คู่มือการติดตั้ง RADIUS server สำหรับบริการ eduroam สำหรับการเป็นผู้ให้บริการหลัก (Sub-Realm) ของสถาบัน

บทนำ

eduroam ย่อมาจาก “educational roaming” เป็นเครื่องหมายที่จดทะเบียนโดย TERENA ที่ก่อกำเนิดจากเครือข่ายการศึกษาและวิจัยของยุโรป (NRENs) เพื่อการใช้งานเครือข่ายที่เรียบง่าย ปลอดภัย และรองรับผู้ใช้งานที่ขยายตัวเพิ่มมากขึ้นได้ โดย eduroam เป็นบริการเครือข่ายโรมมิ่งเพื่อการศึกษาและวิจัยสำหรับนักศึกษาและบุคลากรของสถาบันการศึกษาที่เป็นสมาชิกเครือข่าย eduroam เพื่ออำนวยความสะดวกในการใช้งานเครือข่ายอินเตอร์เน็ตได้ โดยอยู่ภายใต้เงื่อนไขการใช้งานของสถาบันผู้ให้บริการเครือข่าย (Service Provider)

eduroam เริ่มต้นขึ้นในปี 2546 จากการสาธิตความเป็นไปได้สำหรับการให้บริการงานเครือข่ายโรมมิ่งข้ามเครือข่าย โดยการใช้มาตรฐาน 802.1x ทำงานร่วมกับ RADIUS Server ของแต่ละสถาบันเพื่อให้บริการกับนักศึกษาและนักวิจัยจากสถาบันสมาชิกจาก 5 ประเทศ ประกอบด้วย เนเธอเลนด์ ฟินแลน โปรตุเกส โครเอเชีย และสหราชอาณาจักร

สำหรับในประเทศไทย สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) จะทำหน้าที่เป็นผู้ดำเนินการหลักของประเทศไทย (National Roaming Operator for Thailand: NRO) เป็นผู้รับผิดชอบการให้บริการ eduroam สำหรับประเทศไทย และเป็นผู้กำหนดนโยบายการใช้งานระดับประเทศ

คู่มือฉบับนี้เป็นขั้นตอนการติดตั้งแม่ข่าย freeradius สำหรับสถาบันสมาชิกในประเทศไทย เพื่อเชื่อมเข้าต่อบริการเข้ากับ eduroam ประเทศไทย และให้บริการตรวจสอบบัญชีผู้ใช้ของสถาบันที่เชื่อมต่อเข้ากับบริการ eduroam

ขั้นตอนการติดตั้ง จะประกอบด้วย 3 ขั้นตอนหลัก ประกอบด้วย

1. การติดตั้งและทดสอบพื้นฐาน
   เป็นขั้นตอนที่จะทำให้ RADIUS Server ทำงานได้ด้วยตัวเอง ใช้บัญชีผู้ใช้ที่มีอยู่ในไฟล์ของโปรแกรม
2. การเชื่อมต่อกับเครื่องให้บริการหลัก (Main Realm) ของสถาบัน

เป็นขั้นตอนที่จะทำให้ RADIUS Server ของสถาบันส่วนย่อย Sub-Realm เชื่อมต่อ RADIUS Server ของสถาบันส่วนหลัก Main Realm

3. การเลือกใช้ฐานข้อมูลบัญชีผู้ใช้จากระบบภายนอก
   เป็นขั้นตอนหลักที่จะทำให้ RADIUS Server ของสถาบันตรวจสอบบัญชีผู้ใช้ภายในสถาบันได้ โดยบัญชีผู้ใช้ที่ RADIUS Server ใช้ในการตรวจสอบนั้นมาจากฐานข้อมูลบัญชีผู้ใช้ที่อยู่ภายนอกโปรแกรม RADIUS Server ในคู่มือฉบับนี้มีขั้นตอนแนะนำสำหรับใช้ฐานข้อมูลบัญชีผู้ใช้ภายนอกจำนวน 4 ทางเลือก
   - การติดตั้งโดยมี LDAP Server เป็นฐานข้อมูลบัญชีผู้ใช้
   - การติดตั้งโดยมี MySQL เป็นฐานข้อมูลบัญชีผู้ใช้
   - การติดตั้งโดยมี Microsoft NPS (Network Policy Service) เป็นบริการตรวจสอบบัญชีผู้ใช้
   - การติดตั้งโดยมี Microsoft Active Directory เป็นฐานข้อมูลบัญชีผู้ใช้

วิธีการติดตั้ง เป็นการแนะนำคำสั่งในการดำเนินการอย่างเป็นลำดับ พร้อมตัวอย่างคำสั่งที่ตรงกับสภาพแวดล้อมของ เครื่องมากที่สุด เช่รน การติดตั้งแพคเกจ การแก้ไขไฟล์ การทดสอบการทำงาน เป็นต้น โดยคุณสมบัติของโปรแกรม เกือบทั้งหมด เป็นการนำไฟล์สำเร็จรูปที่ผ่านการปรับรูปแบบเพื่อไม่ให้ซ้ำกับไฟล์คุณสมบัติเดิมของโปรแกรม นำมาติดตั้ง ดำเนินการแก้ไขเนื้อหาในไฟล์ให้เหมาะสม และใช้งาน

เพื่อให้การติดตั้งมีความถูกต้องและสามารถทำงานได้อย่างไม่มีข้อผิดพลาด จำเป็นต้องดำเนินการตามลำดับขั้นโดยละเอียด ยกเว้นการเลือกใช้ฐานข้อมูลบัญชีผู้ใช้ที่สามารถเลือกได้อย่างใดอย่างหนึ่ง

ในหัวข้อ การตรวจวิเคราะห์และตรวจสอบการทำงานของ RADIUS server เป็นส่วนของการแนะนำการปรับแต่งคุณสมบัติ เพื่อให้ RADIUS server ทำงานที่แตกต่างหรือเพิ่มเติมจากการติดตั้งนี้ รวมถึงการตรวจสอบกิจกรรมที่เกิดขึ้นที่บันทึกไว้ในไฟล์ Log

ในหัวข้อ การติดตั้ง Wireless Controller หรือ Anonymous Access Point ร่วมกับ RADIUS server แนะนำวิธีการกำหนดคุณสมบัติของ RADIUS server และอุปกรณ์ WLC หรือ AP ให้ทำงานร่วมกัน

ลักษณะเด่นของการกำหนดคุณสมบัติในการติดตั้งนี้คือ สามารถเปิดโอกาสให้สมาชิกภายในองค์กรใช้บริการเครือข่ายภายในองค์กรได้ ประโยชน์ก็เพื่อให้สมาชิกดำเนินการกำหนดคุณสมบัติการเชื่อมต่อจากเครือข่ายภายในให้สำเร็จก่อน แก้ปัญหาให้เสร็จก่อน จากนั้นจึงจะไปใช้บริการจากผู้ให้บริการอื่นได้ทันที

สภาพแวดล้อมและโครงสร้างทางเครือข่าย

รุ่นของระบบปฏิบัติการและโปรแกรม freeradius ที่ติดตั้ง

การติดตั้งและกำหนดคุณสมบัติของโปรแกรมในคู่มือการติดตั้ง RADIUS server สำหรับบริการ eduroam นี้จะดำเนินการบนของระบบปฏิบัติการ Debian Linux 10.2 และโปรแกรม freeradius รุ่น 3.0 แต่อาจสามารถนำขั้นตอนหรือหลักการไปปรับใช้กับระบบปฏิบัติการอื่น หรือโปรแกรม freeradius รุ่นอื่นนั้น

คำสั่งและไฟล์จะอ้างอิงตามระบบปฏิบัติการและโปรแกรม freeradius จึงควรเลือกใช้คำสั่งอย่างถูกต้อง ดังนี้

```
- Debian 10.2 (buster)
      cat /etc/debian_version
- Freeradius 3.0
      freeradius -v
```

โครงสร้างเครือข่ายประกอบการติดตั้ง

คุณสมบัติหรือการตั้งค่าการทำงานของโปรแกรม freeradius และบริการประกอบ จะเป็นไปตามโครงสร้างการเชื่อมต่อเครือข่ายดังภาพต่อไปนี้

```
|   +------------------+
+---| eduroam-TH       |
|   +------------------+
|    202.28.112.6
|
|   +------------------+
+---| RADIUS server    |  Main Realm
|   +------------------+  eduroam@uxx.ac.th
|    radius.uxx.ac.th (192.168.1.1)
|
|   +------------------+
+---| RADIUS server    |  Sub-Realm
|   +------------------+  eduroam@abc.uxx.ac.th
|    radius.abc.uxx.ac.th (192.168.1.111)
```

```
|
|
|
|   +-------------------+
+---| LDAP/MySQL server |  ldap.uxx.ac.th
|   +-------------------+  user@uxx.ac.th
|    ldap.uxx.ac.th (192.168.1.2)
|    mysql.uxx.ac.th (192.168.1.2)
|     (radius:radpass@mysql.uxx.ac.th/radius)
|          or
|   +------------------+
+---| Microsoft NPS    |  ad.uxx.local/UXX.LOCAL
|   +------------------+  user@abc.uxx.ac.th
|    ad.uxx.ac.th (192.168.1.3)
|    ipaddr = xxx.xxx.xxx.xxx
|    port = 1812
|    secret = XXXXXXXXXXXXXXXX
|
+---[ WLC or AP ]


== Hosts Account/Password ==
Linux: root/asdf
Windows: Administrator/Asdf1234
```

1) การติดตั้งและทดสอบขั้นพื้นฐาน

เป็นการติดตั้งและกำหนดคุณสมบัติพื้นฐานให้ RADIUS server สามารถทำงานได้ด้วยตัวเอง ประกอบด้วยการติดตั้งโปรแกรม ติดตั้งแพคเกจพื้นฐาน ติดตั้งแพคเกจสนับสนุน ติดตั้งโปรแกรมสำหรับทดสอบ แก้ไขคุณสมบัติพื้นฐาน และทดสอบการทำงาน โดยการทดสอบจะนำข้อมูลผู้ใช้แบบไฟล์ข้อความที่มีอยู่ไฟล์ user-eduroam.conf มาใช้งาน

1.1 อัพเกรดแพคเกจล่าสุดและแพคเกจพื้นฐาน

```
apt update
apt upgrade -y
```

อาจต้องรีสตาร์ทเครื่อง

```
apt install ntp -y
service ntp restart
```

1.2 ติดตั้งแพคเกจ freeradius และแพคเกจสนับสนุน

```
apt install freeradius -y
apt install easy-rsa -y
apt install wget -y

update-rc.d freeradius enable
```

1.3 ดาวน์โหลดและคอมไพล์เครื่องมือสำหรับทดสอบ

เป็นเครื่องมือหรือโปรแกรมสำหรับใช้ทดสอบการทำงานไปยัง RADIUS Server โดยสามารถทดสอบกับ RADIUS Server เกี่ยวกับ WPA-Enterprise ถึงขั้น phase-2 ได้

```
apt install gcc make pkg-config -y
apt install libssl-dev libnl-3-dev libnl-genl-3-dev -y

cd /etc/freeradius/3.0
```

```
wget \
http://www.rmuti.ac.th/user/prakai/p/2020-01-freeradius-test-t
ool.tar.gz

tar vxfz 2020-01-freeradius-test-tool.tar.gz

cd tool/wpa_supplicant-2.7/wpa_supplicant

cp -f defconfig .config

nano .config
    --------
    ...
    #CONFIG_DRIVER_NL80211=y
    ...
    CONFIG_EAPOL_TEST=y
    ...

make eapol_test
cp eapol_test ../../bin
```

ref: http://deployingradius.com/scripts/eapol_test

1.4 ดาวน์โหลดชุดไฟล์คุณสมบัติสำเร็จรูป

เป็นไฟล์คุณสมบัติสำเร็จรูปจะได้รับการปรับแต่งค่าตัวแปรบางส่วนไว้แล้ว

```
cd /etc/freeradius/3.0
wget \
http://www.rmuti.ac.th/user/prakai/p/2020-01-freeradius-3-debi
an-eduroam.tar.gz
```

1.5 แตกไฟล์คุณสมบัติสำเร็จรูป

แตกไฟล์คุณสมบัติสำเร็จรูป โดยไฟล์คุณสมบัติสำเร็จรูปมีหลายไฟล์ ได้รับการปรับแต่งค่าตัวแปรบางส่วนไว้แล้ว รวมถึงได้ตัดคำอธิบาย (comment) ออกไป เพื่อให้เนื้อหาในไฟล์มีความกระชับขึ้น

```
tar vxfz 2020-01-freeradius-3-debian-eduroam.tar.gz
```

รายการไฟล์คุณสมบัติสำเร็จรูปมีดังนี้

- คุณสมบัติหลักของ freeradius 3.0 ใช้ดูเพื่อเทียบสำหรับแก้ไขไฟล์ปัจจุบัน
  `radiusd-eduroam.conf`
- การคัดกรองบัญชีผู้ใช้หรือ realm ที่ไม่ถูกต้อง
  `eduroam-realm-checks.conf`
  `eduroam-mon-checks.conf`
- ประกาศไซต์หรือการบริการของ freeradius สำหรับ eduroam แบบ Main realm หรือ Sub-realm
  `sites-available/eduroam-main`
  `sites-available/eduroam-sub`
  `sites-available/eduroam-inner-tunnel`
  `sites-available/eduroam-status`
- การเชื่อมต่อกับ radius เครื่องอื่น เช่น NRO, Main realm หรือ Sub-realm
  `proxy-eduroam-main.conf`
  `proxy-eduroam-sub.conf`
  `clients-eduroam-main.conf`
  `clients-eduroam-sub.conf`
- คุณสมบัติโมดูล EAP และ attr_filter
  `mods-available/eap-eduroam`
  `mods-config/attr_filter/pre-proxy`
- บัญชีผู้ใช้แบบไฟล์
  `mods-available/files-eduroam`
  `mods-config/files-eduroam/accounting`
  `mods-config/files-eduroam/pre-proxy`
  `mods-config/files-eduroam/authorize`
- บัญชีผู้ใช้จาก LDAP server
  `mods-available/ldap-eduroam`
- บัญชีผู้ใช้จาก Microsoft Active Directory
  `mods-available/mschap-eduroam`

- บัญชีผู้ใช้จาก MySQL server
  `mods-available/sql-eduroam`
  `mods-config/sql/main/mysql/queries-eduroam.conf`

1.6 แก้ไขไฟล์ radiusd.conf

โดยปรับแก้เฉพาะจุดโดยเทียบจากไฟล์ radiusd-eduroam.conf

```
cd /etc/freeradius/3.0

nano radiusd.conf
    --------
    # Change some configurations in radiusd.conf as show below

    # PROXY CONFIGURATION
    #
    proxy_requests  = yes
    $INCLUDE proxy.conf
    #  eduroam
    $INCLUDE proxy-eduroam.conf

    ...

    # CLIENTS CONFIGURATION
    #
    $INCLUDE clients.conf
    #  eduroam
    $INCLUDE clients-eduroam.conf
```

1.7 สำเนาไฟล์สำหรับการเป็นผู้ให้บริการหลัก (Main Realm) ของสถาบัน

เลือกใช้ไฟล์สำหรับ Main Realm

```
cd /etc/freeradius/3.0
```

```
cp proxy-eduroam-sub.conf  proxy-eduroam.conf
cp clients-eduroam-sub.conf  clients-eduroam.conf
cp sites-available/eduroam-sub  sites-available/eduroam
```

1.8 แก้ไขไฟล์ proxy-eduroam.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano proxy-eduroam.conf
    --------
    #
    #  Realm abc of UXX.AC.TH at local service
    #
    realm abc.uxx.ac.th {
            auth_pool = localhost
            nostrip
    }
```

1.9 แก้ไขไฟล์ sites- available/eduroam

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano sites-available/eduroam
    --------
    authorize {

    # Change realm to be LOCAL for local user
    if( (&Realm =~ /^abc.uxx.ac.th$$/) ) {
        #
        # If user database is on local (file, LDAP, MySQL),
        # uncomment this block.
```

```
        #
        update control {
             Proxy-To-Realm := LOCAL
        }
        #
        # - OR -
        # If user database is on NPS, uncomment this block
        #
        #update control {
        #    Proxy-To-Realm := "nps.abc.uxx.ac.th"
        #}
    }
    ...

    pre-proxy {

        # Update Operator-Name to IdP
        if (!Operator-Name) {
             update proxy-request {
                 Operator-Name := "1abc.uxx.ac.th"
             }
        }
        ...
    }
```

1.10 ยกเลิกไซต์เดิม และเปิดใช้ไซต์ใหม่

```
cd /etc/freeradius/3.0/sites-enabled

rm -f default
rm -f inner-tunnel
ln -s ../sites-available/eduroam
ln -s ../sites-available/eduroam-inner-tunnel
ln -s ../sites-available/eduroam-status
cd ..
```

1.11 เปิดใช้โมดูล eap-eduroam และ files-eduroam

```
cd /etc/freeradius/3.0/mods-enabled

ln -s ../mods-available/eap-eduroam
ln -s ../mods-available/files-eduroam
cd ..
```

1.12 สร้างไฟล์ Certificate

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0/certs

rm *
cp /usr/share/doc/freeradius/examples/certs/* .

nano ca.cnf
    --------
    [ CA_default ]
    ...
    default_days        = 3650
    ...

    [certificate_authority]
    countryName         = TH
    stateOrProvinceName = Bangkok
    localityName        = -
    organizationName    = XX University
    emailAddress        = eduroam@uxx.ac.th
    commonName          = "UXX Wi-Fi Certificate Authority"
```

```
nano server.cnf
    --------
    [ CA_default ]
    ...
    default_days        = 3650
    ...

    [server]
    countryName         = TH
    stateOrProvinceName = Bangkok
    localityName        = -
    organizationName    = XX University
    emailAddress        = eduroam@uxx.ac.th
    commonName          = "UXX Wi-Fi Certificate"


nano client.cnf
    --------
    [ CA_default ]
    ...
    default_days        = 3650
    ...

    [client]
    countryName         = TH
    stateOrProvinceName = Bangkok
    localityName        = -
    organizationName    = XX University
    emailAddress        = eduroam@uxx.ac.th
    commonName          = eduroam@uxx.ac.th

nano Makefile
    --------
    ...
    dh:
        $(OPENSSL) dhparam -dsaparam -out dh $(DH_KEY_SIZE)

./bootstrap
```

```
cd ..
```

1.13 เปลี่ยนสิทธิ์หรือเจ้าของของไฟล์

```
chown -R freerad:freerad /etc/freeradius/3.0
```

1.14 ทดสอบการทำงานแบบพื้นฐาน

บัญชีผู้ใช้สำหรับการทดสอบอยู่ในไฟล์ mods-config/files-eduroam/authorize

```
nano mods-config/files-eduroam/authorize
    --------
    eduroam  Cleartext-Password := "TESTING-PASSWORD"
```

หน้าจอที่ 1

```
service freeradius stop
freeradius -X
   --------
   (stop debugging with CTRL+C)
```

หน้าจอที่ 2

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
          -u 'eduroam@abc.uxx.ac.th' \
          -p 'TESTING-PASSWORD' \
          -v -m IEEE8021X \
          -s eduroam -e PEAP -2 MSCHAPV2
   --------
```

```
access-accept; 0
RADIUS message: code=2 (Access-Accept) identifier=8
length=187
   Attribute 27 (Session-Timeout) length=6
     Value: 600
   Attribute 1 (User-Name) length=21
     Value: 'eduroam@abc.uxx.ac.th'
   Attribute 79 (EAP-Message) length=6
     Value: 03080004
   Attribute 80 (Message-Authenticator) length=18
     Value: 6668fe5c30e59946dc91ad7200c0a810
```

2) การเชื่อมต่อกับเครื่องให้บริการหลัก (Main-Realm) ของสถาบัน

2.1 แก้ไขไฟล์ radiusd.conf

โดยปรับแก้เฉพาะจุดโดยเทียบจากไฟล์ radiusd-eduroam.conf

```
cd /etc/freeradius/3.0

nano radiusd.conf
    --------
    # Change some configurations in radiusd.conf as show below

    # PROXY CONFIGURATION
    #
    proxy_requests  = yes
    $INCLUDE proxy.conf
    #  eduroam
    $INCLUDE proxy-eduroam.conf

    # CLIENTS CONFIGURATION
    #
    $INCLUDE clients.conf
    #  eduroam
    $INCLUDE clients-eduroam.conf
```

2.2 แก้ไขไฟล์ proxy-eduroam.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano proxy-eduroam.conf
    --------
    #
```

```
#  home server for UXX.AC.TH -- Main Realm
#
home_server eduroam-uxx-ac-th {
    type = auth+acct
    ipaddr = xxx.xxx.xxx.xxx # 192.168.1.1
    port = 1812
    secret = XXXXXXXXXXXXXXXX
    #src_ipaddr = xxx.xxx.xxx.xxx
    status_check = status-server
    require_message_authenticator = yes

    #check_interval = 30
    #check_timeout = 8

    #revive_interval = 360

    #response_window = 60
    #response_timeouts = 8

    #num_answers_to_alive = 3
    #zombie_period = 60
}

#
#  home server pool for UXX.AC.TH -- Main Realm
#
home_server_pool eduroam-uxx-ac-th {
    type = fail-over
    home_server = eduroam-uxx-ac-th
}

#
#  realm for UXX.AC.TH -- Main Realm
#
realm eduroam {
    auth_pool = eduroam-uxx-ac-th
    nostrip
}
```

2.3 แก้ไขไฟล์ clients-eduroam.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano clients-eduroam.conf
    ------
    #
    #  UXX.AC.TH server -- Main Realm
    #
    client eduroam-uxx-ac-th {
            ipaddr = xxx.xxx.xxx.xxx # 192.168.1.1
            netmask = 32
            secret = XXXXXXXXXXXXXXXX
            require_message_authenticator = no
            shortname = eduroam-uxx-ac-th
            nastype = other
            virtual_server = eduroam
    }
```

2.4 ทดสอบการทำงานด้วยผู้ใช้ eduroam จากเครื่องให้บริการหลัก (Main Realm) ของสถาบัน

บัญชีผู้ใช้สำหรับการทดสอบอยู่ใน**ไฟล์ที่เครื่องให้บริการหลักของสถาบัน**

```
mods-config/files-eduroam/authorize
```

หน้าจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หน้าจอที่ 2

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
          -u 'eduroam@uxx.ac.th' \
          -p 'TESTING-PASSWORD' \
          -v -m IEEE8021X \
          -s eduroam -e PEAP -2 MSCHAPV2
       --------
       access-accept; 0
       RADIUS message: code=2 (Access-Accept) identifier=8
       length=187
          Attribute 27 (Session-Timeout) length=6
            Value: 600
          Attribute 1 (User-Name) length=21
            Value: 'eduroam@uxx.ac.th'
          Attribute 79 (EAP-Message) length=6
            Value: 03080004
          Attribute 80 (Message-Authenticator) length=18
            Value: 4f334b7622ec20537163ac31c1926d84
```

3) การติดตั้งโดยมี LDAP Server เป็นฐานข้อมูลบัญชีผู้ใช้

เป็นการติดตั้งและกำหนดคุณสมบัติพื้นฐานให้ RADIUS Server สามารถทำงานกับ LDAP server (OpenLDAP) เพื่อใช้บัญชีผู้ใช้จากฐานข้อมูล LDAP ข้อมูลบัญชีผู้ใช้ควรมีการเก็บรหัสผ่านในรูปแบบ NT/LM Hash (NT-Password, LM-Password)

การทำงานของ RADIUS Server จะติดต่อโดยตรงไปยัง LDAP server ผ่านโมดูลที่มีอยู่ใน RADIUS Server

3.1 โครงสร้างข้อมูลใน LDAP Server

ตัวอย่างโครงสร้างหลักโดยย่อของข้อมูลผู้ใช้ใน LDAP Server

```
dn: dc=uxx,dc=ac,dc=th
objectClass: top
objectClass: organization
dc: u

dn: ou=People,dc=uxx,dc=ac,dc=th
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=uxx,dc=ac,dc=th
ou: Group
objectClass: top
objectClass: organizationalUnit

dn: cn=Users,ou=Group,dc=uxx,dc=ac,dc=th
cn: Users
objectClass: posixGroup
gidNumber: 1001
description: Group of Users on Unix System

dn: uid=user,ou=People,dc=uxx,dc=ac,dc=th
```

```
cn: User
sn: User
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
uid: user
uidNumber: 1001
gidNumber: 1001
loginShell: /bin/bash
homeDirectory: /home/user
gecos: User User
description: User User
displayName: User User
sambaAcctFlags: [U       ]
sambaLMPassword: C8DFD5AC0546E95DFF17365FAF1FFE89
sambaNTPassword: 2C47AA9B5AC02360473ECE87B6800920
sambaSID: ...
sambaPrimaryGroupSID: ...
userPassword::
e1NTSEF9Y0F1dXBVNURlbVFhakxxaDFSU2VVTHl5Wi9NQ1dlSXM=
```

3.2 ติดตั้งแพคเกจ freeradius-ldap

ติดตั้ง module เสริม เพื่อให้ freeradius เข้าถึงข้อมูลจาก LDAP ได้

```
apt install freeradius-ldap -y
```

3.3 แก้ไขไฟล์ sites-available/eduroam-inner-tunnel

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0
```

```
nano sites-available/eduroam-inner-tunnel
    --------
    authorize {

        ...
        group {
             #  Read the 'users-eduroam' file
             files-eduroam {
                  # return if match
                  ok = return
                  update = return
             }
             #
             # for LDAP
             ldap-eduroam {
                  # return if match
                  ok = return
                  update = return
             }
             # for Active Directory
             #mschap-eduroam {
             #    # return if match
             #    ok = return
             #    update = return
             #}
             # for MySQL
             #sql-eduroam {
             #    # return if match
             #    ok = return
             #    update = return
             #}
             ...
        }
        ...
    }

    authenticate {
```

```
        # PAP Authentication
        Auth-Type PAP {
             pap
        }
        ...
        #
        # MSCHAP Authentication
        # for file-eduroam and/or LDAP and/or MySQL
        Auth-Type MS-CHAP {
             mschap
        }

        # MSCHAP Authentication
        # for Active Directory
        #Auth-Type MS-CHAP {
        #    mschap-eduroam
        #}

        # Allow EAP authentication.
        eap-eduroam

    }
    ...
```

3.4 แก้ไขไฟล์ modules/ldap-eduroam

โดยปรับแก้ทุกจุดให้ถูกต้อง สัมพันธ์กับ LDAP server

```
cd /etc/freeradius/3.0

nano mods-available/ldap-eduroam
    --------
    ldap ldap-eduroam {

    #   server = "your-ldap-server-host-name" # ldap.uxx.ac.th
        server = "your-ldap-server-host-ip" # 192.168.1.2
```

```
#   port = 398

#   identity = "cn=admin,dc=uxx,dc=ac,dc=th"
#   password = mypass

    basedn = "dc=uxx,dc=ac,dc=th "

    update {
         control:Password-With-Header += 'userPassword'
#        control:NT-Password          := 'ntPassword'
         control:NT-Password          := 'sambaNTPassword'
         ...
    }
    ...
    user {
         ...
         filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
         ...
         access_attribute = 'uid'
         ...
    }
    ...
}
```

3.5 เปิดใช้งานโมดูล ldap-eduroam

```
cd /etc/freeradius/3.0/mods-enabled

ln -s ../mods-available/ldap-eduroam
```

3.6 เปลี่ยนสิทธิ์หรือเจ้าของของไฟล์

```
chown -R freerad:freerad /etc/freeradius/3.0
```

3.7 ทดสอบการทำงานด้วยผู้ใช้จาก LDAP Server

หน้าจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หน้าจอที่ 2

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
            -u 'user@abc.uxx.ac.th' -p 'Asdf1234' \
            -v -m IEEE8021X \
            -s eduroam -e PEAP -2 MSCHAPV2
       --------
       access-accept; 0
       RADIUS message: code=2 (Access-Accept) identifier=8
       length=187
          Attribute 27 (Session-Timeout) length=6
            Value: 600
          Attribute 1 (User-Name) length=21
            Value: 'user@abc.uxx.ac.th'
          Attribute 79 (EAP-Message) length=6
            Value: 03080004
          Attribute 80 (Message-Authenticator) length=18
            Value: 4f334b7622ec20537163ac31c1926d84
```

4) การติดตั้งโดยมี MySQL เป็นฐานข้อมูลบัญชีผู้ใช้

เป็นการติดตั้งและกำหนดคุณสมบัติพื้นฐานให้ RADIUS Server สามารถทำงานโดยเข้าถึงฐานข้อมูลผู้ใช้ที่เก็บไว้ในเซิร์ฟเวอร์ MySQL

ข้อมูลบัญชีผู้ใช้ที่เก็บในรูปแบบของฐานข้อมูลนั้น สามารถมีโครงสร้างใดก็ได้ ขึ้นอยู่กับมหาวิทยลัยออกแบบและจัดเก็บ แต่ในคู่มือนี้ จะอ้างอิงรูปแบบการจัดเก็บข้อมูลตามวิธีการพื้นฐานของ freeradius-mysql

4.1 โครงสร้างข้อมูลใน MySQL Server

องค์ประกอบพื้นฐานที่สุดของการจัดเก็บข้อมูลบัญชีผู้ใช้ ตามรูปแบบของ freeradius-mysql นั้น ข้อมูลผู้ใช้จะเก็บไว้ในตาราง ชื่อ radcheck มีรูปแบบของข้อมูลผู้ใช้ ดังนี้

```
mysql> select * from radcheck;
+----+----------+--------------------+----+----------+
| id | username | attribute          | op | value    |
+----+----------+--------------------+----+----------+
|  1 | user     | Cleartext-Password | := | Asdf1234 |
+----+----------+--------------------+----+----------+

mysql> select * from radcheck;
+----+----------+-------------+----+----------------------+
| id | username | attribute   | op | value                |
+----+----------+-------------+----+----------------------+
|  1 | user     | NT-Password | := | 2C47AA9B5AC02360473..|
|  2 | user     | LM-Password | := | C8DFD5AC0546E95DFF1..|
+----+----------+-------------+----+----------------------+
```

4.2 ติดตั้งแพคเกจ freeradius-mysql

ติดตั้ง module เสริม เพื่อให้ freeradius เข้าถึงข้อมูลจาก MySQL ได้

```
apt-get install freeradius-mysql -y
```

4.3 แก้ไขไฟล์ sites-available/eduroam-inner-tunnel

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano sites-available/eduroam-inner-tunnel
    --------
    authorize {
        ...
        group {
            #  Read the 'users-eduroam' file
            files-eduroam {
                # return if match
                ok = return
                updated = return
            }
            #
            # for LDAP
            #ldap-eduroam {
            #   # return if match
            #   ok = return
            #   updated = return
            #}
            # for Active Directory
            #mschap-eduroam {
            #   # return if match
            #   ok = return
            #   updated = return
            #}
            # for MySQL
            sql- eduroam {
                 # return if match
                 ok = return
```

```
                updated = return
            }
            ...
        }
        ...
    }

    authenticate {

        # PAP Authentication
        Auth-Type PAP {
             pap
        }
        ...
        # MSCHAP Authentication
        # for file-eduroam and/or LDAP and/or MySQL
        Auth-Type MS-CHAP {
             mschap
        }

        # MSCHAP Authentication
        # for Active Directory
        #Auth-Type MS-CHAP {
        #    mschap-eduroam
        #}

        eap-eduroam

    }
    ...
```

4.4 แก้ไขไฟล์ mods-available/sql-eduroam

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0
```

```
nano mods-available/sql-eduroam
    --------
    sql sql-eduroam {
        ...
        #
        driver = "rlm_sql_mysql"
        dialect = "mysql"
        ...
        # Connection info:
        server = "<mysql_server_host_address>" # 192.168.1.2
        #port = 3306
        login = "radius"
        password = "radpass"

        radius_db = "radius"

        acct_table1 = "radacct"
        acct_table2 = "radacct"
        ...
    }
```

4.5 แก้ไขไฟล์ mods-config/sql/main/mysql/queries-eduroam.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

กรณีมีฐานข้อมูลบัญชีผู้ใช้ที่ไม่เป็นไปตามรูปแบบของ freeradius-mysql จำเป็นต้องแก้ไขคำสั่ง SQL เพื่อให้เหมาะสมกับโครงสร้างข้อมูลนั้น

```
cd /etc/freeradius/3.0

nano mods-config/sql/main/mysql/queries-eduroam.conf
    --------
    ...
    #  Query config:  Username
```

```
...
sql_user_name = "%{%{Stripped-User-Name}:-%{%{User-Name}:-DEFAULT}}"
#sql_user_name = "%{User-Name}"
...
#  Authorization Queries
...
authorize_check_query = "\
        SELECT id, username, attribute, value, op \
        FROM ${authcheck_table} \
        WHERE username = '%{SQL-User-Name}' \
        ORDER BY id"

authorize_reply_query = "\
        SELECT id, username, attribute, value, op \
        FROM ${authreply_table} \
        WHERE username = '%{SQL-User-Name}' \
        ORDER BY id"
...
#group_membership_query = "\
#       SELECT groupname \
...
#       ORDER BY priority"

#authorize_group_check_query = "\
#       SELECT id, groupname, attribute, \
...
#       ORDER BY id"

#authorize_group_reply_query = "\
#       SELECT id, groupname, attribute, \
...
#       ORDER BY id"
...
```

4.6 เปิดใช้งานโมดูล ldap-eduroam

```
cd /etc/freeradius/3.0/mods-enabled

ln -s ../mods-available/sql-eduroam
```

4.7 เปลี่ยนสิทธิ์หรือเจ้าของของไฟล์

```
chown -R freerad:freerad /etc/freeradius/3.0
```

4.8 ทดสอบการทำงานด้วยผู้ใช้จาก MySQL

หน้าจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หน้าจอที่ 2

```
 cd /etc/freeradius/3.0/tool

 ./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
            -u 'user@abc.uxx.ac.th' -p 'Asdf1234' \
            -v -m IEEE8021X \
            -s eduroam -e PEAP -2 MSCHAPV2
        --------
        access-accept; 0
        RADIUS message: code=2 (Access-Accept) identifier=8
        length=187
           Attribute 27 (Session-Timeout) length=6
             Value: 600
           Attribute 1 (User-Name) length=21
             Value: 'user@abc.uxx.ac.th'
```

```
Attribute 79 (EAP-Message) length=6
  Value: 03080004
Attribute 80 (Message-Authenticator) length=18
  Value: 4f334b7622ec20537163ac31c1926d84
```

5) การติดตั้งโดยใช้ Microsoft NPS เป็นกลางเข้าถึงฐานข้อมูลบัญชีผู้ใช้

กรณีที่สถาบันมีบัญชีผู้ใช้อยู่ใน Microsoft Active Directory บนเครื่อง Microsoft Windows Server 2012 ขึ้นไป จะมีโปรแกรมที่เป็นช่องทางในการเข้าถึงฐานข้อมูลบัญชีผู้ใช้โดยไม่ต้องเข้าถึงบริการ Microsoft Active Directory โดยตรง โปรแกรมที่ Microsoft พัฒนาขึ้นมาให้ใช้นี้คือ Microsoft NPS (Network Policy Service)

โปรแกรม Microsoft NPS มีช่องทางการใช้บริการเช่นเดียวกันกับ RADIUS มาตรฐาน ดังนั้น กรณีเป็นการกำหนดคุณสมบัติของโปรแกรม freeradius ให้ส่งต่อการร้องขอไปยัง Microsoft NPS และโปรแกรม Microsoft NPS จะดำเนินการตรวจสอบบัญชีผู้ใช้ใน Microsoft Active Directory อีกชั้น

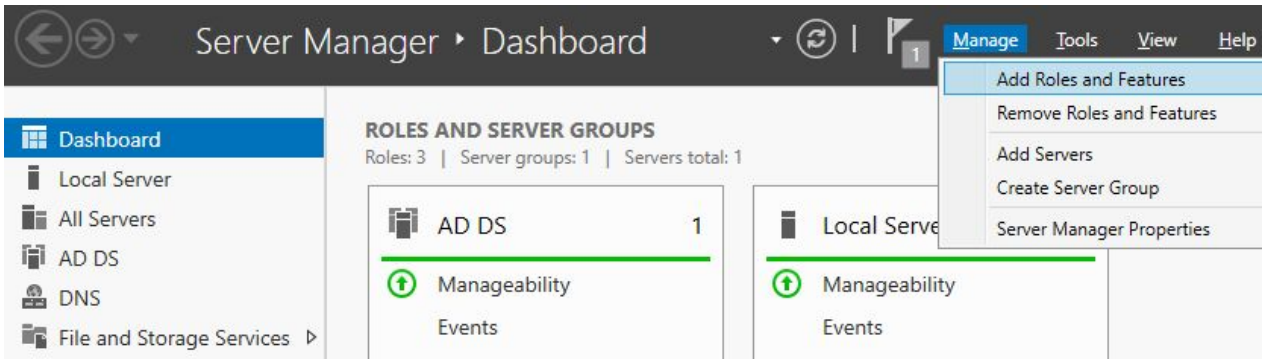
การกำหนดคุณสมบัตินี้เป็นการทำให้ freeradius ทำหน้าที่เป็น proxy ไปยัง Microsoft NPS หรือ เมื่อมีการร้องขอตรวจสอบบัญชีผู้ใช้มายัง freeradius โปรแกรม freeradius จะส่งต่อการร้องขอทั้งหมดไปยัง Microsoft NPS และในทางกลับกัน โปรแกรม freeradius จะรับผลการร้องขอจาก Microsoft NPS และส่งต่อไปยังเครื่องต้นทางที่ร้องขอการตรวจสอบบัญชีผู้ใช้

ในคู่มือนี้จะแนะนำการกำหนดคุณสมบัติโดยมี Microsoft Active Directory อยู่แล้ว จึงเหลือขั้นตอนการดำเนินการ 2 ส่วน และ 1 ส่วนเสริม ประกอบด้วย

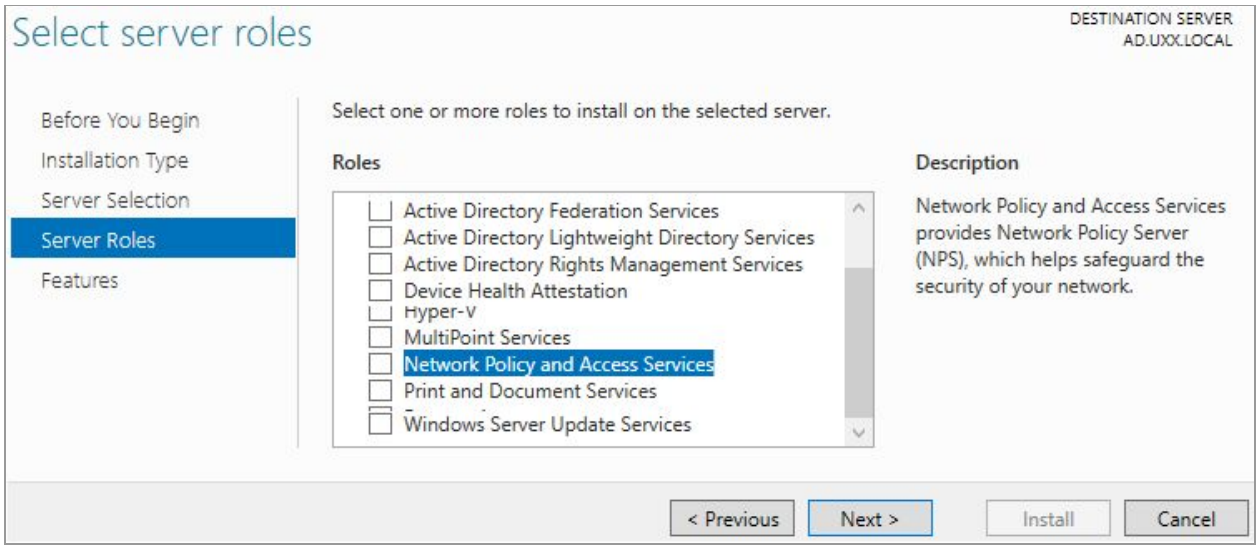
1) การติดตั้งและกำหนดคุณสมบัติของโปรแกรม Microsoft NPS (5.1 - 5.3)
2) (เสริม) เพิ่ม Realm ให้ Active Directory (5.4 - 5.6)
3) การกำหนดคุณสมบัติโปรแกรม freeradius (5.7+)

5.1 เพิ่มบริการ Microsoft Network Policy and Access Service ใน Microsoft Windows Server

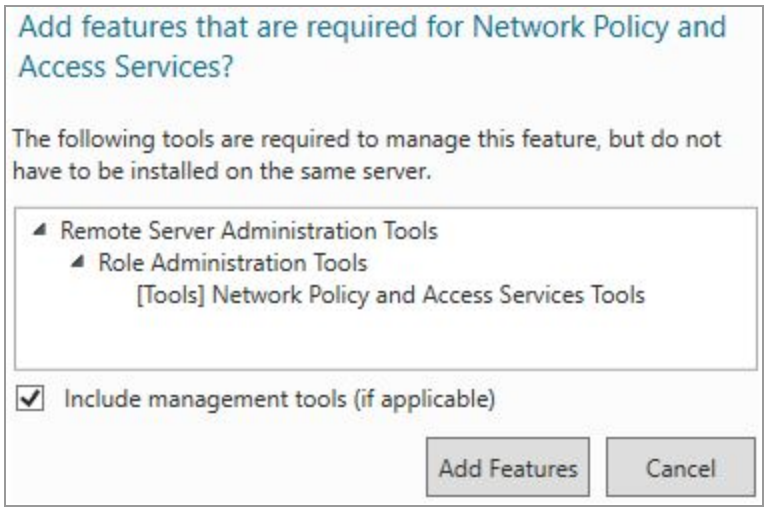
- ที่โปรแกรม **Server Manager** คลิกรายการ **Dashboard** ที่รายการด้านซ้าย
- ที่เมนูด้านบนขวา คลิกเมนู **Manage** >> **Add Roles and Features**



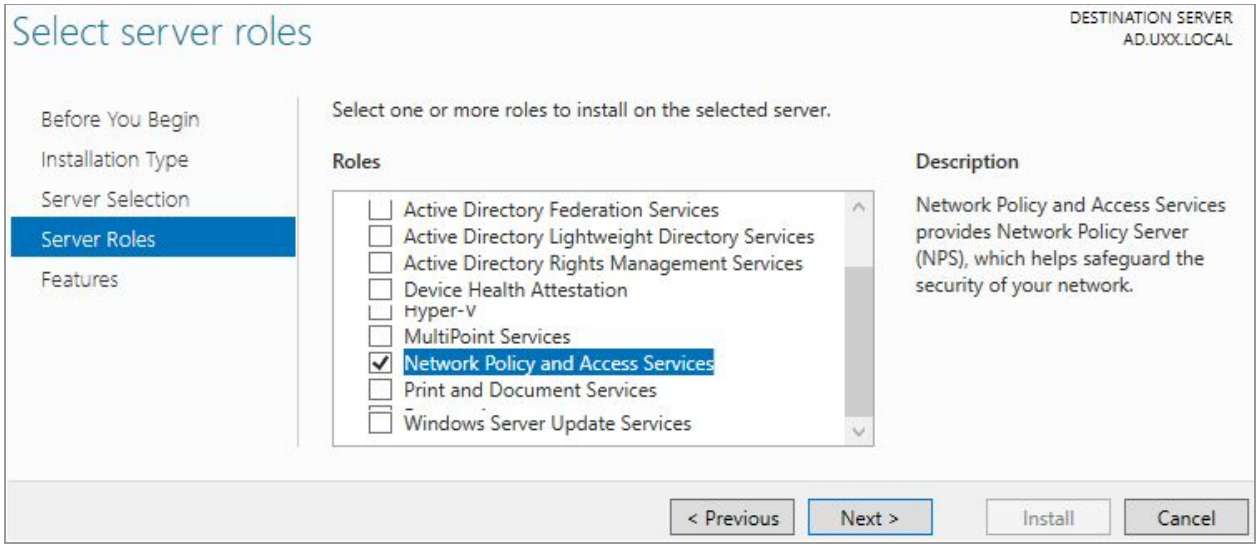
- ที่หน้าต่าง Before you begin คลิกปุ่ม **Next**
- ที่หน้าต่าง Select installation type เลือก Role-based and feature-based installation และคลิกปุ่ม **Next**
- ที่หน้าต่าง Select destination server เลือก **Select a server from the server pool** เลือกเซิร์ฟเวอร์จากรายการ และคลิกปุ่ม **Next**
- ที่หน้าต่าง Select server roles ในรายการ Role เลือก **Network Policy and Access Service**



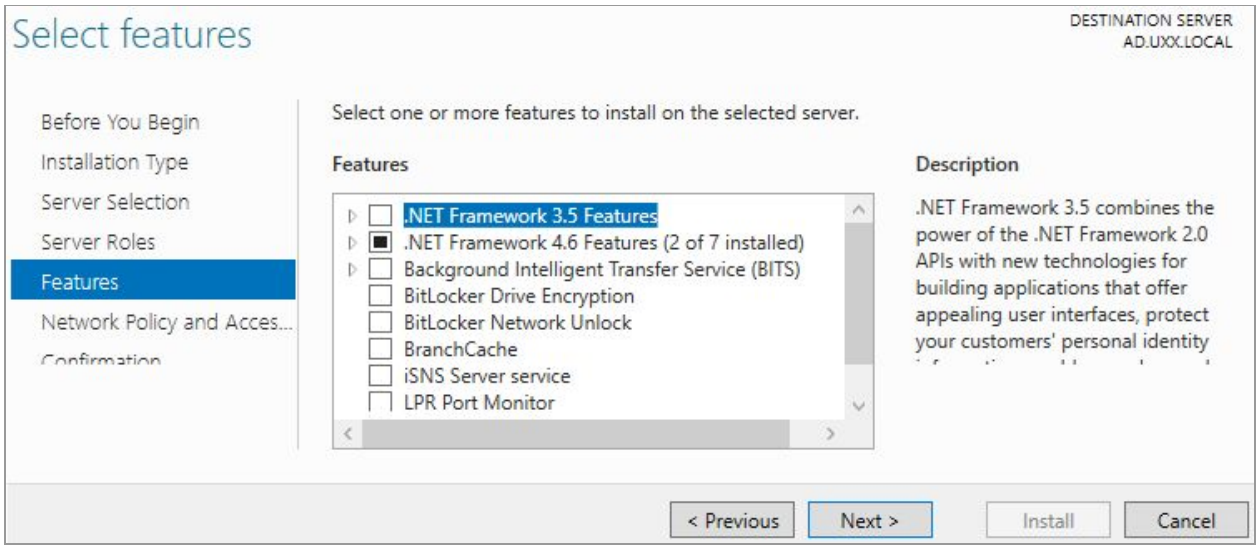
- ที่หน้าต่าง Add features that are required for Network Policy and Access Service? คลิกปุ่ม **Add Features**



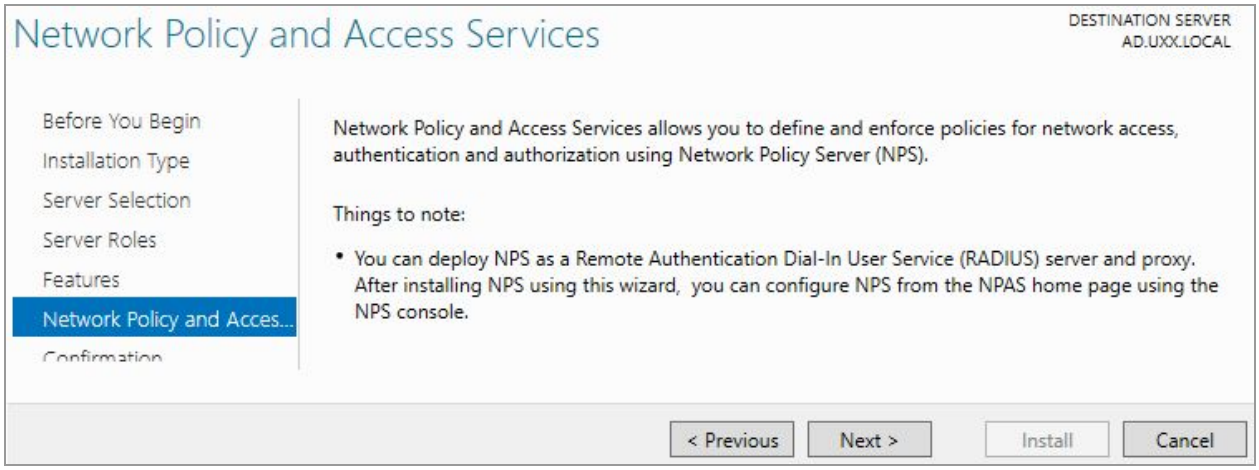
- ที่หน้าต่าง Select server roles ในรายการ Role คลิกปุ่ม **Next**



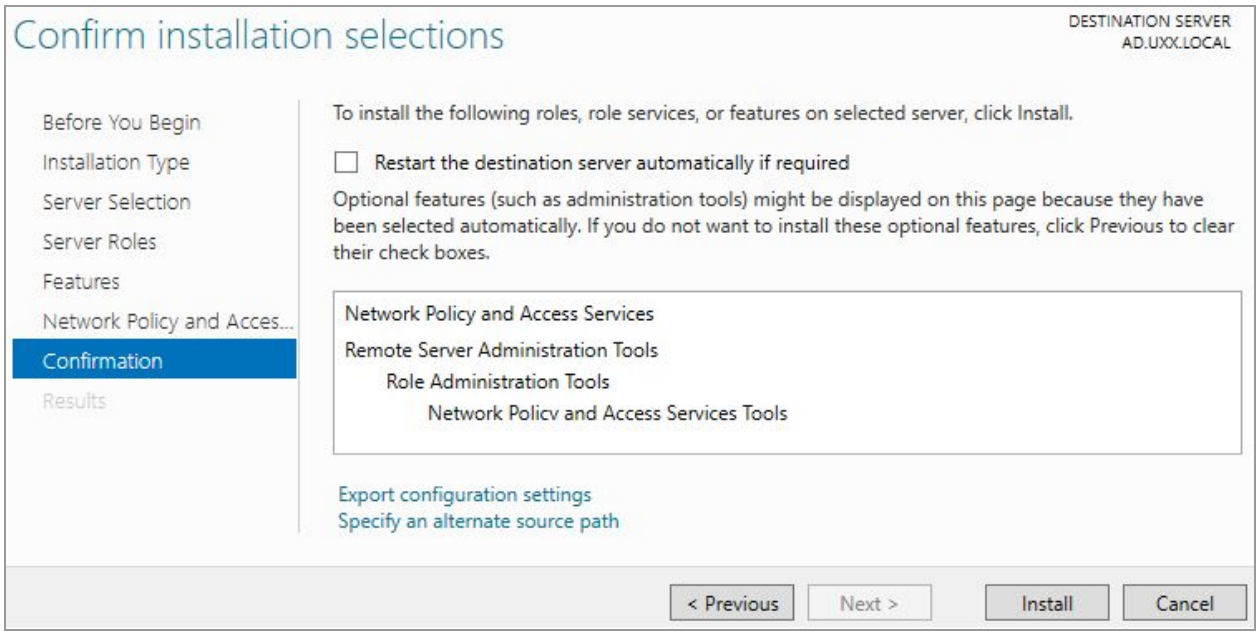
- ที่หน้าต่าง Features คลิกปุ่ม **Next**



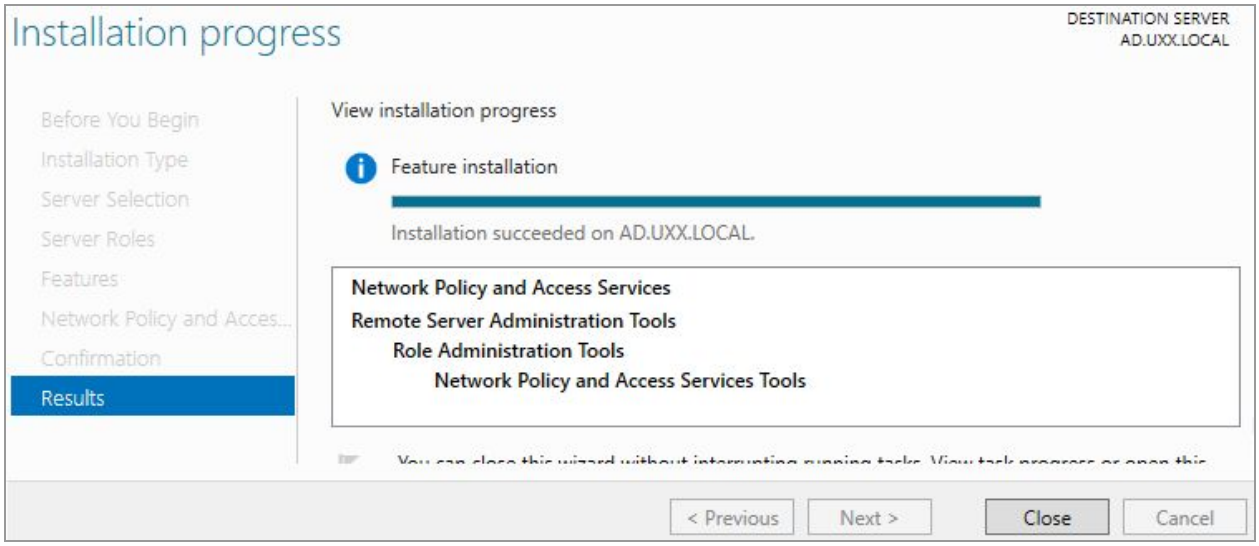
- ที่หน้าต่าง Network Policy and Access Service คลิกปุ่ม **Next**



- ที่หน้าต่าง Confirm installation selection คลิกปุ่ม Install



- หลังจากดำเนินการติดตั้งบริการแล้วเสร็จ ที่หน้าต่าง Installation progress คลิกปุ่ม **Close**



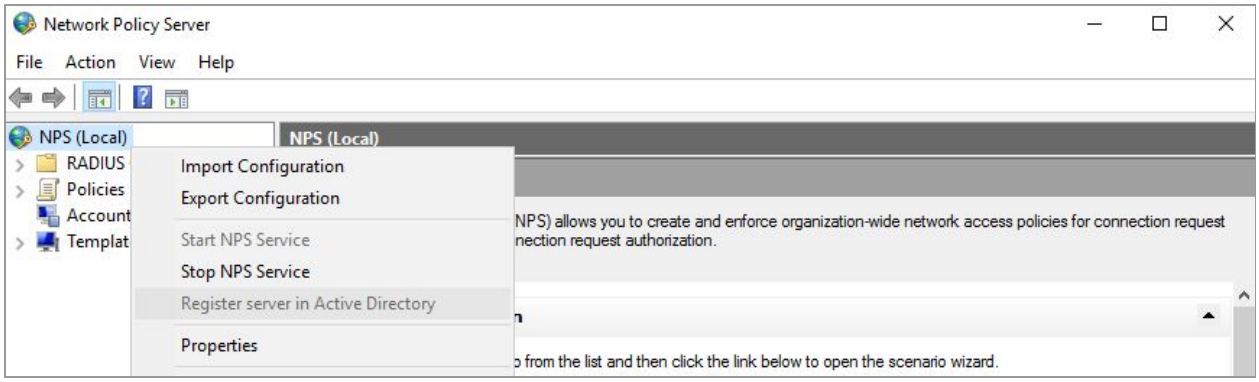
5.2 สร้าง Self-signed Certificate

- เปิดโปรแกรม **Windows PowerShell**
- สร้าง Self-signed Certificate ด้วยคำสั่ง (ในบรรทัดเดียว)

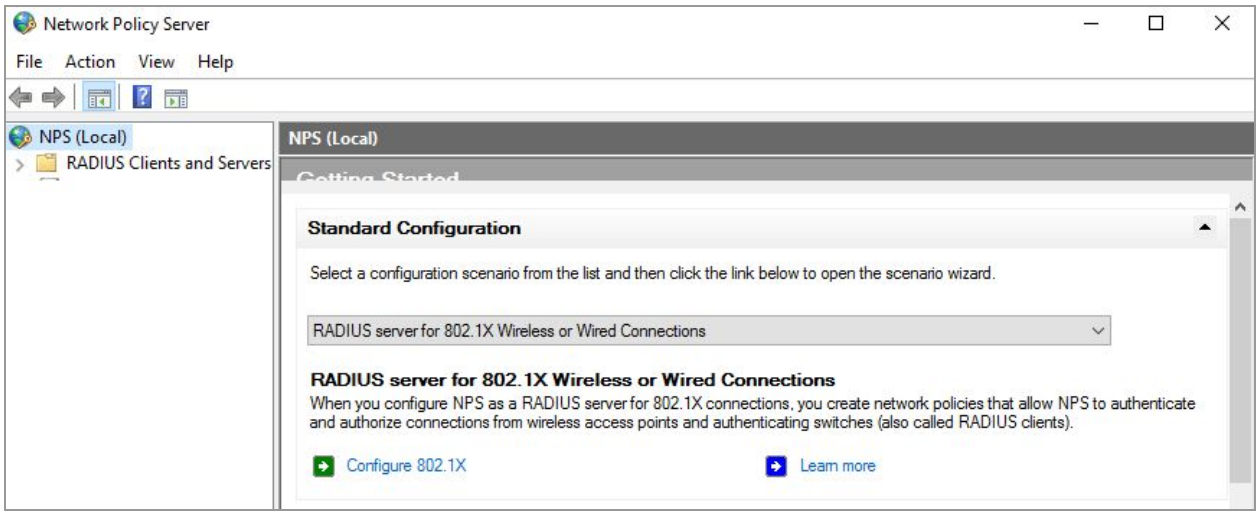
```
PS C:\> New-SelfSignedCertificate
          -DnsName eduroam.uxx.ac.th
          -CertStoreLocation cert:\LocalMachine\My
          -NotAfter (Get-Date).AddYears(10)
```

5.3 กำหนดคุณสมบัติ Microsoft Network Policy Service

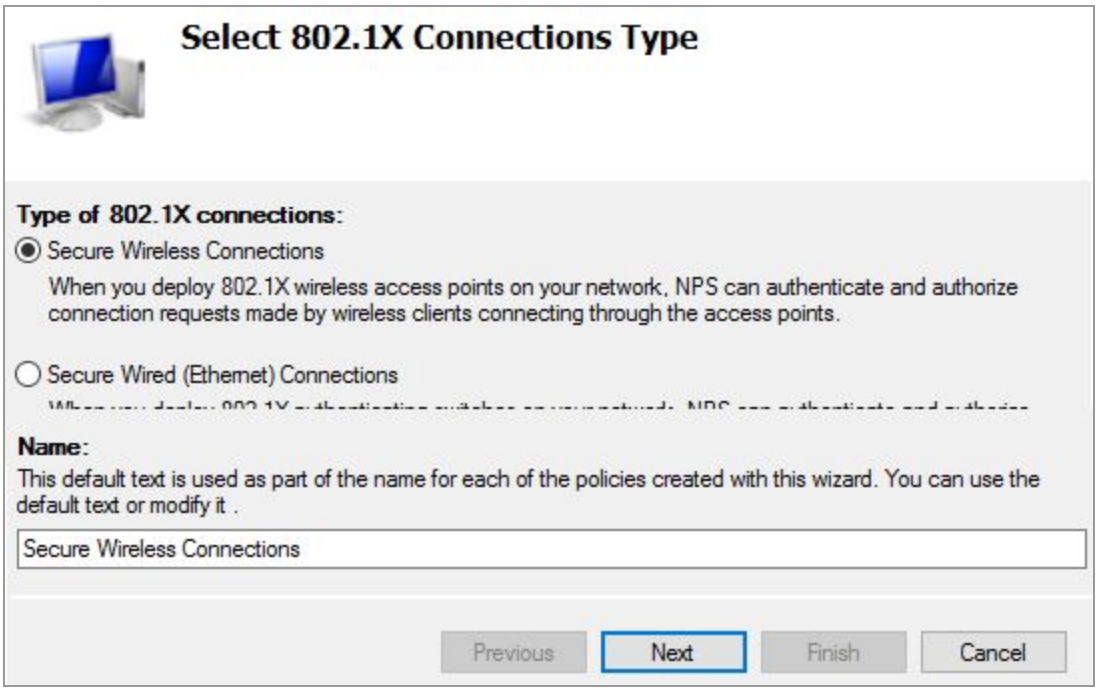
- ที่โปรแกรม **Server Manager** ที่เมนูด้านบนขวา คลิกเมนู **Tools** >> **Network Policy Service**
- ที่โปรแกรม Network Policy Service คลิกปุ่มด้านขวามของเมาส์ที่รายการด้านซ้าย รายการ **NPS (Local)** แล้วเลือกเมนู **Register server in Active Directory** และยอมรับหรือดำเนินการต่อไปจนแล้วเสร็จ



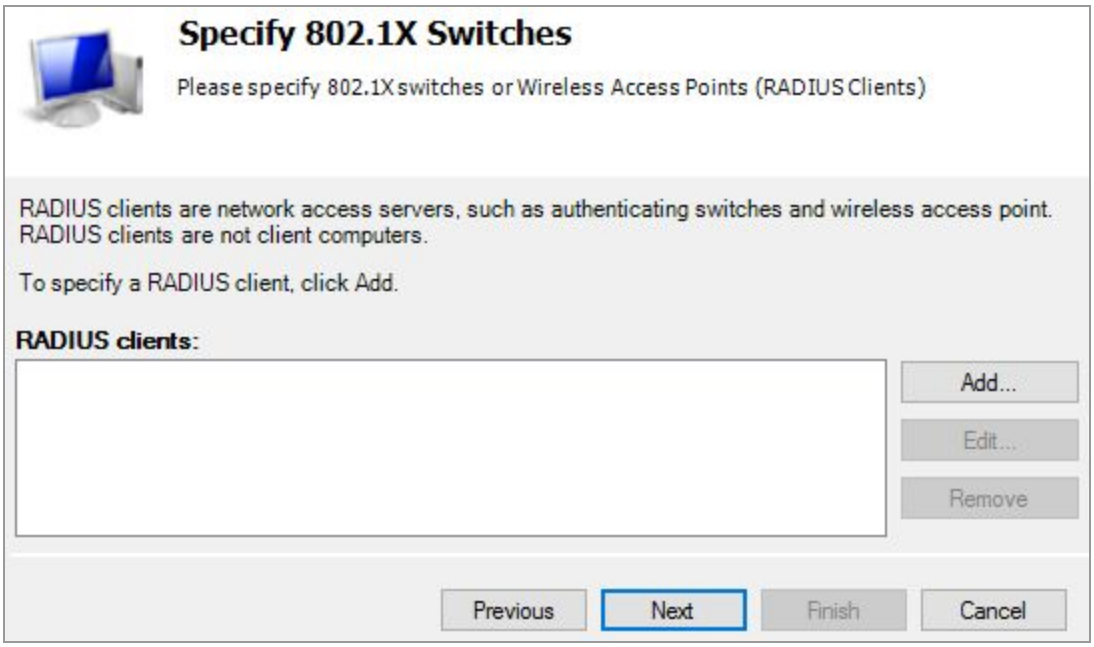
- ที่โปรแกรม Network Policy Service เลือกรายการกลางหน้าจอ รายการ **RADIUS server for 802.1X Wireless or Wired Connections** และคลิกลิงค์ **Configure 802.1X**



- ที่หน้าต่าง Select 802.1X Connections Type เลือก **Secure Wireless Connections** และคลิกปุ่ม **Next**

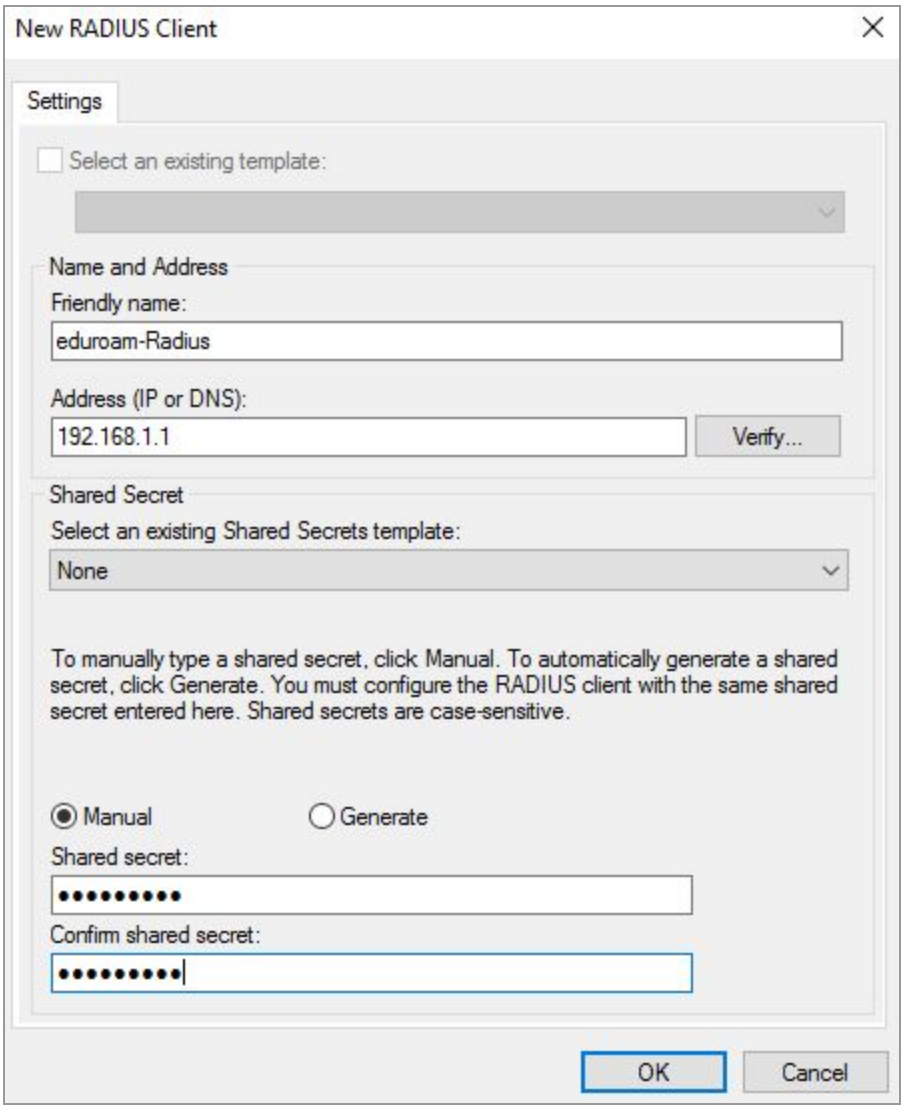


- ที่หน้าต่าง Specify 802.1X Switches คลิกปุ่ม **Add...**

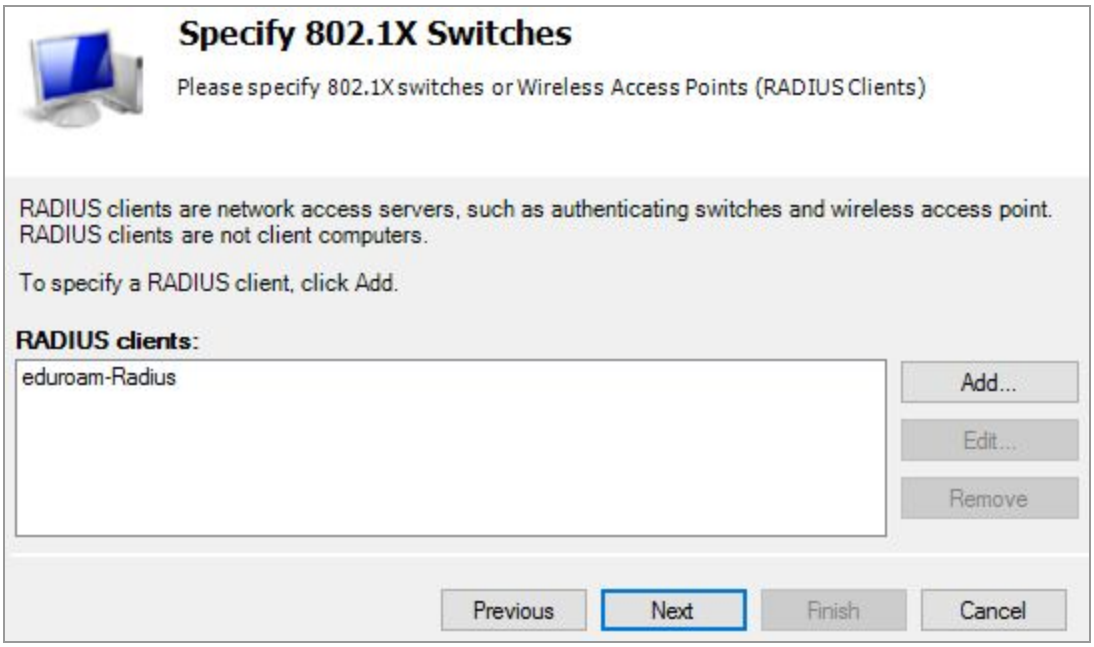


- ที่หน้าต่าง New RADIUS Client ให้กรอกรายละเอียดของ RADIUS Server ของ eduroam และข้อกำหนดของการสื่อสาร แล้วคลิกปุ่ม **Next** โดยรายละเอียดประกอบด้วย

- Friendly name: **eduroam-Radius**
- Address (IP or DNS): **192.168.1.111**
- **(0) Manual**
- Shared secret/Confirm shared secret: **XXXXXXXXXXXXXXXX** (X จำนวน 16 ตัว)

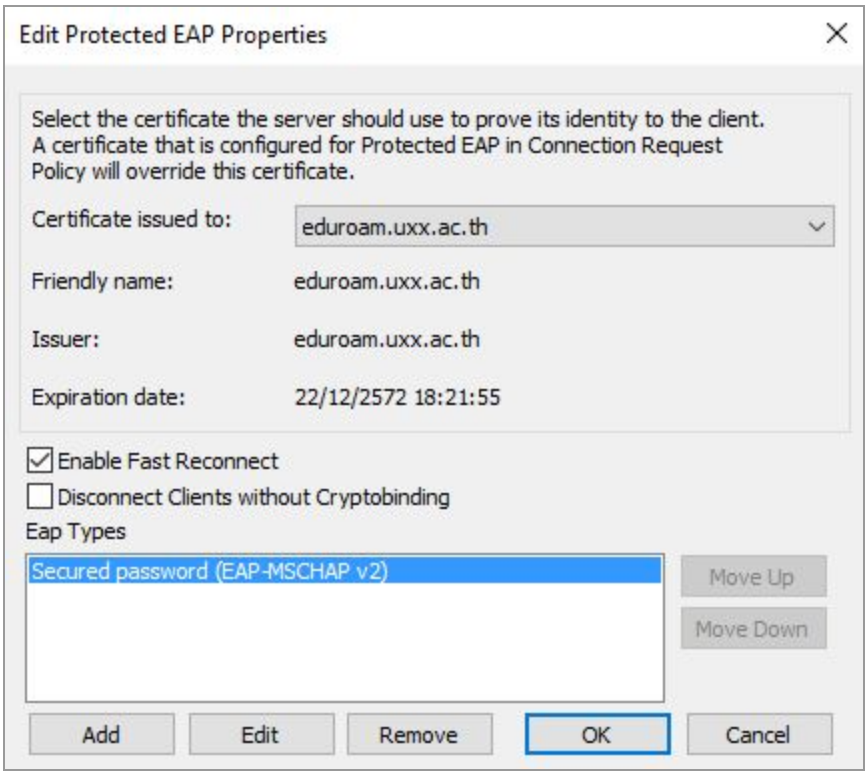


- ที่หน้าต่าง Specify 802.1X Switches คลิกปุ่ม **Next**



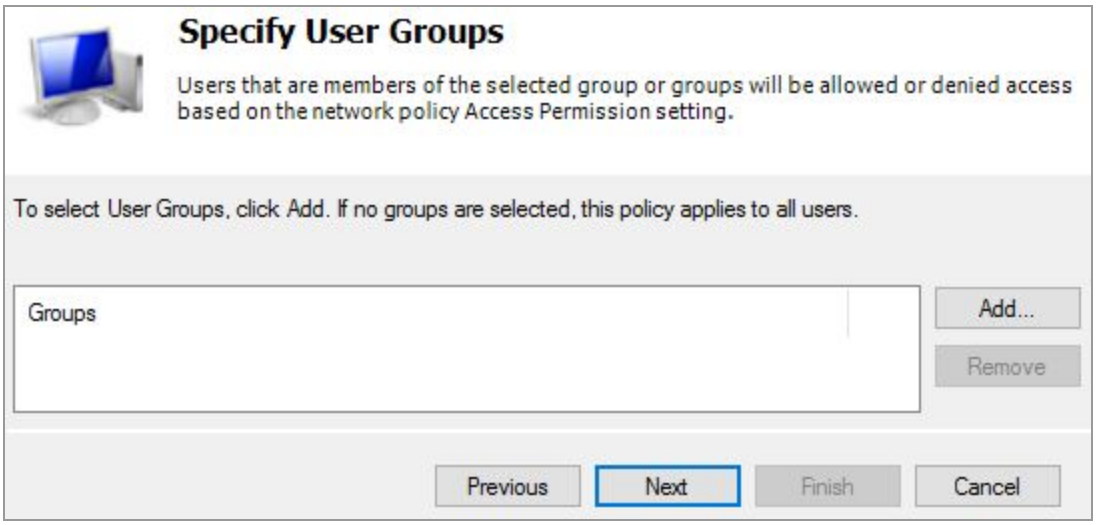
- ที่หน้าต่าง Configure and Authentication Method เลือกรายการ Type (): เป็น **Microsoft: Protected EAP (PEAP)** และคลิกปุ่ม **Configure...**

- ที่หน้าต่าง Edit Protected EAP Properties เลือก Certificate issued to: **eduroam.uxx.ac.th** และคลิกปุ่ม **OK**

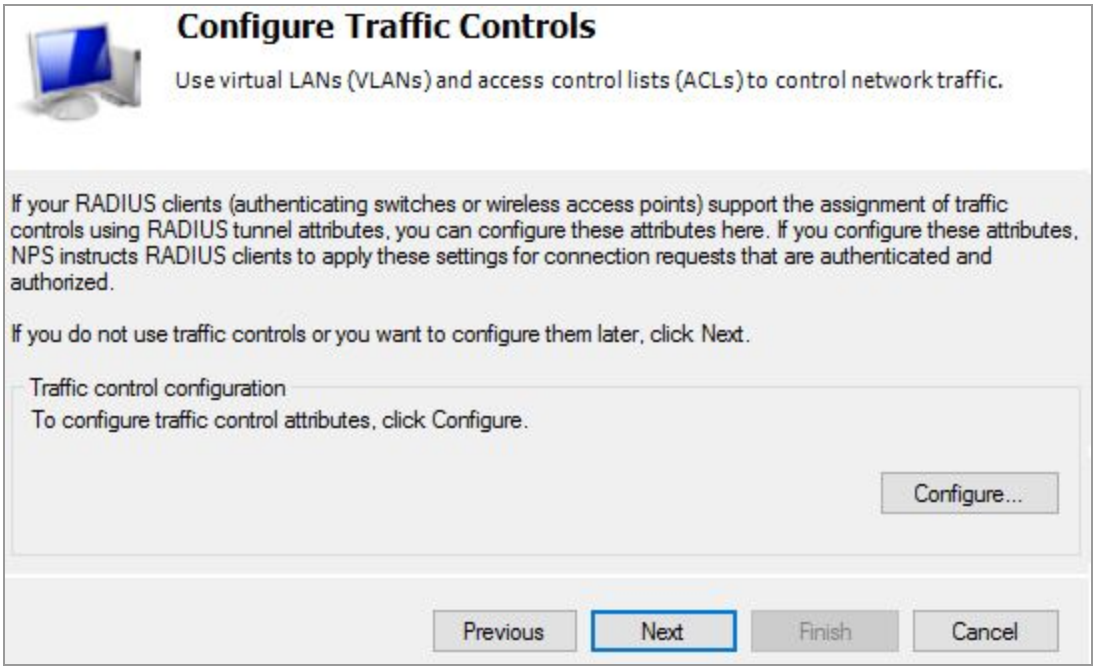


- ที่หน้าต่าง Configure and Authentication Method คลิกปุ่ม Next

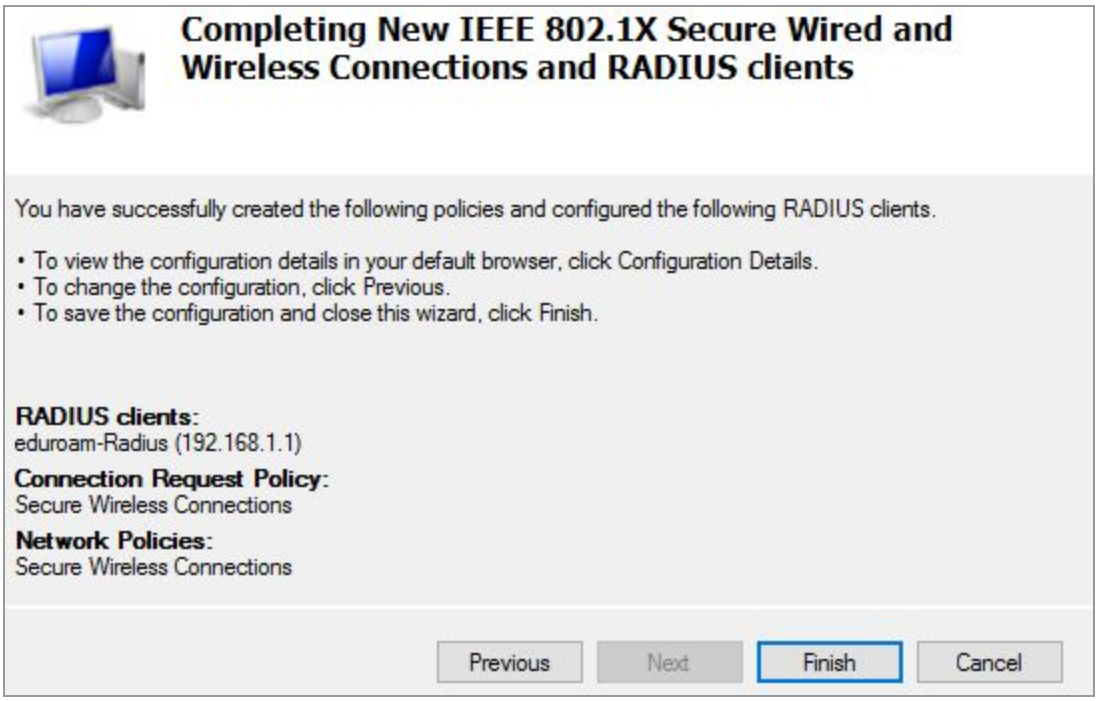
- ที่หน้าต่าง Specify User Groups คลิกปุ่ม **Next**



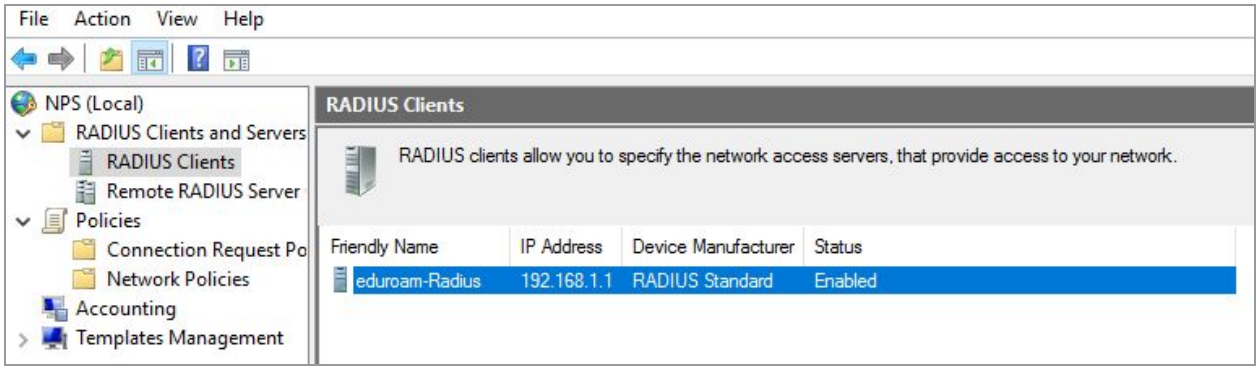
- ที่หน้าต่าง Configure Traffic Controls คลิกปุ่ม **Next**



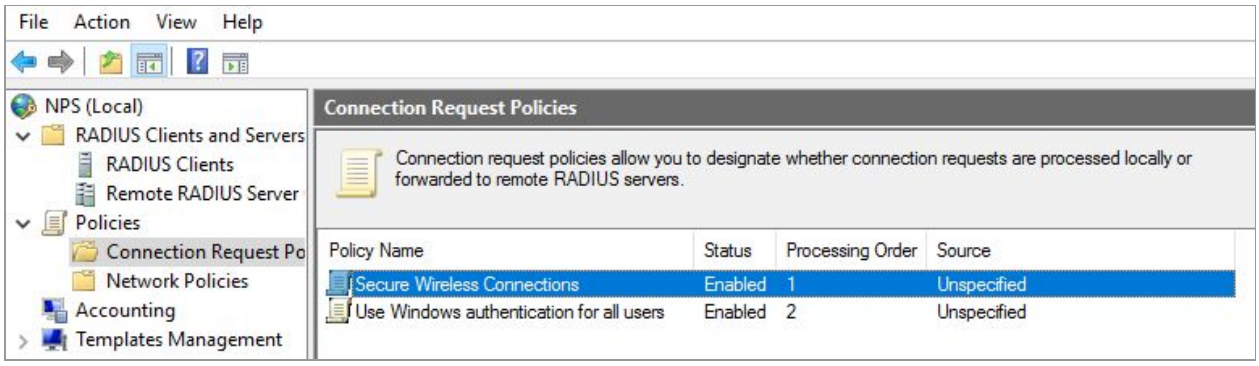
- ที่หน้าต่าง Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients คลิกปุ่ม **Finish**



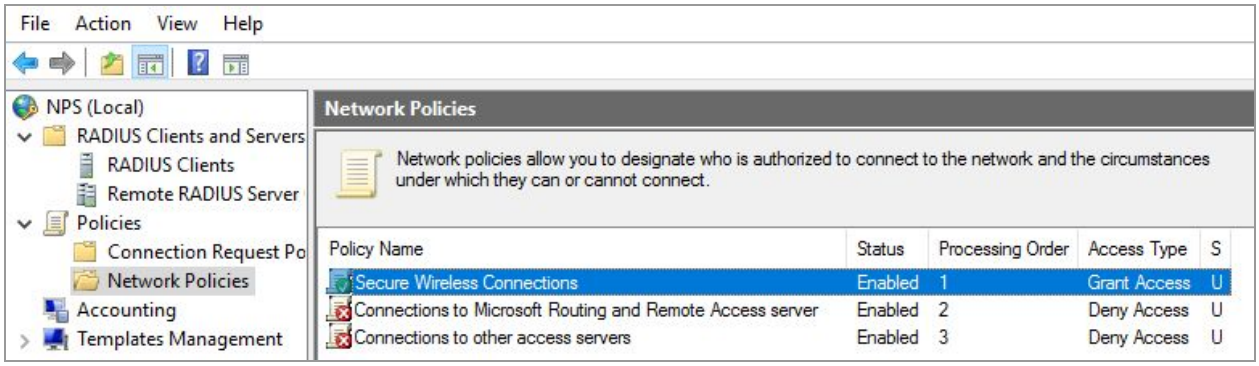
- ผลกำหนดคุณสมบัติเกี่ยวกับ RADIUS server for 802.1X Wireless or Wired Connections ส่วนของ **RADIUS Client** ชื่อ **eduroam-Radius** อยู่ในรายการ **RADIUS Clients and Servers** >> **RADIUS Clients** สามารถปรับแต่งได้



- ผลกำหนดคุณสมบัติเกี่ยวกับ RADIUS server for 802.1X Wireless or Wired Connections ส่วนของ **Connection Request Policies** ชื่อ **Secure Wireless Connections** อยู่ในรายการ **Policies >> Connection Request Policies** สามารถปรับแต่งได้



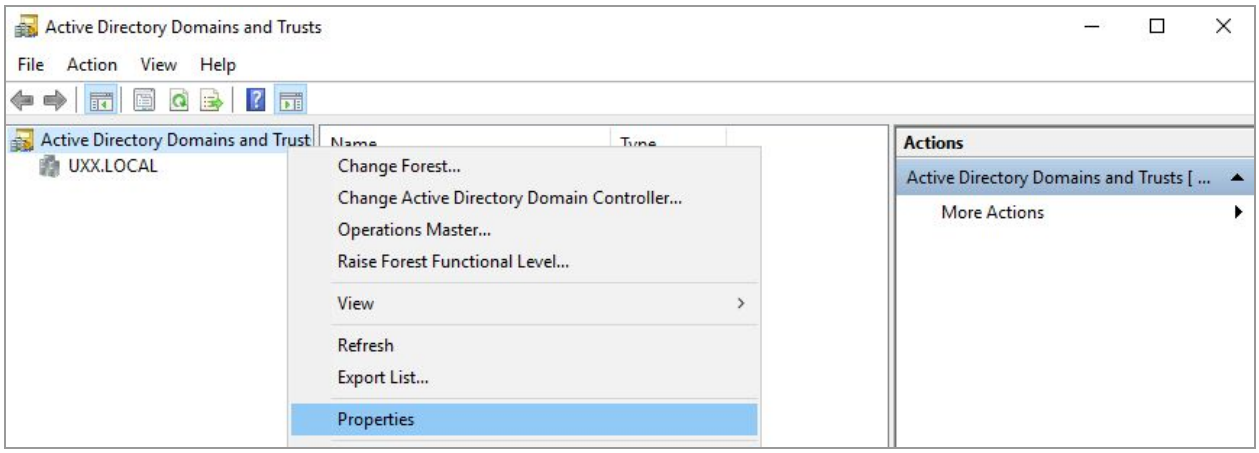
- ผลกำหนดคุณสมบัติเกี่ยวกับ RADIUS server for 802.1X Wireless or Wired Connections ส่วนของ **Network Policies** ชื่อ **Secure Wireless Connections** อยู่ในรายการ **Policies >> Network Policies** สามารถปรับแต่งได้



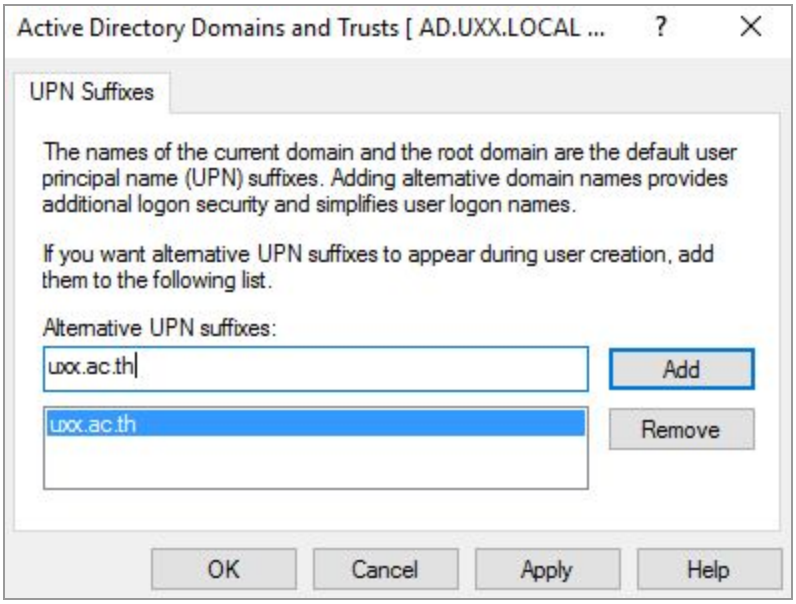
5.4 เพิ่ม Realm ให้ Active Directory

กรณีที่มีการประกาศ Active Directory โดยมี Realm หรือชื่อในโครงสร้าง (Forest) ไม่ตรงกับการใช้งานของ eduroam จำเป็นต้องทำให้ Active Directory มี Realm ตรง หรือใช้วิธีการเพิ่ม Realm เข้าไปในโครงสร้างเดิม

- ที่โปรแกรม **Server Manager** ที่เมนูด้านบนขวา คลิกเมนู **Tools** >> **Active Directory Domains and Trusts**
- ที่โปรแกรม Active Directory Domains and Trusts คลิกปุ่มด้านขวามของเมาส์ที่รายการด้านซ้าย รายการ **Active Directory Domains and Trusts** แล้วเลือกเมนู **Properties**



- ที่หน้าต่าง Active Directory Domains and Trusts [AD.XXX.DOMAIN.XXX] เพิ่ม Realm ในช่อง **Alternative UPN suffixes**: **abc.uxx.ac.th** แล้วคลิกปุ่ม **Add** และคลิกปุ่ม **OK** เพื่อสิ้นสุด

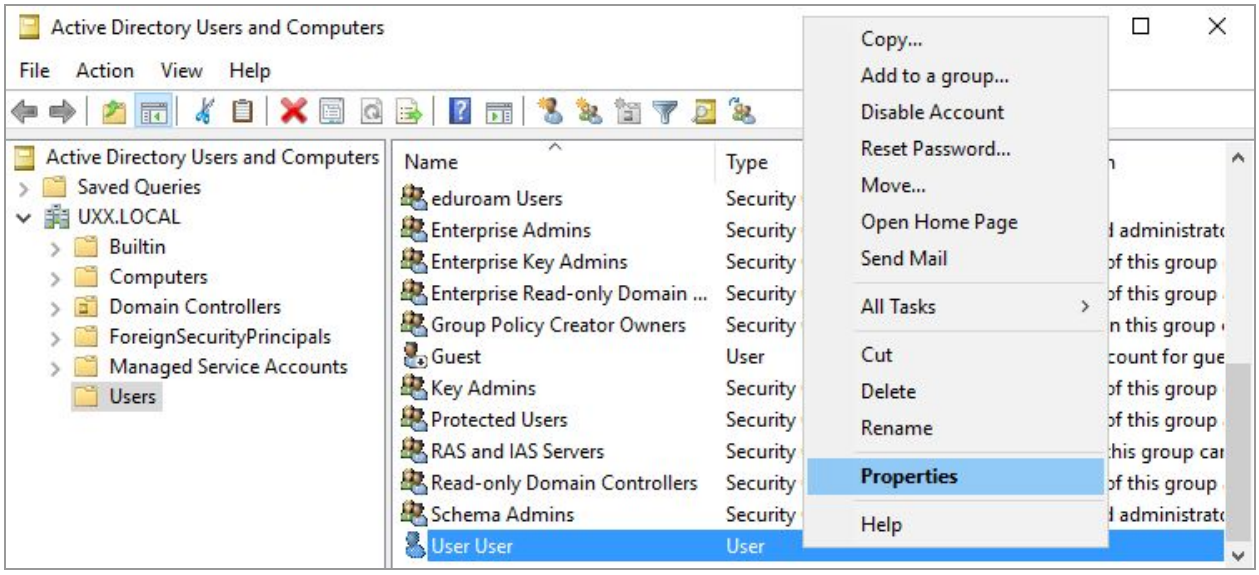


5.5 แก้ไข Realm ให้บัญชีผู้ใช้

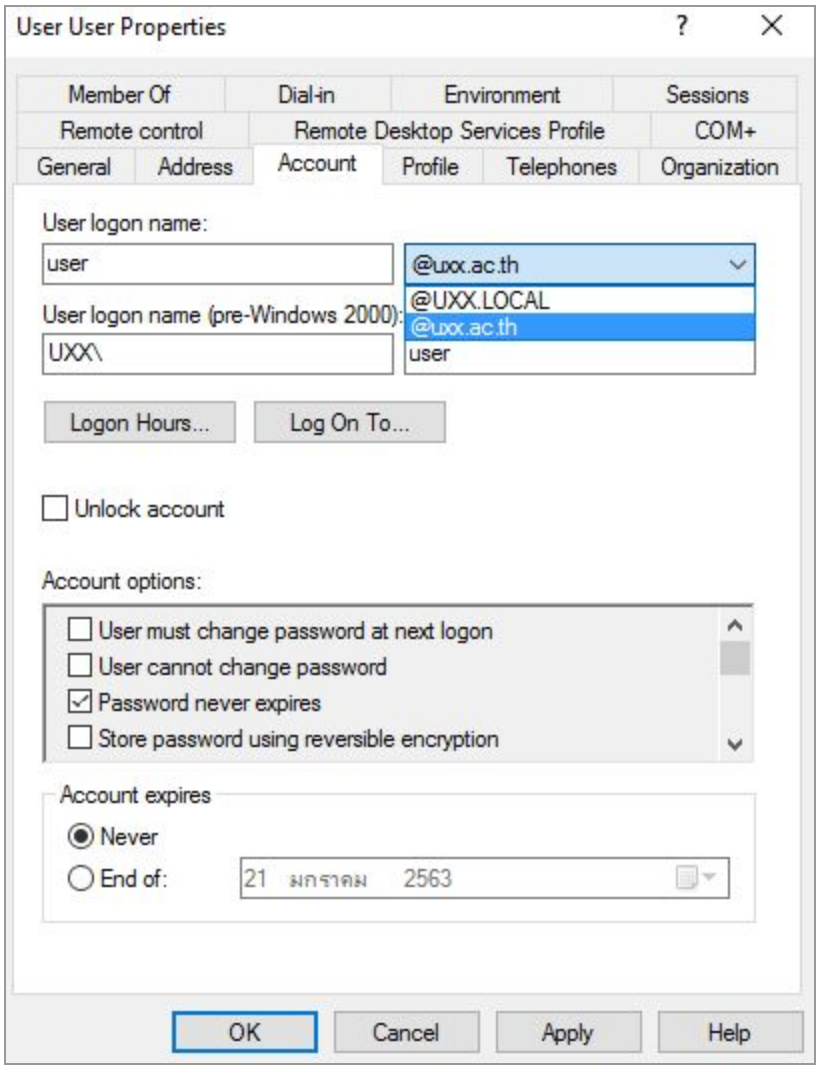
โดยปกติบัญชีผู้ใช้ใน Active Directory จะมี Realm ตามชื่อในโครงสร้าง (Forest) เดิม แต่หากต้องการใช้เป็นบัญชีของ eduroam จำเป็นต้องแก้ไข Realm ของบัญชีผู้ใช้ด้วย โดยการเปลี่ยนจาก Realm เดิมไปเป็น Realm ใหม่

- ที่โปรแกรม **Server Manager** ที่เมนูด้านบนขวา คลิกเมนู **Tools** >> **Active Directory Users and Computers**

- ที่โปรแกรม Active Directory Users and Computers คลิกรายการด้านซ้าย **Active Directory Users and Computers** >> **[XXX.DOMAIN.XXX]** >> **Users**
- ในรายการบัญชี ให้คลิกเมาส์ด้านขวาที่บัญชีที่ต้องการแก้ไขข้อมูล แล้วเลือกเมนู Properties



- ที่หน้าต่างคุณสมบัติของผู้ใช้ (User's Properties) คลิกแท็บ **Account** แล้วเลือก Realm จากรายการหลังบัญชีผู้ใช้ เช่น **@abc.uxx.ac.th** และคลิก **OK** เพื่อสิ้นสุด



5.6 เพิ่ม Realm ให้ Active Directory และแก้ไข Realm ให้บัญชีผู้ใช้ทั้งระบบด้วย Script

หากต้องการเพิ่ม Realm ให้ Active Directory และแก้ไข Realm ให้บัญชีผู้ใช้ทั้งระบบด้วย Script สามารถดาวน์โหลดและเรียกใช้สคริปต์สำเร็จรูปได้ที่

```
https://gallery.technet.microsoft.com/scriptcenter/Add-new-domain-suffix-and-9f42e43f
```

5.7 แก้ไขไฟล์ radiusd.conf

โดยปรับแก้เฉพาะจุดโดยเทียบจากไฟล์ radiusd-eduroam.conf

```
cd /etc/freeradius/3.0

nano radiusd.conf
    --------
    # Change some configurations in radiusd.conf as show below

    # PROXY CONFIGURATION
    #
    proxy_requests  = yes
    $INCLUDE proxy.conf
    #  eduroam
    $INCLUDE proxy-eduroam.conf

    # CLIENTS CONFIGURATION
    #
    $INCLUDE clients.conf
    #  eduroam
    $INCLUDE clients-eduroam.conf
```

5.8 แก้ไขไฟล์ proxy-eduroam.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano proxy-eduroam.conf
    --------
    #
    #  home server for local service at NPS
    #
    home_server nps-uxx-ac-th {
           type = auth
           ipaddr = xxx.xxx.xxx.xxx # 192.168.1.3
           port = 1812
```

```
        secret = XXXXXXXXXXXXXXXX
        #src_ipaddr = xxx.xxx.xxx.xxx
        require_message_authenticator = yes

        status_check = request
        username = "status_check_user" #"check@u00.ac.th"
        password = "don't use"

        #check_interval = 30
        #check_timeout = 8

        #revive_interval = 360

        #response_window = 60
        #response_timeouts = 8

        #num_answers_to_alive = 3
        #zombie_period = 60
}

#
#  home server pool for local service at NPS
#
home_server_pool nps-uxx-ac-th {
        type = fail-over
        home_server = nps-uxx-ac-th
}

#
#  realm for local service at NPS
#
realm nps.uxx.ac.th {
        auth_pool = nps-uxx-ac-th
        nostrip
}
```

5.9 แก้ไขไฟล์ sites- available/eduroam

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano sites-available/eduroam
    --------
    authorize {

    # Change realm to be LOCAL for local user
    if( ("%{Realm}" =~ /abc.uxx.ac.th$$/) ) {
        #
        # If user database is on local (file, LDAP,...),
        # uncomment this block
        #
        #update control {
        #     Proxy-To-Realm := LOCAL
        #}
        #
        # - OR -
        # If user database is on NPS, uncomment ...
        #
        update control {
             Proxy-To-Realm := "nps.uxx.ac.th"
        }

    ...
```

5.10 ทดสอบตรวจสอบบัญชีผู้ใช้จาก Microsoft NPS โดยตรง

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 192.168.1.3 -P 1812 -S XXXXXXXXXXXXXXXX \
```

```
            -u 'user@abc.uxx.ac.th' \
            -p 'Asdf1234' \
            -v -m IEEE8021X \
            -s eduroam -e PEAP -2 MSCHAPV2
        -------
        access-accept; 0
        RADIUS message: code=2 (Access-Accept) identifier=8
        length=187
           Attribute 27 (Session-Timeout) length=6
             Value: 600
           Attribute 1 (User-Name) length=21
             Value: 'user@abc.uxx.ac.th'
           Attribute 79 (EAP-Message) length=6
             Value: 03080004
           Attribute 80 (Message-Authenticator) length=18
             Value: 4f334b7622ec20537163ac31c1926d84
```

5.11 ทดสอบการทำงานด้วยผู้ใช้จากเครื่อง RADIUS ไปยัง Microsoft NPS

หน้าจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หน้าจอที่ 2

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
            -u 'user@abc.uxx.ac.th' \
            -p 'Asdf1234' \
            -v -m IEEE8021X \
            -s eduroam -e PEAP -2 MSCHAPV2
        -------
        access-accept; 0
```

```
RADIUS message: code=2 (Access-Accept) identifier=8
length=187
   Attribute 27 (Session-Timeout) length=6
     Value: 600
   Attribute 1 (User-Name) length=21
     Value: 'user@abc.uxx.ac.th'
   Attribute 79 (EAP-Message) length=6
     Value: 03080004
   Attribute 80 (Message-Authenticator) length=18
     Value: 4f334b7622ec20537163ac31c1926d84
```

6) การติดตั้งโดยมี Microsoft Active Directory เป็นฐานข้อมูลบัญชีผู้ใช้

เป็นการติดตั้งและกำหนดคุณสมบัติพื้นฐานให้ RADIUS Server สามารถทำงานร่วมกับ Microsoft Active Directory เพื่อตรวจสอบผู้ใช้จากบัญชีผู้ใช้ใน Active Directory

การทำงานของ RADIUS Server จะตรวจสอบตัวตนของผู้ใช้ผ่านโปรแกรมภายนอก คือ samba หรือ winbind จึงจำเป็นต้องกำหนดคุณสมบัติของ samba หรือ winbind ให้สามารถติดต่อกับ Active Directory เสียก่อน

6.1 แก้ไขไฟล์ /etc/resolv.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
nano /etc/resolv.conf
    --------
    ...
    search uxx.local
    nameserver <dc_server_address> # 192.168.1.3
    nameserver <other_dns_server> # 8.8.8.8
```

6.2 แก้ไขไฟล์ /etc/hosts

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
nano /etc/hosts
    --------
    ...
    <dc_server_address>   ad.uxx.local   ad.uxx.ac.th  ad
    #192.168.1.3   ad.uxx.local   ad.uxx.ac.th   ad
```

6.3 ติดตั้งแพคเกจสนับสนุนเกี่ยวกับ samba, krb5 และ winbind

```
apt install samba winbind krb5-user krb5-config -y
    --------
    Default Kerberos version 5 realm:
            UXX.LOCAL

    Kerberos servers for your realm:
            ad.uxx.local

    Administrative server for your Kerberos realm:
            ad.uxx.local
```

ถ้าไม่พบหน้าจอการตั้งค่า สามารถกำหนดคุณสมบัติอีกครั้ง

```
dpkg-reconfigure -plow krb5-config
```

6.4 แก้ไขไฟล์ /etc/samba/smb.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข และเพิ่ม

```
nano /etc/samba/smb.conf
    --------
    [global]

    # Change this to the workgroup/NT-domain name ...
        workgroup = UXX

    # Add new all lines below to this location
        security = ADS
        realm = UXX.LOCAL
        encrypt passwords = yes
        client use spnego = yes

        idmap config *:backend = tdb
```

```
        idmap config *:range = 1000-9999
        idmap config UXX:backend = ad
        idmap config UXX:schema_mode = rfc2307
        idmap config UXX:range = 10000-99999

        winbind nss info = rfc2307
        winbind trusted domains only = no
        winbind use default domain = yes
        winbind enum users  = yes
        winbind enum groups = yes
        winbind refresh tickets = yes
    ...
```

6.5 แก้ไขไฟล์ /etc/krb5.conf

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
nano /etc/krb5.conf
    --------
    [libdefaults]
        default_realm = UXX.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
        forwardable = true

    [realms]
        UXX.LOCAL = {
            kdc = ad.uxx.local
            admin_server = ad.uxx.local
        }

    [domain_realm]
        .uxx.local = UXX.LOCAL
        uxx.local = UXX.LOCAL
```

6.6 รีสตาร์ตโปรแกรม samba

```
/etc/init.d/samba restart
```

6.7 Join เครื่อง RADIUS Server ไปเป็นสมาชิกของ Active Directory Domain

```
net ads join -U Administrator
    --------
    Enter Administrator's password: <Administrator's password>
    Using short domain name -- UXX
    Joined 'YOUR-RADIUS-SERVER' to dns domain 'UXX.LOCAL'
```

6.8 รีสตาร์ตโปรแกรม samba และ winbind

```
/etc/init.d/samba restart
/etc/init.d/winbind restart
```

6.9 ทดสอบผลการ Join เครื่อง RADIUS Server ไปเป็นสมาชิกของ Active Directory Domain

```
wbinfo -u
    --------
    administrator
    user
    and other users
```

หากไม่ได้ผล โดยมั่นใจว่า Active Directory ทำงาน และไฟล์คุณสมบัติถูกต้อง ให้ดำเนินการซ้ำในข้อ 35-37

6.10 ทดสอบใช้บัญชีผู้ใช้จาก Active Directory

```
/usr/bin/ntlm_auth --domain=UXX.LOCAL --username=user \
          --password=Asdf1234
        --------
        NT_STATUS_OK: Success (0x0)
```

6.11 เพิ่มสิทธิ์ให้ผู้ใช้ที่รันโพรเซส RADIUS Server เข้าในกลุ่มของผู้ใช้ที่รันโปรเซส winbind

```
chown root:winbindd_priv /var/lib/samba/winbindd_privileged

usermod -a -G winbindd_priv freerad
```

6.12 แก้ไขไฟล์ modules/mschap-eduroam

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano modules/mschap-eduroam
    --------
    mschap mschap-eduroam {
        use_mppe = yes

        require_encryption = yes
        require_strong = yes

        ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key
           --domain=UXX.LOCAL --username=%{Stripped-User-Name}
           --challenge=%{mschap:Challenge:-00}
           --nt-response=%{mschap:NT-Response:-00}"

        #ntlm_auth_timeout = 10
```

```
        ...
    }
```

6.13 แก้ไขไฟล์ sites-available/eduroam-inner-tunnel

ปรับแก้ในไฟล์เฉพาะจุดที่ต้องแก้ไข

```
nano sites-available/eduroam-inner-tunnel
    --------
    authorize {
        ...
        group {
            #  Read the 'users-eduroam' file
            files-eduroam {
                 # return if match
                 ok = return
                 updated = return
            }
            #
            # for LDAP
            #ldap-eduroam {
            #     # return if match
            #     ok = return
            #     updated = return
            #}
            # for Active Directory
            mschap-eduroam {
                 # return if match
                 ok = return
                 updated = return
            }
            # for MySQL
            #sql- eduroam {
            #     # return if match
            #     ok = return
            #     updated = return
```

```
            #}
            ...
        }
        ...
    }

    authenticate {
            # PAP Authentication
            Auth-Type PAP {
                      pap
            }

            # MSCHAP Authentication
            # for file-eduroam and/or LDAP and/or MySQL
            #Auth-Type MS-CHAP {
            #    mschap
            #}

            # MSCHAP Authentication
            # for Active Directory
            Auth-Type MS-CHAP {
                 mschap-eduroam
            }

            eap-eduroam
    }
    ...
```

6.14 เปิดใช้งานโมดูล mschap-eduroam

```
cd /etc/freeradius/3.0/mods-enabled

ln -s ../mods-available/mschap-eduroam
```

6.15 เปลี่ยนสิทธิ์หรือเจ้าของของไฟล์

```
chgrp -R freerad /etc/freeradius
```

6.16 ทดสอบการทำงานด้วยผู้ใช้จาก Active Directory

หน้าจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หน้าจอที่ 2

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
            -u 'user@abc.uxx.ac.th' \
            -p 'Asdf1234' \
            -v -m IEEE8021X \
            -s eduroam -e PEAP -2 MSCHAPV2
       -------
       access-accept; 0
       RADIUS message: code=2 (Access-Accept) identifier=8
       length=187
          Attribute 27 (Session-Timeout) length=6
            Value: 600
          Attribute 1 (User-Name) length=21
            Value: 'user@abc.uxx.ac.th'
          Attribute 79 (EAP-Message) length=6
            Value: 03080004
          Attribute 80 (Message-Authenticator) length=18
            Value: 4f334b7622ec20537163ac31c1926d84
```

การติดตั้ง Wireless Controller หรือ Anonymous Access Point ร่วมกับ RADIUS Server

RADIUS Server: แก้ไขไฟล์ clients.conf หรือ clients-eduroam.conf

เพิ่ม IP address หรือเครือข่ายของ Anonymous Access Point

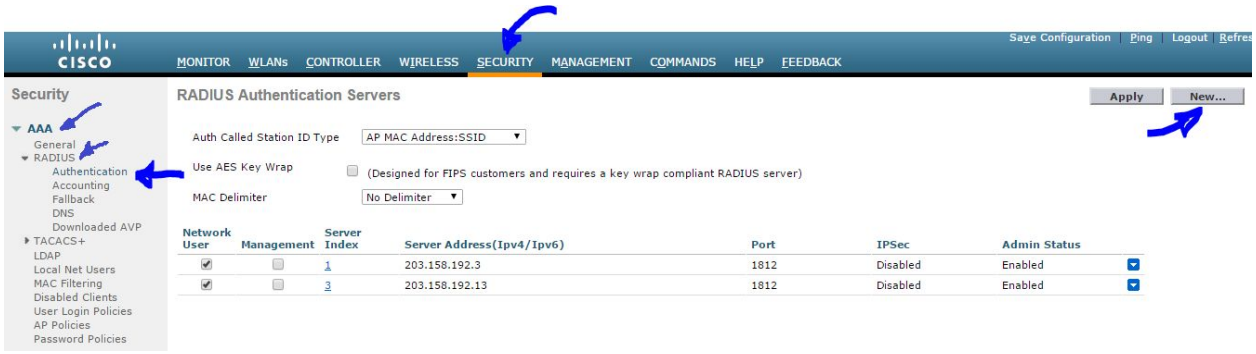
```
cd /etc/freeradius/3.0

nano clients.conf
     --------
     client <ip_or_network_of_access_point_or_wlc> {
          secret = testing123
          shortname  = my_access_point
     }

     client 172.16.11.8 {
          secret = secret_for_172_16_11_8
          shortname  = ap_172_16_11_8
     }

     client 192.168.0.0/24 {
          secret = secret_for_net_192_168_0_0_24
          shortname  = ap_in_net_192_168_0_0_24
     }
```

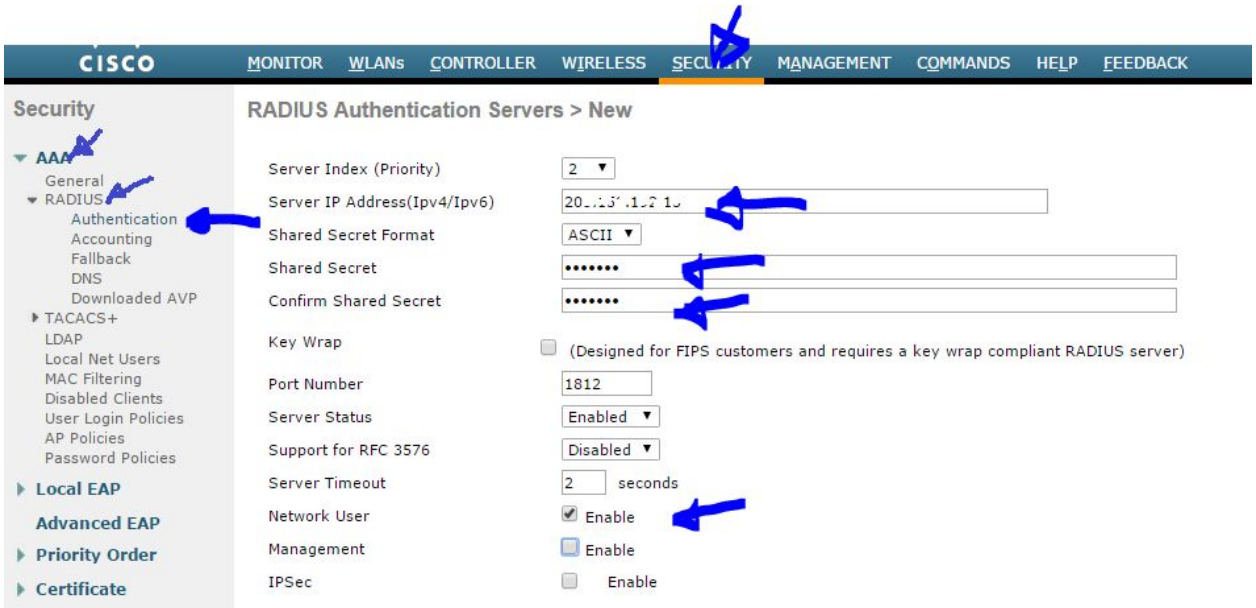
Cisco Wireless Controller

1. Add/Edit RADIUS profile

```
SECURITY > AAA > RADIUS > Authentication > [New…] or Edit
    Server IP Address(Ipv4/Ipv6): <radius_server_ip_address>
    Shared Secret Format: ASCII
    Shared Secret: <secret_shared_with _radius_server>
    Confirm Shared Secret: <secret_shared_with _radius_server>
    Key Wrap: [ ]
    Port Number: 1812
```

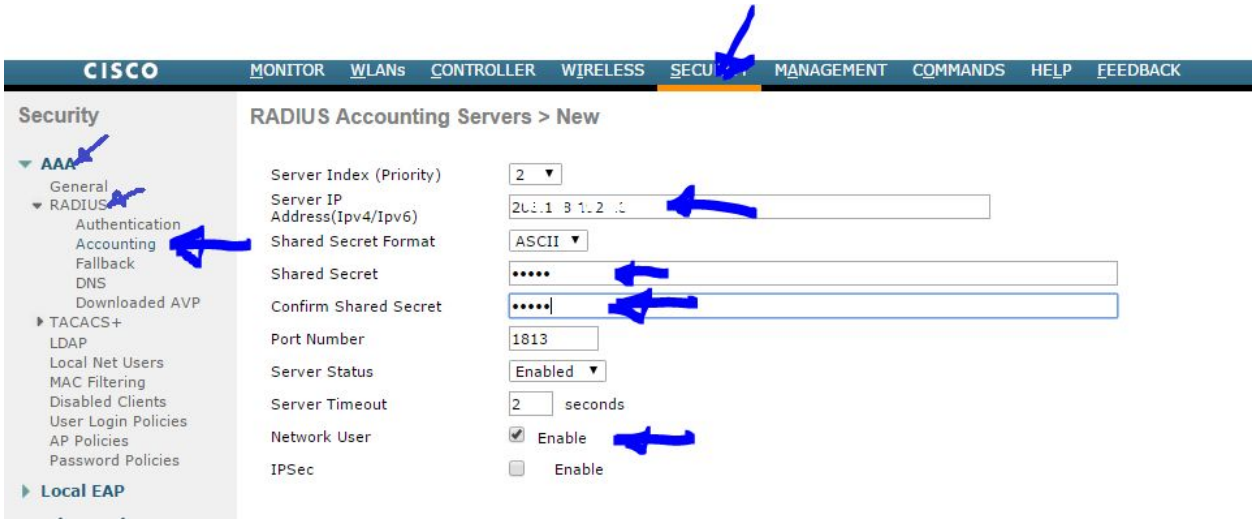
Server Status: Enabled
Network User: [/] Enable





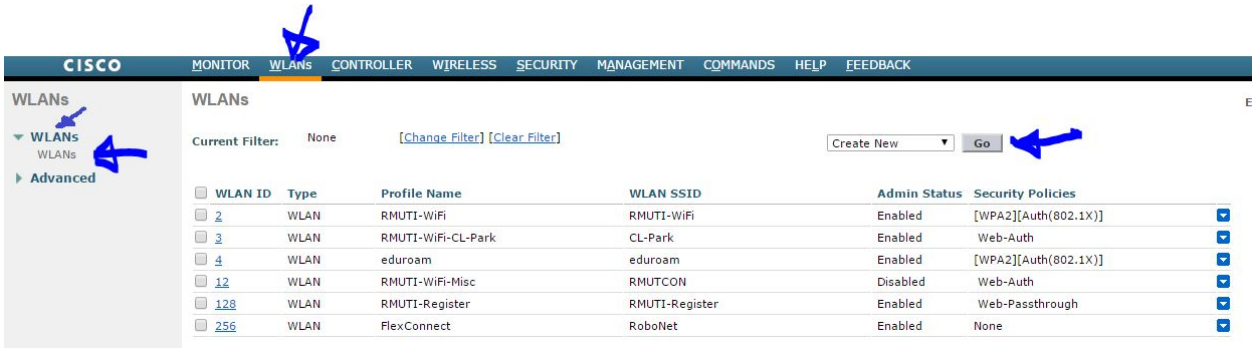
SECURITY > AAA > RADIUS > Accounting > [New…] or Edit

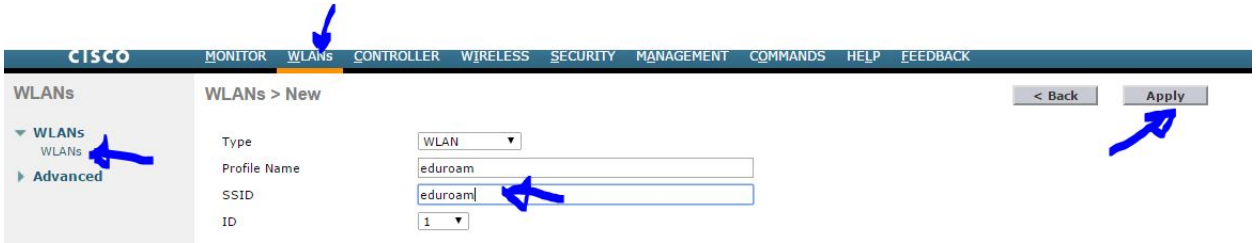
Server IP Address(Ipv4/Ipv6): <radius_server_ip_address>
Shared Secret Format: ASCII
Shared Secret: <secret_shared_with _radius_server>
Confirm Shared Secret: <secret_shared_with _radius_server>
Port Number: 1813
Server Status: Enabled
Network User: [/] Enable



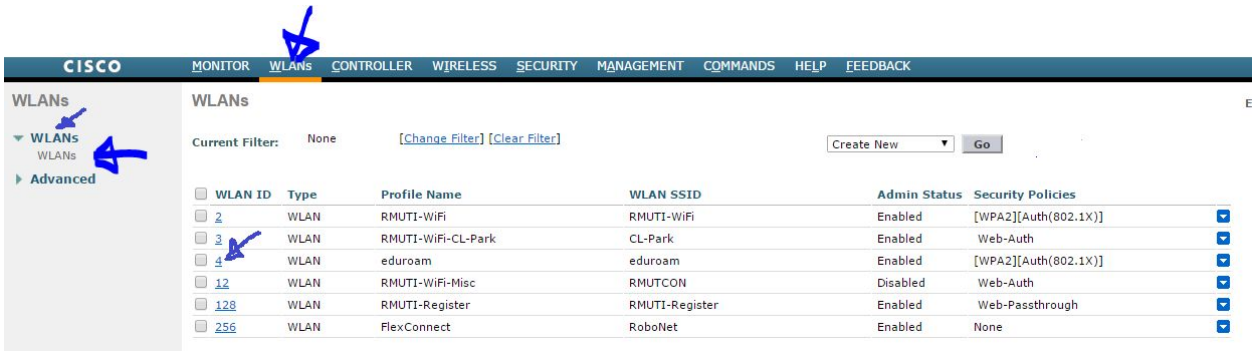
2. <u>Add/Edit Wireless LAN profile</u>

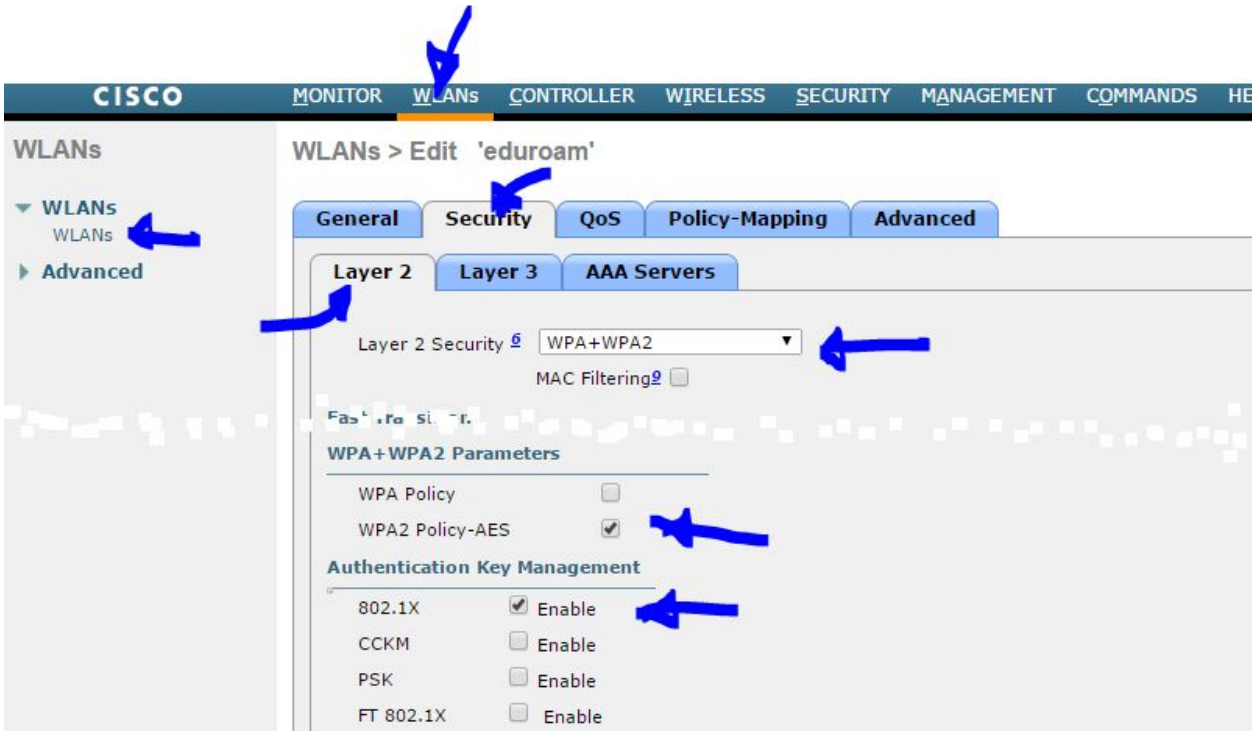
```
WLANs > WLANs > WLANs > [Create new…] or Edit
    Type: [WLAN]
    Profile Name: <wlan_profile>
    SSID: <wlan_ssid>
```



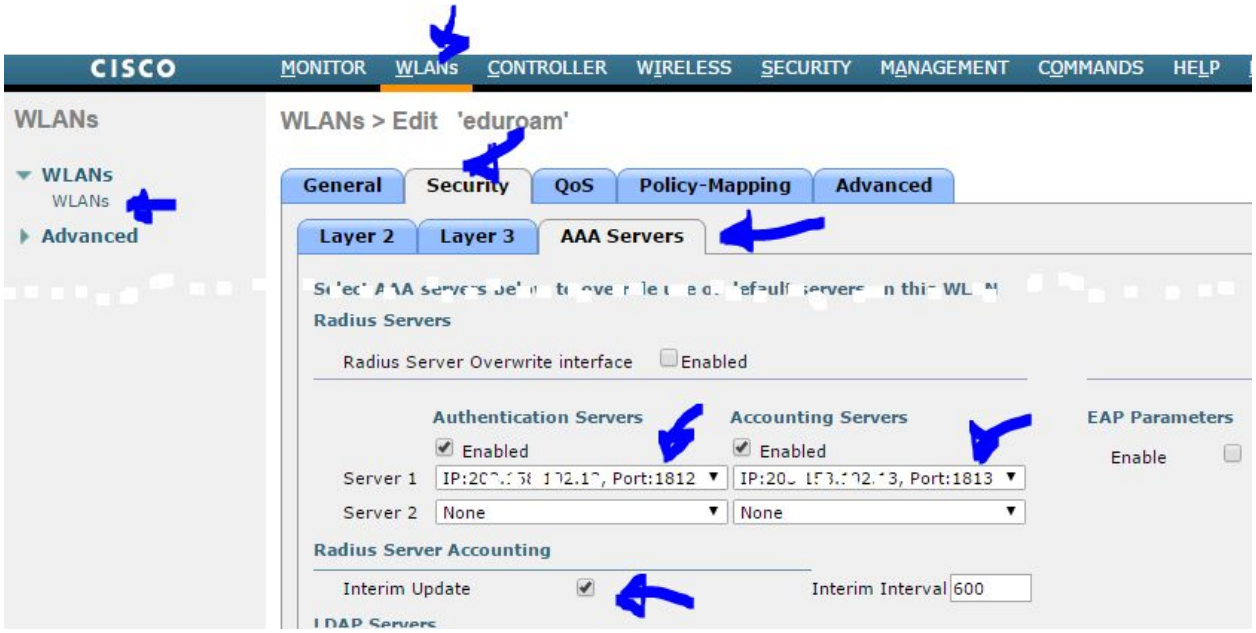


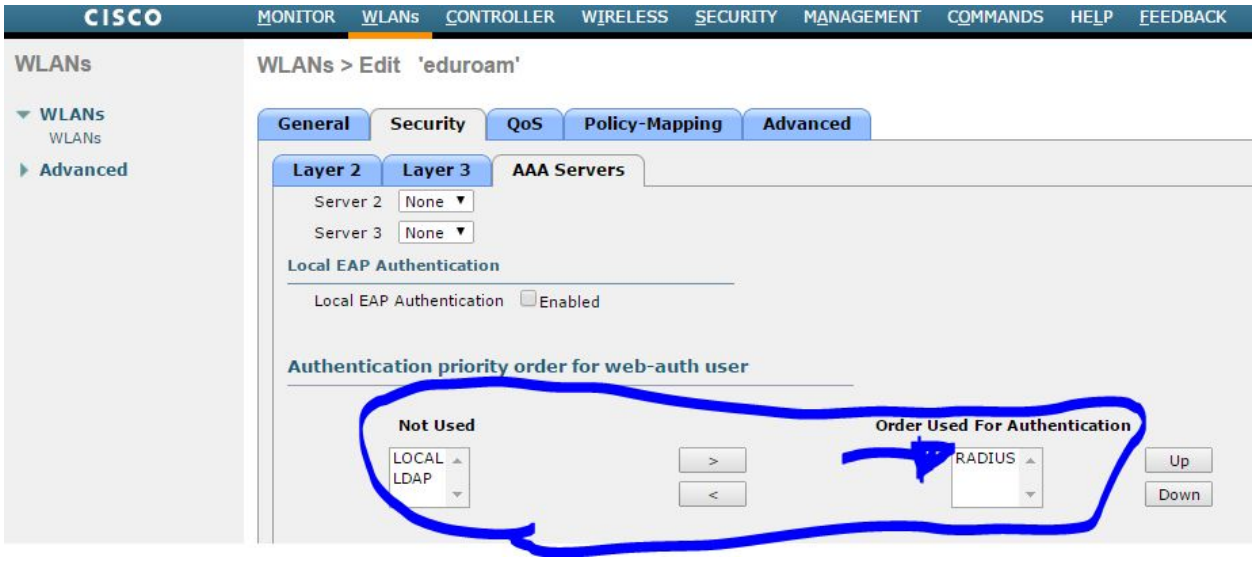

```
WLANs > WLANs > WLANs > [wlan_profile] > Security > Layer 2
    Layer 2 Security: WPA+WPA2

    WPA+WPA2 Parameters
         WPA Policy: [ ]
         WPA2 Policy-AES: [/]

    Authentication Key Management
         802.1X: [/] Enable
```






```
WLANs > WLANs > WLANs > [wlan_profile] > Security > AAA Server
        Authentication Servers Accounting Servers
                [/] Enabled          [/] Enabled
    Server 1     [auth_radius_ip:port]
                 [acct_radius_ip:port]

    Radius Server Accounting
         Interim Update: [/]
```





Aruba Wireless Controller

1. <u>Create RADIUS Server profile</u>

   Configuration > Security > Authentication > Servers > RADIUS Server

2. Edit RADIUS Server profile

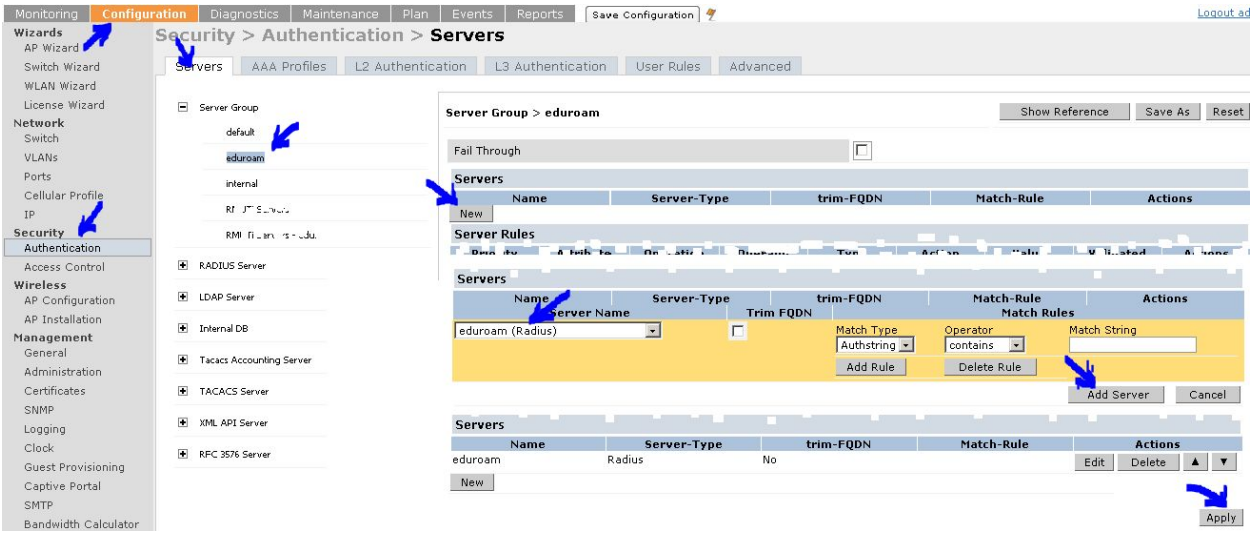
Configuration > Security > Authentication > Servers > RADIUS Server > eduroam

3. Create Server Group profile

Configuration > Security > Authentication > Servers > Server Group

4. Add RADIUS to Server Group profile

Configuration > Security > Authentication > Servers > Server Group > eduroam

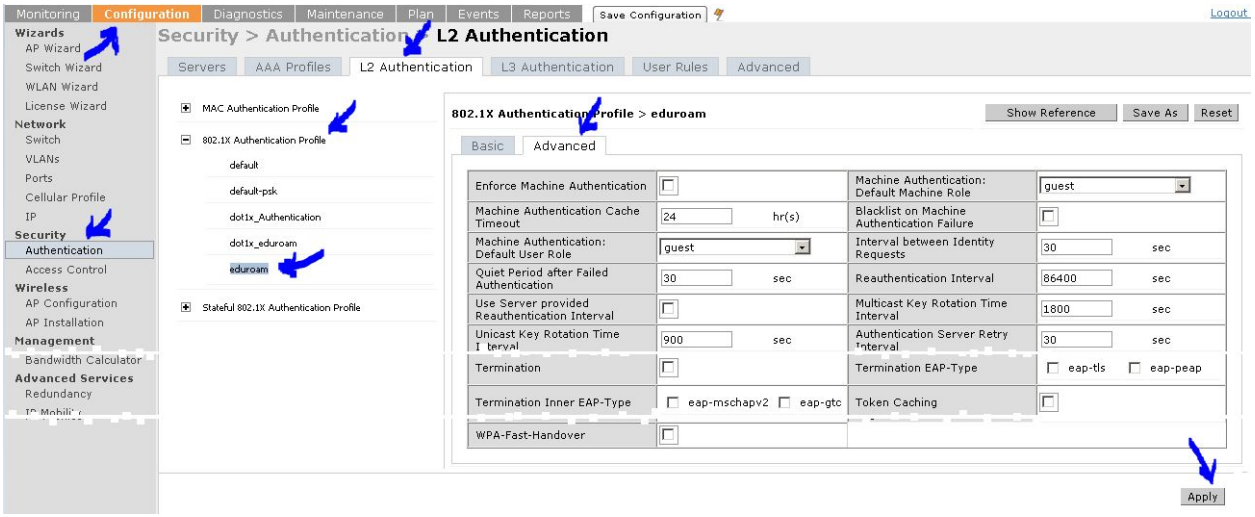


5. Create L2 Authentication profile

Configuration > Security > Authentication > L2 Authentication > 802.1X Authenticaion Profiles

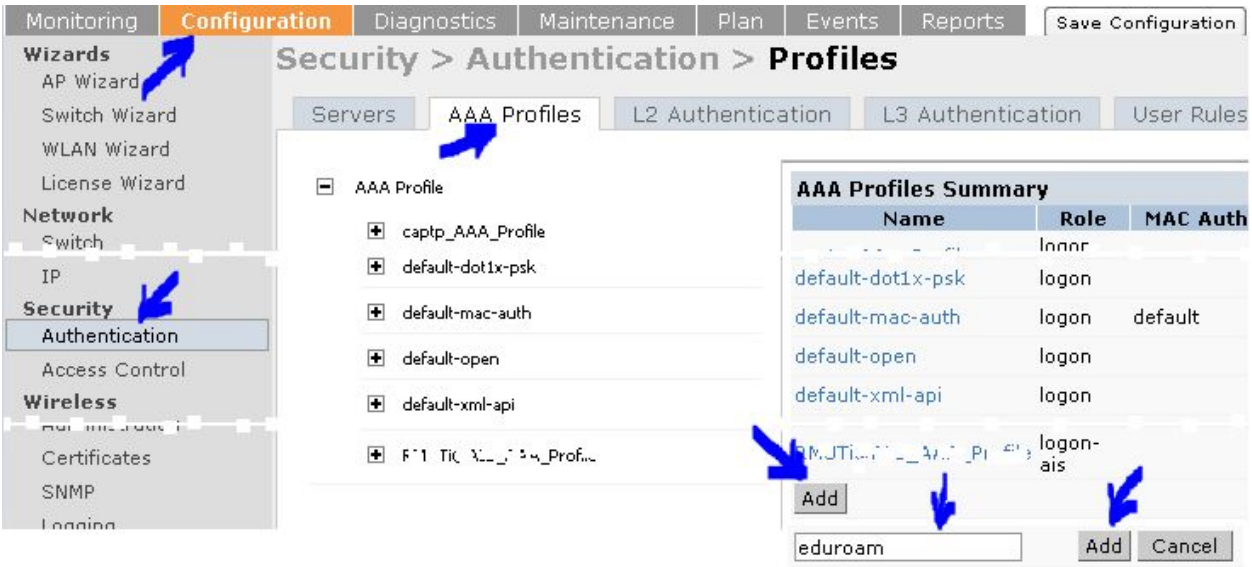
6. Edit L2 Authentication profile

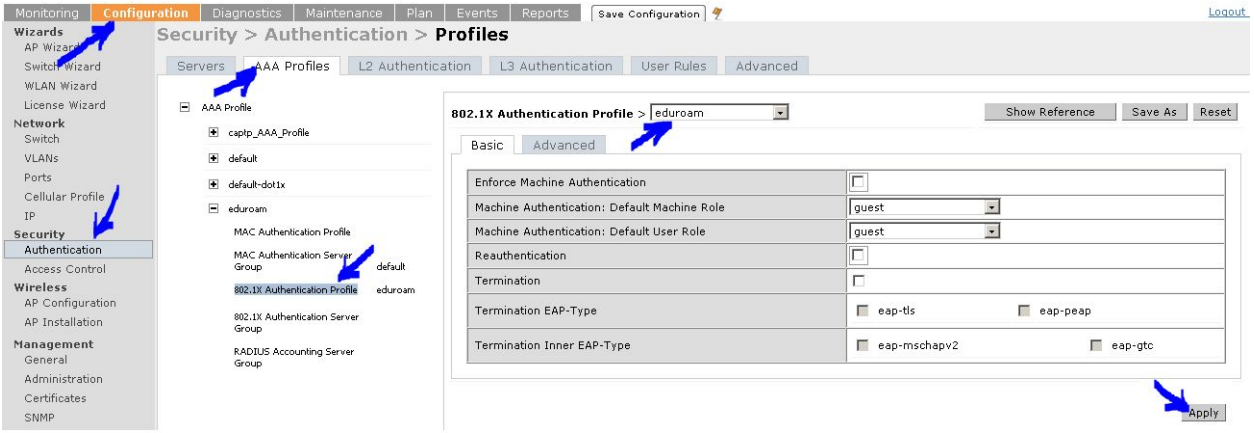
Configuration > Security > Authentication > L2 Authentication > 802.1X Authenticaion Profiles > eduroam

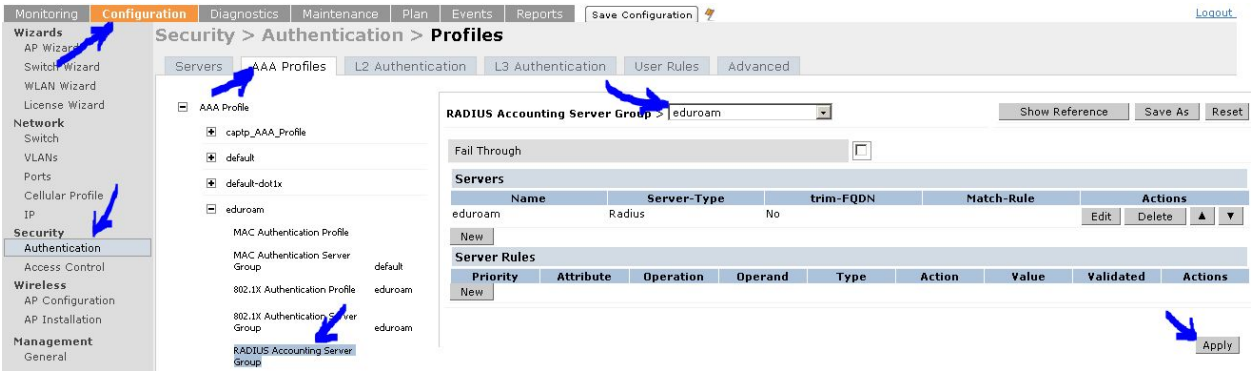


7. Create AAA Authentication profile

Configuration > Security > Authentication > AAA Authentication





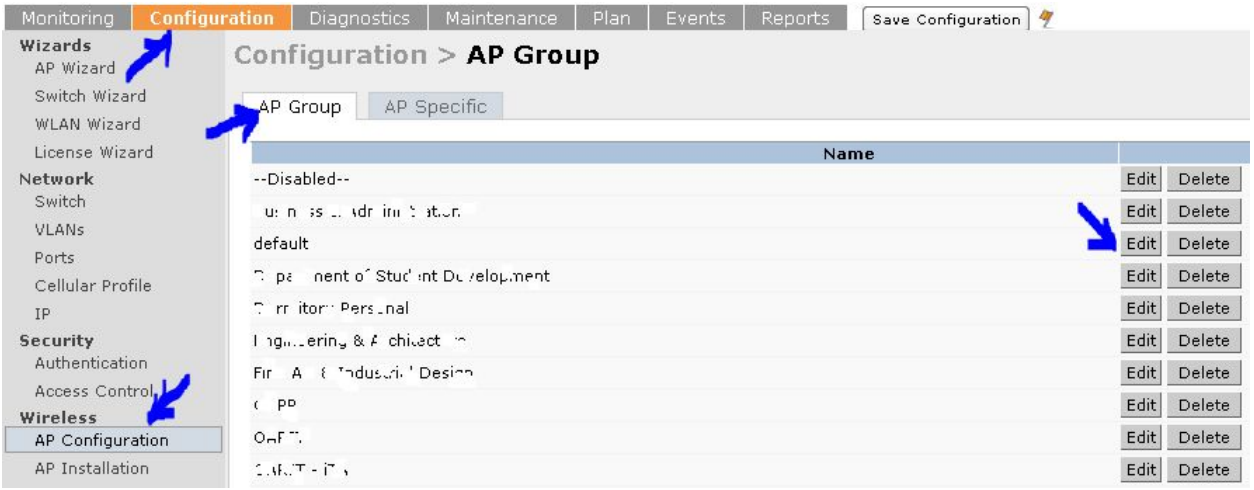


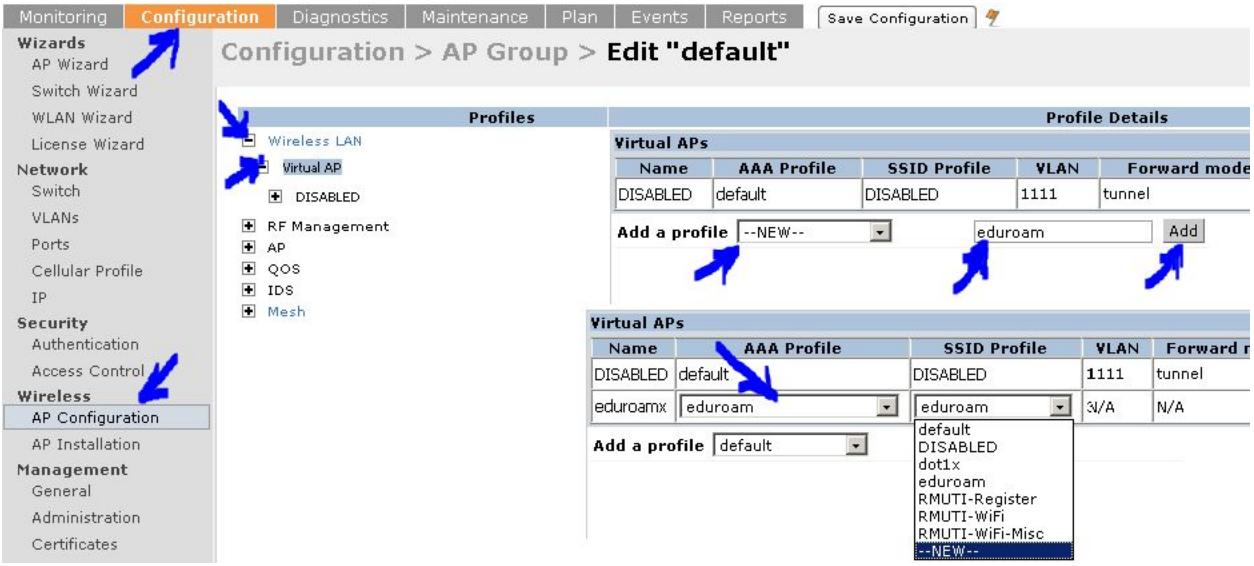
8. Modify Advanced Authentication

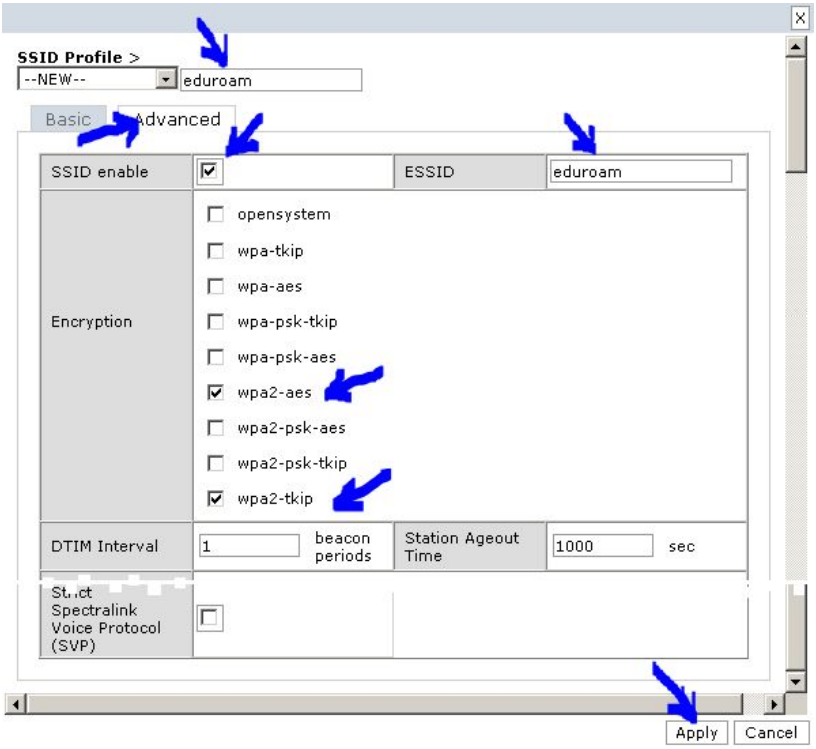
Configuration > Security > Authentication > Advanced

9. Modify AP Configuration

Configuration > Wireless > AP Configuration > AP Group


Monitoring
Configuration
Diagnostics
Maintenance
Plan
Events
Reports
Save Configuration
Wizards
AP Wizard
Switch Wizard
WLAN Wizard
License Wizard
Network
Switch
VLANs
Ports
Cellular Profile
IP
Security
Authentication
Access Control
Wireless
AP Configuration
AP Installation
Configuration > AP Group
AP Group
AP Specific
Name
--Disabled--
default
Edit
Delete


Monitoring
Configuration
Diagnostics
Maintenance
Plan
Events
Reports
Save Configuration
Wizards
AP Wizard
Switch Wizard
WLAN Wizard
License Wizard
Network
Switch
VLANs
Ports
Cellular Profile
IP
Security
Authentication
Access Control
Wireless
AP Configuration
AP Installation
Management
General
Administration
Certificates
Configuration > AP Group > Edit "default"
Profiles
Wireless LAN
Virtual AP
DISABLED
RF Management
AP
QOS
IDS
Mesh
Profile Details
Virtual APs
Name
AAA Profile
SSID Profile
VLAN
Forward mode
DISABLED
default
DISABLED
1111
tunnel
Add a profile
--NEW--
eduroam
Add
Virtual APs
Name
AAA Profile
SSID Profile
VLAN
Forward
DISABLED
default
DISABLED
1111
tunnel
eduroamx
eduroam
eduroam
N/A
N/A
Add a profile
default
default
DISABLED
dot1x
eduroam
RMUTI-Register
RMUTI-WiFi
RMUTI-WiFi-Misc
--NEW--


SSID Profile >
--NEW--
eduroam
Basic
Advanced
SSID enable
ESSID
eduroam
Encryption
opensystem
wpa-tkip
wpa-aes
wpa-psk-tkip
wpa-psk-aes
wpa2-aes
wpa2-psk-aes
wpa2-psk-tkip
wpa2-tkip
DTIM Interval
1
beacon periods
Station Ageout Time
1000
sec
Spectralink Voice Protocol (SVP)
Apply
Cancel

Monitoring
Configuration
Diagnostics
Maintenance
Plan
Events
Reports
Save Configuration
Wizards
AP Wizard
Switch Wizard
WLAN Wizard
License Wizard
Network
Switch
VLANs
Ports
Cellular Profile
IP
Security
Authentication
Access Control
Wireless
AP Configuration
AP Installation
Configuration > AP Group > Edit "default"
Profiles
Wireless LAN
Virtual AP
DISABLED
eduroam
RF Management
802.11a radio profile
802.11g radio profile
RF Optimization profile
RF Event Thresholds profile
AP
Wired AP profile
default
Profile Details
Virtual APs
Name
AAA Profile
SSID Profile
VLAN
Forward mode
DISABLED
default
DISABLED
1111
tunnel
eduroam
eduroam
eduroam
3022
tunnel
Add a profile
default
Add
Apply

การตรวจวิเคราะห์และตรวจสอบการทำงานของ RADIUS Server

การทำงานของ RADIUS Server นั้น จะมีการรับข้อมูลการร้องขอการเข้าถึง (Access-Request) จากภายนอก และส่งต่อเป็นลำดับขั้นการทำงานตามลำดับที่ประกาศไว้ในไฟล์คุณสมบัติ โดยลำดับขั้นสำคัญจะอยู่ในไฟล์ไซต์ที่ประกาศใช้ ประกอบด้วยไฟล์ sites-enabled/eduroam และไฟล์ sites-enabled/eduroam-inner-tunnel

เมื่อ RADIUS Server ได้รับการร้องขอ จะนำข้อมูลการร้องขอเข้าไปประมวลผลตามขั้นตอนในไฟล์ sites-enabled/eduroam เป็นไฟล์แรก และอาจส่งต่อไปยังการประมวลผลภายในในไฟล์ sites-enabled/eduroam-inner-tunnel หรือส่งต่อไปยัง RADIUS Server เครื่องถัดไป

1. การเขียนภาษา unlang ใช้ใน RADIUS Server

ผู้ใช้สามารถเขียนภาษา unlang เพื่อประมวลผลข้อมูลและตัดสินใจการทำงานได้ เช่น เขียนเพื่อการตรวจสอบรูปแบบบัญชีผู้ใช้ให้เหมาะสม หรือเป็นไปตามกฎของการใช้บริการ eduroam เป็นต้น

รูปแบบของภาษา unlang จะใกล้เคียงกับภาษา C สามารถเขียนให้มีการตรวจสอบค่าหรือตัวแปร กำหนดเส้นทางการทำงานตามรูปแบบของภาษาโปรแกรม และกำหนดผลการทำงาน สามารถเขียนภาษา unlang ได้ในส่วนการประมวลข้อมูล เช่น authrize {}, authenticate {} เป็นต้น

ตัวแปรของภาษา unlang จะเป็นตัวแปรภายใน ไม่สามารถประกาศขึ้นเองได้ ตัวแปรที่เกิดขึ้น จะขึ้นกับ 3 ส่วน คือ ส่วนของการทำงานของโมดูล จากการกำหนดเป็น Attribute ในไฟล์ dictionary และสิ่งที่ลูกข่ายส่งเข้ามาขณะร้องขอบริการ

การกำหนดค่าให้ตัวแปร ใช้ใน section ชื่อ update ใน 3 ตำแหน่ง control, request และ response ตัวอย่างเช่น

```
update request {
     User-Name := "login_name"
}
update control {
     Proxy-To-Realm := "LOCAL"
```

```
}
update response {
     Operator-Name := "1abc.ac.th"
}
```

การอ้างถึงตัวแปร ใช้รูปแบบ %{Variable-Name} เช่น ไม่ต้องดำเนินการใน section ใดๆ เช่น

```
if( "%{Realm}" =~ /rmuti.ac.th$$/ ) {
     reject
}
```

ตัวกระทำในภาษา unlang มีเช่นเดียวกับโปรแกรมภาษา C แต่มีความยืดหยุ่นกว่า เช่น

<u>การเปรียบเทียบ</u>

```
(!foo)          Negation
(foo || bar) Or
(foo && bar) And
(foo == bar)  Equal
(foo != bar)  Not equal
(foo =~ bar) Regular expression (match)
(foo !~ bar) Negate regular expression (not match)
(foo < bar)  Less than
(foo > bar)  More than
```

<u>การกำหนดค่า</u>

foo = “value” Add the attribute to the list, if and only if an attribute of the same name is not already present in that list.

foo := “value” Add the attribute to the list. If any attribute of the same name is already present in that list, its value is replaced with the value of the current attribute.

foo += “value” Add the attribute to the tail of the list, even if attributes of the same name are already present in the list. When the right hand side of the expression resolves to multiple values, it means add all values to the tail of the list.

ตัวอย่างตัวแปรที่มักมีการอ้างถึง สามารถดูได้จากการรันโปรแกรมแบบ Debug เช่น

การร้องขอ (Request)

```
Received Access-Request Id 0 from 127.0.0.1:59868 to ...
        User-Name = 'user@rmuti.ac.th'
        NAS-IP-Address = 127.0.0.1
        Calling-Station-Id = '70-6F-6C-69-73-68'
        Framed-MTU = 1400
        NAS-Port-Type = Wireless-802.11
```

การตอบกลับ (Response)

```
Sending Access-Challenge Id 0 from 127.0.0.1:1812 to ...
        EAP-Message = 0x010100061920
        Message-Authenticator = 0x000000000000000000...

Sending Access-Accept Id 9 from 127.0.0.1:1812 to ...
        User-Name := 'user@rmuti.ac.th'
        EAP-Message = 0x03090004
        Message-Authenticator = 0x000000000000000000...
```

การกำหนดเส้นทางการไหลของโปรแกรม สามารถใช้การกระทำแบบเลือกทางพื้นฐาน คือ if else elseif ได้ เช่น

```
if( "%{Realm}" =~ /rmuti.ac.th$$/ ) {
        update control {
                Proxy-To-Realm := LOCAL
        }
}
else {
        update request {
                Realm := "eduroam"
        }
}
```

2. การคัดกรองบัญชีผู้ใช้ที่ไม่เหมาะสม

เพื่อคัดกรองบัญชีที่ผิดปกติ จำเป็นต้องเขียนภาษา unlange เพิ่มเข้าไปในไซต์ ตัวอย่างชื่อบัญชีที่ไม่เหมาะสม คือ บัญชีที่ไม่มี realm หรือไม่มี @xxxx หรือบัญชีที่เกิดจากการทำงานโดยอัตโนมัติของบางระบบปฏิบัติการ เช่น 3gppnetwork.org เป็นต้น

ในการติดตั้งนี้ ได้มีการเขียนภาษา unlang เพื่อคัดกรองบัญชีที่ไม่เหมาะสมตามที่ได้รวบรวมไว้แล้ว ไว้ในไฟล์ eduroam-realm-checks.conf และได้นำไฟล์นี้ไปประกอบเป็นส่วนหนึ่งของไฟล์ไซต์ sites-enabled/eduroam

```
sites-enabled/eduroam
    --------
    authorize {
        $INCLUDE ${confdir}/eduroam-realm-checks.conf
    }
```

3. การกำหนดเครือข่ายให้เหมาะสมกับผู้ใช้ที่ต่างกัน

หากต้องการผู้ใช้ต่างการถูกทำให้เชื่อมต่อเข้ากับเครือข่ายที่ต่างกัน สามารถทำได้โดยการส่งข้อมูลหมายเลข VLAN จาก RADIUS Server ไปยัง Wireless Controller (WLC) หรือ Access Point (AP) ได้ ทั้งนี้ ที่ WLC หรือ AP จะต้องประกาศ VLAN ด้วยหมายเลขที่ตรงกับที่ตอบกลับโดย RADIUS Server ตัวอย่างเช่น ต้องการแยกระหว่างอาจารย์ (User-Name: txxxxxx) กับนักศึกษา (User-Name: sxxxxxx) ให้ใช้เครือข่ายที่ต่างกันดังผังเครือข่าย

```
                                +-- Teacher
+---------------+    +-----------+ VID:100 for Teachers .++.
| RADIUS Server |----| L2 device |=====================|AP|
+---------------+    +-----------+ VID:200 for Students +--+
                                +-- Student
```

```
sites-enabled/eduroam
     --------
     post-auth {
          update reply {
               Tunnel-Type := "VLAN"
               Tunnel-Medium-Type := "IEEE-802"
          }
```

```
        if( "%{User-Name}" =~ /^t*/ ) {
            update reply {
                Tunnel-Private-Group-Id := 100
            }
        }
        elseif( "%{User-Name}" =~ /^s*/ ) {
            update reply {
                Tunnel-Private-Group-Id := 200
            }
        }
        else {

        }
    }
```

4. การดูกิจกรรมการทำงานของโปรแกรมโดยละเอียด (Full debuging)

การตรวจสอบการทำงานของโปรแกรม RADIUS Server ว่าทำงานอย่างถูกต้องหรือไม่นั้น วิธีที่ดีที่สุดคือการสั่งรันโปรแกรมแบบ full debuging โปรแกรมจะพิมพ์ผลการทำงาน หรือกิจกรรมที่เกิดขึ้นโดยละเอียดออกทางจอภาพ ในเครื่องหนึ่งเครื่องจะสามารถรันโปรแกรม RADIUS Server ได้เพียงหนึ่งโปรแกรม ดังนั้น หากจะรันโปรแกรมแบบ full debuging จะต้องปิดโปรแกรมเดิมก่อน และสิ้นสุดด้วยการพิมพ์ CTRL+C การดำเนินการเป็นดังนี้

```
service freeradius stop
freeradius -X
```

หรือการบันทึกผลการทำงานไว้ในไฟล์

```
freeradius -X > text.txt
```

5. การบันทึกกิจกรรมใน Log

คุณสมบัติเกี่ยวกับการบันทึกกิจกรรมการทำงานที่กำหนดไว้การติดตั้งนี้ ใช้ไฟล์โมดูลเดิม และมีตำแหน่งการบันทึกตามค่าดั้งเดิมของ RADIUS Server ประกอบด้วย

```
sites-enabled/eduroam
     --------
     authorize {
          # get request from local user and NRO (as IdP and SP)
          # config: ${configdir}/(modules or
          mods-enabled)/detail.log
          # log:
          ${logdir}/radacct/<client_ip>/auth-detail-<date>
          auth_log
     }
     accounting {
          # accounting request from local user and NRO (as IdP
          # and SP)
          # config: ${configdir}/(modules or
          mods-enabled)/detail
          # log: ${logdir}/radacct/<client_ip>/detail-<date>
          detail
     }
     post-auth {
          # get result after authentication process (as IdP)
          # config: ${configdir}/(modules or
          mods-enabled)/detail.log
          # log:
          ${logdir}/radacct/<client_ip>/reply-detail-<date>
          reply_log
     }
     pre-proxy {
          # process and forward request to NRO (as SP)
          # config: ${configdir}/(modules or
          mods-enabled)/detail.log
          # log:
          ${logdir}/radacct/<client_ip>/pre-proxy-detail-<date>
          pre_proxy_log
     }
     post-proxy {
          # get response from NRO (as SP)
```

```
        # config: ${configdir}/(modules or
        mods-enabled)/detail.log
        # log:
        ${logdir}/radacct/<client_ip>/post-proxy-detail-<date>
        post_proxy_log
    }
```

ตัวอย่างเนื้อหาในไฟล์ auth-detail

```
    Fri Oct 23 22:39:14 2015
        Packet-Type = Access-Request
        User-Name = "eduroam@rmuti.ac.th"
        NAS-IP-Address = 127.0.0.1
        Calling-Station-Id = "70-6F-6C-69-73-68"
        Stripped-User-Name = "eduroam"
        NAS-Port-Type = Wireless-802.11
        Realm = "rmuti.ac.th"
```

ตัวอย่างเนื้อหาในไฟล์ reply-detail

```
    Sat Oct 24 02:01:00 2015
        Packet-Type = Access-Accept
        Session-Timeout = 600
        User-Name = "eduroam@rmuti.ac.th"
```

ตัวอย่างเนื้อหาในไฟล์ pre-proxy-detail

```
    Sat Oct 24 00:05:49 2015
        Packet-Type = Access-Request
        User-Name = "eduroam@rmuti.ac.th"
        NAS-IP-Address = 127.0.0.1
        Calling-Station-Id = "70-6F-6C-69-73-68"
        Realm = "eduroam"
        Proxy-State = 0x30
```

ตัวอย่างเนื้อหาในไฟล์ post-proxy-detail

```
Mon Oct 26 15:33:43 2015
     Packet-Type = Access-Accept
     Session-Timeout = 600
     User-Name = "eduroam@rmuti.ac.th"
     Proxy-State = 0x39
```

อ้างอิง

- https://www.eduroam.us/node/89
- http://confluence.diamond.ac.uk/display/PAAUTH/Using+Active+Directory+as+authentication+source
- https://wiki.samba.org/index.php/Setup_a_Samba_AD_Member_Server
- http://freeradius.org/radiusd/man/unlang.html
- https://www.tobtu.com/lmntlm.php
-