Technical Quick Guides

How to disable tamper warnings

The Bosch Solution panels (and many auxiliary products) have inbuilt tamper switches to ensure that the security setup cannot be tampered with by intruders. While important in real installations, these tamper warnings can be irritating in demo/test environments.

This guide will outline the different tamper warnings on the Bosch 2/3/4000 panels and how they can be disabled.

System-Wide Tamper

Disabling the system-wide tamper disables all tamper warnings within the entire setup.

Note: This feature is unavailable on 2000/3000 panels with earlier firmware than v2.1.002.

Disable system-wide tamper on a text keypad IUI-SOL-TEXT

Enter the Installer code (default is 1234) then # to enter the installer menu.

Press 3 (*System*), 5 (*Fault*), then 9 (*System-wide Tamper*).

Press 0 to set the system-wide tamper to *Off*. This disables all tamper warnings in the setup.

When leaving the installer menu, make sure to press # to *Confirm to Save Parameter Changes*.

Disable system-wide tamper on an icon keypad IUI-SOL-ICON

Enter the Installer code (default is 1234) then # to enter the installer menu. The STAY and AWAY icons will flash to indicate Installer mode.

Enter 0109# to enter the system-wide & codepad tamper location. By default, this location is set to 7 (system-wide & codepad tamper fully enabled).

Enter 0 then * (STAY) to set the System-wide tamper to *Off*. This disables all tamper warnings in the setup.

Enter 960# to save changes and reset the system.

Onboard Tamper

The onboard tamper confirms that the panel PCB itself is installed correctly and hasn't been tampered with.

Disable onboard tamper on a text keypad IUI-SOL-TEXT

Enter the Installer code (default is 1234) then # to enter the installer menu.

Press 3 (*System*), 5 (*Fault*), then 8 (*Onboard Tamper*).

Press 0 to disable the onboard tamper.

When leaving the installer menu, make sure to press # to *Confirm to Save Parameter Changes*.

Disable onboard tamper on an icon keypad IUI-SOL-ICON

Enter the Installer code (default is 1234) then # to enter the installer menu. The STAY and AWAY icons will flash to indicate Installer mode.

Enter 0495# to enter the onboard tamper location. By default, this location is set to 6 (onboard tamper enabled).

If this location has a value between 4 and 7, onboard tamper is enabled. If it's less than 4, onboard tamper is already disabled.

Enter 2 then * (STAY) to disable the onboard tamper.

Enter 960# to save changes and reset the system.

Codepad Tamper

The codepad tamper confirms that the codepads have been installed correctly and haven't been tampered with.

Note: This feature is unavailable on 2000/3000 panels with earlier firmware than v2.1.002.

Disable system-wide tamper on a text keypad IUI-SOL-TEXT

Enter the Installer code (default is 1234) then # to enter the installer menu.

Press 3 (*System*), 2 (*Codepad*), then 8 (*Codepad Tamper Enable*).

Press 0 to disable the codepad tamper (for all codepads).

When leaving the installer menu, make sure to press # to *Confirm to Save Parameter Changes*.

Disable system-wide tamper on an icon keypad IUI-SOL-ICON

Enter the Installer code (default is 1234) then # to enter the installer menu. The STAY and AWAY icons will flash to indicate Installer mode.

Enter 0109# to enter the system-wide & codepad tamper location. By default, this location is set to 7 (system-wide & codepad tamper fully enabled).

Important: This location is for both system-wide AND codepad tamper. To disable tampers systemwide, we set this location to 0, but to disable just the codepad tamper, we remove 4 from the current value. E.g. if it's 7 (as it is by default) then change it to 3!

Enter 3 (or 4 less than current value) then * (STAY) to disable the onboard tamper.

Enter 960# to save changes and reset the system.

Zone (EoL) Tamper

Zones can raise a tamper warning if they have been set up with EoL resistors. These warnings will only be raised if a zone input has physically been removed or the EoL resistors have been incorrectly configured. These tampers provide useful feedback regarding configuration (as opposed to an annoying warning that means nothing) and so disabling them shouldn't be a priority, rather addressing them.

RF Receiver Tamper

There is no option to disable the RF receiver tamper in the panel's settings. The tamper switch must be physically taped down.

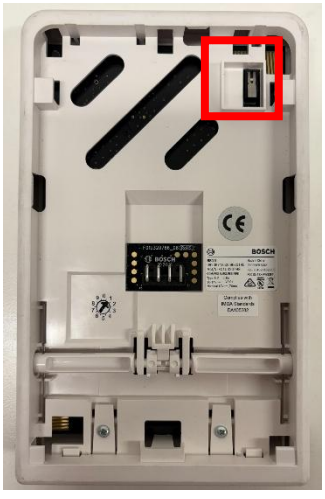
Physical methods to disable tampers

If you're using an older version 2000/3000 panel, you're getting a tamper warning you can't disable (such as RF Receiver Tamper), or a tamper warning is still overriding your settings, you may need to physically close the tamper circuit to remove the tamper warning.

Tamper Switches

On some products there is a physical switch that is pressed down when the unit is installed correctly, and is no longer depressed when the unit is removed from its

installation. These tamper switches can be disabled by taping the switch in the pressed position.



Open Tamper Circuits

On some products rather than there being a switch to press down, the built-in tamper is instead a pair of open terminals. These terminals are then connected to an external switch, which closes the circuit when the unit is installed correctly. You can disable these tampers by simply closing the circuit with a small piece of wire.