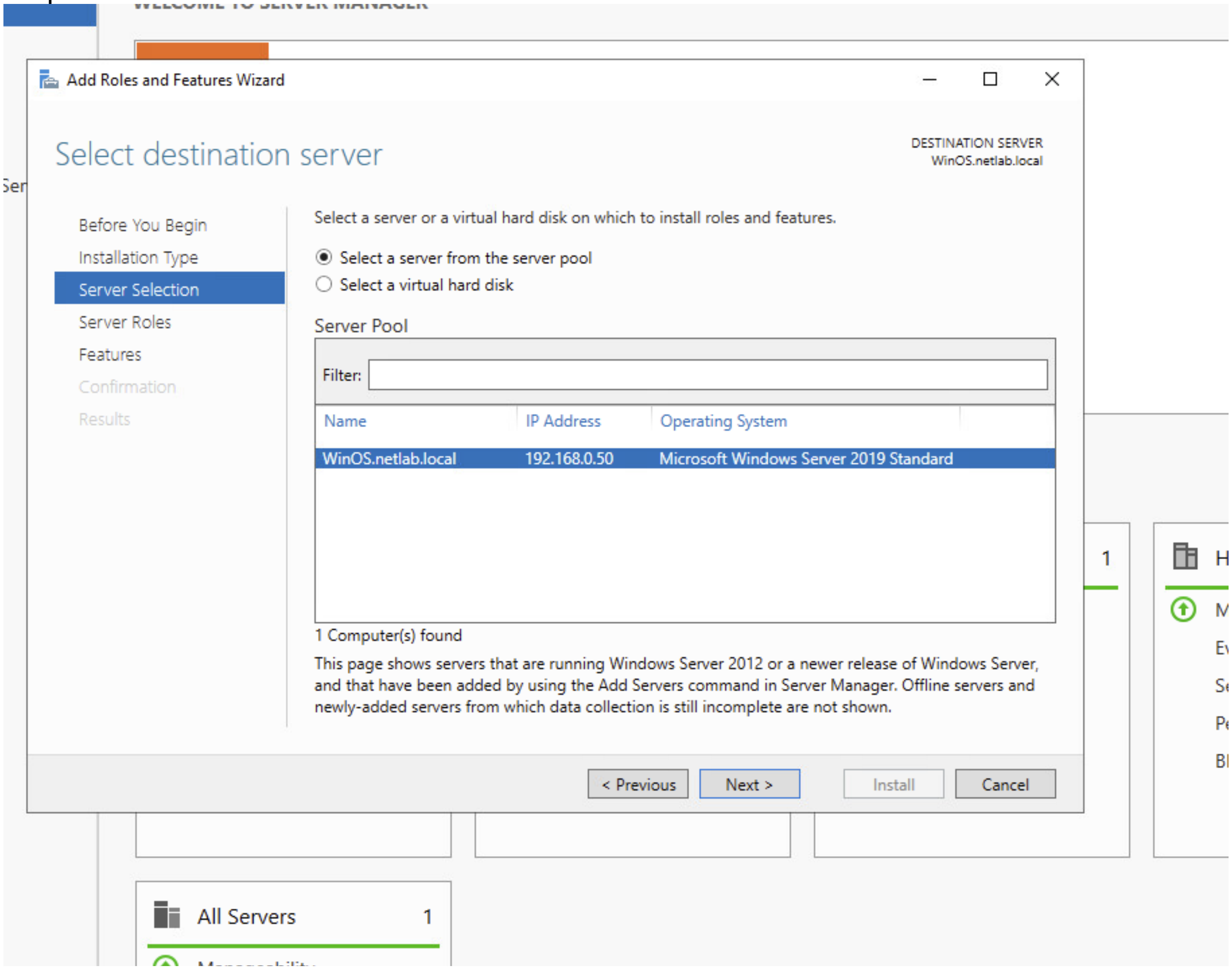
Peter Sanford
IT 2700
NetLab Lab 11
12/6/2023

1.1
Step 6:



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WinOS.netlab.local

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

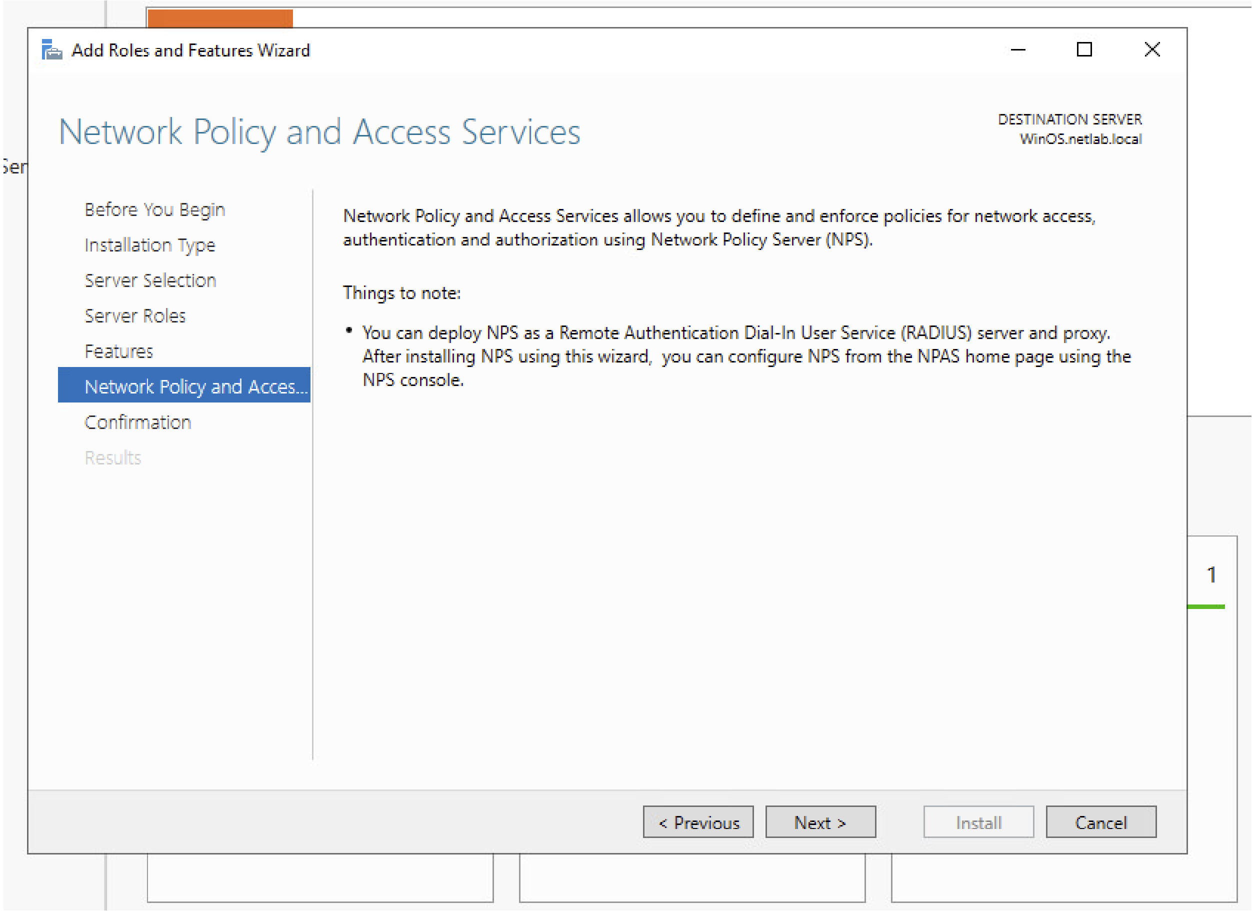
Filter:

Name	IP Address	Operating System
WinOS.netlab.local	192.168.0.50	Microsoft Windows Server 2019 Standard

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.

Step 10:



Network Policy and Access Services

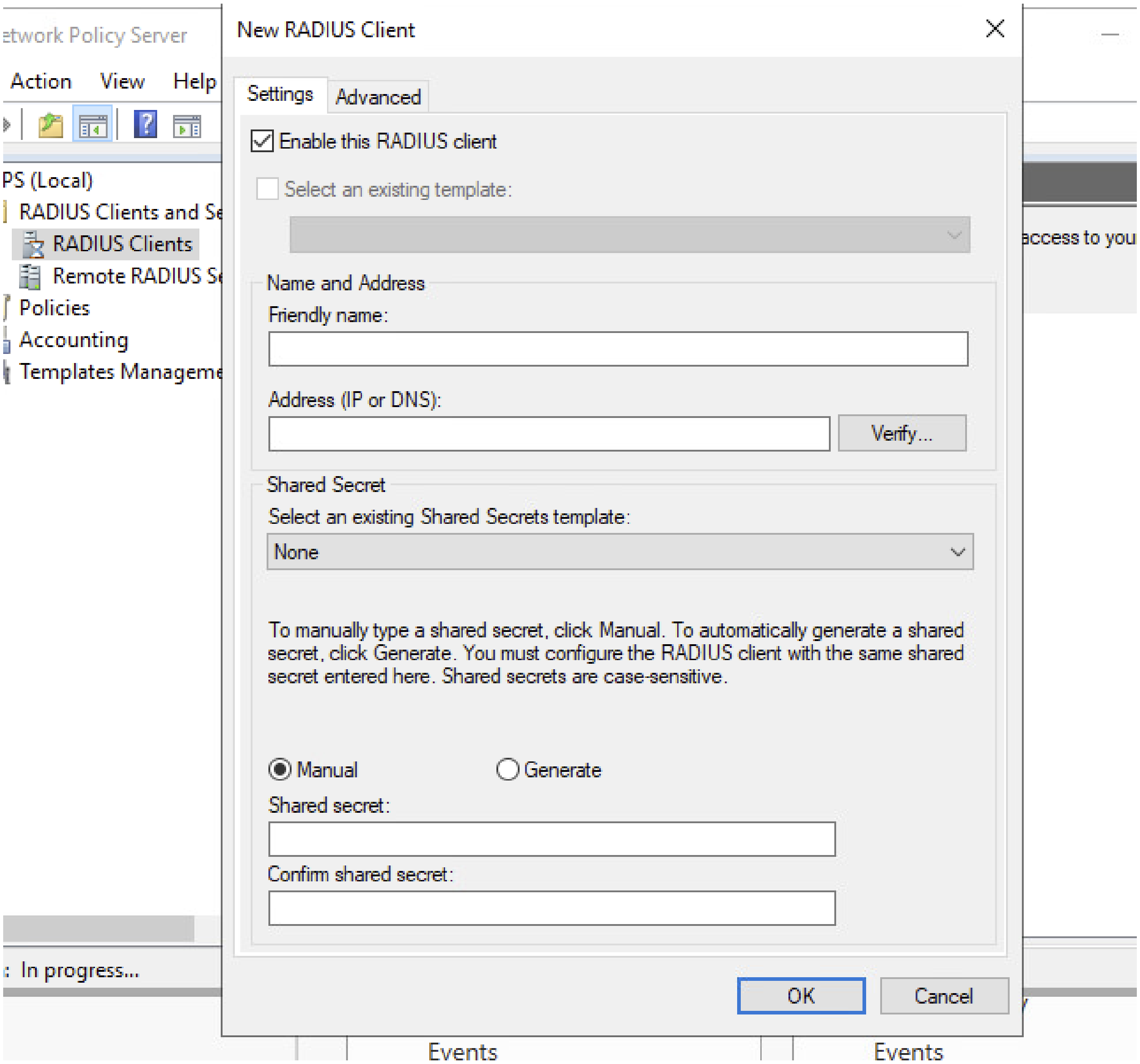
Network Policy and Access Services allows you to define and enforce policies for network access, authentication and authorization using Network Policy Server (NPS).

Things to note:

- You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.

1.2

Step 5:



New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name:

Address (IP or DNS):

Shared Secret

Select an existing Shared Secrets template:

None

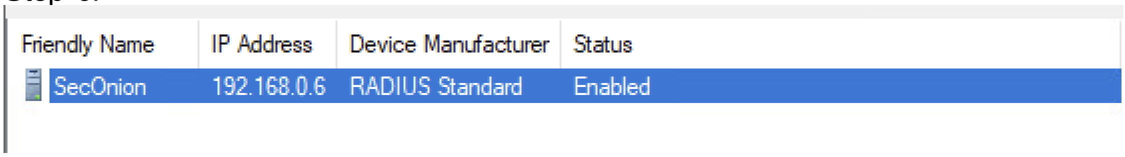
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret:

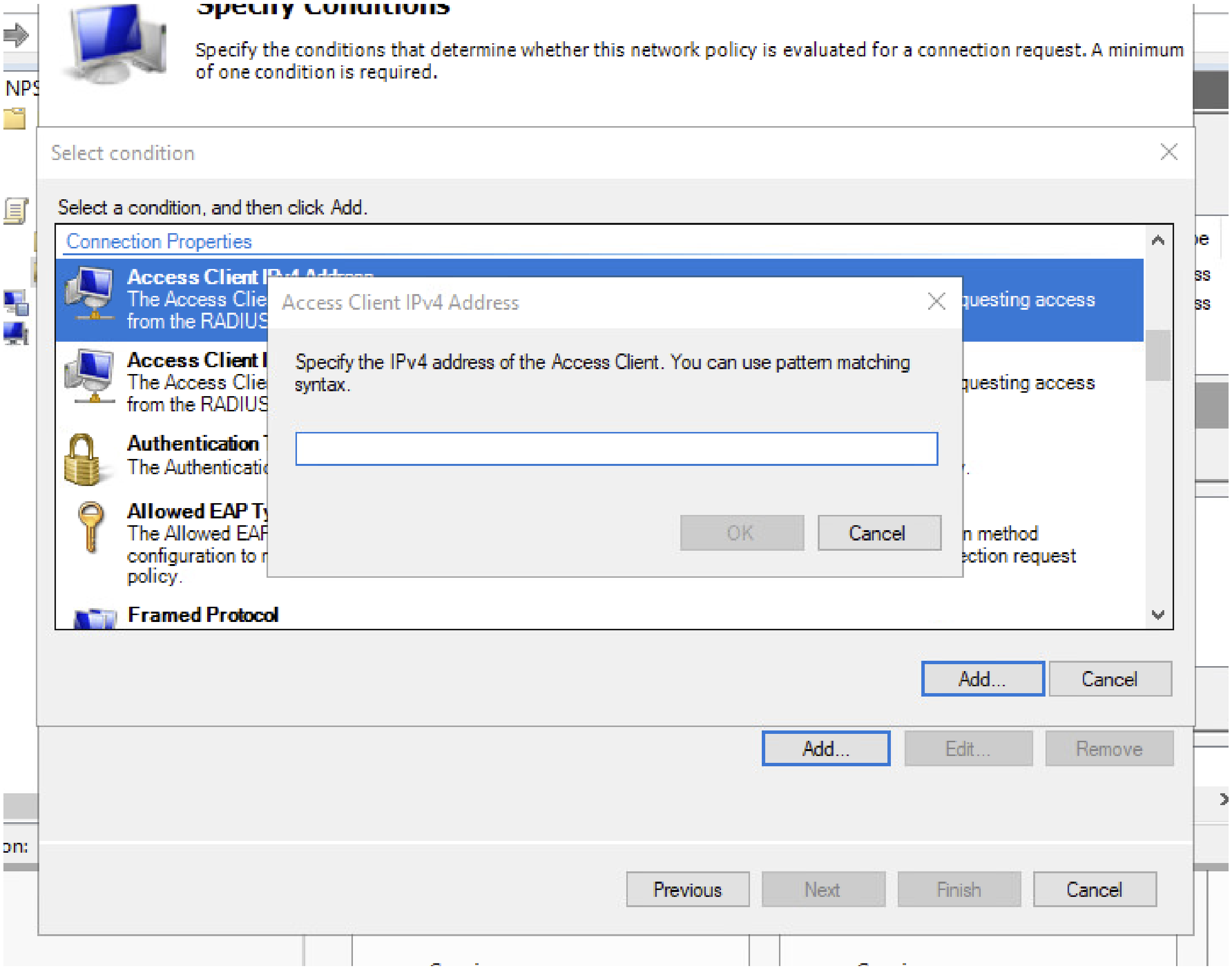
Confirm shared secret:

Step 6:



Friendly Name	IP Address	Device Manufacturer	Status
SecOnion	192.168.0.6	RADIUS Standard	Enabled

Step 12:



Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

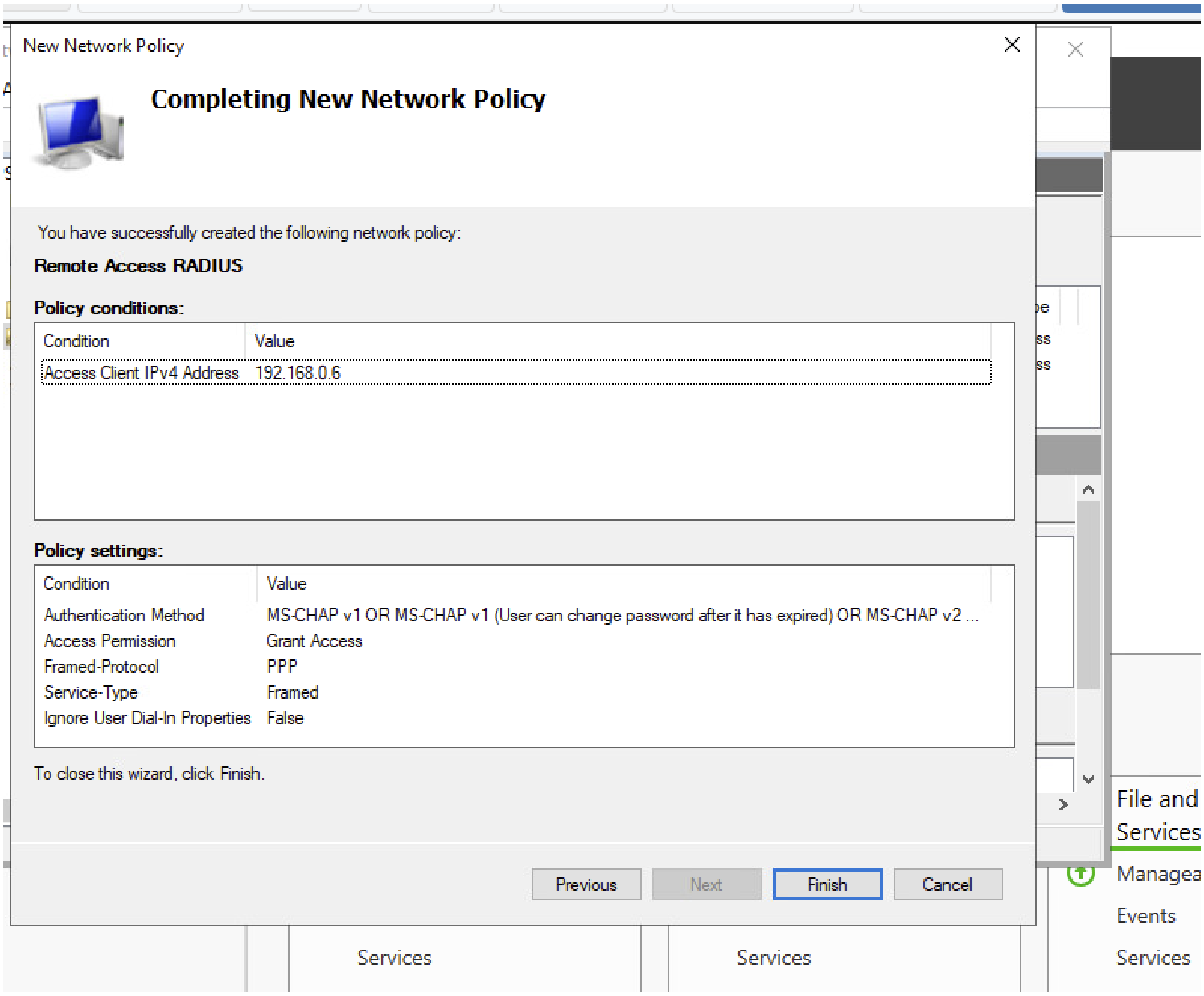
Select a condition, and then click Add.

Connection Properties

Access Client IPv4 Address

Specify the IPv4 address of the Access Client. You can use pattern matching syntax.

Step 19:



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Remote Access RADIUS

Policy conditions:

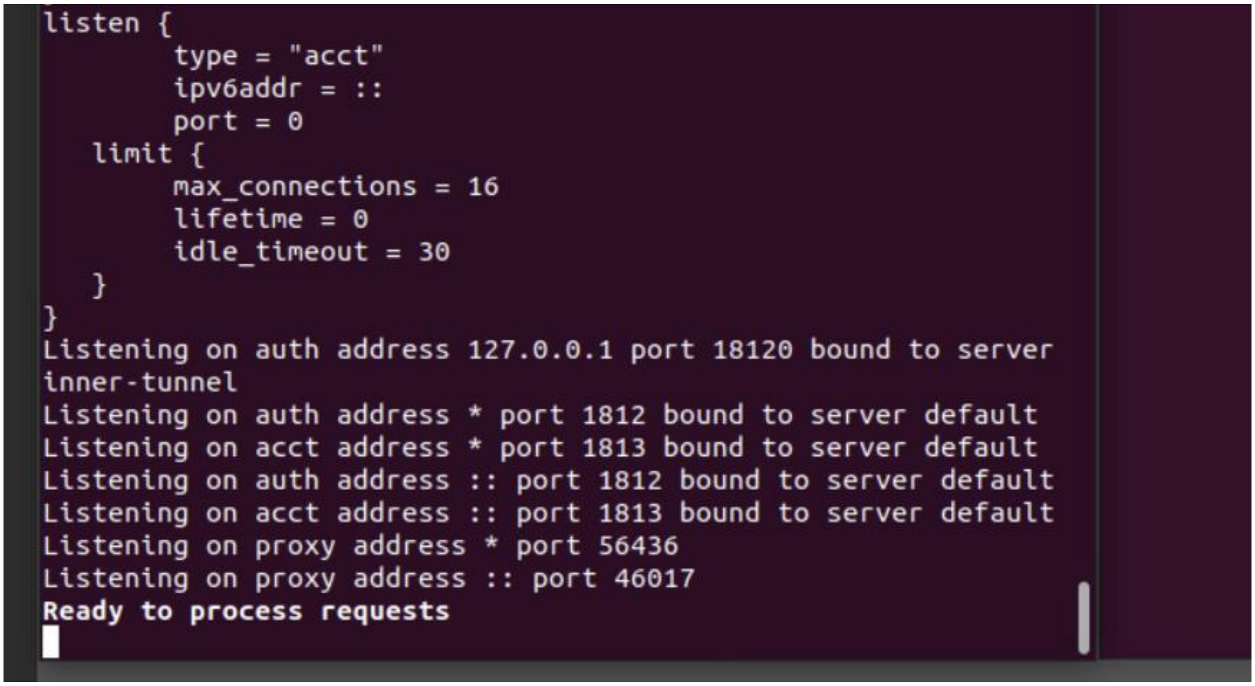
Condition	Value
Access Client IPv4 Address	192.168.0.6

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False

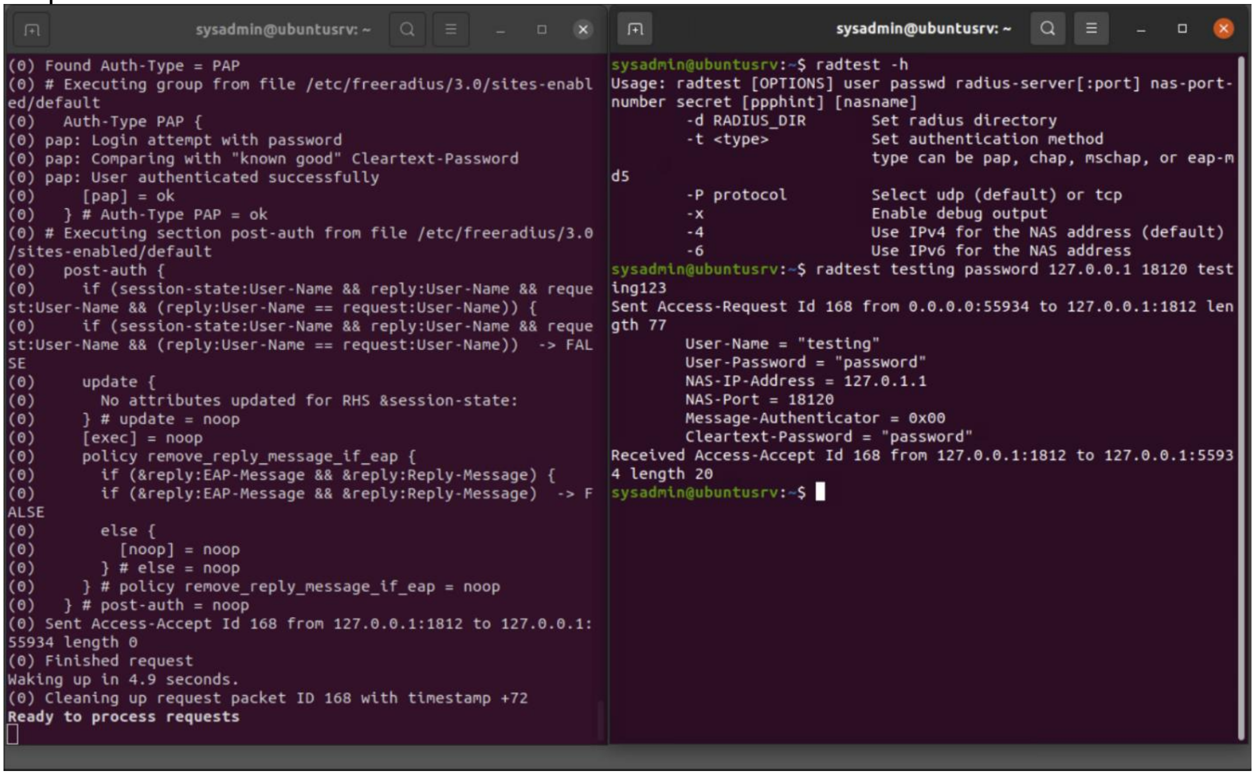
To close this wizard, click Finish.

2
Step 11:



```
listen {
        type = "acct"
        ipv6addr = ::
        port = 0
   limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
   }
}
Listening on auth address 127.0.0.1 port 18120 bound to server
inner-tunnel
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on proxy address * port 56436
Listening on proxy address :: port 46017
Ready to process requests
```

Step 14:



```
(0) Found Auth-Type = PAP
(0) # Executing group from file /etc/freeradius/3.0/sites-enabl
ed/default
(0)   Auth-Type PAP {
(0) pap: Login attempt with password
(0) pap: Comparing with "known good" Cleartext-Password
(0) pap: User authenticated successfully
(0)     [pap] = ok
(0)   } # Auth-Type PAP = ok
(0) # Executing section post-auth from file /etc/freeradius/3.0
/sites-enabled/default
(0)   post-auth {
(0)     if (session-state:User-Name && reply:User-Name && reque
st:User-Name && (reply:User-Name == request:User-Name)) {
(0)     if (session-state:User-Name && reply:User-Name && reque
st:User-Name && (reply:User-Name == request:User-Name))  -> FAL
SE
(0)     update {
(0)       No attributes updated for RHS &session-state:
(0)     } # update = noop
(0)     [exec] = noop
(0)     policy remove_reply_message_if_eap {
(0)       if (&reply:EAP-Message && &reply:Reply-Message) {
(0)       if (&reply:EAP-Message && &reply:Reply-Message)  -> F
ALSE
(0)       else {
(0)         [noop] = noop
(0)       } # else = noop
(0)     } # policy remove_reply_message_if_eap = noop
(0)   } # post-auth = noop
(0) Sent Access-Accept Id 168 from 127.0.0.1:1812 to 127.0.0.1:
55934 length 0
(0) Finished request
Waking up in 4.9 seconds.
(0) Cleaning up request packet ID 168 with timestamp +72
Ready to process requests
```

```
sysadmin@ubuntusrv:~$ radtest -h
Usage: radtest [OPTIONS] user passwd radius-server[:port] nas-port-
number secret [ppphint] [nasname]
        -d RADIUS_DIR       Set radius directory
        -t <type>           Set authentication method
                            type can be pap, chap, mschap, or eap-m
d5
        -P protocol         Select udp (default) or tcp
        -x                  Enable debug output
        -4                  Use IPv4 for the NAS address (default)
        -6                  Use IPv6 for the NAS address
sysadmin@ubuntusrv:~$ radtest testing password 127.0.0.1 18120 test
ing123
Sent Access-Request Id 168 from 0.0.0.0:55934 to 127.0.0.1:1812 len
gth 77
        User-Name = "testing"
        User-Password = "password"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 18120
        Message-Authenticator = 0x00
        Cleartext-Password = "password"
Received Access-Accept Id 168 from 127.0.0.1:1812 to 127.0.0.1:5593
4 length 20
sysadmin@ubuntusrv:~$
```

Commentary:

In this lab looked at a RADIUS server and saw how it functions to authenticate users/devices. I learned that it can be useful in business applications as it can be an easy way to have everything authenticated from one place. Knowing this information, companies can use it to make their life easier, but also need to understand how it works so that they can secure it correctly.