



Network remotes & target device security

Purpose:

This document addresses a common problem Ashly customers have when configuring security in their network remotes, specifically the neWR-5, FR-8, FR-16, and Ashly Remote for iPad®.

The problem is that a remote can be properly networked, assigned to a target device, programmed, and appear to work fine, yet the targeted device does not respond to the remote control functions.

The solution is to properly set security settings on the targeted device and target device security settings on the remote.

Cause:

The lack of response by a targeted Ashly amplifier or signal processor is caused by a mismatch between its <Security Settings> and the <Target Device Security> of the assigned remote control.

Note: Security settings and target device security are not the same thing. Every Ashly networked device has its own security tab in software, offering multiple username-based password protections for that device alone. In addition, every networked *remote control* device has a separate but important target device security section in its main control surface for entering the security settings of its target device.

Security Settings:

A typical security tab for all Ashly networked amplifiers, processors, or remotes is shown here.

Username and password settings, where individual users are added for this device are circled in green. Access levels are circled in blue. Access levels allow each named user to have from full

access to view only privileges. Devices which have not yet been configured or have had a factory reset will have usernames of <default> and <admin>. They will also have blank passwords and full access. Passwords are case sensitive.

User Name	Password	Access Level
		Full Access
		Full Access
		Full Access
		Full Access
admin		Full Access
default		Full Access

For a remote control to be allowed access to its intended parameters on an amplifier or DSP processor, the remote's target device user name and password must exactly match the security settings of the target device, with access level set high enough on the target device to allow the intended functions.

Remote Control Target Device Security:

The main software control surface tab for an Ashly network remote device such as the neWR-5 or FR-8/16 is shown below. There may be differences in appearance between the models but the purpose and functions are the same. Target device security for the Ashly Remote app has the same function and can be found under the *Misc* menu while in the edit mode.

Target device security data for remotes is entered into the field circled in green below. If the target device has password user accounts set up, uncheck <Use Default Security Settings> and enter the same user name and password as used on target device. <Target User Name> and <Target User Password> need to *exactly* match the security credentials used in the target amplifier or signal processor, and are case sensitive.

By default, the neWR5, FR-8/16, and tablet remotes initialize with a username of “default” and a blank password. If no user accounts have been set up on the target device, leave the <Use Default Security Settings> box checked, and the default settings on both devices will allow full access without having to change the security settings.

If later on user accounts are set up on the target device, be sure to make the same changes to the remote’s target device security or they will stop working together.

The screenshot shows the 'neWR-5' software interface with the 'Security' tab selected. The 'Target Device Security Login Information' section is highlighted with a green circle. This section includes the following fields and options:

- Target Name: [Text Field]
- Target MAC: [Text Field]
- Target IP: [Text Field]
- Scan for Target IP Address:
- Target Status: [Text Field]
- Target Device Security Login Information:
 - Target User Name: [Text Field]
 - Target User Password: [Text Field]
 - Use Default Security Settings:

Other visible sections include 'Zone Setup' with 'Zone Upper Limit' (99) and 'Zone Lower Limit' (0), and a table of buttons (1-6) with their functions and preset channels.