Client-Side Configuration Locks

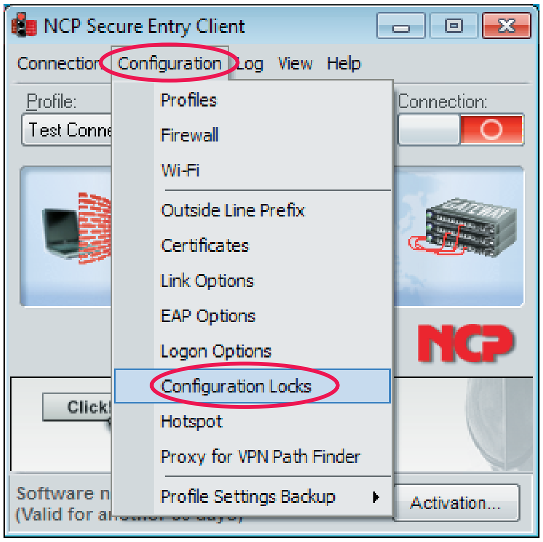
The configuration locks and parameter locks of the NCP Client software have two important functions. On the one hand, the complexitys of the configuration options is reduced, which gives the software interface a more streamlined appearance. Any parameter fields for functions that are not required, are deactivated, and the user only sees setting options relevant for his working environment. On the other hand, default settings can be defined, which cannot be changed by the user. This eliminates misconfigurations and unwanted connections. In this case the user only needs to enter his personal passwords after installation, in order to establish a connection.

The configuration locks at the Secure Entry Client have to be set up individually on each user PC by the administrator.

Terminology “Profile”

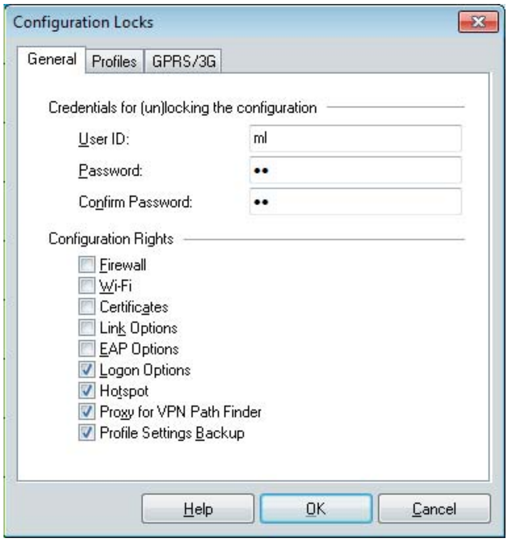
For the purposes of better understanding, a **Profile** can also be called a **Link Profile**, as opposed to “Wi-Fi profile”, “certificate profile”, etc. The term “link profile” also appears in server components of the NCP Secure Client software, and describes the complete configuration within Remote Access solutions. This configuration is required for certain attributes (e.g. security), in order to establish a client-server connection.

The configuration menu and settings options for the profiles can be modified via configuration locks in the main menu of the monitor (see illustration below) that the user cannot modify any default configurations, or that selected parameter fields will not be accessible for the user in profile settings. These configuration locks apply in their predefined format for all link profiles available on the Entry Client.



General

The administrator defines user specific (customized) configuration locks for each PC user individually. An ID consisting of “user” and “password” is entered for each configuration lock. (The ID should be unique for each Entry Client).



Credentials for (un)locking the configuration

User ID: ml

Password: ••

Confirm Password: ••

Configuration Rights

- □ Firewall
- □ Wi-Fi
- □ Certificates
- □ Link Options
- □ EAP Options
- ☑ Logon Options
- ☑ Hotspot
- ☑ Proxy for VPN Path Finder
- ☑ Profile Settings Backup

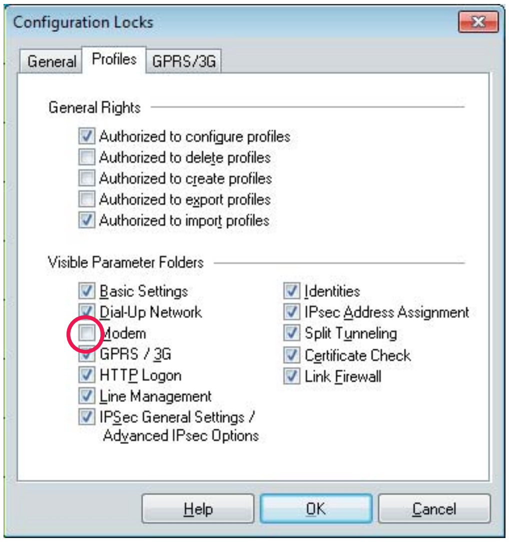
Please note that an ID is necessary for defining or removing configuration locks. Should you forget your ID, there will be no possibility to remove or edit locks!

Configuration locks are applied in their defined form for the three configuration fields, once settings have been confirmed with “OK”. If you click on “Cancel”, all settings are rolled back to their default settings.

Then user access rights for menu options in the main menu “Configuration” can be set. By default, the user can open all menu options, and edit any configuration. Once the check for a particular menu option is removed, then this option is greyed out and will no longer be available.

Profile

Access rights for editing configuration fields in profile settings are grouped into three categories:
– General access rights
– Visible profile parameter folders
– GPRS / 3G



Configuration Locks

General Rights

☑ Authorized to configure profiles
☐ Authorized to delete profiles
☐ Authorized to create profiles
☐ Authorized to export profiles
☑ Authorized to import profiles

Visible Parameter Folders

☑ Basic Settings
☑ Dial-Up Network
☐ Modem
☑ GPRS / 3G
☑ HTTP Logon
☑ Line Management
☑ IPSec General Settings / Advanced IPsec Options
☑ Identities
☑ IPsec Address Assignment
☑ Split Tunneling
☑ Certificate Check
☑ Link Firewall

General Rights

General access rights refer to (configuration of) profiles only. Example: “New profiles can be created” is defined, and “Profiles can be configured” remains inaccessible - that means that new profiles can be defined, but parameter changes cannot be carried out at a later stage. Where only profile configuration is allowed, then only those profiles provided by the administrator can be modified. Where all general access rights are denied, only existing profiles can be selected, but not viewed.

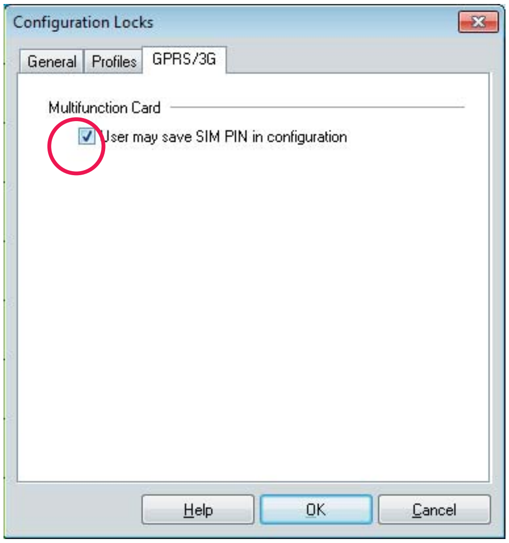
Visible Profile Parameter Folders

All previously mentioned configuration folders can be deactivated for the user. Please note that parameters of an invisible folder cannot be configured, and vice versa that configuration folders will not be visible, where profiles cannot be configured. In the example illustrated above, the configuration folder “Basic Setup” and “Network Dial-Up” can be configured for all existing profiles.

GPRS / 3G

The option “Store SIM PIN in Configuration” is located in the dialog for entering the SIM PIN for GPRS/3G cards (multifunction cards). If this function is activated, the SIM PIN is entered once, and then used with the connection medium GPRS / 3G for each profile, eliminating the need for individual entries.

This function is not visible in the Entry Client default setting. It becomes visible and configurable for the user, once access has been granted via the parameter locks under “GPRS / 3G”, i.e. once “Allow user to save the SIM PIN in the configuration” has been activated (see illustration above). This function is particularly useful if the parameter modem has been made invisible (see illustration above), since the user would otherwise have to enter his SIM PIN every time a connection is established.



Configuration Locks

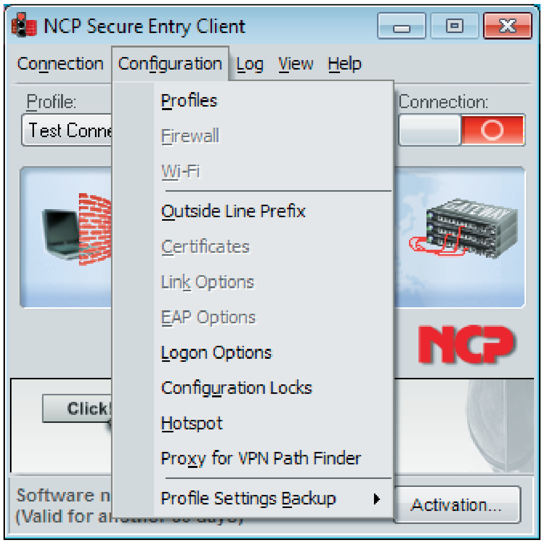
Multifunction Card

☑ User may save SIM PIN in configuration

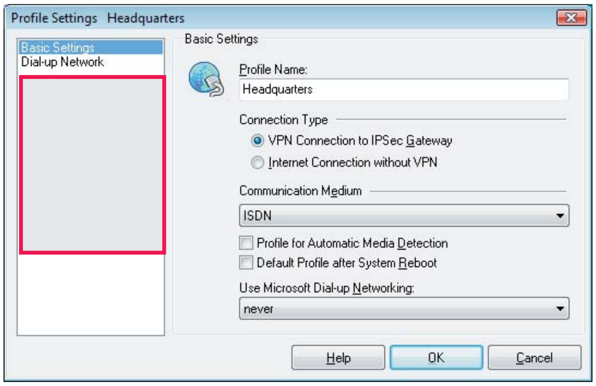
Please also see the description:
Secure Client Mobile Computing and
Secure Client Parameters

Lock Depiction in the User Interface of the Entry Client

Once the configuration locks have been activated, the Client’s configuration menu is displayed as depicted in the following illustration.



The configuration fields of a profile will appear as in the example below.



Basic Settings

Profile Name: Headquarters

Connection Type

● VPN Connection to IPSec Gateway

○ Internet Connection without VPN

Communication Medium: ISDN

□ Profile for Automatic Media Detection

□ Default Profile after System Reboot

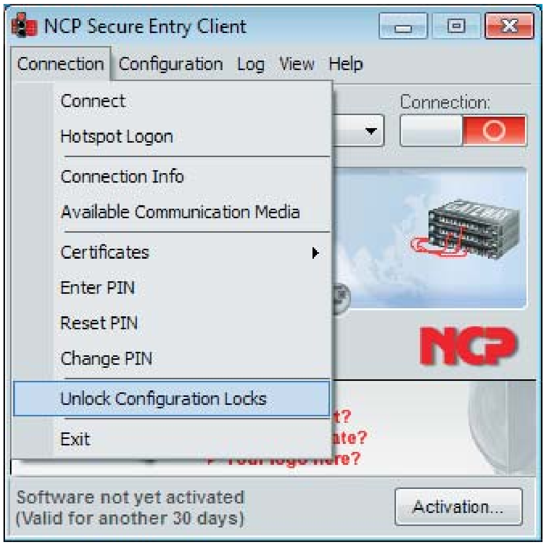
Use Microsoft Dial-up Networking: never

Those configuration fields that are to remain inconfigurable for the user, are no longer displayed.

Unlock Configuration Locks

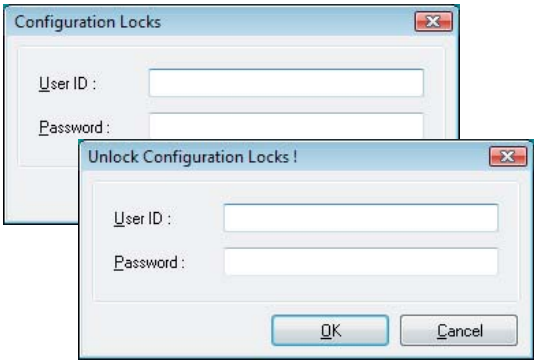
Unlocking or editing of locks should only be carried out by the administrator, since configuration security can no longer be guaranteed, once the configuration lock ID has been made public.

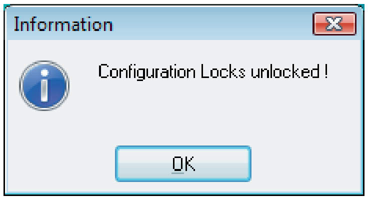
Once the configuration lock ID has been published, the administrator should upload new profile settings, or a new ID for the configuration lock to the user’s Entry Client as soon as possible.



Software not yet activated
(Valid for another 30 days)

Removing configuration locks via the connection menu (all locks are deleted, see illustrations below), and modifying locks via the configuration menu require the same ID.





Configuration Locks unlocked !