SE16XXL – Neue Administrations-Funktionen

April 2025 Neue Version **4.1** mit folgenden Funktionen:

- Übergeordnete Rollen in den Zugriffsrechten Mehr…
- Script-Versionen Mehr…
- Globale Favoriten-Cluster zuweisen Mehr…
- Berechtigungsprüfungen mit ACTVT = ‘03’ Mehr…

Oktober 2024 Neue Version **4.0** mit folgenden Funktionen:

- Download/Upload-Funktionalität für Einstellungen Mehr…
- Neue Option für Berechtigungen auf Satzebene Mehr…

März 2024 Neue Version **3.6E** mit folgenden Funktionen:

- Verschiedene Einstellungen auf Rollenebene Mehr…
- Tool zum Löschen von alten TXBAT-Einträgen Mehr…

November 2023 Neue Version **3.6D** mit folgender Funktion:

- Programm zum Befüllen von /TFTO/TBASSOCS Mehr…

Juli 2023 Neue Version **3.6C** mit folgender Funktion:

- Pflegedialog für Berecht. für CDS-View-Entitäten Mehr …

April 2023 Neue Version **3.6B** mit folgender Funktion:

- Zwei neue Rollen eingeführt Mehr …

Dezember 2022 Neue Version **3.6A** mit folgenden Funktionen:

- Initialwerte für benutzerspezifische Default-Dateipfade Mehr …
- Neue Transaktion zum Anzeigen einer Internetseite Mehr …

Mai 2022 Neue Version **3.6** mit folgenden Funktionen:

- Dialog der Globalen Einstellungen umgestaltet Mehr …
- Berechtigungsprüfungen mit Primärtabellen Mehr …
- View-Berechtigungs-Ausnahmen Mehr …
- Einschränkungen für F.Codes auf Rollenebene Mehr …
- Referenzbenutzer berücksichtigt Mehr …
- CDS-Views mit ihren Berechtigungsprüfungen Mehr …

November 2021 Neue Version **3.5B** mit folgender Funktion:

- Neue Rollen fürs Summieren/Zählen auf der Datenbank Mehr …

April 2021 Neue Version **3.5A** mit folgender Funktion:

- Einstellung für Data-Aging-Zugriff Mehr …

November 2020 Neue Version **3.5** mit folgenden Funktionen:

- Globale Einstellung für RFC-Zugriff Mehr …
- PflegeDialog für Erlaubte RFC-Destinationen Mehr …

Januar 2020 Support Package mit folgenden Funktionen:

- Administration von Benutzer-Einstellungen Mehr …
- Berechtigungen für Standard-ALV-Layouts Mehr …

November 2019 Neue Version **3.4A** mit folgenden Funktionen:

- Zugriffsrechte für Pseudo-Tabellen Mehr …
- Pflege-Dialog für $TABCOUNT-Ausnahmen Mehr …

August 2018 Neue Version **3.3D** mit folgenden Funktionen:

- Neue Optionen für die Rollen eines globalen Scripts Mehr …
- Einträge für das Security Auditlog Mehr …
- Neue globale Einstellungen für Scripts Mehr …
- Berechtigungen auf Satzebene – Bemerkungs-Feld Mehr …

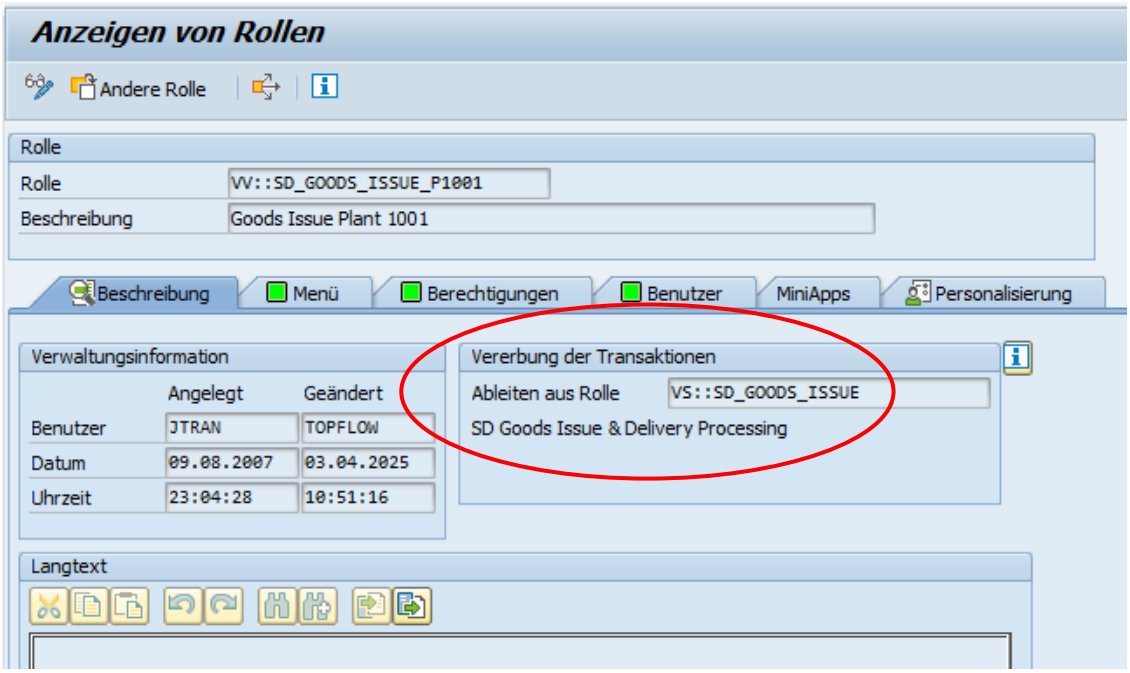
Übergeordnete Rollen in den Zugriffsrechten

In den Zugriffsrechten für Tabellen & Felder ist es möglich, einer **Zugriffsrolle** eine **SAP-Rolle** zuzuweisen. Wenn mit Hilfe der Transaktion PFCG die SAP-Rolle einer bestimmten Person zugeordnet wird, wird die zugehörige Zugriffsrolle (**indirekt und automatisch**) dieser Person zugeordnet, ohne dass eine explizite Zuordnung erforderlich ist. Dies erleichtert es der Systemadministration, die Zugriffsrechte für Tabellen & Felder so zu verwalten, dass sie mit den anderen Benutzerberechtigungen kompatibel sind.

Diese Logik, die schon lange verfügbar war, wurde nun durch die Berücksichtigung sogenannter **übergeordneter Rollen** verbessert. Auf diese Weise wird es möglich, den Benutzerberechtigungen eine gewisse Struktur zu verleihen.

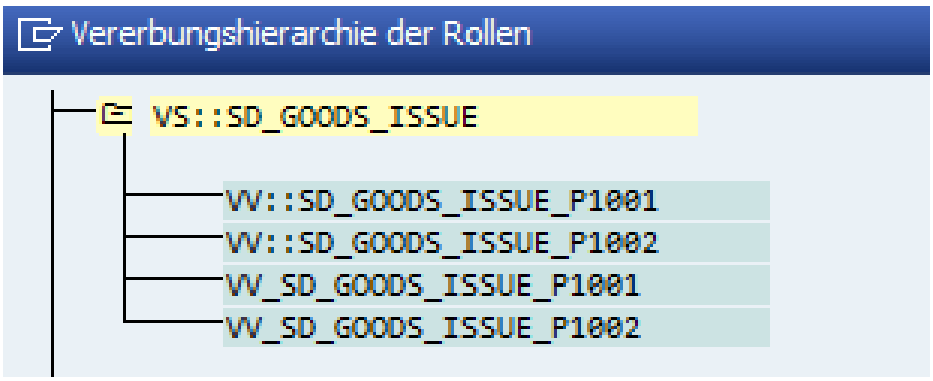
Was sind übergeordnete Rollen?

In der Transaktion **PFCG** (Pflege von Rollen) kann eine bestimmte SAP-Rolle eine sogenannte "**vererbende Rolle**" haben, wie in folgender Abbildung zu sehen ist:



Wenn eine SAP-Rolle angelegt wird, ist es möglich, einige ihrer Komponenten von einer anderen SAP-Rolle abzuleiten, die im SAP-Jargon als "vererbende Rolle" bezeichnet wird. In dieser Dokumentation nennen wir sie jedoch "**übergeordnete Rolle**", weil dies angemessener erscheint. Auf diese Weise kann eine bestimmte übergeordnete Rolle in einer Art Rollenhierarchie über eine **Reihe von abgeleiteten Rollen** gestellt werden. Nachträgliche Änderungen an der übergeordneten Rolle haben keine automatische Auswirkung auf die darunterliegenden abgeleiteten Rollen.

Um eine Vorstellung von den abgeleiteten SAP-Rollen einer bestimmten übergeordneten Rolle zu bekommen, zeigen Sie einfach in der Transaktion PFCG die übergeordnete Rolle an und klicken Sie dann auf (Vererbungshierarchie). Das System reagiert mit folgendem Popup:

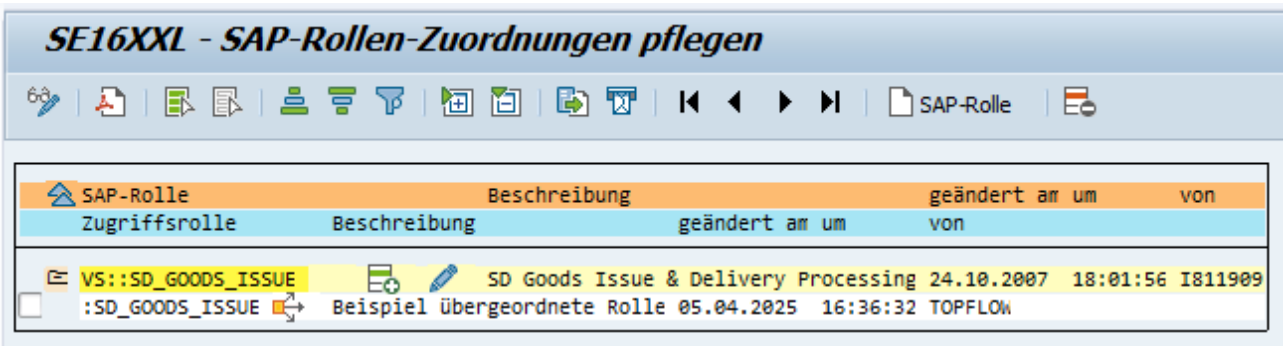


Übergeordnete Rollen und Zugriffsrechte für Tabellen & Felder

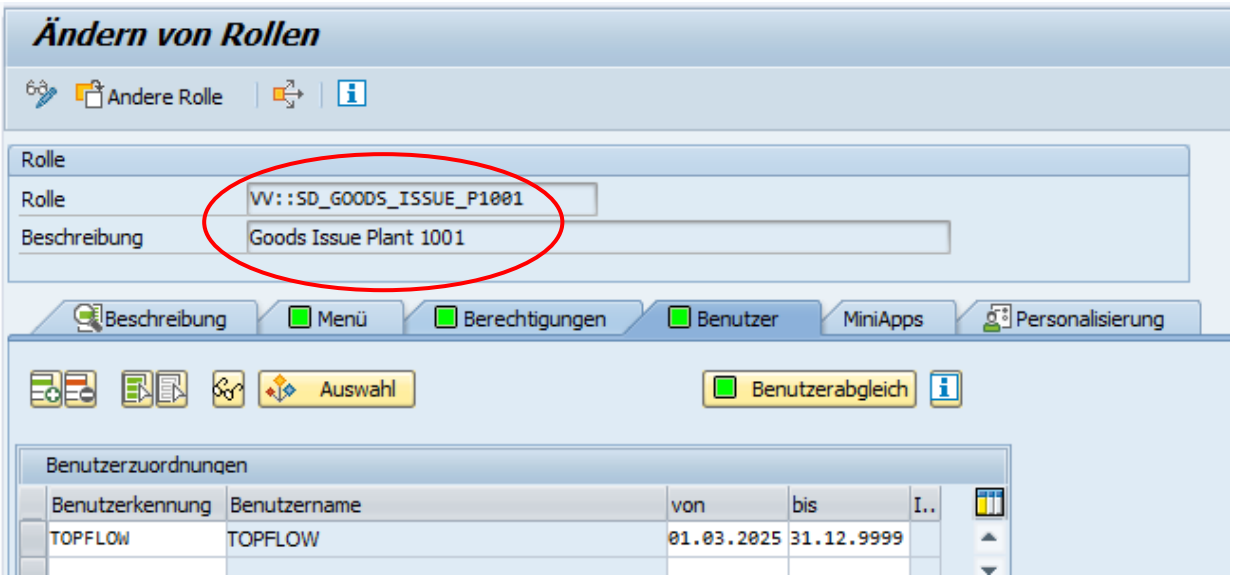
Um in den Zugriffsrechten für Tabellen & Felder wirksam zu sein, ist es notwendig, dass eine bestimmte übergeordnete SAP-Rolle einer Zugriffsrolle zugewiesen wird. Wenn dies geschehen ist, ist diese Zugriffsrolle allen Logon-Kennungen automatisch zugeordnet, die über eine der von dieser übergeordneten Rolle abgeleiteten SAP-Rollen verfügen. Diese etwas verwirrende Situation soll nun anhand eines Beispiels verdeutlicht werden.

Beispiel einer übergeordneten Rolle

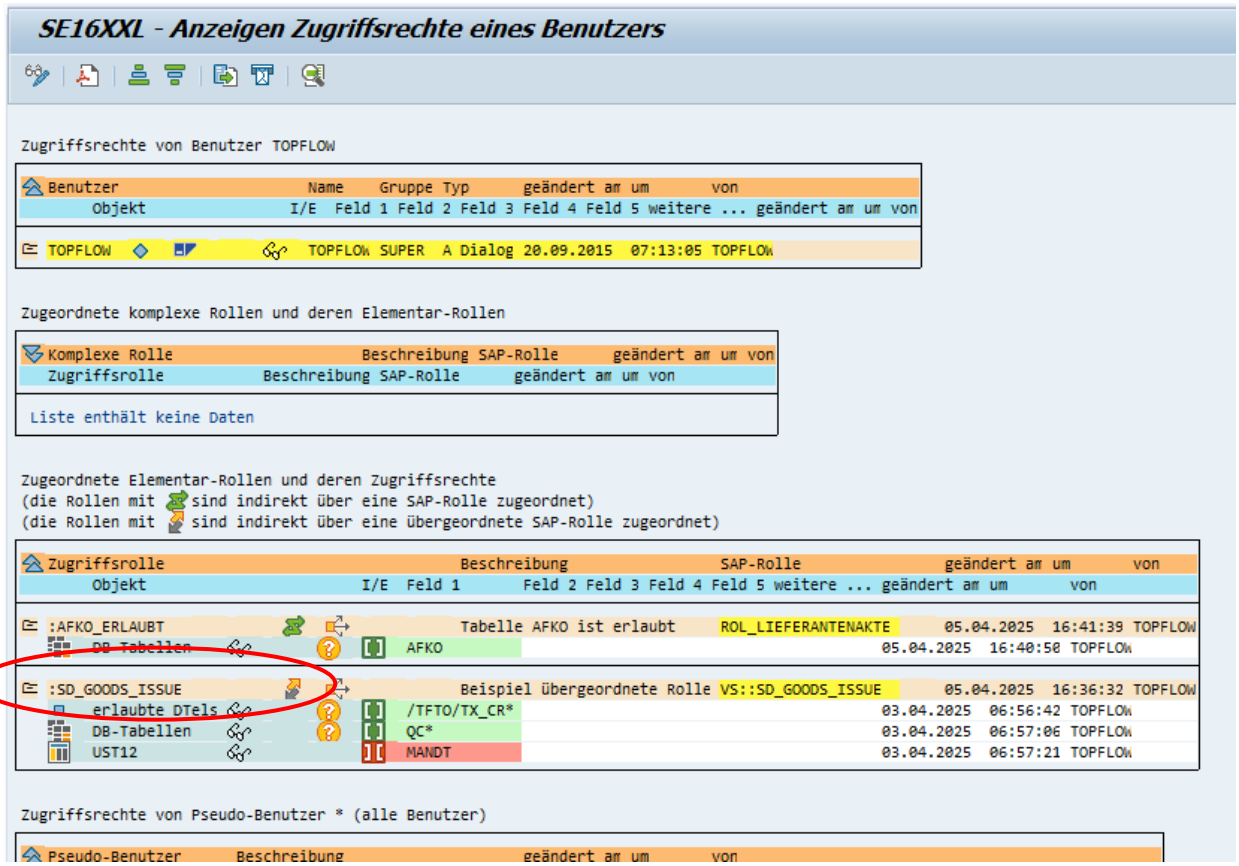
In den Zugriffsrechten für Tabellen & Felder weisen wir die oben erwähnte übergeordnete Rolle einer Zugriffsrolle zu:



Nun ordnen wir in der Transaktion PFCG der Logon-Kennung **TOPFLOW** die erste abgeleitete SAP-Rolle der übergeordneten Rolle (**VV::SD_GOODS_ISSUE_P1001**) zu:



Abschließend werfen wir in den Zugriffsrechten für Tabellen & Felder einen Blick auf die Berechtigungen der Kennung TOPFLOW:



Wie man sehen kann, wurde die Zugriffsrolle **:SD_GOODS_ISSUE** indirekt über die übergeordnete Rolle **VS::SD_GOODS_ISSUE** zugewiesen (gekennzeichnet durch die Ikone).

Erklärung der Logik

Wahrscheinlich werden Sie sich immer noch fragen, was das alles bedeutet. Nun, mit Hilfe einer übergeordneten Rolle könnte folgendes Konstrukt implementiert werden:

1) Die übergeordnete Rolle ist einer Zugriffsrolle zugeordnet, die eine **Gruppe von Datenbanktabellen** definiert, die für eine bestimmte Aktivität innerhalb des Unternehmens relevant sind.

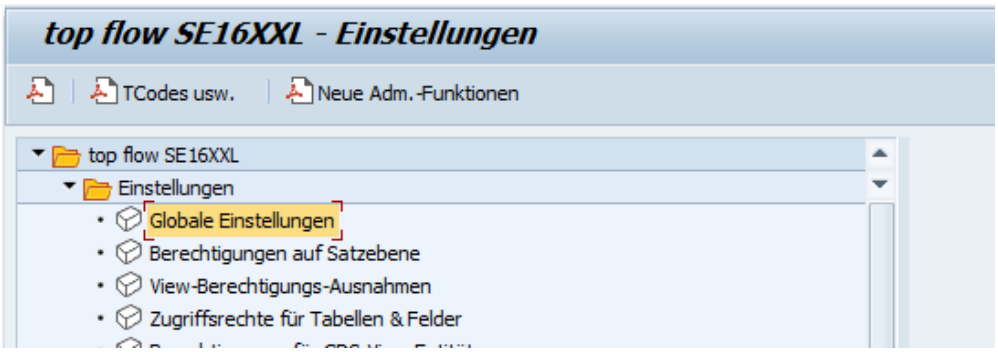
2) Die abgeleiteten Rollen enthalten die Berechtigungen, die für den Zugriff auf eine Teilmenge der relevanten Daten erforderlich sind, z.B. nur auf eine **bestimmte Verkaufsorganisation** oder einen **bestimmten Buchungskreis** usw.

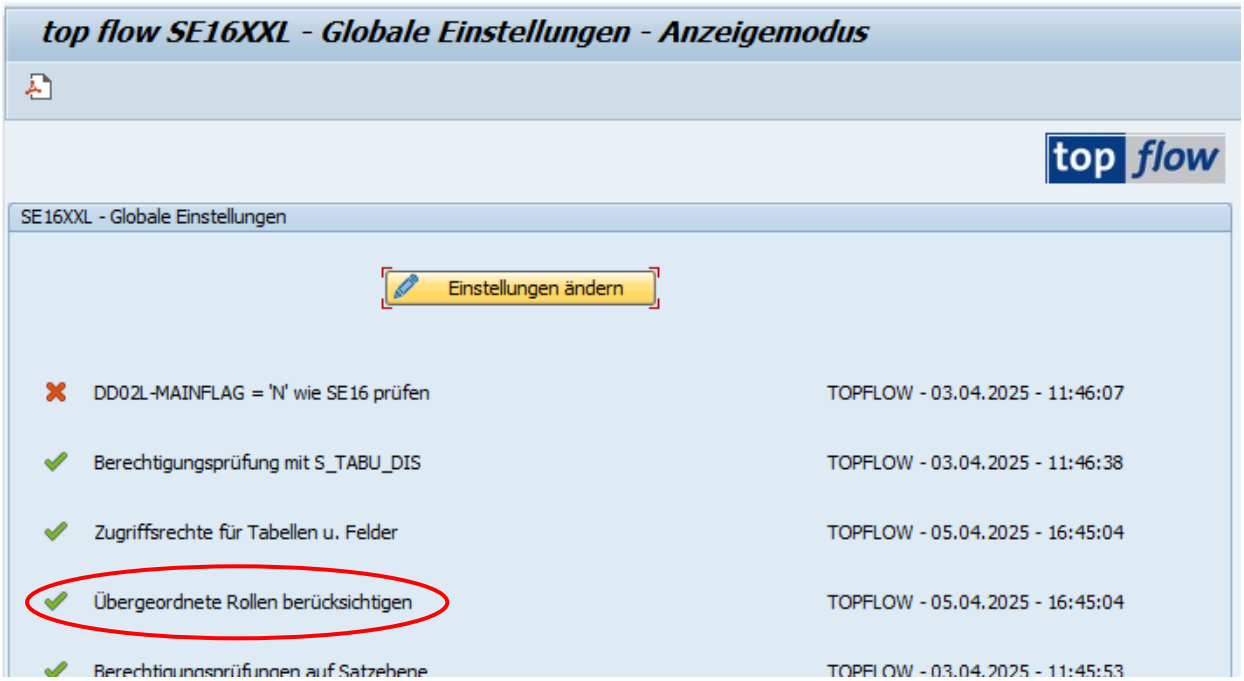
3) Angenommen, es gibt fünf VKOrgs und fünf Personengruppen, die jeweils für eine bestimmte VKOrg arbeiten, dann ist es nur notwendig, den Mitgliedern jeder Gruppe die entsprechende abgeleitete SAP-Rolle zuzuweisen, um das gewünschte Ergebnis zu erzielen, d.h. dass jede Person auf die **beteiligten Datenbanktabellen** zugreifen darf und gleichzeitg nur berechtigt ist, die **Datensätze zu selektieren**, die sich auf die **eingeschränkte VKOrg** beziehen.

Es ist nicht erforderlich, die **Zugriffsrolle** der übergeordneten Rolle explizit zuzuweisen, da dies **automatisch** durch die Abhängigkeit der abgeleiteten Rollen von der übergeordneten Rolle erfolgt.

Kompatibilität

Die Logik mit den übergeordneten SAP-Rollen wirkt sich möglicherweise auf die Zugriffsrechte für Tabellen & Felder aller Personen die SE16XXL verwenden. Der Grund dafür ist, dass die aktuell zugeordneten SAP-Rollen eine übergeordnete Rolle haben könnten, die derzeit ignoriert wird, aber von der neuen Logik berücksichtigt würde. Daraus folgt, dass die neue Logik **explizit** von der Systemadministration **aktiviert** werden muss.
Dies geschieht in den globalen Einstellungen (**/TFTO/XXL_SETTINGS**):

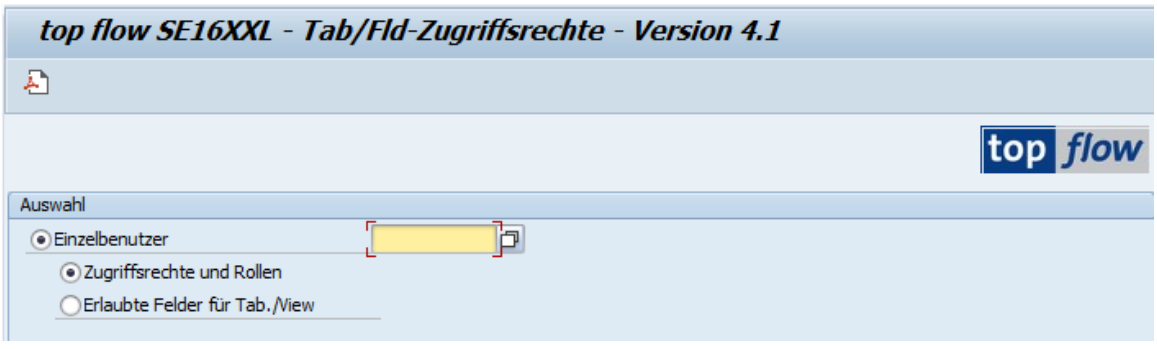




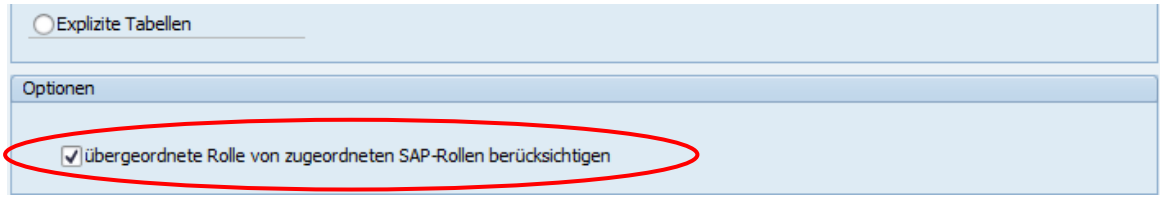
Die Einstellung "***Übergeordnete Rollen berücksichtigen***" greift nur, wenn zusätzlich die Haupteinstellung "***Zugriffsrechte für Tabellen u. Felder***" aktiviert wird.

Pflegedialog "Zugriffsrechte für Tabellen & Felder"

Nachdem die Aktivierung der Logik mit den übergeordneten Rollen optional ist, muss der Pflegedialog in der Lage sein, beide Situationen, d.h. mit oder ohne die neue Logik, zu unterstützen. Zu diesem Zweck wurde eine neue Option auf der Selektionsmaske eingeführt:



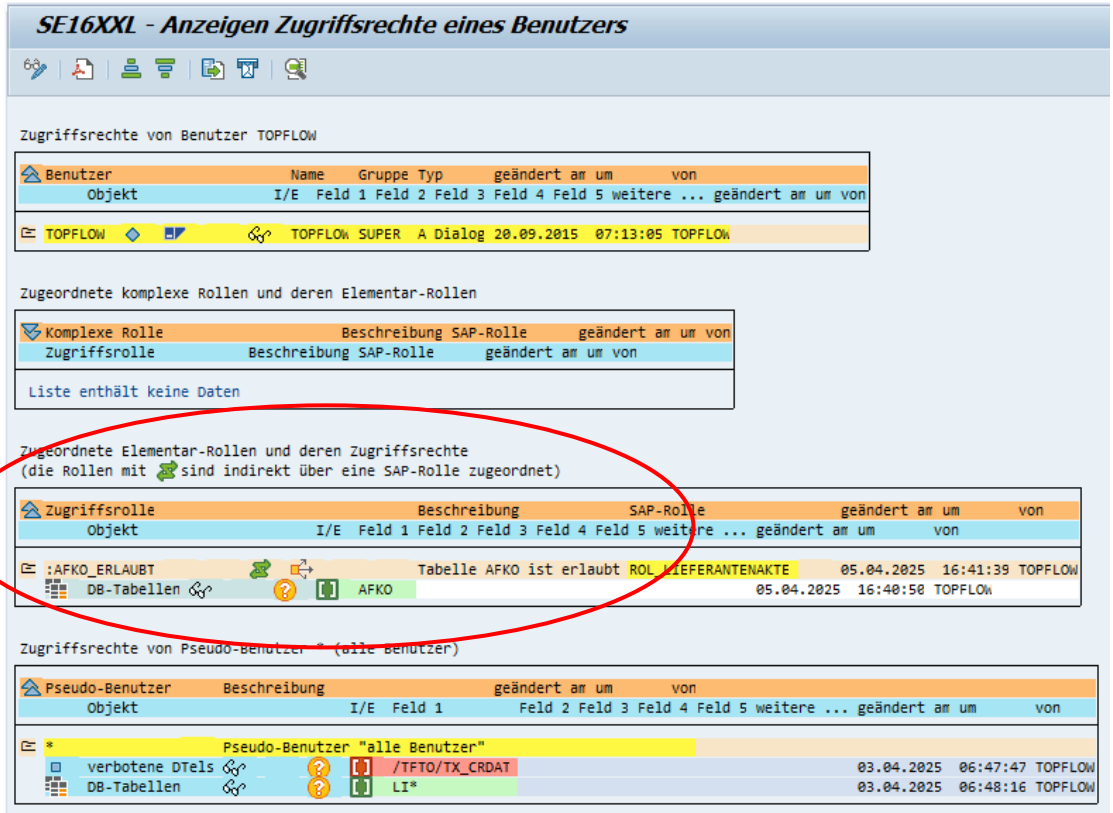
…



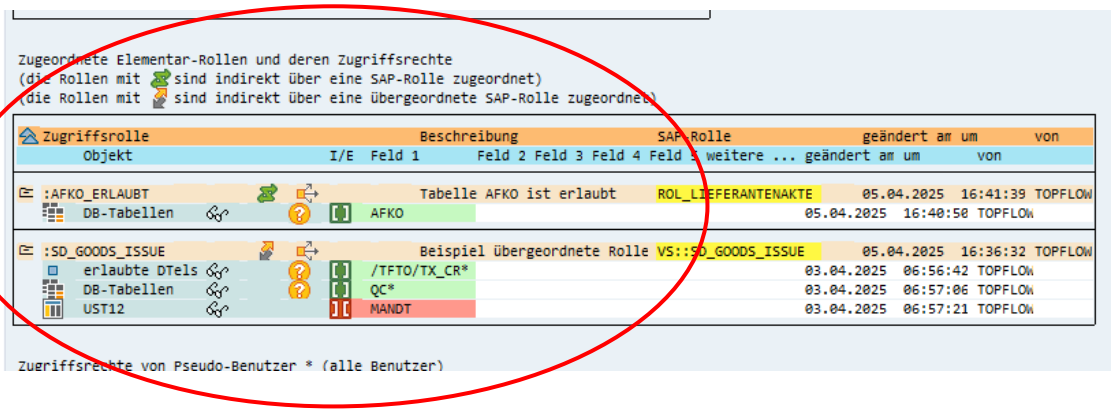
ANMERKUNG: Wenn diese Option aktiviert wird, auch wenn die globale Einstellung nicht aktiv ist, ist es möglich zu sehen, wie sich die neue Logik auf die aktuellen Zugriffsrechte auswirken würde.

Um eine Vorstellung davon zu geben, zeigen wir in beiden Situationen die Zugriffsrechte der Kennung TOPFLOW an.

Ohne die neue Logik:



Mit der neuen Logik:



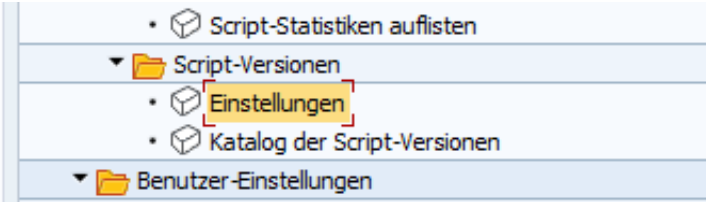
Zum Anfang

Script-Versionen

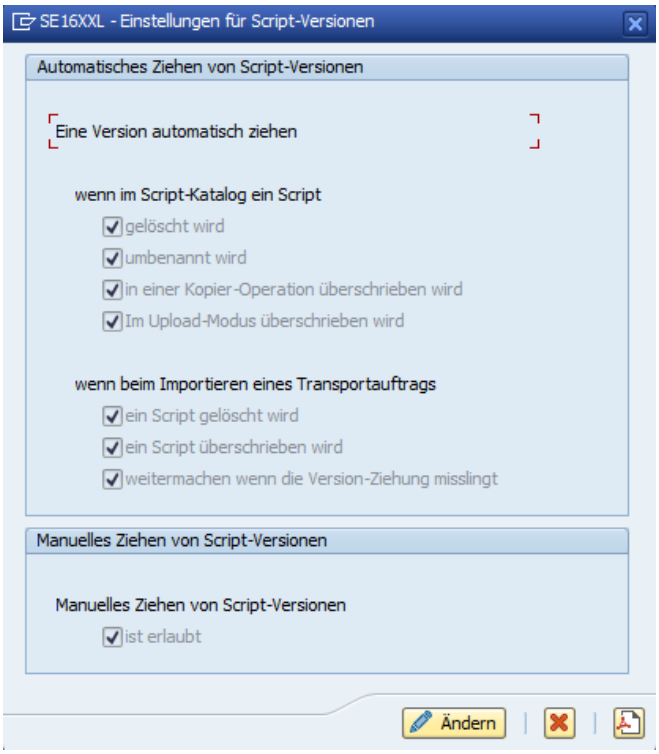
Ab **Version 4.1** unterstützt SE16XXL **Script-Versionen**. Eine Script-Version ist eine **vollständige Kopie** eines Scripts (entweder global oder benutzerspezifisch), einschließlich der inaktiven Version (falls vorhanden), der Script-Varianten, der scriptspezifischen ALV-Layouts und der Default-ALV-Layouts. Für ein bestimmtes Script kann eine beliebige Anzahl von Versionen generiert werden. Jede hat ihren eigenen Zeitstempel, so dass es möglich ist, sie nach Generierungsdatum und -zeit zu sortieren. Auf diese Weise ist es sehr einfach, die letzte Version eines bestimmten Scripts zu ermitteln.

Eine Version eines Scripts kann entweder **automatisch** von SE16XXL oder **manuell** von einer interessierten Person gezogen werden. Die Systemadministration legt fest, für welche Situationen eine Script-Version automatisch erstellt werden soll. Sie kann auch die manuelle Ziehung von Script-Versionen erlauben (oder verbieten).

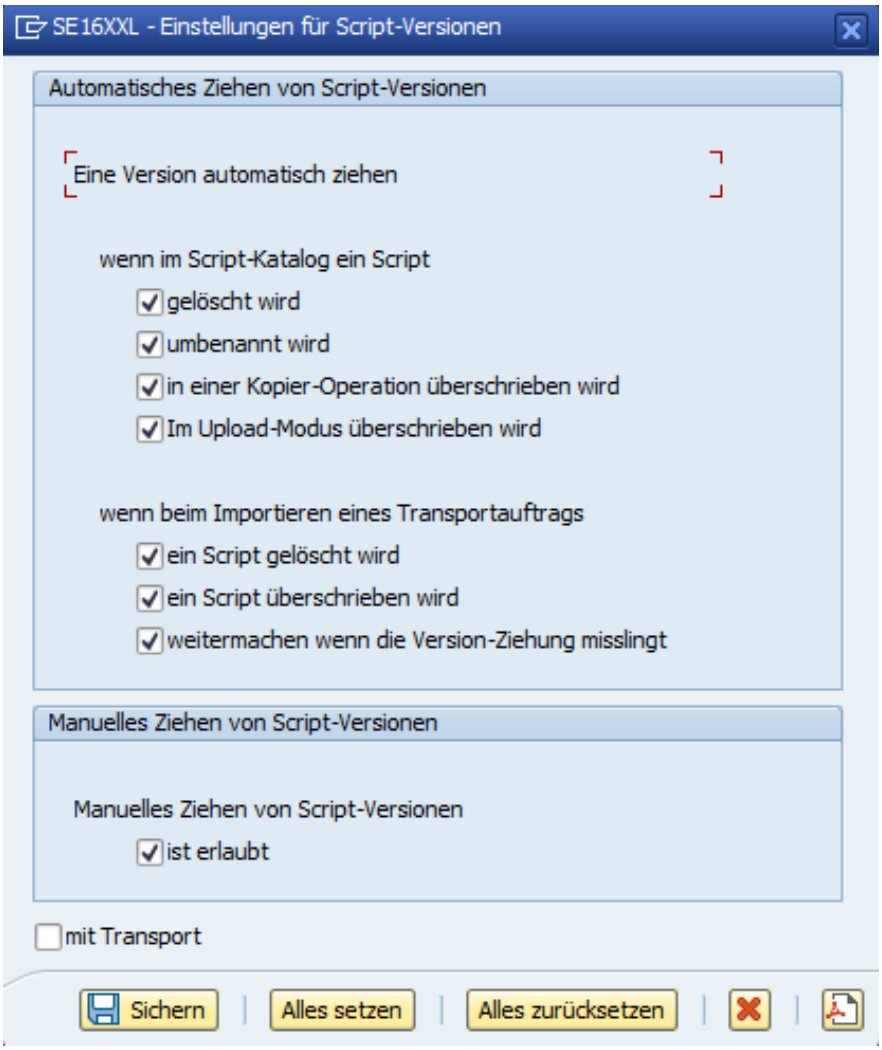
Die Einstellungen für Script-Versionen können mit Hilfe der Transaktion /TFTO/XXL_SETTINGS angepasst werden:



Mit einem Doppelklick auf Einstellungen öffnet sich folgendes Dialogfenster:



Betätigen Sie die Schaltfläche Ändern, um die Einstellungen zu ändern:



ANMERKUNG: Sie benötigen **Administrationsrechte**, um die Einstellungen ändern zu dürfen. Andernfalls wird das Dialogfenster im **Anzeigemodus** ohne die Schaltfläche Ändern ausgegeben.

Falls die Option mit Transport aktiviert wird, fragt das Programm nach einem Transportauftrag, wenn Sichern betätigt wird.

Weitere Informationen zu diesem Thema finden Sie in der Dokumentation des **Katalogs der Script-Versionen**.

Zum Anfang

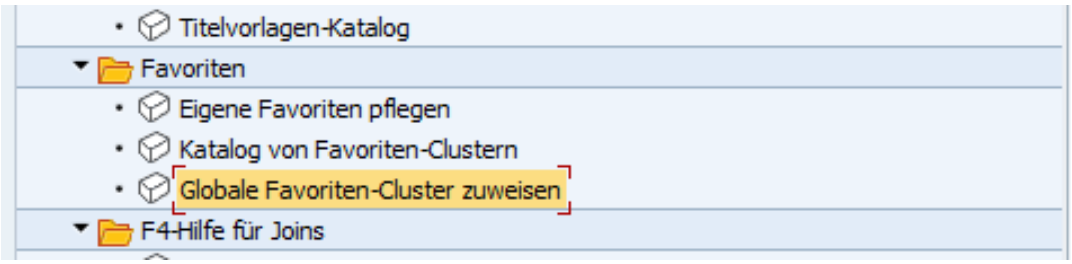
Globale Favoriten-Cluster zuweisen

Favoriten wurden eingeführt, damit man die SE16XXL Scripts, die man am häufigsten verwendet, leichter finden kann, ohne sich ihre genauen Namen merken oder mit Hilfe der F4-Hilfe nach ihnen suchen zu müssen. Die Favoriten enthalten meist eigene Scripts und eine Reihe von globalen Scripts, die in der Regel von anderen Personen erstellt wurden.
In einem Unternehmen erstellen nur wenige Personen globale Scripts, die übrigen verwenden sie lediglich. Und ein globales Script ist in der Regel nur für einen kleinen Kreis von Personen relevant.
Im Laufe der Zeit werden immer mehr globale Scripts erstellt. Irgendwann wird es notwendig, all diesen Scripts eine gewisse Struktur zu geben – dies geschieht in der Regel durch die Zuweisung zu einer Reihe von **globalen Favoriten-Clustern**, die jeweils einer bestimmten **Tätigkeit** innerhalb des Unternehmens gewidmet sind.

Die Suche nach den relevanten globalen Favoriten-Clustern war bisher der Initiative jedes Einzelnen überlassen. Dieser Ansatz ist nicht besonders effizient und kann in einer großen Organisation zu Situationen führen, in denen die neuesten Scripts lediglich von einem Bruchteil der Personen, für die sie tatsächlich entwickelt wurden, vewendet werden.

Aus diesem und anderen Gründen steht ab **Version 4.1** von SE16XXL ein **neues Tool** zur Verfügung, mit dem eine Reihe von globalen Favoriten-Clustern in einem Durchgang den Favoriten mehrerer Personen **zugewiesen** werden kann. Zusätzlich können auch veraltete oder falsch zugewiesene globale Cluster aus den Favoriten ausgewählter Personen wieder **entfernt** werden.

Das Tool steht in den SE16XXL Einstellungen (Transaktion **/TFTO/XXL_SETTINGS**) zur Verfügung:



Detaillierte Informationen finden Sie unter Globale Favoriten-Cluster zuweisen.

Zum Anfang

Berechtigungsprüfungen mit ACTVT = '03'

Bisher wurden die meisten Berechtigungsprüfungen in SE16XXL mithilfe einer AUTHORITY_CHECK Anweisung durchgeführt, die dem folgenden Beispiel ähnelt:

```
AUTHORITY-CHECK OBJECT 'V_VBAK_VKO'
    ID 'VKORG' FIELD LS_A001-VKORG
    ID 'VTWEG' FIELD LS_A001-VTWEG
    ID 'SPART' FIELD LS_A001-SPART
    ID 'ACTVT' DUMMY.
```

In dieser Anweisung wurde das Feld **ACTVT** nicht berücksichtigt (DUMMY). Man ist nämlich davon ausgegangen, dass der harmloseste Wert "**03**" (**Anzeige**) wäre.

Unglücklicherweise gilt diese Annahme für die neueren SAP-Versionen nicht mehr. **ACTVT** kann nun auch den Wert "**F4**" (**Anzeige in Wertehilfe**) annehmen. Daraus resultiert dass, wenn die Berechtigungsprüfungen weiterhin mit ACTVT = DUMMY durchgeführt würden, eine Person, die **nur mit ACTVT = 'F4'** ausgestattet ist, Datensätze selektieren könnte, die eigentlich unzugänglich sein sollten.

Aus diesem Grund werden ab Version **4.1** von SE16XXL alle AUTHORITY-CHECK-Anweisungen, die ein Berechtigungsobjekt mit dem Feld ACTVT betreffen, wie im folgenden Beispiel ausgeführt:

```
AUTHORITY-CHECK OBJECT 'V_VBAK_VKO'
    ID 'VKORG' FIELD LS_A001-VKORG
    ID 'VTWEG' FIELD LS_A001-VTWEG
    ID 'SPART' FIELD LS_A001-SPART
    ID 'ACTVT' FIELD '03'.
```

Dies gilt auch für spezielle Berechtigungen und Sekundär- → Primärtabellen.

ANMERKUNG: Diese Logikänderung erfolgt **automatisch** und muss nicht explizit aktiviert werden.

Zum Anfang

Download/Upload-Funktionalität für Einstellungen

Folgende SE16XXL-Pflegedialoge für Einstellungen bieten nun eine **Download/ Upload**-Funktionalität an:

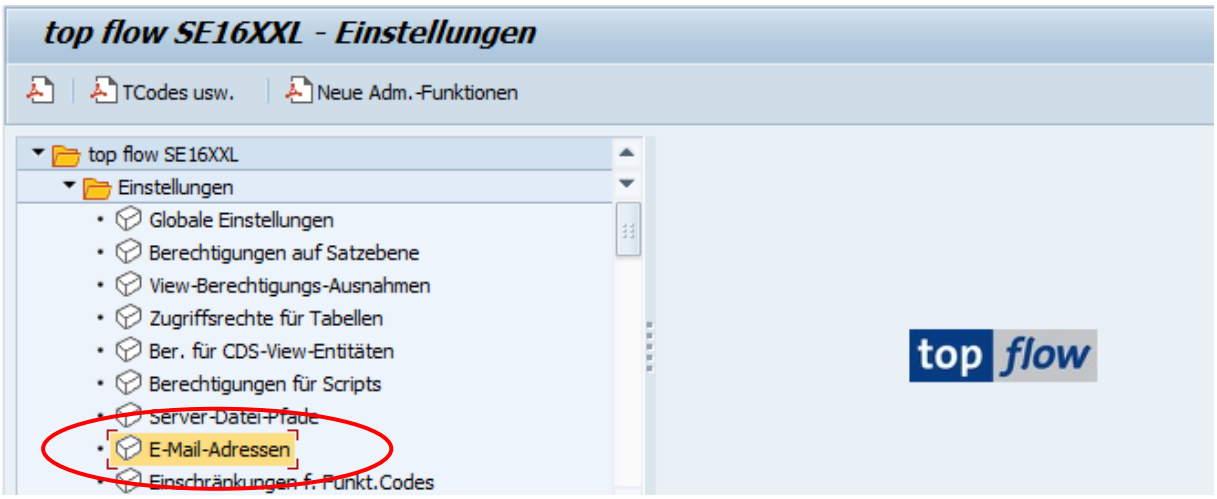
- View-Berechtigungs-Ausnahmen
- Berechtigungen für CDS-View-Entitäten
- Erlaubte Server-Datei-Pfade
- Erlaubte E-Mail-Adressen
- Einschränkungen für Funktionscodes
- Erlaubte RFC-Destinationen
- Spezielle Berechtigungen → Relevante Tabellen/Views
- Sekundär- → Primärtabellen → Definitionen
- Transaktionsaufruf-Parameter
- Spezialtexte - Festlegungen

Dadurch ist es möglich, ausgewählte Einstellungen von einem System in ein anderes zu übertragen, ohne das Transportsystem nutzen zu müssen. Es ist auch möglich, die Einstellungen vor jeder größeren Änderung zu sichern und evtl. auf ihre vorherigen Werte zurückzusetzen.

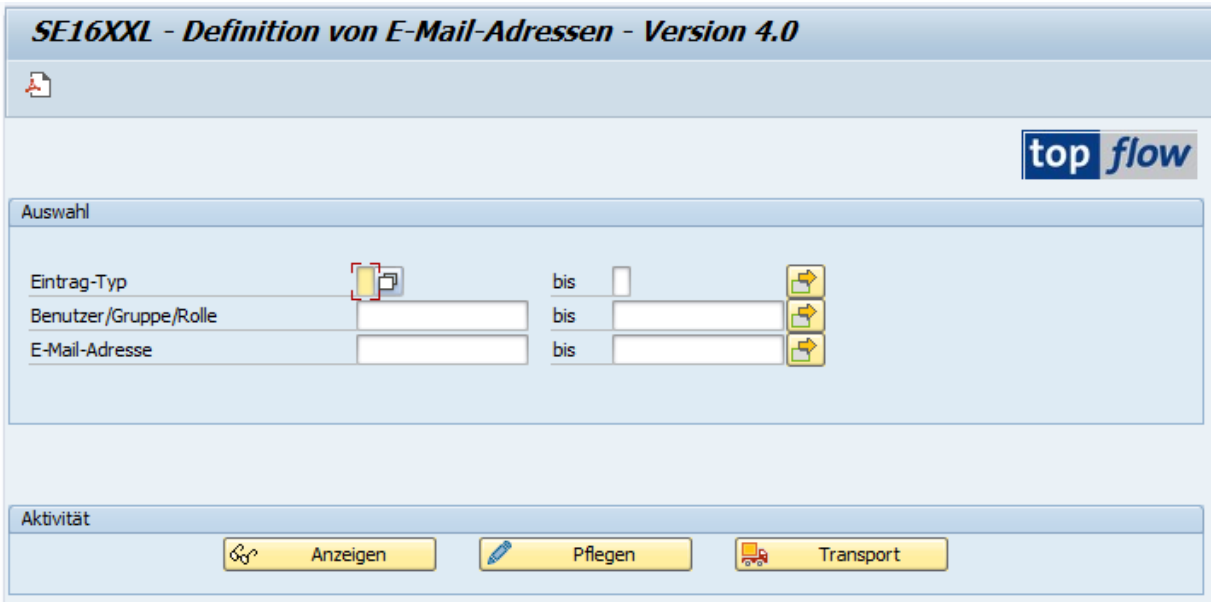
Wir werden nun diese Neuerung anhand eines Beispiels verdeutlichen. Nachdem die Download-/Upload-Funktionalität für alle oben genannten Dialoge ähnlich arbeitet, beschränken wir unser Beispiel auf den Pflegedialog für die erlaubten E-Mail-Adressen.

Beispiel – Erster Teil – Download der Einstellungen

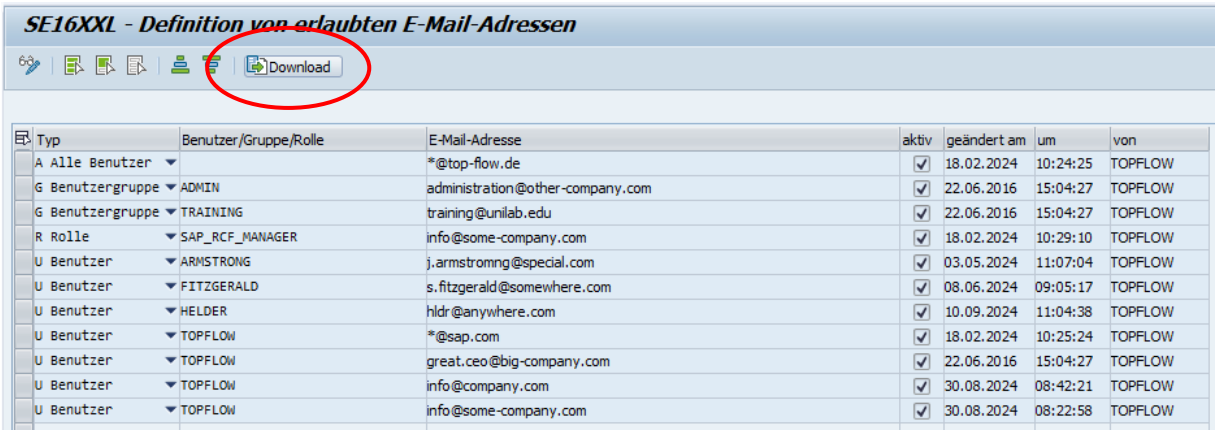
Wir beginnen unser Beispiel mit dem Aufruf der SE16XXL-Einstellungen mit Hilfe des Transaktionscodes **/TFTO/XXL_SETTINGS**:



Nach einem Doppelklick auf E-Mail-Adressen erscheint folgende Startmaske:

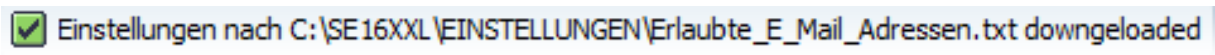


Nun betätigen wir Anzeigen, um die definierten Einträge anzuzeigen:



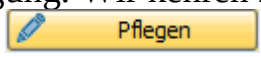
Typ	Benutzer/Gruppe/Rolle	E-Mail-Adresse	aktiv	geändert am	um	von
A Alle Benutzer		*@top-flow.de	☑	18.02.2024	10:24:25	TOPFLOW
G Benutzergruppe	ADMIN	administration@other-company.com	☑	22.06.2016	15:04:27	TOPFLOW
G Benutzergruppe	TRAINING	training@unilab.edu	☑	22.06.2016	15:04:27	TOPFLOW
R Rolle	SAP_RCF_MANAGER	info@some-company.com	☑	18.02.2024	10:29:10	TOPFLOW
U Benutzer	ARMSTRONG	j.armstromng@special.com	☑	03.05.2024	11:07:04	TOPFLOW
U Benutzer	FITZGERALD	s.fitzgerald@somewhere.com	☑	08.06.2024	09:05:17	TOPFLOW
U Benutzer	HELDER	hldr@anywhere.com	☑	10.09.2024	11:04:38	TOPFLOW
U Benutzer	TOPFLOW	*@sap.com	☑	18.02.2024	10:25:24	TOPFLOW
U Benutzer	TOPFLOW	great.ceo@big-company.com	☑	22.06.2016	15:04:27	TOPFLOW
U Benutzer	TOPFLOW	info@company.com	☑	30.08.2024	08:42:21	TOPFLOW
U Benutzer	TOPFLOW	info@some-company.com	☑	30.08.2024	08:22:58	TOPFLOW

Für die Download-Operation muss mindestens ein Eintrag markiert werden. In diesem Beispiel möchten wir alle Einträge herunterladen, daher verwenden wir die Schaltfläche auf der Anwendungsleiste. Jetzt können wir Download betätigen, um die Operation durchzuführen. Nach Auswahl des Verzeichnisses und des Dateinamens führt das Programm den Download durch und gibt dann folgende Meldung aus:

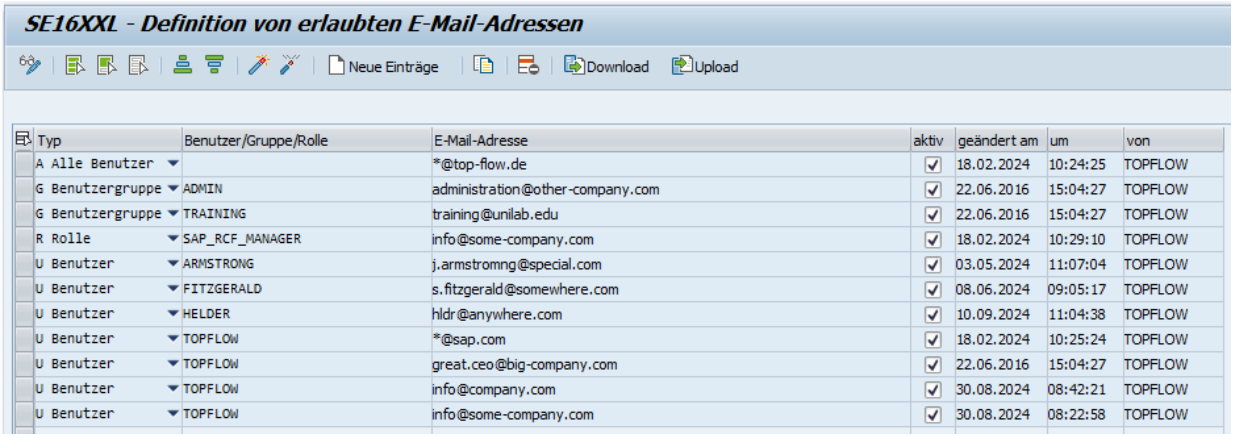


ANMERKUNG: Die Download-Funktion ist auch im **Pflegemodus** verfügbar.

Beispiel – Zweiter Teil – Upload der Einstellungen

Nachdem wir nun eine Download-Datei mit den Einstellungen erstellt haben, können wir die Upload-Funktionalität veranschaulichen. Diese Funktion steht nur im Pflegemodus zur Verfügung. Wir kehren zur Startmaske des Pflegedialogs zurück und betätigen diesmal 

. Die Liste der definierten Einträge erscheint nun in Pflegemodus:

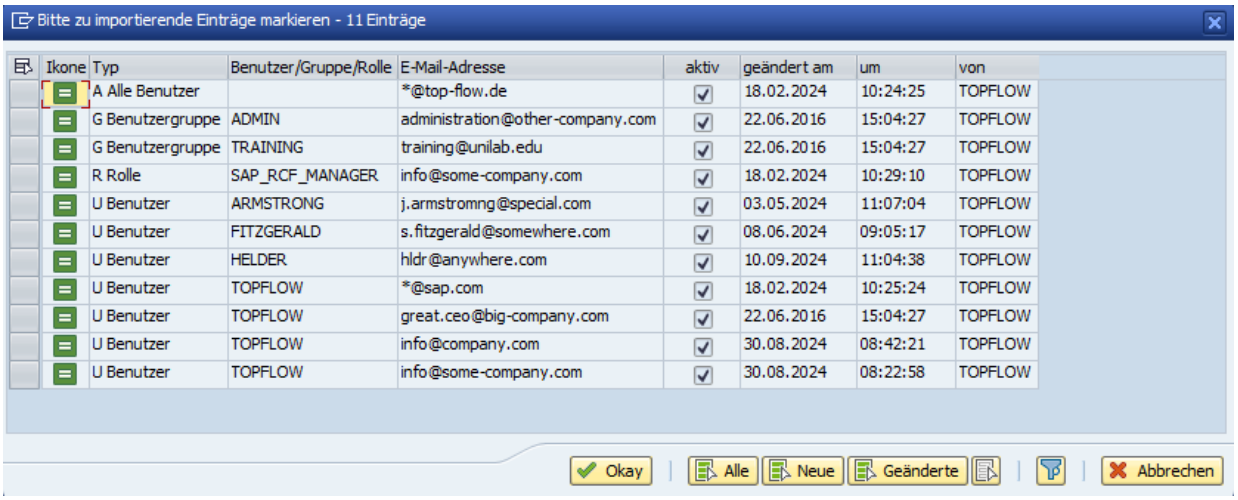


Typ	Benutzer/Gruppe/Rolle	E-Mail-Adresse	aktiv	geändert am	um	von
A Alle Benutzer		*@top-flow.de	☑	18.02.2024	10:24:25	TOPFLOW
G Benutzergruppe	ADMIN	administration@other-company.com	☑	22.06.2016	15:04:27	TOPFLOW
G Benutzergruppe	TRAINING	training@unilab.edu	☑	22.06.2016	15:04:27	TOPFLOW
R Rolle	SAP_RCF_MANAGER	info@some-company.com	☑	18.02.2024	10:29:10	TOPFLOW
U Benutzer	ARMSTRONG	j.armstromng@special.com	☑	03.05.2024	11:07:04	TOPFLOW
U Benutzer	FITZGERALD	s.fitzgerald@somewhere.com	☑	08.06.2024	09:05:17	TOPFLOW
U Benutzer	HELDER	hldr@anywhere.com	☑	10.09.2024	11:04:38	TOPFLOW
U Benutzer	TOPFLOW	*@sap.com	☑	18.02.2024	10:25:24	TOPFLOW
U Benutzer	TOPFLOW	great.ceo@big-company.com	☑	22.06.2016	15:04:27	TOPFLOW
U Benutzer	TOPFLOW	info@company.com	☑	30.08.2024	08:42:21	TOPFLOW
U Benutzer	TOPFLOW	info@some-company.com	☑	30.08.2024	08:22:58	TOPFLOW

Um zu sehen, was passiert, betätigen wir zunächst 

auf der Anwendungsleiste. Dann wählen wir unsere Download-Datei für den Upload aus. Bevor der Inhalt der Datei angezeigt wird, gibt das Programm folgende Meldung aus:

Zum Schluss erscheinen die Upload-Einträge in einem Dialogfenster wie folgt:



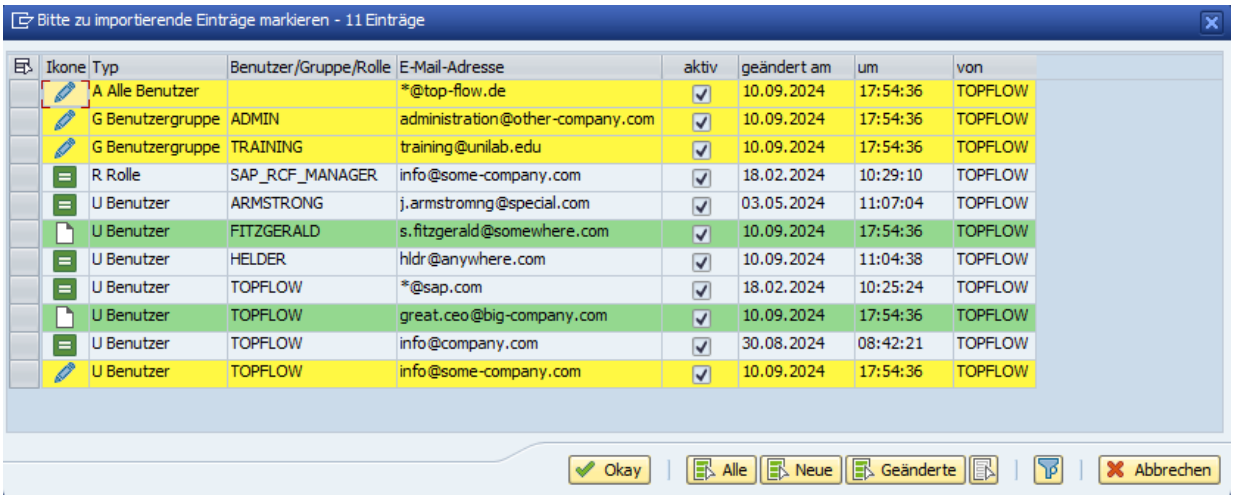
Ikone	Typ	Benutzer/Gruppe/Rolle	E-Mail-Adresse	aktiv	geändert am	um	von
	A Alle Benutzer		*@top-flow.de	☑	18.02.2024	10:24:25	TOPFLOW
	G Benutzergruppe	ADMIN	administration@other-company.com	☑	22.06.2016	15:04:27	TOPFLOW
	G Benutzergruppe	TRAINING	training@unilab.edu	☑	22.06.2016	15:04:27	TOPFLOW
	R Rolle	SAP_RCF_MANAGER	info@some-company.com	☑	18.02.2024	10:29:10	TOPFLOW
	U Benutzer	ARMSTRONG	j.armstromng@special.com	☑	03.05.2024	11:07:04	TOPFLOW
	U Benutzer	FITZGERALD	s.fitzgerald@somewhere.com	☑	08.06.2024	09:05:17	TOPFLOW
	U Benutzer	HELDER	hldr@anywhere.com	☑	10.09.2024	11:04:38	TOPFLOW
	U Benutzer	TOPFLOW	*@sap.com	☑	18.02.2024	10:25:24	TOPFLOW
	U Benutzer	TOPFLOW	great.ceo@big-company.com	☑	22.06.2016	15:04:27	TOPFLOW
	U Benutzer	TOPFLOW	info@company.com	☑	30.08.2024	08:42:21	TOPFLOW
	U Benutzer	TOPFLOW	info@some-company.com	☑	30.08.2024	08:22:58	TOPFLOW

Die Ikone links neben einem Eintrag zeigt an, dass der hochgeladene Eintrag mit dem entsprechenden Eintrag auf dem Computer identisch ist. Solche Einträge können nicht importiert werden, da sie bereits ein identisches Pendant auf dem System haben. Nachdem alle Einträge identisch sind, kann man in diesem speziellen Fall nur die Schaltfläche Abbrechen betätigen.

Um zu zeigen, was passiert, wenn nicht alle Einträge identisch sind, ändern wir an dieser Stelle einige der definierten Einträge und löschen einige andere:

Typ	Benutzer/Gruppe/Rolle	E-Mail-Adresse	aktiv	geändert am	um	von
A Alle Benutzer		*@top-flow.de	☐	18.02.2024	10:24:25	TOPFLOW
G Benutzergruppe	ADMIN	administration@other-company.com	☐	22.06.2016	15:04:27	TOPFLOW
G Benutzergruppe	TRAINING	training@unilab.edu	☐	22.06.2016	15:04:27	TOPFLOW
R Rolle	SAP_RCF_MANAGER	info@some-company.com	☑	18.02.2024	10:29:10	TOPFLOW
U Benutzer	ARMSTRONG	j.armstromng@special.com	☑	03.05.2024	11:07:04	TOPFLOW
U Benutzer	HELDER	hldr@anywhere.com	☑	10.09.2024	11:04:38	TOPFLOW
U Benutzer	TOPFLOW	*@sap.com	☑	18.02.2024	10:25:24	TOPFLOW
U Benutzer	TOPFLOW	info@company.com	☑	30.08.2024	08:42:21	TOPFLOW
U Benutzer	TOPFLOW	info@some-company.com	☐	30.08.2024	08:22:58	TOPFLOW

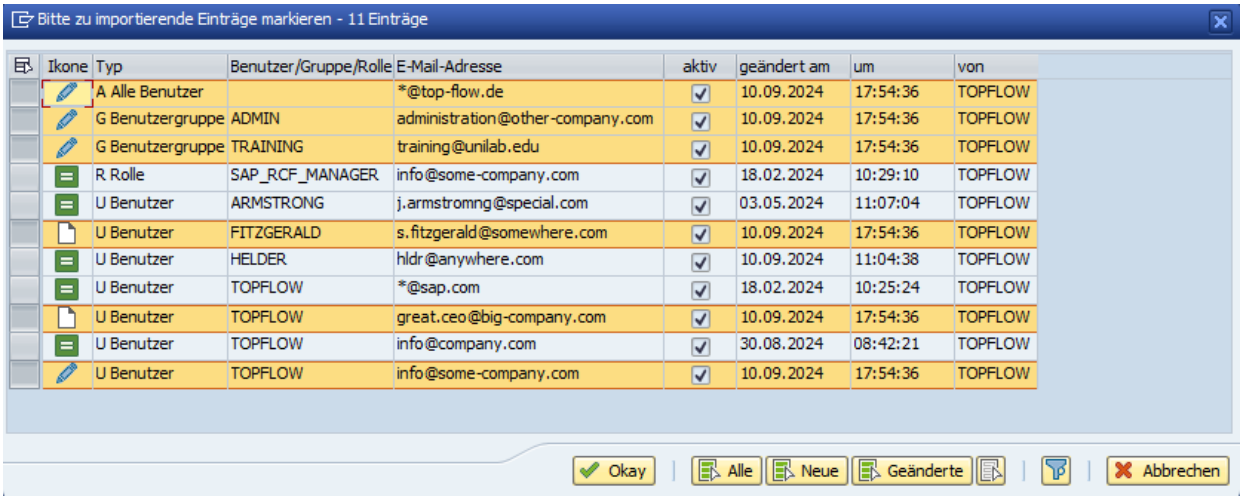
Nun betätigen wir erneut die Schaltfläche Upload auf der Anwendungsleiste. Dieses Mal sind die hochgeladenen Einträge wie folgt:



Die geänderten oder neuen Einträge sind in verschiedenen Farben hervorgehoben. Zusätzlich sind sie mit einer entsprechenden Ikone versehen. Über die folgenden Schaltflächen können Sie die zu importierenden Einträge markieren:

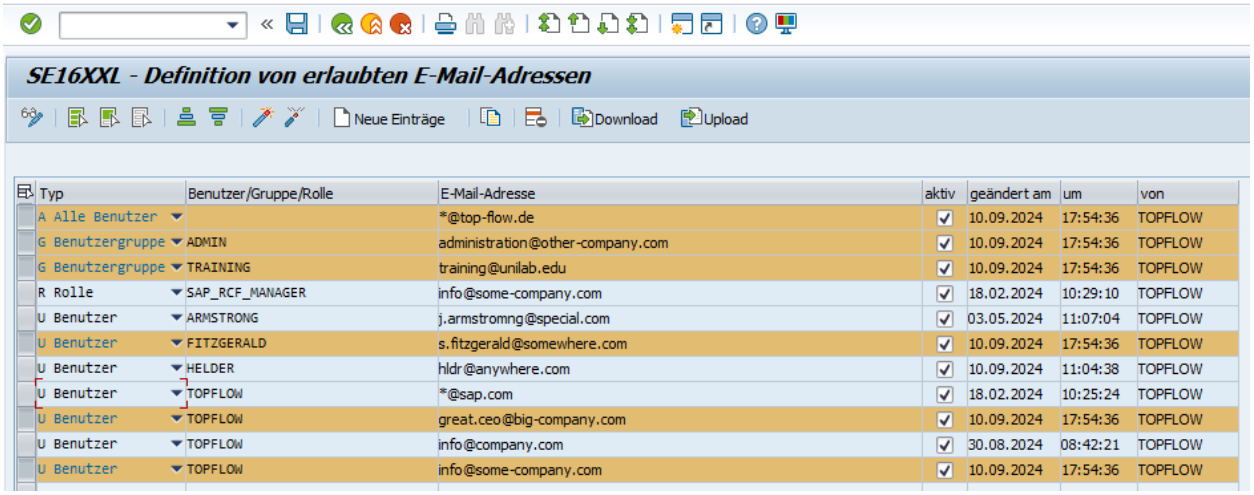
Schaltfläche	Wirkung
Alle	Alle neuen oder geänderten Einträge markieren
Neue	Alle neuen Einträge markieren
Geänderte	Alle geänderten Einträge markieren

In diesem Beispiel betätigen wir Alle und erhalten:



Ikone	Typ	Benutzer/Gruppe/Rolle	E-Mail-Adresse	aktiv	geändert am	um	von
	A Alle Benutzer		*@top-flow.de	☑	10.09.2024	17:54:36	TOPFLOW
	G Benutzergruppe	ADMIN	administration@other-company.com	☑	10.09.2024	17:54:36	TOPFLOW
	G Benutzergruppe	TRAINING	training@unilab.edu	☑	10.09.2024	17:54:36	TOPFLOW
	R Rolle	SAP_RCF_MANAGER	info@some-company.com	☑	18.02.2024	10:29:10	TOPFLOW
	U Benutzer	ARMSTRONG	j.armstromng@special.com	☑	03.05.2024	11:07:04	TOPFLOW
	U Benutzer	FITZGERALD	s.fitzgerald@somewhere.com	☑	10.09.2024	17:54:36	TOPFLOW
	U Benutzer	HELDER	hldr@anywhere.com	☑	10.09.2024	11:04:38	TOPFLOW
	U Benutzer	TOPFLOW	*@sap.com	☑	18.02.2024	10:25:24	TOPFLOW
	U Benutzer	TOPFLOW	great.ceo@big-company.com	☑	10.09.2024	17:54:36	TOPFLOW
	U Benutzer	TOPFLOW	info@company.com	☑	30.08.2024	08:42:21	TOPFLOW
	U Benutzer	TOPFLOW	info@some-company.com	☑	10.09.2024	17:54:36	TOPFLOW

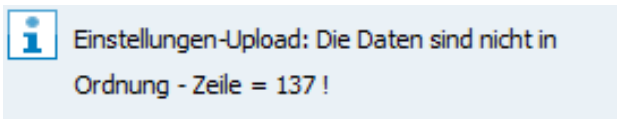
Jetzt können wir die Operation abschließen, indem wir Okay betätigen. Die Liste der definierten Einträge ändert sich entsprechend:



Typ	Benutzer/Gruppe/Rolle	E-Mail-Adresse	aktiv	geändert am	um	von
A Alle Benutzer		*@top-flow.de	☑	10.09.2024	17:54:36	TOPFLOW
G Benutzergruppe	ADMIN	administration@other-company.com	☑	10.09.2024	17:54:36	TOPFLOW
G Benutzergruppe	TRAINING	training@unilab.edu	☑	10.09.2024	17:54:36	TOPFLOW
R Rolle	SAP_RCF_MANAGER	info@some-company.com	☑	18.02.2024	10:29:10	TOPFLOW
U Benutzer	ARMSTRONG	j.armstromng@special.com	☑	03.05.2024	11:07:04	TOPFLOW
U Benutzer	FITZGERALD	s.fitzgerald@somewhere.com	☑	10.09.2024	17:54:36	TOPFLOW
U Benutzer	HELDER	hldr@anywhere.com	☑	10.09.2024	11:04:38	TOPFLOW
U Benutzer	TOPFLOW	*@sap.com	☑	18.02.2024	10:25:24	TOPFLOW
U Benutzer	TOPFLOW	great.ceo@big-company.com	☑	10.09.2024	17:54:36	TOPFLOW
U Benutzer	TOPFLOW	info@company.com	☑	30.08.2024	08:42:21	TOPFLOW
U Benutzer	TOPFLOW	info@some-company.com	☑	10.09.2024	17:54:36	TOPFLOW

ANMERKUNG: Die importierten Einträge sind nur im virtuellen Speicher vorhanden. Um sie in der Datenbank zu haben, müssen Sie auf der Systemleiste betätigen.

WICHTIG: Falls die Download-Datei manipuliert wird (z. B. mithilfe eines Texteditors), gibt das Programm beim Hochladen der Datei eine Meldung wie folgende aus:



Zum Anfang

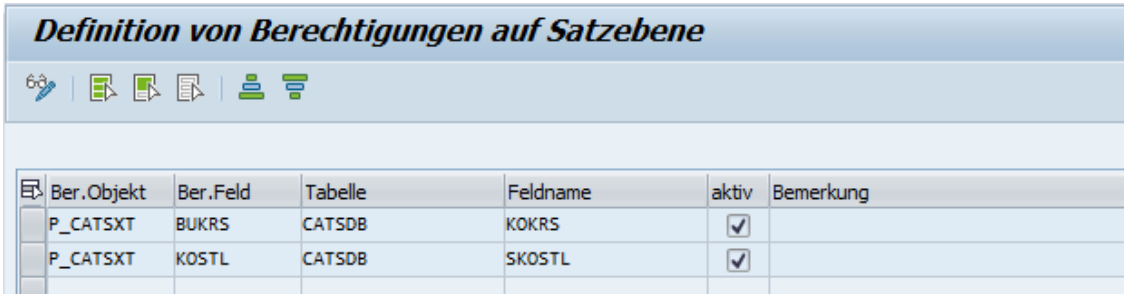
Neue Option für Berechtigungen auf Satzebene

Bisher wurden die **Berechtigungsprüfungen auf Satzebene** nur dann durchgeführt, wenn alle beteiligten Felder **nicht initial** waren. Mit anderen Worten, wenn für einen bestimmten Satz eines oder mehrere der für eine Berechtigungsprüfung definierten Felder **initial waren**, wurde die Prüfung für diesen Datensatz **nicht durchgeführt**. Diese Logik hat lange Zeit gut funktioniert. Es sind jedoch Situationen entstanden, die eine andere Vorgehensweise erfordern. Aus diesem Grund wurde ab Version 4.0 von SE16XXL eine **neue Option** in die Definitionen der Berechtigungen auf Satzebene aufgenommen. Wenn diese Option für ein bestimmtes Feld gesetzt ist, findet die Berechtigungsprüfung eines Datensatzes auch dann statt, **wenn der Feldwert initial ist**.

Ein paar Beispiele werden die Auswirkungen dieser neuen Option verdeutlichen.

Beispiel 1 – Bisheriges Verhalten von SE16XXL

In diesem Beispiel haben wir es mit der Tabelle **CATSDB** (CATS: Datenbanktabelle des Arbeitszeitblattes) zu tun. In den Berechtigungen finden wir folgende Einträge:



Ber.Objekt	Ber.Feld	Tabelle	Feldname	aktiv	Bemerkung
P_CATSXT	BUKRS	CATSDB	KOKRS	☑	
P_CATSXT	KOSTL	CATSDB	SKOSTL	☑	

Diese Definitionen bewirken, dass für jeden selektierten Satz der Tabelle CATSDB eine Berechtigungsprüfung für das Berechtigungsobjekt **P_CATSXT** mit den beiden Feldern **KOKRS** und **SKOSTL** durchgeführt wird. Diese Prüfung wird jedoch nur dann durchgeführt, wenn beide Felder nicht initial sind.

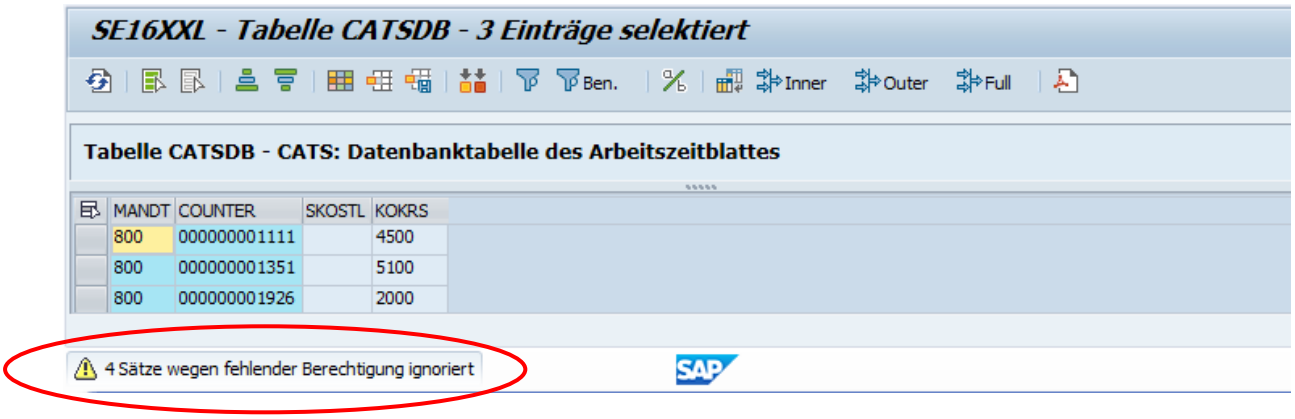
In diesem Beispiel werden folgende Datensätze von CATSDB selektiert:

Tabelle CATSDB - CATS: Datenbanktabelle des Arbeitszeitblattes

MANDT	COUNTER	SKOSTL	KOKRS
800	000000000021	2200	1000
800	000000001111		4500
800	000000001351		5100
800	000000001791	1810	2000
800	000000001801	1814	2000
800	000000001901	2250	2000
800	000000001926		2000

Wie man sehen kann, ist in einigen Datensätzen das Feld **SKOSTL initial**.

In der Annahme, dass die Logon-Kennung der Selektion keine Berechtigung hat, wäre das Ergebnis der Selektion der oben aufgeführten Datensätze wie folgt:

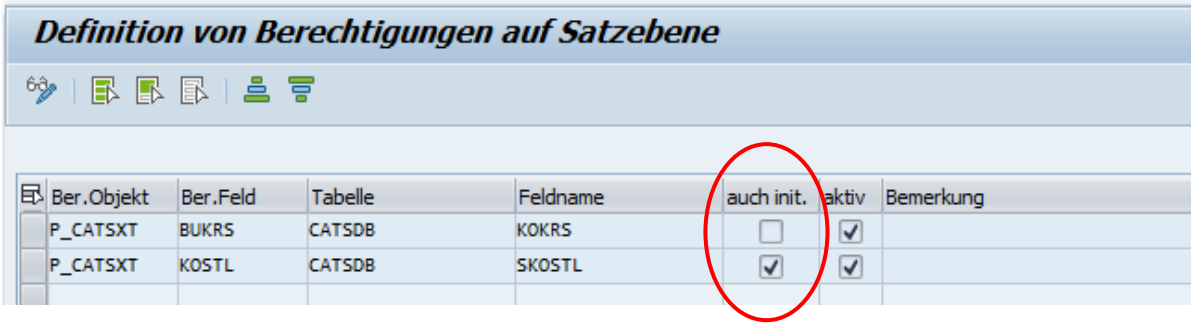


Wie zu erwarten war, wurden die Datensätze mit einem initialen SKOSTL-Wert nicht geprüft und sind daher in der Ergebnisliste vorhanden. Es wurden nur die Datensätze mit nicht initialen Feldern geprüft und mangels Berechtigung verworfen.

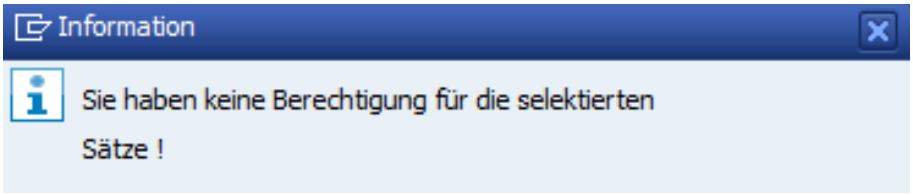
Im nächsten Beispiel zeigen wir, was passiert, wenn die **neue Option** aktiviert wird.

Beispiel 2 – Neue Option aktiviert

In diesem Fall sind die beteiligten Berechtigungseinträge wie folgt definiert:



Für das Feld **SKOSTL** wurde die neue Option "**auch init.**" aktiviert. Das bedeutet, dass nun **auch** dann die Berechtigungsprüfung durchgeführt wird, wenn es sich um ein **initiales** Feld handelt. Findet die Selektion erneut statt, lautet das Ergebnis:



Zum Anfang

Verschiedene Einstellungen auf Rollenebene

Bis dato konnten folgende SE16XXL-Einstellungen

- Erlaubte Server-Datei-Pfade
- Erlaubte E-Mail-Adressen
- Erlaubte RFC-Destinationen

auf drei verschiedenen Ebenen definiert werden:

- Alle Benutzer
- Benutzergruppe
- Benutzer

Dieser Ansatz ist jedoch ungünstig, wenn die definierten Benutzer nicht nach Benutzergruppen, sondern nach zugewiesenen Rollen (sowohl Einzelrollen als auch Sammelrollen) klassifiziert werden.

Um dieser Situation gerecht zu werden, wurden die oben aufgelisteten Pflege-Dialoge neu gestaltet, um **auch Rollen** zu berücksichtigen. Dadurch können die Definitionen nun auf vier Ebenen durchgeführt werden:

- Alle Benutzer
- Benutzergruppe
- Rolle (sowohl Einzel- als auch Sammelrolle)
- Benutzer

Durch die Zuweisung dieser Rollen zu einzelnen Benutzern ist es möglich, sie auf verschiedene Arten zu gruppieren, ohne die gewünschten Einstellungen einzeln festlegen zu müssen.

Weitere Informationen finden Sie in den folgenden Dokumentationen:

Definition von Erlaubten Server-Datei-Pfaden
Definition von Erlaubten E-Mail-Adressen
Definition von Erlaubten RFC-Destinationen.

Zum Anfang

Tool zum Löschen von alten TXBAT-Einträgen

Wenn in SE16XXL ein Script im Hintergrund ausgeführt werden soll, wird die entsprechende Anforderung in die Datenbanktabelle **/TFTO/TXBAT** eingetragen. Das Ergebnis der Scriptausführung wird ebenfalls in diese Tabelle eingetragen. Ältere Hintergrund-Anforderungen und -Ergebnisse sollten von Zeit zu Zeit über die Übersicht der Hintergrund-Jobs gelöscht werden. Diese Art der Reinigung wird jedoch aus verschiedenen Gründen nur selten durchgeführt. Infolgedessen wächst die Anzahl der Einträge der Tabelle /TFTO/TXBAT mit der Zeit und kann, wenn die Hintergrundfunktionalität intensiv genutzt wird, beträchtliche Ausmaße erreichen.

Aus diesem Grund wurde ein **spezielles Tool** entwickelt, um eine große Anzahl von /TFTO/TXBAT-Einträgen **effizient löschen** zu können.

Um das Programm ausführen zu können, werden entweder **Administrationsrechte** benötigt, oder zumindest die Berechtigung, die **globalen Einstellungen** von SE16XXL zu pflegen. Das Programm läuft im **Anzeigemodus**, wenn lediglich die Berechtigung zur Anzeige der globalen Einstellungen vorhanden ist.

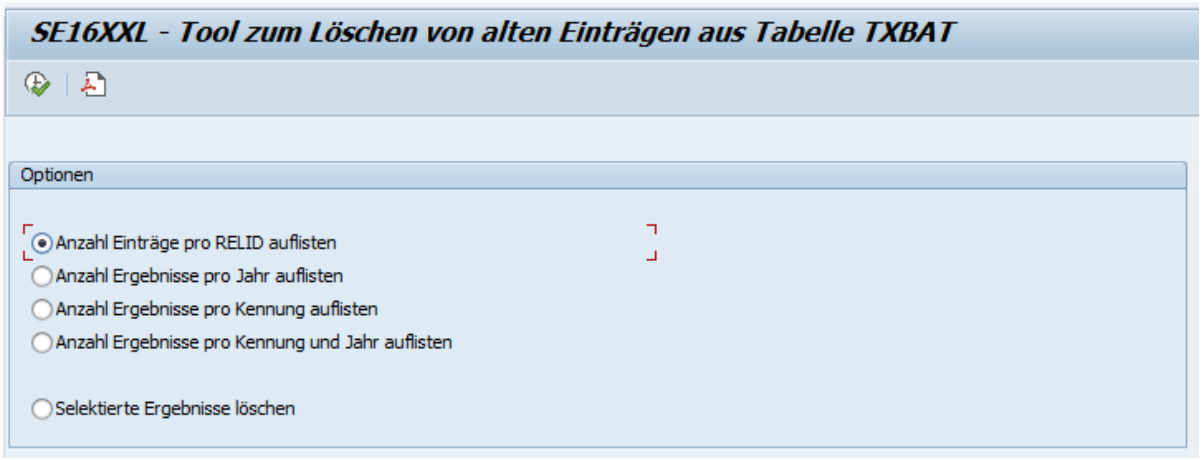
Das Tool kann entweder über die Transaktion SE38 mit dem Programm

/TFTO/TX_PURGE_TXBAT

aufgerufen werden oder durch die Nutzung des Transaktionscodes

/TFTO/PURGE_TXBAT.

Die dazugehörige Selektionsmaske ist recht unspektakulär:



Weitere Infos finden Sie unter Tool zum Löschen von alten TXBAT-Einträgen.

Zum Anfang

Programm zum Befüllen von /TFTO/TBASSOCS

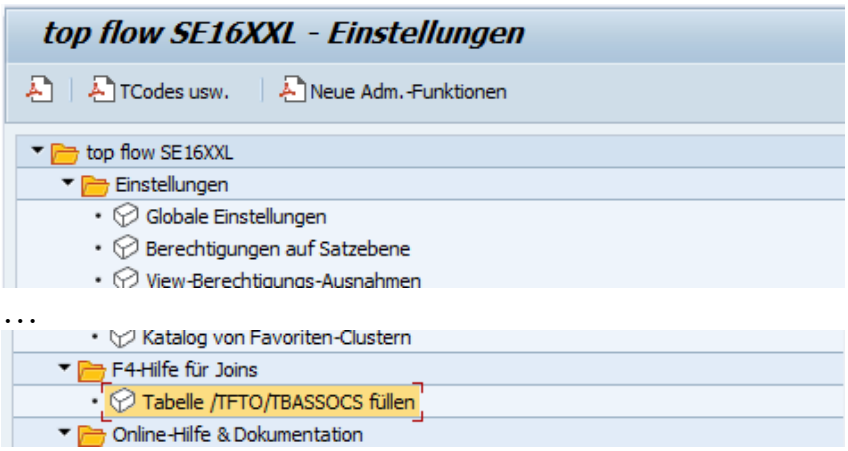
In den neueren Versionen von SAP gibt es sogenannte **DDIC-basierte CDS-Views**, die in einem separaten System (Eclipse) definiert und dann als Definition an das Data Dictionary übergeben werden. Diese CDS-Views enthalten, unter anderem, sogenannte "**Assoziationen**", die über Join-Kriterien zusätzliche Views definieren, die mit der Hauptview verknüpft sind. Die zusätzlichen Felder der Assoziationen können in einer SELECT-Anweisung so selektiert werden, als wären sie Teil der Hauptview selbst. In SE16XXL werden die CDS-View-Assoziationen verwendet, um die Vorschläge für die Wertehilfe für Views zu erzeugen.

Leider ist diese Art von Informationen für Datenbanktabellen nicht verfügbar, da Assoziationen nur als Verknüpfungen zwischen einem CDS-View und anderen Views definiert sind.

Nachdem jedoch DDIC-basierte CDS-Views und normale Views auf Datenbank-tabellen basieren, d.h. die Beziehung zwischen einem gegebenen View und den zugrundeliegenden Datenbanktabellen vollständig bekannt ist, ist es durchaus möglich, aus den View-Assoziationen die entsprechenden Beziehungen zwischen den beteiligten Datenbanktabellen zu extrahieren. Anhand solcher Informationen ist es dann möglich, Vorschläge für die F4-Hilfe für Datenbanktabellen zu erstellen.

Um die oben besprochenen Informationen zur Erstellung von Wertehilfevorschlägen (F4-Hilfe) für Datenbanktabellen nutzen zu können, wurde ein spezielles Programm implementiert, um die zugehörigen Daten aus den View-Assoziationen zu extrahieren.

Dieses Programm ist über die Transaktion **/TFTO/XXL_SETTINGS** zu erreichen:



…

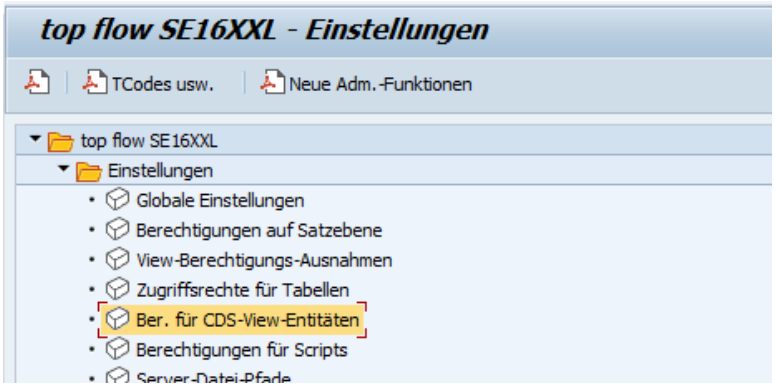
Für weitere Informationen siehe Tabelle /TFTO/TBASSOCS mit Daten befüllen.

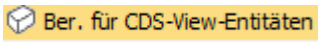
Zum Anfang

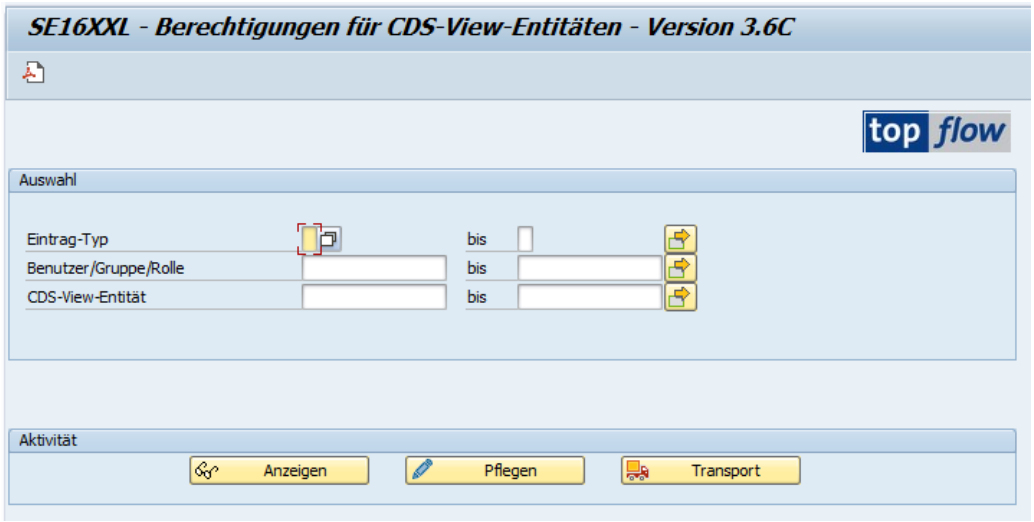
Pflegedialog für Berecht. für CDS-View-Entitäten

SE16XXL unterstützt **CDS-View-Entitäten** ab Version **3.6C**. Für diese Art von Views sind im Gegensatz zu CDS-DDIC-basierten Views **keine Informationen** zu den zugrunde liegenden Datenbanktabellen im Data Dictionary verfügbar.
Aus diesem Grund können die Zugriffsrechte für Tabellen & Felder, die für normale Views verwendet werden, **nicht** auf CDS-View-Entitäten **angewendet werden**. Als Konsequenz wurde ein neuer Mechanismus zur Regulierung des Zugangs zu diesen Views implementiert.

Der zugehörige Pflegedialog ist, wie alle anderen SE16XXL-Einstellungen, über die Transaktion /TFTO/XXL_SETTINGS zu erreichen:



Ein Doppelklick auf  genügt und die vertraute Einstiegsmaske erscheint:



Weitere Informationen finden Sie unter Berechtigungen für CDS-View-Entitäten.

Zum Anfang

Zwei neue Rollen eingeführt

Die erste Rolle ist **/TFTO/XXL_ALV_LAYOUTS_MAINT**. Sie ermöglicht es der damit ausgestatteten Person, den vollen Funktionsumfang des **Tools zur Verwaltung scriptspezifischer ALV-Layouts** zu nutzen. Dieses Tool kann aus der Einstiegs-maske von SE16XXL mithilfe folgender Menüfunktion erreicht werden:

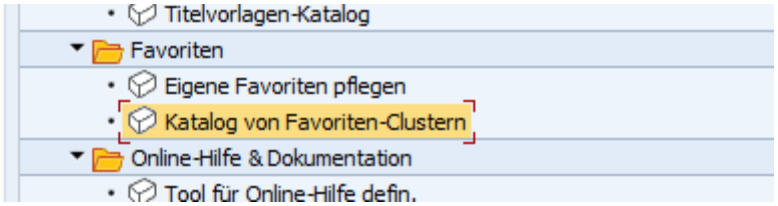
Springen → Scriptspezifische ALV-Layouts …

Anstelle der Rolle ist es möglich, eine Berechtigung für das Berechtigungsobjekt **/TFTO/XALV** mit **ACTVT 70** (verwalten) zu vergeben.

Die zweite Rolle ist **/TFTO/XXL_GLOBAL_FAVS**. Ausgestattet mit dieser Rolle ist es möglich, **globale SE16XXL-Favoriten-Cluster** zu erstellen und zu bearbeiten, wenn der Katalog der Favoriten-Cluster verwendet wird. Dieses Programm kann aus der Einstiegsmaske von SE16XXL mithilfe folgender Menüfunktion erreicht werden:

Favorites → Katalog von Favoriten-Clustern

Es kann auch über die SE16XXL-Einstellungen wie folgt erreicht werden:



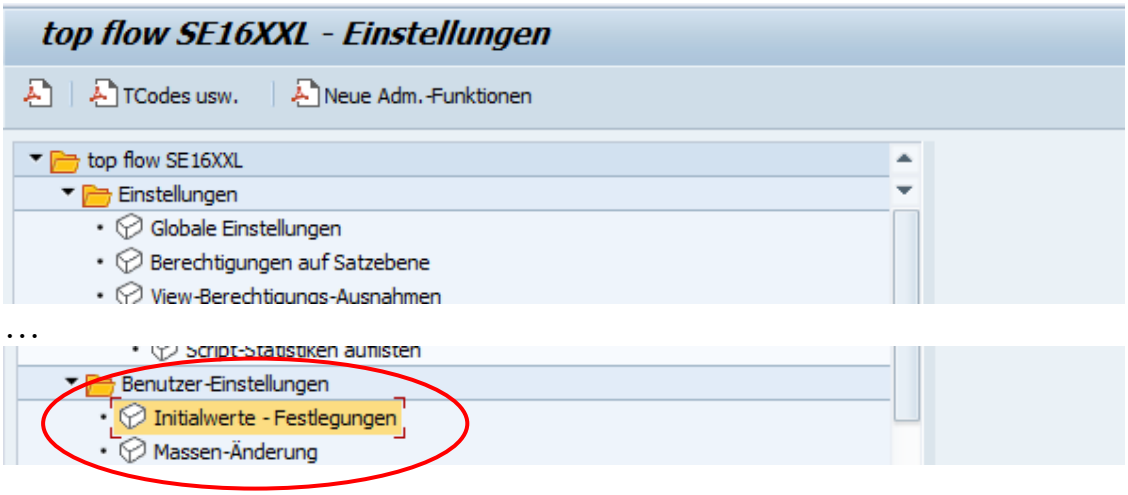
Anstelle der Rolle ist es möglich, eine Berechtigung für das Berechtigungsobjekt **/TFTO/XGLF** mit **Aktivität 23** (Pflege) zu vergeben.

Zum Anfang

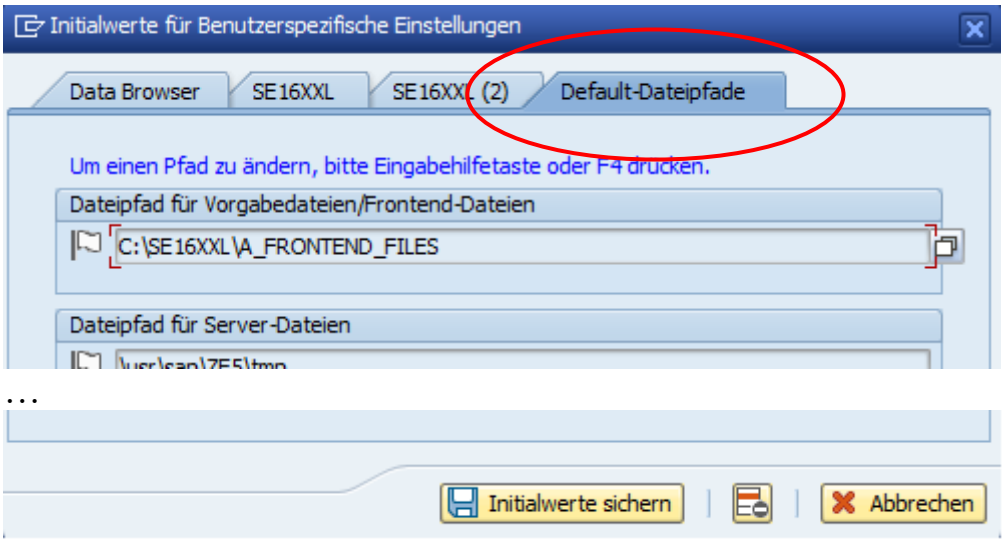
Initialwerte für benutzerspezifische Default-Dateipfade

Die benutzerspezifischen Einstellungen bieten nun eine **vierte Registerkarte** zum Angeben einer Reihe von **Default-Dateipfaden** für die häufigsten Situationen, in denen eine Datei beteiligt ist.

Dadurch wurde auch der zugehörige Dialog auf Administrationsseite erweitert (Transaktion /TFTO/XXL_SETTINGS):



Die vierte Registerkarte hat folgendes Layout:



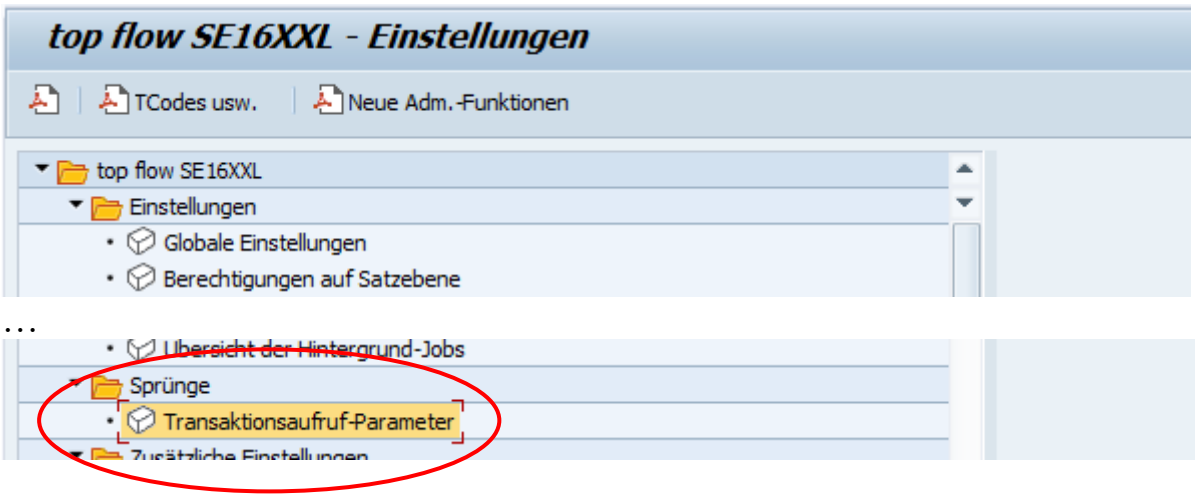
Die Pfadnamen haben eine Ikone ( ) auf der linken Seite, um anzuzeigen, dass es sich um Initialwerte handelt. Sie werden verwendet, wenn keine individuellen benutzerspezifischen Werte definiert wurden.

Zum Anfang

Neue Transaktion zur Anzeige einer Internetseite

Für den Aufruf einer **Internetseite** aus einer SE16XXL-Ergebnisliste mittels "**Sprung**" wurde ein neuer Transaktionscode **(/TFTO/SHOW_URL)** eingeführt.

Wie für alle Transaktionen, die in Sprüngen verwendet werden sollen, ist es notwendig, die **SET/GET-Parameter-IDs** zu definieren, die für die Übergabe von Werten an die Transaktion benötigt werden.
Diese Definition erfolgt in den **SE16XXL-Einstellungen**:

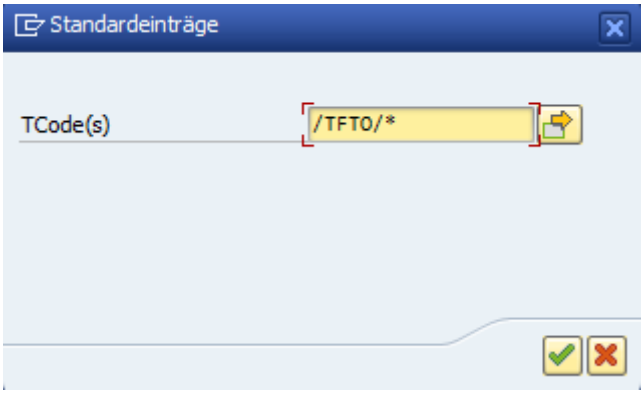


Wenn dieser Definitions-Dialog im **Pflegemodus** aufgerufen wird, ist es möglich, folgende Menüfunktion

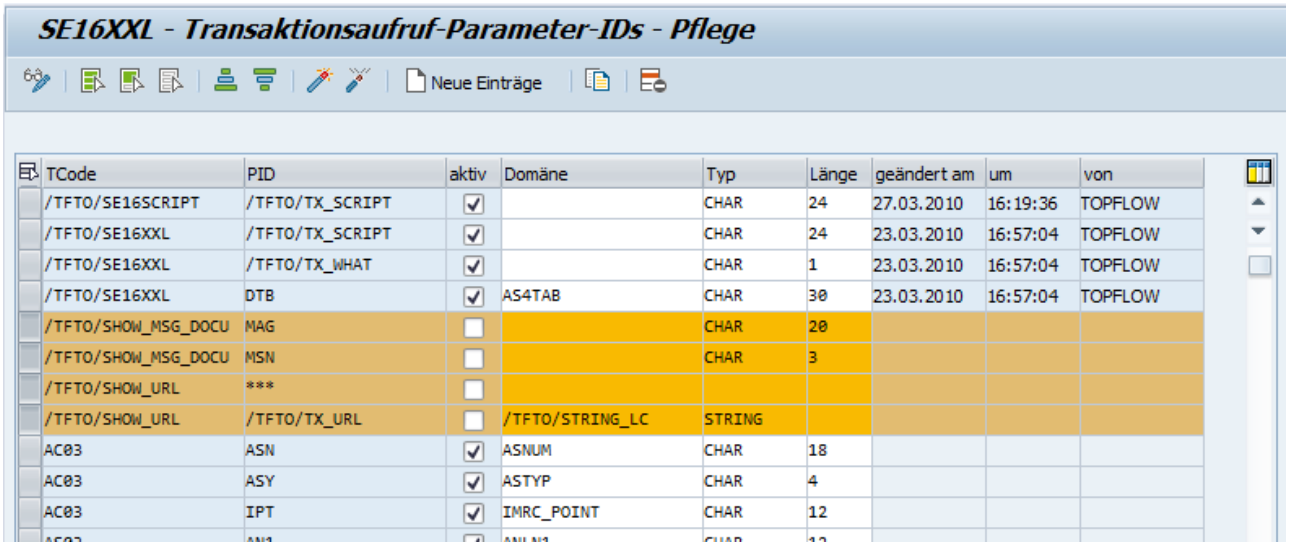
Einträge → Standardeinträge hinzufügen

zu nutzen, um die benötigten Einträge zu den verfügbaren hinzuzufügen.

Da die betreffende Transaktion in diesem Fall zum Namensraum /TFTO/ gehört, empfiehlt es sich, die Standardeinträge wie im folgenden Dialogfenster einzuschränken:

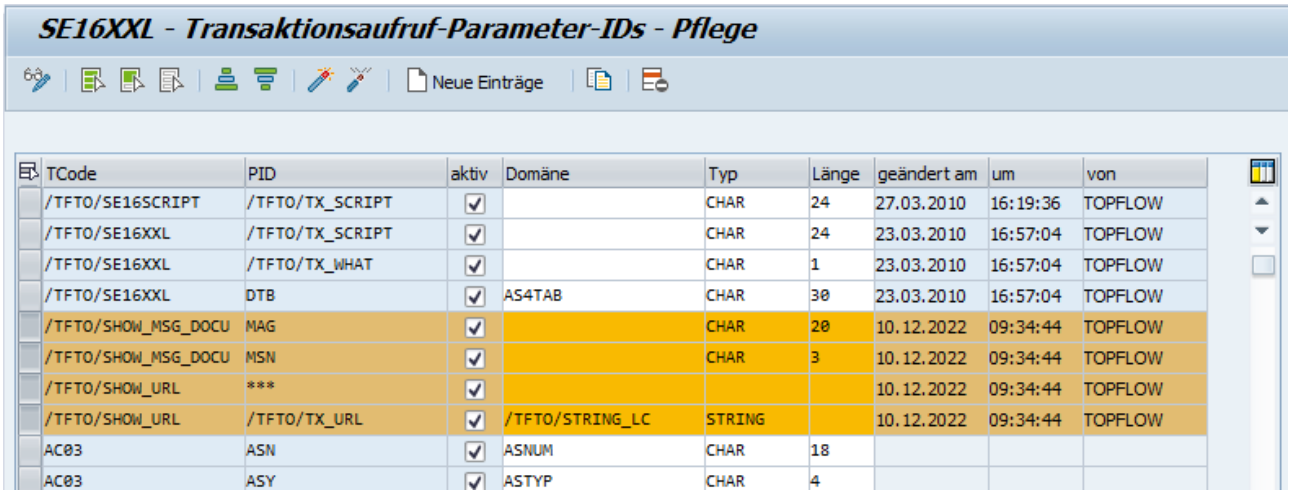


Als Ergebnis werden die gewünschten Einträge zur Liste der verfügbaren Parameter-IDs hinzugefügt:



TCode	PID	aktiv	Domäne	Typ	Länge	geändert am	um	von
/TFTO/SE16SCRIPT	/TFTO/TX_SCRIPT	☑		CHAR	24	27.03.2010	16:19:36	TOPFLOW
/TFTO/SE16XXL	/TFTO/TX_SCRIPT	☑		CHAR	24	23.03.2010	16:57:04	TOPFLOW
/TFTO/SE16XXL	/TFTO/TX_WHAT	☑		CHAR	1	23.03.2010	16:57:04	TOPFLOW
/TFTO/SE16XXL	DTB	☑	AS4TAB	CHAR	30	23.03.2010	16:57:04	TOPFLOW
/TFTO/SHOW_MSG_DOCU	MAG	☐		CHAR	20			
/TFTO/SHOW_MSG_DOCU	MSN	☐		CHAR	3			
/TFTO/SHOW_URL	***	☐						
/TFTO/SHOW_URL	/TFTO/TX_URL	☐	/TFTO/STRING_LC	STRING				
AC03	ASN	☑	ASNUM	CHAR	18			
AC03	ASY	☑	ASTYP	CHAR	4			
AC03	IPT	☑	IMRC_POINT	CHAR	12			

Über die Schaltfläche (“**markierte Einträge aktivieren**”) können die neu eingefügten Einträge aktiviert werden:



TCode	PID	aktiv	Domäne	Typ	Länge	geändert am	um	von
/TFTO/SE16SCRIPT	/TFTO/TX_SCRIPT	☑		CHAR	24	27.03.2010	16:19:36	TOPFLOW
/TFTO/SE16XXL	/TFTO/TX_SCRIPT	☑		CHAR	24	23.03.2010	16:57:04	TOPFLOW
/TFTO/SE16XXL	/TFTO/TX_WHAT	☑		CHAR	1	23.03.2010	16:57:04	TOPFLOW
/TFTO/SE16XXL	DTB	☑	AS4TAB	CHAR	30	23.03.2010	16:57:04	TOPFLOW
/TFTO/SHOW_MSG_DOCU	MAG	☑		CHAR	20	10.12.2022	09:34:44	TOPFLOW
/TFTO/SHOW_MSG_DOCU	MSN	☑		CHAR	3	10.12.2022	09:34:44	TOPFLOW
/TFTO/SHOW_URL	***	☑				10.12.2022	09:34:44	TOPFLOW
/TFTO/SHOW_URL	/TFTO/TX_URL	☑	/TFTO/STRING_LC	STRING		10.12.2022	09:34:44	TOPFLOW
AC03	ASN	☑	ASNUM	CHAR	18			
AC03	ASY	☑	ASTYP	CHAR	4			

Die neuen Einträge sind verfügbar, sobald die Änderungen gesichert werden ( ).

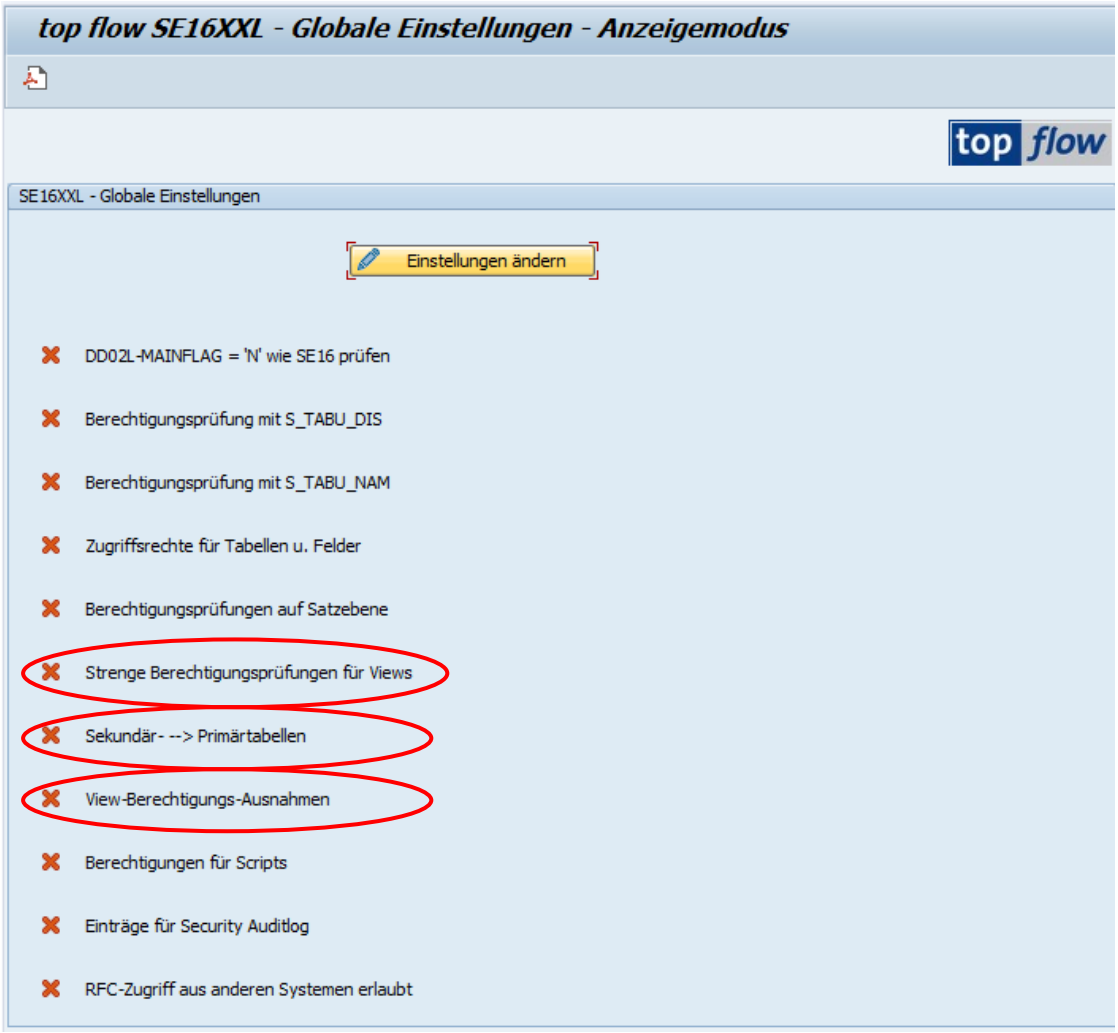
ANMERKUNG: Die Transaktion /TFTO/SHOW_MSG_DOCU kann verwendet werden, um die Langtexte anzuzeigen, die mit Meldungen der Pseudo-Tabelle **$APPLOGS** verknüpft sind.

Zum Anfang

Dialog der Globalen Einstellungen umgestaltet

Mit der Version 3.6 wurden **drei neue globale Einstellungen** auf der Maske des entsprechenden Dialogs hinzugefügt. Diese Maske war jedoch bereits an ihrem Limit, so dass es bei einigen Bildschirmauflösungen notwendig war, nach unten zu scrollen, um einen Überblick über die globale Einstellungssituation zu erhalten. Aus diesem Grund wurde das **Layout** der Maske "Globale Einstellungen" **neu gestaltet**. Der für jede globale Einstellung reservierte Platz ist jetzt viel kleiner, sodass nun alle Einstellungen gleichzeitig sichtbar sind.

Das neue Layout der Maske ist wie folgt (die neuen Einstellungen sind hervorgehoben):



Weitere Informationen finden Sie unter Globale Einstellungen.

Zum Anfang

Berechtigungsprüfungen mit Primärtabellen

Bisher wurden die Berechtigungsprüfungen auf Satzebene für einzelne Datenbanktabellen definiert und von SE16XXL durchgeführt, wenn Datensätze einer dieser Tabellen von den Benutzern selektiert wurden. Dieser Ansatz ist sinnvoll und deckt die wichtigsten Tabellen ab. Das Problem ist jedoch, dass Informationen, die sich auf einen bestimmten Bereich von SAP beziehen, nicht in einer einzigen Datenbanktabelle liegen, sondern auf eine ganze Reihe von Tabellen verteilt sind, die die hierarchische Struktur der Daten repräsentieren. Nur um ein einfaches Beispiel zu nennen, die Kundenaufträge werden nicht nur durch die Tabelle **VBAK** dargestellt, die die Kopfdaten enthält, sondern auch durch **VBAP**, **VBEP**, **VBKD**, **VBUK**, **VBUP** und so weiter. Die wichtigeren Berechtigungsprüfungen können allerdings in der Regel nur mit den Kopfdatensätzen, in diesem Fall VBAK, durchgeführt werden. Diese Logik wird von SAP in den Standardtransaktionen verwendet, die die relevanten Daten intern selektieren und für die Anwender sinnvoll aufbereiten.
In solchen Fällen schützt die Transaktion die Daten vor dem ungeordneten Zugriff. Es ist nicht möglich, auf die Positionen eines Kundenauftrags zuzugreifen, ohne den Kopfsatz zu selektieren und damit die entsprechenden Berechtigungsprüfungen durchzuführen. In SE16XXL ist die Situation anders. Es ist möglich, VBAP-Datensätze zu selektieren, ohne die entsprechenden VBAK-Sätze zu selektieren. Und da die wichtigsten Berechtigungsprüfungen auf der letztgenannten Tabelle durchgeführt werden, ist es möglich, ohne ausreichende Berechtigung auf sensible Daten zuzugreifen.

Bisher bestand die einzige Lösung für dieses Dilemma darin, ausschließlich die Verwendung **vordefinierter Scripts** zuzulassen, die alle notwendigen Datensätze konsistent und geordnet selektieren.

Ab **Version 3.6** von SE16XXL ist es nun möglich, für einzelne Tabellen, die in diesem Zusammenhang als "**Sekundärtabellen**" bezeichnet werden, eine Reihe von "**Primärtabellen**" zu definieren, die durch festgelegte Join-Kriterien mit den ersteren verbunden sind. Wenn Datensätze einer solchen Sekundärtabelle aus der Datenbank selektiert werden, werden **intern** auch die relevanten Datensätze der zugehörigen Primärtabellen **selektiert** und die definierten Berechtigungsprüfungen an diesen Primärdatensätzen durchgeführt. Nur wenn alle Primärdatensätze die Prüfungen bestehen, zeigt SE16XXL den entsprechenden Sekundärdatensatz an. Andernfalls wird der Sekundärdatensatz verworfen.

Weitere Informationen finden Sie unter Sekundär- → Primärtabellen.

Zum Anfang

View-Berechtigungs-Ausnahmen

Bei einer View werden die entsprechenden Berechtigungsprüfungen aus den zugrunde liegenden Datenbanktabellen übernommen. Mit anderen Worten, Views **erben** die Berechtigungsprüfungen von ihren zugrunde liegenden Datenbanktabellen. (Dies gilt nicht für spezielle Berechtigungsprüfungen).

Es gibt allerdings ein Problem mit Views: Eine bestimmte View **enthält nicht unbedingt** alle Felder, die zur Durchführung der definierten Berechtigungs-prüfungen erforderlich sind.

Um einzelnen Benutzern den Zugriff auf bestimmte Views zu ermöglichen, auch wenn ihnen die notwendigen Berechtigungen fehlen, wurde ein spezieller Pflege-Dialog implementiert.

Weitere Informationen finden Sie unter View-Berechtigungs-Ausnahmen.

Zum Anfang

Einschränkungen für F.Codes auf Rollenebene

Bisher konnten die Einschränkungen für Funktionscodes auf drei verschiedenen Ebenen definiert werden:

- Alle Benutzer
- Benutzergruppe
- Benutzer

Dieser Ansatz ist jedoch ungünstig, wenn die definierten Benutzer nicht nach Benutzergruppen, sondern nach zugewiesenen Rollen (sowohl Einzelrollen als auch Sammelrollen) klassifiziert werden.

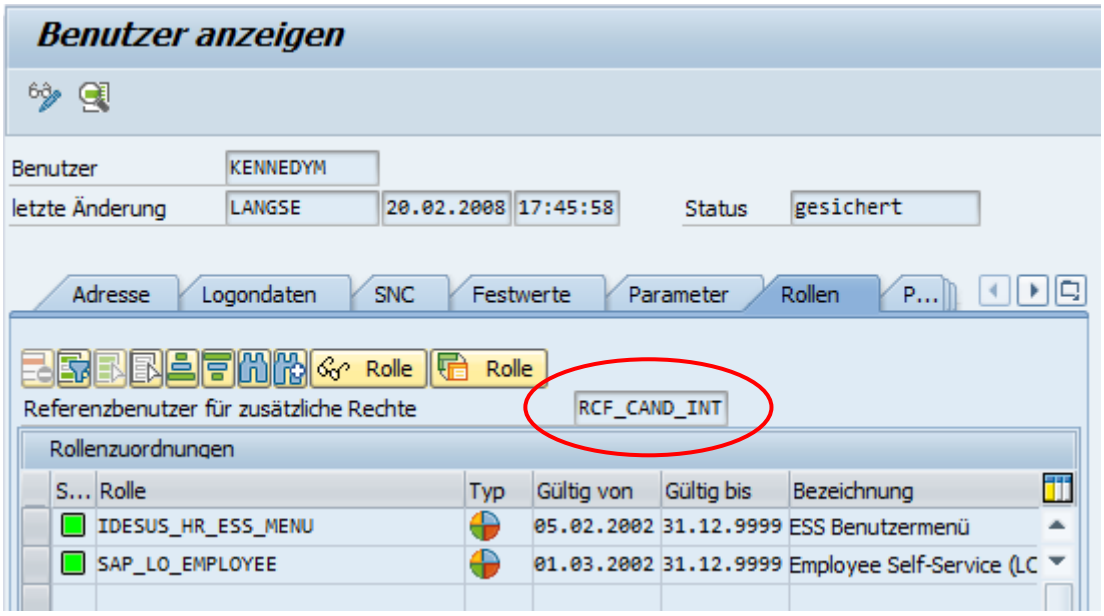
Um dieser Situation gerecht zu werden, wurde der Pflege-Dialog zur Einschränkung der Funktionscodes neu gestaltet, um auch Rollen zu berücksichtigen.
Es ist nun möglich, Funktionscode-Einschränkungen sowohl Einzelrollen als auch Sammelrollen zuzuordnen. Durch die Zuweisung dieser Rollen zu einzelnen Benutzern ist es möglich, sie auf verschiedene Arten zu gruppieren, ohne die gewünschten Einschränkungen für jeden Einzelnen definieren zu müssen.

Weitere Informationen finden Sie unter Einschränkungen für Funktionscodes.

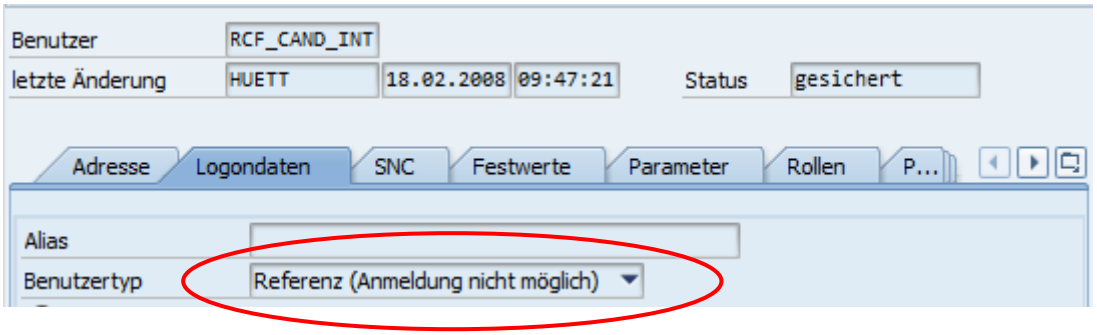
Zum Anfang

Referenzbenutzer berücksichtigt

In der Transaktion **SU01** ist es möglich, einem gegebenen Logon-Benutzer einen sogenannten Referenzbenutzer zuzuordnen. Dies geschieht unter dem Reiter “Rollen” wie im folgenden Beispiel:



Der Referenzbenutzer hat einen speziellen Benutzertyp:



Ab **Version 3.6** von SE16XXL wird der Referenzbenutzer eines Logon-Benutzers berücksichtigt. Das bedeutet, dass alle Rollen, die dem Referenzbenutzer zugewiesen sind, **implizit** auch den Benutzern **zugewiesen** werden, die mit diesem Referenz-benutzer ausgestattet sind.

Zum Anfang

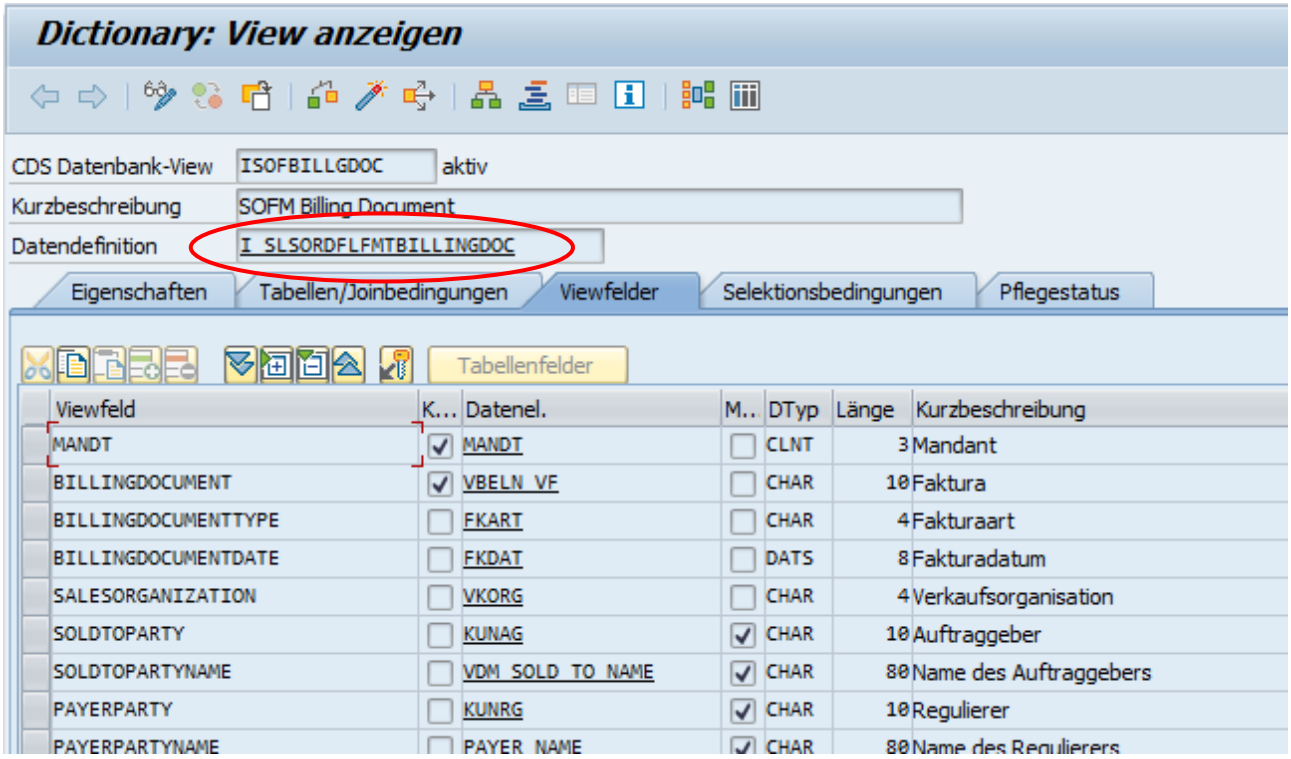
CDS-Views mit ihren Berechtigungsprüfungen

In SE16XXL wurden bisher bei der Selektion der Datensätze einer CDS-View **keine der für die View definierten Berechtigungsprüfungen**, falls vorhanden, intern durchgeführt. Dies lag daran, dass in SE16XXL für die SELECT-Klausel der **Viewname** verwendet wurde, wie er im Data-Dictionary angezeigt wird. Es gibt allerdings einen **anderen Namen** für eine CDS-View, der durch Doppelklick auf den **Datendefinitionsnamen** in der Transaktion SE11 angezeigt werden kann. Wird dieser interne Name in der SELECT-Klausel verwendet, werden die definierten Berechtigungsprüfungen **tatsächlich durchgeführt**. Aus diesem Grund nutzt SE16XXL **ab Version 3.6**, zur Erhöhung der Datensicherheit, immer diesen internen Namen beim Zugriff auf eine CDS-View.

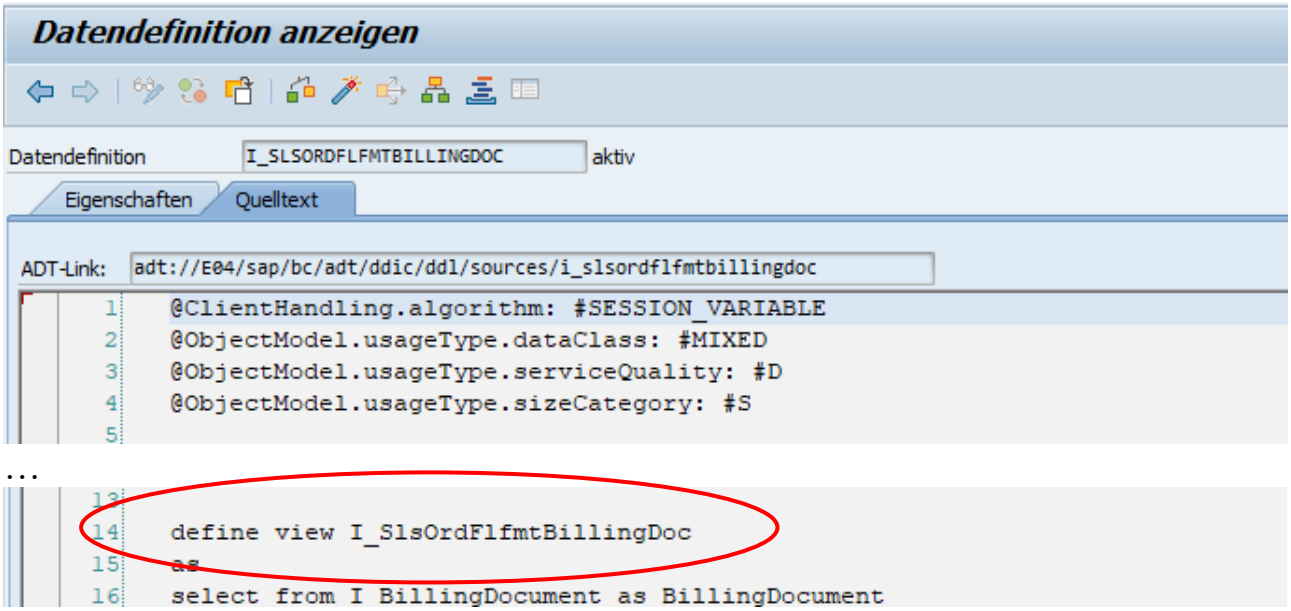
Wir werden diese Situation nun anhand einer echten CDS-View veranschaulichen.

Beispiel mit CDS-View ISOFBILLGDOC

Im Data Dictionary (Transaktion SE11) wird die betreffende CDS-View wie folgt angezeigt:

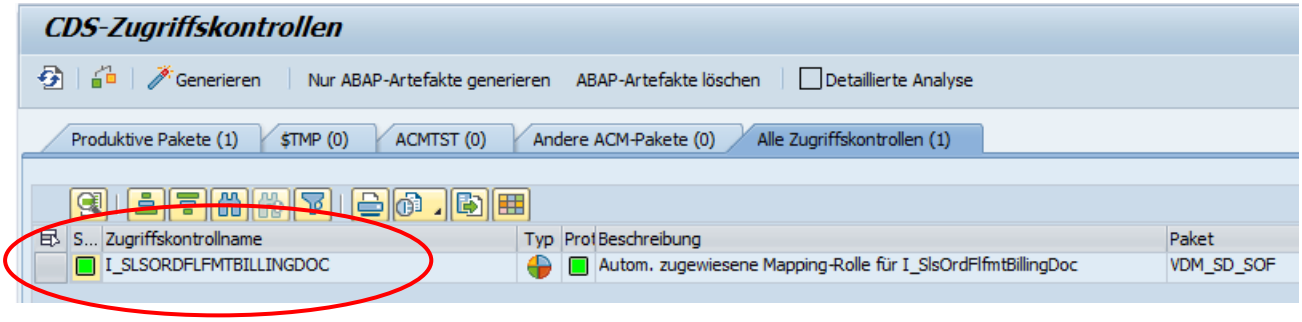


Der oben erwähnte interne Name kann durch Doppelklick auf den **Datendefinitions**-namen **I_SLSORDFLFMTBILLINGDOC** aus der angezeigten Datendefinition der CDS-View ermittelt werden:



ANMERKUNG: In diesem Beispiel sind der Datendefinitionsname und der interne Name identisch. Es gibt jedoch andere CDS-Views, bei denen dies nicht der Fall ist.

Falls die CDS-View über Berechtigungsprüfungen verfügt, können diese mittels der Transaktion **SACMDCLS** entweder anhand des internen Namens oder des Datendefinitionsnamens ermittelt werden:

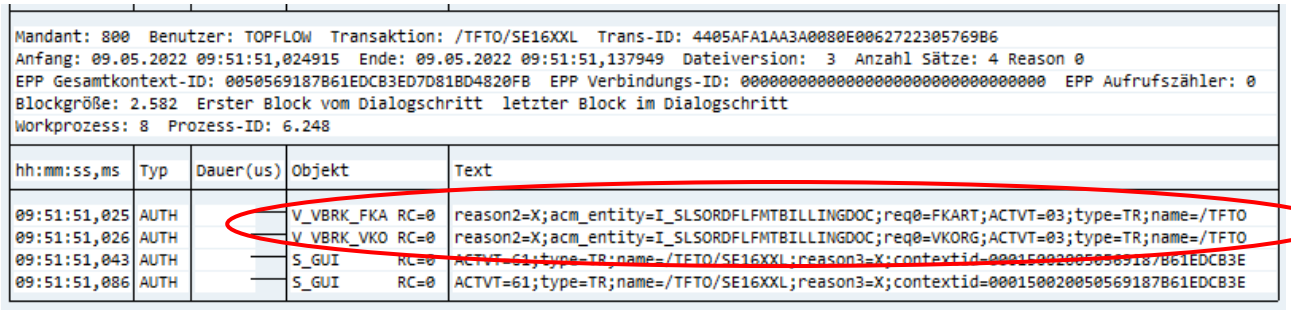


Ein Doppelklick auf den **Zugriffskontrollnamen** zeigt die Definition im Detail an:

```
@EndUserText.label: 'Auto assigned mapping role for I_SlsOrdFlfmtBillingDoc'
@MappingRole: true
define role I_SlsOrdFlfmtBillingDoc {
    grant select on I_SlsOrdFlfmtBillingDoc
    where ( BillingDocumentType ) =
    aspect pfcg_auth (  V_VBRK_FKA,
                        FKART,
                        actvt = '03' )
    and   ( SalesOrganization ) =
    aspect pfcg_auth(  V_VBRK_VKO,
                        VKORG,
                        actvt = '03' )
    ;
}
```

Nachdem wir festgestellt haben, dass in unserer CDS-View einige Berechtigungs-prüfungen definiert sind, selektieren wir einige Datensätze. Zuvor aktivieren wir mithilfe der Transaktion **ST01** den **Systemtrace für Berechtigungsprüfungen**.

Wenn danach die Trace-Einträge angezeigt werden, sind die entsprechenden Berechtigungsprüfungen darin sichtbar:



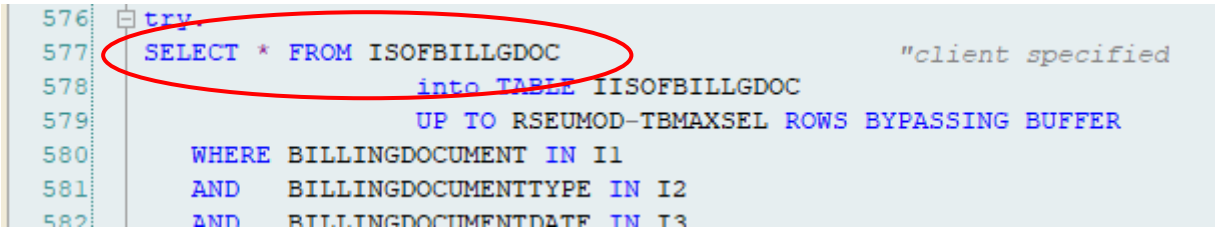
```
Mandant: 800  Benutzer: TOPFLOW  Transaktion: /TFTO/SE16XXL  Trans-ID: 4405AFA1AA3A0080E006272230576986
Anfang: 09.05.2022 09:51:51,024915  Ende: 09.05.2022 09:51:51,137949  Dateiversion:  3  Anzahl Sätze: 4 Reason 0
EPP Gesamtkontext-ID: 005056187B61EDCB3ED7D81BD4820FB  EPP Verbindungs-ID: 00000000000000000000000000000000  EPP Aufrufszähler: 0
Blockgröße: 2.582  Erster Block vom Dialogschritt  letzter Block im Dialogschritt
Workprozess: 8  Prozess-ID: 6.248
```

hh:mm:ss,ms	Typ	Dauer(us)	Objekt	Text
09:51:51,025	AUTH		V_VBRK_FKA RC=0	reason2=X;acm_entity=I_SLSORDFLFMTBILLINGDOC;req0=FKART;ACTVT=03;type=TR;name=/TFTO
09:51:51,026	AUTH		V_VBRK_VKO RC=0	reason2=X;acm_entity=I_SLSORDFLFMTBILLINGDOC;req0=VKORG;ACTVT=03;type=TR;name=/TFTO
09:51:51,043	AUTH		S_GUI RC=0	ACTVT=61;type=TR;name=/TFTO/SE16XXL;reason3=X;contextid=0001500200505691B7B61EDCB3E
09:51:51,086	AUTH		S_GUI RC=0	ACTVT=61;type=TR;name=/TFTO/SE16XXL;reason3=X;contextid=0001500200505691B7B61EDCB3E

ANMERKUNG: Da diese Berechtigungsprüfungen direkt vom System durchgeführt werden und nicht von SE16XXL, wird keine Meldung bezüglich ignorierter Sätze ausgegeben.

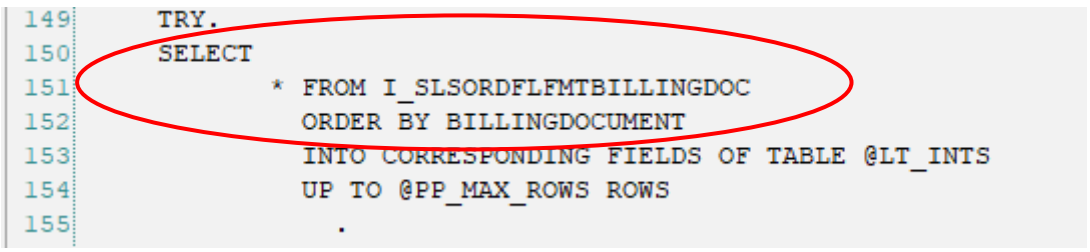
Wird dieselbe Operation mit der Standardtransaktion **SE16** mit dem Namen der CDS-View (**ISOFBILLGDOC**) wiederholt, finden sich im Systemtrace keine solchen Einträge.

Falls wir das Coding des Programms /1BCDWB/DBISOFBILLGDOC inspizieren, das von SE16 generiert wurde, stellen wir fest, dass in diesem Fall der **externe Name der View** in der SELECT-Klausel verwendet wird:



```
576  try.
577  SELECT * FROM ISOFBILLGDOC                    "client specified
578                    into TABLE IISOFBILLGDOC
579                    UP TO RSEUMOD-TBMAXSEL ROWS BYPASSING BUFFER
580     WHERE BILLINGDOCUMENT IN I1
581     AND   BILLINGDOCUMENTTYPE IN I2
582     AND   BILLINGDOCUMENTDATE IN I3
```

Das von SE16XXL generierte Coding hingegen lautet wie folgt:



```
149     TRY.
150     SELECT
151           * FROM I_SLSORDFLFMTBILLINGDOC
152             ORDER BY BILLINGDOCUMENT
153             INTO CORRESPONDING FIELDS OF TABLE @LT_INTS
154             UP TO @PP_MAX_ROWS ROWS
155               .
```

Zum Anfang

Neue Rollen fürs Summieren/Zählen auf der Datenbank

Im Rahmen der neuen Funktionalität der **Summierung/Zählung direkt auf der Datenbank** wurden zwei neue Rollen (und zwei äquivalente **Berechtigungsobjekte**) definiert. Sie sind unten aufgeführt.

Rolle /TFTO/XXL_SCR_DB_SUMS_AUTH

Diese Rolle ermöglicht es dem Benutzer, ein Script mit der Option "***DB-Summen verwenden wenn möglich***" auszuführen, auch wenn für die beteiligten Tabellen Berechtigungsprüfungen aktiv sind.

Erläuterung: Wenn ein Script mit Summierung/Zählung auf der Datenbank ausgeführt wird, enthalten die resultierenden Sätze nur die Felder, die an diesen Summier-/Zähl-Operationen beteiligt sind. Die für die Berechtigungsprüfungen relevanten Felder fehlen in der Regel. Dadurch können von SE16XXL nur die Berechtigungsprüfungen in Bezug auf die verfügbaren Felder vollzogen werden. In den meisten Fällen können überhaupt keine Prüfungen stattfinden. Aus diesem Grund, wenn Berechtigungsprüfungen für die beteiligten Tabellen aktiv sind und der Benutzer keine allgemeine Berechtigung (alle Werte = **'*'**) für diese Prüfungen besitzt, wird die Summierung/Zählung auf der Datenbank nicht durchgeführt.

Das entsprechende **Berechtigungsobjekt** ist **/TFTO/XADB** mit **ACTVT = 16**.

Rolle /TFTO/XXL_SCR_DB_SUMS_SAC

Diese Rolle ermöglicht es dem Benutzer, ein Script mit der Option "***DB-Summen verwenden wenn möglich***" auszuführen, auch wenn für die beteiligten Tabellen **spezielle Berechtigungsprüfungen** aktiv sind.

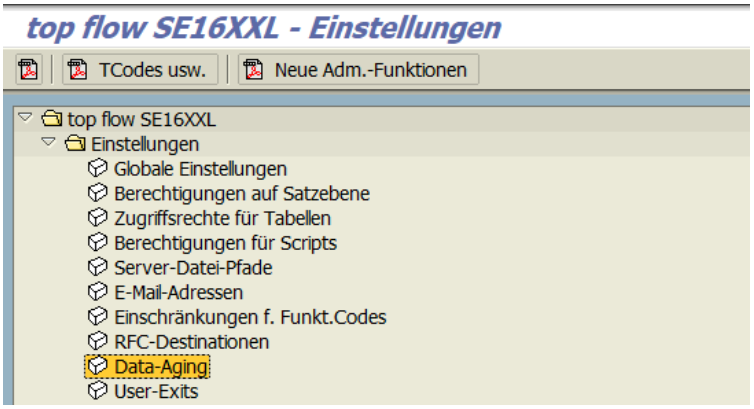
Erläuterung: Wenn ein Script mit Summierung/Zählung auf der Datenbank ausgeführt wird, enthalten die resultierenden Sätze nur die Felder, die an diesen Summier-/Zähl-Operationen beteiligt sind. Die für die speziellen Berechtigungs-prüfungen relevanten Felder fehlen in der Regel. Dadurch können von SE16XXL nur die speziellen Berechtigungsprüfungen in Bezug auf die verfügbaren Felder vollzogen werden. In den meisten Fällen können überhaupt keine speziellen Prüfungen stattfinden. Aus diesem Grund, falls spezielle Berechtigungsprüfungen für die beteiligten Tabellen aktiv sind, wird die Summierung/Zählung auf der Datenbank nicht durchgeführt.

Das entsprechende **Berechtigungsobjekt** ist **/TFTO/XSDB** mit **ACTVT = 16**.

Zum Anfang

Einstellung für Data-Aging-Zugriff

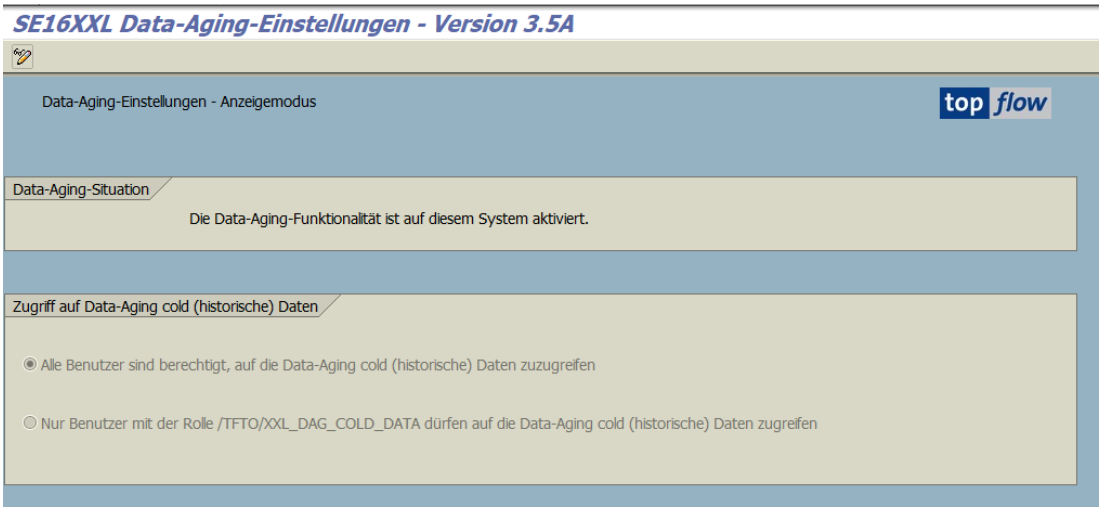
Die Version **3.5A** von SE16XXL unterstützt die **SAP® Data-Aging-Funktionalität**. Das zugehörige Einstellungs-Dialog kann, wie alle anderen Einstellungen, über die Transaktion /TFTO/XXL_SETTINGS erreicht werden:



ANMERKUNG: Dieser Knoten ist nur für Benutzer mit Administratorrechten sichtbar.

Ein Doppelklick auf 

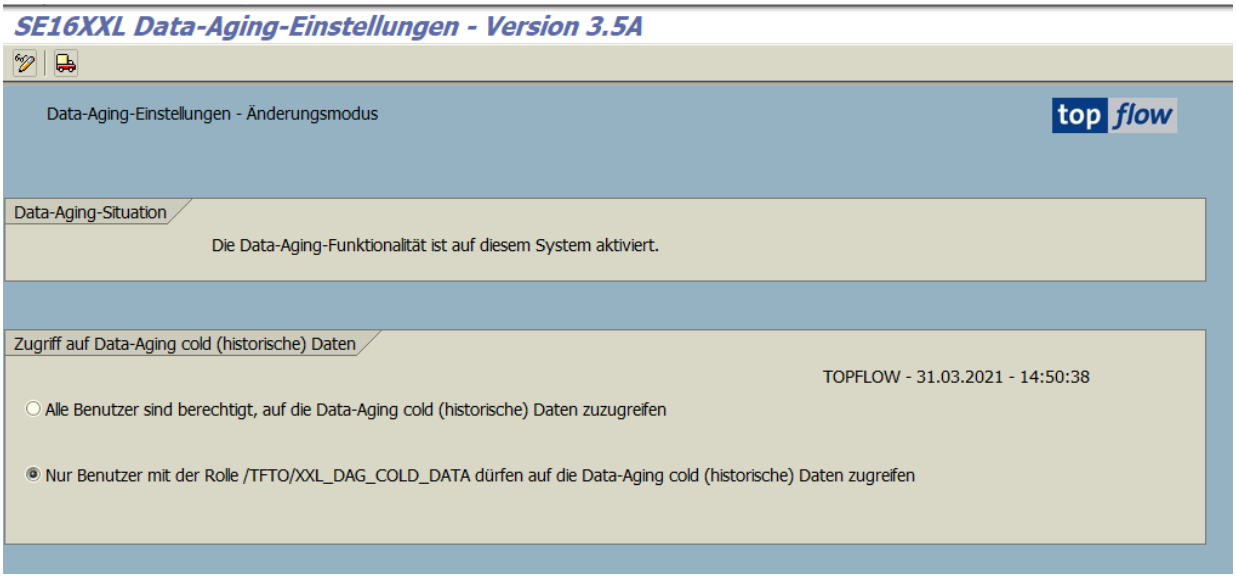
bewirkt, dass das Einstellungs-Dialog angezeigt wird. Wenn Data Aging auf dem System aktiviert ist, stellt sich der Dialog wie folgt dar:



Durch Betätigen der  Taste ist es möglich, in den Änderungsmodus zu wechseln und die Einstellung zu ändern.

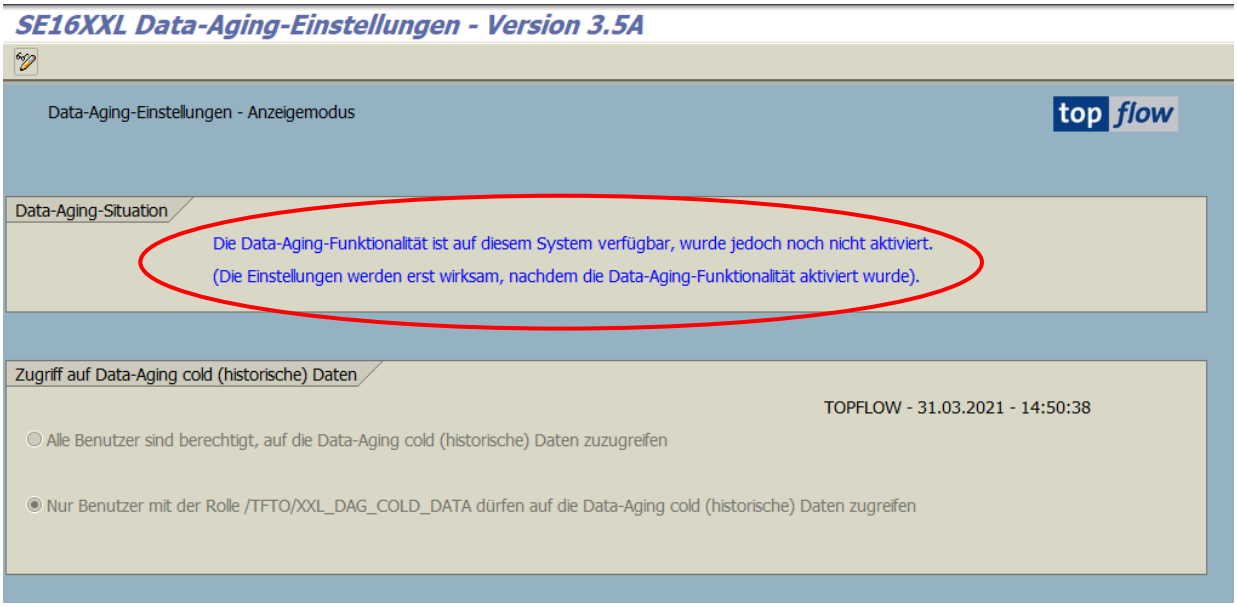
Der Hauptzweck der Data-Aging-Funktionalität besteht darin, die Datenbank zu entlasten. Wenn jeder Benutzer auf die cold (historischen) Daten zugreifen darf, bleibt die Gesamtbelastung der Datenbank wahrscheinlich unverändert. Es erscheint daher vernünftig, den Zugriff auf den historischen Bereich der Datenbank auf einige wenige Benutzer zu beschränken.

Nach der Auswahl der zweiten Option wird der Dialog wie folgt erscheinen:



Von nun an können nur Benutzer, die mit der Rolle **/TFTO/XXL_DAG_COLD_DATA** ausgestattet sind (oder eine entsprechenden Berechtigung besitzen), historische Daten aus der Datenbank selektieren. Alle übrigen Anwender werden nicht einmal mit-bekommen, dass es diese Möglichkeit gibt.

ANMERKUNG: Die Einstellung kann auch vorweg gesetzt werden, falls das Data Aging vom System zwar unterstützt wird, jedoch noch nicht aktiviert wurde.
In einer solchen Situation zeigt der Dialog eine entsprechende Meldung an:



Zum Anfang

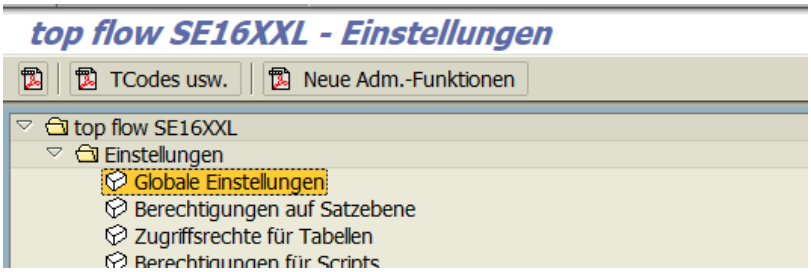
Globale Einstellung für RFC-Zugriff

Ab Version **3.5** ist es in SE16XXL möglich, einen Join mit einer Datenbank-Tabelle durchzuführen, die sich auf einem Remote-SAP-System befindet (**RFC-Selektion**). In Bezug auf Sicherheitsaspekte stehen dem Administrator **zwei Funktionen** zur Verfügung:

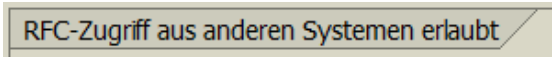
- Eine globale Einstellung, um den RFC-Zugriff auf das System (aus anderen SAP-Systemen) zu gestatten.
- Ein Pflege-Dialog zur Festlegung der erlaubten RFC-Destinationen.

Im vorliegenden Abschnitt werden wir den ersten Punkt, d. h. die globale Einstellung, erörtern.

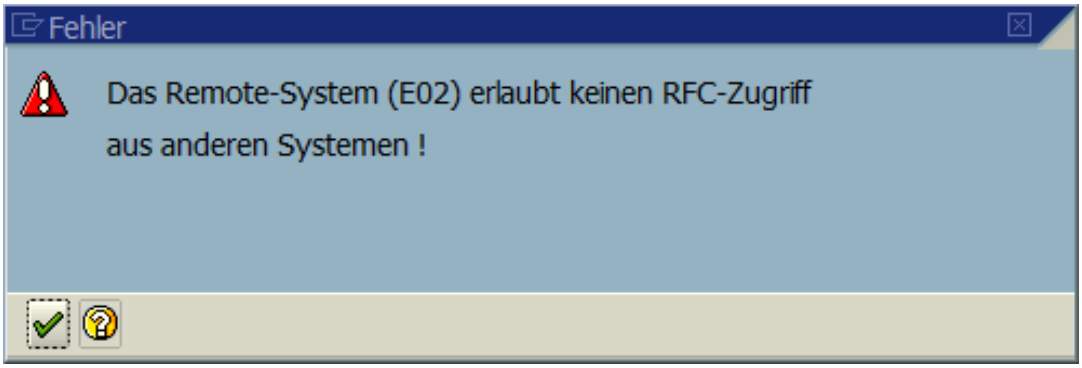
In der Transaktion **/TFTO/XXL_SETTINGS** stellt das oberste Element die globalen Einstellungen dar:



Ein Doppelklick auf  bewirkt, dass folgende Maske ausgegeben wird:

Die Einstellung  ist standardmäßig **deaktiviert**.

Ein Versuch, eine RFC-Selektion mit diesem System als Ziel durchzuführen, wird in diesem Fall mit folgender Fehlermeldung abgewiesen:



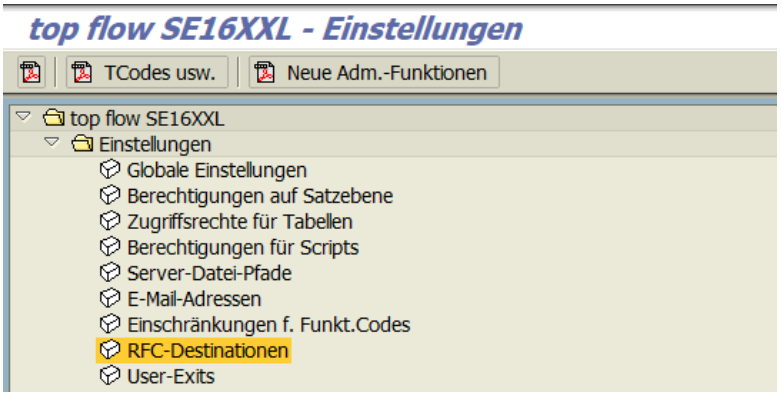
Mit anderen Worten, diese globale Einstellung **schützt** das System vor jeder Art von Fernzugriff mittels SE16XXL.

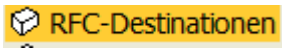
Zum Anfang

Pflege-Dialog für Erlaubte RFC-Destinationen

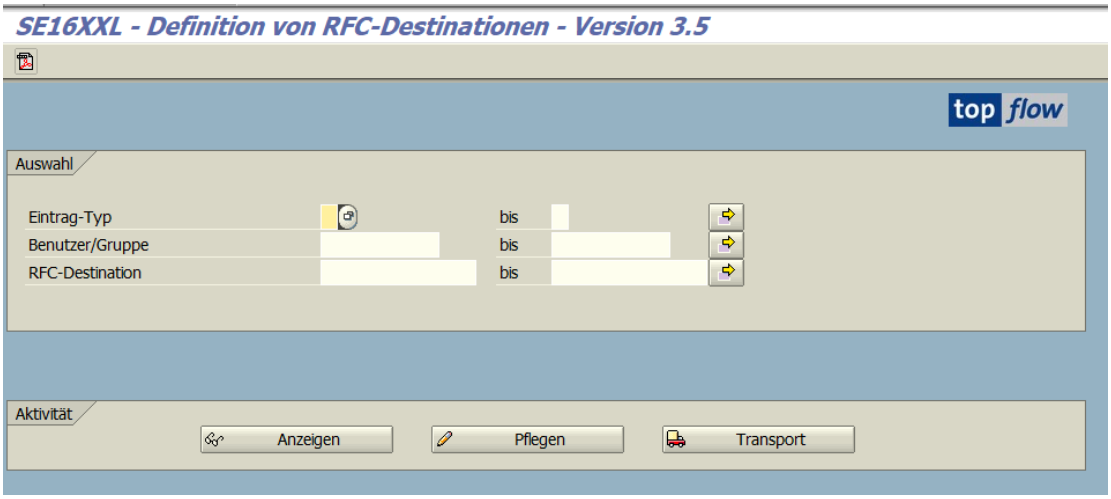
Wie bereits im vorherigen Thema erwähnt, steht dem Administrator ein Pflege-Dialog zur Verfügung, um die RFC-Destinationen zu definieren, welche für die Remote-Selektion mit SE16XXL verfügbar sein sollen. Von den zahlreichen in der Transaktion SM59 definierten RFC-Verbindungen ist in der Regel nur ein Bruchteil für den Einsatz in Kombination mit SE16XXL gedacht. Und es wäre wahrscheinlich keine gute Idee, eine Liste der RFC-Destinationen zu spezifizieren, die von allen Anwendern genutzt werden könnten. Daher wurde ein Pflege-Dialog implementiert, der es ermöglicht, die ausgewählten RFC-Destinationen auf drei Ebenen, **allen Benutzern, Benutzergruppen** und **einzelnen Benutzern** anzugeben.

Der Pflege-Dialog ist, wie alle anderen SE16XXL-Einstellungen, über die Transaktion **/TFTO/XXL_SETTINGS** zu erreichen:



Ein Doppelklick auf 

und die vertraute Einstiegsmaske erscheint:

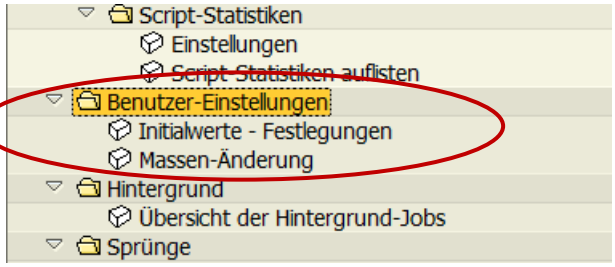


Weitere Informationen finden Sie unter Erlaubte RFC-Destinationen.

Zum Anfang

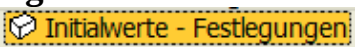
Administration von Benutzer-Einstellungen

Administratoren stehen nun zwei neue Funktionen zur Verfügung, um die benutzer-spezifischen Einstellungen der verschiedenen SE16XXL-Benutzer zu beeinflussen. Sie sind wie folgt im Baum der **SE16XXL-Einstellungen** positioniert:

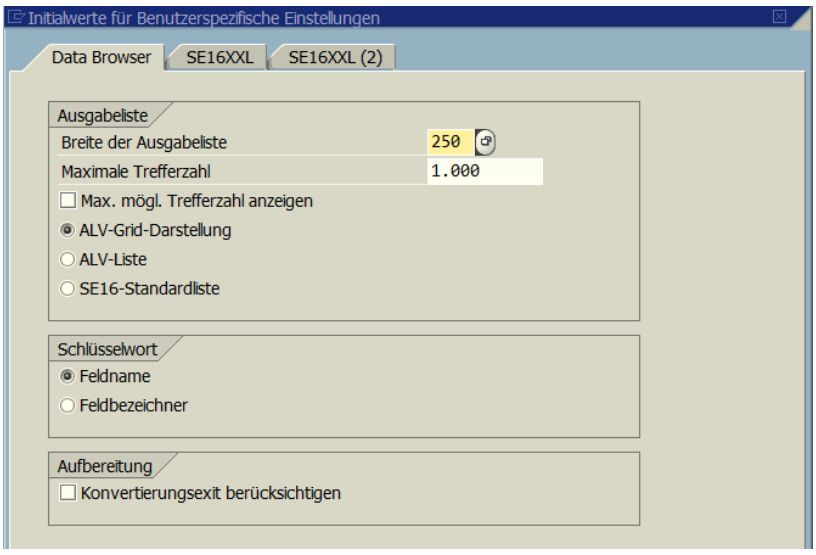


Der Knoten **Benutzer-Einstellungen** und seine Unterknoten sind nur für Benutzer mit Administrationsrechten sichtbar. Für normale Benutzer sind sie unsichtbar.

Erste Funktion – Initialwerte – Festlegungen

Mithilfe dieser Funktion ist es möglich, die Initialwerte für die benutzerspezifischen Einstellungen zu definieren, die für **neu angelegte Benutzer** verwendet werden sollen. Ein Doppelklick auf den Unterknoten 

bewirkt, dass folgendes Dialogfenster angezeigt wird:

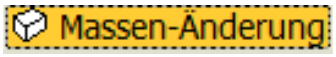


…

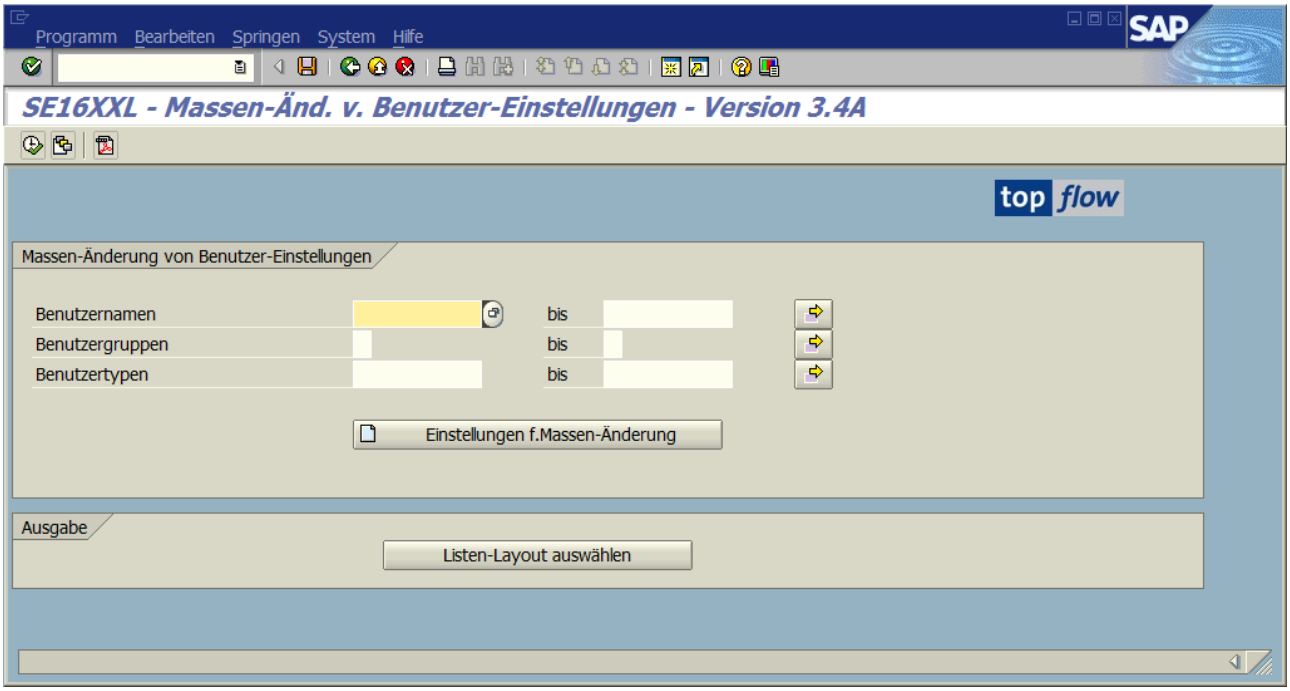
Die hier angegebenen Werte werden verwendet, wenn ein Anwender zum ersten Mal den Dialog für die Benutzer-Einstellungen ( ) aufruft.

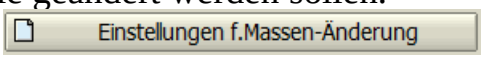
Zweite Funktion – Massen-Änderung von Benutzer-Einstellungen

Diese zweite Funktion wird bereitgestellt, um bestimmte Einstellungen und Optionen von bereits vorhandenen Benutzern ändern zu können. Die "**Maximale Trefferzahl**" könnte z.B. für eine bestimmte Gruppe von Benutzern auf 2000 festgelegt werden.

Nach einem Doppelklick auf 

erscheint die Selektionsmaske des Programms:



Vor der Ausführung des Programms muss der Administrator die benutzerspezifischen Einstellungen und/oder Optionen angeben, die geändert werden sollen.
Dies wird durch Betätigung der Schaltfläche 

bewerkstelligt.

Für mehr Details lesen Sie bitte Massen-Änderung von Benutzer-Einstellungen.

Zum Anfang

Berechtigungen für Standard-ALV-Layouts

SE16XXL-Ergebnislisten werden meistens mithilfe von **ALV-Grid** oder **ALV-List** angezeigt. Dadurch ist es möglich, von **ALV-Layouts** Gebrauch zu machen, um der Liste eine persönliche Note zu verleihen.

ALV ist eine SAP-**Standard**-Funktionalität für die Anzeige von Listen. Sie ist **nicht** Teil des SE16XXL-Add-ons. Auch ALV-Layouts nicht. Sie können dazu verwendet werden, SE16XXL-Ergebnislisten ansprechender zu gestalten, sind aber **nicht** Teil von SE16XXL. Sie werden in Standard-SAP-Tabellen gespeichert, nicht im Namensraum von SE16XXL.

SE16XXL und ALV-Layouts

Die Grundannahme von ALV-Layouts ist, dass ein bestimmter ABAP-Report eine oder mehrere ALV-Listen produziert. Für jede Liste können ALV-Layouts angelegt und später geladen werden. Ein ALV-Layout ist (unter anderem) durch den Namen des **Reports**, den Namen des **Layouts** und ggf. den Logon-Namen des **Anwenders** (im Falle eines Benutzerlayouts) characterisiert. Diese Annahme ist optimal für normale Reports, jedoch **völlig unbrauchbar** für SE16XXL. Warum? Weil in SE16XXL **dasselbe Programm** alle möglichen Ergebnislisten produziert. Wenn man den echten Programm-Namen zum Sichern der ALV-Layouts verwenden würde, würden **sämtlich existierende** SE16XXL-ALV-Layouts bei der F4-Hilfe auftauchen, auch solche, die nichts mit der aktuellen Liste zu tun hätten.

Zum Glück **prüft ALV nicht**, ob der angegebene Report tatsächlich existiert.

SE16XXL fasst ALV-Layouts nach **Struktur der Ergebnisliste** zusammen. Falls z.B. die Ergebnisliste aus einen Join von MARA und MVKE besteht, stehen alle ALV-Layouts für diese Kombination (MARA + MVKE) zum Laden zur Verfügung – und nur diese. Diese Gruppierung (oder Trennung) wird intern durch den **Namen eines Pseudo-Reports** erreicht, der von der Kombination der beteiligten Tabellen abgeleitet wird. In unserem Beispiel wäre der abgeleitete Report-Name **/TFTO/TX~~MARA~MVKE**. Der Report-Name kann bis zu 40 Stellen lang sein. Join-Strukturen können bis zu 20 Tabellen umfassen. Die Logik zum Ableiten des Namens schlägt fehl, falls der Name zu lang wird. Für solche Situationen ist eine spezielle Logik implementiert worden, um eindeutige Report-Namen zu produzieren.

An dieser Stelle muss nochmal betont werden, dass ALV-Layouts **nicht direkt in Verbindung** mit SE16XXL-Scripts stehen. Sie sind stattdessen der Struktur der Ergebnisliste eines Scripts zugeordnet. Wird diese geändert, z.B. durch Einfügen einer zusätzlichen SELECT-Operation, verschwinden die "alten" ALV-Layouts aus der F4-Hilfe des Scripts, um durch neue ersetzt zu werden, sofern es welche für die neue Tabellen-Kombination gibt.

Nach dieser kurzen Einführung können wir zum eigentlichen Thema zurückkehren, den Berechtigungen zum Verwalten von Standard-ALV-Layouts.

Standard-ALV-Layouts (deren Name mit einem Schrägstrich beginnt) stehen allen Benutzern zur Verfügung. Wie bereits erwähnt, werden sie von allen Scripts gemeinsam genutzt, die Ergebnislisten mit derselben Tabellenstruktur erstellen. Dies bedeutet, dass, wenn ein Benutzer ein bestimmtes Standard-ALV-Layout **ändert oder löscht**, **alle Scripts, die dieses Layout verwenden, betroffen sind**. Andere Benutzer, die nach diesem Layout suchen, werden es entweder überhaupt nicht finden oder überrascht sein, dass die Ergebnisliste ein anderes Aussehen hat. Diese Situation entsteht, weil einige Benutzer nicht wissen, dass Standard-ALV-Layouts nicht einem bestimmten SE16XXL-Script zugeordnet sind.
Um die negativen Auswirkungen dieser Situation zu minimieren, wurden zwei neue Rollen eingeführt, um die Anzahl der Benutzer zu begrenzen, die Standard-ALV-Layouts in der SE16XXL-Umgebung ändern oder löschen dürfen. Die neuen Rollen lauten wie folgt:

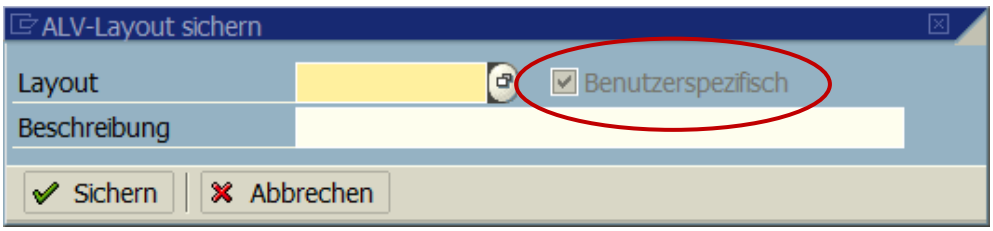
Rolle	Beschreibung
/TFTO/XXL_STD_ALV_LAYOUTS_SAVE	Berechtigung zum Anlegen, Ändern und Uploaden von Standard-ALV-Layouts. Ein Benutzer ohne diese Rolle kann nur seine eigenen benutzerspezifischen Layouts speichern.
/TFTO/XXL_STD_ALV_LAYOUTS_DELE	Berechtigung zum Löschen von Standard-ALV-Layouts. Diese Rolle funktioniert nur in Kombination mit der ersten Rolle, d.h. /TFTO/XXL_STD_ALV_LAYOUTS_SAVE.

In Alternative kann folgendes **Berechtigungsobjekt** verwendet werden:

Rolle	Ber.Objekt	ACTVT
/TFTO/XXL_STD_ALV_LAYOUTS_SAVE	**/TFTO/XALV**	**32**
/TFTO/XXL_STD_ALV_LAYOUTS_DELE	**/TFTO/XALV**	**06**

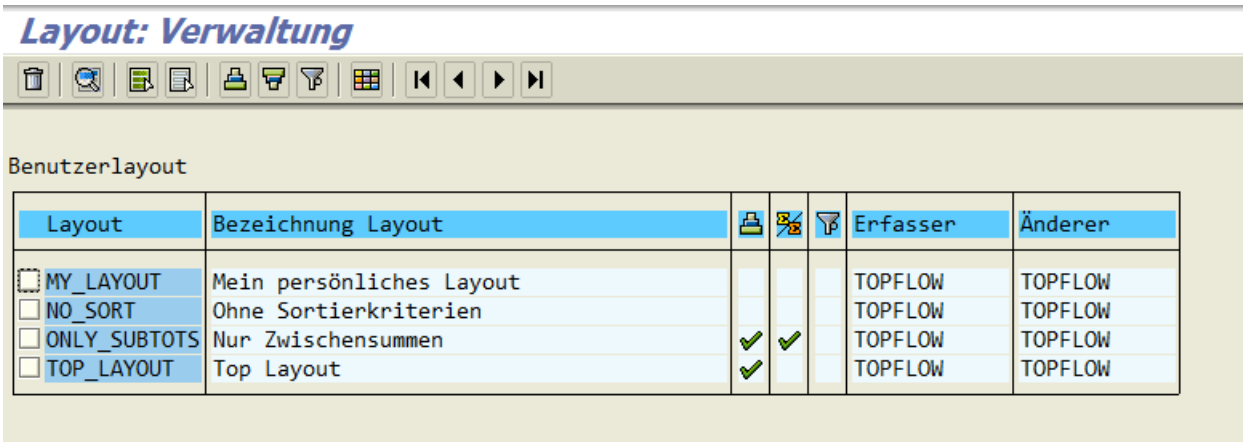
Wirkung von Fehlenden Berechtigungen

Wenn ein Benutzer nicht berechtigt ist, Standard-ALV-Layouts zu sichern, wird das Dialogfenster zum Sichern eines Layouts wie folgt ausgegeben:



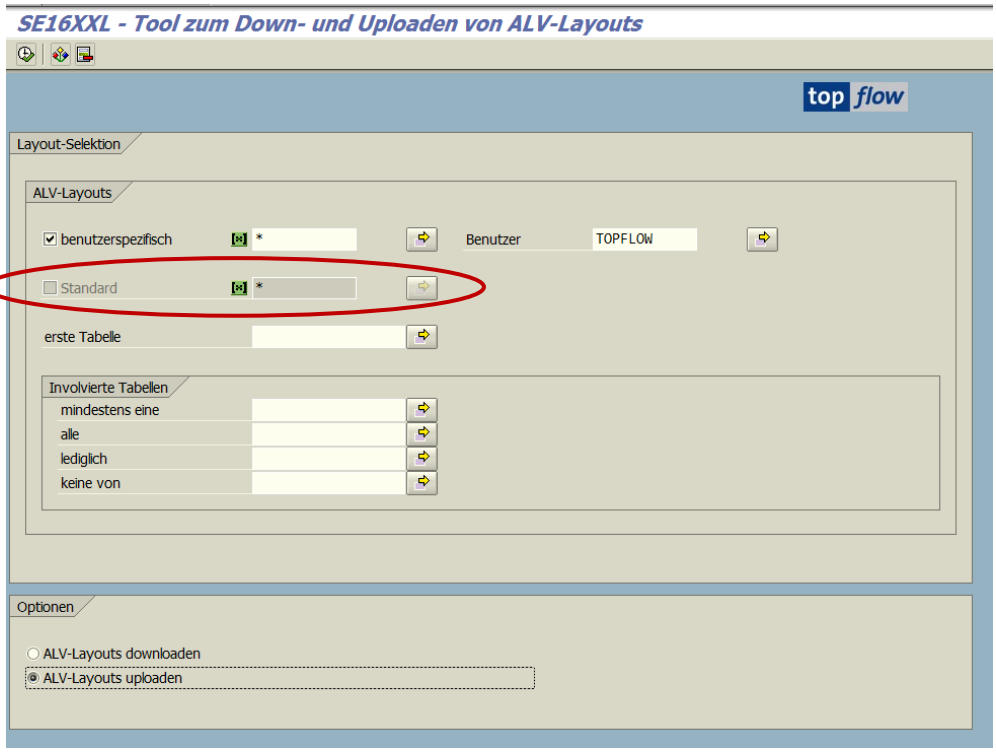
Beachten Sie, dass das Kästchen "Benutzerspezifisch" **aktiviert und geschützt** ist.

Darüber hinaus zeigt die Menüfunktion ***Einstellungen → Layout → Verwalten ...*** die Liste der ALV-Layouts wie folgt, d.h. nur benutzerspezifische Layouts:



Die Menüfunktion ***Einstellungen → Standardlayout*** ist deaktiviert. Somit ist es dem Anwender nicht möglich, Standard-ALV-Layouts zu löschen oder zu importieren.

Schließlich wird das **Tool zum Down- und Uploaden von ALV-Layouts**, das von der Startmaske von SE16XXL über ***Springen → ALV-Layouts …*** gestartet werden kann, folgende Selektionsmaske anzeigen, wenn die Upload-Option aktiviert ist:



Beachten Sie, dass Standard-Layouts **nicht** selektiert werden können.

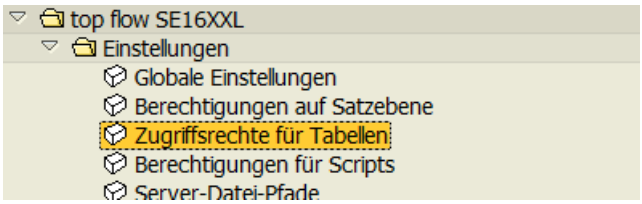
Zum Anfang

Zugriffsrechte für Pseudo-Tabellen

Bis dato konnten Pseudo-Tabellen wie **$CLASSIF** oder **$JOBLOG** beim Definieren der **Zugriffsrechte** in den SE16XXL-Einstellungen nicht direkt angegeben werden. Stattdessen beruhte die Zugriffslogik auf den Datenbanktabellen, auf denen diese Pseudo-Tabellen basieren. Das Problem bei dieser Logik ist, dass es nicht ohne weiteres ersichtlich ist, welche die Basistabelle einer Pseudo-Tabelle ist. Um die Transparenz der Zugriffsrechte zu erhöhen, ist es nun möglich, **Pseudo-Tabellen direkt** anzugeben, jedoch **nur namentlich**, nicht explizit auf Feldebene.
Diese Verbesserung wurde insbesondere mit der Einführung der Pseudo-Tabelle $JOBLOG notwendig, deren Zugriff möglicherweise eingeschränkt werden sollte.

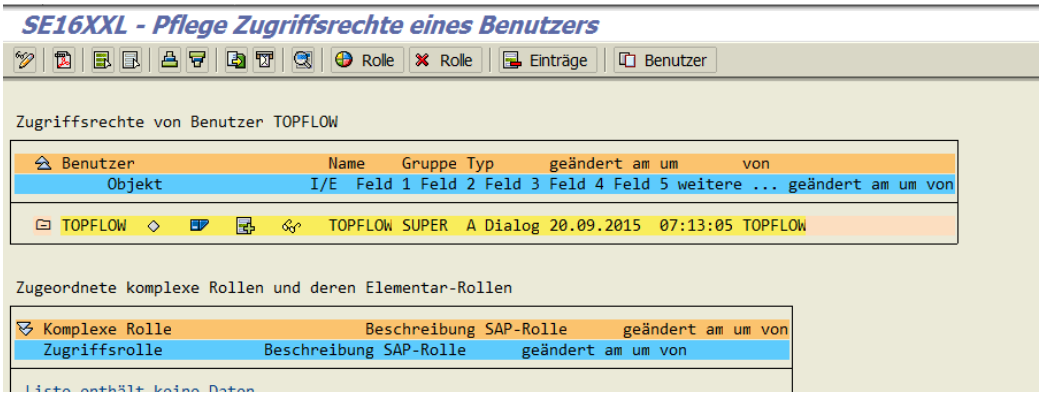
Ein kurzes Beispiel wird diese neue Funktionalität veranschaulichen.

Wir beginnen mit Zugriffsrechte für Tabellen in den SE16XXL-Einstellungen:

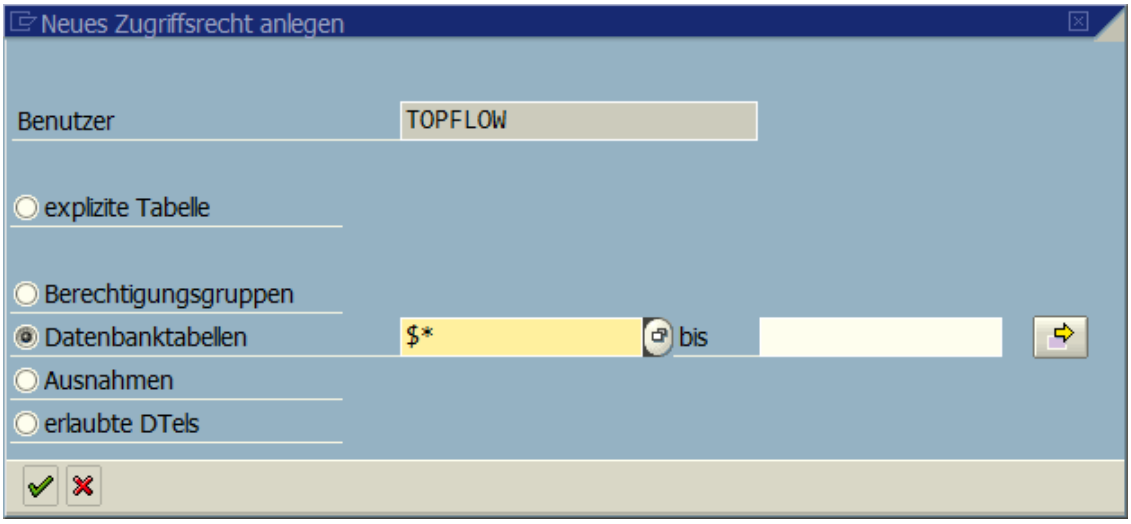


Wir betrachten die Zugriffsrechte des Benutzers TOPFLOW:

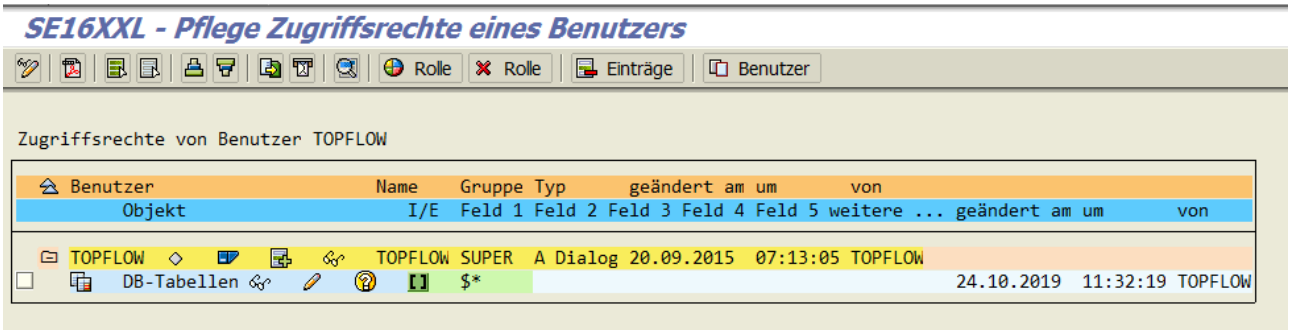
Das Programm zeigt die Details für diesen Benutzer an:



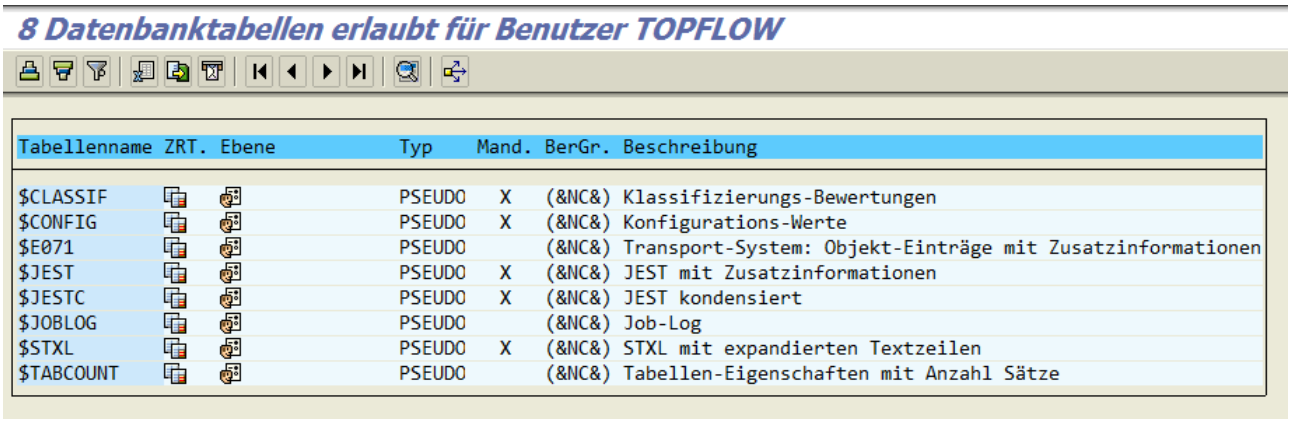
Nun weisen wir dem Benutzer ein Zugriffsrecht (nach Namen) für **alle Pseudo-Tabellen** zu. Da noch keine Rechte dieser Art vergeben wurden, müssen wir auf die Ikone ( ) rechts neben dem Namen des Benutzers klicken. Sämtliche Pseudo-Tabellen beginnen mit einem $-Zeichen:



Die Liste der Details ändert sich entsprechend:



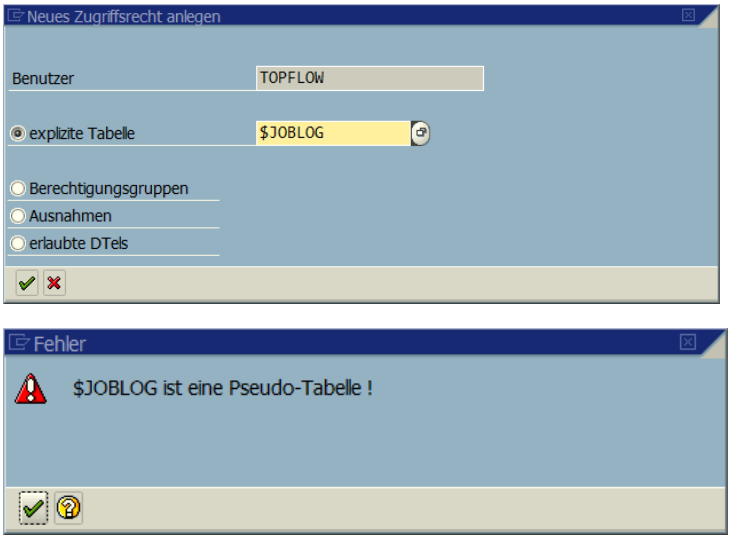
Mithilfe der Menüfunktion ***Funktionen → Alle erlaubten Tabellen auflisten*** können wir überprüfen, ob unsere Zuweisung korrekt war:



Wie erwartet enthält die Liste alle derzeit verfügbaren Pseudo-Tabellen.

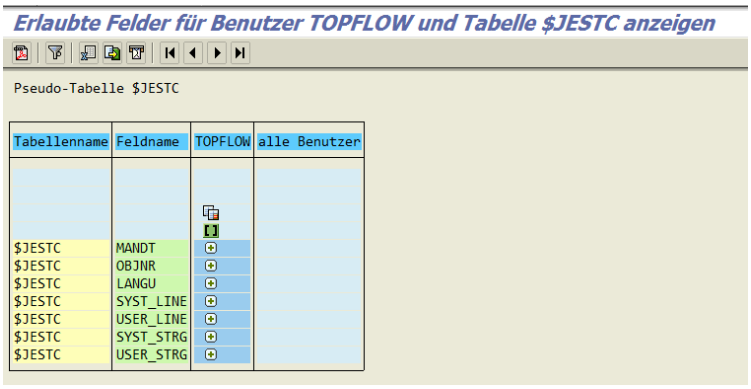
Wie man sich vorstellen kann, kann diese Zuordnung von Pseudo-Tabellen auch für Zugriffsrollen durchgeführt werden, so wie jede andere Datenbanktabelle.

Was nicht möglich ist, ist eine Pseudo-Tabelle explizit zuzuweisen, d.h. auf Feldebene. Wenn wir noch einmal auf die Ikone ( ) rechts neben dem Benutzer klicken und dieses Mal „explizite Tabelle“ auswählen, werden wir feststellen, dass diese Zuordnung nicht erlaubt ist:



Der Grund dafür ist, dass sämtliche Felder einer Pseudo-Tabelle immer erlaubt sind, und es daher nicht sinnvoll ist, zu versuchen, die Zugriffsrechte auf Feldebene zu definieren.

Aus Kompatibilitätsgründen funktioniert die Funktion ***Benutzer & Tabelle/View in Detail*** ( ) jedoch auch für Pseudo-Tabellen:



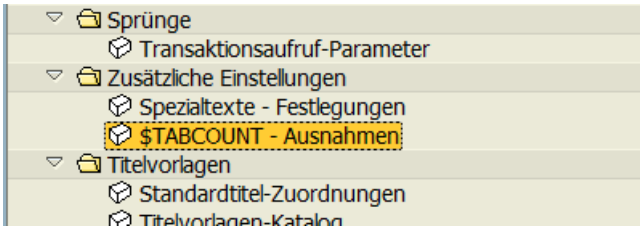
ANMERKUNG: Die bisherige Logik mit der Basistabelle der Pseudo-Tabelle ist weiterhin gültig. Findet das Programm kein Zugriffsrecht für die Pseudo-Tabelle selber, schaltet es automatisch auf die alte Logik um.

Zum Anfang

Pflege-Dialog für $TABCOUNT-Ausnahmen

Wie bereits in Bezug auf Pseudo-Tabelle **$TABCOUNT** erwähnt wurde, gibt es im System Datenbanktabellen und Views, die nicht einfach gezählt werden können, da jeder Versuch, die Datensätze zu zählen, selbst mit einer sehr niedrigen Obergrenze, zu **extrem langen Laufzeiten** führt. Dieses ungewöhnliche Verhalten kann leider nicht von vornherein erkannt werden. Es ist deshalb notwendig geworden, eine **Tabelle von Ausnahmen** zu implementieren. Diese Tabelle wird nur mit wenigen Einträgen ausgeliefert, kann jedoch vom Administrator jederzeit erweitert werden, wenn ähnliche Fälle bekannt werden.

Die Position des neuen Pflege-Dialogs in den SE16XXL-Einstellungen ist wie folgt:



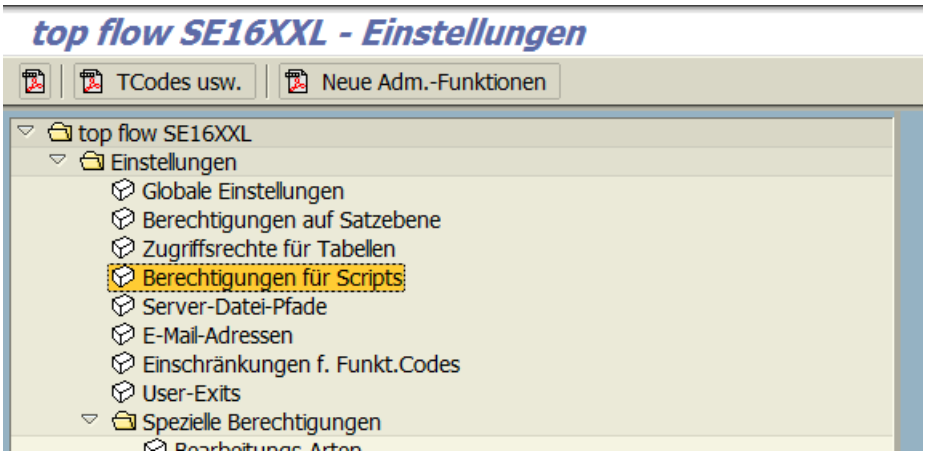
Ein Doppelklick auf  führt zu folgender Selektionsmaske:

Weitere Informationen finden Sie unter $TABCOUNT-Ausnahmen.

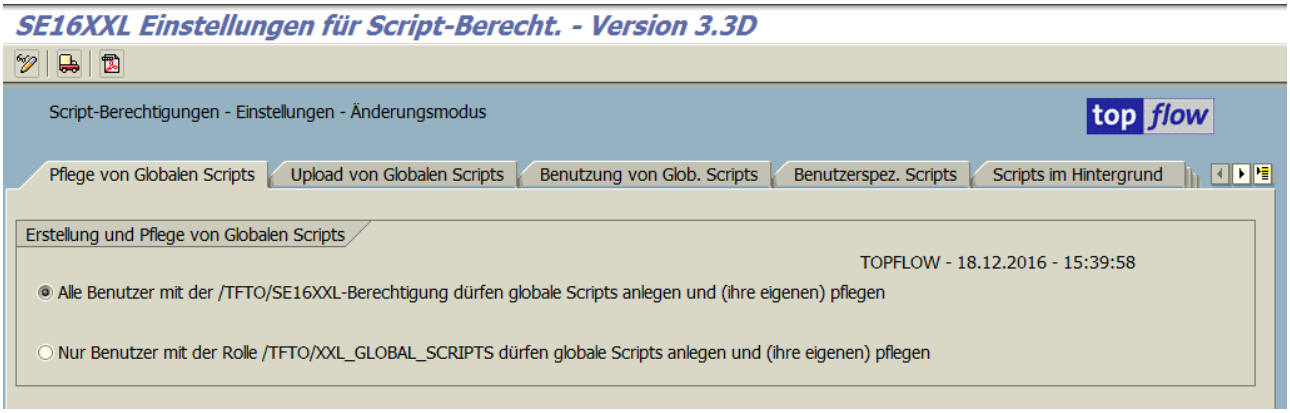
Zum Anfang

Neue Optionen für die Rollen eines globalen Scripts

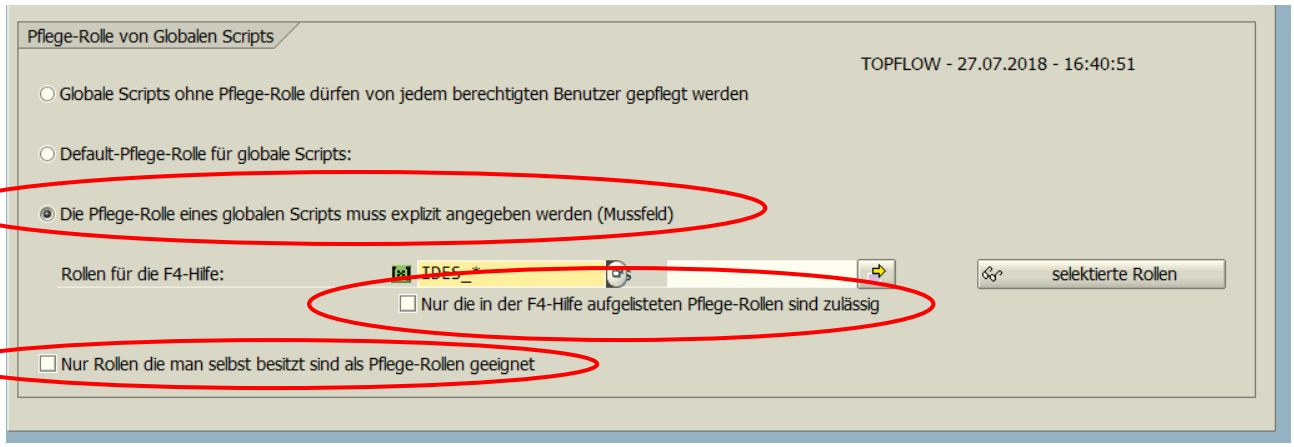
Die Berechtigungen für Scripts bieten neue Optionen in Bezug auf die Pflege- und Ausführungs-Rollen von globalen Scripts. Der Knoten im Einstellungen-Baum ist:



Auf dem **ersten Reiter** (Pflege von Globalen Scripts) sind folgende Optionen neu:



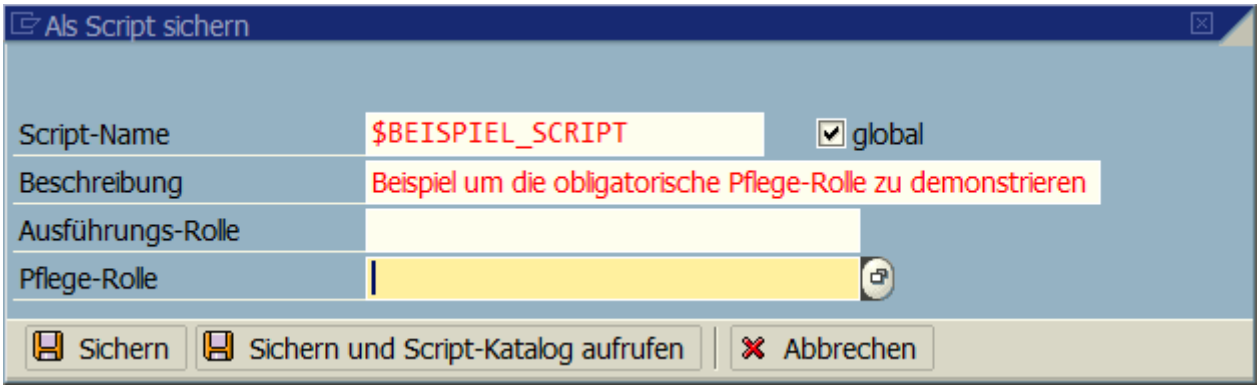
…



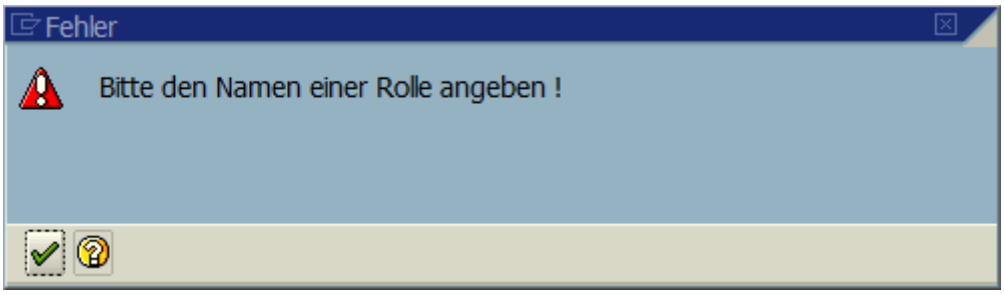
Auf den nachfolgenden Seiten werden die drei neuen Optionen kurz diskutiert.

Explizite Angabe der Pflege-Rolle

Wenn diese Option aktiviert wird muss die Pflege-Rolle eines globalen Scripts beim Sichern **explizit** angegeben werden:

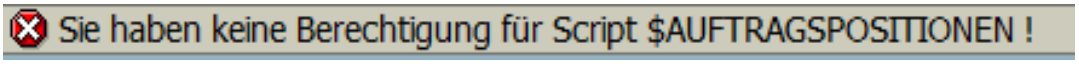


Eine leergelassene Pflege-Rolle verursacht folgende Fehlermeldung:



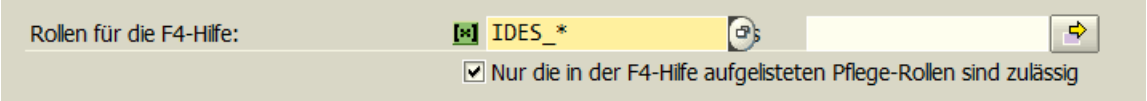
Diese Option ist für Unternehmen mit strikten Berechtigungs-Regeln zu empfehlen. Dadurch gibt es keine Default-Pflege-Rolle – jedem globalen Script muss eine eigene explizite Pflege-Rolle zugewiesen sein.

Ältere Scripts, die ohne Pflege-Rolle gesichert wurden werden so behandelt, als ob ihnen eine **inexistente** Rolle zugeordnet wäre, mit der Konsequenz, dass sie nicht pflegbar sind:

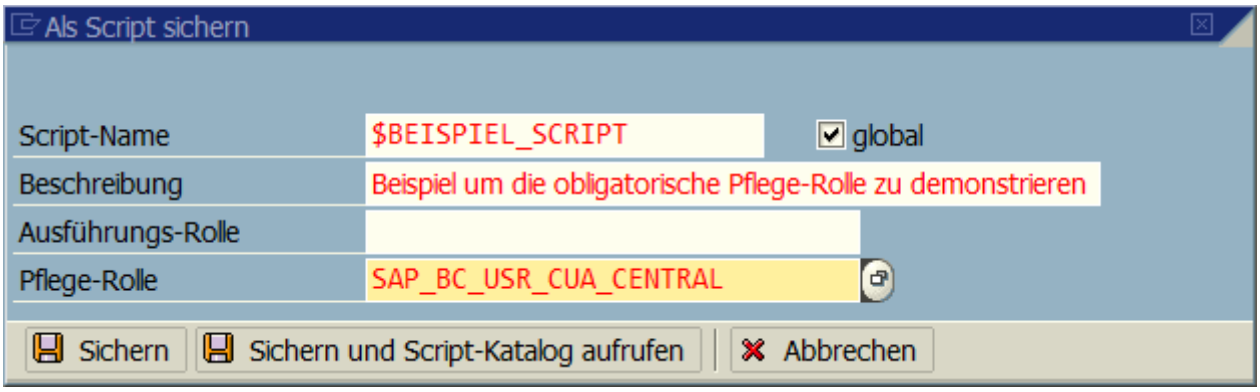


ANMERKUNG: Diese Regel betrifft nur Fremd-Anwender, d.h. diejenigen, die das Script nicht angelegt haben.

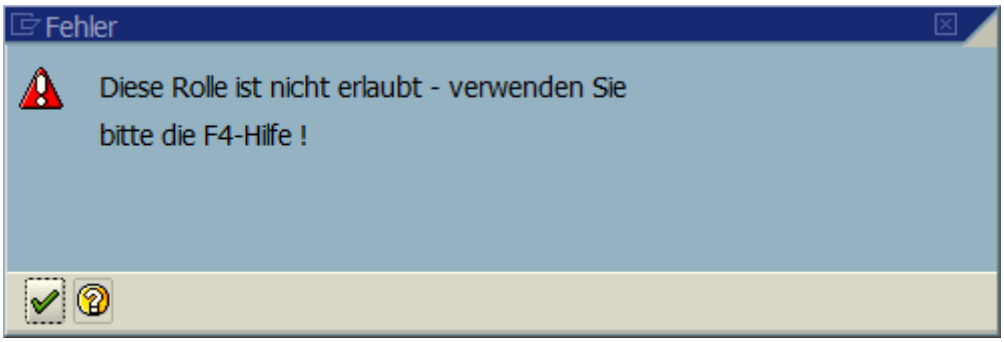
Nur Pflege-Rollen aus der F4-Hilfe sind zulässig



Eine zusätzliche Einschränkung. Normalerweise kann beim Sichern eines Scripts die F4-Hilfe verwendet werden – es ist jedoch möglich, eine Rolle zu spezifizieren, die in der F4-Hilfe nicht vorkommt.
Ist allerdings die obige Option aktiv, dann dürfen nur Rollen aus der Auflistung der F4-Hilfe angegeben werden:



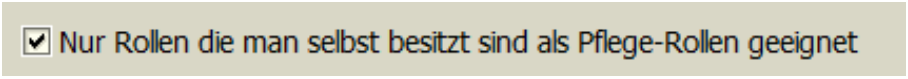
Nachdem die angegebene Rolle nicht in der F4-Hilfe vorkommt, erscheint folgende Fehlermeldung:



Diese Option dürfte "clevere" Anwender davon abhalten, beliebige Rollen einzugeben, nur um die Anforderungen des Dialogfensters zu überlisten.

ANMERKUNG: Bereits vorhandene Scripts sind nicht betroffen, solange deren Pflege-Rolle nicht geändert wird.

Zusätzliche Einschränkung der geeigneten Rollen

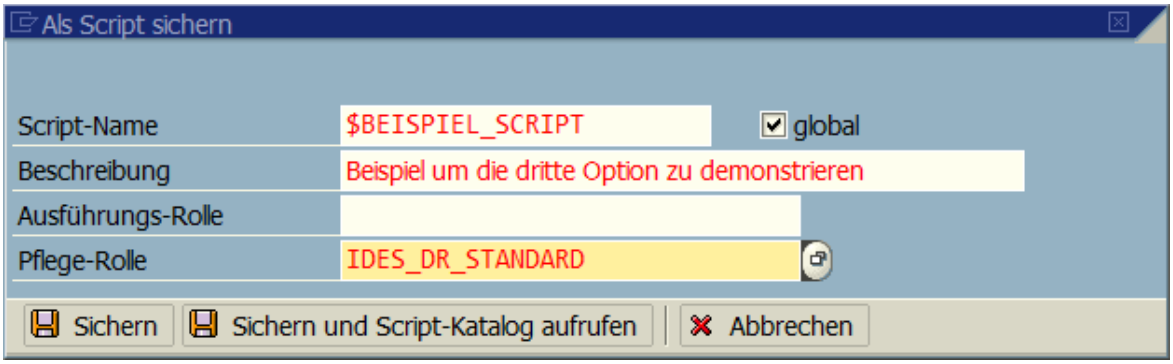


Wenn diese Option aktiv ist, unterliegt die beim Sichern eines Scripts angegebene Pflege-Rolle einer weiteren Restriktion – d.h. die Person die die Operation durchführt, muss für die spezifizierte Rolle eine Berechtigung aufweisen.

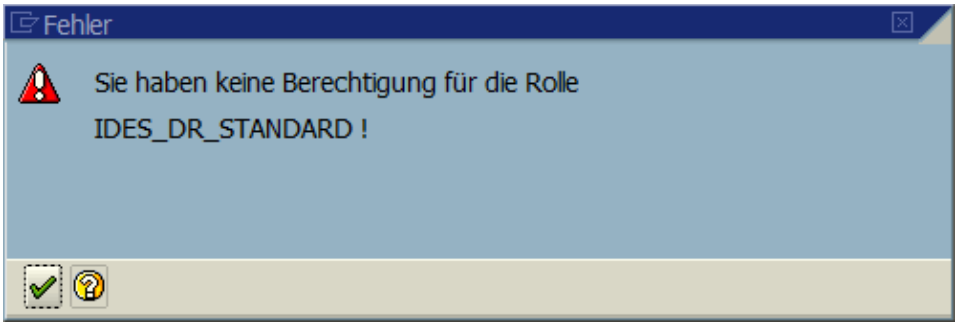
Anwender mit Administrations-Befugnissen sind davon ausgenommen.

Bereits vorhandene Scripts sind nicht betroffen, solange deren Pflege-Rolle nicht geändert wird.

Wird ein Script gesichert und dabei eine unberechtigte Pflege-Rolle angegeben,



erscheint eine entsprechende Fehlermeldung:



Neue Optionen für "Ausführungs-" Rollen

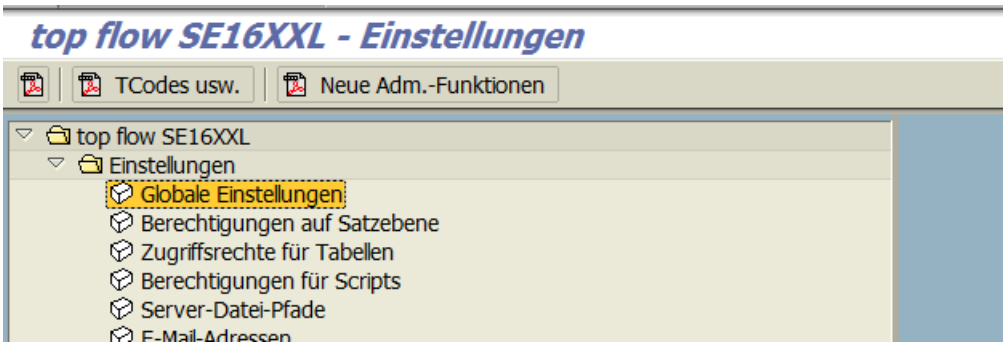
Ähnliche Optionen stehen auch auf dem **dritten Reiter** der Berechtigungen für Scripts (Benutzung von Glob. Scripts) zur Verfügung. Für sie gelten dieselben Bemerkungen wie für die Pflege-Rollen.

Zum Anfang

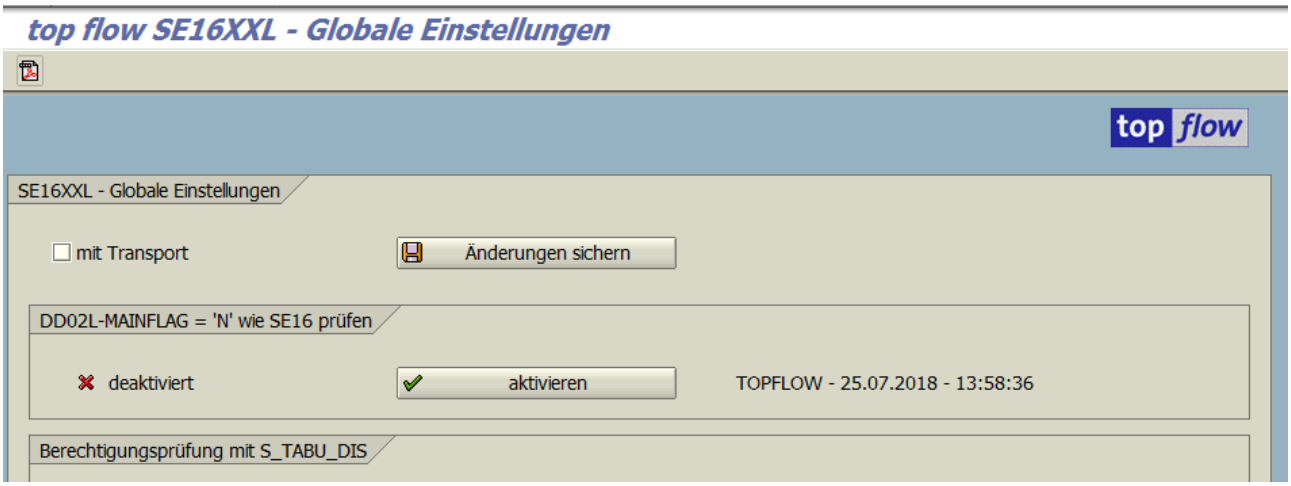
Einträge für das Security Auditlog

Der Administrator kann nun das Schreiben von Einträgen in das **Security Auditlog** (SAL) in SE16XXL aktivieren. Solche Einträge halten die Datenbank-Tabellen und Views auf die zugegriffen wurde fest.

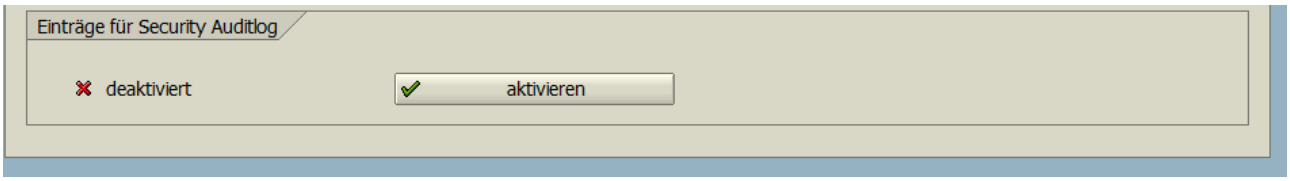
Auf dem Baum der Einstellungen ist folgender Knoten betroffen:



Die neue Einstellung ist am Ende der Dialogmaske angefügt worden:



…



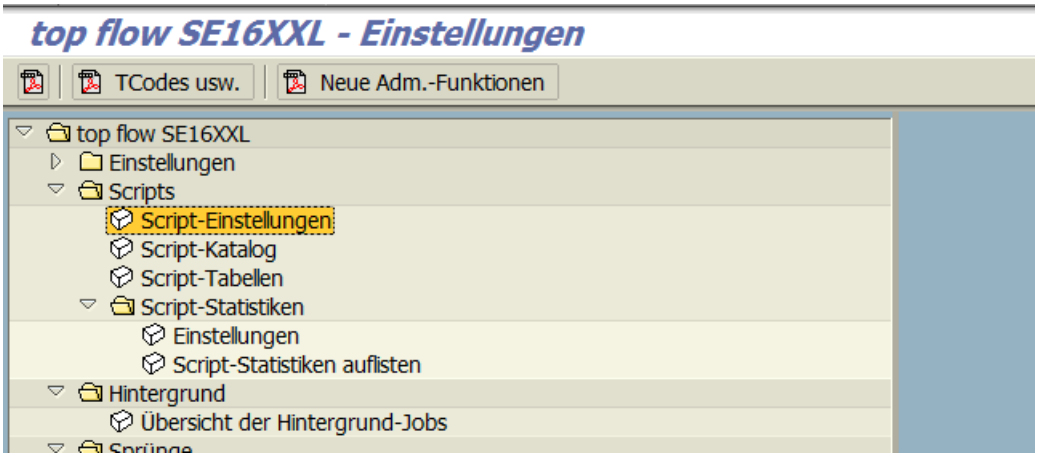
ANMERKUNG: Diese Funktionalität ist nicht auf allen SAP-Systemen verfügbar.

Die geschriebenen Einträge können mithilfe der Transaktion SM20 analysiert werden.

Zum Anfang

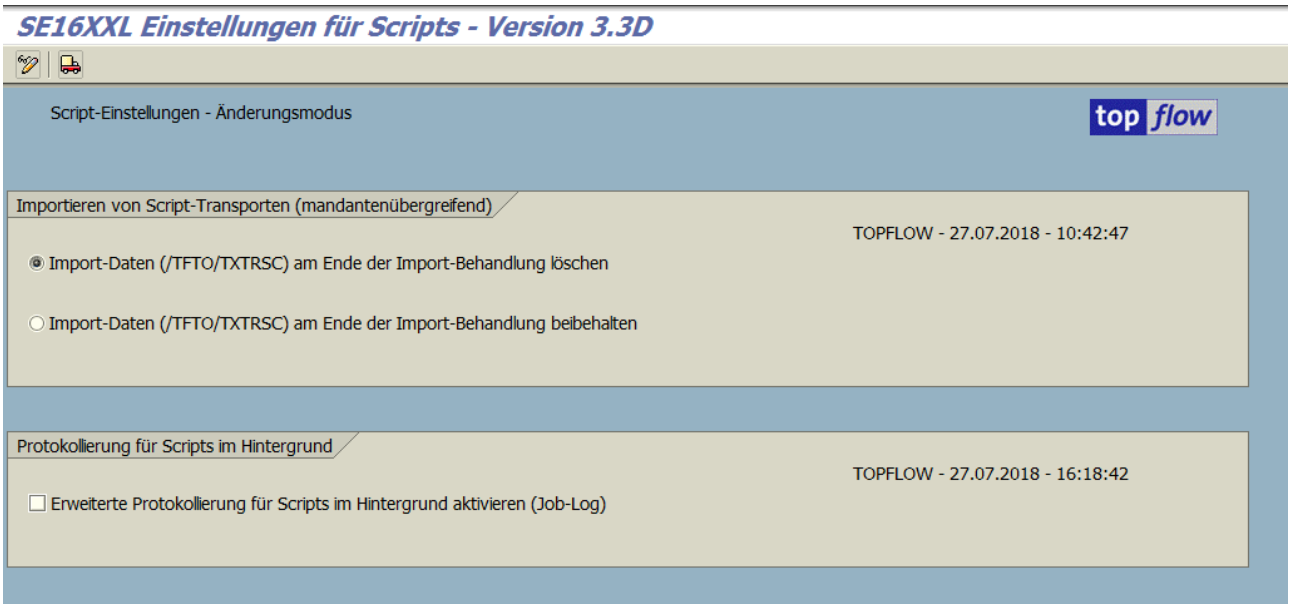
Neue Globale Einstellungen für Scripts

Zwei neue Einstellungen stehen zur Verfügung. Nachdem sie nichts mit Script-Berechtigungen zu tun haben, ist ein **neuer Knoten** zum Baum der SE16XXL-Einstellungen hinzugefügt worden:



ANMERKUNG: Dieser Knoten ist nur für Administratoren sichtbar.

Ein Doppelclick auf Script-Einstellungen führt zu folgende Dialogmaske:



Die erste Einstellung betrifft den Transport von Scripts und ist **mandanten-übergreifend**, d.h. sie gilt für sämtliche Mandanten des Systems. Sie sollte auf dem Zielsystem verwendet werden.

Die zweite Einstellung ist für Scripts im Hintergrund relevant.

Auf den nachfolgenden Seiten werden diese zwei Einstellungen näher erläutert.

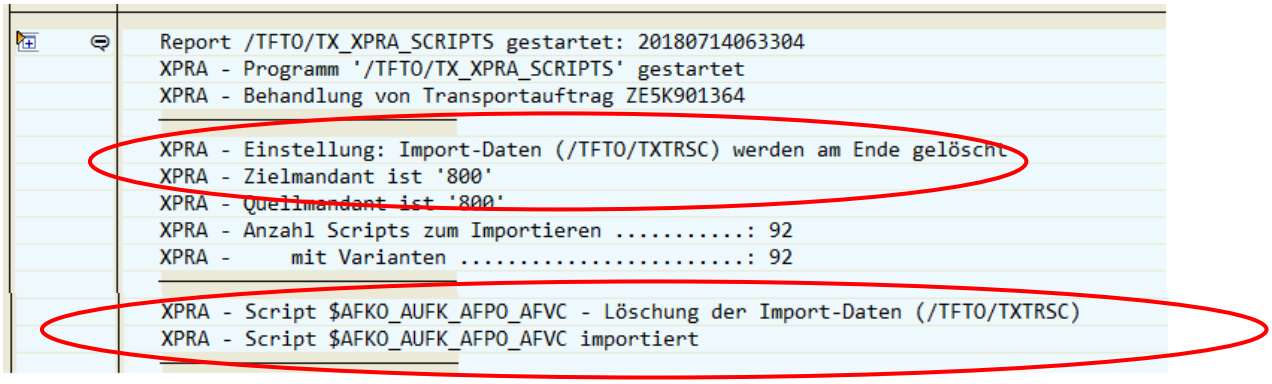
Importieren von Script-Transporten (mandantenübergreifend)

Die Tabelle **/TFTO/TXTRSC** wird von der SE16XXL-Transport-Funktionalität als Vehikel für den Transport von Scripts verwendet. Wenn im Script-Katalog ein Script einer Transport-Aufgabe hinzugefügt wird, wird der Inhalt des Scripts in diese Tabelle gespeichert und ein passender Schlüssel der Aufgabe hinzuaddiert.
Die Einträge werden mithilfe eines **R3TR TABU** Objekts zum Zielsystem transportiert, wo ein **XPRA**-Programm dafür sorgt, dass sie in echte SE16XXL-Scripts umgewandelt werden.

Bis dato wurden diese Einträge am Ende der Import-Behandlung automatisch gelöscht. Es gibt allerdings Situationen, bei denen eine automatische Löschung **zu Problemen** führt. Deswegen ist die Löschung nun **optional**. Das Import-Log des XPRA-Programms protokolliert was in dieser Hinsicht getan wurde.

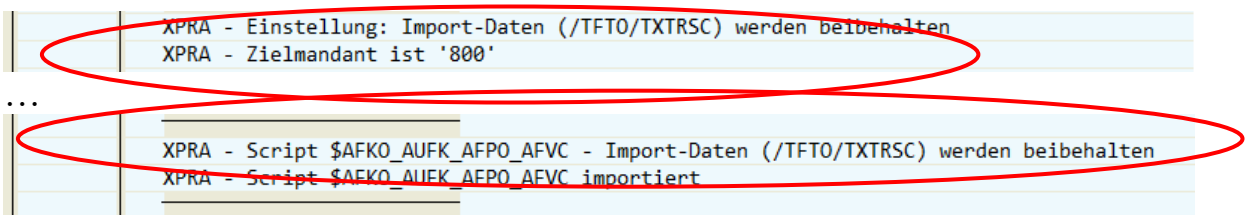
Import-Daten (/TFTO/TXTRSC) am Ende der Import-Behandlung löschen

Wenn diese Option aktiv ist werden die /TFTO/TXTRSC-Einträge auf dem Zielsystem gelöscht, sobald das entsprechende Script angelegt (oder überschrieben) worden ist. Das ist die **Standard**-Einstellung. Ein typisches XPRA-Import-Log könnte wie folgt sein:

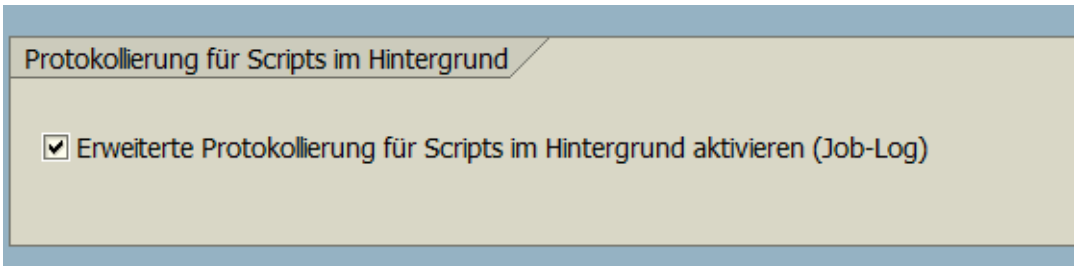


Import-Daten (/TFTO/TXTRSC) am Ende der Import-Behandlung beibehalten

Wenn diese Option aktiv ist werden die /TFTO/TXTRSC-Einträge auf dem Zielsystem **NICHT GELÖSCHT** sobald das entsprechende Script angelegt (oder überschrieben) worden ist.
Diese Option sollte aktiviert werden, falls die Protokolleinträge des XPRA-Programms darauf hinweisen, dass **keine Script-Daten gefunden wurden**. Das Import-Log würde in diesem Fall wie folgt aussehen:



Erweiterte Protokollierung für Scripts im Hintergrund



Diese Einstellung ist eingeführt worden, um die Fehlersuche in Bezug auf Script im Hintergrund zu erleichtern.

Wenn diese Option aktiv ist, werden zusätzliche Meldungen in das Job-Log von Scripts im Hintergrund geschrieben. Diese Zusatzinformationen können bei der Analyse von Fehlersituationen hilfreich sein.

Ein typisches Job-Log könnte wie folgt aussehen (Option deaktiviert):

Datum	Uhrzeit	Nachrichtentext
27.07.2018	17:20:27	Job wurde gestartet
27.07.2018	17:20:27	Step 001 gestartet (Programm /TFTO/TX_BATCH_SCRIPT_X, Variante &0000000000733, Benutzername TOPFLOW)
27.07.2018	17:20:28	Globales Script $KD_AUFTRAEGE wird ausgeführt
27.07.2018	17:20:28	Option "mit reduziertem Speicherbedarf" ist aktiv
27.07.2018	17:20:28	Die Datenbank-Join-Funktionalität wird verwendet
27.07.2018	17:20:28	Job wurde beendet

Die Aktivierung der Option würde zu folgendem Job-Log (Ausschnitt) führen:

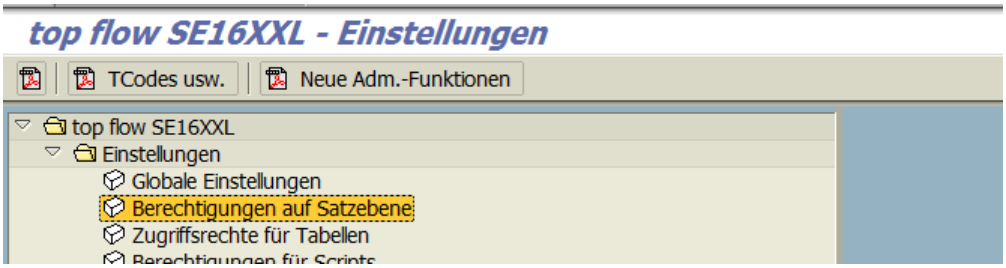
Datum	Uhrzeit	Nachrichtentext
27.07.2018	17:22:13	Job wurde gestartet
27.07.2018	17:22:13	Step 001 gestartet (Programm /TFTO/TX_BATCH_SCRIPT_X, Variante &0000000000734, Benutzername TOPFLOW)
27.07.2018	17:22:13	/TFTO/TX_BATCH_SCRIPT_X - CHECK IF ALREADY DONE - TOPFLOW 201807271722130000 (QX)
27.07.2018	17:22:13	---> OKAY
27.07.2018	17:22:13	/TFTO/TX_BATCH_SCRIPT_X - CHECK IF ALREADY DONE - TOPFLOW 201807271722130000 (QX)
27.07.2018	17:22:13	---> OKAY
27.07.2018	17:22:13	/TFTO/TX_BATCH_SCRIPT_X - IMPORT REQUEST - TOPFLOW 201807271722130000 (QX)
27.07.2018	17:22:13	/TFTO/TX_BATCH_SCRIPT_X - EXPORT REQUEST - TOPFLOW 201807271722130000 (QD)
27.07.2018	17:22:13	TOPFLOW 27.07.2018 17:22:13 X
27.07.2018	17:22:13	----------
27.07.2018	17:22:13	/TFTO/TX_BATCH_SCRIPT - CHECK IF ALREADY DONE - TOPFLOW 201807271722130000 (QD)
27.07.2018	17:22:13	---> OKAY
27.07.2018	17:22:13	/TFTO/TX_BATCH_SCRIPT - CHECK IF ALREADY DONE - TOPFLOW 201807271722130000 (QD)

ANMERKUNG: Die Meldungen sind **nicht unbedingt** in chronologischer Reihenfolge.

Zum Anfang

Berechtigungen auf Satzebene – Bemerkungs-Feld

Der Dialog "Berechtigungen auf Satzebene" ermöglicht die Festlegung der Berechtigungs-Prüfungen, die für einzelne Einträge von bestimmten Tabellen durchzuführen sind. Auf dem Baum der Einstellungen ist folgender Knoten betroffen:

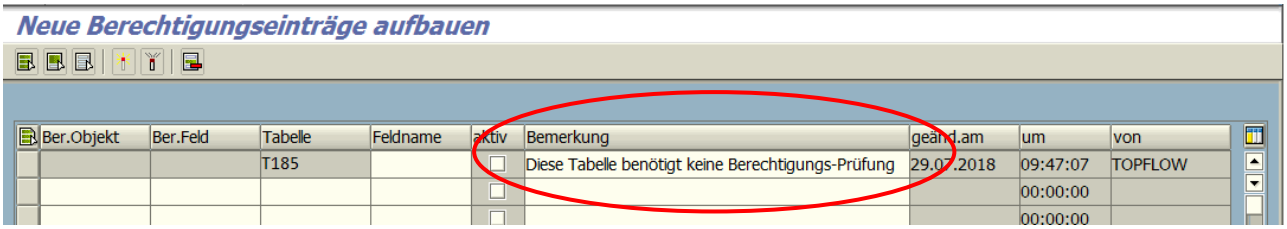


Bis dato hatte die Definitionsmaske folgende Struktur:

Es mussten für jeden Eintrag alle vier Werte (Ber.Objekt, Ber-Feld, Tabelle und Feldname) angegeben werden. Das scheint vernünftig zu sein.

Allerdings gibt es einen anderen Aspekt dieser Funktionalität. In großen Unternehmen kann dieser Dialog zu einer ansehnlichen Anzahl Einträge anwachsen. Es kann dabei vorkommen, dass eine bestimmte Datenbank-Tabelle gar keine Prüfungen benötigt – dennoch möchte der Administrator diese Tatsache festhalten, um zu einem späteren Zeitpunkt das ganze Prozedere nicht wiederholen zu müssen. Was benötigt wird, ist die Möglichkeit einen Eintrag zu erfassen, bestehend **nur aus dem Namen der Tabelle** und ggf. einer **kurzen Bemerkung**.

Genau das ist nun implementiert worden:



Zum Anfang