wePresent

WiPG/WiCS Devices

DEPLOYMENT GUIDE

Version: 2.05

Contents

1. Introduction 1

2. User Experience 2
- Standby Screen Display 2
- Hostname & SSID 2
- IP Address 2
- 4-Digit Security Code 2

3. WiPG/WiCS Device Installation 3
- Stand-Alone Connection Mode 3
- Network Connection Mode – Option A 4
- Network Connection Mode – Option B 5
- Network Connection Mode – Option C 6
- Deployment Options for Guest Network Access 7
- VLAN Based Network – Option D 7
- Physical Air-Gap Network – Option E 8
- Data Transport 9

4. Connecting to WiPG/WiCS Devices 10
- PC Connection 10
- MirrorOp Software Deployment 11
- Mobile Devices Connection – Smartphones and Tablets 11
- MirrorOp Device Discovery 12

5. WiPG/WiCS Customization 13
- Customizing Hostname/SSID 13
- Admin Panel 13
- Firewall Rules 13
- Port Table 14
- Wi-Fi Protocol 16

6. WiPG/WiCS Device Security 17
- WiPG/WiCS Device Security 17
- WiPG/WiCS Security Features 18

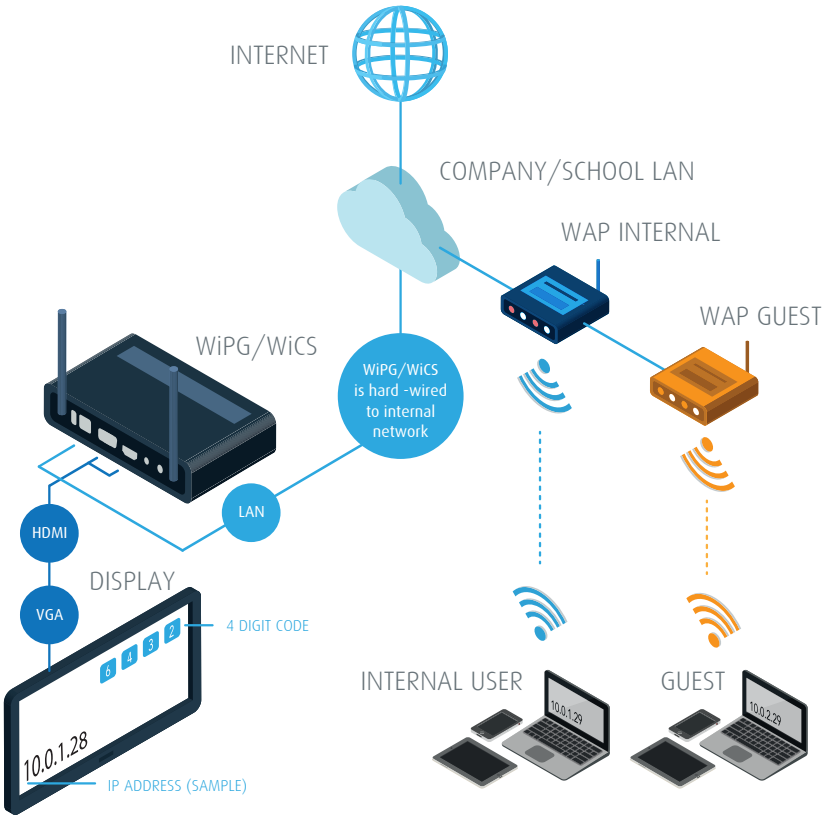
7. Firmware Upgrades 19
- Single Device (Web Interface) 19
- Multiple Devices 19

1. Introduction

The **wePresent WiPG/WiCS devices** help users to bridge the technology gap, allowing businesses and classes to enjoy the benefits of wireless presentation.

When connected to a display or projector, users can mirror their content without the need for connecting cables. The WiPG/WiCS products can be used as stand-alone devices, generating their own Wi-Fi signal or connected to a network through the LAN Ethernet port.

Windows and macOS users can share their desktop by installing and running free software called MirrorOp (Sender). The MirrorOp software is available from the wePresent website and WiPG/WiCS admin panel. Android and iOS users can share their content by installing the free MirrorOp (Presenter) application available from Google Play and the App Store.



◀ Basic WiPG/WiCS deployment example

The wePresent WiPG/WiCS devices are designed for commercial implementation in corporate, education, government, healthcare and public environments. This documentation provides deployment information for three current wePresent models (WiPG-1000, WiPG-1600W and WiCS-2100).

For more information, please visit our website http://wepresentwifi.com or email our help team at help@wepresentwifi.com.

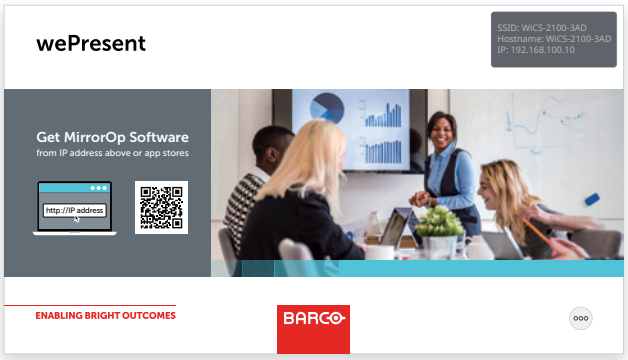
2. User Experience

Standby Screen Display

The WiPG/WiCS devices show the standby screen when the connected display/projector is turned on. Elements shown on the standby screen include the hostname, SSID, IP address, software download instructions and 4-digit security code (login code/passcode). The display can be personalized to allow custom login code and branding.

(WiPG)

◄ Standby Screen Display



(WiCS)

Hostname & SSID

The hostname and SSID can be customized/ renamed so that users can easily identify and log into the correct device if multiple units have been deployed on the network.

IP Address

Each WiPG/WiCS device will be assigned an IP address. By typing the IP address in a web browser, users will have access to software download, admin panel, control panel, and WebSlides for that particular device.

4-Digit Security Code

The security code prevents people outside the conference room/classroom from being able to log into the presentation.

There are three settings of operation for the security login:

1) Random: a new 4-digit code is generated after the last user disconnects.

2) Fixed: a static 4-digit code can be set from the admin panel

3) Disabled: 4-digit security code can be disabled through the admin panel

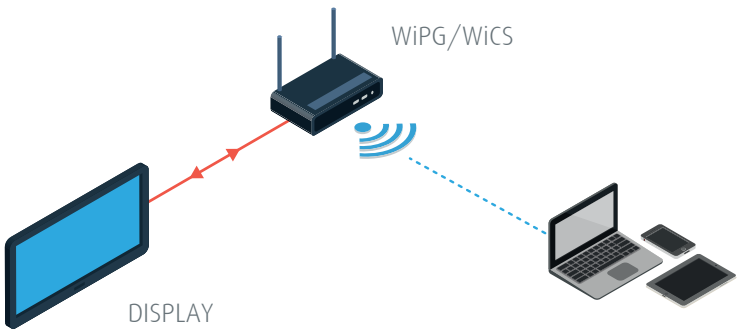
3. WiPG/WiCS Device Installation

Before presenting, users need to connect to the WiPG's/WiCS's Wi-Fi signal in stand-alone mode or connect to the network's Wi-Fi if the WiPG/WiCS device is connected to the network.

Stand-Alone Connection Mode

The WiPG/WiCS device is able to broadcast its own Wi-Fi signal, becoming an access point/hotspot that users can connect to. No internet access is required. The WiPG/WiCS device supports dual band and is able to broadcast on 2.4GHz band or 5.0GHz band.

NOTE: Wi-Fi interference can cause disruption or lag during a presentation (Wi-Fi pollution).



◂ Stand-Alone Connection Mode Basic Diagram

Recommended Environment

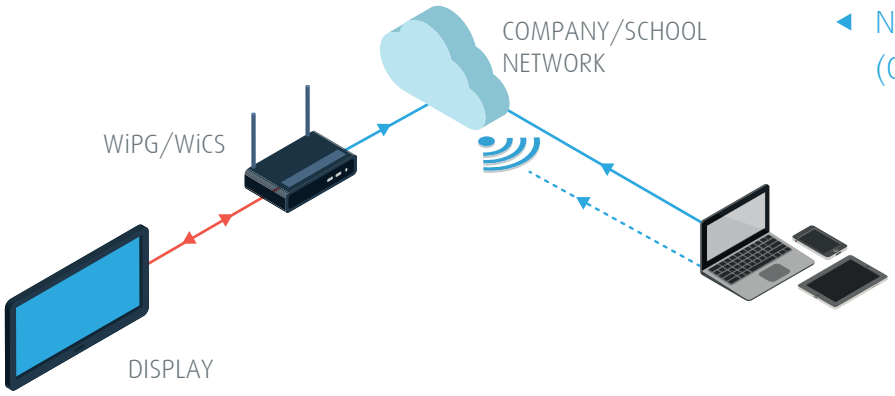
Small to medium size room with clear Wi-Fi having no more than 5 other access points.

3. WiPG/WiCS Device Installation

Network Connection Mode (Option A)

Join Corporate Network through Ethernet with WiPG/WiCS Wi-Fi Off

The WiPG/WiCS device is able to connect to the local enterprise/school network via the Ethernet/LAN port located in the back of the device using an Ethernet cable. In the network connection mode Option A, the Wi-Fi signal of the WiPG/WiCS device will be disabled. Both guest and internal users will access the WiPG/WiCS device through the access point (AP) on the enterprise/school network.



◀ Network Connection Mode (Option A) Basic Diagram

Recommended Environment

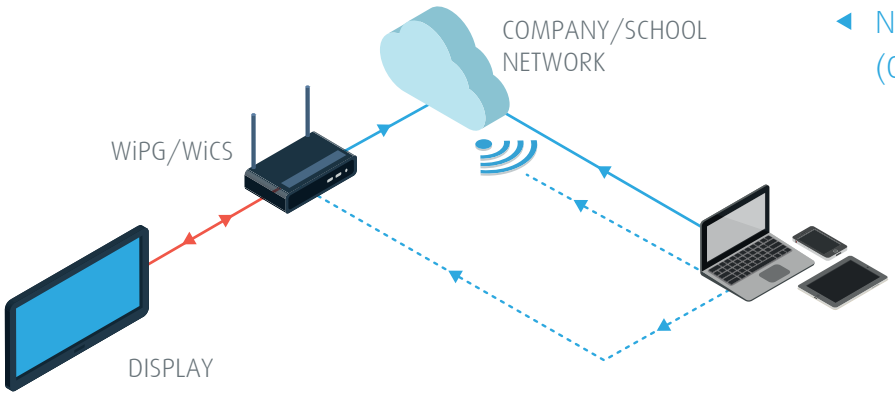
Office or school with many access points currently installed. Network connection mode Option A is a good option in environments where more than 10 WiPG/WiCS units are closely deployed. This option is ideal for networks that do not allow additional Wi-Fi APs due to security concerns.

3. WiPG/WiCS Device Installation

Network Connection Mode (Option B)

Join Corporate Network through Ethernet with WiPG/WiCS Wi-Fi On

The WiPG/WiCS device is able to connect to the local enterprise/school network via the Ethernet/LAN port in the back of the device using an Ethernet cable. In the network connection mode Option B, the WiPG/WiCS device will continue to broadcast a Wi-Fi signal, acting as a wireless access point (WAP). This scenario allows guest users to connect to the WiPG/WiCS Wi-Fi while internal users connect to the corporate Wi-Fi. The Gatekeeper security feature from the admin panel allows administrators to customize guest access - allow all / block all / internet only - according to the security level of the network.



◀ Network Connection Mode (Option B) Basic Diagram

Recommended Environment

Office or school with many access points currently installed. Network connection mode Option B is a good option in environments where more than 10 WiPG/WiCS units are closely deployed. Also ideal for scenarios where no corporate Wi-Fi AP exists or the corporate Wi-Fi is not open to guest users.

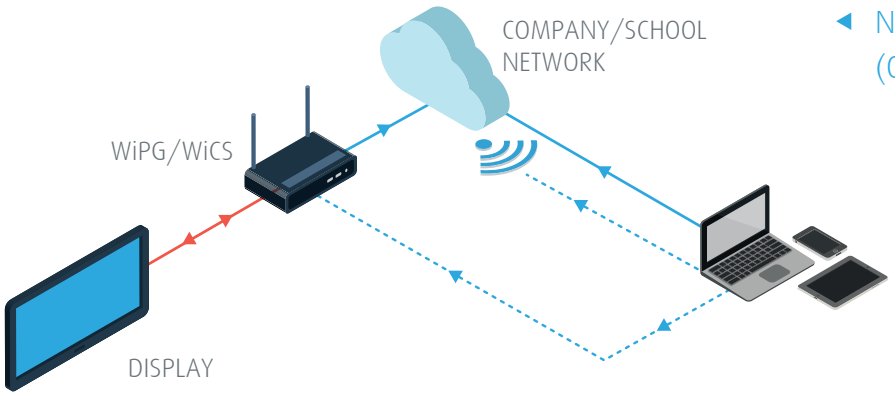
3. WiPG/WiCS Device Installation

Network Connection Mode (Option C)

Join Corporate Network through Wi-Fi Station Mode

The WiPG/WiCS device is able to connect to the local enterprise/school network using the WiPG's/WiCS's Wi-Fi. Network administrators need to configure the WiPG/WiCS device into the Wi-Fi Station mode in the admin panel of the target device. Both guests and internal users will access the WiPG/WiCS device through the AP on the enterprise/school network.

NOTE: Performance may not be optimal due to having two air hops between the computer/mobile device and the WiPG/WiCS device.



◀ Network Connection Mode (Option C) Basic Diagram

Recommended Environment

Office or school with many access points currently installed. Also a good option when the enterprise/school network consists of different VLANs for guest users and internal users. This option is ideal for networks that do not allow additional Wi-Fi APs due to security concerns, and for where the Ethernet connection to enterprise/school networks is not available.

3. WiPG/WiCS Device Installation

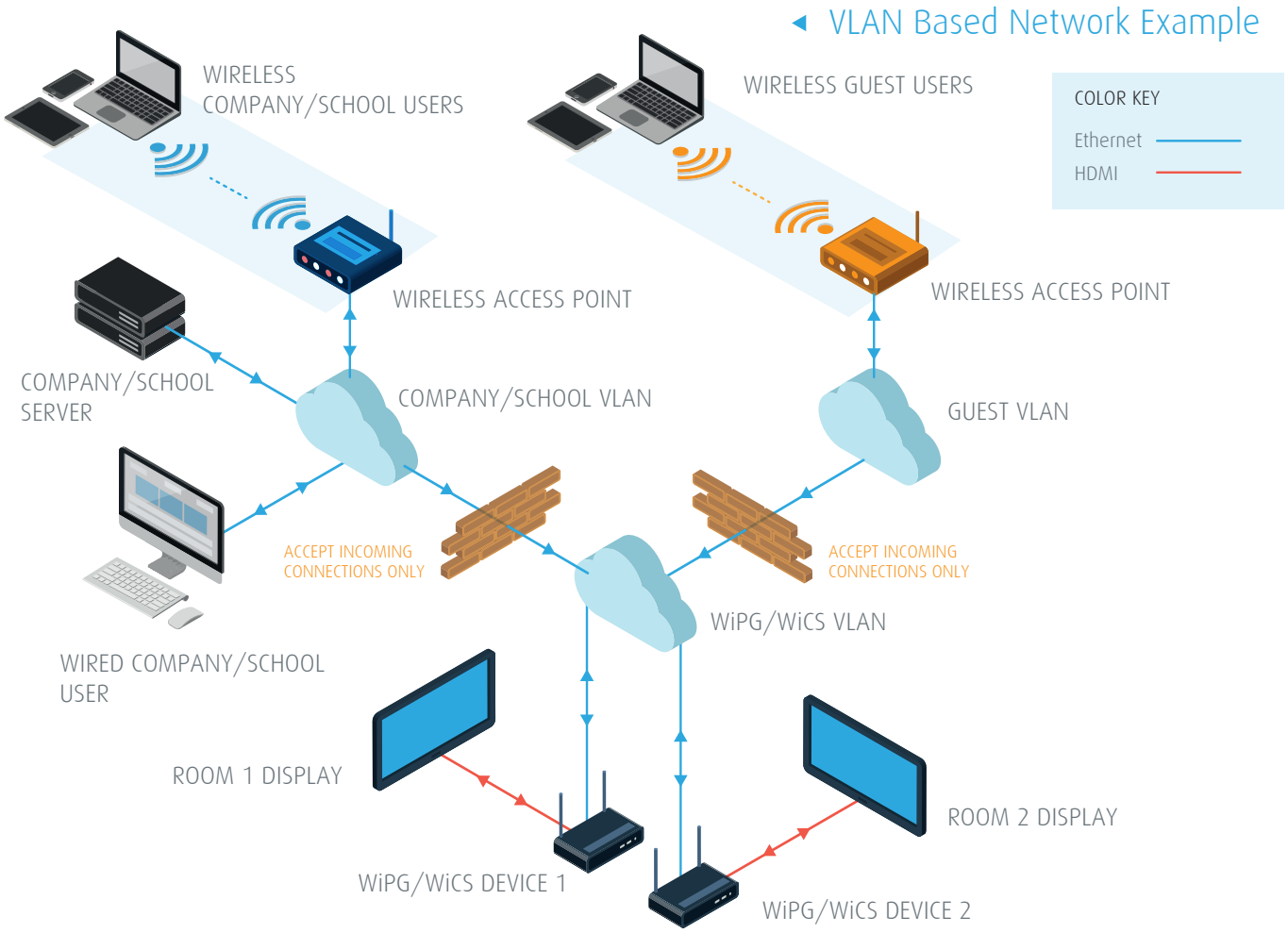
Deployment Options for Guest Network Access

In conference rooms, classrooms or meeting rooms, network managers need to be able to accommodate both internal and guest users and their respective network privileges. The standard network practice is to have a separate network for guest users to access, either a VLAN-based network or a physical air-gap network.

VLAN Based Network (Option D)

Virtual LANs (VLANs) are partitions that network administrators have set to provide separate networks for internal users and guest users in order to match different security requirements. The VLAN deployment diagram shows how the WiPG/WiCS devices communicate with the internal VLAN and guest VLAN.

◀ VLAN Based Network Example

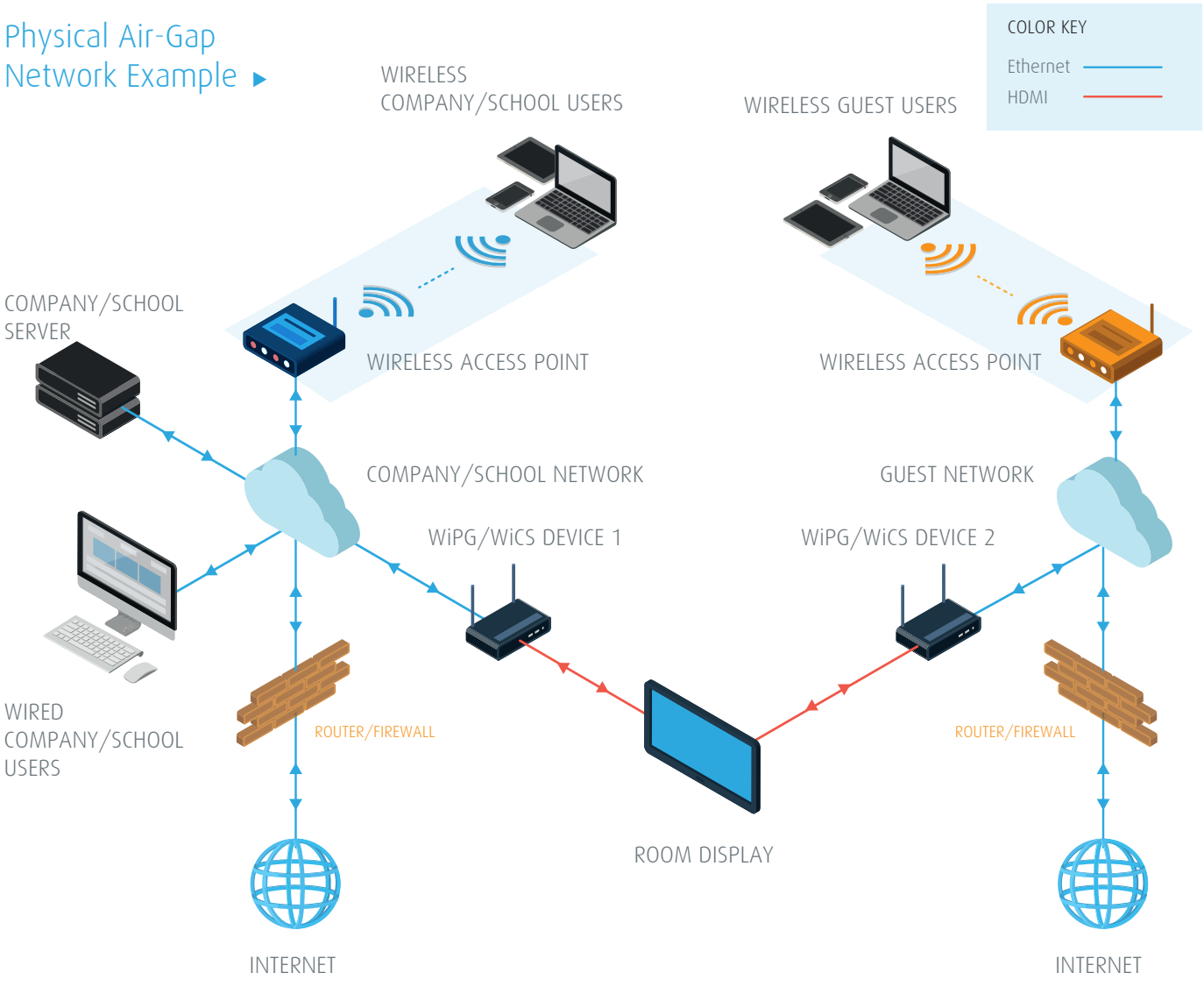


3. WiPG/WiCS Device Installation

Physical Air- Gap Network (Option E)

An air-gap (air-wall) network is used when network administrators want to physically isolate the internal network from the guest network. In this scenario, one WiPG/WiCS device is needed for the internal network and another WiPG/WiCS device needed for the guest network. Using a matrix switcher allows users to switch from viewing one unit's presentation to the other.

Physical Air-Gap Network Example ▸

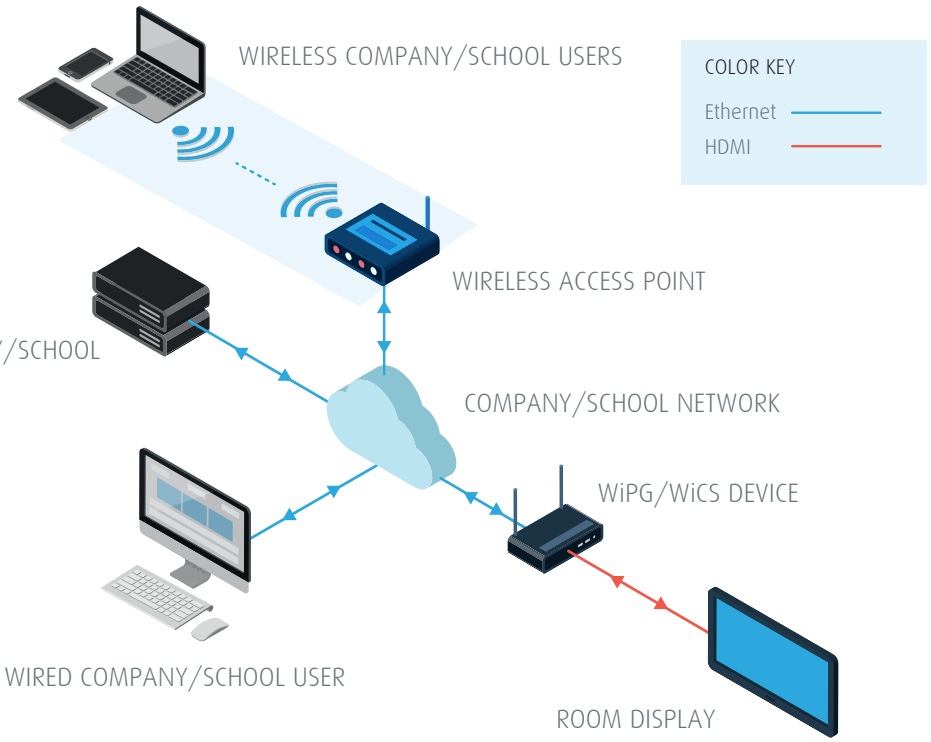


3. WiPG/WiCS Device Installation

Data Transport

The WiPG/WiCS device employs a proprietary protocol to transport the screen data from a computer or smart mobile unit to the WiPG/WiCS device. The data is encrypted and users accessing the data will need the four-digit code shown on the display/projector when launching the MirrorOp software.

WiPG/WiCS Data Transport ▸



4. Connecting to WiPG/WiCS Device

Computer Connection

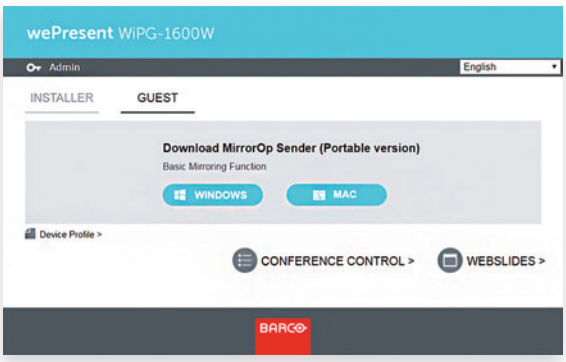
Internal Users

When presenting from a computer, internal users are suggested to install the MirrorOp software from wepresentwifi.com, or the admin panel/web page, MirrorOp is compatible with both Windows and macOS environments. Those who use any wePresent WiPG/WiCS device are authorized to execute MirrorOp. No software purchase is required.

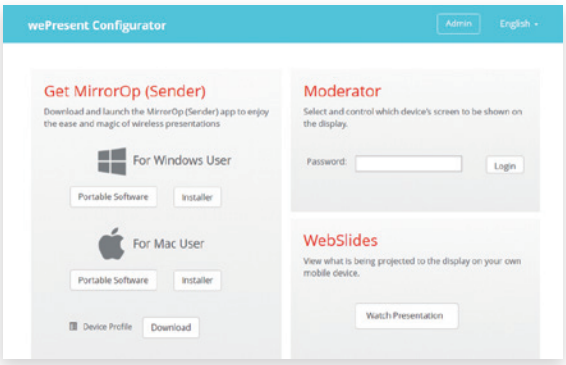
Guest Users

Guest users are recommended to download the MirrorOp executable file (portable software) from the admin panel/web page. The MirrorOp executable file will allow users to launch software and connect to the WiPG/WiCS device without needing to install full software.

Software Download Web Page ▸



(WiPG)



(WiCS)

4. Connecting to WiPG/WiCS Device

MirrorOp Software Deployment

Listed below are a few options for software deployments.

Admin Panel/Web Page

Users or the IT department can install the full MirrorOp (Sender) software directly from the admin panel/web page of the WiPG/WiCS device. The option to download the quick executable application (portable software) to launch MirrorOp is also available on the admin panel/web page.

Device Profile

The WiPG/WiCS "Device Profile" file provides a quick way to connect to a predefined receiver. A user can download the "Device Profile" file (an MOP file) from the admin panel/web page. Double click on the MOP file and it will connect to the predefined WiPG/WiCS device automatically.

Plug-N-Show (PnS) Token

Click on the "Make PnS Token" icon on the standby screen to copy the MirrorOp (Sender) executable file (protable software) to the attached USB drive. (Guest) users can launch the MirrorOp executable file directly from the PnS token to connect to the target WiPG/WiCS device.

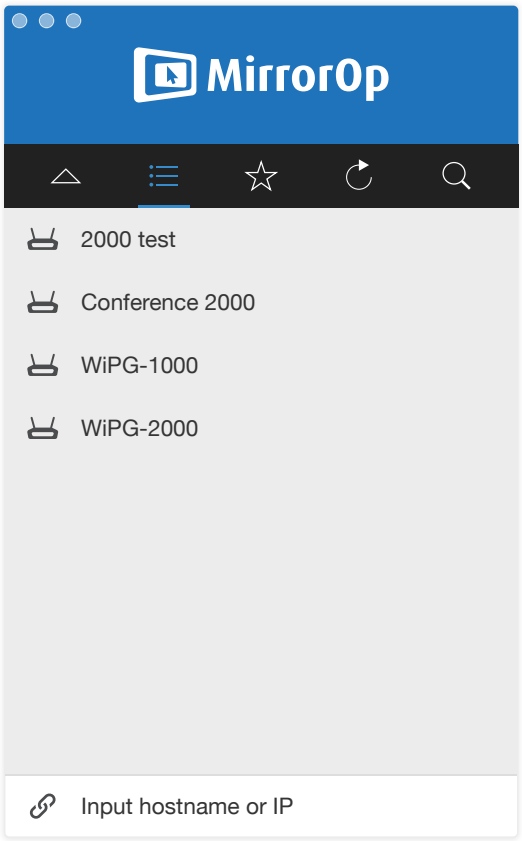
Mobile Devices Connection – Smartphones and Tablets

When presenting from an iOS or Android device (smartphone/tablet), users will need to install the MirrorOp Presenter App. MirrorOp Presenter can be downloaded for free from the Apple App Store or Google Play Store.

4. Connecting to WiPG/WiCS Device

MirrorOp Device Discovery

Managing the rooms in which the WiPG/WiCS device is installed can be a significant task. There may be multiple devices deployed in a certain room or across the enterprise/school network. The WiPG/WiCS device has two methods to access the connection parameters of a room: hostname and manual entry.



◄ MirrorOp Device Discovery Screen

Device (SSID) Listing

To view a current listing of connected WiPG/WiCS devices, click on the refresh icon from the menu on computers or drag down the window on mobile devices.

Manual Entry

The WiPG/WiCS device allows users to manually enter the hostname or IP address of the device in order to locate the device. The hostname or IP address can be entered in the "Input hostname or IP" field located at the bottom of Device Discovery Screen on computers. On mobile devices, IP address or hostname can be entered in the search field.

5. WiPG/WiCS Customization

Customizing Hostname/SSID

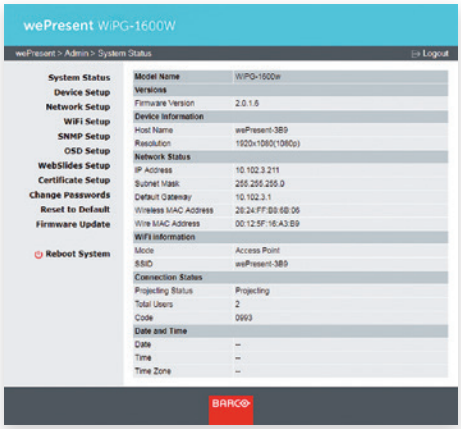
wePresent recommends that each WiPG/WiCS device be given a unique hostname/SSID that will assist users in identifying the target WiPG/WiCS device.

- NetBIOS resolution: utilized when the hostname/SSID is 15 characters or less and is disabled when the hostname is longer than 15 characters.

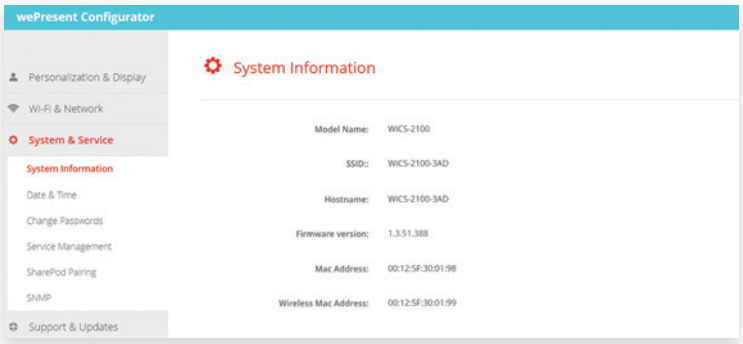
Admin Panel

The WiPG/WiCS device can be customized and configured through the built-in web pages of the device called the "admin panel". Parameters such as device IP address, WebSlides settings, centralized management, and WiPG/WiCS connected (display) devices are set under the **admin** menu option. The default password is **admin**, which can be changed.

◀ System Status/Information Panel



(WiPG)



(WiCS)

Firewall Settings

The MirrorOp software communicates with the target WiPG/WiCS device passing through network security systems such as firewalls. A set of rules need to be established so that traffic can be filtered and passed through the firewall. The firewall administrator will be prompted by the operating system to add a rule if a rule does not exist.

Port Table: The firewall administrator can allow or restrict certain data to be communicated from the user to the WiPG/WiCS device using the port table.

5. WiPG/WiCS Customization

Port Table (WiPG-1000/1600W) :

	USAGE	DIRECTION	PORT#	NOTE
TCP	Command	Both	443	AirPlay also uses this port.
			3268	
			389	
			5566	
	Data	Both	8080	
			31865	
			515	
	Audio	Both	1688	Used for screen projection and audio data transfer; need to open it to let audio projection work
	Video	Both	1041	
	UoIP	Both	3240	
			6000	
	DLNA	Both	2869	DLNA CMD port for connection created
			49152	
			49153	
	AirPlay		7000	
			7100	
			47000	
			4101~4199	
	Web Page		80	
			443	
	REST API		4001	
UDP	AirPlay	Both	5353	
	Device Discovery	Inbound	1047	Used for device discovery to find available devices; suggest opening all these 3 ports (1047~1049), and otherwise application can't find devices; may need to enter IP/hostname manually.
			1048	
			1049	
	NetBIOS Name Service	Both	137	Standard port number. This is for hostname used with windows.
			138	
	SNMP	Both	161	Standard port number. This is SNMP protocol port number.
	DLNA	Both	1900	SSDP broadcast used
			50000-65500	DLNA will select one of these ranges to do user action.
	DNS		53	
	DHCP		67	

5. WiPG/WiCS Customization

Port Table (WiCS-2100) :

	USAGE	PORT#
TCP	MirrorOp Projection	1234
	AirPlay & Google Cast	8008
		8009
		47000
		7000
		7100
		4101~4199
	UoIP	3240
		6000
	Web Page	7020
		80
		443
	REST API	4001
	DNS	53
UDP	Device Discovery	5353
	Google Cast	2048~65535
	NetBIOS Name Service	137
		138
	MirrorOp Projection	54022
	DNS	53
	DHCP	67

5. WiPG/WiCS Customization

Wi-Fi Protocol

WiPG/WiCS devices have both 2.4G and 5G Wi-Fi capability. Actual performance might vary due to radio-frequency (RF) interference. For small-scale deployment, a Wi-Fi channel analysis tool to find the proper available channel for the WiPG/WiCS device is recommended. For large-scale deployment, consulting a professional Wi-Fi integrator, or utilizing the enterprise/school network's Wi-Fi via the Ethernet connection is recommended.

Channel Lists for the WiPG devices:

2.4G BAND			
CHANNEL	FREQUENCY (MHz)	EU*	WW
1	2412	V	V
2	2417	V	V
3	2422	V	V
4	2427	V	V
5	2432	V	V
6	2437	V	V
7	2442	V	V
8	2447	V	V
9	2452	V	V
10	2457	V	V
11	2462	V	V
12	2467	V	
13	2472	V	

5G BAND			
CHANNEL	FREQUENCY (MHz)	NA	EU*
36	5180	V	V
40	5200	V	V
44	5220	V	V
48	5240	V	V
149	5745	V	
153	5765	V	
157	5785	V	
161	5805	V	
165	5825	V	

* EN 300 328 V1.9.1. Regulation

Adaptive Frequency Hopping of EN 300 328 V1.9.1 regulation requests the WiPG/WiCS device to implement the mechanism like Detect and Avoid (DAA) when an equipment identifying frequencies is being used by other devices. The Wi-Fi signal of the WiPG/WiCS device needs to be temporarily turned off if there is interference from different Wi-Fi access points or RF devices in the same environment.

Channel Lists for the WiCS devices:

2.4G BAND				
CHANNEL	FREQUENCY (MHz)	NA	EU*	WW
1	2412	V	V	V
2	2417	V	V	V
3	2422	V	V	V
4	2427	V	V	V
5	2432	V	V	V
6	2437	V	V	V
7	2442	V	V	V
8	2447	V	V	V
9	2452	V	V	V
10	2457	V	V	V
11	2462	V	V	V
12	2467		V	V
13	2472		V	V

5G BAND			
CHANNEL	FREQUENCY (MHz)	NA	EU*
36	5180	V	V
40	5200	V	V
44	5220	V	V
48	5240	V	V
52 (DFS)	5260	V	V
56 (DFS)	5280	V	V
60 (DFS)	5300	V	V
64 (DFS)	5320	V	V
100 (DFS)	5500	V	V
104 (DFS)	5520	V	V
108 (DFS)	5540	V	V
112 (DFS)	5560	V	V
116 (DFS)	5580		V
132 (DFS)	5660	V	V
136 (DFS)	5680	V	V
140 (DFS)	5700	V	V
149	5745	V	
153	5765	V	
157	5785	V	
161	5805	V	
165	5825	V	

6. WiPG/WiCS Device Security

WiPG/WiCS Device Security

Network security consists of different polices adopted to prevent and monitor unauthorized access, misuse, and/or modification of network resources. The WiPG/WiCS device has been designed to work in and adhere to a variety of computer network security environments: businesses, education, government and other public entities.

When the WiPG/WiCS device is connected to a corporate/school network, all traffic from the device is treated as from the corporate/school network. With the WiPG/WiCS WiFi disabled, the device sits on the network like any other network device (printer, etc.). It is important to remember that when connected to a corporate/school network, the WiPG/WiCS device is as secure as the standards set by the supporting network.

6. WiPG/WiCS Device Security

WiPG/WiCS Security Features

Enhanced security features are implemented in the WiPG/WiCS system to ensure the confidentiality, integrity and availability of the information communicated with the WiPG/WiCS system.

MODULE/APPLICATION	SECURITY ENHANCEMENT	NOTE
MirrorOP		
Screen data	Salsa20 encryption, 256-bit key	(WiPG-1000/1600W, WiCS-2100)
Audio data	No encryption	(WiPG-1000/1600W, WiCS-2100)
Web		
Web server	http (port 80) https (port 443)	Lighttpd (version: 1.4.4.1) OpenSSL (version: 1.0.2h)
Download	http (port 80) https (port 443)	(WiPG-1000/1600W) (WiCS-2100)
Conference control	http (port 80) https (port 443)	(WiPG-1000) (WiPG-1600W, WiCS-2100)
Web management data	http (port 80) https (port 443)	(WiPG-1000) (WiPG-1600W, WiCS-2100)
Web security assessment (WiPG-1000/1600W)	Patched	OWASP TOP 10 common Web Vulnerabilities
Remote Management		
SNMP (WiPG-1000/1600W, WiCS-2100)	SNMP v2 Protocol SNMP v3 Protocol	(WiPG-1000) (WiPG-1600W, WiCS-2100)
CMGS (WiPG-1000/1600W, WiCS-2100)		Based on REST API
WiFi Network		
WiFi	WEP, WPA, WPA2, WPA-Enterprise, WPA2-Enterprise.	(WiPG-1000/1600W, WiCS-2100) (WiPG-1000/1600W) (WiPG-1000/1600W)
wePresent System		
Firmware	MD5 encryption AES 256, RSA 4096	(WiPG-1000/1600W) (WiCS-2100)
Telnet, SSH	Disabled	
Port scan (WiPG-1000/1600W)	Done	
Vulnerability scan (WiPG-1000/1600W)	Patched	Nexpose.com
Application		
Windows	Digital signature	
Mac	Digital signature	

7. Firmware Upgrades

Single Device (Web Interface)

The WiPG/WiCS device supports firmware upgrades via the web interface. The upgrade is deployed as a single file that is uploaded and programmed by the device. The firmware upgrade takes approximately 5 minutes to load.

Multiple Devices

wePresent provides a management feature to upgrade multiple WiPG-1000/WiPG-1600W/ WiCS-2100 devices remotely. Remote device configuration and firmware upgrade can be performed via SNMP/REST API (CMGS) .