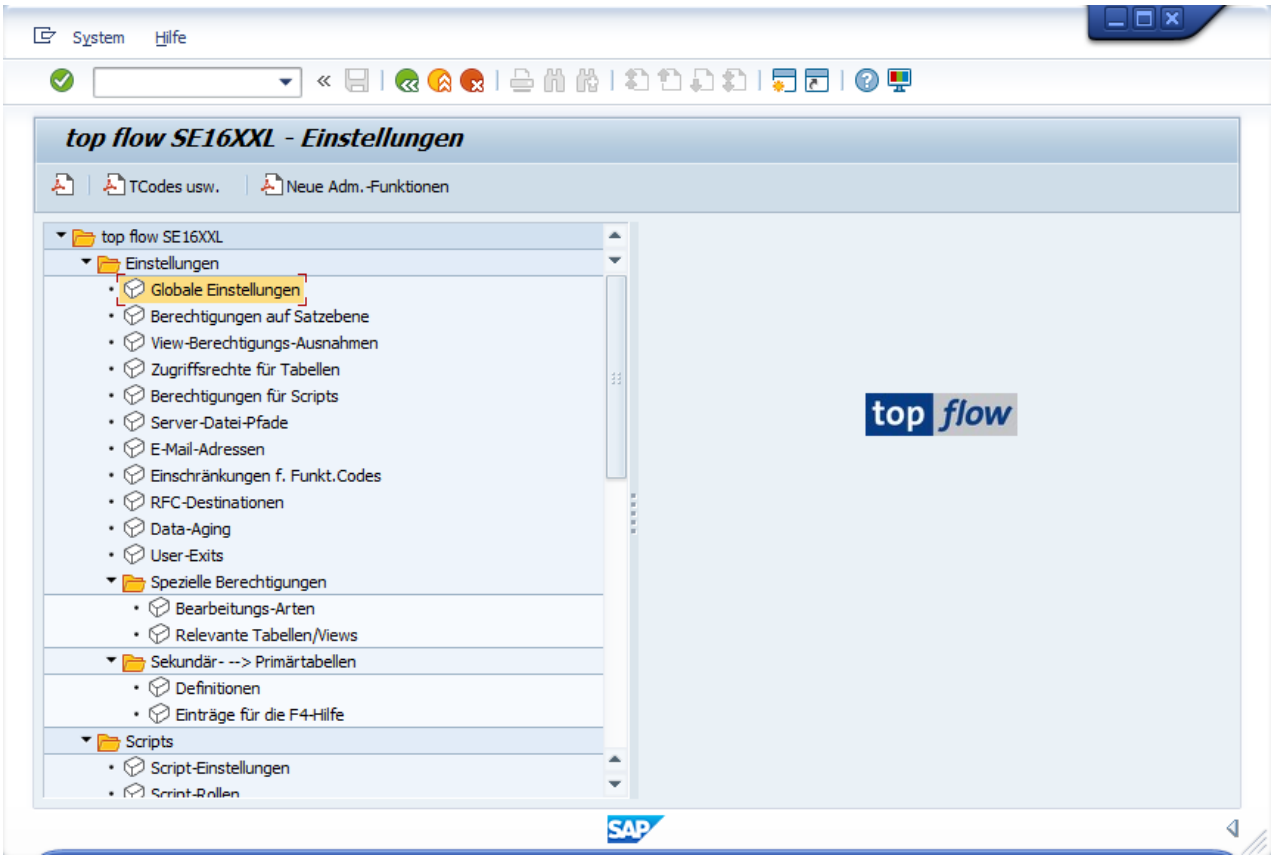
SE16XXL – Globale Einstellungen

SE16XXL bietet die Möglichkeit, bestimmte Zugriffe einzuschränken. Standardmäßig sind diese Einschränkungen deaktiviert, können aber jederzeit eingeschaltet (und wieder ausgeschaltet) werden.

Mit Hilfe der Transaktion **/TFTO/XXL_SETTINGS** können diese Einstellungen vorgenommen werden:



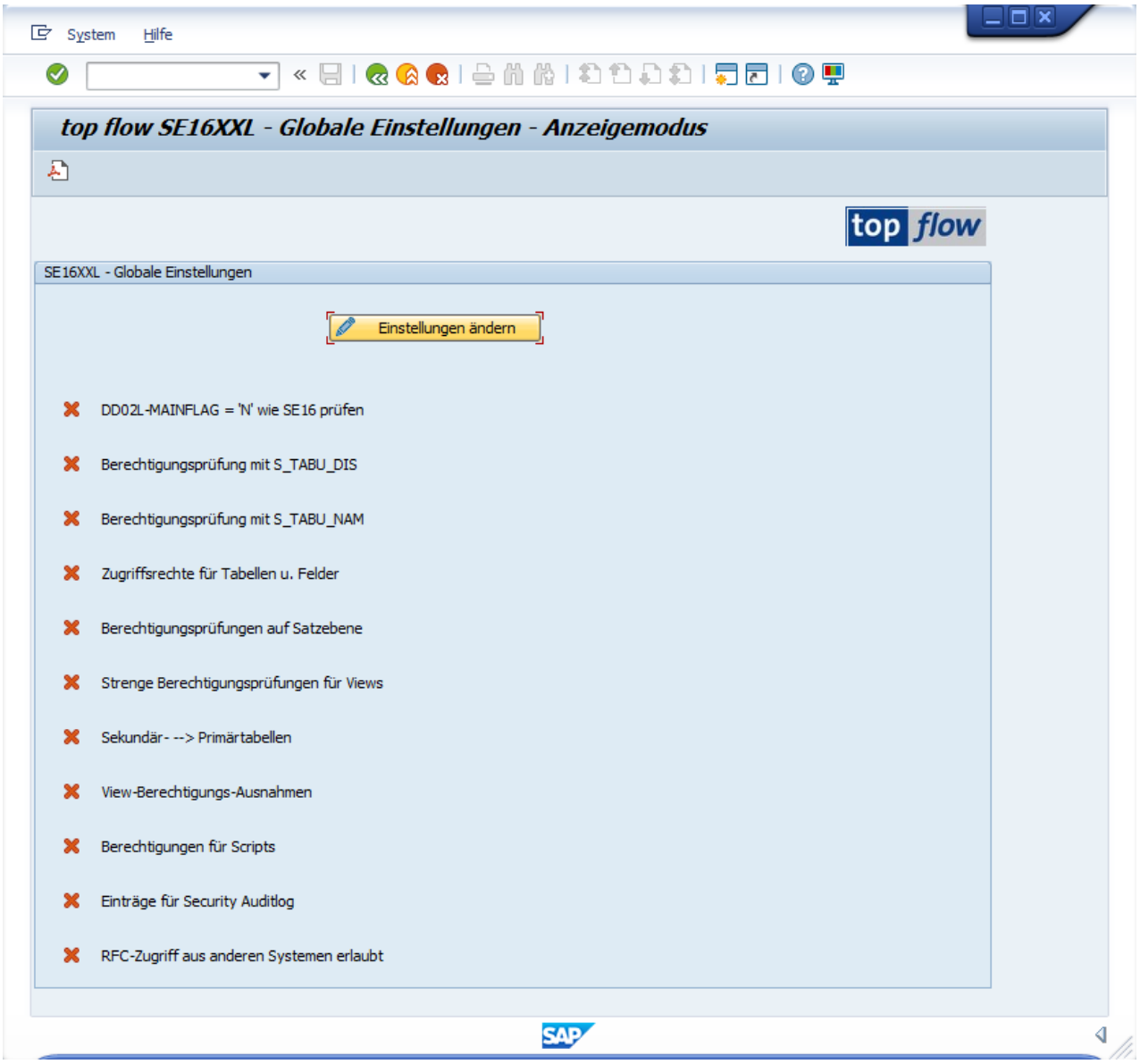
Berechtigt sind diejenigen Benutzer, die eine der folgenden Rollen besitzen:

- **/TFTO/XXL_GLOB_MAINT** (Pflegeberechtigung)
- **/TFTO/XXL_GLOB_DISPL** (Anzeigeberechtigung)

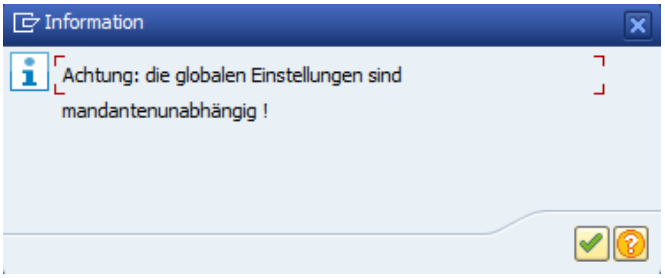
Diese Rollen sind eigentlich leer. Es wird lediglich geprüft, dass sie dem Anwender zugeordnet sind.

Anstelle der Rollen kann Berechtigungsobjekt **/TFTO/XGLB** zugewiesen werden (siehe Transaktionscodes, Rollen und Berechtigungsobjekte).

Nach einem Doppelklick auf Globale Einstellungen erscheint folgende Maske:

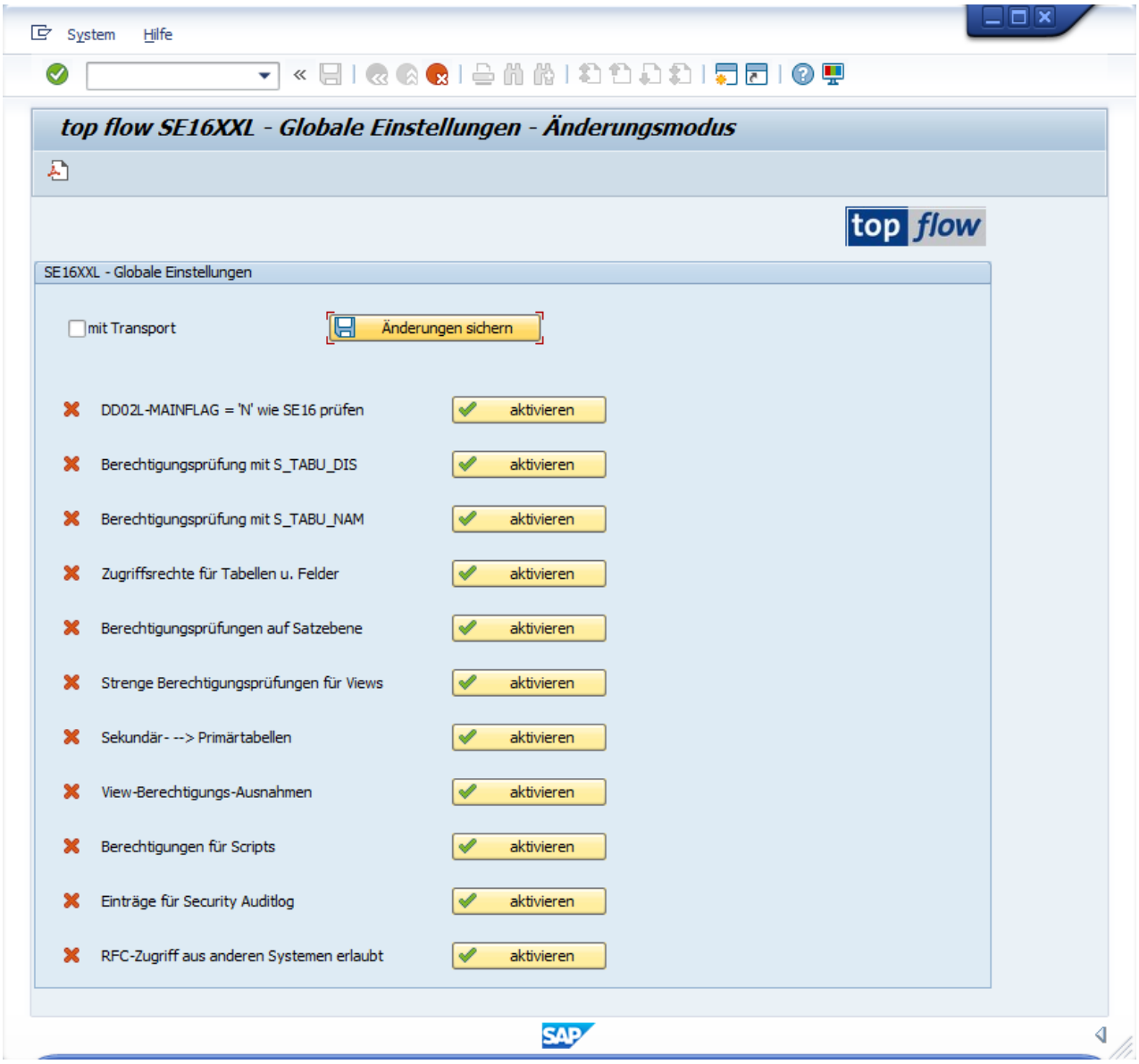


Zunächst sind alle Einschränkungen ausgeschaltet. Wird nun die Schaltfläche Einstellungen ändern betätigt, erscheint folgende Meldung:



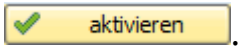
Die globalen Einstellungen sind **mandantenübergreifend**, gelten also für das gesamte System. Nachdem jedoch die meisten Restriktionen selber mandanten-abhängig sind, ist die Auswirkung von Mandant zu Mandant unterschiedlich.

Nun verwandelt sich die Maske wie folgt:



Die Hauptschaltfläche lautet nun 

.

Und jede Einstellung zeigt rechts eine Schaltfläche 

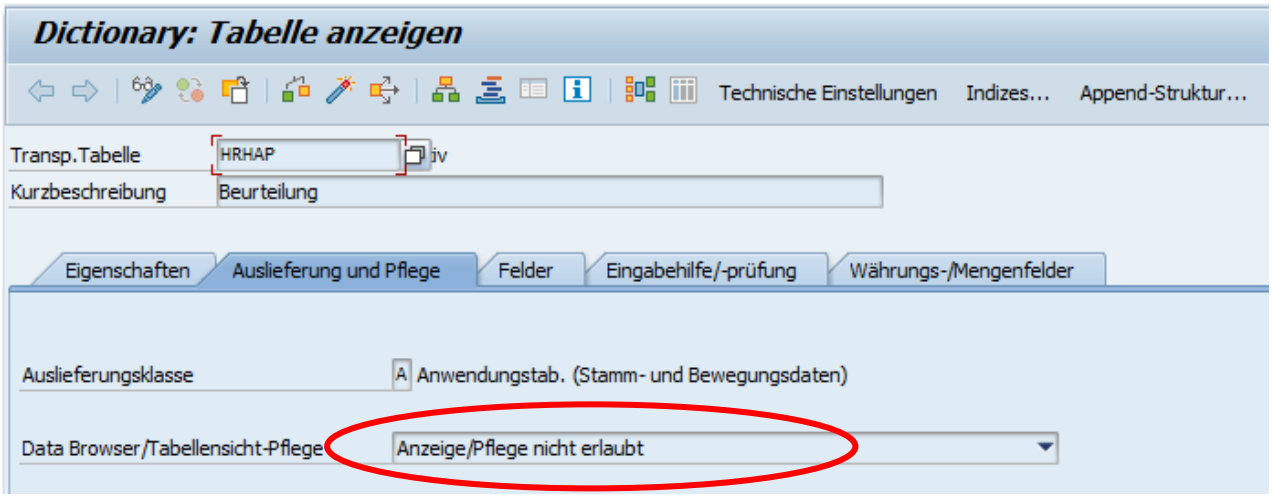
.

Die verschiedenen Prüfungen können nun je nach Bedarf aktiviert werden.

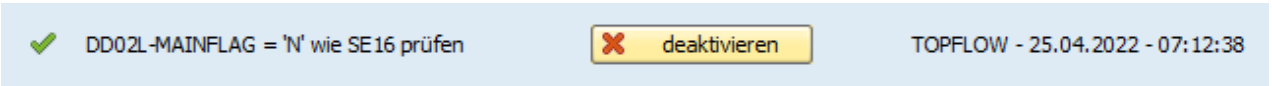
Die einzelnen Einstellungen werden auf den nächsten Seiten in Detail erläutert.

Globale Einstellung “DD02L-MAINFLAG = 'N' wie SE16 prüfen”

Diese Prüfung bezieht sich auf das Kennzeichen **DD02L-MAINFLAG = ‘N’**.
Das tragen solche Tabellen, die in der Transaktion SE11 wie folgt charakterisiert sind (**Anzeige/Pflege nicht erlaubt**):



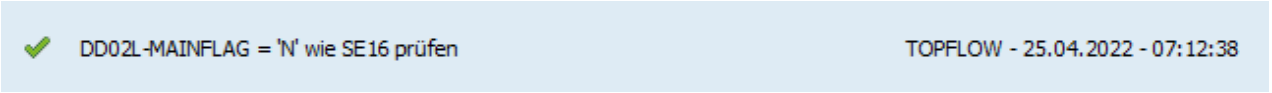
Solche Tabellen können mit dem Standard-Data-Browser (SE16/SE16N) nicht angezeigt werden. Wird gewünscht, dass SE16XXL sich genauso verhält, so muss diese Einstellung aktiviert werden.
Auf der Maske ändert sich die Erscheinung entsprechend:



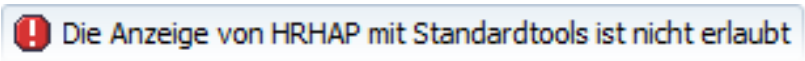
ANMERKUNG: Vergessen Sie nicht, die Schaltfläche 

zu betätigen.

Danach erscheint die Einstellung wie folgt:



Wenn die globale Einstellung aktiviert ist, erhält ein Benutzer, der versucht, obige Tabelle mit SE16XXL anzuzeigen, folgende Meldung:



Globale Einstellung "Berechtigungsprüfung mit S_TABU_DIS"

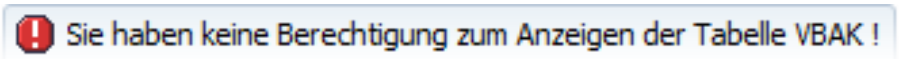
Hier geht es um die Berechtigungsprüfung einer Tabelle anhand des Berechtigungs-objekts "**S_TABU_DIS"**. Diese Prüfung wird ebenfalls von der SE16/SE16N durchgeführt. Wird ein ähnliches Verhalten seitens von SE16XXL verlangt, muss diese Einstellung aktiviert werden.

Es wird die **Berechtigungsgruppe** der Tabelle geprüft, die anhand der Transaktion **SE54** gepflegt werden kann. Viele Tabellen haben eine Berechtigungsgruppe.
Für die übrigen wird standardmäßig **"&NC&"** angenommen.

NOTA BENE: eine Datenbanktabelle und ihre Views können unterschiedliche Berechtigungsgruppen haben. Hat also ein Anwender nur die Berechtigung für eine Gruppe, dann kann es passieren, dass er die Daten der Originaltabelle nicht anschauen darf, wohl aber die Daten einer View, die auf die Tabelle basiert.

Berechtigungsgruppen werden auch bei "Zugriffsrechte für Tabellen und Felder" verwendet. Da werden allerdings Views anhand ihrer Datenbanktabellen geprüft. Bei diesen Prüfungen spielt die Berechtigungsgruppe der View selber keine Rolle.

Wenn diese Einstellung aktiviert ist, erhält eine Person, der z.B. versucht, die Tabelle VBAK ohne die erforderliche Berechtigung anzuzeigen, folgende Meldung von SE16XXL:



Globale Einstellung "Berechtigungsprüfung mit S_TABU_NAM"

Diese Prüfung steht nur zur Verfügung, wenn das Berechtigungsobject "**S_TABU_NAM**" auf dem System vorhanden ist. Es wird der **Name** der Tabelle geprüft. Falls keine Einschränkungen auf Feld- oder Datenelement-Ebene notwendig sind, kann diese Prüfung anstelle der "Zugriffsrechte für Tabellen und Felder" verwendet werden – mit dem Unterschied, dass die Zugriffsrechte immer auf die Datenbanktabellen von Views geprüft werden, während S_TABU_NAM Tabellen und Views gleich behandelt.

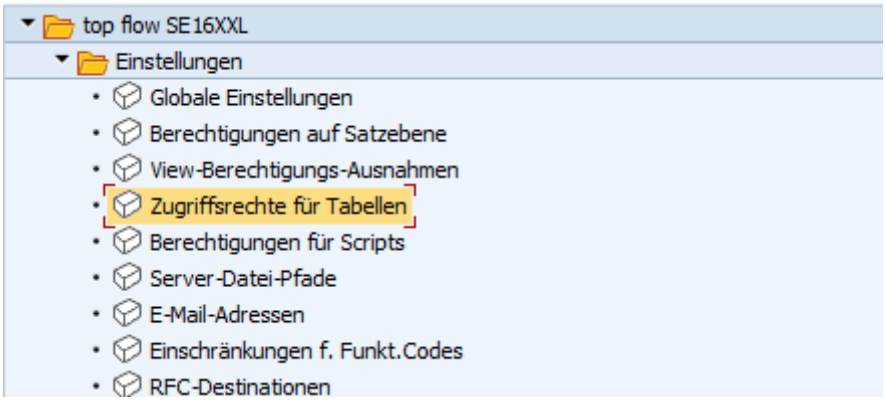
ANMERKUNG: S_TABU_DIS und S_TABU_NAM können zusammen aktiviert werden – schlägt die Prüfung mit S_TABU_DIS fehl, wird weiter mit S_TABU_NAM geprüft.

Globale Einstellung “Zugriffsrechte für Tabellen u. Felder”

Diese Prüfung ist ein Ersatz für die Prüfung auf S_TABU_DIS oder auf S_TABU_NAM.

Anhand von globalen und expliziten Zugriffsrechten kann festgelegt werden, für welche Benutzer welche Datenbanktabellen erlaubt sind. Innerhalb einer Tabelle können bestimmte Felder ausgenommen werden. Und das alles auf mehreren Ebenen. Diese Funktionalität ist relativ komplex.

An dieser Stelle wird nur festgelegt, ob diese Funktionalität aktiv sein sollte. Die konkreten Zugriffsrechte werden in einem separaten Dialog definiert. Dieser Dialog ist ebenfalls über die Transaktion **/TFTO/XXL_SETTINGS** zu erreichen:



Weitere Informationen finden Sie unter Zugriffsrechte für Tabellen & Felder.

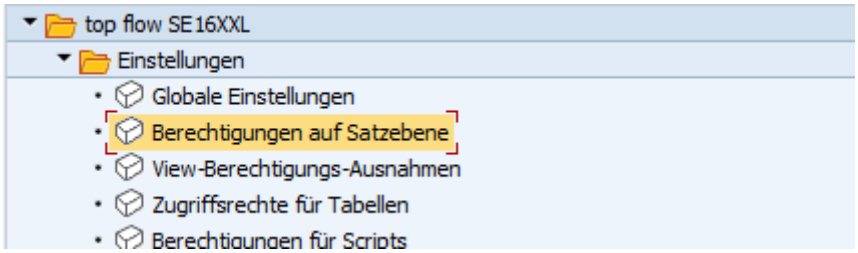
Globale Einstellung “Berechtigungsprüfungen auf Satzebene”

Die bisher betrachteten Einschränkungen betreffen die Berechtigung, auf eine bestimmte Tabelle und ihre Felder zugreifen zu dürfen, unabhängig vom Inhalt der Einträge. Es gibt jedoch Situationen, in denen es sinnvoll ist, den Zugriff auf nur einige der in einer Tabelle enthaltenen Datensätze zuzulassen, abhängig von den Werten bestimmter Felder.

Die vorliegende Einschränkung hat mit Berechtigungsprüfungen zu tun, die auf Datensatzebene durchgeführt werden. Man kann z.B. festlegen, dass jeder selektierte Datensatz der Tabelle VBAK mit ‘S_VBAK_VKO’ in Kombination mit dem Inhalt des Feldes VKORG einer Berechtigungsprüfung unterzogen wird.
Für jeden Datensatz können mehrere Prüfungen durchgeführt werden. Nur wenn sämtliche Prüfungen erfolgreich sind, wird der Datensatz angezeigt.

An dieser Stelle wird nur die globale Festlegung getroffen, ob überhaupt solche Berechtigungsprüfungen in SE16XXL aktiviert werden sollten.

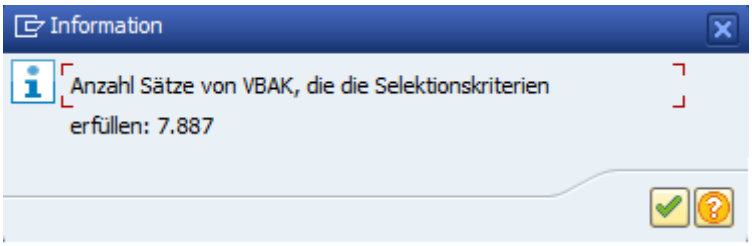
Was im Detail zu prüfen ist, und für welche Tabellen, das wird in einer separaten Transaktion bestimmt. Diese ist ebenfalls anhand von **/TFTO/XXL_SETTINGS** zu erreichen:



Weitere Informationen finden Sie unter Berechtigungsprüfungen auf Satzebene.

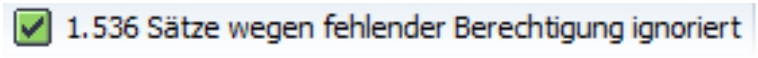
Eine Person, die sämtliche Rechte besitzt, merkt von diesen Prüfungen nichts.

Hingegen kann eine Person mit eingeschränkten Rechten folgende Situation erleben: Zunächst fragt sie nach, anhand von “Anzahl Treffer”, wie viele Datensätze eine bestimmte Tabelle enthält. Die Antwort lautet:



Dann führt sie die tatsächliche Selektion durch, erhält aber nur 6351 Datensätze:

Begleitet von der folgenden Meldung:



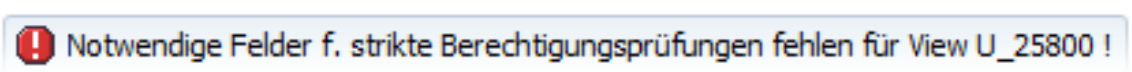
Wenn kein Datensatz erlaubt ist, erscheint folgende Meldung:

Globale Einstellung “Strenge Berechtigungsprüfungen für Views”

Datenbank- und Projektions-Views basieren auf Datenbanktabellen. Sie **erben** die Berechtigungsprüfungen auf Satzebene, die für die zugrunde liegenden Datenbank-tabellen definiert wurden. Es kann jedoch vorkommen, dass eine bestimmte View nicht alle Felder enthält, die zur Durchführung dieser Berechtigungsprüfungen erforderlich sind. In solchen Fällen werden nur die Prüfungen durchgeführt, für die die Felder in der View vorhanden sind. Die übrigen Prüfungen werden nicht durchgeführt. Dieses Verhalten ist für die meisten Views sinnvoll, da sie keine sensible Informationen enthalten.

Es kann jedoch Views geben, die die meisten Felder der zugrunde liegenden Tabellen enthalten, einschließlich sensibler Daten, aber nicht die Felder, die zum Ausführen der Berechtigungsprüfungen erforderlich sind. Die vorliegende globale Einstellung steht für solche Situationen zur Verfügung. Wenn “Strenge Berechtigungsprüfungen für Views” aktiviert ist, **verweigert** SE16XXL die Anzeige der Einträge dieser Views, es sei denn, man ist mit einer allgemeinen Berechtigung (alle Werte = '*') für die Berechtigungsobjekte ausgestattet, die nicht direkt geprüft werden können.

Wenn eine solche Situation eintritt, erhält man folgende Meldung:



Globale Einstellung “Sekundär- → Primärtabellen”

Die “Berechtigungsprüfungen auf Satzebene” sind für solche Datenbanktabellen definiert, die die nötigen Felder zur Durchführung der jeweiligen Prüfungen enthalten. Es gibt allerdings auch Datenbanktabellen, die logisch zu einem gegebenen Bereich gehören, ohne die Felder zu besitzen, die für die Durchführung der gewünschten Berechtigungsprüfungen erforderlich sind.

Die Tabelle **VBAP** enthält z.B. die Positionen von Verkaufsbelegen. Eine Berechtigungsprüfung für die Verkaufsorganisation **VKORG** kann jedoch nur über die Tabelle **VBAK** (Verkaufsbeleg: Kopfdaten) stattfinden, die über das Feld **VBELN** (Verkaufsbelegnummer) logisch mit **VBAP** verbunden ist.
In ähnlicher Weise kann eine Prüfung der Berechtigungsgruppe **BEGRU** nur mittels der Tabelle **MARA** (Allgemeine Materialdaten) durchgeführt werden, die über das Feld **MATNR** (Materialnummer) mit **VBAP** verbunden ist.

Mit anderen Worten, eine Person, der die erforderliche Berechtigung sowohl für VKORG als auch für BEGRU fehlt, **könnte trotzdem Datensätze der Tabelle VBAP lesen**, obwohl die Sätze der vebundenen Tabellen VBAK und MARA außerhalb ihrer Reichweite sind.

Um diese Art von Missbrauch zu **verhindern**, ist es möglich, für einzelne Tabellen – in diesem Zusammenhang als “**Sekundärtabellen**” bezeichnet – eine Reihe von “**Primärtabellen**” zu definieren, die durch festgelegte Join-Kriterien mit den Sekundärtabellen verknüpft sind. Wenn in SE16XXL Datensätze einer Sekundärtabelle selektiert werden, werden auch die relevanten Datensätze der zugehörigen Primärtabellen intern selektiert und die gewünschten Berechtigungs-prüfungen an diesen durchgeführt. Ein bestimmter Datensatz der Sekundärtabelle wird nur angezeigt, wenn alle zugehörigen Primärtabellen-Datensätze die angegebenen Berechtigungs-prüfungen erfüllen. Andernfalls wird der Datensatz verworfen.

Im obigen Beispiel ist VBAP die **Sekundärtabelle** und VBAK und MARA die zugehörigen **Primärtabellen**. Die gewünschten Prüfungen für VBAK und MARA müssen in den “Berechtigungsprüfungen auf Satzebene” festgelegt werden.

Die hier beschriebene globale Einstellung gibt nur an, ob diese Art von Berechtigungsprüfungen durchgeführt werden soll.

Die Beziehungen zwischen Sekundär- und Primärtabellen werden in einer separaten Transaktion spezifiziert. Diese ist ebenfalls anhand von **/TFTO/XXL_SETTINGS** zu erreichen:

Weitere Informationen finden Sie unter Sekundär → Primärtabellen.

Globale Einstellung “View-Berechtigungs-Ausnahmen”

Wie bereits erwähnt, gibt es ein Problem mit Views: Eine View **enthält nicht unbedingt alle Felder**, die zur Durchführung der definierten Berechtigungs-prüfungen erforderlich sind.
Die Reaktion von SE16XXL in einer solchen Situation ist je nach Art der Berechtigungsprüfung wie folgt:

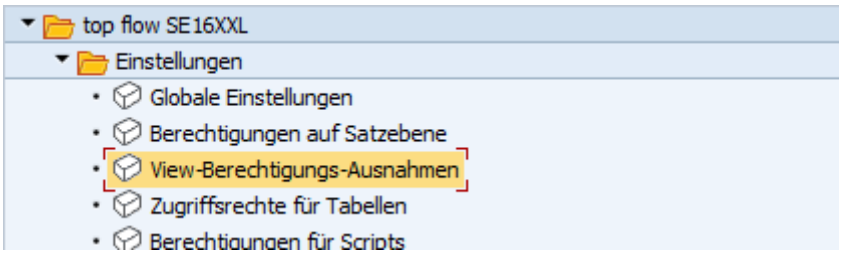
1) Bei normalen Berechtigungsprüfungen werden nur die möglichen durchgeführt. Wenn jedoch die globale Einstellung “**Strenge Berechtigungsprüfungen für Views**” aktiviert wurde, ermittelt das Programm, ob der Benutzer über eine allgemeine Berechtigung ('*') für alle fehlenden Felder verfügt. Ist dies der Fall, werden die möglichen Prüfungen durchgeführt. Andernfalls **weigert** sich das Programm, die Datensätze der View zu selektieren.
   Beispiel: View **U_25800**, basierend auf VBAK, aber ohne das Feld VKORG.

2) Im Falle von Primär-Berechtigungsprüfungen wird immer “streng” vorgegangen, d.h. das Programm **weigert** sich, die Sätze der View zu selektieren, falls der Benutzer keine allgemeine Berechtigung für die Felder der Primärtabellen besitzt, die wegen fehlender Felder nicht greifbar sind.
   Beispiel: View **U_16022**, basierend auf VBAP, aber ohne das Feld MATNR.

Die oben beschriebene **Weigerung** kann unterdrückt werden, indem eine Ausnahme für die betreffende View definiert wird.

Die hier beschriebene globale Einstellung legt nur fest, ob die View-Berechtigungs-Ausnahmen berücksichtigt werden sollen.

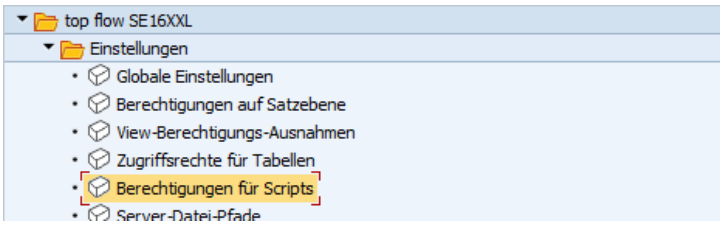
Die Views, für die eine Ausnahme gemacht werden soll, können in einer separaten Transaktion angegeben werden, die auch in **/TFTO/XXL_SETTINGS** zu finden ist:



Weitere Informationen finden Sie unter View-Berechtigungs-Ausnahmen.

Globale Einstellung “Berechtigungen für Scripts”

Mit dieser globalen Einstellung kann die Verwendung von SE16XXL Scripts eingeschränkt werden.
Die entsprechenden Festlegungen werden in einem separaten Dialog getroffen:



Weitere Informationen finden Sie unter Script-Berechtigungen.

Globale Einstellung “Einträge für Security Auditlog”

Anhand dieser globalen Einstellung kann der Administrator das Schreiben von Einträgen in das **Security Auditlog** (SAL) in SE16XXL aktivieren. Solche Einträge halten die Datenbanktabellen und Views fest auf die zugegriffen wurde. Die geschriebenen Einträge können mithilfe der Transaktion SM20 analysiert werden.

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

Globale Einstellung “RFC-Zugriff aus anderen Systemen erlaubt”

Ab Version **3.5** ist es in SE16XXL möglich, einen Join mit einer Datenbanktabelle durchzuführen, die sich auf einem Remote-SAP-System befindet (**RFC-Selektion**).

Die betreffende globale Einstellung steht zur Verfügung, um einen RFC-Zugriff auf das lokale System von anderen entfernten SAP-Systemen aus zu ermöglichen. Ist sie deaktiviert, ist ein RFC-Zugriff via SE16XXL auf das System nicht möglich.

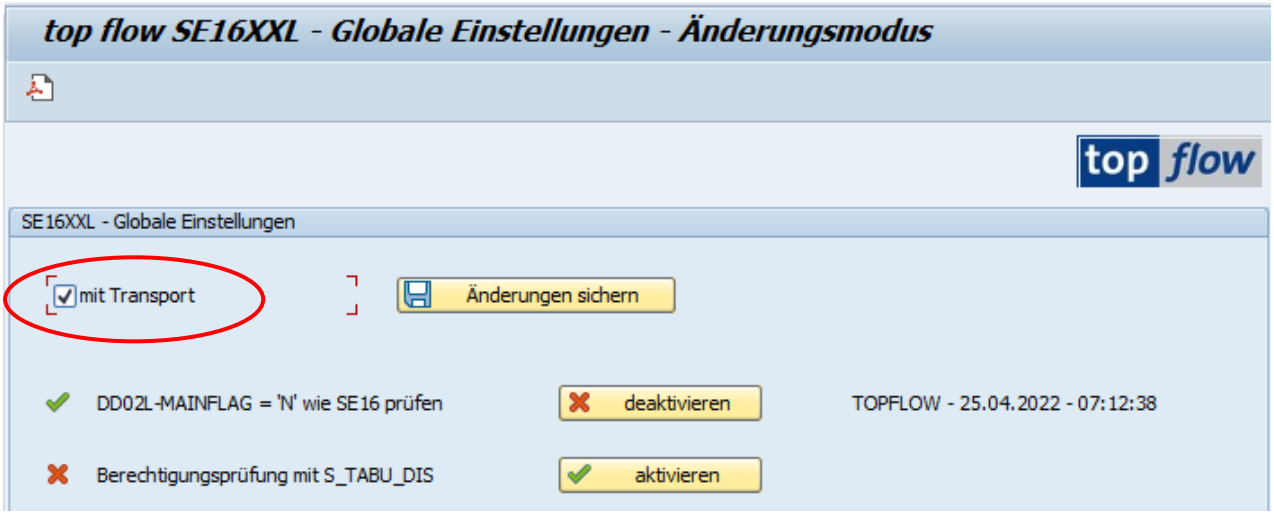
Ein Versuch, eine RFC-Selektion mit diesem System als Ziel durchzuführen, wird in diesem Fall mit folgender Fehlermeldung abgewiesen:

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

Transport

Die globalen Einstellungen können auch transportiert werden.

Hierzu muss vor dem Sichern die Option "**mit Transport**" gewählt werden:



Sie werden dann nach einem Workbench-Auftrag gefragt, in den die Einstellungen (in Form von R3TR TABU ...) hinterlegt werden sollten.

Es ist allerdings auch möglich, die Einstellungen in jedem System separat vorzunehmen.