Joni Tähjä

Eduroam-vierailijaverkko Aruba Instant -ympäristössä

Tradenomi

Tietojenkäsittely

Kevät 2020

Tiivistelmä

Tekijä(t): Tähjä Joni

Työn nimi: Eduroam-vierailijaverkko Aruba Instant -ympäristössä

Tutkintonimike: Tradenomi (AMK), Tietojenkäsittely

Asiasanat: eduroam, RADIUS, 802.1X, WLAN, lähiverkko

Opinnäytetyön tavoitteena oli luoda ja ottaa käyttöön eduroam-verkko Kajaanin ammattikorkeakoulun kampuksella olemassa olevaan Aruba Instant -verkkoon. Lähtötilanteessa kampuksella ei ollut minkäänlaista vierailijaverkkoa.

Eduroam on RADIUS-palvelimiin pohjautuva verkko, jossa käyttäjä voi käyttää yhden organisaation tunnuksia muissa eduroamia hyödyntävissä organisaatioissa. Toiminta perustuu RADIUS-palvelinten hierarkiaan, jossa autentikointipyyntö voidaan välittää oikealle organisaatiolle, ja käyttäjä autentikoitua. Eduroam perustuu IEEE:n 802.1X-standardiin pohjautuvaan autentikointiin.

Aruba Instant on Aruba Networksin verkkoteknologia, jossa yksittäinen tukiasema ottaa perinteisen verkkokontrollerin roolin. Tämä soveltuu hyvin erityisesti pienempiin verkkoihin, ja maksimi koko onkin rajattu 128:aan tukiasemaan.

Työn käytännön osuudessa luotiin testiympäristö Kajaanin ammattikorkeakoulun datacenter laboratorioon, ja sen pohjalta verkkototeutus vietiin toimeksiantaja KamIT:in tuotantoympäristöön. Testiympäristössä tehtiin alusta lähtien RADIUS-palvelimen asennus, sekä vaadittavat verkkosäännöt ja käyttäjätietokannat.

Lopputuloksena kampukselle saatiin toimiva eduroam-verkkoympäristö, joka otettiin käyttöön syksyllä 2018. Tämä mahdollistaa vierailijoiden, joilla on tunnukset jossakin toisessa eduroam-organisaatiossa, yhdistämisen suoraan kampuksen verkkoon. Verkko on myös saatavilla kampuksen omille opiskelijoille ja henkilökunnalle.

Abstract

Author(s): Tähjä Joni

Title of the Publication: Eduroam Guest Network in Aruba Instant Environment

Degree Title: Bachelor of Business Administration, Business Information Technology

Keywords: eduroam, RADIUS, 802.1X, WLAN, local network

The goal of this thesis was to create and deploy an eduroam network into the existing Aruba Instant environment at the Kajaani University of Applied Sciences (KAMK) campus. There was no previous guest network on the campus.

Eduroam is a network based on RADIUS servers, where the user can use one organization's credentials at other organizations using eduroam, to authenticate into the network. It is based on a hierarchy of RADIUS servers, where the authentication request can be relayed to the correct organization, allowing the user to be authenticated. Eduroam is based on authentication defined in IEEE's 802.1X standard.

Aruba Instant is a network technology from Aruba Networks, where a single Wi-Fi access point takes the role of a traditional network controller. This works well especially for smaller networks, and the maximum size is limited to 128 access points.

In the practical part of this thesis, a test environment was set up in the datacenter laboratory of KAMK. Based on that implementation, it was then deployed into the production network at the campus, which is managed by the client of this thesis, KamIT. A RADIUS server and the necessary network rules and user databases were set up in the test environment.

As a result, a working eduroam network environment was set up on the campus, the use of which started in autumn 2018. This enables guests who have credentials in other eduroam organizations to directly connect to the campus network. The network is also available to students and employees of the campus.

Sisällys

Liitteet

1 Johdanto

Globalisaation edistyessä ihmisten liikkuvuus lisääntyy, ja muunmuassa koulumaailmassa vaihto-opiskelu on arkipäivää. Tämän helpottamiseksi monet organisaatiot pitävät yllä vierailijaverkkoja, joihin joko tietyt vierailijat, tai jopa kaikki, voivat yhdistää verkkoa hyödyntävät laitteensa. Eduroam on vierailijaverkko, joka on hyvin laajalle levinnyt korkeakoulujen ja yliopistojen keskuudessa kansainvälisesti. Sitä hyödyntämällä eri koulutuslaitosten opiskelijat voivat yhdistää laitteensa verkkoon muissa koulutuslaitoksissa käyttäen oman organisaationsa käyttäjätunnuksia, täten helpottaen vierailijoiden verkkoon yhdistämistä, kuitenkaan verkkoa avaamatta kaikille ulospäin.

Opinnäytetyön aiheena on eduroam-vierailijaverkon luominen olemassaolevaan Aruba Instant -ympäristöön. Toimeksiantajalle Eduroam-verkon luonti on velvoite CSC:ltä, joka hallinnoi Suomen korkeakouluverkkoa, Funetia. Toimeksiantajalta tai CSC:ltä ei löydy aiempaa kirjallista tietoa siitä, että verkkoa olisi toteutettu Instant-ympäristöä käyttäen. Täten työhön kuuluu tutkimusta siitä, voiko verkolle saada samaa toiminnallisuutta kuin perinteiselle kontrolleripohjaiselle verkolle. Keskeinen tavoite on luoda toimiva eduroam-verkko Kajaanin ammattikorkeakoulun kampukselle. Verkko myös sallisi muista korkeakouluista vierailevien henkilöiden yhdistää verkkoon käyttäen omien korkeakoulujensa tunnuksia.

Opinnäytetyö on jaettu kahteen osioon. Ensimmäisessä osiossa käsitellään työn teoriaa ja siihen liittyviä asioita. Toisessa osuudessa käydään läpi työn käytännön osuus. Tämän lisäksi liitteistä löytyy opinnäytetyön aikana tuotettu dokumentaatio.

2 Toimeksiantaja - KamIT

KamIT on Kajaanin kaupungin alainen tietohallintoyksikkö, joka vastaa asiakkaiden ICT-palvelujen ylläpidosta ja kehittämisestä. Sillä on noin 10 500 asiakasta Kajaanin, Kuhmon, Sotkamon, Suomussalmen, Kuusamon ja Vantaan alueella. Eri toimipisteitä on 26 kappaletta. Työasemia noin 5000. KamIT:in tilat sijaitsevat Kajaanin ammattikorkeakoulun kampuksella. KamITin palveluita ovat mm. konesalipalvelut, tiedonhallinta, helpdesk ja muut tukipalvelut sekä opetusteknologiaan liittyvät palvelut.

3 Langattomat verkot

Langattomilla verkoilla yleisesti ottaen tarkoitetaan WLAN:ia, joka tulee sanoista Wireless Local Area Network, eli langaton lähiverkko, ja se perustuu IEEE:n 802.11-standardeihin. Kaupallisena nimenä WLAN:ista käytetään termiä Wi-Fi. WLAN-laitteet toimivat joko 2,4 GHz:in, tai 5 GHz:in taajuudella. WLAN:in kanssa tulisi aina käyttää jotain salausta, jotta erinäiset väärinkäytökset voitaisiin estää. Kotikäytössä näistä yleisimpiä ovat WEP (Wired Equivalent Privacy), WPS (Wi-Fi Protected Setup), sekä WPA (Wi-Fi Protected Access). [1]

Ihmisten liikkuessa, ja verkkoon yhdistettävien laitteiden määrän kasvaessa, on vierailijaverkoista syntynyt kilpailuvaltti erinäisille tahoille. Niitä löytää muun muassa lentokentiltä, muilta julkisilta paikoilta sekä monista liiketiloista. Näissä kaikissa ajatuksena on tarjota vierailijalle ilmainen pääsy internetiin. Tämä voidaan toteuttaa joko langallisesti tai langattomasti. Vierailijaverkko on tyypillisesti avoin, tai vähintäänkin mm. verkon salasana on julkisesti ja helposti saatavilla. Vierailijaverkot ovat yleensä myös eristettyjä organisaation muusta verkosta, jolloin vältytään mahdollisilta haavottuvaisuuksilta.

Vierailijaverkkojen kanssa täytyy pitää huoli verkon suojauksesta, sillä mikäli verkko on julkinen kaikille, väärinkäytön riski kasvaa. Tätä riskiä voidaan pienentää esimerkiksi käyttäjien todentamisella. Käyttäjien todentamisen voi suorittaa muun muassa captive portal -ratkaisulla, joka hyödyntää RADIUS-palvelinta. Muita tapoja suojata käyttäjiä on muun muassa verkon SSID-tiedon mainostamisen ottaminen pois päältä, tai suora suodattaminen laitteiden MAC-osoitteiden avulla. Eduroamin tapauksessa käytetään RADIUS-palvelinta, mutta captive portal -ratkaisua ei hyödynnetä tietoturvariskien takia. [2]

Internetiin yhdistetyjen laitteiden lisääntyessä tietoturvaan tulee kiinnittää entistä enemmän huomiota. Strategy Analyticsin mukaan vuoden 2018 loppuun mennessä internetiin oli yhdistettynä jopa 22 miljardia laitetta, ja ennusteen mukaan tämä luku lähentelisi jo 50 miljardia vuoteen 2030 mennessä [3]. Internet of Things, eli Esineiden Internet käsitteenä kattaa kaikki internetiin yhdistetyt esineet ja laitteet. Tänä päivänä tämä tarkoittaa eri kodin älylaitteita, kuten televisiot, mahdolliset valvonta ja kodinhallintalaitteet, ja jopa jääkaappeja. Sitä mukaan kun verkkoon liitetään laitteita, myös haavoittuvuuspinta-ala kasvaa, ja jo yksittäinen heikommin turvattu laite voi altistaa verkon hyökkäyksille.

WEP julkaistiin alun perin ensimmäisessä 802.11-1997-standardissa, ja on täten vanhin langattomien verkkojen suojaukseen luotu standardi. Sen seuraajaksi nimettiin vuonna 2003 WPA. WPA perustui joko 40-bittiseen (WEP-40), tai 104-bittiseen (WEP-104) salausavaimeen. Lukuisten salausavaimiin liittyvien heikkouksien vuoksi WEP-salaus voidaan kuitenkin oikeilla työkaluilla murtaa minuuteissa, joten sen käyttöä tulisi aina välttää. [4]

WPS on Wi-Fi Alliancen kehittämä ja vuonna 2006 julkaistu langattomien verkkojen suojaus, jonka tavoitteena oli tehdä suojauksen käyttöönotto ja käyttö mahdollisimman helpoksi käyttäjälle. Verkkoon yhdistäminen tapahtui joko painamalla reitittimessä olevaa fyysistä WPS-painiketta tai käyttämällä lyhyttä PIN-koodia. WPS:n heikkous kohdistuu nimenomaan PIN-koodiin, joka on vain kahdeksan numeroa pitkä. Tämän lisäksi reititin tarkistaa PIN-koodin neljä ensimmäistä lukua, joka tekee brute-force hyökkäyksen äärimmäisen helpoksi, sillä mahdollisia numeroyhdistelmiä on vain hyvin pieni määrä. Tämän vuoksi myöskään WPS-suojausta ei suositella käytettäväksi. [5, 6, 7]

WPA on myös Wi-Fi Alliancen kehittämä protokolla, joka kehitettiin WEP:n korvaajaksi. Se julkaistiin 2003 väliaikaisratkaisuksi, ja vuonna 2004 julkaistu WPA2 korvasi sen. Myös WPA2 onnistuttiin murtamaan vuonna 2017, mutta sen seuraajana toimivaa WPA3:a tukevia laitteita on tulossa markkinoille. WPA:n autentikointi perustuu käyttäjän itse asettamaan salasanaan. Yksi suurimmista korjauksista siirryttäessä WEP:istä WPA:han oli TKIP:n, eli Temporal Key Integrity Protocolin käyttöönotto. TKIP:n avulla jokaisella verkkopaketilla on oma salausavain, toisin kuin WEP:issä, jossa kaikki paketit käyttivät samaa avainta. WPA2:n mukana tuli myös AES, joka korvasi TKIP:n. [8, 9]

4 Eduroam

Eduroam on GÉANTin koordinoima kansainvälinen tutkimus- ja opiskelijaroaming-verkko. Verkon ajatuksena on se, että jäsenorganisaatioiden käyttäjät voivat vierailla muissa jäsenorganisaatioissa, ja pystyvät käyttämään oman organisaationsa kirjautumistietoja verkkoon tunnistautuakseen. Suomessa eduroamista vastaa Tieteen tietotekniikan keskus Oy, CSC, ja se toimii sen ylläpitämässä Funet-verkossa.

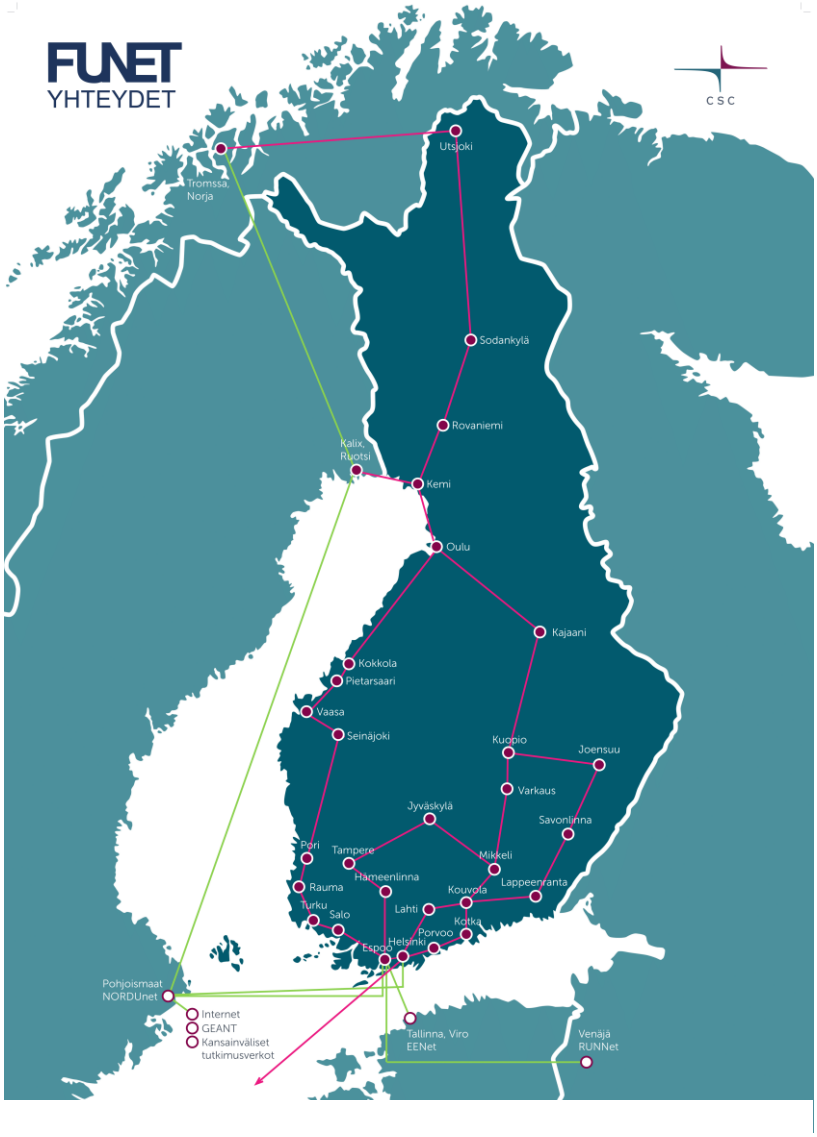
Eduroamin pohja luotiin vuonna 2003, ja kirjoitushetkellä maita, joissa on eduroam-jäseniä, on 89 kappaletta. Suomessa organisaatioita on 39 kappaletta, sisältäen kaikki yliopistot sekä ison osan ammattikorkeakouluista. [10, 11, 12, 13]

Eduroam on lähtökohtaisesti turvallisempi käyttää kuin avoimet verkot, ja se perustuu jo olemassaoleviin ja tunnettuihin salaus- ja autentikointitekniikoihin, kuten WPA2-salaukseen. Kajaanin ammattikorkeakoulun osalta eduroam-verkon ja internetin välissä on palomuuri sekä pakettisuodatus, mutta tätä ei pidä silti ottaa oletuksena välttämättä muissa organisaatioissa. Tämän lisäksi voidaan myös hyödyntää esimerkiksi SSH ja SSL tekniikoita lisäturvan takaamiseksi.

4.1 Funet

Funet on maanlaajuinen tutkimuksen ja korkeakoulujen verkko. Se palvelee lähinnä korkeakouluja sekä tutkimuslaitoksia. Kartta Funet-verkosta löytyy kuvasta 1. Sen palveluihin kuuluvat mm. verkkoyhteydet, langattomat verkot kuten eduroam, eri verkkopalvelut kuten aikapalvelimet, sekä Haka-autentikointi. Eduroamin osalta Funet-verkossa toimii Suomen maajuuret. [14, 15]

Funet on osa pohjoismaista NORDUnetiä, joka kattaa kaikki Pohjoismaat. Tällä välityksellä Funet on myös osa Euroopan laajuista GÉANT-verkkoa. NORDUnet vastaa myös kansainvälisistä internetyhteyksistä. [14, 16, 17]



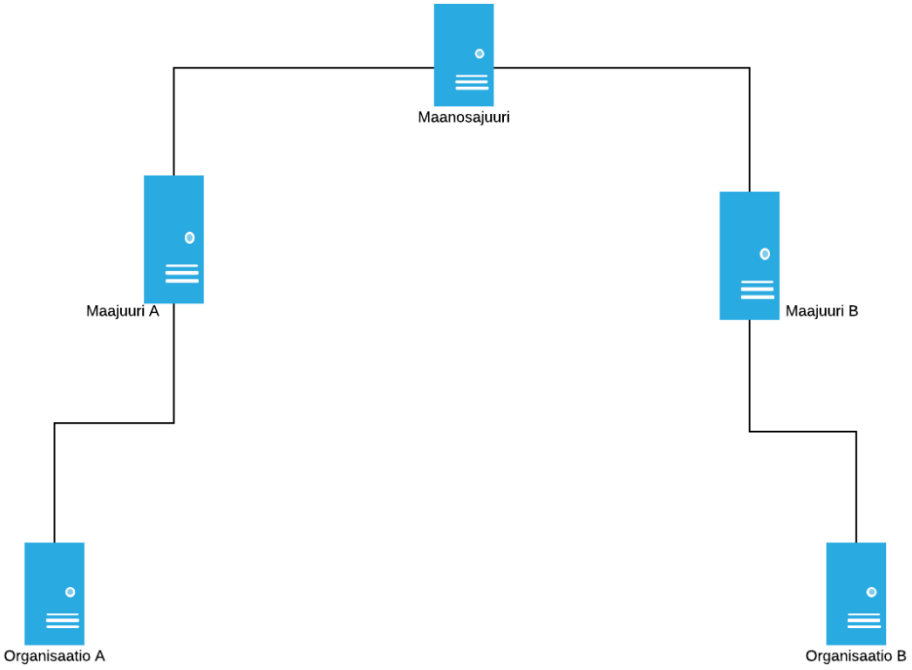
Kuva 1 - Funet-verkkokartta. Lähde: https://wiki.eduuni.fi/display/funet/Tulostettavat+julisteet

4.2 Miten eduroam toimii

Eduroamin runko pohjautuu RADIUS-palvelimiin sekä IEEE 802.1X -standardiin. Ideana on, että käyttäjä voi kirjautua omilla käyttäjätunnuksillaan mihin tahansa eduroam-verkkoon maailmanlaajuisesti, ja käyttäjän tiedot autentikoidaan kotiorganisaatiossa. Käytännössä tämä tapahtuu RADIUS-palvelinten välityksinä, joka muodostaa tietynlaisen hierarkian. Jos

organisaation A (kuva 2) käyttäjä vierailee organisaatiossa B, voivat he kirjautua organisaatio B:n eduroam-verkkoon tunnuksillaan, jotka he ovat saaneet organisaatiosta A. Tällöin organisaatio B:n RADIUS-palvelin välittää autentikointipyynnön maajuurien A ja B sekä maanosajuuren kautta organisaatiolle A. Organisaation A RADIUS-palvelin suorittaa autentikoinnin ja vastaa organisaatio B:n lähettämään pyyntöön. Mikäli autentikointi on onnistunut, organisaation A käyttäjä on nyt yhdistettynä verkkoon. [18]

RADIUS-palvelimet suorittavat lopullisen autentikoinnin paikallisesta käyttäjätietokannasta. Tämä voi olla esimerkiksi Microsoftin Active Directory, jokin muu LDAP-pohjainen järjestelmä tai esimerkiksi MySQL-tietokanta. Käyttäjän yhdistäessä verkkoon tältä kysytään käyttäjätunnuksia.



Kuva 2 - Eduroam RADIUS-hierarkia

Syöttämisen jälkeen ne välitetään määritetylle RADIUS-palvelimelle. Tämä etsii käytettyjä tunnuksia käyttäjätietokannasta. Mikäli autentikointi onnistuu, käyttäjän sallitaan yhdistää verkkoon. RADIUS-kyselyn yhteydessä voidaan myös välittää attribuutteja, joilla voidaan esimerkiksi määrittää käyttäjän VLAN. [19, 20]

4.2.1 Aruba ClearPass Policy Manager

ClearPass Policy Manager on Aruba Networksin verkon pääsynhallintaratkaisu, jonka avulla voidaan suorittaa pääsynhallintaa käyttäen mm. RADIUS:ta. Se ajetaan CentOS-pohjaisen

käyttöjärjestelmän päällä. ClearPass voidaan toteuttaa joko dedikoidulla palvelimella, tai ClearPass voidaan myös asentaa virtualisoidun palvelimen päälle. ClearPass myös sallii erinäistä verkon käytön valvontaa. Clearpassista löytyy tuki useille eri autentikointilähteille, kuten Microsoftin Active Directorylle, LDAP:ille, tai SQL-tietokannoille. Alustan käyttö vaatii lisenssin, jonka kustannukset riippuvat käyttäjämääristä. Lisää ClearPass Policy Managerin käyttöönotosta ja ominaisuuksista löytyy liitteestä 1.

4.2.2 Eduroam CAT

Eduroam CAT, eli Eduroam Configuration Assistant Tool, on GÉANTin ylläpitämä hallinnointityökalu, jonka avulla verkkoylläpitäjät voivat luoda ja jakaa Eduroamin käytön vaatimat konfiguraatiotiedostot. Tämä tekee myös niiden jakamisen loppukäyttäjille helpoksi. Palvelu on verkossa, joten sen käyttö onnistuu lähes millä tahansa käyttöjärjestelmällä.

Ylläpitäjille on saatavilla työkalut, joilla julkaista Eduroam-verkon käyttäjille tarkoitettu konfiguraatiopaketti, joka sisältää mm. verkon tiedot sekä vaadittavat sertifikaatit. Tämän lisäksi on käyttäjille suunnattu osio, jonka kautta käyttäjät voivat hakea ja ladata tarvitsemansa organisaation paketin. Ylläpitäjien näkymästä löytyy lisää liitteen 1 sivulta 27, ja käyttäjien näkymästä sekä pakettien lataamisesta liitteestä 2.

4.3 IEEE 802.1X

802.1X on alun perin vuonna 2001 julkaistu IEEE:n standardi, joka käsittelee autentikointia LAN tai WLAN verkoissa. Sen kirjoitushetkellä uusin versio julkaistiin vuonna 2010. Standardin pohjana on IEEE:n 802 LAN -teknologia, kuten 802.11, joka koskee WLAN teknologioita. Autentikointi itsessään hyödyntää EAP-protokollaa, joka on määritelty RFC 3748 -dokumentissa. Varsinaisesta kapseloinnista käytetään termiä EAPOL, joka tulee käsitteestä ”EAP over LAN”. [21]

Eri EAP-tyyppejä on lukuisia, taulukko 1 määrittää joitain käytetyimpiä ja niiden ominaisuuksia.

EAP-tyyppi Ominaisuus	TLS Transport Level Security	TTLS Tunneled Transport Level Security	PEAP Protected Transport Level Security
Käyttäjäsertifikaatti	Kyllä	Ei	Ei
Palvelinsertifikaatti	Kyllä	Ei	Kyllä
Käyttöönoton vaikeus	Vaikea	Keskinkertainen	Keskinkertainen
WLAN-turvallisuus	Erittäin hyvä	Hyvä	Hyvä

Taulukko 1. EAP-tyyppien vertailua

Paras tyyppi ratkaisulle riippuu vaadituista ominaisuuksista sekä käytetyistä järjestelmistä. Jotkut käyttöjärjestelmät eivät tue joitain tyyppejä. [22]

Kuten EAP-tyyppien vertailussa ilmeni, osa tyypeistä vaatii sertifikaattien hyödyntämistä. Sertifikaatit perustuvat SSL-teknologiaan, ja niiden tarkoituksena on mahdollistaa eduroamin kohdalla RADIUS-palvelimen identiteetin varmistaminen. RADIUS-käytössä palvelinsertifikaatti tulee olla asennettuna käytetylle RADIUS-palvelimelle sekä käyttäjän omalle laitteelle. Mikäli organisaatio käyttää jotain julkista, tunnettua certificate authorityä, eli CA:ta, voi palvelinsertifikaatin juuri olla jo oletuksena luotettu. Mikäli käytetään esimerkiksi organisaatiossa olemassa olevaa omaa CA:ta, voi käyttäjä mahdollisesti joutua asentamaan uuden juurisertifikaatin. Käyttäjä joutuu joka tapauksessa asentamaan mahdolliset muut osat sertifikaattiketjussa. Esimerkki sertifikaatin asentamisesta sekä sertifikaattiketjusta löytyy liitteestä 1 sivulta 15. [23]

5 Verkkokontrollerit

Verkkokontrolleri on lähiverkossa oleva laite, jonka tarkoituksena on hallinnoida lähiverkkoon kuuluvia langattomia tukiasemia. Pääasiallinen hyöty tulee siitä, että organisaation kaikkia langattomia tukiasemia ei tarvitse konfiguroida yksitellen manuaalisesti, vaan konfiguraatio voidaan luoda verkkokontrollerilla ja välittää siitä kaikille verkkoon kuuluville tukiasemille. Tämä helpottaa verkon ylläpitoa ja pitää huolen, että jokainen tukiasema on konfiguroitu samalla tavalla. [24]

Aruba Instant on Aruba Networksin verkkoteknologia, jolla yksittäinen langattoman verkon tukiasema voi ottaa verkkokontrollerin roolin. Yleensä kontrollerit vaativat myös erillisen lisenssin, joka kattaa tietyn määrän tukiasemia. Aruba Instant ei itsessään vaadi erillistä lisenssiä, mutta se tarvitsee Aruban yhteensopivia tukiasemia. Koska yhden tukiaseman on hoidettava kontrollerin tehtävät, tämä asettaa suuren kuorman tukiasemalle. Tämän vuoksi Aruba ei suosittele Instant-klusterin kooksi yli 128:aa tukiasemaa. [25]

6 Toteutussuunnitelma

Projekti lähtee liikkeelle tilanteesta, jossa kampuksella on kaksi eri hallinnoitua langatonta verkkoa, eikä minkäänlaista vierailijaverkkoa. CSC:llä on vaatimus, että Funet-jäsenorganisaatiolla tulee olla eduroam-verkko saatavilla. Tavoitteena on tuottaa toiminnallinen eduroam-verkko, johon sekä omat käyttäjät että vierailijat voivat yhdistää.

Pääasiallinen suunnitelma koostuu kolmesta osasta. Ensimmäisessä vaiheessa perehdytään aiheeseen pääasiallisesti Aruba Instant -ympäristöön liittyvän dokumentaation avulla, ja muiden organisaatioiden raportteihin ja dokumentteihin eduroam-verkkoihin liittyen. Toisessa vaiheessa luodaan demoympäristö Kajaanin Ammattikorkeakoulun datacenter-laboratorioon samoilla laitteilla, joita varsinaisessa verkossa käytetään. Tässä vaiheessa ei voida testata yhteyksiä muiden organisaatioiden tunnuksilla, mutta paikallisen toiminnallisuuden onnistuminen on vaikein osa. Viimeisessä vaiheessa verkko pystytetään toimeksiantajan tuotantoympäristöön ja pyritään ottamaan käyttöön ennen vuoden 2018 syyslukukautta.

7 Käytännön toteutus

7.1 Aloitus

Opinnäytetyö käynnistyi maaliskuussa 2018. Tällöin sovittiin työn aiheesta, tavoitteista sekä alustavasta aikataulusta. Aiheen vierauden takia työn ensimmäiset viikot kuluivat aineistoon perehtyessä dokumentaation muodossa. Näihin lukeutuivat muun muassa Aruba Instant- sekä Aruba ClearPass -käyttöohjeet sekä CSC:n oma eduroam-opas. [25, 26, 27]

7.2 Testiympäristö

Aiheeseen perehtymisen jälkeen pystytettiin datacenter-laboratorioon testiympäristö, jossa laitteistoon ja niiden hallinnointiin pystyi tutustumaan ennen tuotantoympäristöön koskemista. Tavoitteena oli saada käyttäjäautentikointi toimimaan ensin paikallisesti ja myöhemmin testata ulkoverkkoon liittyvät yhteydet tuotantoympäristössä. Laitteistona toimi yksittäinen Aruban langaton tukiasema sekä virtualisoitu Aruba ClearPass -RADIUS-palvelin.

Asennus alkoi Aruba ClearPass Policy Managerin virtuaaliappliancen asennuksella. Asennus itsessään on hyvin yksinkertaista appliancella, ja asennuksen jälkeen oli heti mahdollista konfiguroida alustaa. Peruskonfigurointi koostui IP-osoitteen, hostnamen sekä DNS-osoitteiden asettamisesta. Tämän jälkeen ClearPass voitiin liittää Microsoft Active Directory domainiin käyttämällä komentoriviä. Konfiguroinnin jälkeen ClearPassiin oli mahdollista yhdistää verkkoselaimen avulla, jonka kautta myös loput konfiguroinnista tehtiin.

Ensimmäisenä verkkopaneelista oli kirjautumisen jälkeen syötettävä tarvittavat lisenssit. ClearPassin osalta kyse oli Platform-lisenssistä, joka sallii alustan käytön, sekä Access-lisenssi, joka sallii sääntöjen ja palveluiden luonnin. Tämän jälkeen siirryttiin testikäytössä olevaan langattomaan tukiasemaan. Instant-ympäristön tukiasemilla on oma verkkohallintapaneelinsa, johon pystyi yhdistämään heti tukiaseman käynnistyttyä ja sen oletusverkkoon liityttyä. Heti ensimmäisenä tuli luoda uusi verkko, sillä oletuksena oleva verkko on täysin suojaton, eikä se ole muokattavissa. Uuden verkon luonnin jälkeen asetettiin halutut VLAN (Virtual Local Area Network) -asetukset, jotta eri käyttäjäryhmät voidaan lokeroida paremmin, ja täten parantaa tarvittaessa tiettyjen käyttäjäryhmiten tietoturvaa. Näiden asetusten myötä VLAN-hallinta

voidaan toteuttaa ClearPassin päässä, sillä Aruban teknologioina ne voivat helposti toimia keskenään. Verkko asetettiin myös käyttämään asennettua ClearPass-palvelinta RADIUS-autentikointipalvelimena.

Seuraavaksi tehtiin tarkempaa konfigurointia Clearpassin puolelta. Ensimmäisenä luotiin Clearpassiin laiteryhmä, jota voidaan käyttä autentikointisäännöissä. Tähän ryhmään asetettiin käytetty tukiasema. Toisena ryhmänä oli Funet eduroam proxy -palvelimet. Seuraavana luotiin Clearpassin käyttämät palvelin- sekä palvelusertifikaatit. Tämän jälkeen luotiin itse palvelusäännöt, joiden avulla käyttäjä pystytään tunnistamaan käyttäjätunnuksen perusteella, ja asettamaan käyttäjä haluttuun VLAN:iin eri attribuuttien avulla. Eri palveluiden luonnin jälkeen luotiin asennusprofiili käyttäen Eduroam CAT -ympäristöä. Profiilin luonti vaati käytetyn CA-sertifikaatin sekä käytetyt EAP-tyypit, ja muita haluttuja tietoja. Testiympäristön tarkemmat toteutusvaiheet löytyvät liitteestä 1.

7.3 Tuotanto

Eduroam-verkko siirrettiin tuotantoon toukokuussa 2018, ja se sujui pääsääntöisesti ongelmitta käyttäen testivaiheessa tuotettua dokumentaatiota. Tuotantoon viennin jälkeen tuotettiin myös käyttäjille suunnattu ohje siitä, kuinka he voivat liittää omat laitteensa verkkoon. Tämä dokumentti löytyy liitteestä 2. Verkon varsinainen käyttöönotto suoritettiin elokuussa 2018.

7.4 Ongelmat toteutuksessa

Vaikka työ sujui hyvin, ei ongelmilta vältytty täysin. Ensimmäinen ongelma syntyi testivaiheen lopulla, kun tukiasema ei tunnistanut verkkoon yhdistyneitä käyttäjiä, vaikka varsinainen RADIUS-tunnistautuminen onnistui. Tälle ongelmalle ei löytynyt ratkaisua, mutta se ei toistunut enää tuotannossa.

Toisena ongelmana oli ulkoverkosta tulevat KAMK:in käyttäjien autentikoinnit. Näissä tapauksissa autentikointiyritys ei koskaan tullut RADIUS-palvelimelle saakka. Tämän ratkaisuna oli lopulta käyttäjätunnuksen @domain päätteen vaihtaminen, sillä CSC suodattaa listan hyväksytyistä organisaatioista, ja täten autentikointipyynnöt jäivät kiinni. Tämän muutoksen jälkeen autentikointi toimi ongelmitta.

8 Yhteenveto

Teoriaosuudessa selvitettiin eduroamin taustaa, sen toimintaperiaatteita sekä sen hyödyntämiä teknologioita. Työssä selvisi eduroamin käytön laajuus, sen ylläpitäjät sekä tietoa Aruban olemassaolevista verkkoteknologioista. Käytännön osuudessa eduroam-ympäristö asennettiin KamIT:in olemassa olevaan verkkoon Kajaanin ammattikorkeakoulun kampuksella. Käyttöönotto itsessään suoriutui ongelmitta, vaikkakin joihinkin ongelmiin törmättiin testiympäristön kanssa, mutta ne saatiin ratkaistua.

Eduroam-verkko on nähnyt käyttöä kampuksella erityisesti vierailijoiden keskuudessa, joten työ on ollut hyödyllinen. Myös työn aikana tuotettu dokumentaatio toimeksiantajalle on luotu onnistuneesti.

Toteutukseen ei luultavasti ole tarpeen tehdä suurempia muutoksia, mikäli verkkoinfrastruktuuria itsessään ei muuteta. Yksi mahdollinen jatkotoimi, mikäli toimeksiantaja sen jossain vaiheessa tarpeelliseksi näkee, on tietyille käyttäjäryhmille vaadittava käyttäjäsertifikaatti. Tämän suhteen työ keskittyisi lähinnä sertifikaattien luomiseen ja jakeluun.

Lähteet

[1] Kyberturvallisuuskeskus. Langattomasti, mutta turvallisesti. 2014.

[2] Strengell,V. Langaton vierailijaverkko. 2012.

[3] Mercer,D. Global Connected and IoT Device Forecast Update. 2019.

[4] Bittau,A, Handley,M, Lackey,J. The final nail in WEP's coffin.
2006.

[5] How does Wi-Fi Protected Setup work? https://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work Viitattu 6.1.2020.

[6] Langattomien verkkojen suojauksessa käytetty WPS-tekniikka murtuu helposti. 2012; https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2012/01/ttn201201041606.html Viitattu 6.1.2020.

[7] Hoffman C. Wi-FI Protected Setup (WPS) is Insecure: Here's Why You Should Disable It
. 2017; https://www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why-you-should-disable-it/ Viitattu 6.1.2020.

[8] Wi-Fi Alliance Introduces Next Generation of Wi-Fi Security. 2004; https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-next-generation-of-wi-fi-security Viitattu 6.1.2020.

[9] Viestintävirasto julkaisi varoituksen WiFi-verkkojen salauksessa paljastuneista haavoittuvuuksista. 2017;
https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/10/ttn201710161625.html Viitattu 6.1.2020.

[10] eduroam and GÉANT. https://www.eduroam.org/eduroam-and-geant/ Viitattu 10.5.2018.

[11] eduroam About. https://www.eduroam.org/about/ Viitattu 10.5.2018.

[12] Where can I eduroam? https://www.eduroam.org/where/ Viitattu 10.5.2018.

[13] Verkkoon myös kampuksesi ulkopuolella
. https://www.eduroam.fi/verkkoon-kampuksen-ulkopuolella Viitattu 10.5.2018.

[14] Funet-runkoverkko. https://wiki.eduuni.fi/display/funet/Funet-runkoverkko Viitattu 12.5.2018.

[15] Palvelut. https://wiki.eduuni.fi/display/funet/Palvelut Viitattu 12.5.2018.

[16] NORDUnet member networks. https://www.nordu.net/content/nordunet-member-networks Viitattu 12.5.2018.

[17] GÉANT. https://www.nordu.net/content/g%C3%A9ant.

[18] Wierenga,K, Florio,L. Eduroam: Past, present and future. 2005.

[19] Rigney,C, Willens,S, Rubens,A, Simpson,W. Remote Authentication Dial In User Service (RADIUS). 2000.

[20] Rigney,C. RADIUS Accounting. 2000.

[21] IEEE 802.1X-2010 - IEEE Standard for Local and metropolitan area networks- Port-Based Network Access Control. 2010.

[22] 802.1X Overview and EAP Types. https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html Viitattu 22.5.2018.

[23] What is an SSL certificate. https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/ Viitattu 8.4.2019.

[24] Mareco D. Controller vs. Controllerless Wifi: What's the Difference? 2013; https://www.securedgenetworks.com/blog/controller-vs-controllerless-wifi-whats-the-difference.

[25] Aruba Instant 6.5.4.0 User Guide.

[26] Aruba ClearPass Policy Manager 6.6 User Guide.

[27] eduroam-verkkovierailu
. https://wiki.eduuni.fi/display/funet/eduroam-verkkovierailu Viitattu 10.9.2018.

Liiteluettelo

Liite 1 – Eduroam admin guide

Liite 2 – Eduroam user guide

Liite 1: Eduroam Admin Guide

Eduroam

Admin Guide

Sisällys

1 Johdanto

Tässä dokumentissa käydään läpi Eduroam-verkon pystytys Aruba Instant -ympäristöön Clearpassin kanssa. Ohjeissa käydään läpi vaihe vaiheelta verkon luonti tukiasemalle, Clearpassin asennus ja konfigurointi, sekä viimeisenä eduroam CAT-palvelun käyttö.

2 Järjestelmävaatimukset

Clearpass virtual appliance:

CLABV (Evaluation)	
Prosessori	2 ydintä
RAM	6 GB
Levytilaa	80 GB

C1000V	
Prosessori	8 ydintä
RAM	8 GB
Levytilaa	1000 GB
Verkkoyhteys	2 kpl Gigabit liitäntää
Levynopeus (IOP)	Read/Write 40-60, 4K random 75

C2000V	
Prosessori	8 ydintä
RAM	8 GB
Levytilaa	1000 GB
Verkkoyhteys	2 kpl Gigabit liitäntää
Levynopeus (IOP)	Read/Write 40-60, 4K random 105

C3000V	
Prosessori	24 ydintä
RAM	64 GB
Levytilaa	1800 GB
Verkkoyhteys	2 kpl Gigabit liitäntää
Levynopeus (IOP)	Read/Write 40-60, 4K random 350

Lisäksi verkkoon vaaditaan jokin käyttäjätietokanta ja domainpalvelu, kuten Microsoft Active Directory.

3 Clearpassin asennus

Aloita asennus luomalla Clearpassin virtual appliance. Luonnin jälkeen appliancelle täytyy lisätä halutun version (C1000V, C2000V, C3000V) vaatimat laiteresurssit, mikäli ne eivät vastaa oletuksia. Tämän jälkeen käynnistä appliance, ja etene alkukonfigurointiin. Clearpassin oletus käyttäjätunnukset ovat käyttäjänimi appadmin, ja salasanana eTIPS123.

3.1 Peruskonfigurointi ja domain

Kuva 1 - Peruskonfigurointi

Ensimmäisen kirjautumisen yhteydessä tulee tehdä peruskonfigurointi. Tässä syötetään palvelimen hostname ja muut verkkoasetukset. Mikäli palvelimen kanssa käytetään kahta verkkokorttia, voidaan liikenne jakaa Management ja Data –verkoille erikseen. Täten hallintaverkon voi pitää erillisenä, ja normaali RADIUS-liikenne tulee toisen verkon kautta. Aseta DNS-palvelimeksi käytetyn domainin IP.

Tämän jälkeen appliancen voi liittää domainiin käyttämällä komentoa ad netjoin <domaincontroller.domain>.

Kuva 2 - Clearpassin liittäminen domainiin

3.2 Verkkopaneeli ja lisenssit

Peruskonfiguroinnin jälkeen Clearpassin verkkopaneeliin tulisi päästä asetetusta management IP:stä. Tänne kirjaudutaan käyttäjänimellä admin, ja salasanalla joka annettiin konfiguroinnin yhteydessä. Clearpass todennäköisesti vaati heti lisenssiä, ja tämän tulee olla Clearpassin Platform-lisenssi, tämä sallii alustan käytön. Lisäksi, verkkopaneeliin päästyä kannattaa myös lisätä Access-lisenssi, joka sallii sääntöjen ja palveluiden luonnin.

4 Instant-verkon asennus

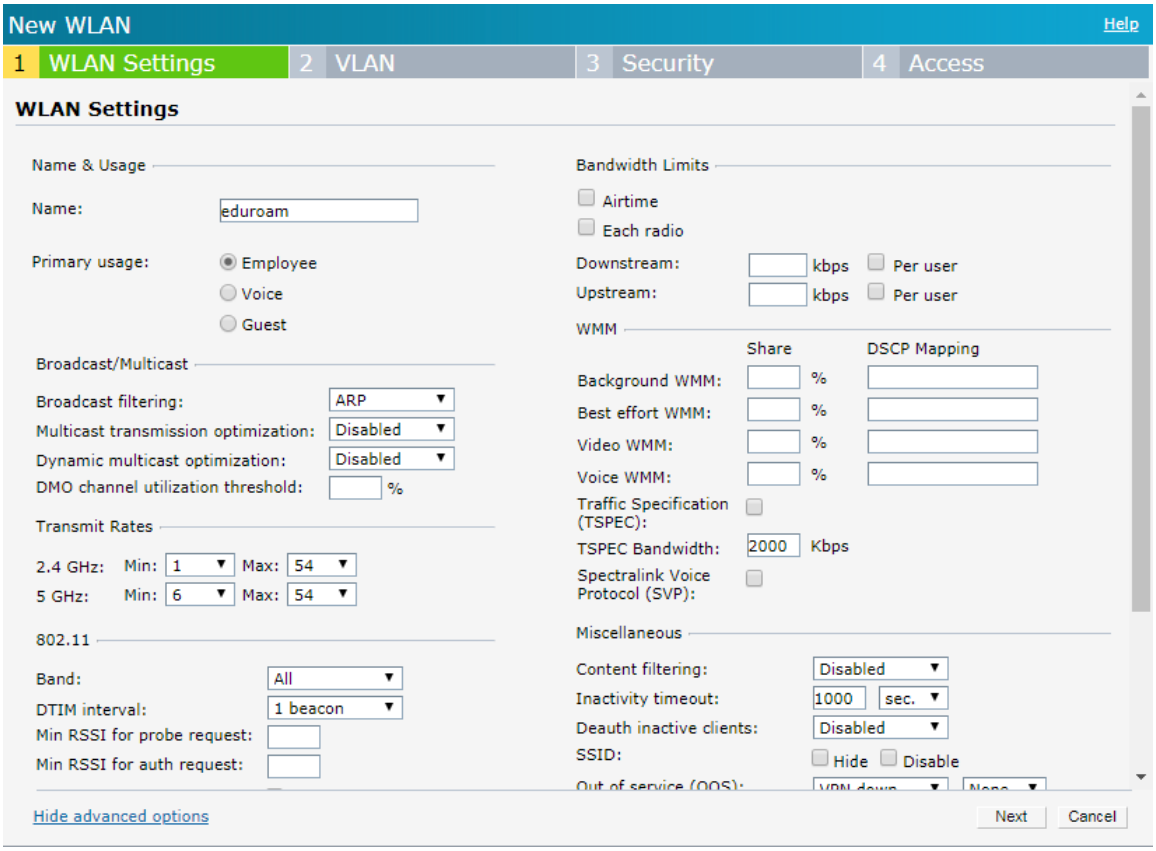
Liitä käytetty tukiasema verkkoon. Tämän jälkeen hallintapaneeliin pääsee kiinni laitteen IP-osoitteella, tai yhdistämällä sen oletuksella broadcastaavaan Instant-SSID:hen. Myös konsoliportin kautta hallitseminen toimii, mikäli hallinnan haluaa suorittaa komentoriviltä. Mikäli laitteeseen yhdistää sen oletusverkon kautta, se aina uudelleenohjaa osoitteeseen http://instant.arubanetworks.com, joka on sen hallintapaneeli. Oletustunnukset tukiasemalle ovat käyttäjätunnus admin, ja salasana admin. Suosittelen uuden verkon luontia välittömästi, sillä oletusverkko on salaamaton, ja sitä ei voi muokata.

4.1 Eduroam-verkon luonti

Aloita painamalla ’New’ vasemmassa reunassa olevassa verkkopaneelissa. Tämä aukaisee ikkunan, jossa uutta verkkoa pääsee konfiguroimaan.

4.1.1 WLAN Settings

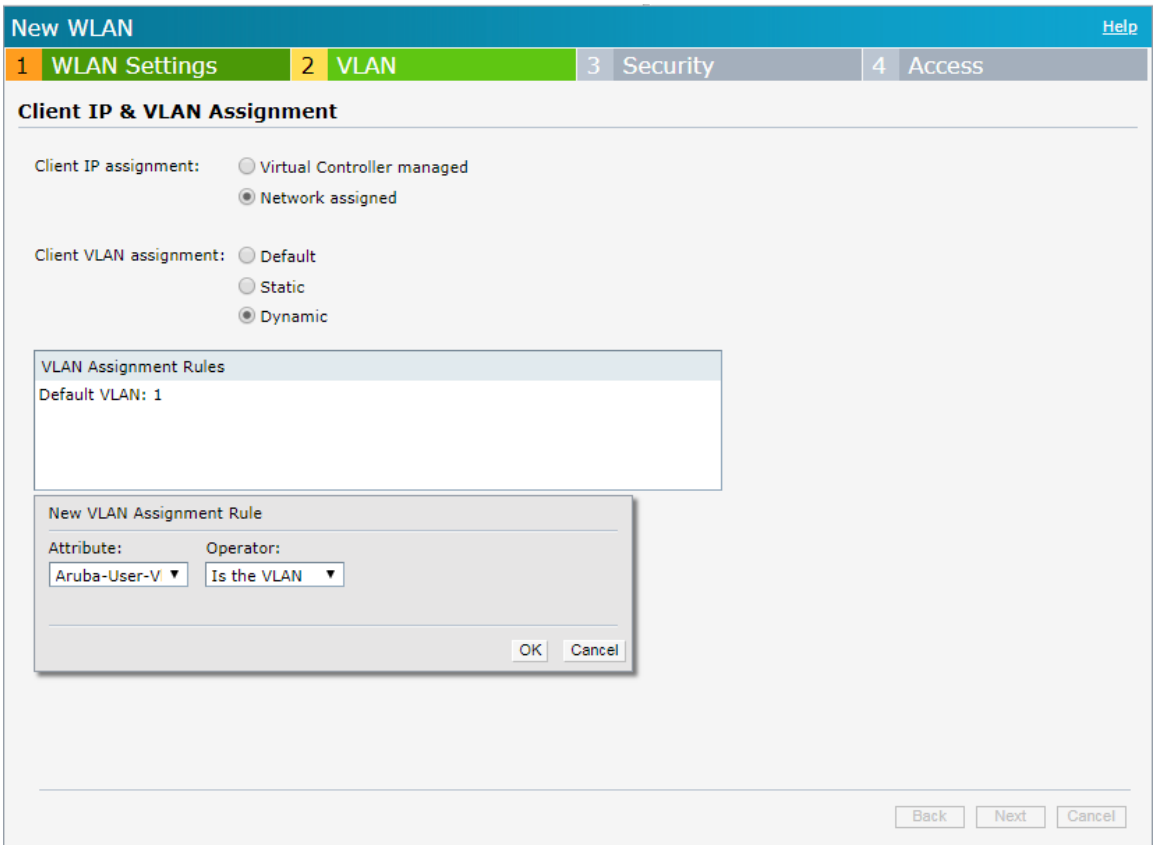
Ensimmäisenä välilehtenä on WLAN Settings, täällä voit asettaa verkon perusasetukset, kuten nimen, pääasiallisen käyttötarkoituksen, sekä Advanced Optionsin alta useita muista asetuksia. Täältä voi myös piilottaa SSID:n. Eduroam-verkon kohdalla aseta nimeksi eduroam, ja jätä pääasiallinen käyttö ’Employee’-tilaan.



Kuva 3 - WLAN Settings -välilehti

4.1.2 VLAN

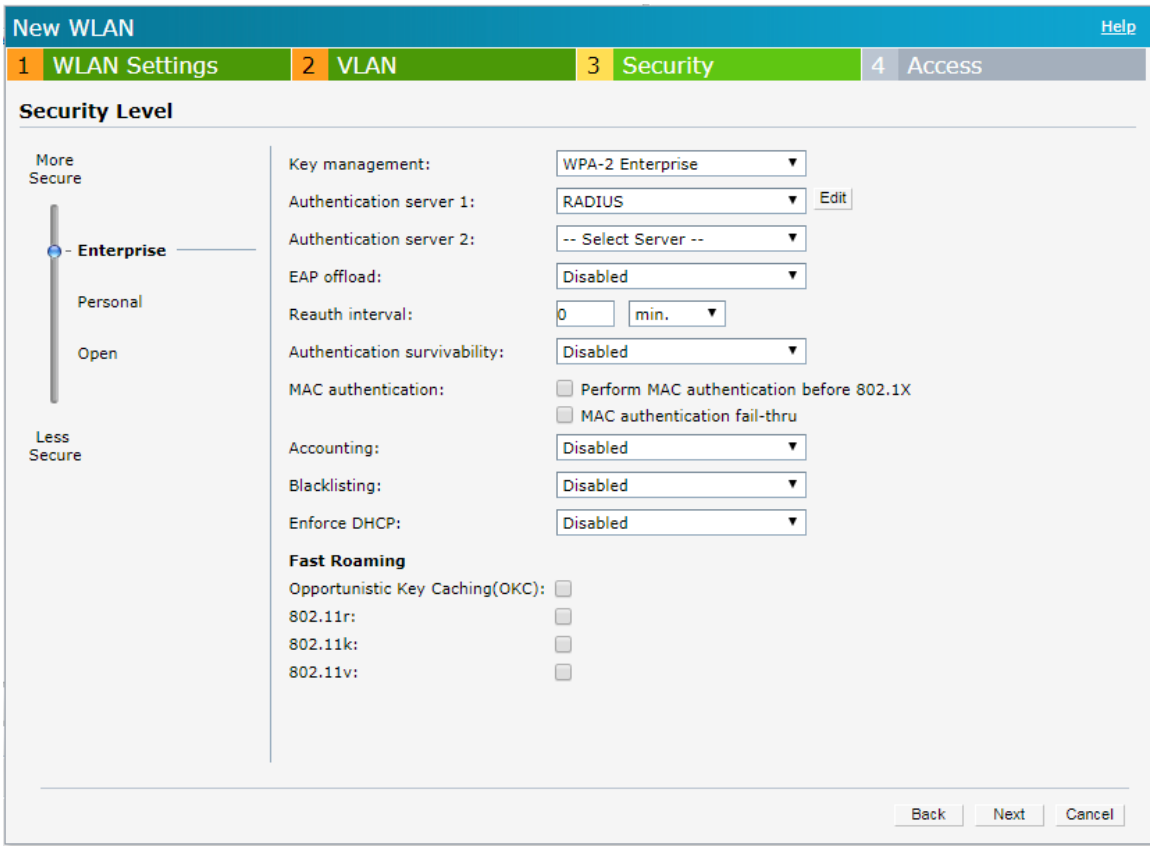
VLAN-välilehdeltä löytyvät käyttäjien IP ja VLAN asetukset. Aseta ’Client IP assignment’ Network assigned asetukselle, mikäli halutaan käyttää ulkoista DHCP-palvelinta, tai Virtual Controller managed, mikäli halutaan tukiaseman itse hoitavan DHCP-tehtävät. ’Client VLAN assignment’:illa voidaan hallita mihin VLAN:iin käyttäjät asetetaan. Default asetus käyttää asetettua oletus VLANia kaikille käyttäjille, Staticilla voidaan määrittää jokin tietty ei-oletus VLAN, ja Dynamic asetuksella voidaan määritellä käyttäjän VLAN erilaisita säännöistä riippuen. Eduroam-käytössä halutaan verkon hallitsema jadynaaminen, mikäli eri käyttäjäryhmät ovat eri VLANeissa. Tämän jälkeen voidaan luoda sääntö VLAN-vaihtoja varten. Täydessä Aruba ympäristössä voidaan käyttää Aruba-User-VLAN attribuuttia, ja operaattorina ’Is the VLAN’, täten käyttäjän VLAN muutetaan Clearpass sääntöjen perusteella.



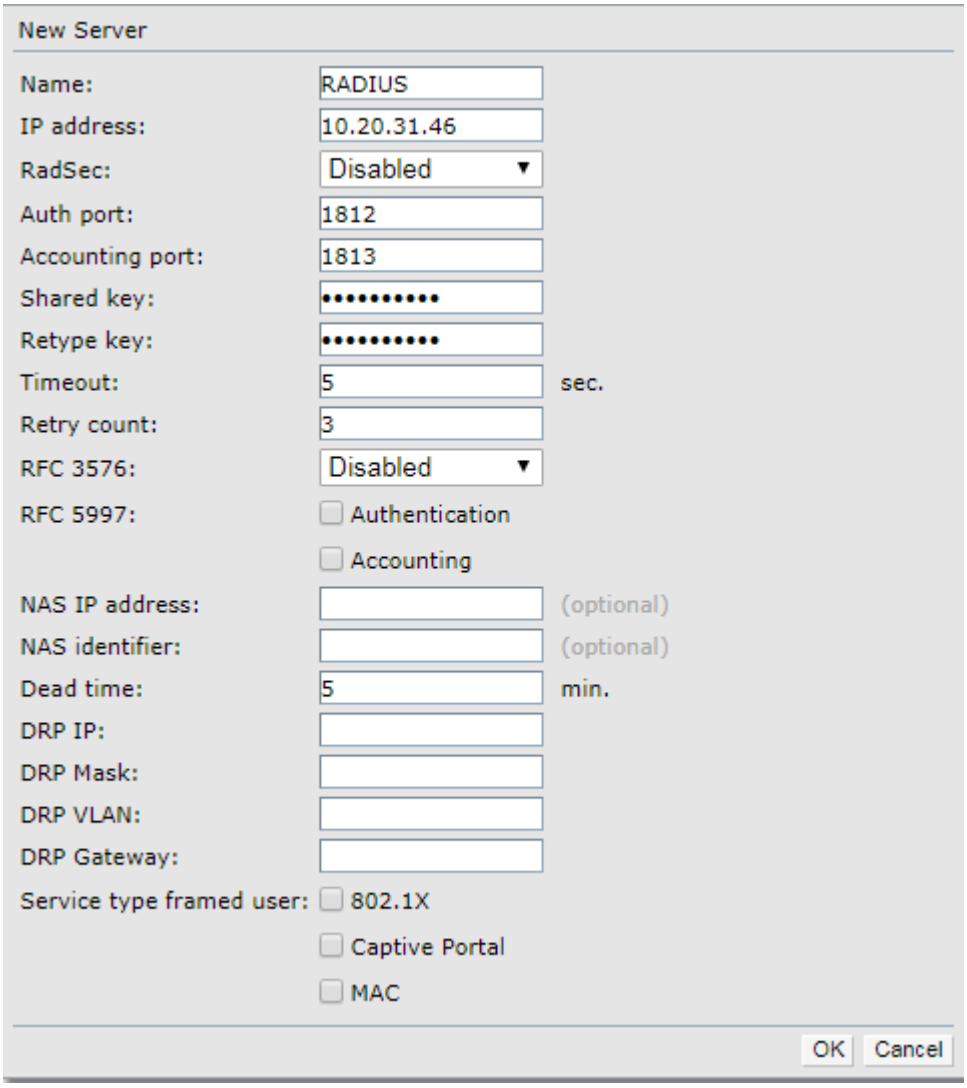
Kuva 4 - VLAN-välilehti

4.1.3 Security

Security-välilehdellä voidaan asettaa verkon turvallisuusasetuksia. Eduroam-käytössä halutaan Enterprise-taso, ja suojaustavaksi WPA-2 Enterprise. Valitse ’Authentication server 1’:ksi uusi palvelin, ja anna sille kuvaava nimi. Tämä palvelin on autentikointiin käytettävä RADIUS-palvelin, tässä tapauksessa Clearpass. Anna IP-osoitteeksi Clearpassin IP. Auth ja Accounting portit voi jättää oletukseksi tai vaihtaa halutessa, mutta tulee huomioida että ulkoa tulevat RADIUS-pyynnöt tulevat näihin portteihin Clearpassille, joten niiden kannattaa olla oletuksena. Aseta palvelimelle jokin Secret key, tällä Clearpass ja tukiasema varmentavat toisensa. Tämä tulee syöttää myös myöhemmin Clearpassissa. Enforce DHCP – asetuksella voidaan halutessaan estää staattisten IP-osoitteiden käyttö.



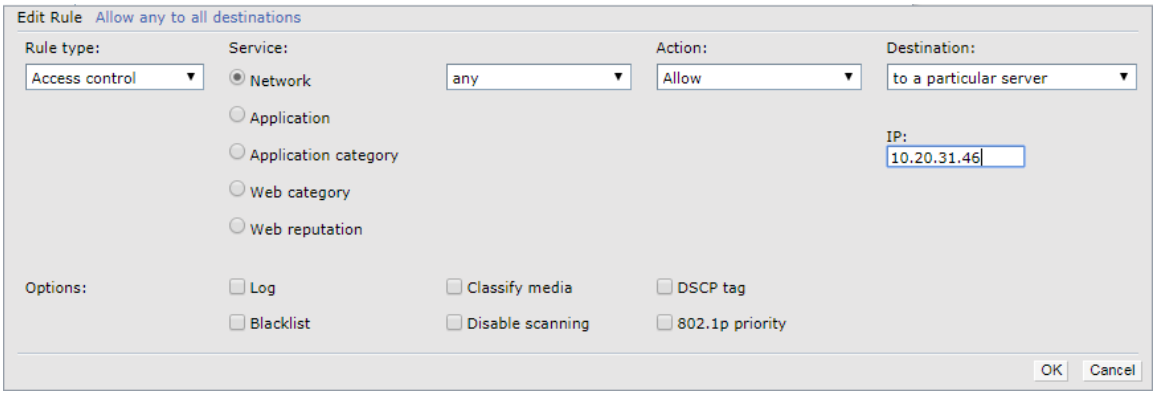
Kuva 5 - Security-välilehti



Kuva 6 - Uuden autentikointipalvelimen lisäys

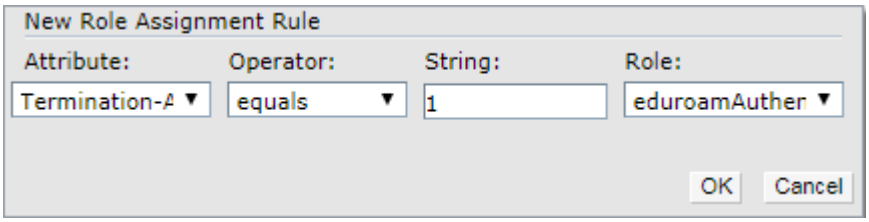
4.1.4 Access

Access välilehdellä voidaan luoda sääntöjä eri käyttäjärooleille, jolloin niiden pääsyä eri verkkopalveluihin voidaan rajata. Vaihda tasoksi Role-based, ja valitse roolilistalta SSID:tä vastaava rooli, tässä tapauksessa eduroam. Valitse olemassa oleva sääntö Access Rules -listalta, ja paina Edit. Täältä rajaa sääntö muotoon, jossa Rule typenä on Access control, servicenä Network, ja säännön muoto on any, allow, to a particular server. Näin autentikoimattoman käyttäjän liikenne voidaan rajata vain tiettyyn palvelimeen, kuten RADIUS-palvelimelle, jolloin vain autentikointiliikenne voi tapahtua. Aseta IP:ksi Clearpassin IP.



Kuva 7 - Access Control -sääntö

Tämän jälkeen luo listaan uusi rooli. Aseta roolin nimeksi eduroamAuthenticated, ja aseta sille sääntö joka sallii kaiken liikenteen kaikkialle. Tämän jälkeen aseta alareunassa olevasta Role Assignment Rulesista uusi sääntö, ja aseta säännön attribuutiksi Termination-Action, operaattoriksi equals, stringiksi 1, ja rooliksi eduroamAuthenticated. Näin käyttäjälle annetaan oikeudet autentikoinnin tapahduttua. RADIUS-terminointi lähtetään myös autentikoinnin epäonnistuessa, mutta tällöin myös yhteys katkaistaan välittömästi.

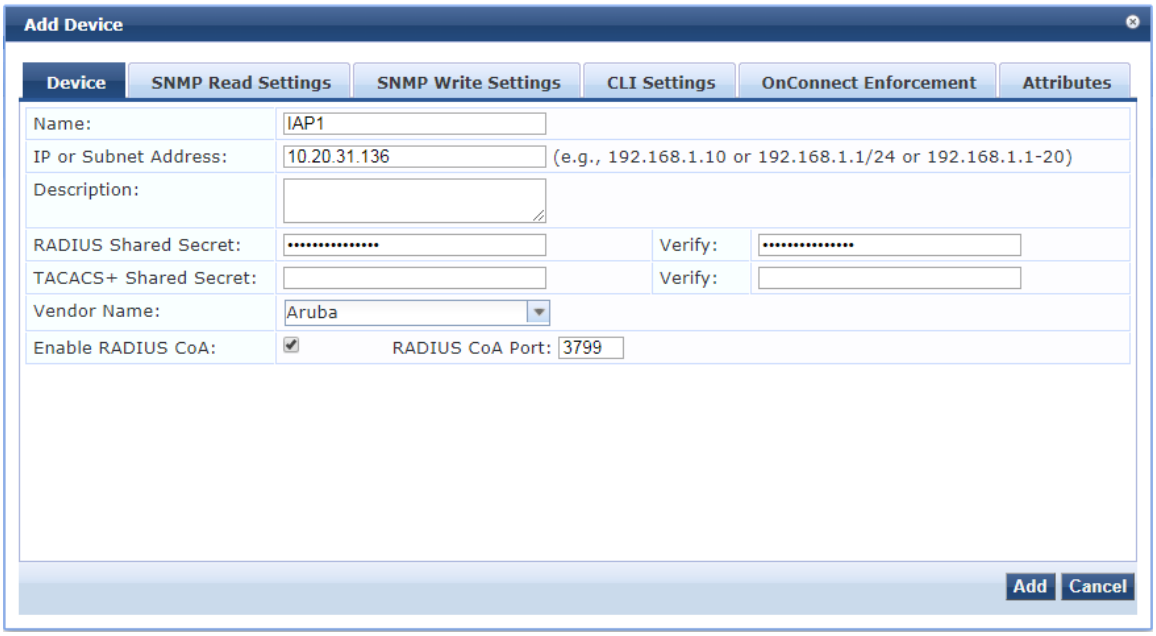


Kuva 8 - Role Assignment -sääntö

5 Clearpass-konfigurointi

5.1 Laitteiden yhdistäminen

Clearpassin hallintapaneelista, Configurationin alta löytyy Network-alavalikko, ja sen alta devices. Tällä sivulla voidaan lisätä laitetietoja Clearpassiin, kuten tukipisteitä tai controllereja. Tätä voi hyödyntää myöhemmin sääntöjen kanssa. Add-painikkeen kautta voit lisätä uuden laitteen, ja antaa siitä tarvittavat tiedot; Nimen, IP-osoitteen, kuvauksen sekä tukiaseman konfiguroinnin yhteydessä annetus RADIUS Shared Secretin. Instant-verkon tukiasemien osalta voi käyttää joko tukiasemien omia osoitteita, tai esimerkiksi master-tukiaseman local controlleria. Tällöin voidaan vähentää tarvittavien laitelisäysten määrää, ja verkkoa voidaan kasvattaa ilman tarvetta muuttaa Clearpass sääntöjä. Tähän voi myös käyttää Clearpassista löytyvää Network Scan –toimintoa, joka sallii tietyn aliverkon laitteiden skannaamista.

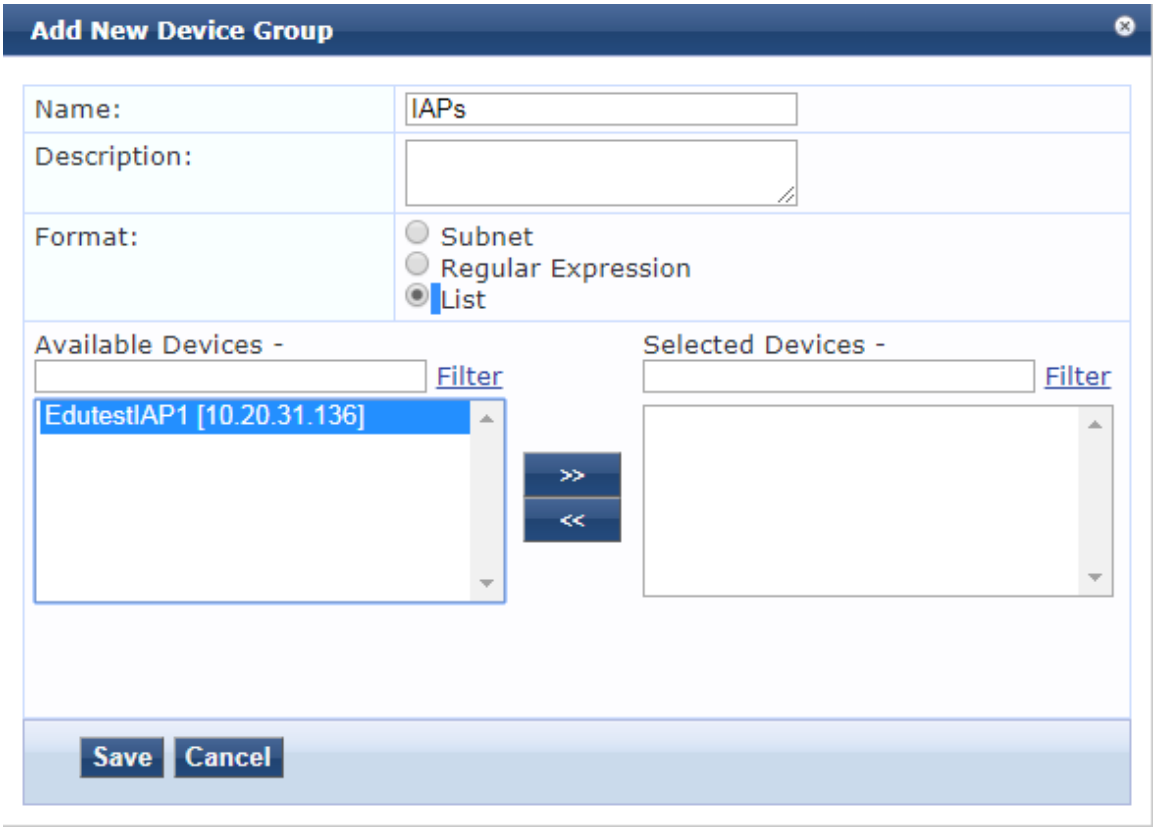


Kuva 9 - Uuden laitteen liittäminen

Lisää myös Funetin Eduroam proxy –palvelimet listaan.

Tämän jälkeen Device Groupsista voi luoda uuden ryhmän yhdistetyistä laitteista. Nämä voivat olla aliverkkoja, regular expression –muotoisia, tai laitelistoja. Aliverkolla ryhmään kuuluvat kaikki lisätyt laitteet, jotka kuuluvat tiettyyn aliverkkon. Regular expressionilla voidaan luoda kaava, johon sopivat laitteet valitaan. Listalla voi manuaalisesti valita

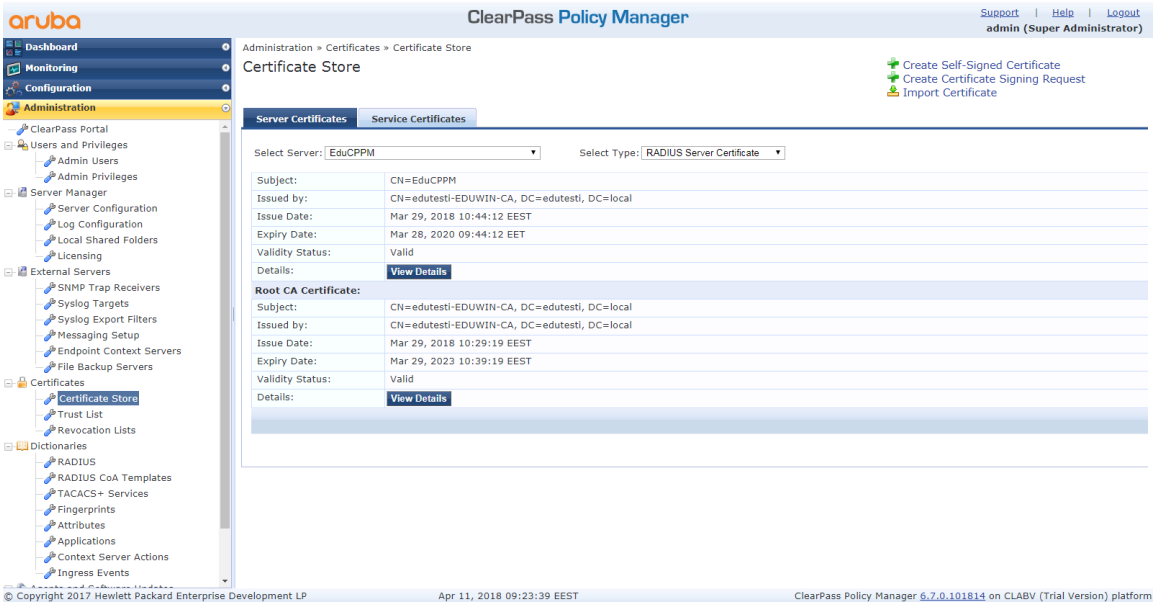
halutut laitteet. Luo ryhmät sekä access pointeille tai WLAN controllereille, ja Funetin eduroam pxoryille.



Kuva 10 - Laiteryhmän luonti

5.2 Sertifikaatit

Administrationin alta löytyy sertifikaattien alavalikko, Certificate Storen kautta voidaan tarkastella voimassa olevia sertifikaatteja, ja luoda uusia tarvittaessa. Sertifikaatit ovat välttämättömiä RADIUS-autentikoinnissa. Luo uusi sertifikaattipyyntö, ja vahvista se halutulla CA:lla. Luo sekä palvelin-, että palvelusertifikaatti. CA-sertifikaatti tulee myös jakaa käyttäjille, jotta autentikointi onnistuu. Tarkista myös Trust Listista, että ladattu palvelinsertifikaatti on luotettu.



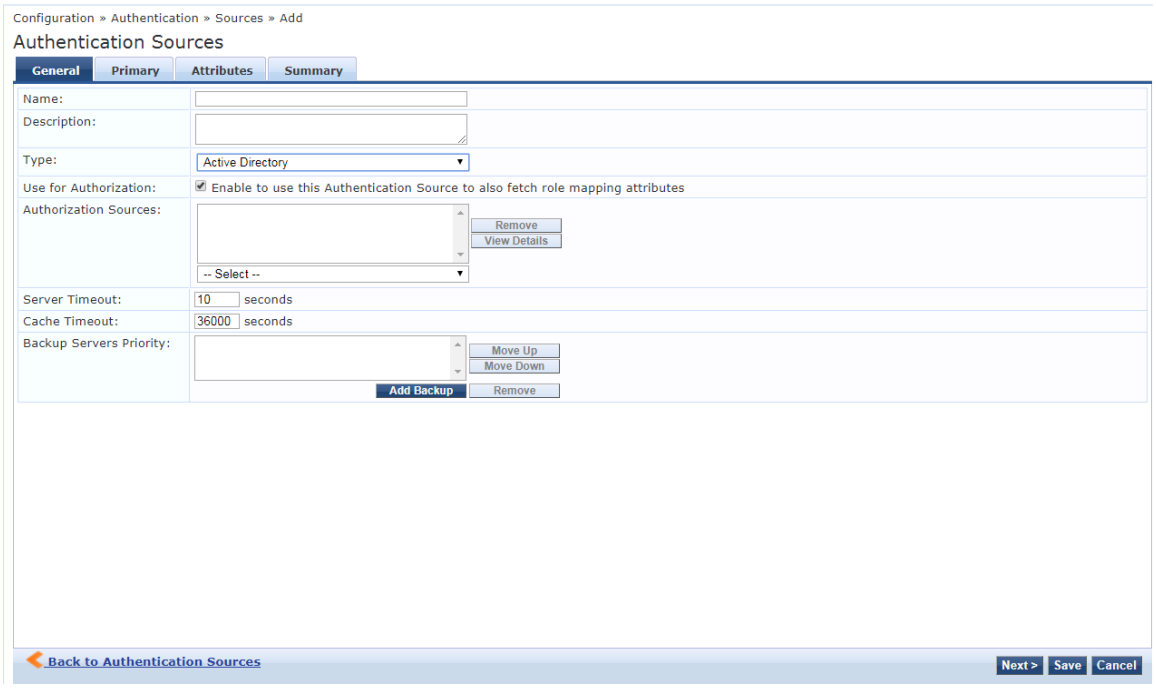
Kuva 11 - Sertifikaattisivu

5.3 Authentication Source

Clearpassin autentikointilähteen lisääminen tapahtuu Configuration sivun alta, Authentication alavalikosta Sourcesista. Aloita uuden lähteen lisääminen painamalla New.

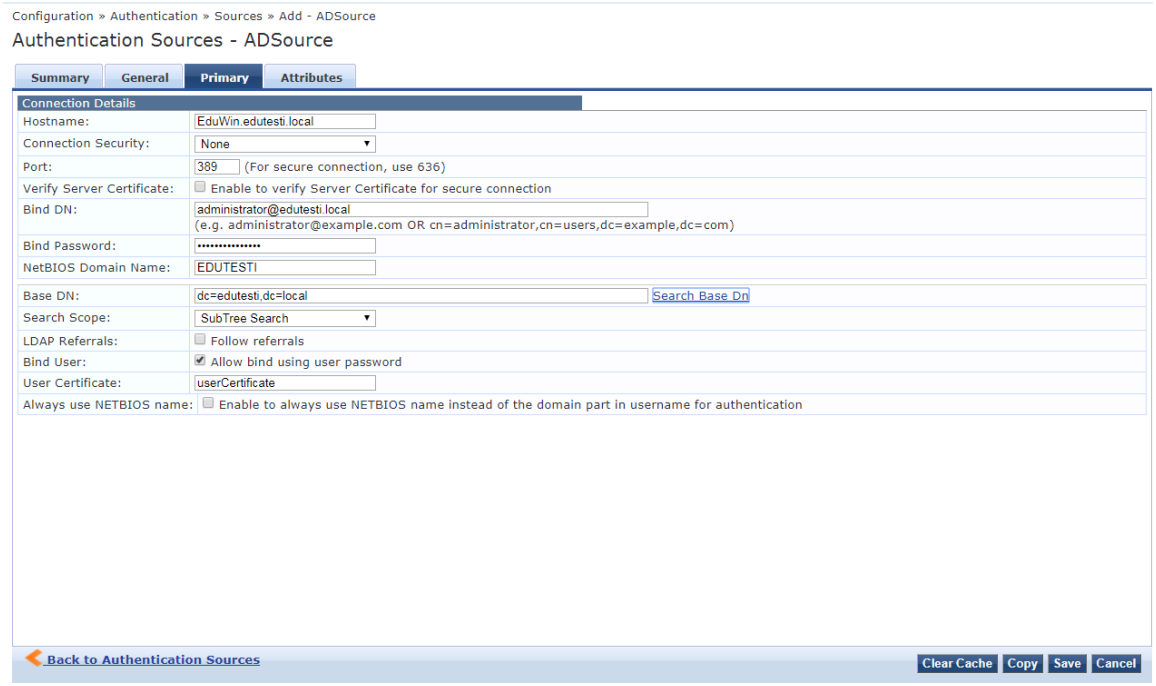
5.3.1 AD-lähde

Anna lähteelle nimi ja kuvaus. Valitse tyypiksi käytetty autentikointilähde. Tässä esimerkissä käytetään AD:ta. Varmista että ’Use for Authorization’ asetus on valittuna, ja siirry Primary-välilehdelle.

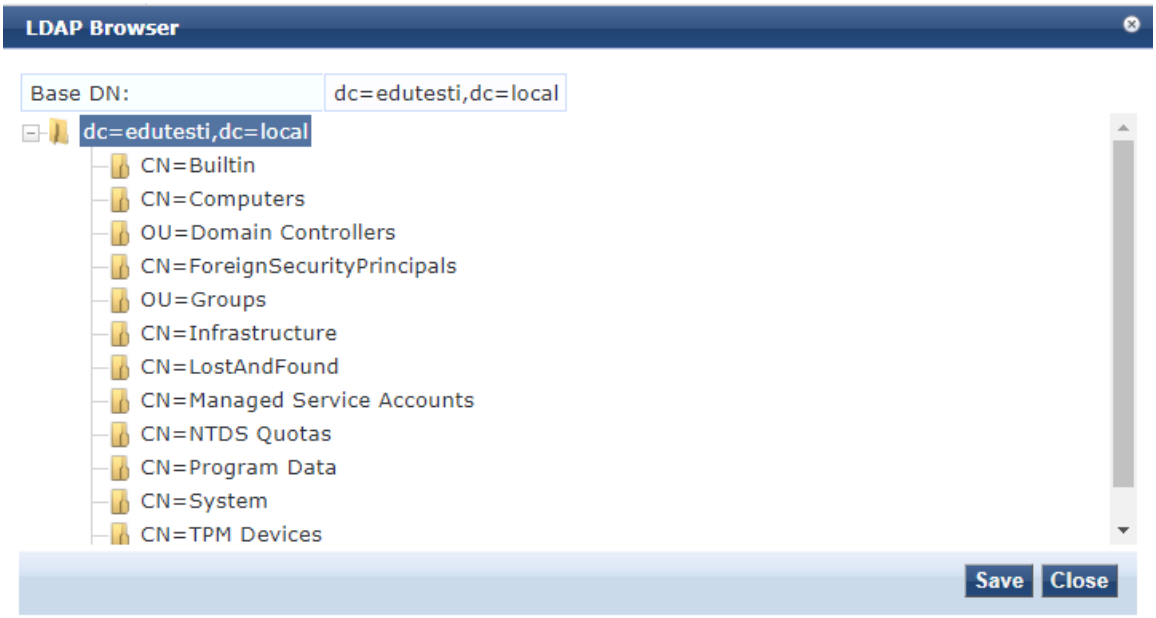


Kuva 12 – General-välilehti

Primary-välilehdellä annetaan tarvittavat tiedot AD-yhteyteen. Anna hostnameksi AD:ta hallinnoiva palvelin, muodossa <hostname.domain>. Connection Securitystä voi halutessaan valita StartTLS- tai AD over SSL –suojauksen, jos näitä käytetään.Verify Server Certificate –asetuksella voit pakottaa yhteyden varmistamaan palvelin sertifikaatin lisäsuojauksen saamiseksi. Bind DN –asetukseen tarvitaan Administrator-tilin tiedot. Tämä voi olla alla annetuissa muodoissa, AD:n kanssa on mahdollista käyttää muotoa <käyttäjänimi@domain>. Anna käyttäjän salasana Bind Password kohdassa. Aseta domainin NetBIOS –nimi NetBIOS Domain Name asetukseen. Mikäli yhteys toimii, voit valita Base DN:n käyttämällä ’Search Base Dn’ asetusta. Tämä antaa graafisen näkymän josta valita. Tässä on hyvä valita ylin haara, jonka alla kaikki käyttäjät jotka halutaan autentikoida ovat. Search Scopella voidaan muuttaa kuinka kaukaa autentikointi etsii käyttäjää. Base Objectilla se hakee vain valitulta tasolta, One Levelillä valitulta tasolta ja yhdeltä alempaa, ja SubTree Searchilla se hakee valitulta tasolta, ja kaikilta alemmilta. Näiden asetusten tulisi riittää AD:n osalta.



Kuva 13 - Primary-välilehti

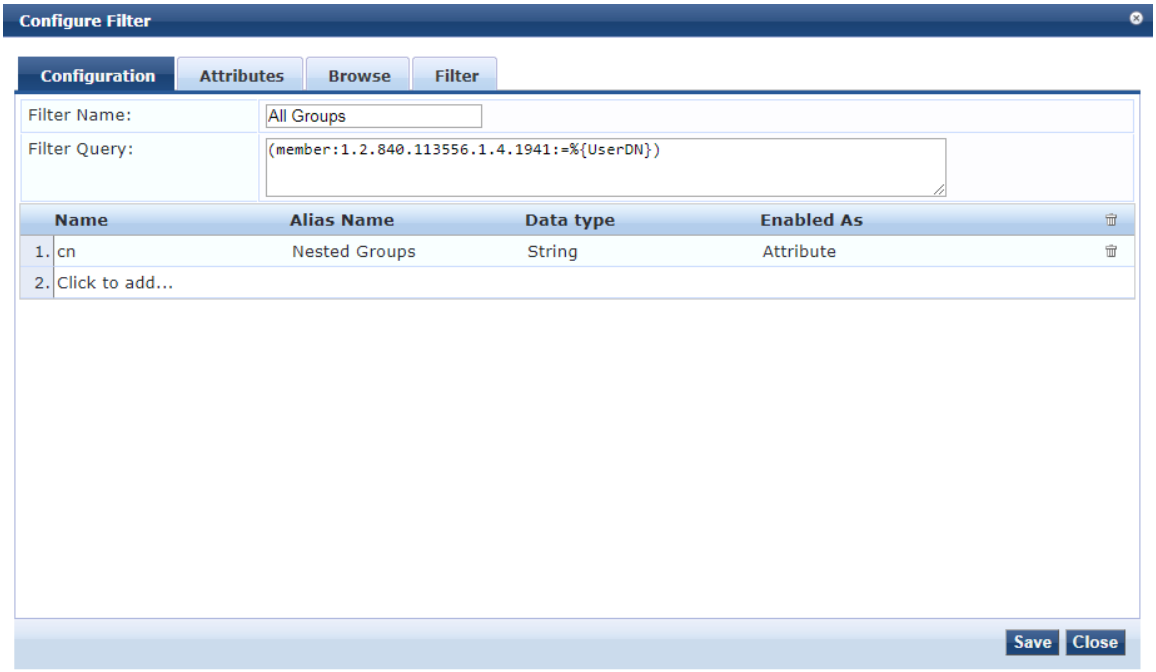


Kuva 14 - Search Base Dn -asetuksen avaama valikko

Mikäli käytössä on sisäkkäisiä ryhmiä, joita haluaa käyttää, tarvitsee Attributes -välilehdelle luoda ylimääräinen filter. Paina oikeasta alakulmasta ’Add More Filters’, joka avaa konfigurointi-ikkunan. Siirry Configuration -välilehdelle. Anna filterille kuvaava nimi, ja aseta queryksi

(member:1.2.840.113556.1.4.1941:=%{UserDN}

Tämän jälkeen syötä muut tiedot alla olevaan listaan. Anna nimeksi ’cn’, alias name voi olla mitä tahansa, tämä näkyy attribuuttiryhmän nimenä yhdistämistiedoissa. Data tyypiksi String, ja Enabled As asetuksesta valitse Attribute.



Kuva 15 - Filterin konfigurointinäkymä

5.3.2 Eduroam proxyt

Lisätään toinen authentication source. Valitse sille tyypiksi RadiusServer. Lisää haluttu määrä backup palvelimia, tämän tulisi vastata Funetin proxyjen määrää. Aseta Primary-välilehdellä palvelimen osoite (IP tai hostname), portti sekä RADIUS secret. Tee sama kaikille backupeille. Attributes –välilehdelle asetetaan RADIUS Pre Proxy –attribuutiksi

Radius:IETF Operator-Name <domain>

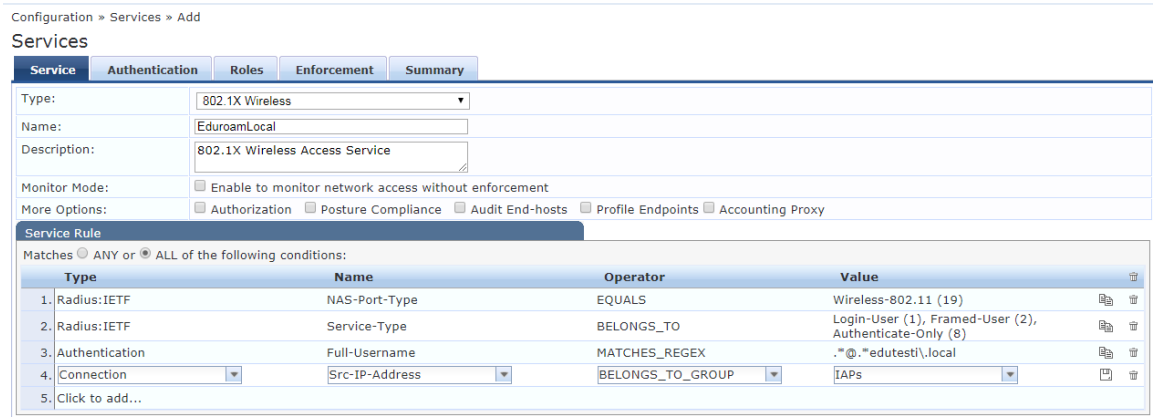
Autentikointilähteen tulisi olla tämän jälkeen valmis.

5.4 Servicet

Palveluiden luonti tapahtuu Configuration-valikosta, Services-sivulta. Luo uusi palvelu oikeasta yläkulmasta.

5.4.1 Local

Ensimmäisenä palveluna luodaan Local-palvelu, joka vastaa paikallisten käyttäjien autentikoinnista.



Kuva 16 - Service-välilehti

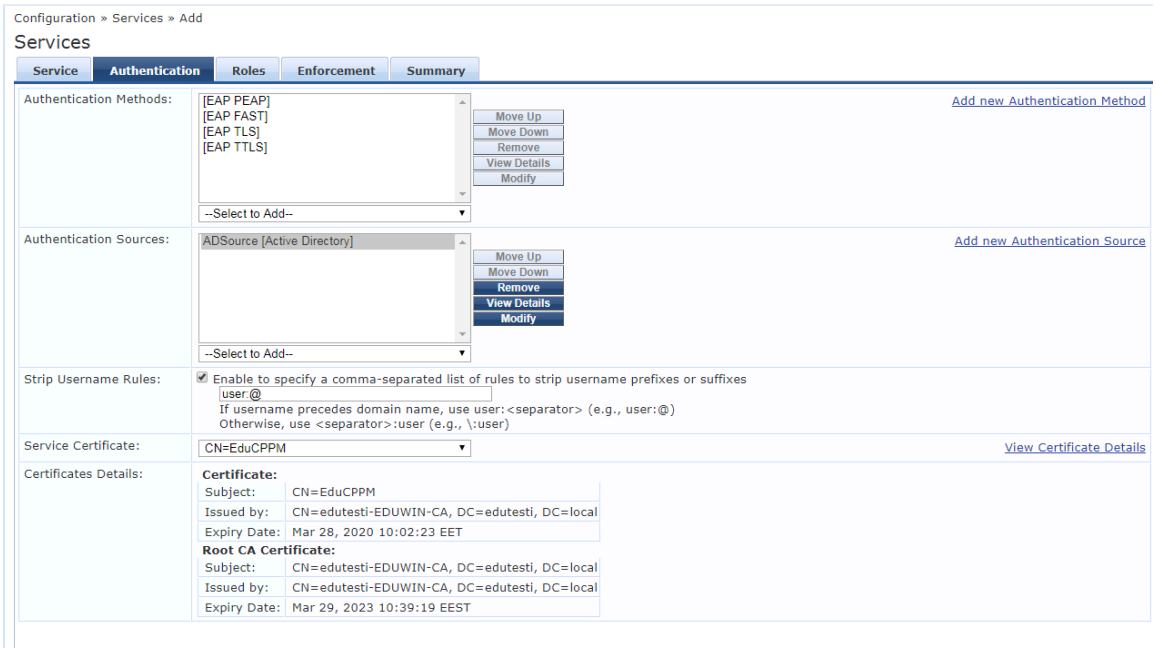
Valitse verkon tyypiksi 802.1X Wireless, ja lisää sääntöihin seuraavat säännöt:

Authentication Full-Username MATCHES_REGEX

ja kirjoita omaa domainia vastaava regular expression. Ota huomioon, että käyttäjänimi tulee olemaan muodossa user@realm. Kirjoita lisäksi sääntö:

Connection Src-IP-Address BELONGS_TO_GROUP <IAP-ryhmä>

IAP-ryhmään tulee kuulua joko tukiasemat, tai local controllerit, joiden kautta pyynnöt reititetään.

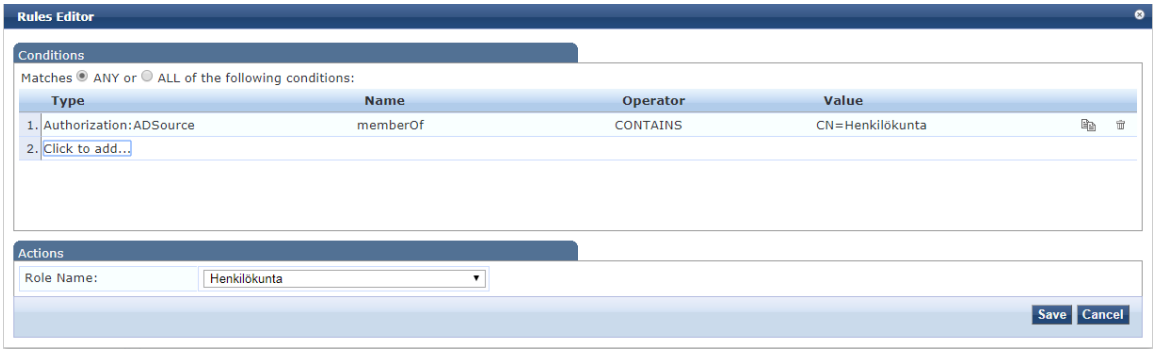


Kuva 17 - Authentication-välilehti

Authentication-välilehdellä voit asettaa mitä autentikointimenetelmiä RADIUS-palvelu käyttää. Näissä voi käyttää oletuksia, ellei näe tarvetta luoda omia. Menetelmissä tulee ottaa huomioon yhteensopivuus eri alustojen kanssa. Tiedot eri menetelmistä löytyy osoitteesta https://cat.eduroam.org ja ’About eduroam CAT’ –sivulta. Lisää Authentication Sourceksi aiemmin luotu AD-yhteys. Rastita ’Strip Username Rules’, ja laita säännöksi user:@, tällöin käyttäjänimet ovat halutussa muodossa. Lisäksi palvelulle on hyvä antaa sertifikaatti.

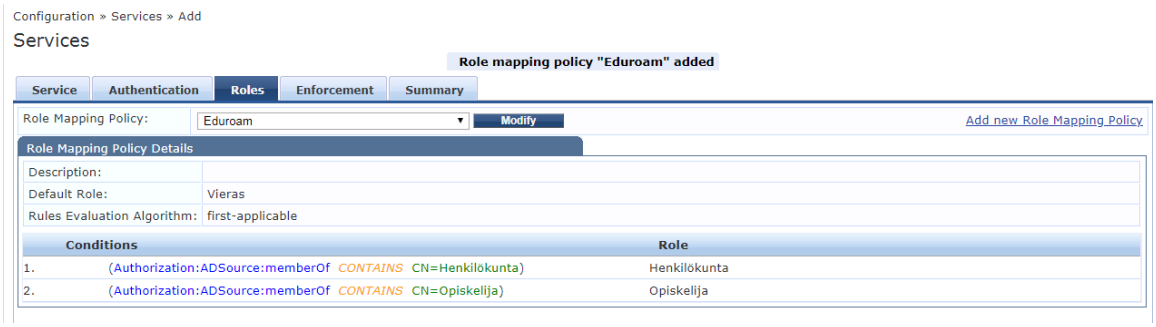
Roles-sivulla tehdään RADIUS-rooleihin liittyvät säännöt. Ensimmäisenä tarvitsee luoda Role Mapping Policy, luo uusi sivun oikeasta reunasta. Aseta policylle nimi, ja luo halutut roolit oikeasta reunasta, kuten Henkilökunta, Opiskelija sekä Vieras. Tämän jälkeen aseta haluttu rooli oletukseksi.

Rooleihin liittyvät säännöt luodaan Mapping Rules –välilehdeltä. Tänne lisätään säännöt, joiden perusteella käyttäjä voidaan eritellä ryhmiin. Painamalla Add Rule –painiketta, aukeaa säännön luonti ikkuna.



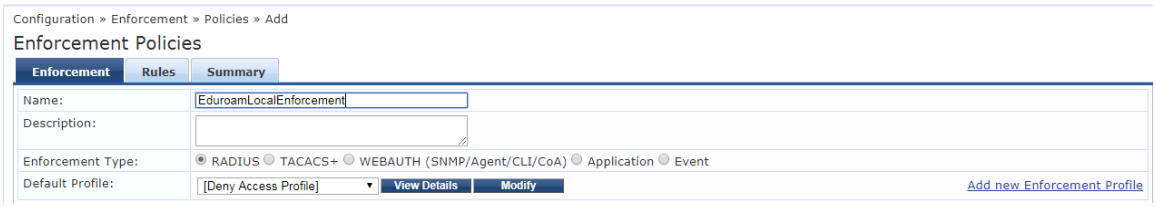
Kuva 18 - Role Mapping -säännön luonti

Valitse tyypiksi Authorization:ADSource, nimeksi memberOf, operaattoriksi Contains ja arvoksi CN=<AD-ryhmä>. Valitse alhaalta Actions-valikosta rooli, jonka haluaa käyttäjälle antaa jos sääntö täsmää. Luo vastaava sääntö kaikille ryhmille jotka halutaan erotella. Oletusrooli ei tarvitse sääntöä, sillä sitä käytetään jos mikään muu ei täsmää. Policyn tallentamisen jälkeen valitse se Roles-sivulta, ja luotujen sääntöjen tulisi näkyä sen alapuolella.



Kuva 19 – Roles-välilehti

Enforcement-välilehti toimii samalla tavalla kuin Roles. Luo uusi Enforcement Policy. Anna policylle kuvaava nimi ja kuvaus. Aseta oletusprofiiliksi Deny Access. Näin käyttäjät jotka eivät täsmää sääntöjä eivät saa palvelua. Luo samalla alhaalta Enforcement Profiilit eri hallinnoiduille käyttäjäryhmille. Aseta Device Group Listiin access pointeista tai kontrollereista koostuva ryhmä.



Kuva 20 - Enforcement Policies - Enforcement

Kuva 21 - Enforcement Profiilin säännöt

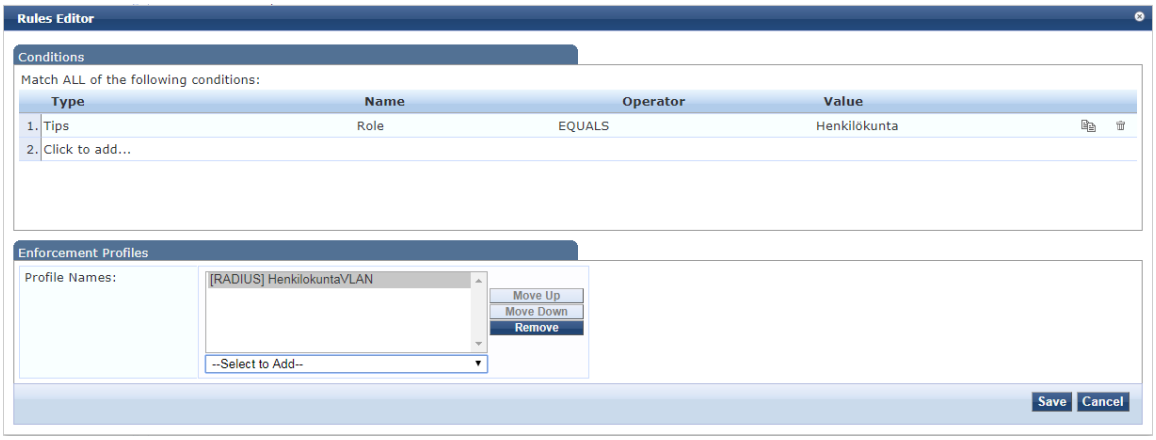
Aseta enforcement profiilin säännöiksi seuraavat:

Radius:IETF	Termination-Action	RADIUS-Request(1)
Radius:IETF	Tunnel-Type	VLAN(13)
Radius:IETF	Tunnel-Medium-Type	IEEE-802(6)
Radius:Aruba	Aruba-User-Vlan	<VLAN>

Näillä säännöillä käyttäjä asetetaan haluttuun VLAN:iin. Kun kaikki profiilit on luotu, voidaan palata Enforcement Policyn luontiin Rules-välilehdelle. Täällä luodaan säännöt, jotka käyttävät eri enforcement profiileja. Jokaiselle hallinnoidulle käyttäjäryhmälle tulee oma sääntönsä, joka noudattaa samaa muotoa:

Tips	Role	EQUALS	<Rooli>

Valitut roolit luotiin Role Mapping Policy kohdassa. Valitse alta roolia vastaava enforcement profiili.

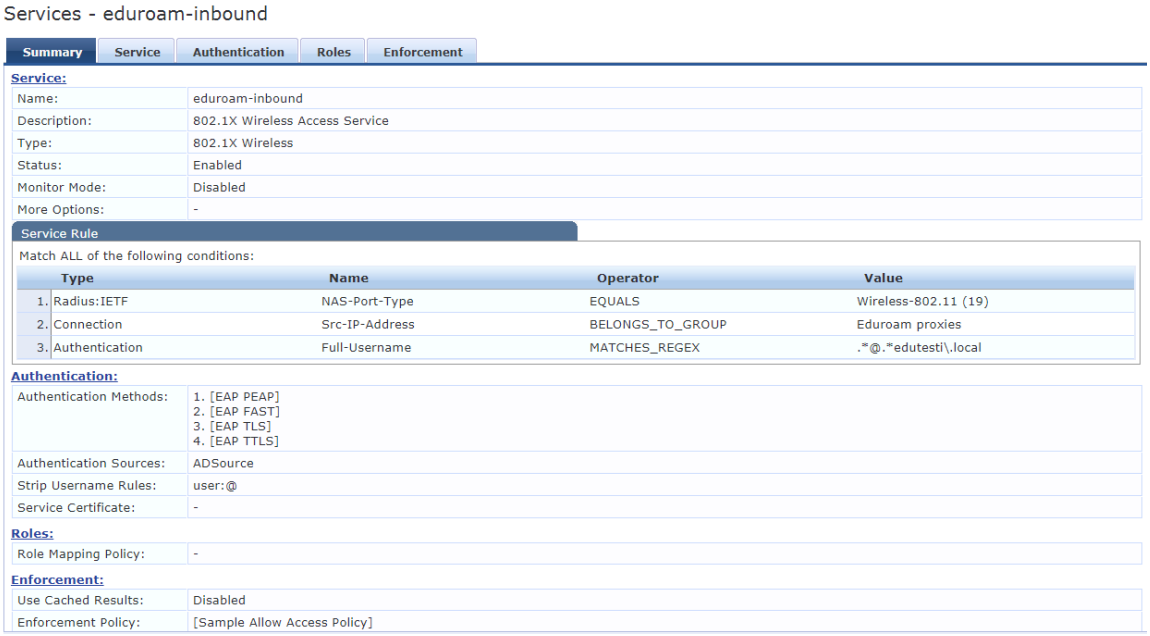


Kuva 22 - Enforcement Policies -säännön luonti

Tämän vaiheen jälkeen enforcement policy on valmis, ja palvelun luonti voidaan viimeistellä.

5.4.2 Inbound

Inbound-palvelulla hoidetaan omien käyttäjien autentikointi, kun he yhdistävät jonkin muun organisaation eduroam-verkkoon. Palvelu luodaan samalla tavalla kuin local-palvelu, mutta joitain asetuksia muutetaan.


Services - eduroam-inbound

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	eduroam-inbound
Description:	802.1X Wireless Access Service
Type:	802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Connection	Src-IP-Address	BELONGS_TO_GROUP	Eduroam proxies
3.	Authentication	Full-Username	MATCHES_REGEX	.*@.*edutesti\.local

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS]
Authentication Sources:	ADSource
Strip Username Rules:	user:@
Service Certificate:	-

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	[Sample Allow Access Policy]

Kuva 23 - Eduroam-inbound -palvelun asetukset

Palvelussa käytetään taas 802.1X Wireless – tyyppiä. Säännöiksi listataan:

Radius:IETF NAS-Port-Type EQUALS Wireless-802.11 (19)

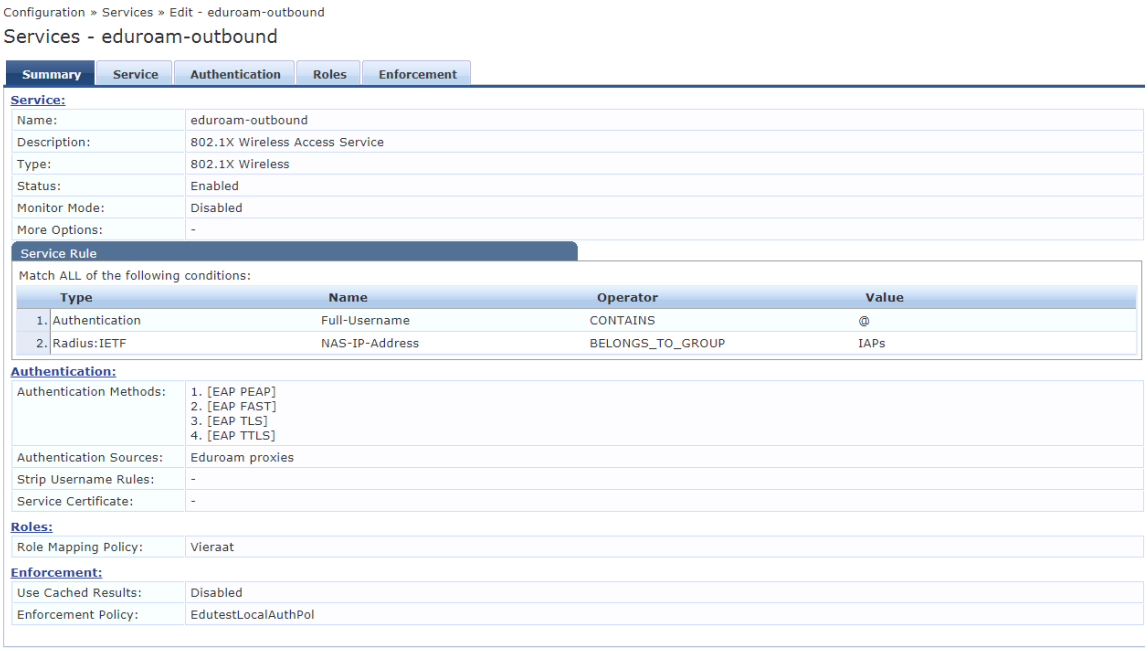
Connection Src-IP-Address BELONGS_TO_GROUP Eduroam proxies

Authentication Full-Username MATCHES_REGEX <regex>

Regexinä käytetään samaa, kuin local-palvelussa. Authentication sourceksi laitetaan AD, ja käyttäjänimen säännöksi taas user:@. Rooli- tai enforcement-asetuksia ei tarvitse asettaa, sillä palvelun tarkoitus on vain autentikoida, ja välittää tiedot takaisin toiselle organisaatiolle. Sample Allow Access Policy on geneerinen policy, joka on aina salliva.

5.4.3 Outbound

Outbound on viimeinen kolmesta palvelusta. Tämä käsittää verkkoon liittyvät käyttäjät, jotka eivät ole paikallisia. Heidät täytyy autentikoida toisessa organisaatiossa.


Configuration » Services » Edit - eduroam-outbound

Services - eduroam-outbound

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	eduroam-outbound
Description:	802.1X Wireless Access Service
Type:	802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Full-Username	CONTAINS	@
2.	Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	IAPs

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS]
Authentication Sources:	Eduroam proxies
Strip Username Rules:	-
Service Certificate:	-

Roles:

Role Mapping Policy:	Vieraat

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	EdutestLocalAuthPol

Kuva 24 - Eduroam-outbound – palvelun asetukset

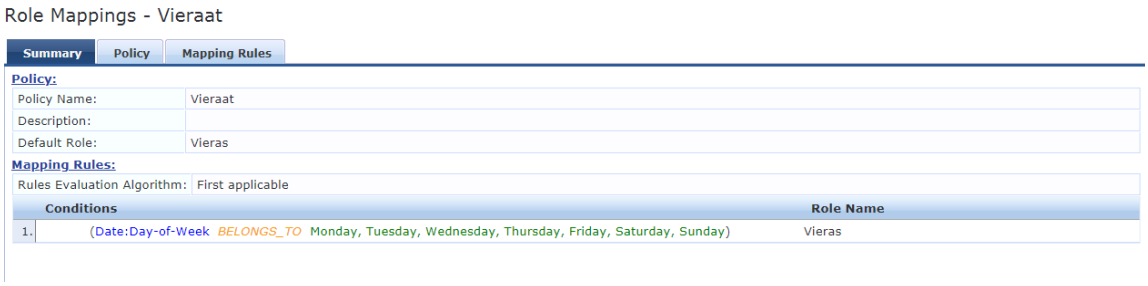
Jälleen palvelun tyyppinä on 802.1X Wireless. Säännöiksi listataan:

Authentication Full-Username CONTAINS @

Radius:IETF NAS-IP-Address BELONGS_TO_GROUP <IAPt>

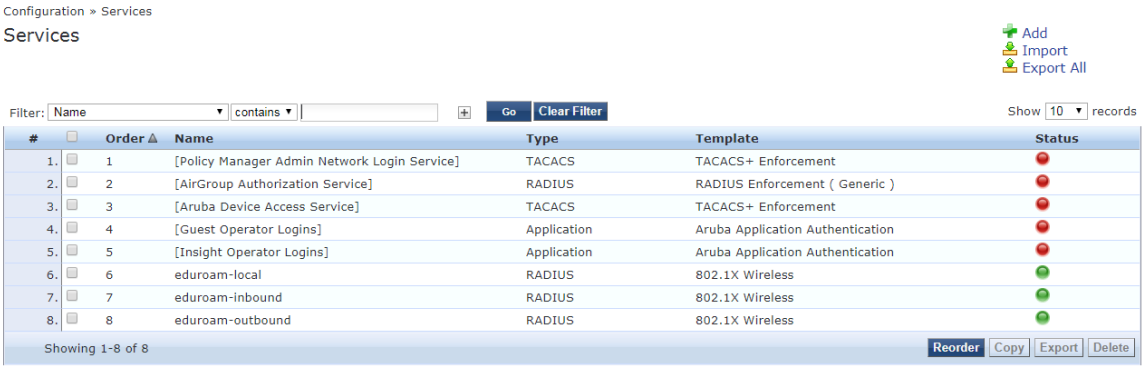
Autentikointilähteeksi asetetaan Eduroam proxyt, ja käyttäjänimisääntöjä ei tarvita. Luodaan role mapping policy vieraskäyttäjille. Policyn oletusrooliksi asetetaan Vieras, ja säännöksi:

Date Day-of-Week BELONGS_TO Monday, Tuesday,…, Sunday



Kuva 25 - Vieraat -role mapping policy

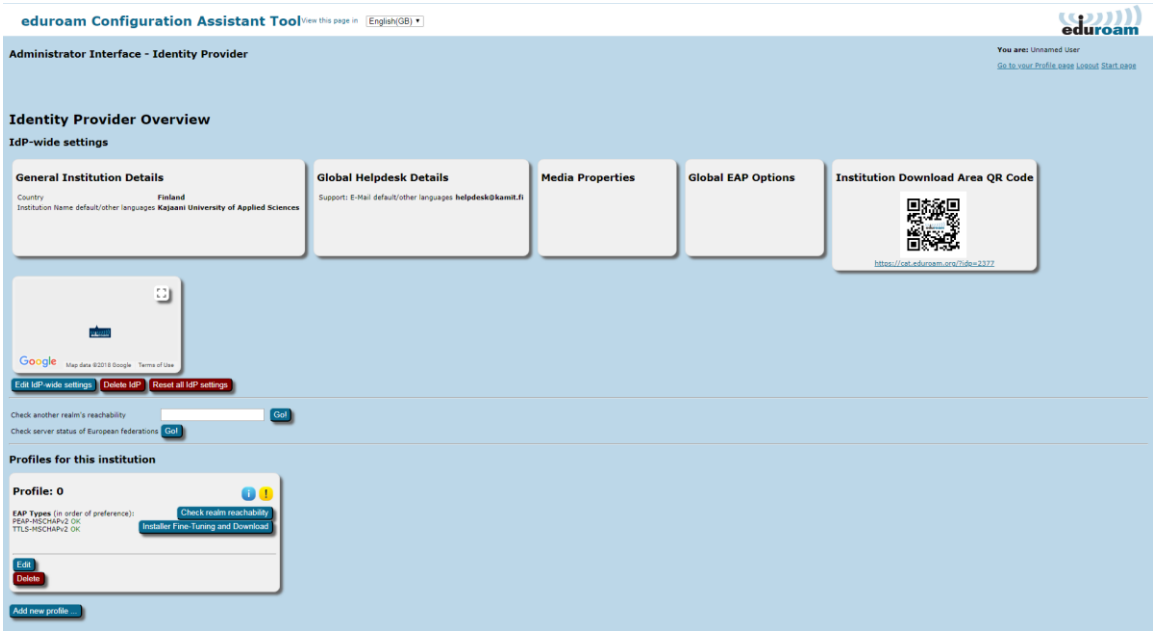
Ja actioniksi tulee Vieras-rooli. Näin kaikki tämän palvelun alle jäävät käyttäjät saavat Vieras-roolin, joka voidaan enforcettaa vieraille tarkoitettuun VLAN:iin. Aseta enforcement policyksi local-palvelua varten luotu policy. Kun kaikki palvelut ovat valmiit, niiden täytyy olla listattuna oikeassa järjestyksessä. Oikea järjestys on local, inbound ja viimeisenä outbound.



Kuva 26 - Eduroam-palvelujärjestys

6 Eduroam CAT

Eduroam CAT, eli eduroam Configuration Assistant Tool on työkalu, jonka kautta voi julkaista ja jakaa konfigurointipaketteja käyttäjälle useille eri käyttöjärjestelmille. Tämä voi yksinkertaistaa eduroamin käyttöönottoa loppukäyttäjälle. Hallinnoija voi saada kutsulinkin/tokenin CSC:n kautta Suomessa.

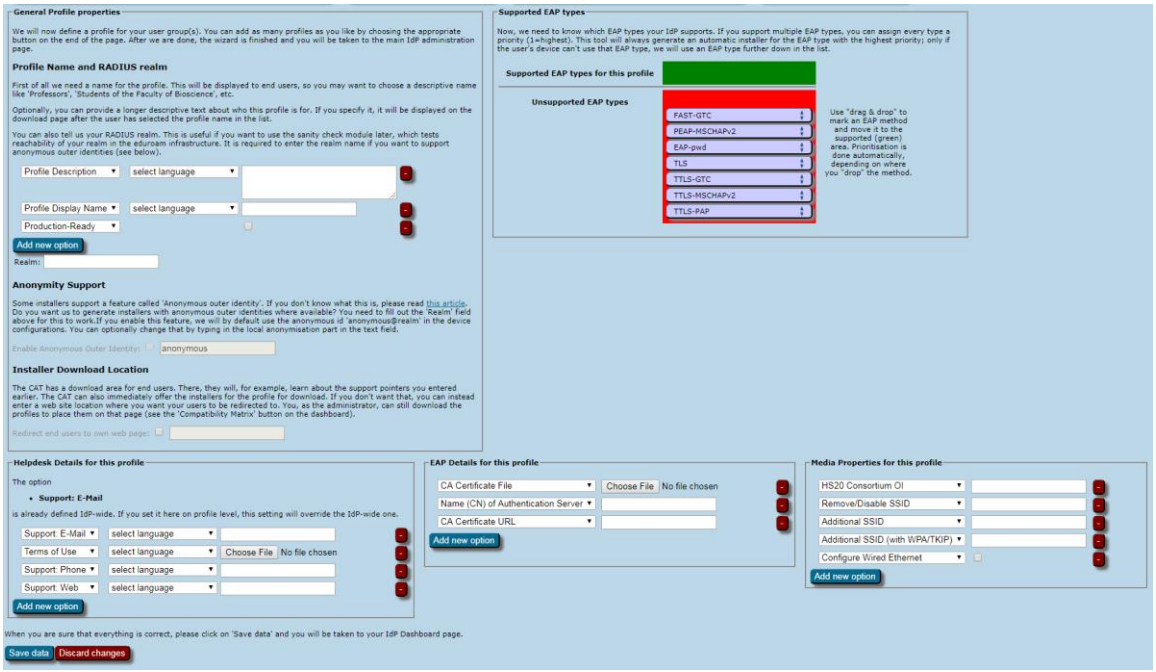


Kuva 27 - CAT-hallinnointinäkymä

Painamalla alhaalta ’Add new profile…’, voit luoda uuden profiilin. Profiilin eri tiedot on jaettu viiteen kategoriaan. Niistä ensimmäisenä on ’General Profile properties’. Tänne voit lisätä haluamasi profiilin kuvauksen, nimen, valita onko profiili tuotantokäytössä, ja mikä on hallittu realm. Realmiksi tulee valita sama, jota käytettiin RADIUS-palvelimen käyttäjänimisäännöissä. Tässä voi myös valita tuetaanko anonymiteettiä, ja halutaanko latauspaketit jakaa jostain muualta. Ota huomioon, että Production-Ready attribuutti tekee profiilista julkisen, jolloin sen voi ladata.

Toinen ryhmä on ’Supported EAP types’. Tähän tulee listata eri EAP-tyypit ja niiden prioriteettijärjestys, joita RADIUS-autentikointi tukee. Kolmantena on ’Helpdesk Details for this profile’. Tähän voi liittää eri tietoja jotka koskevat vain tiettyjä profiileja. Neljäntenä on ’EAP Details for this profile’. Tänne tulee ladata sama sertifikaatti, jota käytetään RADIUS-palvelimella. Kun sertifikaatit ovat listattuna, voi itse palvelinsertifikaatin poistaa, sen tulisi näkyä punaisena listauksessa. Tätä sertifikaattia ei tarvitse lähettää kättelyn yhteydessä,

sillä palvelin lähettää sen joka kerta siitä huolimatta. Viidennessä osiossa ’Media Properties for this profile’ voi asettaa muita tietoja, joita paketin yhteydessä asetetaan käyttäjälle.



Kuva 28 - Uuden CAT-profiilin luonti

Eduroam on korkeakoulujen ja tutkimuslaitosten yhteinen verkkovierailujärjestelmä. Tämä opas sisältää ohjeet siitä, kuinka erilaiset päätelaitteet yhdistetään eduroam-verkkoon.

Päätelaitteelle asennetaan ennen verkon käyttöä eduroam-asennuspaketti, joka sisältää eduroam-verkon vaatimat konfiguroinnit ja tietoturva-asetukset laitteelle.

Valitse seuraavilta sivuilta päätelaitettasi vastaava ohjeistus siitä, kuinka voit liittää laitteen eduroamiin!

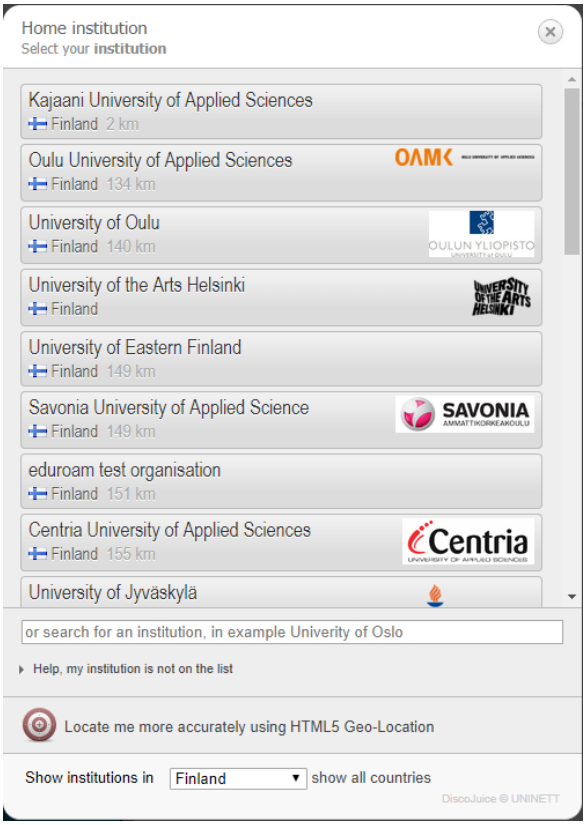
Lisätietoa eduroam-verkon käytöstä löytyy osoitteesta: http://www.eduroam.fi

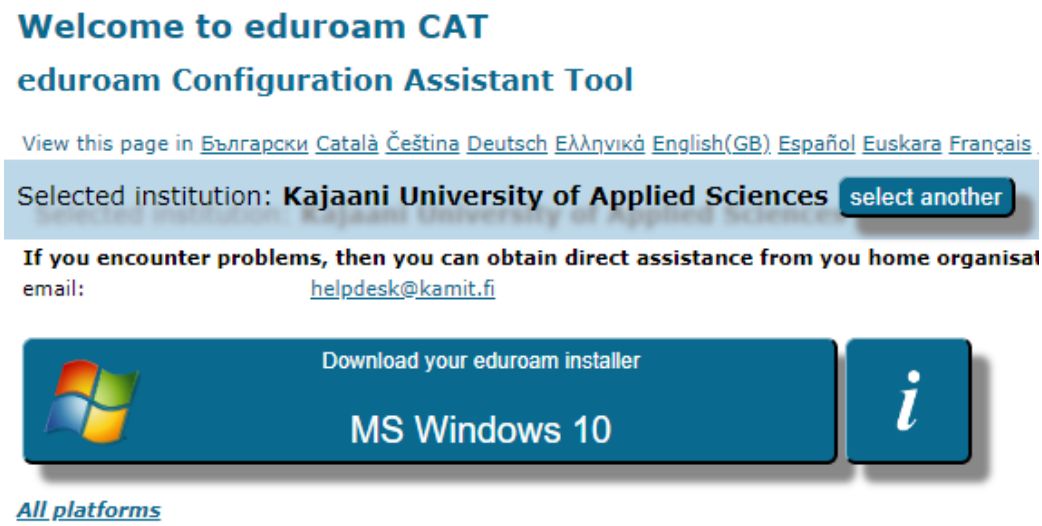
QR-koodi: lataa laitteellesi sopivan eduroam-asennuspaketin

Sisällys

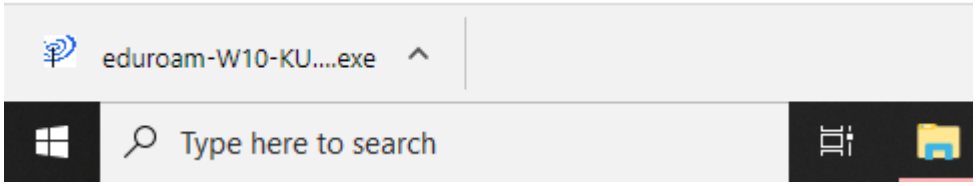
1 Windows

- avaa selainohjelmisto osoitteeseen https://cat.eduroam.org.
- paina alhaalla näkyvää **eduroam user -**painiketta
- valitse listalta **Kajaani University of Applied Sciences** tai etsi se kirjoittamalla hakukenttään ”Kajaani”
- Sivu näyttää tämän jälkeen käyttöjärjestelmällesi sopivan eduroam-asennuspaketin latauspainikkeen. Lataa asennuspaketti laitteellesi painamalla em. painiketta.

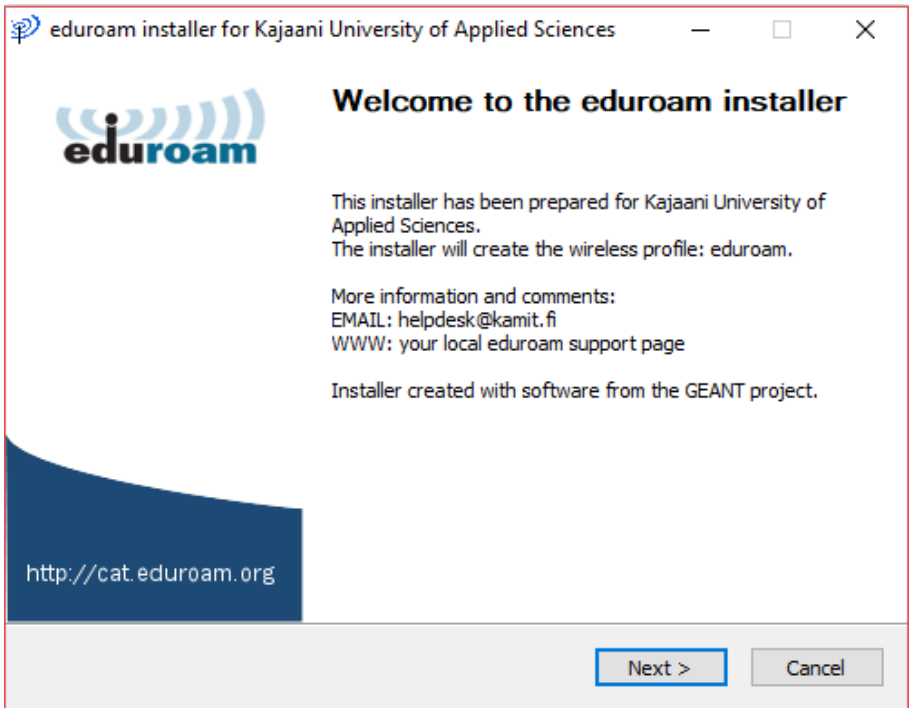


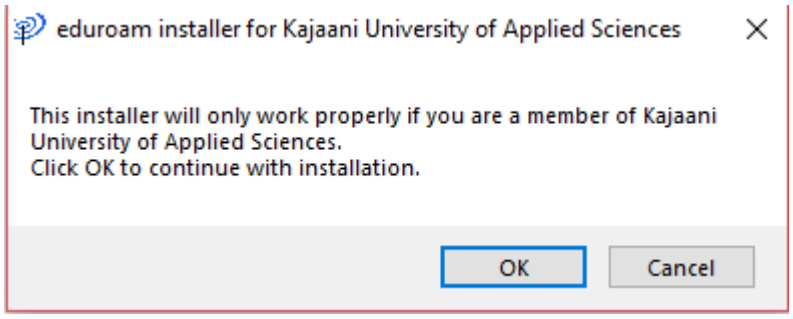


- asennuspaketti latautuu laitteellesi (riippuu selaimestasi miten latauksen valmistumisesta ilmoitetaan), klikkaa ladattua asennustiedostoa ja asennus käynnistyy.

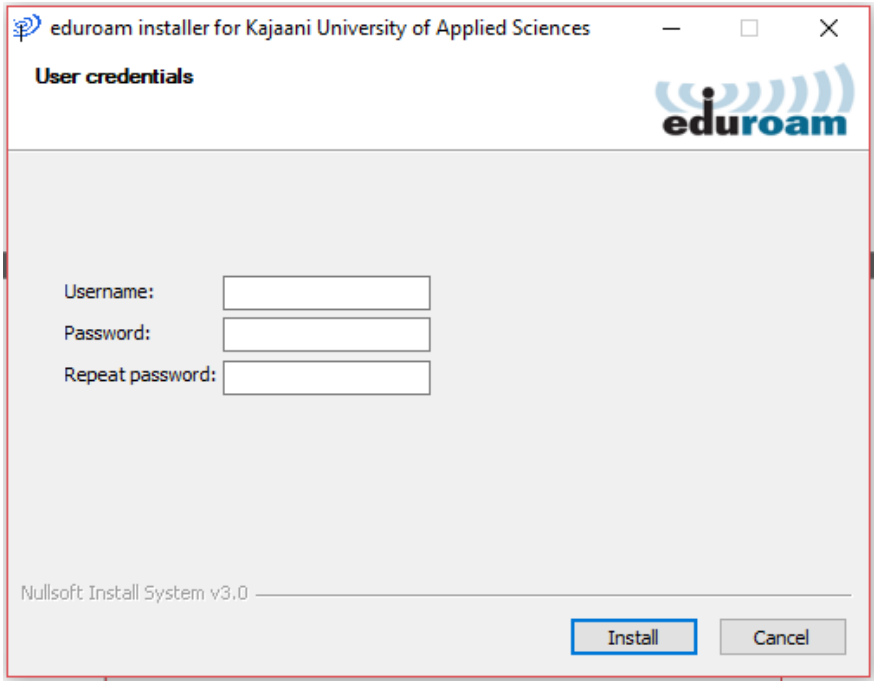


- asennuksen käynnistyttyä paina **Next ja OK**





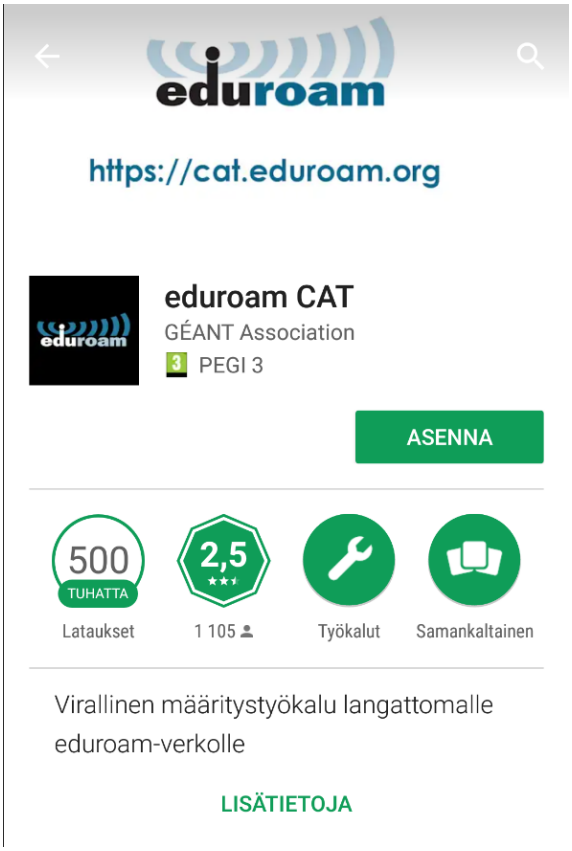
- asennus pyytää Kajaanin ammattikorkeakoulun KamIT-käyttäjätunnusta ja salasanaa. Käyttäjätunnus syötetään muodossa **KamIT-käyttäjätunnus@kamk.fi.** Paina **Install**.

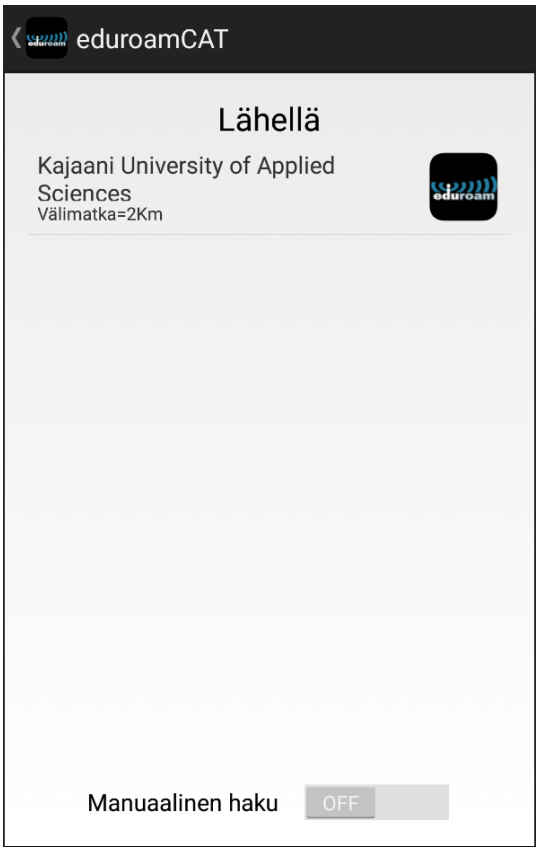


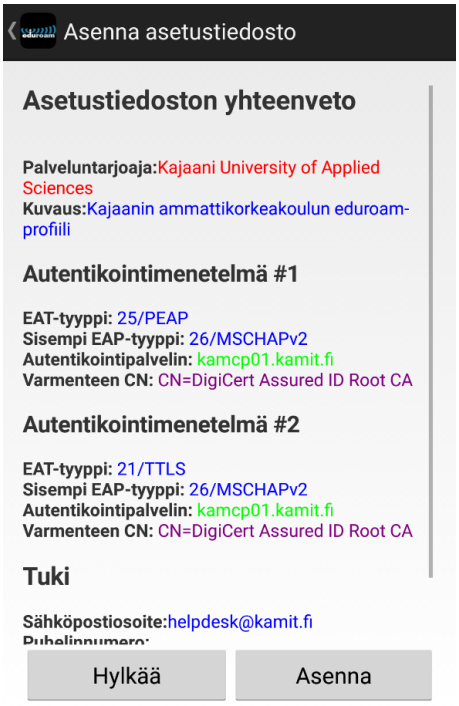
- tämän jälkeen laite voidaan yhdistää eduroam-verkkoon kaikissa eduroamia tarjoavissa organisaatioissa

2 Android (puhelimet ja tabletit)

- lataa ja asenna Play-kaupasta **eduroam CAT** -sovellus. Suora linkki: https://play.google.com/store/apps/details?id=uk.ac.swansea.eduroamcat
- valitse sovelluksen ehdottama **Kajaani University of Applied Sciences -profiili** tai valitse alhaalta Manuaalinen haku ja kirjoita ”Kajaani”.
- syötä kenttiin Kajaanin ammattikorkeakoulun **KamIT-käyttäjätunnus ja salasana**. Käyttäjätunnus syötetään muodossa **KamIT-käyttäjätunnus@kamk.fi** Asenna profiili valitsemalla **Asenna**.
- tämän jälkeen laite voidaan yhdistää eduroam-verkkoon kaikissa eduroamia tarjoavissa organisaatioissa





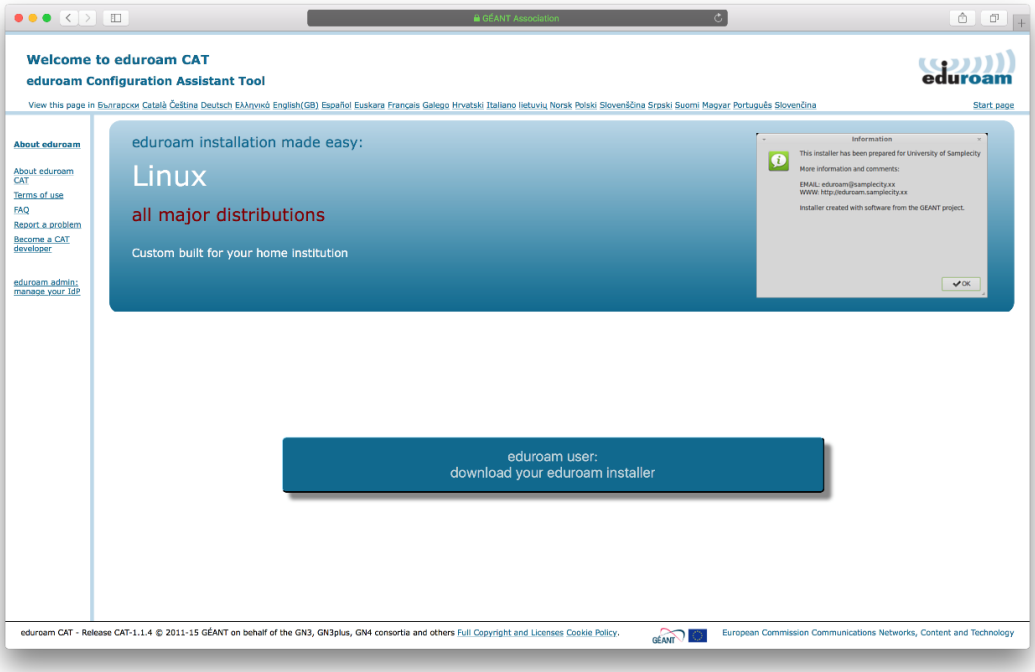


Vaihtoehtoisesti:

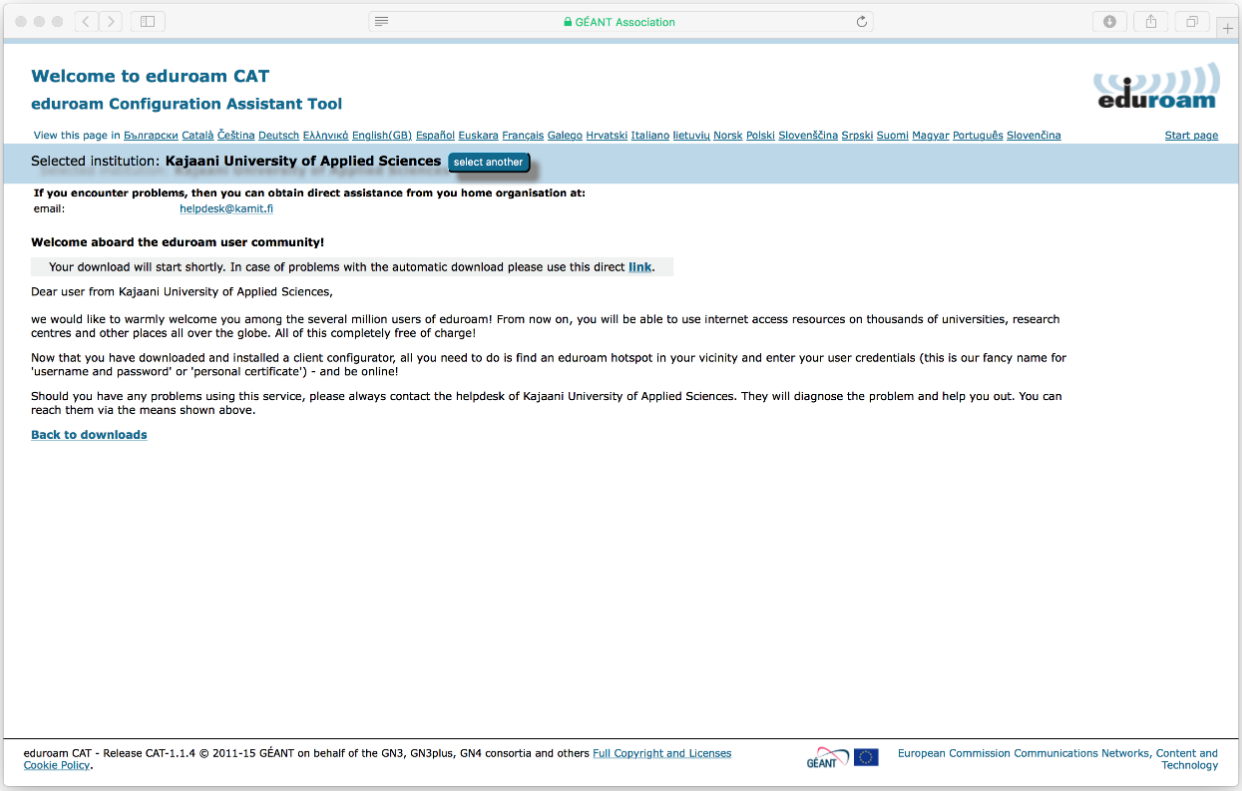
Mene laitteella osoitteeseen cat.eduroam.org ja valitse kotiorganisaatioksi Kajaani University of Applied Sciences. Valitse asennusohjelmaksi oman laitteesi Android-versiota vastaava eduroam-asennuspaketti. Tämän tulisi tapahtua laitteella automaattisesti. Asennus etenee muutoin edellä olevien kuvien mukaisesti.

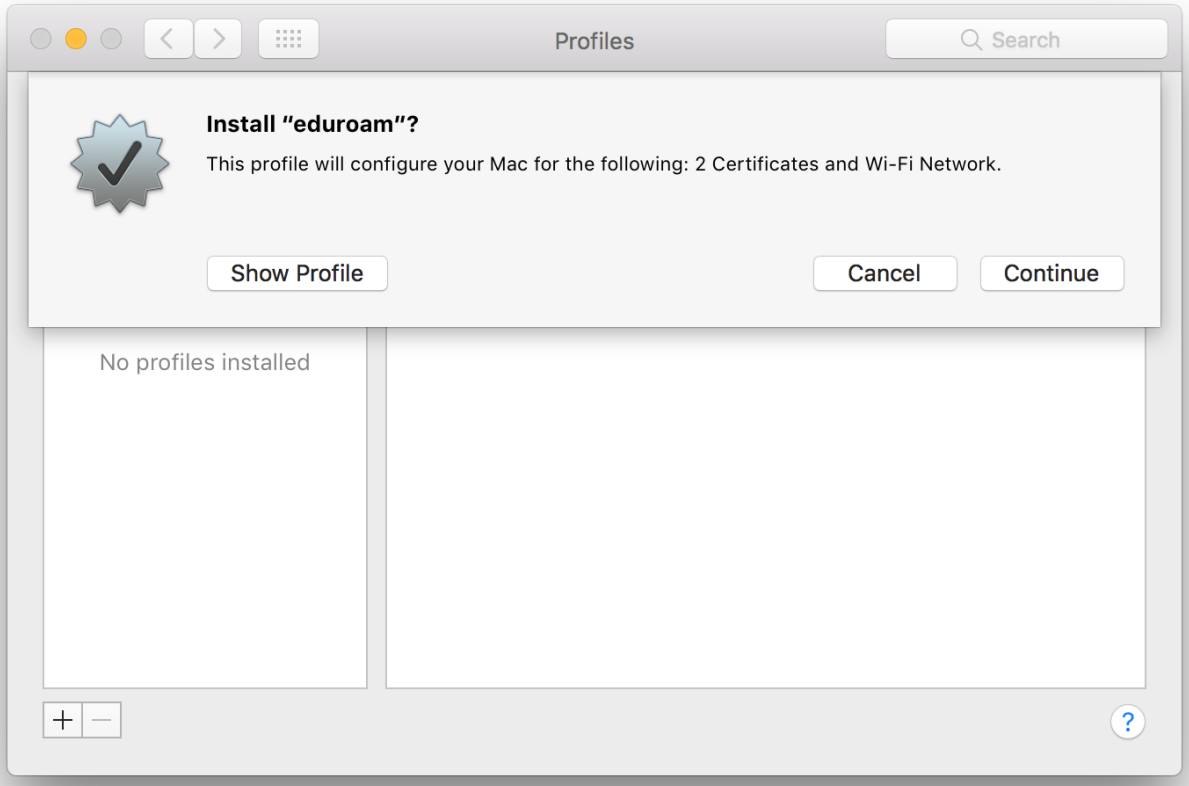
3 OSX / macOS / Linux (Mac ja Linux-tietokoneet)

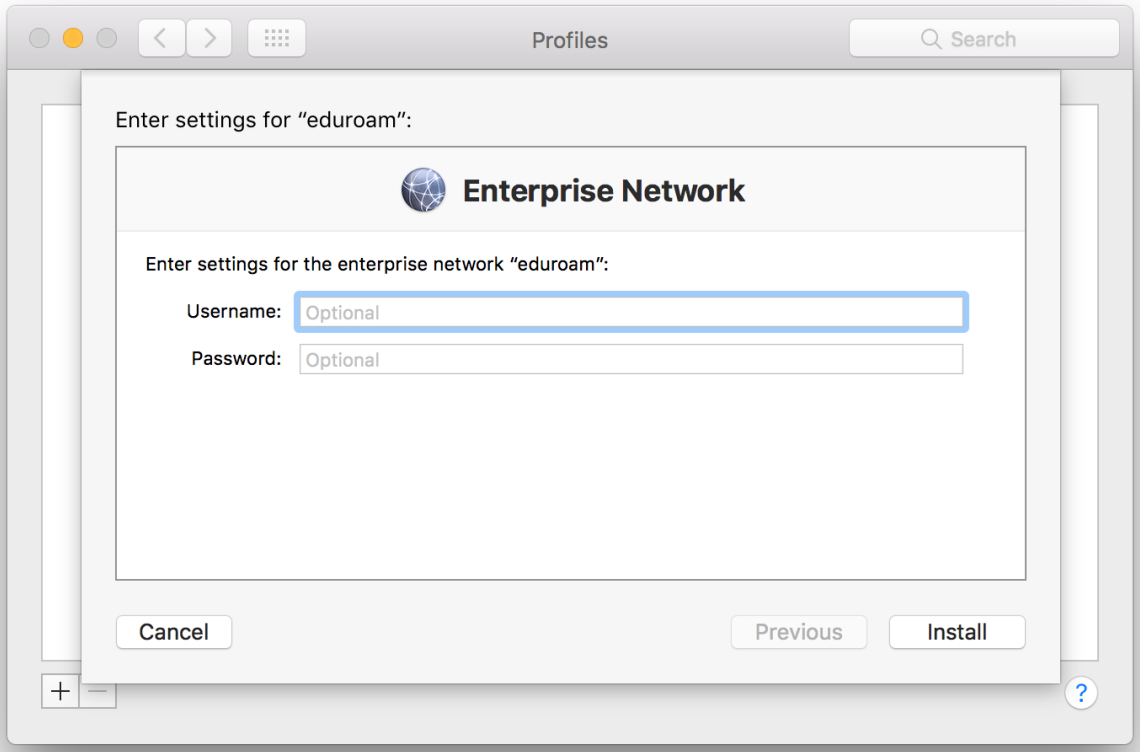
- avaa selainohjelmisto osoitteeseen https://cat.eduroam.org.
- paina alhaalla näkyvää **eduroam user -painiketta**
- valitse listalta **Kajaani University of Applied Sciences** tai etsi se kirjoittamalla hakukenttään ”Kajaani”
- Sivu näyttää tämän jälkeen käyttöjärjestelmällesi sopivan eduroam-asennuspaketin latauspainikkeen. Lataa asennuspaketti laitteellesi painamalla em. painiketta.



- asenna profiili laitteellesi **”Install eduroam”** ja **”Continue”**
- asennus pyytää Kajaanin ammattikorkeakoulun KamIT-käyttäjätunnusta ja salasanaa. Käyttäjätunnus syötetään muodossa **KamIT-käyttäjätunnus@kamk.fi**.
- tämän jälkeen laite voidaan yhdistää eduroam-verkkoon kaikissa eduroamia tarjoavissa organisaatioissa


GÉANT Association
Welcome to eduroam CAT
eduroam Configuration Assistant Tool
eduroam
View this page in Български Català Čeština Deutsch Ελληνικά English(GB) Español Euskara Français Galego Hrvatski Italiano lietuvių Norsk Polski Slovenščina Srpski Suomi Magyar Português Slovenčina
Start page
Selected institution: Kajaani University of Applied Sciences
select another
If you encounter problems, then you can obtain direct assistance from you home organisation at:
email: helpdesk@kamit.fi
Welcome aboard the eduroam user community!
Your download will start shortly. In case of problems with the automatic download please use this direct link.
Dear user from Kajaani University of Applied Sciences,
we would like to warmly welcome you among the several million users of eduroam! From now on, you will be able to use internet access resources on thousands of universities, research centres and other places all over the globe. All of this completely free of charge!
Now that you have downloaded and installed a client configurator, all you need to do is find an eduroam hotspot in your vicinity and enter your user credentials (this is our fancy name for 'username and password' or 'personal certificate') - and be online!
Should you have any problems using this service, please always contact the helpdesk of Kajaani University of Applied Sciences. They will diagnose the problem and help you out. You can reach them via the means shown above.
Back to downloads
eduroam CAT - Release CAT-1.1.4 © 2011-15 GÉANT on behalf of the GN3, GN3plus, GN4 consortia and others Full Copyright and Licenses
Cookie Policy.
GÉANT
European Commission Communications Networks, Content and Technology

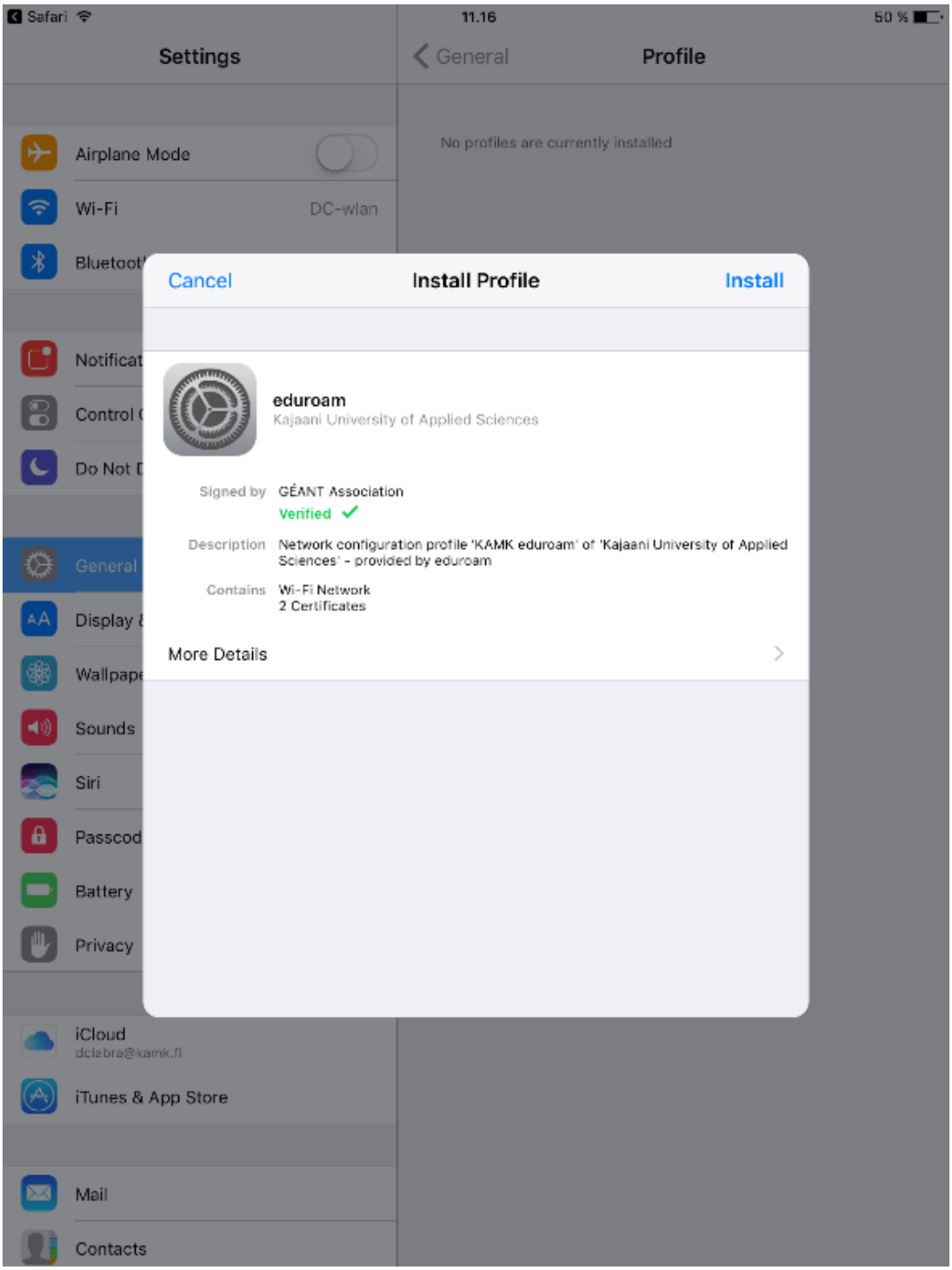

Profiles
Search
Install “eduroam”?
This profile will configure your Mac for the following: 2 Certificates and Wi-Fi Network.
Show Profile
Cancel
Continue
No profiles installed


Profiles
Search
Enter settings for “eduroam”:
Enterprise Network
Enter settings for the enterprise network “eduroam”:
Username:
Optional
Password:
Optional
Cancel
Previous
Install

4 iOS (iPhone ja iPad)

- avaa selainohjelmisto osoitteeseen https://cat.eduroam.org.
- paina alhaalla näkyvää **eduroam user -painiketta**
- valitse listalta **Kajaani University of Applied Sciences** tai etsi se kirjoittamalla hakukenttään ”Kajaani”
- Sivu näyttää tämän jälkeen käyttöjärjestelmällesi sopivan eduroam-asennuspaketin latauspainikkeen **Apple iOS mobile devices…**. Lataa asennuspaketti laitteellesi painamalla em. painiketta.

- asenna profiili laitteellesi valitsemalla **Install**
- asennus pyytää Kajaanin ammattikorkeakoulun KamIT-käyttäjätunnusta ja salasanaa. Käyttäjätunnus syötetään muodossa **KamIT-käyttäjätunnus@kamk.fi**
- tämän jälkeen laite voidaan yhdistää eduroam-verkkoon kaikissa eduroamia tarjoavissa organisaatioissa



5 Vaihtoehtoinen yhdistämistapa

Edellä mainittujen tapojen lisäksi laitteen voi liittää eduroam-verkkoon tekemällä laitteella wlan-verkon profiilin käsin seuraavilla asetuksilla: (tämä ei ole suositeltavaa, koska asetuksien termit voivat vaihdella eri laitteilla):

- **Verkon nimi (SSID):** eduroam
- **Suojaus:** WPA2-Enterprise (Android-ympäristössä 802.1X EAP)
- **EAP-tapa:** PEAP
- CA-varmennetta ei tarvitse vahvistaa
- **Identiteetti:** Kamit-tunnus muodossa **KamIT-käyttäjätunnus@kamk.fi**
- Anonyymi identiteetti tyhjä
- **Salasana:** Kamit-käyttäjätunnuksen salasana

6 Eduroamin käytön turvallisuus

Eduroam-verkon käyttö perustuu tällä hetkellä yleisimmin käytössä oleviin turvallisiin salaus- ja autentikointitekniikoihin. Eduroamia käytetään hlökohtaisella organisaation käyttäjätunnuksella ja liikenne salataan WPA2 / AES-salauksella. Eduroamin käyttö on siten aina turvallisempaa kuin avointen wlan-verkkojen käyttäminen. Tästäkin huolimatta oman laitteen tietoturvasta on huolehdittava.

KAMK käyttää eduroamin ja internetin välissä palomuuria ja tietoliikenteen pakettisuodatusta, mutta näin ei ole välttämättä jokaisessa organisaatiossa. Verkossa on suositeltavaa käyttää salaustekniikoita kuten ssh ja ssl.

Verkon käyttöönotto tässä ohjeessa kuvatun eduroam-asennuspaketin avulla varmistaa sen, että tietoturva-asetukset tulevat laitteelle vaaditulle tasolle.

Eduroam-verkon käyttäjä sitoutuu aina noudattamaan sekä kotiorganisaationsa että vierailtavan organisaation verkon käyttösääntöjä.

Lisätietoa eduroamin turvallisuudesta ja verkon käytöstä yleensä saa kotiorganisaation IT-tuesta, KamIT Helpdesk (helpdesk@kamit.fi)