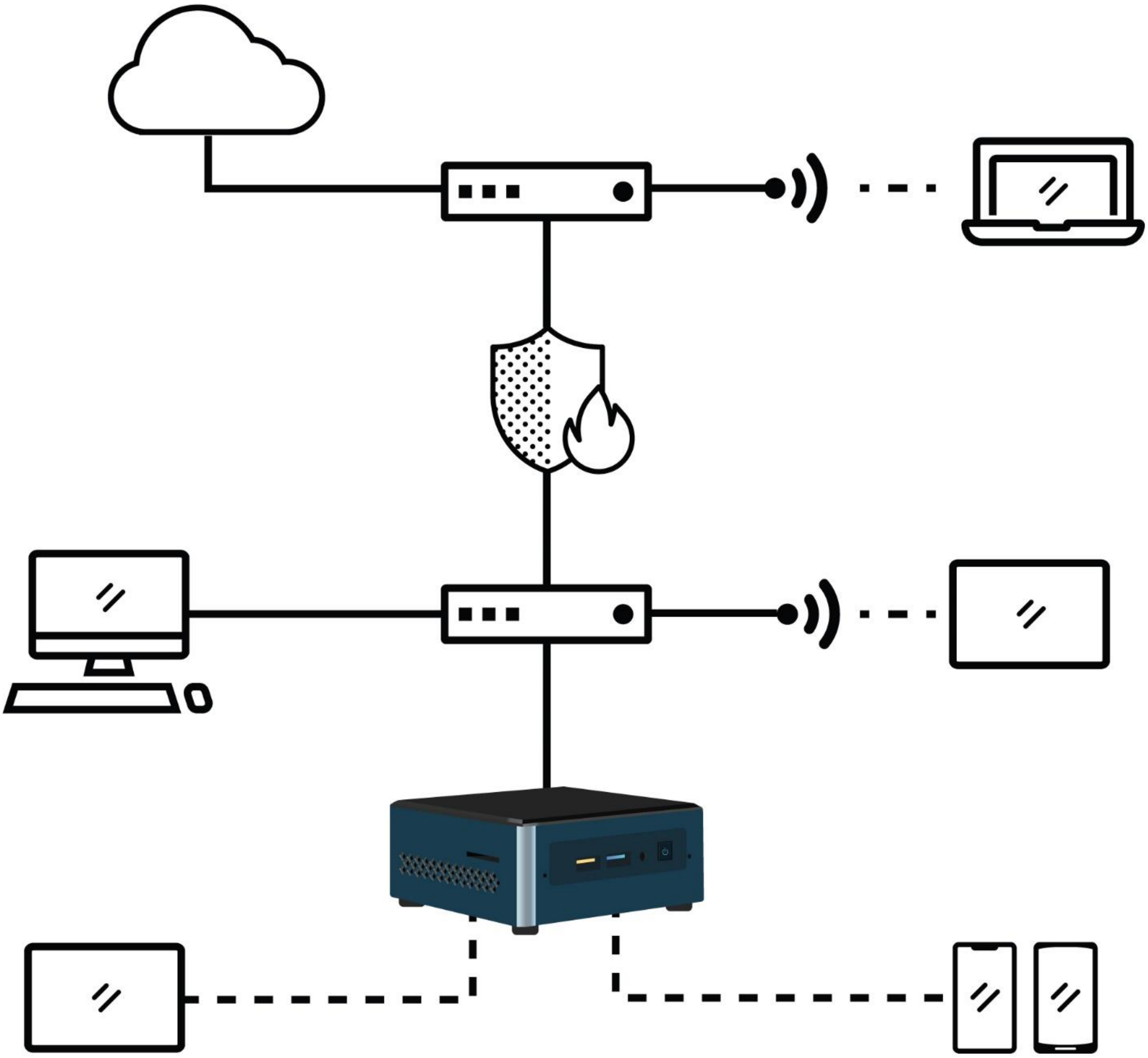
AirServer Connect

Developed by App Dynamic



Networking Overview

Version 1.1 – October 2019

AirServer Connect

Networking Overview

Contents

Introduction

The AirServer Connect brings together all major vendor supported screen mirroring protocols into one device. It supports AirPlay, Google Cast and Miracast. Guest connectivity is enabled by including a built-in Wi-Fi hotspot.

In order to get the best connectivity for both internal and external users, it is vital to configure both the AirServer Connect and the network to work together.

This guide will go through the features available on the AirServer Connect, the network requirements for different protocols and best practice for deployment and network configuration. For information about connecting to and using the AirServer Connect, please refer to the User Guide.

Visit our support site (https://support.airserver.com) for more information such as Release Notes and Knowledge Base or to create support tickets for any technical issues.

AirServer Connect Network Connectivity

The AirServer Connect has both wired and wireless networking capabilities:

- **Wired ethernet:** Connects the AirServer Connect to the building infrastructure network. Provides capabilities for Remote Management, updates and mirroring connections through infrastructure.
- **Wi-Fi:** Provides Wi-Fi hotspot for guest connectivity as well as Wi-Fi Direct beaconing for Miracast discovery. The built-in Wi-Fi cannot be used to connect to the building infrastructure network. Remote Management can be accessed through the Wi-Fi hotspot.
- **Optional USB Wi-Fi adapter:** From version 2.6 of AirServer Connect firmware there is the option to add selected USB Wi-Fi adapters to connect to the building infrastructure network. It is recommended to use wired ethernet whenever possible as two Wi-Fi links will increase noise and can increase latency. Please see our support page: https://support.airserver.com for a list of tested USB Wi-Fi adapters.

Screen Mirroring Protocols

AirPlay

AirPlay is used by MacOS and iOS devices. AirServer Connect provides AirPlay mirroring as well as audio only and video playback. AirPlay relies on Bonjour mDNS discovery, see section on Network Settings below on how to enable Bonjour in your network.

AirPlay mirroring streams are encoded using H.264 video compression and transmitted as TCP packets. Resolution can be up to 1080p at 60 fps and Apple recommend a bandwidth of 25 Mbps per mirroring stream. Average bitrates will be significantly lower, depending on the content.

Latency for AirPlay on AirServer is around 150 ms under good network conditions.

Content protected with Digital Rights Management (DRM) such as (but not limited to) Netflix, Hulu, Amazon Prime and rentals from Apple cannot be transmitted over AirPlay mirroring for copyright and legal reasons. This is a limitation set by the content providers.

Google Cast

Google Cast is used by most Android devices as well as Chrome OS and when casting from the Chrome browser. AirServer provides Google Cast mirroring only. Like AirPlay Google Cast relies on Bonjour mDNS for discovery, see section on Network Settings below on how to enable mDNS in your network.

Google Cast mirroring streams are encoded in H.264 or VP8 formats and transmitted as UDP packets. Most Android devices encode Google Cast at a resolution of 720p at 30 fps, but Chrome OS and casting from the Chrome browser as well as a few devices offer higher resolution. Maximum bitrate can be as high as 20 Mbps but average bitrates will be significantly lower.

Latency for Google Cast on AirServer is around 400 ms under good network conditions.

Most devices will not transmit video protected with Digital Rights Management (DRM) such as Netflix for copyright and legal reasons, this however is device vendor specific and is a limitation set by the content providers.

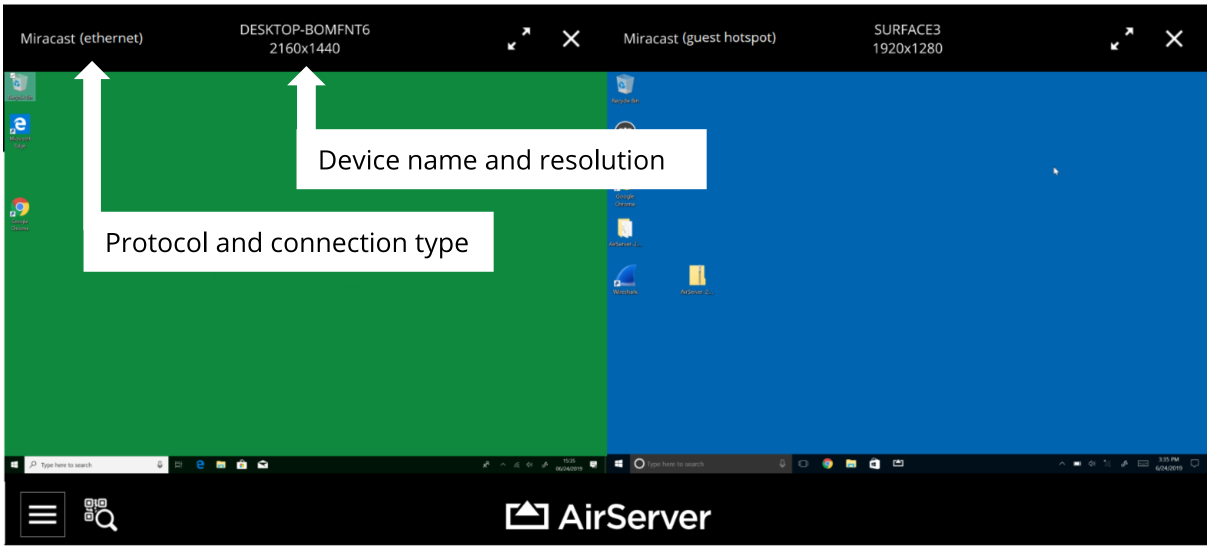
Miracast

Miracast is used by Microsoft Windows devices and some Android manufacturers, notably Samsung and LG. Miracast is developed by the Wi-Fi Alliance and is based on the Wi-Fi Direct standard. Miracast uses Wi-Fi beaconing to indicate the presence of a Miracast receiver. To initiate the connection the AirServer Connect sets up a Wi-Fi SSID starting with DIRECT- that Miracast senders can discover.

There are two different ways AirServer supports Miracast:

1. Standard or Ad-hoc Miracast: In this case the sender connects to the Direct Wi-Fi SSID and mirrors over that connection. The sender can also be on other Wi-Fi networks at the same time.
2. Miracast over Infrastructure: This is a vendor extension from Microsoft that is available for Windows 10 versions starting with 1703. It uses the Wi-Fi Direct beaconing for discovery but connects through the building infrastructure network.

Whenever possible, we recommend using Miracast over Infrastructure as it has more stability and shorter connection times. If Miracast over Infrastructure is not achieved, the sender will fall back to using Ad-hoc Miracast. If you are unsure which connection was established, you can check by enabling the home screen overlay on the AirServer Connect. That is done by pressing SPACE on a keyboard connected or by touching a touch enabled display.



For each connection there will be information on the connection type. The possibilities for Miracast are:

- Miracast (ethernet) = Miracast over Infrastructure
- Miracast (guest hotspot) = Ad-hoc Miracast or sender connected to built-in Wi-Fi hotspot first and the connection is Miracast over Infrastructure through the hotspot.

Miracast can support resolutions up to 4K 60 fps with capable sending devices and good network conditions. Average bitrates will depend on the content and resolution, but can be up to 35 Mbps for 4K video streams.

Latency for Miracast is around 180 ms with good network conditions. AirServer also implements hardware cursor on supported platforms where the mouse cursor shape and location are sent separately with very low latency.

To verify that a computer running Windows is capable of transmitting Miracast perform the following:

1. Open up a Command Prompt window and type: "*netsh wlan show driver*". The output will show information about the Wi-Fi interface. If Miracast is supported, you will get the following information:

   Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)

2. Open Powershell and type "*Get-NetAdapter | Select Name, NdisVersion*". The output will show NDIS versions that need to be 6.3 or higher for the Wi-Fi adapter.
3. Miracast requires Windows Display Driver Model (WDDM) 1.3 or newer. WDDM 1.3 was included with Windows 8.1. To check the WDDM version run the DxDiag tool (DirectX Diagnostic Tool), press "*Save All Information...*". Save and open the resulting text file and search for WDDM.

Network Settings

For full functionality of the AirServer Connect, the network connectivity must be correctly configured. This section covers what is needed for discovery and connection through the building infrastructure network as well as settings to optimize the Wi-Fi hotspot.

Discovery over Network

Discovery of the mirroring protocols that the AirServer Connect provides is done through network protocols. Discovery usually works without issues when connected to the built-in Wi-Fi hotspot, but some issues can come up when connecting through the building infrastructure network.

Bonjour Discovery

AirPlay and Google Cast rely on the Bonjour protocol for discovery over the network. Bonjour uses multicast DNS (mDNS) which cannot be routed across different segments of the network with standard settings on network equipment. For instructions on how to enable Bonjour across subnets, please refer to documentation from your network equipment manufacturer. An example can be found from Cisco:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-11/config-guide/b_wl_16_11_cg/b_wl_16_11_cg_chapter_01110100.html

It is also possible to deploy standalone mDNS gateways for instance using Avahi:

https://community.spiceworks.com/how_to/38251-build-your-own-bonjour-gateway

AirServer Connect announces the following Bonjour services:

- _airplay._tcp
- _googlecast._tcp
- _display._tcp
- _airserver._tcp
- _raop._tcp

Network interface isolation does not allow devices on the subnet to see other devices or discover services available. This is a common setting for guest networks and must be turned off for Bonjour to work.

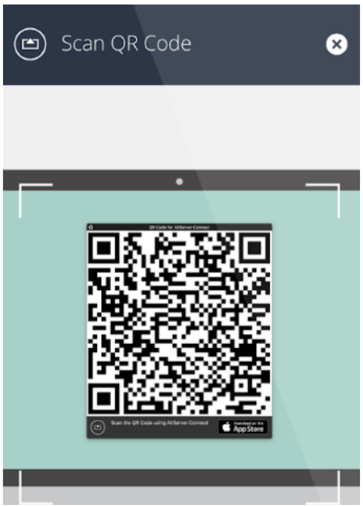
Discovery Assistance Apps

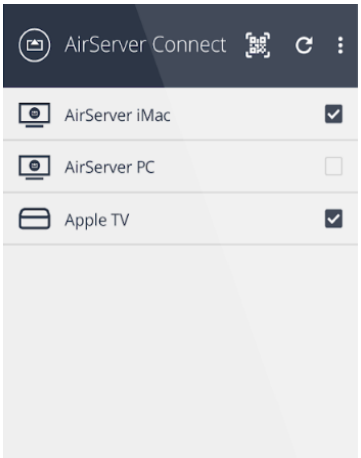
In some cases, it is not possible or feasible to provide Bonjour discovery across a large network. To help with discovery in these situations, AirServer Connect provides an option to show a network discovery QR code on-screen and apps for iOS and Android to help set up a connection.

Android: https://play.google.com/store/apps/details?id=com.appdynamic.airserverconnect

Apple iOS: https://apps.apple.com/gb/app/airserver-connect/id967004087

The QR code contains the hostname and IP address of the AirServer Connect device as well as the port to use for establishing a connection. The Android or iOS app then sets up a Bonjour proxy on the device using this information so that the built-in discovery tools see the AirServer Connect device as a screen mirroring receiver.



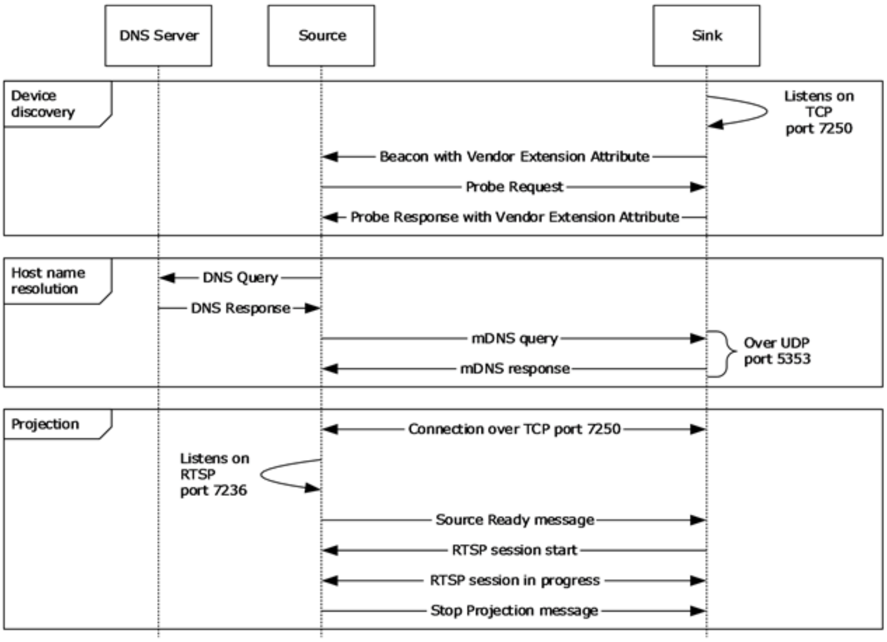


Note that this requires all relevant ports to be open between the sending and receiving device, see section on Port Openings below.

Miracast Discovery

Miracast receivers are discovered through Wi-Fi using Wi-Fi Direct beaconing.

In the case of ad-hoc/standard Miracast the rest of the setup is done be setting up a Wi-Fi connection between the sender and receiver. In Miracast over Infrastructure, the beaconing starts the communications over the building infrastructure. The following diagram from Microsoft explains that setup where Source is the sending device and Sink is the AirServer Connect:



Port Openings

The screen mirroring protocols used by AirServer rely on a number of ports to be open between the sending device and the AirServer Connect. A comprehensive list is not possible as all protocols use ephemeral ports and many outbound ports are chosen by the sending device.

The following table shows the list of UDP and TCP ports that need to be open between the sending device and AirServer Connect:

	Inbound		Outbound	
	TCP	UDP	TCP	UDP
All Protocols	32768-61000	5353, 32768-61000	32768-61000	32768-61000
AirPlay	5000-5010, 7100			
Google Cast	8008-8019	1900		
Miracast	7250		7236	
Management/updates	53, 80, 123, 443		443	

Fixed IP Address and Proxy

The AirServer Connect can be configured to work on networks that require a static IP address or a proxy for connectivity.

The following settings are available through both the on-screen menu or the Remote Management interface:

- Static IP: On or Off
- IP Address
- Gateway
- Netmask
- DNS 1
- DNS 2
- Proxy
- Hostname
- Port

802.1X Port Based Authentication

Starting with firmware version 2.6 AirServer Connect has support for environments with 802.1X port-based authentication. Currently there is support for PEAPv0/EAP-MSCHAPv2, but other authentication methods will be added later.

802.1X settings are available from the Network menu in Remote Management. Settings can be applied but only take effect when connected to an 802.1X managed network.

IPv6 Support

AirServer Connect has basic support for IPv6 networks and mixed IPv4 and IPv6 networks. Full support for IPv6 will be added in later versions. If you encounter any issues with connectivity, it is recommended to revert to using IPv4.

Hotspot Settings

The built-in Wi-Fi hotspot allows guests to connect easily to the AirServer Connect and start mirroring. The hotspot SSID and passphrase are shown along with a QR code in the bottom right of the AirServer screen overlay.

There are two possible methods for guest connectivity:

1. Use the built-in Wi-Fi hotspot
2. Advertise the in-house (guest) Wi-Fi on the screen overlay.

Settings for hotspot are accessible through the on-screen menu system or through Remote Management. For advanced use, we recommend using the Remote Management as it has more features than the on-screen menu system.

Built-in Wi-Fi Hotspot Settings

The AirServer Connect sets up a WPA2 secured hotspot with an eight-character random passphrase that is regenerated every 24 hours or when users select to End Session using the on-screen interface or Remote Management.

It is also possible to set your own passphrase, but not recommended as that can result in a lot of clients reconnecting to the hotspot when not mirroring, impacting the screen mirroring performance. To automatically regenerate passphrases, leave the passphrase field empty.

Wi-Fi Hotspot Access

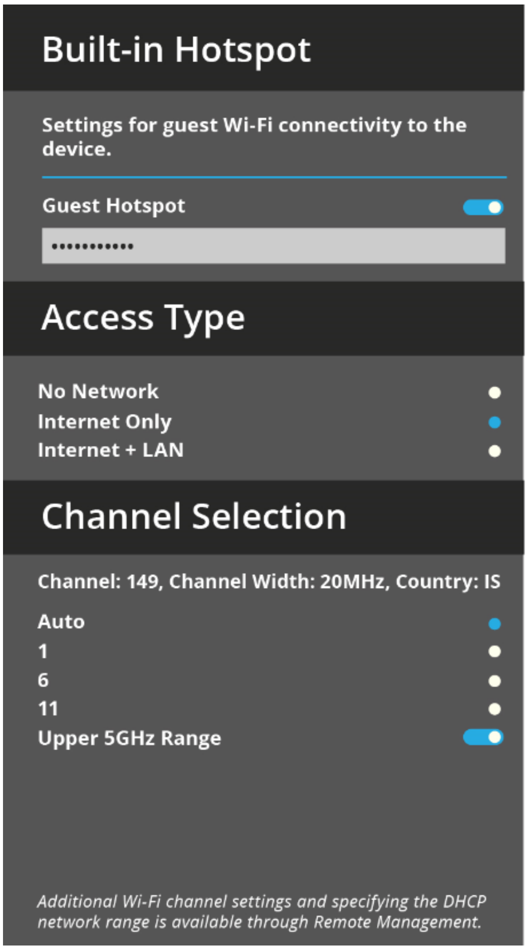
You can select which level of access guests get to the building network through the guest hotspot:

1. **No Access (Isolated Network)**
   Only allows those connected to the Wi-Fi hotspot to cast their screens to AirServer Connect. It provides no access to internal networks or internet. This is achieved with a firewall rule that blocks all IP addresses outside of the AirServer Connect.

2. **Internet Only (Guest Network)**
   Gives devices connected to the hotspot only access to mirror to the AirServer Connect and access public internet. This is achieved with a firewall rule that blocks typically reserved private IPv4 addresses, these are:

   - 10.0.0.0 – 10.255.255.255
   - 172.16.0.0 – 172.31.255.255
   - 192.168.0.0 – 192.168.255.255

   Any IPv6 addresses are not routed.



Built-in Hotspot

Settings for guest Wi-Fi connectivity to the device.

Guest Hotspot ●

•••••••••••

Access Type

No Network ○
Internet Only ●
Internet + LAN ○

Channel Selection

Channel: 149, Channel Width: 20MHz, Country: IS

Auto ●
1 ○
6 ○
11 ○
Upper 5GHz Range ●

Additional Wi-Fi channel settings and specifying the DHCP network range is available through Remote Management.

3. Internet + LAN

Gives devices connected to the hotspot full access to the building infrastructure network that the AirServer is connected to. Network administrators can place restrictions for that network to limit the access.

Visibility from Network

If using either of the two settings that allow for internet and/or LAN connectivity, the AirServer Connect routes traffic from the devices connected to the hotspot and uses Network Access Translation (NAT) towards the building infrastructure network. Only the MAC address of the AirServer Connect is visible towards the network.

DHCP Network Range

By default, the DHCP range for the hotspot is set to 192.0.2.1 – 192.0.2.254 but the range can also be set to:

- 198.51.100.1 – 192.51.100.254
- 203.0.113.1 – 293.0.113.254

Wi-Fi Channels

The Wi-Fi hotspot supports both 2.4 GHz and 5 GHz Wi-Fi channels and can be set to automatic or manual channel selection.

With automatic channel selection, a network scan is performed when starting the AirServer Connect and the best available band is selected. The highest preference is for the lower 5 GHz bands, then upper 5 GHz bands and finally channels 1, 6 or 11 on 2.4 GHz.

If using manual channel selection, it is recommended to perform a site survey or channel scan to select the best Wi-Fi channel.

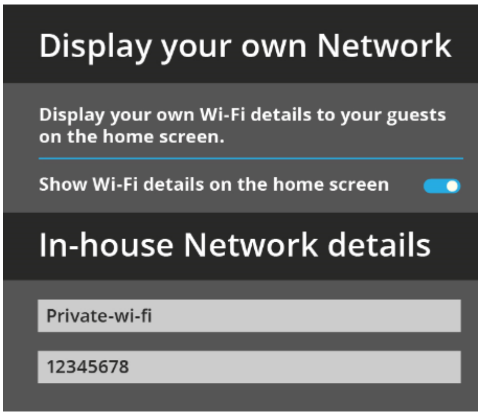
Wi-Fi channel availability depends on the country or region that the Wi-Fi access point detects using 802.11d regulatory domain beaconing from other access points. If there are multiple regulatory domains detected the hotspot will select worldwide domain that limits 5 GHz bands. The settings menu for the hotspot will indicate which channel, bandwidth and country settings are active.

Some client devices are not able to connect to upper 5 GHz channels (149-165). Starting with firmware version 2.6 these channels are by default restricted as some client devices do not support them. It is possible to enable upper channels through the on-screen or Remote Management interface.

Display your own Network

It is possible to display the connection details for the infrastructure Wi-Fi network on the home screen of the AirServer Connect.

If “Show Wi-Fi details on the home screen” is enabled, the home screen will display the network SSID and passphrase entered in this menu, but the built-in guest hotspot can still be enabled.



Display your own Network

Display your own Wi-Fi details to your guests on the home screen.

Show Wi-Fi details on the home screen

In-house Network details

Private-wi-fi

12345678