Eduroam Radius NPS Setup

Step 1 - RADIUS Clients and Servers

Radius Clients

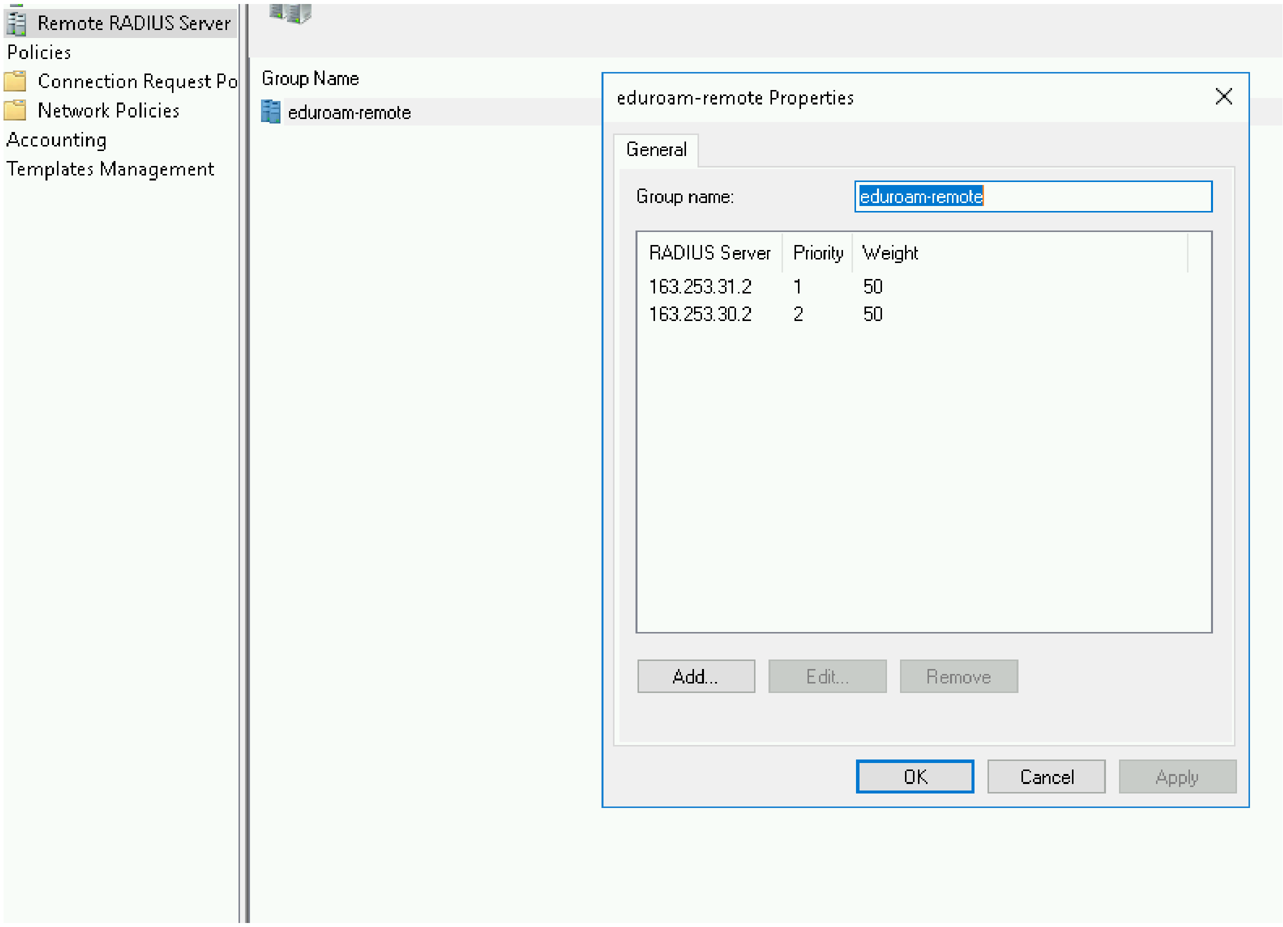
Add the two radius clients, the two ip addresses eduroam provides. (at the time of writing this, there are 2 old ip addresses and 2 new ip addresses that will take effect in January, attempt using the two new ones or add all 4)

These are the New ones:
163.253.31.2
163.253.30.2

You'll need to allow these ip addresses on the firewall to access your NPS server using radius port: 1812 / udp

Friendly name needs to be something like eduroam-x where x could be 1 for first ip.
Create a shared secret that you will use on the eduroam.us website to link the NPS radius with eduroam radius.

Remote RADIUS Server



Group name: eduroam-remote

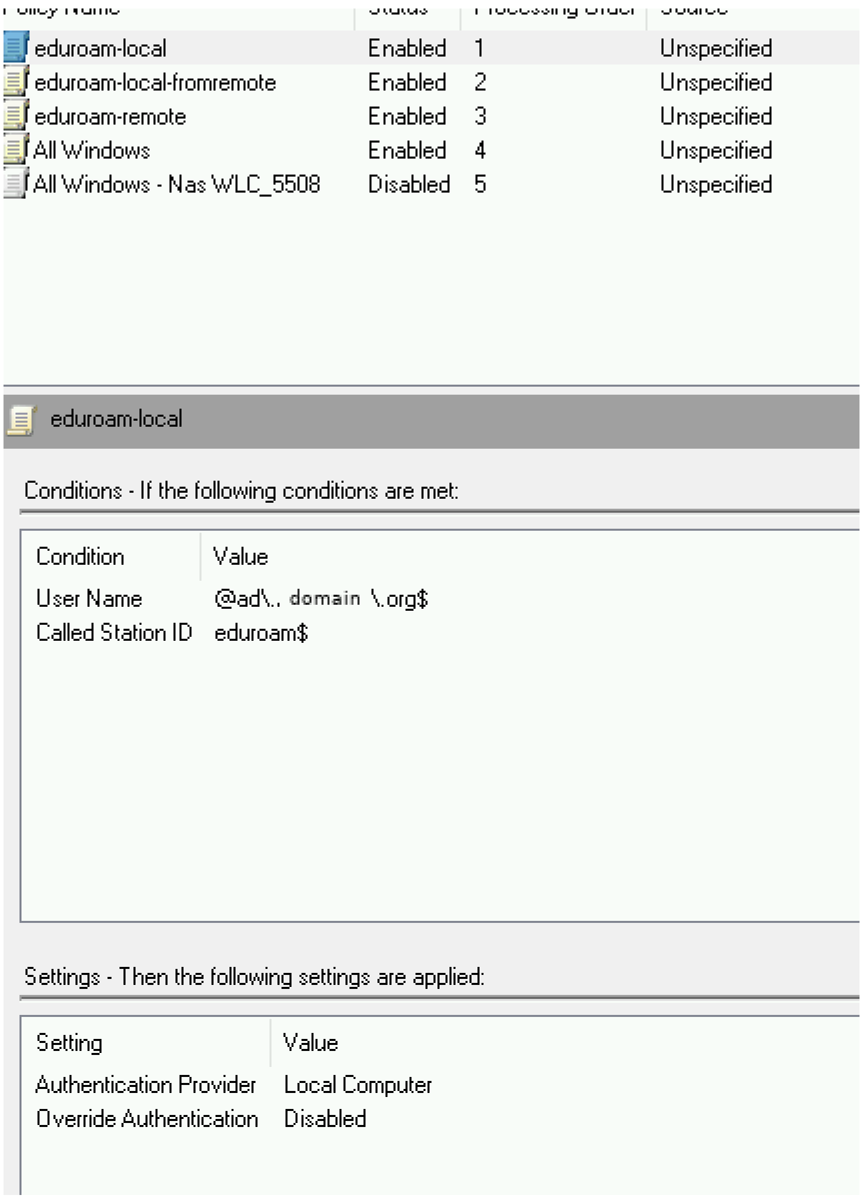
RADIUS Server	Priority	Weight
163.253.31.2	1	50
163.253.30.2	2	50

Step 2 - Policies

This is where things get tricky. If the district already has 802.1x NPS working for their AD users, we need to split off a local user vs a visitor and also determine if that local user is trying to use eduroam ssid.

Connection Request Policies

3 policies are needed to make this work.



Policy Name	Status	Processing Order	Source
eduroam-local	Enabled	1	Unspecified
eduroam-local-fromremote	Enabled	2	Unspecified
eduroam-remote	Enabled	3	Unspecified
All Windows	Enabled	4	Unspecified
All Windows - Nas WLC_5508	Disabled	5	Unspecified

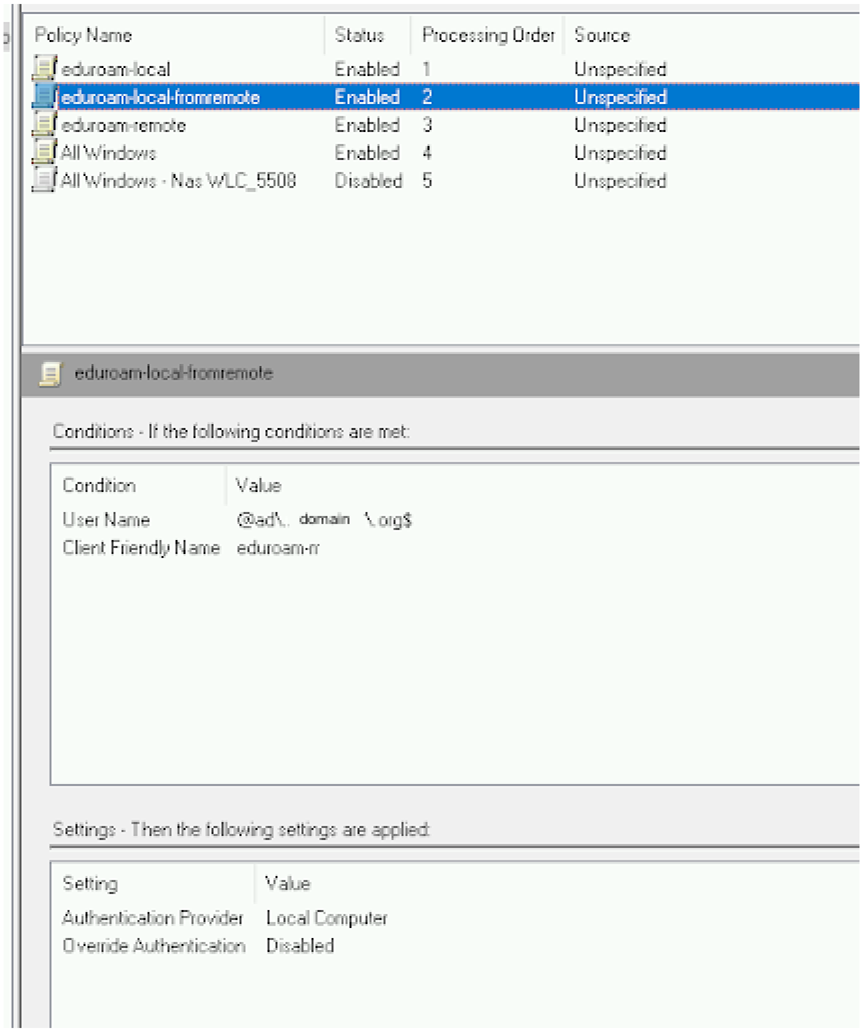
eduroam-local

Conditions - If the following conditions are met:

Condition	Value
User Name	@ad\.. domain \.org$
Called Station ID	eduroam$

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer
Override Authentication	Disabled



Policy Name	Status	Processing Order	Source
eduroam-local	Enabled	1	Unspecified
eduroam-local-fromremote	Enabled	2	Unspecified
eduroam-remote	Enabled	3	Unspecified
All Windows	Enabled	4	Unspecified
All Windows - Nas WLC_5508	Disabled	5	Unspecified

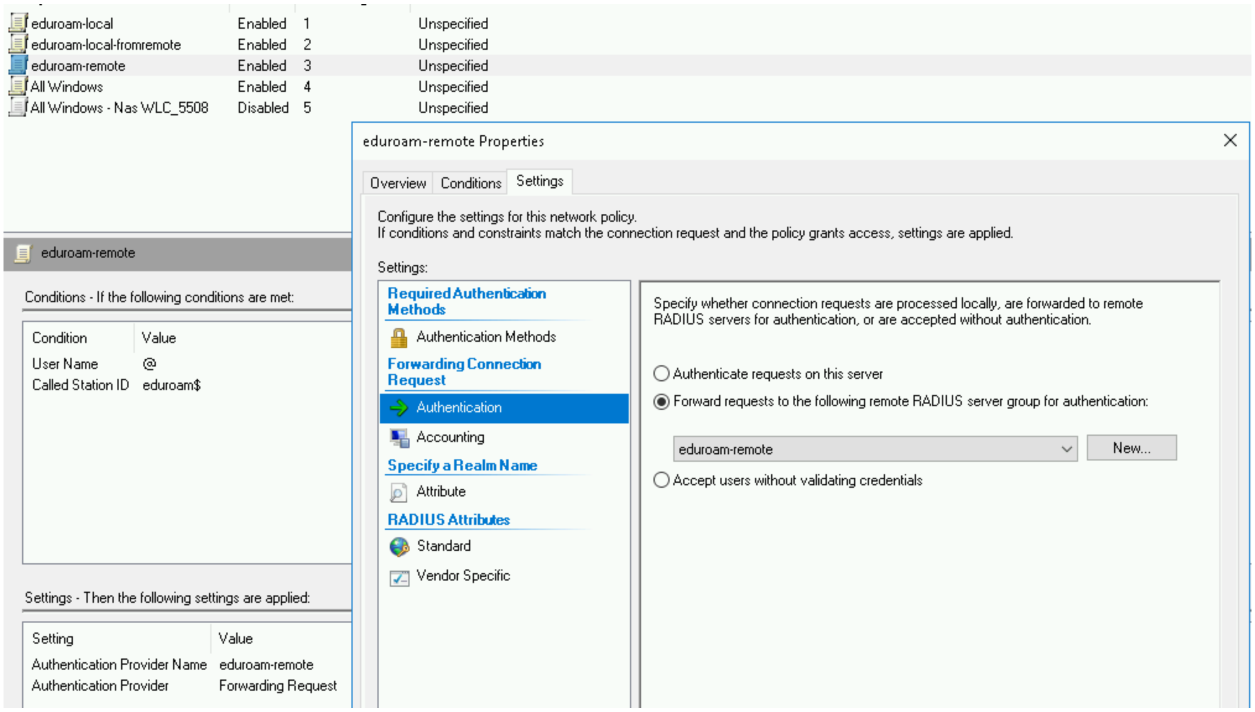
eduroam-local-fromremote

Conditions - If the following conditions are met:

Condition	Value
User Name	@ad\.. domain \.org$
Client Friendly Name	eduroam-r

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer
Override Authentication	Disabled



eduroam-local	Enabled	1	Unspecified
eduroam-local-fromremote	Enabled	2	Unspecified
eduroam-remote	Enabled	3	Unspecified
All Windows	Enabled	4	Unspecified
All Windows - Nas WLC_5508	Disabled	5	Unspecified

eduroam-remote

Conditions - If the following conditions are met:

Condition	Value
User Name	@
Called Station ID	eduroam$

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider Name	eduroam-remote
Authentication Provider	Forwarding Request

eduroam-remote Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

○ Authenticate requests on this server

● Forward requests to the following remote RADIUS server group for authentication:

eduroam-remote

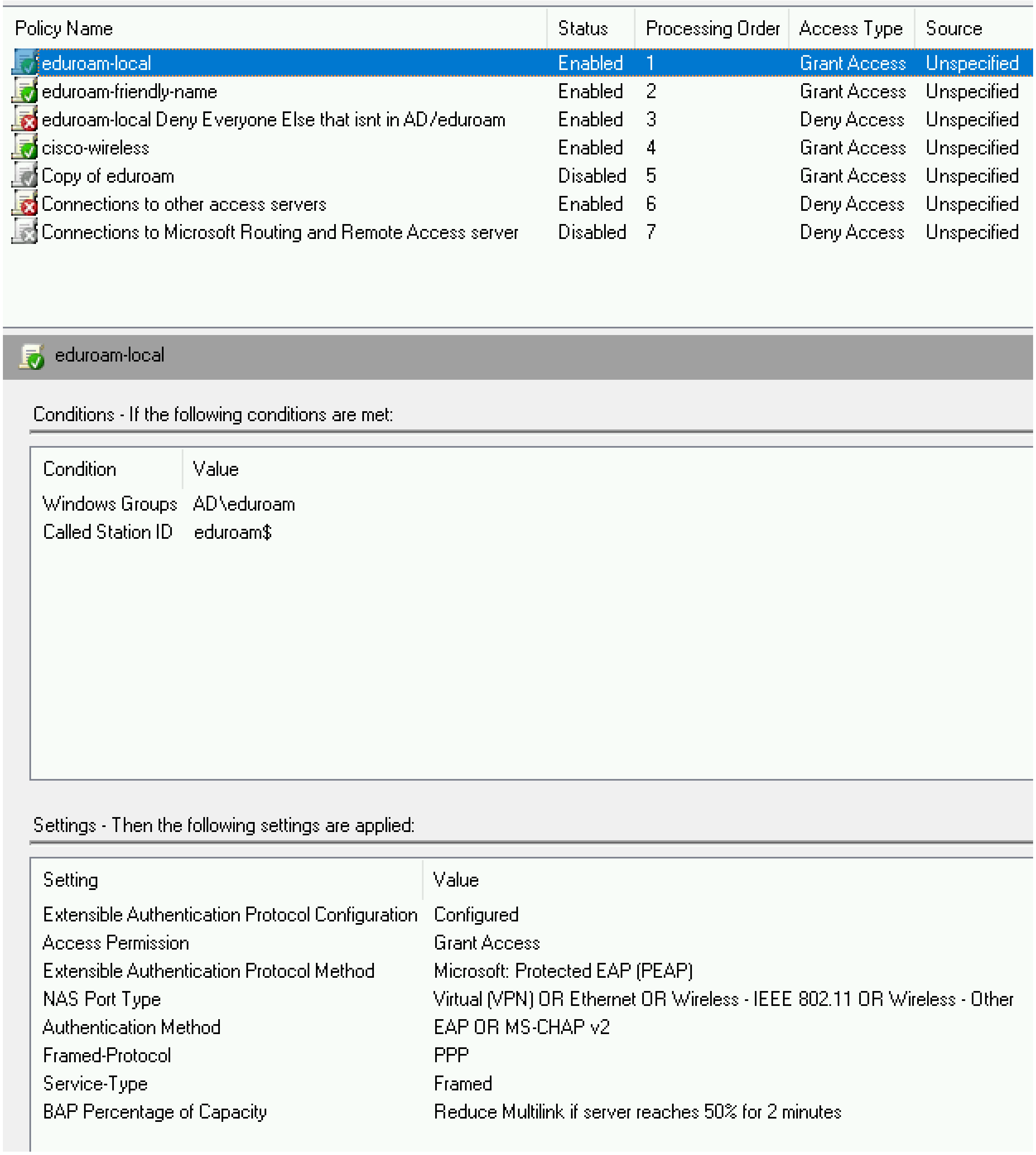
○ Accept users without validating credentials

Network Policies

These need three policies, 2 to allow and 1 to deny. We want to say only members of eduroam on AD are allowed to access eduroam SSID. So first we need to grant eduroam users, then deny.

You will need to make sure you have a valid certificate to use for mschapv2 and 802.1x to use. This doc won’t go into that, google search that.

Eduroam-local and eduroam-friendly-name are similar.



Policy Name	Status	Processing Order	Access Type	Source
eduroam-local	Enabled	1	Grant Access	Unspecified
eduroam-friendly-name	Enabled	2	Grant Access	Unspecified
eduroam-local Deny Everyone Else that isnt in AD/eduroam	Enabled	3	Deny Access	Unspecified
cisco-wireless	Enabled	4	Grant Access	Unspecified
Copy of eduroam	Disabled	5	Grant Access	Unspecified
Connections to other access servers	Enabled	6	Deny Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Disabled	7	Deny Access	Unspecified

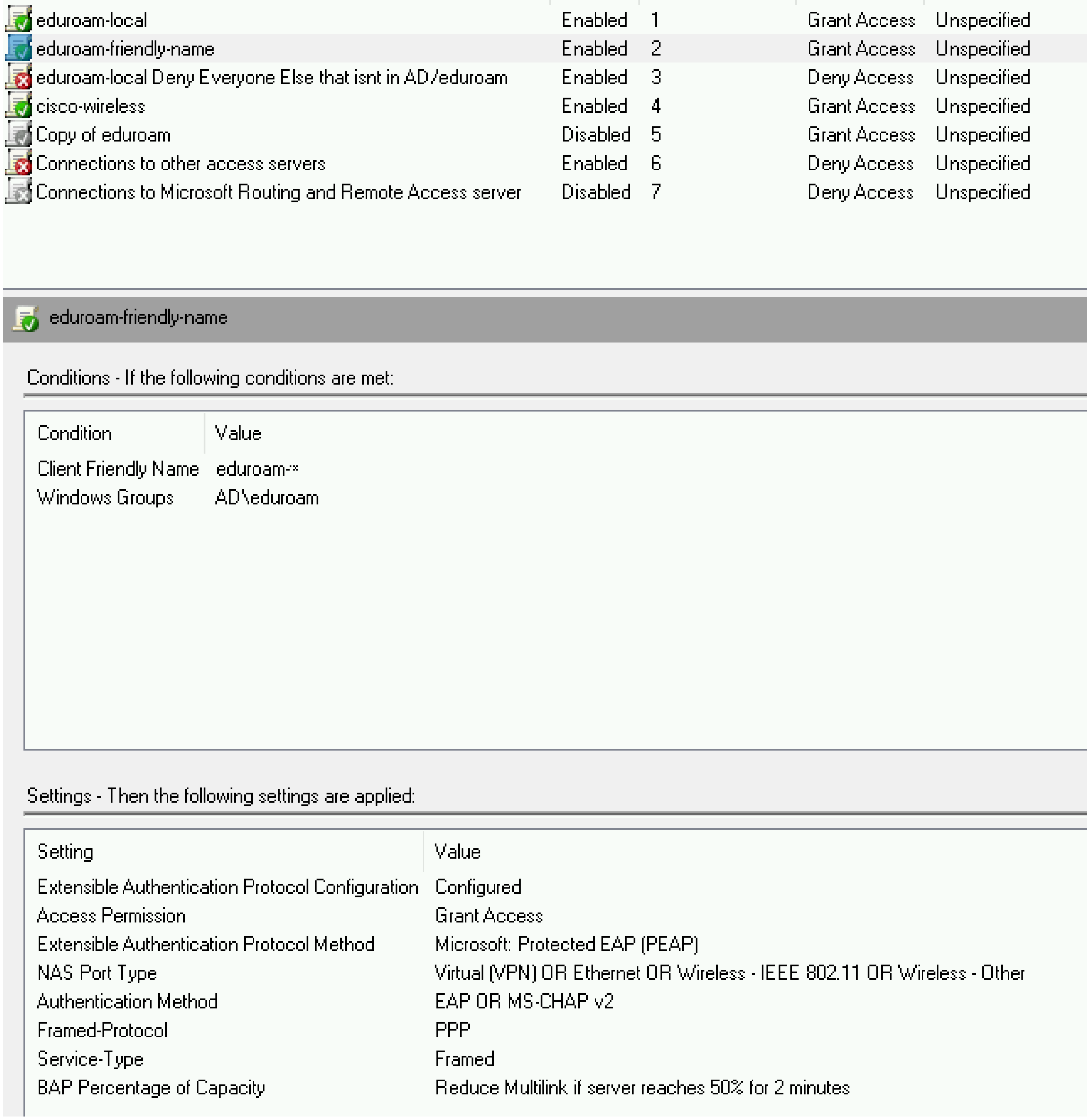
eduroam-local

Conditions - If the following conditions are met:

Condition	Value
Windows Groups	AD\eduroam
Called Station ID	eduroam$

Settings - Then the following settings are applied:

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Virtual (VPN) OR Ethernet OR Wireless - IEEE 802.11 OR Wireless - Other
Authentication Method	EAP OR MS-CHAP v2
Framed-Protocol	PPP
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes



eduroam-local	Enabled	1	Grant Access	Unspecified
eduroam-friendly-name	Enabled	2	Grant Access	Unspecified
eduroam-local Deny Everyone Else that isnt in AD/eduroam	Enabled	3	Deny Access	Unspecified
cisco-wireless	Enabled	4	Grant Access	Unspecified
Copy of eduroam	Disabled	5	Grant Access	Unspecified
Connections to other access servers	Enabled	6	Deny Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Disabled	7	Deny Access	Unspecified

eduroam-friendly-name

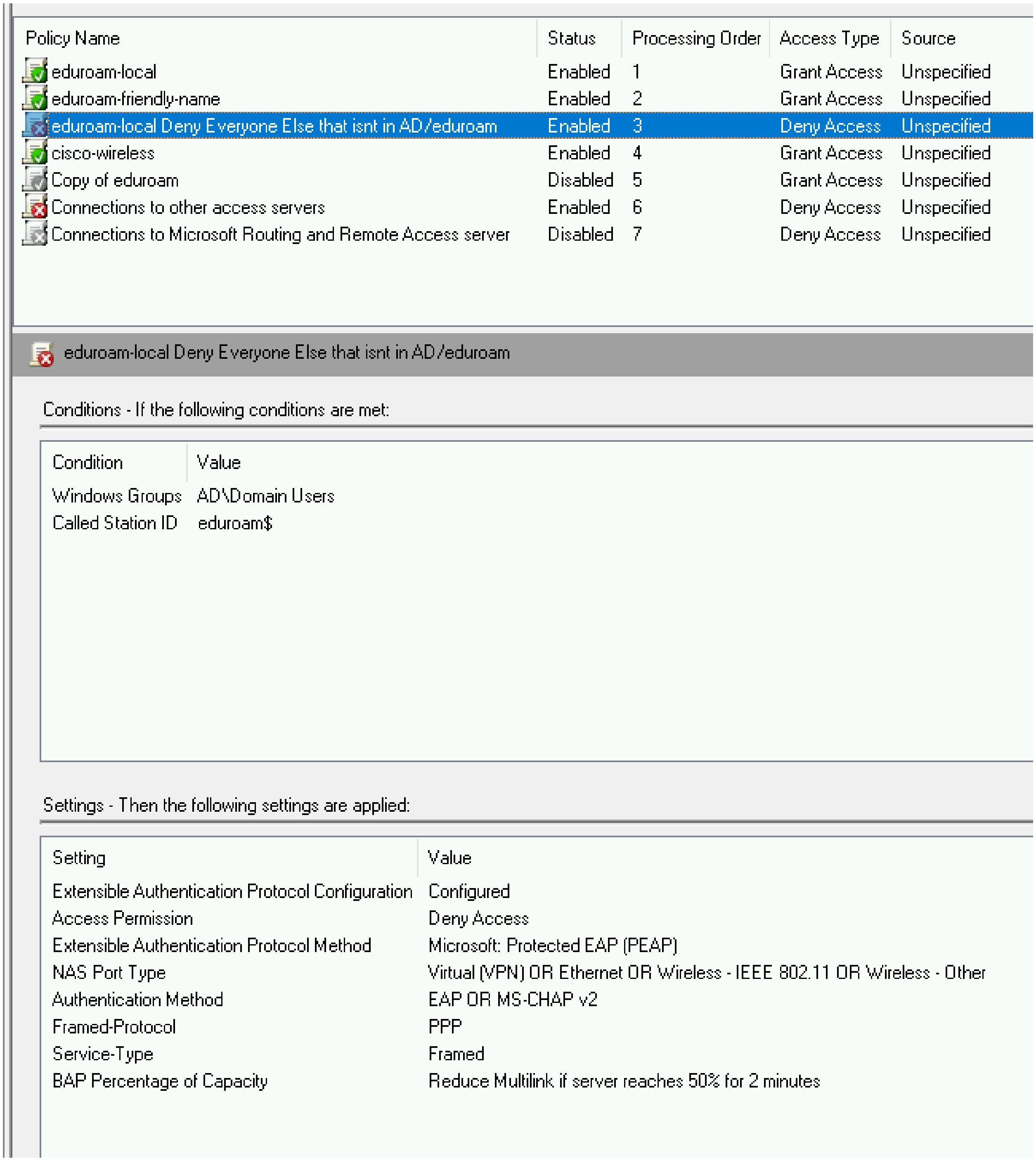
Conditions - If the following conditions are met:

Condition	Value
Client Friendly Name	eduroam-*
Windows Groups	AD\eduroam

Settings - Then the following settings are applied:

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Virtual (VPN) OR Ethernet OR Wireless - IEEE 802.11 OR Wireless - Other
Authentication Method	EAP OR MS-CHAP v2
Framed-Protocol	PPP
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

With denying, its checking only AD\Domain users, everyone is assigned to that group, where before the two policies were looking for an eduroam group, so if it didn't pass the first two policies it will go to this deny policy and if you connect to eduroam with a Domain users group, you’ll get a deny.



Policy Name	Status	Processing Order	Access Type	Source
eduroam-local	Enabled	1	Grant Access	Unspecified
eduroam-friendly-name	Enabled	2	Grant Access	Unspecified
eduroam-local Deny Everyone Else that isnt in AD/eduroam	Enabled	3	Deny Access	Unspecified
cisco-wireless	Enabled	4	Grant Access	Unspecified
Copy of eduroam	Disabled	5	Grant Access	Unspecified
Connections to other access servers	Enabled	6	Deny Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Disabled	7	Deny Access	Unspecified

eduroam-local Deny Everyone Else that isnt in AD/eduroam

Conditions - If the following conditions are met:

Condition	Value
Windows Groups	AD\Domain Users
Called Station ID	eduroam$

Settings - Then the following settings are applied:

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Access Permission	Deny Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Virtual (VPN) OR Ethernet OR Wireless - IEEE 802.11 OR Wireless - Other
Authentication Method	EAP OR MS-CHAP v2
Framed-Protocol	PPP
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

The cisco-wireless looks for the client friendly name and grants access to Domain Users to those SSID’s on the network but eduroam is restricted which is what we want.