

Introduction

This technical bulletin describes how to use Settings Protection on L-Acoustics LA2Xi, LA4, LA4X, LA8 and LA12X amplified controllers.

Settings Protection is for a fixed installation System Integrator, Application Engineer or Technical Director to:

- protect the settings of an L-Acoustics system using a password
- use tuning variant by authorizing only some Session files

! Settings Protection does not prevent actions done from the USB Terminal utility (reset to factory default settings, modification of IP settings).

Take measures to restrict access to the USB port of the amplified controller.

Settings Protection is not supported on P1 processors.

Access rights

Settings Protection is based on three levels of users.

- Administrator: defines the password, the PIN code, and enables/disables the system protection
- Advanced User: uses the PIN code for temporary bypass of the system protection
- General User: has restricted access

Access rights have been defined by L-Acoustics to meet the needs of 90% of the fixed installation applications. This policy cannot be modified by the Administrator.

Security and reset

The protection is stored on the amplified controller.

The protection cannot be bypassed by reformatting the computer hosting LA Network Manager, using another computer, using an older version of LA Network Manager, resetting the amplified controller to factory default settings, nor updating the firmware.

In case the Administrator loses the password(s), protection may be reset to default parameters using Protection Reset from LA Network Manager. Refer to section [Resetting the protection](#) (p.8).

Field of application

The protection applies to:

- remote control from LA Network Manager
- local control from the front panel keys

The protection does not apply to third party control solutions (AMX, Crestron, SNMP). If needed, it is up to the System Integrator to implement a separate settings protection.

When Settings Protection is enabled by the Administrator:

only the Administrator can	the Advanced User can (with the PIN code)	the General User can
<ul style="list-style-type: none">• load non-authorized Session files• delete a user preset• reset Units to factory default parameters• update firmware• use quick access to gain from front panel	<ul style="list-style-type: none">• load a factory preset• store a preset• modify any group parameter• modify a preset parameter• access M1• modify the IP address of a Unit	<ul style="list-style-type: none">• load authorized Session files• restore Session• load user presets• select the input mode• mute/solo• set in standby / wake-up

Why both a password and a pin code?

The password:

- is exclusively for the Administrator
- allows enabling or disabling the protection
- is stored in the physical Units

The PIN code:

- is defined by the Administrator
- grants temporary rights to selected Advanced Users for a subset of functions
- is stored in the physical Units and the virtual Units
- must match between physical and virtual Units when loading Session. Otherwise a PIN conflict is displayed

Recommendations

- Do not forget the Administrator password or the PIN code.
- Carefully select who needs to know the PIN code.
- Avoid using different passwords or PIN codes on Units pertaining to the same system. Rather use one password and one PIN code for the entire system.
- Do not use Settings Protection on spare Units.
- Do not use Settings Protection on Units rented with complementary speakers.

Initial setup

Recommended procedure for initial setup.

Prerequisite

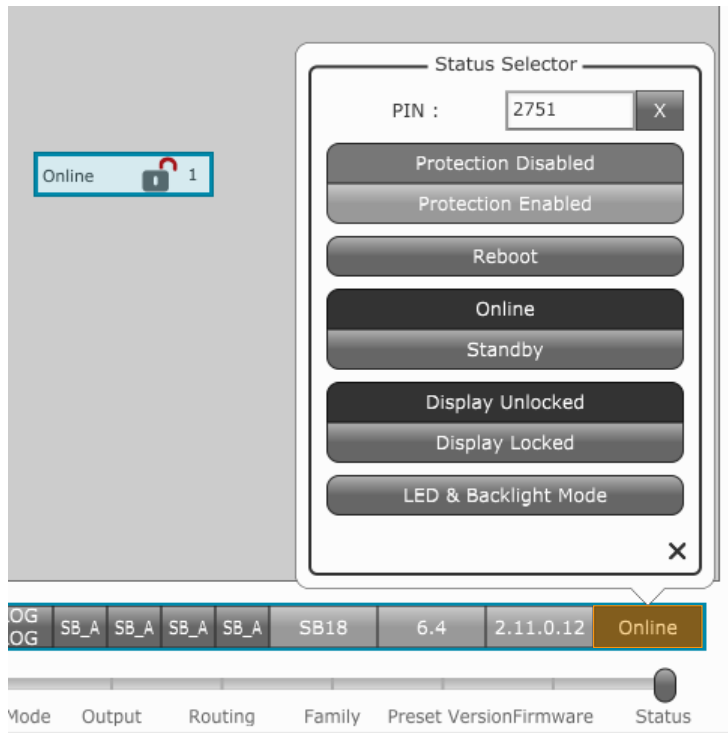
Make sure all physical Units of the system are correctly detected by LA Network Manager.

Creating the PIN code and password

Procedure

1. Add all physical Units to the Workspace.
2. If necessary, update all LA4 and LA8 Units to at least firmware 2.1.2.0 and all LA4X Units to at least firmware 1.0.2.0.
3. Save a "raw.nwm" Session file.
This file is used later to check the protection.
4. Perform the system check as usual and make a first reference calibration.
Variant calibrations, if required, are done at a later stage.
5. Select all physical Units.

6. Click the status on the Unit control bar to open the **Status Selector**.



7. In the **PIN** field, enter a PIN code of four digits and press the Enter key.

The **Status Selector** displays the password dialog box.



8. Enter the default password: `admin` and click **Modify Password**.

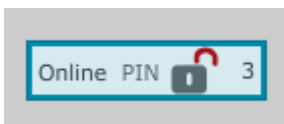
The **Status Selector** displays the new password dialog box to modify the default password.



9. Choose an Administrator password, then confirm and click **OK**.


Results

The PIN code is stored in the Units. This is indicated in the Workspace: when the slider is on the status, the Units have a grey on white **PIN**.



Enabling the Settings Protection

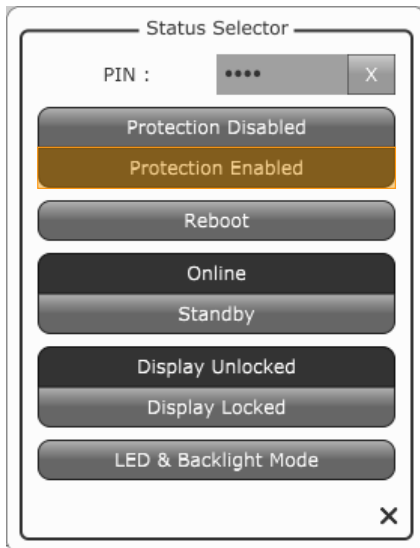
About this task

- 
Enable Settings Protection before saving the Session
 If the Session file is saved before enabling the Settings Protection, the PIN code is visible in the Session file when opened in **Offline** mode.

Procedure

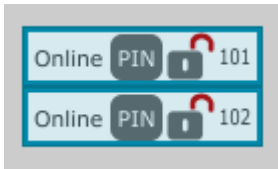
1. Select all physical Units.
2. Click the status on the Unit control bar to open the **Status Selector**.

3. Click Protection Enabled.



4. Enter the Administrator password when prompted.

Settings Protection is enabled. This is indicated in the Workspace: when the slider is on the status, the Units have a white on grey **PIN**.



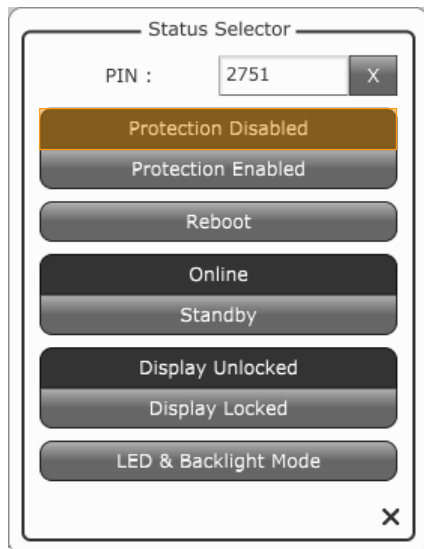
5. Save a "bases.nwm" Session file.

Disabling the Settings Protection

If required, follow these steps to disable the Settings Protection.

Procedure

1. Select all physical Units.
2. Click the status on the Unit control bar to open the **Status Selector**.
3. Click **Protection Disabled**.



4. Enter the Administrator password when prompted.

Results

Settings Protection is disabled.

Creating authorized Session files

Procedure

1. Load the "bases.nwm" Session file.
2. Disable the Settings Protection.
Refer to procedure [Disabling the Settings Protection](#) (p.6).
3. Perform the tuning for the variant calibration.



Preset Family conflict

Make sure a switch from a variant Session file to another does not create any Preset Family conflict.

If a Preset Family conflict occurs when using the variant, resolving the conflict requires to enter the PIN code.

4. Enable the Settings Protection.
Refer to procedure [Enabling the Settings Protection](#) (p.4).



Enable Settings Protection before saving the Session

If the Session file is saved before enabling the Settings Protection, the PIN code is visible in the Session file when opened in **Offline** mode.

5. Save the variant Session file.
Examples: "speech.nwm", "movie.nwm", "live.nwm", etc.
6. Repeat steps 2 (p.7) to 5 (p.7) for each variant calibration.

Checking Settings Protection

Procedure

1. Check that all Session files saved for tuning variants can be loaded.
2. Check that "raw.nwm" cannot be loaded.

Differentiating Disp. Lock / Disp. Unlck features from Settings Protection

Identifying locked/unlocked units

Disp. Lock/Disp. Unlck allows you to lock/unlock the front panel keys of online physical Units to prevent accidental modification of settings.

This is indicated in the Workspace. When the Unit View slider is on **Status**:

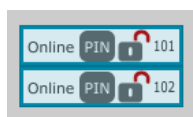
- a closed padlock  indicates locked Units
- an open padlock  indicates unlocked Units

Identifying protected/unprotected units

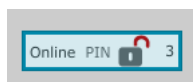
Settings Protection allows you to protect access to the Units with a PIN code.

This is indicated in the Workspace. When the Unit View slider is on **Status**:

- a white on grey **PIN** indicates Settings Protection is active on the Unit



- a grey on white **PIN** indicates Settings Protection is not active on the Unit



Modifying the setup

Modifying the password

Procedure

1. Select all relevant physical Units.
2. Click the status on the Unit control bar to open the **Status Selector**.
3. Click **Protection Enabled** or **Protection Disabled**.
The **Status Selector** displays the password dialog box.
4. Click **Modify Password**.
5. Enter the Administrator password and confirm.
6. Click **Protection Enabled** or **Protection Disabled** again if necessary.

Modifying the PIN code

Procedure

1. Select all relevant physical Units.
2. If a protection is enabled, click **Protection Disabled** and enter the Administrator password.
3. Enter a new PIN code and press the Enter key.
4. Enter the Administrator password when prompted.

Resetting the protection

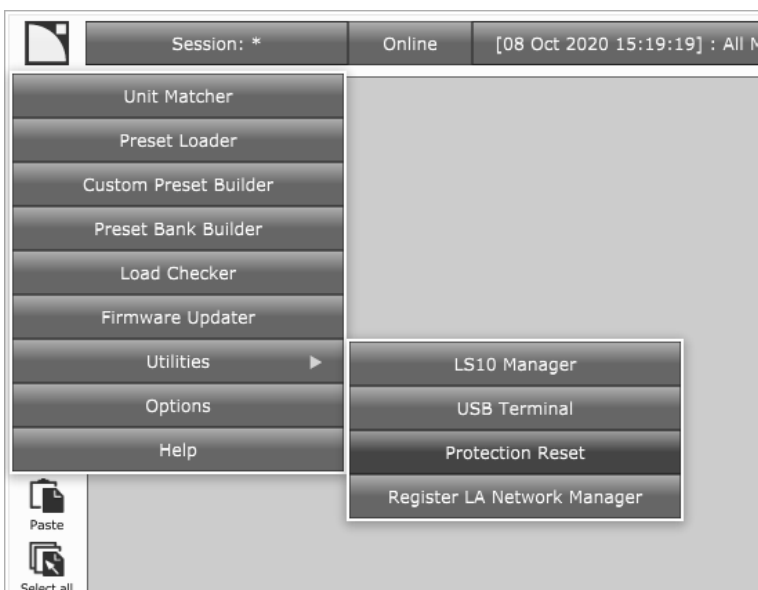
If the password or PIN code are lost, Settings Protection can be reset.

Prerequisite

Make sure that all Units to be reset are detected by LA Network Manager, either on the Workspace or on the network scanning zone.

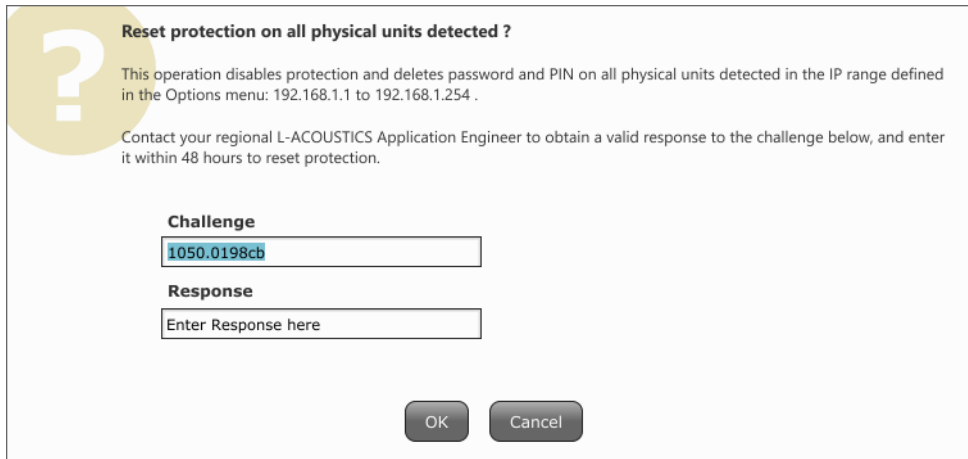
Procedure

1. Click the L-Acoustics logo to open the menu.



2. Click **Protection Reset**.

LA Network Manager displays the Reset protection dialog box.



Reset protection on all physical units detected ?

This operation disables protection and deletes password and PIN on all physical units detected in the IP range defined in the Options menu: 192.168.1.1 to 192.168.1.254 .

Contact your regional L-ACOUSTICS Application Engineer to obtain a valid response to the challenge below, and enter it within 48 hours to reset protection.

Challenge

1050.0198cb

Response

Enter Response here

OK Cancel

3. Contact L-Acoustics and provide the Application Engineer with the code generated in the **Challenge** field.

4. Enter the code provided by the L-Acoustics Application Engineer in the **Response** field within 48 hours, and click **OK**.

Results

All passwords and PIN codes are reset.

Updating the firmware on protected Units

Procedure

1. Disable the Settings Protection.
Refer to procedure [Disabling the Settings Protection](#) (p.6).
2. Update the firmware.
Refer to the LA Network Manager help.
3. When the firmware update is complete, enable the Settings Protection.
Refer to procedure [Enabling the Settings Protection](#) (p.4).