
# Xiting User Locking Tool

Dieses Dokument beschreibt die Nutzung des Xiting User Locking Tool.

Version SP17

## Produktherkunft

Das Xiting User Lock Tool ist eine frei verfügbare Komponente der Xiting Times, Automatic Role Builder, Role Profiler, ABAP Alchemist und Security Architect Produkte der Xiting AG, Schweiz. Das Produkt kann auch als Service von SAP angefordert werden, um SYSTEM Benutzer-Berechtigungen zu korrigieren und zu verwalten.

Weitere Informationen finden Sie auf www.xiting.ch

## Hintergrund

Viele Kunden haben unterschiedliche Tools entwickelt, um Massen(ent)sperren von Benutzern durchzuführen. Diese werden häufig für Wartungsfenster in den Systemen benötigt.

Hierbei gibt es einige Herausforderungen, wie die folgenden:

- Schützen der Administratoren, um sich nicht selbst auszusperren.
- Verhindern des Sperrens von SYSTEM und SERVICE Benutzern.
- Sperren nur der User, die nicht bereits gesperrt sind.
- Entsperren nur der User, die ursprünglich nicht gesperrt waren.
- Ermöglichen der Änderungsbelege durch Nutzung von freigegebenen APIs.

Dieses SAP spezifische frei verfügbare Produkt Xiting User Locking Tool ermöglicht es Ihnen, temporär eine große Anzahl von Benutzern zu (ent)sperren. Dabei „merkt“ es sich, was Sie für Aktionen durchgeführt haben, so dass nur diese wieder zurücknehmen können.

Zusätzlich schützt es Sie vor sich selbst, wenn Sie versehentlich alle, inklusive sich selbst, gesperrt haben sollten.

## Technische Information für Installations-Administratoren:

Die Selektion der Benutzer, die gesperrt werden, wird in der Xiting Anwendung gespeichert. Ausgewählte Benutzer und Benutzergruppen können durch die Anwendung gegen ein Sperren gesichert werden.

Nur die User, die von der Anwendung gesperrt worden sind, können später wieder entsperrt werden.

Die Integration in das System basiert auf der Nutzung von freigegebenen BAPIs. Vergl. Transaktion BAPI im SAP System.

## Anmerkung zur Nachvollziehbarkeit:

Die BAPIs nutzen alle Standard Änderungsbelege bei den Sperrvorgängen an den Benutzern. Diese können über die Transaktion SUIM wie gewohnt ausgewertet werden.

Weitere Audits sind nicht notwendig.

## Anmerkung zur Release-Abhängigkeit:

Dieses Tool wurde für SAP NetWeaver ABAP Umgebungen ab einem Release von 7.00 aufwärts entwickelt. Ein Einsatz in früheren Releases wird nicht unterstützt.

## Anmerkung zu Alternativlösungen ab 2014:

SAP hat mit den 7.21 Kernel für 7.31er Systeme eine neue Lösung über den SAP Hinweis 1891583 eingeführt. Damit können Logonpolicies und Instanz Parameter verwendet werden, um die Anmeldung von

bestimmten Benutzern zu verhindern. Dieses ist sehr viel performanter als die Anwendungsuser zu sperren.

# Index

# 1 Xiting User Locking Tool

Das Xiting User Locking Tool ist ein integrierter Bestandteil der Xiting Produktpalette. Das Tool benötigt keine vorangegangene Konfiguration und kann damit sofort nach dem Import des Transportauftrages genutzt werden.

Sein Hauptzweck ist es, Administratoren zu ermöglichen, alle Benutzer mit Ausnahme sich selbst und bestimmten Benutzern, abhängig ihres Typs oder ihrer Benutzergruppe zu sperren. Dieses wird häufig während einer Wartung wie einem Upgrade oder einer Systemkopie benötigt. Anschließend können die von dem Tool gesperrten Benutzer wieder entsperrt werden. Allerdings nur die, die hierüber gesperrt wurden. User, die z.B. über die SU01 gesperrt wurden, oder deren Kennwort aufgrund von Passwortfehleingaben gesperrt ist, bleiben hiervon unbehelligt. Normalerweise muss dieses mit Hilfe von externen Listen oder „stumpfen" Scripting Tools durchgeführt werden. Dieses Tool ermöglicht nun eine einfache und schnellere Möglichkeit, dieses direkt in der SAP Applikation zu erledigen.

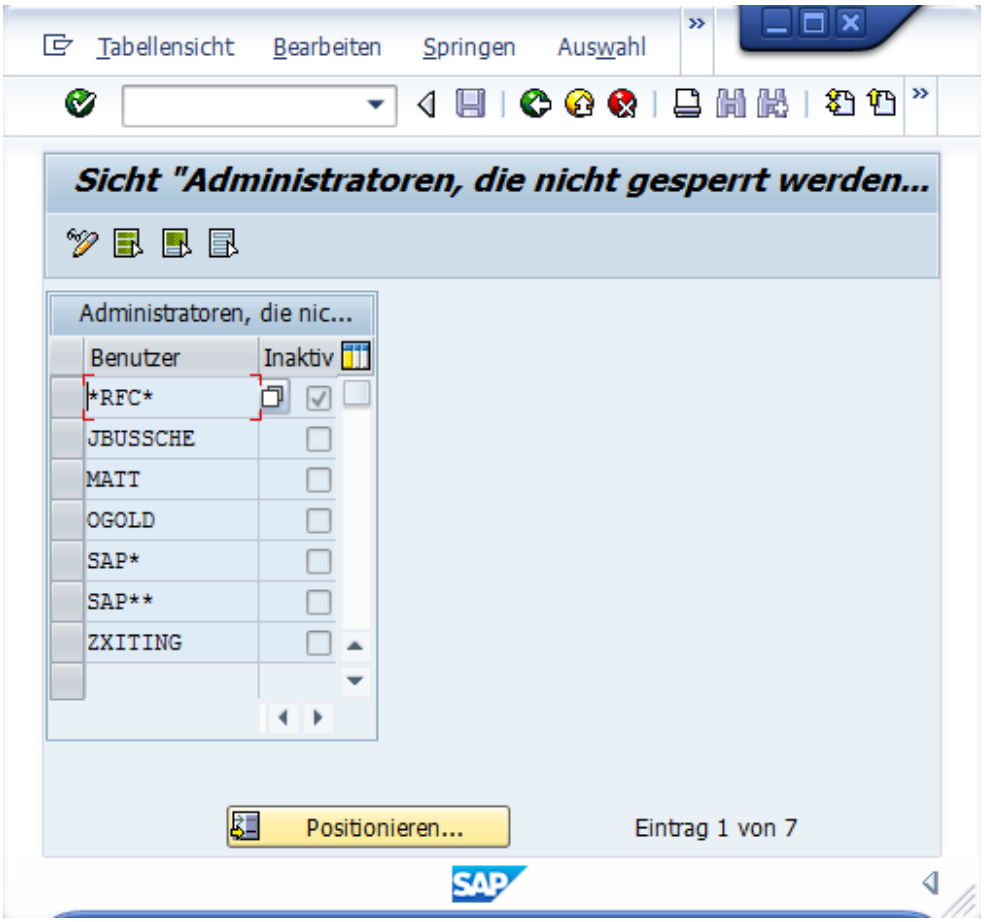
Sie können aber auch Benutzer, die über andere Systemprogramme gesperrt wurde, über dieses Toll wieder entsperren, so dass es zu Ihrem zentralen Einstiegspunkt für alle Sperraktionen werden kann.

Das Tool kann über die Transaktion /XITING/USER_LOCK gestartet werden.

Wenn Benutzer gesperrt werden sollen, soll typischerweise verhindert werden, dass die Administratoren sich selbst auch sperren. Um dieses sicher zu stellen, können Administratoren ihre Benutzernamen in und / oder Benutzergruppen als „nicht-zu-sperren“ in Customizingtabellen hinterlegen. Es kann nützlich sein, auch die Benutzer hier zu hinterlegen, die für die Kommunikation mit anderen Systemen benötigt werden, Jobs ausführen oder andere wichtige, nicht-Dialog-Aktivitäten durchführen.

Beachten Sie, dass dieser Schutz nur bei der Nutzung dieses Tools gegeben ist. Wenn die Berechtigung hierfür vorliegt, können die Benutzer natürlich immer noch über die Transaktionen SU01 oder SU10 gesperrt werden.

Der schnellste Weg zu den Customizingtabellen zu gelangen ist, es, den Button “Admins pflegen” oder “Admin Gruppen pflegen” auf dem Selektionsbildschirm des Tools zu drücken. Einträge in den Tabellen werden nicht in Transportaufträgen erfasst und müssen daher in jedem Mandanten separat erfasst werden.




Beachten Sie, dass Sie auch eine UserID oder eine Benutzergruppe als inaktiv deklarieren können, ohne den Eintrag komplett aus der Tabelle entfernen zu müssen. Zusätzlich können Sie in der User ID Tabelle auch mit generischen Angaben wie im Folgenden aufgeführt arbeiten:

RFC* = Benutzernamen beginnen mit „RFC“.

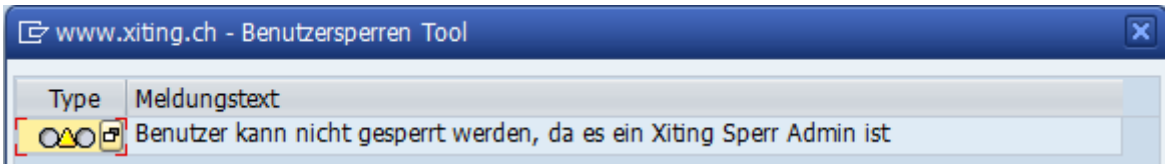
*RFC = Benutzernamen enden mit „RFC“.

*RFC* = Benutzernamen enthalten „RFC“ im Namen.

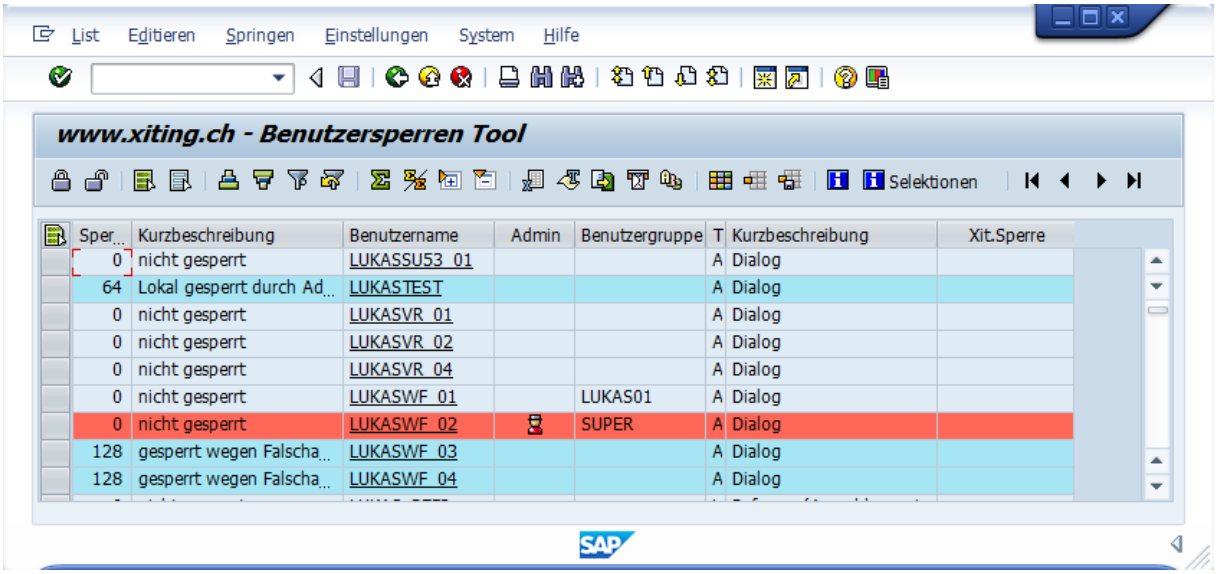
RFC = Der Benutzername ist exakt „RFC“.

Im Spezialfall des Benutzers SAP* muss der Name exakt als „SAP**“ (Zwei Sterne!) hinterlegt werden, da der Eintrag SAP* sonst alle Benutzer beschreiben würde, die mit SAP anfangen (z.B. SAPCPIC, SAPBASIS, etc.).

Wenn Sie versuchen, einen in den Tabellen aufgenommenen User zu sperren, erhalten Sie die folgende Fehlermeldung:



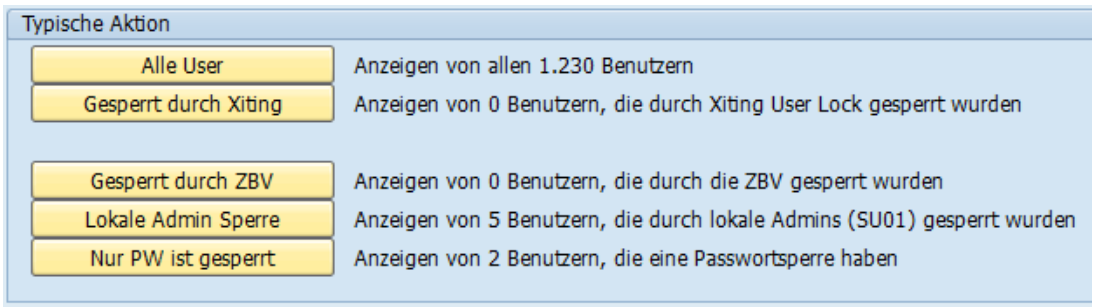

Zusätzlich können diese User in der Vorschau angelistet werden. Sie erscheinen als rote Zeilen mit einem speziellen „Administrator“-Ikon:




Der Fehler unterbricht nicht die Ausführung des Programms. So werden beispielsweise bei dem Versuch, 10 User zu sperren, von denen einer in der Tabelle hinterlegt ist, 9 gesperrt und der Administrator bleibt unberührt. Benutzer, die durch das Tool gesperrt worden sind, erhalten in der letzten Spalte ein Schloss-Ikon und werden blau markiert.

Beachten Sie, dass standardmäßig das Tool einen Selektionsbildschirm hat, über den nach Benutzern gesucht wird, deren Sperrstatus = ‘ ‘ (Leerzeichen), was gleichbedeutend mit „0“ ist, was bedeutet, dass weder der Account noch das Kennwort des Users gesperrt ist.

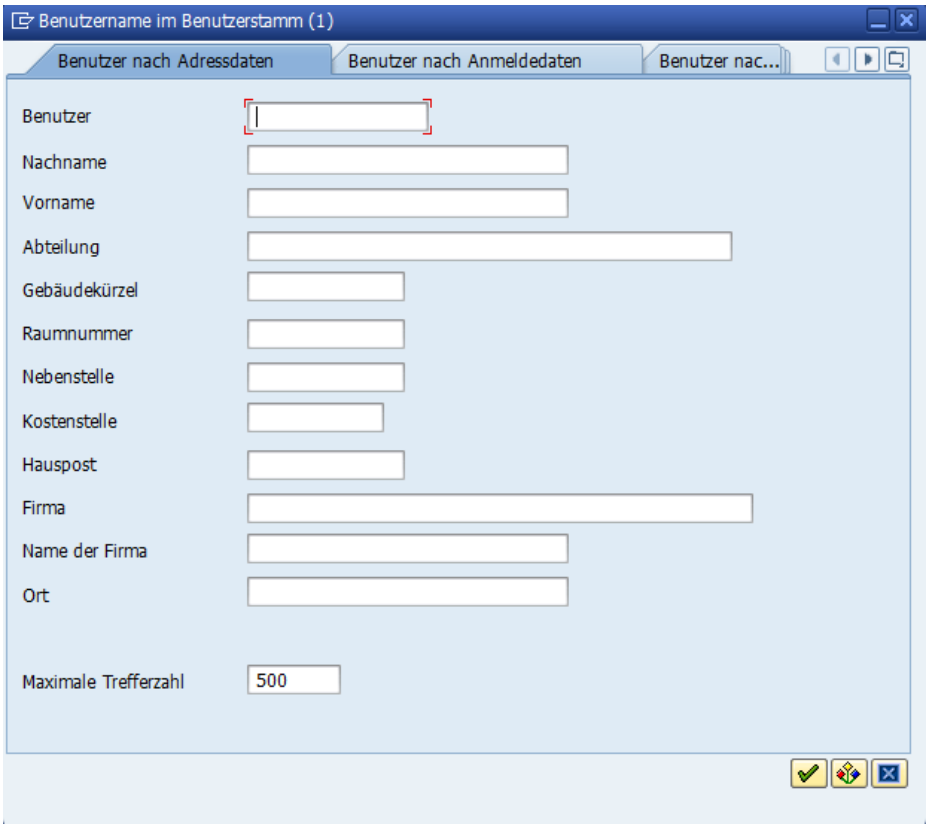
Das Xiting Locking Tool kann auch für viele andere Massensperraktionen im System genutzt werden. Um schnell Benutzer, mit einem bestimmten Sperrstatus zu selektieren, können die hierfür zur Verfügung gestellten Buttons auf dem Selektionsbildschirm verwendet werden.



- Alle User = selektiert alle Benutzer des Systems
- Gesperrt durch Xiting = selektiert alle Benutzer, die über das Xiting Locking Tool vorher gesperrt worden sind.
- Gesperrt durch ZBV = selektiert alle global über die ZBV gesperrten Benutzer (UFLAG = 32)
- Lokale Admin Sperre = selektiert alle lokal gesperrten Benutzer (UFLAG = 64)
- Nur PW ist gesperrt = selektiert alle Benutzer, die durch mehrfache Falscheingabe ihres Kennwortes gesperrt worden sind (UFLAG = 128).

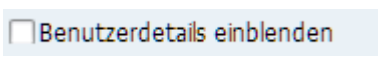
Beachten Sie, dass Kombinationen des UFLAG Status auch möglich sein können, da es sich um ein Bit-Feld handelt. Diese Kombinationen werden auch unterstützt.

Wenn Sie die über die Buttons zur Verfügung gestellten Selektionen nicht nutzen wollen, dann können Sie die zu verwaltende Menge über die F4-Wertehilfe für den Benutzernamen oder den Sperrgrund frei auswählen. Über die Suchhilfe können Sie auf alle Standardsuchen (z.B. Adressdaten, etc.) zugreifen:



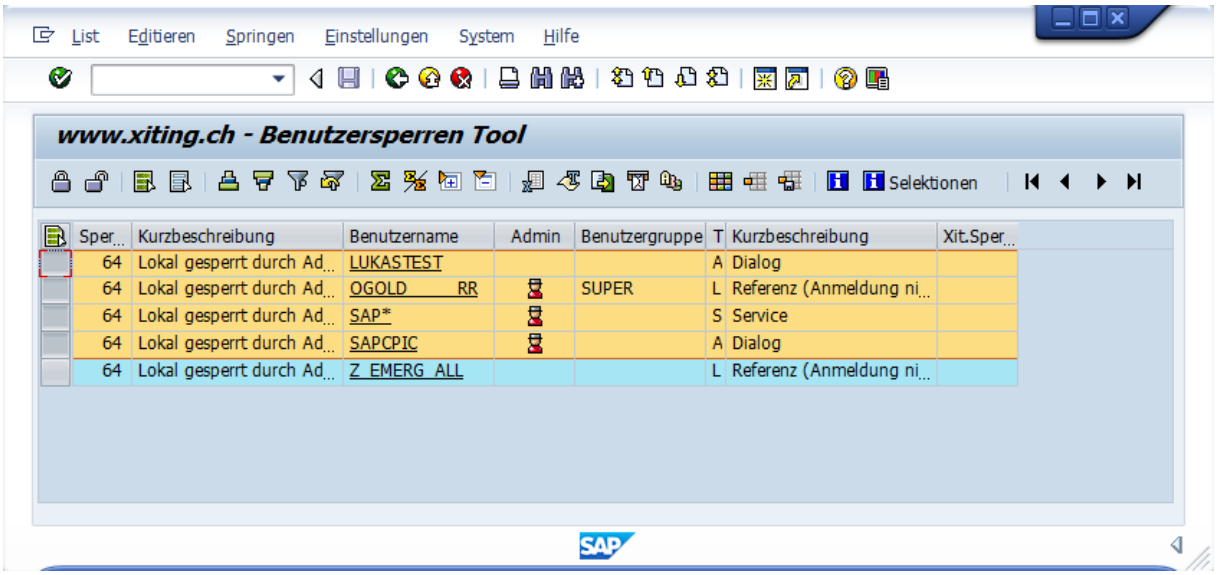

Nach der Selektion der Benutzer wird ein ALV (ABAP List Viewer) mit Informationen über die Benutzer und deren Status angezeigt.

Optional können Sie weitere Benutzerdetails in der Ausgabe anzeigen lassen, wenn Sie auf dem Selektionsbildschirm die entsprechende Option aktivieren:




Bitte beachten Sie, dass diese Option die Performance des Programms leicht reduzieren kann, weil die erweiterten Daten zusätzlich von der Datenbank gelesen werden müssen. Sie sollten diese Option daher nur beim direkten Arbeiten mit dem Programm aktivieren (Dialog), wenn Sie diese Informationen auch benötigen. Standardmäßig werden nicht alle zur Verfügung stehenden Spalten eingeblendet, können aber durch eine Layout-Anpassung des ALVs von Ihnen sichtbar gemacht werden.

Hier können Sie noch einmal überprüfen, ob die korrekte Auswahl getroffen worden ist und bei Bedarf auch nur durch eine Teilauswahl der Zeilen mit den dann markierten Benutzern weiter verfahren.




Um Benutzer zu (ent)sperren:

- Markieren Sie die Benutzer, die verarbeitet werden sollen durch Auswahl der Markierungsspalte ganz links oder verwenden Sie die Standardbuttons „alle markieren“ oder „alle entmarkieren“
- Klicken Sie entweder den „Sperren“ oder „Entsperren“ Button, die in der Menüzeile gefunden werden können.
- Sie erhalten ein Protokoll als Popup mit den Ergebnissen der Aktion (siehe unten):
    - “grüne Ampel” bedeutet, dass der Benutzer erfolgreich gesperrt worden ist.
    - “gelbe Ampel” bedeutet, dass der Benutzer ein Administrator des Tools ist und daher nicht gesperrt werden kann.
    - Jede andere Meldung aus den BAPIs wird als rote Ampel angezeigt, falls etwas nicht geklappt haben sollte. Dazu sollte es allerdings nie kommen, da alle Prüfungen vorher durchgeführt worden sind.

**Wichtiger Hinweis**: Wenn Sie mehr als 1000 Benutzer sperren/entsperren wollen, sollten Sie den Report im Hintergrund ausführen. Eine Ausführung im Dialog-Modus kann zu Programmabbrüchen und Dateninkosistenzen führen!

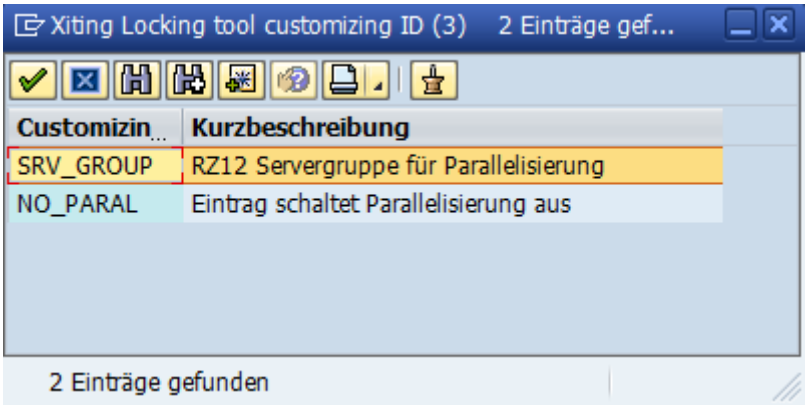
Viel Spaß bei der Verwendung des kostenlosen Xiting Locking Tools und bitte empfehlen Sie es weiter.

Falls Sie Fragen haben, Fehler finden oder Vorschläge haben, können Sie uns unter support@xiting.ch gerne erreichen.

## Hinweise zu Änderungen mit SP8:

Mit SP8 kam es zu einigen Performance-Verbesserungen (Sommer 2013). Einer hiervon ist, dass die Sperraktionen nicht mehr sequentiell sondern parallelisiert durchgeführt wird. Üblicherweise haben Sie keinen Grund, sich darüber Gedanken zu machen, da Sie es nur durch eine Verbesserung der Laufzeit merken werden. Wir bieten nun aber Parameter an, um diese Parallelisierung zu steuern.

Die Parameter werden über die Tabelle /XITING/LOCK_CUS erfasst:

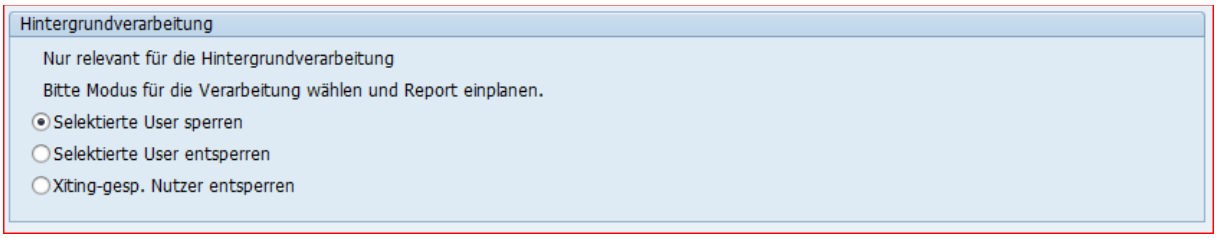



**SRV_GROUP**: Die Parallelverarbeitung nutzt die DEFAULT Servergruppen aus der Transaktion RZ12. Wenn Sie eine andere Gruppe verwenden wollen, kann dieser Parameter dafür verwendet werden, die alternative Gruppe zu erfassen. Invalide Einträge führen wieder zur Nutzung von DEFAULT.

**NO_PARAL**: Wenn Sie aus bestimmten Gründen auf die sequentielle Verarbeitung zurückgreifen wollen und sich auf die Lastverteilung des Administrators, der das Tool startet verlassen können, kann dieser Parameter gesetzt werden (Der Inhalt hierbei ist egal, wir schlagen „TRUE“ vor). Anschließend wird wieder sequentiell verarbeitet und der aktuelle Server hierfür verwendet.

**Bitte beachten Sie,** dass ab SP12 die Parallelverarbeitung nur für den Hintergrundmodus aktiv ist. Wird das Tool im Dialog benutzt, findet immer eine sequentielle Verarbeitung statt.

Nutzen der Hintergrundverarbeitung

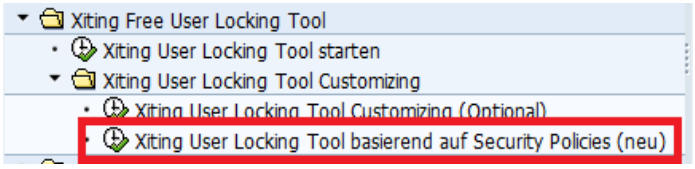


Mit SP11 können Sie den Report nun auch als periodischen Job einplanen und somit in der Hintergrundverarbeitung nutzen. Hierfür gibt es den neuen Bereich auf dem Selektionsbildschirm, über den Sie die gewünschte Verarbeitungsart einstellen können.

Wählen Sie hierfür wie gewohnt die Benutzer aus, die verarbeitet werden sollen und planen Sie anschließend den Report zur Ausführung über F9 im Hintergrund ein oder nutzen Sie alternativ die Standard-Joberstellung über eine Variante.

# 2 Sperren von Usern auf Basis von Security Policies

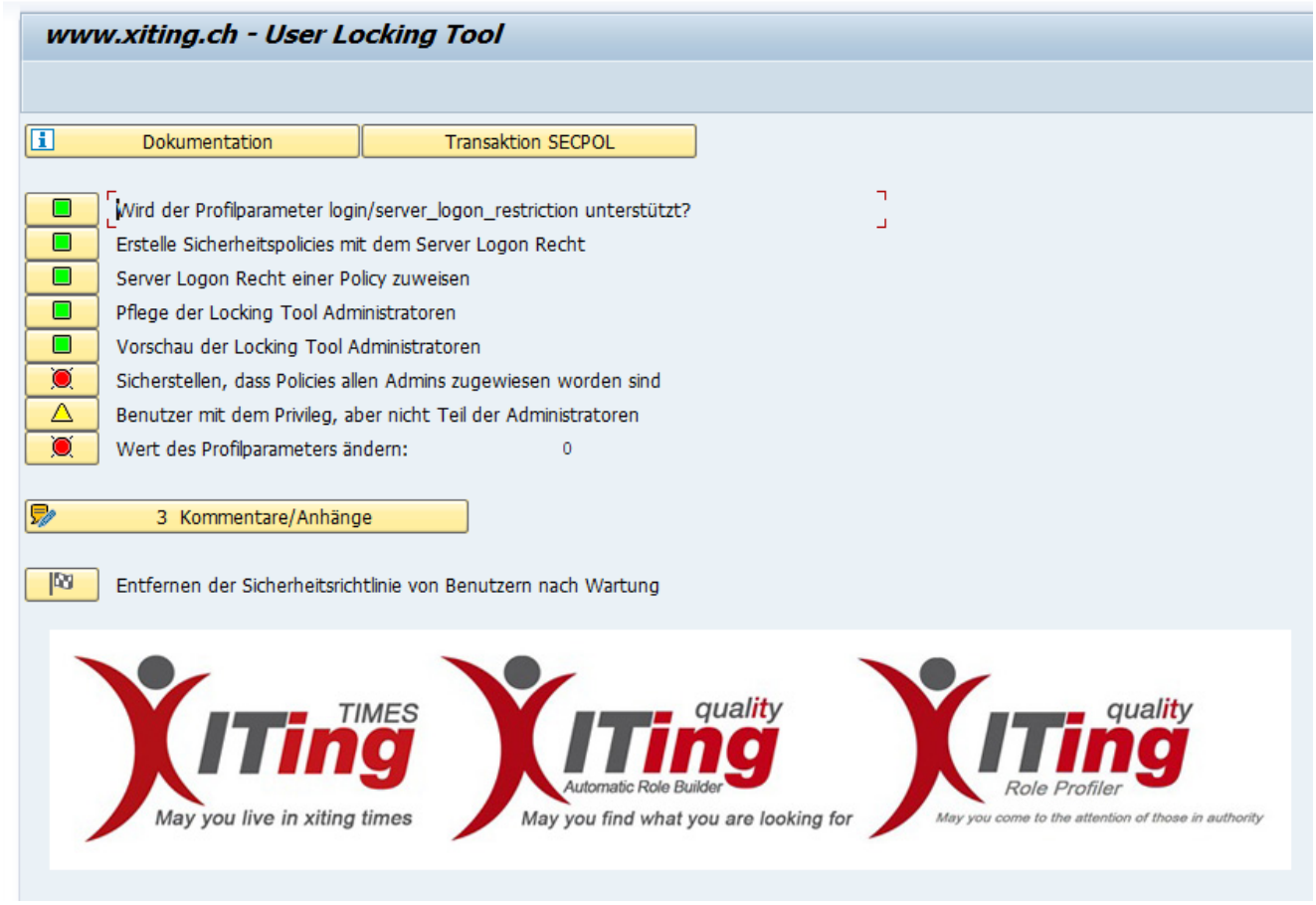
Ab SP10 steht ein weiteres Tool zum Sperren von Benutzern zur Verfügung.




Der Wizard kann über /XITING/ALL oder über die Transaktion /XITING/LOCK_WIZARD gestartet werden.

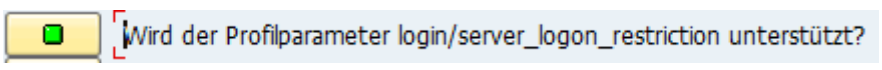
Über dieses Tool können Sie die neuen Security Policies nutzen, um den Zugriff auf das SAP System bei Wartungsarbeiten einzuschränken. Hierfür wird der Profilparameter login/server_logon_restriction genutzt, über den gesteuert werden kann, ob und wenn ja wer sich an dem System anmelden kann.

Die Voraussetzungen zur Nutzung des Tools können Sie im SAP Hinweis 1891583 finden. Das Tool prüft aber bei Programmstart selbst, ob alle Voraussetzungen erfüllt sind und zeigt diese durch Ampeln an:

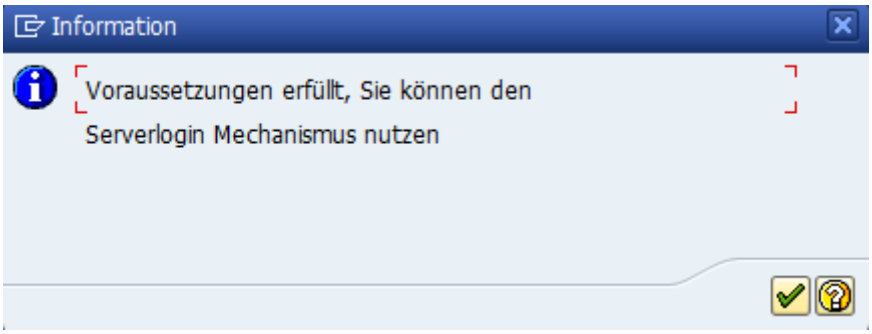



Das Tool ist wie ein Wizard aufgebaut, so dass Sie alle notwendigen Schritte von oben nach unten nacheinander durchgehen können.

Der Erste Schritt ist die Prüfung, ob das aktuelle System das Vorgehen unterstützt.

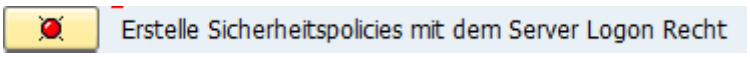


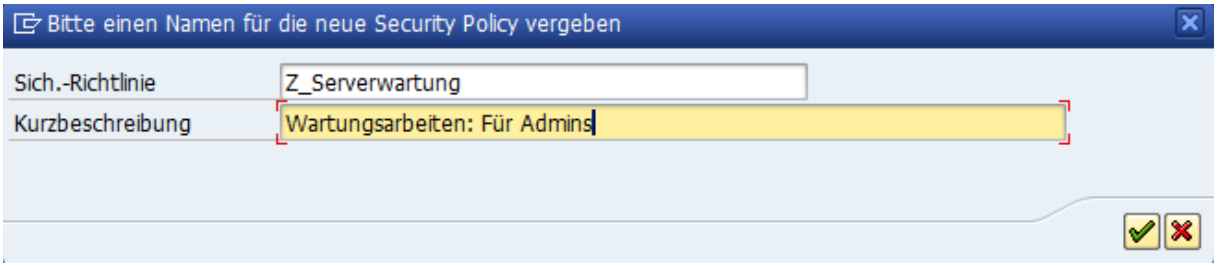

Durch einen Klick auf den Button kann die Prüfung wiederholt werden. Im Erfolgsfall wird dieses mit einer Meldung und der grünen Ampel bestätigt:




Im Fehlerfall erhalten Sie die folgende Meldung:

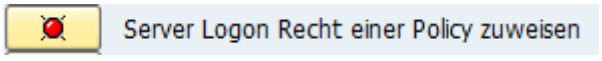

Sie können nun einen neue Sicherheitsrichtlinie definieren, die Sie für die Wartungen verwenden wollen:



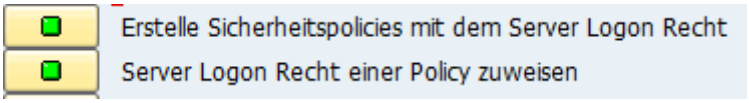




Nach der Abfrage eines Transportauftrages wird die neue Policy dann mit dem Attribut SERVER_LOGON_PRIVILEGE angelegt:

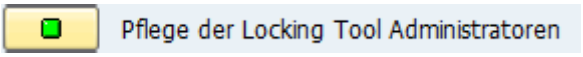

Alternativ dazu können Sie auch bereits bestehende Policies durch das SERVER_LOGON_PRIVILEGE ergänzen:



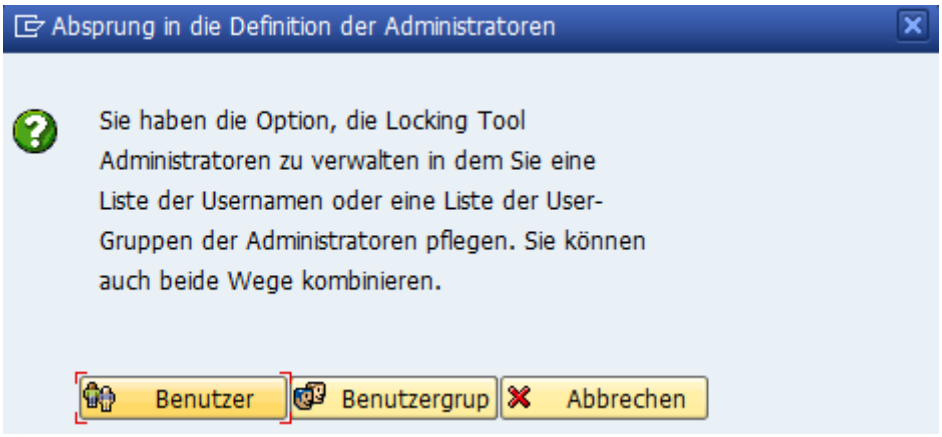

Sobald das System eine Policy mit dem Attribut findet, schalten die beiden Ampeln des WIzards auf grün um und die Schritte gelten als erledigt:




Sie können dann in dem nächsten Schritt

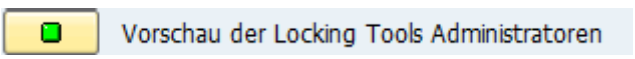



definieren, welche Benutzer von der Sperre ausgenommen werden sollen. Dieses können Sie sowohl über die User-IDs als auch über die Benutzergruppen festlegen:

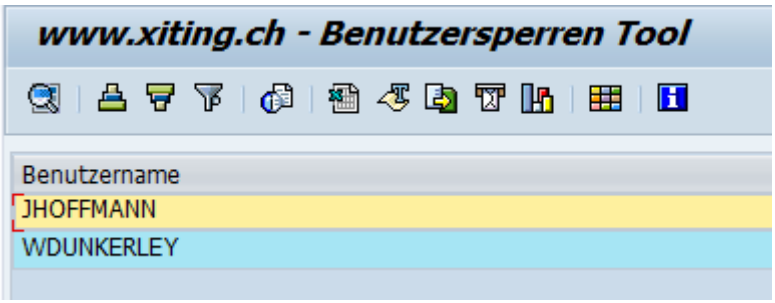


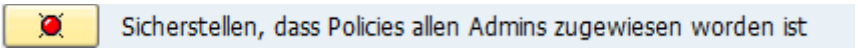

Die Administratoren, die Sie hier hinterlegen, sind dieselben, die auch für das ursprüngliche User-Locking-Tool verwendet werden. Sobald ein Eintrag in einer der Tabellen vorliegt, schaltet die Ampel auf Grün.

Die zugewiesenen Sicherheits-Richtlinien können anschließend in der SU01 eingesehen und/oder wieder entfernt werden:

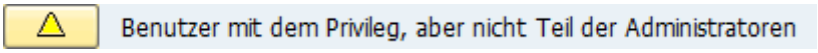




Über diesen Button können Sie sich alle Administratoren noch einmal anzeigen lassen, die sich aus der Summer der direkt hinterlegten Usern und allen Benutzern, die sich aus der Pflege der Benutzergruppen ergeben, zusammensetzen:



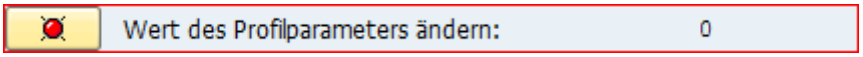

Wenn Sie Administratoren definiert haben, die noch nicht über das Recht zur Anmeldung bei Wartungen verfügen, wird dieser Schritt mit einer roten Ampel markiert. Über einen Klick auf den Button können Sie nun alle Admins auswählen, die der Policy noch nicht zugeordnet sind. Sobald alle definierten Administratoren einer Policy mit dem Attribut zugeordnet sind, schaltet auch dieser Punkt auf Grün.



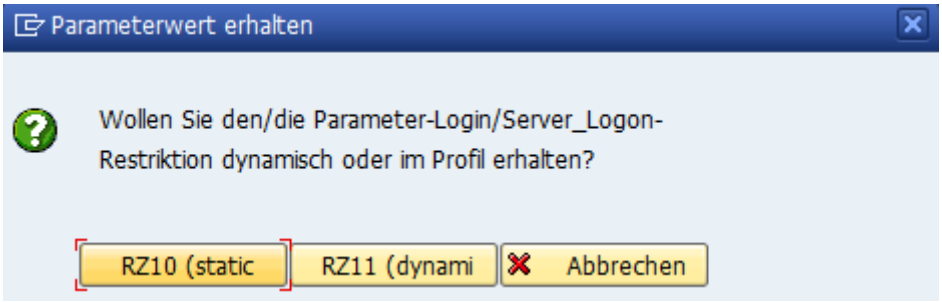

Sie können Prüfen ob es Benutzer gibt, die die Policy zugewiesen haben, aber nicht Teil der definierten Administratoren sind. Dies ist nicht obligatorisch, aber kann ein guter Hinweis sein.

Anschließend können Sie jederzeit über die Transaktion RZ11 den Wert für den Parameter login/server_logon_restriction dynamisch anpassen oder ihn über die Transaktion RR10 im Profil hinterlegen, so dass auch nach einem Neustart des Systems die Einschränkung zum Logon gegeben bleibt.

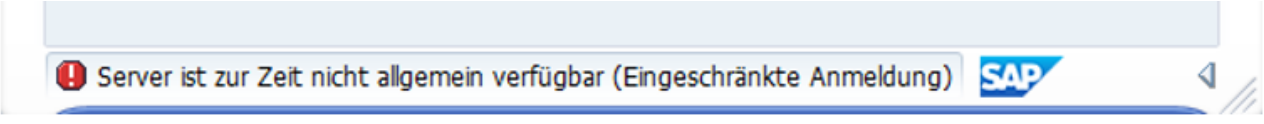
Ab SP11 wird Ihnen der aktuelle Wert des Parameters auch direkt in der Anwendung angezeigt.



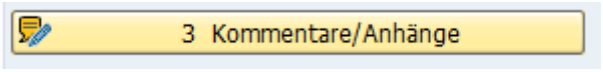

Über einen Klick auf das Ikon können Sie direkt in die entsprechenden Pflegetransaktionen abspringen.




Ist der Parameter auf den Wert 1 gesetzt, so wird verhindert, dass sich Benutzer anmelden können, die nicht über die Security Policy mit dem SERVER_LOGON_PRIVILEGE versorgt wurden:



Ab SP16 ist es möglich Kommentare zu pflegen und Anhänge zu speichern via dem entsprechenden Button.




Wenn die Wartungsarbeiten abgeschlossen sind, kann die Policy den Benutzern via dem folgenden Button wieder entzogen werden: