WiNG 5 Feature Guide

Role Based Firewall

Published: April 2017

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

P/N XXXXX-XX

Contents

Introduction

To augment the firewall services of WiNG 5, one may enable role-based firewall functionality to gain the most granular security filtering and policing based on the user role.

Role-based firewall gives enhanced security to the standard firewall features of WiNG 5. Whereas the standard IP/MAC or Application based firewall rules are applied to physical and logical interfaces as well as WLANs, role-based rules are applied to the wireless clients and follow them as they roam on the network based on various matching criteria.

For further information on the standard Firewall features of WiNG 5, please see the "*WiNG5 Firewall How To"* document.

Overview

Roles allow for dynamic assignment of IP/MAC firewall rules or Application Policies to wireless clients based on one or more match conditions that are evaluated when the client associates to the wireless network. These dynamic rules follow the clients, being migrated to other access points as the clients roam. If a role is established that would affect already connected clients, these roles will be evaluated immediately and put into effect against the client traffic.

Match criteria include:

Location: AP or group of AP's the wireless client is connected to

Authentication: The authentication method used by the client during association, i.e. EAP vs MAC-Auth vs Kerberos vs None

Encryption: The encryption type used by the client (not configured on the WLAN)

Group Membership: The local group the wireless client is assigned to as obtained from

AAA server or LDAP server.

LDAP attributes: emailid, employeeid, country, company, i.e. anything that can be returned back by an LDAP server.

Captive Portal Authentication State: post-login or pre-login

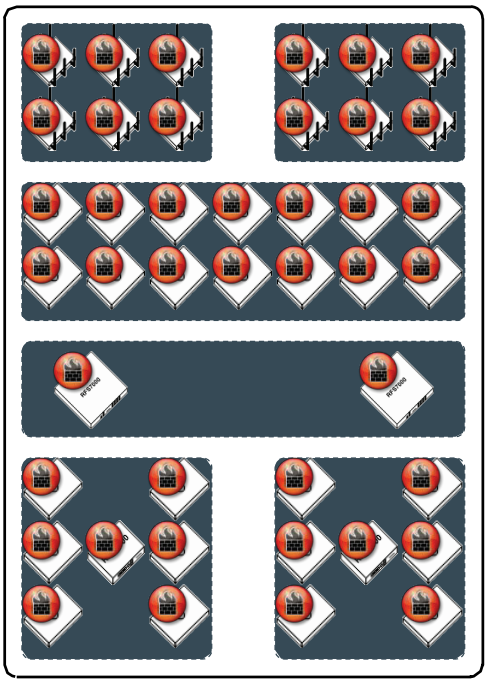
Client Identity: Based on DHCP fingerprint

MAC Address: MAC address or range of the wireless client(s)

SSID: The SSID the wireless client is associated to

Distributed Stateful Inspection

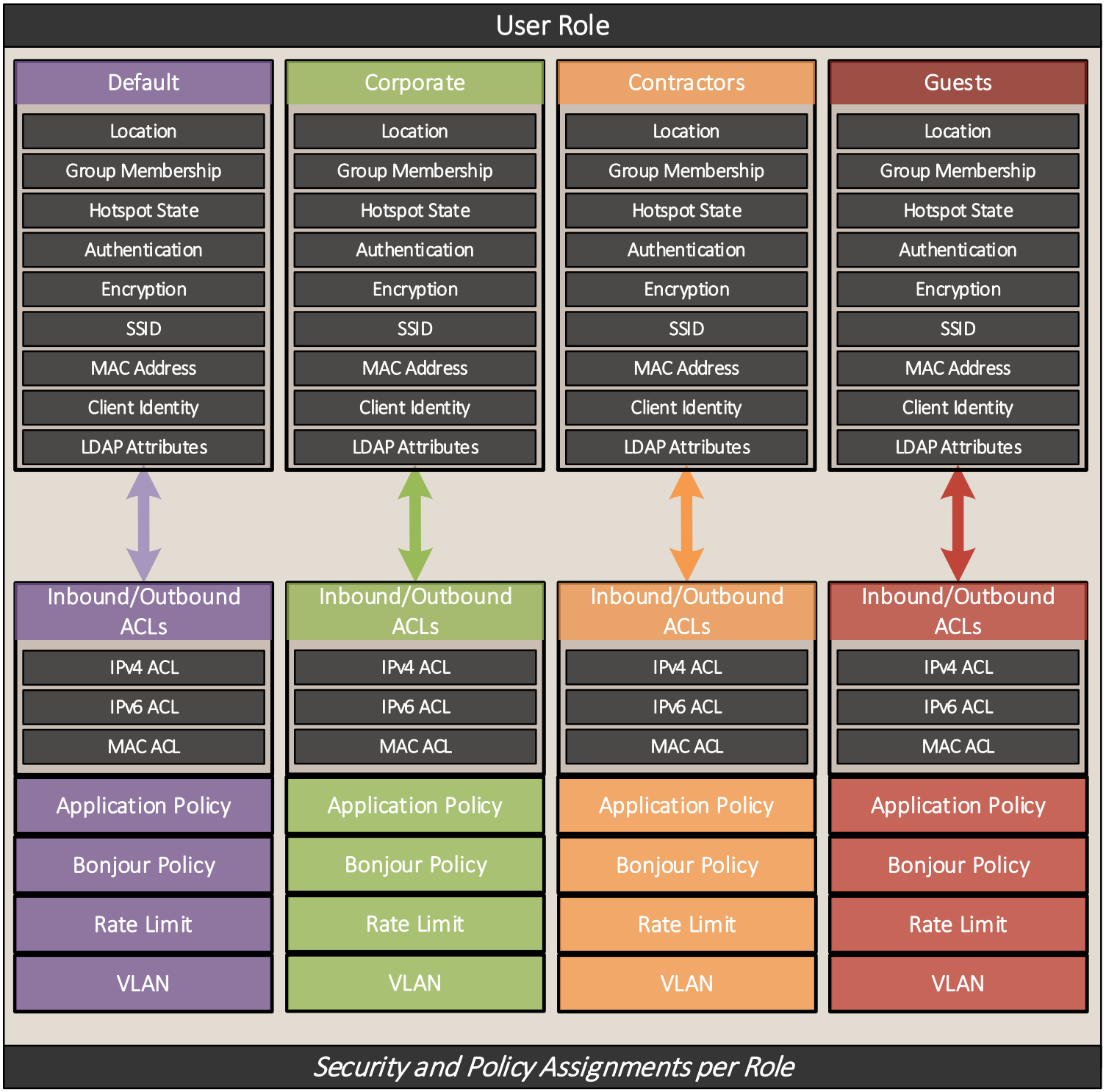
The major feature in WiNG 5 is distribution of services or services at the edge. Since controllers and access points alike run the same OS and thus feature set, processing of traffic for various services is pushed to the edge where it can be performed in real-time and done so dynamically.



The distributed nature of the firewall allows stateful flows to migrate with clients as they roam between access points. Rules are made up of one or more traffic matching conditions, for which an action is then performed (permit, deny, mark, log). As is the case with firewalls, at least one permit action must be met in order for traffic to be forwarded and at the end of a rule set, there is an implied deny for all traffic not meeting a match condition.

Role Based Firewall

Roles based firewall was designed to meet the security needs of the mobile enterprise



It is possible from time to time that while a role is being evaluated, multiple matches may be found. In this case, the role with the lowest precedence will be assigned to the wireless client.

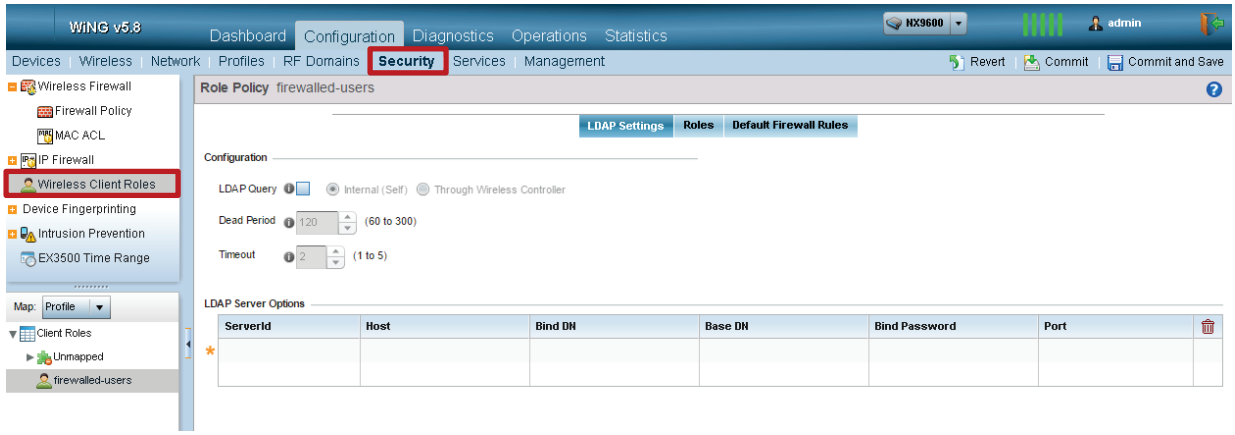
For each user role administrators can define match criteria and values that can individually be ignored, matched and partially matched. For example a group name could be defined in a user role to exactly match the value Sales which would apply to all users in the Sales group. Likewise an ESSID could be defined to partially match the value Corp which would match any devices associated with the ESSIDs named CorpUsers and CorpGuest. Alternatively specific strings can be ignored by selecting a match of Not Contains or all criteria can be matched using a match condition Any.

Components

The components of role-based firewall are listed below:

1. Firewall Rules (Access Control Lists)
   - IPv4 Firewall Rules
   - IPv6 Firewall Rules
   - MAC Firewall Rules
2. Application Rules (Application Policy)
3. Bonjour Services Rules (Bonjour Discovery Policy)
4. Rate-Limiting (from/to client)
5. VLAN Assignment
6. Wireless Client Roles (Role-policy)
7. AAA Policy (optional based on match criteria)

Web UI Role-Policy Options



CLI Role-Policy Options

```
vx9000#conf t

vx9000(config)#role-policy firewalled-users vx9000(config-role-policy-firewalled-users)#? Role Policy Mode
commands:
Role Policy Mode commands:
  default-role     Configuration for Wireless Clients not matching any role
  ldap-deadperiod  Ldap dead period interval
  ldap-query       Set the ldap query mode
  ldap-server      Add a ldap server
  ldap-timeout     Ldap query timeout interval
  no               Negate a command or set its defaults
  user-role        Create a role

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal
```

Use and Configuration

We will examine three scenarios throughout this guide; an easy method based on SSID followed by a slightly more complex method based on the user's group assignment, lastly a more granular role separation based on device OS type and version using DHCP fingerprinting.

During the configuration of the role-policy, the necessary IP or MAC access lists will be specified, so it is helpful to have these created already. Thus, following is a preferred order of configuration. This assumes that the general configuration of the controller and necessary WLAN's already exist. In the case of our second scenario, this document will also include the configuration of AAA and WLAN policies.

1. Configure IP / MAC based access lists
2. Configure Application Policies
3. Configure the Role-policy, define User Roles
4. Apply the role-policy to the device(s)

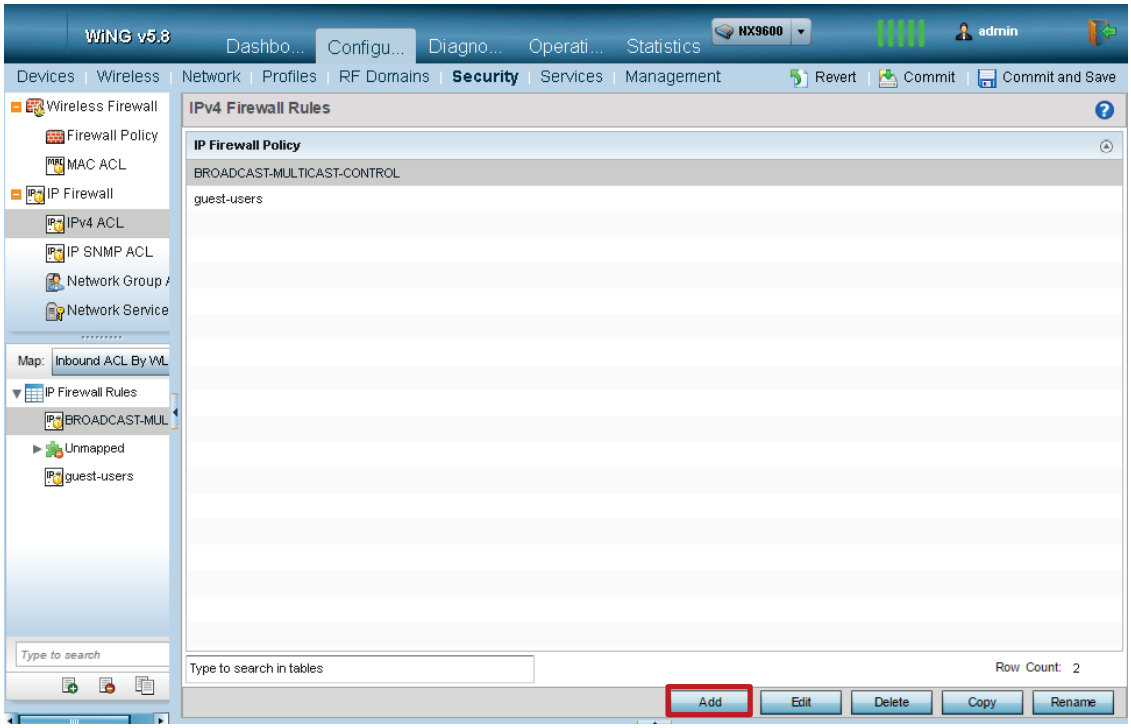
Scenario 1 – Match based on SSID

IP ACL and Application Policy Configuration

In the below example we will create an ACL named "guest-users", which allows DHCP, DNS, HTTP and HTTPS traffic going out to the internet, as well as traffic destined to the Captive Portal. Finally, we are going to drop any other IP traffic and also log drop hits. As a next step we will create an Application Policy that enforces restriction upon dynamic web-based applications that are difficult to track using standard ACLs. Note that Application Policy requires an Access Point to support DPI engine.

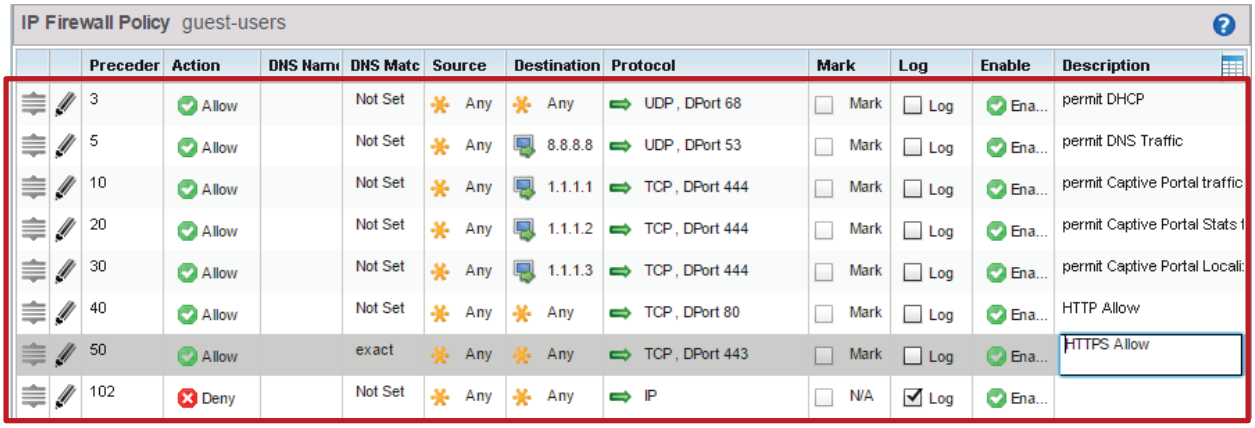
For the Web UI configuration navigate to "Configuration > Security > IP Firewall Rules" (or MAC Firewall Rules is so inclined). Click on "Add"

1. Web UI Creating New IPv4 ACL



Give your ACL a name and begin adding rules, clicking **"+Add Row"** for each new line.

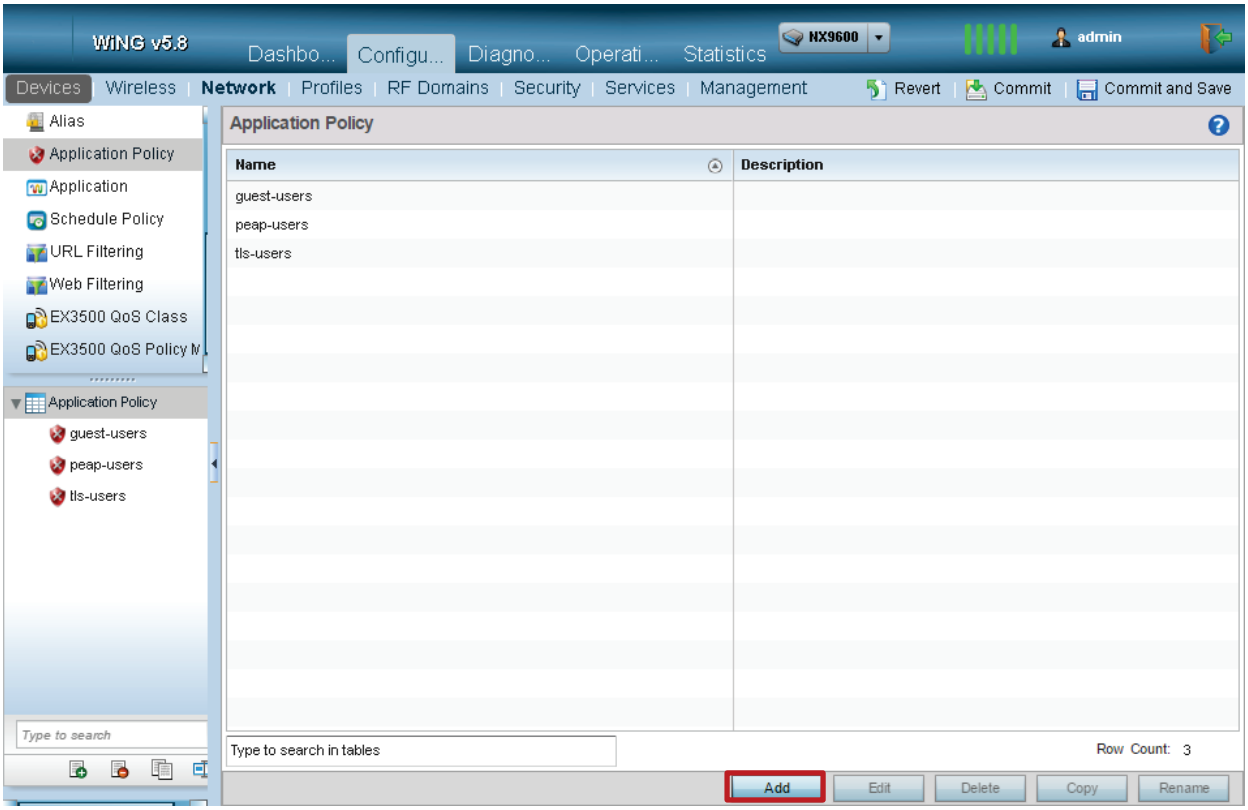
2. Web UI Adding ACL Rules



Once you have added all of your rules, click **">> Ok"**, then commit and save your work.

Navigate to **Configuration** > **Network** > **Application Policy**. Click on "**Add**"

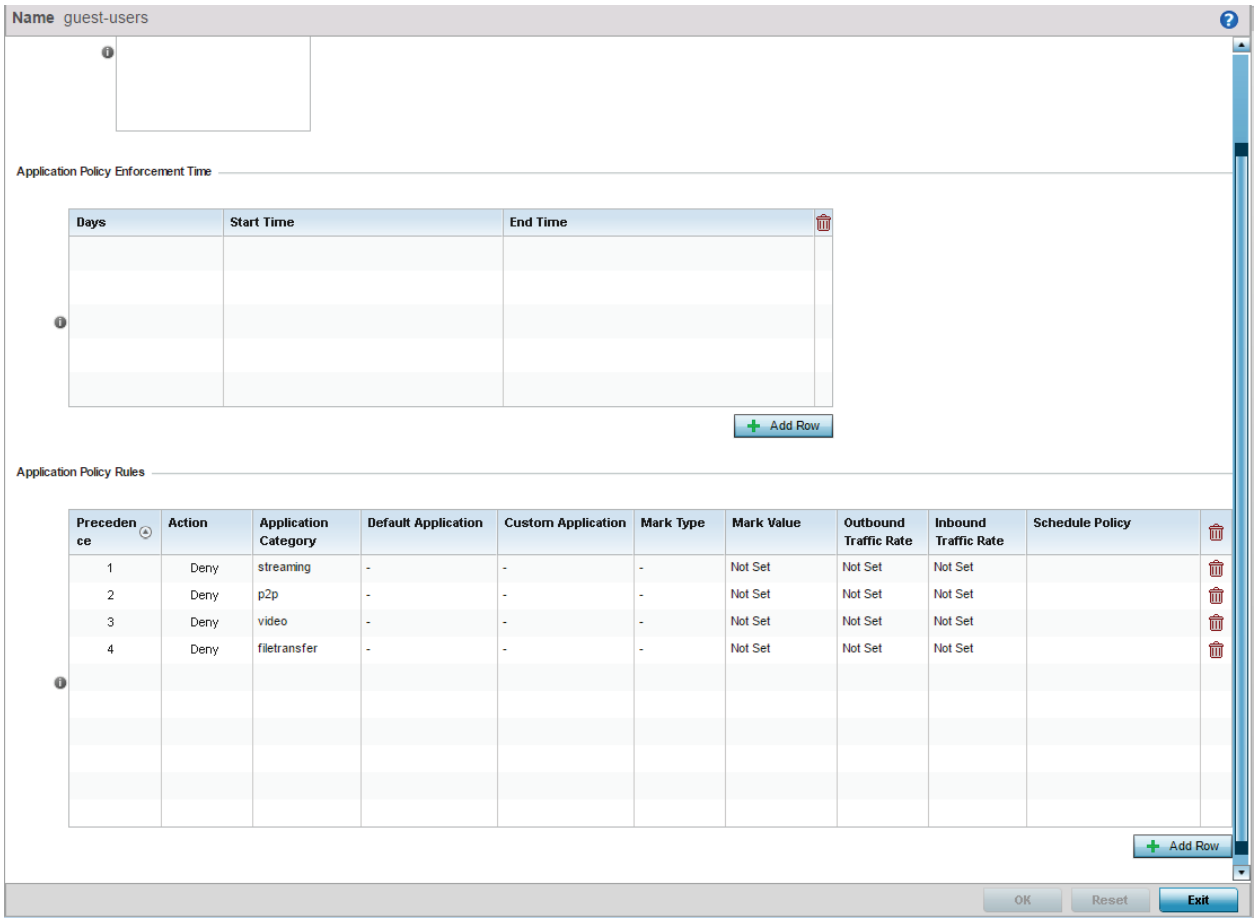
3. Web UI Creating Application Policy



Name your policy, add rules to deny all unwanted applications on a guest network.

Note
Application policy unlike ACL permits all traffic by default.

5. Web UI Adding Application Rules



6. Once you have added all of your rules, click "**>> Ok**", then commit and save your work.

The following section outlines CLI configuration snippet:

1. CLI IP Access List configuration

```
!
ip access-list guest-users
 permit udp any eq 68 any eq dhcps rule-precedence 3 rule-description "permit DHCP"
 permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description "permit DNS traffic"
 permit tcp any host 1.1.1.1 eq 444 rule-precedence 10 rule-description "permit Captive Portal traffic"
 permit tcp any host 1.1.1.2 eq 444 rule-precedence 20 rule-description "permit Captive Portal Stats
traffic"
 permit tcp any host 1.1.1.3 eq 444 rule-precedence 30 rule-description "permit Captive Portal Localization
traffic"

 permit tcp any any eq 80 rule-precedence 40 rule-description "HTTP Allow"
 permit tcp any any eq 443 rule-precedence 50 rule-description "HTTPS Allow"
 deny ip any any log rule-precedence 100
!
```

2. CLI Application Policy configuration

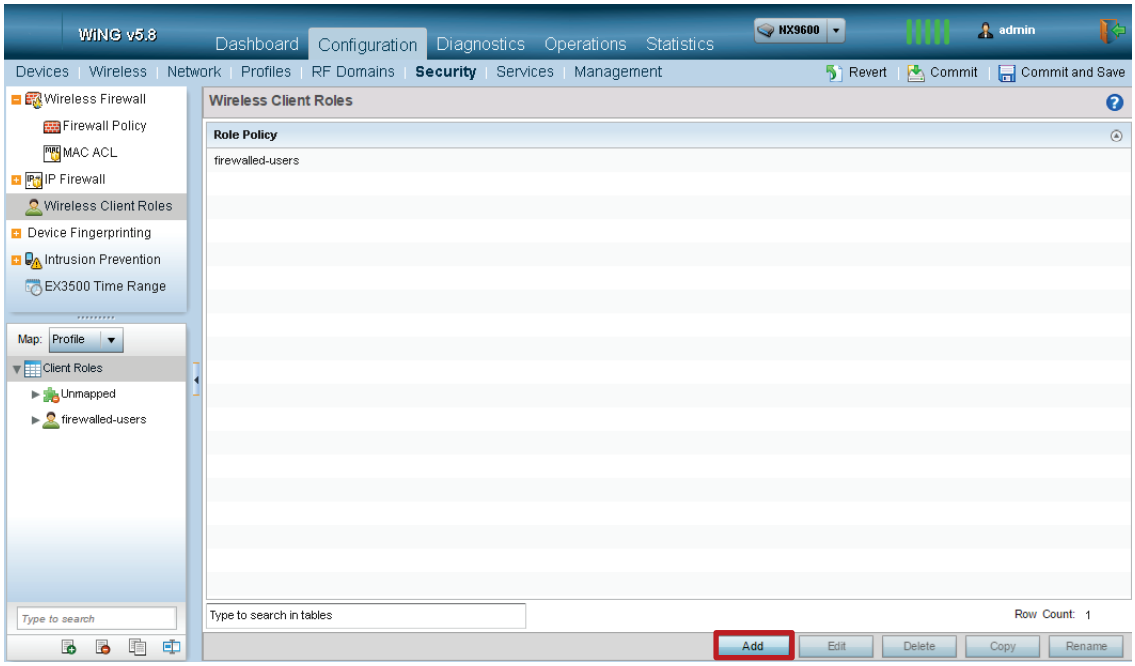
```
!

application-policy guest-users

 deny app-category streaming precedence 1
 deny app-category p2p precedence 2
 deny app-category tunnel precedence 3
!
```

Role Policy Configuration

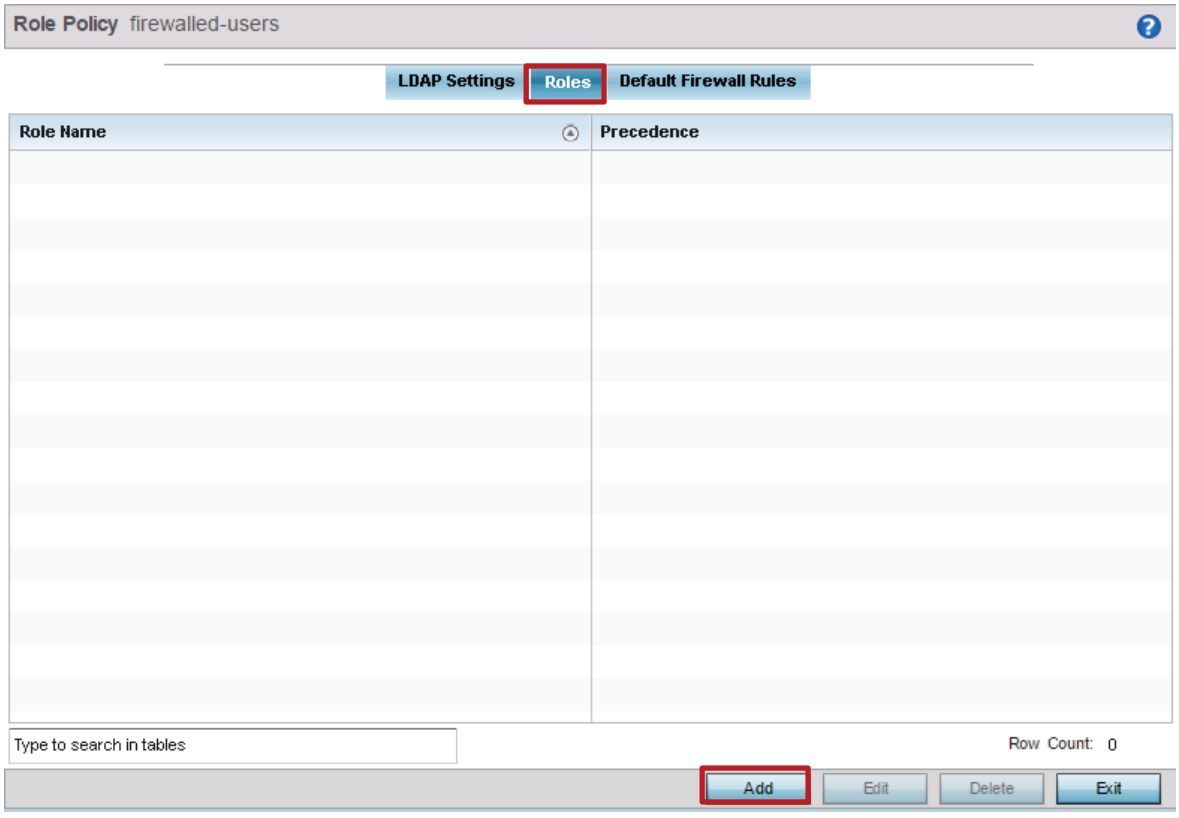
Next we are going to create a role-policy and apply it to the access point profile. We will also enable DPI engine to enable application recognition and control.

In the Web UI navigate to “Configuration > Security > Wireless Client Roles” and click on “Add” to create a new role policy:

1. Web UI Creating Role Policy

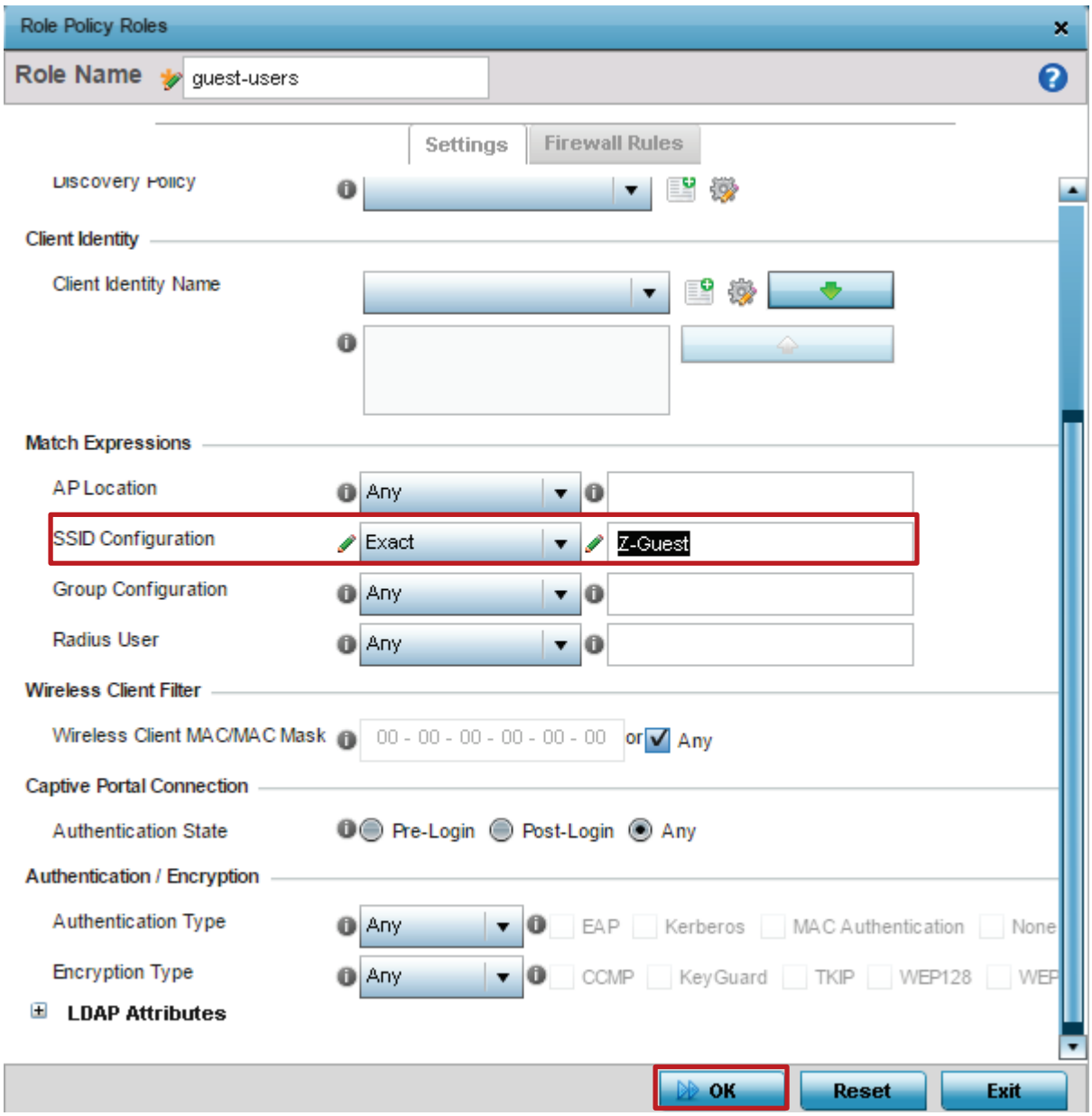


2. Web UI Creating Role Policy



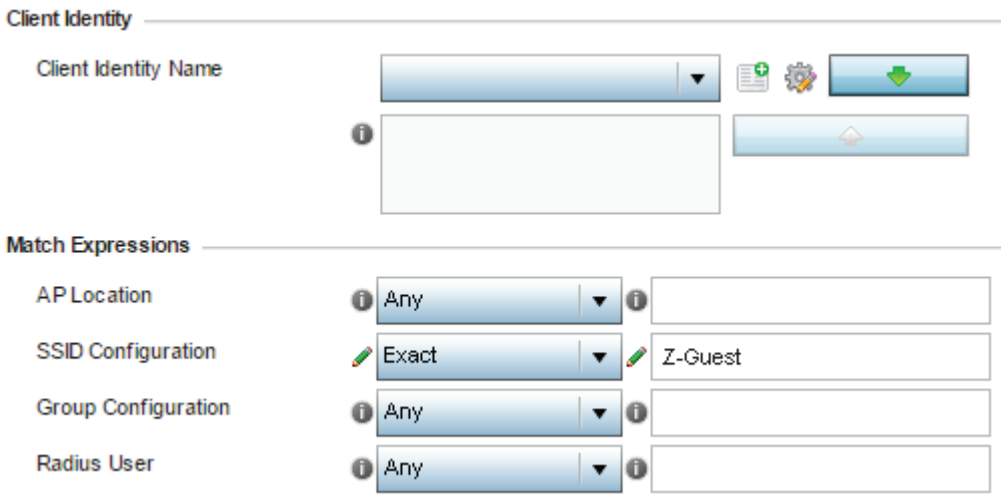
Name the role policy and then click "Add" to begin adding match criteria for the user role.

3. Web UI Creating Role Policy



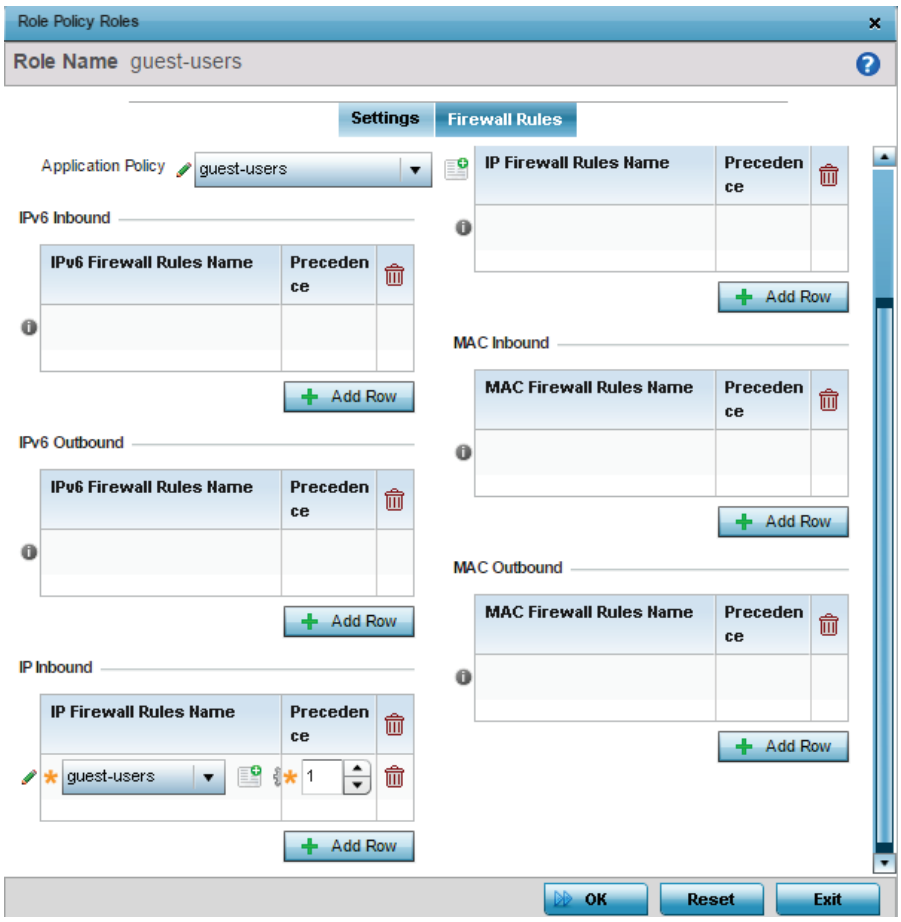
As can be seen, you may select a number of variations for match criteria. We have selected an exact match on the SSID, however other options exist as shown below.

5. Web UI Role Policy Match Expressions



After selecting your match criteria, go to the "Firewall Rules" tab and select the previously configured IP access list or whatever firewall rules you have previously configured. Add additional rows for additional firewall rules as needed by clicking "+Add Row". Also assign Application Policy that you have created earlier.

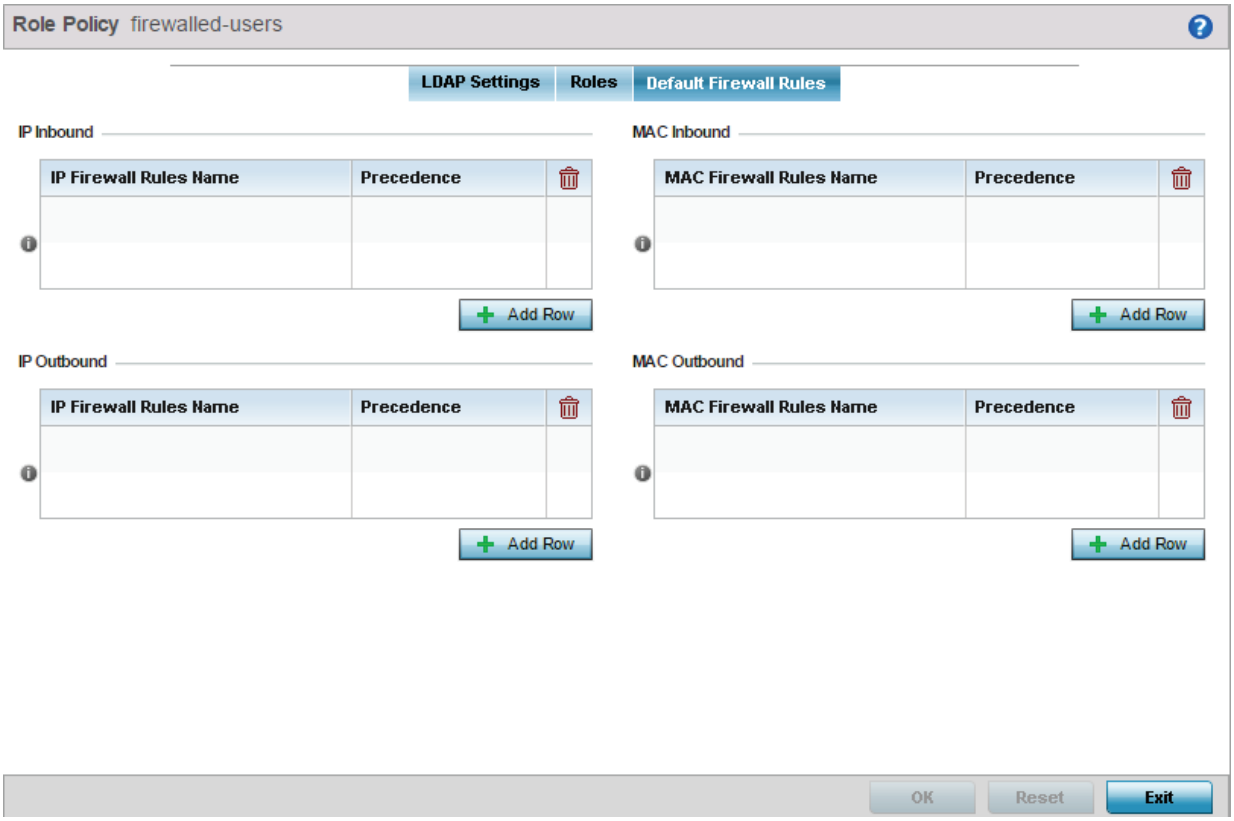
6. Web UI Role Policy Assignements



Note

On the "**Default Firewall Rules**" tab of your role policy, you may select default access lists to be applied whether or not match criteria have been met. Realize that these rules are applied at the level where the role policy has been applied (access point level). Exercise caution to ensure traffic is not interrupted inadvertently due to a default rule. In our case we have specified no defaults, as seen below.

7. Web UI Default Role

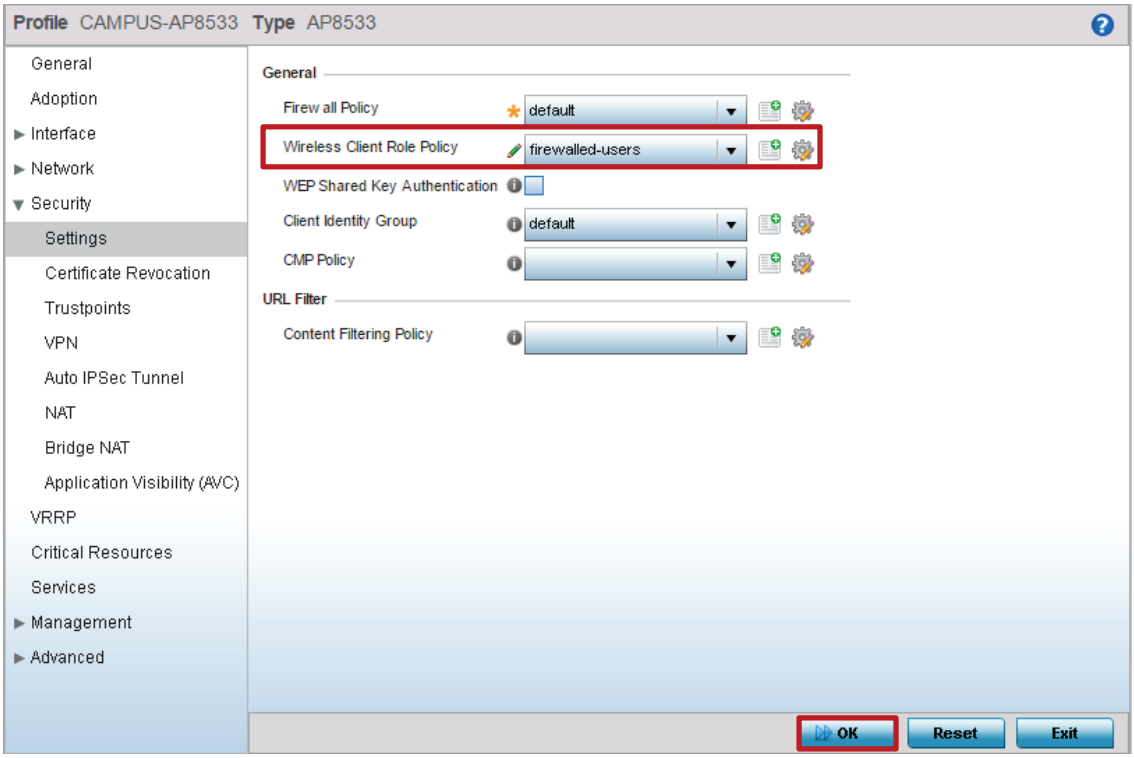


Applying Role Policy

The final step is to apply the role policy to your devices. This will usually be done at the access point level (profile or device override) as that is the point of ingress for the wireless clients.

Navigate to "**Configuration** > **Profiles**" and select / edit the profile you wish to apply the role policy to. Within the profile, navigate to "**Security** > **Settings**" and select your policy from the "**Wireless Client Role Policy**" drop-down box.

1. Web UI Applying Role Policy



Click **">>Ok"** and then **Commit and Save** your work.

The following shows the CLI configuration snippet:

2. CLI Role Policy configuration

```
!
role-policy firewalled-users
 user-role guest-users precedence 1
  ssid exact Z-Guest
  use ip-access-list in guest-users precedence 1
  use application-policy guest-users
!
profile ap8533 CAMPUS-AP8533
 ///configuration removed for brevity///
 use role-policy firewalled-users
 dpi
!
```

Scenario 2 – Match based on the User Group

Scenario 2 is the same basic setup, except for now our match criteria will be based on group membership as gathered from the external AAA server. This is useful when it is required to differentiate between client devices using the same ESSID, but different EAP types, like EAP-TLS vs PEAP-MSCHAPv2 or to differentiate between the users that belong to different user groups, like Sales vs Marketing vs Engineering and so on.

In this example we will use Microsoft NPS as an external RADIUS server that will provide Vendor Specific Attributes with the user group name that will be used by WiNG 5 Role Based Firewall as a match criteria. The same user account will be used for testing, while role assignments are based on returned user group name.

The following sections will just show the configuration of the additional components (in order of configuration), which are:

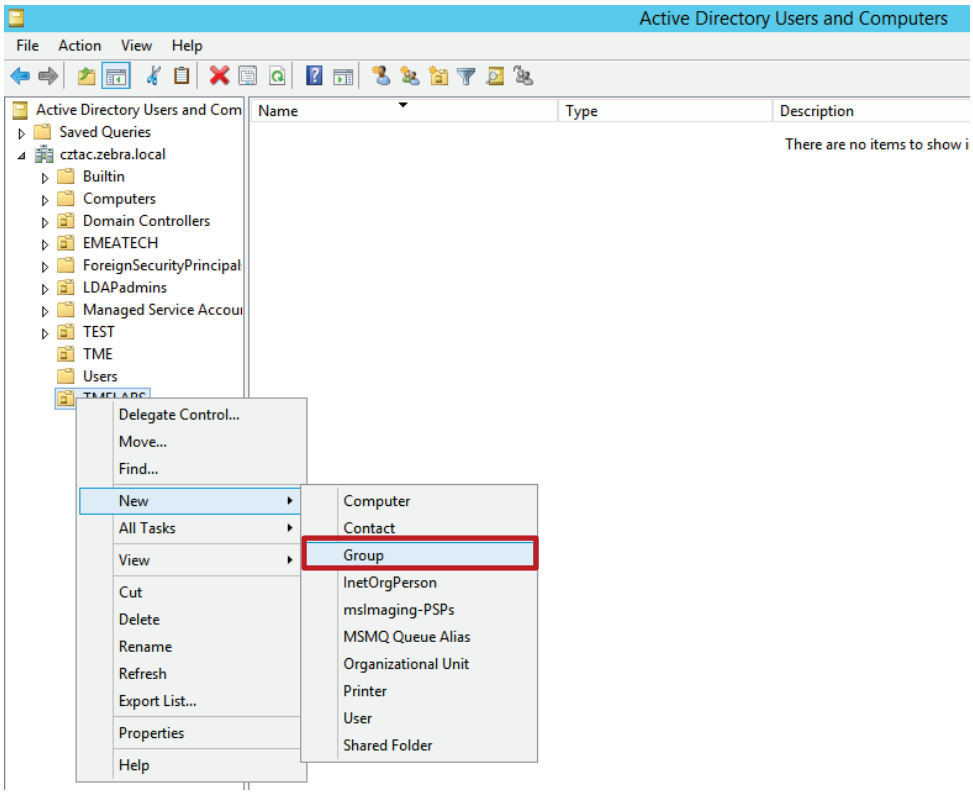
1. External RADIUS Configuration (Microsoft NPS)
2. AAA Policy
3. WLAN Authentication

External RADIUS Configuration (Microsoft Network Policy Server)

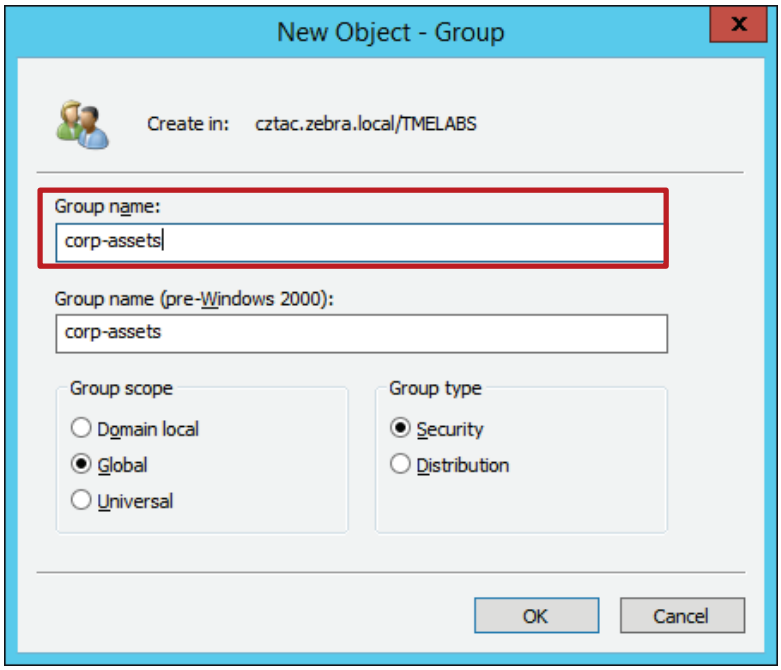
In this scenario, we are using Microsoft NPS as a RADIUS server, but similar approach can be used also with any other RADIUS server, including onboard RADIUS on WiNG5.

In Active Directory we will create a single user for this example that would be member of "corp-assets" group.

1. Active Directory Create New User Group

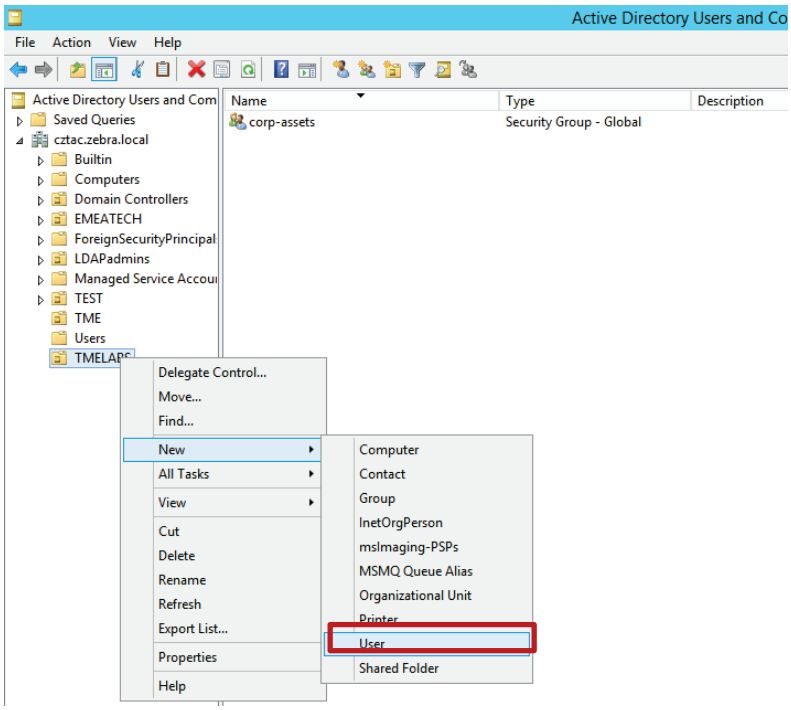


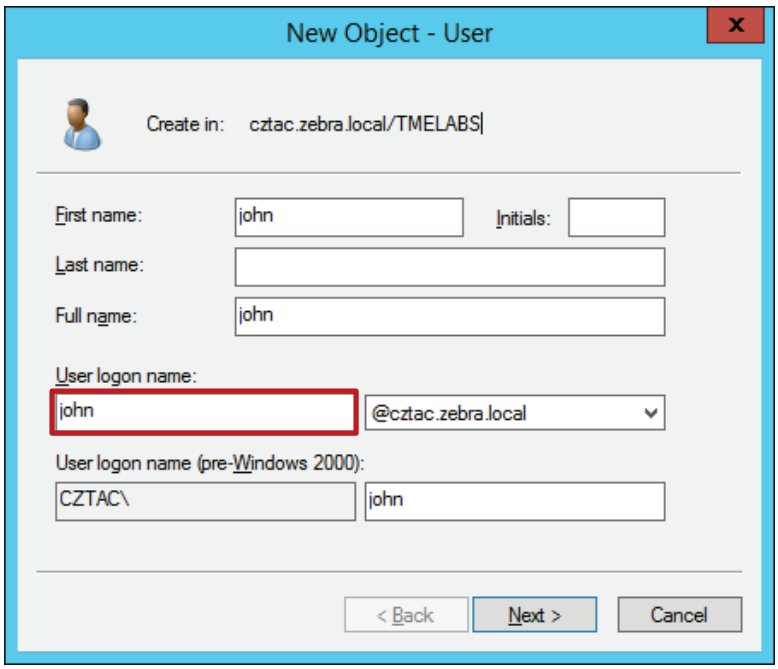
2. Active Directory Create New User Group

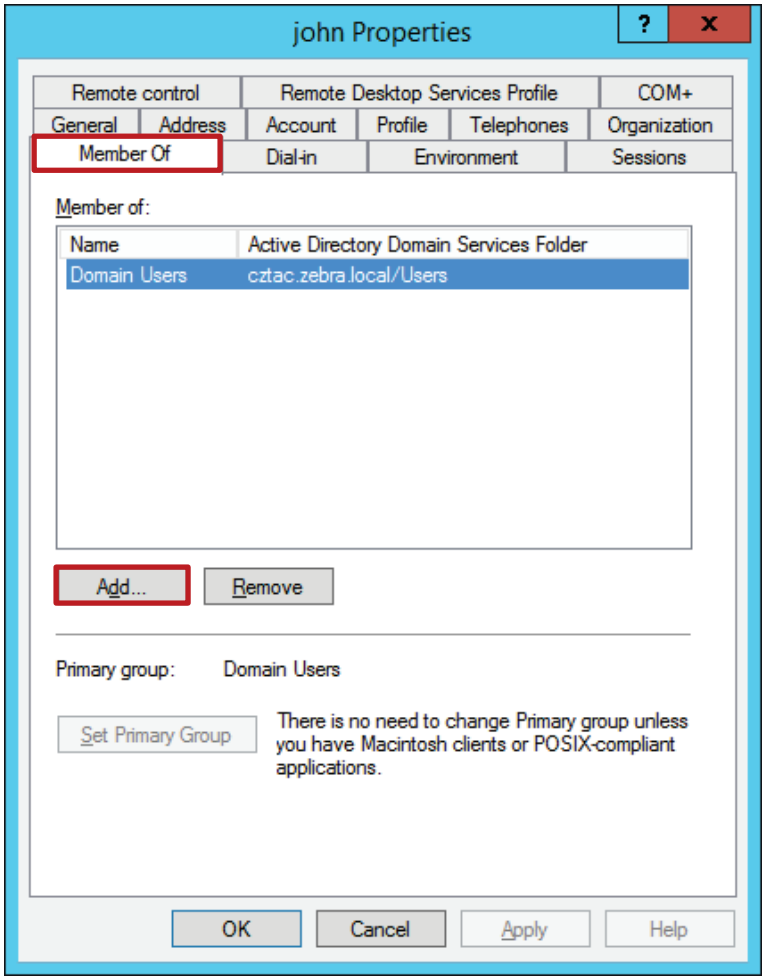


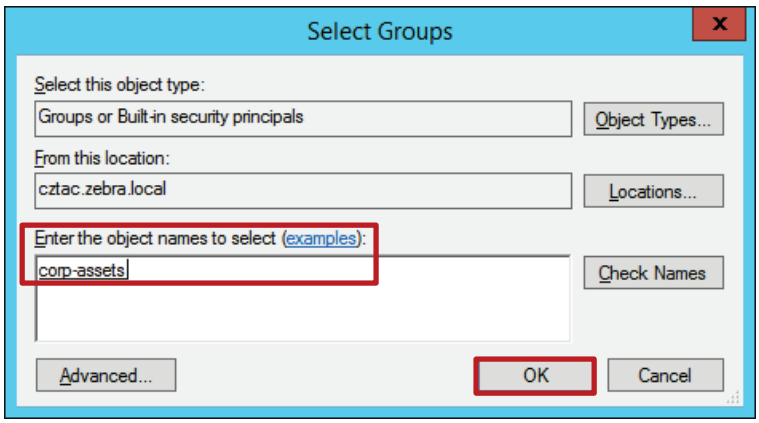
Following group creation, we will create a user and make this user a member of the corp-assets user group.

3. Active Directory Create New User



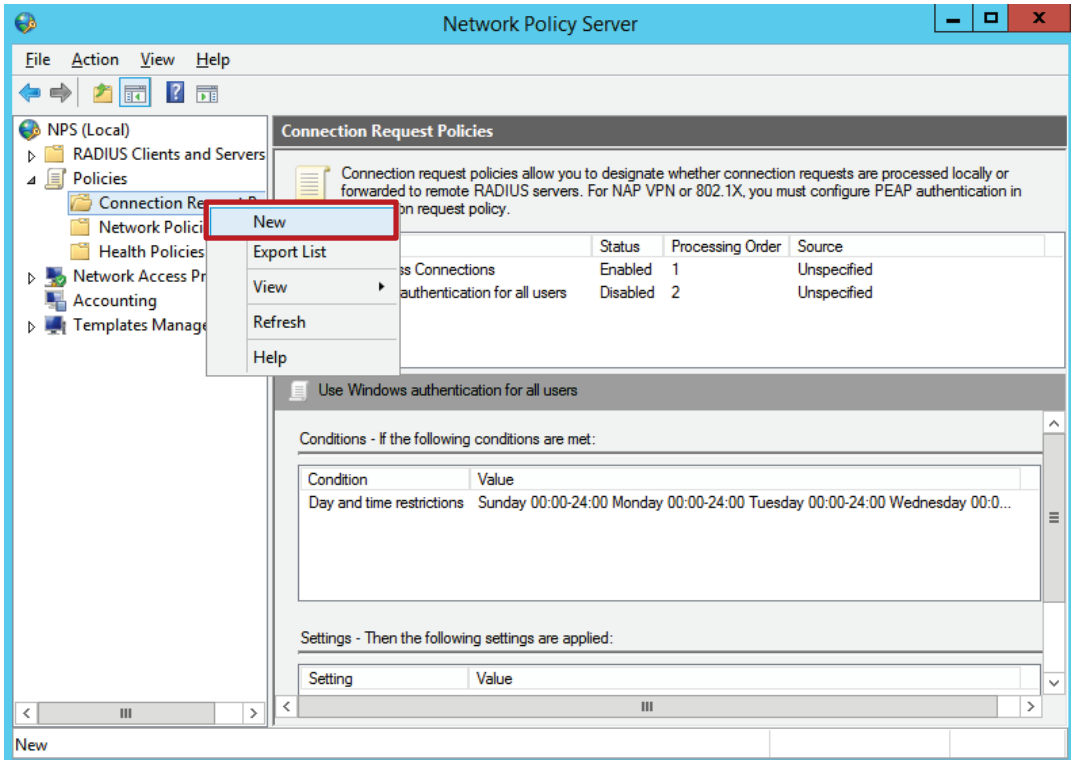


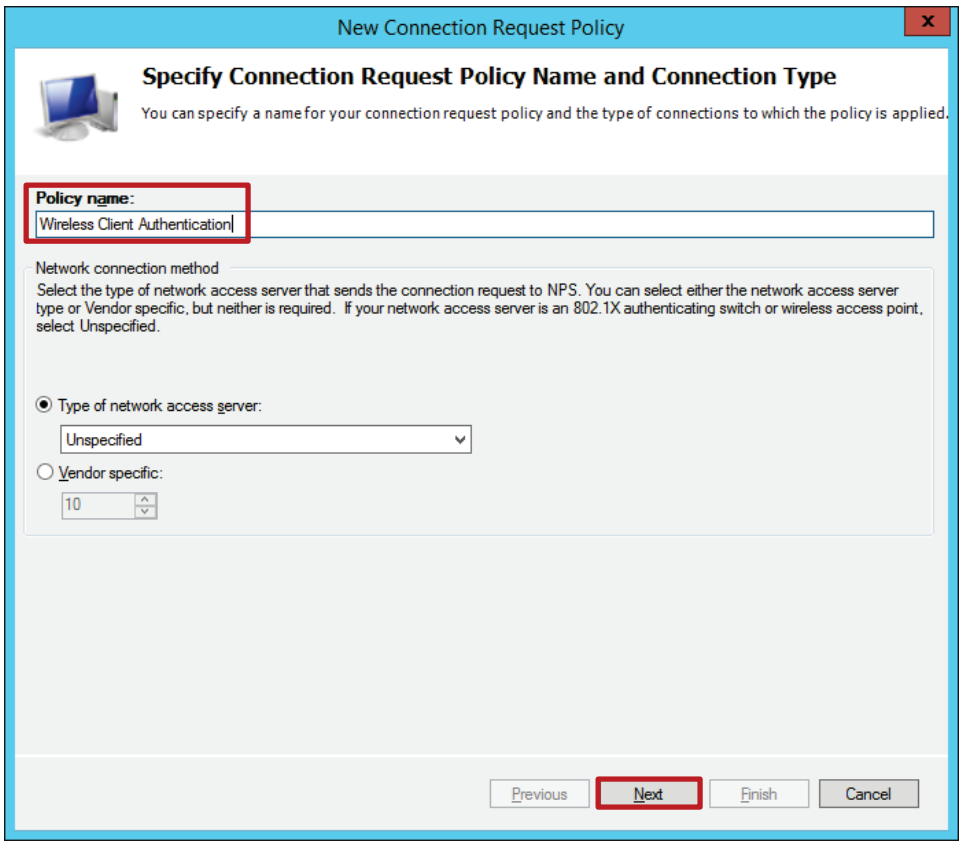


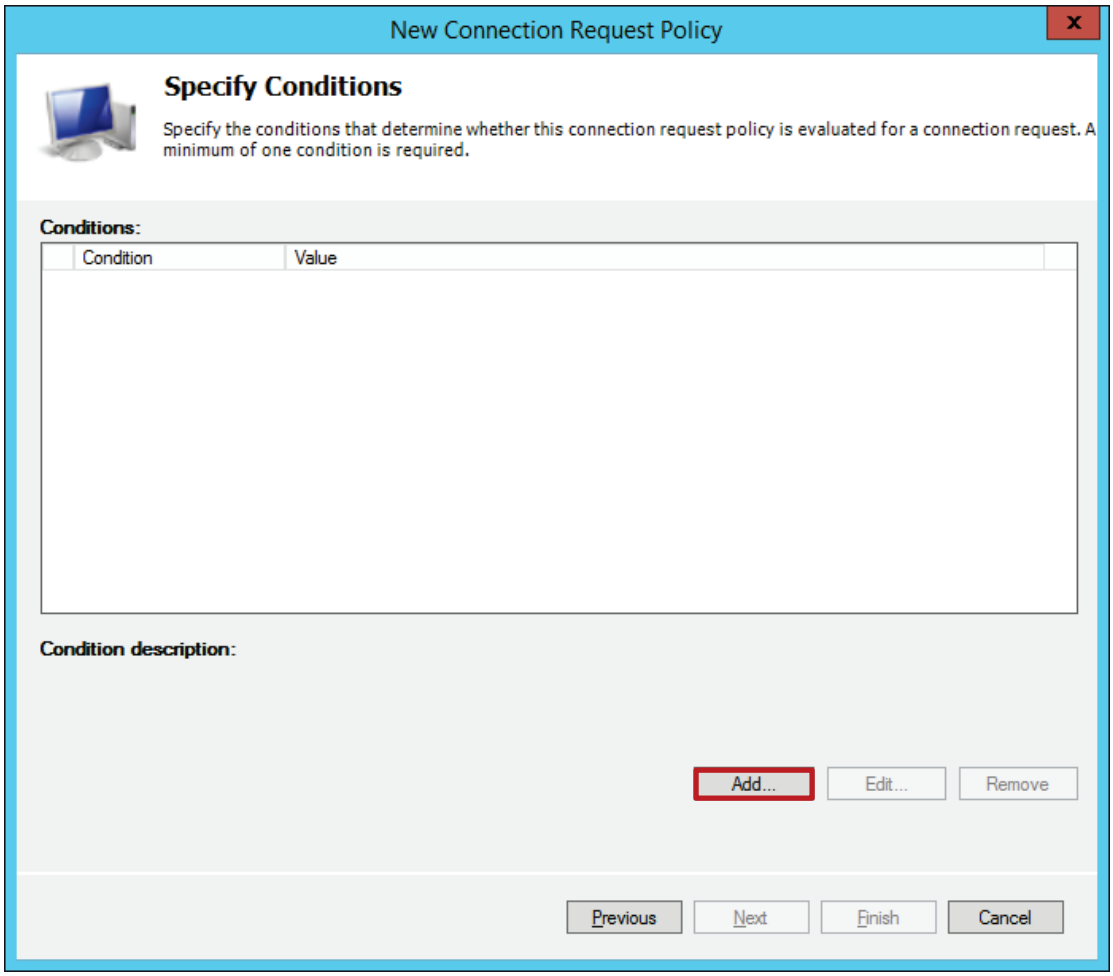


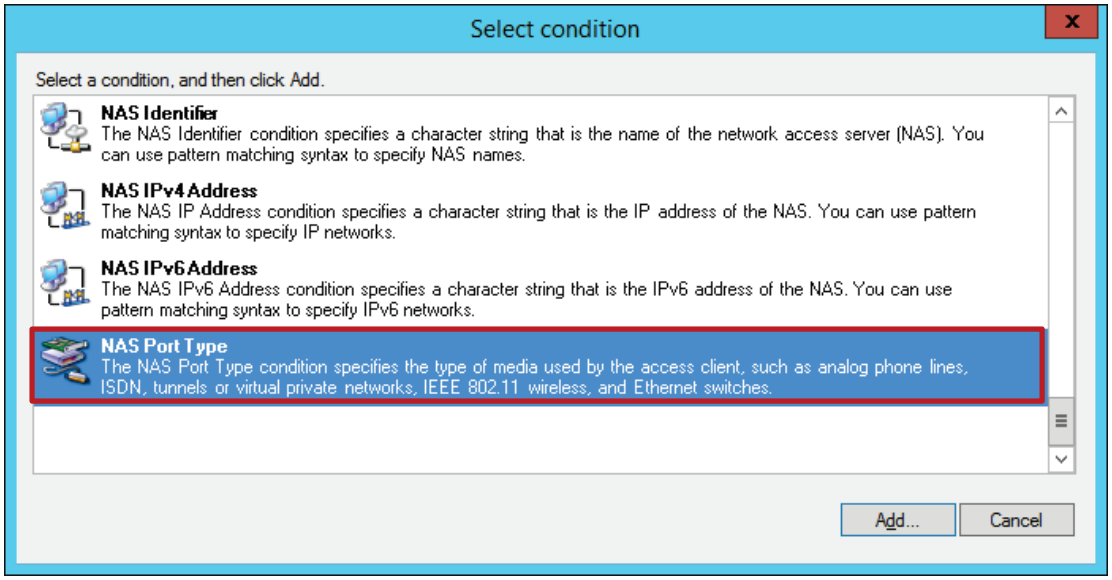
As a next step we will create new connection policy to allow 802.11 Wireless EAP Authentication using either PEAP-MSCHAPv2 or EAP-TLS, followed by a new Network Policy that will further differentiate between the two EAP types and send WiNG Vendor Specific Attribute back to apply correct user role:

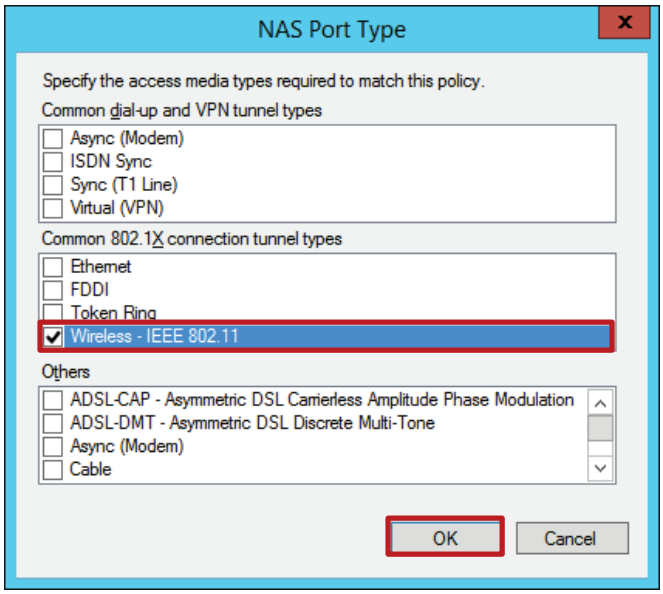
4. Network Policy Server configuration

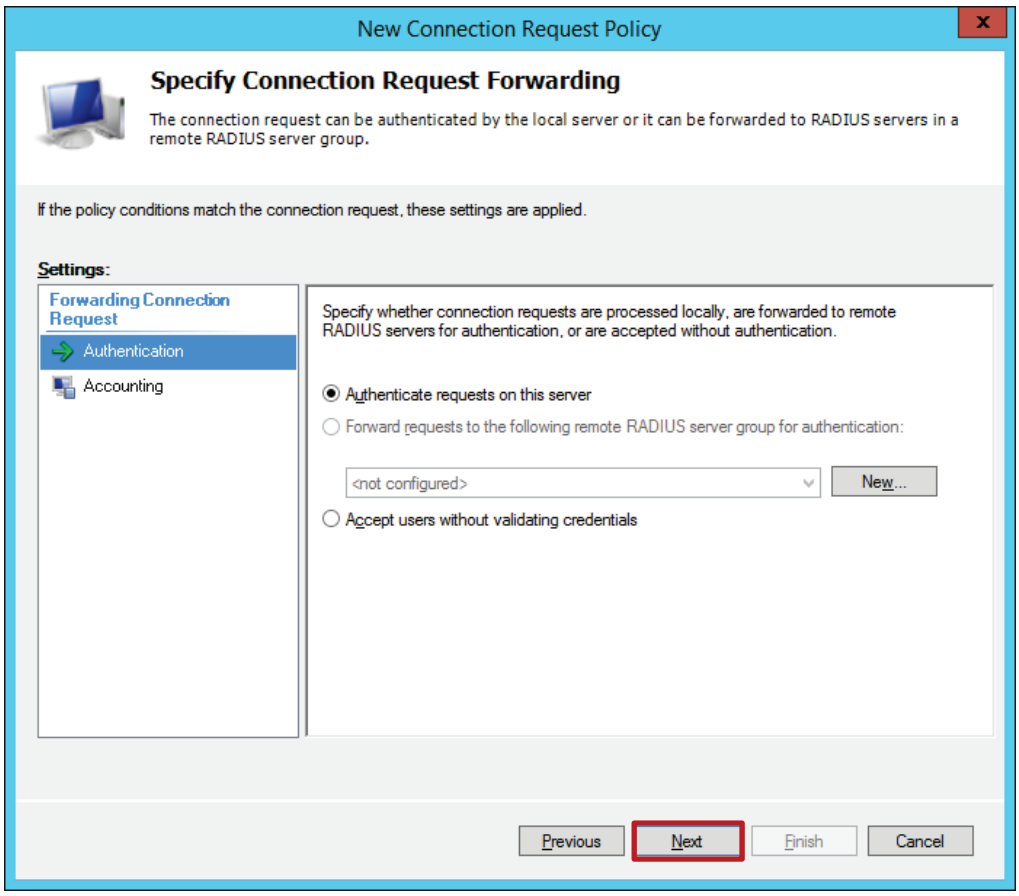


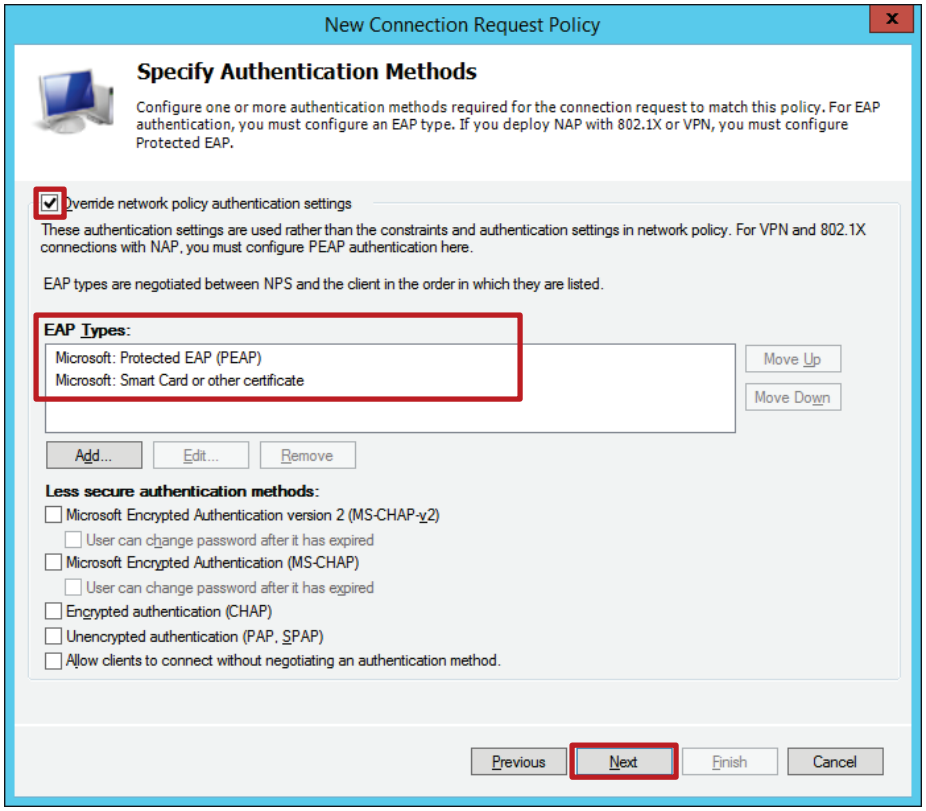


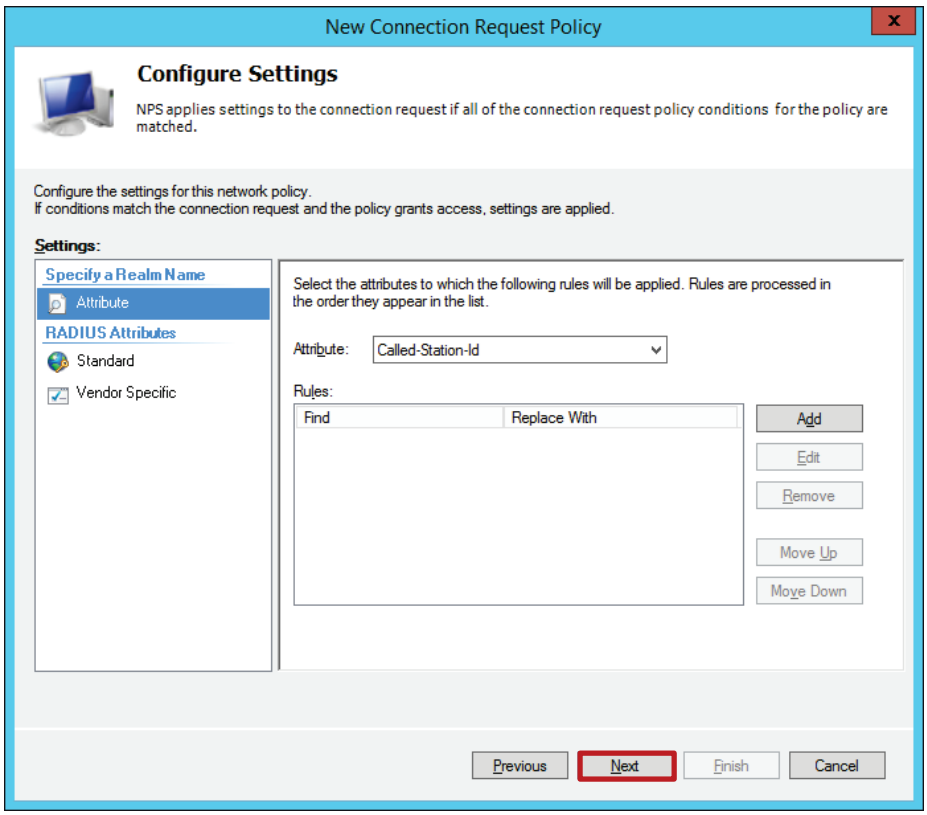


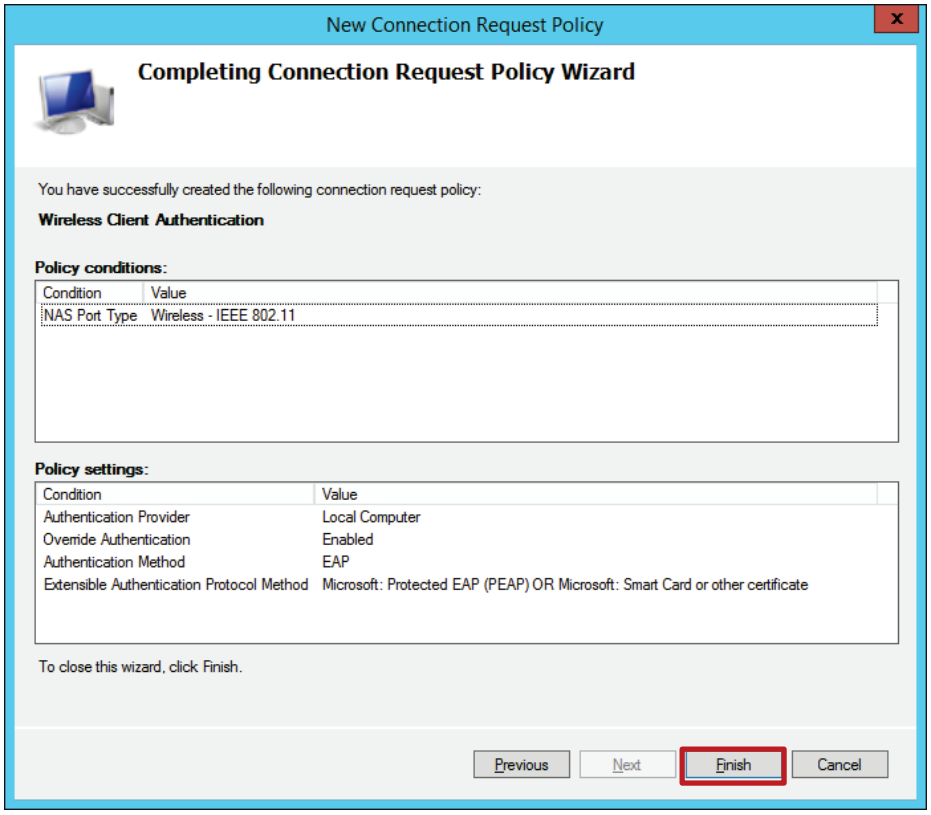




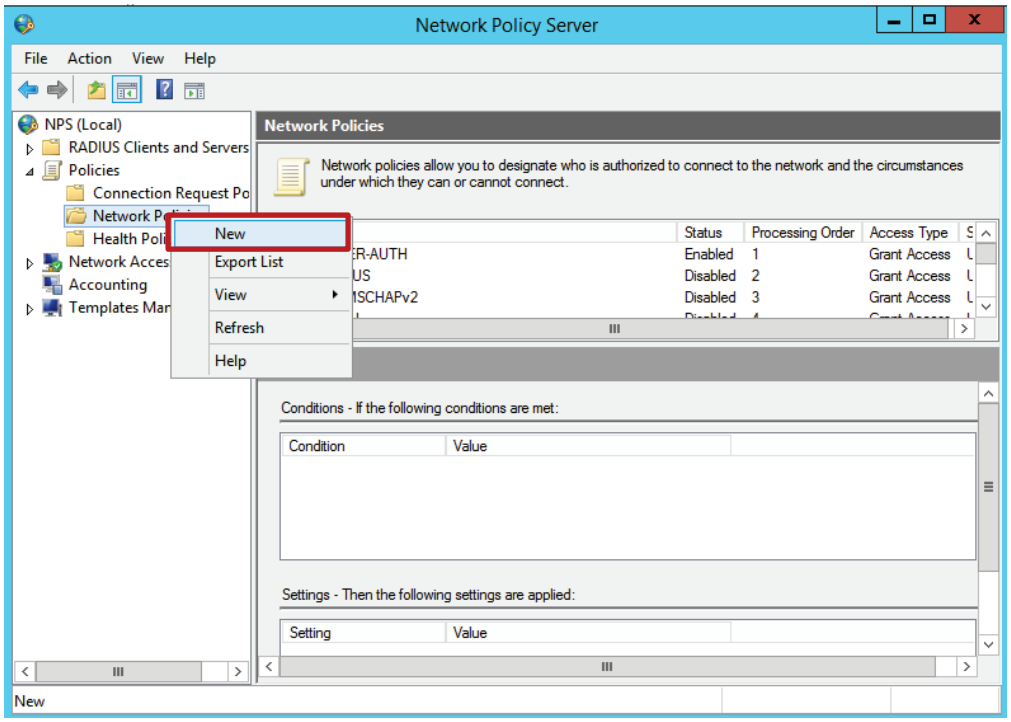


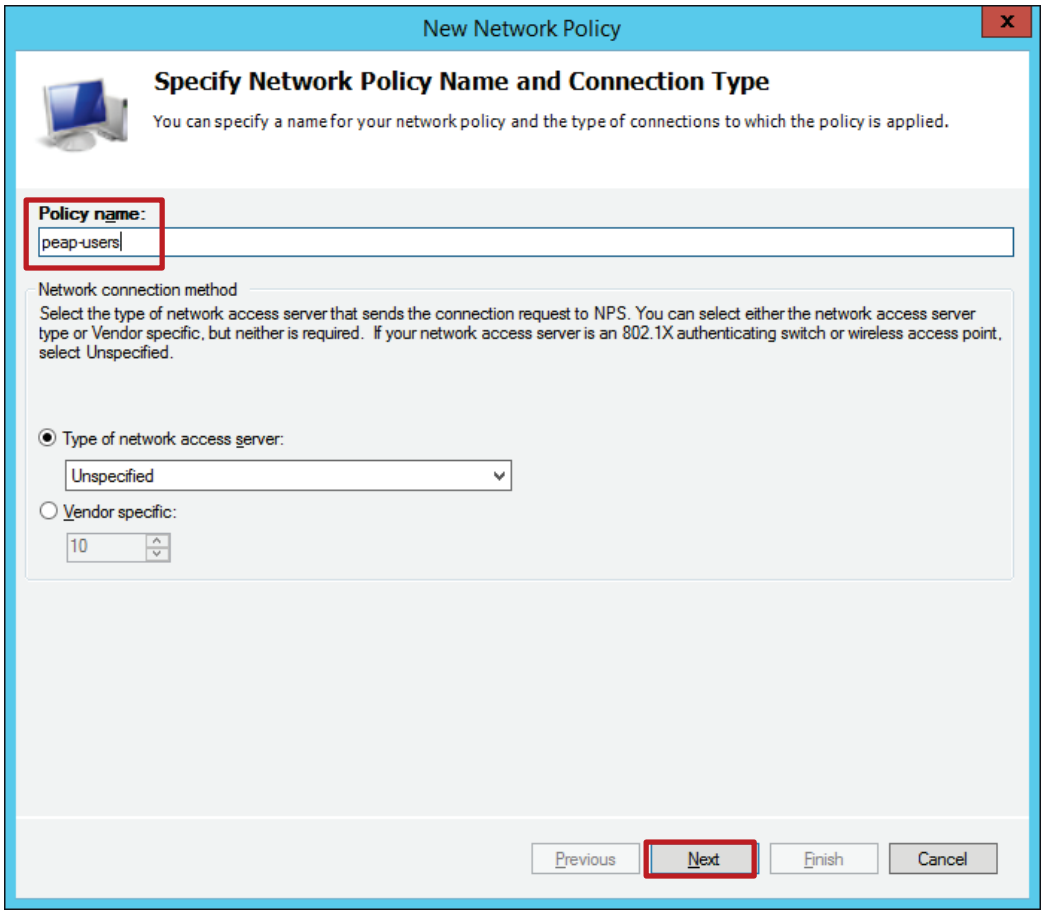


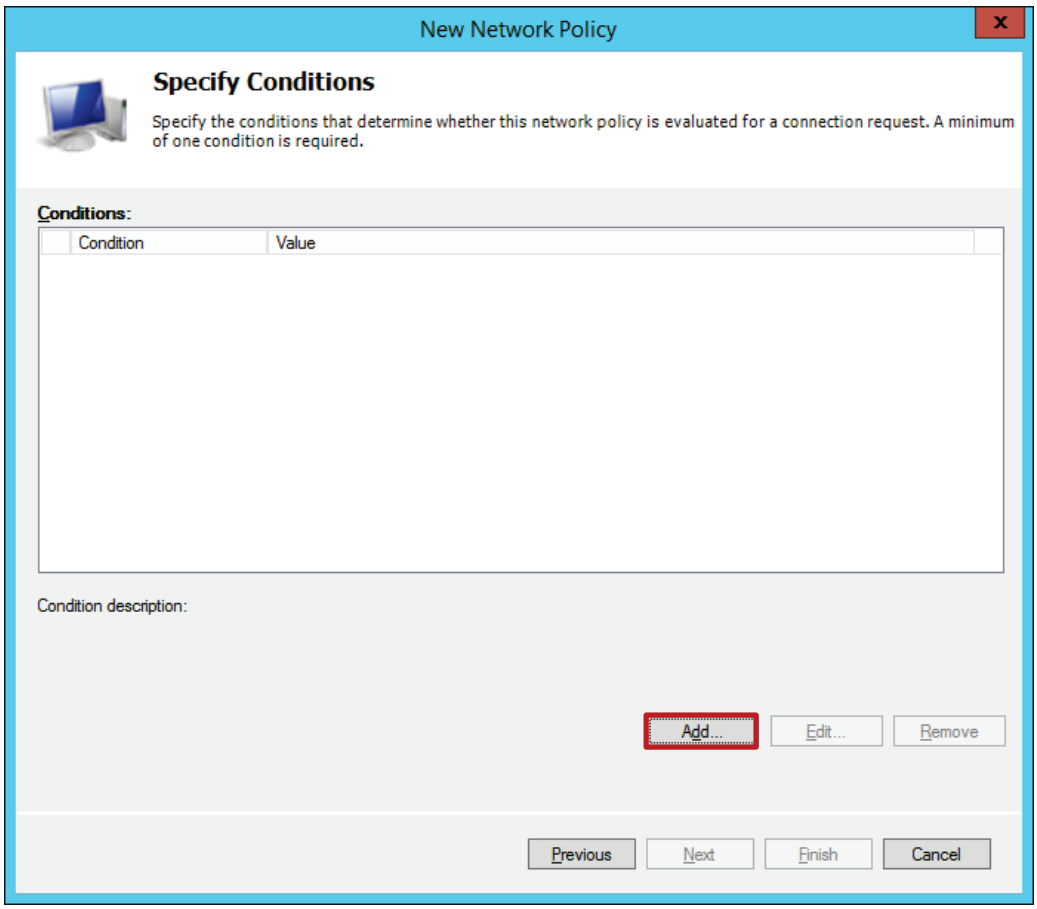


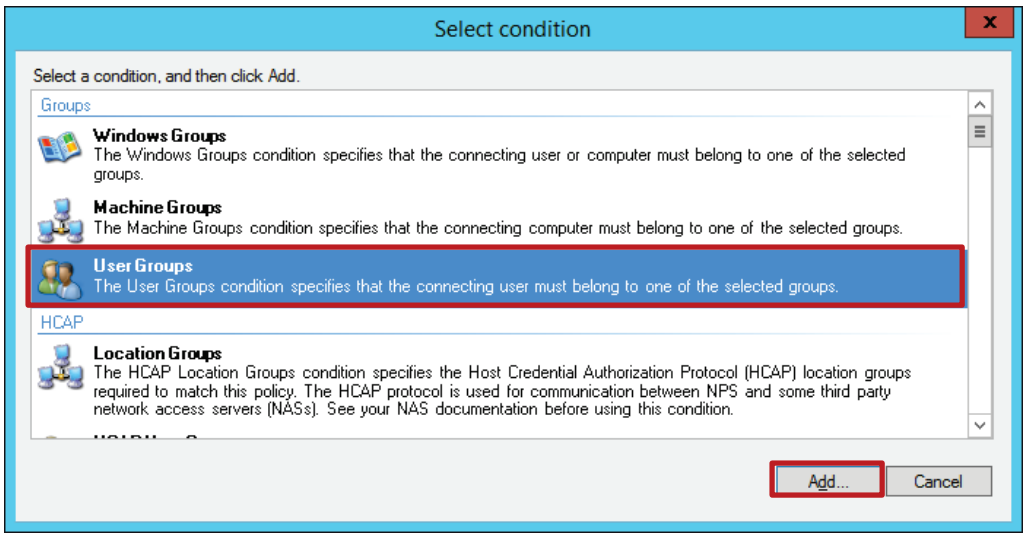


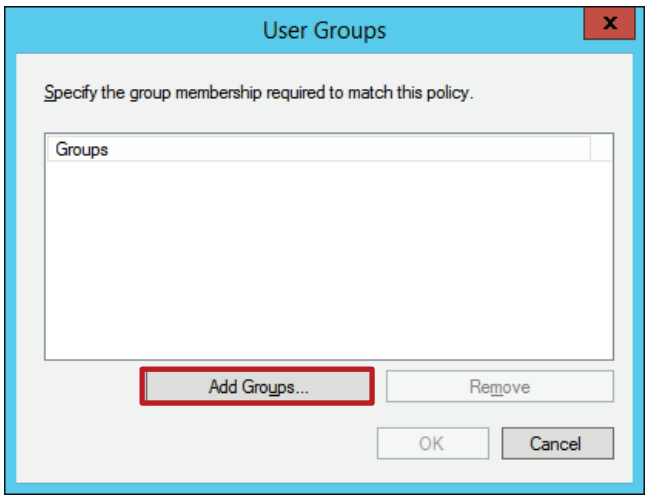
6. NPS Create Network Policies

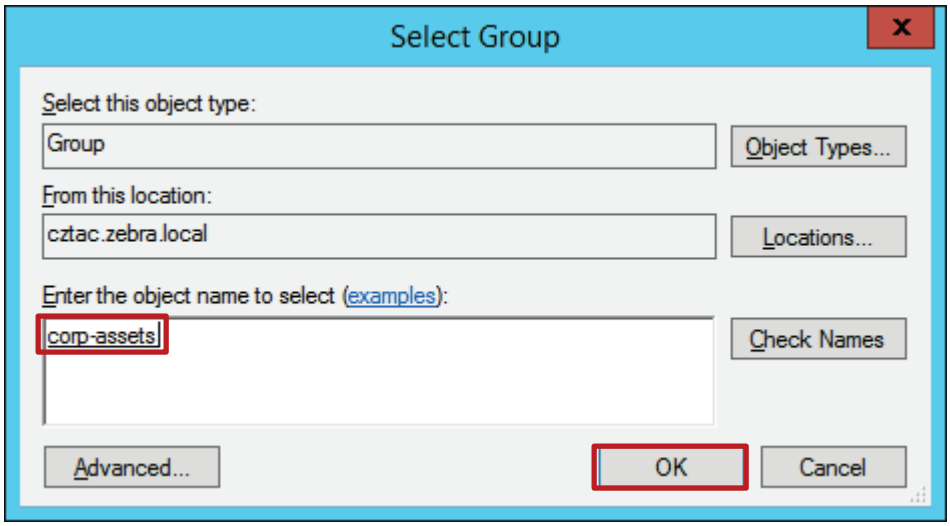


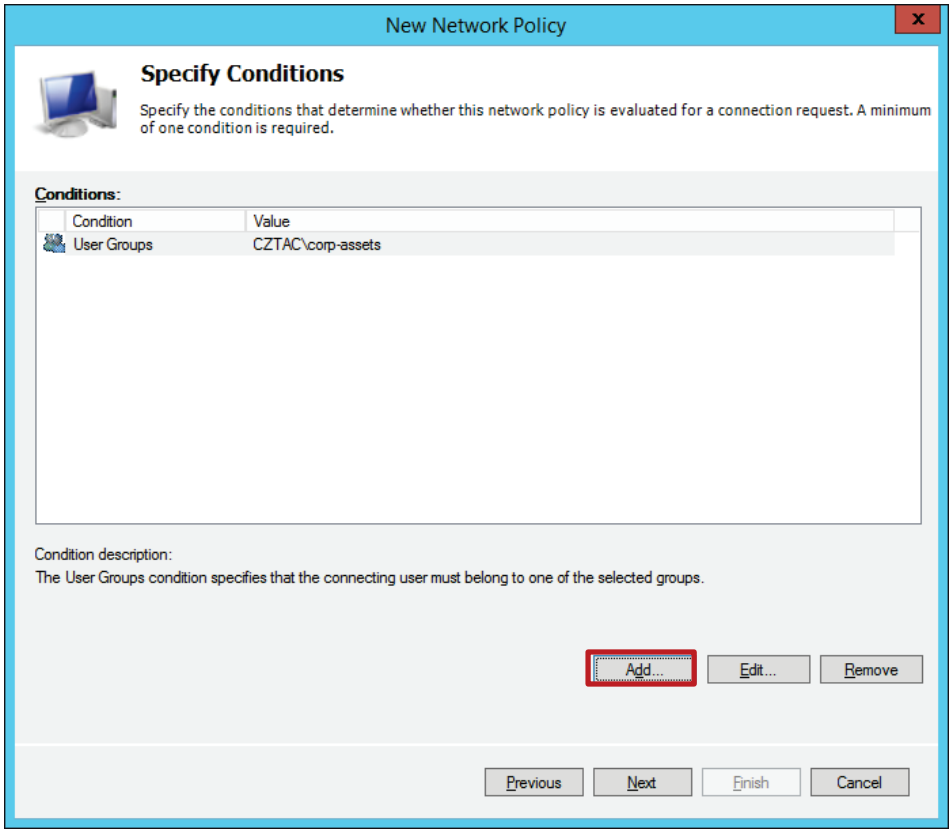


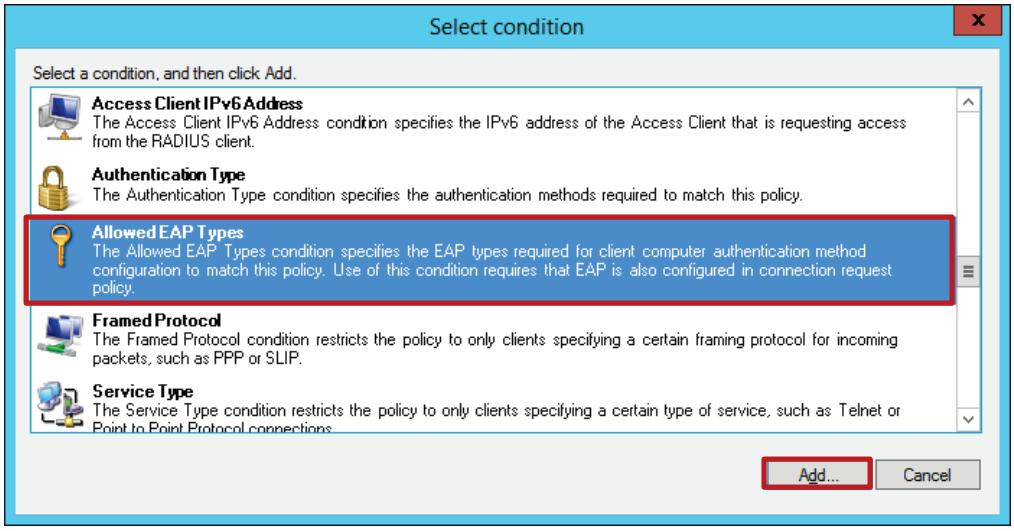


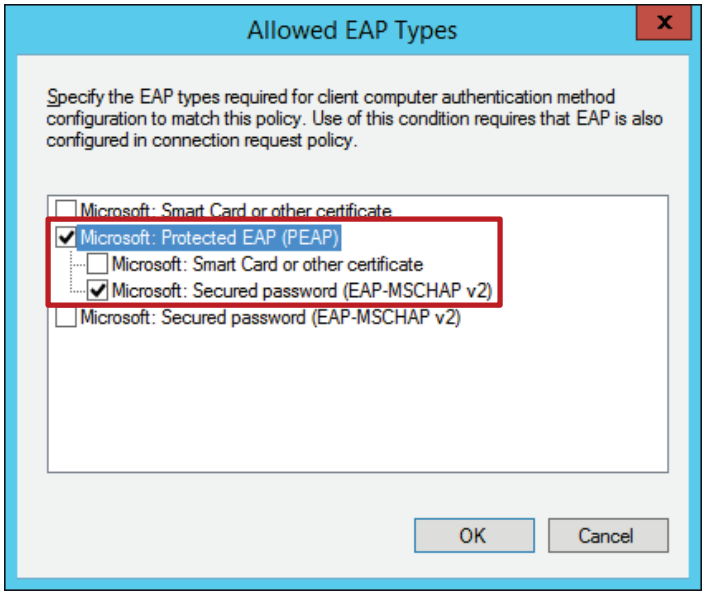


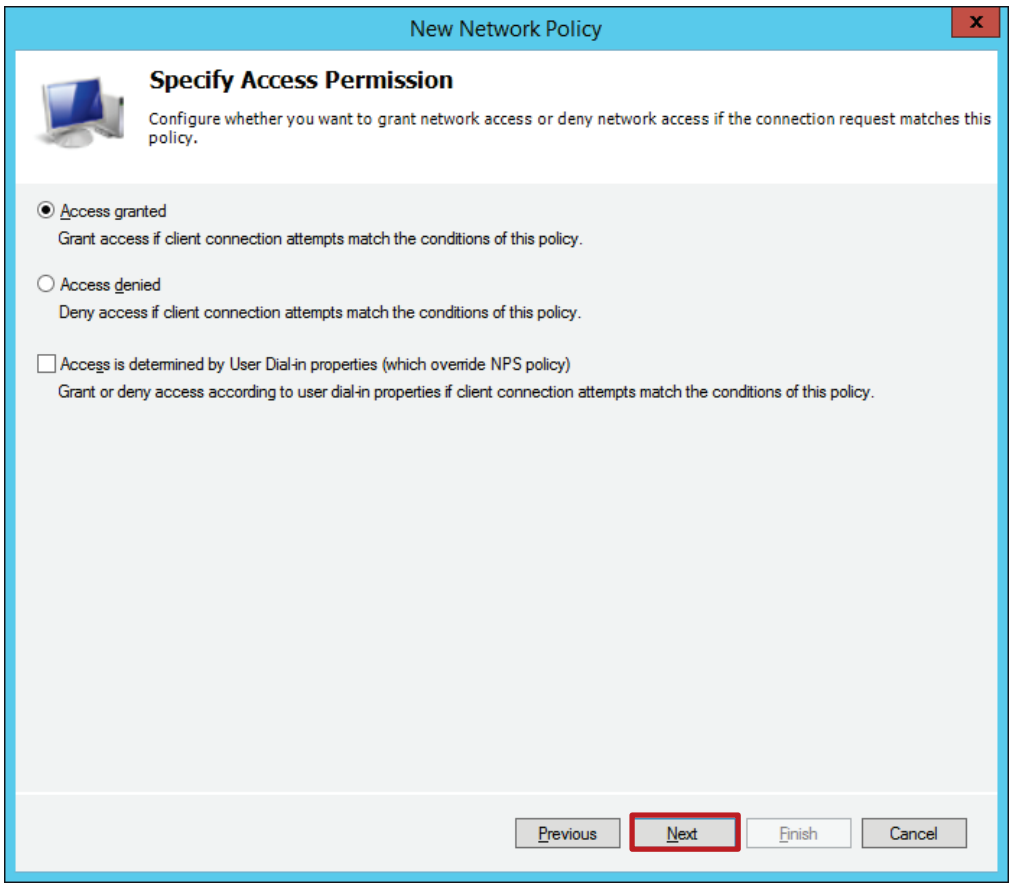


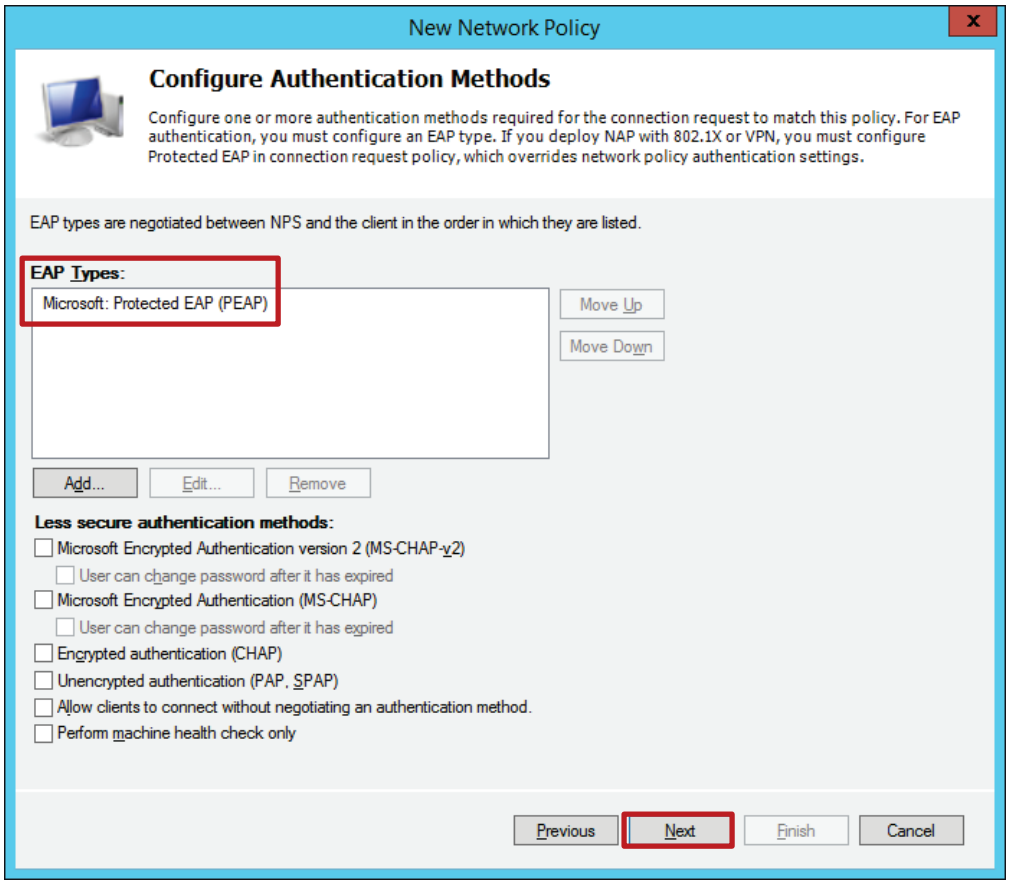


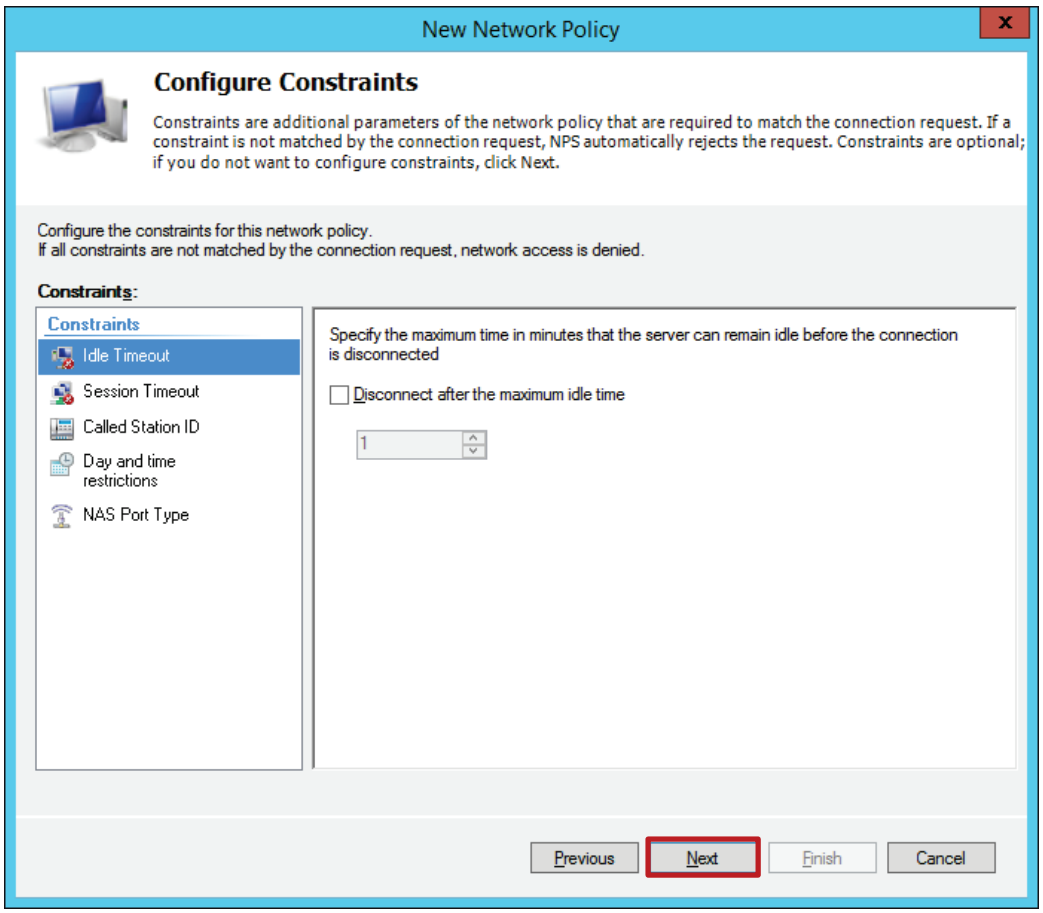


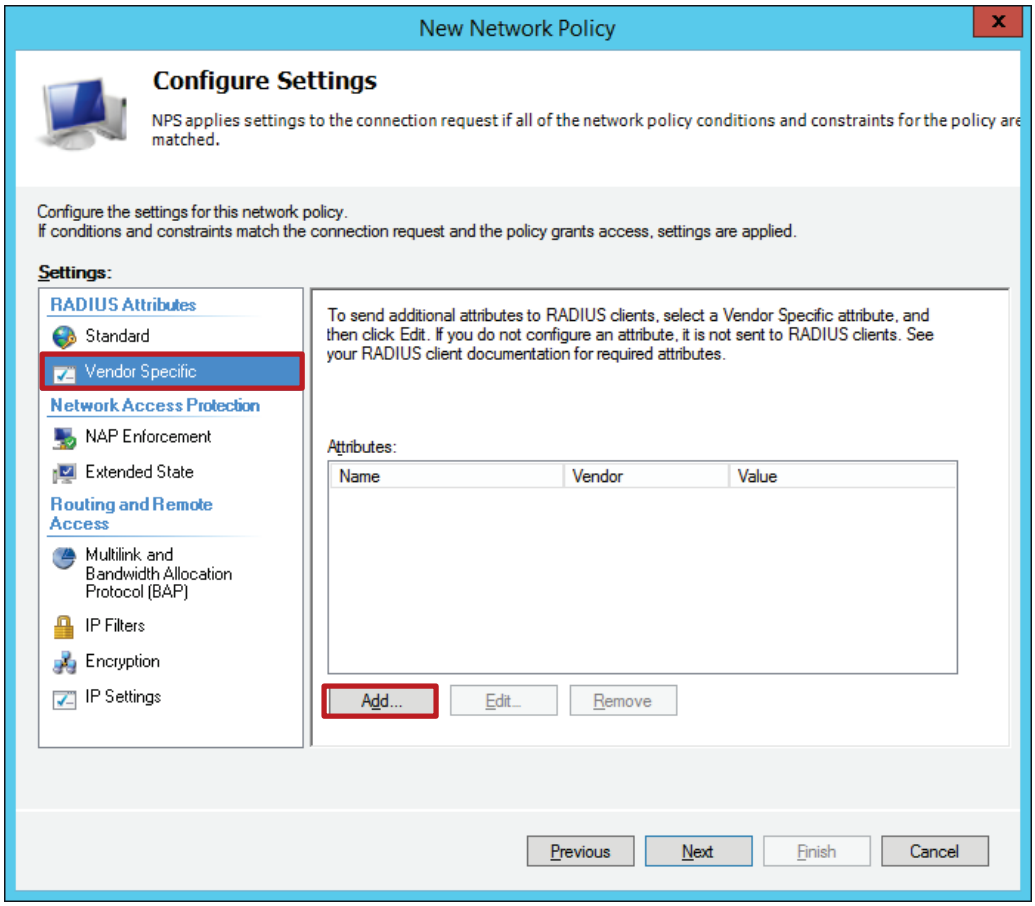




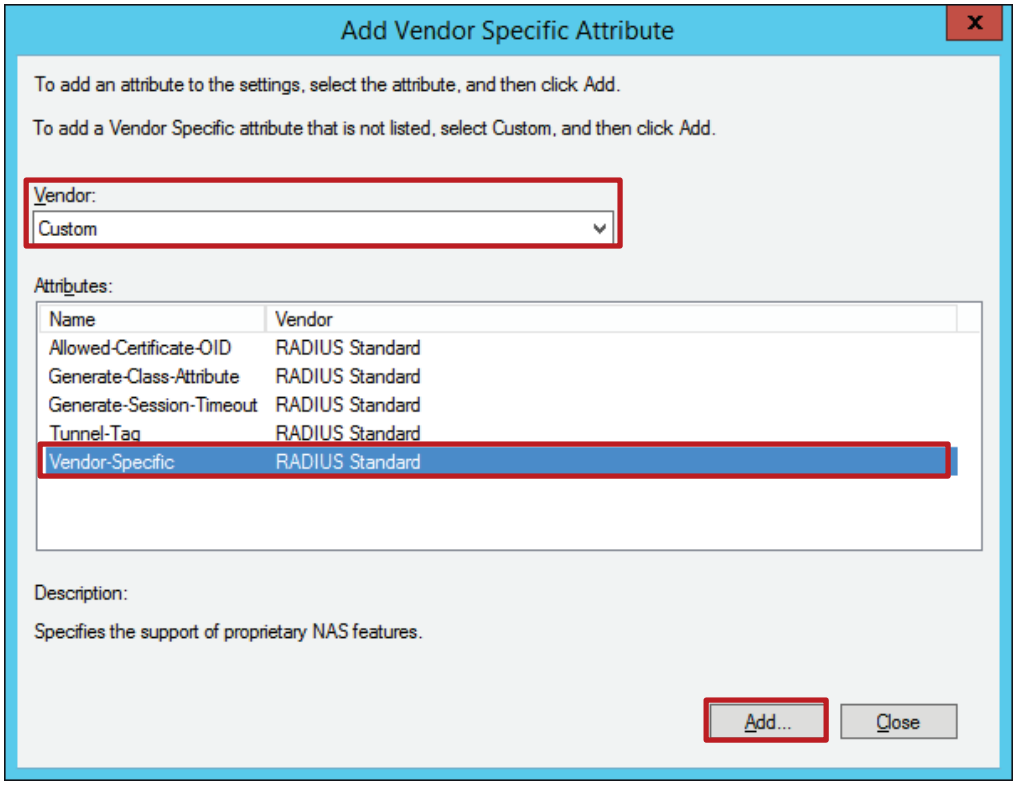


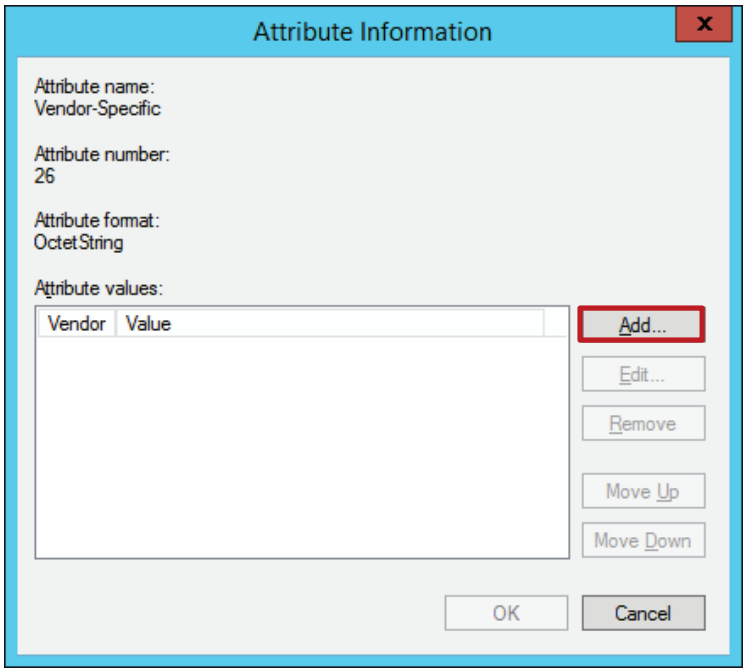


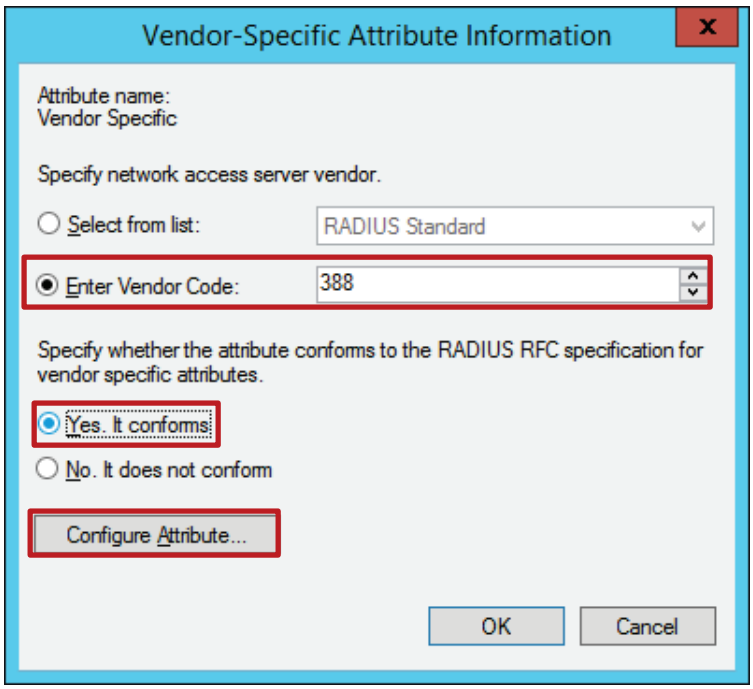


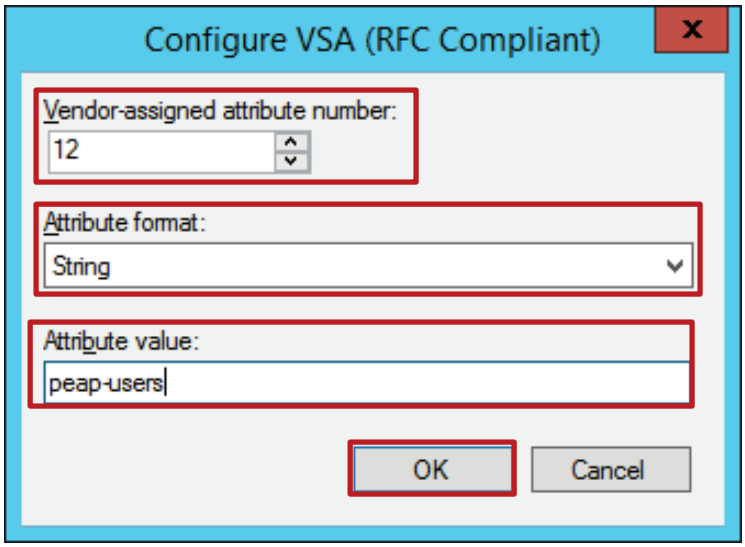


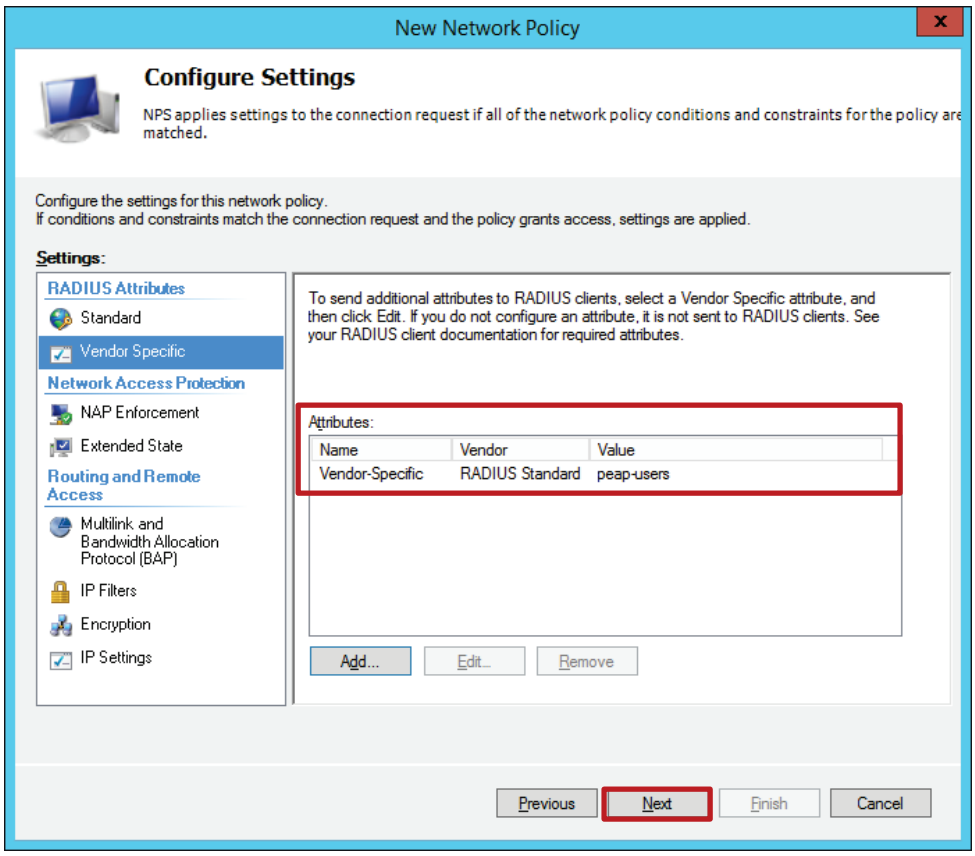
At this stage we need to define a **WiNG-User-Group VSA** that RADIUS server will send back upon successful user authentication. WiNG Vendor Code is 388, attribute number is 12, format is ASCII.

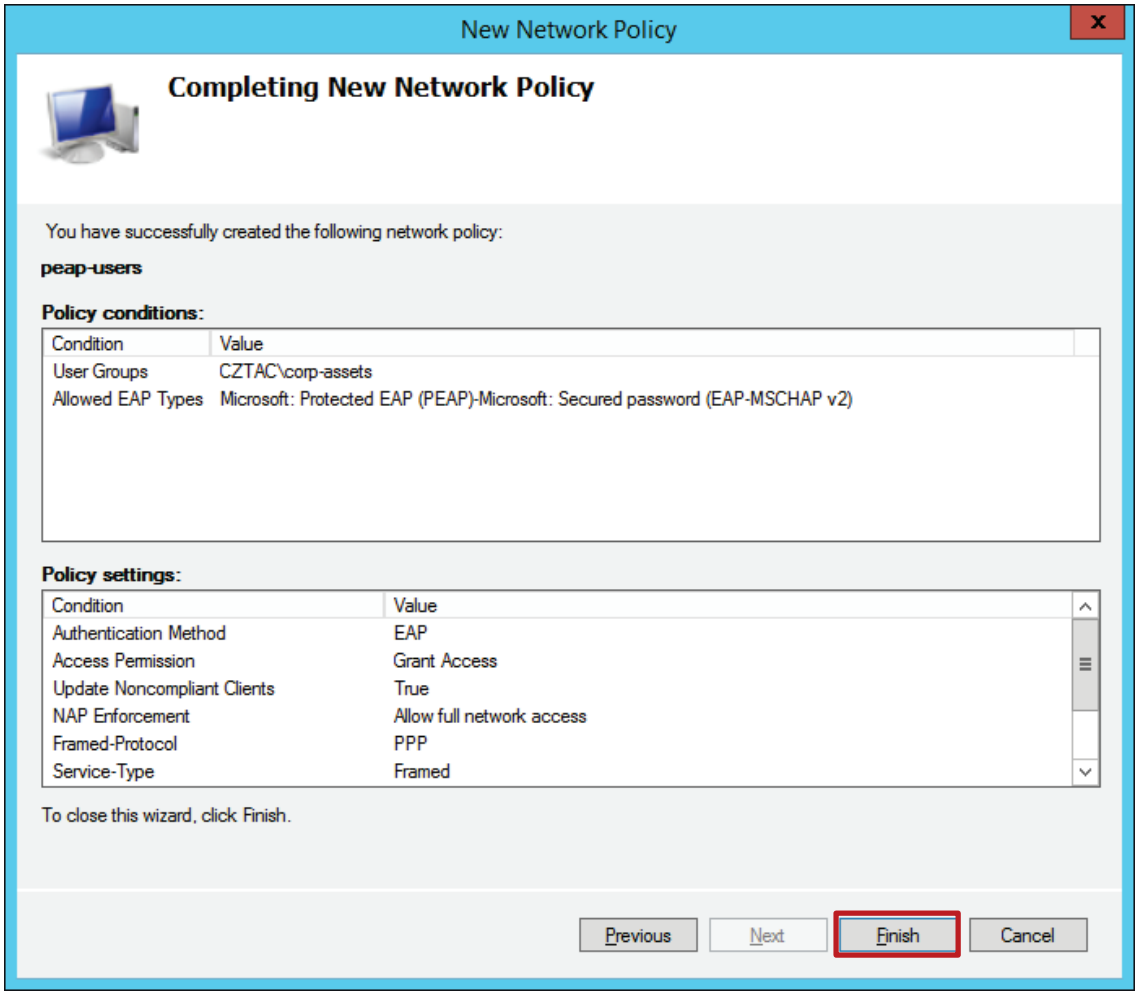




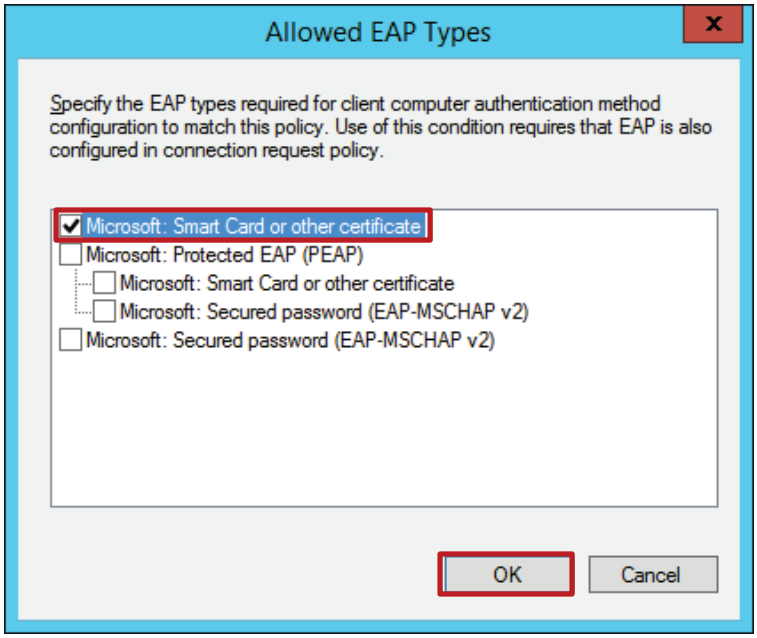


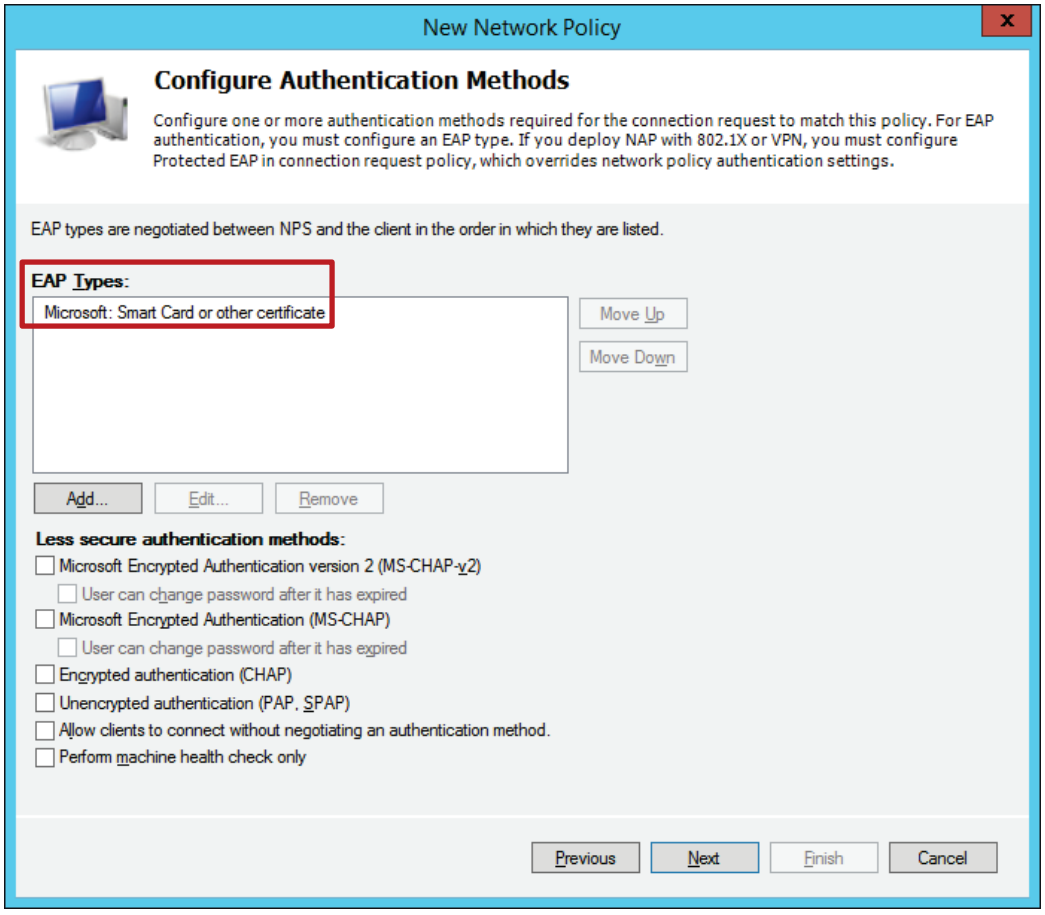


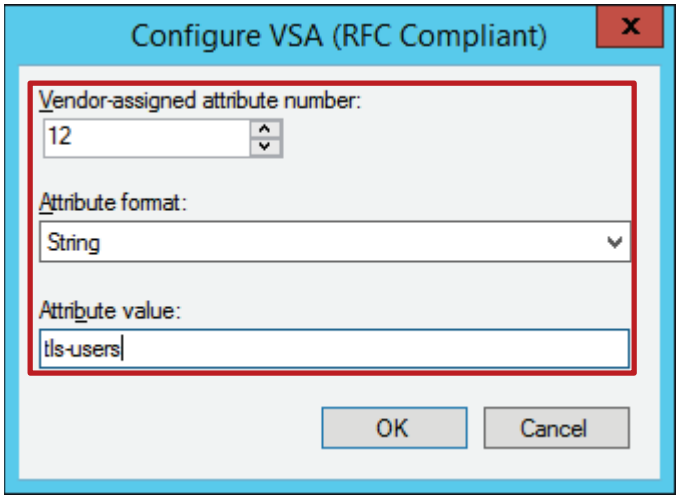


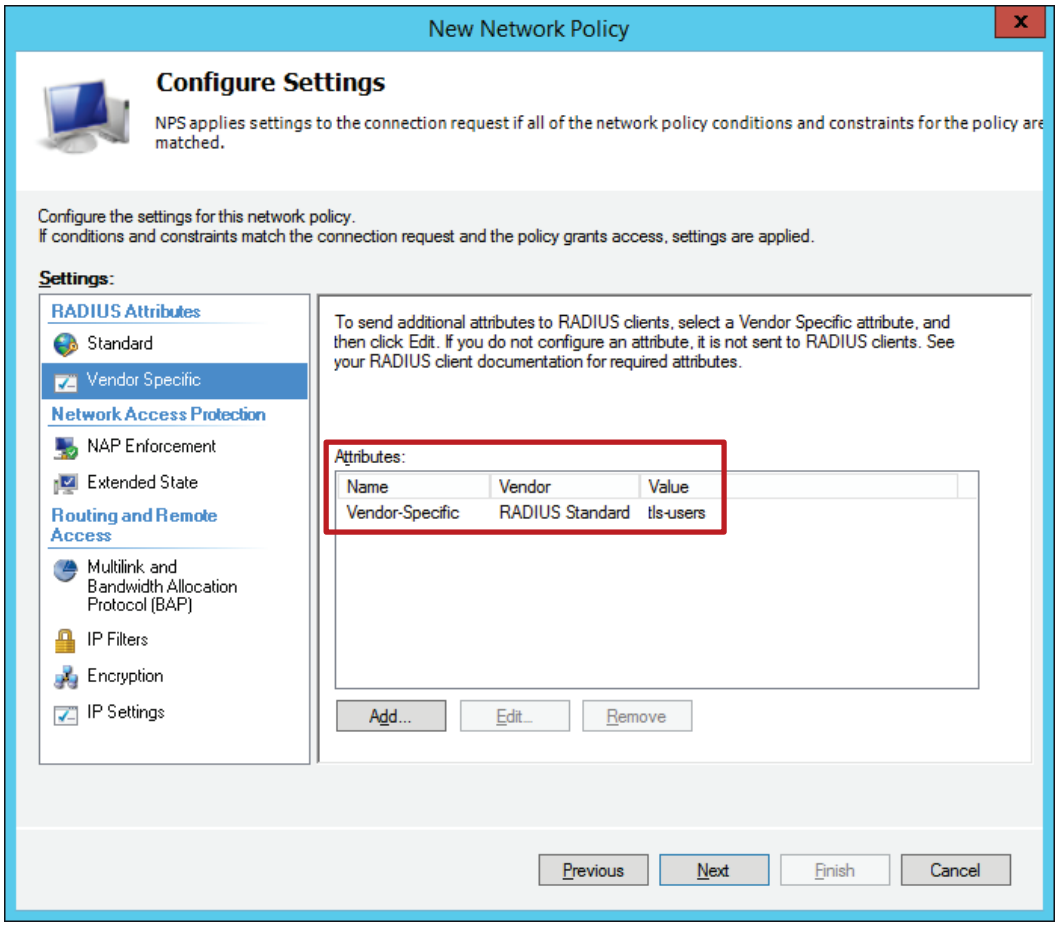


Repeat the process and add another Network Connection Policy for the EAP-TLS authenticated devices. Below are the configuration parts that should be different.



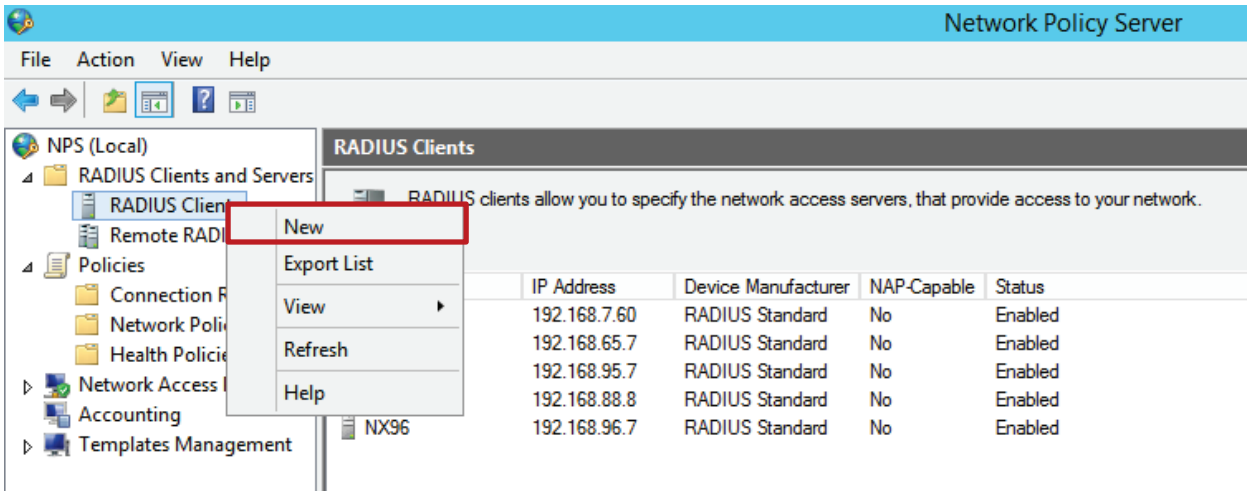


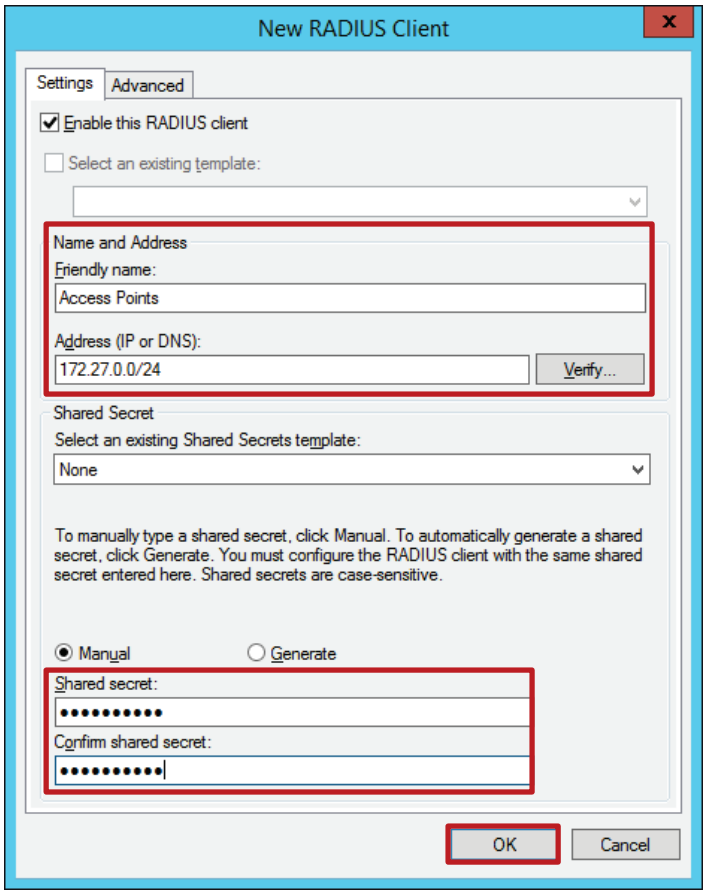




Last configuration part on the NPS side is to add a RADIUS client to allow Access Points to talk to RADIUS server. If Access Points are making requests directly to the RADIUS it is easier to add them using a subnet as a source IP address.

8. NPS Add RADIUS Clients

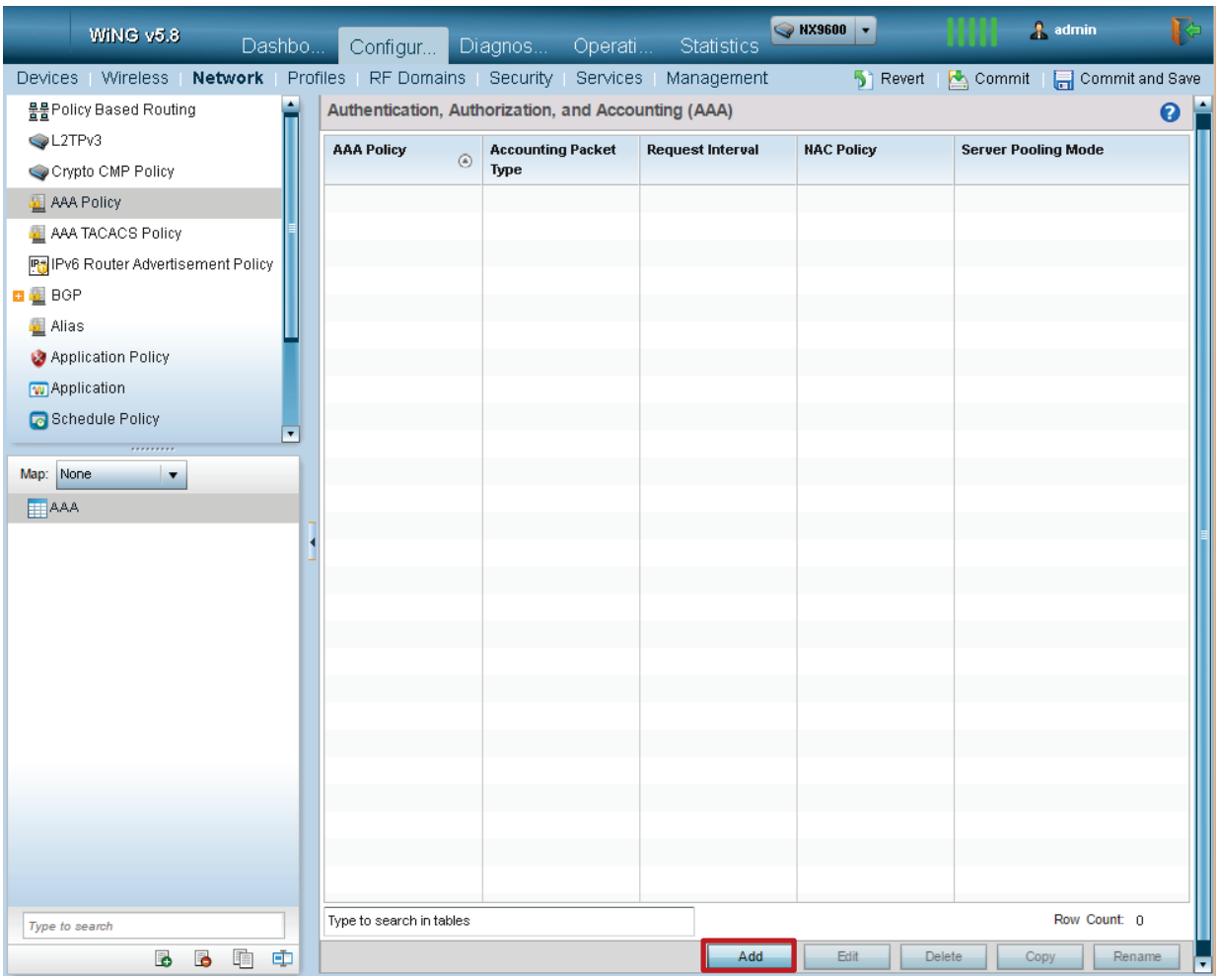


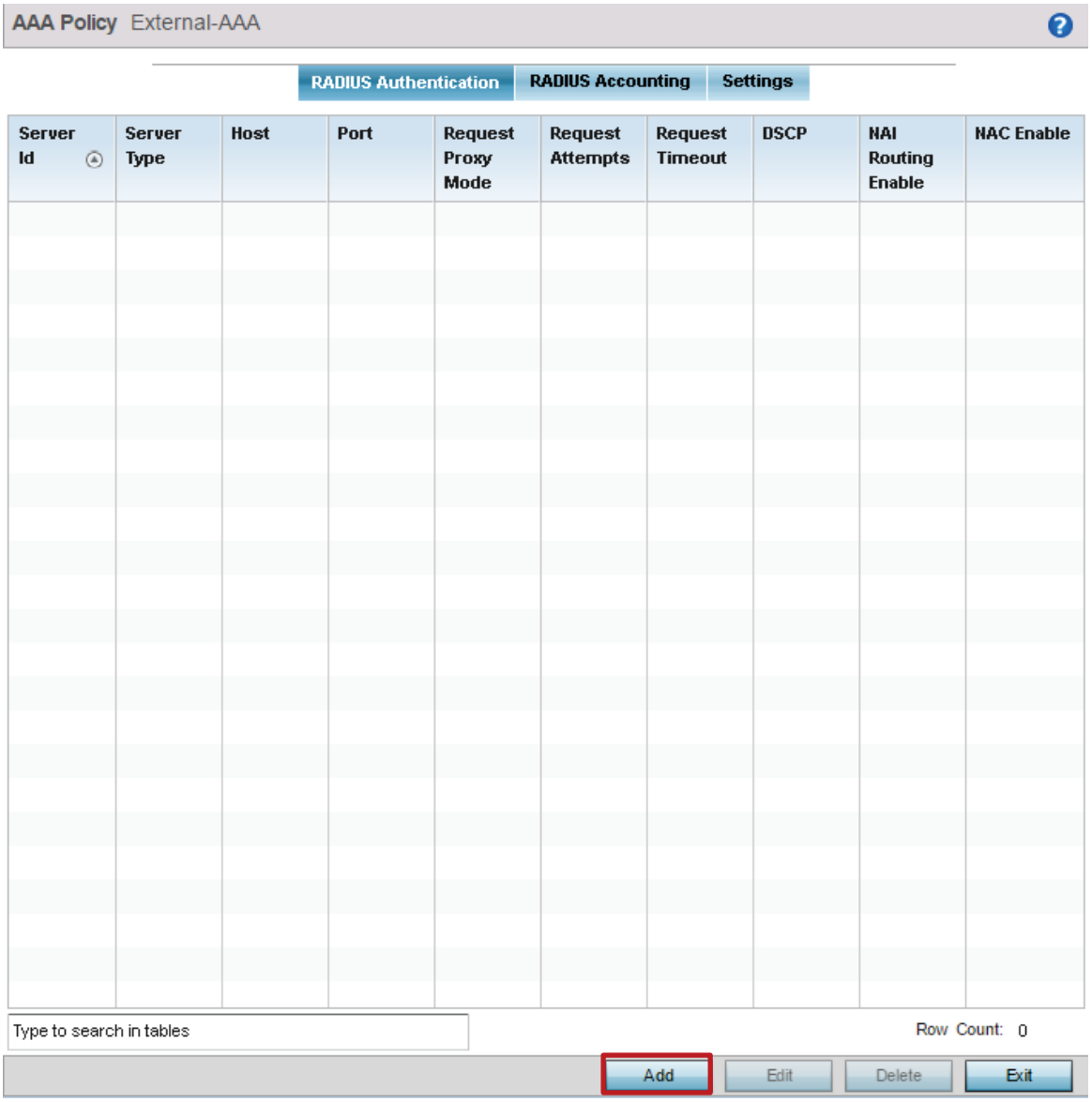


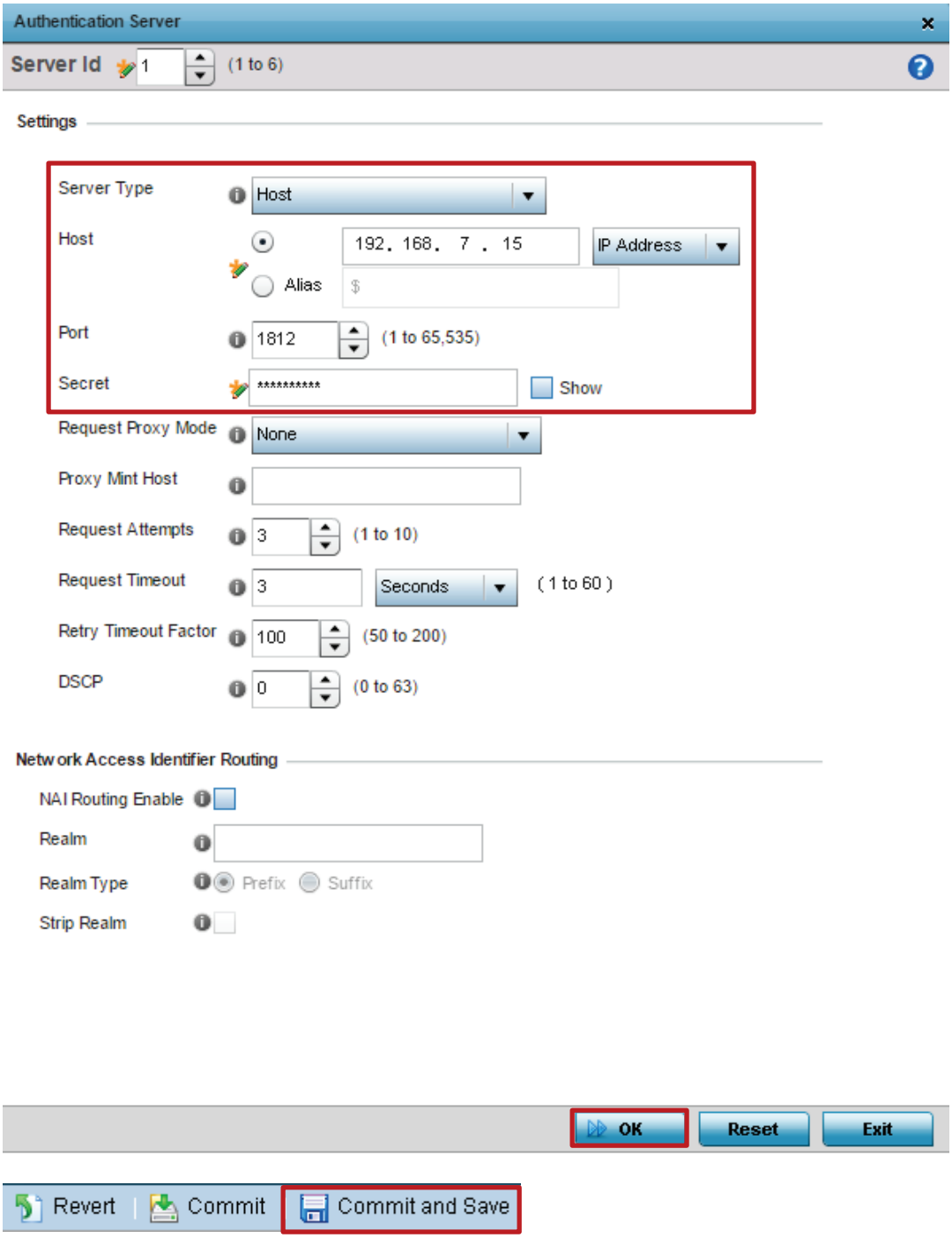
AAA Policy Configuration

We need to create new AAA Policy that will point Access Points to authenticate against our RADIUS server. Navigate to Configuration > Network > AAA Policy and click on Add.

Web UI







CLI

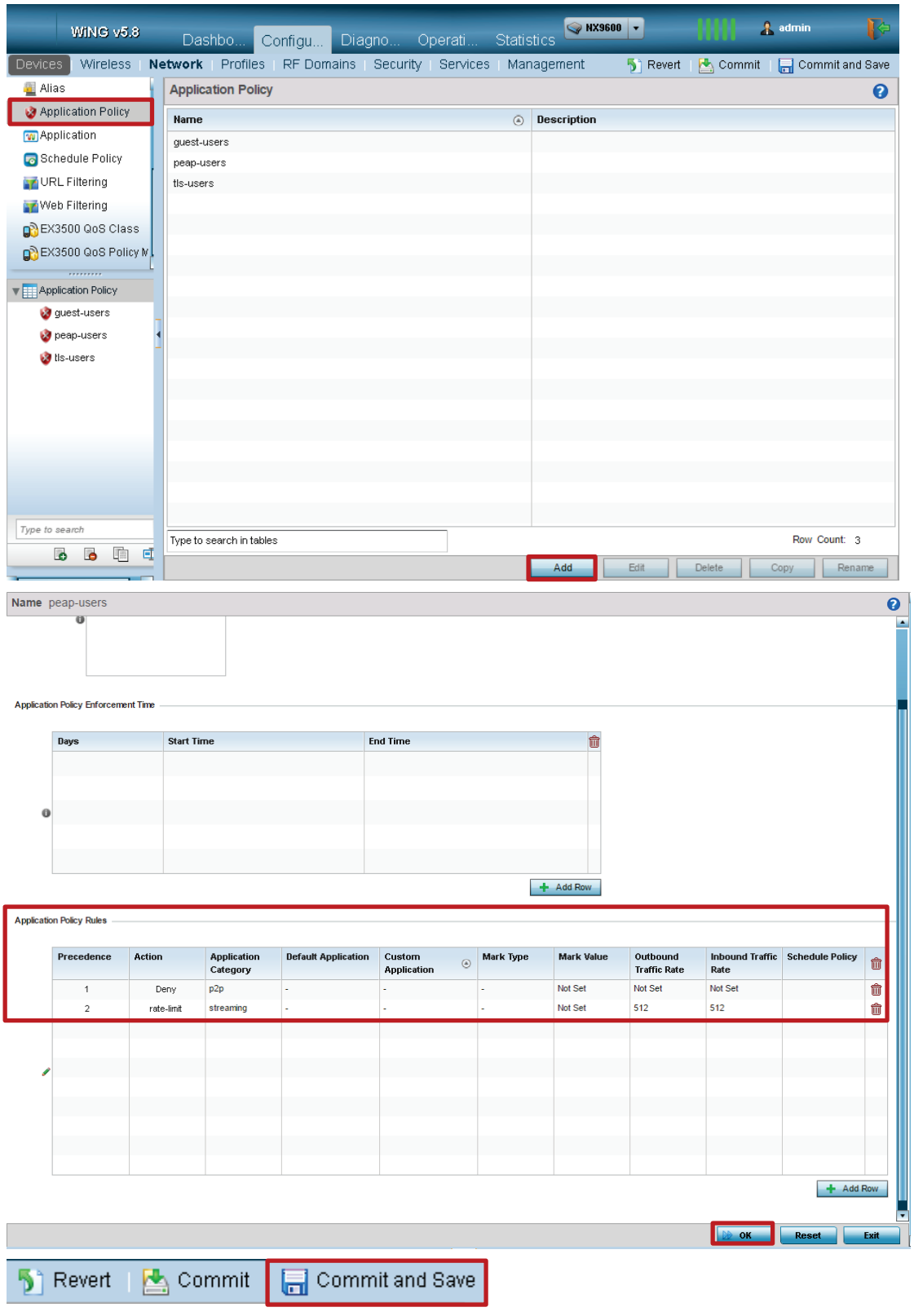
```
!
aaa-policy External-AAA
 authentication server 1 host 192.168.7.15 secret 0 wingsecure
!
```

Application Policy Configuration

In this step we create 2 new Application Policies for devices authenticating using PEAP-MSCHAPv2 and devices authenticating EAP-TLS.

Navigate to **Configuration** > **Network** > **Application Policy** > **Add**:

Web UI



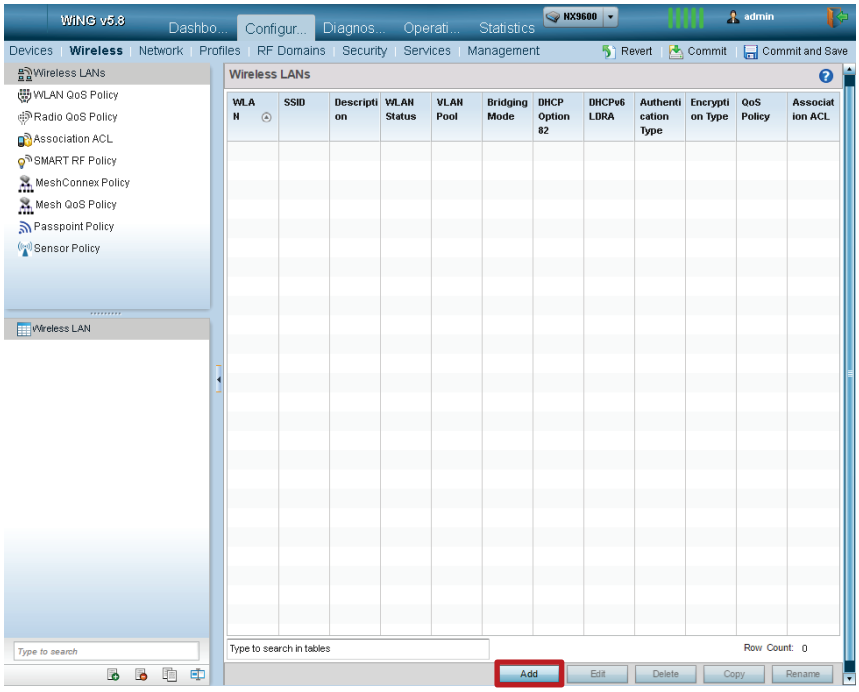
CLI

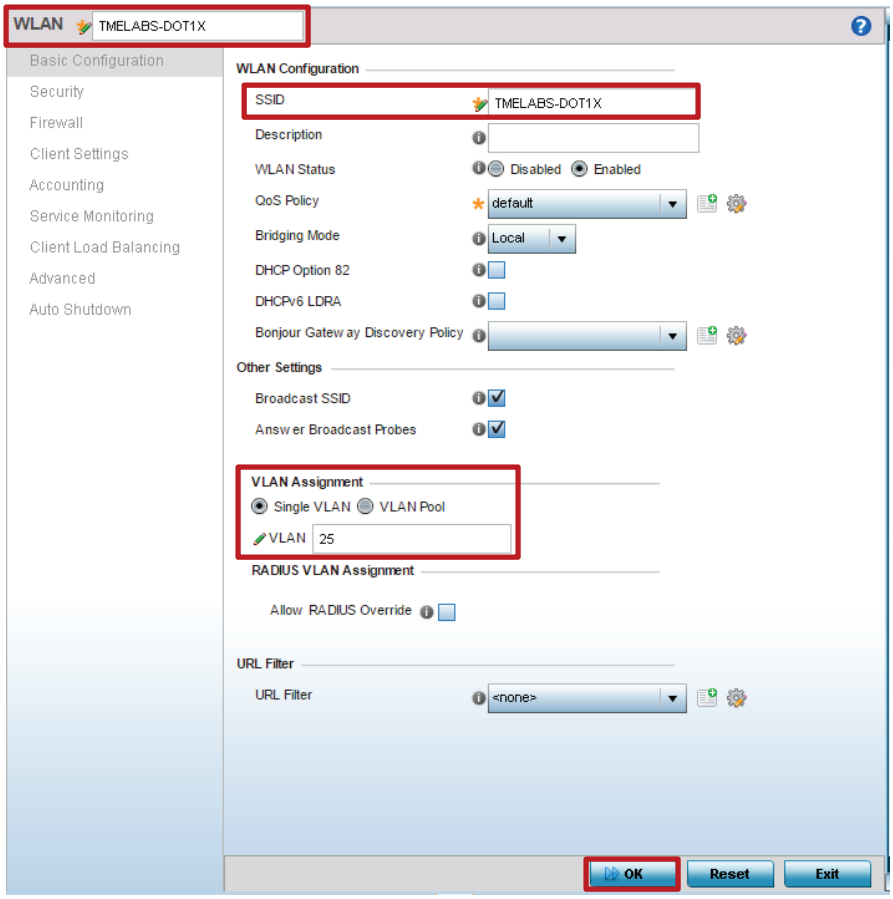
```
!
application-policy peap-users
 deny app-category p2p precedence 1
 rate-limit app-category streaming ingress rate 512 max-burst-size 2 egress rate 512 max-burst-size 2
precedence 2
!
application-policy tls-users
 mark application "Skype for Business_generic" dscp 46 precedence 1
!
```

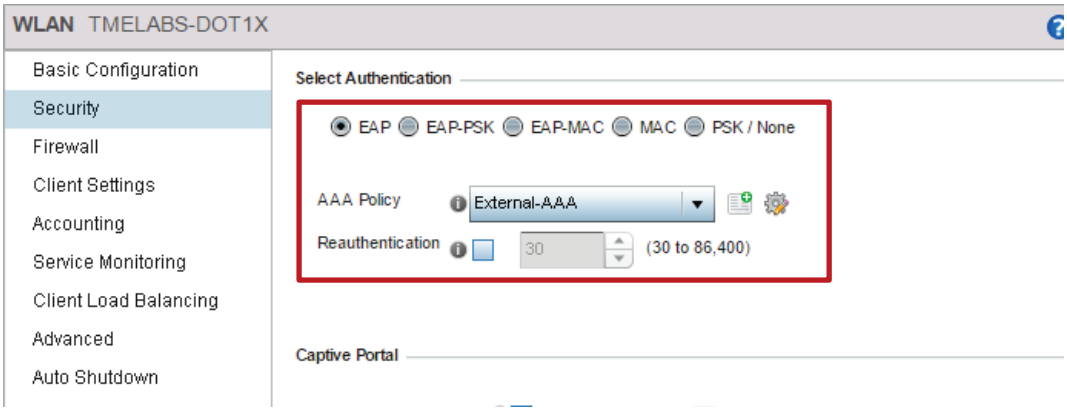
WLAN Configuration

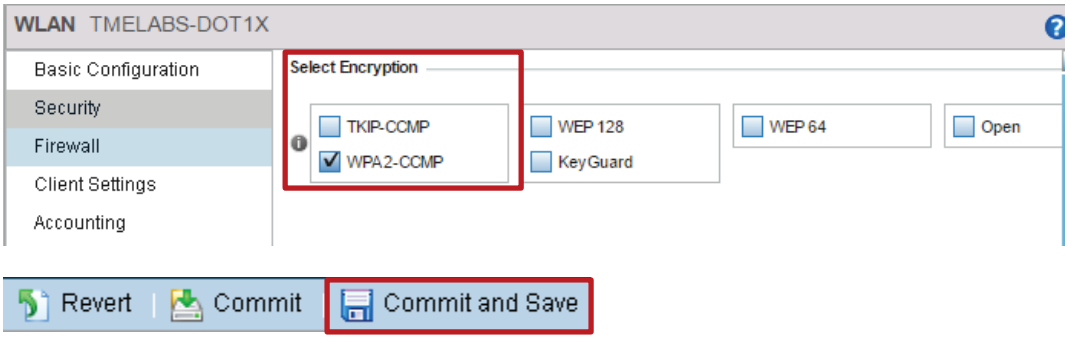
Create a new WLAN and enabled EAP based authentication with CCMP encryption, assign newly created AAA policy. Navigate to Configuration > Wireless > Wireless LANs, click on Add.

Web UI









CLI

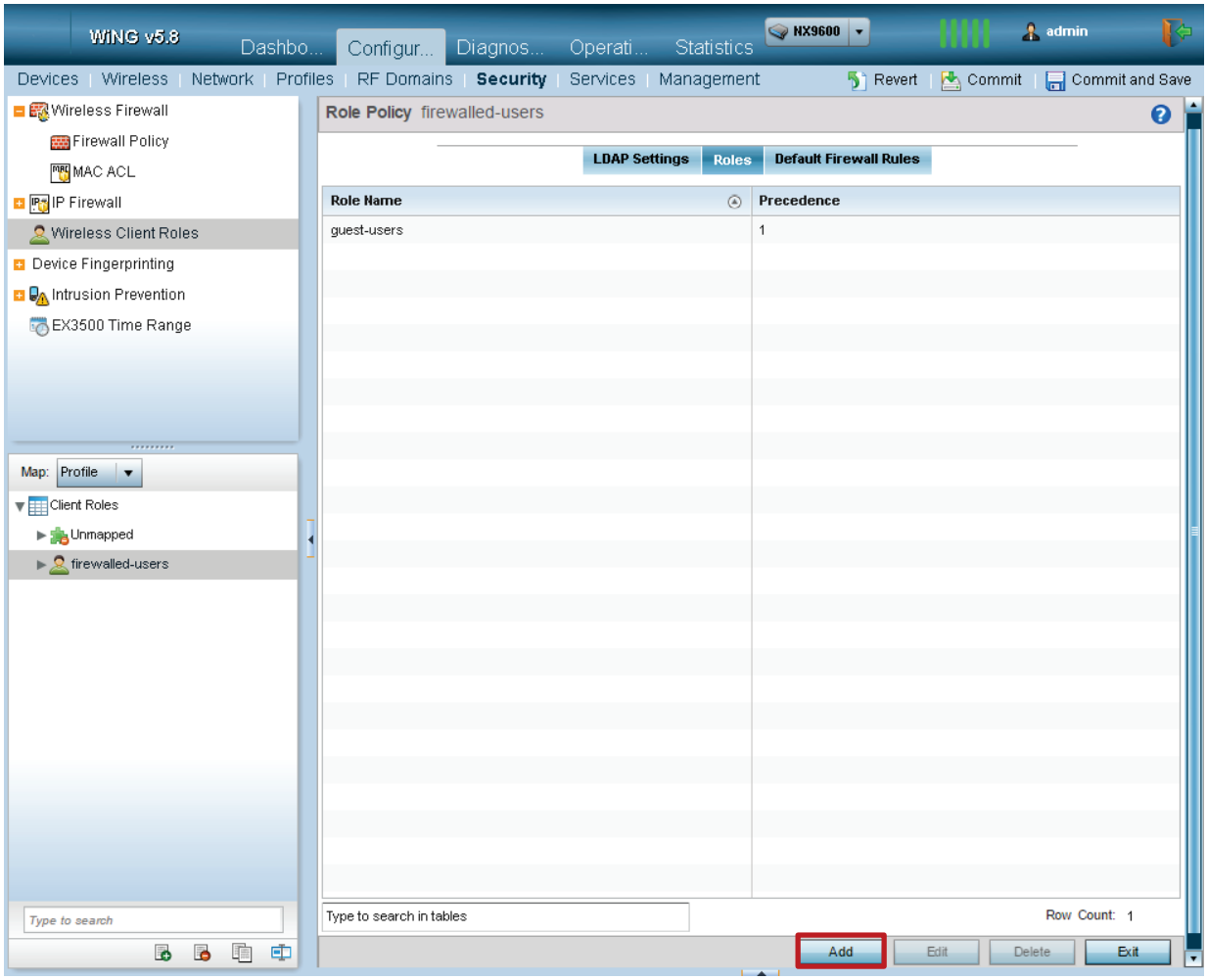
```
!
wlan TMELABS-DOT1X
 ssid TMELABS-DOT1X
 vlan 25
 bridging-mode local
 encryption-type ccmp
 authentication-type eap
 use aaa-policy External-AAA
 use ip-access-list out BROADCAST-MULTICAST-CONTROL
 use mac-access-list out PERMIT-ARP-AND-IPv4
!
```

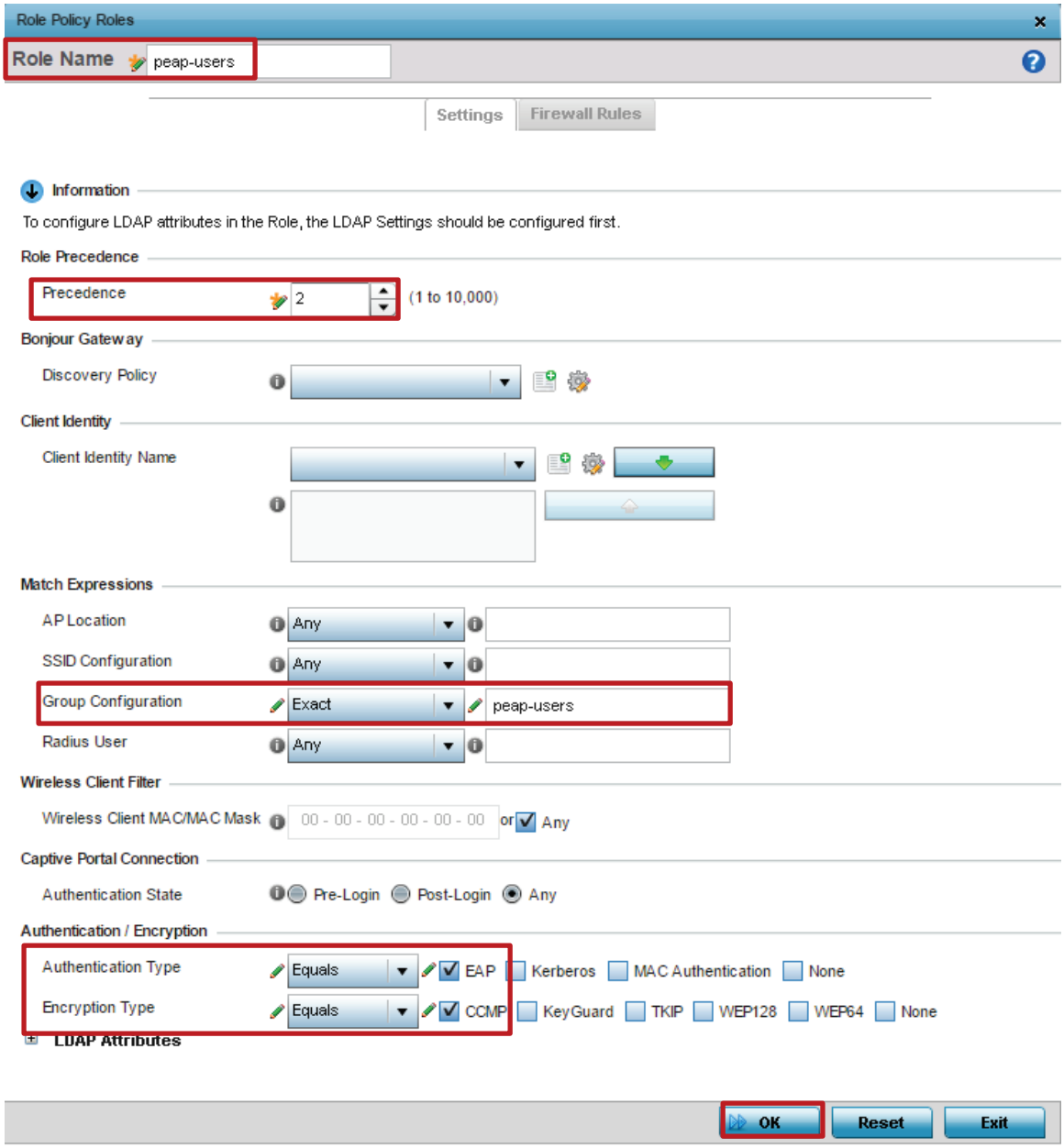
Role Policy Configuration

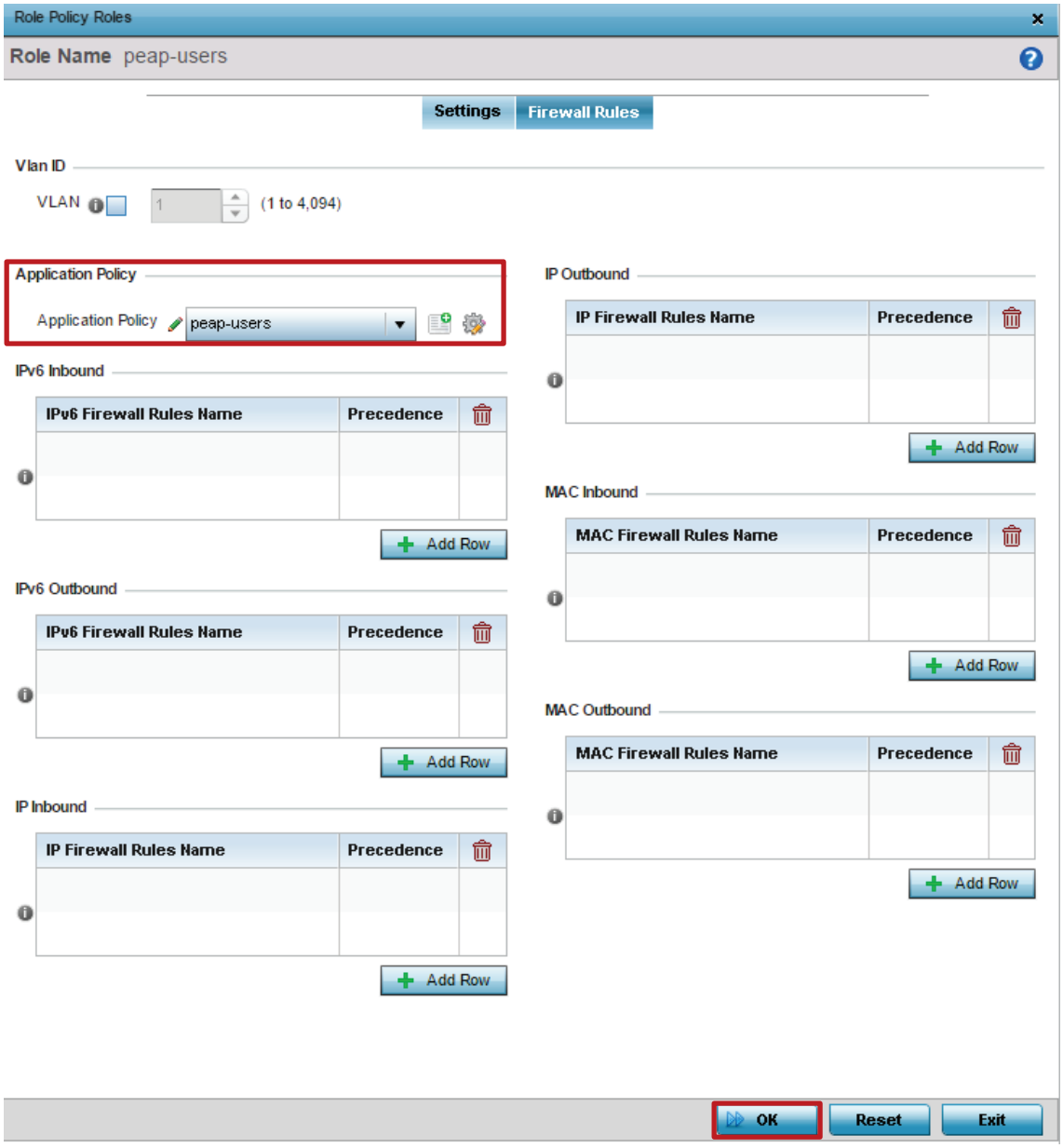
Finally, we need to modify our role policy that was created in the first scenario to add the new role with new match criteria based on the returned user group attribute. In this way, users who associate to the WLAN using PEAP-MSCHAPv2 will get different policies compared to devices authenticated using EAP-TLS method. This can be useful when corporate laptop devices are being staged with client certificates, while mobile devices still use PEAP for simplicity.

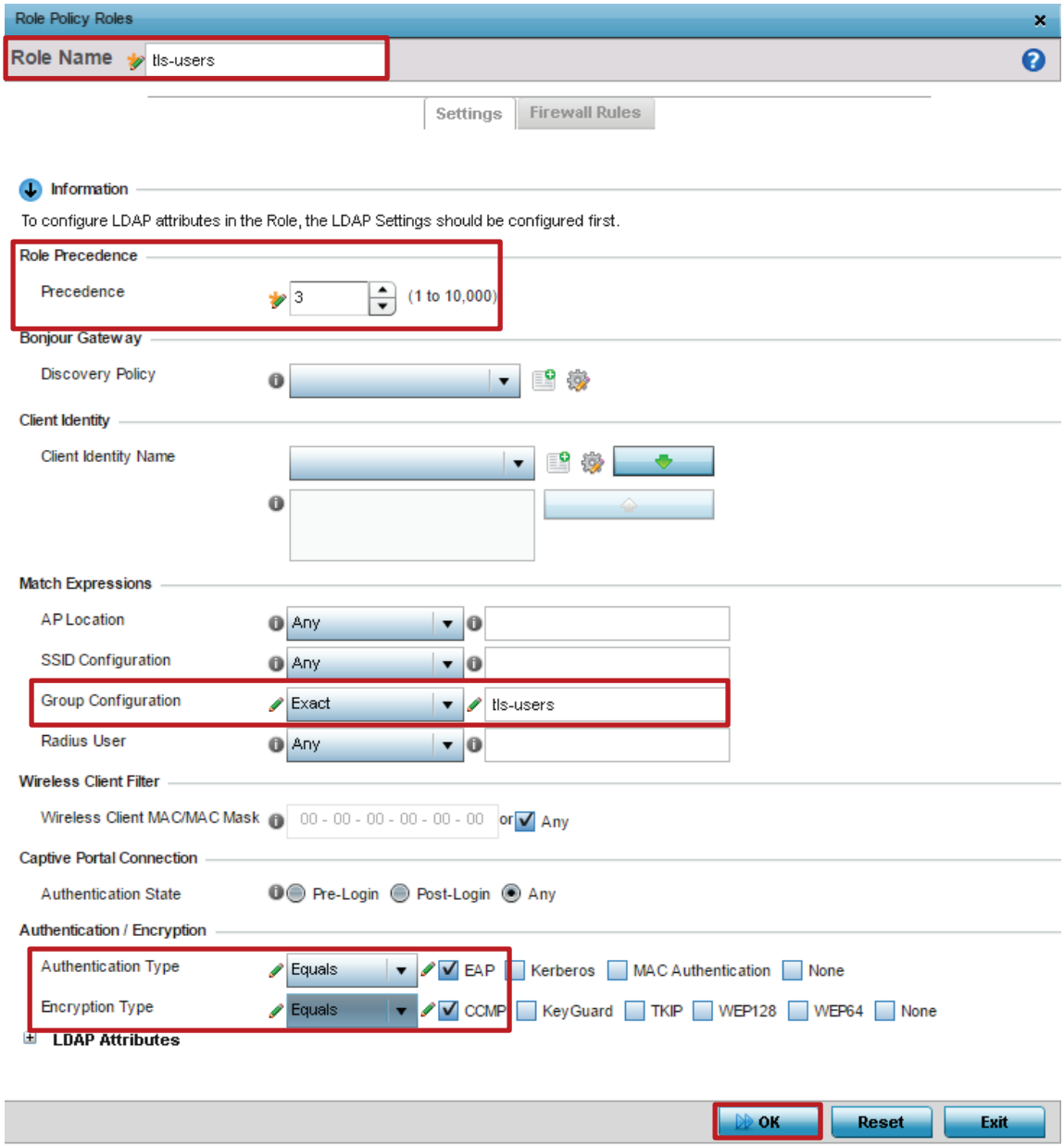
Navigate to **Configuration > Security > Wireless Client Roles >** select **"firewalled-users" > Roles > Add**

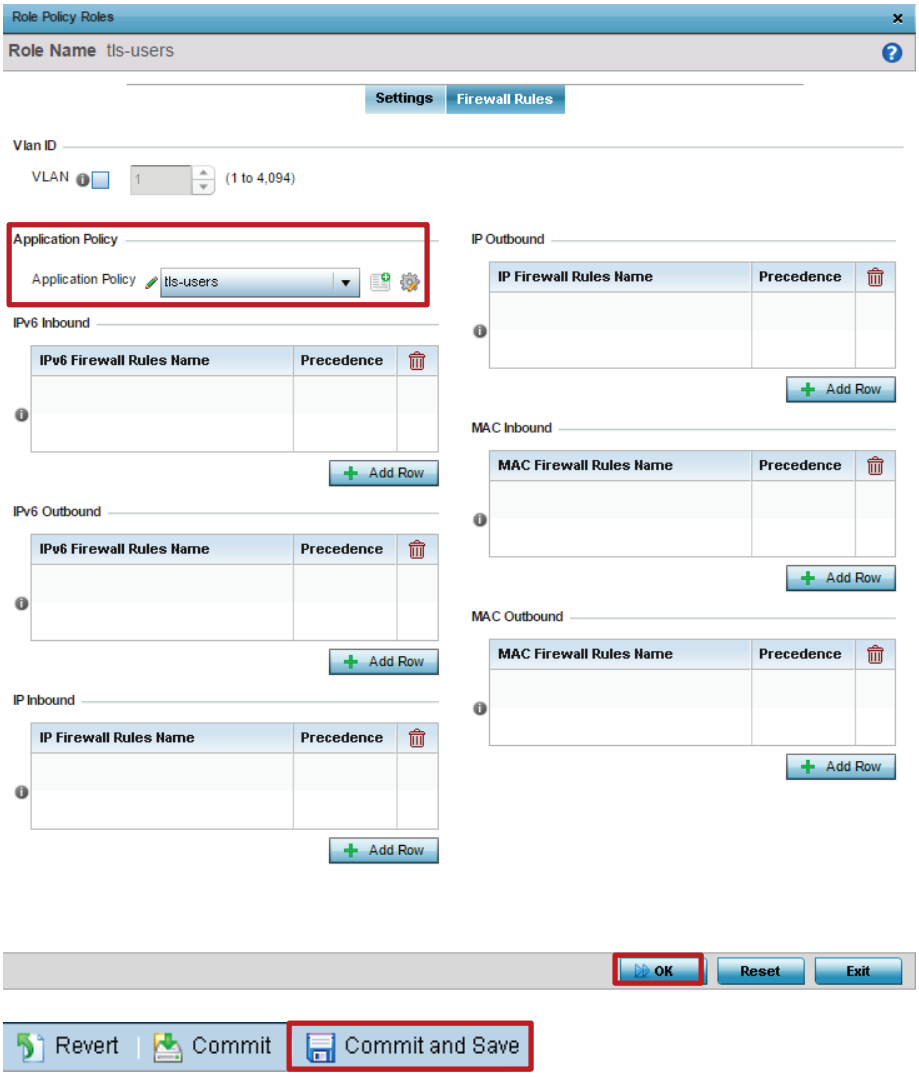
Web UI











CLI

```
!
role-policy firewalled-users
 user-role guest-users precedence 1
  ssid exact Z-Guest
  use ip-access-list in guest-users precedence 1
  use application-policy guest-users
 user-role peap-users precedence 2
  authentication-type eq eap
  encryption-type eq ccmp
  group exact peap-users
  use application-policy peap-users
 user-role tls-users precedence 3
  authentication-type eq eap
  encryption-type eq ccmp
  group exact tls-users
  use application-policy tls-users
!
```

Scenario 3 – Match based on Client Identity (DHCP Fingerprinting)

Scenario 3 will utilize a new approach in assigning roles, which involves client device/OS identification by using DHCP fingerprinting functionality. This is useful when it is required to differentiate between client devices using the same ESSID, same security type, same user identity, but different type of devices, like corporate IT managed Windows laptops and iOS or Android devices that employees are using on the same network, perhaps by enrolling them via company's MDM solution.

By leveraging built-in DHCP fingerprinting functionality it is possible to differentiate between different OS types and their versions. For instance an administrator may want to put a more restrictive policy to mobile devices, which are running outdated software, while only allowing laptops to access corporate apps, etc.

There are handful of built-in device signatures that come in WiNG 5 pre-installed by default, but custom ones can be defined as well based on DHCP options that clients are sending during the DHCP handshake. More details on how to easily track these values can be found in the Troubleshooting chapter of this guide.

In our example we will derive two additional roles out of existing "tls-users" role. All the mobile devices running latest iOS, Android or Windows Phone OS will get better service levels compared to devices running outdated software, while Windows-7 based laptops and only those which follow specific naming format will get access to internal corporate network.

The following sections will just show the configuration of the additional components (in order of configuration), which are:

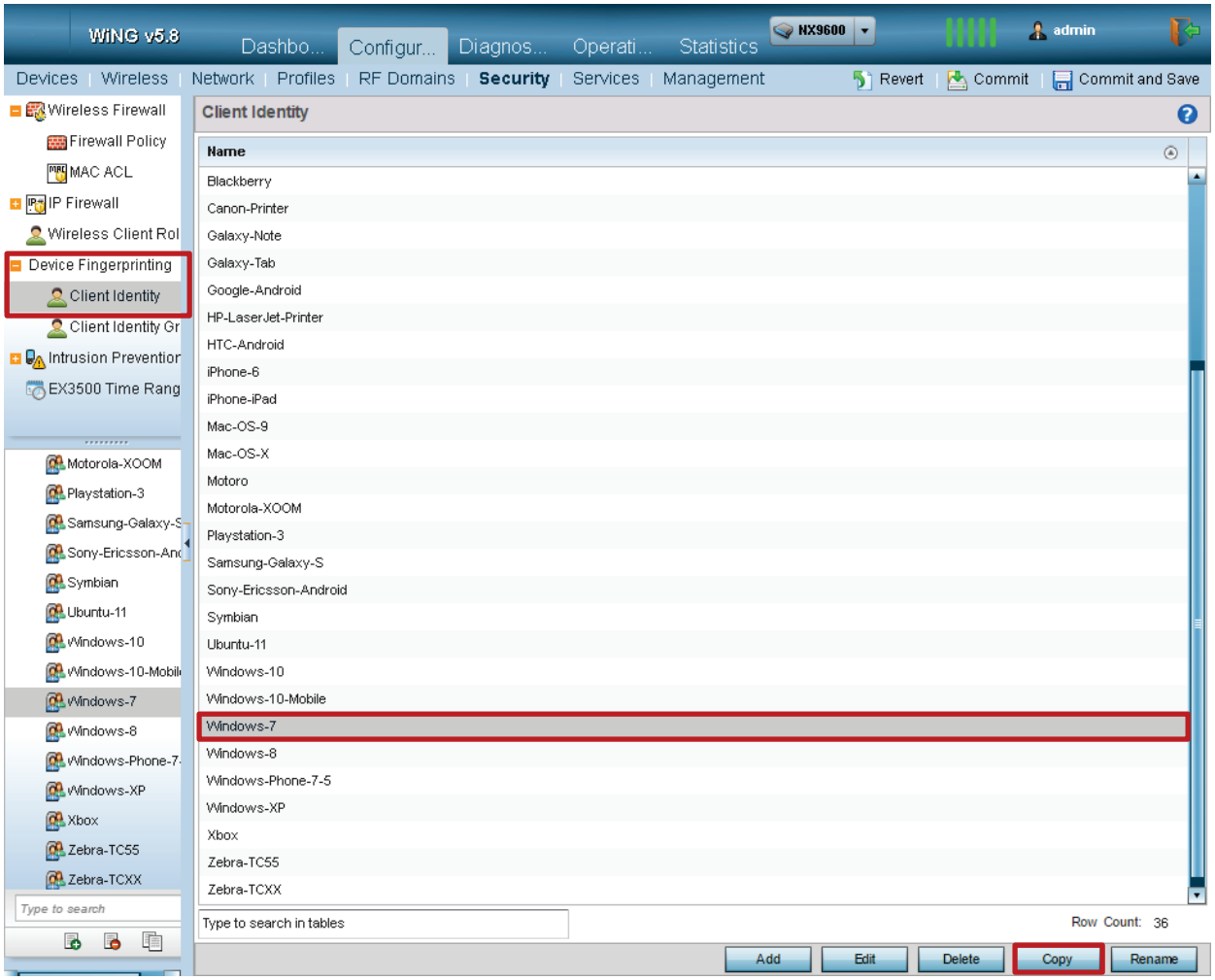
1. Client Identity Configuration to identify corporate IT managed laptops
2. IP Access Lists Configuration
3. Application Policy Configuration
4. WLAN Configuration
5. Role Policy Configuration

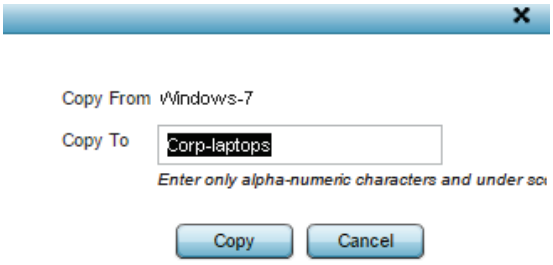
Client Identity Configuration

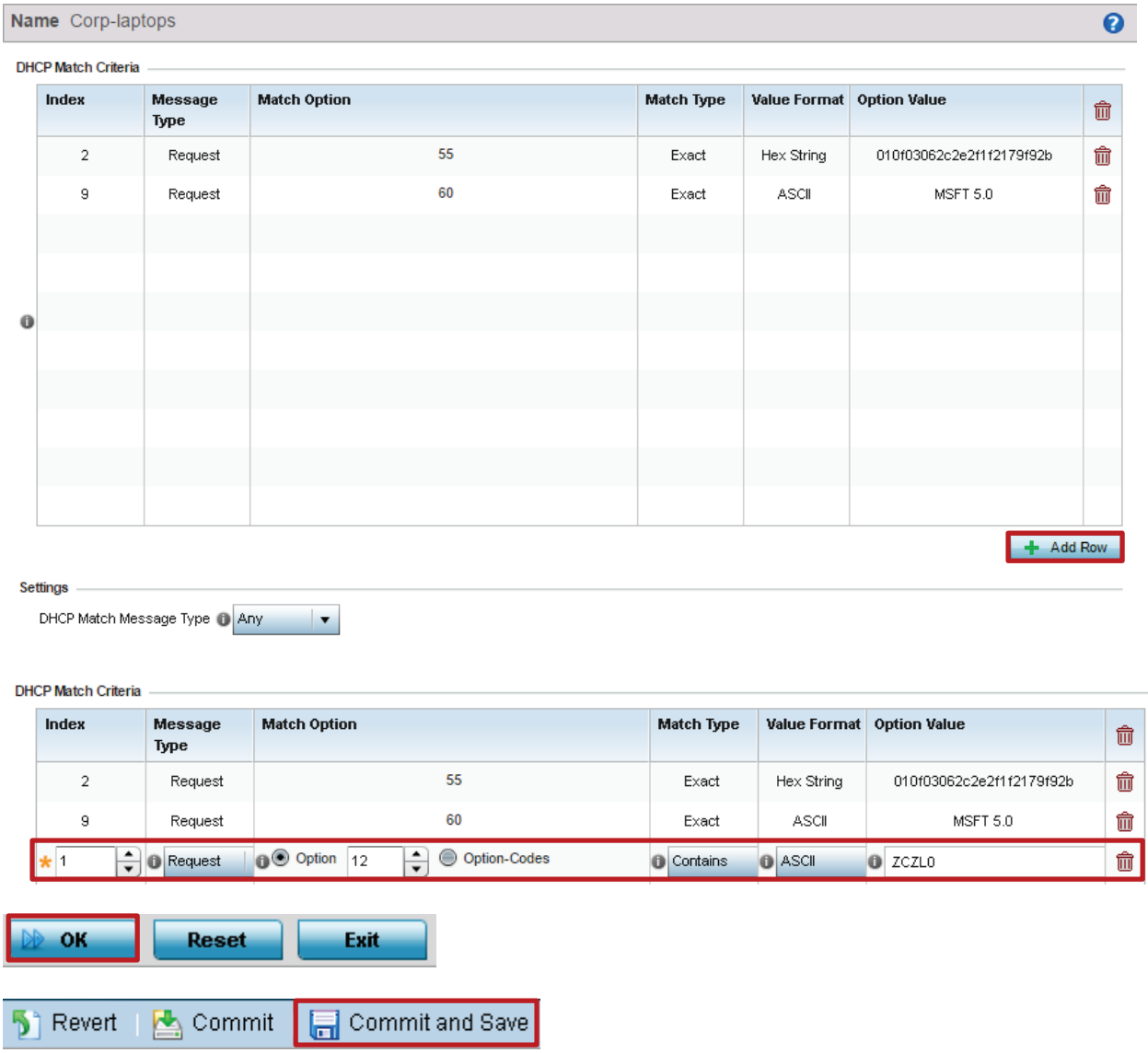
In this section we will define a customized client identity based on Windows-7 identity to include a customized DHCP option 12 syntax that stands for the client name. All Windows 7 laptops that will contain 4 letter organization id will be matched against this identity.

Navigate to Configuration > Security > Device Fingerprinting > Client Identity. Find identity named "Windows-7", select it and click "Copy". Name it as "Corp-laptops".

Client Identity Configuration – Web UI

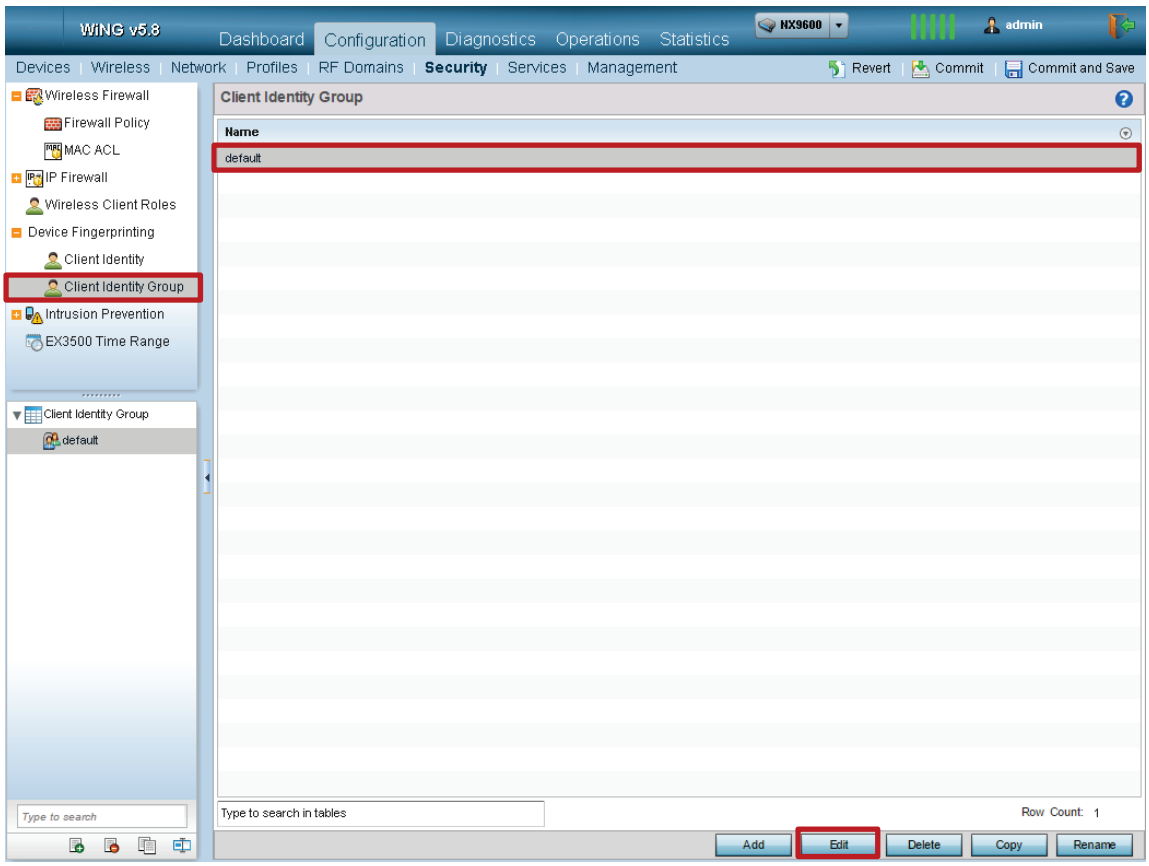


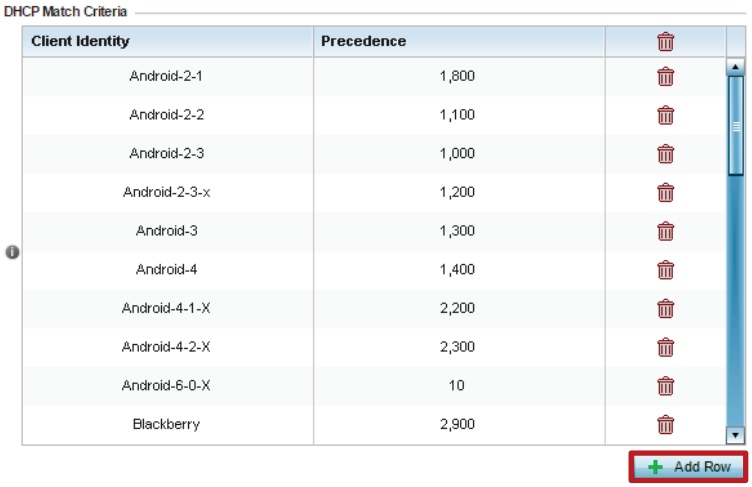




Navigate to **Configuration > Security > Device Fingerprinting > Client Identity Group**. Now we need to add our new Client Identity to the default group to be able to use it for client identification.

Client Identity Group Configuration – Web UI





Client Identity and Identity Group Configuration – CLI

```
!
client-identity Corp-laptops
 dhcp 1 message-type request option 12 contains ascii ZCZ09L
 dhcp 2 message-type request option 55 exact hexstring 010f03062c2e2f1f2179f92b
 dhcp 8 message-type request option 60 exact ascii "MSFT 5.0"
!
client-identity-group default
 client-identity Corp-laptops precedence 5
 client-identity Android-6-0-X precedence 10
 client-identity Windows-10 precedence 20
 client-identity Windows-10-Mobile precedence 30
 client-identity iPhone-6 precedence 40
 client-identity Samsung-Galaxy-S precedence 50
 client-identity Google-Android precedence 100
 client-identity HTC-Android precedence 200
 client-identity Sony-Ericsson-Android precedence 300
 client-identity Galaxy-Note precedence 500
 client-identity Galaxy-Tab precedence 600
 client-identity Motorola-XOOM precedence 700
 client-identity Windows-XP precedence 800
 client-identity Windows-7 precedence 900
 client-identity Android-2-3 precedence 1000
 client-identity Android-2-2 precedence 1100
 client-identity Android-2-3-x precedence 1200
 client-identity Android-3 precedence 1300
 client-identity Android-4 precedence 1400
 client-identity iPhone-iPad precedence 1500
 client-identity Ubuntu-11 precedence 1600
 client-identity Windows-Phone-7-5 precedence 1700
 client-identity Android-2-1 precedence 1800
 client-identity Windows-8 precedence 1900
 client-identity Mac-OS-X precedence 2000
 client-identity Mac-OS-9 precedence 2100
 client-identity Android-4-1-X precedence 2200
 client-identity Android-4-2-X precedence 2300
 client-identity Symbian precedence 2400
 client-identity Playstation-3 precedence 2500
 client-identity Xbox precedence 2600
 client-identity HP-LaserJet-Printer precedence 2700
 client-identity Canon-Printer precedence 2800
 client-identity Blackberry precedence 2900
 load default-fingerprints
!
```

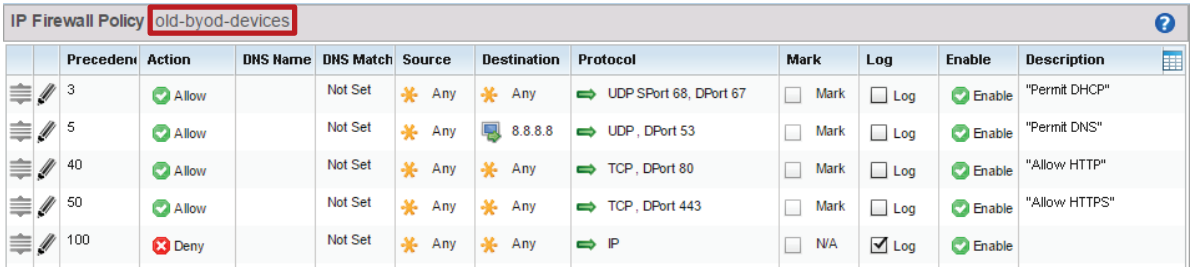
IP Access List and Application Policy Configuration

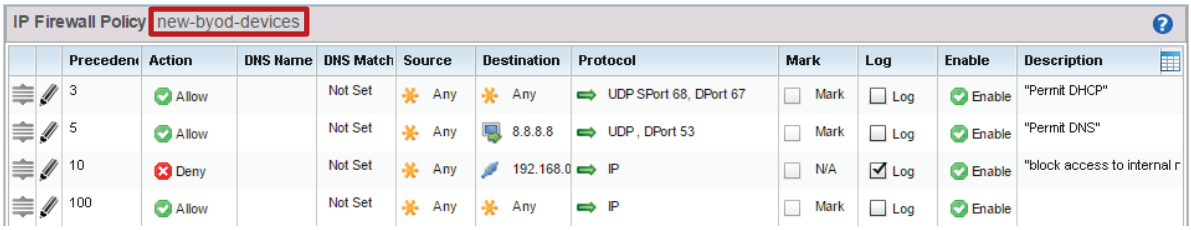
In the below example we have created two ACLs named “old-mobile-units” and “new-mobile-units”. For old mobile devices we will have a restricted ACL that will only allow outgoing web traffic, we are dropping any other IP traffic and logging hits. ACL for the new mobile devices will be more relaxed, only limiting these devices to access internal corporate network, while all the outgoing traffic to the internet is allowed.

Furthermore, we are going to create three application policies for each role. Application policy for legacy mobile devices will take care of dropping peer to peer application traffic, VPN and video streaming services, while app policy for new devices will only set up rate limiters on application markets to prevent these devices to consume all the bandwidth in the event of automatic update push, for example when Apple would release a new iOS version. Note that Application Policy requires an Access Point to support DPI engine.

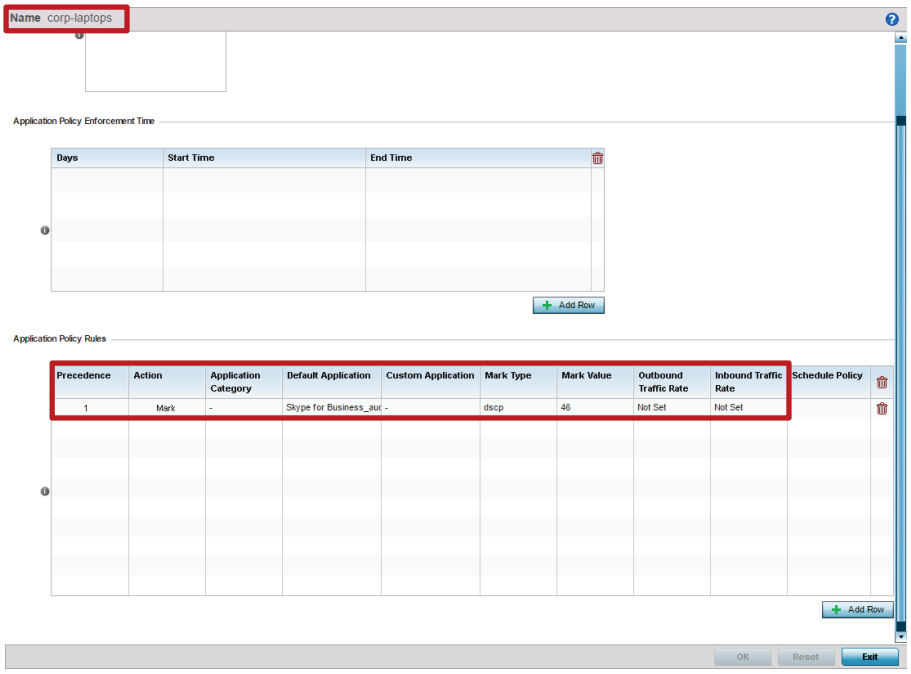
Navigate to Configuration > Security > IP Firewall > IPv4 ACL > Add.

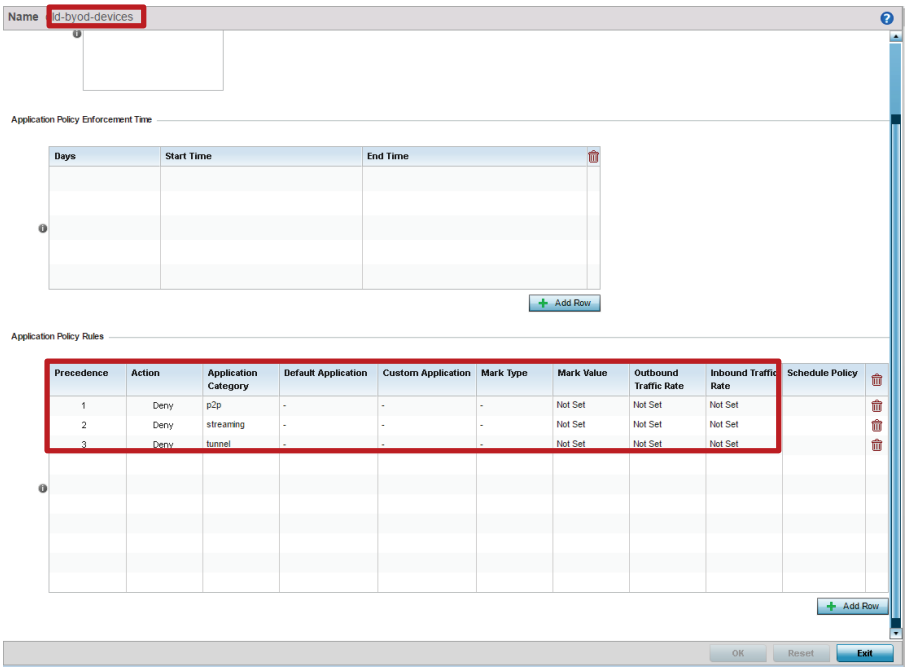
IP Access List Configuration – Web UI

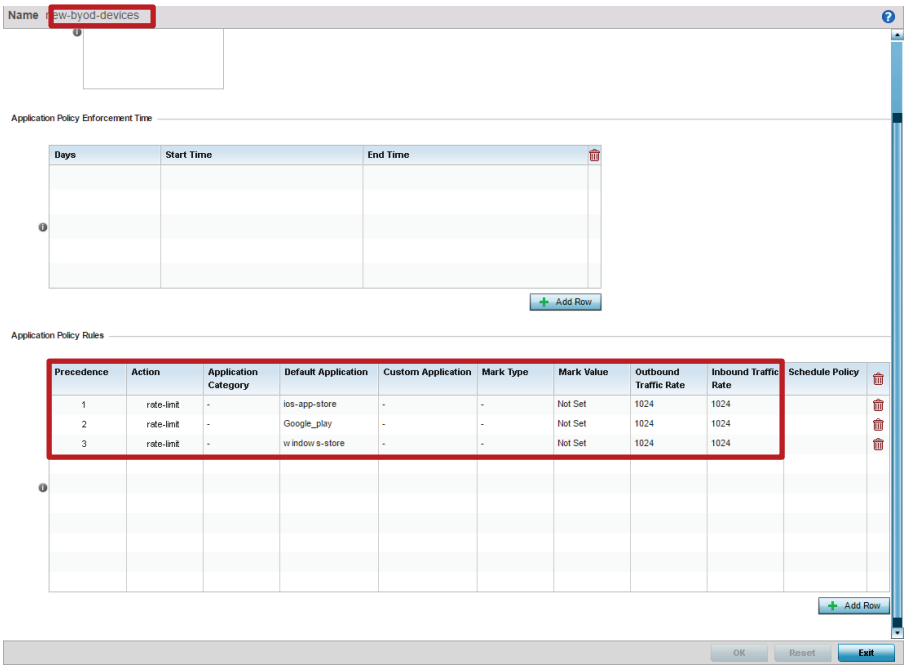




Application Policy Configuration – Web UI







IP Access List Configuration - CLI

```
!

ip access-list old-mobile-units
 permit udp any eq 68 any eq dhcps rule-precedence 3 rule-description "permit DHCP"
 permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description “permit DNS traffic”

 permit tcp any any eq 80 rule-precedence 40 rule-description “HTTP Allow”
 permit tcp any any eq 443 rule-precedence 50 rule-description “HTTPS Allow”
 deny ip any any log rule-precedence 100
!
ip access-list new-mobile-units
 permit udp any eq 68 any eq dhcps rule-precedence 3 rule-description "permit DHCP"
 permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description “permit DNS traffic”
 deny ip any 192.168.0.0/16 log rule-precedence 10 rule-description “block access to internal network and
log hits”
 permit ip any any rule-precedence 50 rule-description “Allow all outgoing traffic”
!
```

Application Policy Configuration - CLI

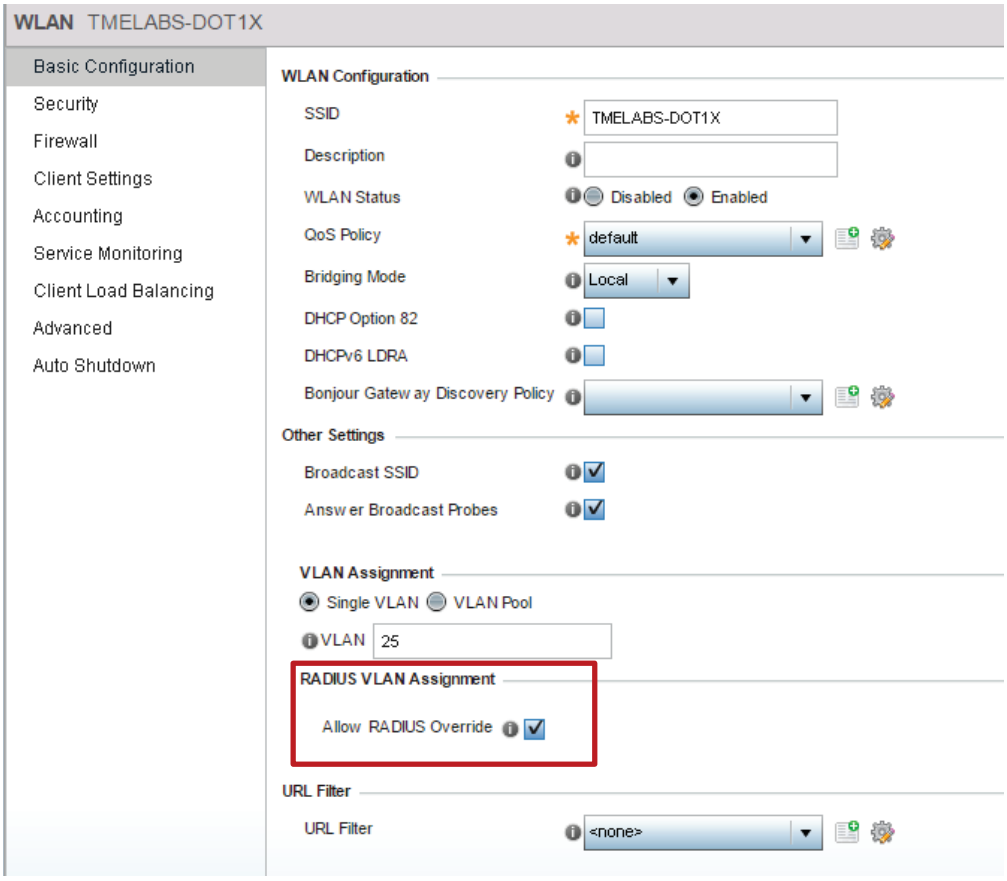
```
!
application-policy old-byod-devices

 deny app-category streaming precedence 1
 deny app-category p2p precedence 2
 deny app-category tunnel precedence 3
!
application-policy new-byod-devices

 rate-limit application ios-app-store ingress rate 1024 max-burst-size 16 egress rate 1024 max-burst-size
16 precedence 4
 rate-limit application windows-store ingress rate 1024 max-burst-size 16 egress rate 1024 max-burst-size
16 precedence 5
 rate-limit application Google_play ingress rate 1024 max-burst-size 16 egress rate 1024 max-burst-size 16
precedence 6
!
application-policy corp-laptops
 mark application "Skype for Business_generic" dscp 46 precedence 1
!
```

WLAN Configuration

WLAN Configuration needs to be edited to allow dynamic VLAN assignments using our Role Based Firewall.

Navigate to **Configuration > Wireless > Wireless LANs >** select "**TMELABS-DOT1X**" > Click "**Edit**".

Web UI



CLI

```
!
wlan TMELABS-DOT1X
 ssid TMELABS-DOT1X
 vlan 25
 bridging-mode local
 encryption-type ccmp
 authentication-type eap
 radius vlan-assignment
 use aaa-policy External-AAA
 use ip-access-list out BROADCAST-MULTICAST-CONTROL
 use mac-access-list out PERMIT-ARP-AND-IPv4
!
```

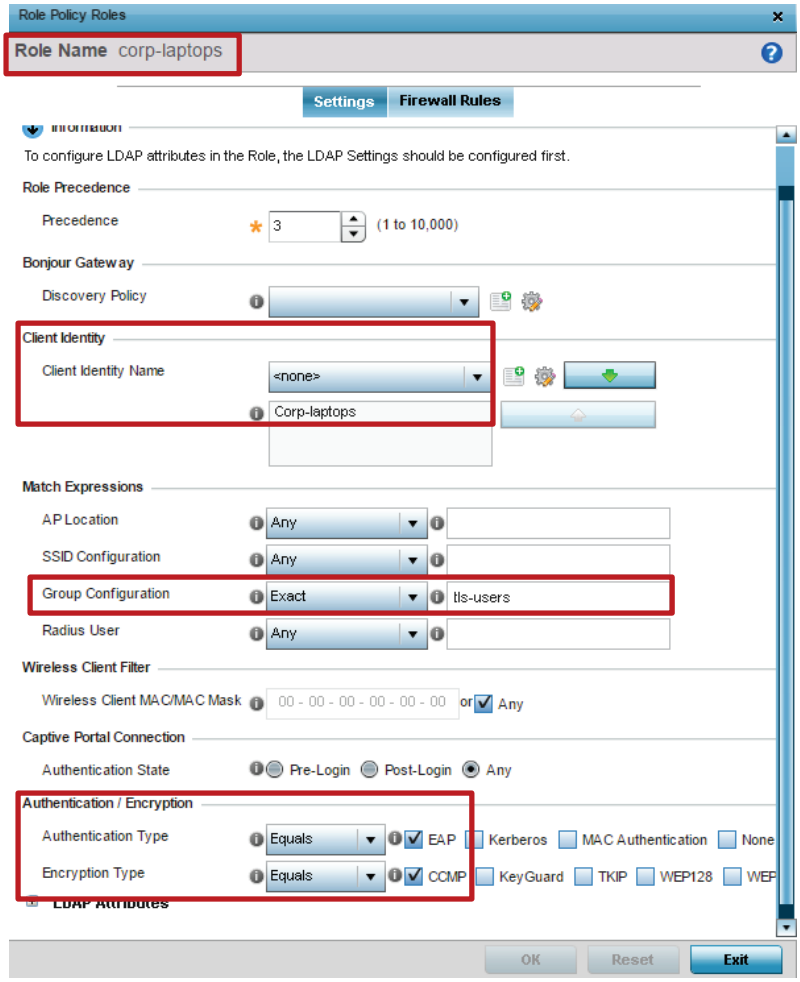
Role Policy Configuration

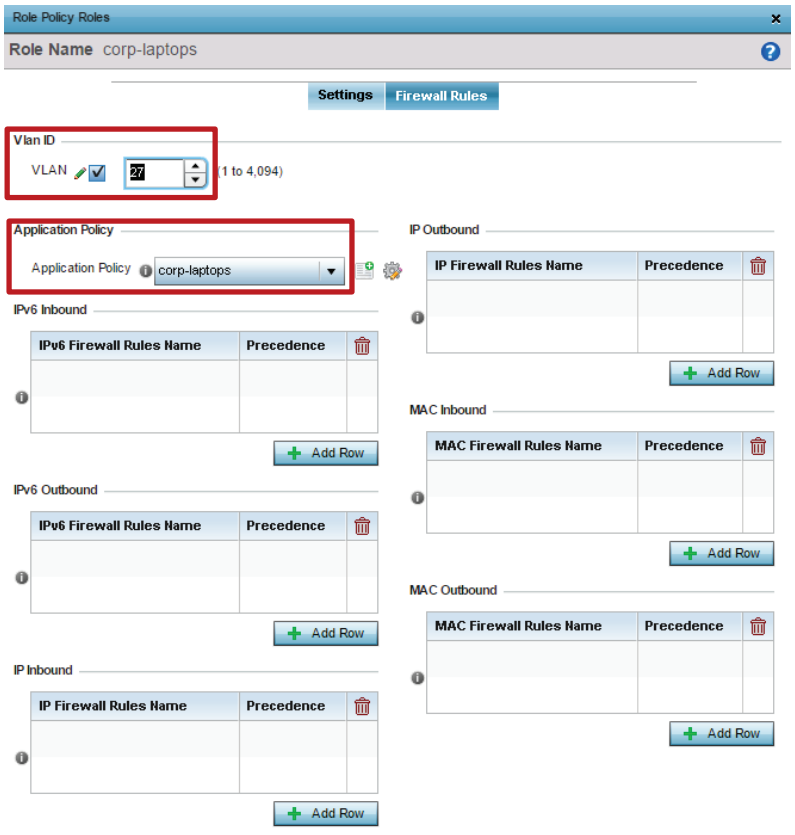
As a last step we need to modify our role policy that was created in the first two scenarios and replace “tls-users” role with three new roles matching based on client identity. Also in this scenario we will make use of the default role for the devices that didn’t match any defined identities. Each role will also assign a device into a different VLAN for traffic isolation.

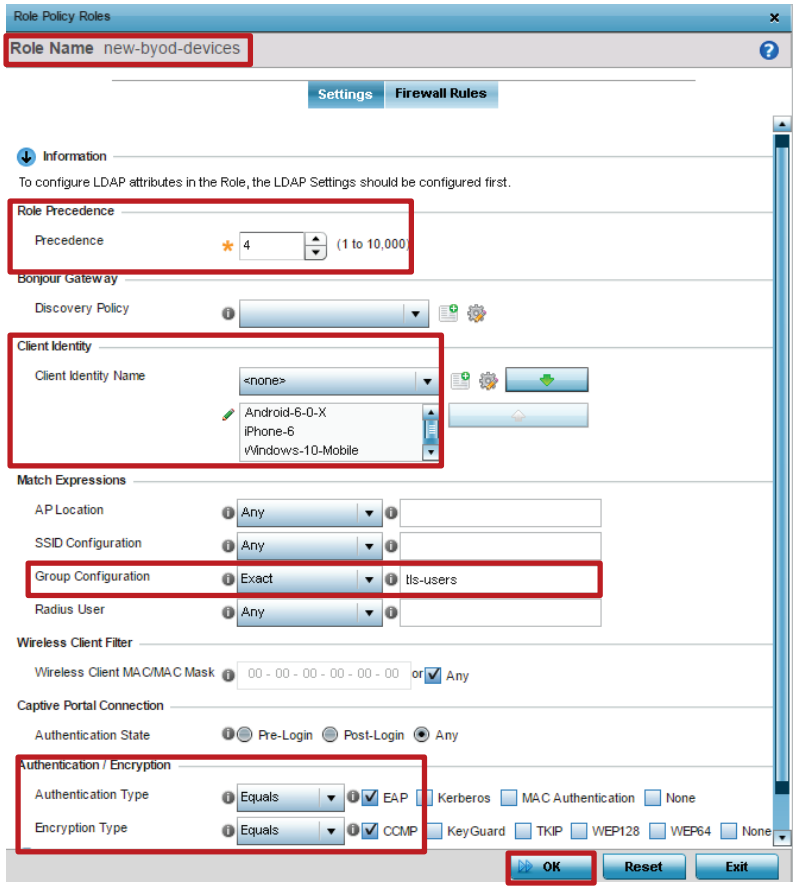
First role will identify corporate Windows 7 laptops to give them no network access restrictions and prioritize Skype for Business traffic. Next role match will identify newer BYOD devices running latest Android, iOS, Windows 10 or MAC OS X and will give them full access to the internet, while restricting access to internal network and rate-limit app stores bandwidth utilization (apple itunes, google play, microsoft store). Last role will not have a match based on client identity, but since role assignment happens based on first-match principle, everything that will not fall under “corp-laptops” or “new-byod-devices” role based on client identity will end up under “old-byod-devices” automatically, since this is our lowest precedence rule.

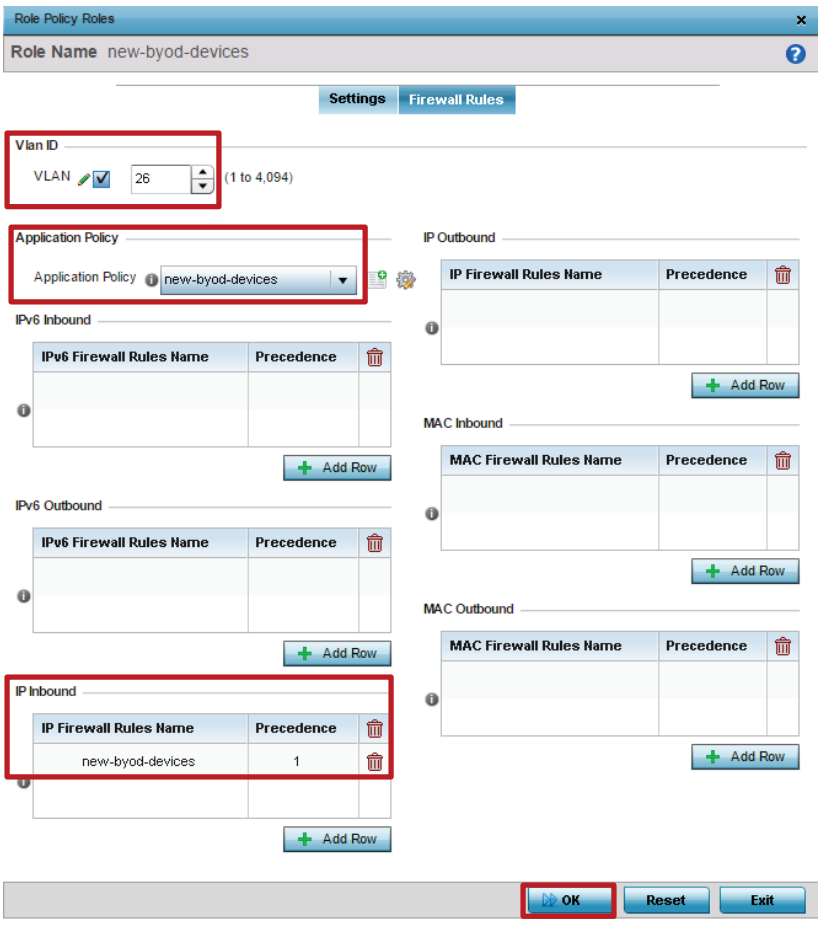
Navigate to Configuration > Security > Wireless Client Roles > select “firewalled-users” > Roles > Add:

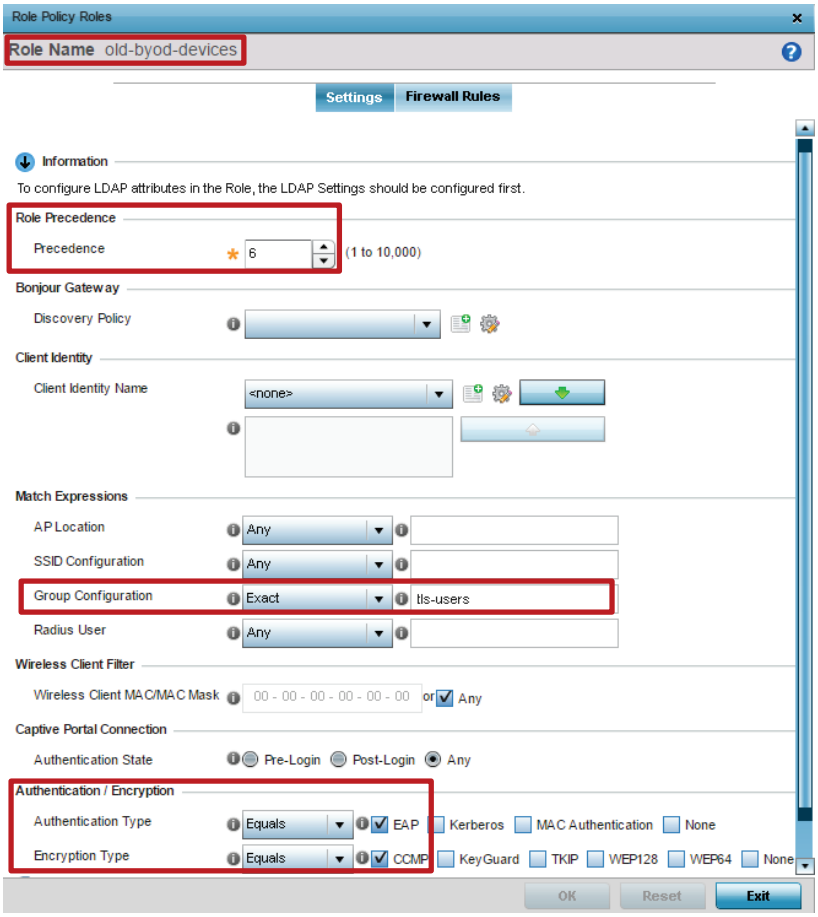
Web UI

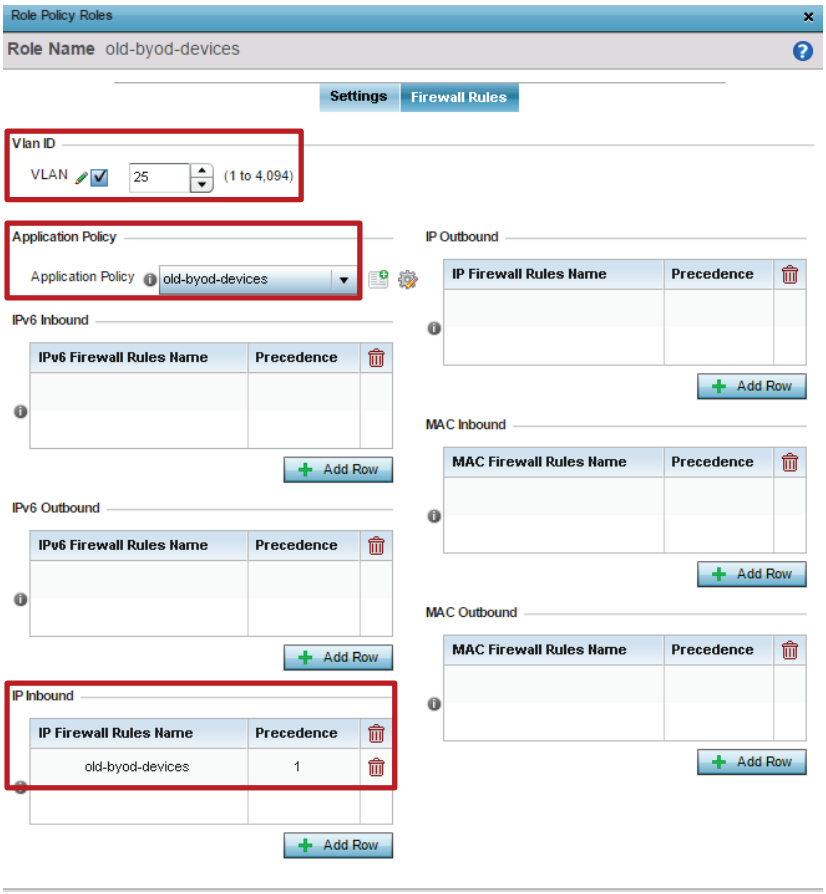












CLI

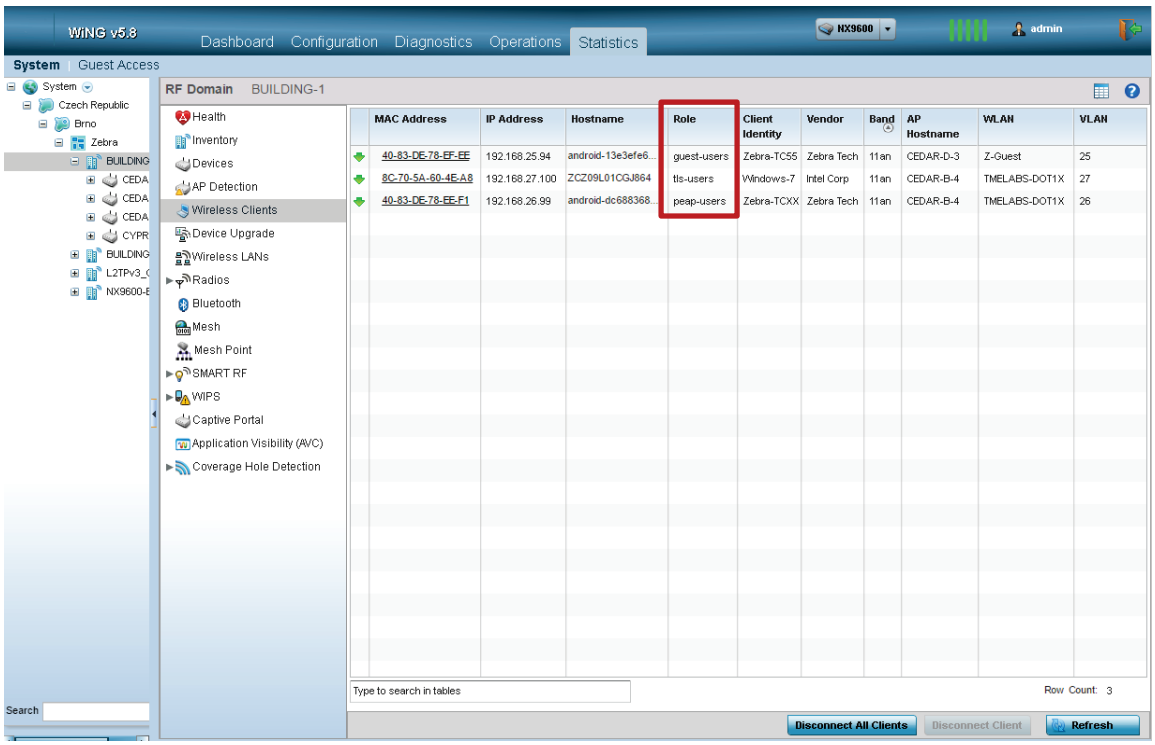
```
!
role-policy firewalled-users
 user-role guest-users precedence 1
  ssid exact Z-Guest
  use ip-access-list in guest-users precedence 1
  use application-policy guest-users
 user-role peap-users precedence 2
  authentication-type eq eap
  encryption-type eq ccmp
  group exact peap-users
  use application-policy peap-users
 user-role corp-laptops precedence 3
  assign vlan 27
  authentication-type eq eap
  encryption-type eq ccmp
  group exact tls-users
  client-identity Corp-laptops
  use application-policy corp-laptops
 user-role new-byod-devices precedence 4
  assign vlan 26
  authentication-type eq eap
  encryption-type eq ccmp
  group exact tls-users
  client-identity Android-6-0-X
  client-identity Mac-OS-X
  client-identity iPhone-6
  client-identity iPhone-iPad
  client-identity Windows-10-Mobile
  client-identity Ubuntu-11
  use ip-access-list in new-byod-devices precedence 1
  use application-policy new-byod-devices
 user-role old-byod-devices precedence 6
  assign vlan 25
  authentication-type eq eap
  encryption-type eq ccmp
  group exact tls-users
  use ip-access-list in old-byod-devices precedence 1
  use application-policy old-byod-devices
!
```

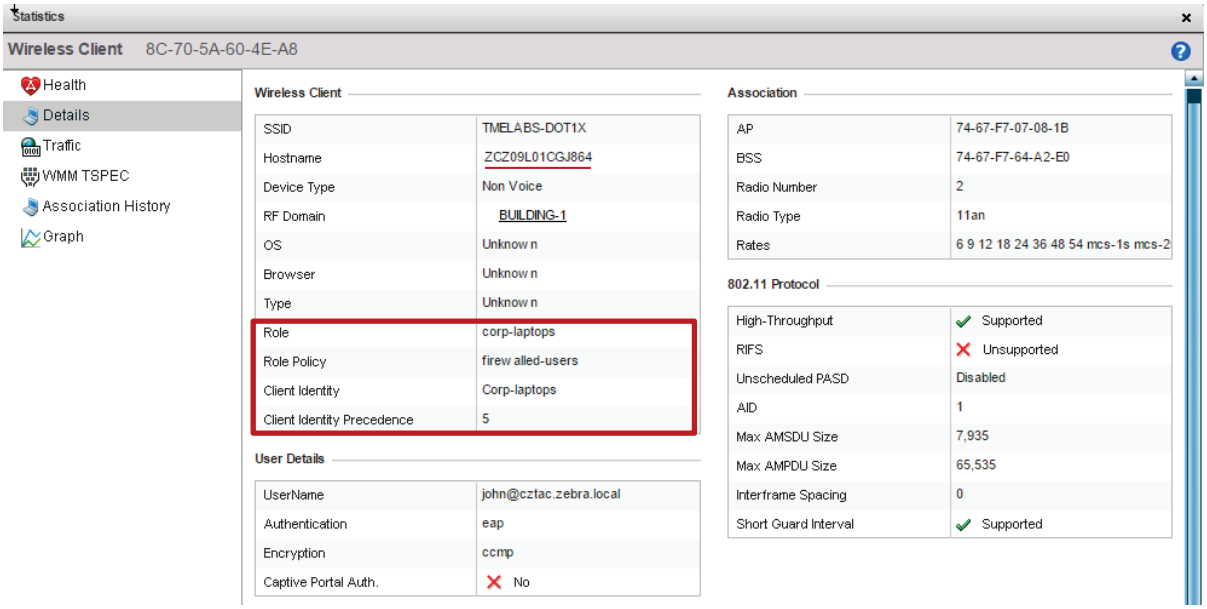
Verification

The configuration has been completed and now we can verify that roles are being assigned correctly. We expect that clients connecting to SSID “Z-Guest” will match our role-policy and will thus only be allowed to go out to the internet without any access to p2p or streaming services. Clients that authenticate using PEAP-MSCHAPv2 will be assigned a different role with p2p services disabled and video streaming services limited to 1024Kbps up and downstream. Finally, clients authenticating using EAP-TLS method will have access to all of the services on the network, additionally Skype for Business traffic will be marked with DSCP 46. All other clients that do not match any criteria will be assigned a default role with no restrictions.

After we connect few clients to our network we can view role policy state under client statistics: CLI Role Policy Verification

Role Statistics – Web UI





Role Statistics – CLI

```
NX9600-Controller-1#show wireless client detail on <AP Hostname>
  ADDRESS          : 40-83-DE-78-EE-F1 - android-dc688368... 192.168.26.99(vlan:26)
  USERNAME         : john
  WLAN             : TMELABS-DOT1X (ssid:TMELABS-DOT1X)
  ACCESS-POINT     : Name:CEDAR-B-4 Location:BUILDING-1
  RADIO-ID         : 74-67-F7-07-08-1B:R2, alias CEDAR-B-4:R2
  RADIO-NAME       : radio2 Bss:74-67-F7-64-A2-E0
  STATE            : Data-Ready
  CLIENT-INFO      : 802.11an, vendor: Extreme Tech
  SECURITY         : Authentication: eap Encryption: ccmp
  FAST-ROAMING     : Fast-BSS-Trans: N
  DATA-RATES       : 6 9 12 18 24 36 48 54 mcs-1s
  MAX-PHY_RATE     : 150 M
  MAX-USER_RATE    : 112 M
  802.11n/802.11ac : Short guard interval: Y Channel width (capability: 40MHz Current: 40MHz)
                   : AMSDU Max-Size: 3839 AMPDU Max-Size: 65535 AMPDU Min-Spacing: 0 uSec
                   : STBC: Y Transmit BeamForming: N MU-MIMO: N
  QoS              : WMM: Y Type: Non Voice
  POWER-MGMT       : PS-Mode: Y  Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
  TPC              : Y : TPC Power 7
  ACTIVITY         : Last Active: 00:27.22 ago
  SESSION INFO     : Session Timeout:   0 days 23:59.56  Idle Timeout: 00.:30.00
  RF-DOMAIN        : BUILDING-1
  ROLE             : peap-users/firewalled-users
  DHCP INFO        : Client Identity: Extreme-TCXX Precedence: 3100
  HTTP INFO        : Type: Unknown OS: Unknown Browser: Unknown

  ADDRESS          : 8C-70-5A-60-4E-A8 - ZCZ09L01CGJ864 192.168.27.100(vlan:27)
  USERNAME         : john@cztac.extreme.local
  WLAN             : TMELABS-DOT1X (ssid:TMELABS-DOT1X)
  ACCESS-POINT     : Name:CEDAR-B-4 Location:BUILDING-1
  RADIO-ID         : 74-67-F7-07-08-1B:R2, alias CEDAR-B-4:R2
  RADIO-NAME       : radio2 Bss:74-67-F7-64-A2-E0
  STATE            : Data-Ready
  CLIENT-INFO      : 802.11an, vendor: Intel Corp
  SECURITY         : Authentication: eap Encryption: ccmp
  FAST-ROAMING     : Fast-BSS-Trans: N
  DATA-RATES       : 6 9 12 18 24 36 48 54 mcs-1s mcs-2s
  MAX-PHY_RATE     : 300 M
  MAX-USER_RATE    : 225 M
  802.11n/802.11ac : Short guard interval: Y Channel width (capability: 40MHz Current: 40MHz)
                   : AMSDU Max-Size: 7935 AMPDU Max-Size: 65535 AMPDU Min-Spacing: 0 uSec
                   : STBC: Y Transmit BeamForming: N MU-MIMO: N
  QoS              : WMM: Y Type: Non Voice
  POWER-MGMT       : PS-Mode: N  Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
  TPC              : Y : TPC Power 8
  ACTIVITY         : Last Active: 00:00.01 ago
  SESSION INFO     : Session Timeout:   0 days 23:48.42  Idle Timeout: 00.:30.00
```

```
  RF-DOMAIN      : BUILDING-1
  ROLE           : tls-users/firewalled-users
  DHCP INFO      : Client Identity: Windows-7 Precedence: 900
  HTTP INFO      : Type: Unknown OS: Unknown Browser: Unknown

Total number of clients displayed: 2

NX9600-Controller-1#show wireless client detail on CEDAR-D-3
  ADDRESS        : 40-83-DE-78-EF-EE - android-13e3efe6... 192.168.25.94(vlan:25)
  USERNAME       : 40-83-DE-78-EF-EE
  WLAN           : Z-Guest (ssid:Z-Guest)
  ACCESS-POINT   : Name:CEDAR-D-3 Location:8533-bld1-fl1
  RADIO-ID       : 74-67-F7-07-09-3D:R2, alias CEDAR-D-3:R2
  RADIO-NAME     : radio2 Bss:74-67-F7-64-9C-51
  STATE          : Data-Ready
  CLIENT-INFO    : 802.11an, vendor: Extreme Tech
  SECURITY       : Authentication: mac Encryption: none
  FAST-ROAMING   : Fast-BSS-Trans: N
  DATA-RATES     : 6 9 12 18 24 36 48 54 mcs-1s
  MAX-PHY_RATE   : 150 M
  MAX-USER_RATE  : 112 M
  802.11n/802.11ac : Short guard interval: Y Channel width (capability: 40MHz Current: 40MHz)
                 : AMSDU Max-Size: 3839 AMPDU Max-Size: 65535 AMPDU Min-Spacing: 0 uSec
                 : STBC: Y Transmit BeamForming: N MU-MIMO: N
  QoS            : WMM: Y Type: Non Voice
  POWER-MGMT     : PS-Mode: Y  Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
  TPC            : Y : TPC Power 14
  PMF            : N
  ACTIVITY       : Last Active: 00:00.05 ago
  SESSION INFO   : Session Timeout:   7 days 00:00.00  Idle Timeout: 12.:00.00
  RF-DOMAIN      : BUILDING-1
  MCAST STREAMS  :
  ROLE           : guest-users/firewalled-users
  DHCP INFO      : Client Identity: Extreme-TC55 Precedence: 3200
  HTTP INFO      : Type: Android Tablet OS: Android Browser: Chrome

Total number of clients displayed: 1

NX9600-Controller-1#show role wireless-clients on CEDAR-B-4
================================================================================
                  Role_policy: firewalled-users
--------------------------------------------------------------------------------
Role: guest-users
--------------------------------------------------------------------------------
Role: tls-users
        8C-70-5A-60-4E-A8
--------------------------------------------------------------------------------
Role: peap-users
        40-83-DE-78-EE-F1
--------------------------------------------------------------------------------
================================================================================

NX9600-Controller-1#show role wireless-clients on CEDAR-D-3
================================================================================
                  Role_policy: firewalled-users
--------------------------------------------------------------------------------
Role: guest-users
        40-83-DE-78-EF-EE
--------------------------------------------------------------------------------
Role: tls-users
--------------------------------------------------------------------------------
Role: peap-users
--------------------------------------------------------------------------------
================================================================================
```

Troubleshooting

The easiest way to troubleshoot or verify role-based firewall functionality is to use remote-debug wireless feature that allows to take logs from the whole site filtered by a particular client MAC.

Role Assignment Debugging –Remote Debug Wireless

EAP-TLS client example, notice received User Group id highlighted:

```
////part of the output remove for brevity///

NX9600-Controller-1#remote-debug wireless rf-domain BUILDING-1 clients 8C-70-5A-60-4E-A8 max-events 999
duration 999 events eap management radius system wpa-wpa2

Printing up to 999 messages from each remote system for up to 999 seconds. Use Ctrl-C to abort
[CEDAR-B-4] 14:45:19.275: mgmt:rx auth-req from 8C-70-5A-60-4E-A8 on radio 1 (mgmt.c:3842)
[CEDAR-B-4] 14:45:19.275: mgmt:tx auth-rsp to 8C-70-5A-60-4E-A8 on radio 1. status: success (mgmt.c:1305)
[CEDAR-B-4] 14:45:19.276: mgmt:rx association-req from 8C-70-5A-60-4E-A8 on radio CEDAR-B-4:R2 signal-
strength is -38dBm (mgmt.c:3823)
[CEDAR-B-4] 14:45:19.276: mgmt:Client 8C-70-5A-60-4E-A8 negotiated WPA2-EAP on wlan (TMELABS-DOT1X)
(mgmt.c:3382)
[CEDAR-B-4] 14:45:19.276: mgmt:tx association-rsp success to 8C-70-5A-60-4E-A8 on wlan (TMELABS-DOT1X)
(ssid:TMELABS-DOT1X) with ftie 0 (m
[CEDAR-B-4] 14:45:19.277: client:state MU_STATE_DOT1X for client 8C-70-5A-60-4E-A8 (mgmt.c:1209)
[CEDAR-B-4] 14:45:19.277: client:wireless client 8C-70-5A-60-4E-A8 changing state from [Roaming] to
[802.1x/EAP Auth] (mgmt.c:625)
[CEDAR-B-4] 14:45:19.277: eap:sending eap-code-request code 1, type 1 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.277: eap:sending eap-id-req to 8C-70-5A-60-4E-A8 (eap.c:990)
[CEDAR-B-4] 14:45:19.331: eap:rx eap id-response from 8C-70-5A-60-4E-A8 (eap.c:696)
[CEDAR-B-4] 14:45:19.331: radius:aaa-policy External-AAA user: john@cztac.extreme.local mac: 8C-70-5A-60-
4E-A8 server_is_candidate: 1 0 0 0
[CEDAR-B-4] 14:45:19.332: radius:access-req sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (rad
[CEDAR-B-4] 14:45:19.335: radius:RAD_MSG_AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.335: radius:rx access-challenge from radius server for 8C-70-5A-60-4E-A8
(radius.c:3811)
[CEDAR-B-4] 14:45:19.335: eap:sending eap-code-request code 1, type 25 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.335: eap:sending eap-req [eap_type:25(peap)] to 8C-70-5A-60-4E-A8 (eap.c:998)
[CEDAR-B-4] 14:45:19.336: eap:rx eap pkt from 8C-70-5A-60-4E-A8 (eap.c:719)
[CEDAR-B-4] 14:45:19.337: radius:access-req sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (radius.c:1181)
[CEDAR-B-4] 14:45:19.338: radius:RAD_MSG_AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.338: radius:rx access-challenge from radius server for 8C-70-5A-60-4E-A8
(radius.c:3811)
[CEDAR-B-4] 14:45:19.338: eap:sending eap-code-request code 1, type 13 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.338: eap:sending eap-req [eap_type:13(eap-tls)] to 8C-70-5A-60-4E-A8 (eap.c:998)
[CEDAR-B-4] 14:45:19.366: eap:rx eap pkt from 8C-70-5A-60-4E-A8 (eap.c:719)
[CEDAR-B-4] 14:45:19.366: radius:access-req sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (rad
[CEDAR-B-4] 14:45:19.368: radius:RAD_MSG_AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.368: radius:rx access-challenge from radius server for 8C-70-5A-60-4E-A8
(radius.c:3811)
[CEDAR-B-4] 14:45:19.368: eap:sending eap-code-request code 1, type 13 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.368: eap:sending eap-req [eap_type:13(eap-tls)] to 8C-70-5A-60-4E-A8 (eap.c:998)
[CEDAR-B-4] 14:45:19.370: eap:rx eap pkt from 8C-70-5A-60-4E-A8 (eap.c:719)
[CEDAR-B-4] 14:45:19.371: radius:access-req sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (rad
[CEDAR-B-4] 14:45:19.375: radius:RAD_MSG_AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.375: radius:rx Client-Group-Name [tls-users] for 8C-70-5A-60-4E-A8 (radius.c:1825)
[CEDAR-B-4] 14:45:19.375: radius:rx access-accept for 8C-70-5A-60-4E-A8 (radius.c:3565)
[CEDAR-B-4] 14:45:19.375: radius:radius: updating interim acct timeout of 8C-70-5A-60-4E-A8 to 1800 seconds
(radius.c:2137)
[CEDAR-B-4] 14:45:19.375: eap:sending eap-success to 8C-70-5A-60-4E-A8 (eap.c:1006)
[CEDAR-B-4] 14:45:19.375: client:802.1x authentication success for client 8C-70-5A-60-4E-A8 (eap.c:1139)
[CEDAR-B-4] 14:45:19.375: client:starting WPA2-CCMP keying for client 8C-70-5A-60-4E-A8 (eap.c:1215)
[CEDAR-B-4] 14:45:19.375: client:wireless client 8C-70-5A-60-4E-A8 changing state from [802.1x/EAP Auth] to
[802.11i Keying] (mgmt.c:625)
[CEDAR-B-4] 14:45:19.376: wpa-wpa2:tx msg #1 to 8C-70-5A-60-4E-A8 attempt: 1 (80211i.c:617)
[CEDAR-B-4] 14:45:19.380: wpa-wpa2:rx msg #2 from mu 8C-70-5A-60-4E-A8 (80211i.c:1164)
[CEDAR-B-4] 14:45:19.381: wpa-wpa2:tx msg #3 to 8C-70-5A-60-4E-A8 attempt: 1 (80211i.c:891)
```

```
[CEDAR-B-4] 14:45:19.382: wpa-wpa2:rx msg #4. WPA2-AES handshake done. 8C-70-5A-60-4E-A8 DATA-READY
(80211i.c:1148)
[CEDAR-B-4] 14:45:19.386: client:wireless client 8C-70-5A-60-4E-A8 changing state from [802.11i Keying] to
[Data-Ready] (mgmt.c:625)
[CEDAR-B-4] 14:45:19.386: client:starting mu-idle timer for 8C-70-5A-60-4E-A8 (mgmt.c:104)
[CEDAR-B-4] 14:45:19.386: client:8C-70-5A-60-4E-A8 session-timeout: unlimited idle-timeout: 1800
(mgmt.c:455)
[CEDAR-B-4] 14:45:19.386: client:credcache_apply_app_policy_name  (credcache.c:1111)
[CEDAR-B-4] 14:45:19.386: client:update_app_policy_name_to_credcache (credcache.c:1032)
[CEDAR-B-4] 14:45:19.386: client:Adding app_policy_name to credcache and sync8C-70-5A-60-4E-A8
(credcache.c:1035)
[CEDAR-B-4] 14:45:19.390: client:RoleInfo: 8C-70-5A-60-4E-A8 idx: 3, client_idx: 0, vlan_id: 27, role_name:
tls-users (extif.c:2149)
[CEDAR-B-4] 14:45:19.390: client:client 8C-70-5A-60-4E-A8 assigned rate-limit (to-air/from-air = 0/0 on
wlan TMELABS-DOT1X (mgmt.c:218)
```

Guest SSID client example:

```
////part of the output remove for brevity///

NX9600-Controller-1#remote-debug wireless rf-domain BUILDING-1 clients E8-B1-FC-
4B-B0-81 max-events 999 duration 999 events all

Printing up to 999 messages from each remote system for up to 999 seconds. Use Ctrl-C to abort

[CEDAR-C-2] 14:56:35.130: mgmt:rx auth-req from E8-B1-FC-4B-B0-81 on radio 1 (mgmt.c:3842)
[CEDAR-C-2] 14:56:35.130: mgmt:tx auth-rsp to E8-B1-FC-4B-B0-81 on radio 1. status: success (mgmt.c:1305)
[CEDAR-C-2] 14:56:35.131: mgmt:rx association-req from E8-B1-FC-4B-B0-81 on radio CEDAR-C-2:R2 signal-
strength is -65dBm (mgmt.c:3823)
[CEDAR-C-2] 14:56:35.131: client:MU E8-B1-FC-4B-B0-81 panBU enab_cap=00 00 00 00, supp_cap=00 00 00 00
(mgmt.c:3085)
[CEDAR-C-2] 14:56:35.131: client:using cached vlan 25 for wireless client E8-B1-FC-4B-B0-81 (mgmt.c:3317)
[CEDAR-C-2] 14:56:35.131: mgmt:tx association-rsp success to E8-B1-FC-4B-B0-81 on wlan (Z-Guest) (ssid:Z-
Guest) with ftie 0 (mgmt.c:3437)
[CEDAR-C-2] 14:56:35.131: client:wireless client E8-B1-FC-4B-B0-81 changing state from [Roaming] to [MAC
Auth] (mgmt.c:625)
[CEDAR-C-2] 14:56:35.131: radius:aaa-policy Internal-NX user: E8-B1-FC-4B-B0-81 mac: E8-B1-FC-4B-B0-81
server_is_candidate: 1 0 0 0 0 0 (r
[CEDAR-C-2] 14:56:35.132: radius:access-req sent to wireless controller to be proxied via its adopter
centralized controller (if any) to 1
[CEDAR-C-2] 14:56:35.132: client:restarting mac_auth timer for E8-B1-FC-4B-B0-81 (radius.c:4677)
[CEDAR-C-2] 14:56:35.133: client:transmitting roam notification for E8-B1-FC-4B-B0-81 (mgmt.c:348)
[CEDAR-C-2] 14:56:35.136: radius:rx access-reject for E8-B1-FC-4B-B0-81 (radius.c:3711)
[CEDAR-C-2] 14:56:35.136: radius:failover to captive-portal for non data-ready MU E8-B1-FC-4B-B0-81
(radius.c:3752)
[CEDAR-C-2] 14:56:35.136: client:wireless client E8-B1-FC-4B-B0-81 changing state from [MAC Auth] to [Data-
Ready] (mgmt.c:625)
[CEDAR-C-2] 14:56:35.137: client:starting mu-idle timer for E8-B1-FC-4B-B0-81 (mgmt.c:104)
[CEDAR-C-2] 14:56:35.137: client:E8-B1-FC-4B-B0-81 session-timeout: unlimited idle-timeout: 43200
(mgmt.c:455)
[CEDAR-C-2] 14:56:35.137: client:credcache_apply_app_policy_name  (credcache.c:1111)
[CEDAR-C-2] 14:56:35.137: client:update_app_policy_name_to_credcache (credcache.c:1032)
[CEDAR-C-2] 14:56:35.137: client:Adding app_policy_name to credcache and sync E8-B1-FC-4B-B0-81
(credcache.c:1035)
[CEDAR-C-2] 14:56:35.231: client:RoleInfo: E8-B1-FC-4B-B0-81 idx: 1, client_idx: 1, vlan_id: 25, role_name:
guest-users (extif.c:2149)
[CEDAR-C-2] 14:56:35.232: client:client E8-B1-FC-4B-B0-81 assigned rate-limit (to-air/from-air = 0/0 on
wlan Z-Guest (mgmt.c:218)
```

Client Identity a.k.a DHCP Fingerprinting Debugging

```
#debug role dhcpfp level debug on <AP hostname>

#show logging on <AP hostname> | include <client MAC>

DPD2: 2016-07-11 16:45:18 dhcpfp.c:493 dhcp_fingerprint_client 8C-70-5A-60-4E-A8: client identified as
(Windows-7, 900), fp state=0x0c
DPD2: 8C-70-5A-60-4E-A8: message-type request option 81 exact hexstring
0000005a435a30394c303143474a3836342e637a7461632e7a656272612e6c6f63616c
DPD2: 8C-70-5A-60-4E-A8: message-type request option 61 exact hexstring 018c705a604ea8
DPD2: 8C-70-5A-60-4E-A8: message-type request option 60 exact ascii MSFT 5.0
DPD2: 8C-70-5A-60-4E-A8: message-type request option 55 exact hexstring 010f03062c2e2f1f2179f92b
DPD2: 8C-70-5A-60-4E-A8: message-type request option 50 exact hexstring c0a81b64
DPD2: 8C-70-5A-60-4E-A8: message-type request option 12 exact ascii ZCZ09L01CGJ864
DPD2: 8C-70-5A-60-4E-A8: message-type request option-codes exact hexstring 353d320c513c37
DPD2: 2016-07-11 16:37:21 dhcpfp.c:577 handle_dhcp_fingerprint fingerprint from wireless client
```