SENNHEISER

Sennheiser MobileConnect

Network Whitepaper

Version 1.0

Table of Contents

Introduction

Sennheiser MobileConnect is an Assistive Listening solution. The system streams audio content via WiFi live and in superior quality to any mobile device. Following the Bring-Your-Own-Device concept, it is an easy-to-use and intuitive Assistive Listening system. Costs and maintenance effort for operators are kept at a minimum. MobileConnect is optimized for use in higher education institutions.

The MobileConnect system consists of three components: the MobileConnect Station, the MobileConnect Manager and the MobileConnect App. The MobileConnect Station is integrated into the existing campus network and distributes the audio content via WiFi to the MobileConnect App on the user's personal smartphone. With the MobileConnect Manager, all MobileConnect Stations in the network can be conveniently administered and remotely managed from anywhere on the campus.

This whitepaper provides recommendations on how to integrate the MobileConnect system into your existing network. The preferred scenarios are the usage of a single network or two separate networks for streaming and control connections. All scenarios support NAT. The system can be integrated in Eduroam.
Select the scenario that fits your network setup best.

For more information, also see the **MobileConnect User Guide**.

In case of questions contact us at mc-support@sennheiser.com.

MobileConnect Manager and Docker considerations

The MobileConnect Manager is delivered in Docker containers. It has to be installed on an on-premise server / hardware.
Understanding the Docker configuration is a requirement in order to setup a custom Docker network installation and is not part of this documentation.

The Docker network will be available on all network interfaces the server might have.

- When using **a single network** (for more see Scenario 1 - One port solution), you can use the default Docker configuration and it will work out of the box.
- When using **two separate networks** (for more see Scenario 2 - Two port solution), for security considerations, it is important and strongly recommended, to use a **firewall**. Otherwise, both - streaming and administration will be accessible through both network interfaces.

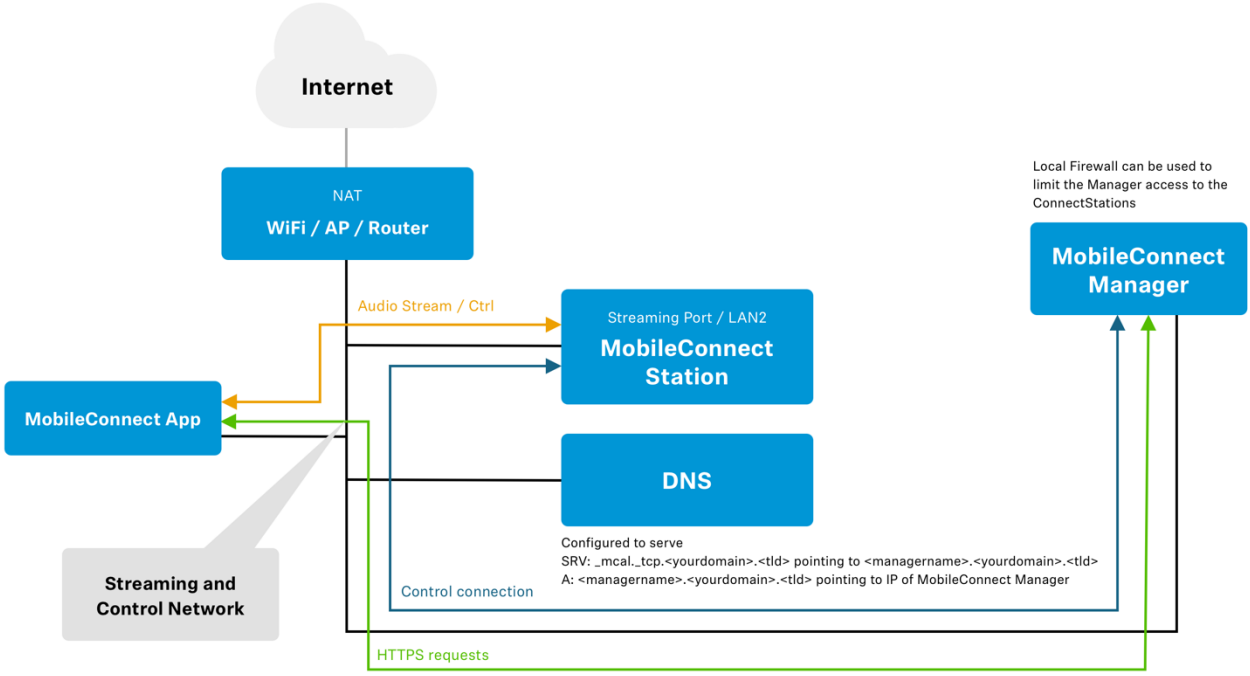
You will find some small firewall configuration scripts for the MobileConnect Manager host inside this document. However, you are encouraged to use your own firewall rules or any external firewall to adapt as best as possible to your specific network situation.

Feel free to send us feedback and information about your final implementation, so we can improve this document.

Scenarios for network integration

Scenario 1 - One port solution

In this scenario, all components (MobileConnect Station, MobileConnect Manager, MobileConnect App clients) are part of the same network. This makes for a very simple setup, light on configuration, as the only component needing active configuration is the SRV-record in the DNS-Server.



Advantages

- Easy to setup
- No additional hardware/software needed

Disadvantages

- The server with the MobileConnect Manager is in the same network as the clients
- The clients can access the MobileConnect Manager web interface if no additional protection measures are taken

Setup

- Connect the MobileConnect Manager to your network
- Connect the streaming port (**PoE/Stream** or **LAN2**) of the MobileConnect Station to your network
- Leave the control port (**Ctrl** or **LAN3**) of the MobileConnect Station unconnected
- Configure the services according to the DNS and DHCP configuration or the **MobileConnect User Guide** Quick Setup
- For increased security, please implement the additional configuration as it suits you.

Additional configuration

In this scenario the MobileConnect Manager should be additionally secured by using a firewall. The following example uses iptables to implement a simple firewall, limiting access to the MobileConnect Manager and reducing the attack surface. The example consists of several rulesets which are implemented as a set of bash-scripts. The bash-scripts expect a global configuration file to be located at */etc/mcm-iptables.conf*. An example file:

```
# executable for iptables
IPTABLES=/sbin/iptables

#executable for ip6tables
IP6TABLES=/sbin/ip6tables

# space separated list of Mac addresses of MobileConnect Stations
CS_MAC_LIST=""

# space separated list of IP addresses allowed to access the
web interface
ADMIN_IP_LIST=""
```

Please note that not every option is used in every ruleset.

The first ruleset disallows all access using IPv6, as the MobileConnect Manager is currently only supporting IPv4. Using this ruleset is recommended.

```
#!/bin/bash

source /etc/mcm-iptables.conf

IP6TABLES=${IP6TABLES:-/sbin/ip6tables}
PORTS_TO_CLOSE_TCP="80 433 8000"

for PORT in ${PORTS_TO_CLOSE_TCP}; do
    ${IP6TABLES} -I FORWARD -p tcp --dport ${PORT} -j REJECT
done
```

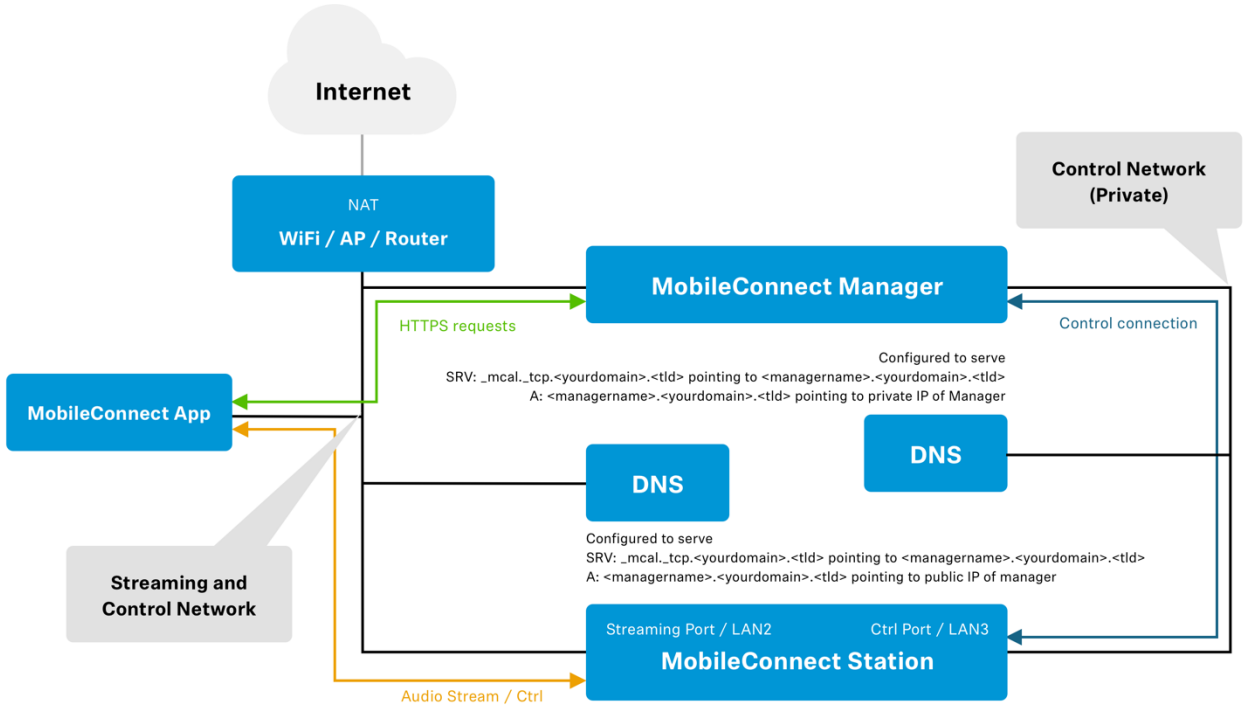
The second ruleset allows to add limitations for the ports used for accessing the MobileConnect Manager web interface and for the interfaces used by the MobileConnect Stations. This increases the maintenance overhead, as it needs all MAC addresses of the MobileConnect Stations and the IP addresses of the systems allowed access to the web interface to be added to the configuration file. Nonetheless this configuration is recommended in the one-port setup. As an alternative to this, have a look at the other network setup scenarios.

```
#!/bin/bash

source /etc/mcm-iptables.conf

IPTABLES=${IPTABLES:-/sbin/iptables}

# Create new chain for the filter for port 80
${IPTABLES} -N mcm-mcs-filter-list

# Create chain for allowed macs
${IPTABLES} -N mcm-mcs-accepted-macs

# Create chain for allowed ips
${IPTABLES} -N mcm-mcs-accepted-ips

# Have all traffic for port 80 go through the filter chain
${IPTABLES} -I FORWARD -p tcp --dport 80 -j mcm-mcs-filter-list
```

```
# Have the filter chain check the accepted macs
${IPTABLES} -A mcm-mcs-filter-list -j mcm-mcs-accepted-macs

# Have the filter chain check the accepted ips
${IPTABLES} -A mcm-mcs-filter-list -j mcm-mcs-accepted-ips

# Reject all other accesses to Port 80
${IPTABLES} -A mcm-mcs-filter-list -j REJECT

# Macs, intended for allowing access for the CS
if [ -n "${CS_MAC_LIST}" ]; then
    for MAC in ${CS_MAC_LIST}; do
        ${IPTABLES} -A mcm-mcs-accepted-macs -m mac --mac-source
${MAC} -j ACCEPT
    done
fi

# IPs, intended for allowing management access
if [ -n "${ADMIN_IP_LIST}" ]; then
    for IP in ${ADMIN_IP_LIST}; do
        ${IPTABLES} -A mcm-mcs-accepted-ips -s ${IP} -j ACCEPT
    done
fi
```

Scenario 2 - Two port solution

In this scenario there are two separate networks. One is used for the public devices, the other is used for control of the MobileConnect Station and access to the MobileConnect Manager web interface. This scenario employs a clear separation between streaming and control communication, allowing for a better confinement of the user-controlled mobile devices. To separate the networks, the MobileConnect Manager is equipped with two network interfaces, which are either in the streaming or in the control network. On the MobileConnect Stations the streaming and the control port are used to connect to the respective networks. In difference to Scenario 1, two DNS-Servers are used, which hand out either the public or the private MobileConnect Manager IP addresses.



Advantages

- By moving the control communication to a separate network, it is clearly separated from the uncontrollable mobile devices
- No need for a complex firewall-based limitation of who is allowed to access the MobileConnect Manager web interface or the MobileConnect Station's services

Disadvantages

- The solution needs two separate networks, which needs additional cabling
- Every network needs to have its own DNS server configured & maintained
- A minimal firewall is needed on the MobileConnect Manager to ensure the access limitation

Setup

- Connect the public interface of your MobileConnect Manager to your streaming network
- Connect the private interface of your MobileConnect Manager to your control network
- Connect the streaming port (PoE/Stream or LAN2) of the MobileConnect Station to your streaming network
- Connect the control ports (Ctrl or LAN3) of the MobileConnect Station to your control network
- Configure the services for the streaming network according to DNS and DHCP configuration, making sure to point the DNS-entry to the public interface of your MobileConnect Manager
- Configure the DNS service for the control network according to DNS and DHCP configuration, making sure to point the DNS-entry to the private interface of your MobileConnect Manager

- Limit the access for clients accessing the MobileConnect Manager from the streaming network to port 8000. The following example is using iptables:

```
# This blocks all tcp access except access to port 8000 for the
interface PUBLIC_INTERFACE.

iptables -I FORWARD -p tcp -i <PUBLIC_INTERFACE> ! --dport 8000 -j
REJECT


# example for an interface called eno1, executed in bash

iptables -I FORWARD -p tcp -i eno1 \! --dport 8000 -j REJECT
```

You can also add this iptables example in the following simple systemd-service.

```
[Unit]
Description=Limit the lister interface to port 8000 IP only
After=docker.service

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/sbin/iptables -I FORWARD -p tcp ! --dport 8000 -i %I -j
REJECT
ExecStop=/sbin/iptables -D FORWARD -p tcp ! --dport 8000 -i %I -j
REJECT

[Install]
WantedBy=multi-user.target
```

It will automatically limit the access at boot-time after docker has established its ruleset. It is dynamically configurable, just save it to */etc/systemd/system/limit_listerinterface@.service* and enable it for an interface with *systemctl enable limit_listerinterface@**<interfacename>**.service*.

DNS and DHCP configuration

Whether you use the one port or two port solution, you need to configure the following in each network:

DNS

The system needs a single SRV record of _mcal._tcp per network:

Service Name	TTL	Class	Type	Priority	Weight	Port	Target
_mcal._tcp.yourdomain.com	3600	IN	SRV	0	0	8000	*mc-manager .yourdomain.com*

- Replace “yourdomain.com" with your own top-level domain
- The hostname "mc-manager" can be replaced with any hostname you want to give to the MobileConnect Manager
- Use FQDN and not a direct IP address
- For Scenario 2, you need two DNS servers or different domains or subdomains.

DHCP

The following DHCP settings are required so that the MobileConnect Apps can discover the MobileConnect Manager:

- For Android → you *must* configure the “domain part" of the DHCP protocol, as Android ignores search domains.
- For iOS → the “domain part" can be used *or* if you have multiple search domains, it *must* be in the search domains.
- The MobileConnect station respects the domain part and the search domains.