Authenticating Aruba Instant ON clients against Microsoft Windows 2016 Server NPS

aruba
a Hewlett Packard Enterprise company

Motivation

1. Quick and ”dirty” demo how to integrate Microsoft NPS and Aruba Instant ON for SMB customers
2. As it would be expected that SMB customers will not have dedicated network and security personnel (or separate AAA infrastructure) this should be enough to allow them to integrate AIO with existing MS AD.

Tested environment

–Microsoft Windows Server W2016

–Aruba Instant ON (AP11, AP12), SW version 1.4.1

–W10, iPhone 6S (iOS 13.3.1), iPad mini (iOS 9.3.5), MacBook (10.15.3)

–For demo purposes W2016 trial (180 days) can be downloaded here

Typical Topology

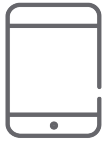
MS W2016
AD with NPS
192.168.1.66
MicroServer G10

Office Connect
1950 switch

Aruba Instant ON
DRP 192.168.1.13

Wireless Clients

Smart Phone



Tablet

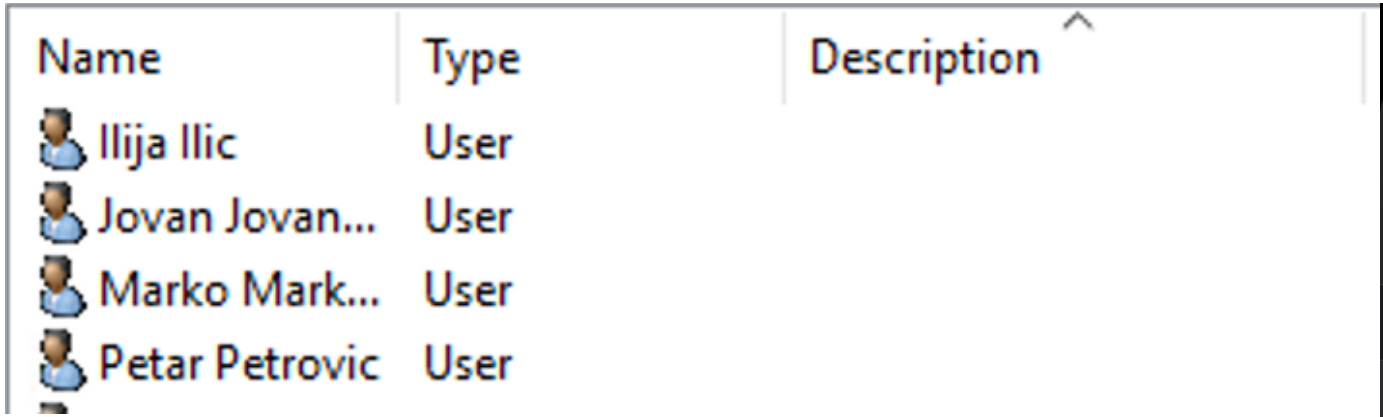
Laptop

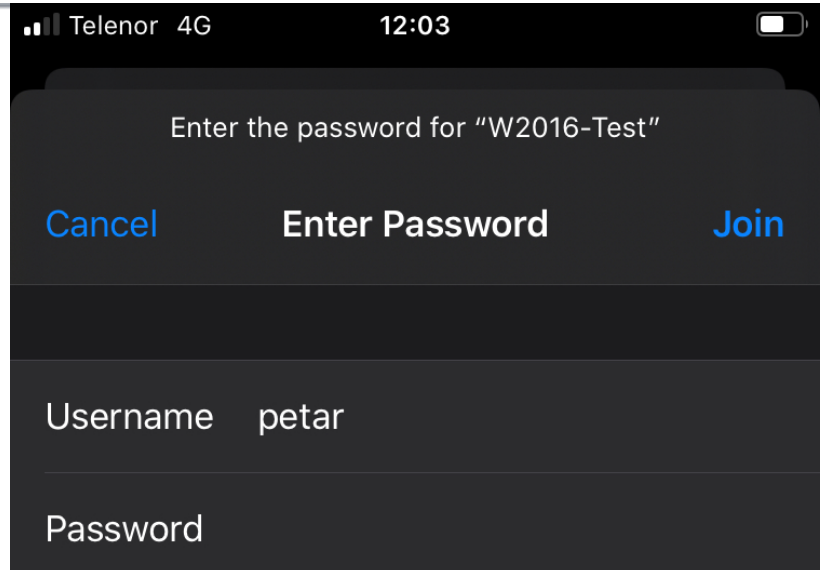
Wired Clients

aruba
a Hewlett Packard
Enterprise company

Use case

– Every client is authenticated against AD user database prior to connecting to Wi-Fi network. In case that user leaves company (removed in AD), access to the network is also forbidden. This can increase security in SMB environment without additional investments.

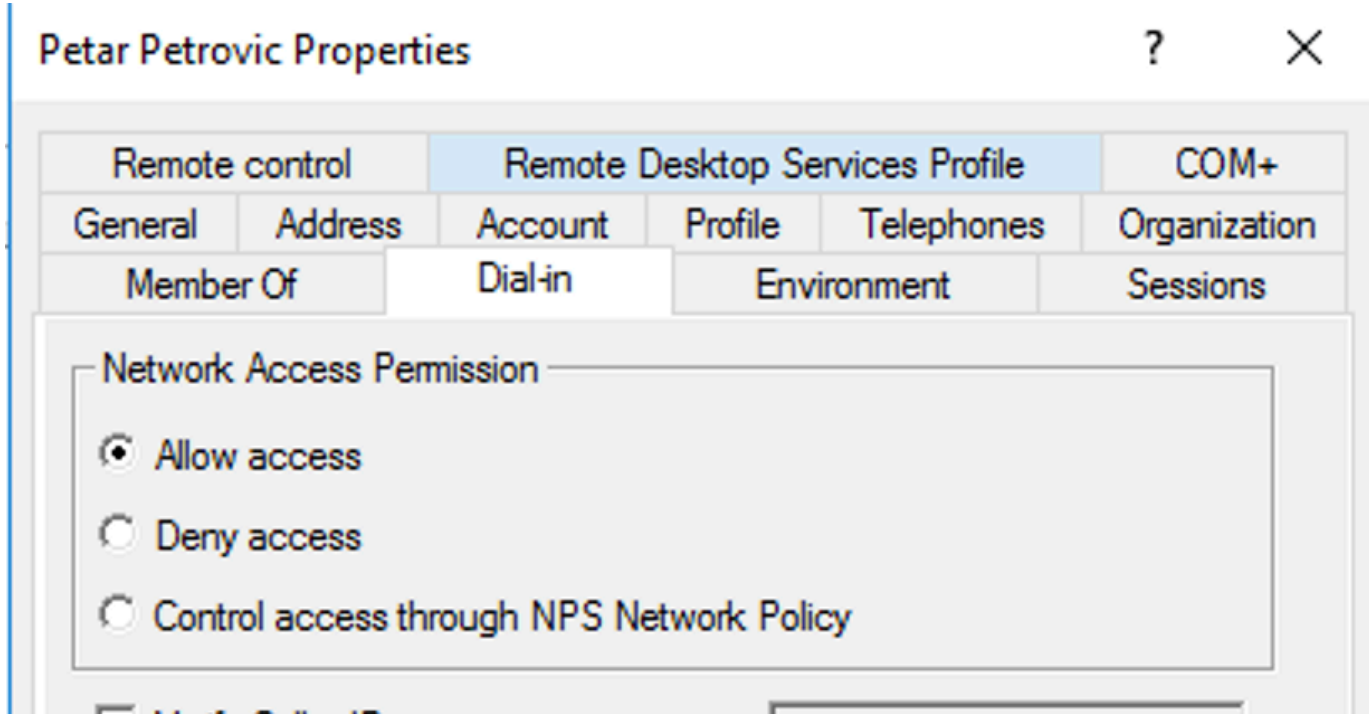




aruba
a Hewlett Packard Enterprise company

Use case (cntd.)

Also, access to the network can be controlled per AD user basis (permit/allow) or by network service policy



Pre- requisites:

– Administrative access to AD

– Free IP address representing AIO cluster (if you will be using Radius Dynamic Proxy - that is Single IP for all APs in AIO cluster) – in our example 192.168.1.13

– Windows Server IP address (192.168.1.66 in our example)

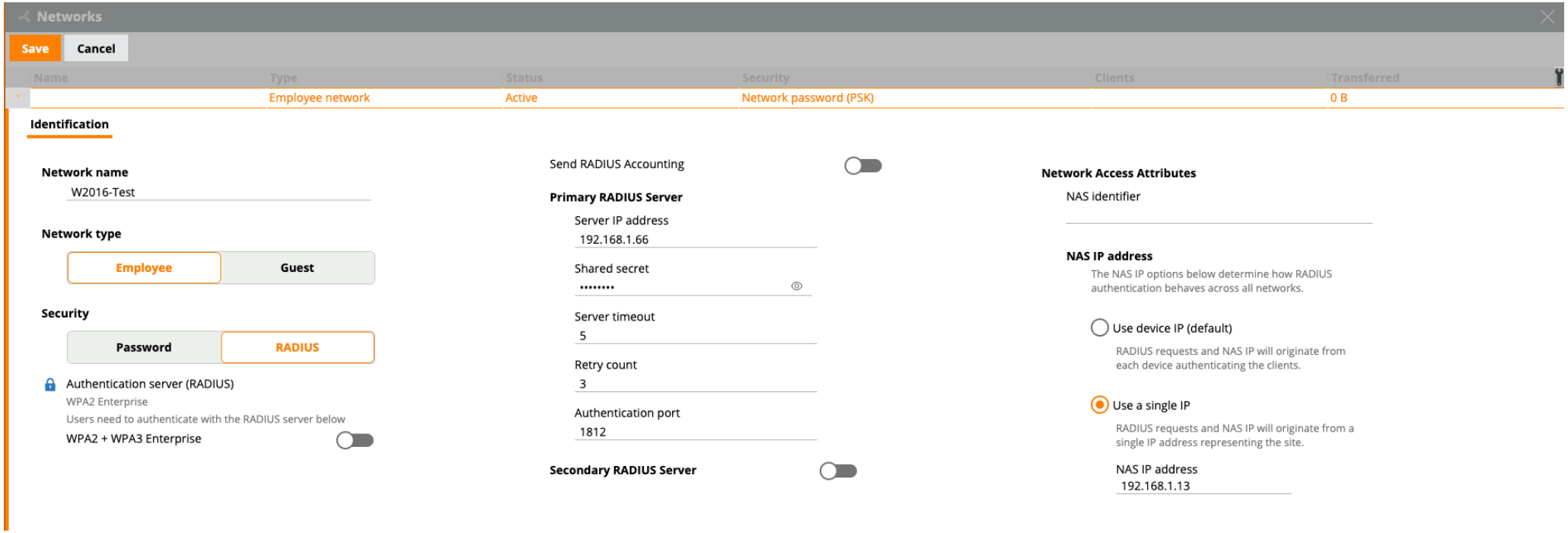
– RADIUS Secret – password that will be protecting communication between NAD (AIO) and RADIUS Server (NPS).

– cca. 90 minutes of time

Aruba Instant On configuration

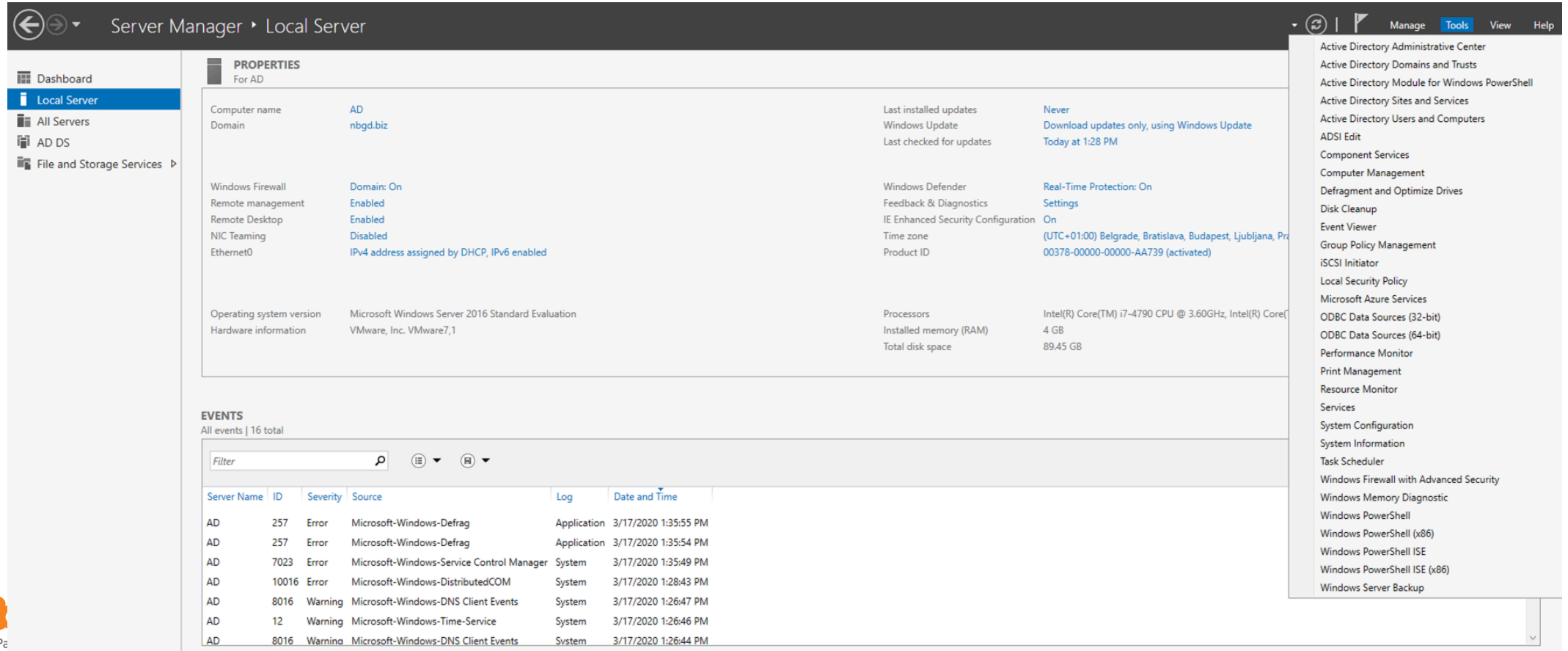
– Login to portal.arubainstanton.com

– Create New network (Networks -> Add) with bellow (or similar) parameters:



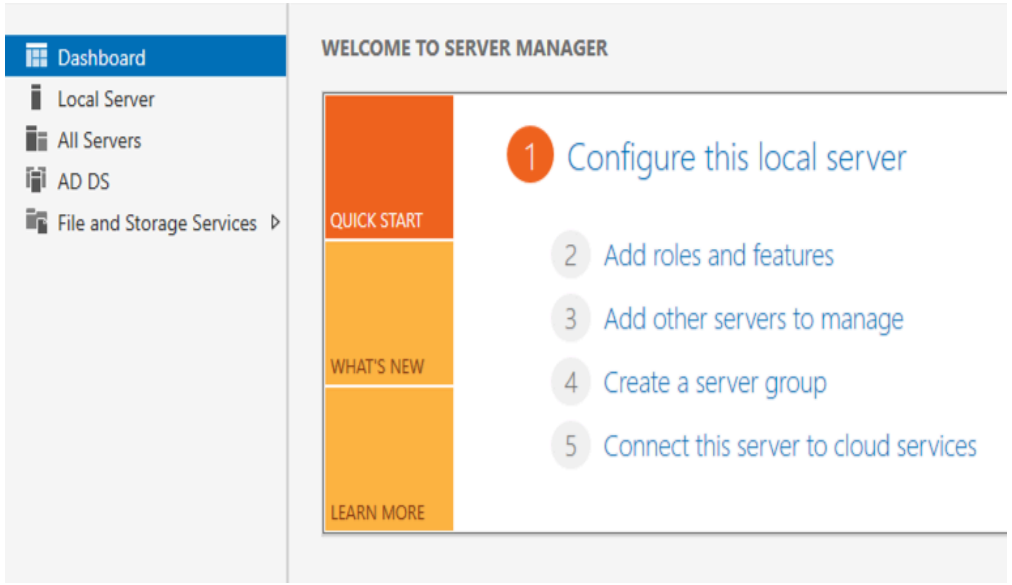
NPS Configuration

– Check if Network Policy Server Feature is installed on your Server. In below case, it is not (not in the list, when you expand ‘Tools’).

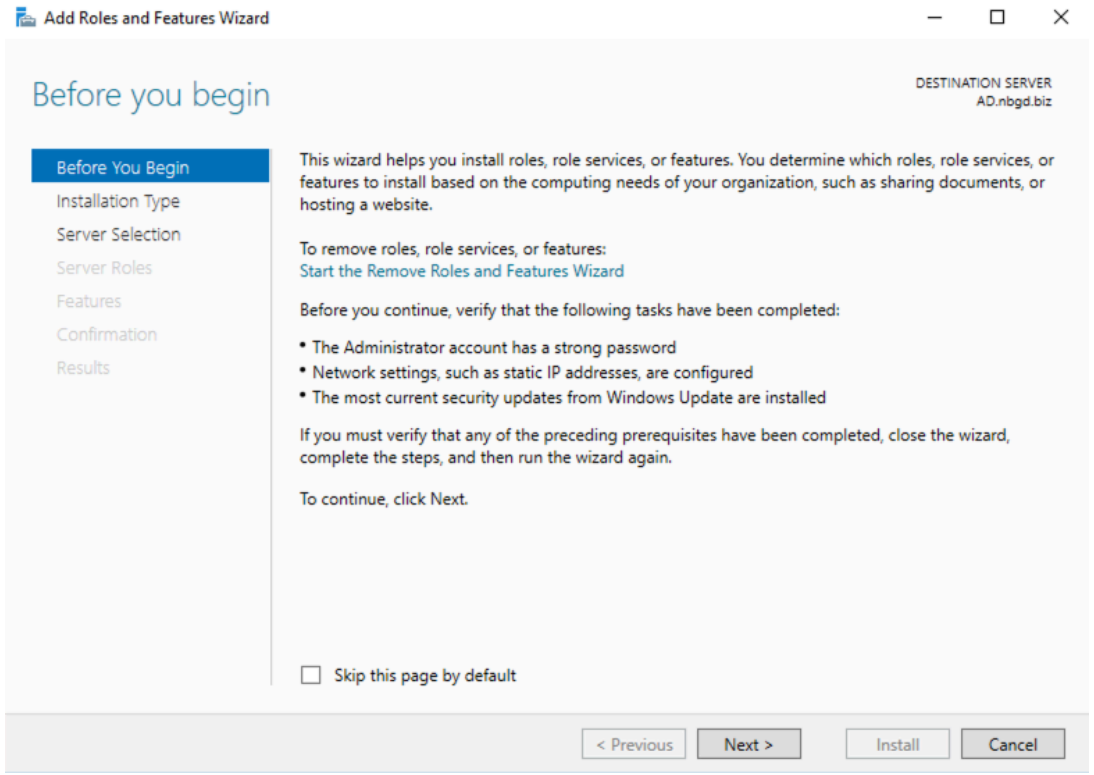


In case there is no NPS installed, add NPS role to the server :

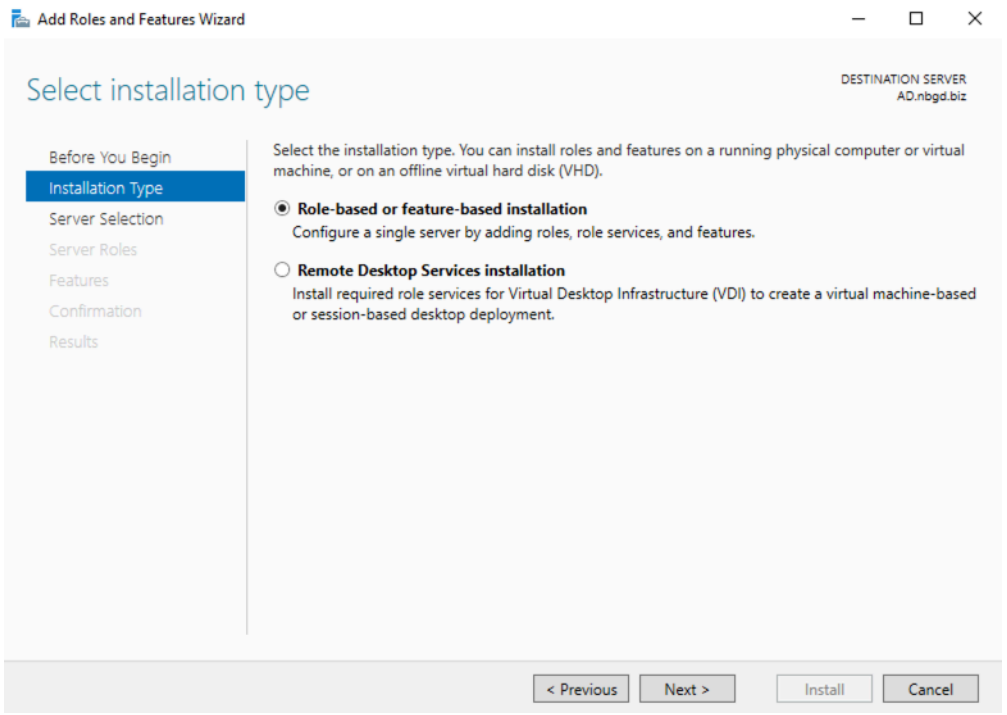
– Go to Server Management, Dashboard

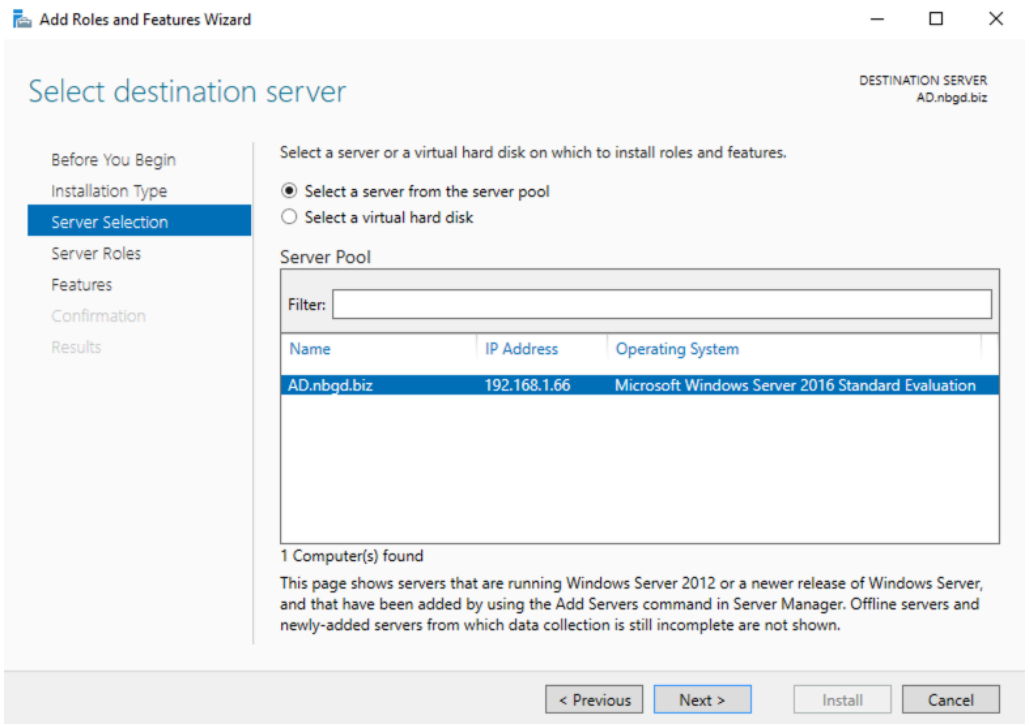


• Add Roles and Features

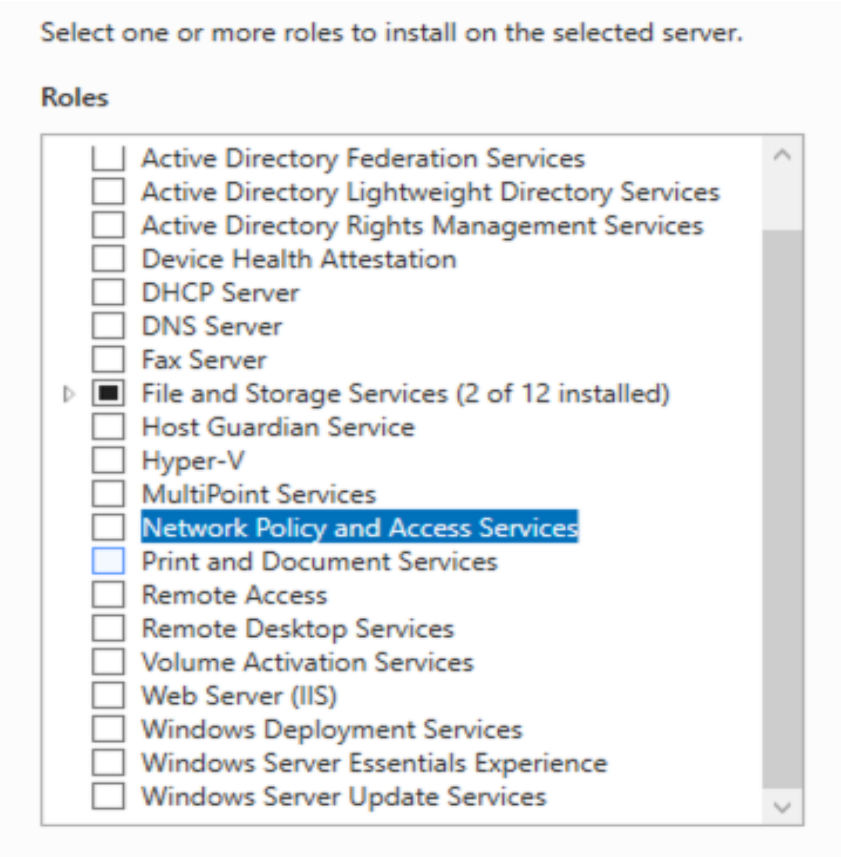


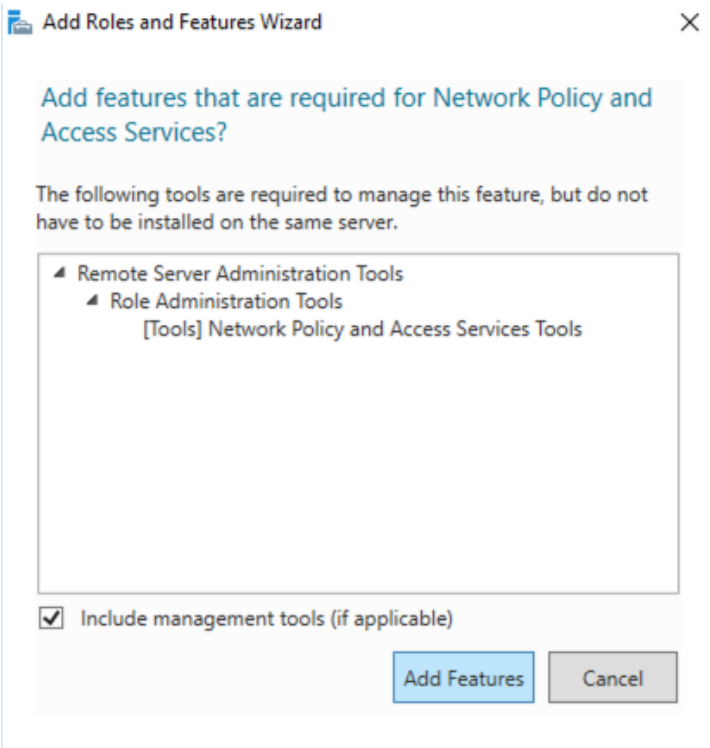
Add NPS (cntd.)


Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
AD.nbgd.biz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

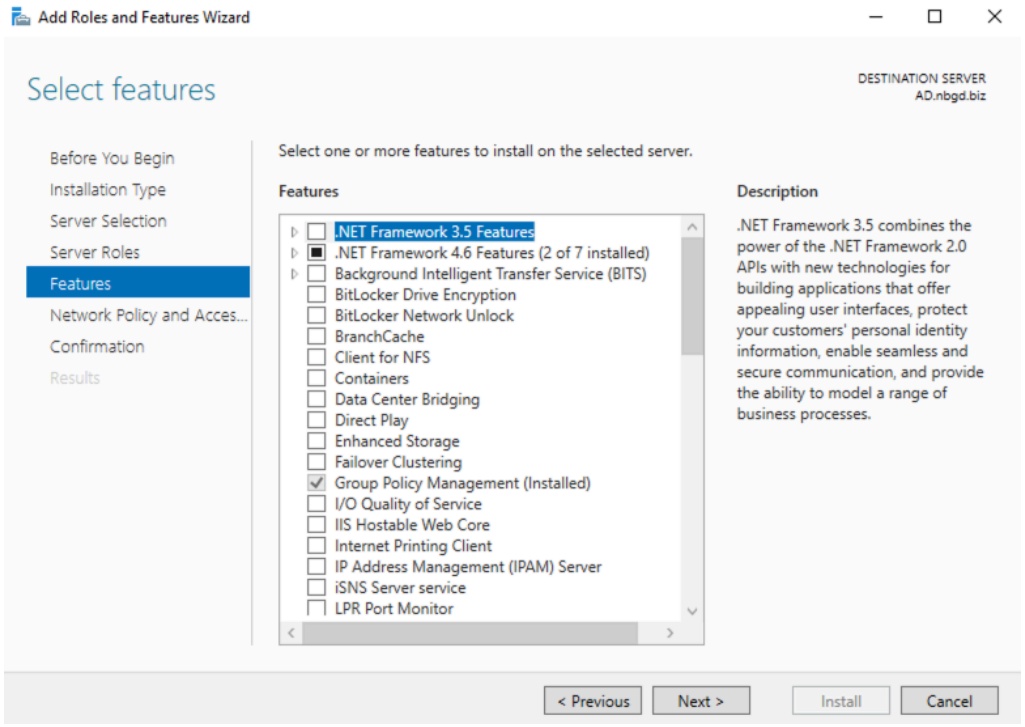

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
AD.nbgd.biz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
AD.nbgd.biz
192.168.1.66
Microsoft Windows Server 2016 Standard Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

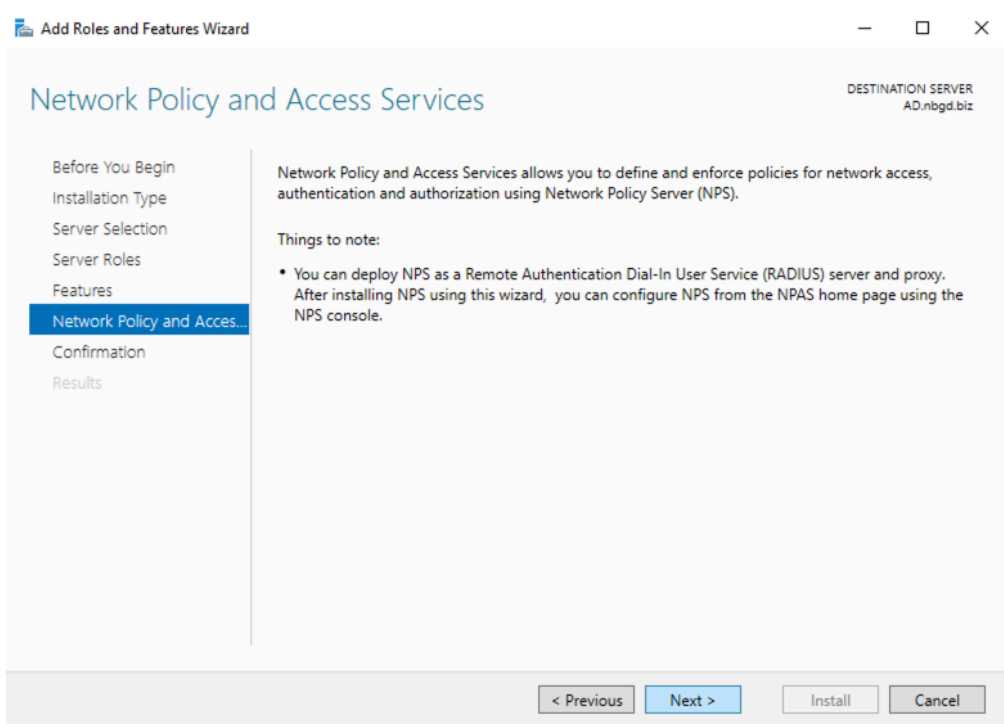
Add NPS (cntd.) – select NPS and pending tools





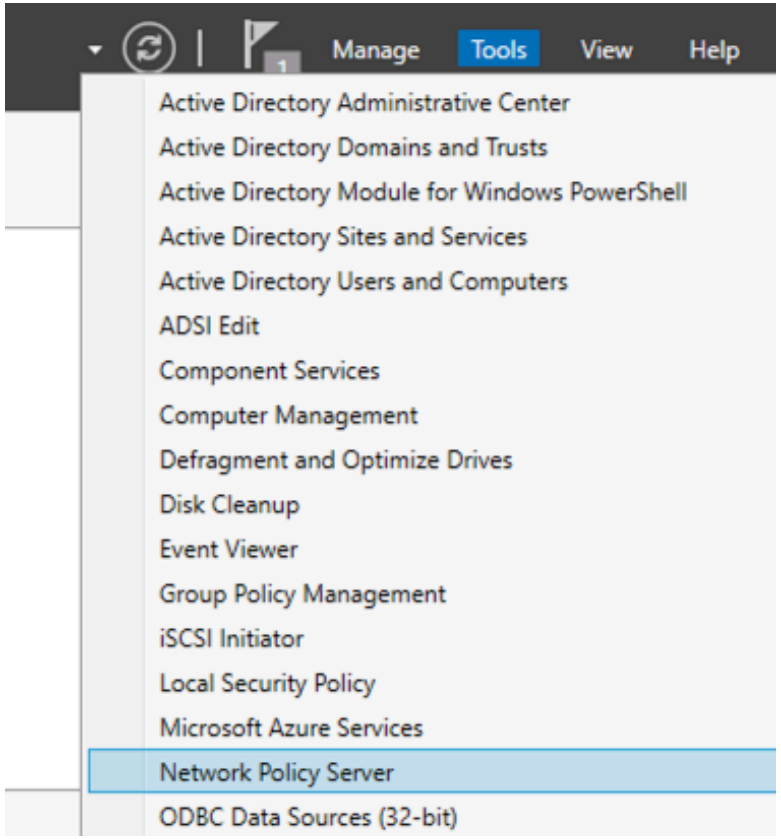
Add NPS (cntd.) – Skip Feature selection, Finish wizard



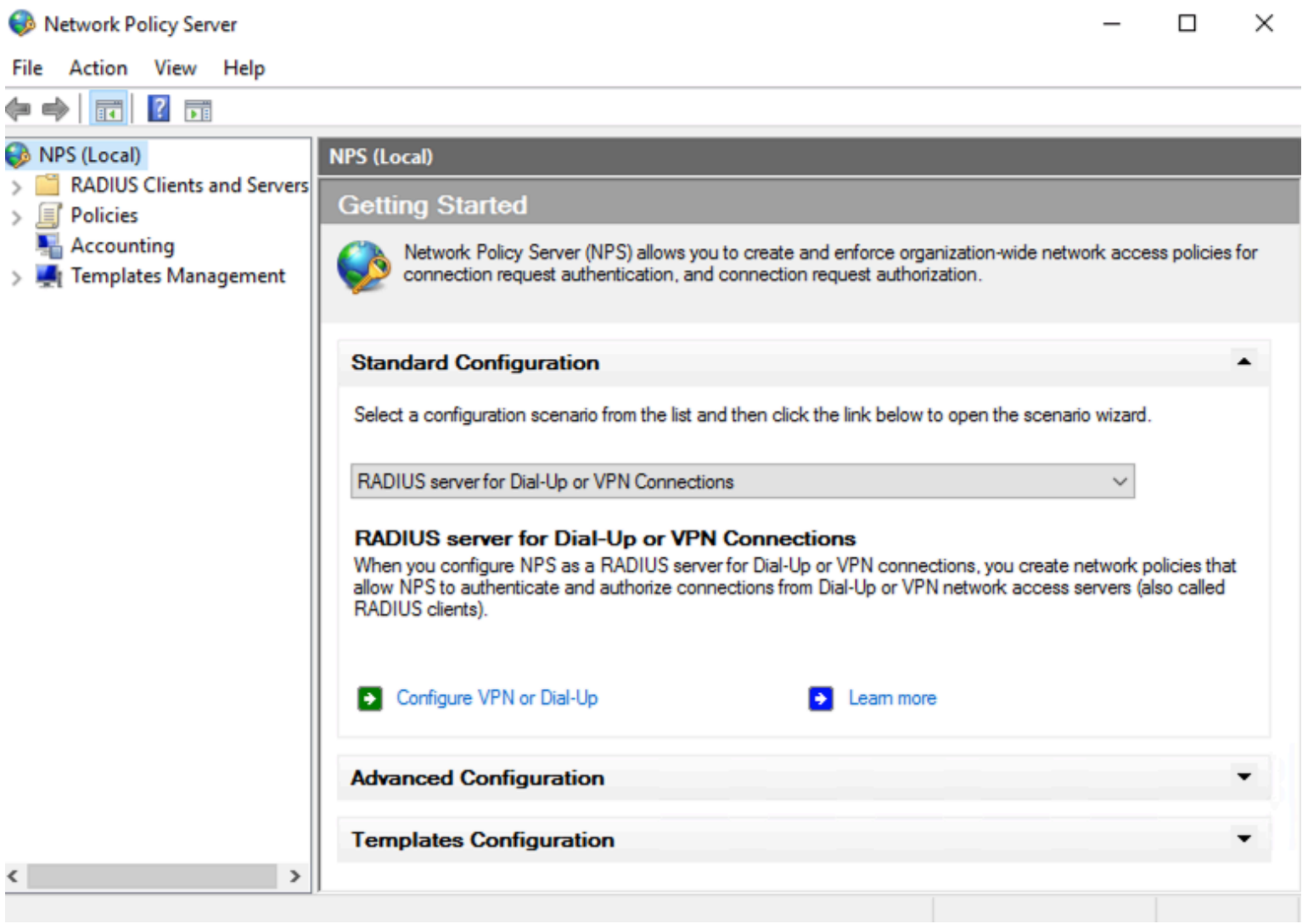


Check if NPS is available

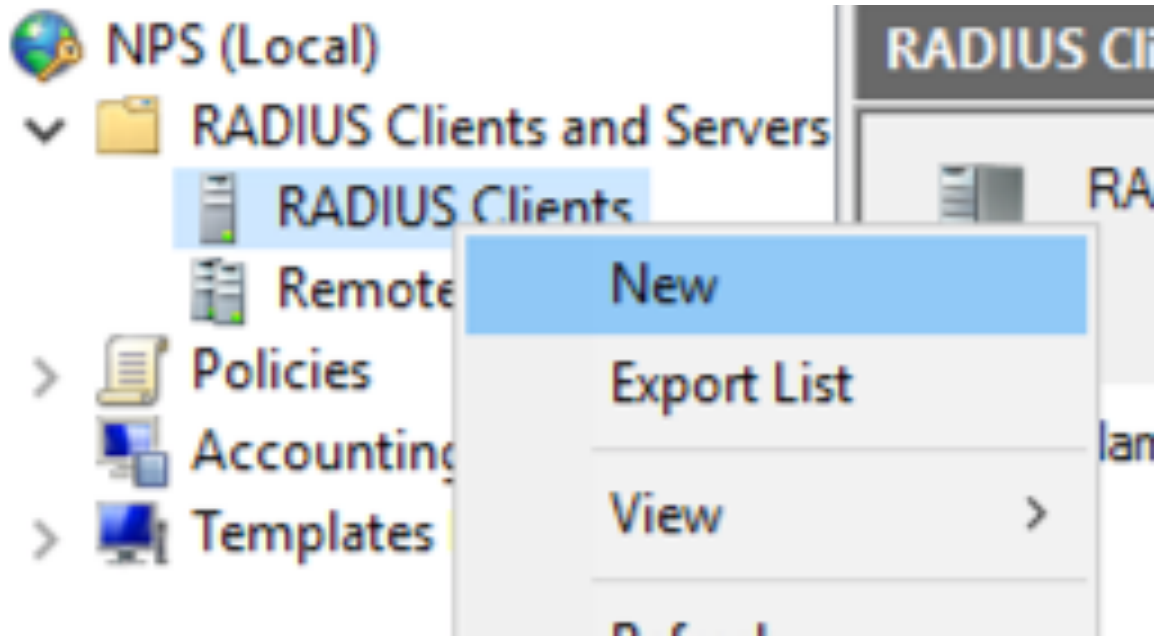
– It will take few minutes to add NPS role to server – after that NPS should be available in Dashboard Tool selector



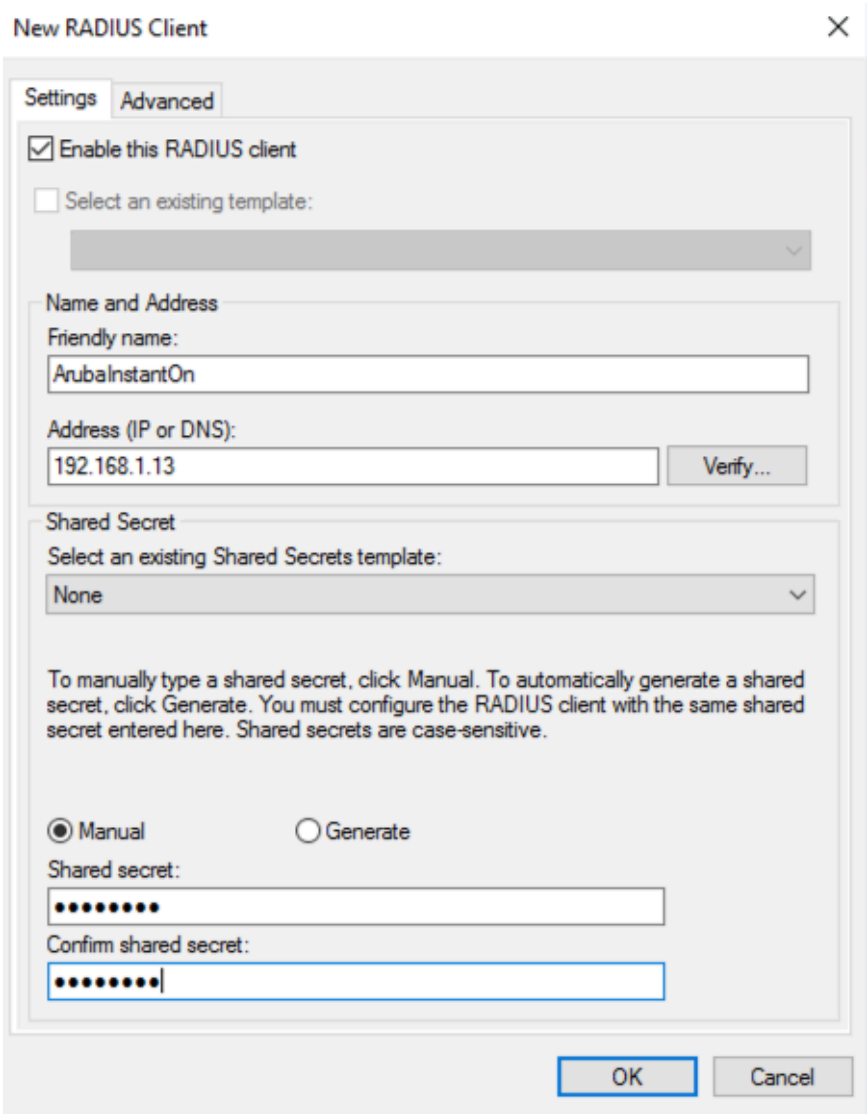
Open Network Policy Server Console



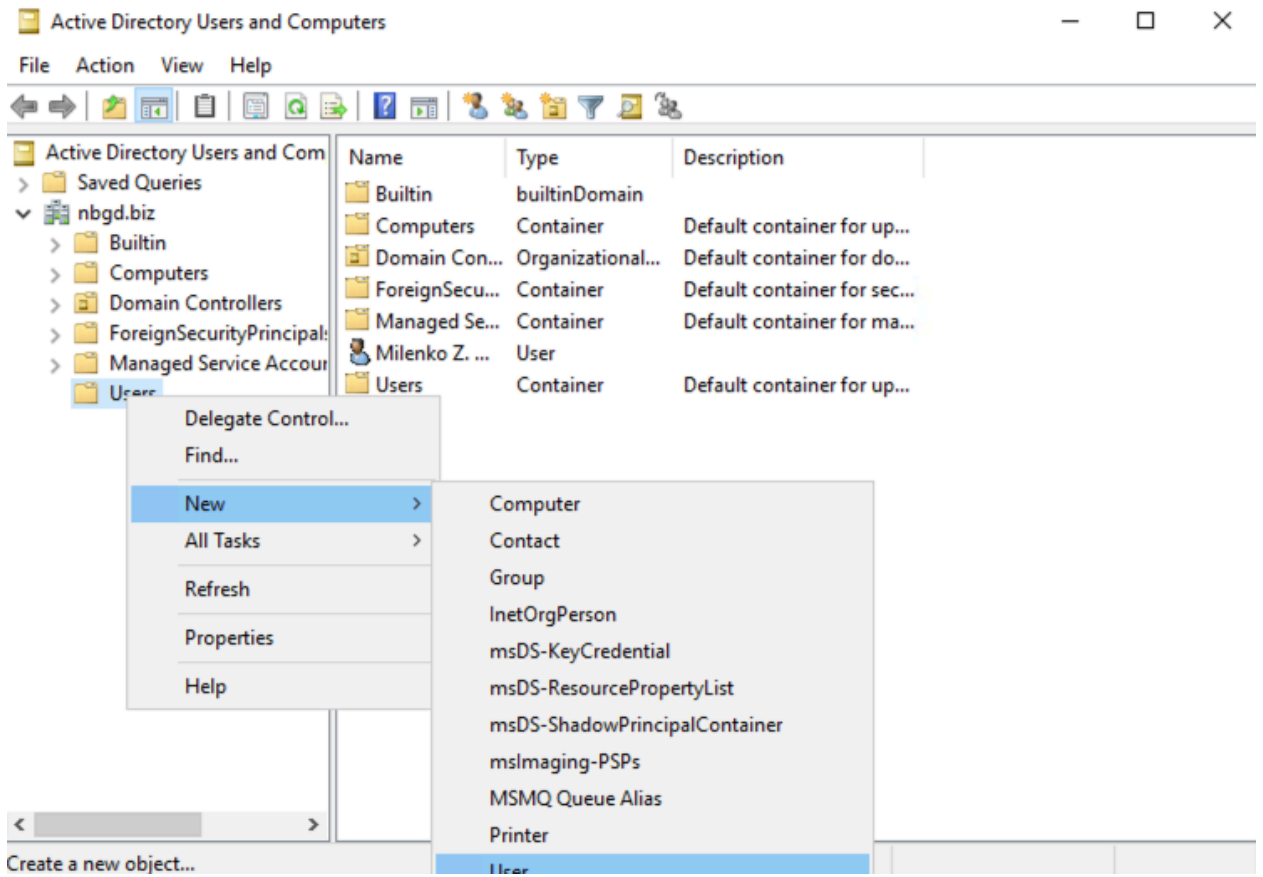
Add new Client (NAD/NAS device) by right clicking on Radius Client:



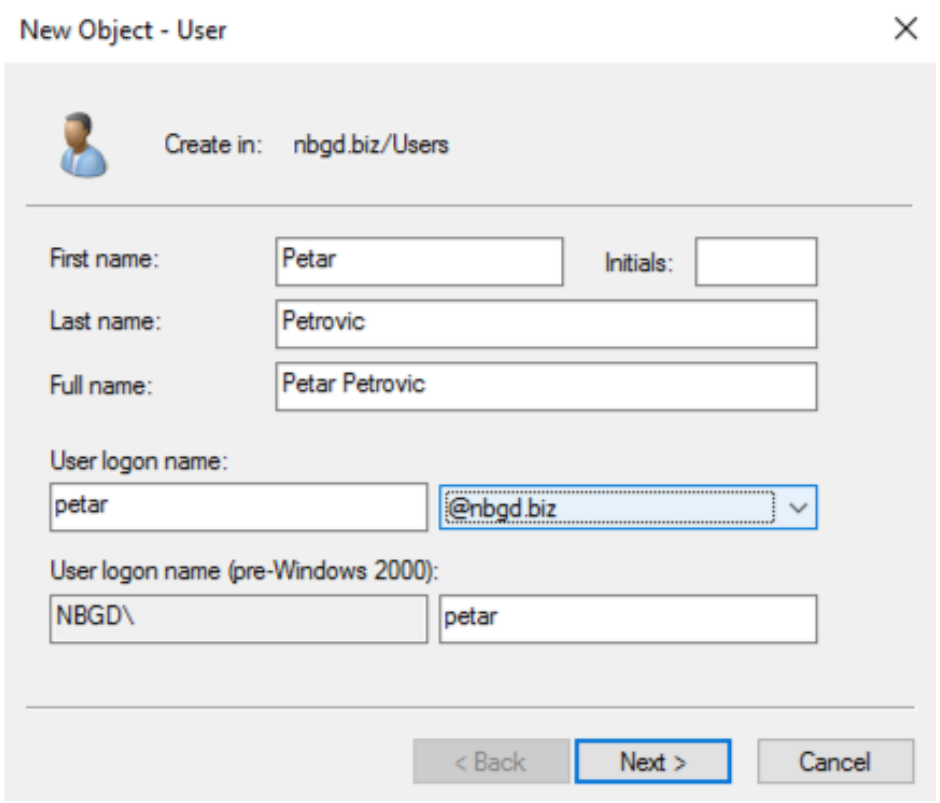
Fill in required Parameters (Name, IP Address and Shared secret)

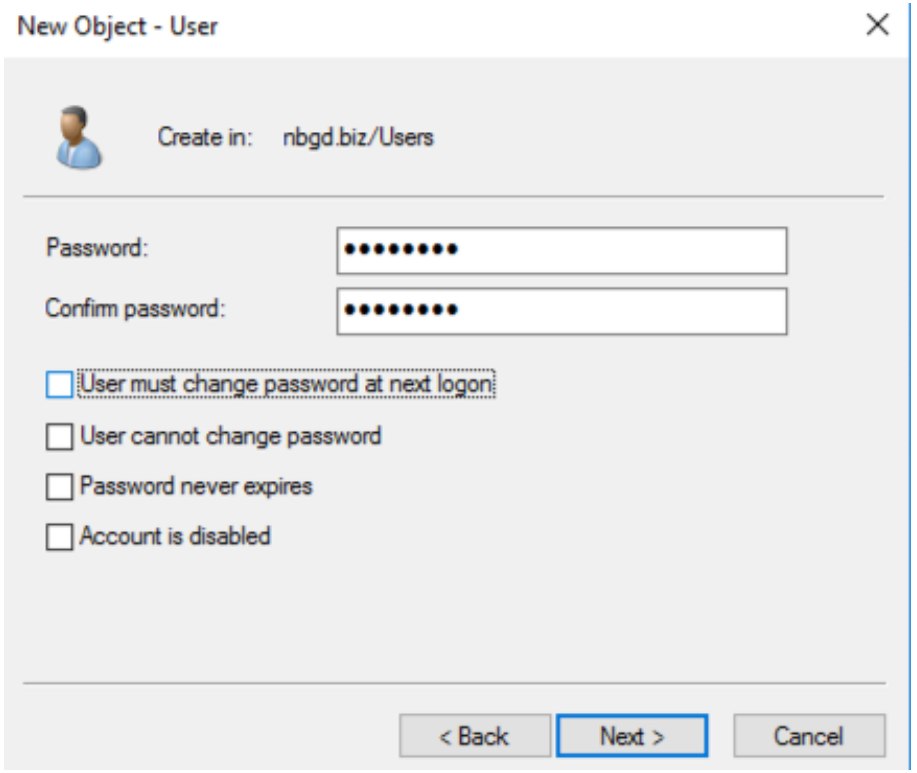


Add test user by going Server Manager, Dashboard, Tools, Active Directory Users and Computers :

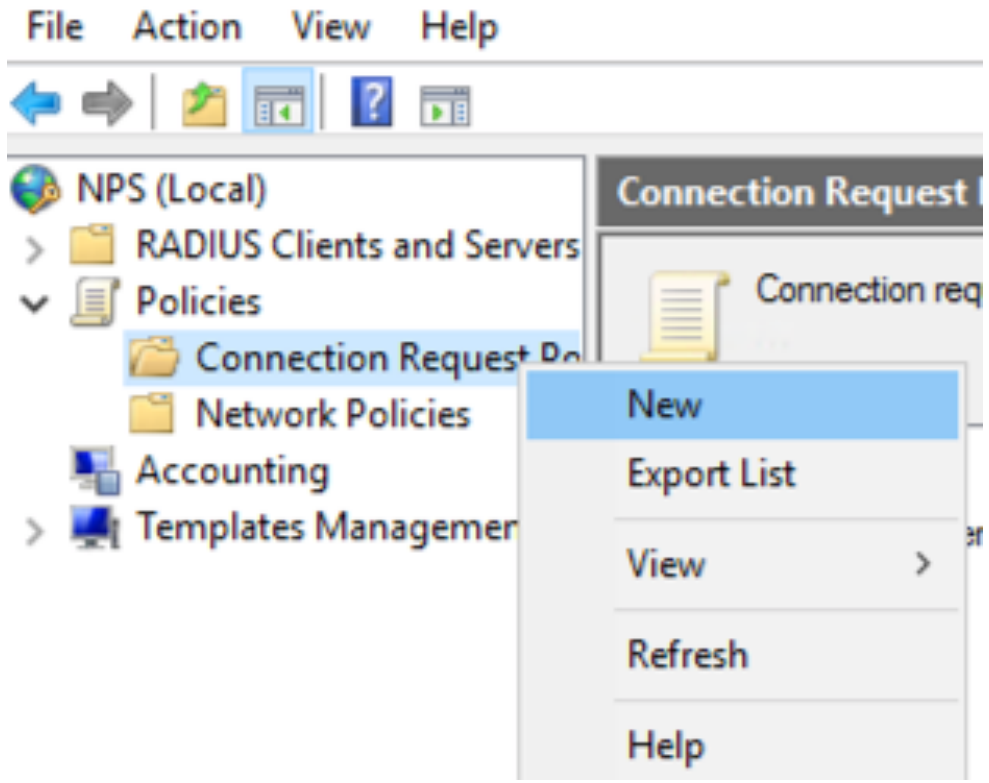


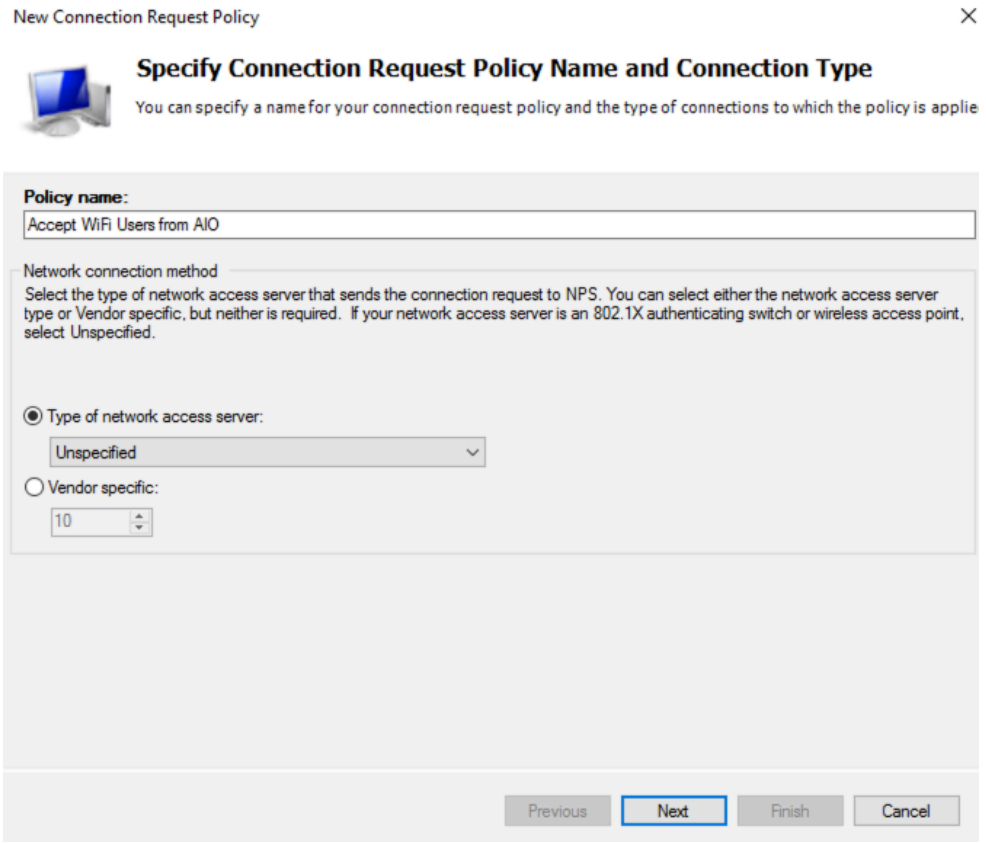
Add new user:


New Object - User
Create in: nbgd.biz/Users
First name:
Petar
Initials:
Last name:
Petrovic
Full name:
Petar Petrovic
User logon name:
petar
@nbgd.biz
User logon name (pre-Windows 2000):
NBGD\
petar
< Back
Next >
Cancel

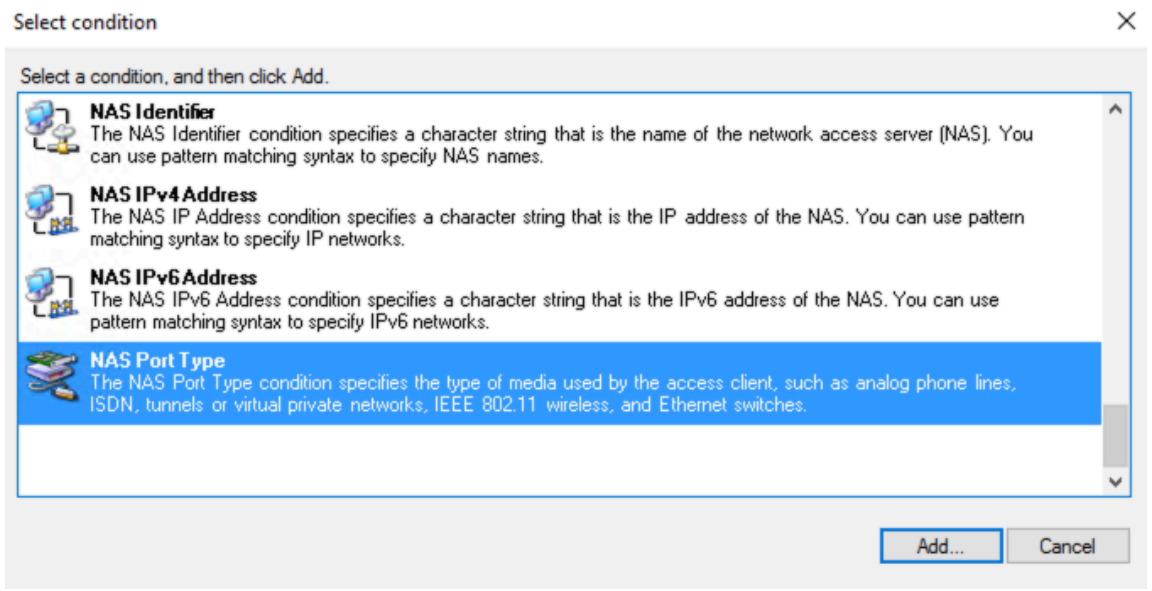

New Object - User
Create in: nbgd.biz/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel

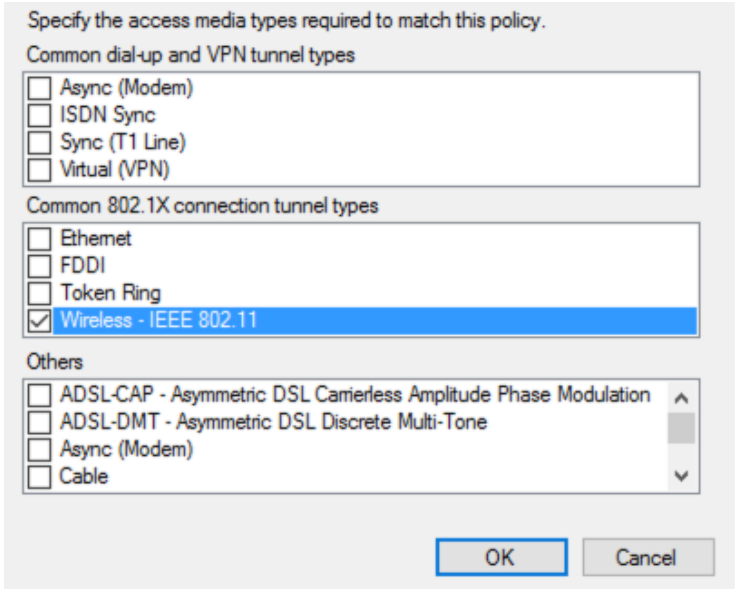
Go back to NPS and create new Network Policy, give it a name



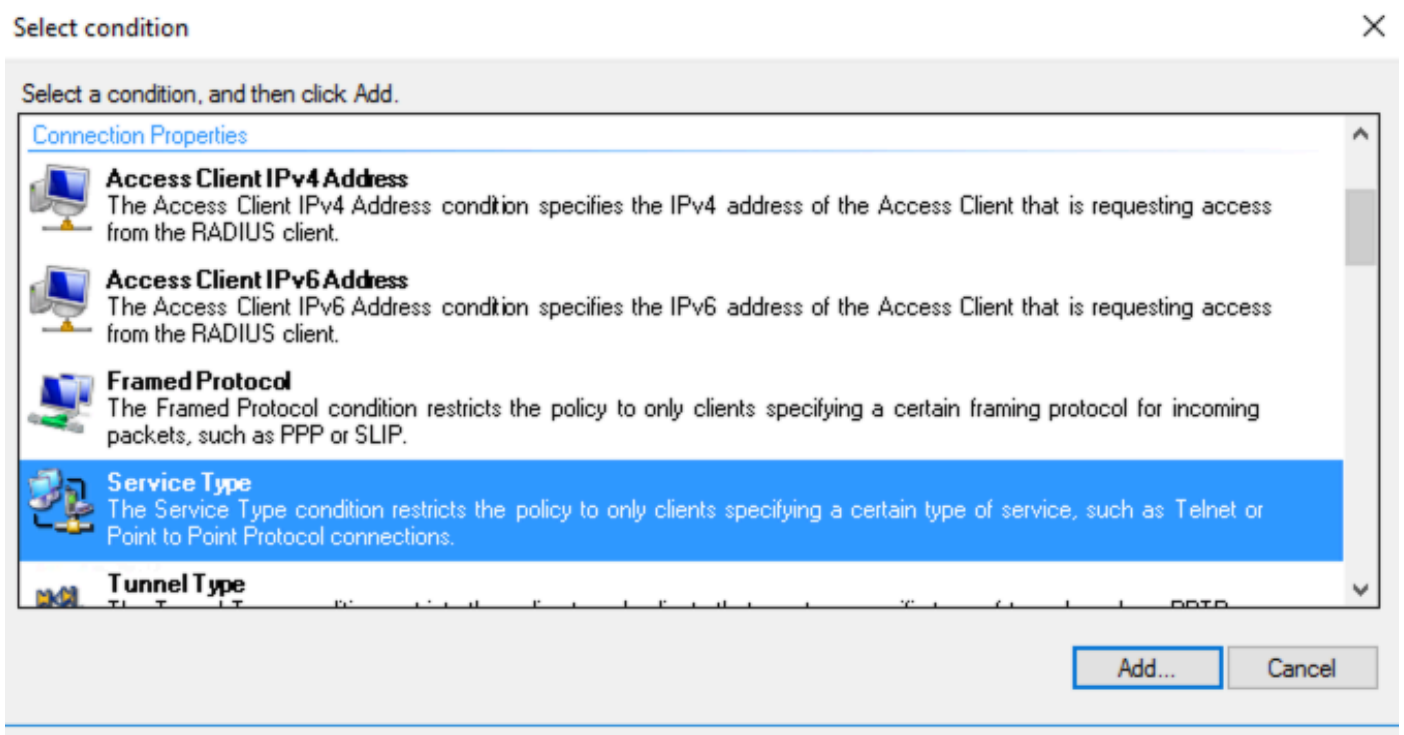


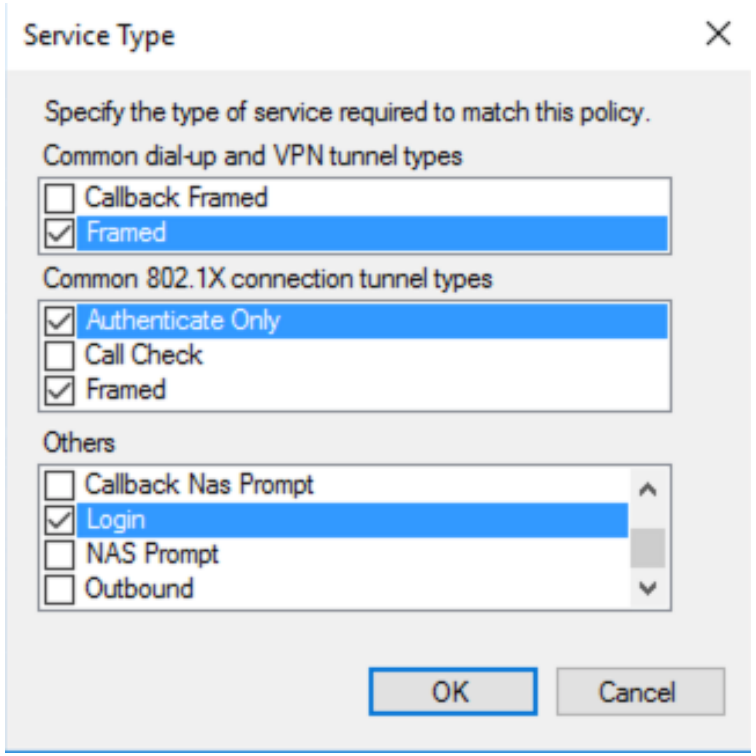
Specify NPS conditions (1. NAS port type)



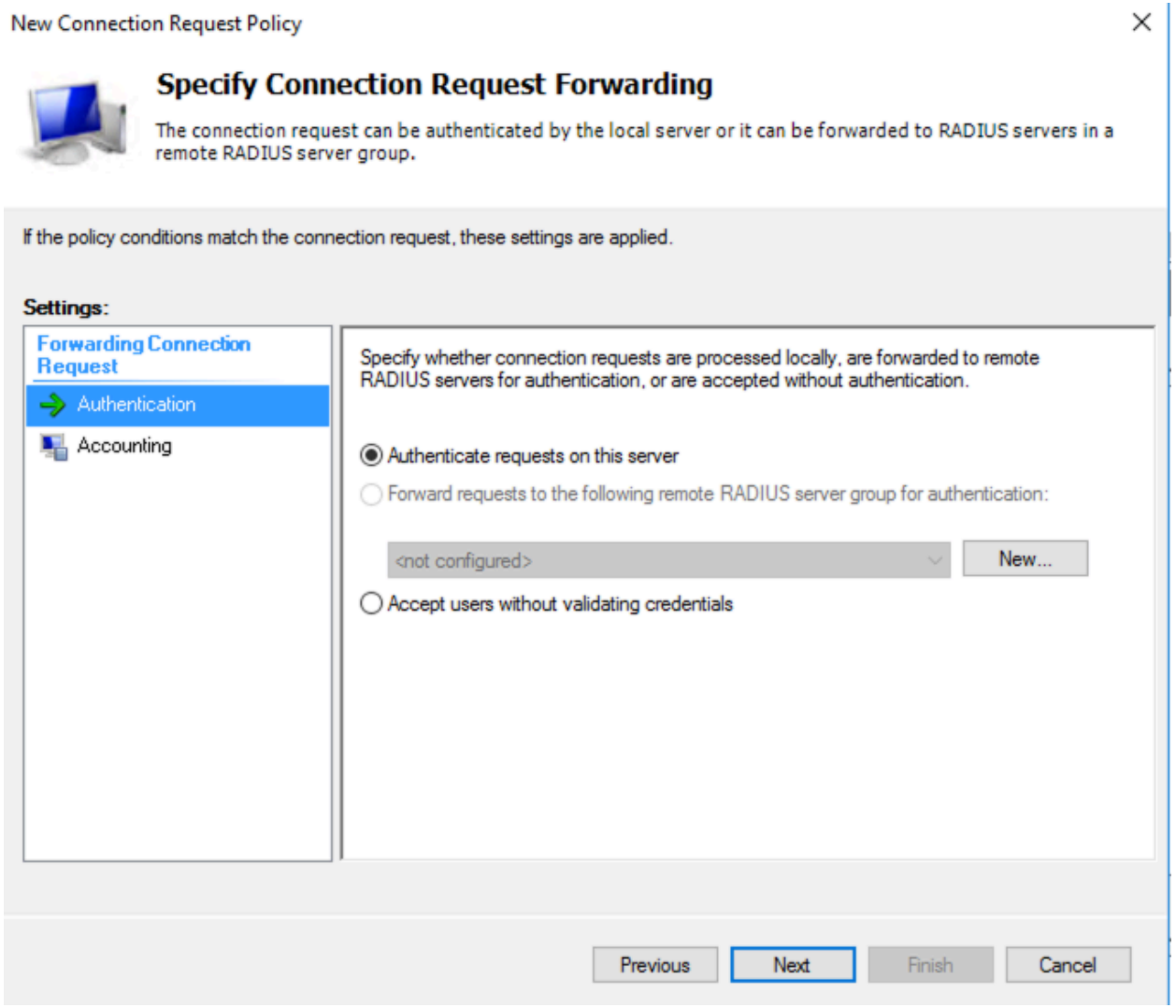


Specify NPS conditions (2. Service Type)

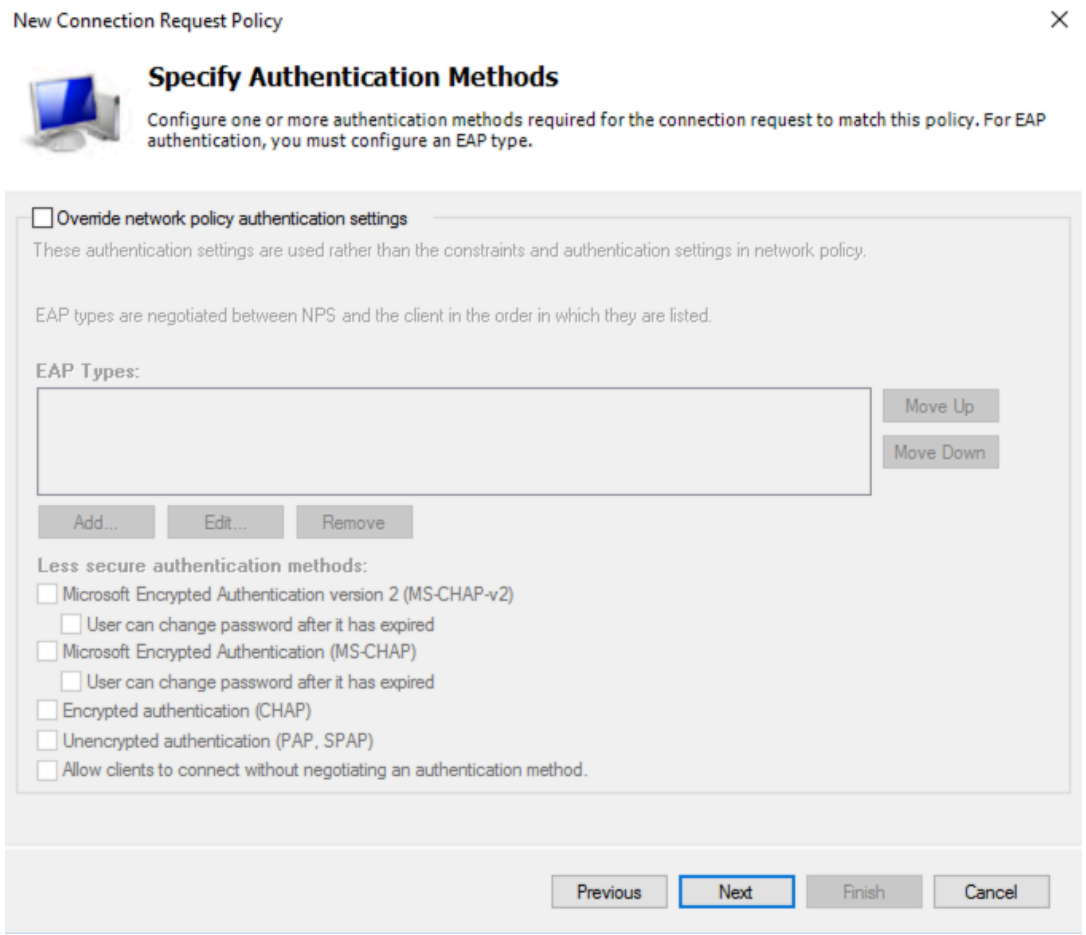




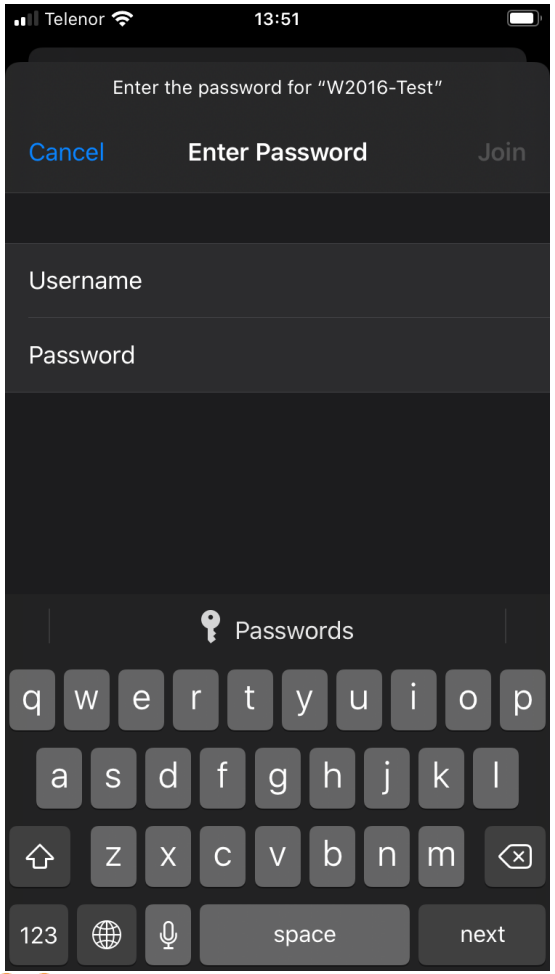
Specify Authentication Source (local in this case)



Specify Authentication Method (leave default for now, we will change this after ”troubleshooting” part of presentation)



Try connecting from your Wi-Fi client :



You will fail – reason for this is in next few slides.

aruba
a Hewlett Packard Enterprise company

First thing to check is Event Viewer on Windows Server. Start Event viewer and go to Windows Logs, Security.

– We are using correct credentials, but authentication failed :

User:

Security ID:	NBGD\petar
Account Name:	petar
Account Domain:	NBGD
Fully Qualified Account Name:	nbgd.biz/Users/Petar Petrovic

Client Machine:

Security ID:	NULL SID
Account Name:	-
Fully Qualified Account Name:	-
Called Station Identifier:	bc9fe4
Calling Station Identifier:	c4618b

NAS (NAD) is represented by correct IP address, correct NAS type and correct NPS policy is selected

NAS:

NAS IPv4 Address:	192.168.1.13
NAS IPv6 Address:	-
NAS Identifier:	192.168.1.32
NAS Port-Type:	Wireless - IEEE 802.11
NAS Port:	0

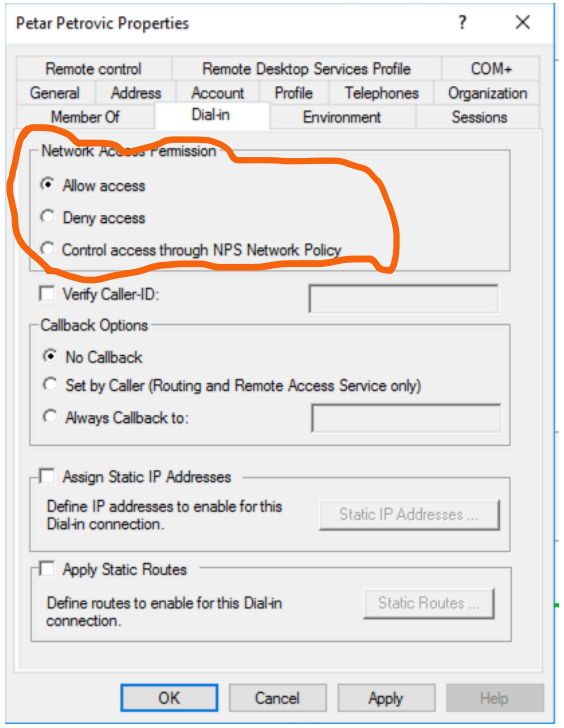
Authentication Details:

Connection Request Policy Name:	Accept WiFi Users from AIO
Network Policy Name:	Connections to other access servers
Authentication Provider:	Windows
Authentication Server:	AD.nbgd.biz
Authentication Type:	EAP
EAP Type:	-
Account Session Identifier:	-
Logging Results:	Accounting information was written to the local log file.

In this case client is declined due to missing Dial-in permissions from account settings

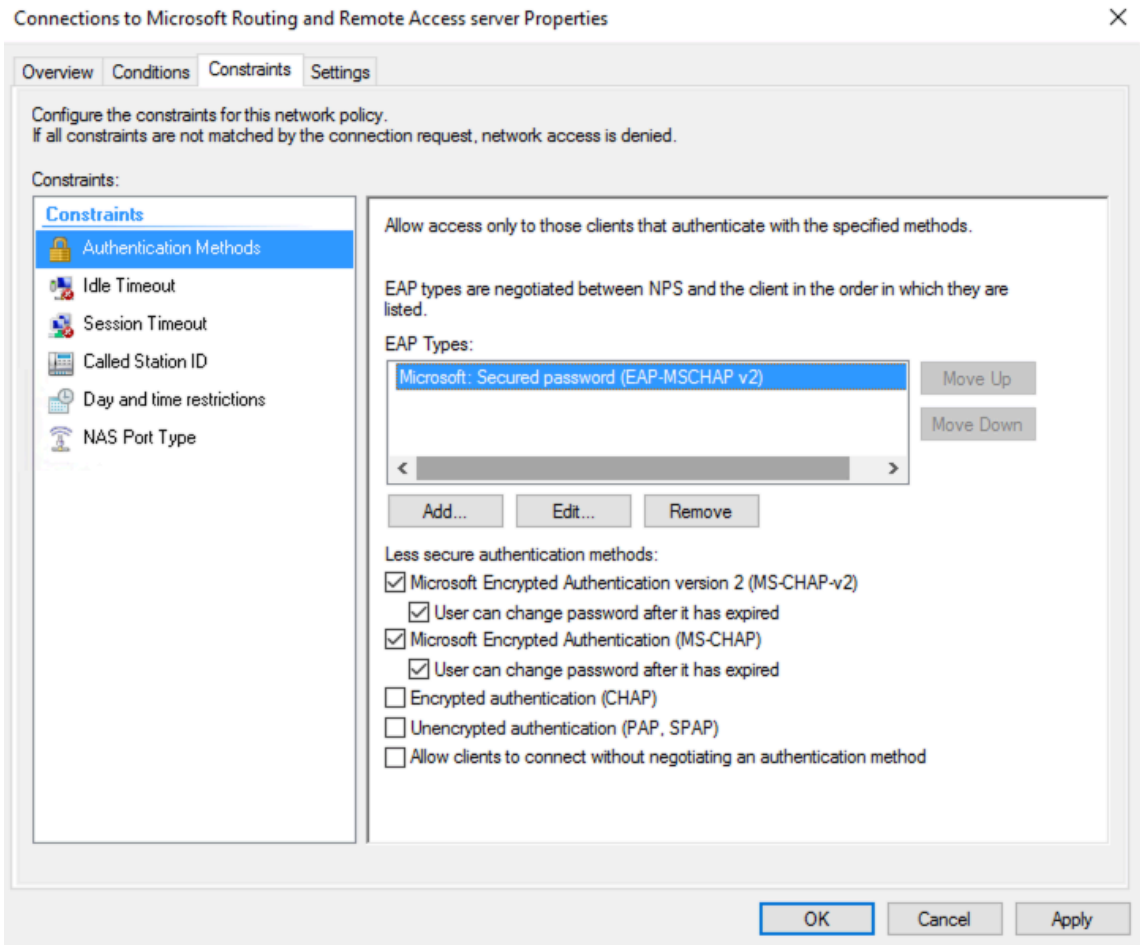
Reason Code: 65
Reason: The Network Access Permission setting in the dial-in properties of the user account in Active Directory is set to Deny access to the user. To change the Network Access Permission setting to either Allow access or Control access through NPS Network Policy, obtain the properties of the user account in Active Directory Users and Computers, click the Dial-in tab, and change Network Access Permission.

In order to fix it, go to Active Directory Users and Computers, and permit Dial-in access :



Authentication method not configured

On next retry we got “…user attempted to use an authentication method that is not enabled on the matching network policy” in Event Viewer. In order to fix this, go to NPS and edit policy settings so that proper authentication methods are available e.g.



Extensible Authentication Protocol (EAP) Type cannot be processed by the serve

If above message is shown in Event Viewer, it means that there is no server certificate available for authentication. This can be fixed by various methods, but most simple one (if you are doing demo) is that you enable CA functionality of windows server. Additional info can be found here

To enable CA role, just follow wizard that can be started from:

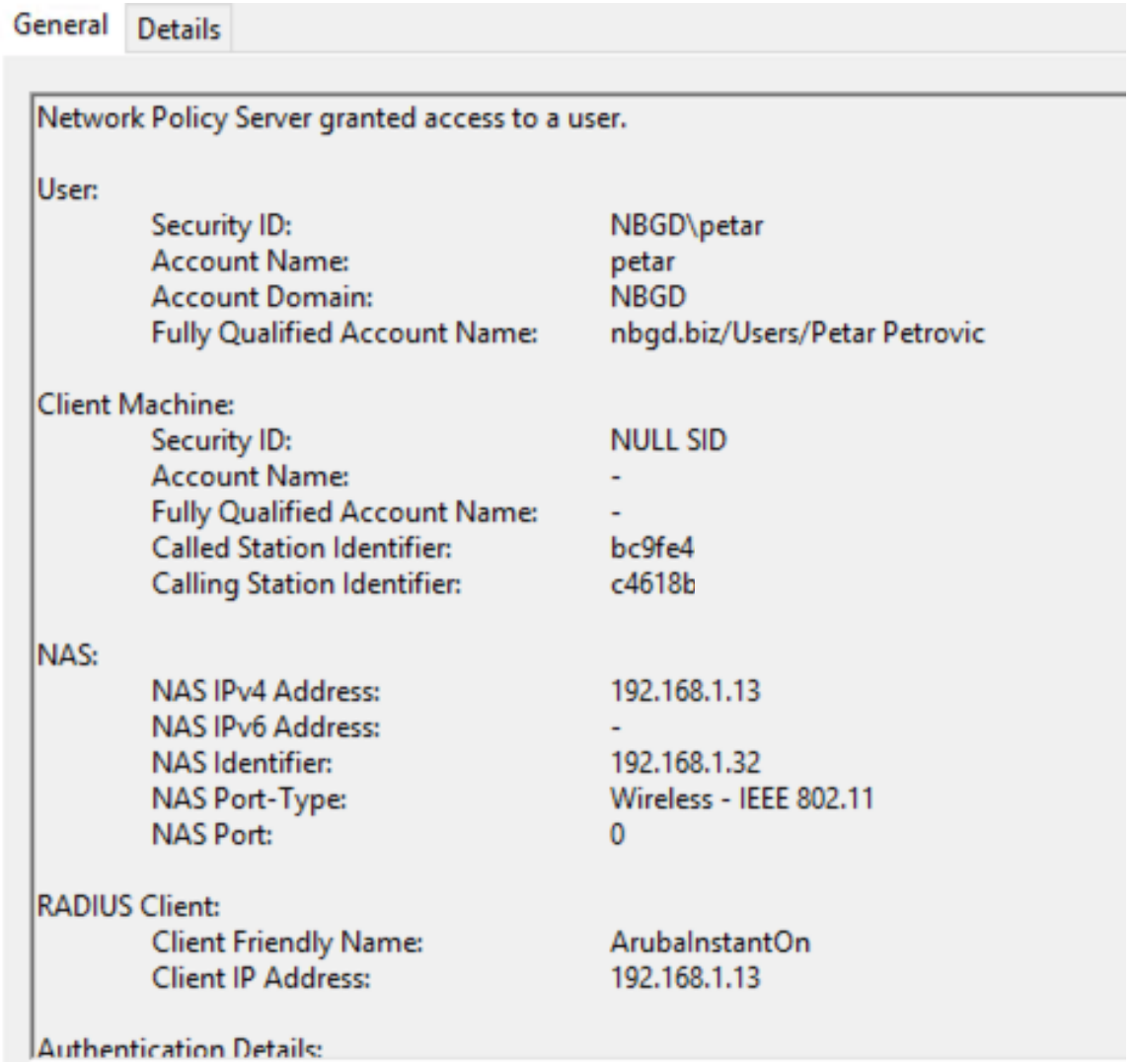
Server Manager ->

Dashboard ->

Add roles and Features ->

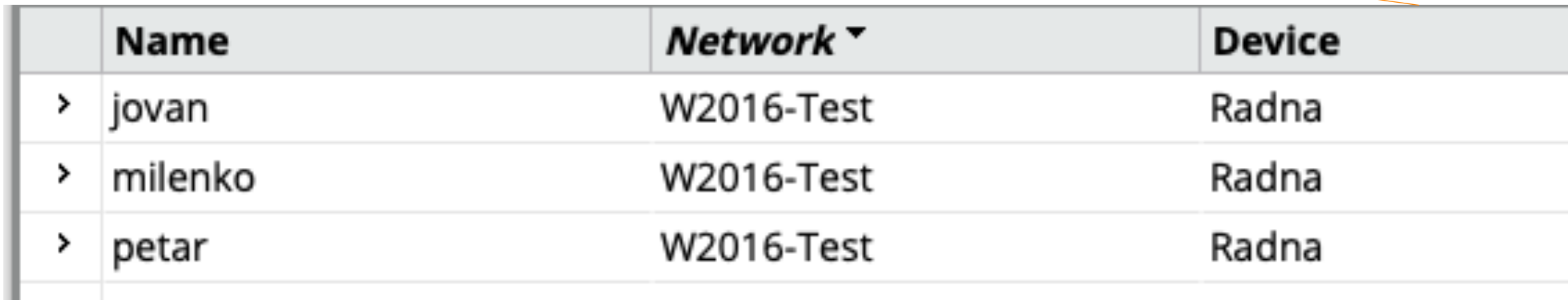
Active Directory Certificate Services.

Successful Authentication



On AIO Portal you will be able to see users identified by their AD credentials

	Name	Network	Device	Duration	Signal	OS	Downloading	Uploading	Transferred	Top Application Category
›	jovan	W2016-Test	Radna	4 minutes ago		Window...	4.47 kbps	3.34 kbps	14.2 GB	Uncategorized
›	milenko	W2016-Test	Radna	17 minutes ago		iPhone	-	-	384 MB	Web
›	petar	W2016-Test	Radna	8 minutes ago		OS X	134 kbps	15.2 kbps	5.54 GB	Web



Thank you!

https://community.arubainstanton.com/

milenko.markov@hpe.com

aruba
Instant On

aruba
a Hewlett Packard
Enterprise company