Xiting User Locking Tool

This document explains the usage of the Xiting User Locking Tool.

Version SP17

Product origin

The Xiting User Lock Tool is a free component of the Xiting Times, Automatic Role Builder, Role Profiler, ABAP Alchemist and Security Architect products of Xiting AG, Switzerland. The products can also be ordered as a service from SAP to correct SYSTEM type user authorizations and management for you.

For further information please see www.xiting.ch

Background

Many customers have developed various tools to perform mass locking and unlocking of users. These are often used for maintenance “windows” in the system.

There are several challenges when doing this, the main ones are:

- Protect the administrator(s) from locking themselves out.
- Prevent the locking of technical SYSTEM and SERVICE users.
- Lock only those users who are not locked already.
- Unlock only those users who were locked intentionally.
- Preserve change documents by respecting released APIs.

This SAP specific free software product Xiting User Locking Tool enables you to temporarily lock and unlock large sets of users. It “remembers” what you have done so that you can only undo changes that you made to a subset of the users.

Additionally it protects you from accidentally locking everyone out, including yourself.

Design concept overview for installation administrators:

The selection of users who are locked is stored within the Xiting application which locked them. Selected users and user groups can be protected from being locked by the application.

Only those users locked by the application itself can then be unlocked again.

The integration is based on released BAPIs. See transaction BAPI in SAP.

Comment on auditing requirements:

The BAPIs respect all standard change document related tasks when locking unlocking the users. These can be audited using transaction SUIM.

No additional auditing is required.

Comment on release dependencies:

This tool is developed for SAP Netweaver ABAP environments from release 7.00 onwards. We do not support use of the tool on lower releases.

Comment on alternate solution as of 2014:

SAP introduced a new solution as of 7.21 kernels for 7.31 systems onwards with SAP Note 1891583. You can now use logon policies and instance parameters to restrict the logon of certain users while protecting others. This is much more performance friendly than locking the application users.

Index

1 Xiting User Locking Tool

An integrated part of the Xiting Products is the Xiting User Locking Tool. The tool does not require any prior configuration, so can be used immediately after importing the transport requests.

Its primary intention is for administrators to be able to lock all users out of the system, except themselves as admins and special users based on their user type or user group. During maintenance periods such as upgrades and system copies this is often required. The users can then later be unlocked again, specifically only those who were locked via this tool and not those prior locked via SU01 (i.e. user master record is locked) or those locked due to incorrect logon attempts (i.e. the password is locked – but non-password based authentication is still possible) Typically this needs to be done manually with external lists or "blunt" scripting tools, which this tool now makes easier and faster to perform within the SAP application.

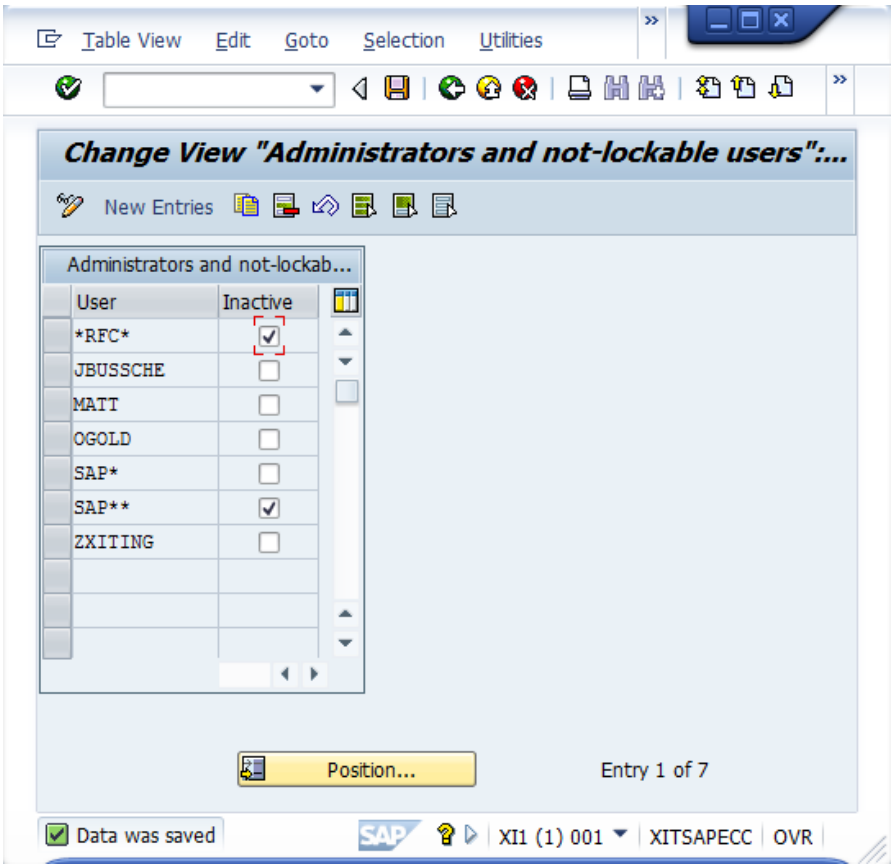
You can unlock users locked through other system tools here as well, so the tool can become your central access point to all user locking / unlocking tasks.

You can start the tool via transaction code /n/XITING/USER_LOCK.

If users are to be locked, the possibility should be avoided that the administrators also lock themselves. To make sure such an unintentional lock cannot happen, administrators can list usernames in the “Locking administrators table” and / or list user groups as “un-lockable” admins. It might be a good practice to list also the users needed for communication with other systems, running jobs and other important non-dialog user activity.

Note that this protection only applies to this tool. If you are authorized, you can still lock these users and yourself in SU01 or SU10.

The quickest way to maintain the “Lock administrators” table is to push the buttons “Maintain admins” or “Maintain admin groups” on the selection screen of the tool. Records of these tables are not subject to transport requests and must be maintained manually in each client of each system.



Note that you can also flag a user ID or a user group as inactive without having to remove it completely from the table. Additionally in the case of the user ID name table, it is supported to additionally use patterns, such as for example:

RFC* = users whose names start with RFC.

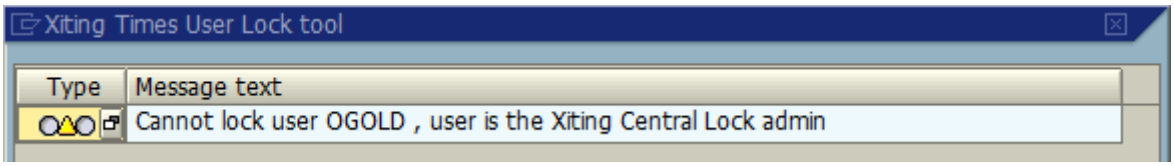
*RFC = users whose names end with RFC.

RFC = users whose names contain the pattern RFC.

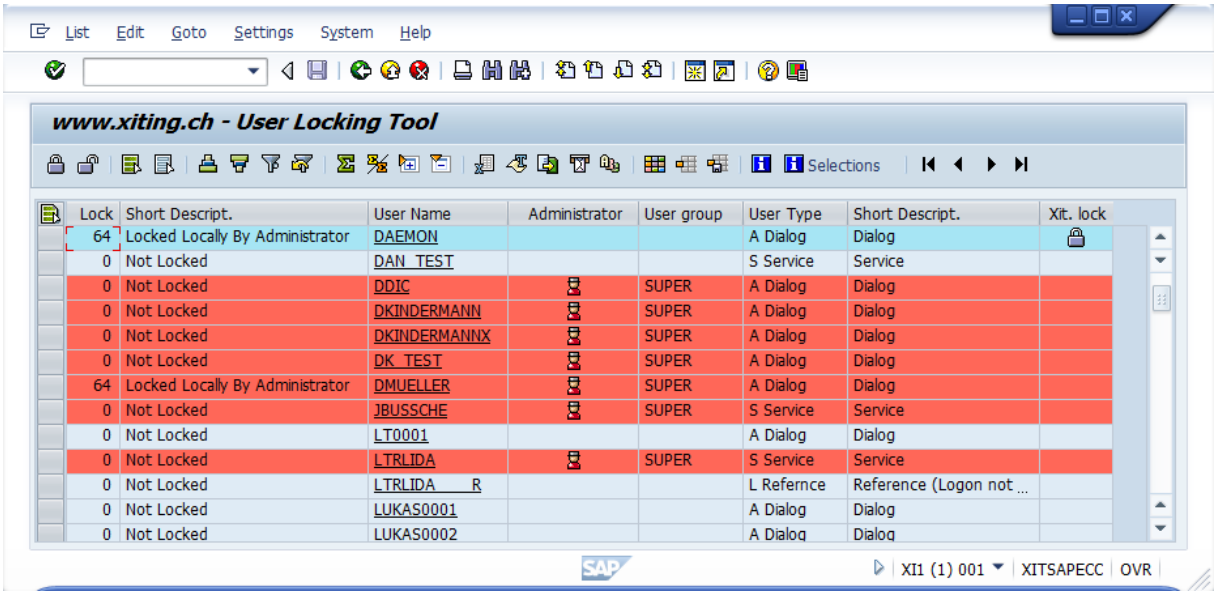
RFC = the user whose name is exactly RFC only.

In the special case of the user SAP*, you must enter the name explicitly as SAP** (two asterisks!) as the entry SAP* means all users whose names start with SAP* (e.g. including SAPCPIC, SAPBASIS, etc).

If you try to lock a user listed in these tables, you get an error message that the user cannot be locked.



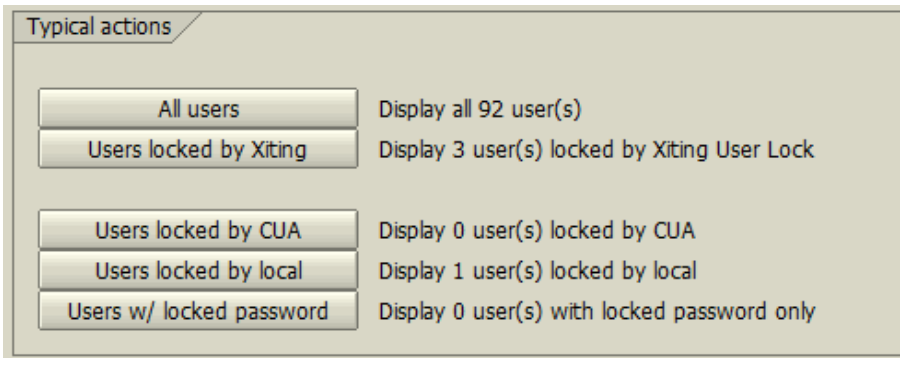
Additionally these users can be previewed and are displayed as red rows in the list with a special "administrator" icon:



The error does however not interrupt the program, so if for example you want to lock 10 users of which one is listed in the "Lock administrators" tables, then the program will lock the other 9 and leave the admin user unlocked. Users who are locked by the Xiting Locking tool have a Lock icon in the last column and will be marked blue.

Note that by default the tool has a selection screen which searches for users who have a lock status = ' ' (empty space) which is the same as "0" meaning that neither the user ID nor their password is locked.

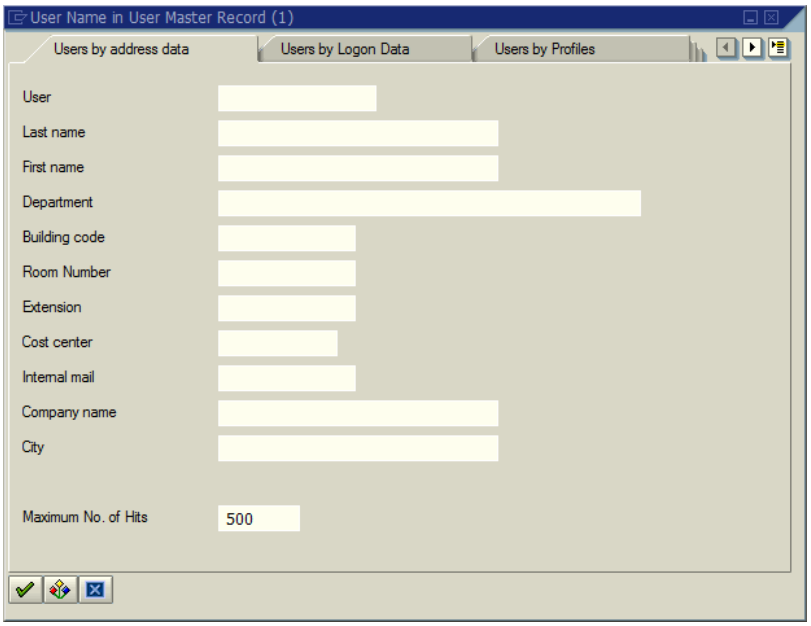
The Xiting Locking Tool can also work for various other mass user locking scenarios in the system. To be able to quickly select users locked with a certain status; you can also use the "push buttons" on the selection screen to automatically fill the selection criteria.



- All users = will select all users existing in the system
- Users locked by Xiting = will select the users who were currently locked using the Xiting Locking Tool
- Users locked by CUA = will select the users locked globally in the CUA (UFLAG = 32)
- Users locked by local = will select the users locked locally in the system (UFLAG = 64)
- Users with locked password = will select those users who were not locked explicitly but only locked their use of a password by entering a wrong password too many times (UFLAG = 128).

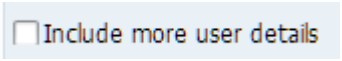
Note that combinations of the UFLAG status are also possible as it is a bit-flag. Combinations of the UFLAG status is also supported.

If you don`t wish to use the selections available through the buttons, you can select the users you want to see / lock / unlock yourself using the F4 search help. You can list users using the SELECT-OPTIONS for user name or for lock type. The F4 search help also offers extended complex search criteria for the users, for example via profile names or via address data attributes:



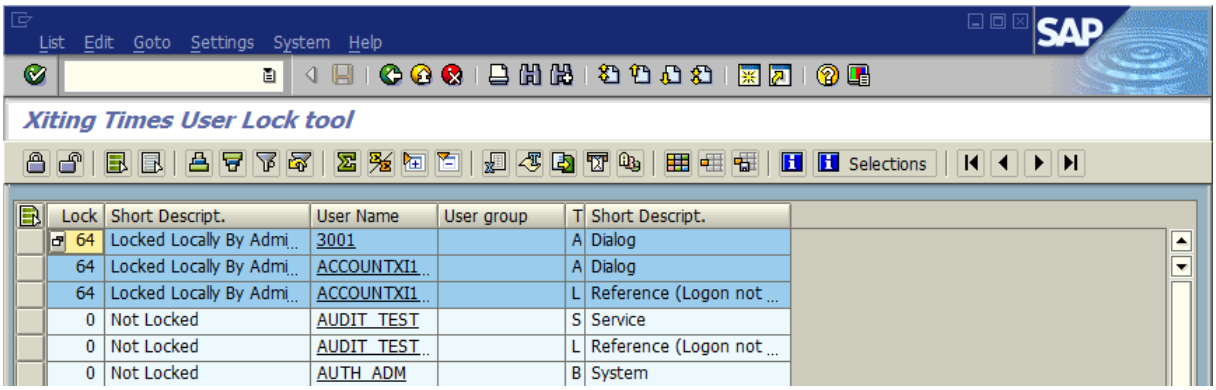
After the selection of the users an ALV (ABAP List Viewer) with information about the selected users and their status is shown.

Optionally you can display further user related details in the list when selecting the check box on the selection screen:



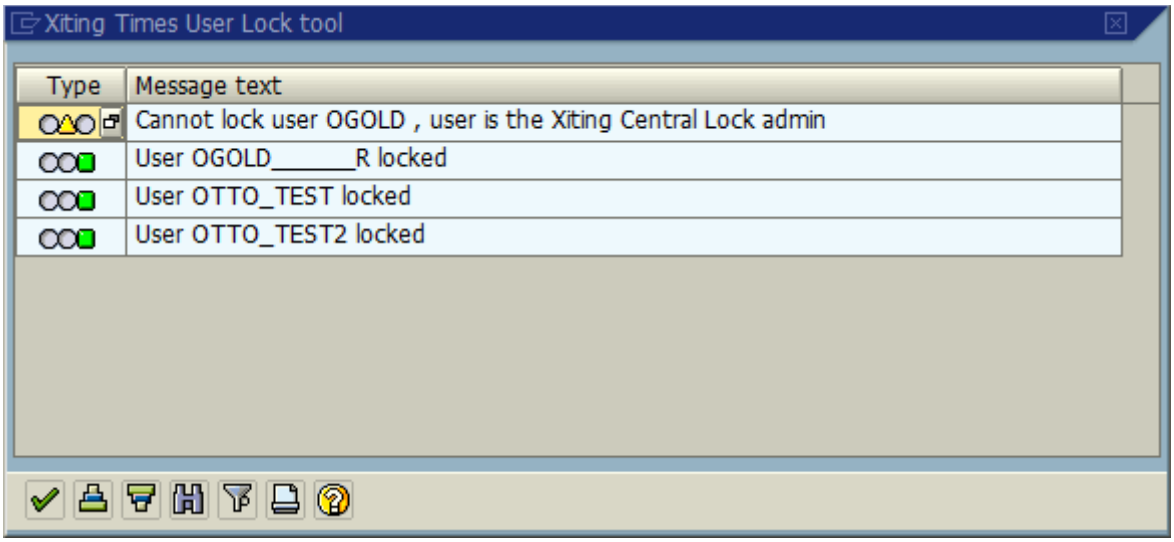
Please note that this option will reduce the performance of the output slightly because the data needs to be selected from the data base in this case. So only use it in dialog mode when you need to access that information in the list. Per default not all available fields are displayed. You can however display them by changing the ALV layout easily.

Here again you can check that the correct users were selected and also mark only sub-sets of the selected users for further processing of the lock or unlock.



For locking and unlocking users:

- Select the users you want to change using the boxes on the far left or you can use ALV standard buttons "Select all" and "Deselect all"
- Click either the "Lock" or "Unlock" button which you can find as first two icons on the bar.
- You will receive a popup protocol with the results of your action (see below):
    - "Green light" means that the users was locked successfully
    - "Yellow light" means that the user is an administrator of the locking tool and cannot be locked.
    - Any other message coming from the system functions / BAPIs would appear in red if anything goes wrong. This should however never happen as all checks are performed prior to the save.



Important Note: If you want to lock/unlock about 1.000 users or more you should execute the report in the background, as doing so in online mode can lead to runtime errors and therefore to data inconsistencies.

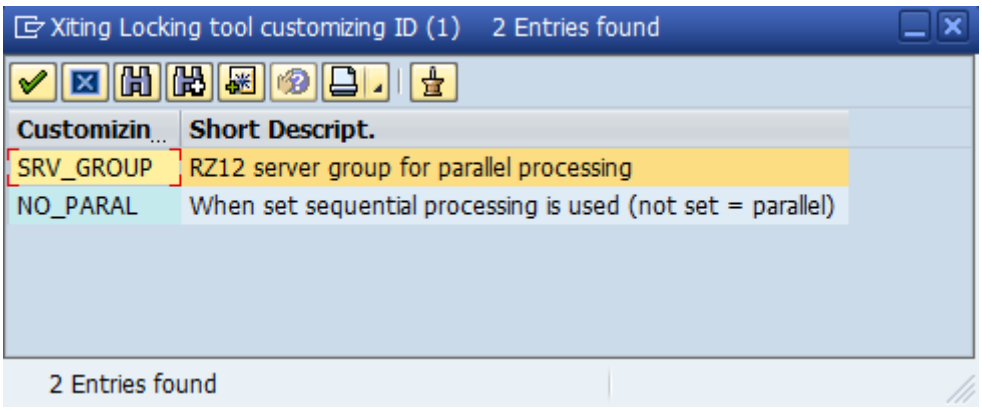
Have fun with the free Xiting Lock Tool and feel free to recommend it further.

In the case of questions, bugs or suggestions, you can contact support@xiting.ch

Notes on changes with SP8:

Several performance improvements were made with SP8 (Summer 2013). One of these was that the locking and unlocking of the users was no longer performed sequentially but use parallel processing of the users in blocks. Normally you will not need to consider this and will only notice improved performance times, but we now offer customizing switches to control the parallelization.

Via table /XITING/LOCK_CUS you can maintain them:

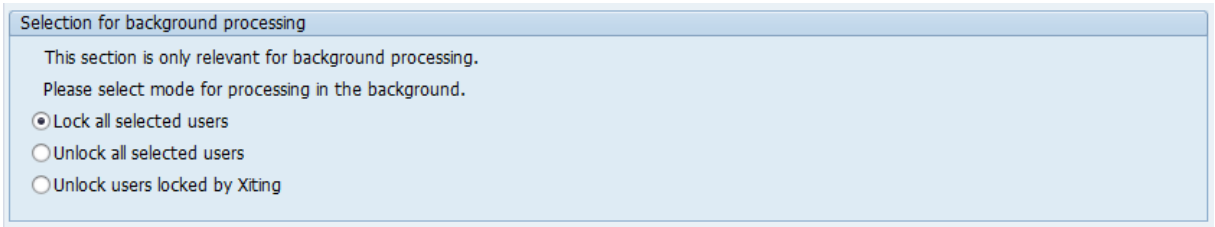


SRV_GROUP: The parallel processing will use the DEFAULT server group from transaction RZ12 for the processing. If you wish to use an alternative server group, then you can use this switch to maintain the alternative group name in the PATH field of the customizing. Invalid group names will divert to DEFAUT again.

NO_PARAL: If for some reason you wish to use sequential processing and rely on the load balancing of the administrator user who is starting the Locking Tool, then you can activate this customizing switch and maintain any value (e.g. "TRUE") in the PATH field. In this case, the locking / unlocking will be performed sequentially and on the server of the currently logged on user.

Please note that as of SP12 the parallel processing is only used for the background processing mode. When the tool is used online then the locking is always done sequentially.

Using the background processing

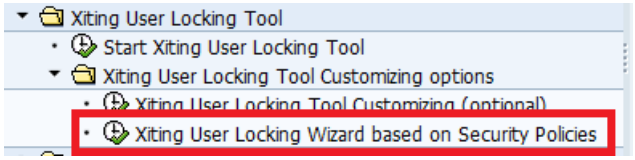


With SP11, you can now schedule the report as a periodic job and use it in the background processing. For this, there is the new field on the selection screen, which allows you to set the required processing.

Therefore select the users which should be processed as usual and then schedule the report for execution via F9 in the background, or alternatively use the standard job creation through a variant.

2 Lock users based on security policies

As of SP10 another tool for locking users is available.



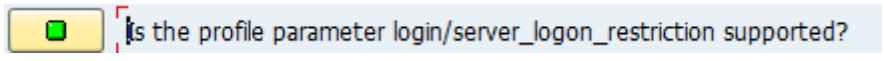
The wizard can be launched from /XITING/ALL or by transaction /XITING/LOCK_WIZARD.

Using this tool, you can use the new security policies to restrict access to the SAP system for maintenance. For this purpose, the profile parameter login/server_logon_restriction is used to control whether and if so who can log on to the system.

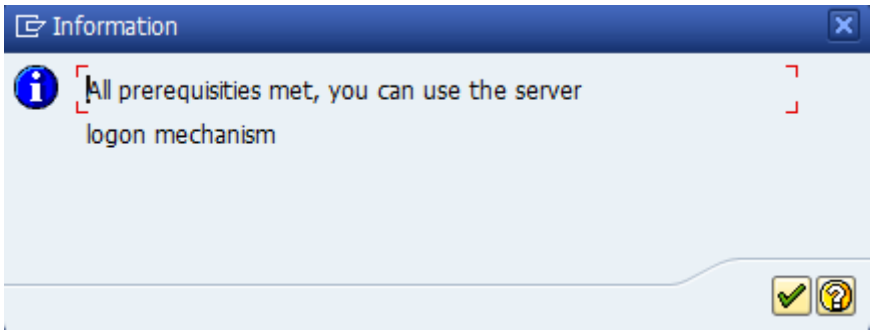
The prerequisites for the use of the tool can be found in SAP Note 1891583. However, the tool checks at startup if all requirements are met and displays the result of it through traffic lights:

The tool is built like a wizard, so you can go through all the necessary steps from top to bottom.

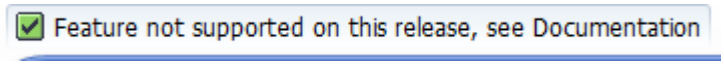
The first step is to check whether the current system supports this procedure.



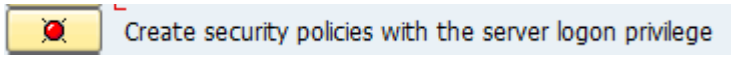
By clicking on the button, the test is repeated. If successful, this is confirmed by following message and the green light:

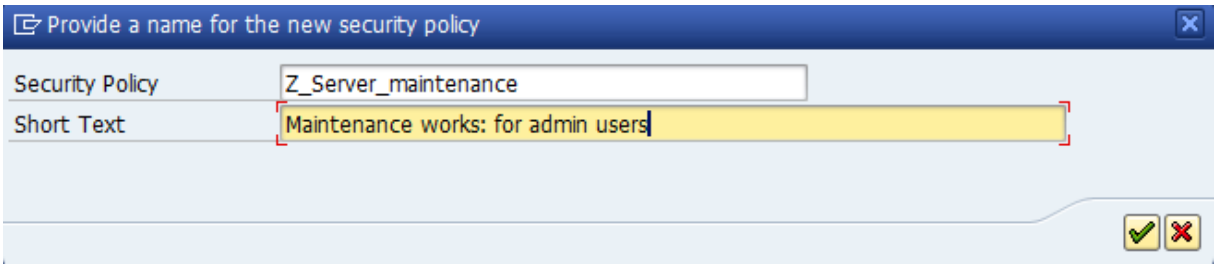


In case of an error you receive the following message:

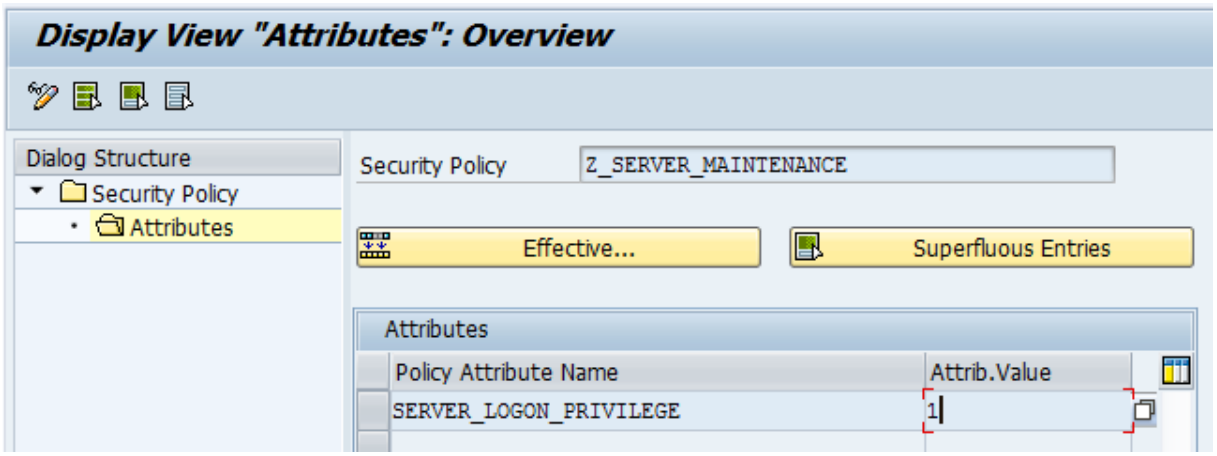


You can now define a new security policy that you want to use for the system maintenances:

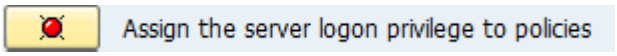




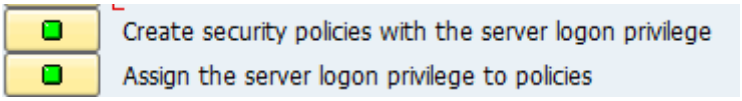
After recording the entry into a transport request, the new policy is created and the attribute SERVER_LOGON_PRIVILEGE will be assigned:



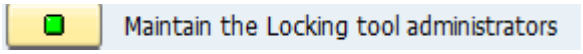
Alternatively, you can also assign the attribute SERVER_LOGON_PRIVILEGE to existing policies:



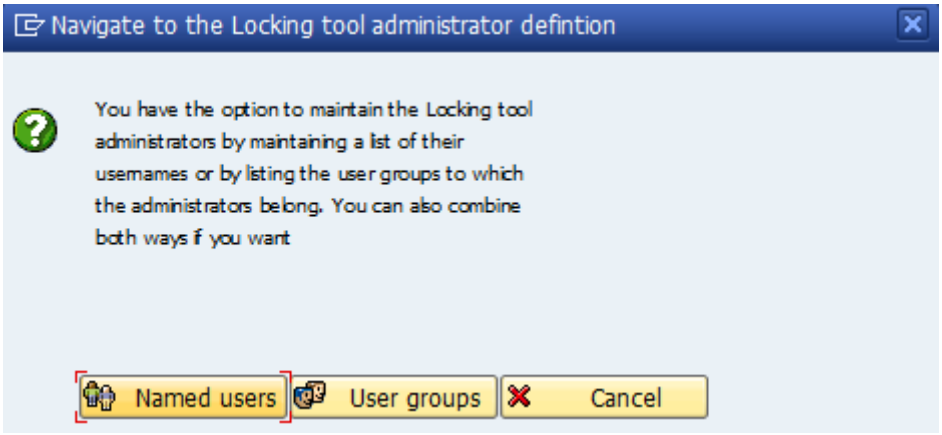
Once the system finds a policy with the attribute, it switches the two buttons with traffic lights to green and the wizard steps are considered to be done:



In the next step

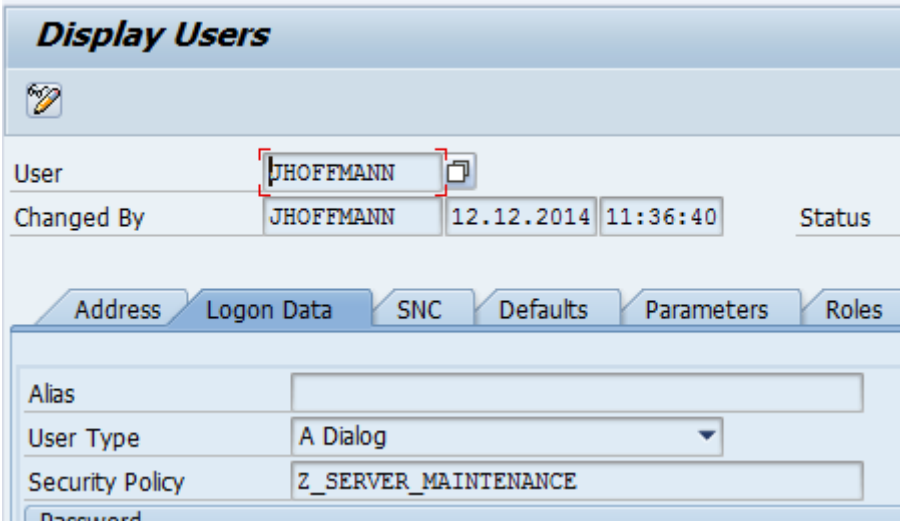


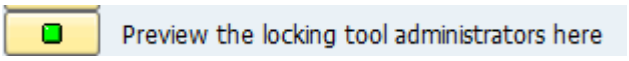
you can define which users should be excluded from the locking. Here you can specify both the user IDs and/or the user groups:



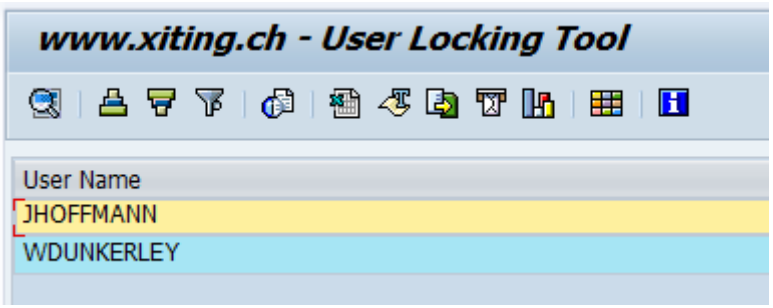
The Administrators you define here are the same as those used for the original user-locking tool. Once an entry is present in one of the tables, the traffic light turns green.

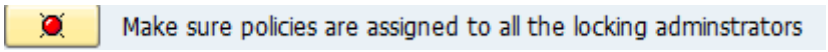
The assigned security policies can then be viewed in transaction SU01 and can also be removed again there:



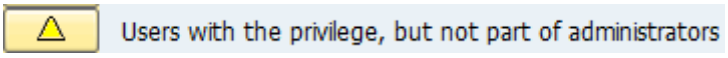


With this button you can view all administrators that are determined by the user IDs or the assignment to a chosen user group:





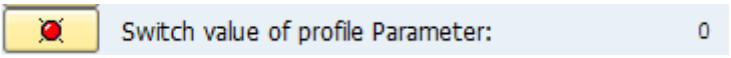
If you have defined administrators who do not yet have the privilege to log on during maintenances yet, this step is marked with a red light. You can now select all admins who are not yet assigned to the policy by clicking on the button. Once all defined administrators are associated with the attribute, this step will turn green.



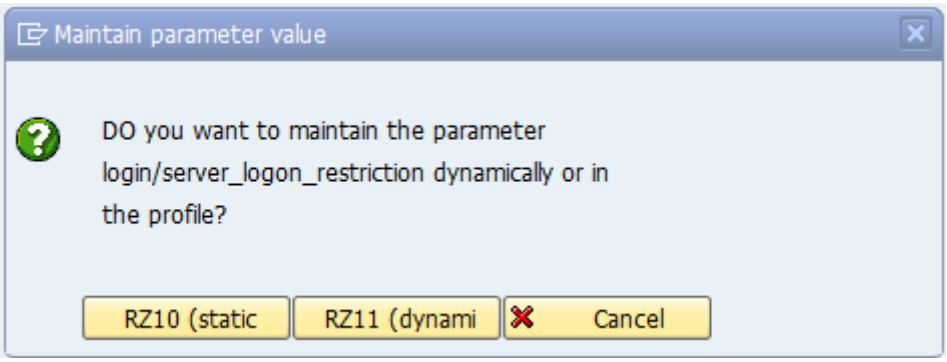
You can check users that have the privilege but are not part of the administrator group with this button. It's not mandatory but might be worth checking who else got the privilege.

Now you can switch the value of the parameter login/server_logon_restriction any time using the transaction RZ11 or RZ10 if you want to make it persist after server restarts.

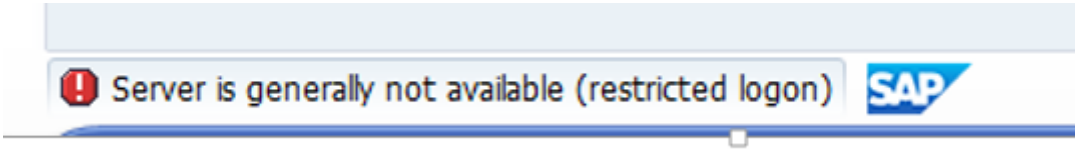
From SP11, the current value of the parameter is displayed directly in the application.



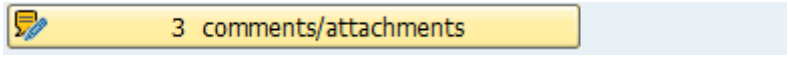
You can jump directly to the corresponding maintenance transactions by clicking on the icon.



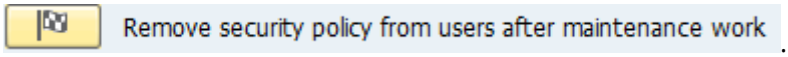
If the parameter is set to the value 1, it prevents users from logging on that have not been assigned a security policy with the SERVER_LOGON_PRIVILEGE attribute:



As of SP16 it is possible to maintain comments and add attachments via the corresponding button



When the maintenance work is done, you can remove a security policy from the users via



.