AircastDB Server

A networked AircastDB setup involves two types of servers:

- An SQL server (PostgreSQL, MSSQL) 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:

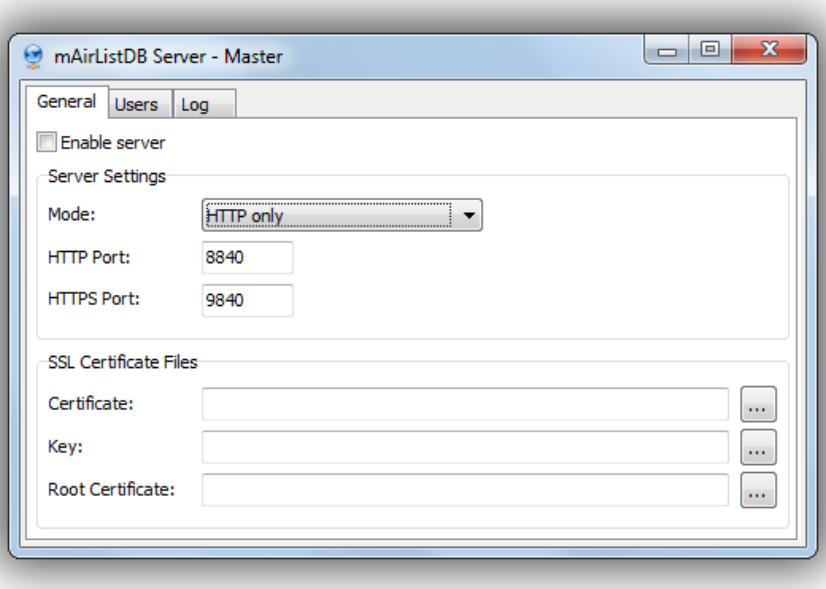
- A working AircastDB connection. The database must be set up properly in the Aircast configuration. Ensure that everything is working fine when using the AircastDB app on the server computer.
- A compatible license. Currently AircastDB Server is included in Aircast Professional Studio and Aircast Professional 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.

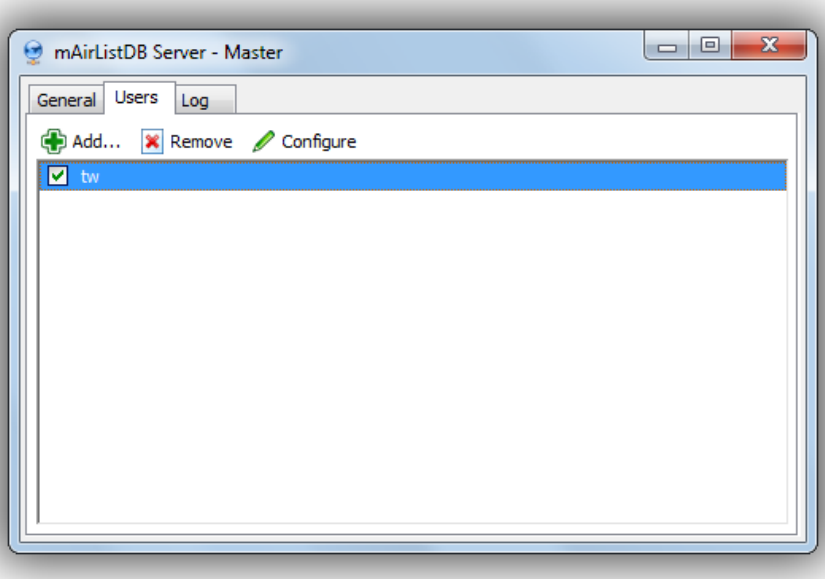
When you run the application, the main window will appear:



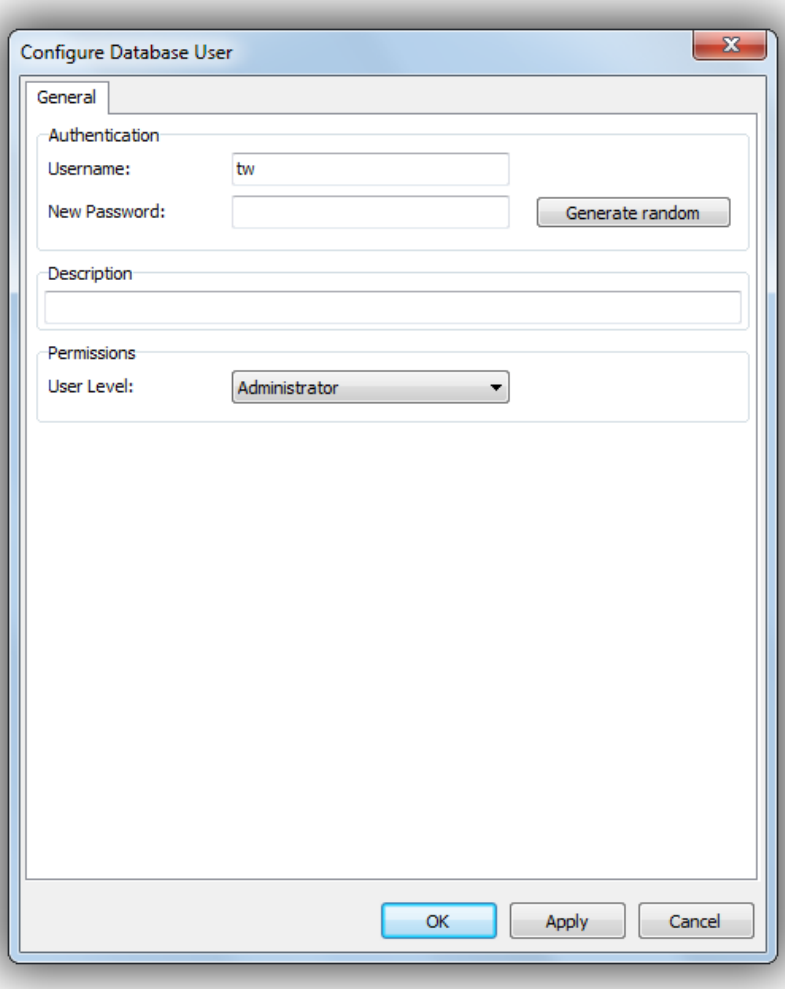
Before you enable the server, you should check the TCP ports that are used for HTTP and HTTPS. The default ports are 8840 (HTTP) and 9840 (HTTPS). It may be necessary to open these ports in your firewall before client computers can access them. (If you use the Windows built-in firewall, you will be prompted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



Then click *Add* to add a new user:



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, …

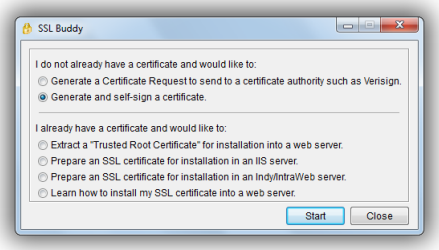
Self-signed certificate with SSL Buddy

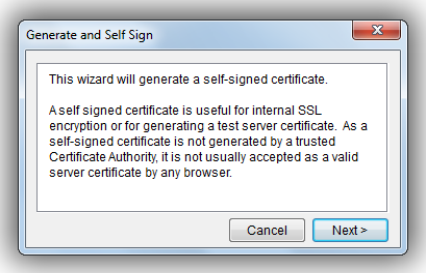
Verwijderd: SSL Buddy is a Windows tool that lets you easily create self-signed certificates. You can download it here: http://www.atozed.com/intraweb/blog/20100413.EN.aspx

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

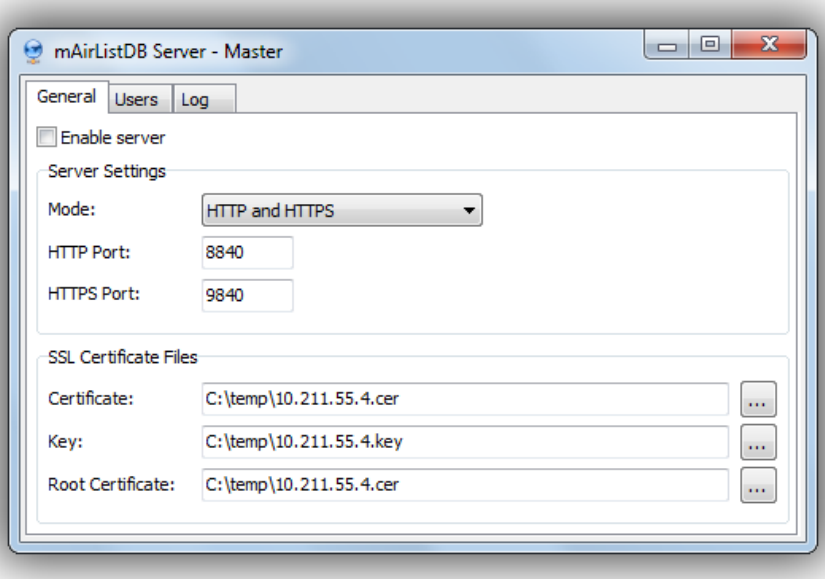
After the installation, run SSL Buddy and follow these steps to create a certificate for your AircastDB server. (See screenshots below for a visual walkthrough.)

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.





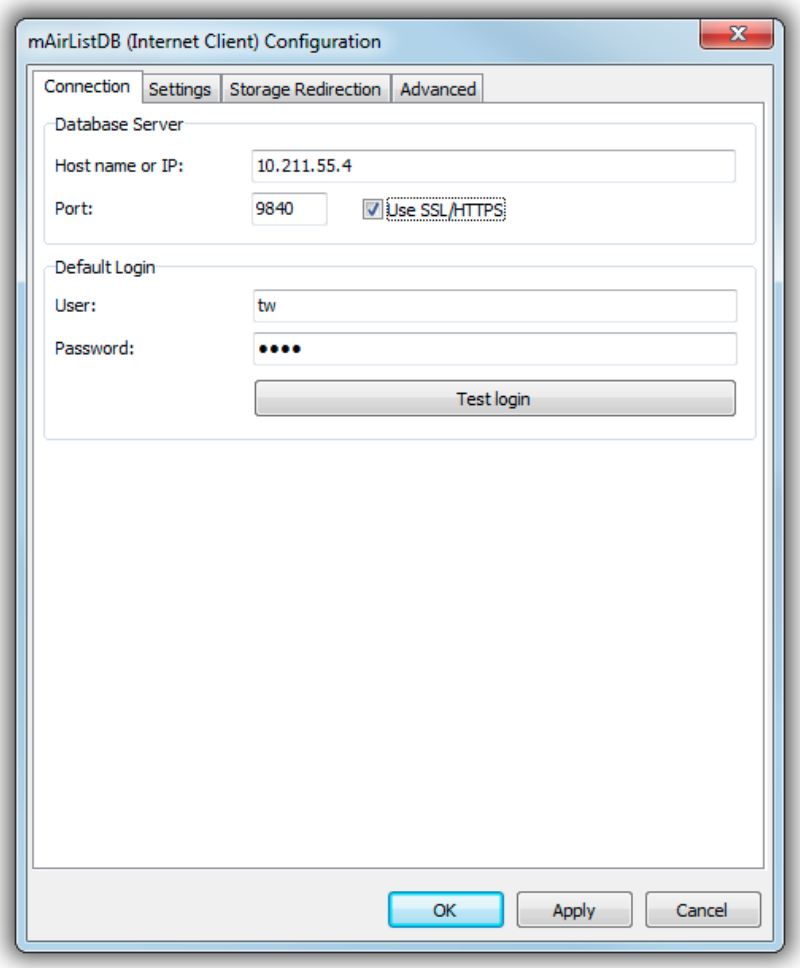
You can now enter the certificate and key file in the AircastDB Server configuration. **Note: As this is a self-signed certificate, we use the certificate (*.der) file as both the certificate and the root certificate.**



Setting up the AircastDB Client computer

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.



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