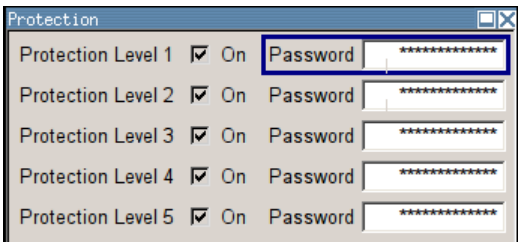


The following functions are protected in the respective levels:

- Protection Level 1
  Protects against accidental changes to certain settings, e.g. clock and date, network settings or instrument names. You can access this protection level with the password *123456*.
- Protection Level 2
  Provides access to the unlocking of protected service functions. It is accessible for authorized personnel of Rohde & Schwarz service departments.
- Protection Level 3-5
  Are reserved for factory internal use.

To unlock or lock a protection level...

1. In the "Password" entry field, enter the password for the corresponding protection level.
2. Confirm with the [Enter] key.

   The checkbox of the protection level is disabled, i.e. the protection is unlocked.
3. To lock a protection level again, select the checkbox.

Protection Level/Password
Locks or unlocks the corresponding protection level.

E.g. protection level 1 expands the functionality of the internal adjustment and to access the selftests.

The password is *123456*.

For access to service functions of protection level 2, see the service manual of your R&S SMB.

Remote command:
`:SYSTem:PROTect<ch>[:STATe]` on page 452

4.2.3.14 Security

The security concept of the R&S SMB helps you to protect your instrument against uncontrolled access and changes. All provided security services require that you enter the security password.

Provided security services are:

- **Password** management secures controlled user access to the instrument

With the two-step password concept, you can assign a user-defined password for the operating system, as well as a security password for accessing the mass storage of the instrument.
For more information concerning the security password, see the description *Resolving Security Issues when Working with an R&S SMB*. You can find this document on the R&S SMB product page at "Downloads" > "Manuals".

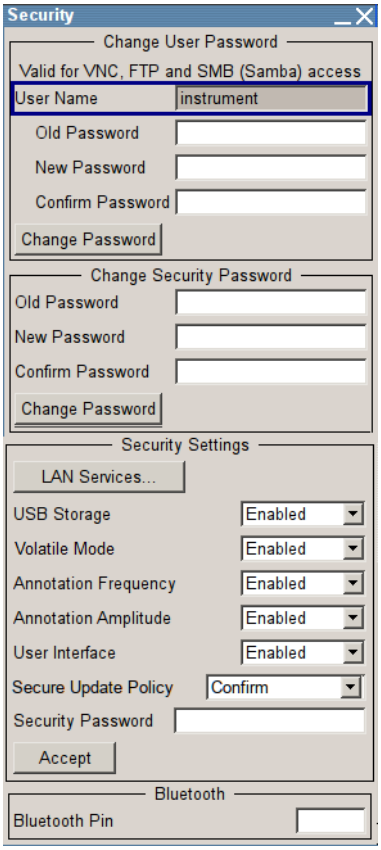
- **LAN Services** secures controlled network access.
  You can individually lock and unlock the supported LAN interface services, see "LAN Services" on page 117.
  Remote control via LAN interface requires that the interface is activated, but you can enable the required services specifically.
- **General** security parameters as:
  - **USB Storage** secures controlled access to the mass memory of the instrument.
  - **Volatile mode** protects against modification or deletion of data in the file system.
  - **Annotation** frequency and amplitude prevents reading the display.
  - **User Interface** prevents front panel operation and/or reading the display
  - **Secure Update Policy** check that verifies the integrity and origin of the firmware package to be installed.
  - **Bluetooth** enables operation of the instrument via Bluetooth.

Changing the password for the operating system or the security password requires that you enter the old password, the new password and that you confirm the new password.

To assign the password, press the "Accept" button. This action can not be undone!

Keep also in mind, that security settings are never reset, even if you perform a factory preset.

► To access this dialog, press the [SETUP] or [MENU] key and select "Protection " > "Security".



The "Security" dialog comprises the parameters for configuring the passwords, as well as the security settings of the mass storage and the LAN services.

The settings in this dialog will not be assigned until you enter the Security Password and confirm with the Accept button.

User Name
Indicates the user name used for access to the Linux operating system.

The user name and password are required for remote access to the instrument via VNC, FTP or SAMBA.

Change User Password
Allows you to change and confirm the user password.

Old Password ← Change User Password
Enters the current user password. The default password is "instrument".

Note: It is highly recommended to change the default user password before connecting the instrument to the network.

New Password ← Change User Password
Enters the new user password.

Confirm Password ← Change User Password
Confirms the new user password by reperating.

Note: The new password will not be assigned until you select the Change Password button.

Change Password ← Change User Password
Changes the user password accordingly.

Note: Keep in mind, that a changed password is never reset, even if you perform a factory preset.

Change Security Password
Enables you to change and confirm the security password.

Old Password ← Change Security Password
Enters the currently used security password. The default password is '123456'.

Note: It is highly recommended to change the default security password before connecting the instrument to the network.

The security password is required when changing the status of the USB and LAN interface.

New Password ← Change Security Password
Enters the new security password.

The security password may contain decimal characters only.

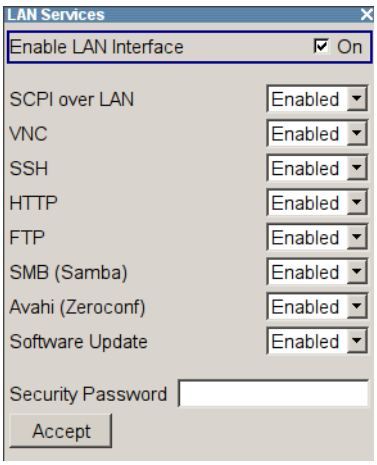
Confirm Password ← Change Security Password
Confirms the new password by repeating.

Note: The new password will not be assigned until you select the Change Password button.

Change Password ← Change Security Password
Changes the password accordingly.

Note: Keep in mind, that a changed password is never reset, even if you perform a factory preset.

LAN Services
Opens the "LAN Services" dialog for individually enabling or disabling the available LAN interface services.



Enable LAN Interface ← LAN Services
Enables the LAN interface in general, and thus provides remote access via all unlocked services.

Note: The activated LAN services will not be assigned until you enter the Security Password and confirm with Accept.

Enable LAN Services individually ← LAN Services
Enables or disables the following interface services individually.

"SCPI over LAN"
activates access over LAN to remotely control the instrument using SCPI (**S**tandard **C**ommands for **P**rogrammable **I**nstruments) commands.

"VNC" activates access via VNC (**V**irtual **N**etwork **C**omputing) interface, a graphical desktop sharing system that uses RFB protocol to remotely control the instrument.

"SSH" activates access via SSH (**S**ecure **Sh**ell), a network protocol for secure data communication.

"HTTP" activates access via HTTP (**H**yper **T**ext **T**ransfer **P**rotocol), the application protocol for hypermedia information systems.

"FTP" activates access via FTP (File Transfer Protocol), used to transfer files from a host to the instrument and vice versa.

"SMB (Samba)"
activates access to SMB (**S**erver **M**essage **B**lock), used for providing shared access to files, printers and serial ports of a network.

"Avahi (Zeroconf)"
activates Avahi, a service for automatic configuration of the instrument in a network environment.

"Software Update"
allows updating the instrument firmware via the LAN interface.
For more information on this topic see the release notes of the instrument, provided on the Internet at the download site or the Rohde & Schwarz Signal Generator home page.

USB Storage
Activates the access to external USB storage media.

This setting has no effect on a mouse or a keyboard, connected via USB.

Note: The setting will not be assigned until you enter the Security Password and confirm with Accept.

Volatile Mode
Acitivates write protection on the file system to prevent modification or erasure of valuable data.

Note: The setting will not be assigned until you enter the Security Password, confirm with Accept, and reboot the instrument.

Remote command:
`:SYSTem:SECurity:VOLMode[:STATe]` on page 443

Annotation Frequency
Enables/disables the display of the currently used frequency in the header of the instrument.

Note: The setting will not be assigned until you enter the Security Password and confirm with Accept.

Remote command:
`:DISPlay:ANNotation:FREQuency` on page 295

Annotation Amplitude
Enables/disables the display of the currently selected level in the header of the instrument.

Note: The setting will not be assigned until you enter the Security Password and confirm with Accept.

Remote command:
`:DISPlay:ANNotation:AMPLitude` on page 295

User Interface
Allows you to lock the manual of the controls of the instrument, and to hide even the entire display.

The setting requires the entry of the security password *123456* and is only accepted after the "Accept" button is pressed.

Tip: Section "Enabling a locked user interface for manual operation" on page 120 describes how you can unlock the control elements and the user interface.

"Enabled" Enables the display and all controls for the manual operation of the instrument.

"VNC Only" Locks the keys at the front panel and externally connected keyboard and mouse.
The display on the screen remains and shows the current settings and changes.
Unlocking is possible via VNC or turning off and on again.

"Display only"

Locks the manual operation of the instrument. The display on the screen remains and shows the current settings and changes.
This security feature protects the instrument against unauthorized access, but still shows the current settings and processes, for example when you operate the instrument via remote control.

The function disables:
- the keys at the front panel of the instrument
- the external mouse and keyboard

The instrument indicates the locked controls by a padlock softkey in the taskbar.

"Disabled"

Locks the display and all controls for the manual operation of the instrument.
This security feature protects the instrument against unauthorized reading and access, for example when you operate the instrument via remote control.

The function disables:
- the display
- the keys at the front panel of the instrument
- the external mouse and keyboard

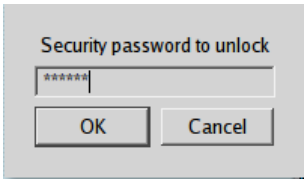
The screen shuts off and shows a padlock instead.

Remote command:
`:SYSTem:ULOCk` on page 442
`:SYSTem:DLOCk` on page 442
`:SYSTem:KLOCk` on page 442

Enabling a locked user interface for manual operation

To unlock the user interface for manual operation you have the following options:

- On the instrument's keypad or external keyboard, enter the security password *123456*.
  Even if you press any key, the instrument prompts you to enter the security password for unlocking.



  Note The character of the first key you pressed is immediately added in the input field. Prior to inserting the password delete this entry.
- In remote control mode, send the command `SYST:ULOC ENABled` to release all locks at once.
  Alternatively, you can use the command `SYST:KLOC OFF` to unlock the keyboard, or `SYST:DLOC OFF` to release the display.

Via remote control, there is no password required.

Remote command:
:SYSTem:ULOCk on page 442
:SYSTem:DLOCk on page 442
:SYSTem:KLOCk on page 442

Secure Update Policy
Allows you to configure the automatic signature verification for firmware installation.

To apply the change: enter the security password and confirm with "Accept". Otherwise the change has no effect.

See also:
- Chapter 4.2.3.14, "Security", on page 114 for more information on the security concept.
- The release notes for details on signature verification when installing new or former firmware versions, available at www.rohde-schwarz.com/firmware/smb100a.

"Confirm Unsigned"
Performs the signature verification.
If the check detects any discrepancies, the instrument issues a warning message. You can still update the firmware or reject updating.
This setting also enables you to downgrade the firmware version.

"All Packages" Accepts all packages without signature verification.

"R&S Signed Packages"
Performs the signature check.
If the check detects any discrepancies, the instrument issues a warning message and locks the update to this firmware.

Remote command:
:SYSTem:SECurity:SUPolicy on page 452

Security Password
Enters the password that is required to enable or to disable the settings protected by a security password. Default is '123456'.

Note: It is highly recommended that you to change the default security password before connecting the instrument to the network.

All settings are only accepted after the "Accept" button is pressed.

Accept
Applies the modified settings, provided the security password is entered correctly.

Note: This action can not be undone. Keep in mind, that a changed password is never reset, even if you perform a factory preset.

Bluetooth Pin
Sets the Bluetooth pin of an external Bluetooth device. The pin is required to enable remote control via an external Bluetooth device.

Requires a Bluetooth adapter (recommended extra, see data sheet) .