BULLETIN

Technical newsletter of BMT Medical Technology s.r.o.

Issue 09
April 2016

Change in Policy of Service Technicians Access Rights for the STERIVAP®/UNISTERI® Devices as from 2016

BMT Medical Technology s. r. o. met the requirements of our clients regarding possibility of validity limitation for the password needed for entering the service menu of large steam sterilization devices. In case of interruption of co-operation with a service technician, he will not have a chance to abuse access to service menu after the password validity termination.

In brief: at the present time, you can encounter five passwords within large steam sterilization:

Password with unlimited validity for older version
UNISTERI® HP
STERIVAP® HP

Password with limited validity - 3, 6 months and 3 years
STERIVAP® HP starting from version V149
UNISTERI® starting from version V131
STERIVAP® SL

Distribution and Conditions for Password Obtaining

The passwords will be generated on request and passed to our partners´ and branch offices´ service management and the passwords will be sent to company e-mails only. Further distribution will be on your decision and responsibility in the given field of activity. Requests for a password assignment can be sent to *support@bmt.cz* – with the subject "limited password". In case you are included in distribution of a monthly password within the scope of MMM GmbH., you will get the passwords in the mail.

The changes are bound to firmware – STERIVAP® SPHP starting from the version V149, UNISTERI® SPS starting from the version V131, STERIVAP® SPSL starting from the version 1.5. That indicates that the new service attitude cannot be applied to devices in field, with lower firmware version. This can naturally be solved by an upgrade of the existing firmware to the latest versions where the circumstances allow doing so (it is not possible to perform upgrade everywhere, due to validated processes.)

Time periods characterizing the password expiration are set by three fixed categories A, B and C (for example login: servB), corresponding to the period of 3 months, 6 months, 3 years. Warning: these are not time periods starting from the moment of access codes generation, but calendar quarters, half-years, respectively years. So the generated codes will be functional in the calendar period in which they were generated. This may lead to the fact that if it is the intention to provide someone with e.g. three-month password, while the quarter is coming to the end, it will be necessary to generate two passwords – one for the rest of the quarter and the other for the following full quarter.

Regarding the devices STERIVAP® SPHP and UNISTERI® SPS there applies that in case of wrong password entering during service technician´s login there is applied a time restriction, which in case of wrong entry may lead up to the error "Unauthorised System Access". The restriction times between the individual trials are as follows: 5, 10, 20, 40 sec. If the restriction time is running, it is not possible to enter the password and the keys Enter and back are grey (inactive).

Regarding the devices STERIVAP® SPHP and UNISTERI® SPS there applies that login of a regular service technician has a limited time validity of 12 hours. After the time limit expiration, the service technician is automatically logged out. Time runs even in switched off device, unlike original solution at older versions. Warning: do not confuse time validity of service technician´s login and password expiration according to A, B and C categories.

The passwords of all the service technicians is now 8 characters long (the password length at original line of devices STERIVAP® SPHP and UNISTERI® SPS was 12 characters).

Devices with the new access application:

- STERIVAP® SPSL – starting from version 1.5
- STERIVAP® SPHP – starting from version V149 (all the mutations of trade names – HP, HP IL, ...)
- UNISTERI® SPS – starting from version V131 (all the mutations of trade names)

In relation to devices STERIVAP® SPHP and UNISTERI® SPS there applies that as from the new versions of firmware, i.e. V149 and V131, there are also re-worked the general access rights of all the possible device users. The adjustment was required by some clients who required for the sterilizers software to comply with regulations according to **FDA – CFR 21, Part 11.** The regulations deal with electronic records and signatures and they affect the access of users to the device (login). The administrator may switch off the new and more strict access, in such a case the device will behave

like with former versions of firmware.

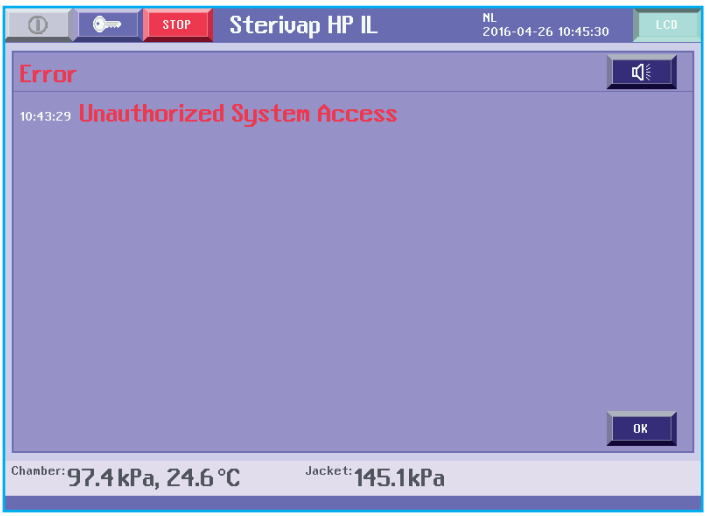
Reworking of Access Rights of Users for the Devices STERIVAP® SPHP and UNISTERI® SPS according to the Regulations FDA – CFR 21, Part 11

The changes are bound to firmware – STERIVAP® starting from the version V149, UNISTERI® starting from the version V131. That indicates that the new access will not function with devices in the field, with lower version of firmware. Naturally, this can be solved by an upgrade of the existing firmware to the newest versions where circumstances allow so. (It is not possible to perform upgrade everywhere – due to validated processes.)

Now, the system-forced passwords have minimal length (number of characters), a shorter password will not be accepted. The password length will be set by an administrator.

In case of a password change, the system remembers the history of three recent passwords and it will not allow for a new password to be used in case of being identical with any password in the history.

In case of wrong password entering during operator´s login there is applied a time restriction, which in case of wrong entry may lead up to the error "Unauthorised System Access". The restriction times between the individual trials as from the second trial are as follows: 5, 10, 20, 40 sec. If the restriction time is running, it is not possible to enter the password and the keys Enter and back are grey.



Similarly to the original line STERIVAP®/UNISTERI®, the administrator has a factory-set access codes: name "admin", password "heslo". But after the first login, he is forced by the system to change the password according to his own selection.

The rights of the administrator remained the same as in case of the original STERIVAP®/UNISTERI® line, there was only added setting of minimal password length, time of users´ passwords expiration and selection of required / non-required signature in the protocol in the end of the cycle.

As well as in case of the original STERIVAP®/UNISTERI® line there remained preserved the basic philosophy of division into the "Individual access rights" (strict mode) and "Mass access rights" (benevolent mode). The administrator is responsible for the branching settings. Now, the users name at mass access rights is "openuser", not the original "freeuser". (The original "freeuser" seemed to native speakers from the US to be rather a cured drug-addict than a nurse.)

In the mode "Individual access rights", each user is forced – after his/her rights setting by the administrator – to select his/her own password. The password set by the administrator always serves for the initial login only.

In the "Individual access rights" mode, the passwords have limited time validity set by the administrator. As soon as the user´s password validity is over, the user must change the password at the following login – logout is not automatically performed. In case of changing a password, it is necessary to enter the old password at first and then to enter the newly selected password twice. The password change may be performed even before the time expiration, via the main menu in the "Access Rights" item.

Any password change of any user is recorded in the audit trail.

Any login of any user is recorded in the audit trail.

If a new option "Password required" is selected in the "Individual access rights" mode, then – in the end of the cycle, after acceptation of login with the end of cycle and before possible printing of the protocol – a screen asking for signature is displayed. The signature is added by an operator responsible for appropriately performed cycle. He does so by adding his login name and password to prepared columns. If he is identical with the currently logged in person, the login name is already filled in, it is necessary to enter the password only. There are 3 trials available for the correct login data entry. If none of the trials is accepted, the protocol will read "Invalid Signature". If everything is OK, the protocol will read "Person responsible for the cycle" plus the name and time of signature. The title "Invalid Signature" does not mean for the cycle not to be performed OK. It only means that the process has not been approved by an authorised person. (Those who do not want to use simply do not have to, but the CFR 21 requires it.)

In case of double-door devices with touch panel on both sides it is possible to add the signature on any side. The signature is a part of the protocol, it will be also included in possible presentation from the PrinterArchiv. A successful signature will look like e.g. the following: "Person responsible for the cycle: Anna Novotná (1) 2015-03-20 14:35:08". Number one in brackets means that the signature was added from the main panel side.

In case of an automatic start, the signature is required in the end of the process and it will look e.g. as follows "Auto-Start- responsible for the cycle: Anna Novotna (1) 2015-03-20 14:35:08".

BMT Medical Technology s.r.o., Cejl 157/50, Zábrdovice, CZ 602 00 Brno
tel.: +420 545 537 370
e-mail: servis@bmt.cz
www.bmt.cz