suchkriterien.

Hinweise zur SQL-Bedingung

Die SQL-Bedingung ist das Kernstück eines Suchkriteriums. Startet der PROXESS-Benutzer eine Suche nach Sortier- und Suchkriterien, steuern die Suchkriterien die Datenbankabfrage.
Die Suchbedingung ist Teil einer SQL-Where-Klausel. Diese darf maximal 255 Zeichen lang sein. Die SQL-Syntax richtet sich danach, welchen Datenbankserver Sie verwenden (z. B. MSQL oder Oracle). Die Grundform einer Suchbedingung ist immer:
[Feldname] = [Wert].
Sie können in der SQL-Bedingung nicht nur die Felder verwenden, die Sie selbst angelegt haben, sondern auch die automatisch erstellten Kernfelder Dokumenttyp, Dokumentname sowie Erstellungs- und Änderungsdatum, Anlageautor und Änderungsautor. Die Namen dieser Datenbankfelder finden Sie in der docs-Tabelle der Datenbank.

Gruppensichtbarkeit

Wählen Sie den Reiter Gruppensichtbarkeit und fügen Sie die Benutzergruppen hinzu, die über den PROXESS Client Zugriff auf das Sortierkriterium haben sollen. Nach der Anlage eines Such- und Sortierkriteriums ist dieses zunächst für keine Benutzergruppe freigeben. Die Rechtvergabe ist nur auf der Ebene der PROXESS Benutzergruppen und nicht für einzelne Anwender möglich.

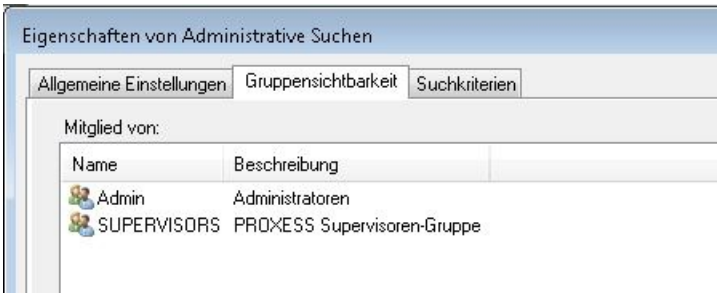


Abb.: Gruppensichtbarkeit des Sortierkriteriums "Administrative Suchen"

Dynamisches Suchkriterium

Beim dynamischen Suchkriterium geben Sie lediglich das Feld an, das ausgewertet werden soll. In Abhängigkeit der bereits vorhandenen Dokumente im Archiv baut sich der Suchzweig für den Anwender dann automatisch auf.

Schritt-für Schritt:

Verbinden Sie sich mit der gewünschten Datenbank und wählen Sie unter Datenbank den Zweig Suchkriterien.

Wählen Sie über das Kontextmenü den Befehl **Neues dynamisches Kriterium..**

Es erscheint dieses Dialogfenster:

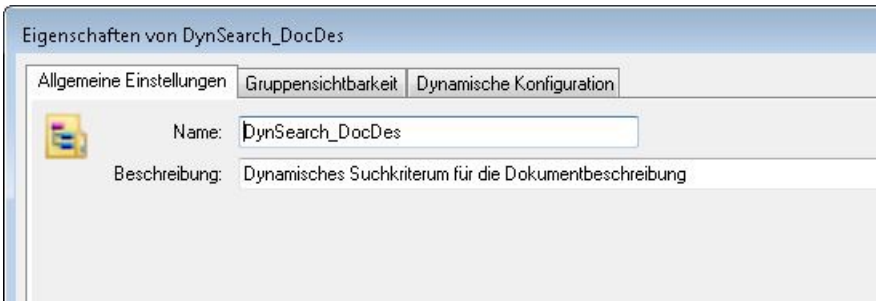


Abb.: Anlegen eines dynamischen Suchkriteriums

Geben Sie einen Namen und (optional) eine Beschreibung für das neue Suchkriterium an.

Wählen Sie aus, ob auf das Feld ein **Index gelegt** werden soll, um die Suche zu beschleunigen. Wenn es in der Datenbank sehr viele Datensätze mit sehr vielen unterschiedlichen Einträgen in diesem Feld gibt, verbessert ein Index die Performance. Gibt es hingegen nur wenige mögliche Einträge in einem Feld, z. B. fünf Länderkennzeichen auf 100.000 Datensätze, wirkt ein Index eher hemmend auf die Performance. Auch zu viele Indizes in einer Datenbank mindern die Performance
Wählen Sie den Befehl **Anlegen**.

Das neue dynamische Suchkriterium erscheint nun in der Liste.

Zur Konfiguration und zur Rechtevergabe auf das Suchkriterium, öffnen Sie das Suchkriterium per Doppelklick.

Gruppensichtbarkeit

Wählen Sie den Reiter **Gruppensichtbarkeit** und fügen Sie hier die Benutzergruppen hinzu, die über den PROXESS Client Zugriff auf das dynamische Suchkriterium haben sollen. Nach der Anlage eines Such- und Sortierkriteriums ist dieses zunächst für keine Benutzergruppe freigeben. Die Rechtvergabe ist nur auf der Ebene der PROXESS Benutzergruppen und nicht für einzelne Anwender möglich.

Dynamische Konfiguration

Im Reiter **Dynamische Konfiguration** haben Sie folgende Einstellungsmöglichkeiten.

Hierarchieebenen der Darstellung	Bei Textfeldern können Sie entscheiden, ob die Suchkriterien volldynamisch gebildet werden sollen oder ob Sie die Einteilung und die Anzahl der Ebenen vorgeben wollen. Steht der Zähler für die Hierarchieebenen auf 0, bedeutet dies, dass die Ebenen und Ebenenbezeichnungen aus dem tatsächlichen Dokumentenbestand abgeleitet werden. In der Regel ist dies die sinnvollste Einstellung, da sie zur übersichtlichsten Darstellung führt. Anwendungsbeispiel: Für ein Postleitzahlenfeld ergibt sich z. B. aus dieser Konfiguration eine Suchkriterienauswahl aus sämtlichen tatsächlich vorhandenen Postleitzahlen. Möchten Sie diese Liste der Übersichtlichkeit halber in Postleitzahlengruppen unterteilen (0er, 1er, 2er, 3er, 4er, usw.), stellen Sie hier die gewünschte Ebenenanzahl ein, in diesem Beispiel 1. Bis zu 50 Ebenen sind vom System her möglich. In der Praxis ist eine so tiefe Verschachtelung allerdings kaum notwendig.
Registerbezeichnungen	Wenn Sie die Hierarchieebenen festlegen, können Sie auch die Registerbezeichnungen bestimmen. Sie können die Zeichen bzw. Zeichenfolgen in das Feld eingeben, und zwar in der gewünschten Reihenfolge nacheinander ohne Trennzeichen. Da solche Registerbezeichnung häufig wie bei Karteikartensystemen aufgebaut sind, können Sie die Kontrollkästchen zum schnellen Ausfüllen benutzen. Doppelte Registerbezeichnungen sind ausgeschlossen, das System überprüft die Liste und meldet eventuelle Mehrfacheinträge. So erreichen Sie mit wenig Aufwand eine sehr differenzierte Auswahl an Suchkriterien.
Ziffern	Wenn Sie Ziffern von 0 -9 als Registerbezeichnungen verwenden wollen, aktivieren Sie dieses Kontrollkästchen. Bei zwei Hierarchieebenen z. B. wird daraus das Register 0 mit den Unterregistern 00 bis 09, dann Register 1 mit den Unterregistern 10 bis 19 usw. bis Register 9 mit den Unterregistern 90 bis 99.
alle Großbuchstaben **alle Kleinbuchstaben**	Für eine alphabetische Registerordnung der Suchkriterien können Sie zwischen Groß- und Kleinbuchstaben unterscheiden. Diese Unterscheidung ist jedoch nur wichtig, wenn Sie eine Oracle-Datenbank verwenden. Für MS SQL Server genügt es, das Kontrollkästchen alle Großbuchstaben zu aktivieren. Kleinbuchstaben werden hier automatisch einsortiert, sofern im Datenbestand Kleinbuchstaben vorhanden sind.
deutsche Sonderzeichen	Wenn in einer alphabetischen Ordnung Umlaute und ß enthalten sein sollen, aktivieren Sie dieses Kontrollkästchen. In Kombination mit Großbuchstaben, werden große Sonderzeichen einsortiert, in Kombination mit Kleinbuchstaben kleine Sonderzeichen.
restliche Sonderzeichen	Eine Auswahl an Sonderzeichen ist zusätzlich hinterlegt, z. B. Paragraphenzeichen. Weitere Sonderzeichen, z. B. dänische Buchstaben, können Sie mit dem ASCII-Code ergänzen. Den ASCII-Code entnehmen Sie der Windows-Zeichentabelle.

Beispiele für Suchkriterien

Hinweise zur SQL-Bedingung

- Die SQL-Bedingung ist das Kernstück eines Suchkriteriums. Startet der PROXESS-Benutzer eine Suche nach Sortier- und Suchkriterien, steuern die Suchkriterien die Datenbankabfrage
- Die Suchbedingung ist Teil einer SQL-Where-Klausel. Diese darf maximal 255 Zeichen lang sein. Die SQL-Syntax richtet sich danach, welchen Datenbankserver Sie verwenden (z. B. MSQL oder Oracle). Die Grundform einer Suchbedingung ist immer:
- [Feldname] = [Wert].
- Sie können in der SQL-Bedingung nicht nur die Felder verwenden, die Sie selbst angelegt haben, sondern auch die automatisch erstellten Kernfelder Dokumenttyp, Dokumentname sowie Erstellungs- und Änderungsdatum, Anlageautor und Änderungsautor. Die Namen dieser Datenbankfelder finden Sie in der docs-Tabelle der Datenbank.

Beispiele zu SQL-Suchbedingungen

1. Suche nach einem bestimmten Dokumenttyp

SQL-Suchbedingung: DocsDocTypeName = "[Dokumenttypname]"
Diese Bedingung können Sie unabhängig von der Systemkonfiguration einsetzen.

2. Suche nach dem Erstellungsdatum

SQL-Suchbedingung: DATEPART (year, dateofcreate)
Das Argument, das den gewünschten Teil spezifiziert, steht in der Klammer. Sie können als SQL-Bedingung auch eine Verknüpfung verwenden.

3. Suche nach Erstellungdatum (Zeitraum):
SQL-Suchbedingung: createdate between '11.03.1997 20:00' and '12.03.1997 16:00'

4. Suche nach dem Ersteller eines Dokuments
Ermittlung der entspechenden UserID durch ISQL/w durch folgende Abfrage in der Hauptdatenbank von PROXESS:
*select userid*10000,shortname from users*
Ergebnis durch 10000 teilen (z. B 2.000,00/10000)
SQL-Suchbedingung eingeben z. B. creator = $0.0002

5. Suche nach doppelten Barcodes
SQL-Suchbedingung: Barcode IN (SELECT barcode FROM docs GROUP BY barcode
HAVING COUNT(barcode) > 1)

6. Suche nach leeren Dokumenten:
SQL-Suchbedingung: docid not in (select docid from files)

7. Suche nach allen Querverweisdokumenten:
SQL-Suchbedingung: docid in (select sourcedoc from seealso)

8. Suche nach leeren Dokumenten, die keine Querverweisdokumente sind:
SQL-Suchbedingung: docid not in (select docid from files) and docid not in (select sourcedoc from seealso)

9. Suche nach angelegten Dokumenten der letzten 30 Tage:
SQL-Suchbedingung: datepart (dy,createdate) > (datepart(dy,getdate()) - 30)

Tipp

Alle Suchkriterien zu einem Sortierkriterium werden mit ODER verknüpft, das Ergebnis mit UND.

Formal: (A oder B oder C oder ...N) und (AA oder BB oder CC oder...NN) und ...
Ob eine Suchbedingung syntaktisch korrekt und sinnvoll ist, wird vom System nicht überprüft.
Wenn Sie sich nicht ganz sicher sind, testen Sie das Suchkriterium in PROXESS.

Validierungsregel anlegen

Validierungsregeln sind Eingabehilfen für Felder. In PROXESS gibt es:

- Thesauren für Textfelder,
- Zeiträume für Datumsfelder,
- Maximum- und Minimumangaben für Komma- und Ganzzahlfelder.
- Externe Thesauren

Durch Validierungsregeln, wie z. B. einer Pull-Down-Liste mit einer Auswahl von möglichen Einträgen für ein Feld, können Tipppfehler oder unplausible Eingaben so weit als möglich ausgeschlossen werden.

Eine Validierungsregel wird zunächst angelegt. In einem zweiten Schritt wird die Regel mit einem oder mehreren Datenbankfeldern verknüpft (siehe: Datenbankfeld Eigenschaften).

Schritt für Schritt:

Wählen Sie im Knotenpunkt Datenbank den Eintrag "**Validierungsregeln**" aus. Wählen Sie nun im Aktionspanel rechts (alternativ über das Kontextmenü) den Befehl **Neu**.

Es erscheint folgender Dialog:

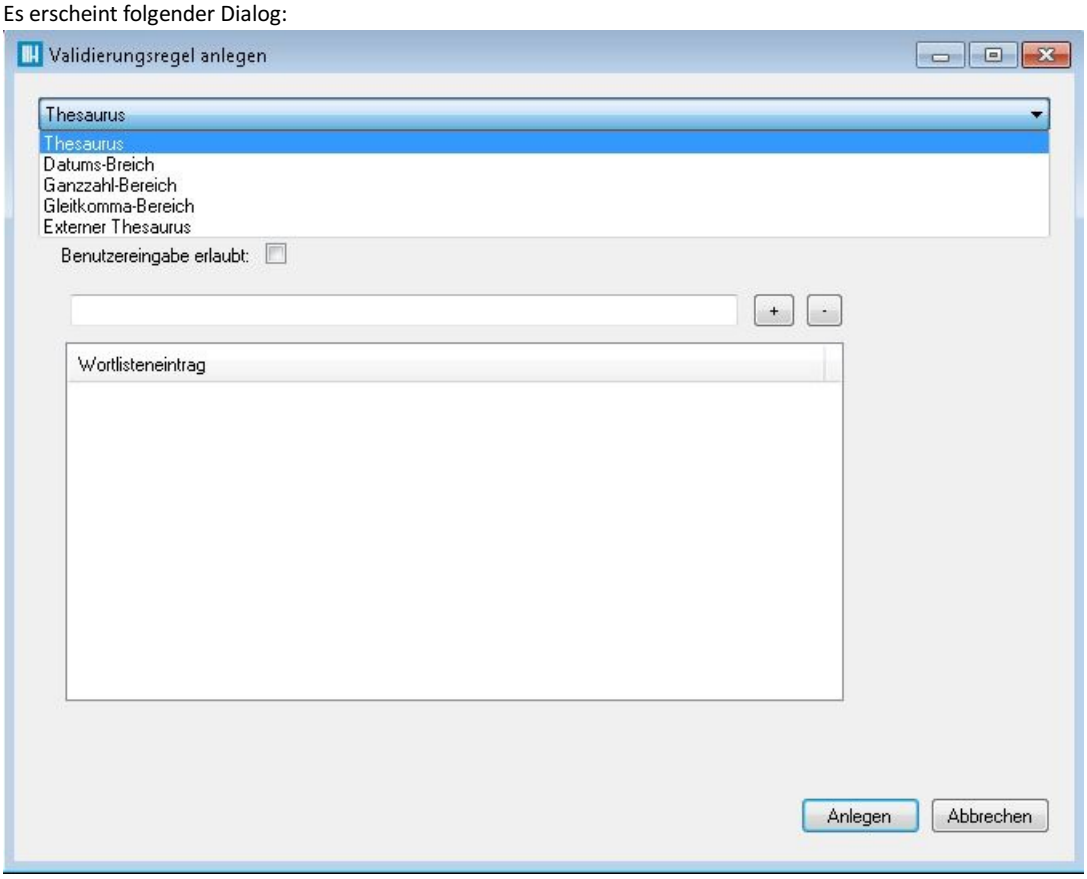


Abb.: Auswahl einer neuen Validierungsregel

Folgende Einstellungen sind möglich:

Thesaurus (für Textfelder)	Hier können Sie einen **Namen für den Thesaurus** vergeben. Zudem können über die **Wortliste** feste Feldeinträge, die der Anwender in Form einer Auswahlliste sieht, vorgegeben werden. Im Feld **Maximale Wortlänge** können Sie die maximale Zeichenanzahl für einen Eintrag festlegen. Über die Option "**Benutzereingabe erlaubt**" kann festgelegt werden, ob Anwender die Liste selbst füllen oder um neue Einträge erweitern können oder ob sie auf die vorgegeben Einträge beschränkt sind.
Datum-Bereich, Ganzzahl-Bereich Gleitkomma-Bereich	Neben dem Namen für den Thesaurus können Sie jeweils eine Unter- und eine Obergrenze für die Benutzereingabe vorgeben.
Externer Thesaurus	Über externe Thesauren können Wertelisten aus externen Systemen wie z. B. aus einer PROXESS-fremden SQL-Datenbank definiert werden. Dieser Zugriff auf externe Datenbanken ermöglicht beispielsweise, Benutzer- und Rechteinformationen auf dem führenden ERP-System online zu verwenden und gleichzeitig eine doppelte Datenpflege zu vermeiden.

Die Verknüpfung der angelegten Validierungsregel mit einem Datenbankfeld nehmen Sie hier vor: Datenbankfeld Eigenschaften

Validierungsregel einem Datenbankfeld zuordnen

Validierungsregeln sind Eingabehilfen für verschiedene Datentypen:

- Thesauren für Textfelder,
- Zeiträume für Datumsfelder,
- Maximum- und Minimumangaben für Komma- und Ganzzahlfelder.

Durch Validierungsregeln, wie z. B. eine Pull-Down-Liste mit einer Auswahl von möglichen Einträgen für ein Feld, können Tipppfehler oder unplausible Eingaben so weit als möglich ausgeschlossen werden.

Validierungsregeln werden zunächst angelegt (siehe: Validierungsregel anlegen) und in einem zweiten Schritt mit Feldern verknüpft. Die Einhaltung der verknüpften Regel wird dann bereits bei der Benutzereingabe überprüft.

Warnhinweis

	**Wenn Sie Felder mit einer Validierungsregel verknüpfen, nachdem Dokumente angelegt worden sind, stellen Sie sicher, dass die Regel alle bereits vorhandenen Feldeinträge berücksichtigt. Sonst gibt es beim Bearbeiten dieser Dokumente Fehlermeldungen.**

Validierungsregel einem Standard-Datenbankfeld zuordnen

Wählen Sie im Knotenpunkt Datenbank den Eintrag Felder aus. Markieren Sie das Feld, das verknüpft werden soll. Nun wählen Sie im Aktionspanel rechts (alternativ über das Kontextmenü) den Befehl **Eigenschaften.**

Es erscheint ein Dialogfenster:

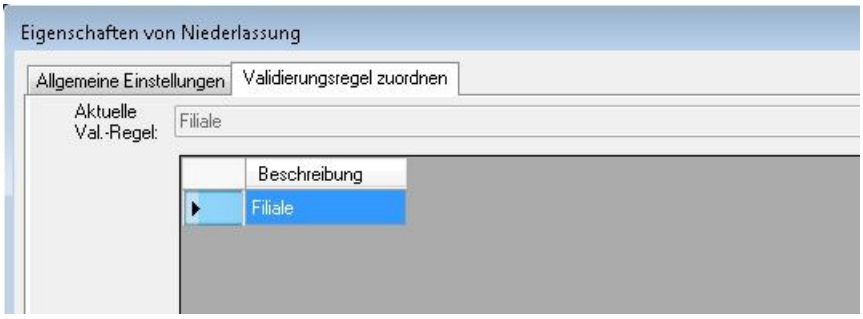


Abb.: Zuordnen der Validierungsregel "Filiale" zu dem Feld "Niederlassung"

Im Register "Allgemeine Einstellungen" finden Sie eine allgemeine Übersicht. Hier können Sie bereits erkennen, ob dem Feld eine Validierungsregel zugeordnet ist.

Regel sichtbar oder nicht?
Ober- und Untergrenzen als Validierungsregel werden oft vorgegeben um Tippfehler bei der Eingabe zu vermeiden. Möchten Sie den Benutzer nicht durch die Angabe von Eingabegrenzen irritieren, so müssen Sie dennoch nicht auf die Validierungsregeln verzichten. Wählen Sie in diesem Fall einfach die Option "Regel nicht sichtbar".

Im Register "Validierungsregel zuordnen" können Sie über den Befehl **Ausgewählte Regel setzen** den aktuell markierten Eintrag in der Liste der vorhandenen Validierungsregeln zuordnen. Ebenso können Sie über den Befehl **Regel entfernen** die Zuordnung wieder auflösen. Speichern Sie Ihre Eingaben.

Validierungsregel einem Dokumenttypfeld zuordnen

Wählen Sie die gewünschte Datenbank und markieren Sie den gewünschten Dokumenttyp.

Wählen Sie nun den Feldmaskeneditor über den Befehl **Feldmaske editieren** im Kontextmenü.

Sobald Sie ein Standardfeld hier zum Dokumenttypfeld umgewandelt haben, können Sie dem Feld eine Validierungsregel zuordnen. Diese Zuordnung gilt dann allerdings nur für den ausgewählten Dokumenttyp.

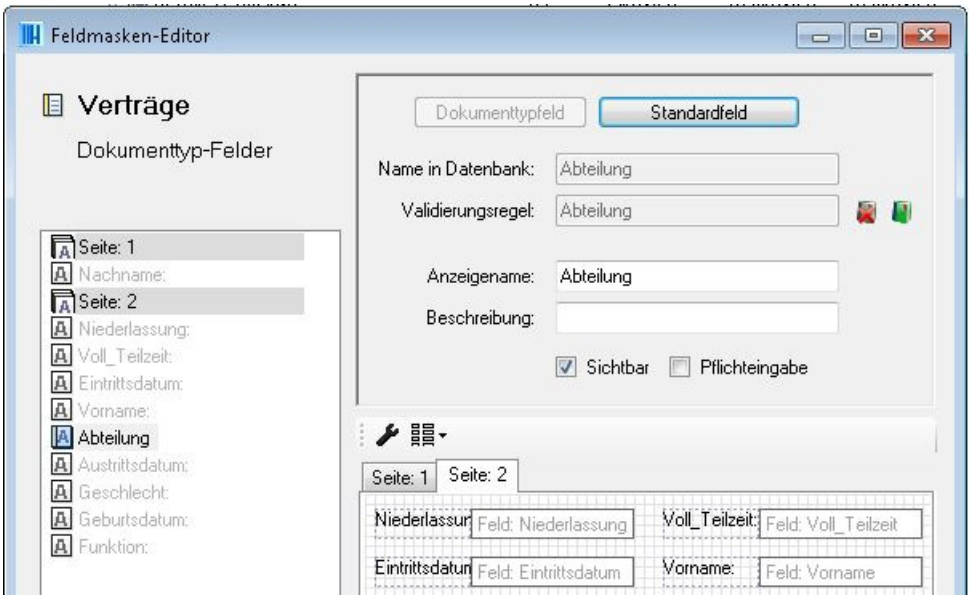


Abb.: Zuordnung einer Validierungsregel "Abteilung" für das Dokumenttypfeld "Abteilung"

Externer Thesaurus

Externe Thesauren ermöglichen es, abhängig vom aktuell angemeldeten Benutzer, individuelle Auswahllisten in einem Feld für die Anlage von Dokumenten und für die Recherche von Dokumenten anzuzeigen.

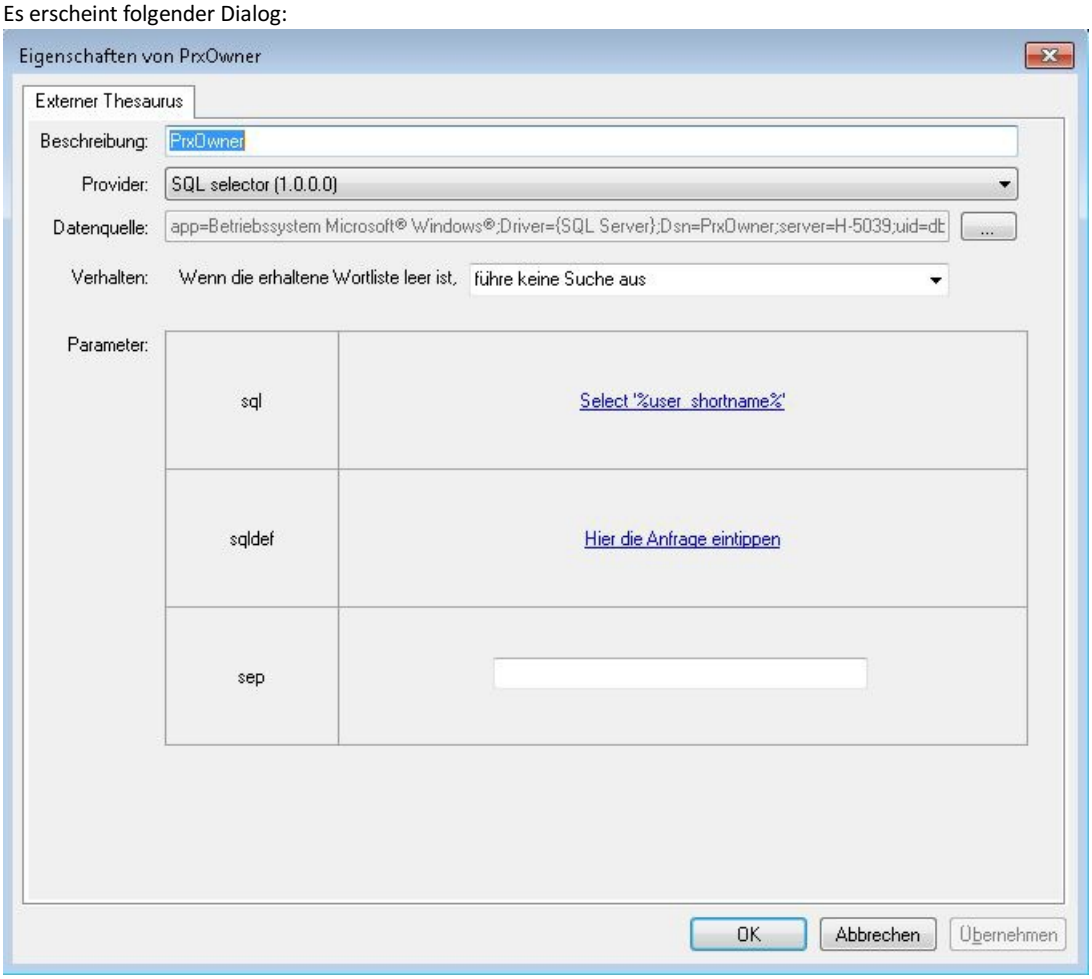
Die Wertelisten werden dabei über frei definierbare SQL-Abfragen online aus externen Systemen wie z. B. einer externen SQL-Datenbank ermittelt. Dies ermöglicht es beispielsweise, Benutzer- und Rechteinformationen auf dem führenden ERP-System online zu verwenden und damit eine doppelte Datenpflege zu vermeiden.

Beispiel:
Sachbearbeiter A ist zuständig für die Auftragsbearbeitung der Region "Nord". Die Zuordnung von Mitarbeiter zu Region findet sich in einer externen SQL-Datenquelle des ERP-Systems. Sie können nun einen externen Thesaurus so anlegen und konfigurieren, dass der Sachbearbeiter A aufgrund seiner PROXESS-Benutzereigenschaften nur Dokumente aus der Region "Nord" aufrufen kann. Andere Auswahlmöglichkeiten im Feld "Region" werden dem Anwender nicht angezeigt.

Schritt für Schritt:

Wählen Sie im Knotenpunkt "Datenbank" den Eintrag "**Validierungsregeln**" aus. Wählen Sie nun im Aktionspanel rechts (alternativ über das Kontextmenü) den Befehl **Neu**.
Wählen Sie hier den Eintrag **Externer Thesaurus** aus.

Es erscheint folgender Dialog:



Beschreibung	Eindeutiger Name für die externe Thesaurusregel

Provider	Name des Validation Providors (Hier: SQL-Providor als Schnittstelle zur SQL-Datenbank)
Datenquelle	Es öffnet sich der Dialog zur Angabe der Verbindungsparameter zur externen Datenquelle. (z.B. zur ODBC-Quelle) Tragen Sie die Login-Informationen für einen Datenbankuser ein. Der hier eingetragene DB-User muss mindestens DB-Owner sein, bzw. über die Rechte eine DB-Owner verfügen. Über den Button OK wird automatisch der entsprechende Connection string erstellt. (siehe unten)
Verhalten	Gibt das Verhalten des PROXESS-Clients an, wenn die durch die SQL-Abfrage ermittelte Werteliste für den aktuellen Benutzer leer ist (entweder ist er nicht als Benutzer in der externen Datenbank eingetragen oder ihm ist kein Wert zugeordnet) Beispiel oben: Der angemeldete Benutzer ist nicht in der externen Datenbank existent oder dem angemeldeten PROXESS-Benutzer ist keine Region zugewiesen. In diesem Fall gibt es zwei Möglichkeiten: a) es wird keine Suche ausgeführt, d. h. es werden keine Dokumente in der Trefferliste angezeigt. b) es werden alle Treffer angezeigt (Beispiel: Dokumente aus allen Regionen werden angezeigt)
sql	Durch Klicken auf den Text können Sie ein frei definierbare SQL-Abfrage mit Ersetzungsvariablen eingeben (siehe unten)
sqldef	Durch Klicken auf den Text können Sie eine Standard-SQL-Abfrage eingeben, die ausgeführt wird, wenn das Ergebnis der eigentlichen SQL-Abfrage leer ist.
sep	Hier geben Sie den verwendeten Separator zwischen den Einträgen in der Werteliste an.

Definition einer ODBC-Datenquelle

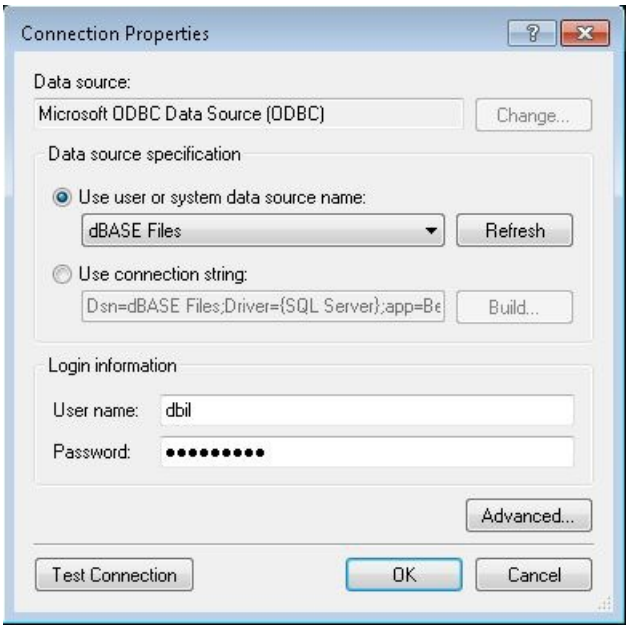


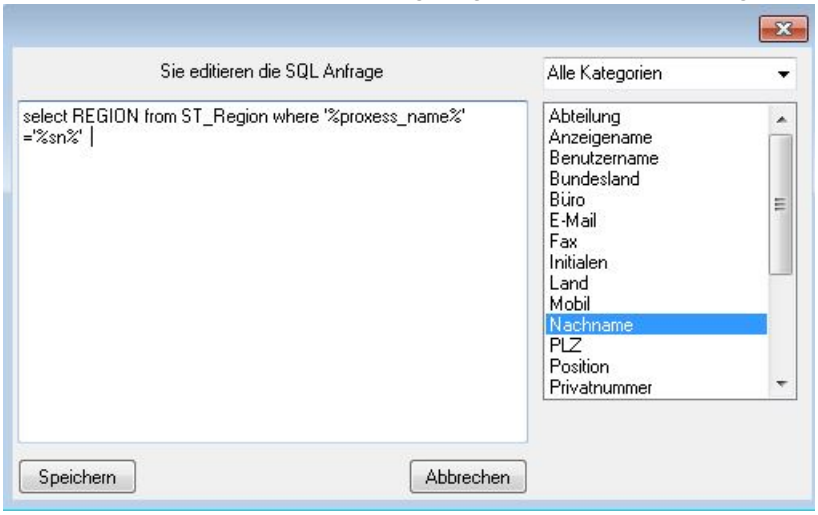
Abb.: ODBC Datenquelle für externen Thesaurus definieren

Schritt-für-Schritt:

1. Wählen Sie den Datenquellennamen aus.
2. Geben Sie die Login-Informationen zur Datenquelle ein.
3. Nach Klicken der Schaltfläche **Build** erscheint der Dialog "SQL-Server-Anmeldung"
4. Hier wählen Sie den Datenbankservernamen aus und durch die Schaltfläche **Optionen** wählen Sie die Datenbank, die als externe Quelle dienen soll.
5. Übernehmen Sie die übrigen Werte aus der Voreinstellung und bestätigen Sie die Eingaben mit **OK**.
6. Durch den Befehl **Test Connection** können Sie die Verbindungsdaten überprüfen.

SQL-Abfrage definieren

Durch Klicken auf den Text "Hier SQL-Abfrage eingeben" öffnet sich das Dialogfenster:



Geben Sie nun die gewünschte SQL-Abfrage ein. Durch Doppelklick auf einen Wert in der Auswahlliste rechts wird die zugehörige Ersetzungsvariable an der Position des Cursers in das SQL-Statement eingefügt.

Beispiel oben:
SQL-Statement: select REGION from ST_Region where '%proxess_name% = '%sn%'

Es wird auf eine SQL-Tabelle zugegriffen, mit einer Zuordnung vom jeweils angemeldeten PROXESS-Benutzer zu bestimmten Regionen (Nord, Süd, Ost, West).

Externen Thesaurus testen

Markieren Sie im Knotenpunkt "Datenbanken/Thesauren" den gewünschten externen Thesaurus und wählen Sie im Kontextmenü den Befehl **Testen.**

Es öffnet sich der Testdialog:

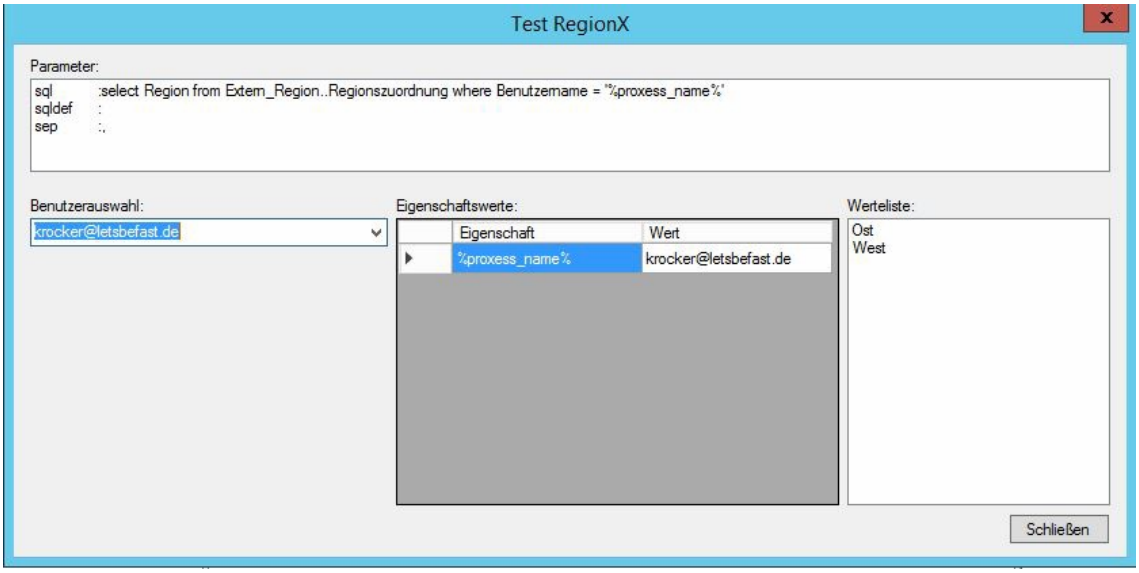


Abb.: Testdialog für externe Thesauren

Im Beispiel oben sind dem Benutzer "krocker@letsbefast.de" die Regionseinträge "Ost" und "West" zugeordnet. D.h. er sieht nur die Dokumente, in denen das Feld "Region" mit einem der beiden Werte gefüllt ist.

Parameter	Zeilenweise Darstellung der konfigurierten Parameter zur Abfrage.

Benutzerauswahl
Hier kann der Benutzer ausgewählt werden, für den die Werteliste angezeigt werden soll, die die SQL-Abfrage ergibt. Ist ein Defaultparameter (sqldef) definiert, so wird dessen Abrageresultat dargestellt, falls das Resultat für den Benutzer leer ist.
Eigenschaftswerte
Darstellung aller in den Parametern verwendeten Ersetzungsvariablen und Ihre Werte für den ausgewählten Benutzer
Werteliste
Die durch die SQL-Abfrage ermittelte Werteliste für den ausgewählten Benutzer. Diese Liste wird dem Anwender angezeigt.

Wichtiger Sicherheitshinweis für Hochsicherheitsdatenbanken:

	Berechtigungen in gesicherten Datenbanken dürfen nur durch den PROXESS Supervisor oder vom ihm autorisierte Datenbankverwalter administriert werden. Im Bereich der Datenbank- und Dokumenttyprechte wird dies systemseitig sichergestellt. **Bei Verwendung der externen Thesauren als Implementierung inhaltsbasierter Zugriffsrechte kann ein Schutz gegen Manipulation der externen Datenquelle jedoch nicht systemseitig sichergestellt werden.** Hier gehört es gerade zum Prinzip, Autorisierungsinformationen aus Drittsystemen verwenden zu können, die sich nicht unter Kontrolle von PROXESS befinden. **Daher obliegt die Sicherung dieser Informationen dem Systembetreiber.**

Vorlagedatei anlegen

Aus Windows-Dateien können Sie Vorlagen erstellen, wie z. B Formulare oder Briefbögen. Diese Vorlagedateien stehen dann für die Dateitypen-Verwaltung zur Verfügung. Das Arbeiten mit Vorlagedateien ist eine Komfortfunktion, aber vom System her nicht notwendig.

Beispiel:
Wenn in Ihrem Unternehmen immer wieder gleichartige Dokumente wie Firmenbriefe erstellt werden, können Sie mit Hilfe einer Vorlagedatei einen Dateityp erstellen, der Ihre Textverarbeitung zusammen mit dem Briefbogen aufruft.

Schritt für Schritt:
Erstellen Sie die benötigten Vorlagedateien mit der gewünschten Anwendung (wie z.B. Winword). Jetzt erst kann die Vorlagedatei in PROXESS eingebunden werden:

Verbinden Sie sich mit der gewünschten Datenbank.

Wählen Sie im Zweig Vorlagedateien den Befehl **Neu** über das Kontextmenü oder über das Aktionspanel.

Abb.: Erstellen einer neuen Vorlagedatei

Vergeben Sie eine Bezeichnung für die Vorlagedatei in PROXESS.

Wählen Sie über den Explorer die bereits vorbereitete Vorlagedatei aus.

Über den Befehl **Anlegen** speichern Sie Ihre Angaben.

Vorlagedatei mit Dateityp verknüpfen

Angelegte Vorlagedateien können mit einem vorhandenen Dateityp verknüpft werden. Dies bedeutet, dass z. B. bei der Neuanlage einer Datei automatisch die hinterlegte Vorlagendatei geöffnet wird.

Ein klassisches Beispiel für eine Vorlagendatei ist eine Word-Vorlage für einen Firmenbrief.

Schritt für Schritt:

Verbinden Sie sich mit der gewünschten Datenbank und wählen Sie im Zweig **Datenbanken/Dateitypen** den gewünschten Dateityp aus.

Nun wählen Sie den Befehl **Eigenschaften** über das Kontextmenü oder über das Aktionspanel rechts.

Wählen Sie das Register "Vorlagedatei":

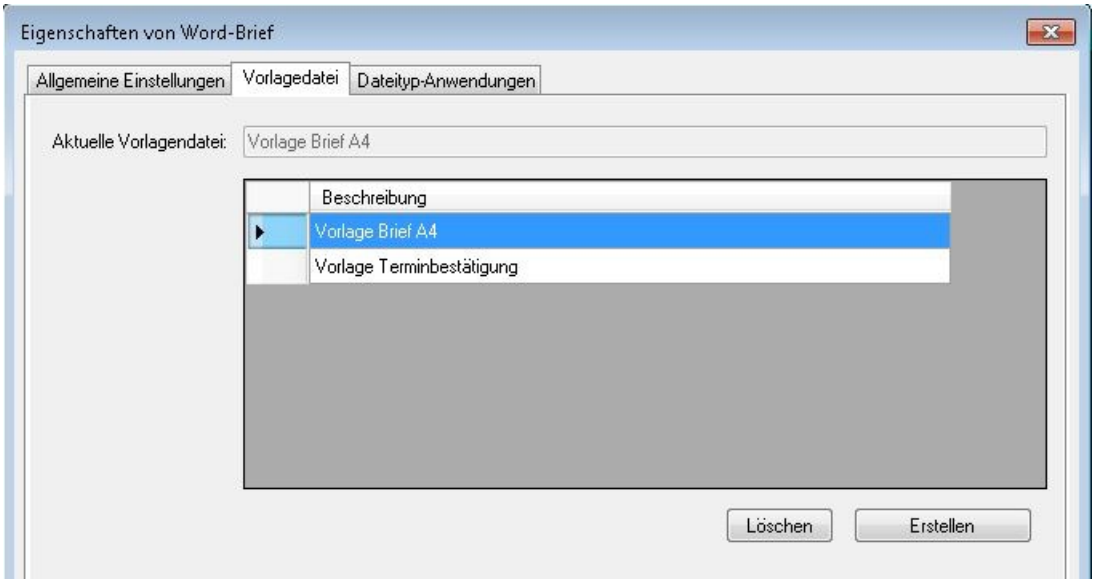


Abb: Vorlagedatei mit Applikation verbinden

Unter **Aktuelle Vorlagendatei** sehen Sie, ob bereits eine Verknüpfung eingerichtet wurde.

Wählen Sie aus der Liste die gewünschte Vorlage aus.

Mit dem Befehl **Erstellen** wird die Verknüpfung von Vorlagedatei zu Dateityp hergestellt.

Mit dem Befehl **Löschen** können Sie die Verknüpfung jederzeit wieder aufheben. Dies wirkt sich nicht rückwirkend auf bereits archivierte Dateien aus.

Parameter für DiaClip-Dateien

Die Option "Diaclip" in den Dateityp-Anwendungen ermöglicht die Darstellung von COLD-Dateien mit einem Hintergrundbild (z. B dem Firmenbriefbogen).

Hierzu stehen Ihnen verschiedene Parameter zur Bestimmung und Justierung des Hintergrundbildes zur Verfügung.

Zunächst geben Sie an, welche TIF-Datei als Hintergrund hinterlegt werden soll. PROXESS liefert bereits weiße Hintergrund-TIF-Dateien in DIN A3 und A4 mit. Wollen Sie ein Firmenformular verwenden, so scannen Sie dieses ein und kopieren Sie die TIF-Datei am besten in das System-Verzeichnis.
Im Feld Programmaufruf geben Sie nun einen oder mehrere Parameter an und weisen diesen einen Wert zu.
Syntax: [Parameter] = [Wert]
Zwischen den Gleichheitsbedingungen geben Sie als Trennzeichen ein Leerzeichen ein. Ob innerhalb eines Ausdrucks Leerzeichen stehen, spielt keine Rolle, ebenso die Groß- und Kleinschreibung.
Die Reihenfolge der Parameter ist beliebig. Falls ein Parameter in der Zeile mehr als einmal vorkommt, wird nur der berücksichtigt, der am weitesten rechts steht.

Übersicht über Parameter und Werte:

Parameter	Erläuterung	Wert
App	Diesen Parameter brauchen Sie nur im Register Anlegen. Er gibt an, mit welcher Applikation die DClip-Datei erstellt wird. Diese Möglichkeit nutzt der Anwender in PROXESS nur, wenn DClip-Dateien per Hand angelegt werden. Normalerweise geschieht dies aber mit COLD-Daten automatisch. Sie können z. B. Notepad angeben.	[Programmname].EXE%1 %1 dient zur Übergabe des Pfades und wird plattformunabhängig verstanden.
TIFF	Definiert das Hintergrund-TIFF und ist unbedingt notwendig.	[Pfadname]\ [Dateiname].TIF Wenn das Frontend im selben Verzeichnis liegt, genügt der Dateiname.
XOFFSET **YOFFSET**	Gibt die Seitenmaße an. X und Y werden nach deutschem Standard interpretiert.	Seitenmaß in TWIPS
FontWidth	Reguliert den Abstand zwischen den Buchstaben.	Weite in TWIPS
FontHeight	Gibt den Schriftgrad an	Höhe in TWIPS
LineHeight	Gibt den Zeilenabstand an	Abstand in TWIPS
CountLines	Gibt an, wann ein Seitenumbruch gesetzt werden soll	Wert 0 = ein Seitenumbruch wird durch ein Formfeed erzeugt Wert 1 = ein Seitenumbruch wird nach einer maximalen Zeilenzahl gesetzt
MaxLines	Gibt die maximale Zeilenzahl auf einer Seite an. Wird nur benutzt, wenn CountLines den Wert 1 hat.	Ganze Zahl z. B. 72 für DIN A4-Seite

Die Tabelle zeigt die Umrechnungsfaktoren für gängige Maßeinheiten unter Windows:

Maßeinheit	**Twips**	**pt**	**Zoll**	**cm**

1 Twip =	1	1/20	1/1440	1/567
1 pt =	20	1	1/72	0,35
1 Zoll =	1440	72	1	2,54
1 cm	567	28,35	0,39	1

Die Cold-Dateien für Diaclip enthalten normalerweise keine Formatierungsinformationen. Dann werden die hier definierten Werte für Seitenränder und Schriftgrade benutzt. Enthält eine Datei Formatanweisungen, werden diese benutzt.

Tipp

Um Formulare einzurichten, müssen Sie wissen, mit welcher Schriftgröße normalerweise gedruckt wird. Stellen Sie dann Schrifthöhe und -breite entsprechend ein.

Benutzerverwaltung - Konzept und Überblick

Mit PROXESS können nur registrierte Benutzer arbeiten. Um die Aufgaben der Benutzerverwaltung wahrnehmen zu können, müssen Sie Supervisor oder Datenbank-Bereichsadministrator sein.

Aufgaben der PROXESS-Benutzerverwaltung sind:

- Erstellung eines systemweiten Benutzerkonzepts
- Umsetzung des Konzepts durch Erstellung von Benutzerkonten und Gruppen
- Verwaltung und Pflege der Benutzerkonten und Gruppen
- Einrichten und Pflege von Zugriffsberechtigungen

Active Directory-Benutzer versus PROXESS-Benutzer

Als Systemadministrator sollten Sie alle Anwender, die mit PROXESS arbeiten, organisatorisch in zwei Benutzerkategorien unterteilen.

1. Benutzer mit Windows-Authentifizierung

Für diese Anwender übernimmt der Systemadministrator die Benutzerdaten des Windows Active Directory und vermeidet hierdurch eine doppelte Administration in Windows und PROXESS. Übernommene AD-Benutzer wählen bei der Anmeldung an PROXESS die Authentifizierungsoption "Windows" im Anmeldedialog des jeweiligen Moduls. Damit werden die Windowsanmeldedaten automatisch für die Anmeldung an PROXESS verwendet. Empfehlenswert ist es dabei, in den jeweiligen Moduleinstellungen den Anmeldedialog für AD-Benutzer nach der ersten Anmeldung zu unterdrücken.

Jedoch haben Mitglieder dieser Kategorie keinen Zugriff auf Hochsicherheitsdatenbanken, also solche mit aktivierter Hochsicherheit und Verschlüsselung. Damit soll verhindert werden, dass AD-Benutzer durch eine einfache Zuordnung in eine AD-Gruppe auf Windows-Ebene automatisch auch Zugriffsrechte auf besonders schützenswerte Dokumente und Daten in PROXESS erhalten, ohne dass diese explizit in PROXESS bekanntgegeben werden müssen. In der Praxis trifft dies wahrscheinlich die Mehrheit der Anwender, die z. B. nicht Mitglied der Geschäftsleitung oder des Personalbereichs sind und so auch keinen Zugriff auf besonders geschützte Daten benötigen. Für diese Benutzer kann durch die Windows Active Directory Integration eine doppelte Administration vermieden werden und damit eine Arbeitserleichterung für den Systemadministrator erreicht werden. Außerdem automatisiert sich für den Anwender die Anmeldung an den PROXESS-Modulen.

Alle Schritte zur Windows Active Directory Integration in PROXESS finden Sie hier.

Alle Schritte zur Windows Active Directory Integration in PROXESS finden Sie im Kapitel "Windows Active Direktory Integration".

Warnhinweis

	Die Authentifizierung über Windows ermöglicht keinen Zugriff auf „gesicherte" Datenbanken, also solche mit aktivierter Hochsicherheit und Verschlüsselung. Auf solche Datenbanken können ausschließlich entsprechend berechtigte Benutzer der internen PROXESS-Benutzerverwaltung zugreifen.

2. Benutzer mit PROXESS-Authentifizierung

Mitglieder dieser Kategorie können auf Hochsicherheitsdatenbanken (z. B. eine Personaldatenbank) zugreifen, wenn Sie mit den erforderlichen Zugriffsrechten in PROXESS ausgestattet sind. In der Praxis betrifft dies wahrscheinlich einen kleineren Kreis von Benutzern (z. B. Geschäftsleitung/ Personalabteilung). Diese Benutzer werden direkt in PROXESS angelegt und verwaltet. Bei der Anmeldung an PROXESS wählt der Anwender die Authentifizierungsoption "PROXESS" und gibt seinen PROXESS-Benutzernamen und sein Kennwort ein.

Alle Erläuterungen zur internen PROXESS-Gruppen und -Benutzerverwaltung finden Sie im Kapitel "Benutzerverwaltung".

Warnhinweis

Vermeiden Sie Benutzer mit "doppelter Identität" als Windows-AD-Benutzer und als PROXESS-Benutzer. Anwender sollten sich grundsätzlich an allen PROXESS-Modulen mit ein- und derselben Authentifizierung anmelden, um so für sich selbst eine einheitliche Daten- und Zugriffsbasis zu gewährleisten.

Siehe auch:

Zugriffsrechte - Konzept und Überblick

Angemeldete Benutzer

Wählen Sie unter dem Knotenpunkt "Benutzer" den Zweig "Angemeldete Benutzer".

Im mittleren Teilfenster sehen Sie nun die Liste aller aktuell angemeldeten Benutzer. Diese Liste können Sie sich auch als TXT-Datei exportieren lassen.

Benutzer anlegen

Nutzen Sie diese Funktion nur dann, wenn Sie Benutzer der Benutzerkategorie "PROXESS-Authentifizierung" anlegen möchten (siehe auch Aufgaben der Benutzerverwaltung). Für die Anlage von Benutzern der Kategorie "Windows-Authentifizierung" folgen Sie bitte den Anweisungen des Kapitels Windows Active Directory Integration.

Das Anlegen von Benutzern wird durch einen Assistenten unterstützt, mit dem Sie beliebig viele Benutzer auf einmal anlegen und mit Eigenschaften versehen können.

1. Schritt: Benutzerdaten anlegen

- Verbinden Sie sich als Supervisor in der PROXESS Administrator Console mit Ihrem PROXESS System.
- Wählen Sie das Verzeichnis "Benutzer" aus.
- Wählen Sie den Befehl **Neuer Benutzer** im Aktionspanel rechts, im Menü "Aktion" oder über das Kontextmenü.
- Es öffnet sich der Benutzer-Assistent (siehe unten).
- Geben Sie die Benutzerdaten ein und bestätigen Sie Ihre Eingaben mit dem Befehl **Hinzufügen**.
- Der angelegte Benutzer erscheint nun im rechten Fensterbereich.
- Über das Kontextmenü rufen Sie den Dialog **Erweiterte Eigenschaften** des Benutzers auf.

Auf diese Weise können Sie weitere Benutzer hinzufügen.

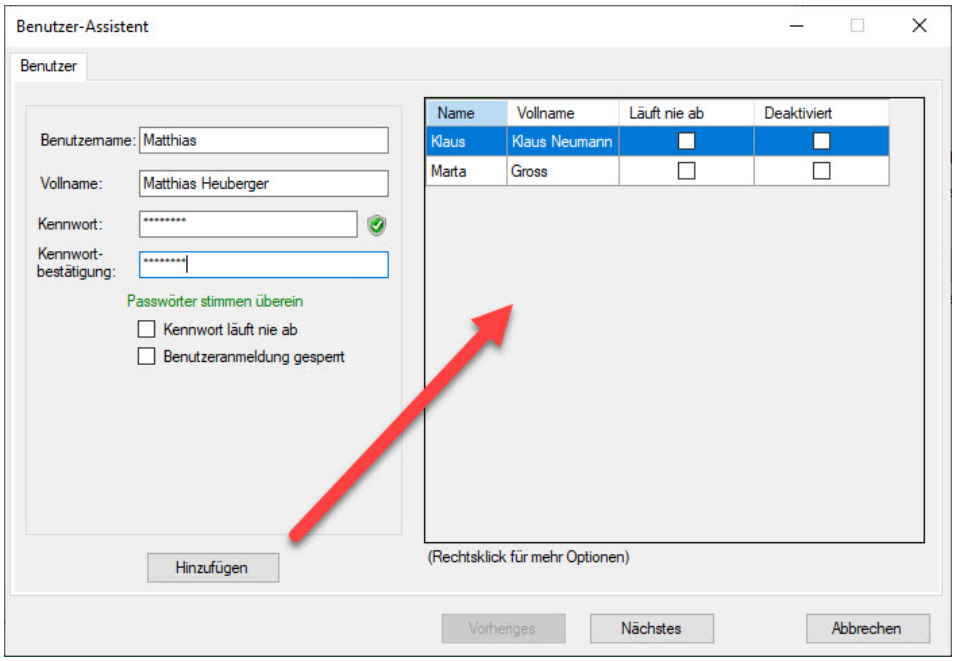


Abb: Dialogfeld zum Anlegen eines neuen Benutzerkontos

Erläuterungen zu den Benutzerdaten:

Benutzername	Hier geben Sie einen Kurznamen für den neuen Benutzer ein, z. B. ein in Ihrem Unternehmen übliches Kurzzeichen. Dies ist der Name, unter dem sich der neue Benutzer in PROXESS anmeldet.
Vollname	Hier geben Sie den vollen Namen des Benutzers ein. Das kann z. B. der Vor- und Zuname oder auch eine Funktionsbeschreibung sein. Der Vollname erscheint nach der Anmeldung in PROXESS in der Statuszeile.

Kennwort/ Kennwortbestätigung	Sie müssen dem neuen Benutzer ein Kennwort zuweisen. Es gelten folgende Kennwortregeln: - Das Kennwortfeld darf nicht leer sein. - Das Kennwort muss mindestens 8 Zeichen lang sein. - Das Kennwort darf nicht identisch sein mit dem Benutzernamen sein. - Das Kennwort muss mindestens eine Ziffer oder ein Sonderzeichen enthalten. Als Sonderzeichen gelten alle Zeichen außer a-z, A-Z und 0-9. - Das Kennwort muss mindestens einen Klein-und einen Großbuchstaben enthalten. Ein grünes Symbol neben dem Kennwortfeld signalisiert, dass alle Regeln erfüllt sind und das Kennwort damit gültig ist.
Kennwort läuft nicht ab	Aktivieren Sie das Kontrollkästchen, bleibt das Kennwort dieses Benutzers zeitlich unbeschränkt gültig. Bei deaktiviertem Kontrollkästchen ist die zeitliche Gültigkeit des Kennwortes beschränkt. Hier wird der Benutzer nach der ersten Anmeldung aufgefordert, sein Kennwort innerhalb der nächsten 14 Tage zu ändern. Tut er dies, gilt von da ab die im Programm "PROXESS Registry Setup" konfigurierte Gültigkeitsdauer des Kennwortes (s. u.). Achtung: Auch ein "leeres Kennwort" läuft ab, wenn dies im System aktiviert ist.
Benutzeranmeldung gesperrt	Ein Benutzerkonto kann - vorübergehend oder dauerhaft - gesperrt werden, So können Sie beispielsweise Systemarbeiten in Ruhe ausführen. Benutzer können nicht gelöscht werden, da Ihre Benutzerdaten mit archvierten Dokumenten verknüpft sein können. Daher können Sie Konten ausgeschiedener Mitarbeiter hier sperren. Sie können die Sperre eines Benutzerkontos jederzeit wieder aufheben.

Warnhinweis

	**Benutzerkonten können aus Sicherheitsgründen nicht gelöscht, sondern nur gesperrt werden.** Im Gegensatz zum endgültigen Löschen eines Benutzerkontos bleiben damit die die Benutzerinformationen in bestehenden Dokumenten nach dem Sperren weiterhin sichtbar.

Tipp

	Der Gültigkeit von Benutzerpasswörtern zeitlich begrenzt werden. Diese Systemfunktion muss zunächst im Programm "PROXESS Registry Setup" systemweit aktiviert werden. Unter dem Menüpunkt Document Manager/Benutzeranmeldung können Sie die relevanten Einstellungen im Optionsfeld **Maximales Kennwortalter** treffen. Nach der Installation ist standardmäßig die Option **Kennwort läuft nie ab** gesetzt. Das Setzen der Option **Kennwort läuft ab nach n Tagen** (n: Maximales Passwortalter in Tagen) aktiviert die Überprüfung des Kennwortablaufs. Welches Kennwort ein Benutzer aktuell verwendet, können Sie nicht sehen. Sie können aktuelle Kennwörter zurücksetzen, wenn ein Benutzer sein Kennwort vergessen hat. Ein Benutzer kann sein Kennwort darüberhinaus selbst ändern im PROXESS Standard Client und im PROXESS Web Client.

2. Schritt: Benutzer zu Gruppen hinzufügen

Sie haben die Möglichkeit einzelnen Benutzern eine oder mehrere Gruppe zuzuweisen oder eine Mehrfachzuweisung vorzunehmen.

1. Einzelzuweisung

Wählen Sie im untenstehenden Dialogfenster einen Benutzer aus. Der aktuell ausgewählte Benutzer wird immer im Infofeld unter "Aktuell ausgewählter Benutzer für Einzelzuordnung" angezeigt.

Markieren Sie in der rechten Spalte mit der Überschrift "Nicht Mitglied in" die gewünschte Gruppe, die Sie zuweisen möchten. Sie können auch mehrere Gruppen markieren und so gleichzeitig zuweisen.

Wählen Sie den Befehl **Zuweisen.** Die zugewiesene Gruppe(n) wird/werden nun in der mittleren Spalte "Mitlied in" angezeigt.

Ebenso können Sie einzelne Benutzer wieder aus einer oder mehreren Gruppen gleichzeitig entfernen.

2. Mehrfachzuweisung

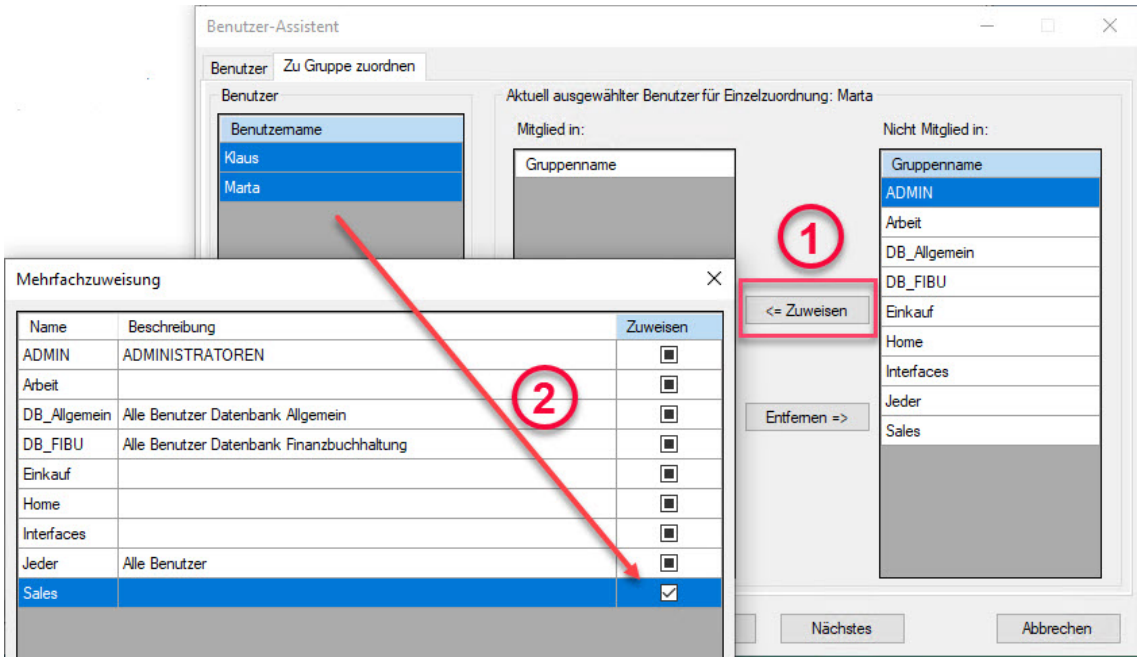
Wählen Sie mehrere Benutzer gleichzeitig aus.

Rufen Sie die Mehrfachzuweisung über die rechte Maustaste auf.

Es erscheint untenstehendes Dialogfenster "Mehrfachzuweisung".

Wählen Sie die gewünschten Gruppen und Zustände aus.

Bestätigen Sie Ihre Auswahl mit **OK**.

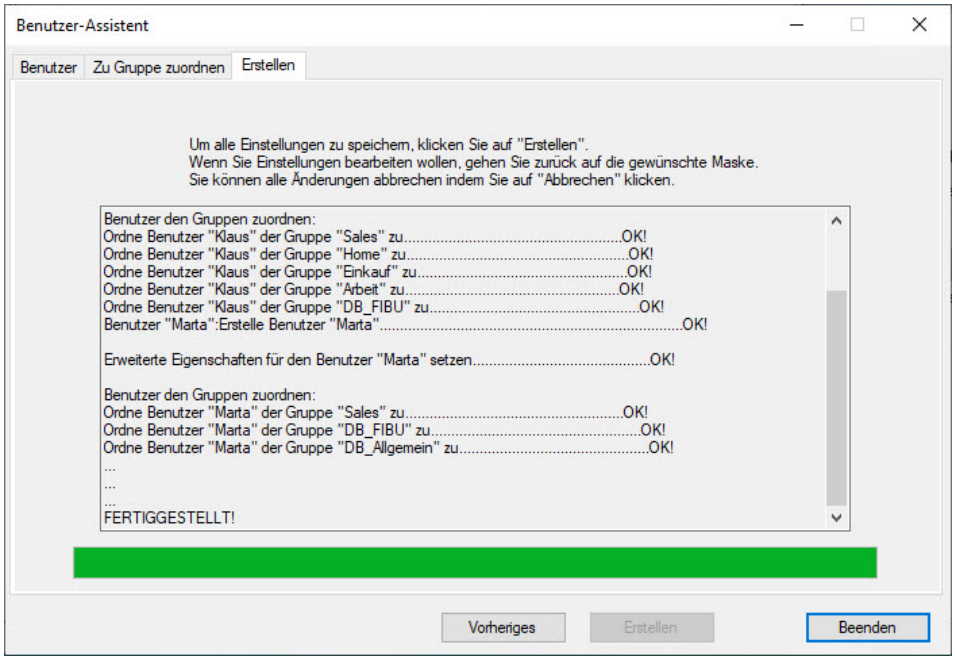


Für die Mehrfachzuweisung gibt es folgende Optionen:

Häkchen gesetzt	Die ausgewählten Benutzer werden zu dieser Gruppe hinzugefügt.
grünes bzw. schwarzes Kästchen	Die ausgewählten Benutzer werden der Gruppe nicht hinzugefügt. Sollte sie bereits Mitglied in dieser Gruppe sein, werden ihnen die Gruppenzugehörigkeit aber auch nicht entzogen. D.h. der aktuelle Zustand bleibt erhalten.
leeres Kästchen	Die ausgewählten Benutzer werden aus der Gruppe entfernt.

Sind alle Benutzer den Gruppen zugewiesen, klicken Sie auf den Button **Nächstes**.

Es erscheint ein Abschlussdialog. Bestätigen Sie hier Ihre Einstellungen mit dem Button **Erstellen**, um die neuen Benutzer tatsächlich anzulegen.



Sie erhalten ein Protokoll und eine Abschlussmeldung, dass alle Einstellungen erfolgreich gespeichert wurden.

Benutzereigenschaften verwalten

Verbinden Sie sich in der PROXESS Administrator Console mit Ihrem PROXESS System.

Markieren Sie das Verzeichnis "Benutzer" und wählen Sie den gewünschten Benutzer aus. Per Doppelklick öffnen Sie den Eigenschaften-Dialog. Alternativ wählen Sie im Aktionspanel rechts oder über das Menü "Aktion" oder über das Kontextmenü den Befehl **Eigenschaften**.

Es erscheint folgendes Dialogfenster:

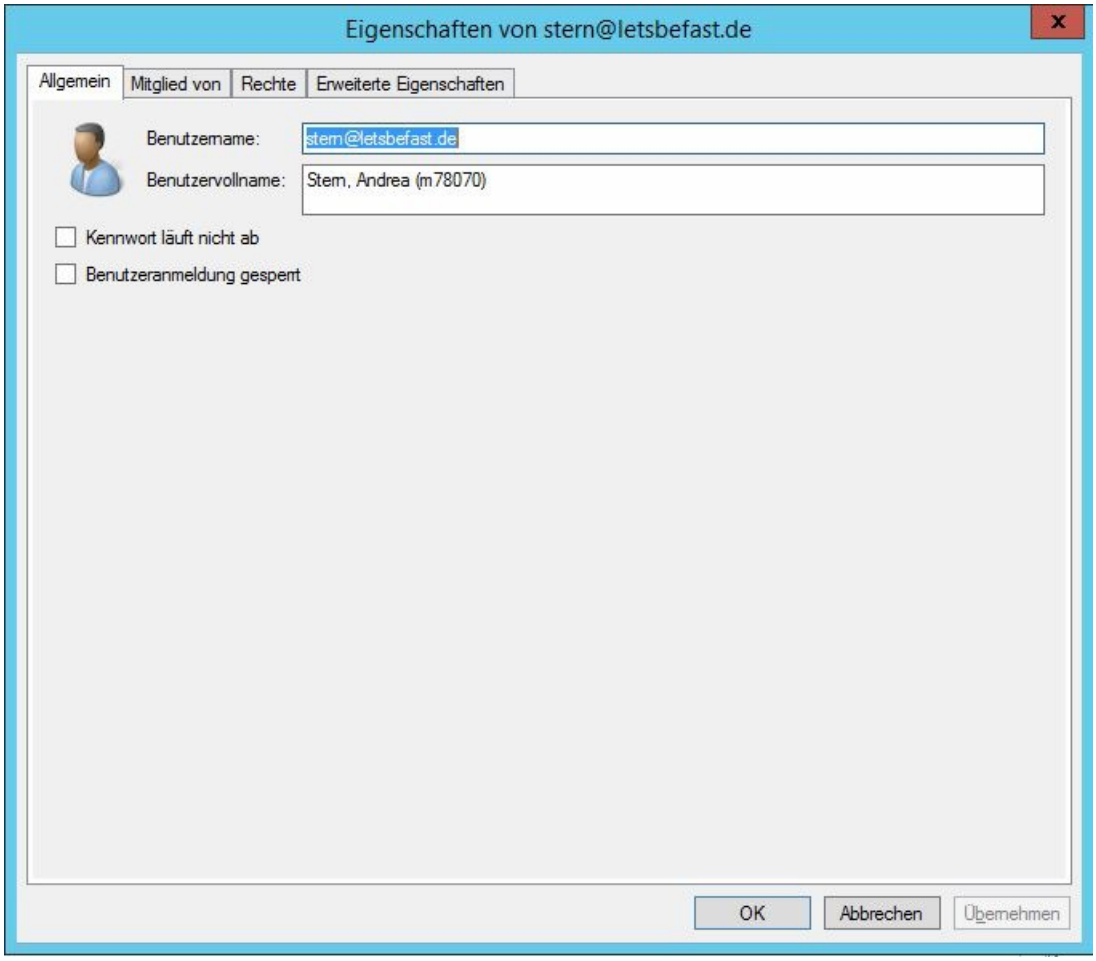


Abb: Allgemeine Benutzereigenschaften der Benutzerin "Andrea Stern".

Allgemeine Eigenschaften

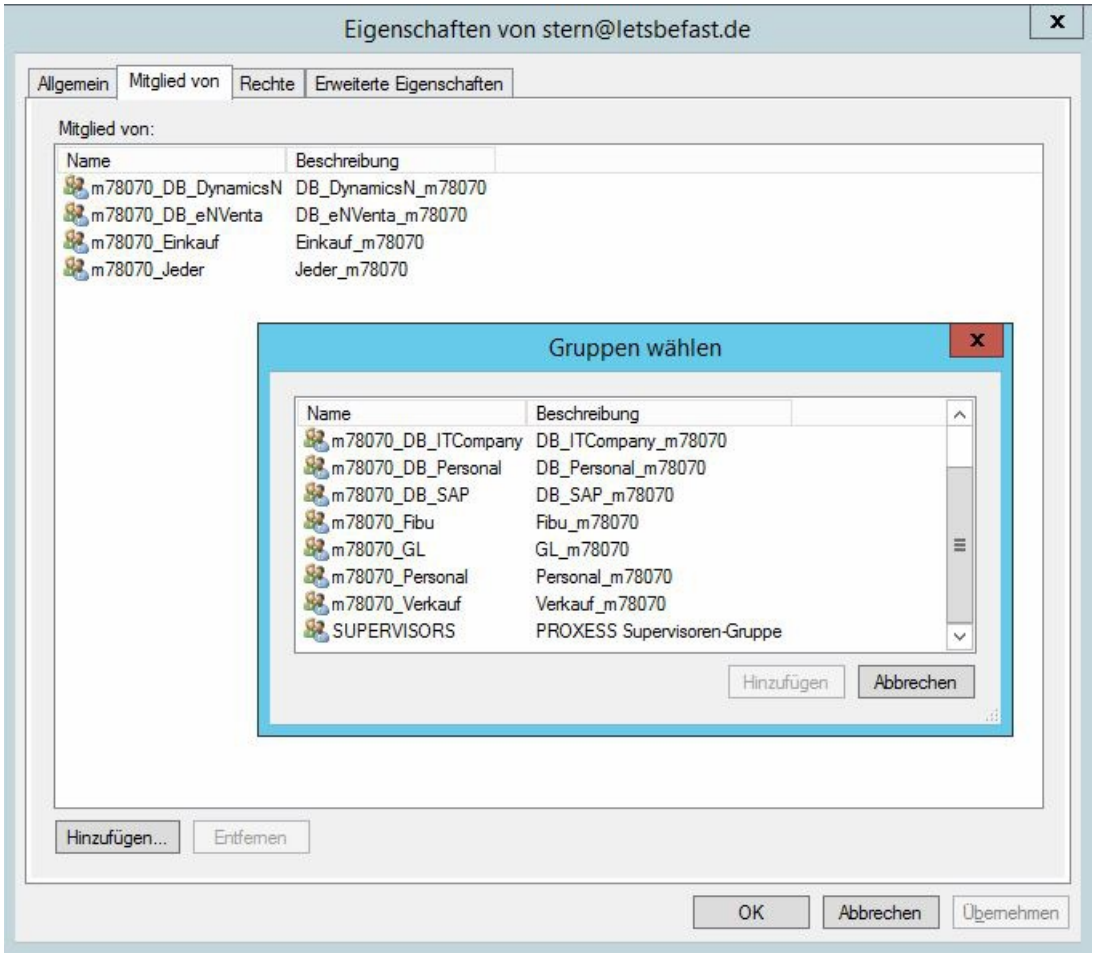
Unter die **Allgemeinen Eigenschaften** eines Benutzers fallen der Kurz- und Vollname, zeitlicher Ablauf des Kennwortes, sowie die Sperrung/Entsperrung des Benutzerkontos. Diese Eigenschaften können Sie bei Bedarf ändern. Für Benutzer der Benutzerkategorie "Windows-Authentifizierung" sind die Felder Benutzername und Benutzervollname allerdings deaktiviert. Eine Änderung dieser Eigenschaften ist nur über das Windows Active Directory möglich. Dort vorgenommene Änderungen werden in die PROXESS-Benutzer-Eigenschaften automatisch übernommen.

Warnhinweis

	Benutzer können nicht gelöscht, sondern nur gesperrt werden. Damit wird gewährleistet, dass benutzerbezogene Protokollierungen im System (z. B. bei der Anlage oder Bearbeitung von Dokumenten) nicht verlorengehen. Über eine Filterfunktion können Sie gesperrte Benutzer ausblenden und sich damit nur aktive Benutzer anzeigen lassen.

Gruppenzugehörigkeit eines Benutzers

Unter dem Reiter "**Mitglied von**" definieren Sie die Gruppenzugehörigkeit des Benutzers. Ein Benutzer kann Mitglied keiner Gruppe, einer oder mehrerer Gruppen sein:



Benutzerrechte

Unter dem Reiter "**Rechte**" werden alle Zugriffs- und Aktionsrechte des Benutzers der verbundenen Archivdatenbank angezeigt. Voraussetzung hierfür ist natürlich, dass Sie sich zuvor mit einer Datenbank verbunden haben. Die Verwaltung der Zugriffsrechte wird im Kapitel "Zugriffsrechte" erläutert.

Tipp

	In der Praxis hat es sich bewährt Rechte auf Gruppenebene zu vergeben und die Benutzer entsprechend den Gruppen zuzuweisen. Ist ein Benutzer Mitglied einer Gruppe, so erhält er auch die entsprechenden Rechte. Daher sollte sich die Zuweisung von Mitgliedern zu Gruppen danach orientieren, welche Rechte ein Benutzer erhalten soll.

Erweiterte Eigenschaften

Unter dem Reiter "**Erweiterte Einstellungen**" werden sämtliche Kontakt- und Adressdaten eines Benutzers in PROXESS verwaltet. Diese Werte können zum Beispiel für die Konfiguration von **Externen Thesauren** herangezogen

werden.

Die Eigenschaften des jeweiligen Benutzers können Sie hier vorbelegen. Die unter der AD-Benutzerverwaltung eingegebene Eigenschaften werden hier automatisch übernommen. Unter **Anzeigename** tragen Sie den Namen ein, der beim Versenden von E-Mails durch den Benutzer angezeigt werden soll. Unter **E-Mail-Adresse** tragen Sie die gültige E-Mailadresse des Benutzers ein. Die dazugehörigen SMTP-Einstellungen werden automatisch vom System eingetragen.

Siehe auch:

Zugriffsrechte - Konzept und Überblick

Datenbankrechte verwalten

Dokumenttyprechte verwalten

PROXESS-Kennwort ändern

Die Festlegung oder Änderung von Kennwörtern ist hier nur für Benutzer der Authentifizierungskategorie "PROXESS" möglich. Für "Windows-Active-Directory-Benutzer" können Benutzereigenschaften wie Benutzername und Kennwort ausschließlich über das Windows-Active-Directory vorgenommen werden. Diese Änderungen werden danach automatisch in PROXESS übernommen.

Verbinden Sie sich als Supervisor oder Datenbank-Bereichsadministrator in der PROXESS Administrator Console mit Ihrem PROXESS System.

Markieren Sie das Verzeichnis "Benutzer" und wählen Sie den gewünschten Benutzer aus.

Wählen Sie im Aktionspanel rechts oder im Menü "Aktion" oder über das Kontextmenü den Befehl **Kennwort festlegen**.

Es erscheint folgendes Dialogfenster:

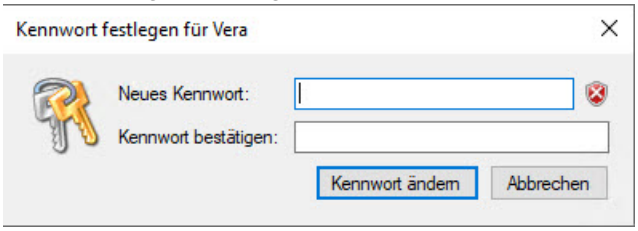


Abb.: Kennwort festlegen oder ändern für einen PROXESS-Benutzer

Hier können Sie ein neues Kennwort vergeben.

Es gelten folgende Regeln bei der Vergabe eines Kennwortes:
- Das Kennwortfeld darf nicht leer sein.
- Das Kennwort muss mindestens 8 Zeichen lang sein.
- Das Kennwort darf nicht identisch mit dem Benutzernamen sein.
- Das Kennwort muss mindestens eine Ziffer oder ein Sonderzeichen enthalten. Als Sonderzeichen gelten alle Zeichen außer a-z, A-Z und 0-9.
- Das Kennwort muss mindestens einen Klein-und einen Großbuchstaben enthalten.

Ein grünes Symbol neben dem Kennwortfeld signalisiert, dass alle Regeln erfüllt sind und das Kennwort damit gültig ist.

Tipp

	Jeder Benutzer sollte aus Sicherheitsgründen nach seiner ersten Anmeldung mit einem neu gesetzten Kennwort dieses wieder in ein individuelles Kennwort ändern. Die Kennwortänderung durch den Benutzer wird im Programm PROXESS vorgenommen.

Siehe auch:
Benutzer verwalten (Kennwort läuft nie ab)

Windows Active Directory Integration

Benutzerkonzept: AD-Benutzer versus PROXESS-Benutzer

Als Systemadministrator sollten Sie alle Anwender, die mit PROXESS arbeiten, organisatorisch in zwei Benutzerkategorien unterteilen.

1. Benutzer mit Windows-Authentifizierung
Für diese Anwender übernimmt der Systemadministrator die Benutzerdaten des Windows Active Directory und vermeidet hierdurch eine doppelte Administration in Windows und PROXESS. Übernommene AD-Benutzer wählen bei der Anmeldung an PROXESS die Authentifizierungsoption "Windows" im Anmeldedialog des jeweiligen Moduls. Damit werden die Windowsanmeldedaten automatisch an PROXESS übergeben. Empfehlenswert ist es dabei, in den jeweiligen Moduleinstellungen den Anmeldedialog für AD-Benutzer nach der ersten Anmeldung zu unterdrücken.

Jedoch haben Mitglieder dieser Kategorie keinen Zugriff auf Hochsicherheitsdatenbanken, also solche mit aktivierter Hochsicherheit und Verschlüsselung. Damit soll verhindert werden, dass AD-Benutzer durch eine einfache Zuordnung in eine AD-Gruppe auf Windows-Ebene automatisch auch Zugriffsrechte auf besonders schützenswerte Dokumente und Daten in PROXESS erhalten, ohne dass diese explizit in PROXESS bekanntgegeben werden müssen. In der Praxis trifft dies wahrscheinlich die Mehrheit der Anwender, die z. B. nicht Mitglied der Geschäftsleitung oder des Personalbereichs sind und so auch keinen Zugriff auf besonders geschützte Daten benötigen. Für diese Benutzer kann durch die Windows Active Directory Integration eine doppelte Administration vermieden werden und damit eine Arbeitserleichterung für den Systemadministrator erreicht werden. Außerdem automatisiert sich für den Anwender die Anmeldung an den PROXESS-Modulen.

Alle Schritte zur Windows Active Directory Integration in PROXESS sind in diesem Kapitel beschrieben.

Warnhinweis

	**Die Authentifizierung über Windows ermöglicht keinen Zugriff auf „gesicherte" Datenbanken, also solche mit aktivierter Hochsicherheit und Verschlüsselung. Auf solche Datenbanken können ausschließlich entsprechend berechtigte Benutzer der internen PROXESS-Benutzerverwaltung zugreifen.**

2. Benutzer mit PROXESS-Authentifizierung
Mitglieder dieser Kategorie können auf Hochsicherheitsdatenbanken (z. B. eine Personaldatenbank) zugreifen, wenn Sie mit den erforderlichen Zugriffsrechten in PROXESS ausgestattet sind. In der Praxis betrifft dies wahrscheinlich einen kleineren Kreis von Benutzern (z. B. Geschäftsleitung/ Personalabteilung). Diese Benutzer werden direkt in PROXESS angelegt und verwaltet. Bei der Anmeldung an PROXESS wählt der Anwender die Authentifizierungsoption "PROXESS" und gibt seinen PROXESS-Benutzernamen und sein Kennwort ein.

Alle Erläuterungen zur internen PROXESS-Gruppen und -Benutzerverwaltung finden Sie im Kapitel "Benutzerverwaltung".

Warnhinweis

	**Vermeiden Sie Benutzer mit "doppelter Identität" als Windows-AD-Benutzer und als PROXESS-Benutzer. Anwender sollten sich grundsätzlich an allen PROXESS-Modulen mit ein- und derselben Authentifizierung anmelden, um so für sich selbst eine einheitliche Daten- und Zugriffsbasis zu gewährleisten.**

Bitte lesen Sie unbedingt zuerst die Ausführungen im vorhergehenden Kapitel: Benutzerverwaltung - Konzept und Überblick.

Schritt für Schritt: Windows Active Directoy-Integration

1. Schritt: Windows-Authentifizierungsgruppe anlegen

Erstellen Sie eine Windows-Authentifizierungsgruppe für PROXESS in der Verwaltung des Windows Active Directory. Der Name hierfür ist frei wählbar. Wählen Sie z. B. den Gruppennamen "PROXESS" oder wie im unten aufgezeigten Beispiel auch einen anderen Namen. In dieser Gruppe werden alle Windows-Benutzer gesammelt, die mit PROXESS arbeiten sollen. **Fügen Sie daher zu dieser Gruppe alle Windows-Benutzer hinzu, die mit PROXESS arbeiten und sich in PROXESS über die automatische Windows-Authentifizierung anmelden sollen.** Am besten arbeiten Sie auf Gruppenebene und fügen alle Windows-Gruppen hinzu, die mit PROXESS arbeiten sollen. Alle Mitglieder einer solchen Gruppe werden so automatisch zur Authentifizierungsgruppe hinzugefügt. Die Verwaltung über Gruppen erleichtert Ihnen auch die spätere Administration und Pflege des Systems. Neu hinzukommende Benutzer werden dann über ihre Windows-Gruppenzugehörigkeit automatisch auch Mitglied der Authentifizierungsgruppe für PROXESS. Eine Windows-Gruppenhierarchie wird in PROXESS dabei nicht übernommen. Es werden Benutzer der Gruppen und Untergruppen gleichstufig übernommen.

Beispiel:
Basierend auf dem PROXESS-Demosystem "Let´s be fast" (LBF) wird hier ein Beispiel mit fiktiven Windowsgruppen beschrieben.

Als erstes legen Sie in der Verwaltung des Windows Active Directory eine Windows-Gruppe mit dem Namen "LBF Jeder" an. Diese soll in unserem Beispiel als Windows-Authentifizierungsgruppe für PROXESS dienen.

Im nächsten Schritt fügen Sie dort die Windows-Gruppen "LBF Verkauf", "LBF Einkauf", "LBF Finanzbuchhaltung", "LBF Geschäftsleitung" zur neu erstellten Gruppe "LBF Jeder" hinzu. Nun haben sie alle Benutzer für die spätere AD-Integration in die zentrale Authentifzierungsgruppe für das PROXESS-System übernommen.

Warnhinweis

	**Die Mitgliedschaft eines Windows-Benutzers in der Authentifizierungsgruppe ist eine unbedingte notwendige Voraussetzung für die spätere Vergabe von PROXESS-Zugriffsrechten für diesen Benutzer.**

2. Schritt: Windows-Authentizierung in PROXESS aktivieren

Öffnen Sie nun das Programm **PROXESS Registry Setup** aus der Programmgruppe PROXESS und wählen Sie diese neue Gruppe im Menü Document Manager/Benutzeranmeldung unter dem Eintrag "Authentifzierungsgruppe" aus. Vorab müssen Sie dafür die Option "Windowsdomäne" im Abschnitt "Externes Benutzersystem" aktivieren. (siehe auch Dokumentation zum PROXESS Registry Setup)

Abb.: Einstellungen zum Externen Benutzersystem im PROXESS Registry Setup

Beispiel: Wählen Sie die in Schritt 1 angelegte Gruppe "LBF Jeder" als Authentifizierungsgruppe aus.

Warnhinweis

Greifen Sie für die PROXESS Authentifizierungsgruppe auf keinen Fall auf bestehende interne Windows-Benutzergruppen, wie z. B. "Jeder" zurück. Da PROXESS regelmäßig die Benutzergruppen synchronisiert, führt dies bei einer größeren Anzahl von Benutzerkonten zu Performance-Problemen.

Um dies zu vermeiden, legen Sie, wie unter Punkt 1 beschrieben, auf jeden Fall eine PROXESS-Gruppe an, die Sie dann im obenstehenden Dialog als Authentifizierungsgruppe auswählen.

3. Schritt: Windows-Gruppen registrieren und Benutzer in PROXESS übernehmen

Verbinden Sie sich jetzt wieder in der PROXESS Administrator Console mit dem gewünschten PROXESS-System und wählen Sie den Knotenpunkt "Gruppen". Wählen Sie im Menü "Aktion" den Menüpunkt **Windows-Gruppe registrieren.**

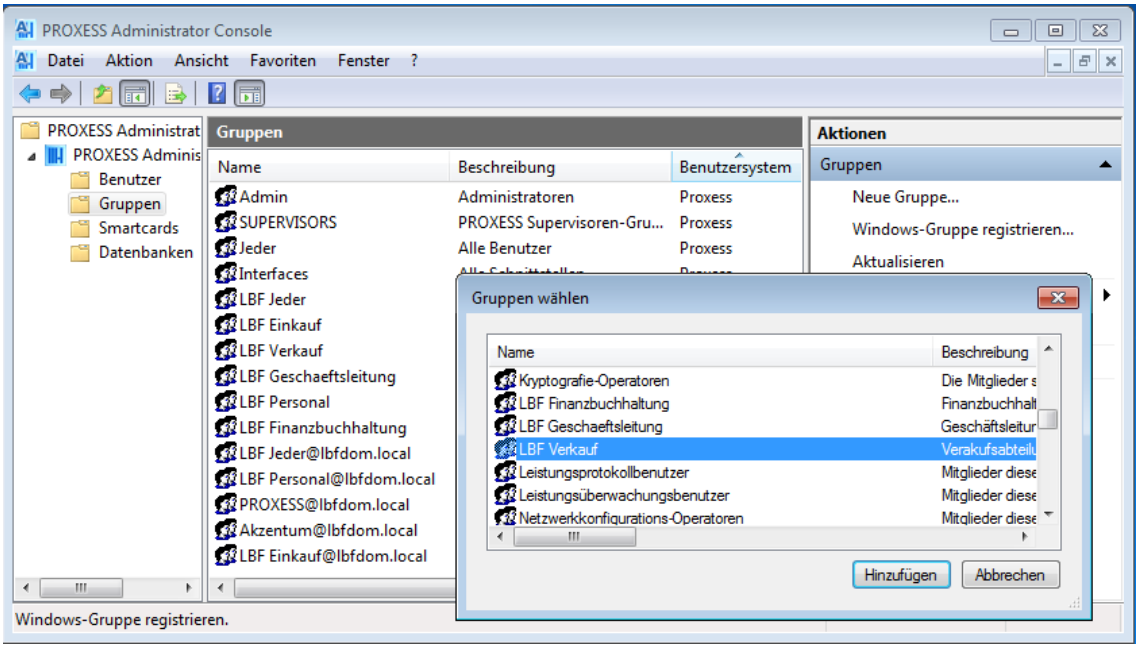


Abb.: Registrierung einer Windows AD-Gruppe in PROXESS

Wählen Sie nun all die Windows-Gruppen hinzu, die mit PROXESS arbeiten sollen. Durch die Registrierung der ersten Windows-Gruppe werden alle Benutzerdaten dieser Gruppenmitglieder in die PROXESS- Benutzerliste übernommen. Mit der ersten Registrierung einer Windows-Gruppe wird automatisch auch die zentrale Windows-Authentifizierungsgruppe und deren Mitglieder mit in die Benutzerverwaltung der PROXESS Administrator Console übernommen. Übernommene Windows-Benutzer und Windows-Gruppen werden in der Übersicht in der Spalte "Benutzersystem" mit dem Eintrag "Windows" gekennzeichnet.

Beispiel:
Wählen Sie die Windows-Gruppen "LBF Verkauf", "LBF Einkauf", "LBF Finanzbuchhaltung", "LBF Geschäftsleitung" zur Registrierung in PROXESS aus. Die Gruppe "LBF Jeder" wird automatisch mit übernommen. Nun übernimmt das PROXESS-System automatisch alle Anmeldedaten der Gruppenmitglieder. Dieses können Sie in der PROXESS-Benutzerübersicht überprüfen.

4. Schritt: PROXESS Rechte vergeben

Vergeben Sie den registrierten Windows-Gruppen nun die gewünschten PROXESS-Zugriffsrechte. (siehe Kapitel:

Zugriffsrechte)

Warnhinweis

	**Eine Vergabe von Rechten ist nur für Mitglieder der angesprochenen Gruppe gültig, die auch Mitglied der oben genannten Windows-Authentifizierungsgruppe sind (siehe oben).**

5. Schritt: Einen neuen Windows-Benutzer hinzufügen

Sind die oben genannten Schritte 1- 4 wie im Beispiel beschrieben ausgeführt, so wird ein neuer Windows-Benutzer über seine Gruppenzugehörigkeit automatisch in die PROXESS Benutzerverwaltung übernommen. Durch die Zuordnung zu einer Windows-Gruppe erhält er auch automatisch die für seine Windows-Gruppe vorgesehenen PROXESS-Zugriffsrechte. Voraussetzung ist dabei wieder, dass seine Windows-Gruppe Teil der Windows-Authentifizierungsgruppe ist.

Fazit: Eine gesonderte Benutzer- und Rechteverwaltung für PROXESS ist damit nicht mehr notwendig.

Benutzer löschen

Benutzerkonten können aus Sicherheitsgründen in PROXESS nicht gelöscht, sondern nur gesperrt werden.

Im Gegensatz zum endgültigen Löschen eines Benutzerkontos bleiben damit die die Benutzerinformationen in bestehenden Dokumenten nach dem Sperren weiterhin sichtbar.

Benutzerliste exportieren

Die jeweils ausgewiesene Benutzerliste können Sie sich über den Befehl **Liste exportieren** im Kontextmenü des Benutzerknotens als TXT-Datei exportieren lassen (siehe auch: Gesperrte und Aktive Benutzer filtern und anzeigen)

Gesperrte bzw. aktive Benutzer filtern und anzeigen

Um sich eine Übersicht über Ihre aktiven und gesperrten Benutzer zu verschaffen, können Sie alle Benutzer über diese Eigenschaften filtern.

Markieren Sie hierzu das Verzeichnis "Benutzer". Wählen Sie nun im Aktionspanel rechts oder über das Menü "Aktion" oder über das Kontextmenü den Befehl **Filter...**

Es erscheint folgender Dialog:

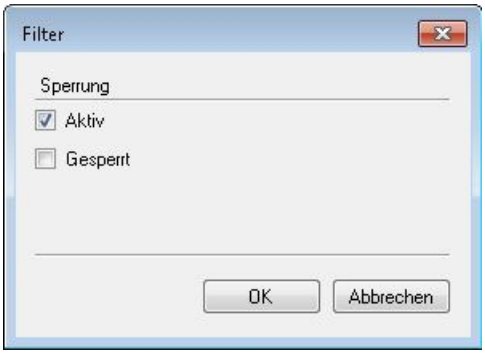


Abb.: Benutzer nach aktiv/gesperrt filtern

Standardmäßig werden alle Benutzer in der Benutzerliste rechts ausgewiesen. Möchten Sie z. B. nur aktive Benutzer in der Benutzerliste sehen, so setzen Sie das Häkchen, wie oben abgebildet, bei Aktiv.

Die jeweils ausgewiesene Liste können Sie sich über den Befehl **Liste exportieren** im Kontextmenü des Benutzerknotens als TXT-Datei exportieren lassen.

Gruppen Funktionsüberblick

Markieren Sie in der Benutzerverwaltung das Verzeichnis "Gruppen" und öffnen Sie das Kontextmenü:

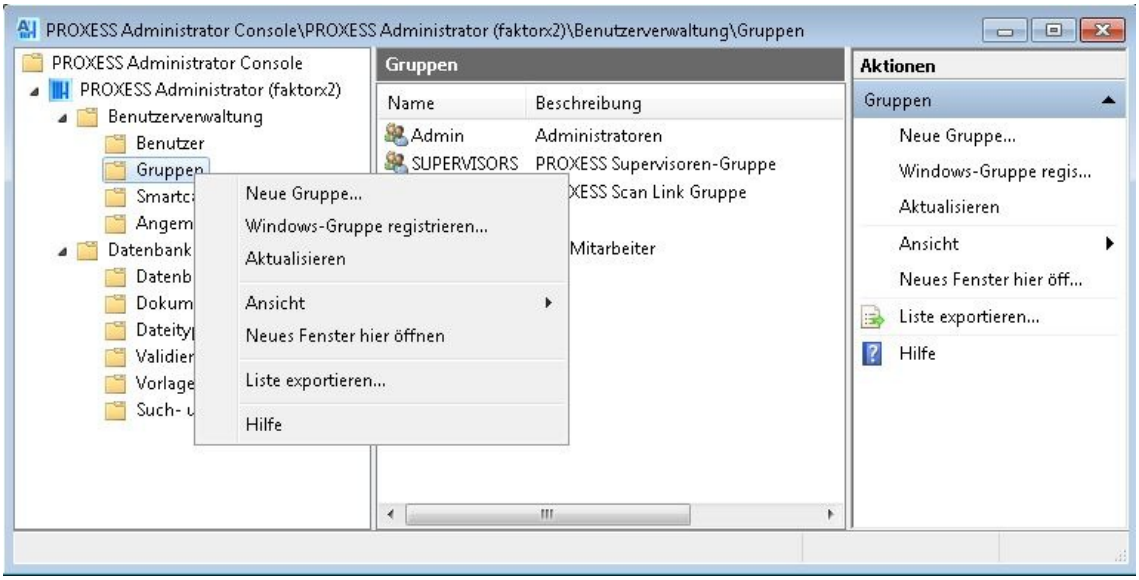


Abb.: Funktionsübersicht zur Gruppenverwaltung

Neue Gruppe...	erstellt eine neue Benutzergruppe
Windows-Gruppe registrieren	öffnet die Windows-Benutzerverwaltung zur Übernahme von bestehenden Windows-Benutzergruppen und deren Mitgliedern in die PROXESS Administrator Console
Aktualisieren	aktualisiert die aktuelle Ansicht
Ansicht	enthält Befehle zum Anpassen der aktuellen Fensteransicht (z. B. zur Spaltendarstellung)
Neues Fenster hier öffnen	öffnet ausgehend von diesem Knotenpunkt ein neues Fenster. Dieser Befehl kann der besseren Übersicht bei umfangreichen Anpassungen dienen. Arbeiten Sie parallel in mehreren Fenstern, so ist der Befehl **Aktualisieren** nützlich.
Liste exportieren...	Die jeweils ausgewiesene Liste des mittleren Fensterbereichs können Sie sich über den Befehl **Liste exportieren** im Kontextmenü als TXT-Datei exportieren lassen. Z. B. können Sie so eine Liste aller Benutzer, aller angemeldeten Benutzer oder eine Datenbankliste exportieren.
Hilfe	öffnet die Online-Hilfe

Gruppe anlegen

Gruppen fassen Benutzer zusammen, die dieselben Rechte erhalten sollen. So müssen Sie nicht jedem Benutzer einzeln Rechte zuweisen. Dies können Sie auf Gruppenbasis erledigen. Ob Sie mit Gruppen oder mit Einzelbenutzern arbeiten, hängt von der Anzahl der PROXESS-Benutzer in Ihrem Unternehmen und von den Vorgaben der Organisationsanalyse ab.

1. Schritt: Gruppen anlegen

Markieren Sie das Verzeichnis "Gruppen" und wählen Sie im Aktionspanel rechts oder im Menü "Aktion" oder über das Kontextmenü den Befehl **Neue Gruppe**.

Geben Sie einen Gruppennamen und eine Beschreibung für Ihre neue Gruppe an.

Bestätigen Sie Ihre Eingaben mit dem Befehl **Hinzufügen**. Die neue Gruppe wird nun im rechten Fensterbereich angezeigt.

Über das Kontextmenü eines markierten Benutzers können Sie diesen wieder aus der Liste entfernen.

Auf diesem Weg können Sie mehrere Gruppen gleichzeitig anlegen.

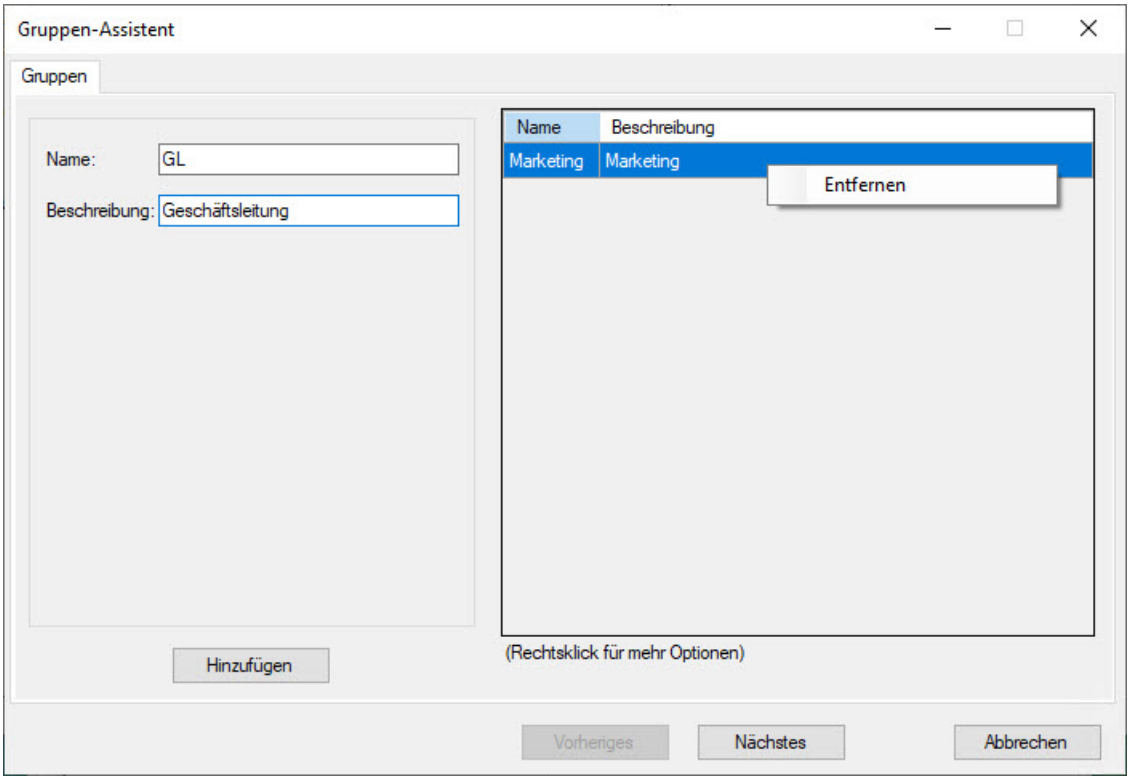


Abb: Gruppen anlegen

2. Schritt: Benutzer zur Gruppe hinzufügen

Sie haben die Möglichkeit einzelnen Gruppen eine oder mehrere Benutzer zuzuweisen oder eine Mehrfachzuweisung vorzunehmen.

1. Einzelzuweisung

Wählen Sie im untenstehenden Dialogfenster eine Gruppe aus. Die aktuell ausgewählte Gruppe wird immer im Infofeld unter "Aktuell ausgewählte Gruppe für Einzelzuordnung" angezeigt.

Markieren Sie in der rechten Spalte mit der Überschrift "Nicht Mitglied in" die gewünschten Benutzer, die Sie

zuweisen möchten. Sie können auch mehrere Benutzer markieren und so gleichzeitig zuweisen.

Wählen Sie den Befehl **Zuweisen.** Der/Die zugewiesene Benutzer wird/werden nun in der mittleren Spalte "Mitglieder" angezeigt.

Ebenso können Sie Benutzer wieder aus einer Gruppe entfernen.

2. Mehrfachzuweisung

Wählen Sie mehrere Gruppen gleichzeitig aus.

Rufen Sie die Mehrfachzuweisung über die rechte Maustaste auf.

Es erscheint untenstehendes Dialogfenster "Mehrfachzuweisung".

Wählen Sie die gewünschten Benutzer und Zustände aus.

Bestätigen Sie Ihre Auswahl mit **OK**.

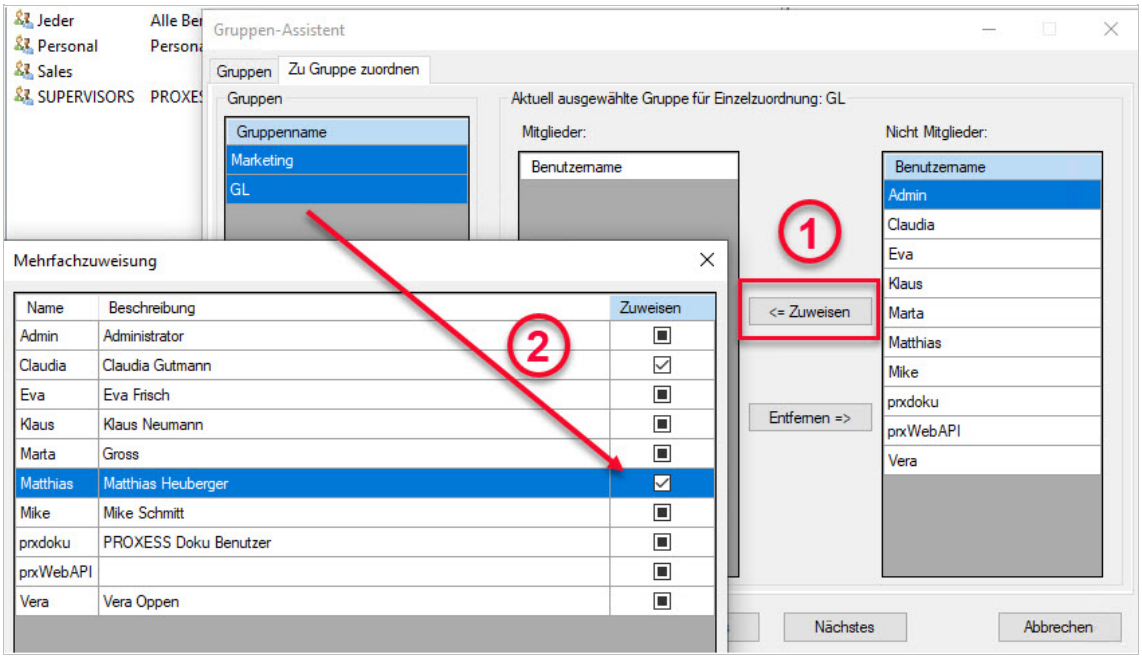


Abb.: Benutzer zu einer oder zu mehreren Gruppen zuweisen

Es gibt folgende Zuweisungsoptionen:

Häkchen gesetzt	Die ausgewählten Benutzer werden zu diesen Gruppen hinzugefügt.
grünes bzw. schwarzes Kästchen	Die ausgewählten Benutzer werden der Gruppe nicht hinzugefügt. Sollten sie bereits Mitglied in dieser Gruppe sein, werden ihnen die Gruppenzugehörigkeit aber auch nicht entzogen. D.h. der aktuelle Zustand bleibt erhalten.
leeres Kästchen	Die ausgewählten Benutzer werden aus der Gruppe entfernt.

3. Schritt: Datenbankrechte zuweisen

Auch hier können Sie einzelnen Gruppen (1) Zugriffsrechte auf die Datenbanken erteilen oder eine Mehrfachzuweisung (2) wie oben vornehmen.

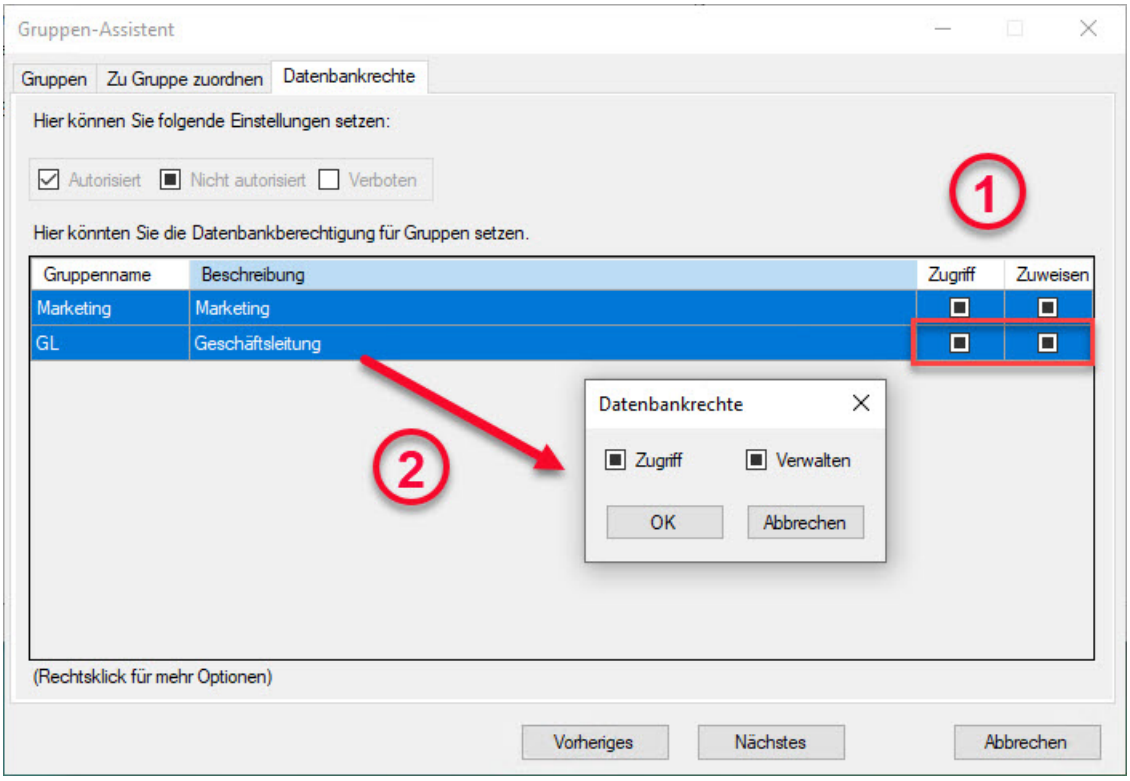


Abb: Einer oder mehreren Gruppen Datenbankrechte zuweisen

4. Schritt: Dokumenttyprechte zuweisen

Im letzten Schritt werden den neu angelegten Gruppen die Dokumenttyprechte zugewiesen.

Auch hier besteht die Möglichkeit nur einen einzelnen Dokumentyp zu markieren und die Rechte auf Gruppenebene zuzuweisen.
Markieren Sie mehrere Gruppen gleichzeitig, haben Sie die Möglichkeit, über das Kontextmenü allen markierten Gruppen gleichzeitig Rechte am Dokumenttyp zuzuweisen.

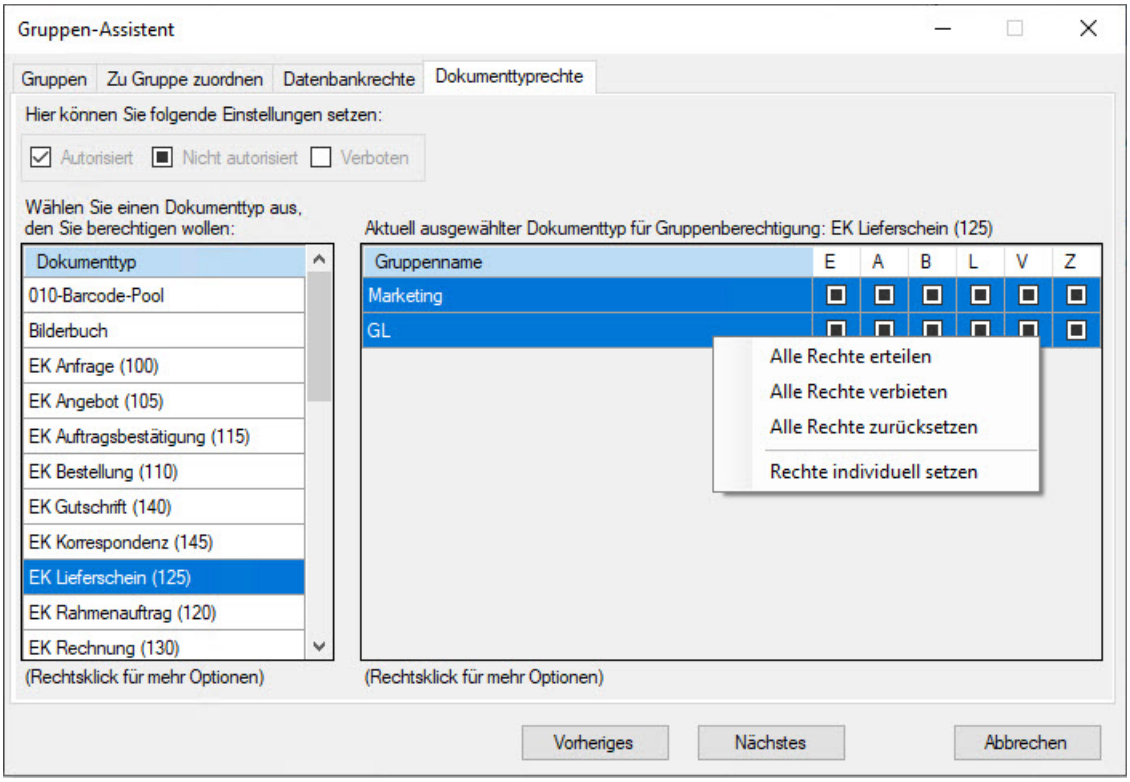


Abb.: Rechte für einen einzelnen Dokumenttyp setzen

Für eine Mehrfachzuweisung markieren Sie mehrere Dokumenttypen.

Wählen Sie dann über das Kontextmenü den Befehl **Mehrfachzuweisung** aus.

Es erscheint der Dialog: Mehrfachzuweisung für Dokumenttyprechte.

Nun setzen Sie im rechten Fensterbereich die Rechte, die für alle ausgewählten Dokumenttypen gleichzeitig gelten sollen.

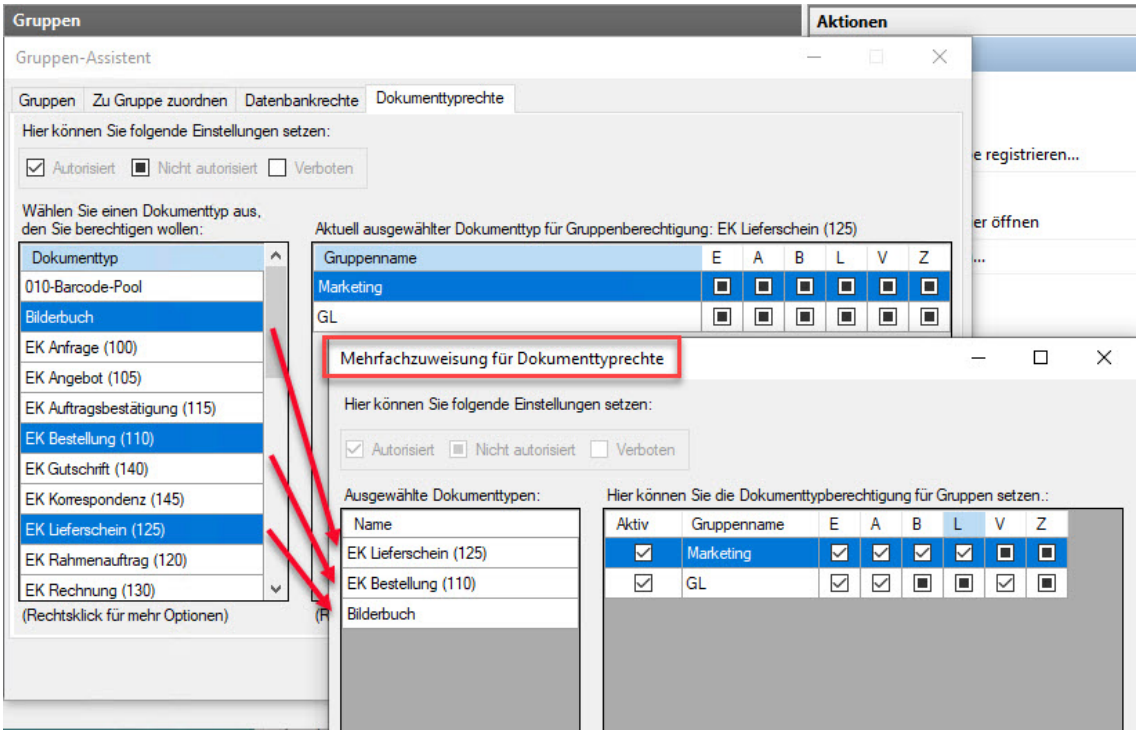


Abb.: Mehrfachzuweisung für Dokumenttyprechte</

PROXESS-Gruppe verwalten

Für Gruppen der Kategorie "Windows-Authentifizierung" können hier keine Benutzer hinzugefügt oder gelöscht werden. Eine Änderung dieser Eigenschaften ist nur über das Windows Active Directory möglich. Dort vorgenommene Änderungen werden in die PROXESS-Gruppen-Eigenschaften automatisch übernommen.

Verbinden Sie sich als Supervisor in der PROXESS Administrator Console mit Ihrem PROXESS System.
Markieren Sie das Verzeichnis "Gruppen" und wählen Sie die gewünschte Gruppe aus. Wählen Sie im Menü "Aktion" den Befehl **Eigenschaften**.

Es erscheint folgendes Dialogfenster:

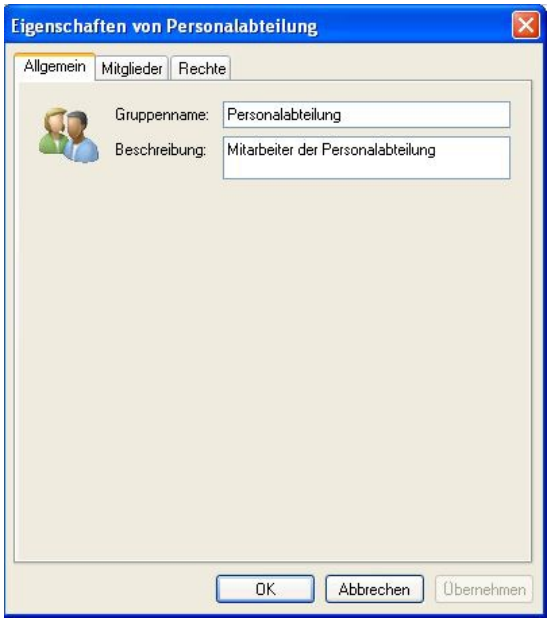


Abb.: Eigenschaften der Gruppe "Personalabteilung"

Unter die Allgemeinen Eigenschaften einer Gruppe fallen der Gruppenname und die Beschreibung. Diese Eigenschaften können Sie bei Bedarf jederzeit ändern. Durch die Änderung der beiden Einträge entsteht keine neue Gruppe. Für Gruppen der Kategorie "Windows-Authentifizierung" sind die Felder "Gruppenname" und "Beschreibung" deaktiviert. Eine Änderung dieser Eigenschaften ist nur über das Windows Active Directory möglich. Dort vorgenommene Änderungen werden in die PROXESS-Gruppen-Eigenschaften automatisch übernommen.

Unter dem Reiter "Mitglieder" definieren Sie die welche Benutzer Mitglied dieser Gruppe sind. Ein Benutzer kann dabei Mitglied in keiner Gruppe oder auch in mehreren Gruppen sein.

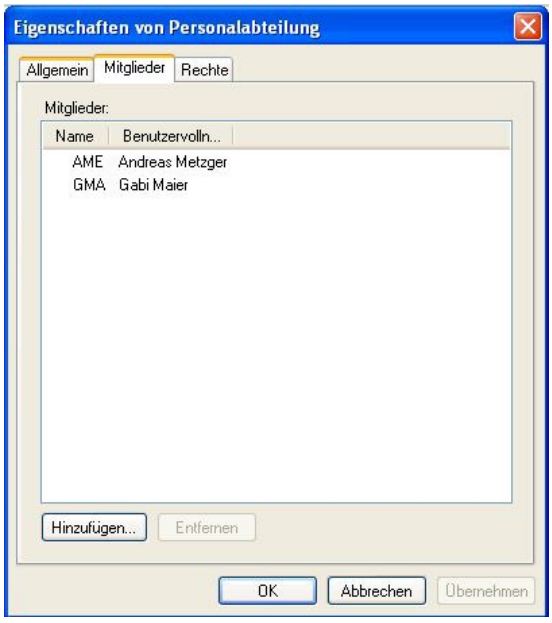


Abb.: Liste der Gruppenmitglieder

Über den Befehl **Hinzufügen** sehen Sie eine Liste aller Benutzer, die noch kein Mitglied dieser Gruppe sind und können diese entsprechend der Gruppe zuordnen.

Markieren Sie einen oder mehrere Benutzer gleichzeitig, können Sie über den Befehl **Entfernen** Gruppenmitglieder wieder aus der Gruppe herausnehmen.

Ihre Änderungen werden erst mit dem Befehl **OK** oder **Übernehmen** wirksam.

Unter dem Reiter "**Rechte**" werden alle Zugriffs- und Aktionsrechte des Benutzers der verbundenen Archivdatenbank angezeigt. Voraussetzung hierfür ist, dass Sie sich zuvor mit einer Datenbank verbunden haben. Die Verwaltung der Zugriffsrechte wird im Kapitel "Zugriffsrechte" erläutert.

Tipp

	In der Praxis hat es sich bewährt Rechte auf Gruppenebene zu vergeben und die Benutzer entsprechend den Gruppen zuzuordnen. Ist ein Benutzer Mitglied einer Gruppe, so erhält er auch die entsprechenden Rechte. Daher sollte sich die Zuweisung von Mitgliedern zu Gruppen danach orientieren, welche Rechte ein Benutzer erhalten soll.

Siehe auch:

Zugriffsrechte - Konzept und Überblick

Datenbankrechte verwalten

Dokumenttyprechte verwalten

PIN Verwaltung der PROXESS Supervisor Smartcards

Als PROXESS Supervisor meldet sich ein Benutzer in PROXESS mit Supervisor Smartcard und PIN-Eingabe an. Der Supervisor ist befugt Benutzer und Gruppen zu verwalten, Zugriffs- und Verwaltungsrechte zu erteilen und zu entziehen und die PROXESS Sicherheitsoptionen wie z. B. Feldverschlüsselung zu aktivieren.

Die voreingestellte Standard User und Admin PIN einer Supervisor Smartcard lautet "1234". Die Verwaltung von Smartcards und PIN´s erfolgt über das Programm Gemalto Classic Client Toolbox.

Warnhinweis

Die PROXESS GmbH empfiehlt aus Sicherheitsgründen ausdrücklich die Änderung der beiden Standard PIN´s in individuelle PIN´s.

Um eine unkontrollierte oder unbefugte Inbetriebnahme der Sicherheitsoptionen in PROXESS zu verhindern, raten wir von der Weitergabe der Smartcard an Dritte dringend ab.

Jede PROXESS Supervisor Smartcard besitzt eine Admin PIN und eine User PIN. Die User PIN wird zur Anmeldung des Supervisors mit seiner Smartcard am PROXESS System verwendet. Die Admin PIN dient ausschließlich der internen Verwaltung der Smartcard. So erlaubt die Anmeldung mit der Admin PIN im Programm Gemalto Classic Client Toolbox neben der Änderung von User PIN und Admin PIN auch das Entsperren einer durch mehrfache Falscheingabe gesperrten User PIN. Die Admin PIN einer Smartcard ist insofern vergleichbar mit der "PUK-Nummer" einer Handy-SIM-Karte.

Empfehlung: Um zu einem späteren Zeitpunkt das Entsperren einer Smartcard zu gewährleisten, sollte ein "Smartcard-Administrator" für die Änderung von Admin PIN´s vor Ausgabe von Supervisor Smartcards zuständig sein.

Änderung der Smartcard User PIN

Legen Sie die zu verwaltende Smartcard in den Smartcard Reader ein und schließen Sie den Smartcard Reader an Ihren Computer an.
Starten Sie das Programm Gemalto/Classic Client Toolbox und wählen Sie im Menü "Card Administration" den Befehl **PIN Management**.
Markieren Sie den angeschlossenen Smartcard Reader und wählen Sie den Befehl **Change PIN**.

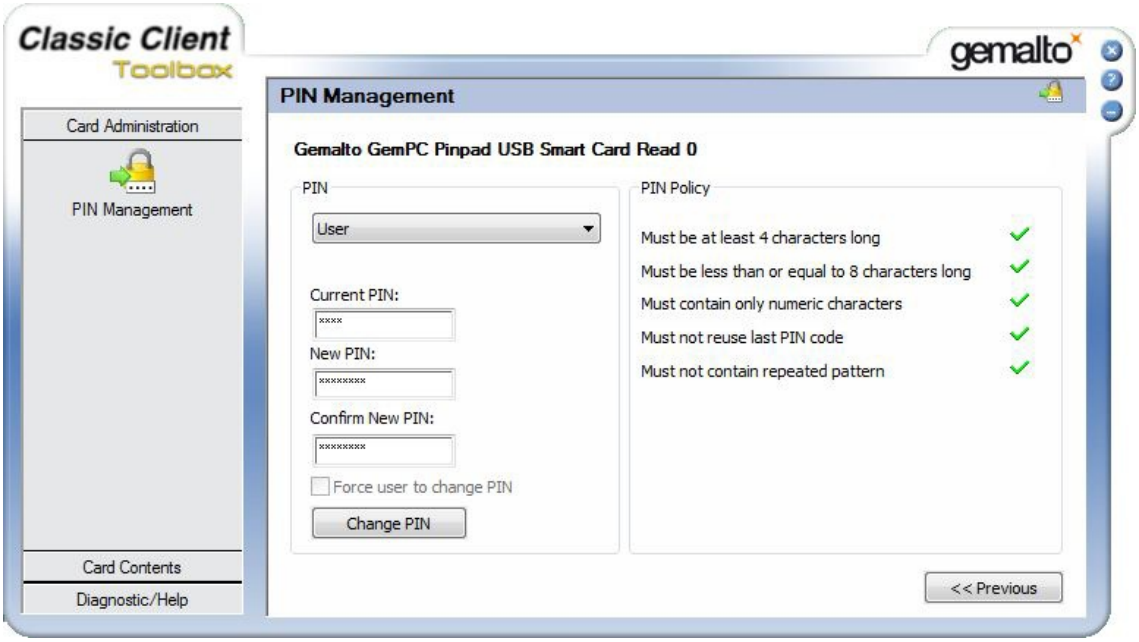


Abb.: Dialogfenster zur Änderung einer Smartcard User PIN

Wählen Sie bei der PIN Auswahl die Option **User**.

Geben Sie nun die aktuelle und die neue User-PIN über die PC-Tastatur ein. In Verlauf der Eingabe der neuen PIN wird die PIN-Sicherheitsrichtllinie überprüft. Das bedeutet, es wird überprüft, ob Ihre neue PIN den notwendigen Sicherheitsanforderungen zu Länge, Zeicheninhalten und Wiederholungszeichen genügt. Das Ergebnis wird durch rote Kreuze oder grüne Haken kenntlich gemacht. Damit eine PIN geändert werden kann, müssen alle Kriterien erfüllt sein.

Über den Befehl **Change PIN** wird die Änderung wirksam. Sie erhalten eine Bestätigung, dass Ihre Änderung erfolgreich durchgeführt wurde.

Änderung der Smartcard Admin PIN

Gehen Sie vor wie unter "Änderung der Smartcard User PIN", wählen Sie im Auswahlfeld "PIN" jedoch die Option **Admin**.

Entsperren der Smartcard User PIN

Gehen Sie vor wie unter "Änderung der Smartcard User PIN", wählen Sie aber den Befehl **Unblock PIN**.

Im Gegensatz zur PIN-Änderung ist nun im Dialogfenster im Feld **PIN** ausschließlich die Auswahl **User** möglich. Geben Sie hier im Feld **Admin PIN** die entsprechende Admin PIN der eingelegten Smartcard ein. Auch hier wird die Einhaltung der PIN-Sicherheitsrichtlinie überprüft (siehe oben). Über den Befehl **Unblock PIN** wird die Änderung wirksam. Sie erhalten eine Bestätigung, dass Ihre Änderung erfolgreich durchgeführt wurde.

Warnhinweise

	Eine Supervisor Smartcard, deren Admin PIN durch mehrfache Falscheingabe gesperrt ist, kann nicht mehr entsperrt werden. Sie sollte in der PROXESS Administrator Console auf den Status "Eingezogen" gesetzt und durch eine neue Supervisor Smartcard ersetzt werden.

Smartcard einziehen

Möchten Sie einem bestehenden Supervisor seine Supervisorprivilegien endgültig entziehen, oder soll die Karte endgültig gesperrt werden (z. B nach Verlust), so wählen Sie die Option "**Smartcard einziehen**".

Die Option "Smartcard sperren" wird dagegen eingesetzt, wenn es sich um einen zeitlich begrenzten Entzug seiner Supervisorprivilegien handeln soll. Beispielsweise können Sie die Karte eines Benutzers als Vorsichtsmaßnahme sperren, wenn der Benutzer in Urlaub ist, oder für einen zeitlich begrenzten Zeitraum andere Aufgaben im Unternehmen wahrnimmt (z. B. Auslandsaufenthalt).

Verbinden Sie sich als Supervisor mit Ihrer Smartcard mit dem eingetragenen PROXESS System.

Wählen Sie den Ordner "Smartcards" und markieren Sie den gewünschten Benutzer in der Liste aus. Wählen Sie im Menü "Aktion" die Auswahl **Einziehen** (Alternativ über Kontextmenü des Benutzers).

Es erscheint folgendes Dialogfenster:

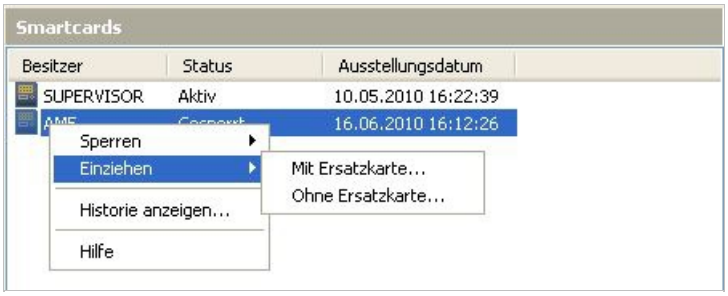


Abb.: Smartcard einziehen mit/ohne Ersatzkarte für den Benutzer AME

Die Option "**Mit Ersatzkarte**" ermöglicht es, dem Benutzer sofort eine neue bereits vorbereitete und erstellte Smartcard zuzuweisen. Die Option "**Ohne Ersatzkarte**" bietet diese Möglichkeit nicht. In beiden Fällen muss eine Begründung für die Smartcardhistorie eingegeben werden.

Warnhinweis

	Damit sich der Benutzer wieder mit seinem Benutzername und seinem Kennwort am System anmelden kann, darf er kein Mitglied der Gruppe "SUPERVISORS" sein (siehe hierzu: Gruppen verwalten).

Smartcard sperren

Die Kartensperre wird eingesetzt, wenn es sich um einen zeitlich begrenzten Entzug seiner Supervisorprivilegien handeln soll. Beispielsweise können Sie die Karte eines Benutzers als Vorsichtsmaßnahme sperren, wenn der Benutzer in Urlaub ist, oder für einen zeitlich begrenzten Zeitraum andere Aufgaben im Unternehmen wahrnimmt (z. B. Auslandsaufenthalt).

Möchten Sie einem bestehenden Supervisor seine Supervisorprivilegien endgültig entziehen, oder soll die Karte endgültig gesperrt werden (z. B nach Verlust), so wählen Sie die Option "Smartcard einziehen".

Verbinden Sie sich als Supervisor mit Ihrer Smartcard mit dem eingetragenen PROXESS-System.

Wählen Sie den Ordner "Smartcards" und markieren Sie den gewünschten Benutzer in der Liste aus. Wählen Sie im Menü "Aktion" den Befehl **Sperren/Sperre setzen** (Alternativ über Kontextmenü des Benutzers).

Es erscheint folgendes Dialogfenster:

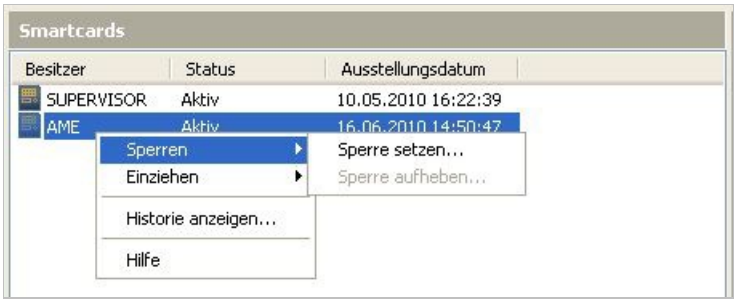


Abb.: Sperren der Smartcard für Benutzer AME

Geben Sie eine Begründung für die Sperre ein.

Die eingegebene Begründung erscheint in der Historie der Smartcard. Wählen Sie hierzu wieder den Ordner "Smartcards" und markieren Sie den gewünschten Benutzer in der Liste aus. Wählen Sie im Menü "Aktion" den Befehl **Historie anzeigen** (Alternativ über Kontextmenü des Benutzers).

Abb.: Historie der Smartcard des Benutzers AME

Smartcard zuweisen

Die Aktion "Smartcard zuweisen" führen Sie nicht für die erste Supervisor Smartcard aus. Die erste Supervisor Smartcard ist bereits in der individuellen Lizenzdatei eingetragen.

Supervisorprivilegien sind jedoch nicht auf einen einzigen Benutzer begrenzt. Aus betrieblichen Gründen (z. B. bei Vertretungsregelungen) kann es sinnvoll sein, zwei oder sogar mehrere Personen mit Supervisorprivilegien auszustatten. Auch können Sie eine zweite Supervisor Smartcard als Ersatzkarte an einem sicheren Ort (z. B. Notar, Banksafe) aufbewahren.

Meldet sich ein Supervisor über Smartcard mit PIN-Eingabe an, so entfällt die Eingabe seines Benutzernamens. Durch die Zuweisung der PROXESS Supervisor Smartcard zu einem Benutzer ist dennoch die Nachprüfbarkeit seiner Aktionen gewährleistet. Über die Zuweisung kann PROXESS sehen, welche Aktion der Benutzer ausführt (z. B. die Anlage oder das Löschen von Dokumenten, Vergabe von Zugriffsrechten oder die Neuanlage eines Benutzers).

Bevor Sie eine neue PROXESS Supervisor Smartcard zuweisen können, muss diese Smartcard bereits vorbereitet und erstellt worden sein (siehe auch "PROXESS Supervisor Smartcard vorbereiten" und "PROXESS Supervisor Smartcard erstellen").

Verbinden Sie sich als Supervisor mit Ihrer Smartcard mit dem eingetragenen PROXESS-System.

Markieren Sie den Ordner "Smartcards" wählen Sie im Menü "Aktionen" (alternativ: Kontextmenü) den Befehl **Smartcard zuweisen.**

Es erscheint folgendes Dialogfenster:

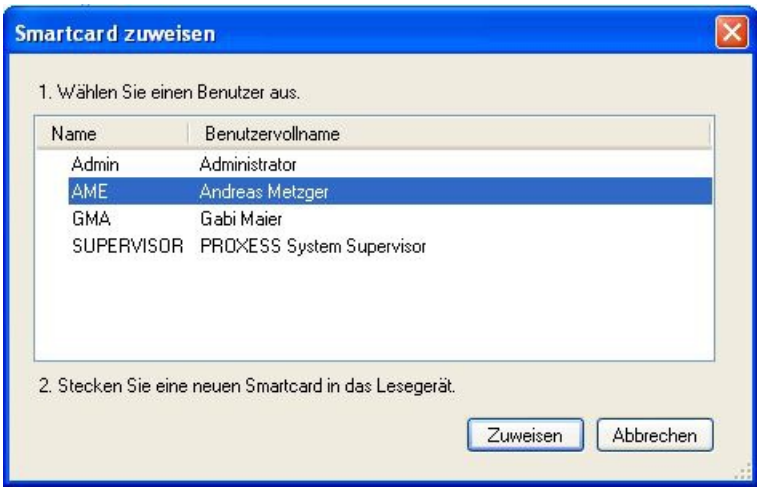


Abb.: Dialogfenster "Smartcard zuweisen"

Markieren Sie den Benutzer, dem Sie die Smartcard zuweisen möchten und wählen Sie den Befehl **Zuweisen**.
Der Benutzer erscheint nun in der Liste "Smartcards" im Ordner "Smartcards".

Warnhinweis

	Damit sich der Benutzer mit seiner Smartcard und PIN-Eingabe am System anmelden kann, muss er ein Mitglied der Gruppe "SUPERVISORS" sein (siehe hierzu: Gruppen verwalten).

Zugriffsrechte - Konzept und Überblick

Warum gibt es Rechte?
In einem elektronischen Archiv sind Dokumente für die Benutzer unternehmensweit leichter und schneller zugänglich als in einem Papierarchiv. Umso wichtiger ist es festzulegen, wer Zugriff auf welche Dokumente haben soll. Dies geschieht in PROXESS über Benutzerrechte auf Datenbanken, Dokumenttypen und Einzeldokumente. Benutzer können nicht nur an einzelne Benutzer, sondern auch an Gruppen vergeben werden. Dies spart in Systemen mit mehreren hundert Benutzern wertvolle Arbeitszeit.

Muss und Kann
In jedem Fall müssen Sie Rechte vergeben, da das System standardmäßig neuen Benutzer und Gruppen keine Rechte erteilt. Das System bietet zur Rechtevergabe zahlreiche Differenzierungsmöglichkeiten. Ob und wie weit Sie davon Gebrauch machen, hängt von der Anzahl der PROXESS-Benutzer und von der Dokument- und Aufgabenstruktur in Ihrem Unternehmen ab.

Ebenen der Rechteverwaltung

Ebene 1: Datenbankrechte
PROXESS unterstützt die Einrichtung und Verwaltung unterschiedlicher Archivdatenbanken. So können Sie große Bereiche wie Auftragswesen oder Lohn und Gehalt komplett voneinander trennen. Damit Benutzer und Gruppen überhaupt mit diesen Archivdatenbanken arbeiten können, benötigen sie zunächst ein Zugriffsrecht auf die entsprechende Datenbank.

Ebene 2: Dokumenttyprechte
Innerhalb einer Archivdatenbank können Sie über die Dokumenttyprechte die Zugriffsmöglichkeiten der Benutzer steuern. Dabei werden folgende Aktionsrechte unterschieden: Ansehen, Anlegen, Bearbeiten, Löschen sowie das Recht "Dokumente verrechten" und Dokumenttyprechte vergeben. Diese Aktionen können Sie im Prinzip beliebig kombinieren, wobei das Recht zum Ansehen natürlich die notwendige Basis für die anderen Aktionsrechte bildet.

Ebene 3: Einzeldokumentrechte
Auch für ein einzelnes Dokument können Rechte in den vier Aktionskategorien "Ansehen", "Anlegen", "Bearbeiten" und "Löschen" vergeben werden. Dies hat den Sinn, dass Benutzer im Einzelfall selbst entscheiden können, ob andere Benutzer Zugriff auf ein einzelnes Dokument erhalten sollen. Dieses Recht trägt der Entscheidungskompetenz der Mitarbeiter im Unternehmen Rechnung und erleichtert somit Arbeitsabläufe, ohne dass ein Eingriff des Supervisors oder des Bereichsadministrators notwendig wird. Es gilt nur für einzelne Dokumente, ersetzt also nicht die vom Supervisor vorgesehene Rechtestruktur, sondern erweitert diese lediglich. Die Erteilung von Rechten auf Einzeldokumente nimmt der Benutzer im PROXESS Standard Client selbst vor.

Beispiel
Sie erteilen Benutzer A das Zugriffsrecht für die Datenbank "Auftrag". In dieser Datenbank geben Sie ihm das Recht auf die Dokumenttypen Angebot, Auftrag, Kaufvertrag, Kundenrechnung und Reklamation.
Angebote darf der Benutzer nicht nur ansehen, sondern selber anlegen, bearbeiten und auch wieder löschen.
Aufträge darf der Benutzer ansehen, anlegen und bearbeiten, aber nicht löschen.
Kaufverträge darf der Benutzer nur ansehen und anlegen.
Kundenrechnungen und Reklamationen darf der Benutzer nur ansehen.
Benutzer B bekommt für Kundenrechnungen das Recht, selbst Rechte zuzuweisen. Um Benutzer A in einem bestimmten Vorgang die Bearbeitung der Rechnung 4711 zu ermöglichen, gibt er ihm das "Bearbeiten-Recht" für diese Rechnung.
Benutzer A kann also alle Kundenrechnungen sehen, aber nur die Rechnung 4711 bearbeiten.

Rechtszustände und Vorfahrtsregeln

Normalerweise genügt es, in der Rechteverwaltung mit "Recht erteilt" und "Recht nicht erteilt" zu arbeiten. Wenn aber ein Benutzer in verschiedenen Gruppen Mitglied ist, kann es Überschneidungen und Widersprüche geben. Daher können Sie in der Rechteverwaltung zusätzlich mit dem Recht "Verbieten" arbeiten, um schnell und sicher ein Recht auszuschalten, das ein Benutzer über seine Gruppenzugehörigkeit besitzt.

Daher werden grundsätzlich drei Rechtszustände unterschieden und folgendermaßen dargestellt:
Es gibt drei Zustände bei der Rechtevergabe:

Häkchen gesetzt	Recht ist erteilt
grünes Kästchen (bzw. ausgegrautes Häkchen im klassischen Windows-Design)	Recht ist nicht erteilt (= Standardeinstellung). Evtl. hat ein Benutzer aber über seine Gruppenzugehörigkeit entsprechende Rechte.
leeres Kästchen	Recht ist explizit entzogen (= verbieten). Das sogenannte "Verbieten" für Einzelbenutzer überstimmt das Recht, das der Benutzer aufgrund seiner Gruppenzugehörigkeit besitzt.

Beispiel:
Sie wollen Benutzer X den Zugriff auf die Datenbank "Lohn" entziehen. Dieser Benutzer ist Mitglied in zehn verschiedenen Gruppen.

Wenn Sie nur mit den beiden Rechtszuständen "Recht haben" und "Recht nicht haben" auskommen müssten, wäre folgendes zu tun:
Die Rechte für jede dieser zehn Gruppen kontrollieren. Drei Gruppen haben das Recht auf die Lohndatenbank. Den Benutzer X aus den drei berechtigten Gruppen herausnehmen.

Der zusätzliche Rechtszustand "Verbieten" reduziert diesen Vorgang auf einen Arbeitsschritt:
Sie entziehen dem Benutzer X einfach explizit den Zugriff auf die Datenbank "Lohn". Dadurch sind alle Rechte, die der Benutzer durch seine Gruppenzugehörigkeit hat, automatisch aufgehoben.

Vorfahrtsregeln
Es gelten ein paar einfache Vorfahrtsregeln. Diese Regeln sind nach Stärkegraden abgestuft, d. h. die erste ist stärker als die zweite und die zweite stärker als die dritte:

Benutzerrecht geht vor Gruppenrecht
Verbot geht vor "Recht haben"
"Recht haben" geht vor "Recht nicht haben"

Mögliche Rechtekonstellationen lassen sich durch eine Kombinationstabelle darstellen. Wenn Sie nicht ganz sicher sind, welche Auswirkungen Ihre Festlegungen haben, kann es hilfreich sein, zuerst eine solche Übersicht anzulegen, bevor Sie Rechte in PROXESS Administrator vergeben.
Die folgende Tabelle zeigt die Kombinationsmöglichkeiten für einen Benutzer X, der in zwei Gruppen Mitglied ist. Je nachdem, wie viele Benutzergruppen es gibt, vervielfältigen sich natürlich die Möglichkeiten. Die rechte Spalte zeigt das jeweilige Ergebnis für Benutzer X, das sich durch die Vorfahrtsregeln ergibt.

Fall	*Benutzer X*	*Gruppe 1*	*Gruppe 2*	*Darf Benutzer X Objekt Y sehen?*
1	*hat kein Recht*	*hat kein Recht*	*hat kein Recht*	*nein*
2	*hat kein Recht*	*hat kein Recht*	*hat Recht*	*ja*
3	*hat kein Recht*	*hat Recht*	*hat Recht*	*ja*
4	*hat kein Recht*	*hat Recht*	*Verbot*	*nein*
5	*hat Recht*			

Index