



How To Setup your InstaShow for Maximum Security



The BenQ InstaShow is a market leading wireless presentation system sold worldwide to many governments, educational, and corporate institutions that operate in high-security environments. Unlike some WiFi Network hub presentation systems that may [expose company networks](#) or notebooks to threats from hackers or 3rd party software applications, the InstaShow is designed to remove as many of these threats as much as possible. Recent testing by Washington DC cybersecurity expert Kenneth Buckler indicated that [InstaShow represents a minimal attack profile](#) and could not be used to hack into the corporate network.

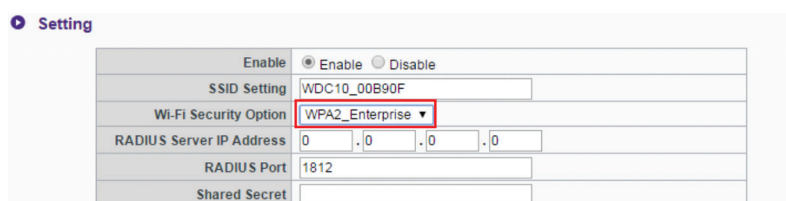
Built-In InstaShow Security Protections

InstaShow is unique since it does not need any software to be loaded onto a notebook to run. This is an effective way to protect your installation from threats associated with third-party software and also enables you to present from “locked down” notebooks without IT support. To protect your content from snoopers, each button transmitter has built-in wireless encryption of video and audio, eliminating any data interaction with the notebook. One benefit of this software-free design is that you can connect additional InstaShow buttons to non-notebook devices such as Blu-Ray players and document cameras to wirelessly share the screen.

Here are some helpful tips to maximize security for your InstaShow deployment.

Setup your password and encryption keys

Each InstaShow has a security password that enables administrators to log in to the device to manage common security requirements such as updating firmware, pairing additional buttons, naming devices, and other functions changing the screen messages. To maximize security, change your password after installation, and the rename the host device to your room name. You can also change the WAN connection from DHCP to Static IP using this menu as well. While all InstaShow wireless transmissions are encrypted using WPA2-PSK, you can also use WPA2_Enterprise for a network that requires critical authentication.

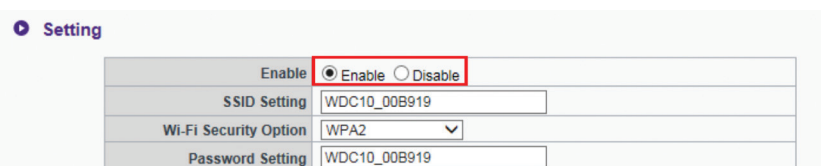


The screenshot shows the 'Setting' menu with the following fields:

Field	Value
Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSID Setting	WDC10_00B90F
Wi-Fi Security Option	WPA2_Enterprise
RADIUS Server IP Address	0 . 0 . 0 . 0
RADIUS Port	1812
Shared Secret	

Hide the Wireless Network

The InstaShow can be configured to hide its private wireless network and not broadcast any SSID information that can be seen on other wireless devices such as cell phones. This limits any login to the InstaShow only through the LAN port. While there are hacker tools to sniff out hidden networks, it is an easy way to keep the network hidden from visitors and curious internal staff.



The screenshot shows the 'Setting' menu with the following fields:

Field	Value
Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSID Setting	WDC10_00B919
Wi-Fi Security Option	WPA2
Password Setting	WDC10_00B919

Setup without connecting to the network

Security conscious IT managers have to approve and monitor every device on their networks for potential security threats from malware and tunneling programs. The InstaShow can be set up without any corporate network connection simply by using the LAN port on an unconnected PC or notebook. The device can be monitored and configured on the network but has been designed without any native ability to access the internet or third-party cloud services. To protect the notebook from data corruption, the USB connection is for power only and does not need to be connected to the computer to work. Any standard cell phone USB power supply will power the InstaShow button, enabling it to be used on non-PC sources such as Blu-Ray players, video conferencing systems, and document cameras.



Other helpful tips

Mix and Match Buttons for smoother meetings

Each InstaShow ships with two transmitter buttons and an attractive holder with space for any adapters you may need in your room. InstaShow buttons are available in both USB-C (Thunderbolt 3) and HDMI/ USB versions, so you can add a button kit to your initial starter kit to enable your team and visitors to choose the button connection that matches their notebook.

Label your buttons

Each button is paired with the specific receiver in that room and cannot be used with a different receiver without having to re-pair the encryption keys. By labeling your buttons, it is easy to identify which room it belongs to if someone has misplaced a transmitter.

To learn more about the security protections built into the InstaShow wireless presentation system, download the InstaShow security white paper [here](#).

Reference –

Wireless Presentation Threats: <https://threatpost.com/bugs-wireless-presentation-systems/144318/>

InstaShow Security Evaluation: <http://caffeinesecurity.blogspot.com/>