# **AircastDB Server**

A networked AircastDB setup involves two types of servers:

- An SQL server (PostgreSQL, MSSQL, MySQL) to hold the metadata for the audio files and scheduling information (library, playlists)
- One or more network drives where the actual audio files are located

This works very well for situations where all computers are within the same LAN and can access both the SQL server and the network shares.

Accessing the AircastDB from outside the LAN, i.e. from the Internet, is very difficult though. In particular, access to the network shares is almost impossible from outside a NAT router without setting up a VPN.

This is where AircastDB Server comes into play. It encapsulates the access to the SQL server and the audio files through a single TCP connection that can be shared through any NAT-enabled router.

# How it works

AircastDB Server is built into Aircast.exe but runs as a standalone process. It creates a HTTP/HTTPS server (on one or two TCP ports) that listens for incoming requests from clients. The TCP ports can easily be forwarded on your NAT router so that road-warrior type clients can connect from anywhere on the Internet.

The HTTP server is not intended for use with a web browser, but instead, the client computer must have a compatible copy of Aircast installed, and set up a "AircastDB (Internet Client)" connection accordingly. Thereafter, the client user can run the AircastDB application to connect to the AircastDB server and work with the database as usual.

Most functions of AircastDB can be used with such a AircastDB Server connection, including:

- Library editing
- Playlist editing
- Scheduling
- Pre-listening and on-air playback of audio files
- File upload
- Voice tracking

A couple of things are not available when connecting through AircastDB Server:

- Storage synchronization (needs direct access to the storage network share)
- Database cloning (needs direct access to the SQL server)

On the client side, you can not only use the AircastDB application to work with the database, but you can also access the database from the Aircast playout application. When you load a playlist or drag a file from the DB library into the playout window, it will be downloaded from the AircastDB server, stored in a temporary file on your hard drive, and automatically deleted after playback. (Please keep in mind that there may be delays depending on the Internet connection speed between the server and the client.)

### **Use cases**

AircastDB server extends the range of your networked AircastDB intallation to outside your LAN.

#### **Remote studios**

If you have more than one studio location, and the remote studios cannot access the LAN of the primary location, AircastDB server can be used to connect those studios to the main audio and scheduling library. If you have a lot of accesses to audio files, it is recommended that you keep a sync'd copy of all audio files on a local server at each location (e.g. using rsync), and use AircastDB storage redirection to point the client to that copy. This will speed up access to the audio files significantly.

#### **Road-warrior DJs**

Some stations have DJs who do library editing and scheduling tasks from their home, or wherever they are. With AircastDB server, you can give these people access to the database from any location. It is even possible to do voice tracking from the remote location, and upload the files to the AircastDB server instantly.

#### Internet radio

In a typical internet radio scenario with multiple DJs who all work and broadcast from their home, AircastDB Server can be used to set up a common audio library that can be shared by all DJs. In particular, the owners of the radio can share a music library with their DJs giving them acccess to the actual files, or even giving them a copy of the entire library (both of which would be a legal issue in most countries).

# Setting up AircastDB Server

#### **Prerequisites**

To run AircastDB Server, you need the following:

- A working AircastDB connection. The database must be set up properly in the Aircast configuration. Ensure that everything is working fine when using the AircastDB app on the server computer.
- A compatible license. Currently AircastDB Server is included in Aircast Professional Studio and Aircast Professional Studio Plus. (Please contact us if you need the server as a standalone license.)

AircastDB Server is built into the main executable (Aircast.exe) and is part of any Aircast installation.

#### **Running AircastDB Server for the first time**

You will find the Database Server app in the Aircast group in the Windows Start Menu. Alternatively, if you're running the Zip distribution of Aircast, you can start AircastDB Server using the batch file DBServer.bat inside the program folder.

When you run the application, the main window will appear:

Seneral Users L	og	
Enable server		
Server Settings		
Mode:	HTTP only	
HTTP Port:	8840	
HTTPS Port:	9840	
SSL Certificate File	S	
Certificate:		
Key:		

Before you enable the server, you should check the TCP ports that are used for HTTP and HTTPS. The default ports are 8840 (HTTP) and 9840 (HTTPS). It may be necessary to open these ports in your firewall before client computers can access them. (If you use the Windows built-in firewall, you will be prompted to grant access when you click *Enable server* for the first time.)

### **Adding Users**

Before a client can connect to the server, you must add user to the account database. Go to the *Users* tab to see the current user list (should be empty at this point):

😌 mAirListDB Server - Master	
General Users Log	
🕀 Add 🔀 Remove 🥒 Configure	
✓ tw	

Then click Add to add a new user:

eneral			
Authentication			
Username:	tw		
New Password:			Generate random
Description			
Permissions			
User Level:	Administrator	•	

The user must have a name and a password. You can either type a password or have Aircast generate a random password for you.

The available User Levels correspond to the security roles used by AircastDB:

- Read-only
- Studio (Read-only + write access to playlist history table)
- DJ (Studio + create/edit playlists)
- Folder Manager (DJ + move items between folders in Library)
- Manager (Folder Manager + full Library editing)
- Administrator (Manager + full configuration rights)

#### **Using HTTPS/SSL**

AircastDB Server supports SSL encrypted connections over HTTPS. We recommend to enable the HTTPS server and only use encrypted connections when accessing the server from the Internet. The HTTPS server runs on a different port (default: 9840) than the unencrypted HTTP server.

AircastDB Server needs a set of SSL certificate files to work:

- 1. A certificate file (the public part of the certificate)
- 2. A key file (the secret part of the certificate)
- 3. A root certificate (the certificate of the authority that issued our certificate)

You can either obtain a "real", paid certificate from a commercial certification authority (CA), or you can create a free self-signed certificate. See below for instructions on how to create a self-signed certificate with SSL Buddy. The client side of Aircast does not verify the certificate chain currently, so a self-signed certificate will work fine as long as you only use Aircast on the client side.

All certificates must be in PEM format. The file extension depends on the software that was used to create the certificate and key: \*.pem, \*.cer, \*.key, ...

#### Self-signed certificate with SSL Buddy

SSL Buddy is a Windows tool that lets you easily create self-signed certificates. You can download it here: http://www.atozed.com/intraweb/blog/20100413.EN.aspx

Edit 2015-03-31: Original download link for SSL Buddy seems to be dead at the moment - here's an alternative link: http://download.Aircast.com/other/sslbuddysetup.exe

After the installation, run SSL Buddy and follow these steps to create a certificate for your AircastDB server. (See screenshots below for a visual walkthrough.)

- 1. Run SSLBuddy, select Generate and self-sign a certificate, then click Start.
- 2. A wizard will appear, click Next.
- 3. Select 1024 or 2048 bit key size, and enter your e-mail address, then click Next.
- 4. Enter you country, state and city, then click Next.
- 5. Enter the domain name this should match the public IP or FQDN hostname under which the clients will access the server later. Also enter your business name (or your personal name) and the directory in which the key and certificate should be saved. Then click *Next*.
- 6. A message will appear saying that the certificate has been created. You will find the certificate (domainname.cer) and the key file (domainname.key) in the output directory you specified.

usary   usary   ut aready have a cefficiate and would like to:   merate a cefficiate sequent to and to a cefficiate withority such as twrision   top have a cefficiate sequent to and to a cefficiate withority such as twrision   top have a cefficiate sequent to and to a cefficiate withority such as twrision   top have a cefficiate sequent to and to a cefficiate withority such as twrision   top have a cefficiate sequent to and to a cefficiate withority such as twrision   top have a cefficiate sequent to and to a cefficiate withority such as twrision   top have a cefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate for instalation into a web server   spore and Sciefficiate instalation into a web server   into the administrative email address:   into gemanitist com   spore into the email address:   into gemanitist com   spore into the instalation into a web server   inter the ing abusineses name:   maintist Groubil<		Generate and Self Sign
<pre>ct deads have a certificate and would like to: merce a certificate Request to send to a certificate withoutly such as Version encered a certificate Request to a certificate withoutly such as Version as have a certificate and would like to: acad a Trainel Root Certificate for installation into a web server. space an SBL certificate for installation into a web server. space an SBL certificate for installation into a web server. space an SBL certificate for installation into a web server. space an SBL certificate for installation into a web server. space an SBL certificate in certificate in a dispense space an SBL certificate in certificate in a dispense space an SBL certificate in certificate in a server. space and SBL certificate in certificate in a server. State The bit state or your key pair. (1024 recommended)</pre>	Buddy	This wizard will generate a self-signed certificate.
A self signed certificate is useful for internal SSL encryption of orgenerating a test is useful for internal SSL encryption of orgenerating a test is useful for internal SSL encryption of orgenerating a test is out encryption of orgenerating a test sorre certificate. As self-signed certificate is not usually accepted as a valid server a SSL certificate inclusion is an indynexifies server page an SSL certificate inclusion is an indynexifies server ann how is including inclusion inclusion is an indynexifies server page an SSL certificate inclusion is an indynexifies server ann how is including inclusion inclusion inclusion inclusion inclusion inclusion inclusion page an SSL certificate inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion inclusion in	not already have a certificate and would like to:	
Interate and set sign a certificate. Into a certificate is not subset to a web server: Into a most set certificate is not subset as a valid server certif	enerate a Certificate Request to send to a certificate authority such as Verisign.	A self signed certificate is useful for internal SSL
high have a constrate and would live to:   that a "made divertificate and would live to:   that a "made divertificate is in hot generated by a fuscion"   that a "made divertificate is in hot generated by a fuscion"   that a "made divertificate is in hot generated by a fuscion"   that a "made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a fuscion"   that a made divertificate is in hot generated by a match as a valid server certificate by any browsec.    Cancel Net  Select the hot is its in hot generated by a fuscion"  Select the hot is its in hot generated by a fuscion"  Select divertificate made by a fuscion"  Select dive	enerate and self-sign a certificate.	encryption or for generating a test server certificate. As
	adultation is confidente and would like for	Self-signed certificate is not generated by a trusted Certificate Authority it is not usually accented as a valid
represe an SBL certificate for insalitation in an indiperative serve: and how the install representation is an indiperative serve: and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the bit size of your Key pair: (1024 recommended) and the the supported key file: and th	aract a "Trusted Root Certificate" for installation into a web server.	server certificate by any browser.
reare and Self Sign Cenerate and Self Sign Ce	repare an SSL certificate for installation in an IIS server.	
ann how is install my SSL conflicate into a web server.  Reat  Cancel Next  Cancel	repare an SSL certificate for installation in an IndylintralWeb server.	
Stat Cose	earn how to install my SSL certificate into a web server.	Cancel Next
rate and Self Sign	Start Close	
rate and Self Sign  Select the bit size of your key pair: (1024 recommended)  1024 bit 512 bit 2048 bit Term: 365 days Enter the administrative email address: Info@mairlist.com  rate and Self Sign  Ret >   Generate and Self Sign  Ret >  Generate and Self Sign  Previous Next   Generate and Self Sign  Vour Certificate Request has been generated.  Your Certificate may now be installed in a web server.  Inter the legal business name: Imairlist GmbH  Select a path for the exported key file: C:tempi  Previous Next>   Certains  C:tempi  Previous Next>   Certains  C:tempi  Previous Next>  Certains  Common Certificate may now be installed in a web server.  Previous Next>  Previous Next> Previous N		
rrate and Self Sign  Select the bit size of your key pair: (1024 recommended)  1024 bit 2048 bit Term: 365 days  inter the administrative email address: Info@mairlist.com <pre> rrate and Self Sign </pre> rrate and Self Sign   Select your Country from the following list:   Generate and Self Sign   Center the full state or province:   Next   Ret the domain name to be secured:   10211.55.4   Inter the legal business name:   mairlist GmbH   Select a path for the exported key file:   C'templ   Previous   Next		
Select the bit size of your key pair: (1024 recommended)  1024 bit 512 bit 2048 bit Term: 365 days Enter the administrative email address: Info@mairlist.com  Info@mairlist.com Info@mairlist.co	erate and Self Sign	Generate and Self Sign
Select the bit size of your key pair: (1024 recommended) <ul> <li>1024 bit</li> <li>512 bit</li> <li>2048 bit</li> <li>Term: 365</li> <li>days</li> </ul> <li>Enter the administrative email address: <ul> <li>info@mairlist.com</li> </ul> </li> <li>enter the administrative email address: <ul> <li>Doftmund</li> </ul> </li> <li>erate and Self Sign  <ul> <li>erate and Self Sign</li> </ul> </li> <li>Generate and Self Sign  <ul> <li>Your Certificate Request has been generated.</li> <li>Your certificate may now be installed in a web server.</li> </ul> </li> <li>erate and for the exported key file: <ul> <li>C'tempi</li> <li>erate and Self Sign</li> </ul> </li>		
1024 bit ● 512 bit     2048 bit Term: 365 ● days Enter the administrative email address: info@mairlist.com <previous next=""> </previous>	Select the bit size of your key pair: (1024 recommended)	Select your Country from the following list:
1024 bit     0 1024 bit     0 512 bit     0 2048 bit     Term: 365		GERMANY
2048 bit Term: 365  days     Enter the administrative email address:     info@mairlist.com <pre>revious</pre>	1024 bit	Enter the full state or province:
	@ 2048 bit Term: 365 Avs	NDW
Enter the administrative email address: info@mairlist.com <pre></pre>		NEW
Info@mairlist.com	Enter the administrative email address:	Enter the city name:
erate and Self Sign          Enter the domain name to be secured:       Cenerate and Self Sign         10.211.55.4       Your Certificate Request has been generated.         Select a path for the exported key file:       Vour certificate may now be installed in a web server.         Select a path for the exported key file:       Image: Select a path for the exported key file:         Select a path for the exported key file:       Image: Select a path for the exported key file:         Select a path for the exported key file:       Image: Select a path for the exported key file:	info@mairlist.com	Dortmund
<pre></pre>		
Inter the domain name to be secured:     Image: Secured:       10.211.55.4     Image: Secured:       Inter the legal business name:     Image: Secured:       Image: Secured:     <	< Previous Next >	< Previous Next
Inter the domain name to be secured:     Image: Secured:       10.211.55.4     Image: Secured:       Inter the legal business name:     Image: Secured:       main rist GmbH     Image: Secured:       Select a path for the exported key file:     Image: Secured:       C:themply     Image: Secured:		(C
Inter the domain name to be secured:     Image: Control of the secured:       10.211.55.4     Image: Control of the secured:       Inter the legal business name:     Image: Control of the secured is a web server.       main rists GmbH     Image: Control of the secured key file:       C:themply     Image: Control of the secured key file:		
Enter the domain name to be secured:     Image: Control of the secured:       10.211.55.4     Image: Control of the secured:       Select a path for the exported key file:     Image: Control of the secured:       C:Itempl     Image: Control of the secured:       Image: Control of the secured:     Image: Control of the secured:		
Enter the domain name to be secured:     Image: Comparison of the secured:       10.211.55.4     Image: Comparison of the secured:       Select a path for the exported key file:     Image: Comparison of the secured:       C:Itempl     Image: Comparison of the secure of t		
Enter the domain name to be secured:     Image: Control of the exported legal business name:       Inter the legal business name:     Image: Control of the exported legal business name:       mainlist GmbH     Image: Control of the exported legal business name:       Select a path for the exported key file:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of the exported legal business name:       Image: Control of the exported legal business name:     Image: Control of t		
Enter the domain name to be secured: 10.211.55.4 Enter the legal business name: mainlist GmbH Select a path for the exported key file: C:Itemp\	erate and Self Sign	Generate and Self Sign
Inter the commain name to be secured.         10.211.55.4         Enter the legal business name:         mainfait GmbH         Select a path for the exported key file:         C:ltemp\                                 Select a path for the exported key file:         C:ltemp\	Enter the demain name to be apprend:	Vaux Cartificate Deputet has been security of
Tot_211.50.4       Enter the legal business name:       mainlist GmbH       Select a path for the exported key file:       C:ltempl	Enter the domain name to be secured:	Tour Certificate Request has been generated.
Enter the legal business name: mairlist GmbH Select a path for the exported key file: C:ltemp\ <previous. next=""></previous.>	10.211.00.4	Your certificate may now be installed in a web server.
mairlist GmbH Select a path for the exported key file: C:ltemp\ <previous. next=""></previous.>	Enter the legal business name:	
Select a path for the exported key file: C:tlemp\	mairlist GmbH	
C:temp\	Select a path for the exported key file:	
< Previous Next > C Previous Finis	C:ltemp\	
< Previous Next > CPrevious Finis		

You can now enter the certificate and key file in the AircastDB Server configuration. **Note: As this is a self-signed certificate, we use the certificate (\*.der) file as both the certificate and the root certificate.** 

General Users L	og
Enable server	
Server Settings	
Mode:	HTTP and HTTPS
HTTP Port:	8840
HTTPS Port:	9840
SSL Certificate File	'S
Certificate:	C:\temp\10.211.55.4.cer
Key:	C:\temp\10.211.55.4.key
	C:\temp\10.211.55.4.cer

## Setting up the AircastDB Client computer Connection setup

On the client computer, follow these steps to add a connection to the AircastDB Server:

- 1. Open Aircast Configuration.
- 2. Go to Databases.
- 3. Click Add, then select AircastDB (Internet Client).
- 4. In the dialog that appears, enter hostname, port, SSL or not, user and password.
- 5. Click OK to save.

mAirListDB (Internet Clien	t) Configuration
Connection Settings St	orage Redirection Advanced
Database Server	
Host name or IP:	10.211.55.4
Port:	9840 Use SSL/HTTPS
Default Login	
User:	tw
Password:	••••
	Test login
	OK Apply Cancel

Now you can run the AircastDB app, or use the database connection from within the playout window.

#### Audio file caching (optional)

Sometimes it's a good idea to keep a synchronized copy of all of your audio files on the client computer, especially when broadcasting from a location with a slow internet connection.

If you have such a synchronized copy of any audio storage folder, you can go to the *Storages* section of the database connection dialog, edit the particular storage and set the *Cache folder* to the folder where the synchronized copy is located:

Name:	Musik
Description:	
Default location:	M: Wusic
Redirect to:	
Backup location:	
Cache location:	

Now when Aircast needs an audio file for playback, it will first check if it's in the cache folder, and only if it's not, the file will be transferred via HTTP. This will save a lot of bandwith.