≈ AIRTAME | Making screens smarter

Airtame 2 Staged pre-deployment guide

≈ AIRTAME | Making screens smarter

Table of contents

Introduction to Airtame

Airtame is a wireless screen sharing solution that will allow your organization to have better meetings, save time on cable management and will help you to use screens better with digital signage options.

This is our "pre-deployment" guide to assist system & network administrators and IT supporters to integrate Airtame into their organization's IT infrastructure.

This includes all the required "need to know" information to consider before deploying the devices.
It will be focused around different use-cases that our end users have - meeting rooms for internal and guest users, Internal users only or digital signage only.

This "guide" will focus on technical aspects of Airtame devices and will not focus on introducing Airtame to your organization and its users.

System requirements

Supported Operating systems (For Airtame application)	Windows, macOS, Chromebook, Linux, Android, iOS
System Minimum (for Airtame Application)	System: Dual Core processor Memory: 2GB RAM WiFi: 802.11g OS: Windows 7, Ubuntu 15.04, Mac OS X 10.13, iOS 9, Android 4.2.2
System Recommended (for Airtame Application)	System: Dual Core Processor from 2013 or later (Core M3/M5, Core i3/5/7 or similar) Memory: 4GB RAM WiFi: 802.11n/ac OS: Windows 10, Ubuntu 15.04, MacOS 10.14, iOS 12, Android 4.2.2
Recommended Wireless Settings	2.4 / 5.2 GHz, 802.11b/g/n/ac, MIMO 2X2, 300Mbit

Pre-Deployment Considerations

Choose a suitable deployment strategy depending on your existing network configuration and how Airtame will be used at your organization.

Here are relevant questions to consider before deploying:

1. How will your organization be using Airtames and who should be able to use the device? Are your end users utilizing multiple VLANs or is the network flat?

2. Who will be allowed to present content to the screen? You can design your network to allow internal and guest users to present without bridging your internal and guest networks.

3. Software deployment: What operating system platforms are used in your IT environment? Will your internal users have the necessary permissions to install the application themselves? Will the application be deployed from your internal software repository? Will guest users have internet access to download the Airtame application?

4. Are there any special considerations that need to be made to stay compliant with your organization security policy? For example: PKI enrollment, security policy compliance, Group Policies, traffic zones and access control lists.

5. Do you have sufficient access to your organization's infrastructure to make necessary configuration changes on your servers/network/systems?

6. How will the Airtames connect into your network? Will you use your wired or wireless infrastructure?

7. How will the device be powered? Power adapter? PoE?

8. Airtame requires internet connectivity for firmware updates and accessing the features of Airtame Cloud. Are there any stipulations that would need to be considered before allowing the Airtame access to the internet? For example, web proxy servers, firewalls, etc.

Physical Installation Considerations

- Airtame is powered via the Aircord, which is plugged into the device's USB-C port.
- Airtame needs 2.5 Amps of power to work.
- It can not be powered using other cables or USB ports of the TV/display.
- To extend the Aircord, the Airtame Extension Cord must be used. It extends the range of Airtame's power supply unit by 1.8m/6ft.
- You can use VGA and DVI adapters, as well as HDMI extenders with Airtame.
- Only use the power adapter that comes in the box with the Airtame device.
- Airtame 2 is compatible with the Airtame PoE Adapter.

Note: The Aircord is not compatible with any USB extenders and, if necessary, should only be extended on the Power-side using Airtame Extension Cord.

Site Survey for Physical Installation

Consider these points to get an idea of the tasks ahead to physically install your new Airtame devices.

1. How are TV/Projectors installed in the rooms? Are they framed or hung on the wall or ceiling?
2. Are there available HDMI ports in the display?
3. Is the HDMI port easily accessible? Are the HDMI ports of the TV screen easily accessible? Does the display need to be un-framed or un-hanged to connect a new HDMI plug?

4. Is there an available wall socket for powering the Airtame device?
5. Where is the network entry point, for the Airtame device, in relation to the display:
    a. **In case of WiFi**: Where is the access point in relation to the display? Is there a clear line of sight between the access point and the display?
    b. **In case of Ethernet/PoE**: Is there an Ethernet port accessible in that room? How far is it from the display? How long of an Ethernet cable will be necessary to connect the Airtame device to the Ethernet port? Is there an available PoE enabled port in the access switch? Will an external PoE injector be needed? Is there a power wall socket available for the PoE injector?

Powering Airtame

Airtame comes with a US power adapter which can be adapted with EU, UK and AUS plugs. To connect the plug of your choice, follow these steps:

1. Take the PSU (power supply unit) and the adapter of your choice.
2. Slide the socket over the prongs of the power adapter.

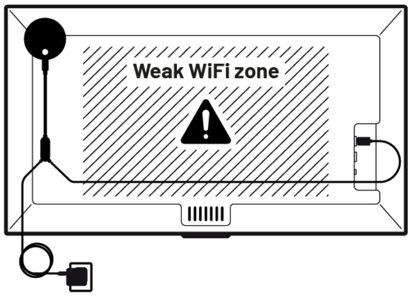
How to use Airtame 2 with Airtame PoE Adaptor

Follow the instructions or watch the video in this article: Airtame PoE Adapter

Mounting Airtame

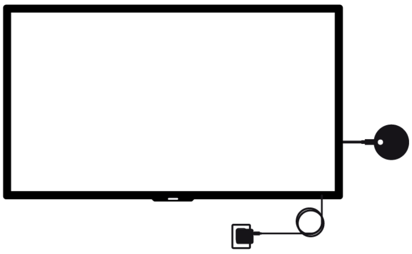
Airtame 2 provides flexible mounting options for both permanent and non-permanent installations. When choosing a spot to place Airtame, remember to:

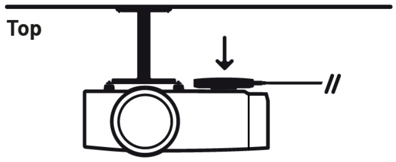
1. Place the Airtame as close to line of sight with the nearest AP as possible.
2. Place Airtame within 30 feet/ 10 meters of an AP.
3. Use an HDMI-in that is in the direction of the nearest AP.
4. Avoid placing Airtame 2 behind WiFi blockers such as the middle of the TV or furniture.
5. Keep the cabling out of sight by using the adhesive strip.

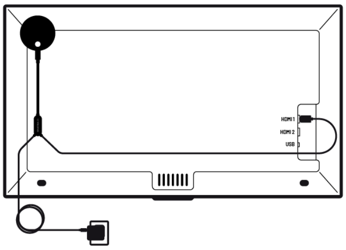


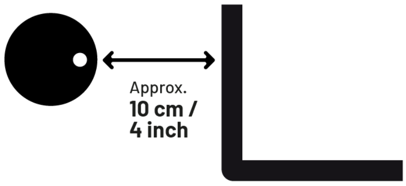
Permanent vs. non-permanent placement

- For permanent installations, use the adhesive strips of the wall mount and Aircable to secure the Airtame 2 to a non-magnetic TV, projector or the wall beside it.
- For non-permanent installations, only use the magnetism of the wall mount to fix the Airtame to a metallic surface of the TV or projector. In such cases, remember to leave the seal on the adhesive pads.



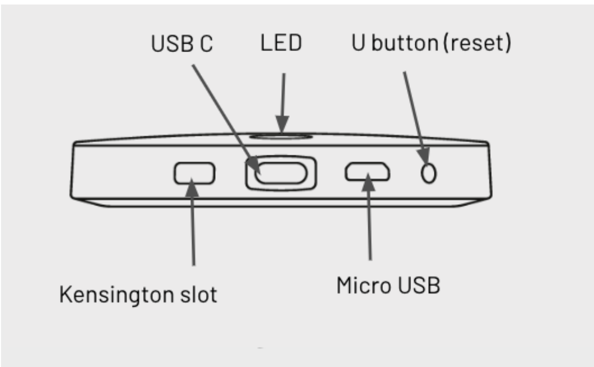






Physical security

Airtame 2 is equipped with a Kensington lock slot that gives a possibility to secure device in classrooms or big meeting rooms with ease. Our partners are bundling Airtame with this model of Kensington lock: Microsaver 2.0



Deployment Strategies & Network Implementations

Knowing how you want to use your Airtame will determine how you should deploy them in your network. We have determined the two most popular use-cases:

- Collaboration for Users in Different Network Segments
- Internal Use Only (in a Windows Enterprise Domain)

Protecting your organization's data is essential for any business and we think that you shouldn't compromise your security posture to allow external and guest users to present content on your meeting room screens.

Depending on how your organization chooses to use the Airtame, the requirements for optimal performance in your network infrastructure could vary.

Before deploying

Regardless of which deployment strategy you wish to use, there are a few requirements that you'll need to keep in mind before you deploy your Airtames.

1. Configure a VLAN for your Airtame devices.

2. Create a DHCP scope to service the Airtames (option 42 to point to a time server) We highly recommend creating a DHCP reservation as well, once your Airtame has received the first available IP address in the DHCP scope.

3. Consider DNS options.
   (If you want to use an internal DNS server, enable option 006 in the DHCP scope with the IP address of your DNS server. The Airtame will use 8.8.8.8 or 8.8.4.4 by default)

4. The MAC address for every device can be found on the box as well as the back of the Airtame in case you wish to "whitelist" your Airtames on a network or security appliance.

5. Make adjustments to ACLs and firewall rules to allow traffic to pass between clients and the Airtames. Below you will find which TCP and UDP ports that are required for optimal performance

Airtame ports list

PORT	TYPE	DIRECTION	SERVICE
AIRTAME			
8002	UDP	Both	Video + audio streaming
1986	TCP	Both	Mobile streaming
8080	TCP	Both	Device management+PIN code
80	TCP	To the Internet	Firmware & Software updates
1900+1901	UDP	Both	SSDP discovery
5353	UDP	Both	mDNS discovery
123	UDP	To the Internet	NTP
443	TCP	To the Internet	Airtame Cloud
AIRPLAY			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
554	TCP/UDP	Both	Real Time Streaming Protocol
1900	UDP	Both	SSDP Discovery
3689	TCP	Both	Digital Audio Access Protocol
5350+5351	UDP	Both	NAT Port Mapping Announcements
5353	UDP	Both	mDNS discovery
7000...	TCP	Both	Server port
7100...	TCP	Both	Data port
2001...	UDP	Both	Timing port
29053...	TCP	Both	Event port
61875...	UDP	Both	Audio Data port
GOOGLE CAST			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
8008-8019	TCP	Both	Google Cast listener ports
1900	UDP	Both	SSDP discovery
7236	TCP	Both	Content Casting
32768-61000	TCP/UDP	Both	Ephemeral Ports Return Traffic
MIRACAST OVER INFRASTRUCTURE			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
7250	TCP	Both	Miracast Packets
5353	UDP	Both	mDNS discovery

Collaboration for Users in Different Network Segments

There are various methods to allow your internal and guest users to stream to a single Airtame device without needing to switch the WiFi they are using.

The method presented here is our most recommended method, as it is the most secure. All the security is handled by your firewall using a secure traffic zone on your firewall. The Airtame will have 1 IP address that will be accessible from both your internal and your guest network. The setup and configuration will vary from vendor to vendor, but the overall steps are as follows:

1. Create a new VLAN on your firewall, create the IP addressing for this new subnet and assign that VLAN to a new traffic zone on your firewall, e.g DMZ.

2. Create a DHCP scope on your firewall that will service your Airtame devices. Make sure that option 42 is enabled and pointing to a NTP server. We highly recommend creating a DHCP reservation as well once your Airtame has received the first available IP address in the DHCP scope.

3. Now create the security rules in the rule base of the firewall. The rules should only allow access from the internal and/or guest network zones to new traffic zone. Allowing traffic between your internal networks and guest networks is not advised. The graphic below dictates which ports are required to be open for the new traffic zone.

4. In order for your internal users to find the Airtames for this type of deployment, make sure that you configure a static route on your core network to point traffic from your internal users to the IP address of the firewall that is directly connected to your core network.

After adding the applicable firewall rules, you will need to configure the routing on your firewall/security appliance. The process for doing this will vary from vendor to vendor. Please reference the administration guides from your vendor for configuration instructions.

Please see our article which has great examples of how one would configure and manage multicast on their network.

Here is the guide for creating a new traffic zone for your Airtames, so that you can allow secure access to them from your internal and guest networks without bridging your networks or compromising your security policies.

Internal Use Only in a Windows Enterprise Domain

As use cases vary from organization to organization depending on business needs, you may have the requirement to use the Airtame in a more restricted environment for internal users to collaborate and share content.

Integrating Airtame into your domain isn't too much different than the scenario above, however there are some extra steps that need to be taken to ensure that the Airtame will be authenticated by the domain.

If you want to authenticate your Airtames in your Windows domain, you'll need to know which authentication method you would like to use. EAP-MSCHAPv2 (PEAP) and EAP-TLS are supported. For more information about these two authentication methods and how to authenticate your Airtame, please reference our guide "Authenticating your Airtame" to learn more about these two authentication methods and how to implement one of these methods in your domain.

Network Requirements:

1. Create a dedicated Airtame VLAN.

2. Add the Airtame VLAN to the VLAN database of your layer 2 switches and create the Airtame layer 3 interface (SVI).

Domain Requirements:

1. Create a DHCP scope to service the Airtames.
   Enable Option 42 to tell Airtame where it can find a timing source.
   If you want to use your internal DNS server, enable option 006 and provide the IP address of your internal DNS server.

2. Create a service account for your Airtames.

3. After you have decided how you would like to authenticate your Airtames, you'll need to set up the Connection Request Policy and Network Access Policy on your RADIUS server. For more information, please refer to our article on Authenticating your Airtame. This article provides some tips and tricks for troubleshooting authentication.

4. Acquire a CA certificate and use the service account credentials to authenticate the Airtame. For more information about creating client certificates and configuring your RADIUS server, please refer to the Authenticating your Airtame guide.

Discovery

In Airtame's case, Multicast is used for the Airtame application to discover all Airtames on the network. In order for the list of available Airtame devices to automatically appear in the Airtame application, Multicast must be enabled. It is fair to expect more bandwidth consumed by Multicast traffic, therefore auto-discovery is optional for Airtame devices to work. It is always possible to connect via manual discovery.

Auto-Discovery

In order for auto-discovery to work properly, multicast routing should be enabled globally on the network appliances handling the traffic and IGMP/PIM should be configured on the VLAN interfaces participating in the passing of multicast messages. The Airtame uses Simple Service Discovery Protocol (SSDP) and/or Multicast Domain Name System (mDNS) to allow end users to discover the Airtame devices in the network. For more information on how to configure multicast and which flavour of PIM you should be using in your network, please read our article on configuring and managing multicast.

Routing Multicast Messages Between VLANs

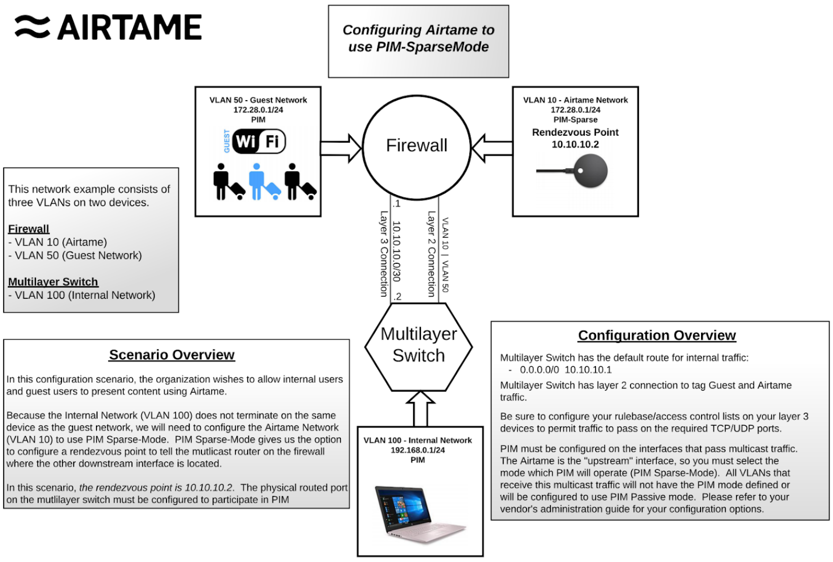
More often than not, multicast routing needs to be enabled in the global configuration of your network appliances as it's usually disabled by default. Once you've enabled multicast routing, you'll need to enable IGMP on the Airtame's VLAN interface (SVI). This will allow local link multicast messages to reach hosts on the same VLAN. However, if you want multicast messages to traverse the layer 3 boundary and reach hosts in other VLANs, you'll need to set up Protocol Independent Multicast (PIM) on the interface.

PIM can be configured to operate in either **dense mode** or **sparse mode**. The decision on which mode to choose largely depends on how your network is designed and where you want to send the multicast messages.

PIM Sparse

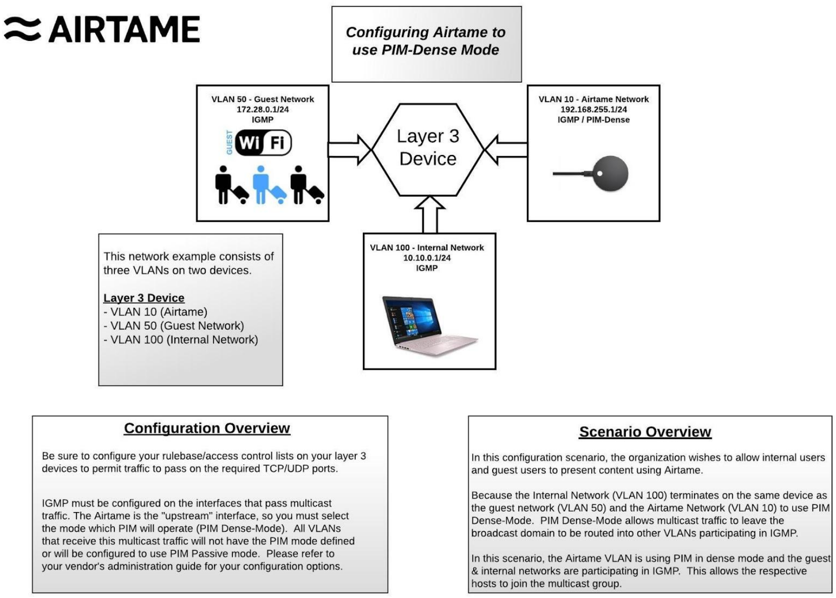
If you want to send Multicast messages to a remote network, you will want to configure **PIM** in **sparse mode** on the layer 3 interface of the **VLAN (SVI).** A typical scenario where one would expect to use **PIM** in **sparse mode** is when you want to send Multicast messages to hosts in a different **VLAN** that terminates on a different network appliance in your network.

In the case of Airtame, you can place your Airtame devices in their own **VLAN** that terminates on your firewall. Because the guest network terminates on the firewall, the firewall will see that subnet as a connected network. Since your internal networks are likely terminated in your core network, you must configure your firewall to know where to send those multicast messages. The **IP address** of the layer 3 interface on your core network will be your **rendezvous point**.



PIM Dense Mode

If your network is designed so that the sender and receivers of Multicast messages are placed in VLANs that terminate on the same appliance, **PIM** in **dense mode** will be configured on the layer 3 interface **(SVI)** of the Airtame **VLAN**. This mode of **PIM** does not forward Multicast messages to remote networks.



IGMP Proxy

Some L3 devices that support multicast may not support **PIM**. Those devices that don't support **PIM** will usually have **IGMP Proxy** as a feature and will be accessible through the GUI of the appliance.

IGMP proxy enables the router to issue **IGMP** host messages on behalf of hosts that the router discovered through standard **IGMP** interfaces. The router acts as a proxy for its hosts.

Configuring multicast routing, IGMP and PIM will be specific to the vendor(s) of your network equipment. We encourage you to look at the vendor documentation to see which multicast options are supported on your network appliances.

Manual Discovery

If your organization does not permit multicast traffic on the network, auto-discovery will not work. Airtame devices are always reachable by typing in IP address.

There are also a few options on how to make manual discovery more convenient.

Option 1 - replicate the list of Airtame devices and pre-saved preferences to multiple apps

For this to work reliably - Airtame devices need static IPs, be sure to read our guide on how to Set a static IP address for more information. The list of bookmarked Airtames and the App preferences are stored in a file within the computer user's profile folder.

This file can be copied to other PCs in the organization, so the list of Airtame devices will be replicated, as well as the App settings.

On Windows:

C:\Users\%USERNAME%\AppData\Roaming\airtame-application\IndexedDB\file__0.indexeddb.leveldb

On MacOS:

~/Library/Application Support/airtame-application/IndexedDB/file__0.indexeddb.leveldb

The file is named:
000003.log
The file is a mixture of plain text and binary code. It is not intended to be edited manually.

Deployment Steps

1. Open the Airtame application on your computer.
2. "Star"/Bookmark the Airtame devices you want other users to have.
3. Click on preferences.
4. Set the preferred settings (if any), for example:
5. Copy the file mentioned above and replace it in the exact same location on the target computers using your preferred deployment method.

This process will overwrite the user's own list of starred Airtame devices and settings in their application. This means users who had already starred some Airtame devices or configured their Airtame App's preferences will lose their customization.

Keep in mind that users will still be able to remove the saved Airtame devices and modify the preferences of the Airtame App on their computer.

Option 2 - connect to Airtame via hostname (Windows only)

If your environment does not support SSDP multicast discovery, you would usually rely on finding and streaming to an Airtame by its IP address into the Airtame application. In this section we will show you an alternative way to connect to an Airtame device on your network by typing its name into the Airtame app instead of its IP address (without multicast).

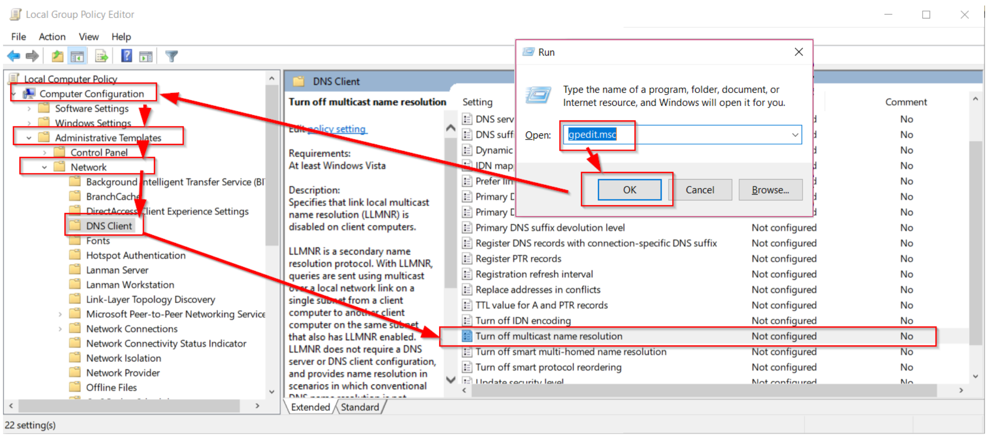
This method is a work-around as it only applies to Windows, and is therefore not a cross-platform solution.

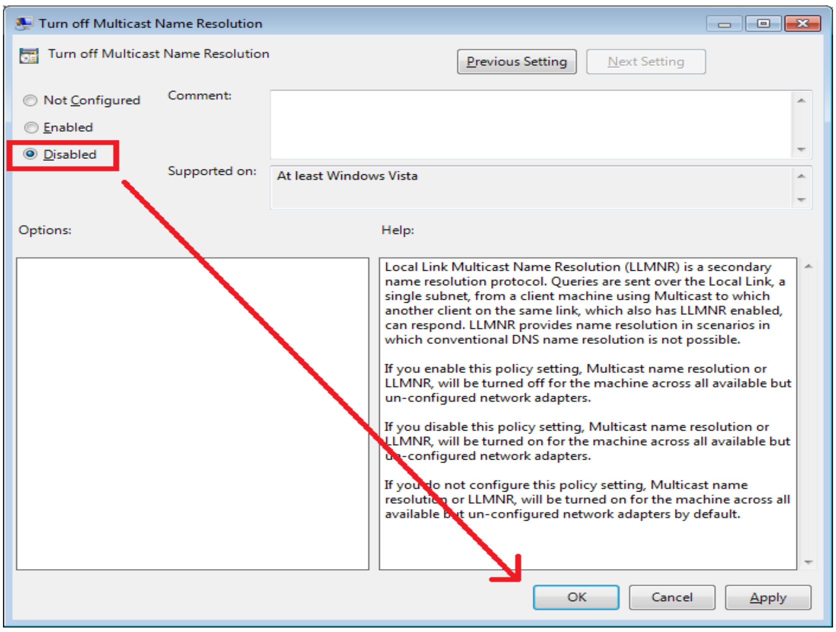
For this to work, we rely on a protocol called Link-Local Multicast Name Resolution (LLMNR) which needs to be enabled in your network. LLMNR resolves single label names (e.g. *COMPUTER1*), on the local subnet, when DNS devolution is unable to resolve the name. This is helpful in a scenario where DNS entries do not include hosts on the local subnet. In order to benefit from LLMNR, you need to enable *Network Discovery* on all nodes on the local subnet. LLMNR queries are sent to and received on port 5355. The IPv4 link- scope multicast address that a given responder listens to, and to which a sender sends queries, is 224.0.0.252. The IPv6 link-scope multicast address a given responder listens to, and to which a sender sends all queries, is FF02:0:0:0:0:0:1:3.

If Network Discovery is not enabled on a client (Computer), it will still send out an LLMNR request unless it has been disabled via group policy, however a host (Airtame device) will not respond to the LLMNR request if *Network Discovery* is not enabled.

This is how to Enable LLMNR with Active Directory GPO:

1. Log in to the Domain Controller of the domain you want to enforce this configuration.
2. Open start by hitting the windows key.
3. Type gpmc.msc.
4. A new window opens up. On the left panel navigate: Forest->Domains->YourDomain.
5. Right click on "Default Domain Policy".
6. Click on Edit.
7. A new window opens up, it's the "Group Policy Management Editor".
8. Navigate "Computer Configuration"->Policies->"Administrative Templates"->Network->"DNS Client".
9. On the Right panel look for the option "Turn off multicast name resolution".





Native streaming protocols

AirPlay

The Airtame AirPlay integration consists of a software component that will run on the Airtame device, and it will make the Airtame device appear in the local network as an Apple TV, advertising the name that was set in the Airtame device settings. When using AirPlay, the user will not use any Airtame software on the laptop/iPhone/iPad side. This means, Airtame cannot control any behavior you might see on the sending side (iPhone/iPad).

To use Airplay in your enterprise network, multicast routing should be enabled globally on the network appliances handling the traffic and IGMP/PIM should be configured on the VLAN interfaces participating in the passing of multicast messages. Airplay relies on SSDP and mDNS to allow end users to discover the Airtame devices in the network.

AIRPLAY			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
554	TCP/UDP	Both	Real Time Streaming Protocol
1900	UDP	Both	SSDP Discovery
3689	TCP	Both	Digital Audio Access Protocol
5350+5351	UDP	Both	NAT Port Mapping Announcements
5353	UDP	Both	mDNS discovery
7000...	TCP	Both	Server port
7100...	TCP	Both	Data port
2001...	UDP	Both	Timing port
29053...	TCP	Both	Event port
61875...	UDP	Both	Audio Data port

Setup option for networks where AirPlay is not available

Some networks do not support AirPlay or some networks do not allow mobile devices on it. In this case it is possible to set a static IP on the WiFi connection to Airtame which keeps the connection directly to Airtame's Access Point but allows internet to go through the LTE:

1. You would need to enable one of Airtames AP's for direct connection. You can see how to set it up here: How to configure Airtames Access Points
2. Follow this guide from Apple on how to force iOS devices to use LTE network while maintaining connection to AirPlay device: How to force iOS to use LTE to access internet with WiFi AirPlay enabled

Considerations for Guest/AirPlay across VLANS

If you would like to permit your guests to use AirPlay to send content to the Airtame from their iOS devices, one needs to consider the type of deployment that is being implemented. The section above titled **Collaboration for Users in Different Network Segments** provides information on how to give both internal users and external/guest users access to the Airtame without bridging your network or compromising your organization's security policy.

The auto-discovery features on the Airtame utilize the same multicast protocols as AirPlay. If auto discovery is operational on the Airtame, AirPlay should work as well.

If you wish to use AirPlay, be sure that considerations have been made for configuring the network and be sure to toggle the Airplay button within the device settings.

You can learn more about AirPlay in our Present to Airtame with AirPlay article.

Google Cast

Google Cast is a native streaming protocol that allows the user to fully mirror their screen from their Android devices, as well as Chrome OS, and when casting via the Chrome browser from any operating system, without the need for the Airtame app.

Google Cast mirroring streams are encoded in H.264 or VP8 formats and transmitted as UDP packets.

Google Cast is using the following ports:

GOOGLE CAST			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
8008-8019	TCP	Both	Google Cast listener ports
1900	UDP	Both	SSDP discovery
7236	TCP	Both	Content Casting
32768-61000	TCP/UDP	Both	Ephemeral Ports for Return Traffic

Google Cast relies on Bonjour mDNS for discovery and uses the following Bonjour services: _googlecast._tcp

Learn more about how to enable and use Google Cast in our Present to Airtame with Google Cast article.

Miracast

Miracast native streaming protocol lets you use the screen sharing functionality that's already built into Windows and Android devices, eliminating the need to install the Airtame desktop app.

Miracast also lets Windows users extend their desktop and use Airtame as an additional display. This is ideal for many presentation scenarios in which someone wants to view their presenter notes privately while sharing a different screen to Airtame.

An additional benefit of Miracast is that it supports Touchback functionality on interactive whiteboards.

Airtame supports both Miracast P2P (Peer to Peer) and Miracast over Infrastructure.

Miracast P2P works the same way as far as the presenter is concerned, but the key difference is that it relies on the Airtame device's own access point (AP) being enabled. The benefit of this is that screen sharing can take place independently of the network, as the connection is direct from a presenter's PC to the Airtame's own access point.

Miracast over Infrastructure is a great option for those who want to let presenters use the built-in screen sharing functionality of their Windows devices, but do not want to have active access points on Airtame devices. The connection goes over the local network (LAN). Initial discovery is still done in a P2P (Peer to Peer) mode, but no APs need to be enabled.

MIRACAST OVER INFRASTRUCTURE			
PORT	TYPE	DIRECTION	SERVICE
7250	TCP	Both	Miracast Packets
5353	UDP	Both	mDNS discovery

Learn more about how to enable and use Miracast in our Present to Airtame with Miracast article.

One feature that is also available with Airtame is Touchback with Miracast. The benefit is that presenters can use the touchback functionality of their interactive displays when presenting via Miracast.

Airtame Application

Desktop app

Windows, MacOS, Linux and Chromebook all use the same Airtame app, with the same functionality and appearance.

- Click the "Share screen" button next to the device name in the app (or type in the IP address) to start streaming your whole screen or only a selected window.
- If you want to stream to multiple Airtame devices simultaneously, click "Start" next to several different devices within the app.
- Application preferences allow you to manually change settings that affect streaming (e.g. frames per second).
- The device settings (under the name of each Airtame), is specific to an individual device and contains the device's configuration (e.g. its background image, network settings).

Chromebook app does not allow for the initial setup of an Airtame device. Setup needs to be done with the app running on Windows or MacOS.

App deployment

The Airtame application can be downloaded from airtame.com/start:

- Regular Installer: This is a normal installer of the app. It requires admin rights.
- Windows Guest app: This is perfect for one-time users such as guests. It does not require neither installation nor admin rights. It opens with just a click.
- Windows Mass deployment installer (MSI): This is a version of the app used to pre-configure and install the app on numerous company laptops at once.

Without the app - Airplay, Google Cast and Miracast

All these native streaming protocols enable you to stream to Airtame without having to download the Airtame app.
With Airtame, you can use Google Cast and Miracast to stream the full screen of your Android and Windows devices. For MacOS and iOS devices, you can use AirPlay.
One feature that is also available with Airtame is Touchback with Miracast. The benefit is that presenters can use the touchback functionality of their interactive displays when presenting via Miracast.

Mass deployment of the Airtame app

In some environments with dozens to hundreds of employees, it becomes mandatory to ease the software deployment processes.
To get the best experience out of Airtame during meetings or classes, it's preferred that computers already have the Airtame application installed on them.
The Airtame MSI has been created to silently pre-install the Airtame app on multiple organization's computers.

Software Deployment

There are a myriad of deployment systems on the market. From Windows CMD/PowerShell to more complex deployment systems. The architecture behind all of them is designed to run the deployment software in a central server with access to the rest of the computers on the network.
Each system may use different methods of connection and running the installation on the target machine.
The basic command looks like this:

msiexec /i "PATH TO MSI FILE" /quiet WRAPPED_ARGUMENTS="CONFIGURABLE OPTIONS"

The installation requires administrator credentials, make sure to run the command with such privileges.

An Airtame application that was installed via MSI will not auto-update itself. Updates need to be pushed via the deployment system. To get notified when updates are released, please sign up to product updates.

Wrapped Arguments (Configurable options)

The Airtame MSI supports two configurable options which affect the behavior of the Airtame app. The desktop icon depends on the deployment software being used, said option does not come as a wrapped argument.

These options are:

- Autostart: If enabled, the Airtame application will automatically start when the computer is booted up.

- Streaming Notification Window: If enabled, whenever a Screen Mirroring/Window Sharing session has started the following small widget appears on the screen as a reminder of the ongoing stream.

The Airtame app can be installed with any of these options either enabled or disabled.

The syntax of the WRAPPED_ARGUMENTS sections changes depending on the software used. We tested both Windows' CMD and PowerShell, and the differences are as follows:

For CMD:
msiexec /i "airtame-application-3.4.0-setup.msi" /quiet
WRAPPED_ARGUMENTS="/autostart=false /streaming_notification=true"

For PowerShell:
msiexec.exe /i "airtame-application-3.4.0-setup.msi" /quiet
WRAPPED_ARGUMENTS='"/autostart=false /streaming_notification=true"'

Notice the single quotation marks employed in the PowerShell syntax surrounding the configurable options. Single quotation marks and double quotation marks are treated differently by PowerShell.

v3.4.0 is used as an example. Version number should be used corresponding to MSI installer you have.

Example 1: PDQ Deploy

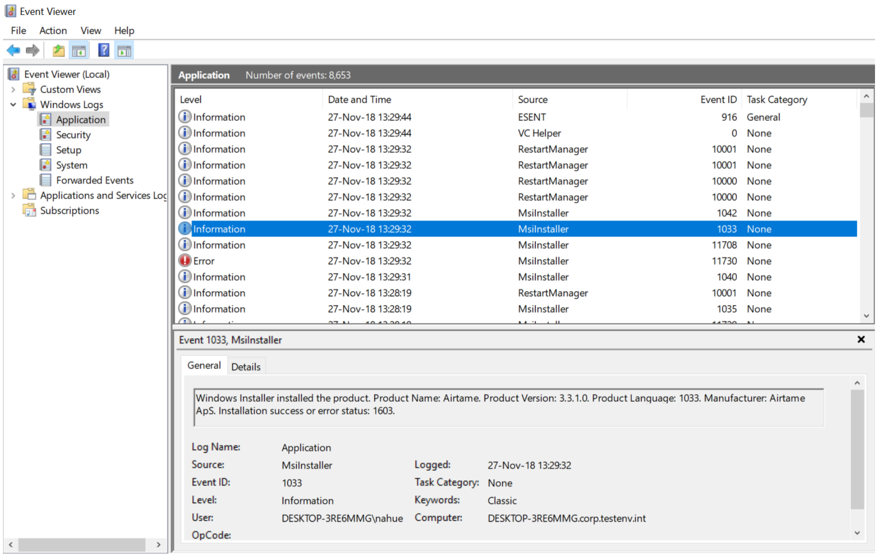
1. Click on "New Package".
2. Name the package, the example is "Airtame App".
3. Click on "Step".
4. Select MSI file to be used.
5. Write the Wrapped Arguments parameters.
6. The package is ready for deployment.

Once installed, you can use the following command to reset these two default MSI settings (autostart=false/streaming_notifications=true) in case the app had already been installed on some computers or if, in the future, you would want to override the changes user has made to these two commands: airtame-application.exe —reset-default

Troubleshooting application mass deployment

1. Check the syntax of the WRAPPED_ARGUMENTS section e.g. single vs. double quotation marks. Please reference the examples for CMD and PowerShell above.

2. Check the deployment software's own log files.
3. Analyze target Windows PC Eventlog. If the MSI installation command reached the destination you'll see an MsiInstaller Eventlog entry, analyze it for error/success codes:



Airtame updates

Airtame device downloads updates from repos.airtame.com. We can not provide specific IP addresses as they are changing based on location and timezone and updates can come from any global mirror. Updates happen over HTTP (TCP port 80) so you need to make sure they are available on your network. Below you'll find a technical explanation about how the update process works.

Timer

1. First of all there are 2 timers, so our script is called 15 minutes after device boot, and every one hour after device boot
2. If auto-update is available, an update will start. If not — it will not

Update script

1. Every time update polls update server with GET request in this format: **repos.airtame.com/checkfw.php?mac=38:4b:76:01:61:16&version=v3.0.1&chann el=ga**

Clarifications:

MAC: MAC address of current Airtame device
Version: current version of Airtame device
Channel: current update channel selected on Airtame device/

If there is a newer version on the current channel, the server will return a special answer, and the device will update.

How an update mechanism works:

1. Get rootfs MD5 from the update server — it is a small file with MD5 hash.
2. Flash rootfs of another partition which we will use to download and update image.
3. Download and unzip big rootfs image file to the other partition (in-memory operation).
4. Compare MD5 of new rootfs with expected MD5 value (because we need to verify that we won't brick the device).
5. Swap old and newer version partitions.
6. Try to download the WiFi calibration file (not accessible for some device models).
7. Reboot the device.

Internal update server

When Airtame does not have direct access to an update server, it can not update its firmware via the traditional OTA method. We always recommend using the latest firmware, therefore new releases are very important. For companies who do not have the possibility to connect Airtame to a network with internet connection for accessing the update server - here are the steps for how to setup a local update server on your network.

Requirements

- Running web server (Apache/IIS/SimpleHTTPServer/any other web server).
- The Airtame's device settings cannot be password protected. You can remove the password, update the Airtames, and then re-enable password protection.

Steps:

1. Create a folder where you will later put the update files.
2. Go to http://repos-cdn.airtame.com/firmware/DG2/ga/ (for Airtame 2) and http://repos-cdn.airtame.com/firmware/DG1/ga/ (for Airtame 1) and download the following files (can be done manually from another network):
    a. **For latest version:**
    latest.rootfs.md5
    latest.rootfs.size
    Latest.rootfs.gz
    b. **For any other version:**
    airtame-fw-v***3.3.1***.rootfs.md5
    airtame-fw-v***3.3.1***.rootfs.size
    Airtame-fw-v**3.3.1**.rootfs.gz

    3.3.1 *is an example here*

3. Run your web server, so it will make your folder publicly available via HTTP.
4. Send the following command to your device:
    curl -X POST -d '{"url": "address_of_your_local_webserver/path/to/update_folder/{your_version}"}' http://device_ip_address/admin/device/update

Real examples:
curl -X POST -d '{"url": "http://192.168.1.6:8000/DG2_update_folder_331/airtame-fw-v3.3.1"}' http://192.168.1.13/admin/device/update
curl -X POST -d '{"url": "http://192.168.1.6:8000/DG2_update_folder_latest/latest"}' http://192.168.1.13/admin/device/update

Additional options

Airtame devices can also be updated or downgraded by pointing to files placed on an internal server.

To rollback to a previous firmware version, please follow these instructions:

1. Access the Airtame device setting
2. Scroll down & click on the blue text "Show Advanced Settings"
3. Scroll down to the "Update channel" option
4. Click quickly at least 5 times over the gray "Update channel" text
5. Click on the dropdown menu and select the "Custom" option
6. A new text box will appear, and please paste the following link: (INSERT RELEVANT LINK DEPENDING ON Airtame 1 OR Airtame 2 AND VERSION)
   For example:
   "http://repos.airtame.com/firmware/DG2/ga/airtame-fw-v3.5.1"

If you would like to download files to the internal server and update devices this way - you would need to use an internal link.

Airtame Cloud

Digital Signage is the use of networked electronic displays that are centrally managed and individually addressable for the display of text, animated or video messages for advertising, information, entertainment and merchandising to targeted audiences.

By using Airtame Cloud, you can manage all of your Airtames throughout your network from one centralized management system. From Airtame Cloud, you can connect your Airtame to an assortment of different applications and services such as Google Slides, Dropbox and OneDrive. Read our guide on Airtame Cloud for more information.

Getting started

- Check on the status for each device (online, offline, streaming).
- View Network connection status (SSID or Ethernet) and RSSI.
- Check the firmware version running on your Airtame.
- Create groups of devices. Expand, collapse, and rearrange the groups.
- Select the orientation of your screen to either landscape or portrait mode.
- Get a visual overview of your Airtame status and what content they are displaying on. their screen (only for digital signage and not if it's being streamed).
- Use the integrated applications including Google Slides, Dropbox, Trello and more.
- Perform a Reboot or Update, remotely.
- Manage all your Airtame settings and perform bulk changes.
- Enable Google Cast, Miracast and Airplay functionalities.

Get started with Airtame Cloud.

Network requirements

The following requirements are needed for Airtame Cloud to work with your Airtame:

1. Your Airtame must have internet access. Port: 443
2. Your Airtame must be able to synchronize their time with either your NTP server or an external NTP server. Port: 123
3. Your network must allow communication with servers in Germany since we host Airtame.cloud on AWS in Germany.

Lite and Plus

Airtame Cloud has 2 different subscription plans: Airtame Cloud Lite and Airtame Cloud Plus.Here is an overview of which features go into these plans:

Lite (Free for all devices):

- Will be able to perform software updates

- Will be able to perform firmware updates
- Global device management
- Have an unlimited number of devices
- Have an unlimited number of users
- Set the screen orientation
- Allowed to allocate user roles and access delegation
- Show branded image and custom background (via Airtame device's settings)
- Show a public website URL (via Airtame device's settings)

Plus (Paid, includes everything in Lite and the following):
- Present a welcome screen with meeting room scheduling
- See real-time overview of your screens
- Automate screens to turn on/off according to office hours
- See meeting room overview
- Schedule imagery and videos to play on loop
- App Integrations with services including Google Calendar, Google slide, Outlook Calendar, Dropbox, Microsoft OneDrive and more

Further information: Airtame Cloud - FAQs & Manage Screens Devices

Prerequisites for Airtame Cloud

Connecting your Airtames to Airtame Cloud requires the following:

1. **A connection to the Internet**

   Airtame will need access to the internet in order to be managed by Airtame Cloud. This means that TCP ports 80/443 must be open from the Airtame VLAN to the internet.

   If your organization is using a web proxy server and/or a firewall, we advise to whitelist the subnet where you've placed your Airtames.

2. **A timing source**

   In order to successfully connect to Airtame Cloud, the Airtame needs to receive the correct time. If your Airtames are in your internal network, you can enable DHCP option 042 and point this to the IP address of your NTP server.

   If you would prefer to use an external NTP server, you'll need to make sure that the Airtame subnet will be able to send UDP port 123 through the firewall so that the Airtames receives correct timing.

Security Considerations for Digital Signage via Airtame cloud

If your organization wishes to use monitors for digital signage and control them via Airtame Cloud, one needs to consider how accessible these digital signage screens are to other users in your network. If the signs are easily accessible, you may run the risk of someone changing what's displayed on the screen. To mitigate this risk, we recommend the following:

1. Create a separate VLAN for your digital signage Airtames.

2. Create an access list (ACL) to only allow traffic to pass into the digital signage VLAN from an approved source to prevent unauthorized access.

3. Lock down access to Airtame Cloud to those who have received approval from the product owner/management and provide the appropriate level of access for new user accounts within Airtame Cloud. Read more about Cloud user roles here.

Display calibration

Image quality is defined by the PC and TV resolution, PC and network performance, and display calibration.

- Image quality depends on screen calibration.
- Overscan causes the picture to be cropped on all edges (i.e. not to fit into screen).
- The picture shown on the TV is the resolution of your computer screen scaled to your TV screen's resolution.
- The aspect ratio of a TV is usually 16:9, and some computers, ex. Mac, use 16:10 which will be fitted. This may result in black bars on the side of the image on the TV screen. To avoid this, change the computer's resolution to 16:9.

Calibrate

To achieve the best image quality, start streaming to the screen and open an Excel style spreadsheet. This includes different gray scales in the rows/columns and the menu bar, which serve as guidelines for the adjustments. Then follow these steps:

1. Find the best looking standard mode (can be named Natural) or reset all adjustments.
2. Reduce contrast until all the lines in the spreadsheet are visible (often around 70-80% of max value).
3. Reduce sharpen until the text looks good and is easy to read (Often 0-20% of maximum).

A setting called "Black levels" in advanced settings can be useful for getting the light gray tones to look good.
Disabling 100 Hz and other image processing settings will remove latency caused by the TV. This will make Airtame appear more responsive. The downside will be that, when playing video, it can look less fluent because the TV doesn't process extra frames.

Resolution

The resolution shown on the TV is the resolution of your computer screen scaled to the resolution of your TV screen. This means that if your computer has a 720p monitor, the image streamed to your TV will also be 720p even though the TV is 1080p.

CEC

CEC stands for Consumer Electronics Control and is a feature of HDMI that allows devices to control each other. A CEC-enabled device such as Airtame can automatically power a CEC-enabled screen on and off. You can learn more about this feature in the Airtame and CEC article.

Audio and video streaming

Latency and Network Consumption

- Sharing with sound OFF: 400 - 800 milliseconds latency (1-5Mbit/s Bandwidth)
- Sharing with sound ON: 1-second set latency (2-7Mbit/s Bandwidth)
- Sharing with highest quality settings in manual mode: Depends on the user PC and network (up to 13Mbit/s Bandwidth)

Streaming Modes

1. Default - Instant Mode

This is the default streaming mode for basic screen sharing.

- Priority: Minimum delay between the computer screen and Airtame's screen.
- When to use: Everything that doesn't require audio, such as when showing work being done, presentations, images, and documents.
- Stream parameters: Quality: 2/5 (Medium), 20fps
- Disadvantages: Does not recover lost frames, does not transmit audio, slightly lower picture quality.

2. Video Mode - Share screen with Audio

This mode is enabled by clicking the audio button in the app.

- Priority: Better video quality, fluid playback, and audio-video synchronization.
- When to use: Streaming content with sound (adds 1s buffer).
- Stream parameters: Quality: 3/5 (Higher), FPS: 24.
- Disadvantages: Set buffer of 1 second, the TV picture will be 1 second behind your computer's screen.

3. Manual Mode

You can enable this mode by going to the app Preferences →Toggle On Manual mode.

- Priority: Flexibility resulting in maximum quality (5/5).
- When to use: When higher quality streaming is needed and both the network and the computer allow it.
- Streaming parameters: Manually adjustable.
- Disadvantages: Highly dependent on computer performance and network stability. Can give worse results than default modes.

Airtame's screen background

Display personalized content

- You can change the background shown when the device isn't being streamed to by uploading a custom image or pasting in a web URL.
- You can change the guide placement: Guide, Guide Left, Minimal or none.
- Change the text shown on the screen.
- Use the integrated applications via Airtame Cloud - this will let you turn your screens into useful information displays or just make your office more inspiring.

Images

Appropriate for branding, showing stock images or company logos. The image should have a resolution of 1920x1080 pixels and cannot exceed 2MB.

Websites

Show company KPI metrics, meeting room agendas, slideshows, presentations, and much more.
Current limitations:

- Video playback and high demanding graphics cannot be displayed.
- Java, Flash, Silverlight, Flexbox and WebGL are not supported.
- Websites that require a login are not yet supported.

Screen layout and overlay text

Airtame's screen can have four different overlays depending on the purpose of the screen. You can fully edit "Guide left" and "Guide" by changing the text, color and transparency of the different overlay layouts.

- Guide left: By default, this layout will show a 3-step guide to help new users get streaming with Airtame.
- Guide: Here, you can see the same information as in Guide left in a more concise manner.
- Minimal: This layout will show the name of your Airtame device and its IP address.
- None: No layout is shown on the screen.

You can fully customize the text shown on the screen background. This is useful if you want to add your organization name, show relevant network information, have a tailored welcome message, etc.

Airtame & Security

Cyber security

- When you stream using Airtame, the stream itself never leaves your network, meaning that it will never be on the Internet. Additionally, Airtame does not collect or store any information regarding the content of the stream.
- The Airtame stream is not encrypted within your network but it is encrypted by your network. This means that no one out of the network can capture your stream, but if someone is already on the network, they could pose a threat if they take the time to snoop the network traffic and reverse engineer Airtame's protocol.
- Airtame supports two networks on one device. One is via Ethernet and the other via WiFi. Usually, the internal network would be connected via Ethernet and the guest network via WiFi. These two connections come via separate interfaces and therefore they cannot be bridged.
- Airtame's settings panel can be locked with a password from within the device's settings.
- When applying settings, HTTP encryption is used between the managing computer and the Airtame device being managed.

Airtame Cloud security

- Airtame Cloud sends information over the Internet. Extra security measures are taken to ensure no information is ever at risk, in addition to passwords and web URLs never being sent to the Cloud.
- The Airtame Cloud solution is hosted on Amazon Web Services. Airtame uses the AWS datacenter in Germany. User account information and passwords are stored on the server and are bcrypt-hashed for maximum security.
- All communication between a user's device, the cloud portal, and the Airtame devices are SSL encrypted (HTTPS). Communication between the airtame device and the cloud portal uses standard WebSocket communication established by the device.
- The information sent is restricted to non-sensitive information such as basic device settings, which means that no passwords are ever sent over the internet.
- Images are only sent to Cloud accounts that have enabled "Screen".
- You can disable sharing images of devices homescreen per-device.
- The images are stored in AWS for one minute then deleted permanently.

Physical security

- Airtame 2 has a Kensington lock slot to secure devices in classrooms or big meeting rooms. The magnetic wall mount keeps the device hidden behind the TV screen and makes it harder to physically remove.
- The non-removable adhesive allows Aircord and the magnetic wall mount to be permanently attached to the wall, thus making it harder or impossible to use it elsewhere.

Airtame domain queries to DNS servers

Airtame device
During normal operation it will always consult:
- data.airtame.com
- api.airserver.com
- repos.airtame.com

To sync its time, when no other NTP server is configured via DHCP:
- 0.fedora.pool.ntp.org
- 1.fedora.pool.ntp.org
- 2.fedora.pool.ntp.org
- 3.fedora.pool.ntp.org

When added to the cloud platform it will always consult:
- airtame.cloud

Airtame Application
During normal operation:
- data.airtame.com
- widget.intercom.io
- js.intercomcdn.com
- api-iam.intercom.io
- nexus-websocket-a.intercom.io
- nexus-websocket-b.intercom.io
- Static.intercomassets.com

Airtame consults different DNS addresses when Cloud apps are involved. Full and updated list can be found in our Overview: Airtame domain queries to DNS servers.

Actionable Checklist

Network Connectivity Checklist

- ❏ Configure a VLAN for your Airtames.

  For content sharing for internal and guest/external users
  If your use case is to allow wireless content sharing from both internal and guest networks, we recommend creating this VLAN on your firewall.

  If this isn't possible, then we recommend creating this VLAN on your core network and placing access control lists (ACLs) on the core network to control the traffic between your Airtames, internal users and guests.

  For digital signage and/or internal use only
  If your use case is for digital signage and internal use only, you can create a VLAN that terminates on your core network or wherever your internal inter-VLAN routing occurs in your internal network

- ❏ Configure the DHCP scope for your Airtame VLAN.

  The Airtame will need to receive an IP address and possibly an NTP configuration from your DHCP server. Once the Airtame has requested and received its IP address from your DHCP server, create a DHCP reservation to bind the MAC address of the Airtame to the IP address that your DHCP server has offered the Airtame.

  NTP requirements based on deployment type
  If your Airtame is **off** your internal network, enable ***DHCP option 42*** to direct the Airtame to connect to the IP address of an external NTP server. This will require the Airtame VLAN to be permitted to send traffic to the internet on port UDP 123. Here you will find a list of reliable sources of time off of your internal network.

  If your Airtame is **on** your internal network, enable ***DHCP option 42*** to direct the Airtame to connect to the IP address of your internal NTP server. If you are in a Windows Domain, the NTP server is likely to be your domain controller.

- ❏ Tag the Airtame VLAN on the relevant trunk connections between your network appliances to ensure layer 2 connectivity between the Airtame device and its default gateway.
  After you have successfully tagged the Airtame VLAN on relevant trunk ports, your Airtame device should receive an IP address from your DHCP server and that address will be reflected on the "active leases" list on your DHCP server.

Preparing Your Network

- ❏ Static Routes

  In a deployment where your Airtames are placed in a VLAN that terminates on your firewall, you may need to create a static route on your core network to ensure layer 3 connectivity between your user VLANs on your core network and the Airtame VLAN on your firewall.

- ❏ Access Control Lists and Firewalls

  If you decide to terminate your Airtame VLAN on your core network, you may be required to secure inter-VLAN routing with access control lists (ACLs). If your Airtame VLAN terminates on your firewall, you'll need to configure the rulebase on your security appliance to allow traffic to pass through your network. Below is a list of required protocol and ports that will aid you in creating ACLs and firewall rules as you deploy your Airtame devices.

AIRTAME			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
8002	UDP	Both	Video + audio streaming
1986	TCP	Both	Mobile streaming
8080	TCP	Both	Device management+PIN code
80	TCP	To the Internet	Firmware & Software updates
1900+1901	UDP	Both	SSDP discovery
5353	UDP	Both	mDNS discovery
123	UDP	To the Internet	NTP
443	TCP	To the Internet	Airtame Cloud
AIRPLAY			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
554	TCP/UDP	Both	Real Time Streaming Protocol
1900	UDP	Both	SSDP Discovery
3689	TCP	Both	Digital Audio Access Protocol
5350+5351	UDP	Both	NAT Port Mapping Announcements
5353	UDP	Both	mDNS discovery
7000...	TCP	Both	Server port
7100...	TCP	Both	Data port
2001...	UDP	Both	Timing port
29053...	TCP	Both	Event port
61875...	UDP	Both	Audio Data port
GOOGLE CAST			
PORT	**TYPE**	**DIRECTION**	**SERVICE**
8008-8019	TCP	Both	Google Cast listener ports
1900	UDP	Both	SSDP discovery
7236	TCP	Both	Content Casting
32768-61000	TCP/UDP	Both	Ephemeral Ports for Return Traffic

Configuring Multicast

- ❏ Survey your network and determine the best way to route multicast traffic from your Airtame VLAN to the receivers of multicast traffic in other VLANs.

  Internet Group Management Protocol (IGMP) must be enabled globally on the appliances servicing the endpoints that will join the multicast group. Once you have enabled IGMP and multicast routing on your network appliances, you'll need to refer to your vendor documentation to verify the multicast features on your appliance. .

- ❏ Configure Protocol Independent Multicast (PIM) on the interfaces for the hosts that will join the multicast group.

  PIM is usually configured in "sparse mode" or "dense mode". If all of your VLANs are terminating on the same appliance, you'll want to use PIM in dense mode.

  If your VLANs are on two devices with a routed connection, you'll need to use PIM in sparse mode. In sparse mode, you will configure a Rendezvous Point (RP), which is the IP address of the appliance that does not have the Airtame VLAN. Configuring an RP tells the Airtame VLAN where to send multicast messages in order for your users to join the IGMP group.

  Auto-Discovery (SSDP, mDNS) and Airplay features are reliant on multicast to be correctly configured in order to function properly.

- ❏ Prepopulated List

  Some organizations do not allow multicast traffic on their networks, but would like to have a list of available Airtames to be displayed within the Airtame application. Here you will find the instructions to create a prepopulated list of Airtames for the Airtame application. This can be incredibly useful if your organization uses a central repository for approved applications.

Configuring Quality of Service (QoS)

- ❏ In order for the Airtame to properly display the content on a screen, it is imperative that the content you're sharing arrives on the screen in a very timely fashion. In order to prioritize the traffic you're sending to your Airtame, it might be necessary to mark this traffic to be prioritized.

- ❏ Speak to your network administrator about configuring QoS on your wireless controller and/or your core network.

- ❏ Streaming traffic to the Airtame that is originating from your user VLANs should be marked as "AF41"

Centralized Software Deployment

- ❏ The Airtame application can be deployed from a central software repository such as PDQ or System Center Configuration Manager (SCCM)
  You can read more about MSI and application deployment here.

- ❏ Speak to your System Administrator to determine how things like Group Policy, access rights and permissions can impact how the Airtame application is deployed throughout your organization.

Preparing Your Windows Domain for Internal Use

- ❏ Create a service account for your Airtame in Active Directory

  In a deployment where you wish to authenticate your Airtames against your Windows domain, you'll need to create a service account and set a password.

- ❏ Decide on which authentication method you would like to use

  Airtame supports EAP-MSCHAPv2 (PEAP) and EAP-TLS. For further instructions on configuring your certificate authority (CA), RADIUS server and one of these methods in your Windows domain, please review Authenticating your Airtame.

Internet Connectivity for your Airtames

- ❏ Ensure Airtame is ready to connect to the Internet.

  Airtame uses ports TCP 80 and TCP 443 in order to connect to Airtame Cloud and to connect to the Airtame repository to check for firmware updates. While it is possible to use your Airtame devices on a restricted network, allowing your Airtames to access the Internet is important in order to use online management solutions and to keep devices up to date with the latest firmware and security patches.

  If you are going to deploy Airtame on your internal network and you have a web proxy, web traffic (80/443) will be diverted by your layer 3 device to pass through the web proxy server before gaining access to the internet.

- ❏ At this time, the Airtame proxy support does ***not*** support Web Proxy Auto Discovery (WPAD) nor does it support sending user credentials for authentication.

If you wish to authenticate your Airtame web traffic against a proxy server, you will need to configure a client certificate for your Airtame.

In order to overcome these limitations, you have a couple of other options.

* Whitelist your Airtame subnet to allow HTTP/HTTPS traffic to the domains found listed here.

* Whitelist your Airtame subnet to pass through your web proxy and lock down the Airtame traffic in your firewall rule base to allow traffic from your Airtame subnet on TCP 80/443 to the domains listed here.

Troubleshooting Tips

Improving streaming

A common issue some people have with their Airtame is that their device does not receive a strong signal from their wireless access point. This article provides a number of tips and tricks to improve the signal strength of the network connection.
How to Test & Improve WiFi for Airtame

Capturing Traffic with Wireshark

While troubleshooting problems, capturing the traffic off of the network between the Airtame and your computer can provide a lot of insight into what could be creating problems.
How to capture network traffic via Wireshark

Log files from your network appliances

There are those times while troubleshooting where the log files of the Airtame do not provide sufficient information to determine what is causing the problem. While troubleshooting your Airtame, be sure to check the log files of your wireless system, firewall or core network as there could be insightful information in these log files. This will allow us to assist you more efficiently to isolate the issue and resolve it.

Downloading the log files from the Airtame device

If you find yourself troubleshooting your Airtame, we recommend writing into Airtame's Customer Success team with the log files of your device. The device logs provide us the best first glance into the state of your Airtame and allows us to find the next steps to resolve any issues.
How to download the log files of an Airtame device

Contact us

Questions, comments, or feedback?

- Contact us via live chat at airtame.com using the blue button in the bottom right corner for general questions, be sure to include the Airtame device log files if you have any technical issues
- Contact us via email at support@airtame.com
- Contact us via our website by submitting a technical request using the form