Enterprise Client Parameter Locks

The parameter locks of the client software have two important functions. On the one hand, the complexities of the configuration options will be reduced, which will give the software interface a more streamlined appearance. Any parameter fields for functions that are not required, are deactivated, and the user will only see setting options relevant for his environment. On the other hand, default settings can be defined, which cannot be changed by the user, which eliminates faulty configurations and unwanted connections. With default settings, the user only needs to enter his personal passwords after installation, in order to establish a connection.

The Secure Enterprise Client software can handle the administration, configuration, and deployment of many users in larger VPN environments via Secure Enterprise Management.

Terminology "Profile"

In older versions of the Enterprise Client (<9.1), the collection of individual configurations was called a "telephone book". Starting with version 9.1 these are called **Profiles**. To edit a profile, select this configuration menu option, then a profile, and open the relevant **Profile Settings**. Completed profile configurations will then be stored as **Profiles** with a unique name in the configuration menu of the Client. For the purposes of better understanding, a **Profile** can also be called a **Link Profile**, as opposed to "Wi-Fi profile", "certificate profile", etc..

Enterprise Client parameter locks can only be created via Secure Enterprise management (SEM). Please read the Management System description (**SEM-Navigator**) for information on how to proceed for the creation of parameter locks. Here, only the required steps for the assignment of general user rights up to the customisation of the software are included.

The administrator uses templates for the creation of a software configuration with the Management System by means of a Client Configuration Plugin, which at first all users can use that are assigned to a specific group.

This template will be modified step by step for each user, resulting in individual profiles with profile specific locks, and also differentiations in regards to parameter locks.

Furthermore, older profiles, which a user may have created earlier, can be deleted automatically during (configuration) updates.

The new profiles with their respective parameter locks will then be automatically distributed with their user specific Monitor menu interfaces (CNF file) by the Management System, providing a (configuration) update. Please also read the automatic update description (and the configuration update) for Secure Enterprise Management.

The following applies for Enterprise Client parameter locks:

– They are created centrally, and distributed automatically to the user's remote PCs;

– Access rights for configurations within the Client Monitor menu are separate from

– Access rights for profile configuration (in the telephone book);

– both can be combined user specifically via separate profiles;

– Parameters can be hidden individually within the configuration fields of a profile, e.g. locks can be differentiated according to specific links;

– parameter locks can be removed by entering "User" and "Password" until the next configuration update, or until the next startup of the Monitor by entering a one-time password.

Configuring a Template with Parameter Locks

Group specific and user specific parameters

All values and entries of a template configuration are identical for all members of an organizational group, for which that template applies – with the exception of personal codes.
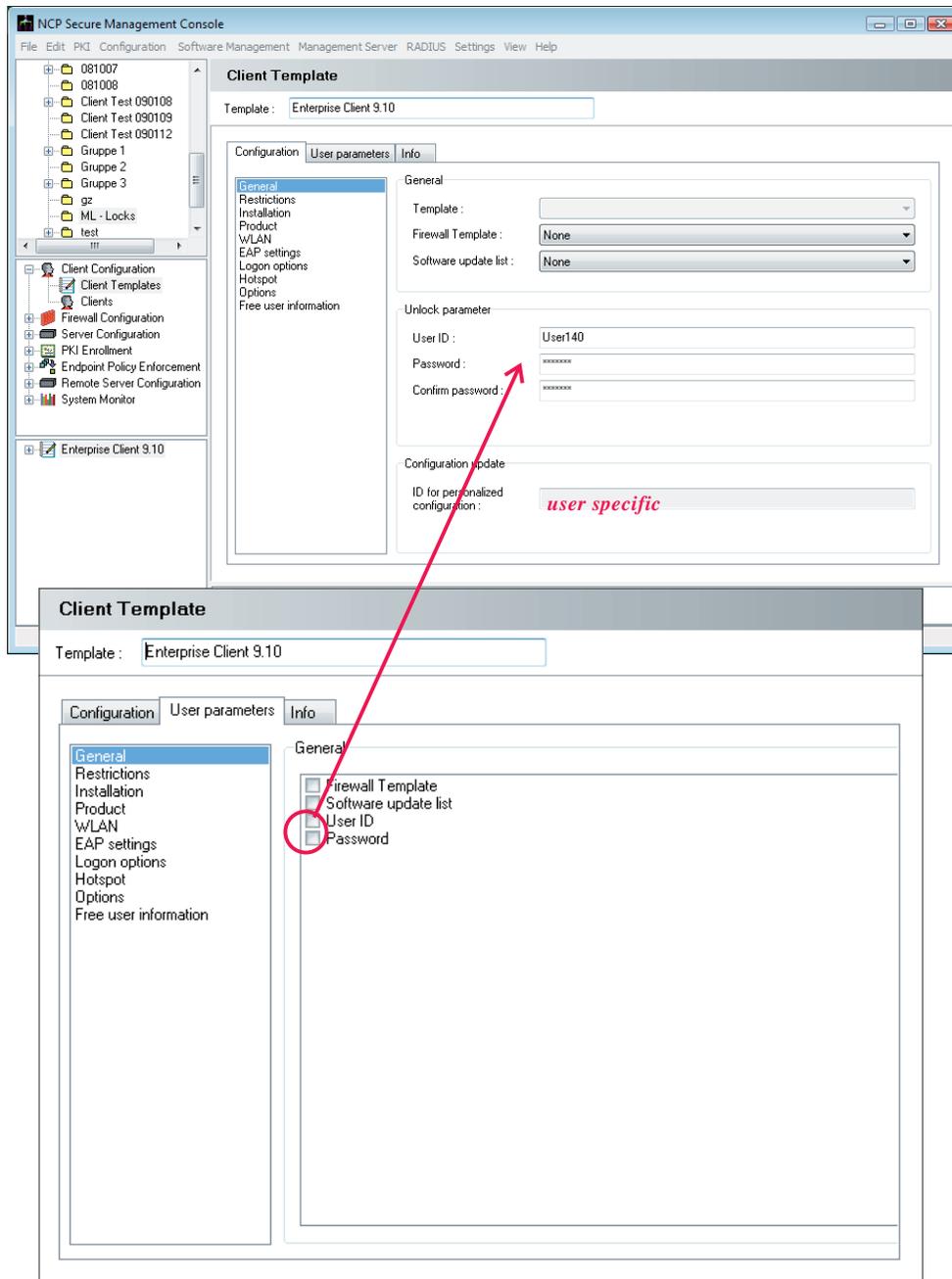
The template parameters, whose entry fields have been deactivated (illustration left), must be entered at the end of each client configuration..

The template parameters, to which this should apply, can be defined in the template field of the user parameters (see illustration bottom left).

Example: By default, the parameters "User ID" and "Password" can be configured, when the template is first opened in the configuration area, while the "ID for personal phonebook", the user specific profiles, can not be modified.

That means that all user configurations, for which this template will be used, will have identical codes for "User ID" and "Password" in order to remove the parameter lock, but will have a unique ID for personal link profiles. This code will have to be entered at the end of the client configuration.

Please note that this configuration defines only, which parameters will be identical for all members of an organizational group, and which will only be entered at the end of the client configuration. These so-called "User Parameters" will have their checkbox selected.

In regards to the parameter lock, this will only define whether all users will receive the same code to remove the parameter lock, or whether they will receive individual codes.

Authorisation

With "Authorisation" (see illustration below), the administrator can define group specific locks. He will define here, how the user interface of the Monitor should look, which configurations should be preset, and whether or not the user will be authorised to modify profiles (in the phonebook).
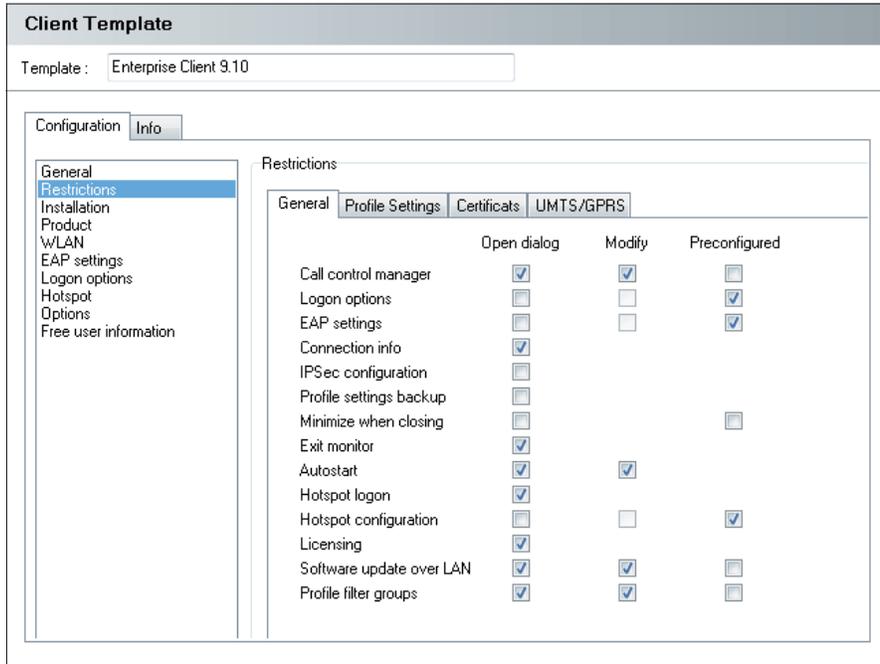

Client Monitor Menu (General)

Authorisations in this field refer to dialogs in the Client Monitor, located in the menu option "Configuration" and "Window". The administrator can define authorisations, which will allow the user to 'only' open dialog boxes, and view default settings, or to modify the parameters displayed there. Where a user is not authorised to open a dialog, it will be displayed as greyed out in the Monitor's main menu. Where a user is not authorised to undertake modifications, no entry fields will be available. Furthermore, the administrator can set checkmarks regarding which parameters he wishes to include in the template by default, and which should not be available for modification by the user.

Where an administrator applies restrictive settings for all configuration options, and restricts the user from undertaking any editing at all, a new CNF file must be supplied for the client in case of failure - provided the client can still establish a connection - or the administrator will have to communicate directly with the user to provide him with the (one-time) password to remove the parameter lock, and the user can then make the necessary changes himself.

Profiles (Phonebook)
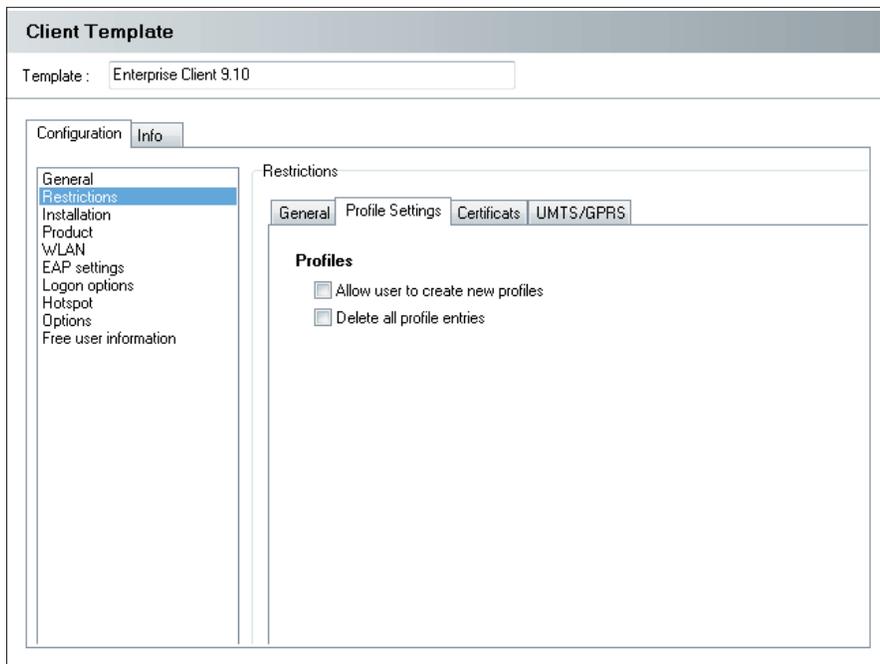
"User can create own entries" means that the user is authorised to create new profiles. Where this option was not check marked by the administrator, the user will only be able to establish a connection with the profiles defined by the administrator, and cannot add new entries.

All profiles, including those defined by the user himself will be deleted via the option "Delete all Client entries" during a configuration update, e.g. once the client has received a new CNF file.

The administrator can lock storing the SIM PIN under **GPRS / 3G**. (See **Mobile Computing**.)

Profile Configuration (Destination Systems)

Profiles (destination systems) are part of the templates. Each user will later have one profile (or more) assigned via the template. (Should, for example, several users within one group have three destination systems assigned, and other users have five, then two separate templates will have to be defined: one for three profiles, and one for five. The same applies also, where various certification utilisations occur.)

Profiles are configured the same way via the management System console, as on the Enterprise Client; a differentiation occurs here in regards to which parameters apply equally for all clients, and which are to be user specific.
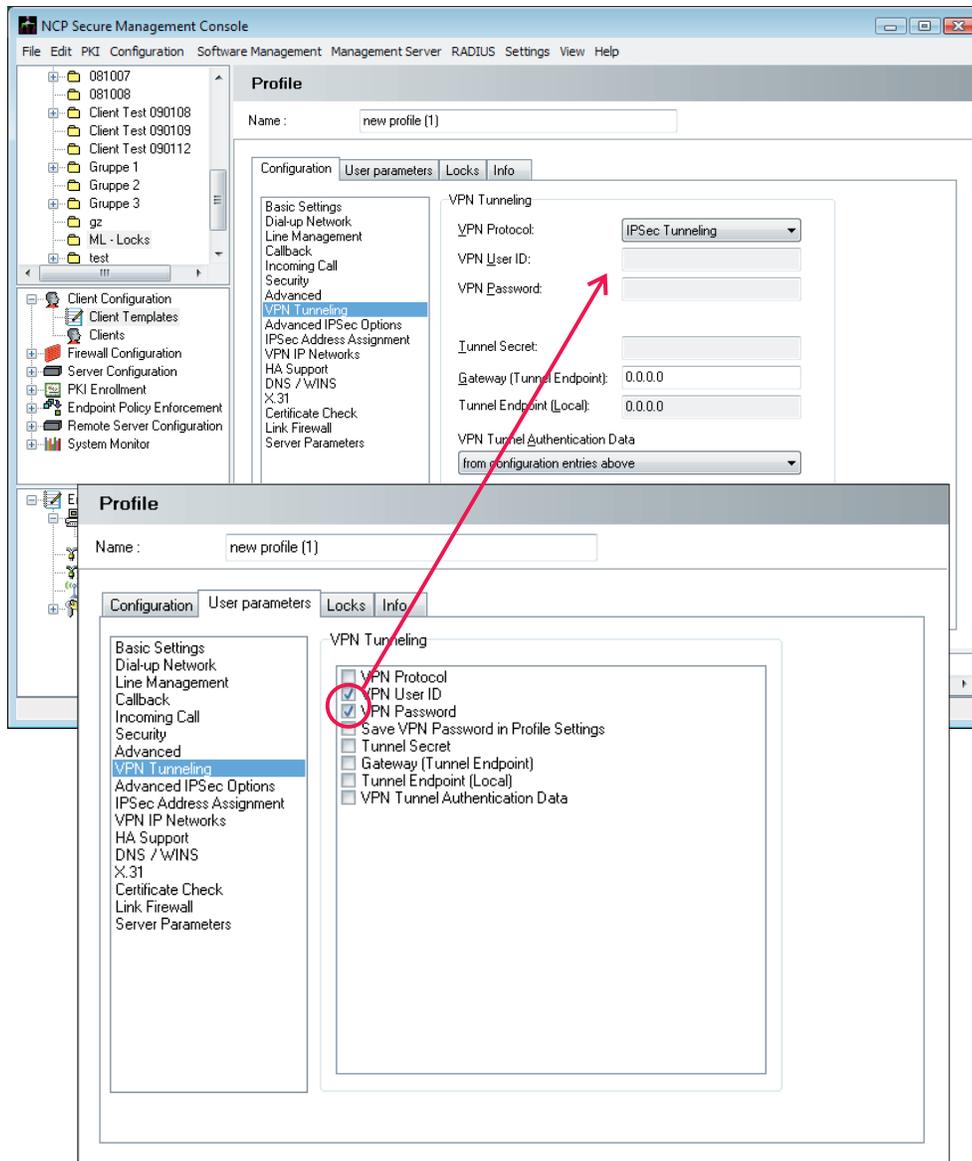
The template parameters, whose entry fields have been deactivated (see illustration left), must be entered at the end of each client configuration. The template parameters, to which this should apply, can be specified by setting a check mark for the template field of the user parameters (see illustration bottom left).

Example: By default, the required authorisation codes for the VPN gateway will not be editable when the template is first opened in the configuration area under "Tunnel Parameters".

That means that all users, who work with this profile, will have individual authorisation codes, which will be entered at the end of the client configuration process, or once the user establishes a connection.
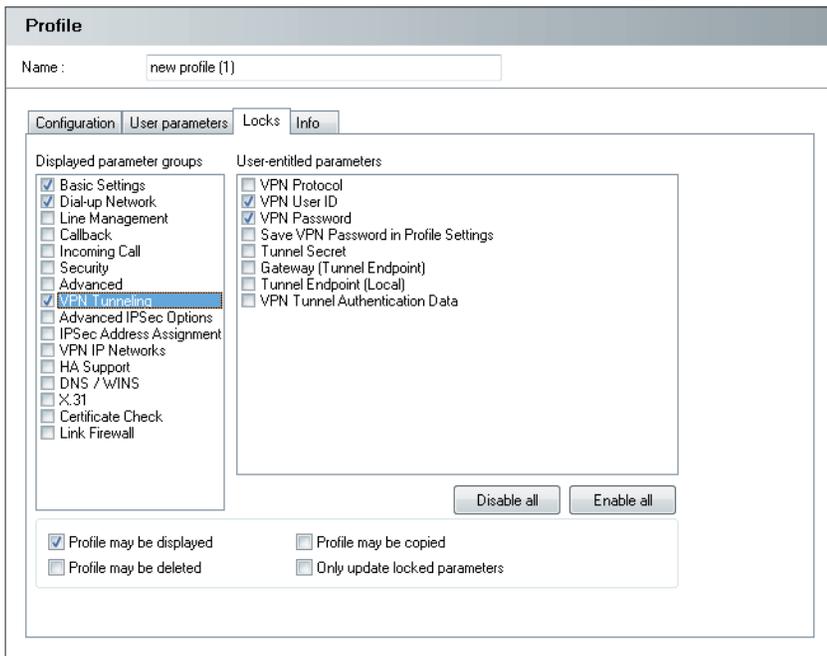
User Parameters

Parameters like **VPN User ID** and **VPN Password** are individual codes for each user, and will therefore need to be entered into the client configuration (where this data is not read from a certificate). See **Secure Client Parameters**.

That means generally that all parameters, which cannot be edited in a template for a certain profile, are personal and unique values, which can only be entered during client configuration in the SEM or directly at the client by the user.

Locks

Locks define the appearance of profile settings in the user interface of the Client software in such a way that the user will not be able to modify or even see certain parameters of the profile settings.

A lock-out is always associated with a profile or a parameter field in the profile settings of the Secure Client.

Visible Parameter Folders

The visible parameter folders list all the titles of all parameter folders from the profile settings of the client. Where titles of parameter folders are check marked, those parameter folders will be visible to the user. Unchecked parameter folders will be completely hidden.

Unlocked Parameters

The list of all unlocked parameters will include all parameters within a checked parameter folder. If a parameter folder is visible to the user, a further definition of which parameters within this field should be locked for user entries, and which should be unlocked.

A parameter with a check mark next to it is available for user entries. Where there is no check mark visible, the parameter remains locked for editing.

Profile Modifications

For additional information, please read the section "Client-side Profile Creation" below.

The functions "Show Profile", "...delete", and "...copy" will toggle all buttons in the profile directory of the Client Monitor (with the exception of "New Entry") between active or inactive, allowing or disallowing the user to undertake modifications. The button "New Entry" is activated, where the user has the authorisation for "User can Create own Entries". This authorisation affects all profiles and not only some, which is why this configuration option is located in the user interface of the template configuration (see section "Authorisation" above.)

The administrator can decide to "Show Profile" for this user by placing a check mark. Where no check mark has been set, the profile entry will not be displayed to the user, which means that also the button "Configure" will remain greyed out. The configuration options "Delete Profile" and "Copy Profile" affect the functionality of the buttons "Delete", and "Copy" in a similar way.

"Only modify locked-out parameters" means that during a configuration update, only the settings of parameters that are locked out will be overwritten. This functionality helps to eliminate overwriting of parameters, which were modified by the user via the Client (e.g. modem settings) during a configuration update.

Profile Preview

Once a profile configuration is complete, and lock-outs have been defined, profiles can be viewed as they will appear to the user on the client by simply clicking the button "Preview" in the taskbar, or selecting "Profile Preview" from the main menu under "Configuration". (Illustration right).
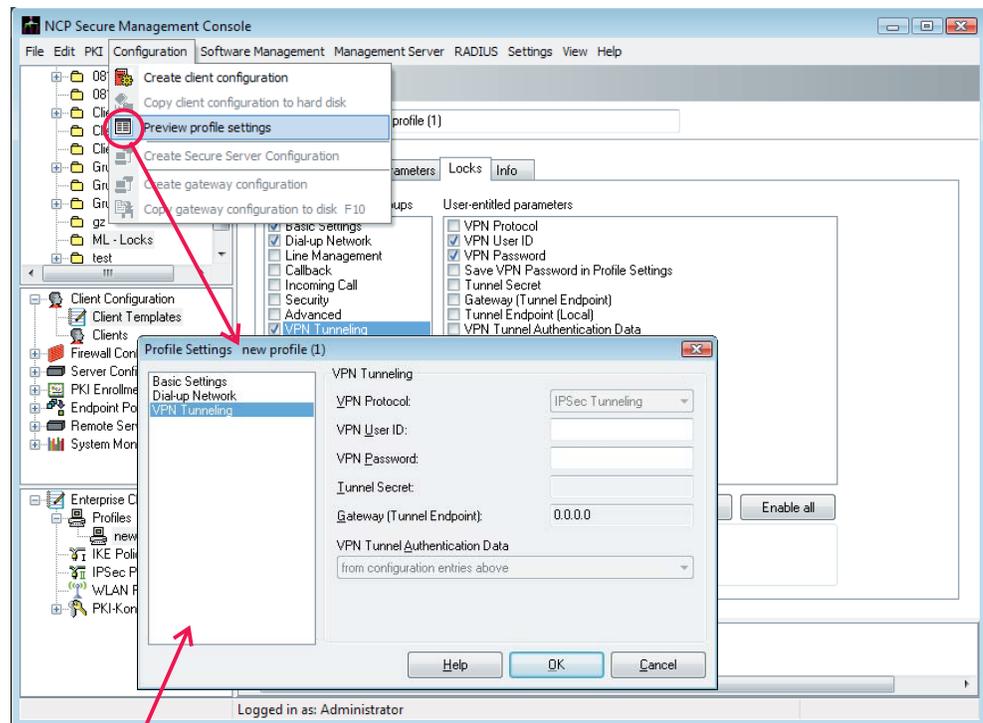
## Parameter Locks Depiction in the User Interface of the Enterprise Client

Following a roll-out or a configuration update, where a user Client receives the software with relevant lock-outs, the configuration menu of the Enterprise Client will be displayed as per the illustration you see here.

Individual configuration fields of a profile will be displayed as per preview on the SEM, provided they can be accessed (see illustration above).
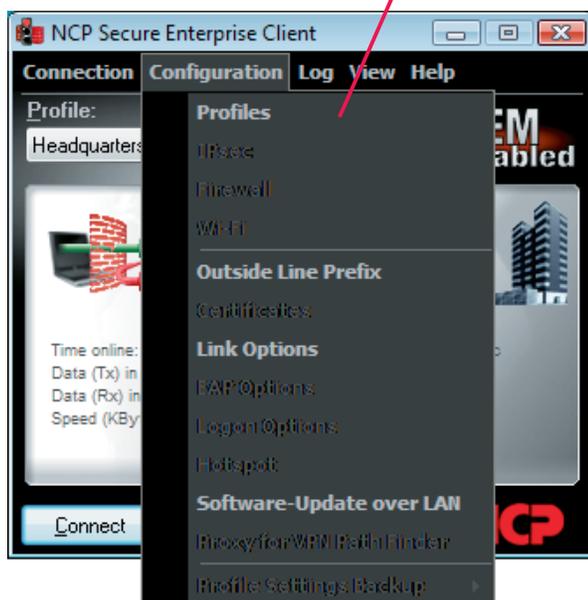
Unlock Parameter Locks

Removing or modifying a lock-out should only be carried out as previously described in order to safe-guard configuration security:
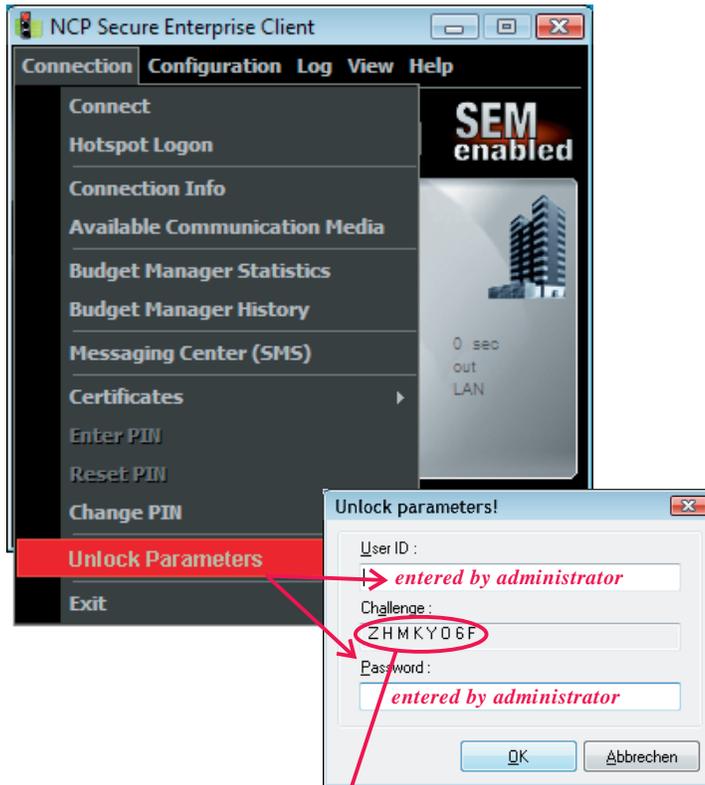

Centrally

The administrator can create a new user configuration centrally via the SEM, and then provide a configuration update for the management server. Once the automatic update has been completed, modifications will have taken effect on the remote client. (For additional information, please read the description regarding configuration updates via SEM.)

Locally

Should the remote client not be able to establish a connection with the Management System anymore, then the administrator can remove the parameter lock-out locally from the Enterprise Client. He selects the option "Remove Parameter Lock-Out" (illustration left) from the configuration menu of the Monitor, and then enters both the user name and the password as configured in the template under SEM (see above: "Group specific and user specific parameters".) Once the modifications have been carried out, the administrator must not forget to reinstate all lock-outs (see below).

Remotely

The Administrator may decide to entrust the remote user with the removal of the parameter locks. For such a scenario, administrator and user must be in contact via telephone.
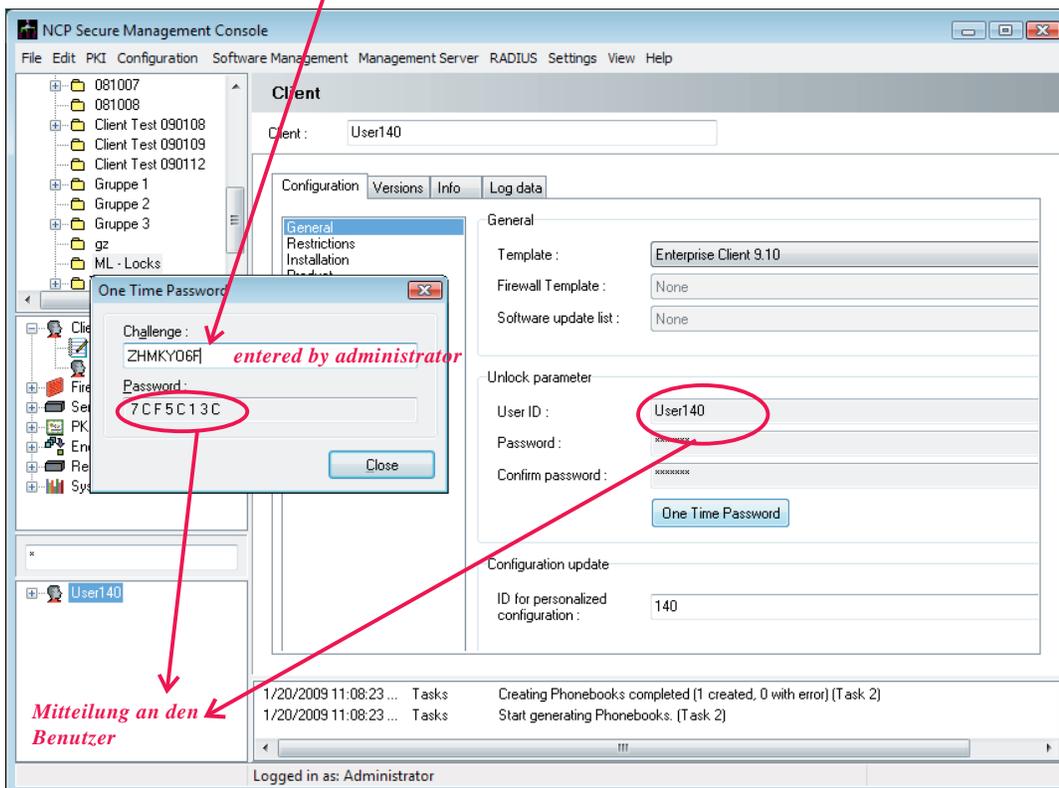
The user will disclose the challenge code to the administrator, which he receives after selecting the menu option "Remove Parameter Lock-Out" (above). He discloses the code to the administrator, who will enter it into the Management console. To this end, the administrator will click on "One-Time Password" for the general client configuration of the caller. He will receive the one-time password after entering the code (illustration above).
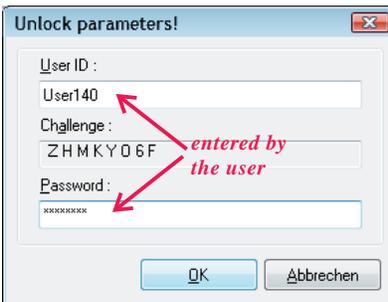
Once the user has entered the one-time password, all lock-outs will be removed (see illustration left).

The lock-outs will remain disabled until the user selects the menu option "Reinstate Parameter Lock-Out", but latest until the Monitor is exited. Once the Monitor has been restarted, the lock-outs will once again be in place.