

Langaton Tampere – yhteisötukiaseman liittäminen

Tässä ohjeessa kerrotaan, miten rekisteröit tukiaseman Yrityksen Tunnistuspalveluun sekä miten teet tukiaseman asetukset. Ohje on tarkoitettu yhteisötukiaseman ohjelmistoversiolle 2.

Yrityskäyttäjän päätelaitteiden asetuksista on erillinen ohje.

1. **Kaksi käyttötapaa**

Käytössäsi on Langattomassa Tampereessa kaksi eri käyttötapaa. Toinen soveltuu paremmin satunnaisille verkkoyhteisön käyttäjille (verkkotunnus eli SSID WirelessTampere) ja toinen verkkoyhteisöä aktiivisemmin käyttäville (verkkotunnus eli SSID LANGATON-WPA).

Organisaatio saa itse valita, kumman käyttötavan WLAN-tukiasemissaan ottavat käyttöön. Langattoman Tampereen suositus on se, että organisaatioiden toteutus sisältäisi kummankin käyttötavan toteuttamisen.

1. 1. **WirelessTampere**

Tämä käyttötapa soveltuu hyvin satunnaisille vieraille. Kyseessä on salaamaton ja avoin verkko, jonka käyttö ei edellytä etukäteen tehtäviä määrittelyjä päätelaitteeseen (esim. työasema tai WLAN-kännykkä).

Kun käyttäjä löytää WirelessTampere –nimisen WLAN-verkon ja valitsee sen, kytkeytyy päätelaite verkkoon. Tämän jälkeen käyttäjän tulee avata WWW-selain ja hakea sillä jotain WWW-sivua. Pyydetyn WWW-sivun asemesta käyttäjälle näytetään tunnistautumissivu, johon käyttäjä syöttää tunnuksensa ja salasanaan. Tämän jälkeen käyttäjä voi käyttää päätelaitteellaan internet-yhteyksiä normaalisti.

1. 2. **LANGATON-WPA**

Tämä käyttötapa soveltuu hyvin Langatonta Tamperetta aktiivisesti käyttävälle. LANGATON-WPA:n langaton yhteys on vahvasti salattu, samoin tunnistustapah-tuma on salattu vahvasti. Nämä salausominaisuudet tekevät LANGATON-WPA:n käytön yritys- ja kotikäyttäjän näkökulmasta muita WLAN-toteutuksia turvallisemman. **Suosittelemme tästä huolimatta VPN-ohjelmistoa yritysten omien järjestelmien käyttämiseksi!**

Kun käyttäjä on tehnyt päätelaitteeseensa etukäteen *Langattoman Tampereen yritysratkaisun päätelaitteen asetukset* -ohjeen mukaiset asetukset, kirjautuu päätelaite automaattisesti Langattomaan Tampereeseen. Tästä johtuen LANGATON-WPA:n käyttö on vaivatonta ja helppoa, jonka lisäksi saadaan hyöty paremmasta turvallisuudesta.

Kotikäyttäjien Langattomaan Tampereeseen liittämät tukiasemat tukevat LANGATON-WPA –käyttötapaa ja niiden käyttö on yrityskäyttäjälle yhtä turvallista, kuin minkä tahansa yritystukiasemankin käyttö. Tästä syystä Langattoman

Tampereen kotikäyttäjän ratkaisu soveltuu erityisen hyvin mahdollistamaan liikkuva työ myös yrityskäyttäjän kotona.

2. **Yhteisötukiasemasta yleistä**

Yhteisötukiaseman avulla kyetään toteuttamaan sekä WWW-tunnistus (WirelessTampere) että WPA-Enterprise (LANGATON-WPA) -käyttötavat. Ensiksi mainittu sopii parhaiten satunnaisille käyttäjille ja jälkimmäinen aktiivisesti Langatonta Tamperetta käyttävälle.

Jälkimmäinen tapa on erityisen tietoturvallinen - tunnistustapahtumaa tai WLAN-radioliikennettä ei kyetä salakuuntelemaan, mutta VPN:n käyttö on tietysti silti suositeltavaa.

Yhteisötukiasema on toteutettu haluttaessa mahdollistaa yrityksille edullinen ja helppo tapa tarjota asiakkailleen molemmat autentikaatitavat.

3. **Tukiaseman rekisteröinti Yrityksen Tunnistuspalveluun**

RADIUS-palvelin ei huoli tunnistautumispyyntöjä rekisteröimättömästä tukiasemasta. Näin jokainen yrityksen tukiasema tulee rekisteröidä.

Lisäät tukiaseman Yrityksen Tunnistuspalvelun käyttöliittymässä www.langatonyritys.fi kohdassa *Tukiasemat/Luo tukiasema*.

Tukiasemat

 [Näytä kaikki tukiasemat](#)

 [Luo tukiasema](#)

Tarvitset tukiaseman lisäämiseksi tiedon sen käyttämästä MAC-osoitteesta (=ethernet-osoite). Huomaa, että yhteisötukiaseman tapauksessa käytetään kahta erillistä MAC-osoitetta, toista WPA-autentikointiin ja toista WWW-autentikointiin. MAC-osoitteita käytetään tukiaseman tunnistamiseen ja mm. sen tunnistamiseen, onko yrityksen vieraskäyttäjä kirjautumassa yrityksen omaan tukiasemaan.

Kahdesta erillisestä käyttötavasta johtuen yhteisötukiasema tulee liittää yritystunnistuspalveluun kaksi kertaa. Seuraavissa kappaleissa selvitetään näiden käyttötapojen liittämiseen liittyvät käytännöt.

3. 1. **WPA-Enterprise käyttötavan rekisteröinti**

Luo tukiasema

MAC-Osoite:

Jaettu salaisuus:

Autentikaation tyyppi:

MAC-osoitteeksi kirjoitetaan WPA-Enterprises tapauksessa tukiaseman pohjasta ja pakkauksesta löytyvä MAC-osoite. Samaa MAC-osoitetta tarvitaan myös tukiaseman asetusten yhteydessä. Huomioi, että MAC-osoite tulee kirjoittaa pelkinä numeroina ja kirjaimina ilman välimerkkejä.

Järjestelmä arpoo uudelle tukiasemalle jaetun salaisuuden. Tukiasemalle voidaan käyttää arvottua salaisuutta tai kirjoittaa kokonaan uusi. Voi olla järkevää varata yrityksen kaikille omille tukiasemille yhteinen jaettu salaisuus ja kirjoittaa se tähän. HUOM: Jaettu salaisuus kirjoitetaan myös tukiaseman asetuksiin, joten ota se itsellesi talteen tukiaseman määrittelyä varten. Tätä jaettua salaisuutta voit käyttää myös tukiaseman root-käyttäjän salasanana, jolloin se on helposti tarkistettavissa yritystunnistuspalvelun käyttöliittymän kautta.

Autentikaation tyyppiä käytetään peittoaluekartassa kertomaan, mitä käyttötapaa kukin tukiasema tukee. Valitse näistä valikosta WPA+WPA2.

Organisaatioksi tulee se yritys, jolle tukiasemaa ollaan pystyttämässä, samoin kuin yrityksen osoitetiedoiksi tulee yrityksen sen toimipaikan osoite jonne tukiasemaa ollaan asentamassa.

Tukiaseman sijaintitiedot määritellään vasta WPA2-käyttötavan asentamisen yhteydessä, joten tässä yhteydessä valintaruutu "Näytä tukiasema kartalla" tulee jättää tyhjäksi. Sen sijaan valintaruutu kohdassa "Tämä on Wifidog-yhteensopiva tukiasema" tulee merkitä täytetyksi. Tukiaseman kaksinkertainen rekisteröinti aiheuttaa sen, että vain toinen tukiaseman rekisteröinnistä kannattaa merkitä näkyväksi. WPA2-rekisteröinnin yhteydessä luotua tukiasemaa ei kannata merkitä näkyväksi vaan näkyväksi kannattaa merkitä WPA2-puolen yhteydessä rekisteröitävä tukiasema.

Tukiaseman luomisen ja "Tukiasema luotu"-vahvistuksen jälkeen käyttäjän tulee siirtyä luomaan tukiasema uudelleen, tällä kertaa hyödyntämään WPA2-tunnistusta.

3.2. WWW-tunnistusta hyödyntävän käyttötavan rekisteröinti

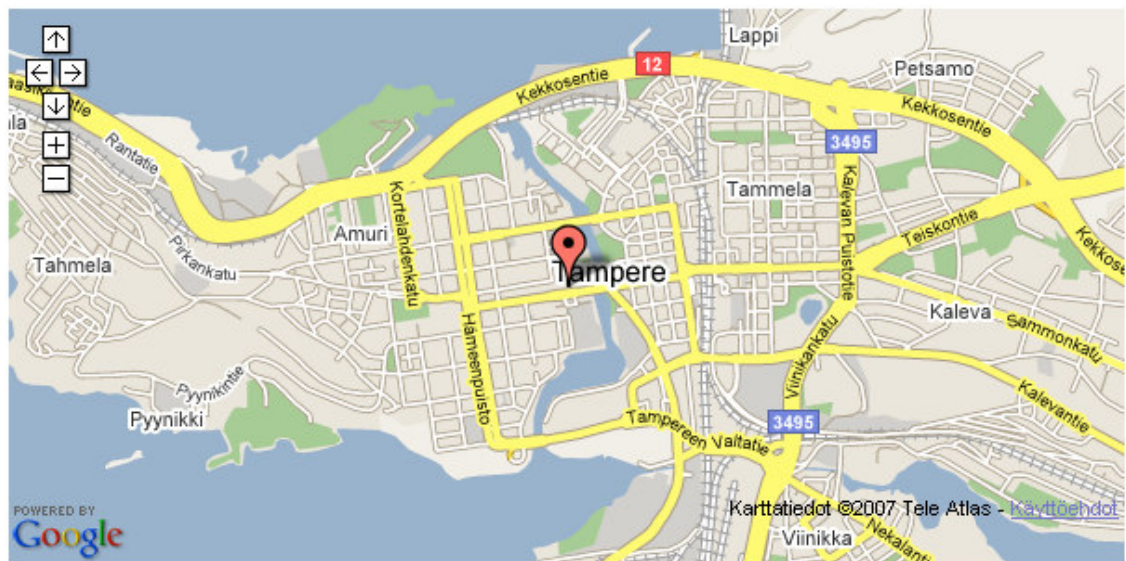
MAC-osoitteeksi kirjoitetaan WPA-Enterpisen tapauksessa tukiaseman pohjasta ja pakkauksesta löytyvä MAC-osoite **sillä erotuksella** että ensimmäisinä numeroina tulee olla "06" WPA-Enterprise kohdassa asetetun "00" sijaan. Huomioi, että MAC-osoite tulee kirjoittaa pelkinä numeroina ja kirjaimina ilman välimerkkejä.

WWW-tunnistuksen yhteydessä jaettuna salaisuutena on aina "LangatonYritys", joka tulee kirjoittaa tukiasemaa luotaessa jaetun salaisuuden kohtaan. Autentikaation tyyppiä valitaan tässä yhteydessä WWW. Myös organisaatitiedot valitaan samalla tavalla kuin kohdassa 3.1.

WWW-tunnistuksen yhteydessä voidaan tukiasemalle määritellä sijaintitieto, jonka perusteella tukiasemat näytetään www.langatontampere.fi -peittoaluekartassa. Oletusarvo tukiaseman sijainnille on yleensä yritykselle ilmoitettu osoite. Tukiaseman sijaintia voi kuitenkin hienosäätää, tarttumalla siitä kiinni ja siirtämällä kartassa oikealle kohdalle.

Koordinaatit:

61.498056 23.760833



Sijaintitiedon asettamisen jälkeen voidaan valita myös muita tietoja tukiaseman yhteyteen, kuten tukiaseman nimi sekä tukiaseman infokuplaan asetettava sisältö. Nämä ovat tukiasemaa hallinnoivan organisaation valittavissa. Tukiasema merkitään näkyväksi, kun sen kautta on onnistuneesti päästy verkkoon sekä WPA- että WWW-tunnistetulta puolelta organisaation omilla ja joillain mulla verkkovierailutunnuksilla.

WWW-käyttötapaa käytettäessä tulee valita myös valintalaatikko "Tämä on Wi-fidog-yhteensopiva tukiasema". Tämän valinnan jälkeen organisaatio voi asettaa käyttäjän näkemälle WWW-kirjautumissivulle omaa informaatiotaan, joka on organisaation valittavissa.

Tämänkin käyttötavan luomisen jälkeen tukiasema on rekisteröity Yrityksen tunnistuspalveluun.

4. Yhteisötukiasemaan tehtävät määrittelyt

4.1. Tietokoneen verkon asetukset

Yhteisötukiaseman asetusten konfiguroimiseksi tulee ottaa yhteys tukiasemaan. Tämä onnistuu ethernet-pariliitoksella tietokoneen ja tukiaseman välillä siten, että tietokoneen kiinteäksi IP:ksi asetetaan 192.168.84.9 ja aliverkon peitteeksi 255.255.255.0 sekä ottamalla WWW-selaimella yhteys osoitteeseen 192.168.84.1.

Yhteisötukiasemaan päästään myös langattoman verkon kautta WWW-puolelta osoitteella 192.168.202.1 ja WPA-puolelta 192.168.201.1. Ensimmäisten asetusten asettamiseen on suositeltavaa käyttää langallista liittymää, mutta muutoin hallintakäyttöliittymä on tavoitettavissa myös langattoman verkon puolelta.

Oletuksena hallintakäyttöliittymään pääsee käsiksi tunnuksella root ja salasanalla LangatonYritys.

LANGATON TAMPERE powered by Arch·Red OpenWrt Wireless Freedom

OpenWrt Kamikaze
Load: 0.04 0.08 0.15
Hostname: OpenWrt

Overview Status System Services Network Changes: 0 Administration

Langaton Tampere / Wireless Tampere

» **Asennusohjeet**

Avaa hallintapaneelin valikosta [Network > Wifi > WIFI0](#).
 Syötä **LANGATON-WPA** -verkon **Key**-kohtaan yrityskäyttöliittymään syötetty jaettu salaisuus.
 Vaihda hallintapaneelin salasana valikon [System > Admin Password](#) -kohdasta.
 Käynnistä lopulta tukiasema uudelleen ([System > Reboot](#)).

Tietoa tukiaseman tilasta on saatavilla osoitteista:
<http://192.168.84.1/cgi-bin/status.cgi> (WAN-liitäntä)
<http://192.168.201.1/cgi-bin/status.cgi> (LANGATON-WPA)
<http://192.168.202.1/cgi-bin/status.cgi> (WirelessTampere)

» **Set-up instructions**

Open [Network > Wifi > WIFI0](#) from the control menu.
 Input the access point shared secret in the **Key** field of the **LANGATON-WPA** network.
 Change the administration password in [System > Admin Password](#).
 Finally reboot the access point ([System > Reboot](#)).

Status of the access point is available at:
<http://192.168.84.1/cgi-bin/status.cgi> (WAN interface)
<http://192.168.201.1/cgi-bin/status.cgi> (LANGATON-WPA)
<http://192.168.202.1/cgi-bin/status.cgi> (WirelessTampere)

Powered by LuCI 0.8

KUVA: Yhteisötukiaseman hallintakäyttöliittymä

4. 2. *Tukiasemaan tehtävät asetukset*

Yhteisötukiaseman WPA-puolen jaettu salaisuus (**kohta 3.1**) asetetaan suoraan LANGATON-WPA -verkon asetuksiin (kuvassa sinisellä pohjalla), joihin pääsee tukiaseman hallintasivulta suoraan (Network → Wifi → WIFIO). On suositeltavaa, että samaa salaisuutta käytetään myös tukiaseman hallintakäyttäjän (root) salasanaksi.

| Interfaces | |
|---|---|
| ESSID | LANGATON-WPA |
| Network | wlan0 <small>Add the Wifi network to physical network</small> |
| Mode | Access Point |
| WDS | <input type="checkbox"/> |
| Transmit Power | <input type="text"/> <small>dBm</small> |
| Encryption | WPA-EAP <small>WPA-Encryption requires wpa_supplicant (for client mode) or hostapd (for AP and ad-hoc mode) to be installed.</small> |
| RadiusServer | 172.22.10.128 |
| Radius-Port | 1812 |
| Key | LangatonYritys |
| NAS ID | <input type="text"/> |
| - Additional Field - <input type="button" value="Add"/> | |

Tämän jälkeen tukiaseman asetuksia voidaan vielä säätää asettamalla esim. haluttu radiokanava tukiaseman ympäristön mukaisesti. Oletuksena tukiasema säätää tämän automaattisesti.

Mikäli tukiaseman asetuksia halutaan myöhemmin muuttaa, käytetään tukiaseman omaa hallintakäyttöliittymää.

5. *WLAN-verkon toteuttaminen yritykseen*

5. 1. *Palomuurin ulkopuolelle*

Yrityksen WLAN-vierasverkko on syytä sijoittaa aina yrityksen palomuurin ulkopuolelle, vähintään palomuurin demilitarisoidulle vyöhykkeelle (DMZ). Jos mahdollista, tukiasema kannattaa sijoittaa ei-NATattuun palomuuramattomaan verkkoon, mikä esim. ADSL-liittymissä tarkoittaa sillattua/IPTV-verkoksi merkittyä verkkoa. NATatun verkon voi tunnistaa myös harmaiden osoitteiden käytöstä eli verkosta, johon tukiasema liitetään, saa osoitteen, joka on 10, 192.168-, tai 172.(16-31)-alkuinen.

5.2. *VPN-yhteydet*

Yrityksen omienkin työntekijöiden tulee käyttää VPN:ää päästäkseen kiinni yrityksen omiin tietojärjestelmiin. Tällöin työntekijöillä on itselläänkin yhdenmukainen tapa käyttää Langatonta Tamperetta, ovat sitten kiinni tukiasemassa kotona, yrityksen neuvottelutiloissa tai vaikkapa autohuollossa.

Varmista, että WLAN-verkon ja internetin välinen reititin tukee VPN-yhteyksiä. Esim. IPSec-toteutukset voivat edellyttää reitittimeltä/palomuurilta kykyä IPSec-yhteyksien mahdollistamiseksi.

5.3. *Pääsyoikeudet*

Salli kaikki liikenne tukiasemalle ja tukiasemalta. Älä säädä tukiaseman palomuuriasetuksia.