Working “DERIVATION ROLE” for DOMAIN and PERSONAL workstation without CPPM Jan14-Tutorial

Goals:

- Separating DOMAIN and PERSONAL WORKSTATION
- Derived role for DOMAIN user group/division
- Derived role for PERSONAL user group/division

This guide is for those who want to separate DOMAIN and PERSONAL workstation in their network without ClearPass. Although the result is almost the same, but it’s not a bullet-proof configuration.

In most case, separation of DOMAIN and PERSONAL can be achieved by using “Enforce Machine Authentication” in 802.1X Auth config.

On DOMAIN workstation that passed both machine and user authentication, it can have derived role as stated on Server Group, but not for PERSONAL workstation which only using “user authentication”.

For this setup, I am using:

- NPS (Windows 2008)
- Aruba Controller 3600 OS 6.3.0.2
- AP 105
- 1 Domain Laptop
- 1 Personal Laptop

Setting up Controller:

- Basic setup
- Radius for Domain

RADIUS Server > ARUBALABS-AD

Show Reference | Save As | Reset

Host	172.16.0.2
Key	•••••••• Retype: ••••••••
Auth Port	1812
Acct Port	1813
Retransmits	3
Timeout	5 sec
NAS ID	10
NAS IP	
Enable IPv6	☐
NAS IPv6	
Source Interface	vlanid ipv6addr
Use MD5	☐
Use IP address for calling station ID	☐
Mode	☑
Lowercase MAC addresses	☐
MAC address delimiter	none
Service-type of FRAMED-USER	☐

- Radius for PERSONAL

RADIUS Server > ARUBALABS-PERSONAL

Show Reference | Save As | Reset

Host	172.16.0.2
Key	•••••••• Retype: ••••••••
Auth Port	1812
Acct Port	1813
Retransmits	3
Timeout	5 sec
NAS ID	11
NAS IP	
Enable IPv6	☐
NAS IPv6	
Source Interface	vlanid ipv6addr
Use MD5	☐
Use IP address for calling station ID	☑
Mode	☑
Lowercase MAC addresses	☐
MAC address delimiter	none
Service-type of FRAMED-USER	☐

- SERVER GROUP

Security > Authentication > Servers

Servers | AAA Profiles | L2 Authentication | L3 Authentication | User Rules | Advanced

- Server Group
  - ARUBALABS-GROUP
  - ARUBALABS-ROLE-DERIV
  - default
  - internal
- RADIUS Server
  - ARUBALABS-AD
  - ARUBALABS-PERSONAL
  - CLOUDESSA-MSI
- LDAP Server

Server Group > ARUBALABS-ROLE-DERIV — Show Reference | Save As | Reset

Fail Through ☑

Servers

Name	Server-Type	trim-FQDN	Match-Rule
ARUBALABS-AD	Radius	No	AuthString starts-with MITRA
ARUBALABS-PERSONAL	Radius	No	

New | Delete

Server Rules

Priority	Attribute	Operation	Operand	Type	Action	Value	Validated
1	Filter-Id	value-of		String	set role		Yes

New | Delete

- When you configure windows EAP-MSCHAP2 wireless property with “Automatically use windows logon”, it will login using format: DOMAIN\USERNAME. In this case, my DOMAIN is MITRA.

- AAA Profile (Basic config for 802.1X)

- AAA
  - ARUBALABS-DOT1X-PROF
  - ARUBALABS-GUEST
  - ARUBALABS-SSO-PROF
    - MAC Authentication
    - MAC Authentication Server Group: default
    - 802.1X Authentication: 802.11-NO-TERMINATION
    - 802.1X Authentication Server Group: ARUBALABS-ROLE-DERIV
    - RADIUS Accounting Server Group: ARUBALABS-ROLE-DERIV
    - XML API server
    - RFC 3576 server
  - default
  - default-dot1x

AAA Profile > ARUBALABS-SSO-PROF — Show Reference | Save As | Reset

Initial role	logon
MAC Authentication Default Role	guest
802.1X Authentication Default Role	authenticated
L2 Authentication Fail Through	☐
User idle timeout	☐ Enable; seconds
RADIUS Interim Accounting	☐
User derivation rules	--NONE--
Wired to Wireless Roaming	☑
SIP authentication role	--NONE--
Device Type Classification	☑
Enforce DHCP	☐

- 802.1X Profile (please ignore the name)

- AAA
  - ARUBALABS-DOT1X-PROF
  - ARUBALABS-GUEST
  - ARUBALABS-SSO-PROF
    - MAC Authentication
    - MAC Authentication Server Group: default
    - 802.1X Authentication: 802.11-NO-TERMINATION
    - 802.1X Authentication Server Group: ARUBALABS-ROLE-DERIV
    - RADIUS Accounting Server Group: ARUBALABS-ROLE-DERIV
    - XML API server
    - RFC 3576 server

802.1X Authentication Profile > 802.11-NO-TERMINATION — Show Reference | Save As | Reset

Basic | Advanced

Max authentication failures	0
Enforce Machine Authentication	☐
Machine Authentication: Default Machine Role	authenticated
Machine Authentication: Default User Role	authenticated
Reauthentication	☐
Termination	☑
Termination EAP-Type	☐ eap-tls ☑ eap-peap
Termination Inner EAP-Type	☑ eap-mschapv2 ☐ eap-gtc

- APGROUP, SSID (Basic config for 802.1X)

Configuration > AP Group > Edit "ARUBALABS-CAP"

Profiles

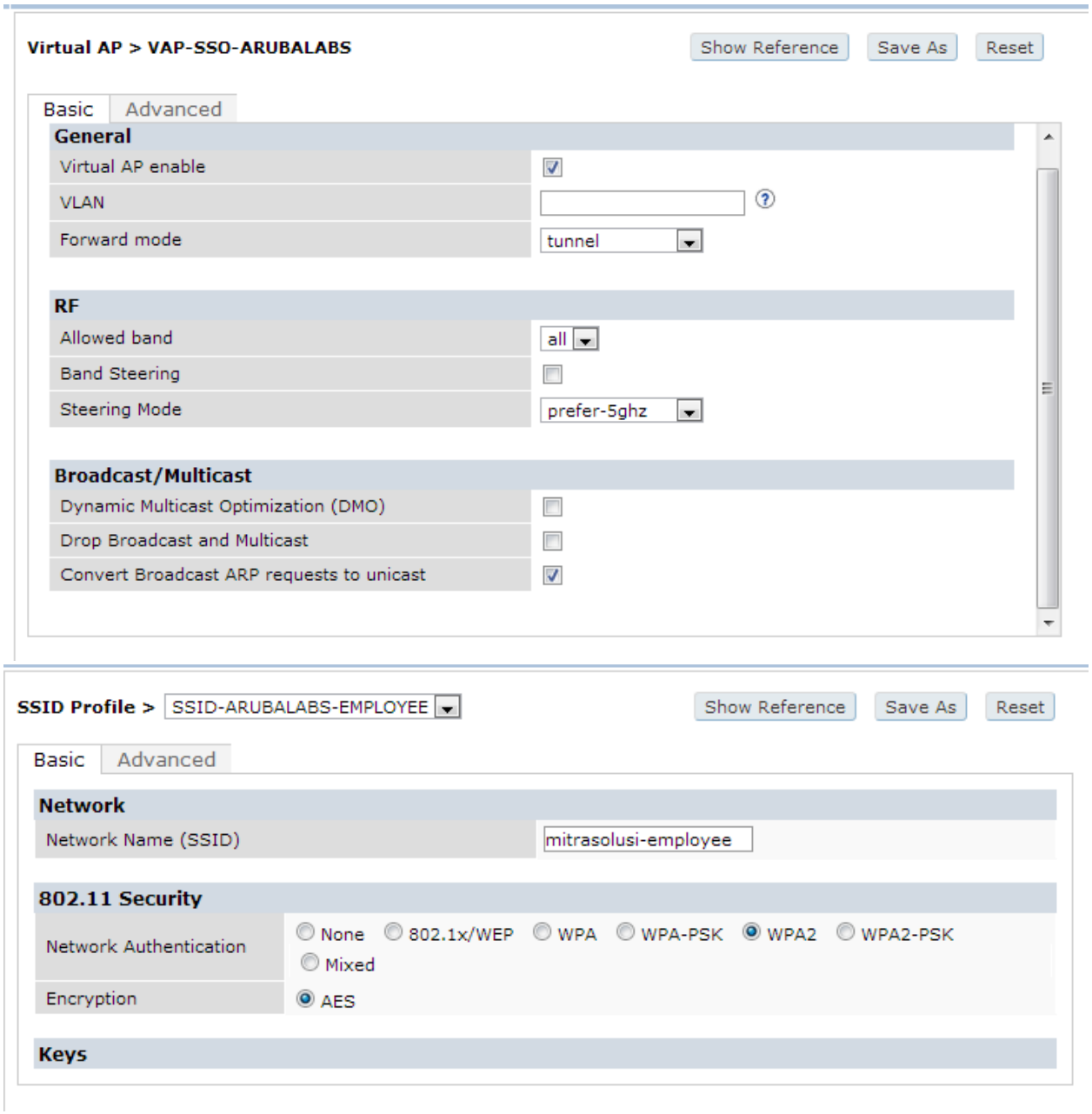
- Wireless LAN
  - Virtual AP
    - VAP-GUEST
    - VAP-SSO-ARUBALABS
- RF Management
- AP
- QOS
- IDS
- Mesh

Profile Details

Virtual APs

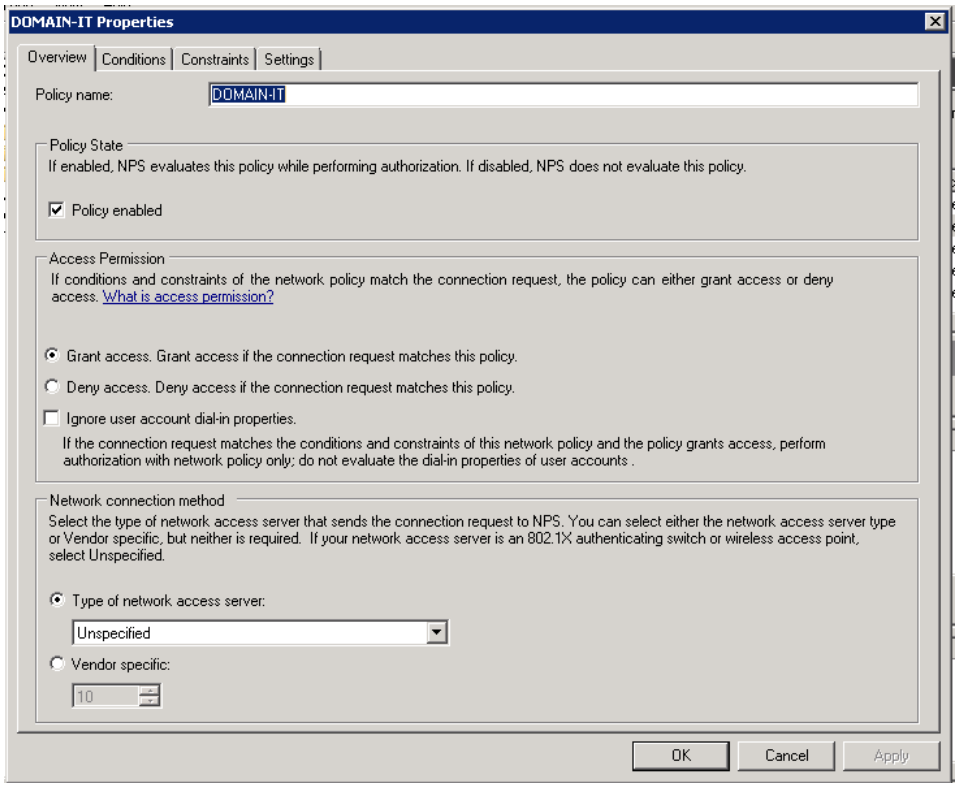
Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable	Actions
VAP-GUEST	ARUBALABS-GUEST	SSID-ARUBALABS-GUEST	2000	tunnel	Enabled	Delete
VAP-SSO-ARUBALABS	ARUBALABS-SSO-PROF	SSID-ARUBALABS-EMPLOYEE		tunnel	Enabled	Delete

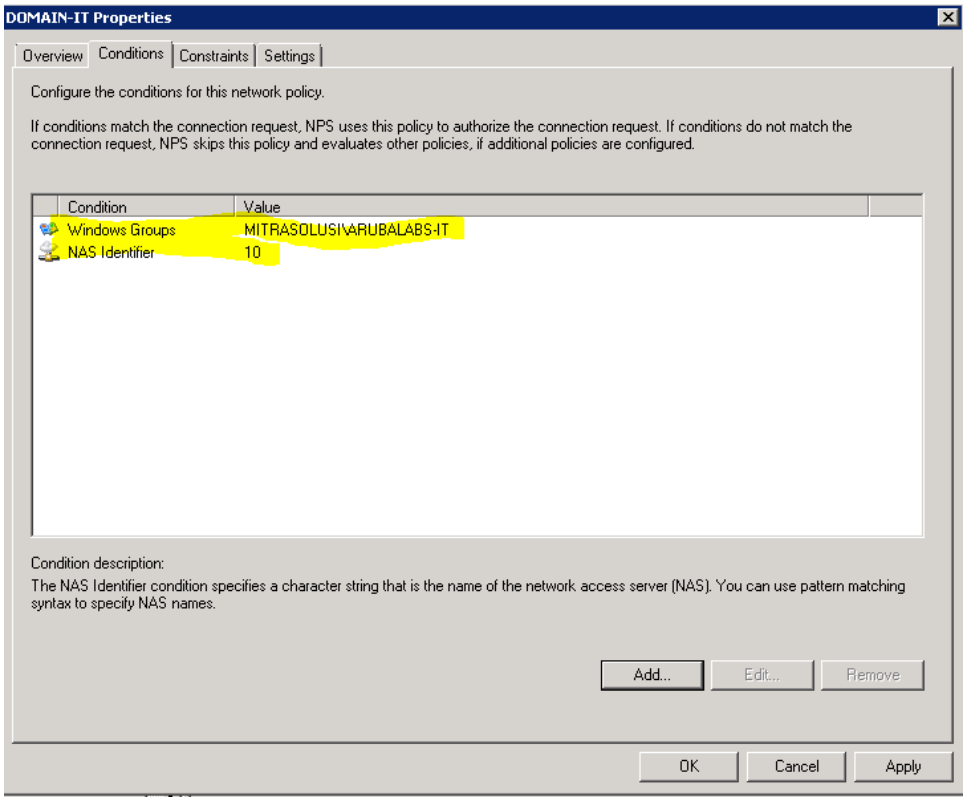
Add a profile default — Add

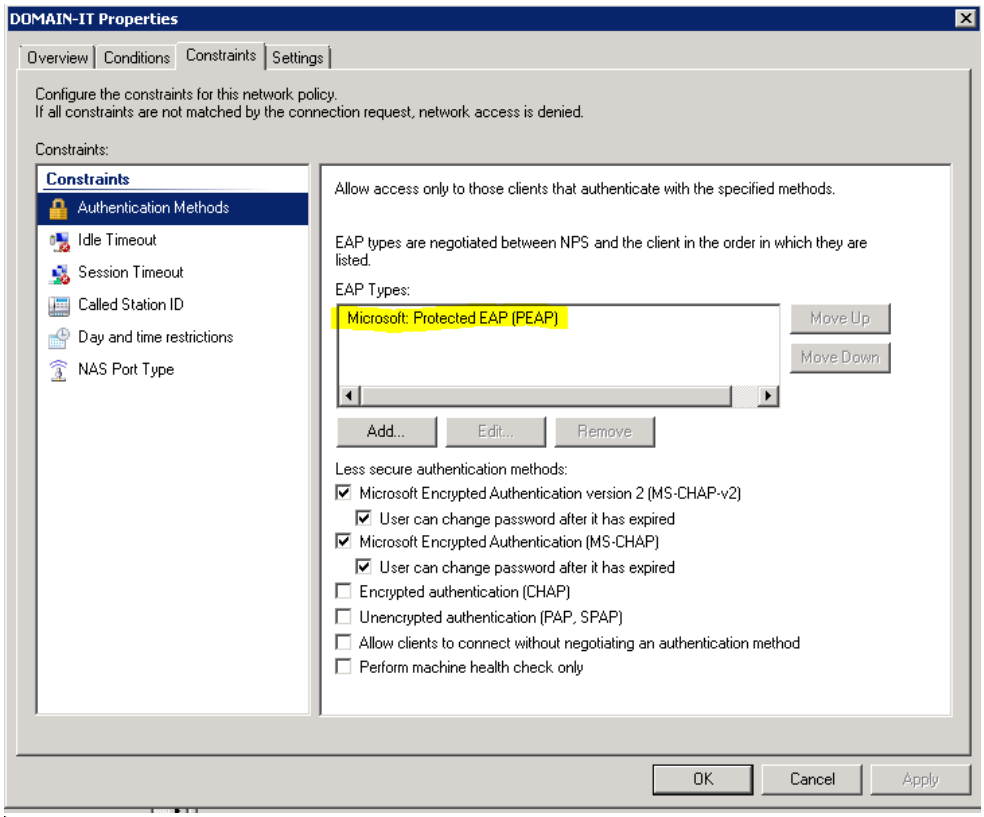

Virtual AP > VAP-SSO-ARUBALABS
Show Reference
Save As
Reset
Basic
Advanced
General
Virtual AP enable
VLAN
Forward mode
tunnel
RF
Allowed band
all
Band Steering
Steering Mode
prefer-5ghz
Broadcast/Multicast
Dynamic Multicast Optimization (DMO)
Drop Broadcast and Multicast
Convert Broadcast ARP requests to unicast
SSID Profile >
SSID-ARUBALABS-EMPLOYEE
Show Reference
Save As
Reset
Basic
Advanced
Network
Network Name (SSID)
mitrasolusi-employee
802.11 Security
Network Authentication
None
802.1x/WEP
WPA
WPA-PSK
WPA2
WPA2-PSK
Mixed
Encryption
AES
Keys

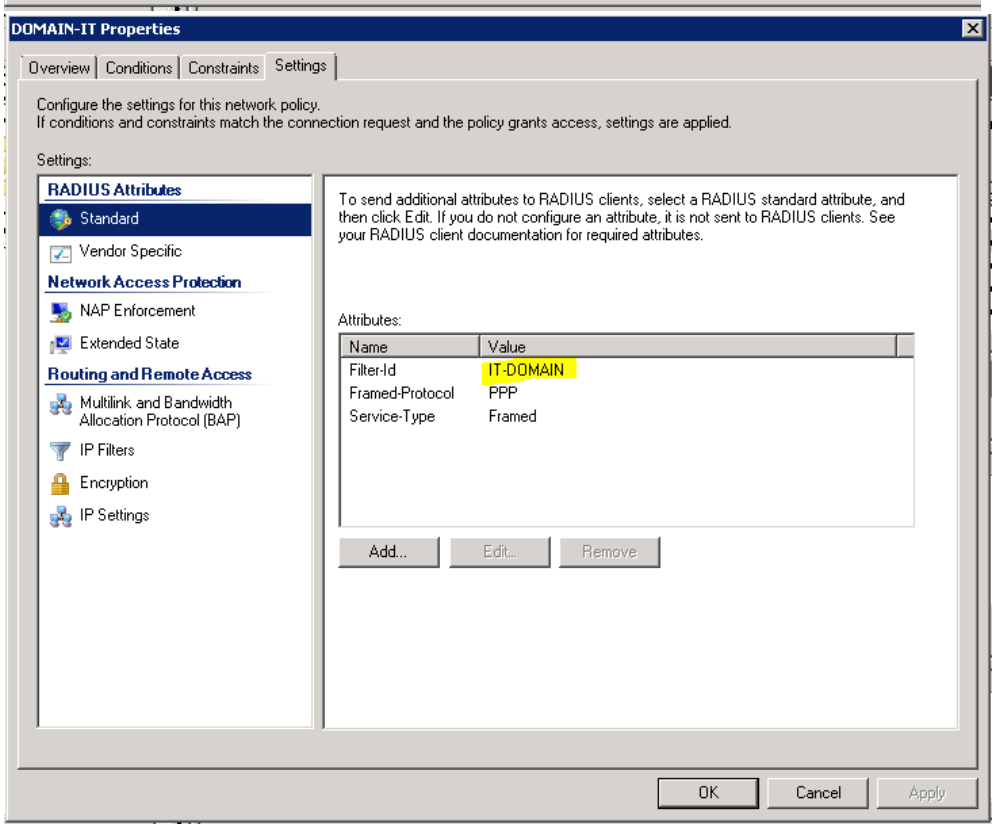
Setting up NPS Policy:

- Basic setup
- Policy for DOMAIN-IT

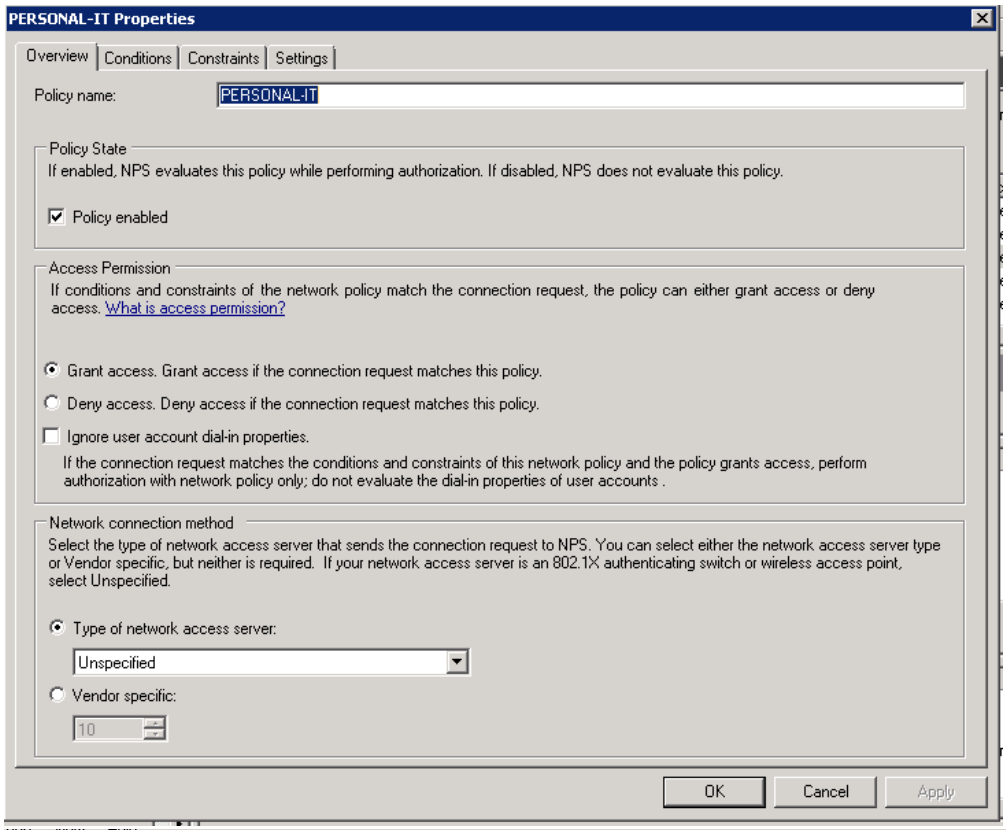


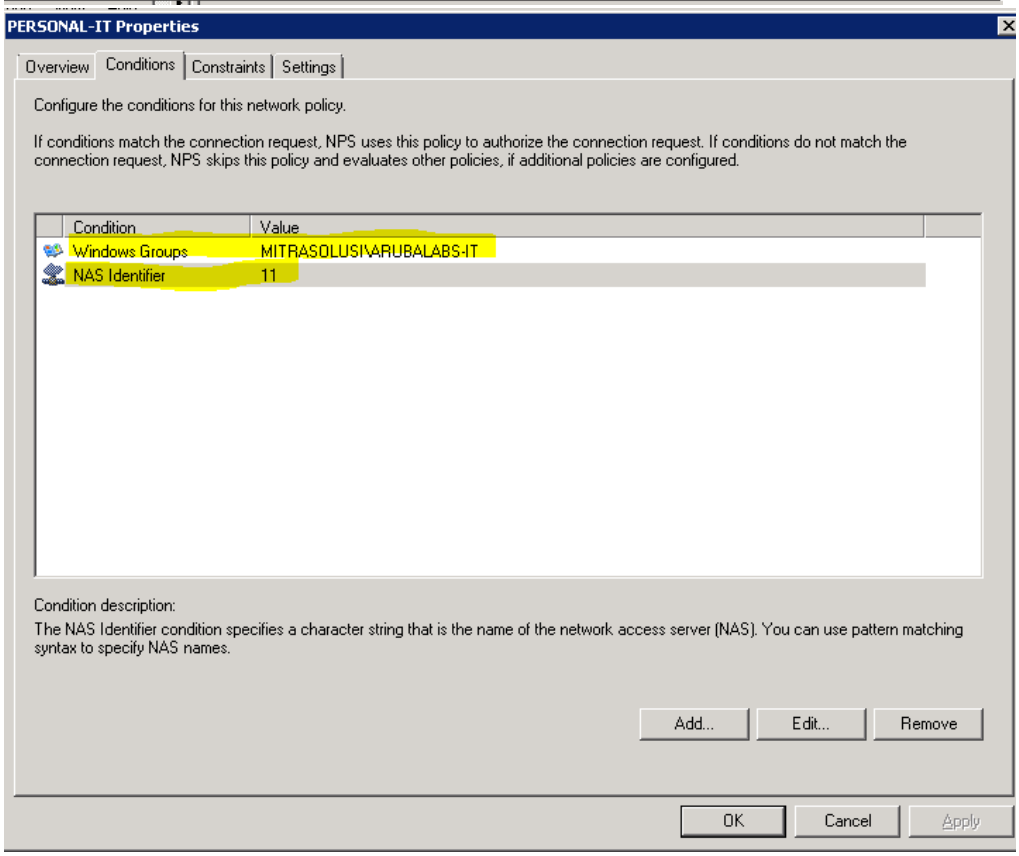


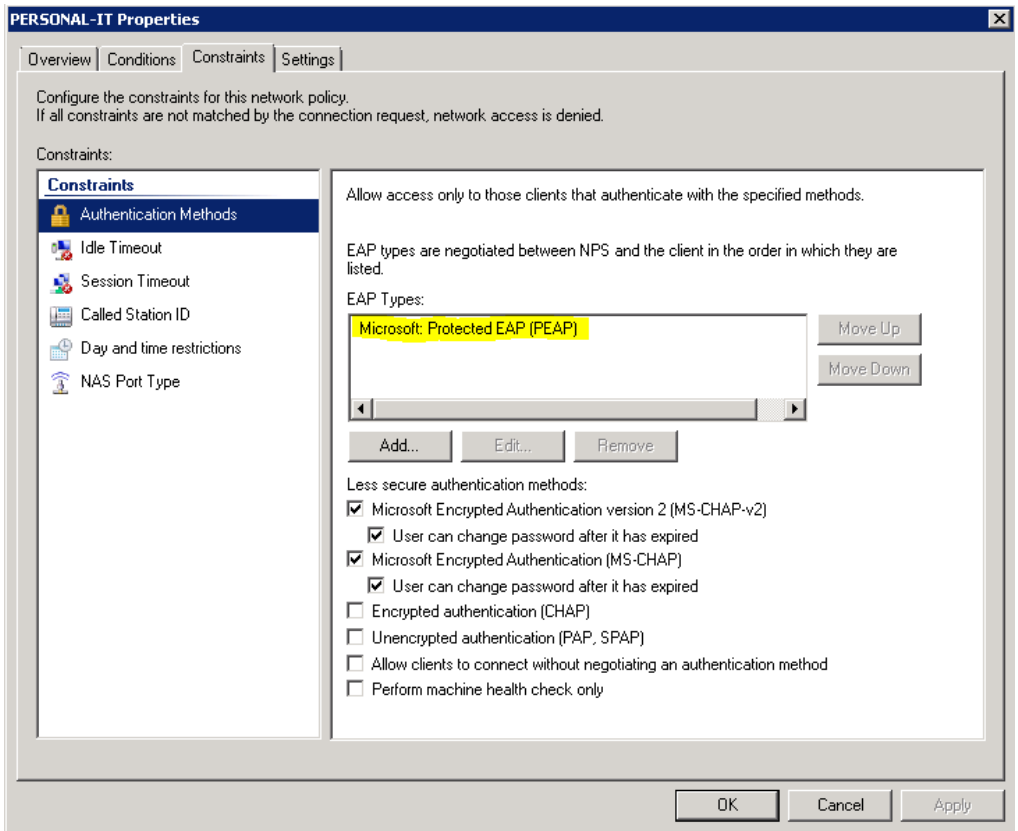

DOMAIN-IT Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
Perform machine health check only
OK
Cancel
Apply

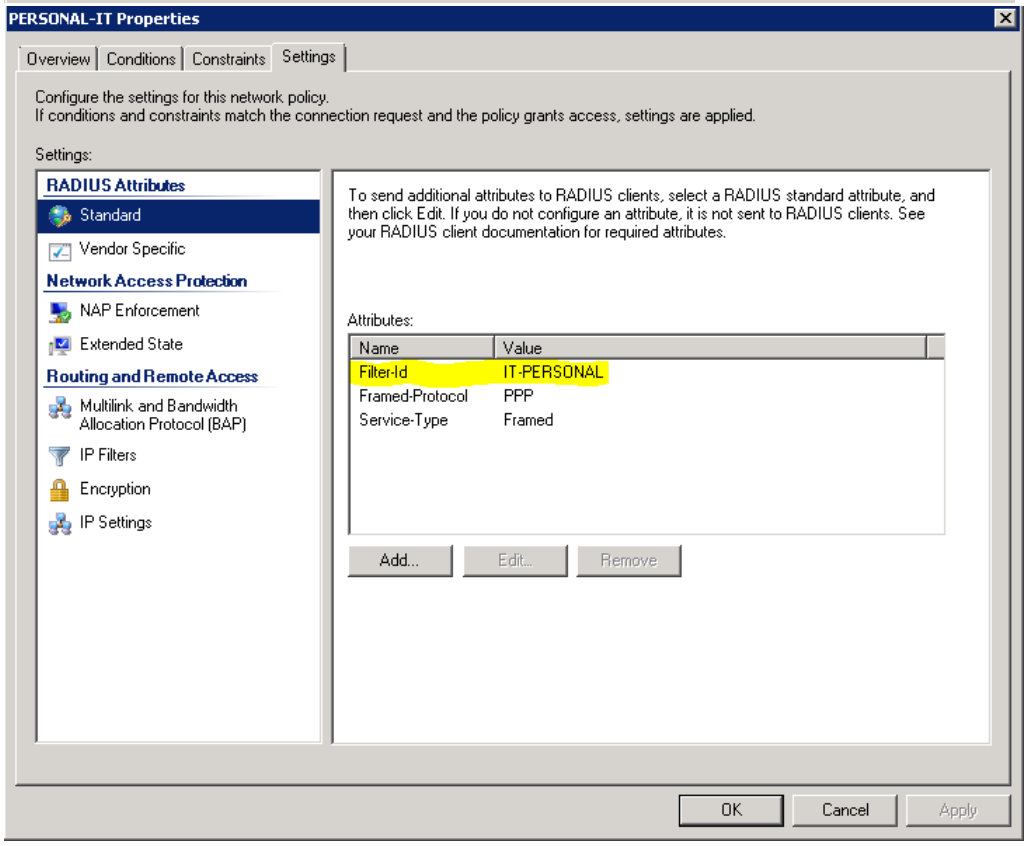

DOMAIN-IT Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Filter-Id
IT-DOMAIN
Framed-Protocol
PPP
Service-Type
Framed
Add...
Edit...
Remove
OK
Cancel
Apply

- Policy for PERSONAL-IT

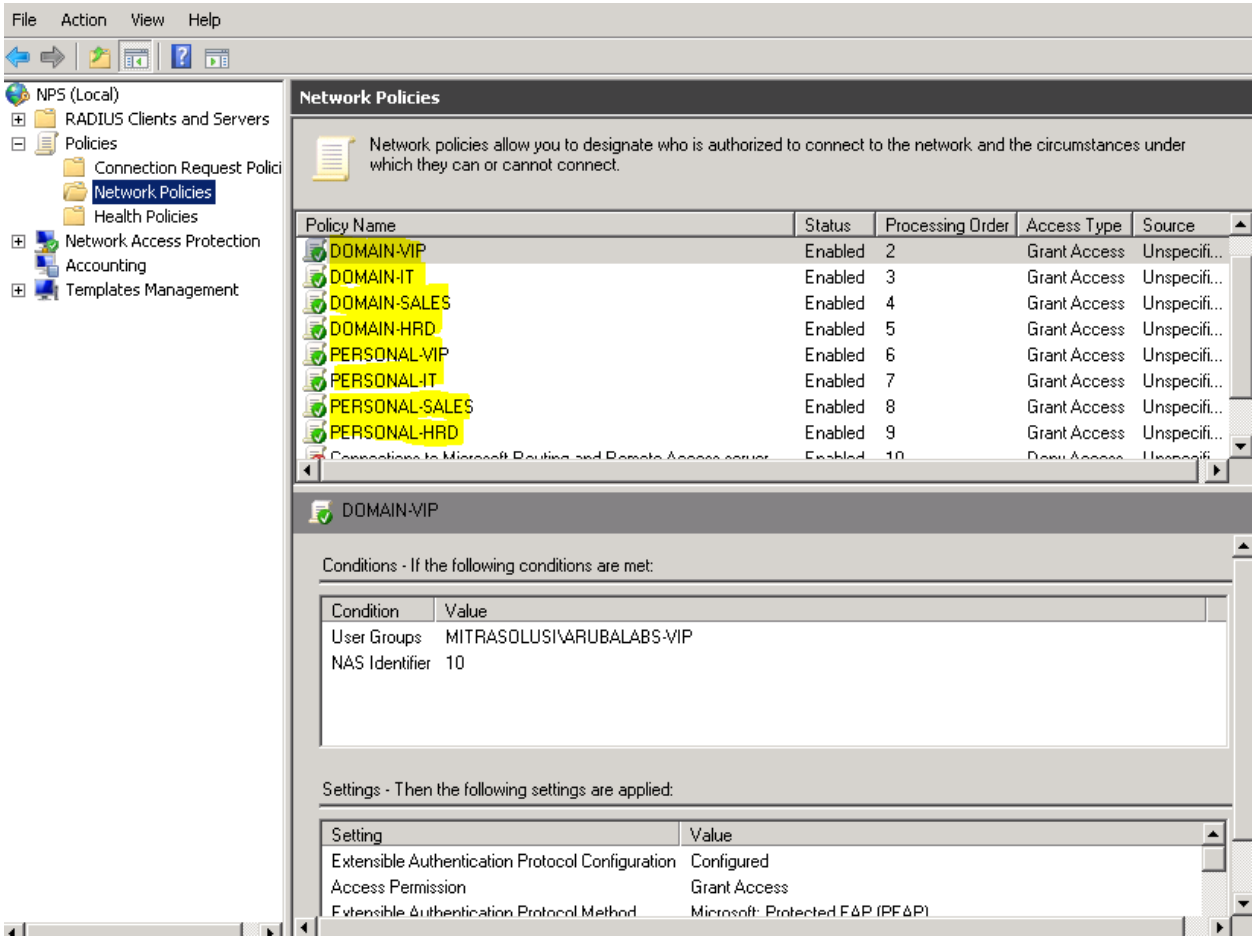





PERSONAL-IT Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
Perform machine health check only
OK
Cancel
Apply

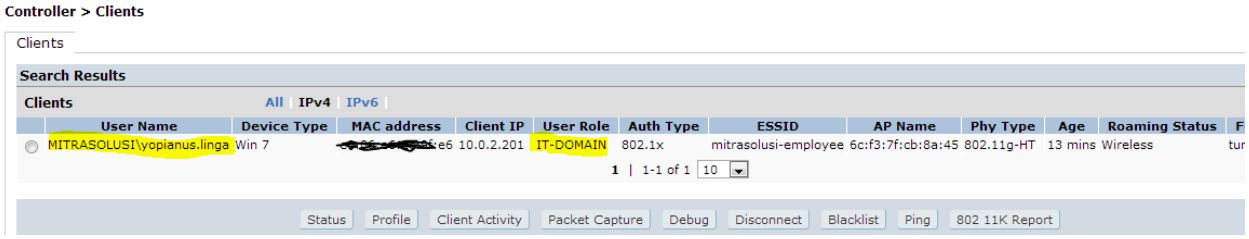

PERSONAL-IT Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Filter-Id
IT-PERSONAL
Framed-Protocol
PPP
Service-Type
Framed
Add...
Edit...
Remove
OK
Cancel
Apply

- Don’t forget to create user account on controller that has exact match with the value of filter-id on each NPS Policy.
- Create as many policies as you need, refer to your own Company’s user group.



Setting up DOMAIN workstation :

- Connect to the SSID
- By default, windows will use your LOGIN credential to connect. *Or admin can push the config from Group Policy*
- User connected to the network with domain-role



- Event viewer log (copied)

Network Policy Server granted full access to a user because the host met the defined health policy.

User:

Security ID:	MITRASOLUSI\yopianus.linga
Account Name:	MITRASOLUSI\yopianus.linga
Account Domain:	MITRASOLUSI
Fully Qualified Account Name:	mitrasolusi.co.vu/Users/Yopianus Linga

Client Machine:

Security ID:	NULL SID
Account Name:	-
Fully Qualified Account Name:	-
OS-Version:	-
Called Station Identifier:	**********
Calling Station Identifier:	**********

NAS:

NAS IPv4 Address:	172.16.0.254
NAS IPv6 Address:	-
NAS Identifier:	10
NAS Port-Type:	Wireless - IEEE 802.11
NAS Port:	0

RADIUS Client:

Client Friendly Name:	Aruba Controller
Client IP Address:	172.16.0.254

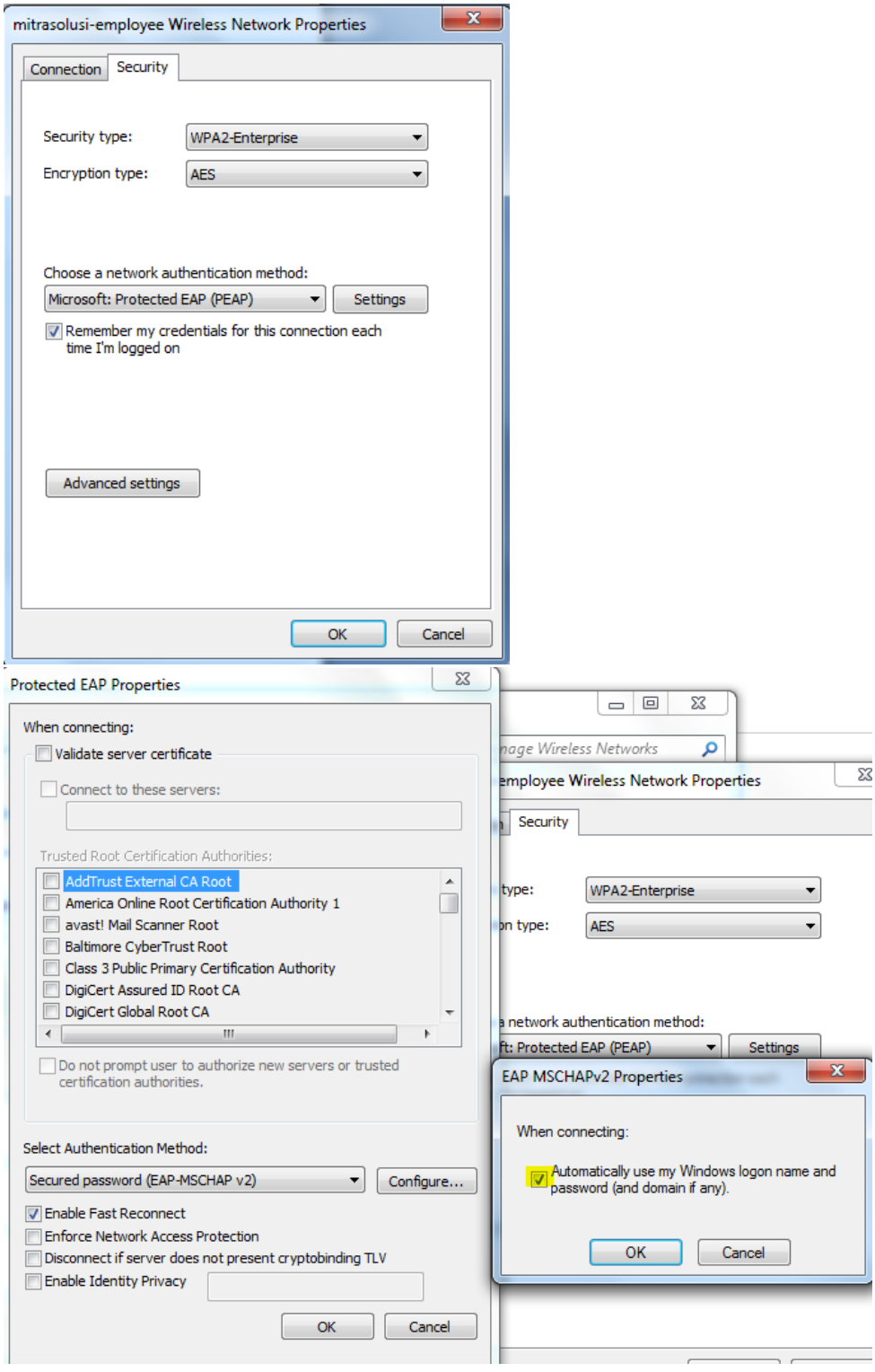
Authentication Details:

Connection Request Policy Name:	1X-EMPLOYEE
Network Policy Name:	DOMAIN-IT
Authentication Provider:	Windows
Authentication Server:	ARUBALABS-SRV01.mitrasolusi.co.vu
Authentication Type:	MS-CHAPv2
EAP Type:	-
Account Session Identifier:	-

Quarantine Information:

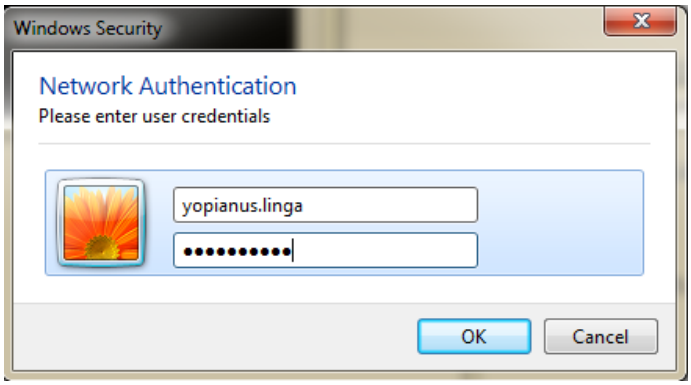
Result:	Full Access
Extended-Result:	-
Session Identifier:	-
Help URL:	-
System Health Validator Result(s):	-

- For manual config :

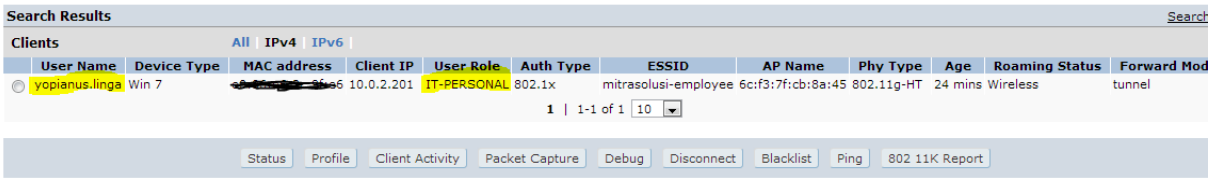

mitrasolusi-employee Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel
Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AddTrust External CA Root
America Online Root Certification Authority 1
avast! Mail Scanner Root
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel
nage Wireless Networks
employee Wireless Network Properties
Security
type:
WPA2-Enterprise
on type:
AES
network authentication method:
ft: Protected EAP (PEAP)
Settings
EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel

Setting up PERSONAL workstation :

- Connect to the SSID
- Login using username and password



- User connected to the network with personal-role



- Event Viewer Log (Copied)

Network Policy Server granted full access to a user because the host met the defined health policy.

User:

Security ID:	MITRASOLUSI\yopianus.linga
Account Name:	yopianus.linga
Account Domain:	MITRASOLUSI
Fully Qualified Account Name:	mitrasolusi.co.vu/Users/Yopianus Linga

Client Machine:

Security ID:	NULL SID
Account Name:	-
Fully Qualified Account Name:	-
OS-Version:	-
Called Station Identifier:	********
Calling Station Identifier:	000000000000

NAS:

NAS IPv4 Address:	172.16.0.254
NAS IPv6 Address:	-
NAS Identifier:	11
NAS Port-Type:	Wireless - IEEE 802.11
NAS Port:	0

RADIUS Client:

Client Friendly Name:	Aruba Controller
Client IP Address:	172.16.0.254

Authentication Details:

Connection Request Policy Name:	1X-EMPLOYEE
Network Policy Name:	PERSONAL-IT
Authentication Provider:	Windows
Authentication Server:	ARUBALABS-SRV01.mitrasolusi.co.vu
Authentication Type:	MS-CHAPv2
EAP Type:	-
Account Session Identifier:	-

Quarantine Information:

Result:	Full Access
Extended-Result:	-
Session Identifier:	-
Help URL:	-
System Health Validator Result(s):	-

As I said earlier, this setup is not bullet-proof. When personal user login with format : DOMAIN\USERNAME, they will get domain role. There are no “workaround” for this hole. (not without CPPM :D)

Cheers

Yopianus Linga
Senior Engineer / ACMP