

SETTINGS PROTECTION

TECHNICAL BULLETIN

VERSION 3.0



Document reference: **SETTINGS-PROTECTION_TB_EN_3.0**

Distribution date: June 9, 2014

© 2014 L-ACOUSTICS®. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without the express written consent of the publisher.

INTRODUCTION

This **TECHNICAL BULLETIN** is for using **Settings Protection** on L-ACOUSTICS® **LA4**, **LA4X** and **LA8** amplified controllers.

LA NETWORK MANAGER from **2.2.0.0** together with LA4/LA8 firmware from **2.1.2.0** and LA4X firmware from **1.0.2.0** offer the possibility to:

- Protect the settings of an L-ACOUSTICS® System using a password
- Use tuning variants by authorizing only certain **Session Files**

These functions are aimed at Fixed Installation applications.

This **TECHNICAL BULLETIN** is a guide intended for the System Integrator, the Application Engineer or the Technical Director in charge of setting up and managing the System protection.

MAIN FEATURES AND CONCEPT

- **Settings Protection** is based on three levels of users:
 - The *Administrator* can define the password, the **PIN Code**, and can enable or disable the protection of the system.
 - The *Advanced User* can use the **PIN Code** to temporarily bypass the protection.
 - The *General User* has only a 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.
- The protection applies both to remote control through **LA NETWORK MANAGER** and to local control from the front panel keys.
- The protection is stored on the amplified controllers and cannot be bypassed by reformatting the PC hosting **LA NETWORK MANAGER**, using another PC, using an older version of **LA NETWORK MANAGER**, or doing a reset to factory defaults or a firmware update.
- In case the Administrator has lost the password(s), protection may be reset to default parameters using the **Protection Reset** tool included in **LA NETWORK MANAGER**. The reset procedure requires contacting an L-ACOUSTICS® Application Engineer to get a password reset specific to the System and valid for 48 hours (Internet access is not necessary for the procedure).
- The protection does not apply to 3rd party control solutions such as AMX or Crestron interfaces or SNMP commands. If protection is needed for them, it is up to the System Integrator to implement a separate settings protection in their specific user interfaces.

PROTECTED SETTINGS AND ACCESS

The table below describes which functions are protected and who can access them when **Settings Protection** is enabled by the Administrator:

| Locked functions | Functions accessible by the <i>Advanced User</i> using the PIN Code | Functions accessible by the <i>General User</i> |
|--|---|--|
| 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 | Load a Factory Preset Store a Preset Modify any Group Parameter Modify a Preset Parameter Modify the IP Address of a Unit | Load authorized Session Files Restore Session Load User Presets Select the Input Mode Mute/Solo 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 Units** and **Virtual Units** when loading **Session Files**. Otherwise a **PIN Conflict** is displayed

ADVICES FOR A BETTER EXPERIENCE WITH SETTINGS PROTECTION

- Don't 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.

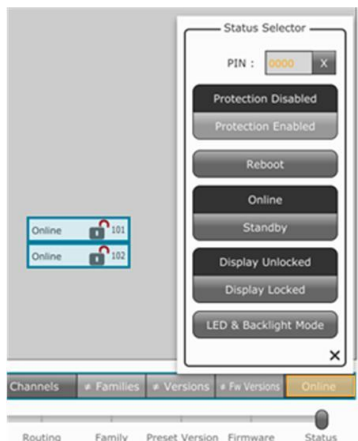
INITIAL SETUP

Below is the recommended procedure for initial setup.

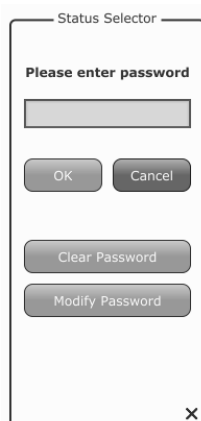
Pre-requisites: All **Physical Units** of the System are correctly detected by **LA NETWORK MANAGER**.

A. CREATING THE PIN CODE AND PASSWORD

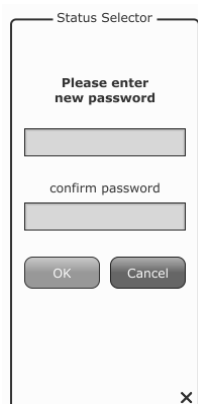
1. Add all **Physical Units** to the **Workspace**.
2. Update all **LA4** and **LA8 Units** to firmware **2.1.2.0** and all **LA4X Units** to firmware **1.0.2.0** (minimum).
3. Save a "raw.lses" Session File.
It will be used later to check the protection.
4. Perform the System check as usual and make a first reference calibration.
Variant calibrations, if required, will be done at a later stage.



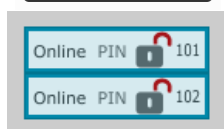
5. Select all **Physical Units**.
6. Click on the status on the **Unit Control Bar** to open the **Status Selector**.
7. In the **PIN** field, enter a **PIN Code** of four digits and press the Enter key.
The **Status Selector** displays the password dialog box.



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. Type the Administrator password of your choice, then confirm and click **OK**.

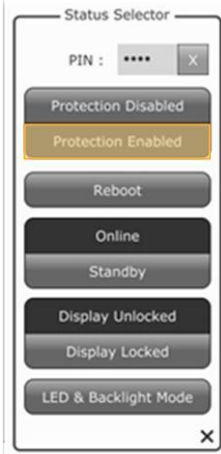


The **PIN Code** is now stored in the **Units**. This is indicated in the **Workspace**: when the slider is on **Status**, the **Units** have a grey on white **PIN**.

B. ENABLING/DISABLING THE SETTINGS PROTECTION

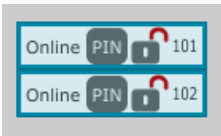
To enable the **Settings Protection**, follow these steps:

1. Select all **Physical Units**.
2. Click on the status on the **Unit Control Bar** to open the **Status Selector**.



3. Click on **Protection Enabled**.

4. Enter the Administrator password when prompted.



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

5. Save a "bases.lses" **Session** file.

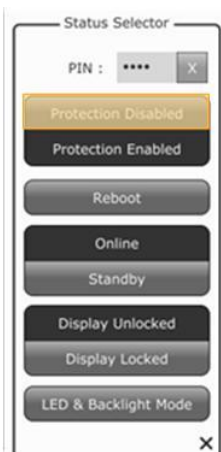


It is important to enable Settings Protection before saving.

If you save the **Session files** before enabling the **Settings Protection**, the **PIN Code** will be visible in the **Session file** when opened in **Offline mode**.

To disable the **Settings Protection** (if required), follow these steps:

1. Select all **Physical Units**.
2. Click on the status on the **Unit Control Bar** to open the **Status Selector**.



3. Click on **Protection Disabled**.

4. Enter the Administrator password when prompted.
Settings Protection is now disabled.

C. CREATING AUTHORIZED SESSION FILES

1. Load the “bases.lses” **Session file**.
2. Disable the **Settings Protection** (refer to procedure B.).
3. Perform the tuning for the variant calibration.



Risk of Preset Family conflict

Make sure a switch from a variant **Session file** to another will not create any **Preset Family Conflict**. In case of a **Preset Family conflict**, using the variant will require entering the **PIN Code** to resolve the conflict.

4. Enable the **Settings Protection** (refer to procedure B.).
5. Save the variant **Session file** (for example as “speech.lses”, “movie.lses”, or “live.lses”, etc.).



It is important to enable Settings Protection before saving.

If you save the **Session files** before enabling the **Settings Protection**, the **PIN Code** will be visible in the **Session file** when opened in **Offline mode**.

6. Repeat steps **2.** to **5.** for each variant calibration.

D. CHECKS

1. Test that all **Session Files** previously saved for tuning variants can be loaded.
2. Test that “raw.lses” cannot be loaded.

UPDATING THE FIRMWARE

Below is the procedure to update the firmware on protected **Units**.

1. Disable the **Settings Protection** (refer to procedure B).
2. Update the firmware.
Refer to the **LA NETWORK MANAGER video tutorial**.
3. When the firmware update is complete, enable the **Settings Protection** (refer to procedure B.)

MODIFYING THE PASSWORD

Below is the procedure to modify the password.

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

MODIFYING THE PIN CODE

Below is the procedure to modify the **PIN Code**.

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

RESETTING THE PROTECTION

Below is the procedure to reset the **Settings Protection** when password or **PIN Code** are lost.

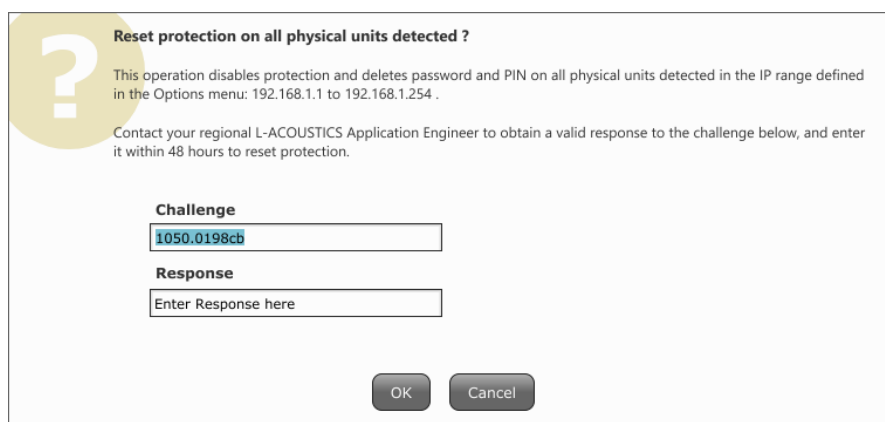
Pre-requisites: Ensure that all **Units** to reset are detected by **LA NETWORK MANAGER**, either on the **Workspace** or on the **Network Scanning Zone**.

1. Click on the **L-ACOUSTICS Cell** to open the menu.



2. Click on **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

Response

3. Contact L-ACOUSTICS® and provide the Application Engineer with the **Challenge** generated by the **Protection Reset** tool.
4. Enter the **Response** provided by the L-ACOUSTICS® Application Engineer within 48 hours. All passwords and **PIN Codes** will be reset.