

## Introduction

Ce bulletin technique décrit comment utiliser la protection des paramètres (Settings Protection) sur les contrôleurs amplifiés L-Acoustics LA2Xi, LA4, LA4X, LA8 et LA12X.

La protection des paramètres (Settings Protection) est à l'intention de l'intégrateur système, de l'ingénieur Application ou du directeur technique d'une installation fixe afin de :

- protéger les paramètres d'un système L-Acoustics à l'aide d'un mot de passe
- utiliser des variations de configuration en n'autorisant que certains fichiers de Session

**! La protection des paramètres ne verrouille pas les actions effectuées à partir de USB Terminal (réinitialiser les paramètres, modifications des réglages IP).**

Prenez des mesures pour limiter l'accès au port USB du contrôleur amplifié.

La protection des paramètres n'est pas disponible pour les processeurs P1.

## Droits d'accès

La protection des paramètres (Settings Protection) se fonde sur trois niveaux d'utilisateurs.

- L'administrateur : définit le mot de passe, le code PIN, et active/désactive la protection
- L'utilisateur avancé : utilise le code PIN pour contourner temporairement la protection
- L'utilisateur standard : a un accès restreint

Les droits d'accès ont été définis par L-Acoustics pour répondre aux besoins de 90% des installations fixes. Cette politique ne peut pas être modifiée par l'administrateur.

## Sécurité et réinitialisation

La protection est sauvegardée dans les contrôleurs amplifiés.

La protection ne peut pas être contournée ni en reformatant l'ordinateur hôte de LA Network Manager, ou en utilisant un autre ordinateur, ou en utilisant une version antérieure de LA Network Manager, ni en réinitialisant les contrôleurs ou en mettant à jour le firmware.

Si l'administrateur oublie le mot de passe, la protection peut être réinitialisée vers les paramètres par défaut à l'aide de l'outil Protection Reset de LA Network Manager. Consultez la section [Réinitialiser la protection](#) à la page 8.

## Champ d'application

La protection s'applique :

- au contrôle à distance via LA Network Manager
- au contrôle local via le panneau avant des unités

La protection ne s'applique pas aux solutions de contrôle tierces (AMX, Crestron, SNMP). Si nécessaire, l'intégrateur système doit installer une protection des paramètres distincte.

Lorsque la protection des paramètres (Settings Protection) est activé par l'administrateur :

seul l'administrateur peut	l'utilisateur avancé peut (avec le code PIN)	l'utilisateur standard peut
<ul style="list-style-type: none"><li>• charger des fichiers de Session non autorisés</li><li>• effacer un preset utilisateur</li><li>• réinitialiser les unités à leurs paramètres usine par défaut</li><li>• mettre à jour le firmware</li><li>• utiliser l'accès rapide au gain via le panneau avant</li></ul>	<ul style="list-style-type: none"><li>• charger un preset usine</li><li>• sauvegarder un preset</li><li>• modifier un paramètre de groupe</li><li>• modifier un paramètre de preset</li><li>• accéder à M1</li><li>• modifier l'adresse IP d'une unité</li></ul>	<ul style="list-style-type: none"><li>• charger des fichiers de Session autorisés</li><li>• restaurer une Session</li><li>• charger des presets utilisateur</li><li>• choisir le mode d'entrée</li><li>• muter / mettre en solo</li><li>• mettre en standby / wake-up</li></ul>

## Pourquoi utiliser à la fois un mot de passe et un code PIN ?

Le mot de passe :

- est à l'usage exclusif de l'administrateur
- permet d'activer ou de désactiver la protection
- est sauvegardé dans les unités physiques

Le code PIN :

- est défini par l'administrateur
- permet temporairement aux utilisateurs avancés sélectionnés d'accéder à un sous-ensemble de fonctions
- est sauvegardé dans les unités physiques et dans les unités virtuelles
- doit correspondre entre les unités physiques et les unités virtuelles lorsque des fichiers Session sont chargés. Dans le cas contraire, un conflit de PIN (PIN conflict) s'affiche

## Recommandations

- N'oubliez pas le mot de passe administrateur ni le code PIN.
- Choisissez avec soin à qui est communiqué le code PIN.
- Évitez d'utiliser des mots de passe ou des codes PIN différents sur les unités d'un système. Utilisez de préférence un seul mot de passe et un seul code PIN pour tout le système.
- N'utilisez pas la protection des paramètres (Settings Protection) sur les unités de rechange.
- N'utilisez pas la protection des paramètres (Settings Protection) sur les unités louées avec des hauts-parleurs complémentaires.

## Mise en place

Procédure recommandée pour la mise en place.

### Avant de commencer

Assurez-vous que toutes les unités physiques du système sont correctement détectées par LA Network Manager.

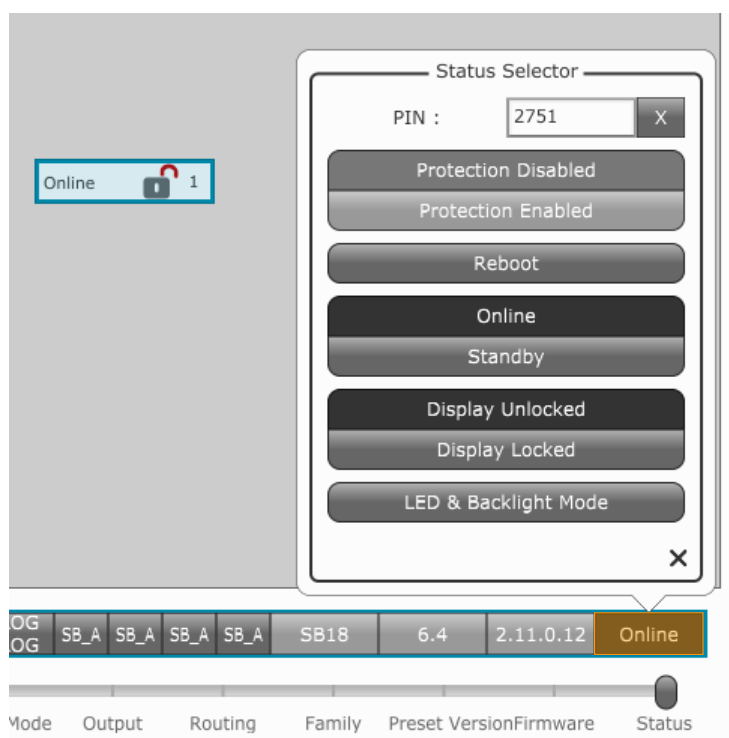
## Créer le code PIN et le mot de passe

---

### Procédure

1. Ajoutez toutes les unités physiques sur le Workspace.
2. Si nécessaire, mettez à jour toutes les unités LA4 et LA8 vers le firmware 2.1.2.0 minimum, et toutes les unités LA4X vers le firmware 1.0.2.0 minimum.
3. Sauvegardez un fichier Session "raw.nwm".  
Ce fichier sert à une étape ultérieure pour tester la protection.
4. Procédez à la vérification standard du système et effectuez la première calibration de référence.  
La calibration des variations, si nécessaire, est faite à une étape ultérieure.
5. Sélectionnez toutes les unités physiques.

6. Cliquez sur le statut dans la barre de commande des unités pour ouvrir le menu **Status Selector**.



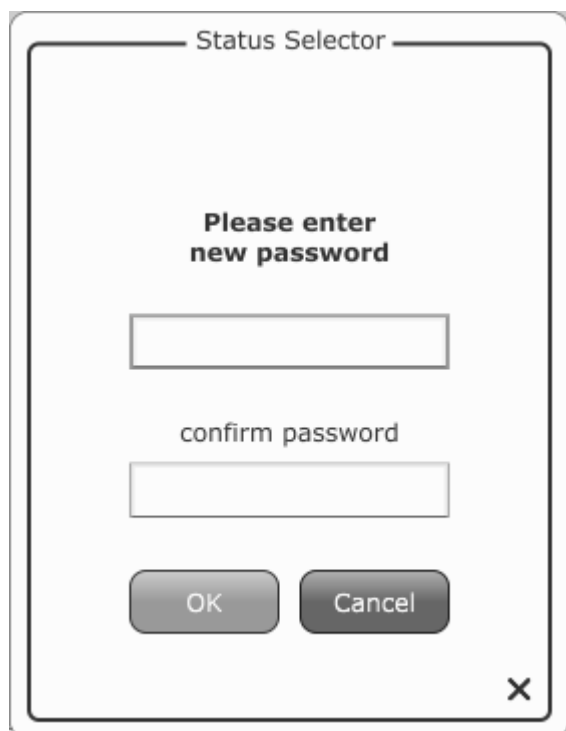
7. Dans le champ **PIN** entrez un code PIN à quatre chiffres et pressez la touche Entrée.

Le **Status Selector** affiche la boîte de dialogue du mot de passe.



8. Saisissez le mot de passe par défaut : `admin` et cliquez sur **Modify Password**.

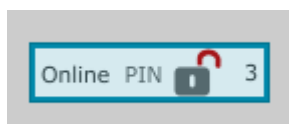
Le **Status Selector** affiche la boîte de dialogue permettant de modifier le mot de passe par défaut.



9. Saisissez le mot de passe administrateur de votre choix, puis confirmez et cliquez **OK**.


### Résultats

Le code PIN est sauvegardé dans les unités. Cela est indiqué sur le Workspace : lorsque le curseur est sur le statut, les unités ont un **PIN** gris sur fond blanc.



## Activer la protection des paramètres (Settings Protection)

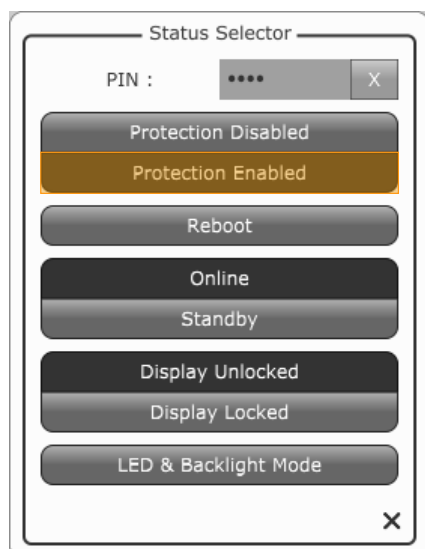
### Pourquoi et quand exécuter cette tâche

- 
**Activer la protection des paramètres (Settings Protection) avant d'enregistrer la Session**  
 Si le fichier Session est enregistré avant d'activer la protection des paramètres (Settings Protection), le code PIN est visible dans le fichier Session lors de son ouverture en mode **Offline**.

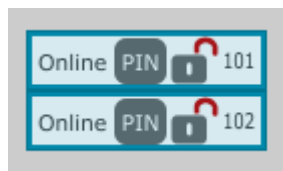
### Procédure

1. Sélectionnez toutes les unités physiques.
2. Cliquez sur le statut dans la barre de commande des unités pour ouvrir le menu **Status Selector**.

**3. Cliquez sur **Protection Enabled**.**



- 4.** Saisissez le mot de passe administrateur lorsque celui-ci est demandé.  
La protection des paramètres (Settings Protection) est active. Cela est indiqué sur le Workspace : lorsque le curseur est sur le statut, les unités ont un **PIN** blanc sur fond gris.



- 5.** Sauvegardez un fichier Session "bases.nwm".

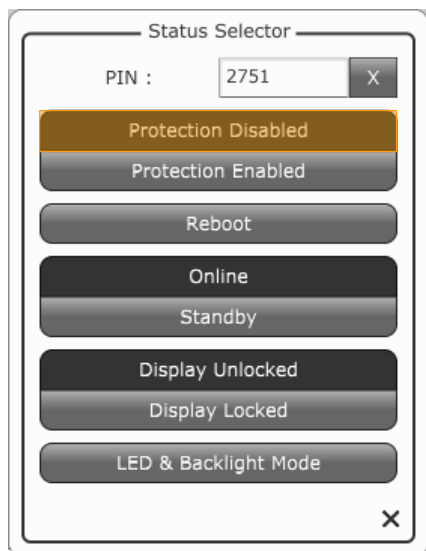
## Désactiver la protection des paramètres (Settings Protection)

---

Si nécessaire, suivez ces étapes pour désactiver la protection des paramètres (Settings Protection)

### Procédure

1. Sélectionnez toutes les unités physiques.
2. Cliquez sur le statut dans la barre de commande des unités pour ouvrir le menu **Status Selector**.
3. Cliquez sur **Protection Disabled**.



4. Saisissez le mot de passe administrateur lorsque celui-ci est demandé.

### Résultats

La protection des paramètres (Settings Protection) est désactivée.

## Créer les fichiers Session autorisés

### Procédure

1. Chargez le fichier Session "bases.nwm".
2. Désactivez la protection des paramètres Settings Protection.  
Consultez la procédure [Désactiver la protection des paramètres \(Settings Protection\)](#) à la page 6.
3. Procédez aux réglages pour la calibration de la variation.



#### Conflit de famille de preset

Assurez-vous que le passage d'un fichier Session à un autre ne provoque pas de conflit de famille de preset. Si un conflit de famille de preset se produit en utilisant le fichier de variation, la résolution du conflit nécessite d'entrer le code PIN.

4. Activez la protection des paramètres (Settings Protection).  
Consultez la procédure [Activer la protection des paramètres \(Settings Protection\)](#) à la page 4.



#### Activer la protection des paramètres (Settings Protection) avant d'enregistrer la Session

Si le fichier Session est enregistré avant d'activer la protection des paramètres (Settings Protection), le code PIN est visible dans le fichier Session lors de son ouverture en mode **Offline**.

5. Sauvegardez le fichier Session de la variation.  
Exemples : "speech.nwm", "movie.nwm", "live.nwm", etc.
6. Répétez les étapes 2 à la page 7 à 5 à la page 7 pour chaque variation.

## Vérifier Settings Protection

### Procédure



1. Vérifiez qu'il est possible de charger tous les fichiers Session des variations.
2. Vérifiez qu'il est impossible de charger le fichier "raw.nwm".

## Différencier les fonctions de verrouillage face avant (Disp. Lock / Disp. Unlck) et de protection des paramètres (Settings Protection)

### Identifier les unités verrouillées/déverrouillées

Vous avez la possibilité de verrouiller/déverrouiller les touches en face avant des unités physiques en ligne afin de prévenir toute modification accidentelle des paramètres.

Cela est indiqué sur le Workspace. Lorsque le curseur est sur **Status**:

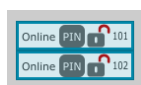
- un cadenas fermé  indique qu'une unité est verrouillée
- un cadenas ouvert  indique qu'une unité n'est pas verrouillée

### Identifier les unités protégées/non protégées

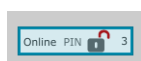
La protection des paramètres (Settings Protection) permet de protéger l'accès aux paramètres des unités à l'aide d'un code PIN.

Cela est indiqué sur le Workspace. Lorsque le curseur est sur **Status**:

- un **PIN** blanc sur fond gris indique que la protection des paramètres est active



- un **PIN** gris sur fond blanc indique que la protection des paramètres n'est pas active



# Modifier la protection

## Modifier le mot de passe

---

### Procédure

1. Sélectionnez toutes les unités physiques.
2. Cliquez sur le statut dans la barre de commande des unités pour ouvrir le **Status Selector**.
3. Cliquez sur **Protection Enabled** ou **Protection Disabled**.  
Le **Status Selector** affiche la boîte de dialogue du mot de passe.
4. Cliquez sur **Modify Password**.
5. Saisissez le mot de passe administrateur, puis confirmez.
6. Cliquez à nouveau sur **Protection Enabled** ou **Protection Disabled** si nécessaire.

## Modifier le code PIN

---

### Procédure

1. Sélectionnez toutes les unités physiques concernées.
2. Si une protection est activée, cliquez sur **Protection Disabled** et saisissez le mot de passe administrateur.
3. Entrez un nouveau code PIN et pressez la touche Entrée.
4. Saisissez le mot de passe administrateur lorsque celui-ci est demandé.

## Réinitialiser la protection

---

Si le mot de passe ou le code PIN sont oubliés, la protection des paramètres (Settings Protection) peut être réinitialisée.

### Avant de commencer

Assurez-vous que toutes les unités à réinitialiser sont détectées par LA Network Manager, soit sur le Workspace soit dans la network scanning zone.

### Procédure

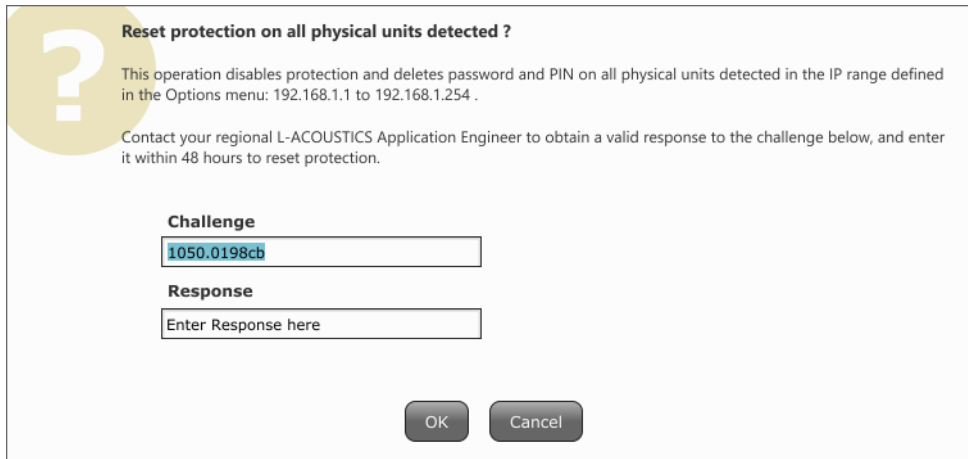
1. Cliquez sur le logo L-Acoustics pour ouvrir le menu.





## 2. Cliquez sur **Protection Reset**.

LA Network Manager affiche la boîte de dialogue Reset protection.



**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. Contactez L-Acoustics et indiquez à l'ingénieur Application la valeur du champ **Challenge** générée par l'outil.
4. Saisissez le code fourni par l'ingénieur Application L-Acoustics dans le champ **Response** dans les 48 heures, et cliquez sur **OK**.

## Résultats

Tous les mots de passe et codes PIN sont réinitialisés.

# Mise à jour du firmware des unités protégées

## Procédure

1. Désactivez la protection des paramètres (Settings Protection).  
Consultez la procédure [Désactiver la protection des paramètres \(Settings Protection\)](#) à la page 6.
2. Mettez à jour le firmware.  
Consultez l'aide de LA Network Manager.
3. Lorsque la mise à jour du firmware est terminée, activez la protection des paramètres (Settings Protection).  
Consultez la procédure [Activer la protection des paramètres \(Settings Protection\)](#) à la page 4.