This series of Access Points offers a wide range of features for a mid-range price. One of the outstanding features in its price class is the ability to use ARP sniffing to determine a client’s IP address even if it changes during a user session. Activating this feature fulfils the requirement for MAC to IP correlation from the confederation policy and obsoletes logging of DHCP leases.

The following steps are needed to set up eduroam on a Lancom L-54 or L-300 series access point. It describes the setup via the web interface and is current as of LCOS Version 8.0. The starting point of this tutorial is a factory-reset device, i.e. it is not configured at all and set up to its defaults.

**Initial provisioning**

After connecting the device to mains power, it will boot with the Power LED on the front becoming steadily green. The LEDs on top flash green-yellow-blank to indicate that the device is unconfigured.

The Access Point defaults to being a DHCP server on a private subnet. For configuration access, simply connect a PC with a cross-over cable and make the PC a DHCP client. After connecting, the client will have an IP address in the 172.23.56.0/24 network. For configuration access, point your PC’s browser to [https://172.23.56.254](https://172.23.56.254)

A wizard will ask you basic questions about your intended configuration which are non eduroam-specific. Please complete the wizard by answering all the questions.

Pay special attention to step 6, where you configure the IP address. Remember to check the box "Configure default gateway" since the access point needs to talk to RADIUS, NTP and syslog servers, which may lie in a different subnet!

At step 8 of 9, you will encounter the first crucial setting for compliance with the eduroam policy: time synchronisation. The device suggests an NTP server (pool.ntp.org), which is a sane default setting. However, if you operate your own NTP server, you can select "Other..." and enter your own server name (see screenshot).

If you changed the IP address of the Access Point with the wizard, re-connect to the Access Point on its new address after finishing the wizard.

**Timezone setup**

The Access point needs to be synchronised with a NTP or SNTP time server (which was set up using the wizard), which requires correct timezone settings. Click on "Configuration" -> "Date & Time" -> "General". and verify that the correct time zone and daylight saving time settings are set (see screenshot).

**Logging**

Another requirement in the eduroam policy is that the eduroam SP is required to maintain logs of the authentication and of MAC-address to IP address bindings. LANCOM devices can satisfy both by logging events via syslog. By default, the device keeps short-term logs by logging to "127.0.0.1". The logs can be viewed by navigating to the menu "LCO Menu Tree" > "Status" > "TCP-IP" > "syslog" > "Last Messages" and look like the following (prefixed with the exact timestamp, left out for readability reasons):

<table>
<thead>
<tr>
<th>AUTH</th>
<th>Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN-1 Associated WLAN station 64:b9:e8:a0:2e:a4 []</td>
<td></td>
</tr>
<tr>
<td>WLAN-1 WLAN station 64:b9:e8:a0:2e:a4 [] authenticated via 802.1x [user name is <a href="mailto:certuser-2010-001@restena.lu">certuser-2010-001@restena.lu</a>]</td>
<td></td>
</tr>
</tbody>
</table>
As you can see, the authentication itself and all MAC -> IP binding actions are logged, both for IPv4 and IPv6.

It is required to log these notices to an external syslog server, since the syslog buffer in the device fills quickly and the information would be lost otherwise. Add your syslog server by selecting the menu item "Configuration" > "Log & Trace" > "Syslog" and make sure the box "Send information..." is checked (it is by default) (see screenshot).

![Syslog configuration screenshot](image)

Then click on "Syslog servers" and on the following page "Add".

Then enter the IP address of your syslog server, and choose the events that shall be logged. We suggest to select at least the sources

- System
- Login
- System time
- Console Login
- Connections
- Administration

and the levels

- Alert
- Error
- Warning
- Information

for a comprehensive overview of events on the device.

**Configuring the wireless LAN**

The network name (SSID) for an eduroam SP is usually "eduroam", and the SSID needs to be broadcasted. Unfortunately, the network cannot be set up via the corresponding wizard, since the wizard only allows to configure WPA-Personal authentication, not eduroam's WPA-Enterprise. So, the necessary settings can only be found under "Configuration" > "Wireless LAN" > "General". (see screenshot)
First, we need to enable the MAC to IP address logging. This is done by checking the box "ARP handling". You should also make sure that you enter the correct country on this page, since the country setting makes your device conformant to national regulations for radio usage.

We also suggest to check the box "Broken LAN link ..." as a safety feature: if the access point detects that the wired backhaul is disconnected, it will stop broadcasting the wireless network. This saves users from frustration if connecting to a defunct access point.

After these settings, go to the sub-menu "Logical WLAN setting – Network", see screenshot below.

![Screen Shot of LANCOM](image)

The device offers eight independent networks. Choose one you want to use for eduroam (for example: WLAN-1) and click on its entry. Now set the properties of this network as follows:

- WLAN network enabled to **On**.
- Network name (SSID) to **eduroam**.
- Deselect the box labelled "Suppress SSID broadcast"
- MAC filter enabled to **Off**.
- Maximum count of clients to **0**.
- Client Bridge support to **No**.

When deploying your hotspot, you should also consider some non eduroam-specific guidelines for WLAN deployment. An incomplete list of things to consider is collected in chapter FOO.

**Security settings**

You need to make two security-relevant settings: configure the RADIUS server to use for authenticating users and configure the eduroam Wireless LAN to use RADIUS at all.

First, let's define a RADIUS server for authentication. As a pure eduroam SP, the RADIUS server in question is likely the one of your national federation. If you are both an eduroam IdP and an eduroam SP, the RADIUS is your own RADIUS server.

Select "Configuration" > "Wireless LAN" > "IEEE 802.1X" > "RADIUS server" and click on "Add". (see screenshot below).

![Screen Shot of LANCOM](image)

Then, fill in your RADIUS server details as negotiated with your eduroam IdP or federation operator.

In the second step, we'll apply the RADIUS server and encryption scheme to the SSID eduroam. To do that, go to the menu "Configuration" > "Wireless LAN" > "802.11i/WEP" > "WPA or Private WEP settings". Then, click on the WLAN network which you chose for the "eduroam" SSID before (see screenshot).
Set the following entries:

- Encryption Activated to Activated
- (Key 1/passphrase is irrelevant)
- Method/Key 1 Length to 802.11i(WPA)-802.1x
- WPA Version to WPA2
- (WPA1 Session Key Type is irrelevant)
- WPA2 Session Key Type to AES
- (WPA rekeying cycle is at your discretion; the default value 0 is a sane default)
- (Client EAP method is irrelevant)
- (Authentication is irrelevant)
- (Default key is irrelevant)

A recurring question is "Why is Client EAP method irrelevant?" The answer is: this setting refers to which authentication method the access point should use when it is in Client mode (i.e. it acts as a supplicant to connect to another access point). When in Access Point mode, its role is by design limited to transparently pass all authentication methods to a RADIUS server.

Using RADIUS/TLS instead of RADIUS (optional)

LANCOM devices have a RADIUS/TLS client built-in. It can be used instead of standard RADIUS for the uplink to an IdP. Please note that most of the value of RADIUS/TLS plays out in long-haul connections, like from an eduroam IdP server to his federation. If your Access Point is located closely to your RADIUS server, using RADIUS is sufficient and you need not follow the steps below.

To use RADIUS/TLS in the eduroam context, you must have been issued an eduroam Service Provider X.509 certificate from your federation operator.

When you have your certificate, the private key, and the CA certificate that issued you your certificate, you need to upload these via the device menu "File Management" > "Upload Certificate or File".

Upload them using the File Type "RADSEC ..." as in the screenshot below.

Then, go to "LCOS Menu Tree" > "Setup" > "IEEE802.1X" > "RADIUS Server" and set the Protocol option to "RADSEC", as in the screenshot below. The shared secret is not security-relevant when using RADIUS/TLS, but it must be set nevertheless. eduroam uses the fixed string "radsec" for all RADIUS/TLS shared secrets.