CCISRD
Center for Communication and Informationsecurity Research and Development

Enterprise wireless with CAPsMAN and Windows NPS

Rein Põdra
Trainer / Consultant
rein.podra@ccisrd.eu
Berlin 2018

Wireless security

- Open wireless - no security at all.
- WEP - minimal security. (Deprecated)
- WPA(2)-PSK - secure, but ..

WPA(2)-PSK

- All users use the same shared secret (Pre Shared Key). If we loose the key, we need replace it on all devices.
  - In RouterOS we can use different PSK for every MAC address, but MAC address is visible for all and it can be cloned.
    It is also very complicated to manage MAC addresses, bind them to users - especially when user have several devices (laptop, smartphone and tablet)
- Cipher key is generated based on SSID and PSK. In same network the generated key is always the same.
- No way to verify AP identity. We can create fake AP and use special tools to steal information. Out off box tools cost ~100USD

WPA-EAP

- We can authenticate users with user name and password or with computer account (in windows domain). Every user have own credentials. It’s easy to change password, disable account or create temporary account.
- We can verify AP or Authenticator (RADIUS server) identity with SSL certificates.
- With SSL user certificates we can use 2FA, credentials and certificate.
- Authenticator generates new cipher key for every session.

Next problem.

- We need to create separate wireless networks (for example): Management, Sales, Production, Guests, etc.
  Not everyone need to have access everywhere!
- The simplest way is to create separate virtual AP for each network. If the users belongs to the sales group - user needs to connect the “Sales” SSID. When users’ role changes (from production to support), the user needs to connect different SSID. It makes difficult to manage such scale of wireless networks.

Dynamic VLAN

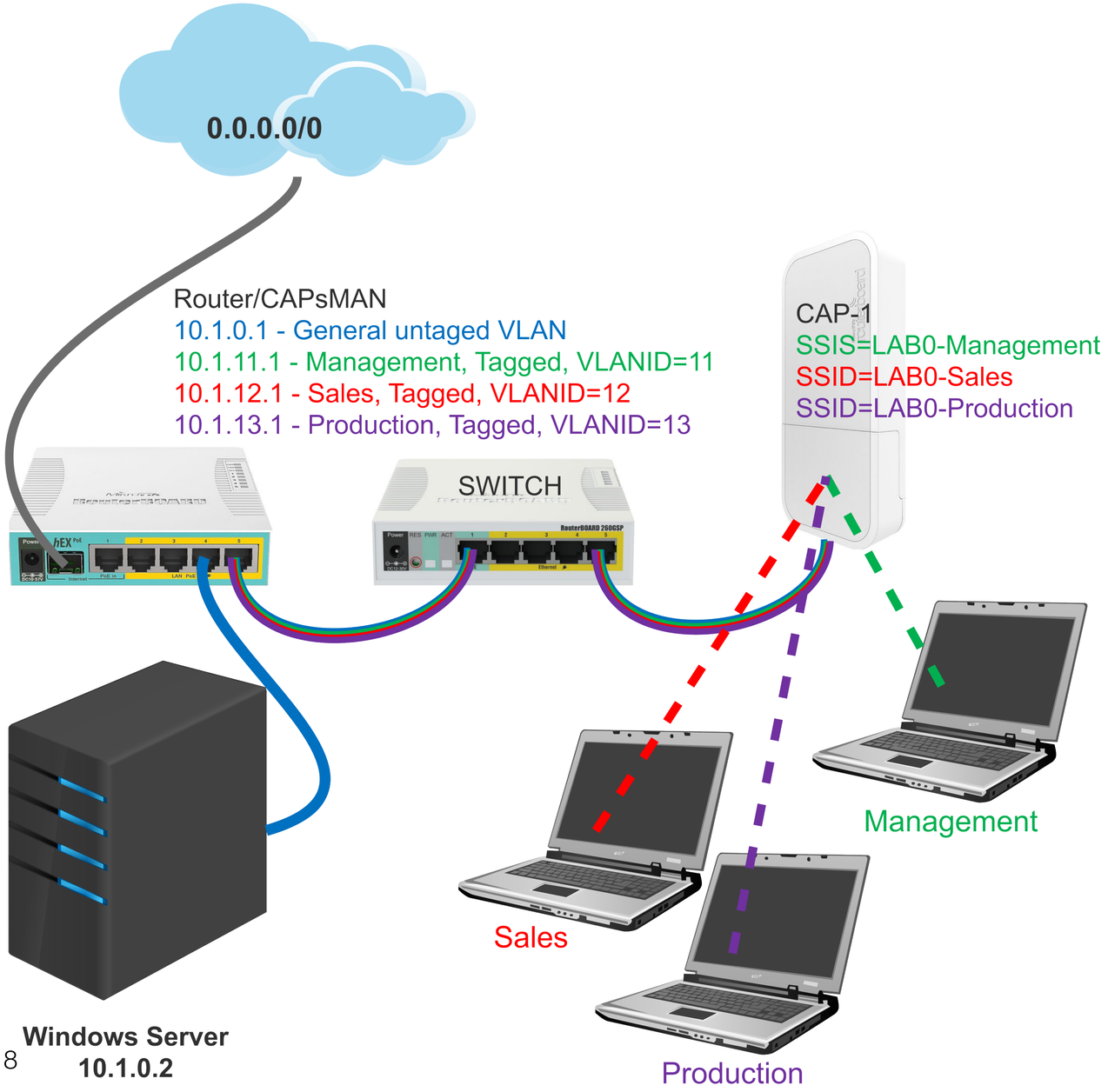
- Why not to use different VLAN's on same SSID?
- After user authentication RADIUS server can send VLAN ID with accept message.
- All traffic coming from this user will be tagged with provided VLAN ID.
- Adding wireless interfaces to bridge, we can create TRUNK and send all vlan's to router/firewall.
- Using CAPsMAN we can automate AP configuration and manage all vlan's and AP's from one spot

CCISRD
Center for Communication and Informationsecurity
Research and Development

Sounds complicated?

What we already have?

- Typically companies have server, lots of them have MS Windows Server and Active Directory, but only for user authentication and file server functionality.
- When we have MikroTik AP's, typically we have also already configured CAPsMAN
- That will be our staring point:
  - Installed Windows AD
  - CAPsMAN



What we need?

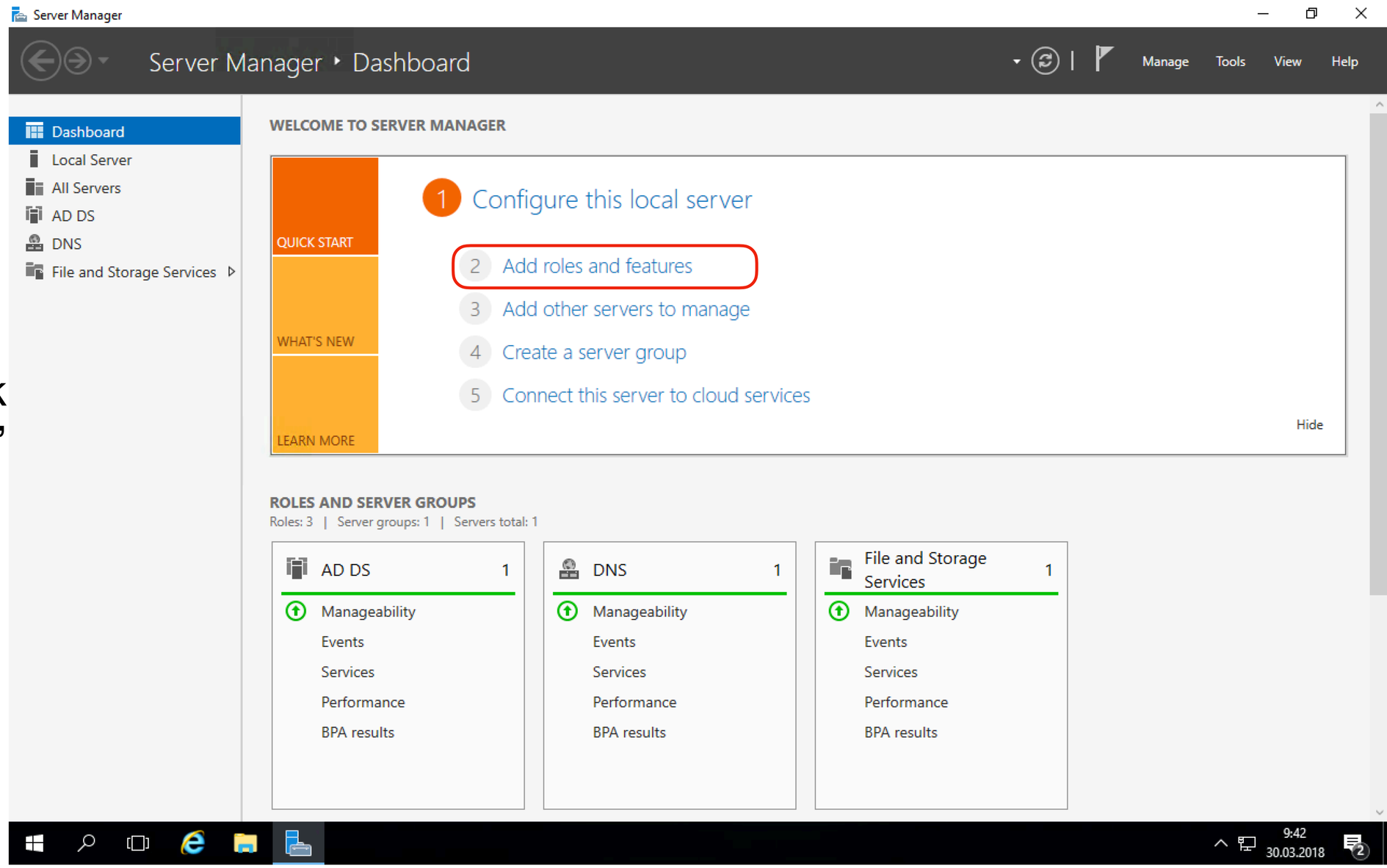
- As mentioned before we need following roles
  - RADIUS Server - Network Access and Protection Server (NPS)
  - SSL Certificates system - Active Directory Certificate Authority (AD CA)

Next Steps

- **Install NPS and CA roles on Windows Server**
- Configure CA
- Configure NPS - RADIUS Server
- Reconfigure CAPsMAN
- Install CA on client device’s - only if not domain member

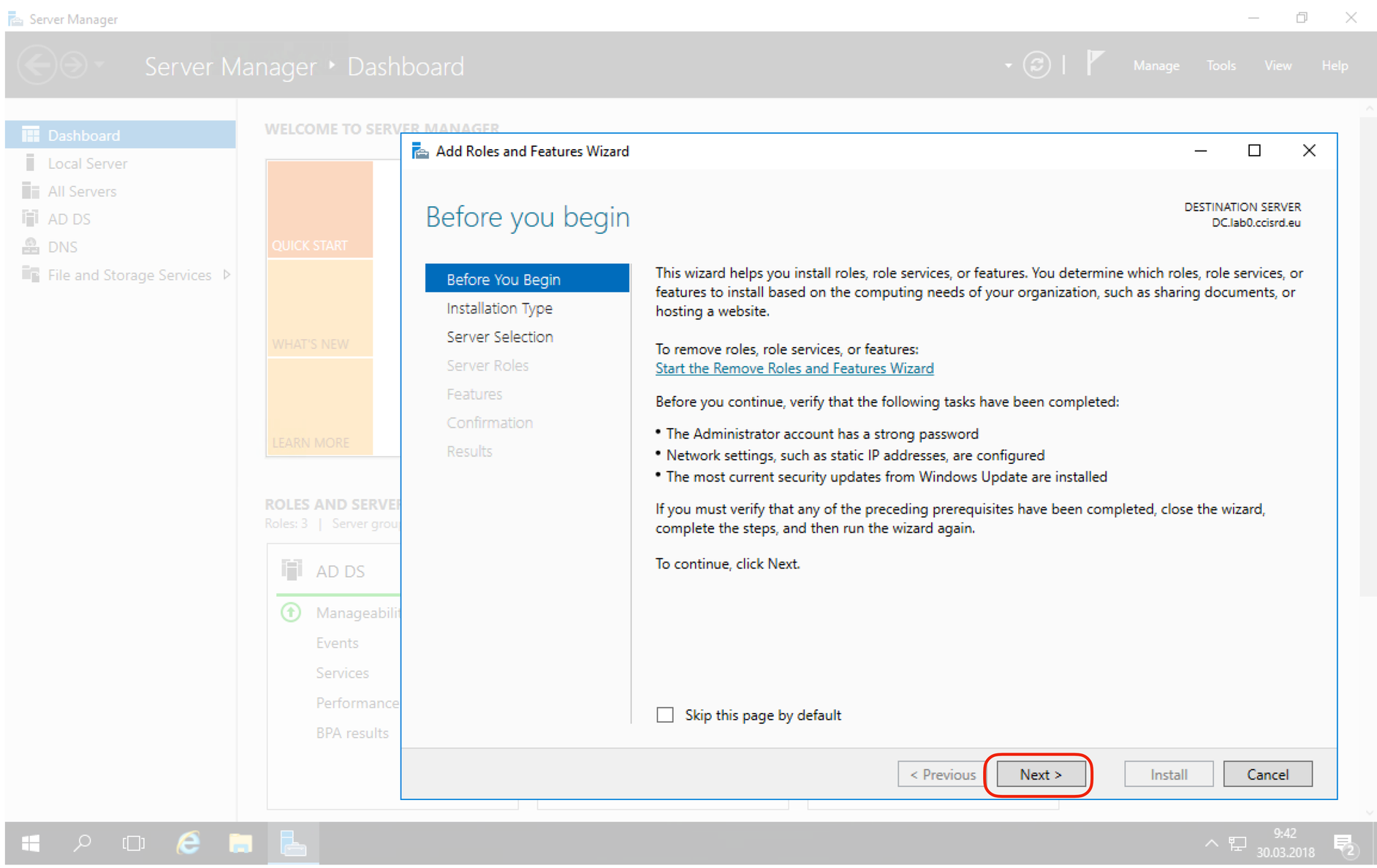
Add roles and features

- In Server Manager click Add roles and features”



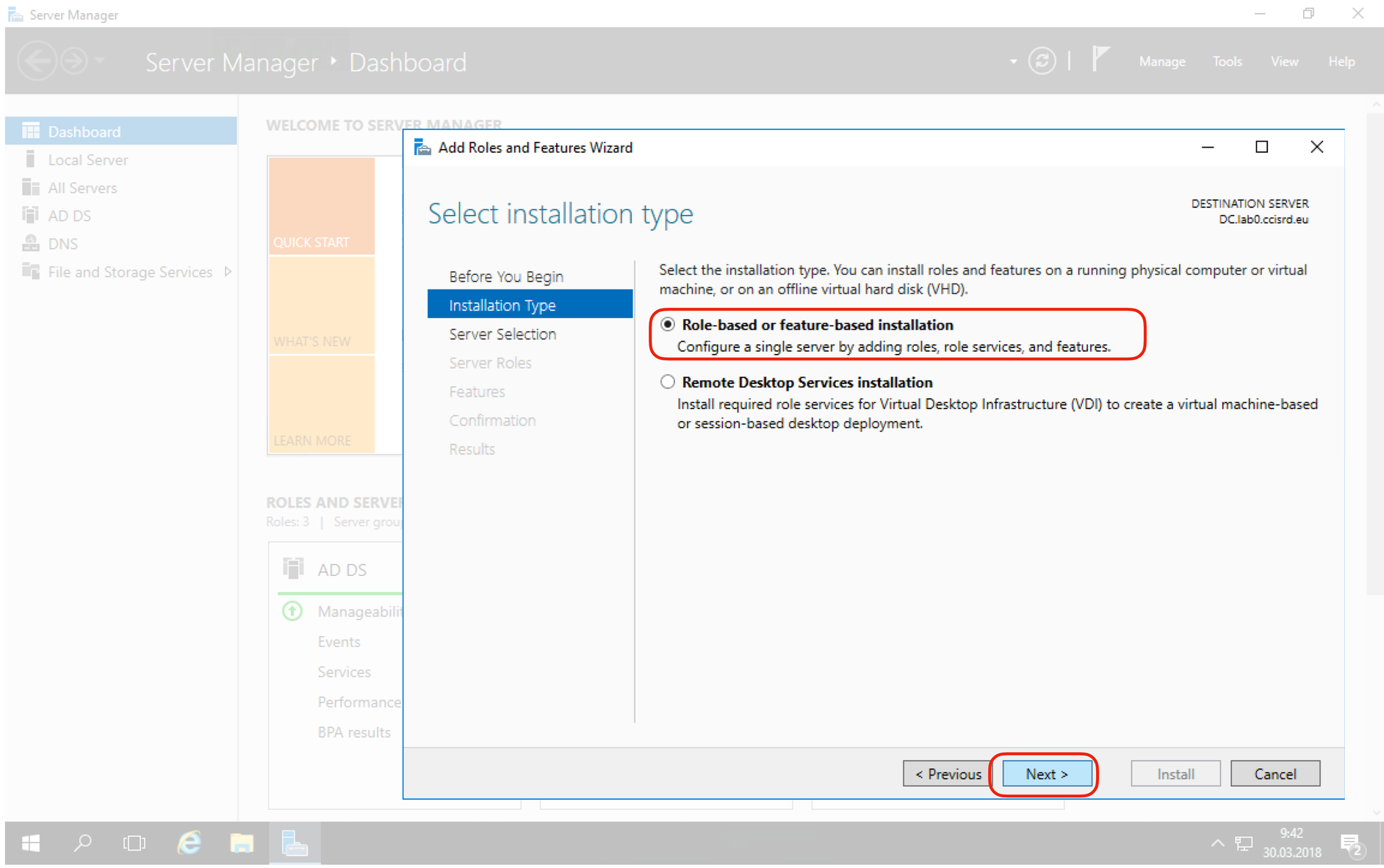
Install Roles

- You may read the information.
- Accept default and click “Next”



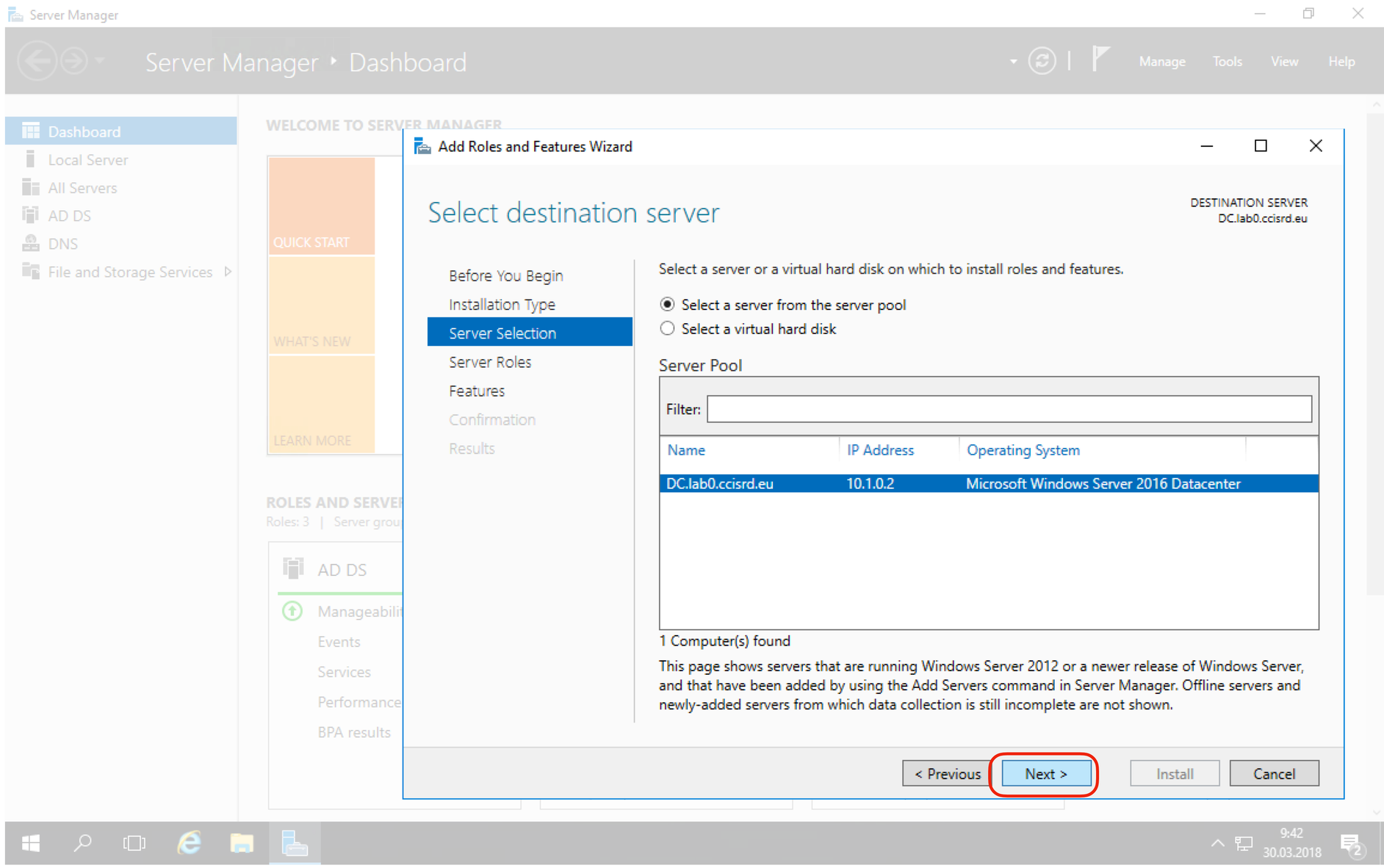
Install Roles - Installation Type

- Select “Role-based or feature-based installation” and click “Next”



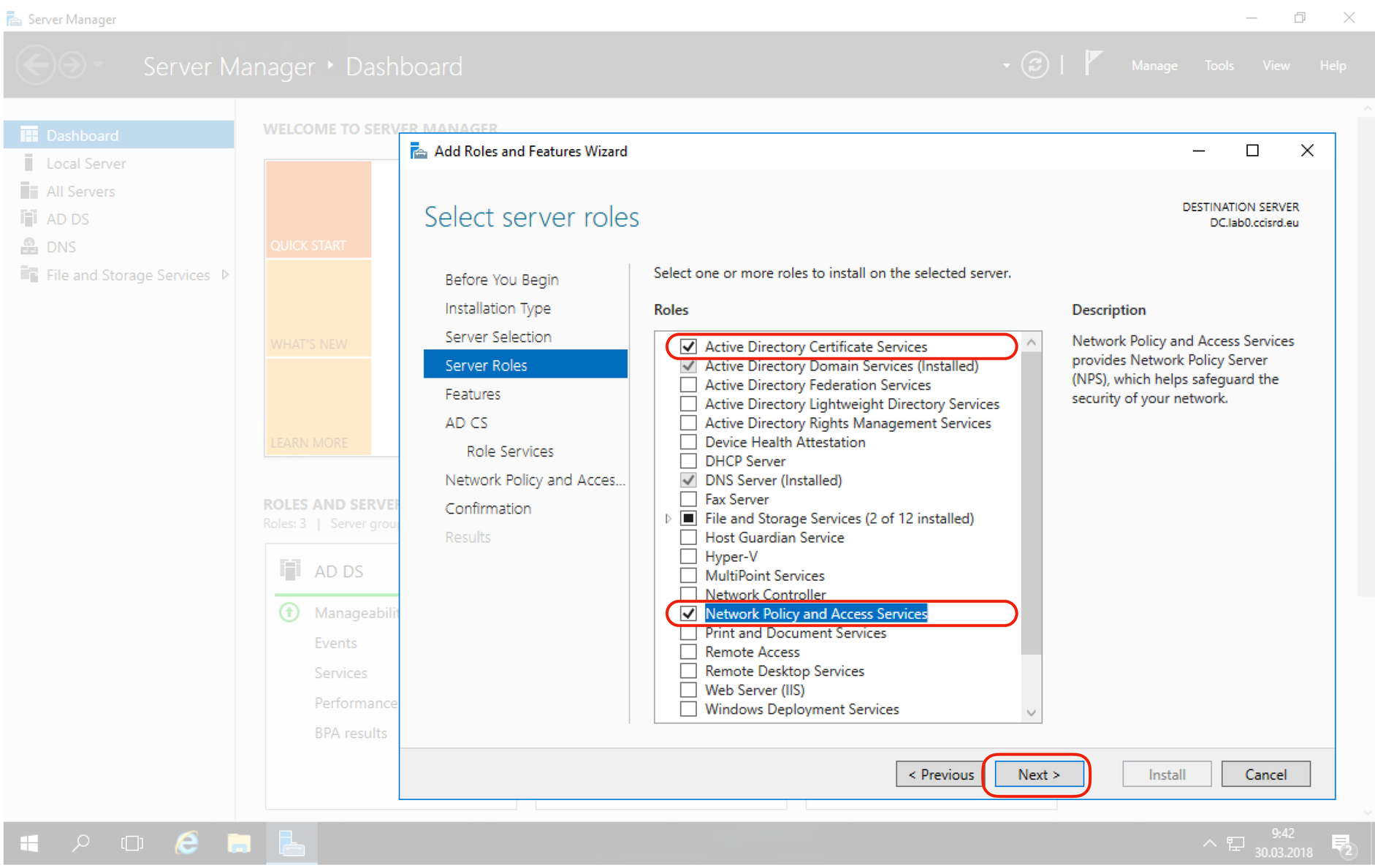
Install Roles - Select Server

- Select server, in our case there is only one server, and click “Next”



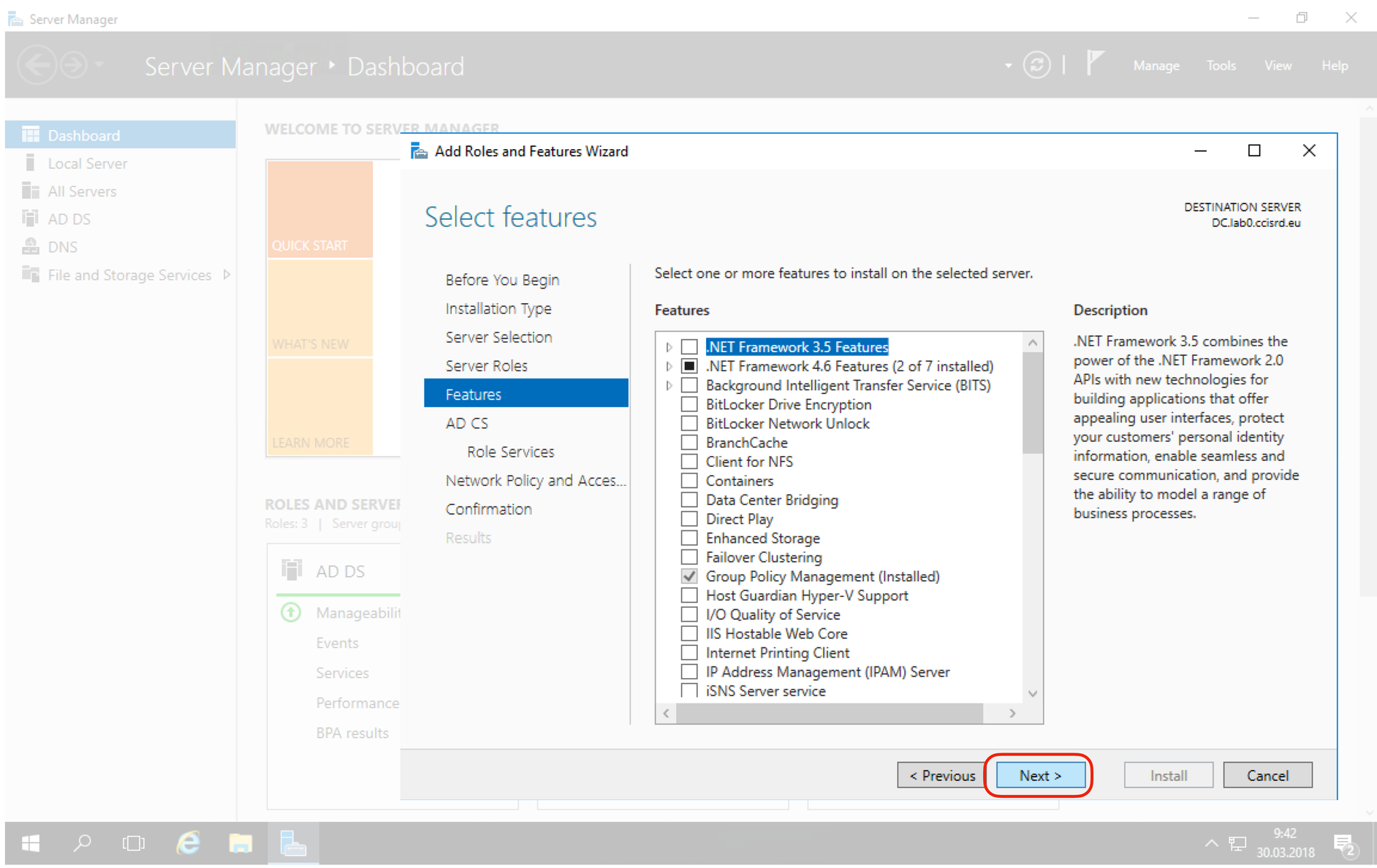
Select Server Roles

- When asked about required features for the selected role, accept default values and click “Next”



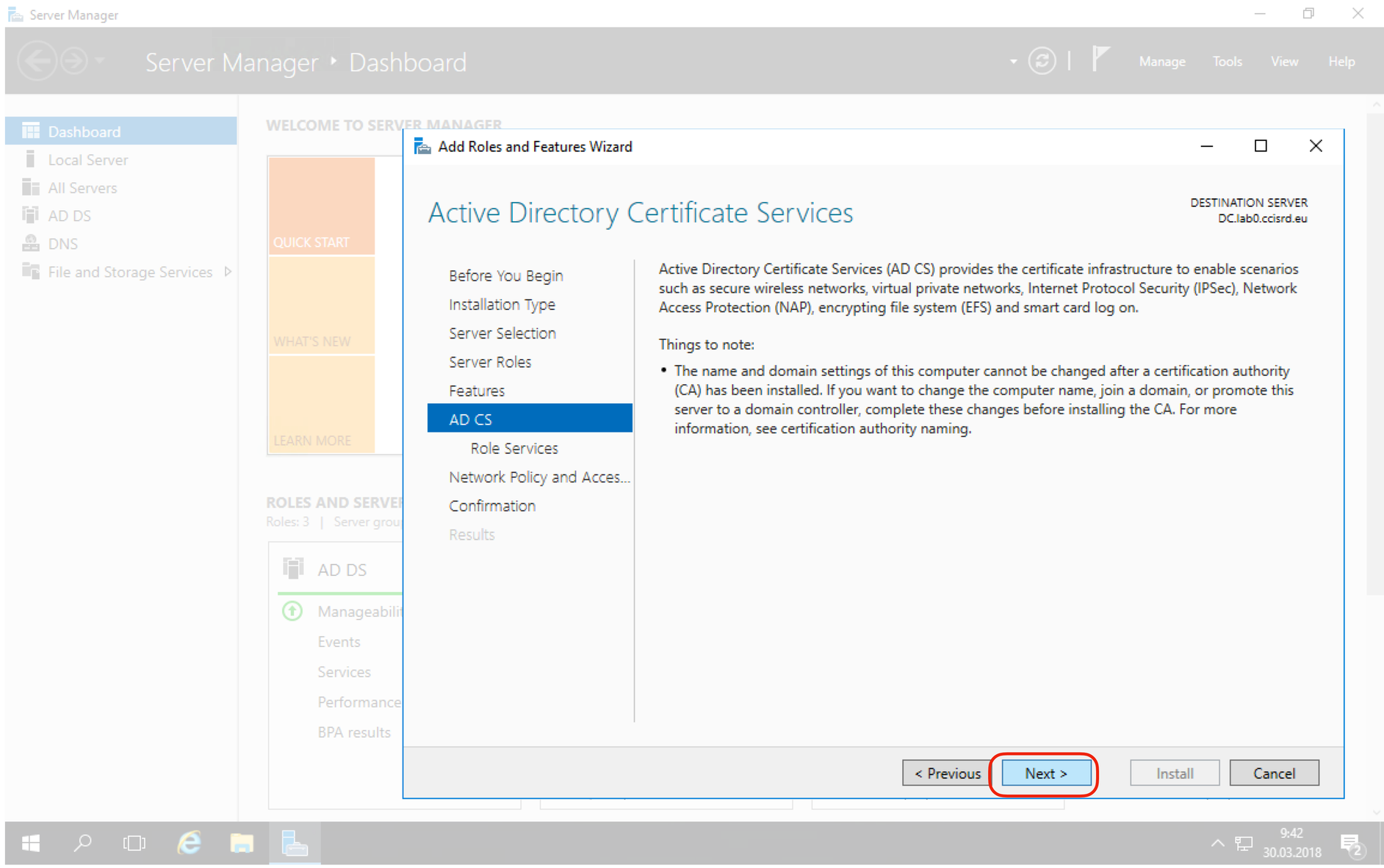
Select features

- Accept default and click “next”



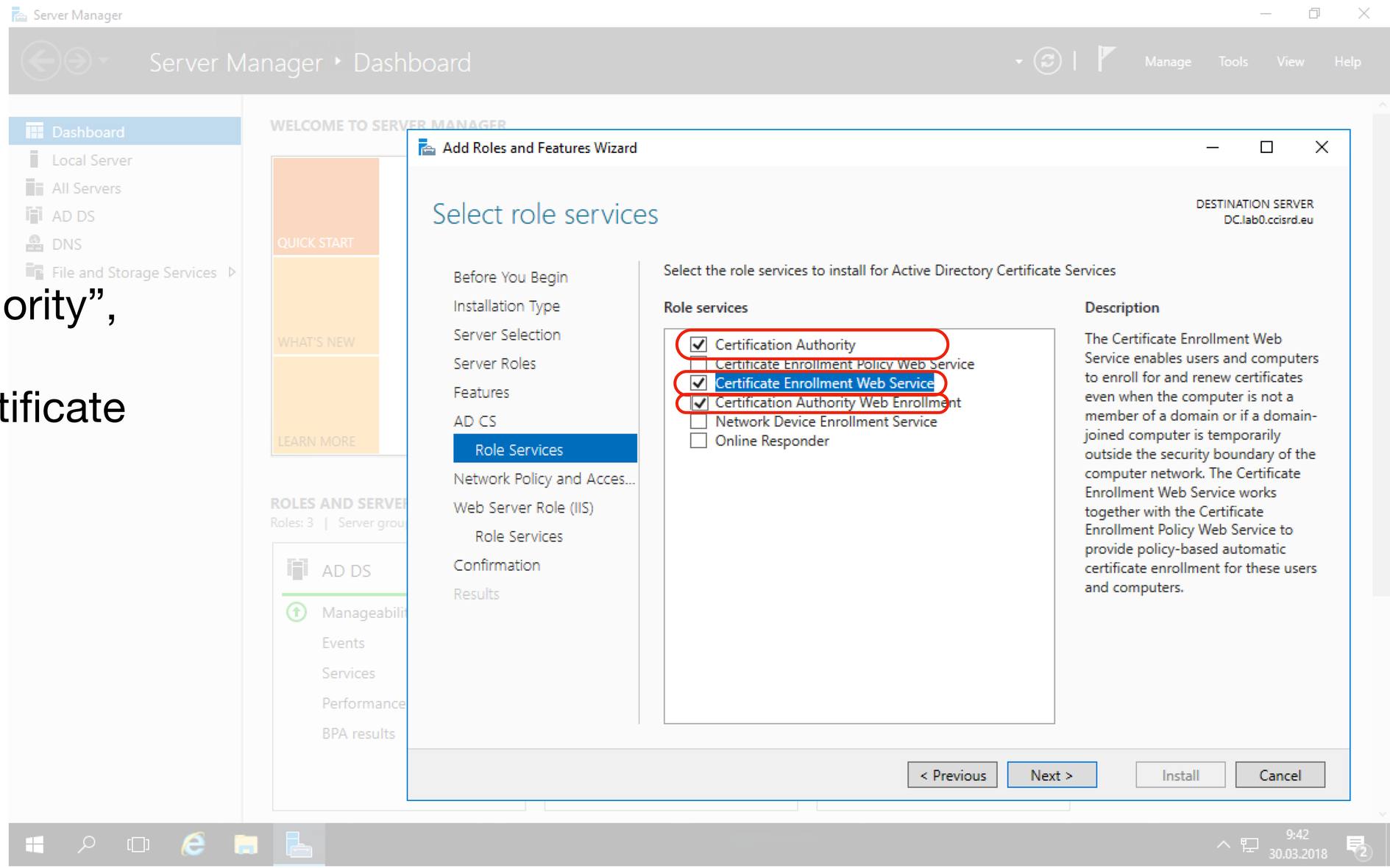
AD Certificate Services

- When asked about required features for the selected role, accept default values.
- Accept default and click “Next”



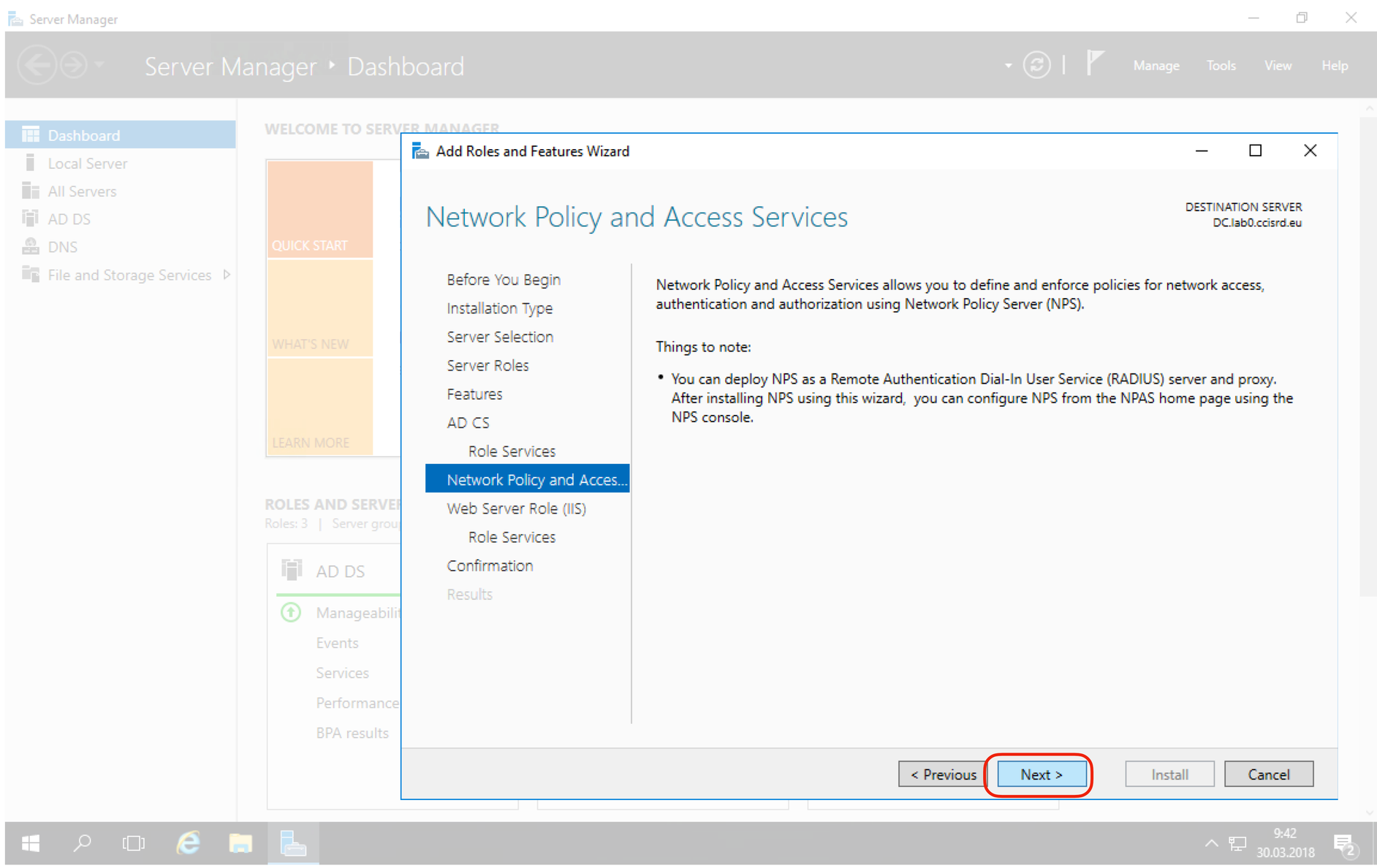
Install CA role

- Select “Certificate Authority”, “Certificate Enrollment Web Service” and “Certificate Authority Web Service”
- Click “Next”



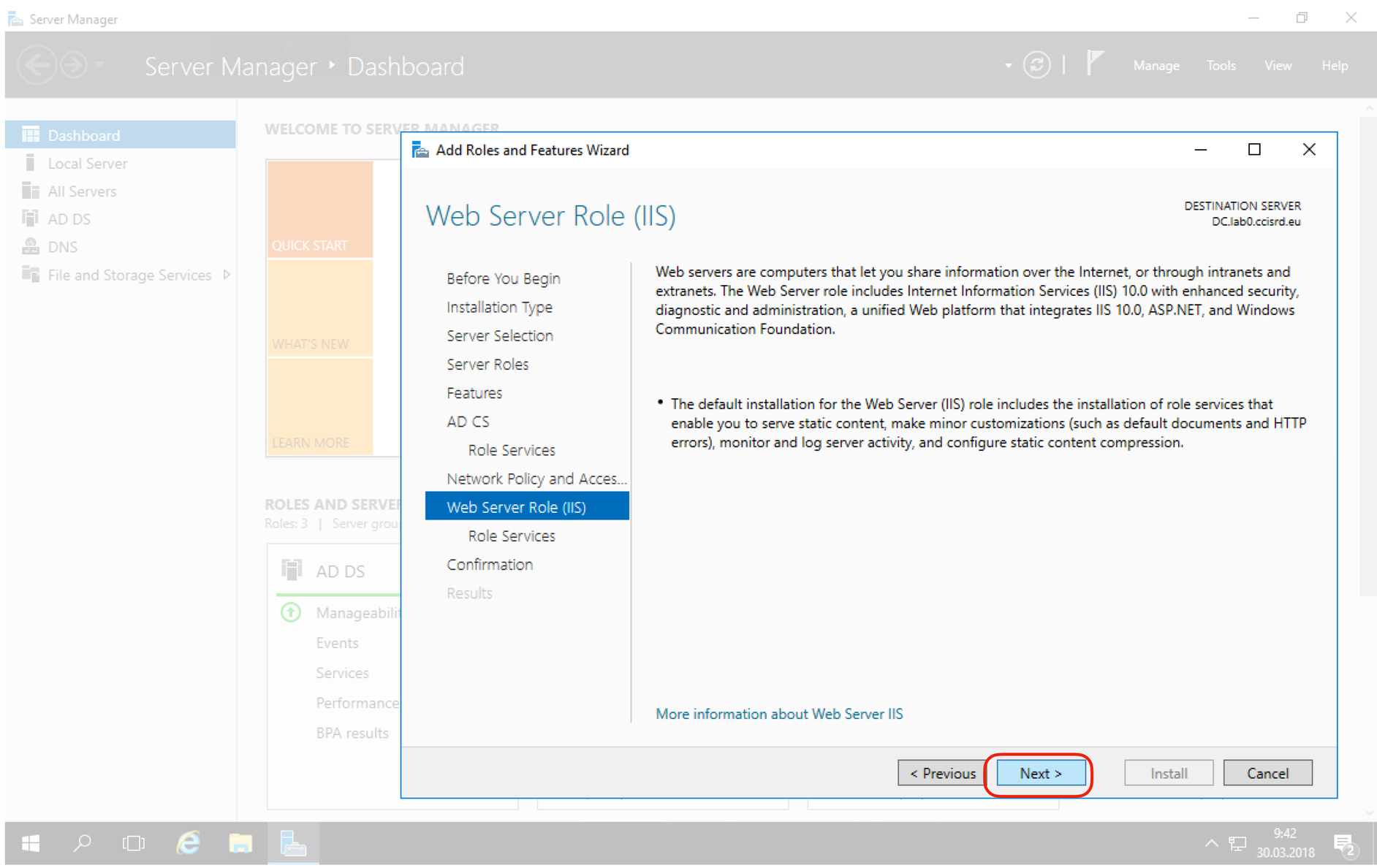
Install NPS role

- Click “Next”



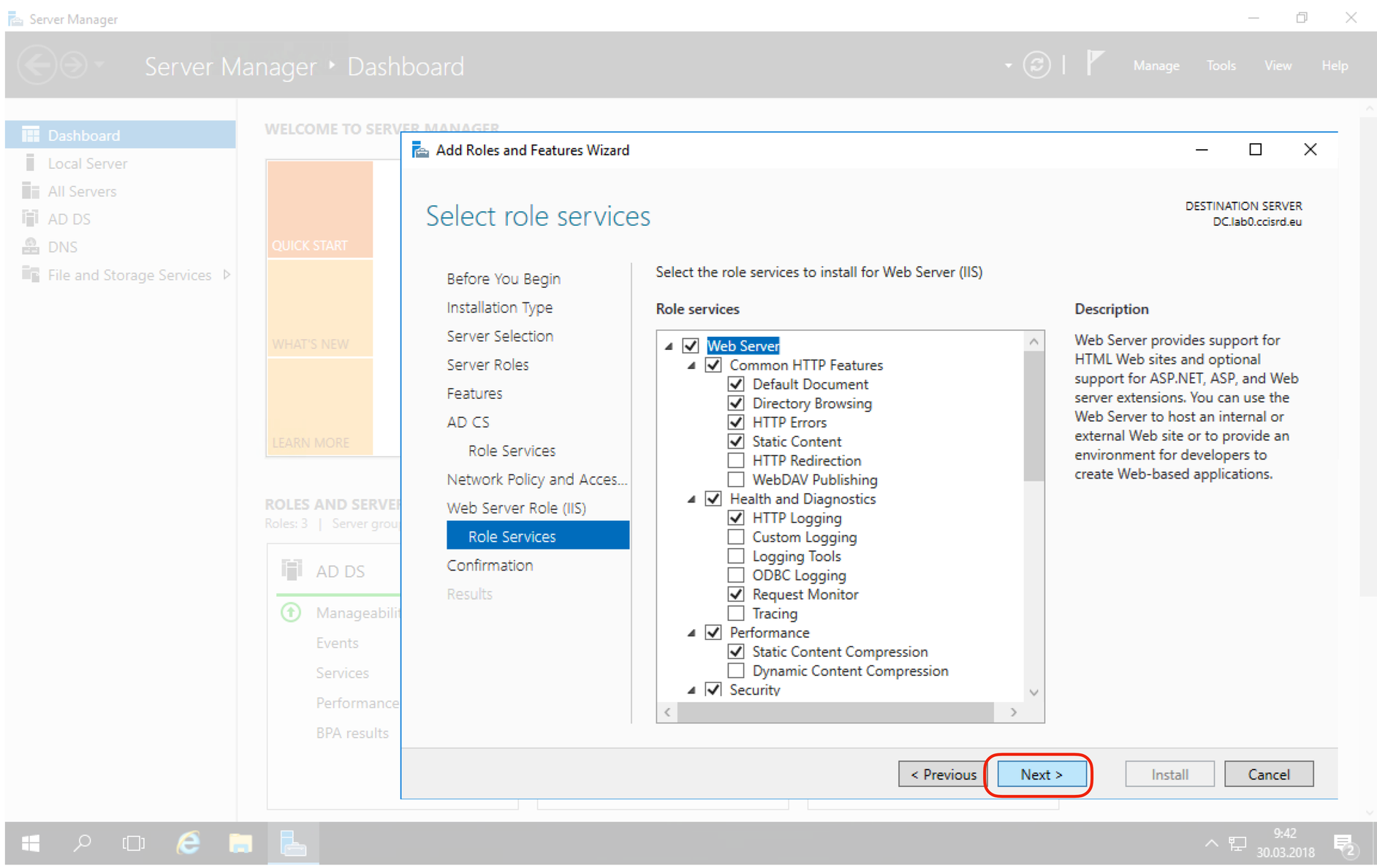
Install NPS and CA role

- Click “Next”



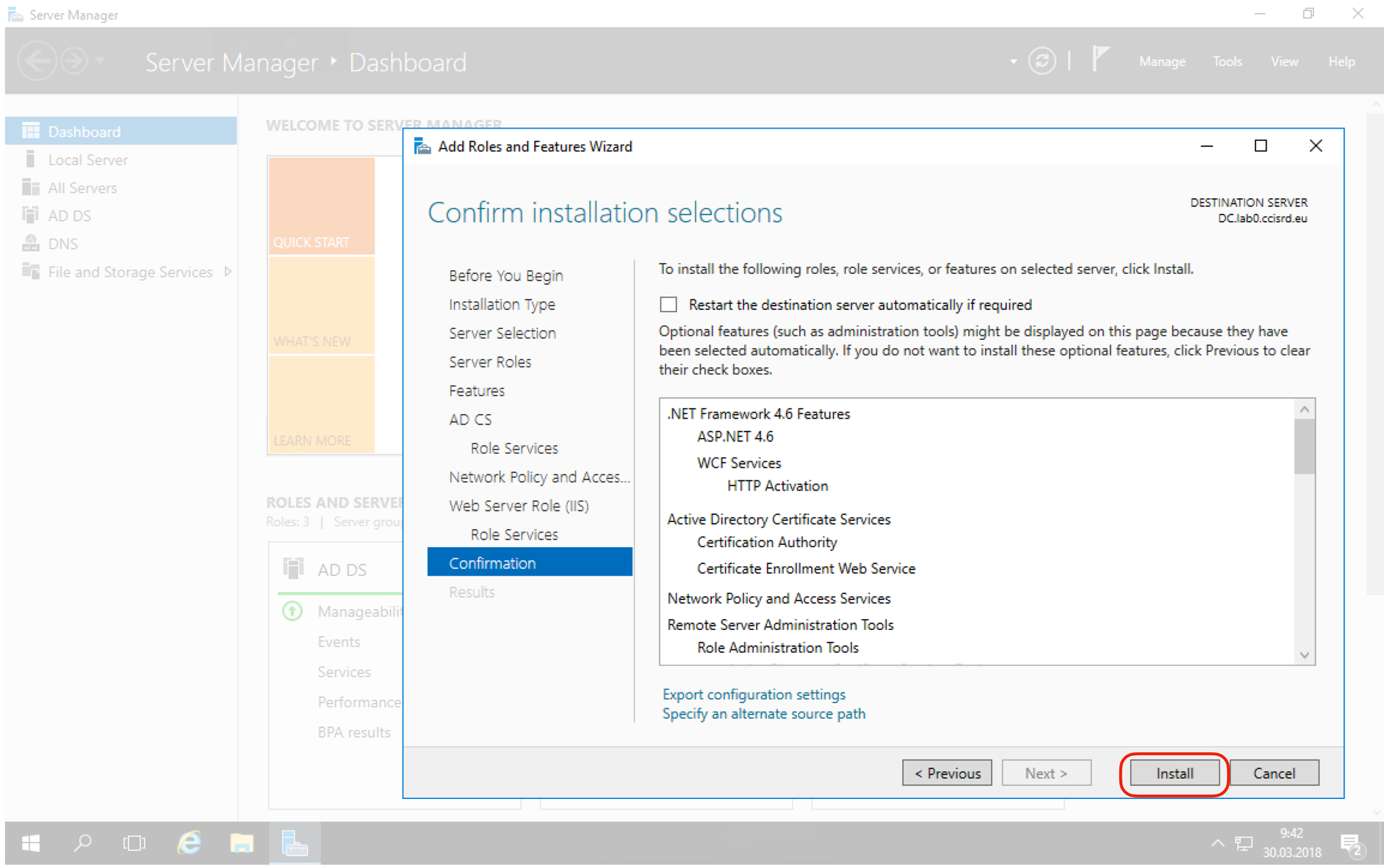
Install NPS and CA role

- Accept default and click “Next”



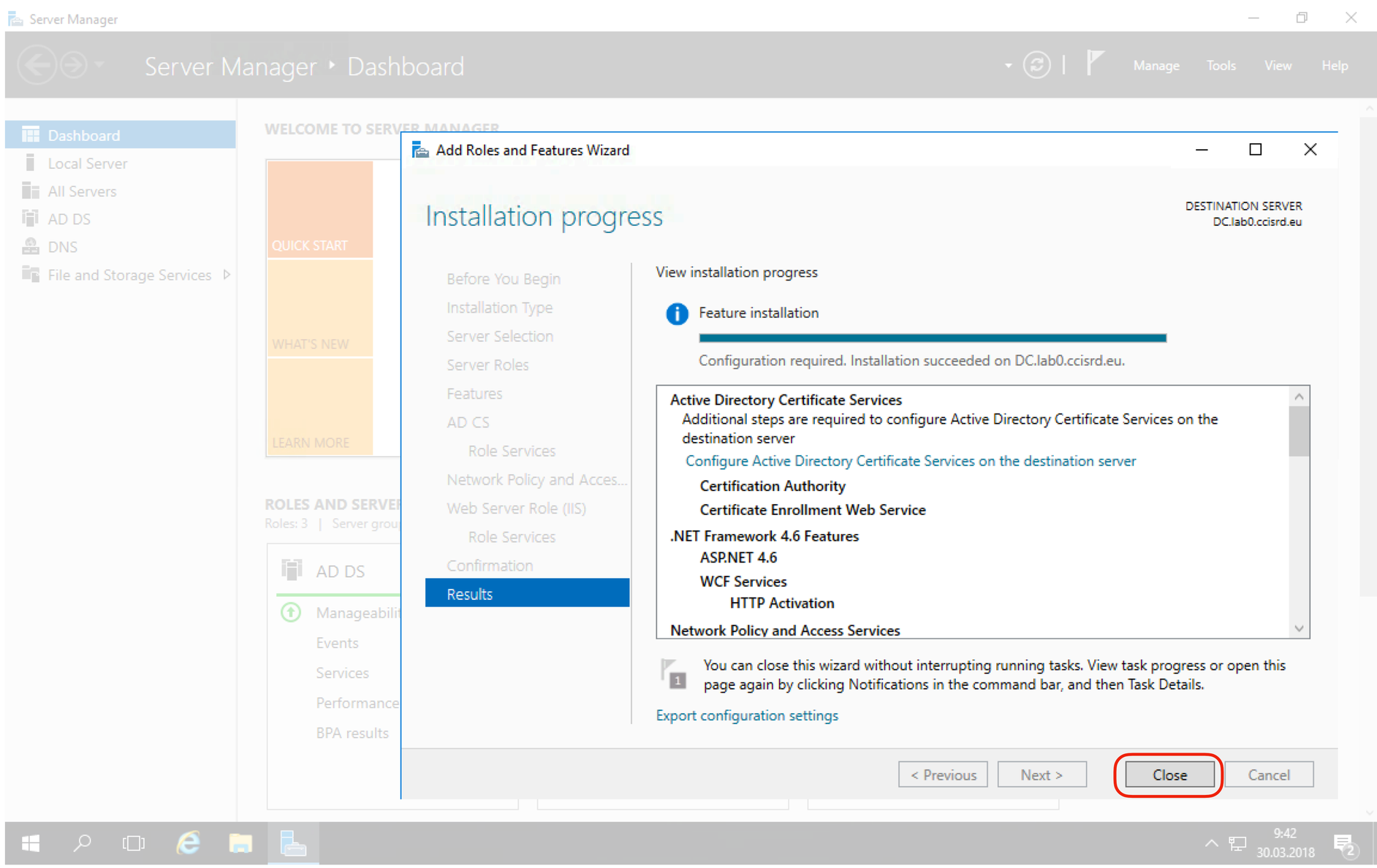
Install NPS and CA role

- Accept default and click “Install”



Install NPS and CA role

- After installation is completed, click “Close”

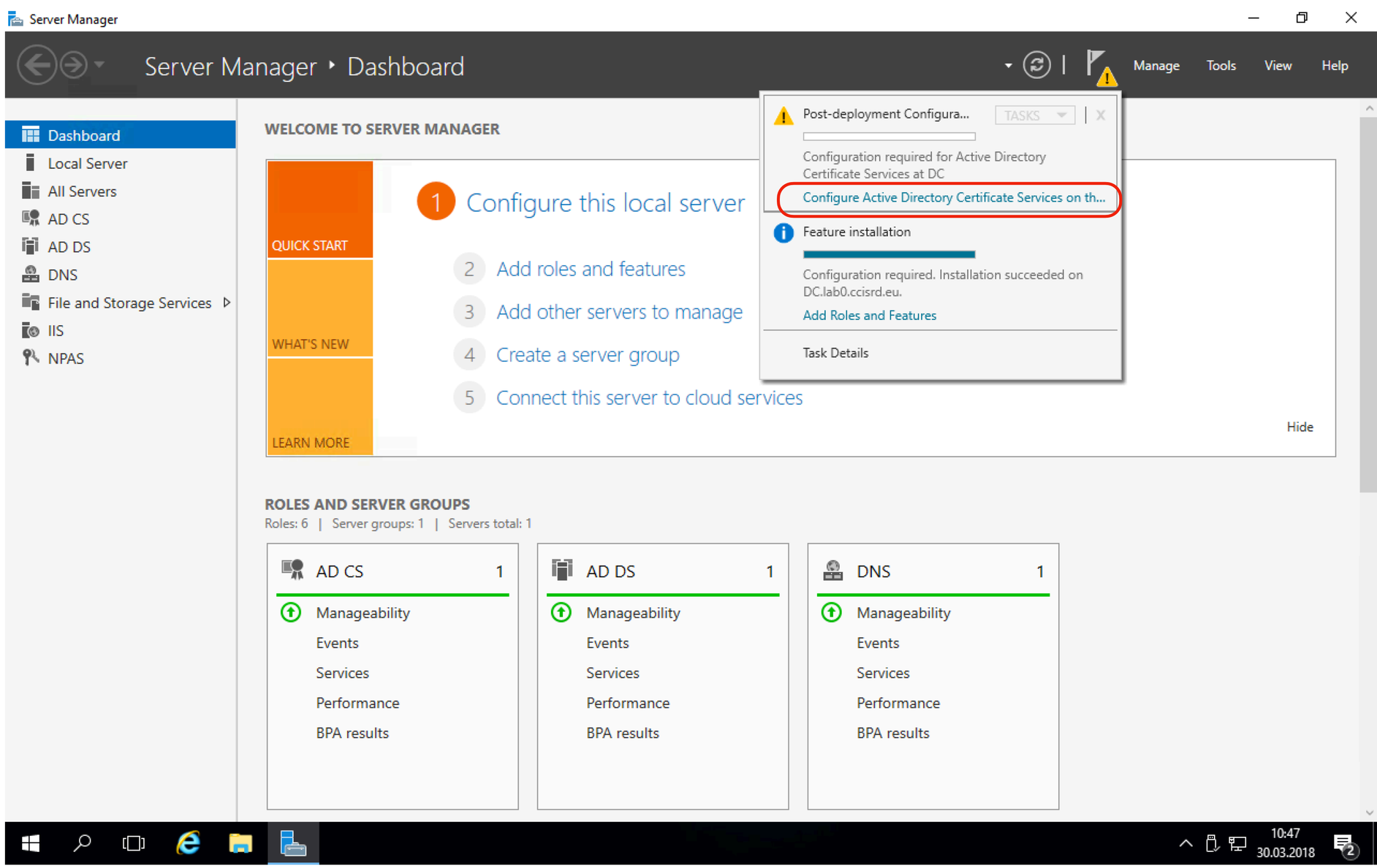


Next Steps

- ~~Install NPS and CA roles on Windows Server~~
- **Configure CA**
- Configure NPS - RADIUS Server
- Reconfigure CAPsMAN
- Install CA on client device's

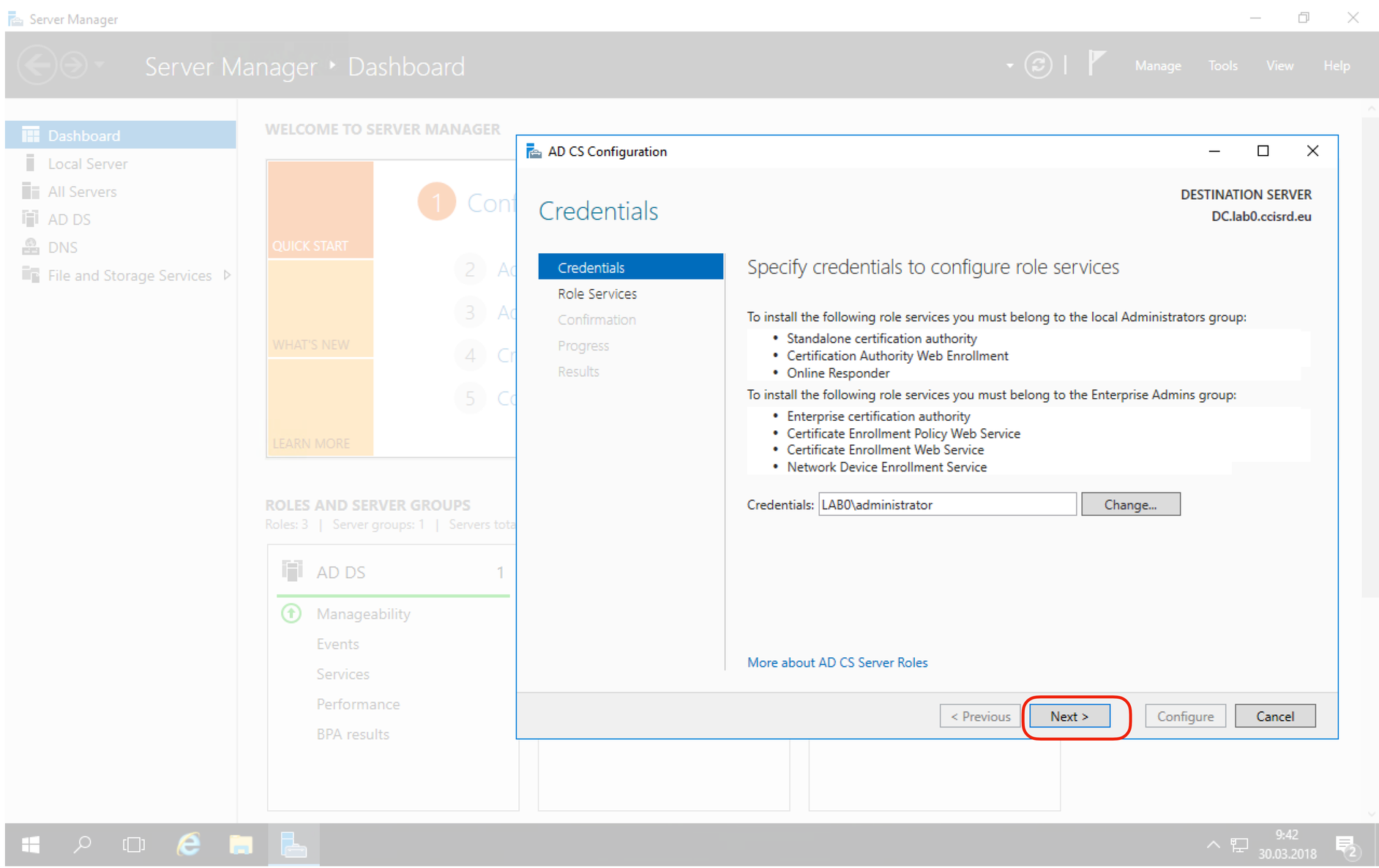
Configure CA

- In Server Manager Dashboard select “Configure Active Directory Certificate Services ..”



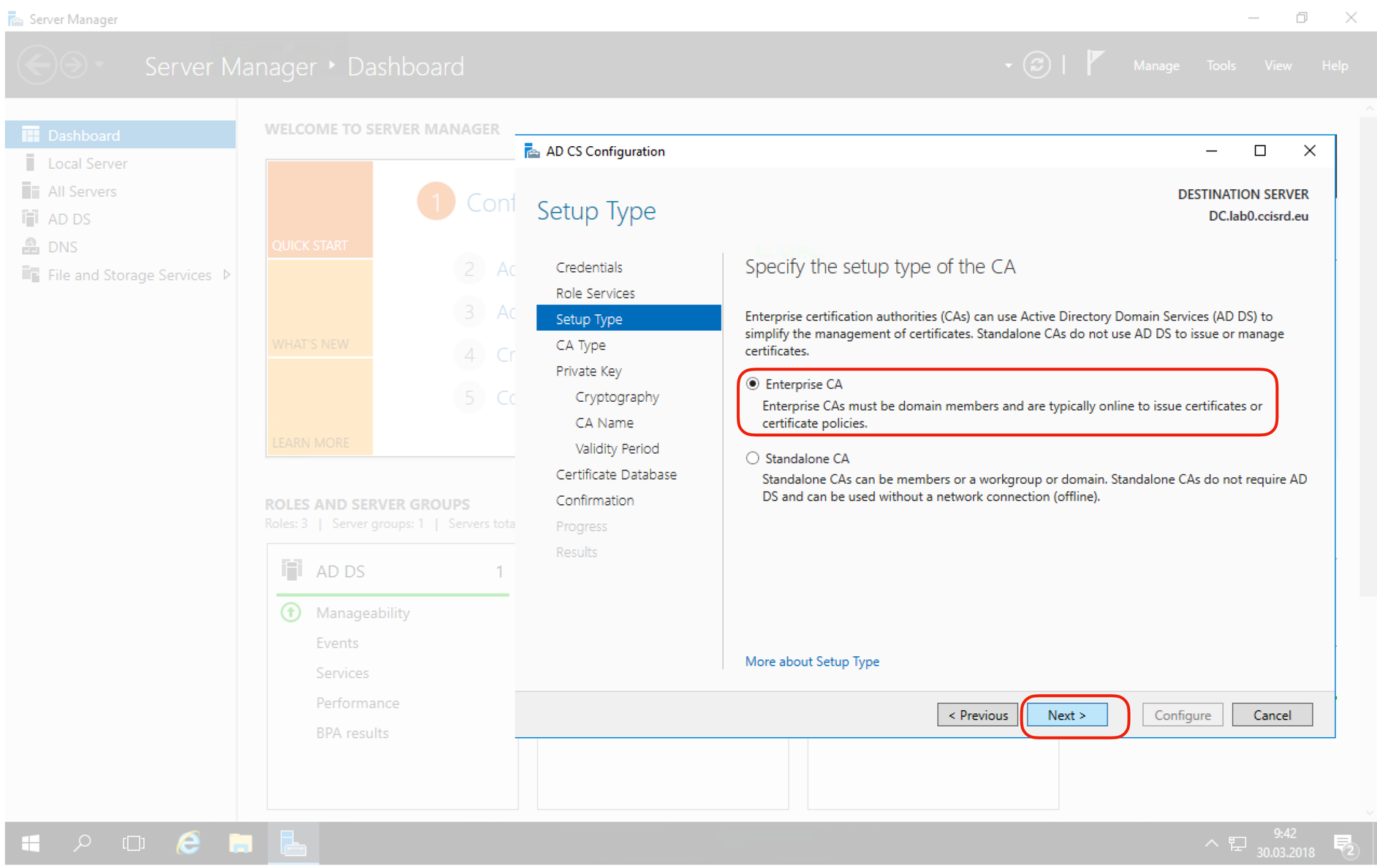
Configure CA

- Accept default and click “Next”



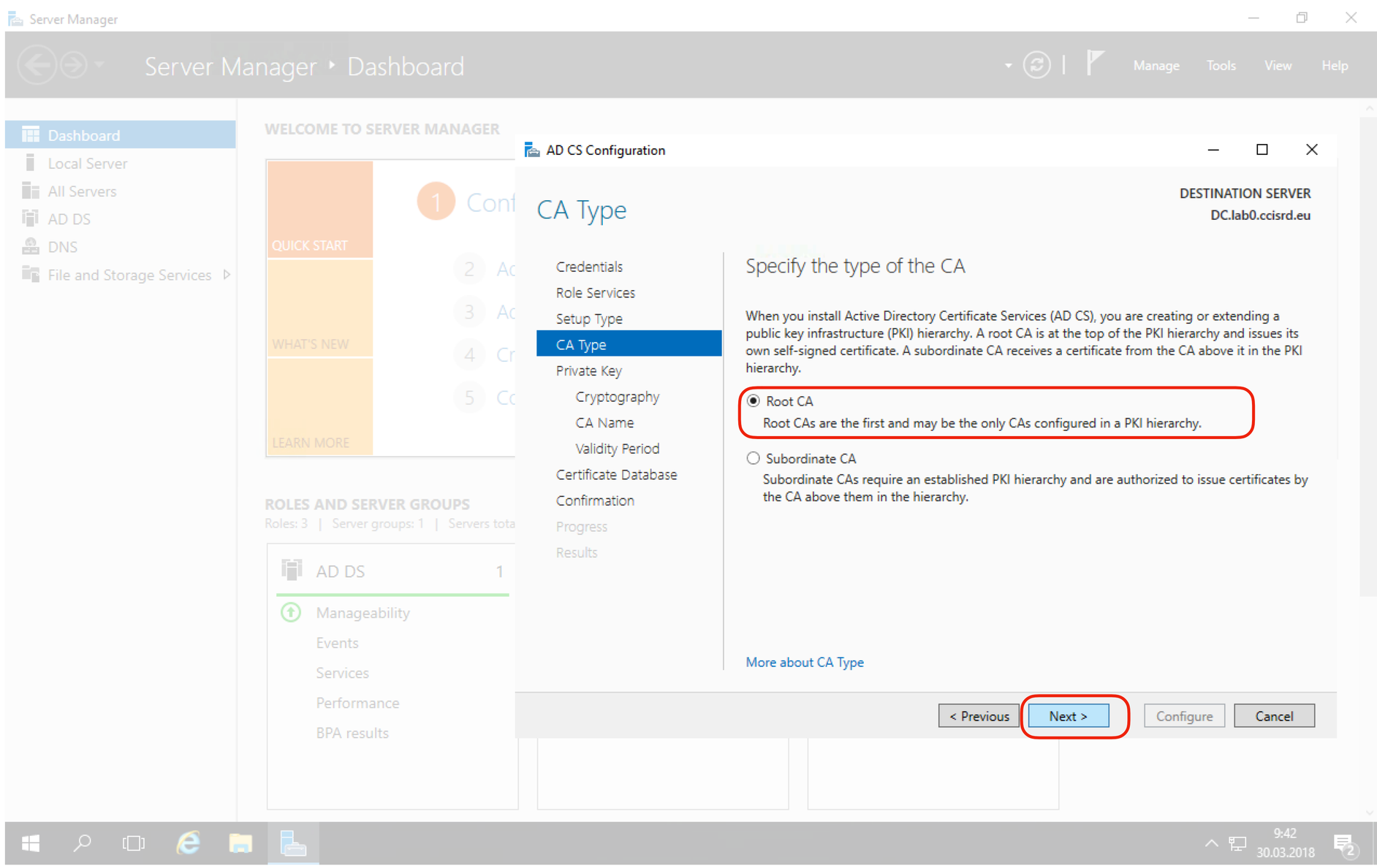
Configure CA

- Select “Enterprise CA” as Setup Type and click “Next”



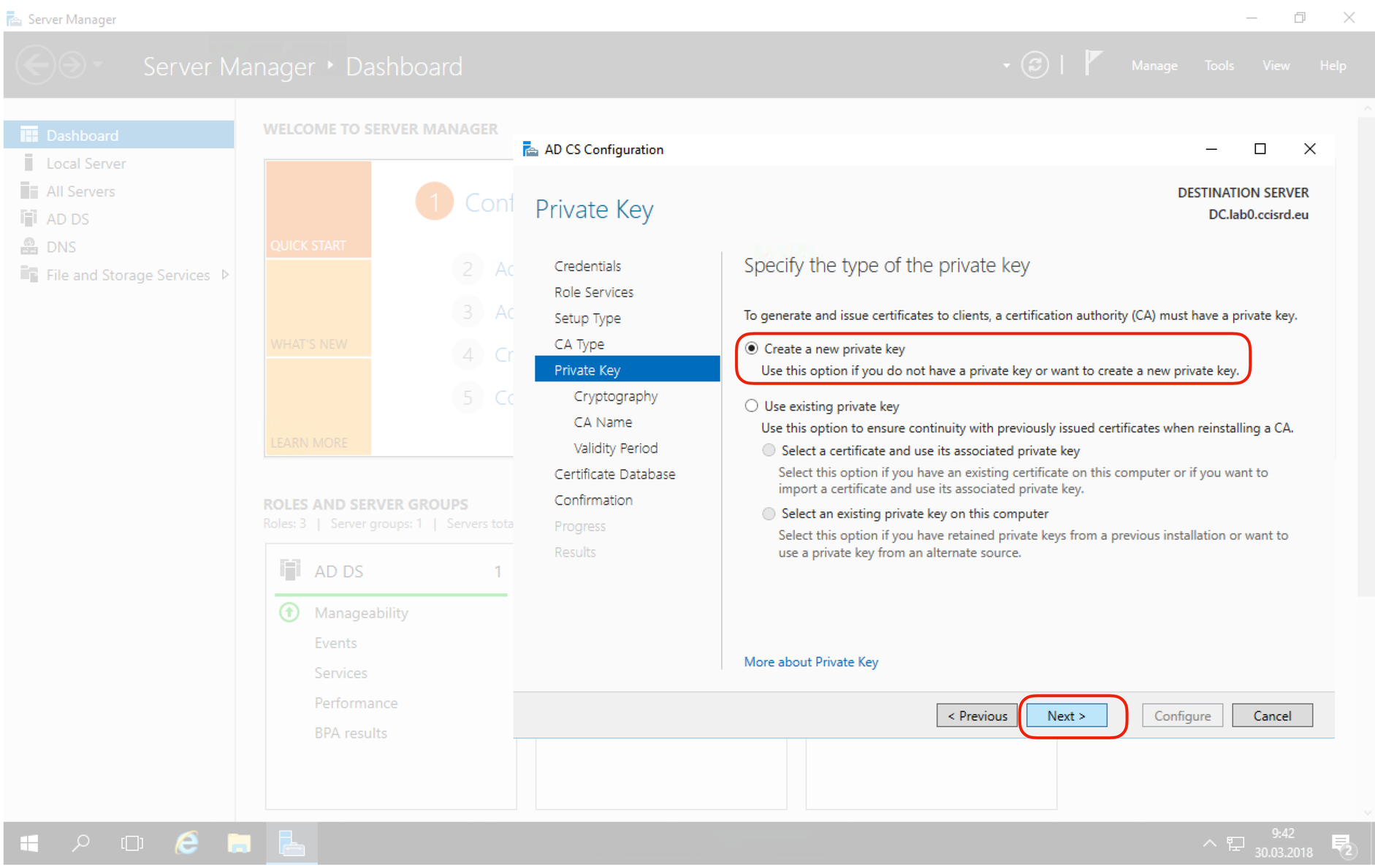
Configure CA

- Select “Root CA” as CA type and click “Next”



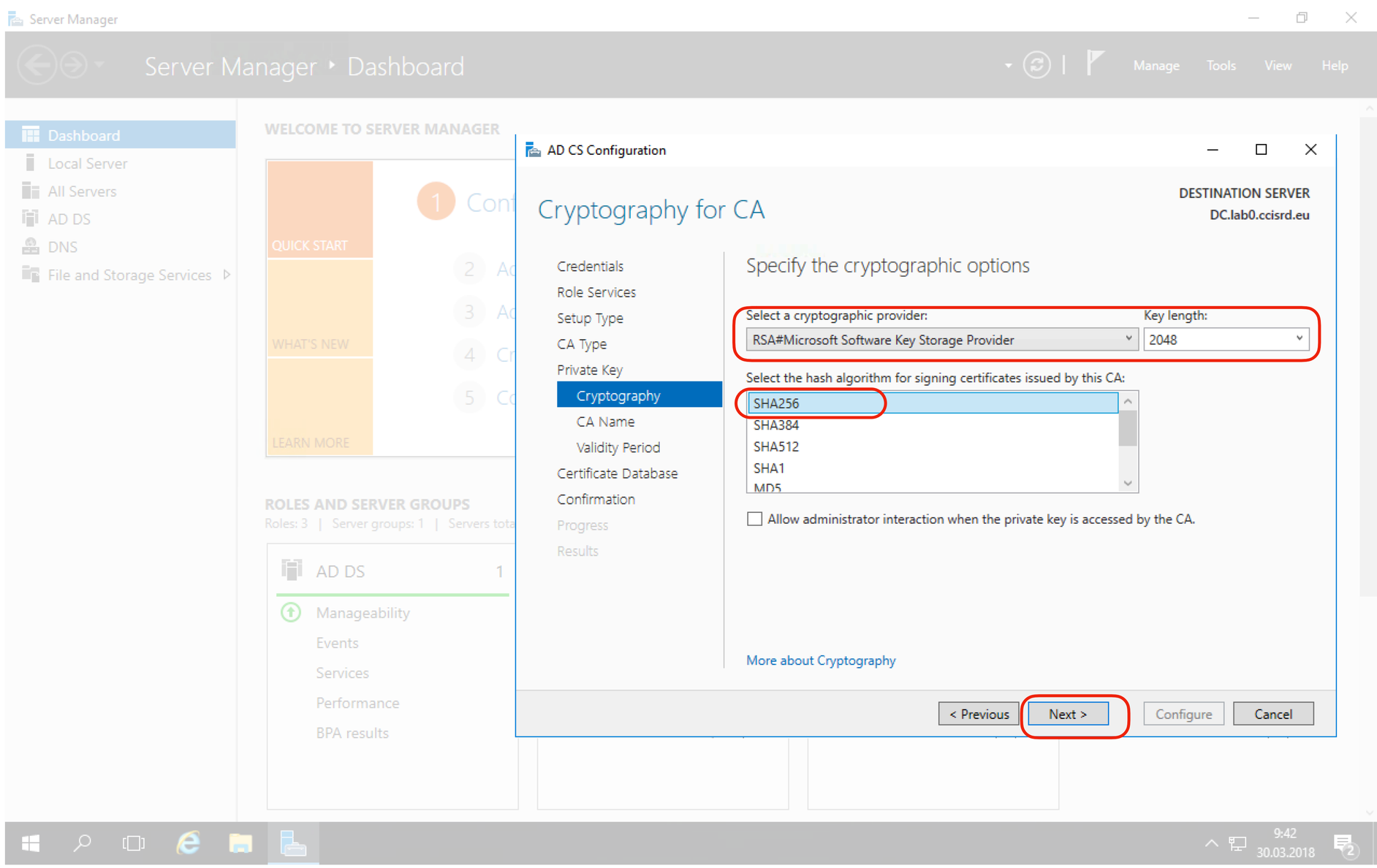
Configure CA

- Select “Create a new private key” and click “Next”



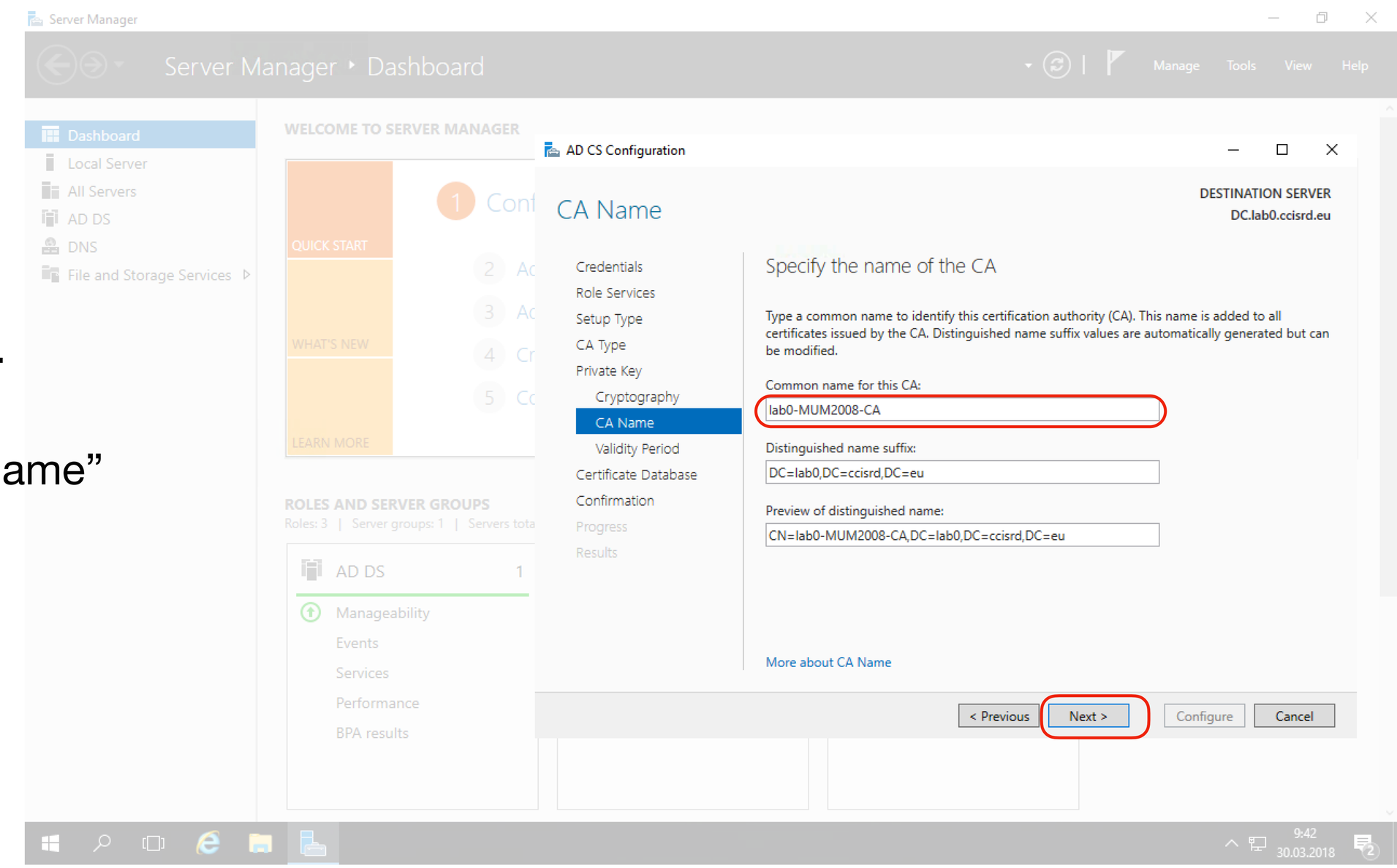
Configure CA

- Select “RSA#Microsoft Software Key Storage Provider” as cryptographic provider
- Set Key lenght to 2048
- Select “SHA256” as hash algorithm
- Click “Next”



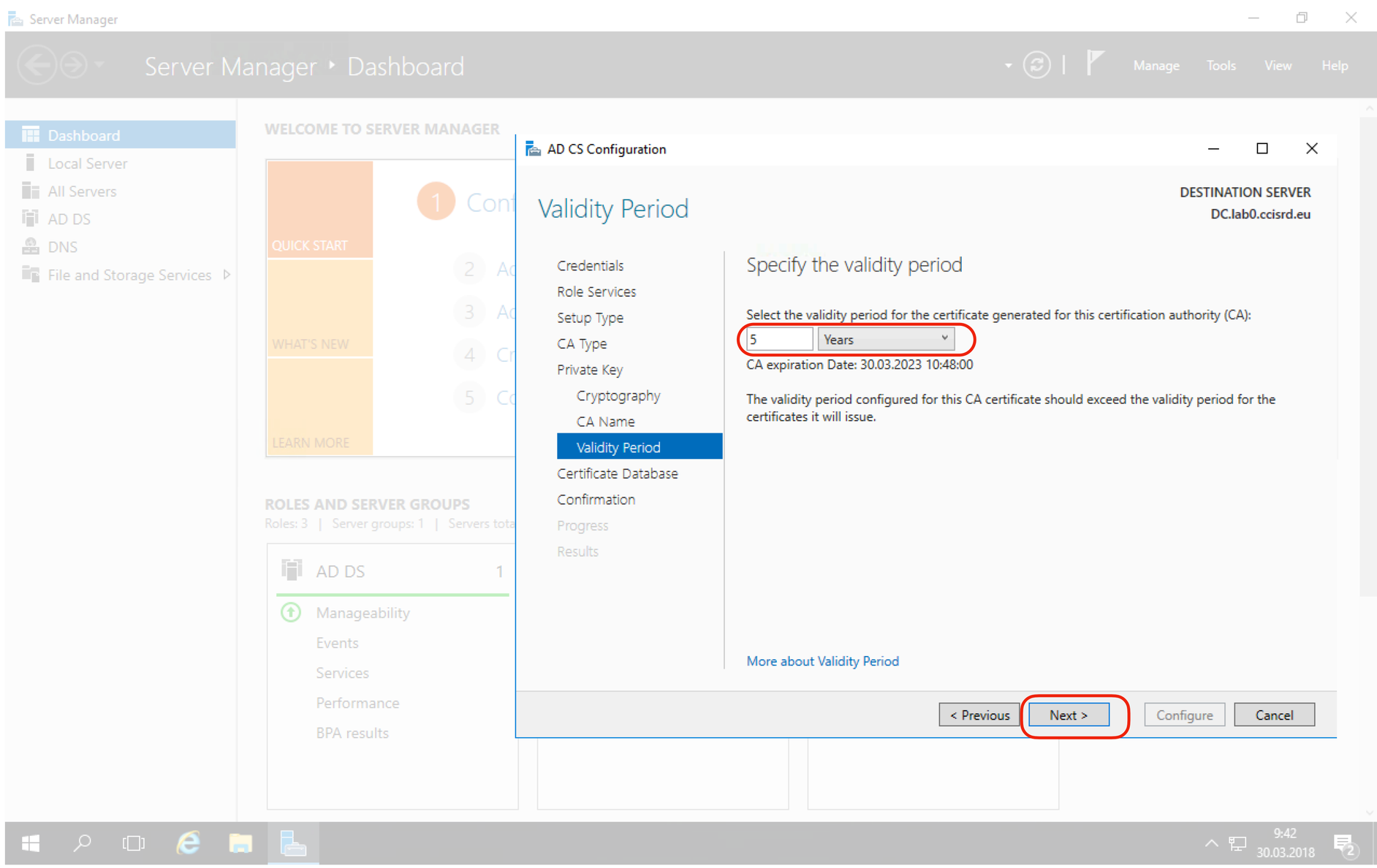
Configure CA

- Set logical “Common name for this CA”, e.g. “lab0-MUM2018-ca”
- Verify “Distinguished name”
- Click “Next”



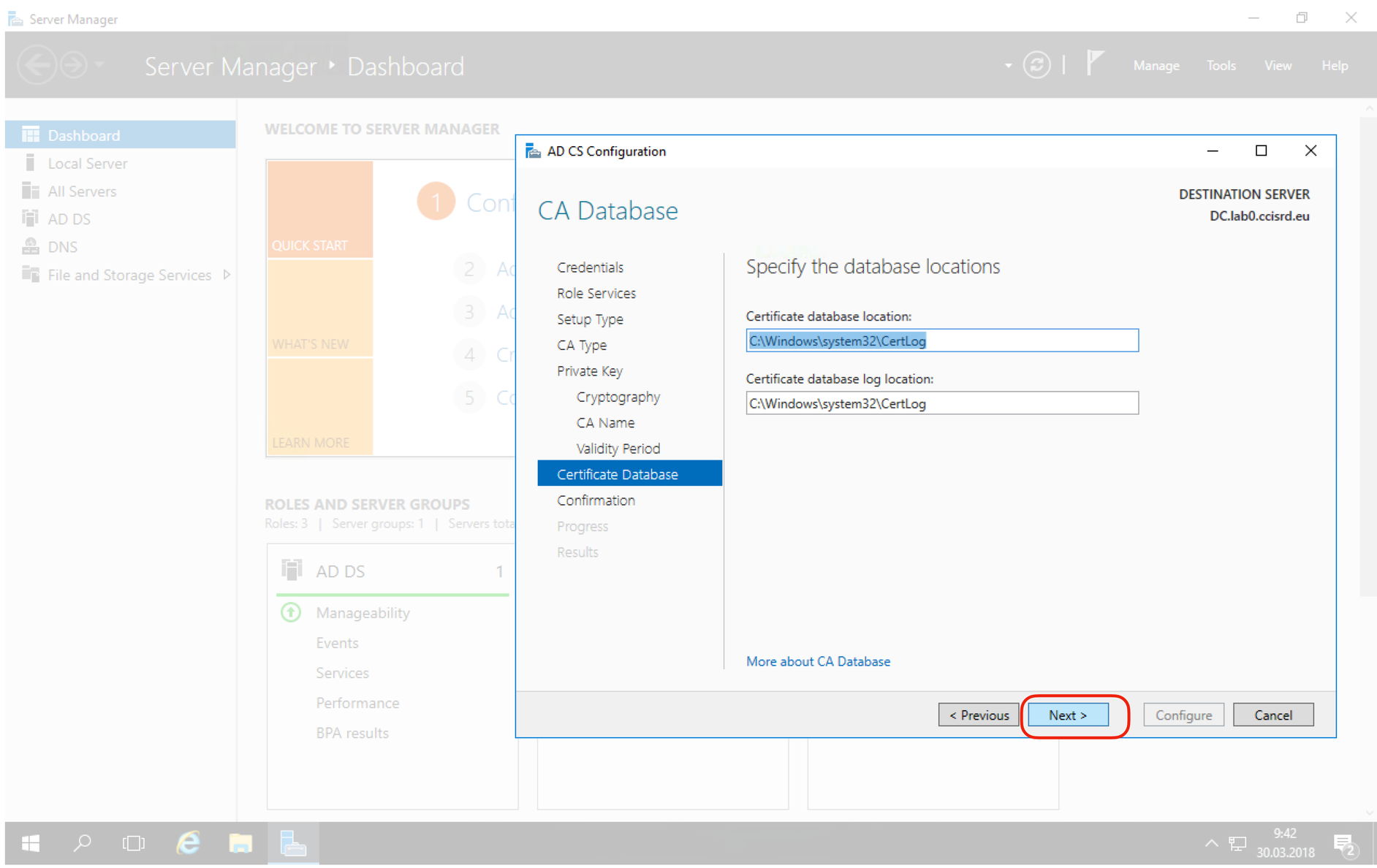
Configure CA

- Set validity period for the CA, e.g. 5 Years
- Click “Next”



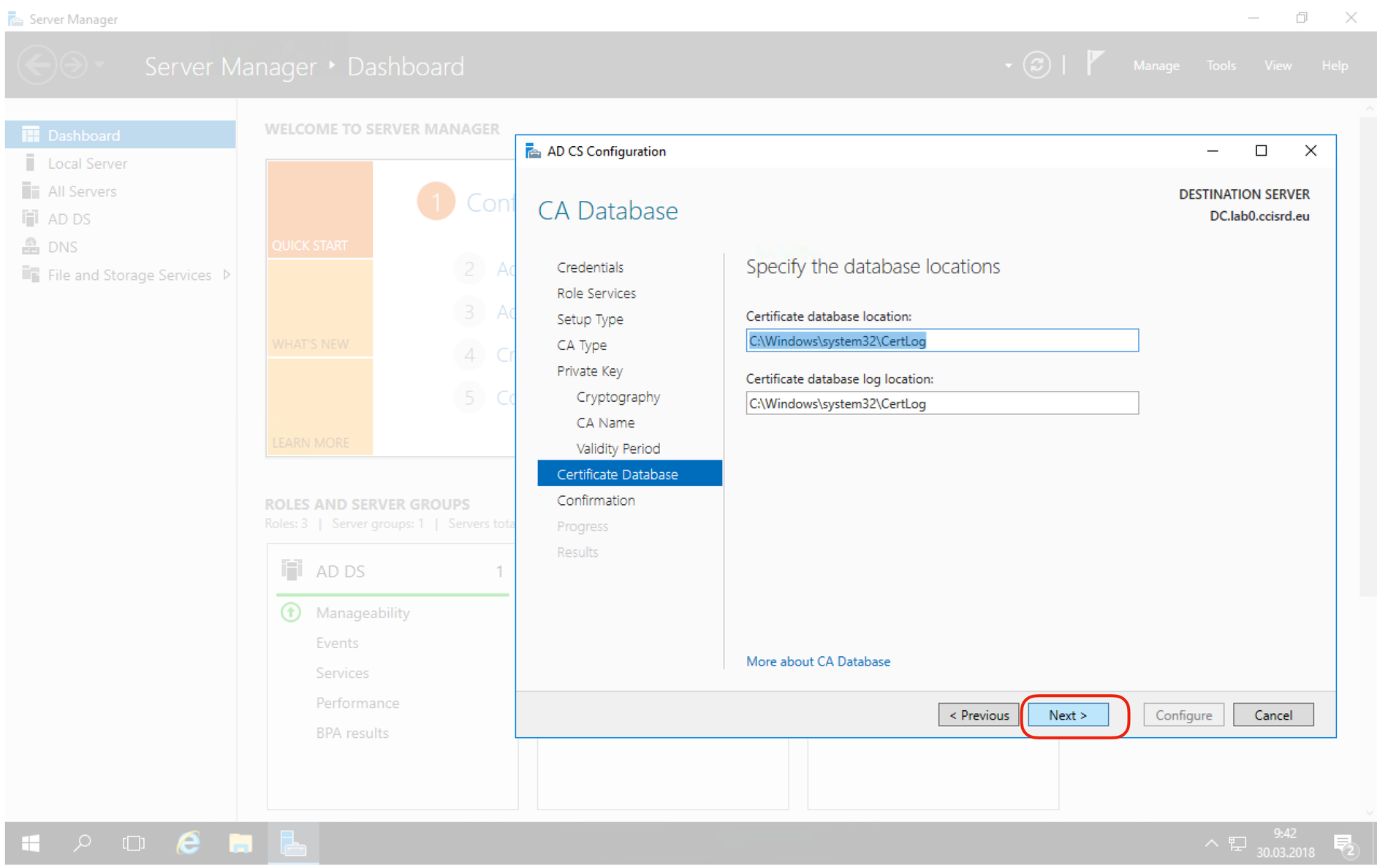
Configure CA

- Accept default and click “Next”



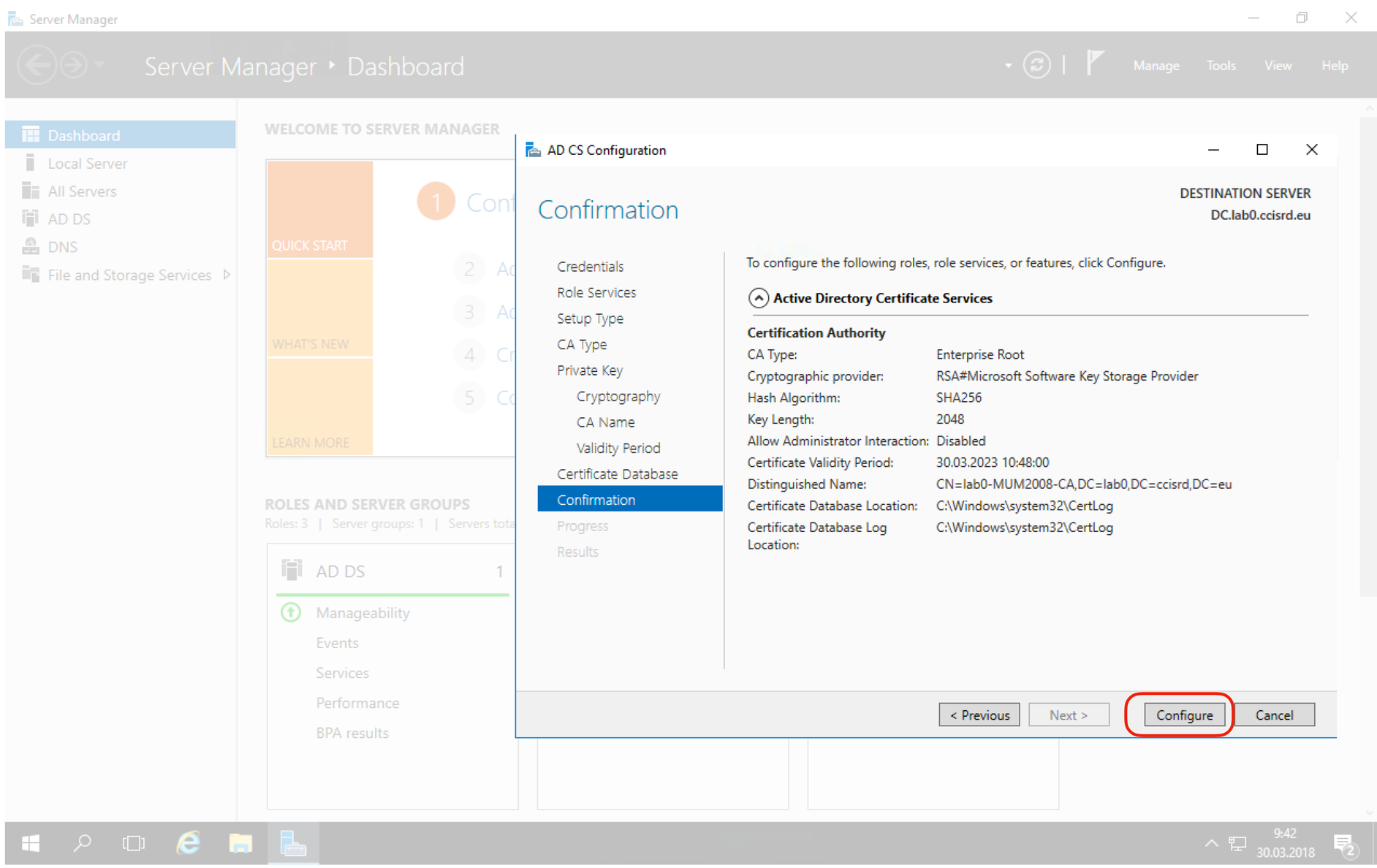
Configure CA

- Accept default and click “Next”



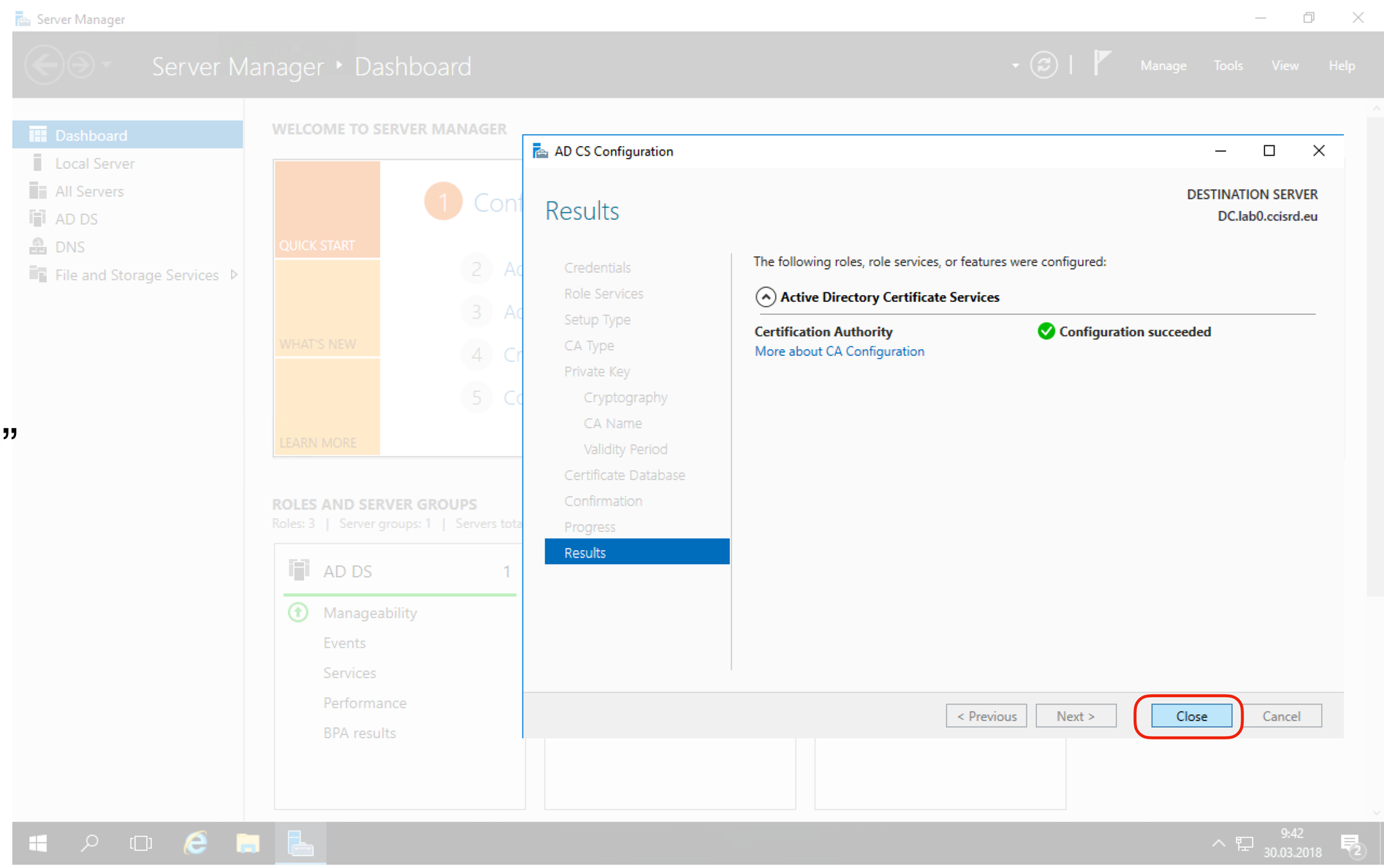
Configure CA

- Accept default and click “Configure”



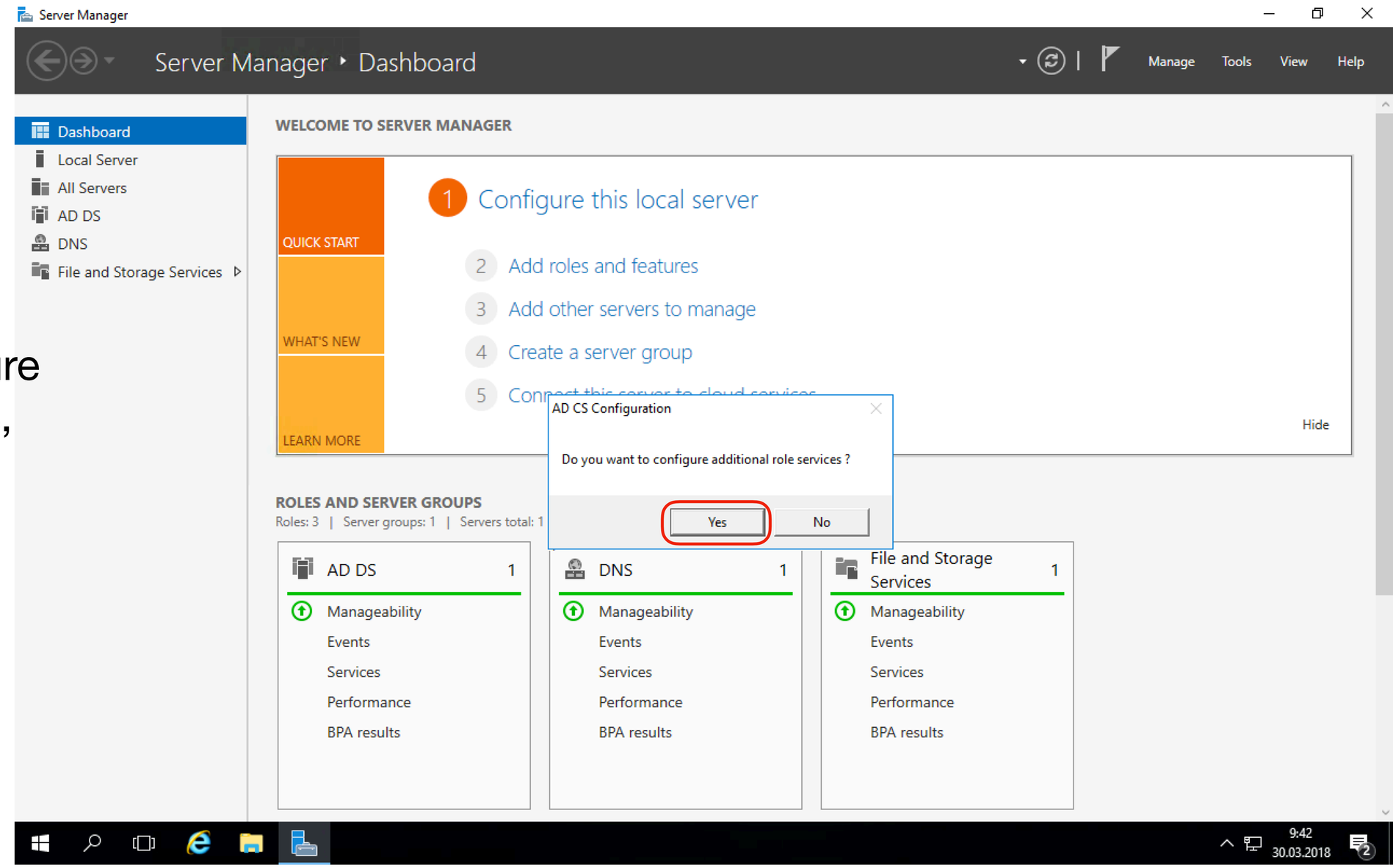
Configure CA

- After configuration complete, click “Close”



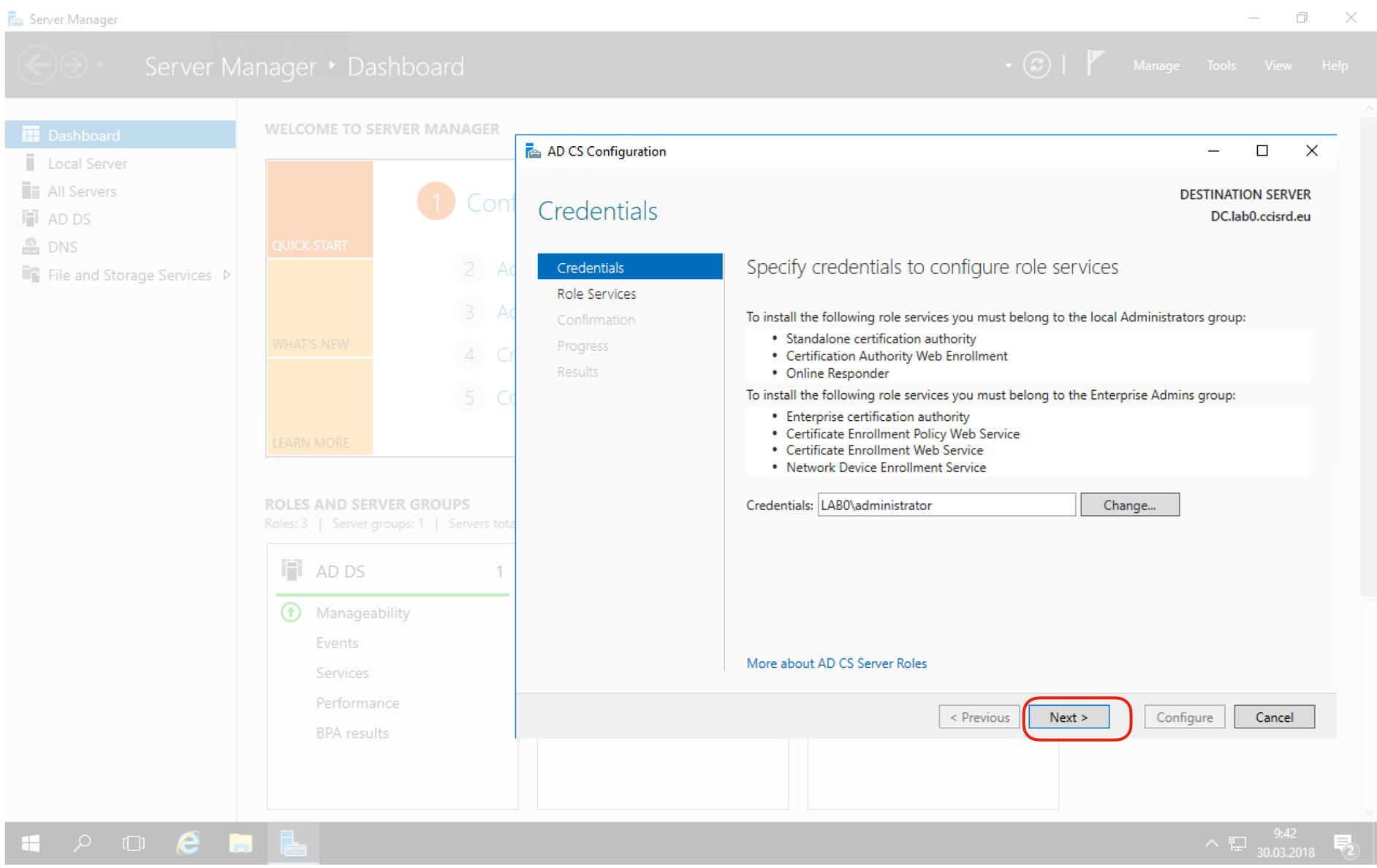
Configure CA

- When asked to configure additional role services, click “Yes”



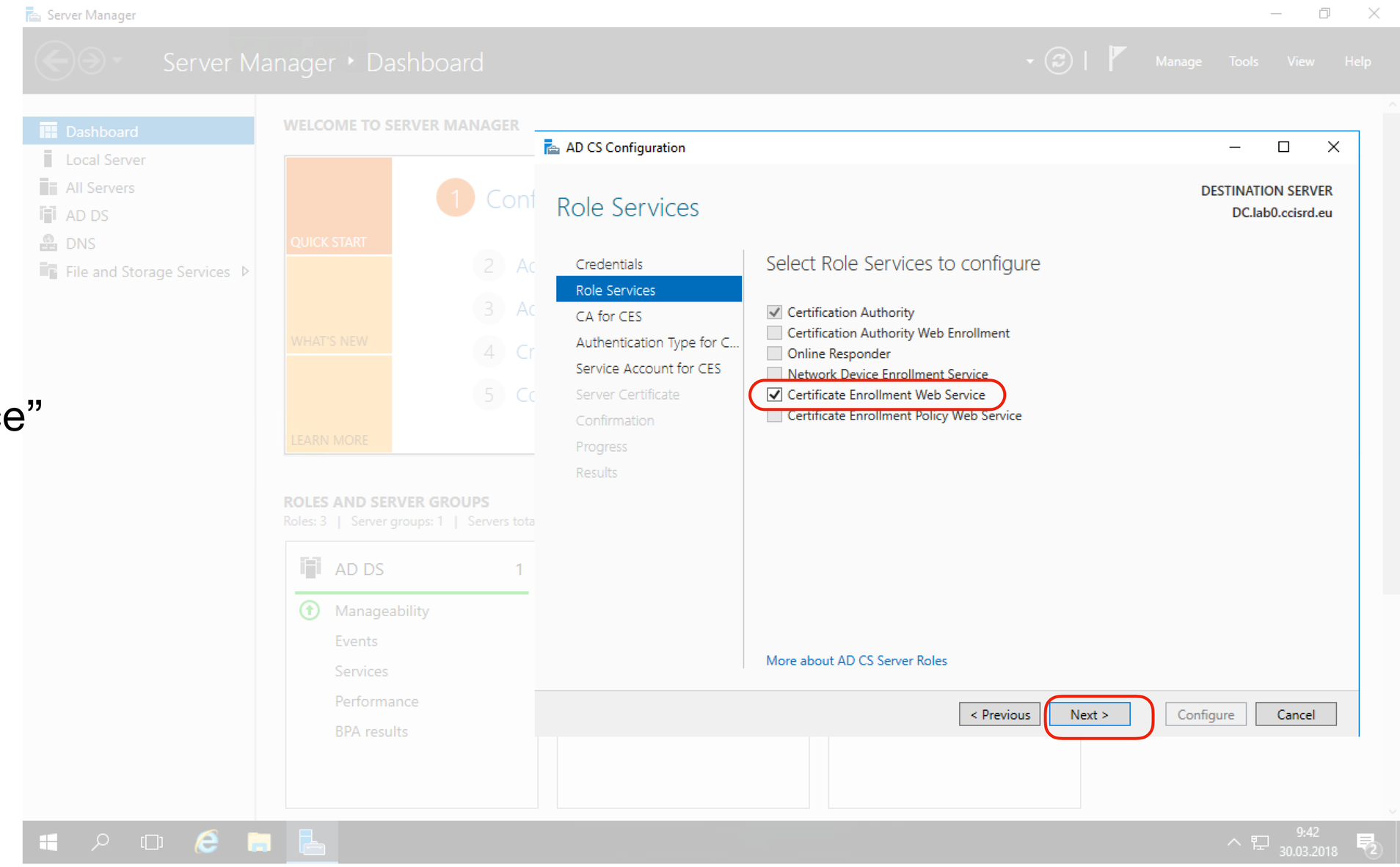
Configure CA

- Accept default and click “Next”



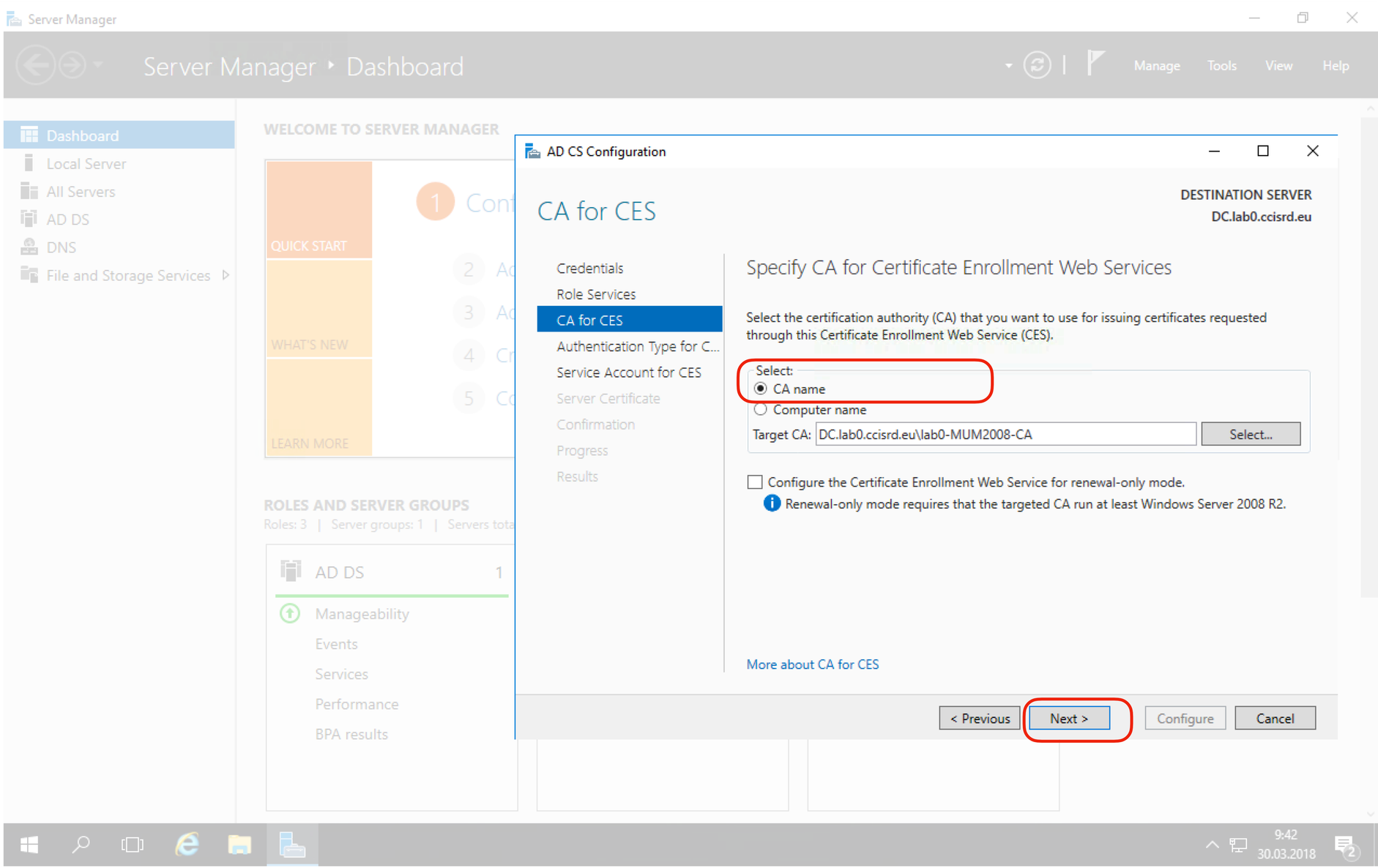
Configure CA

- Select “Certificate Enrollment Web Service” and Click “Next”



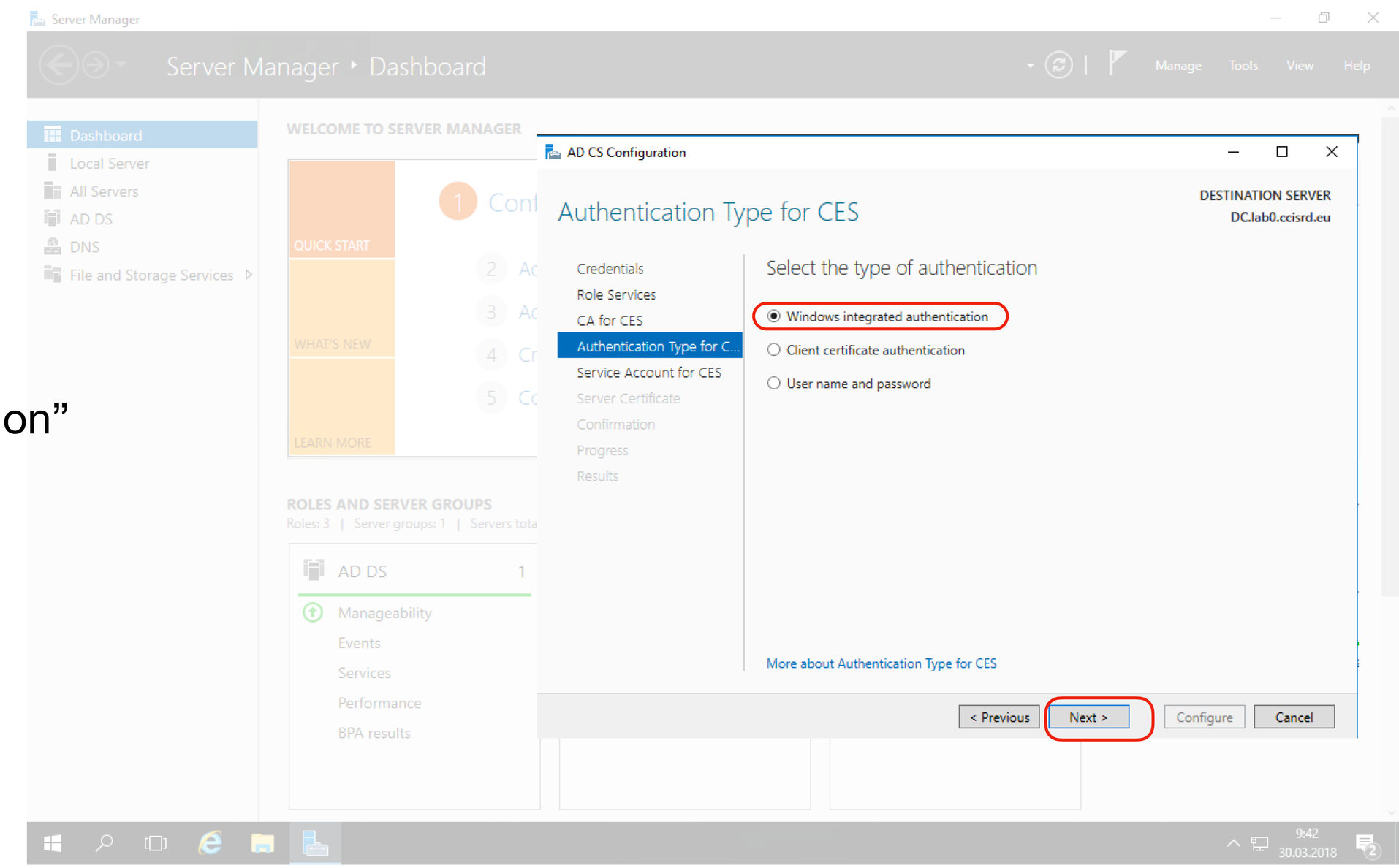
Configure CA

- Select “CA Name” and Click “Next”



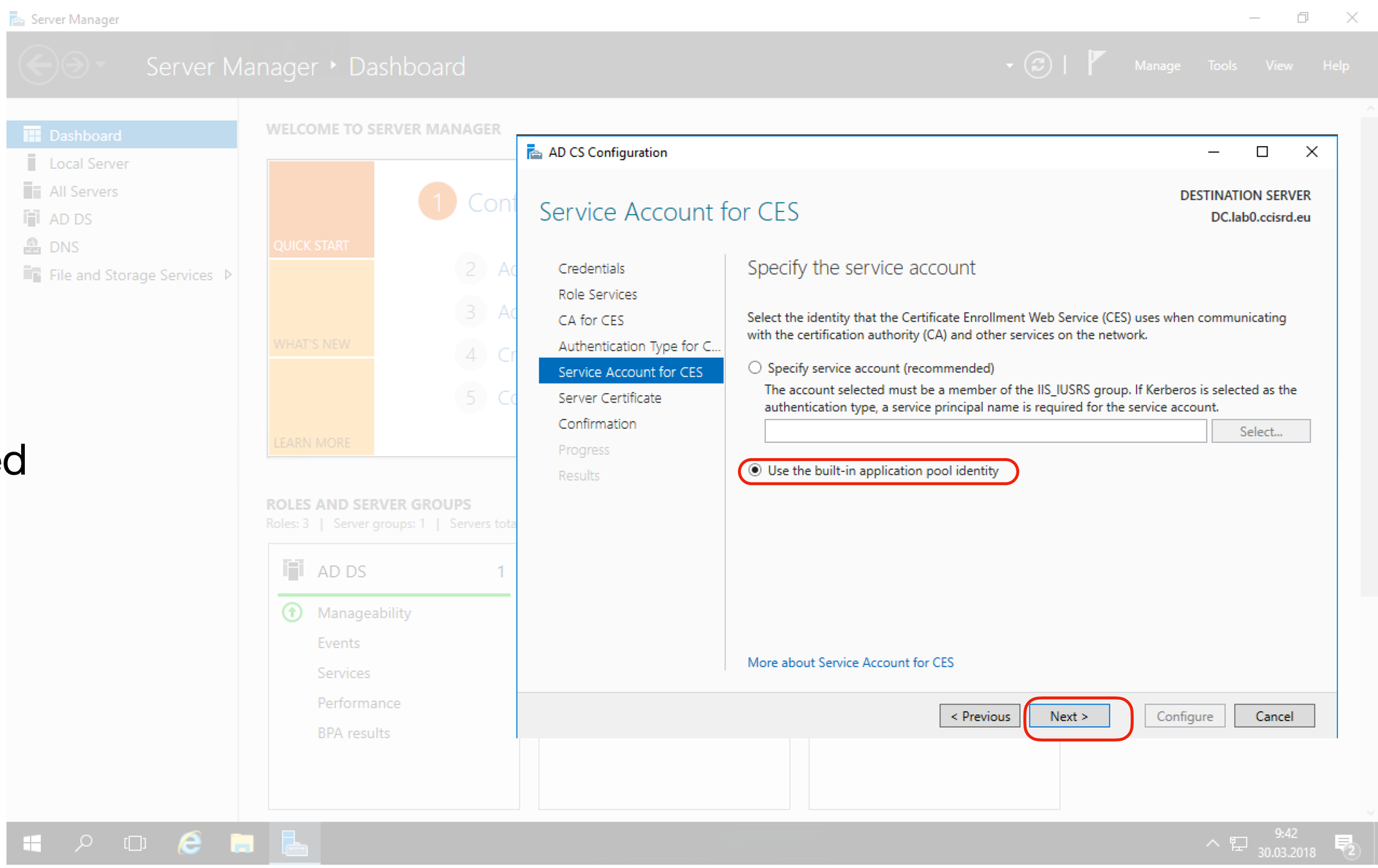
Configure CA

- Select “Windows integrated authentication” and Click “Next”



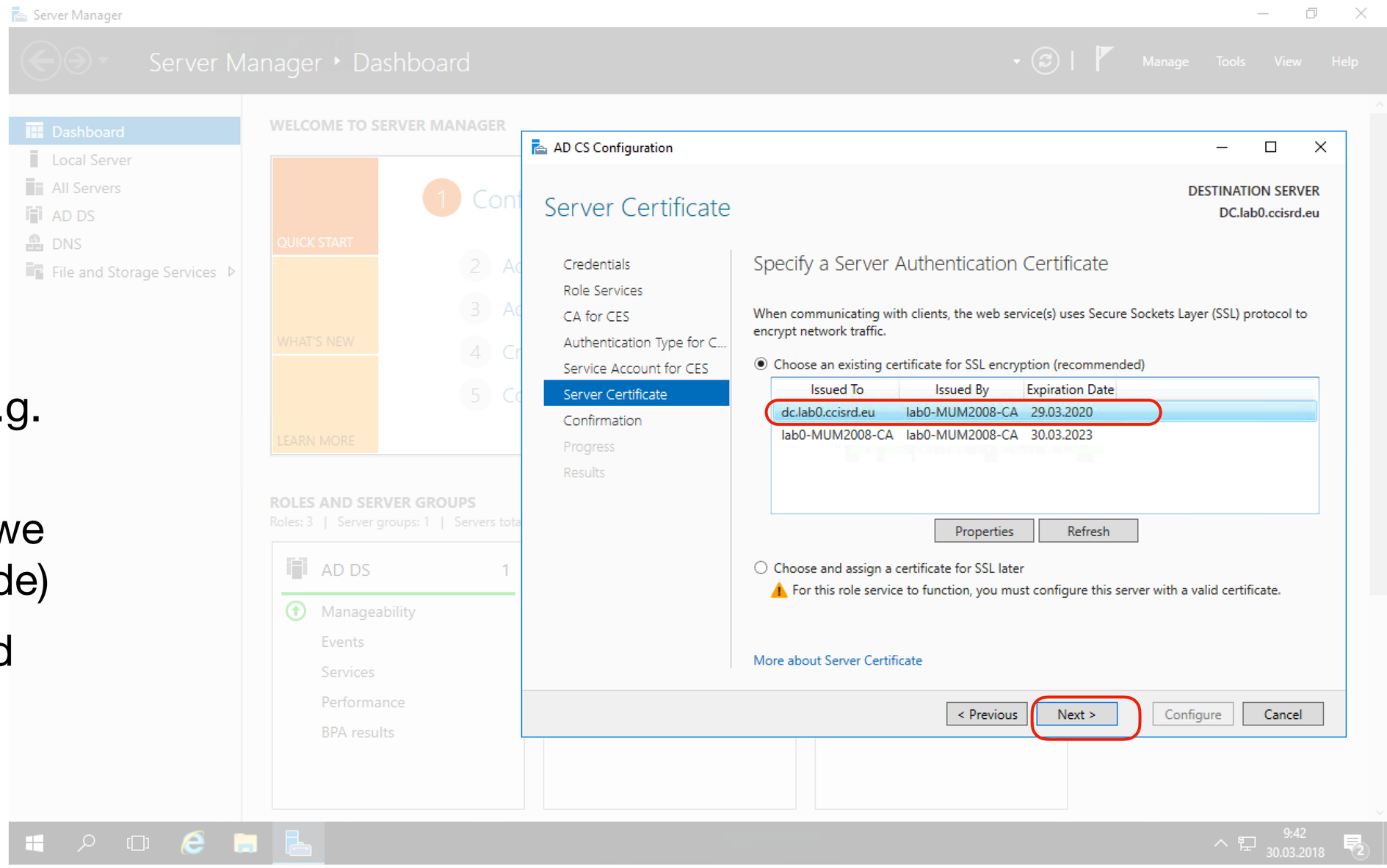
Configure CA

- In our lab select “Use the built-in application pool identity”, in real case specify service account. Usually needed to create new one.
- Click “Next”



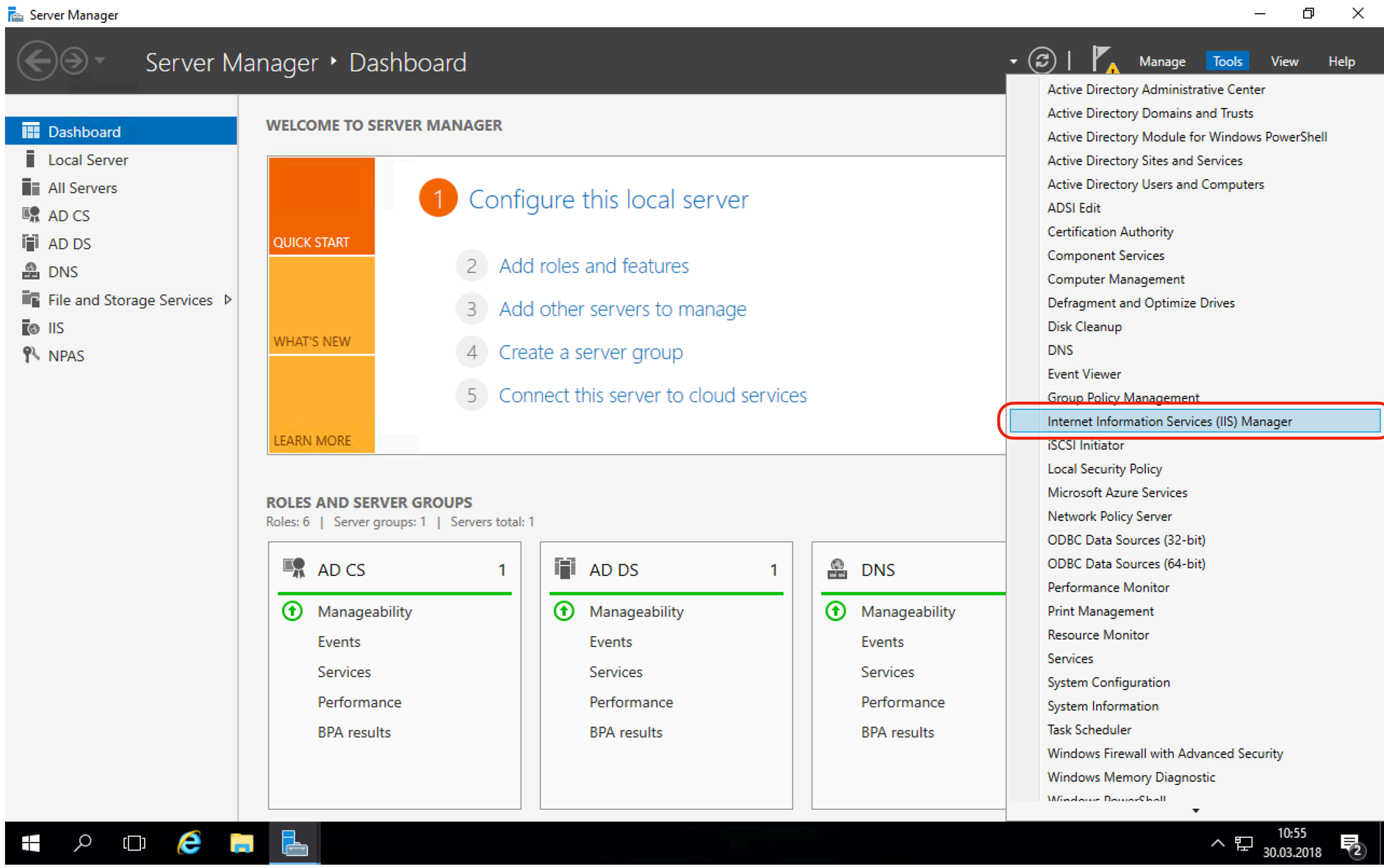
Configure CA

- Specify a Server Authentication Certificate.
- “Issued to” must be server’s fully qualified domain name FQDN (e.g. dc.lab0.ccisrd.eu)
- In such does not exist we will create one (next slide)
- If already exist, proceed to slide #50



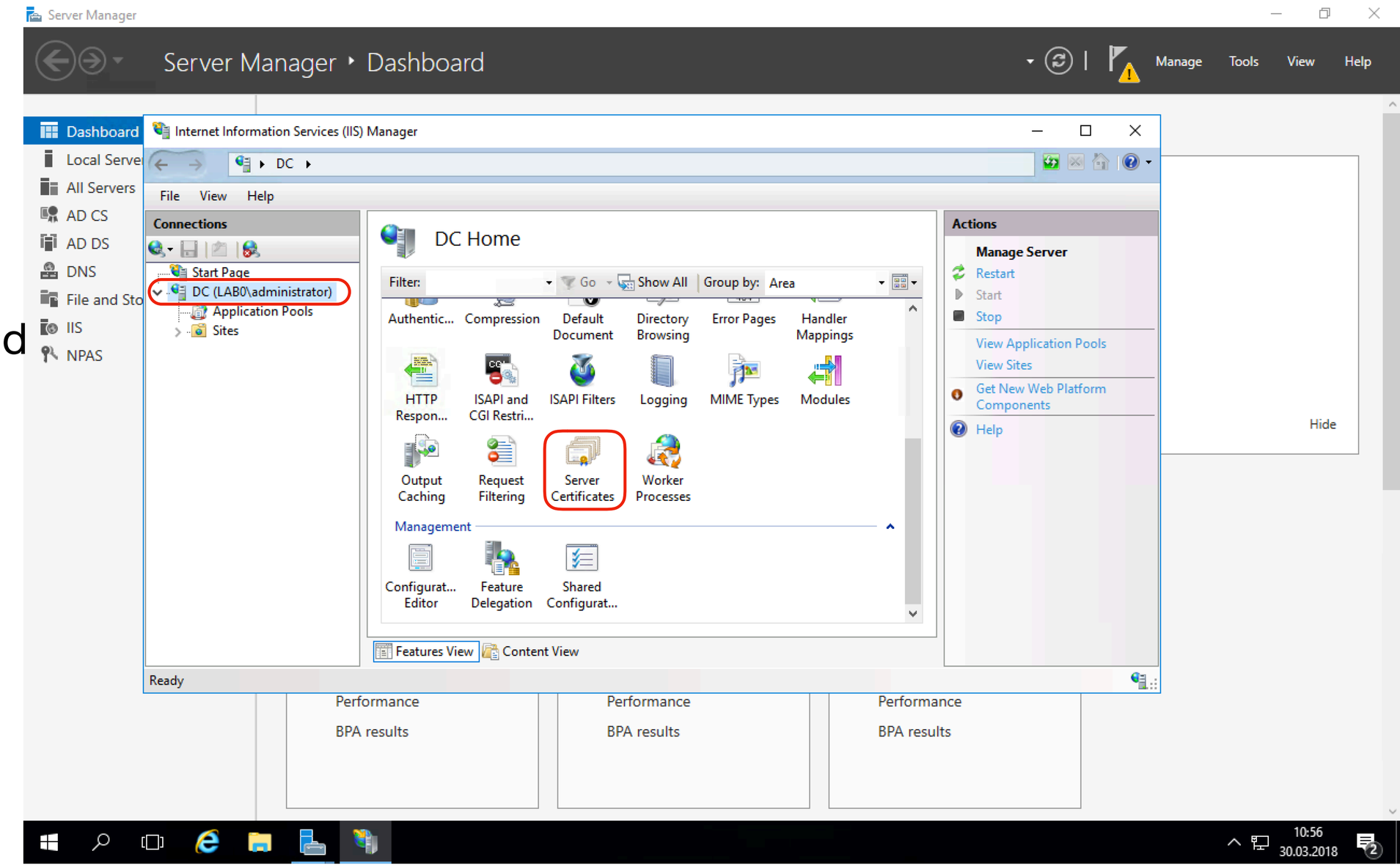
Configure CA

- Open “Internet Information Services (IIS) Manager”.



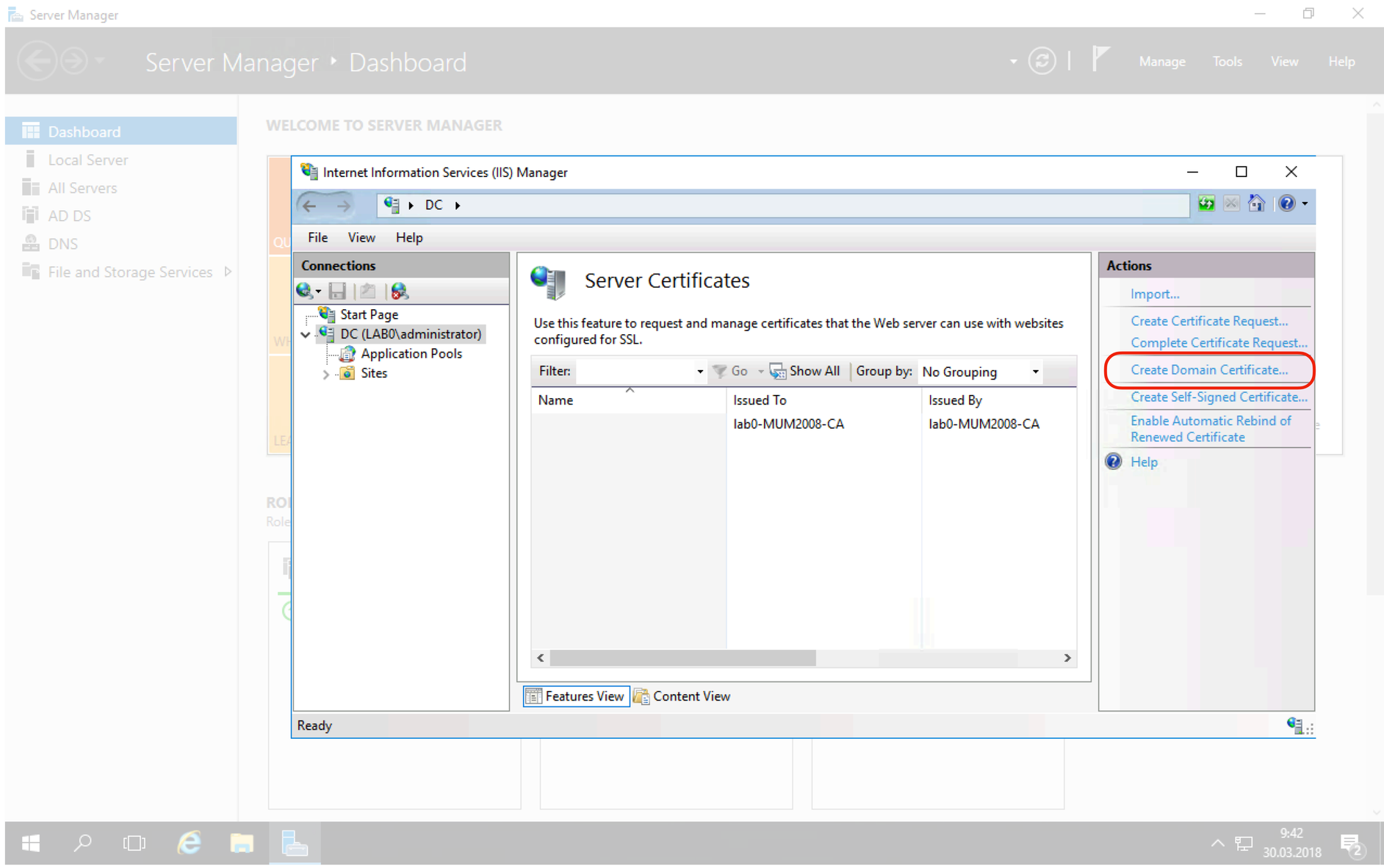
Create web server certificate

- Expand Your server and select “Server Certificates” on the features view pane.



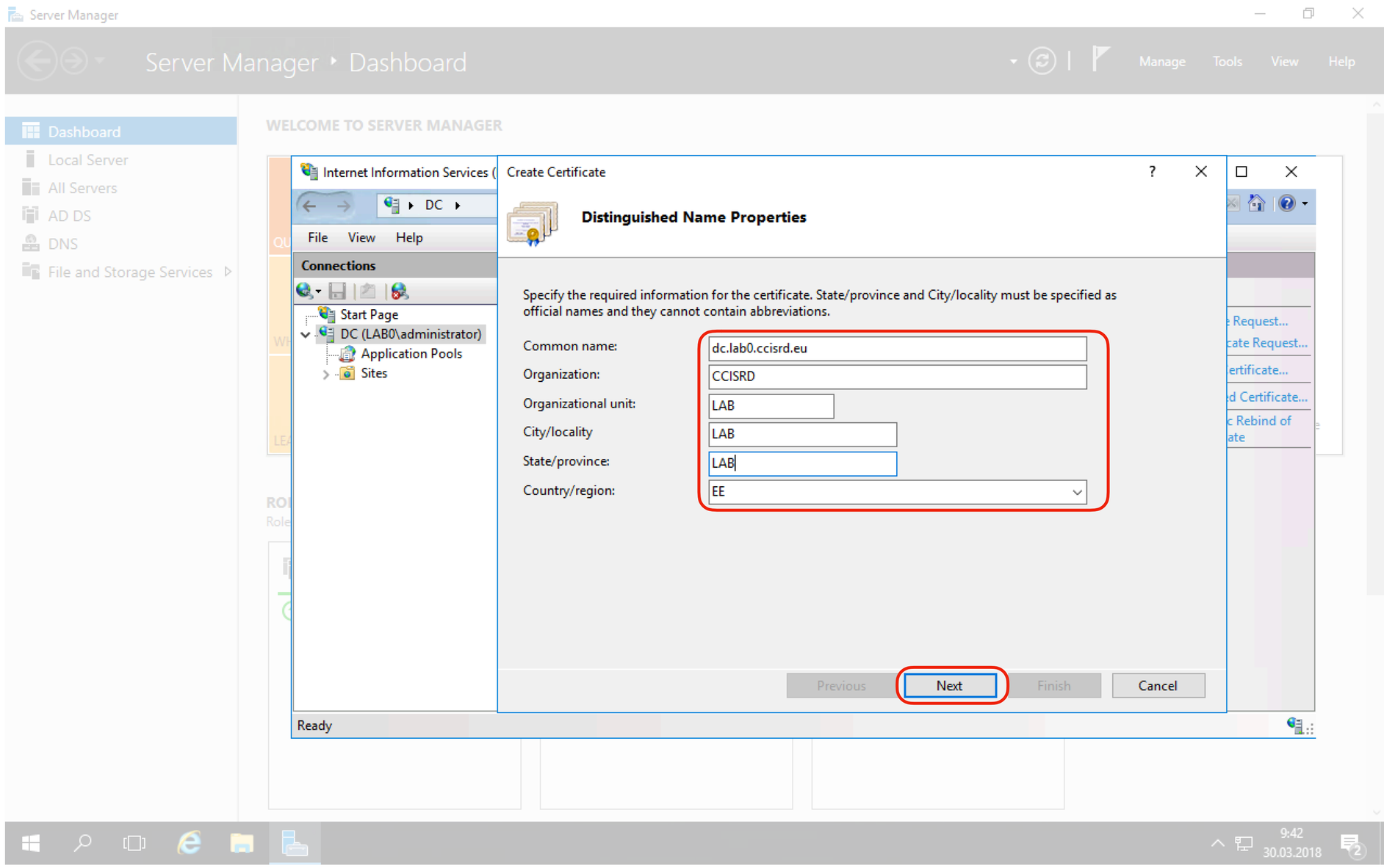
Create web server certificate

- In Action pane click “Create Domain Certificate ..”



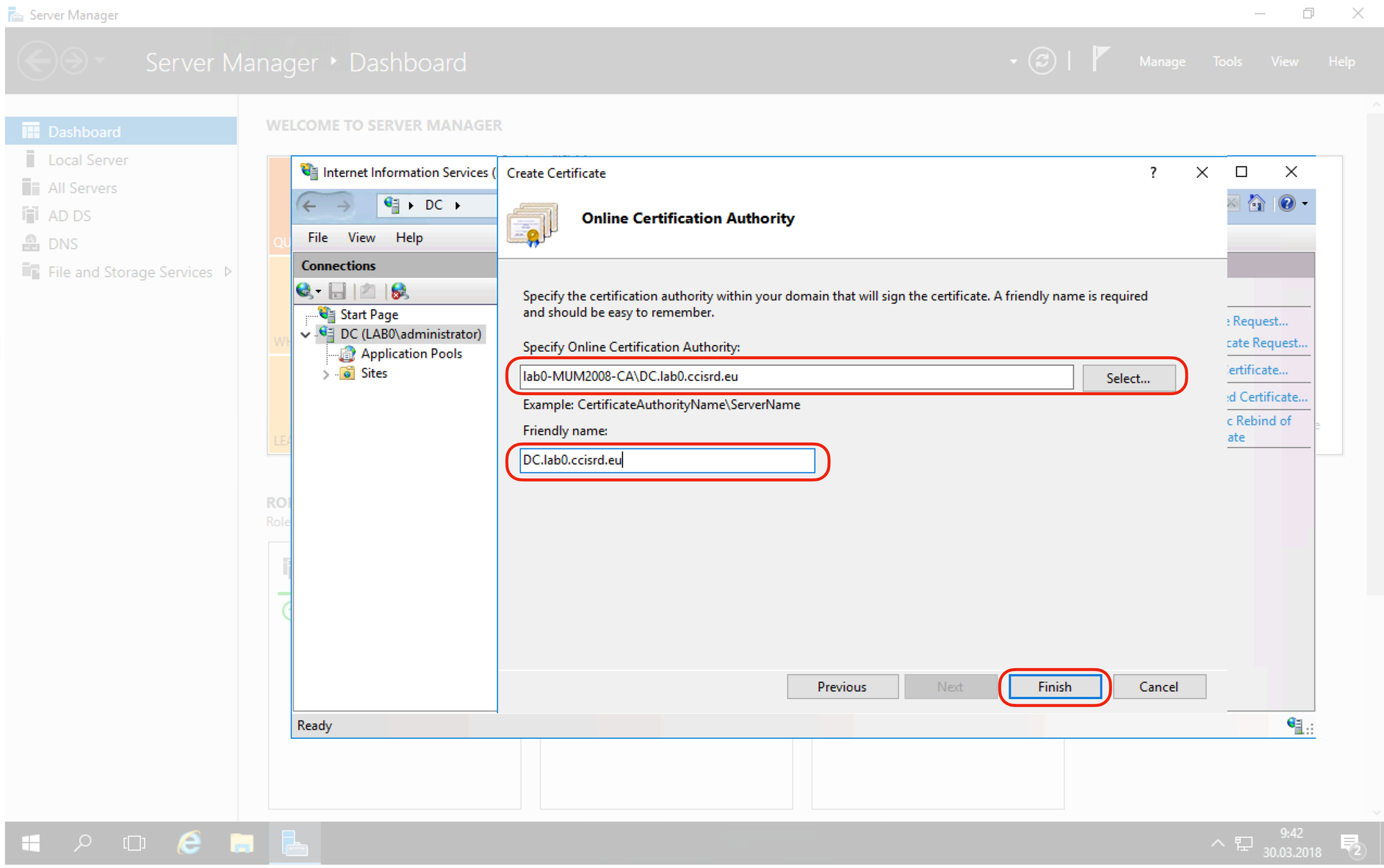
Create web server certificate

- Insert required information.
- Common name is the server FQDN!
- Click “Next”



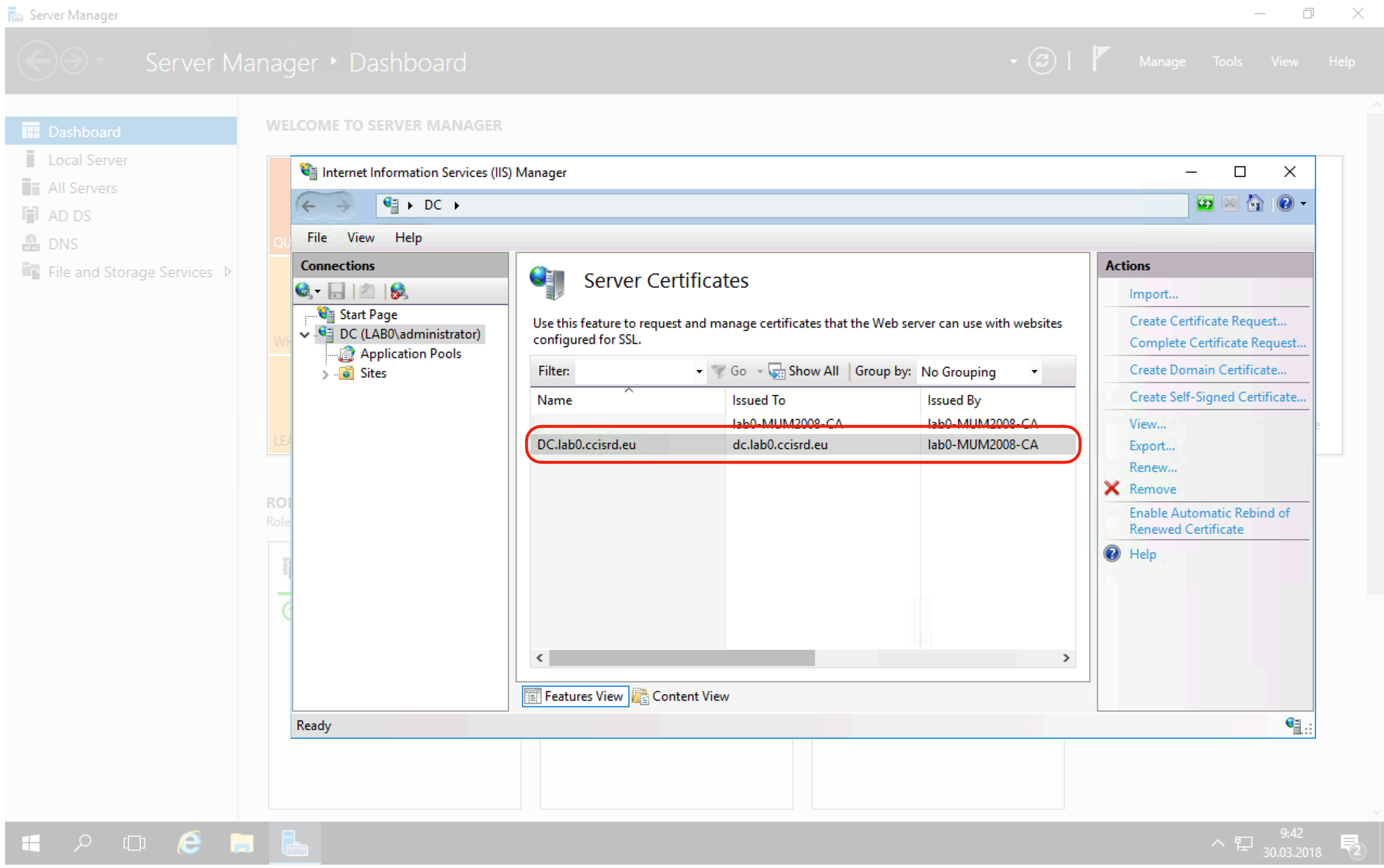
Create web server certificate

- Specify Online Certificate Authority by clicking “Select” button
- Insert a friendly name for the certificate.
  It can be any name.
- Click “Finish”



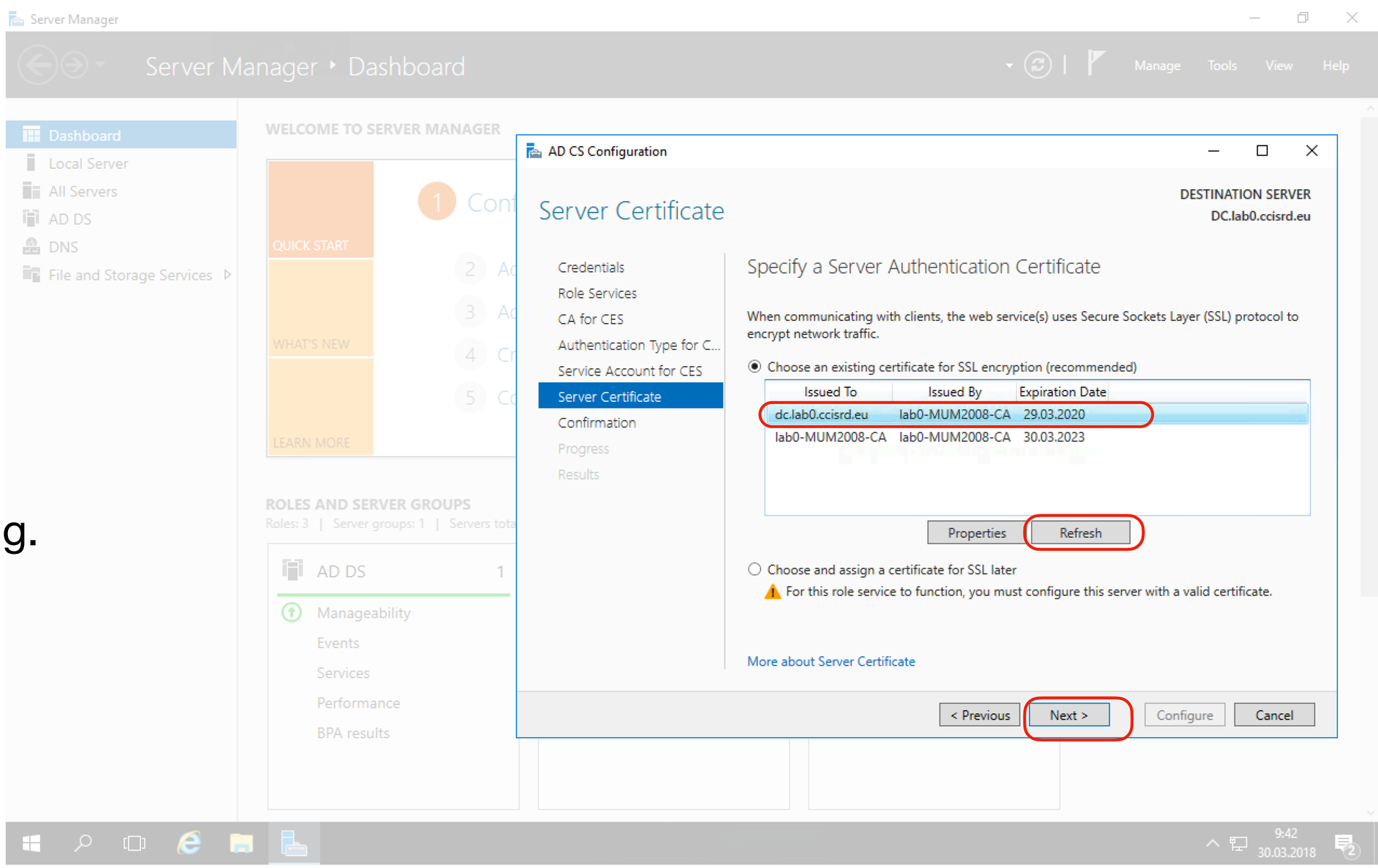
Create web server certificate

- After new certificate is created, close the IIS Manager
- Return to Certificate Web Services configuration



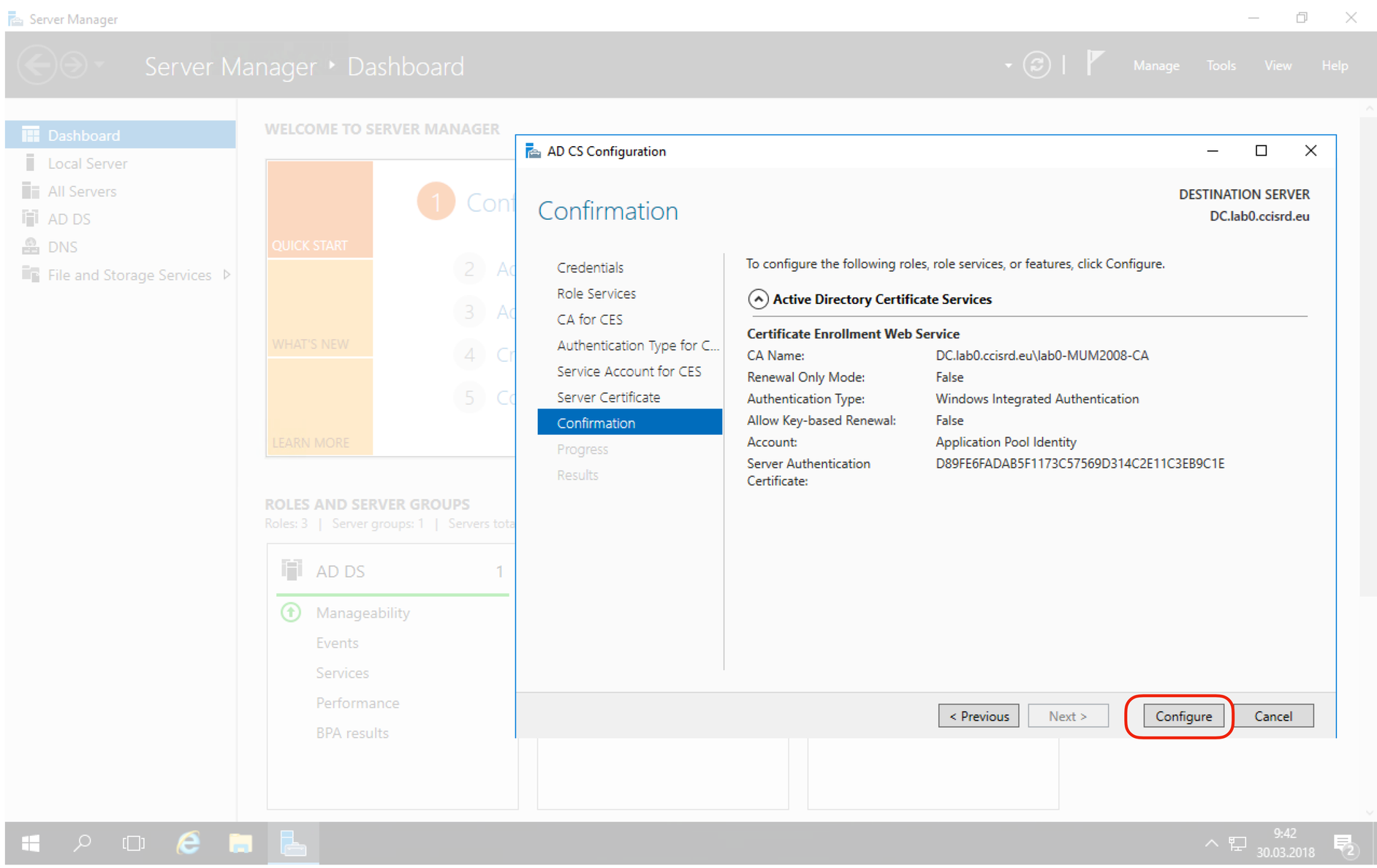
Configure CA

- Click “Refresh”
- Specify a Server Authentication Certificate.
- “Issued to” must be server’s fully qualified domain name FQDN (e.g. dc.lab0.ccisrd.eu)
- Click “Next”



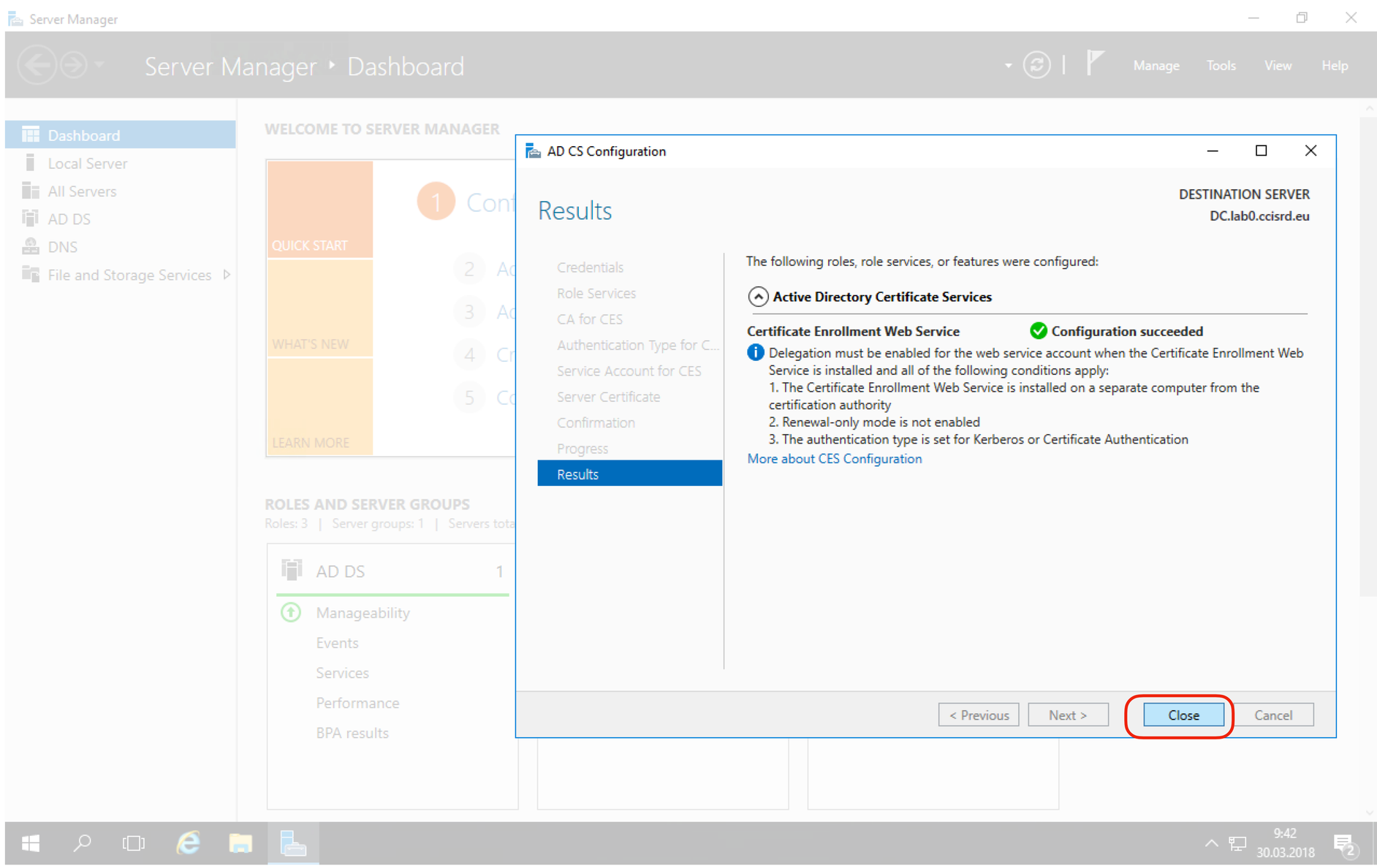
Configure CA

- Click “Configure”



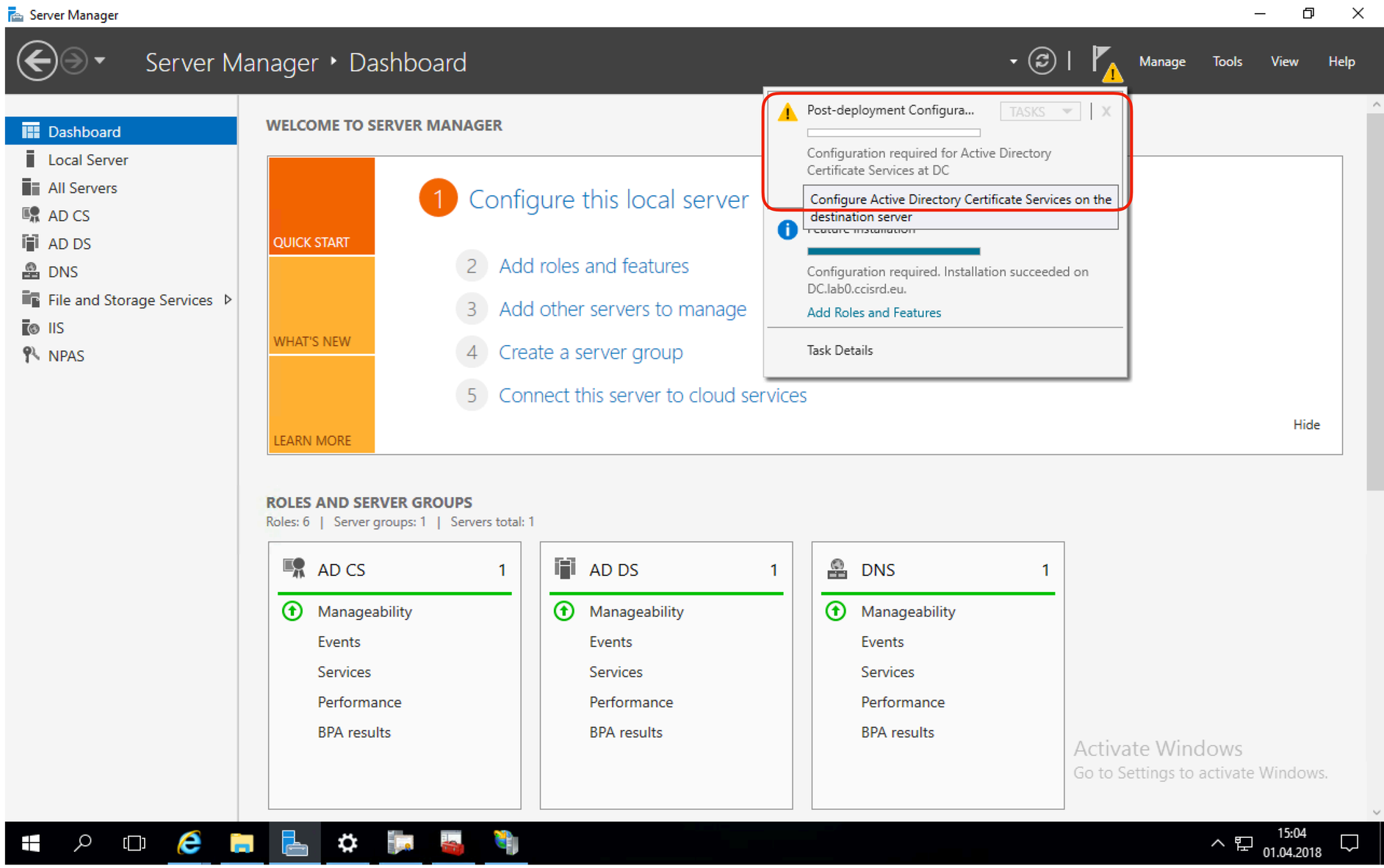
Configure CA

- Click “Close”



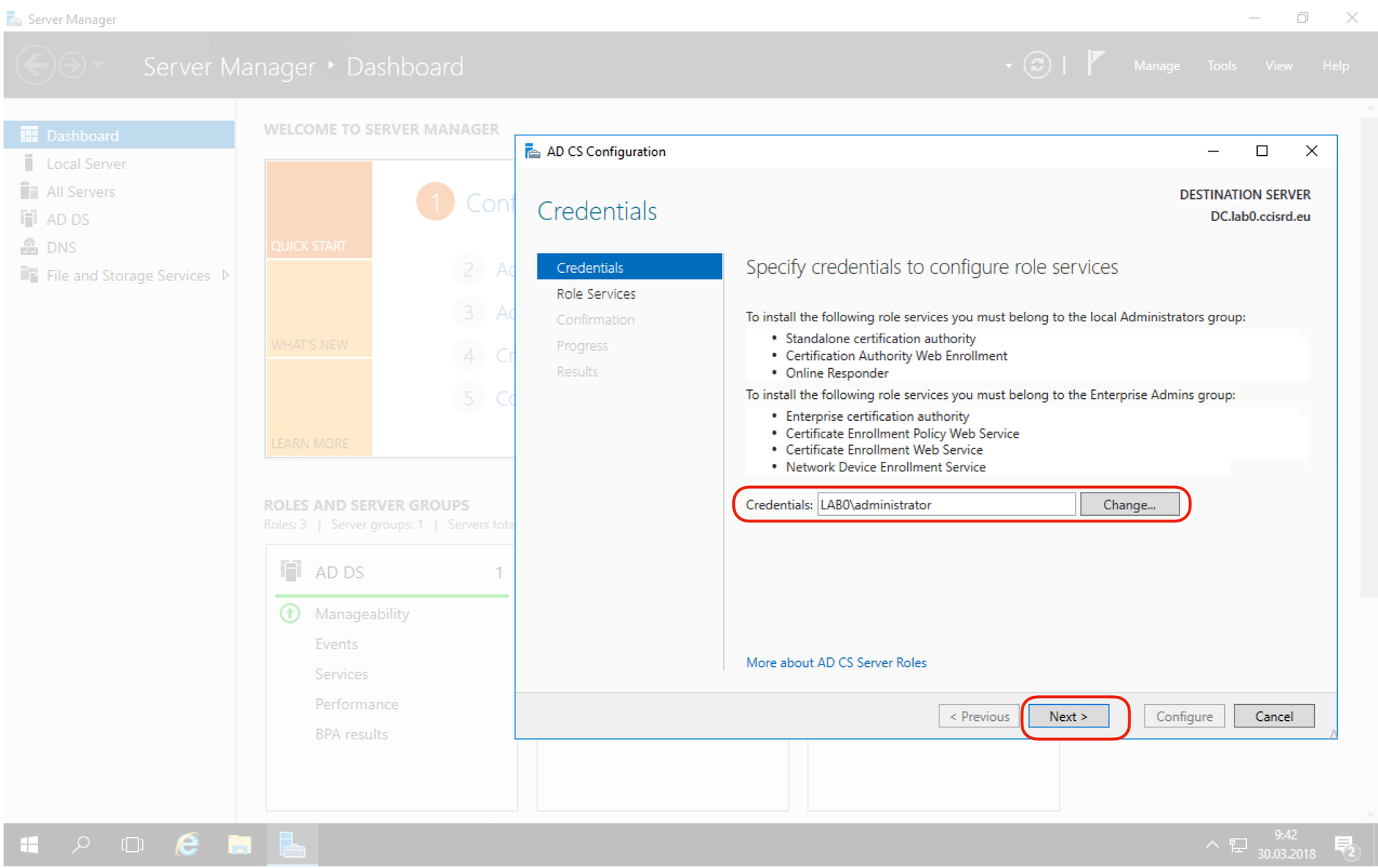
Configure Web Service

- In Server Manager Dashboard, click to configure “Active Directory Certificate Services”



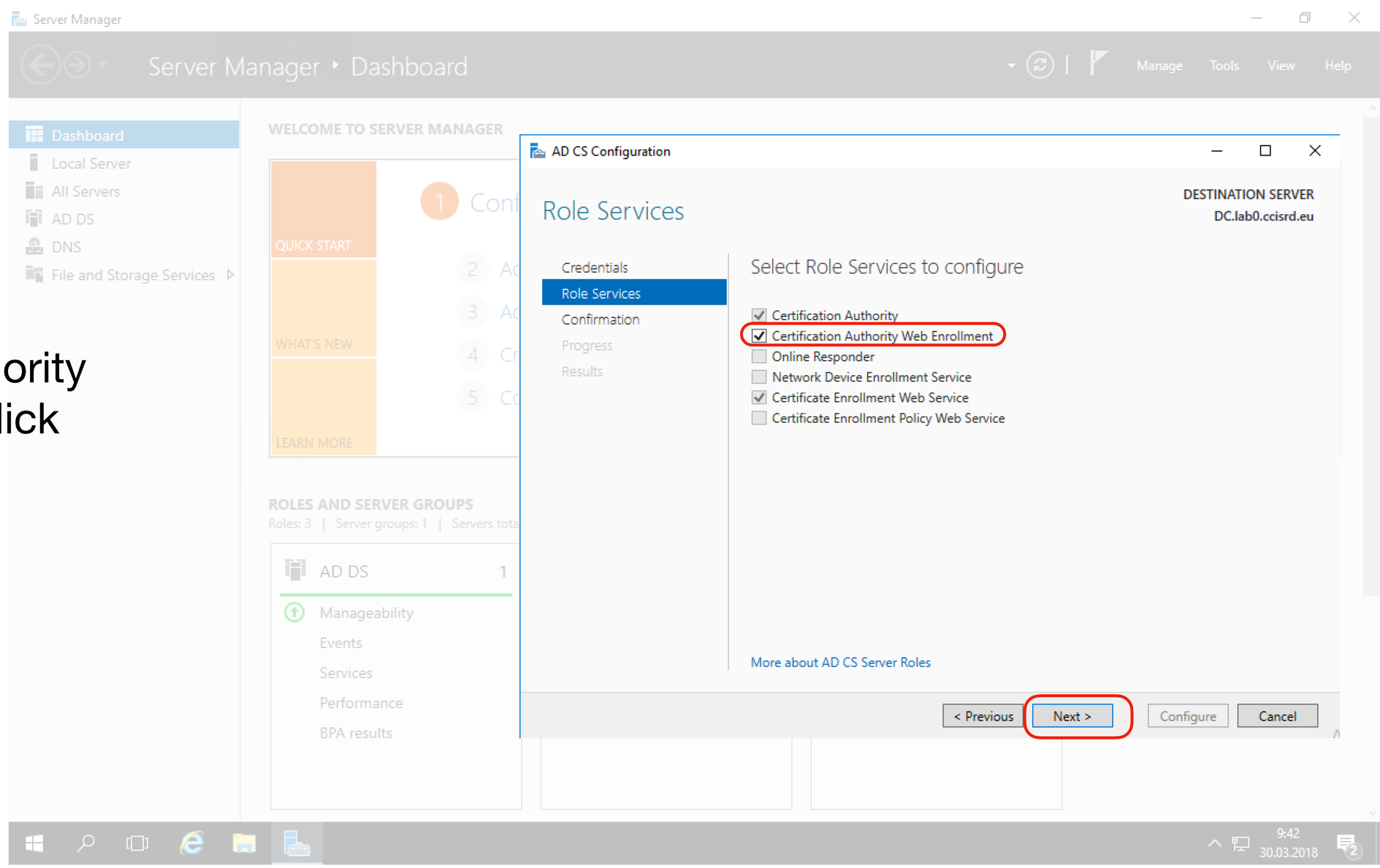
Configure CA

- Verify username and click “Next”



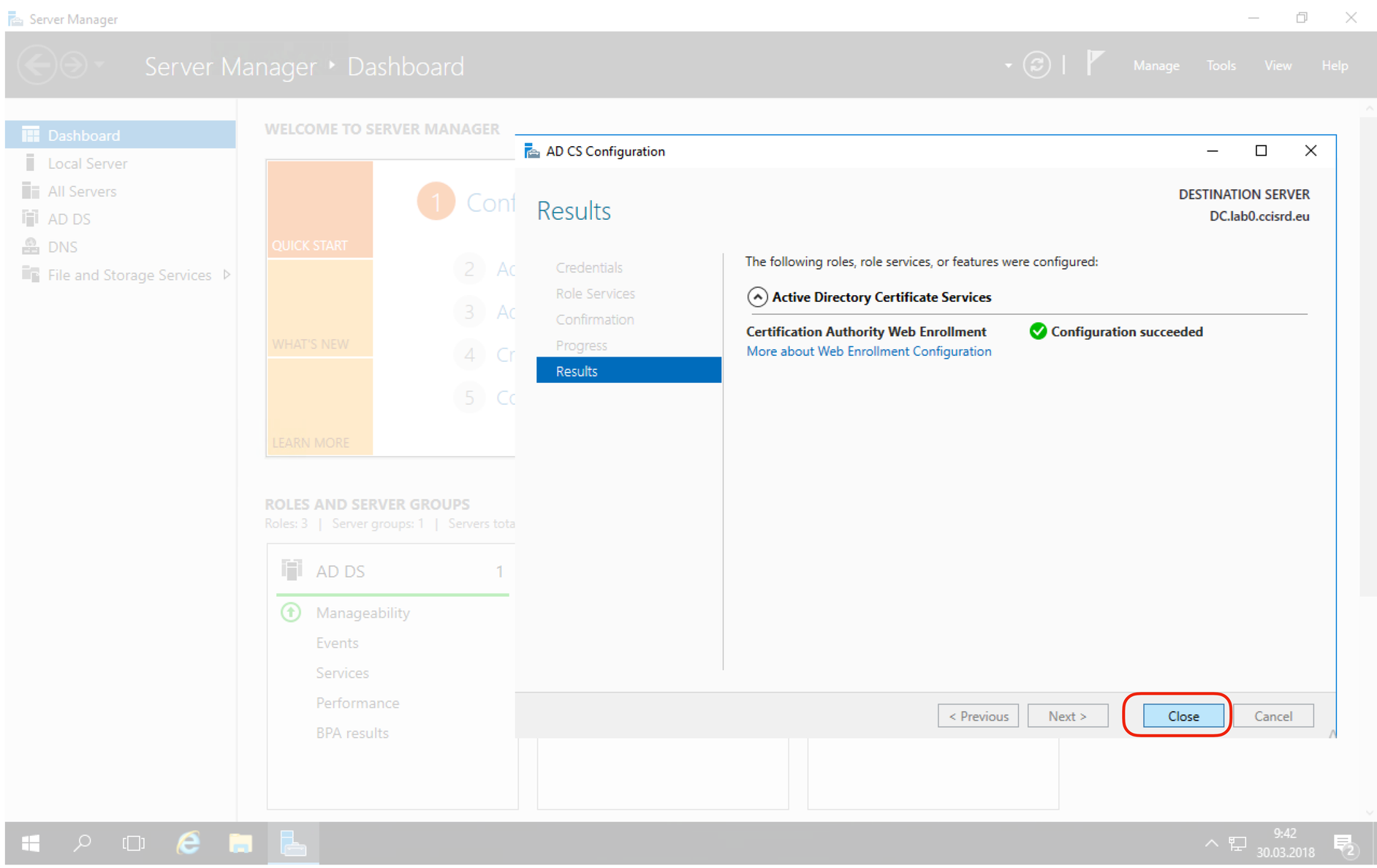
Configure CA

- Select “Certificate Authority Web Enrollment” and click “Next”



Configure CA

- Click “Close”
- Now is CA configured.

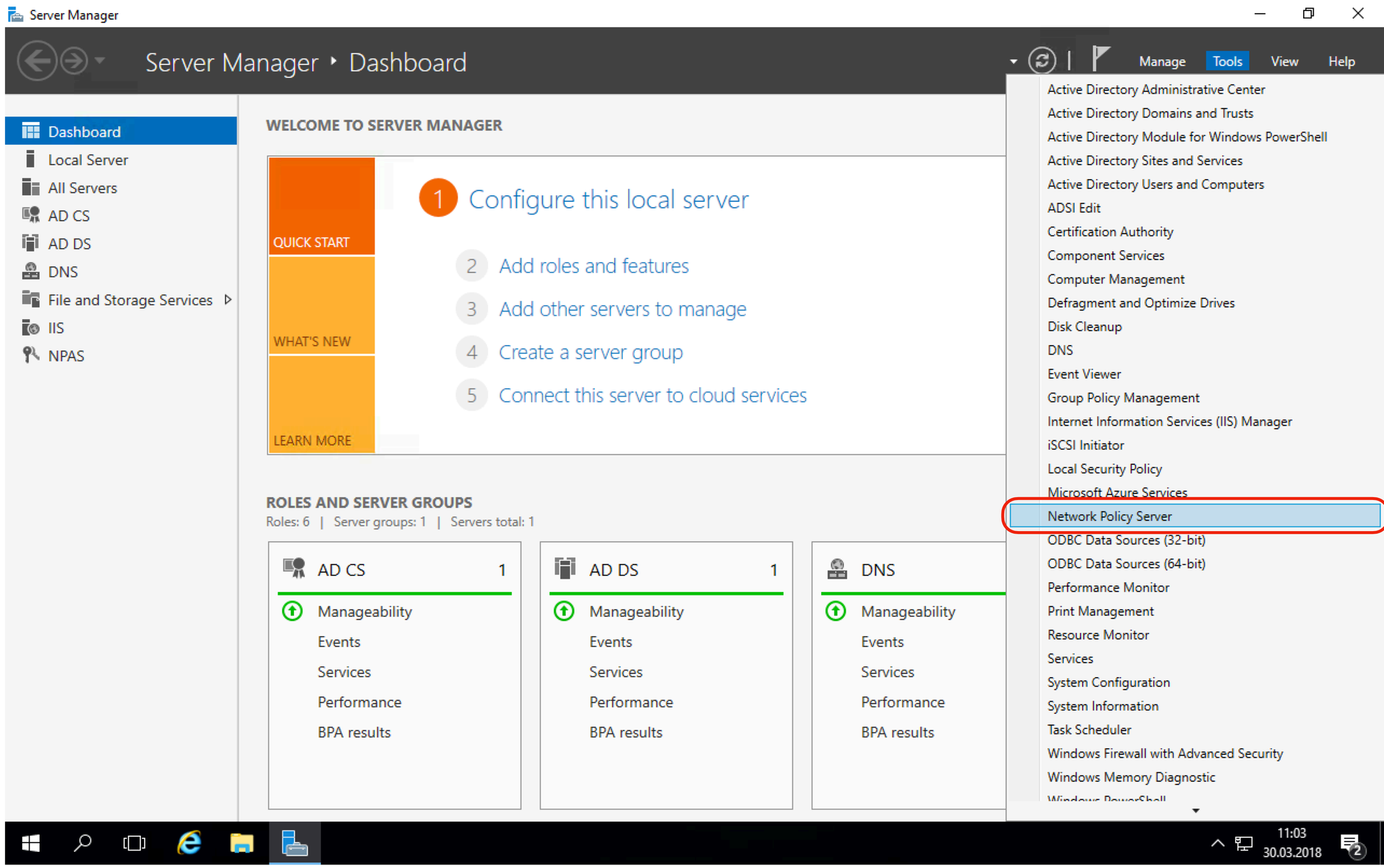


Next Steps

- ~~Install NPS and CA roles on Windows Server~~
- ~~Configure CA~~
- **Configure NPS - RADIUS Server**
- Reconfigure CAPsMAN
- Install CA on client device's

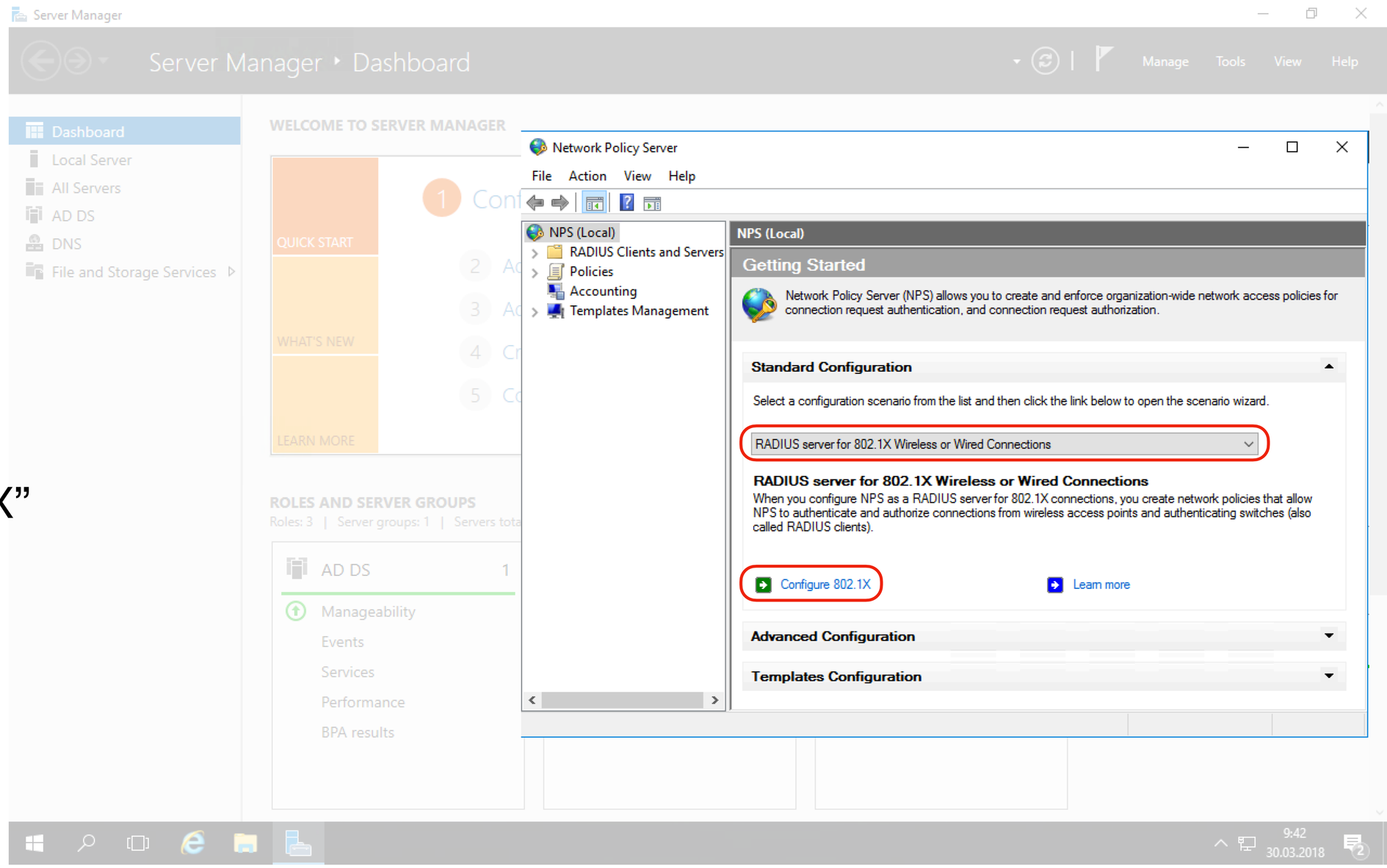
Configure NPS - Radius

- From Server Manager open “Network Policy Server.



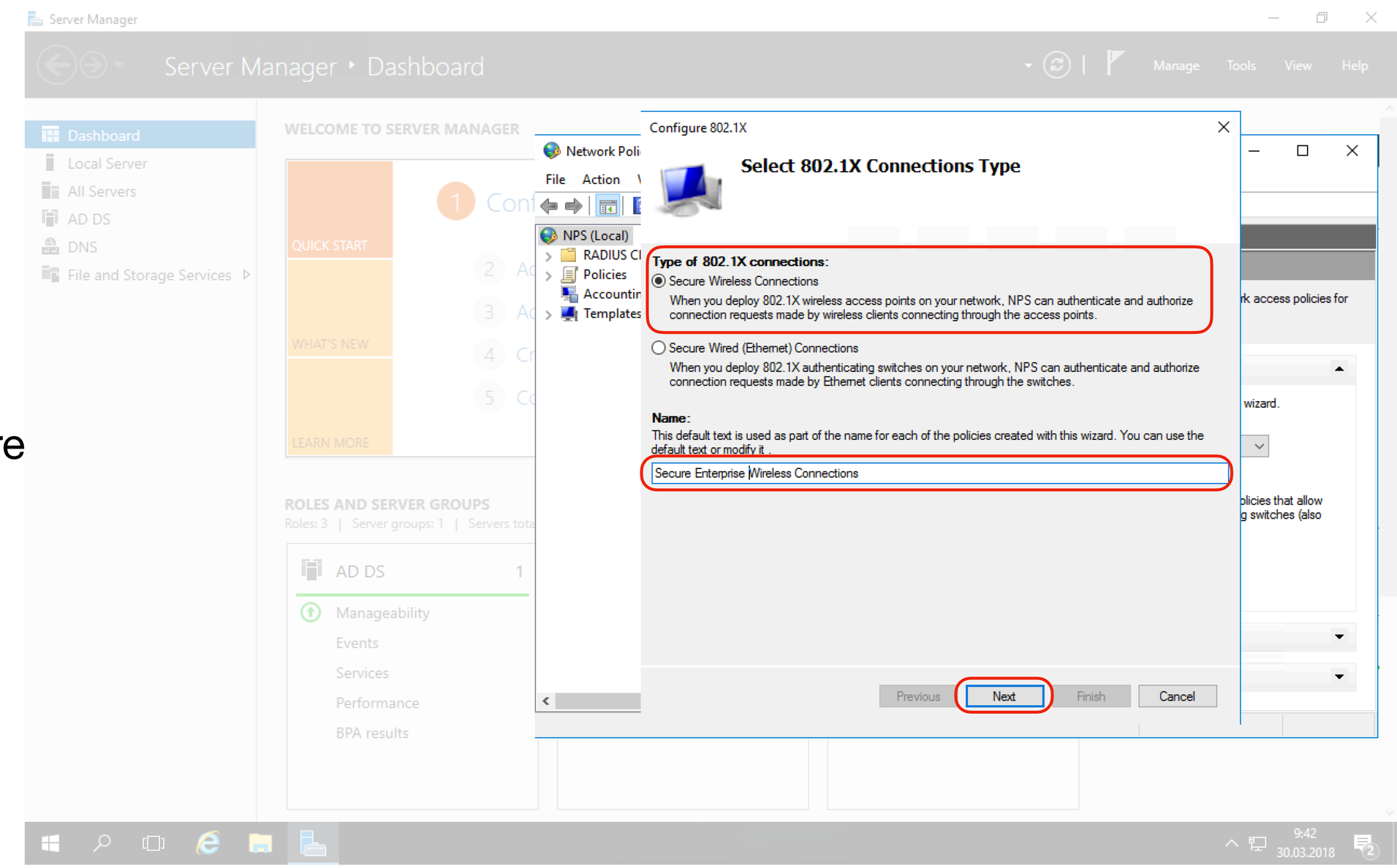
Configure NPS - Radius

- Select “RADIUS server for 802.1X Wireless or Wired Connections
- Click “Configure 802.1X”



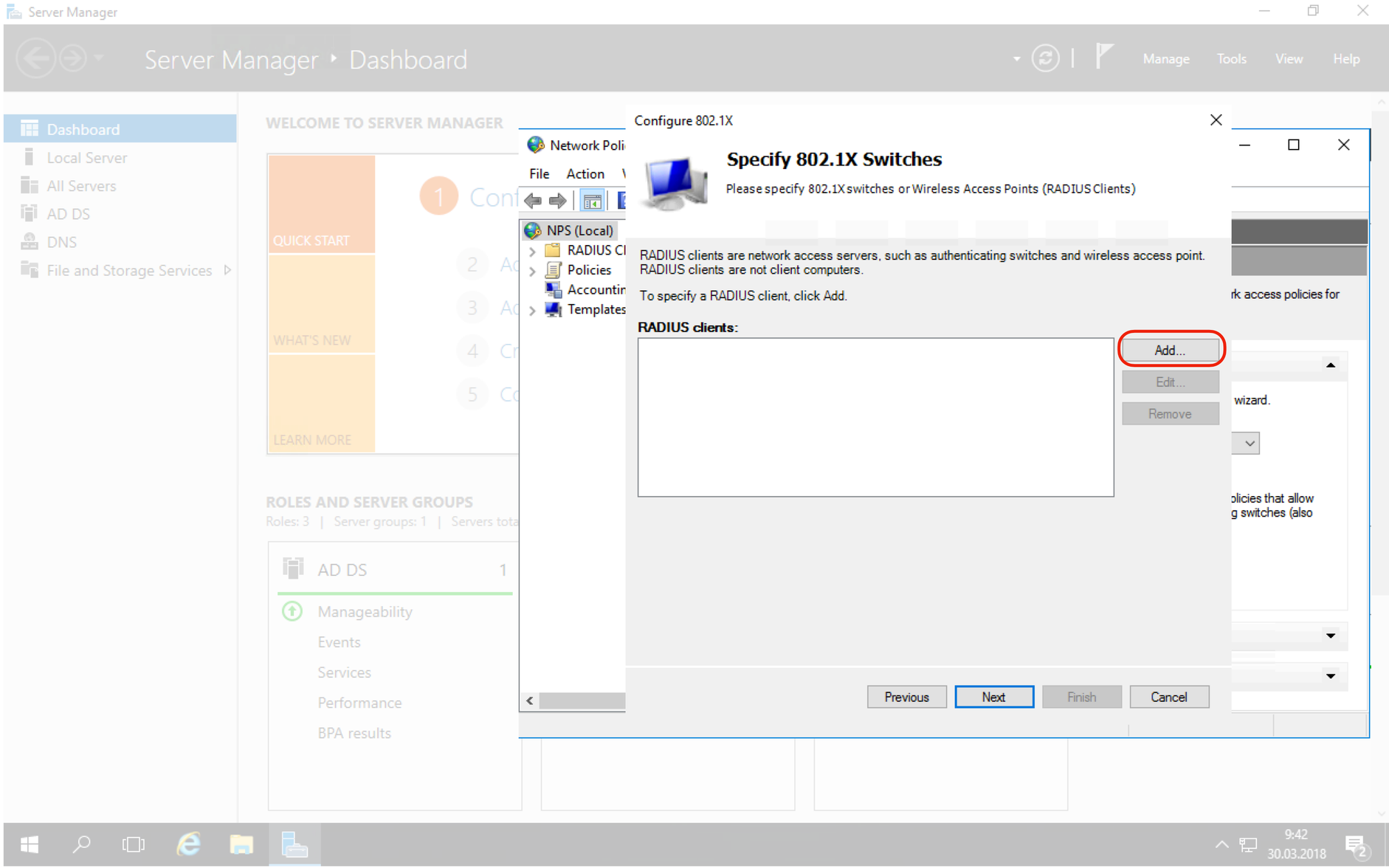
Configure NPS - Radius

- Select wireless as “Type of 802.1X connection”
- Insert name for this connection (e.g. Secure Enterprise Wireless Connection”
- Click “Next”



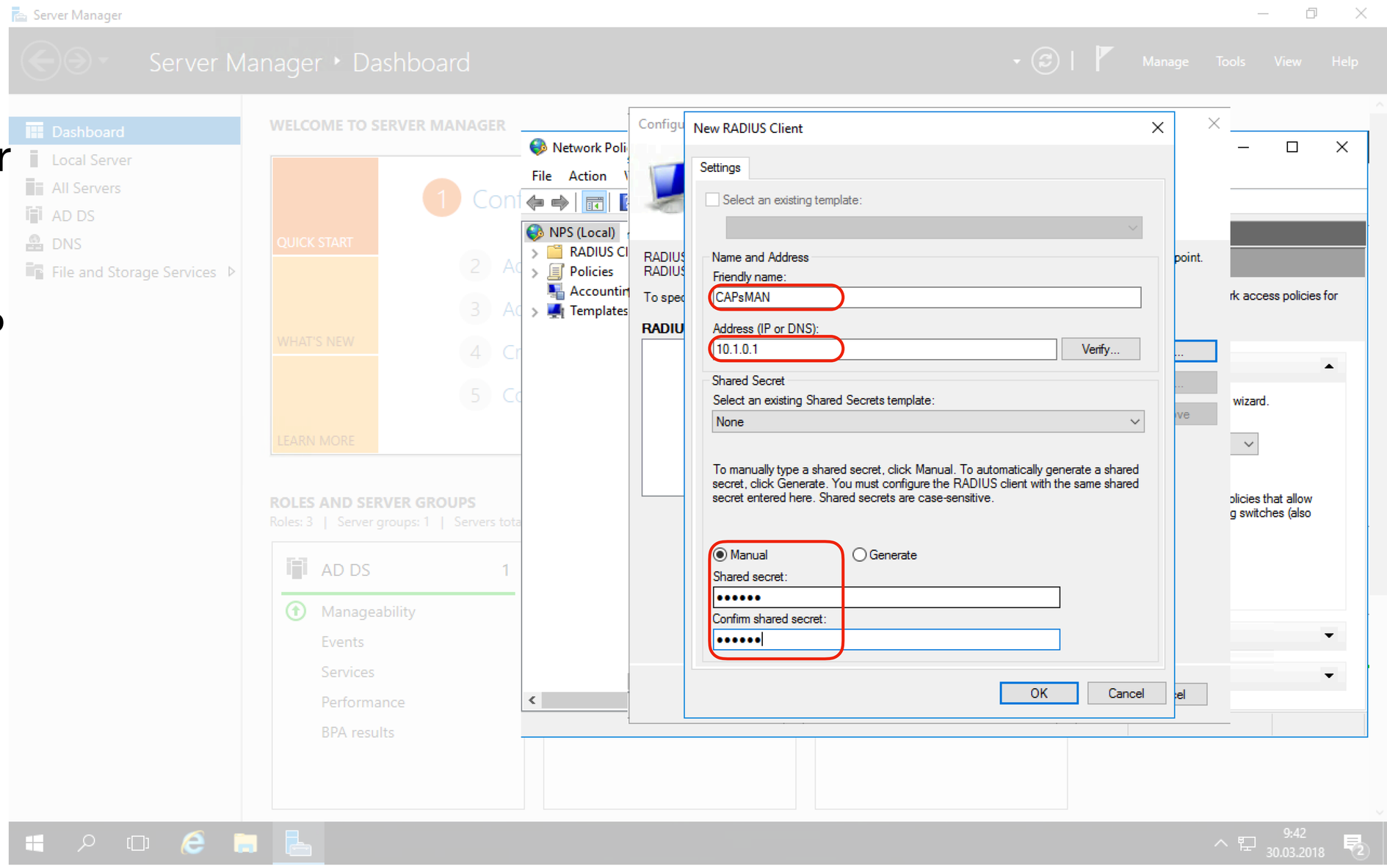
Configure NPS - Radius

- Add RADIUS client. In our case is it the CAPsMAN



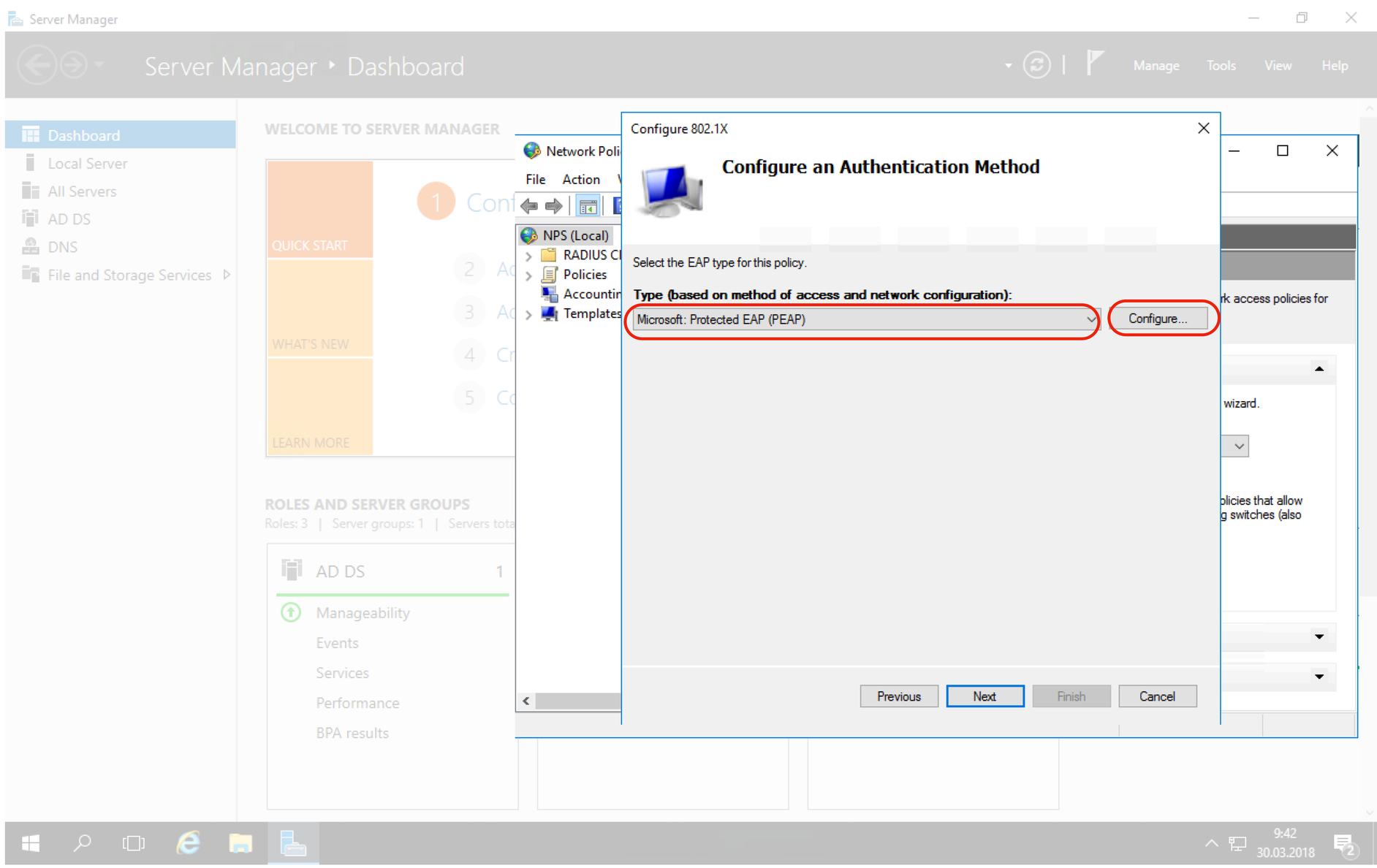
Configure NPS - Radius

- Give a friendly name for the RADIUS client. (e.g. CAPsMAN)
- Insert RADIUS Client IP address (10.1.0.1)
- Insert (or generate) Shared secret for the Radius Client.
- Click “OK” and then “Next”.



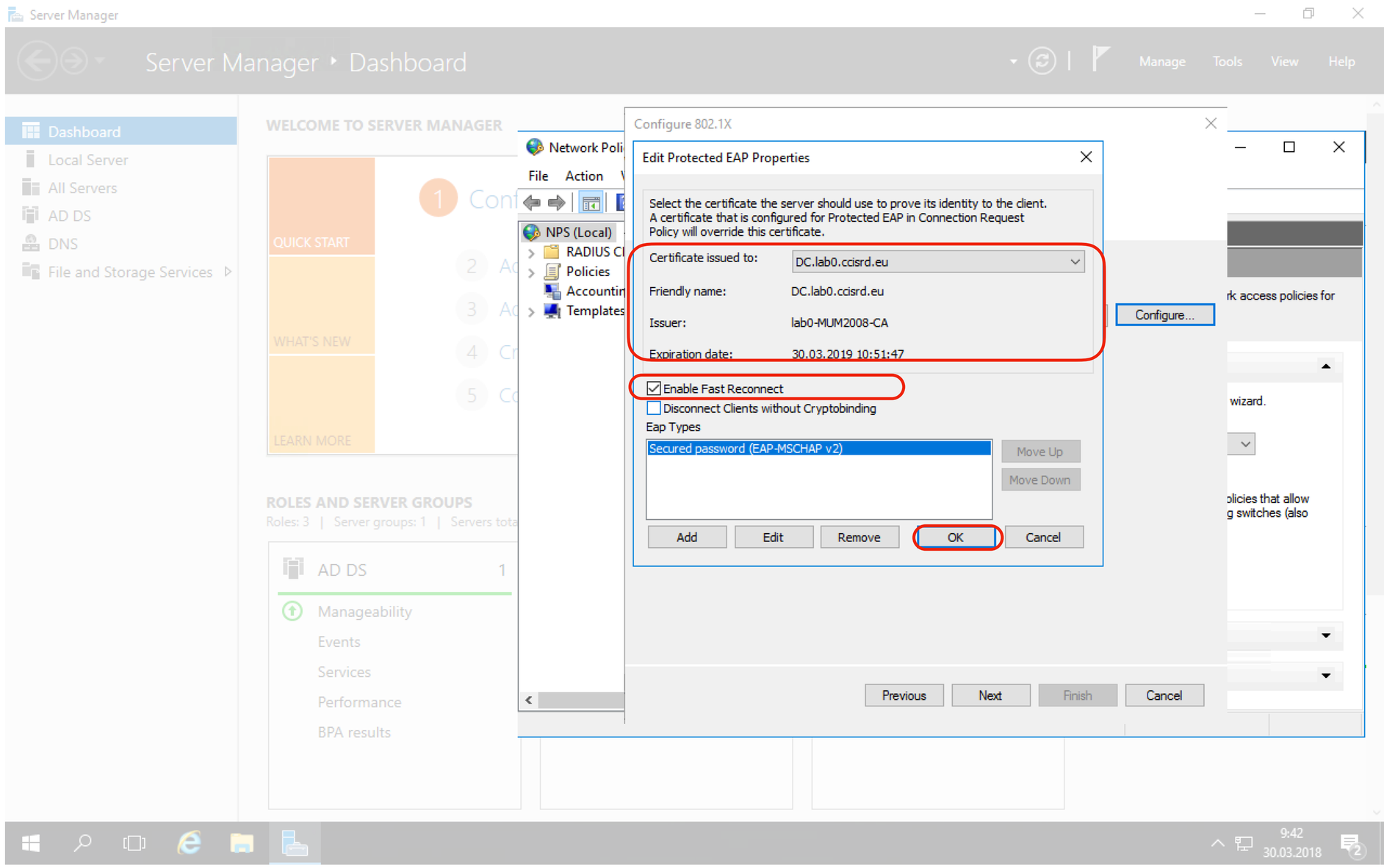
Configure NPS - Radius

- Select “Microsoft Protected EAP (PEAP) as Type.
- Click “Configure”



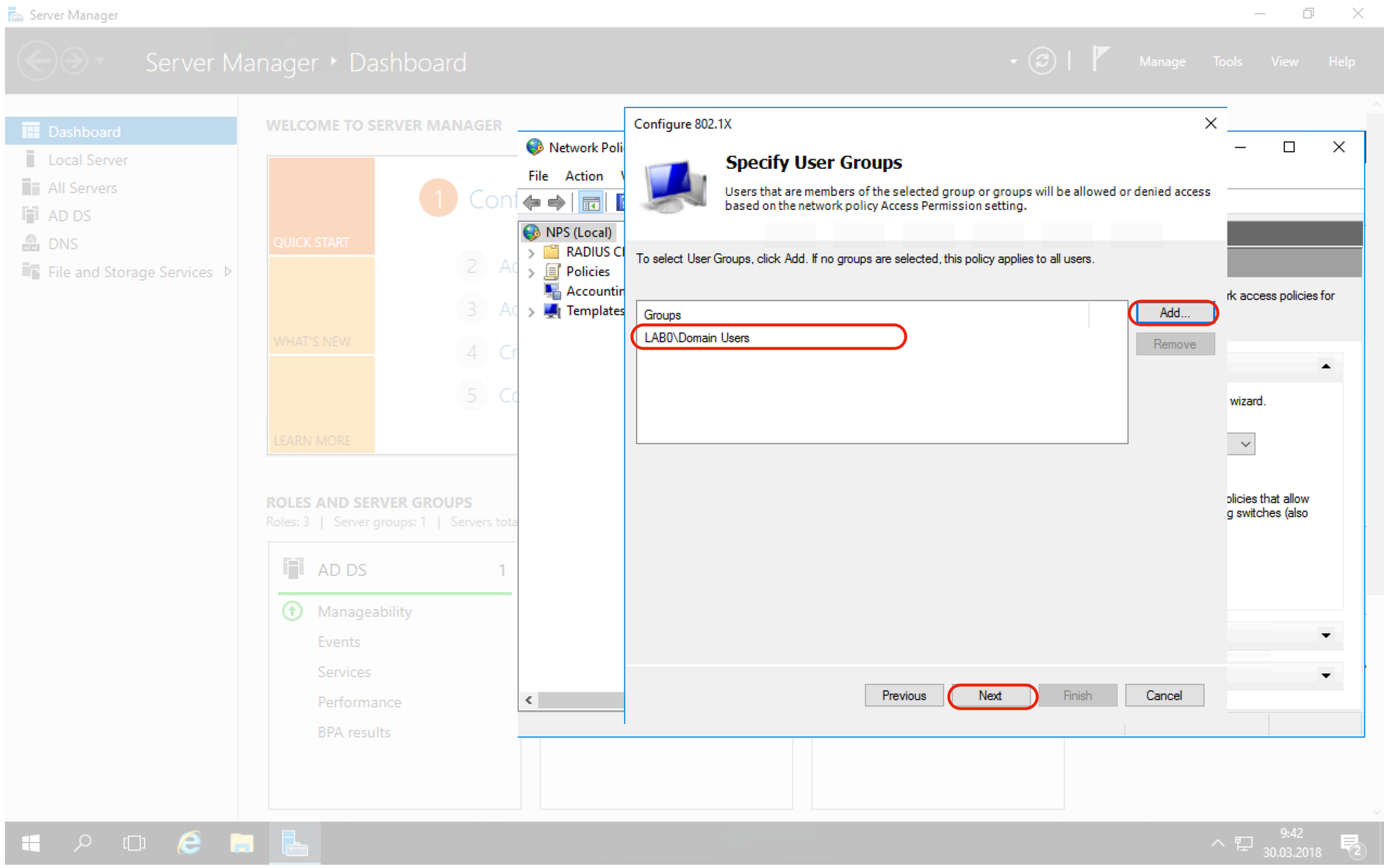
Configure NPS - Radius

- Verify that the correct certificate is selected
- Enable Fast Reconnect
- Click “OK” and then “Next”



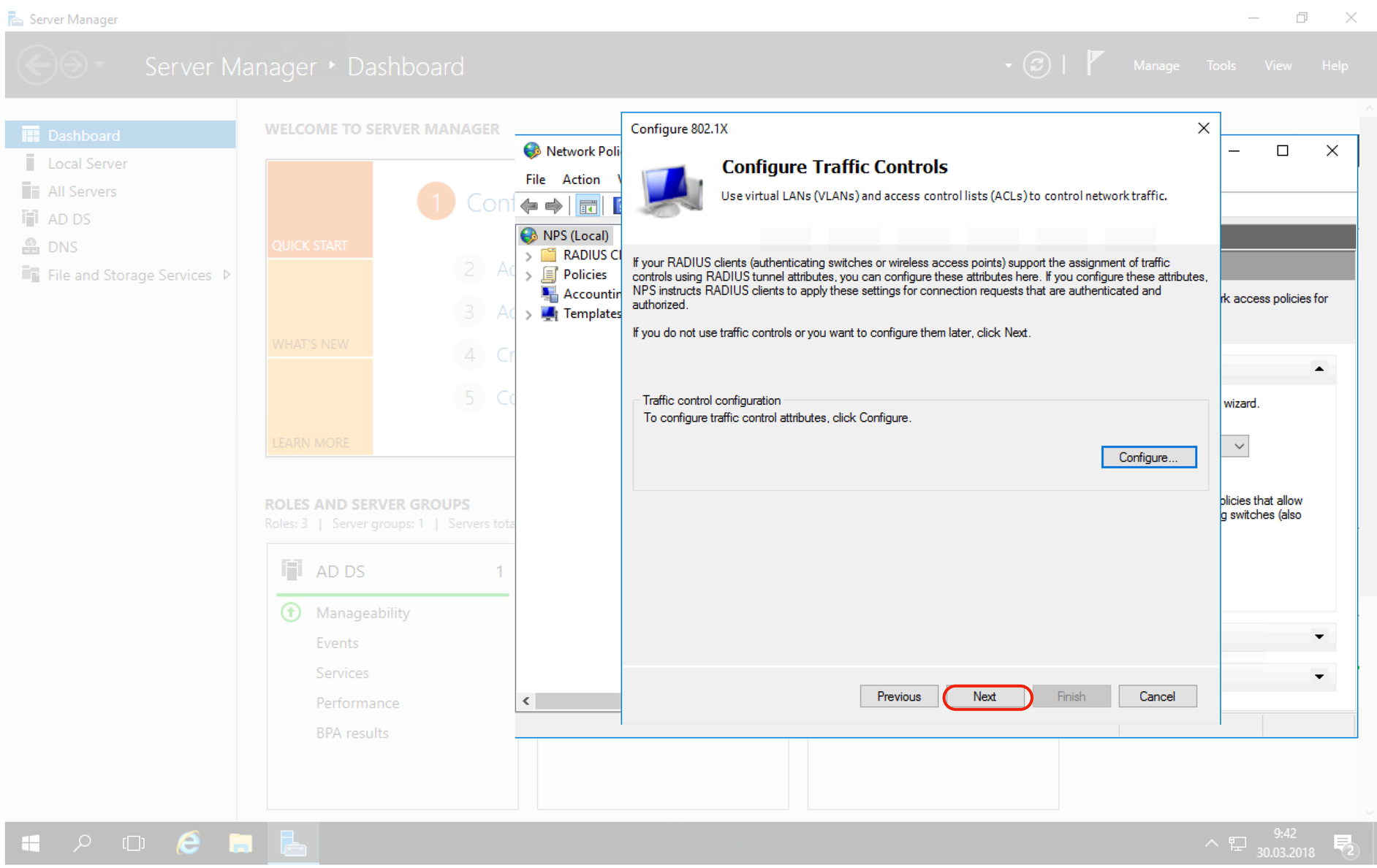
Configure NPS - Radius

- Click “Add” and select User Group(s) to grant permission to use this network.
  In our case this is a general network and all domain users not belonging any special group can use this.
- Click “Next”



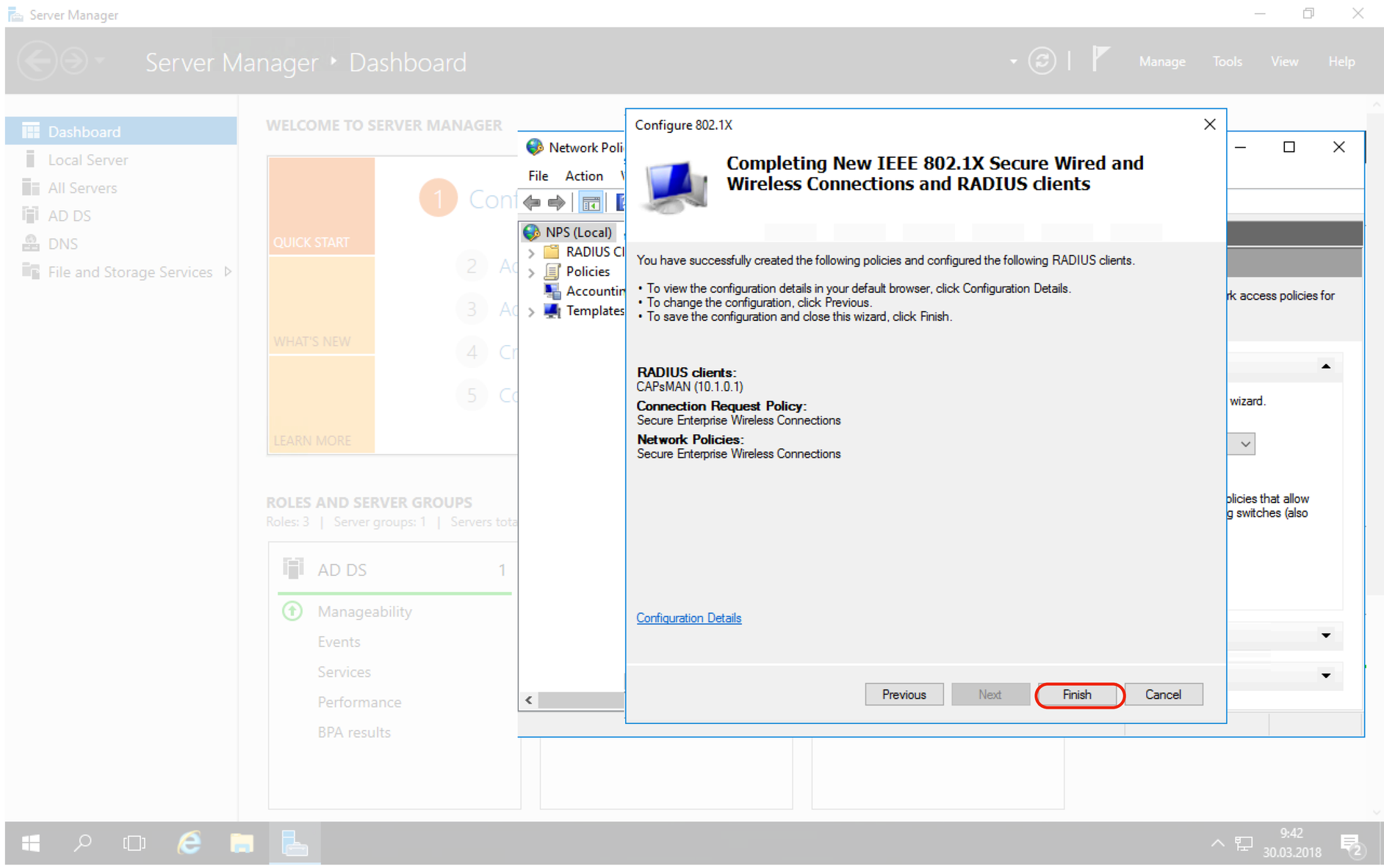
Configure NPS - Radius

- Accept default and Click “Next”



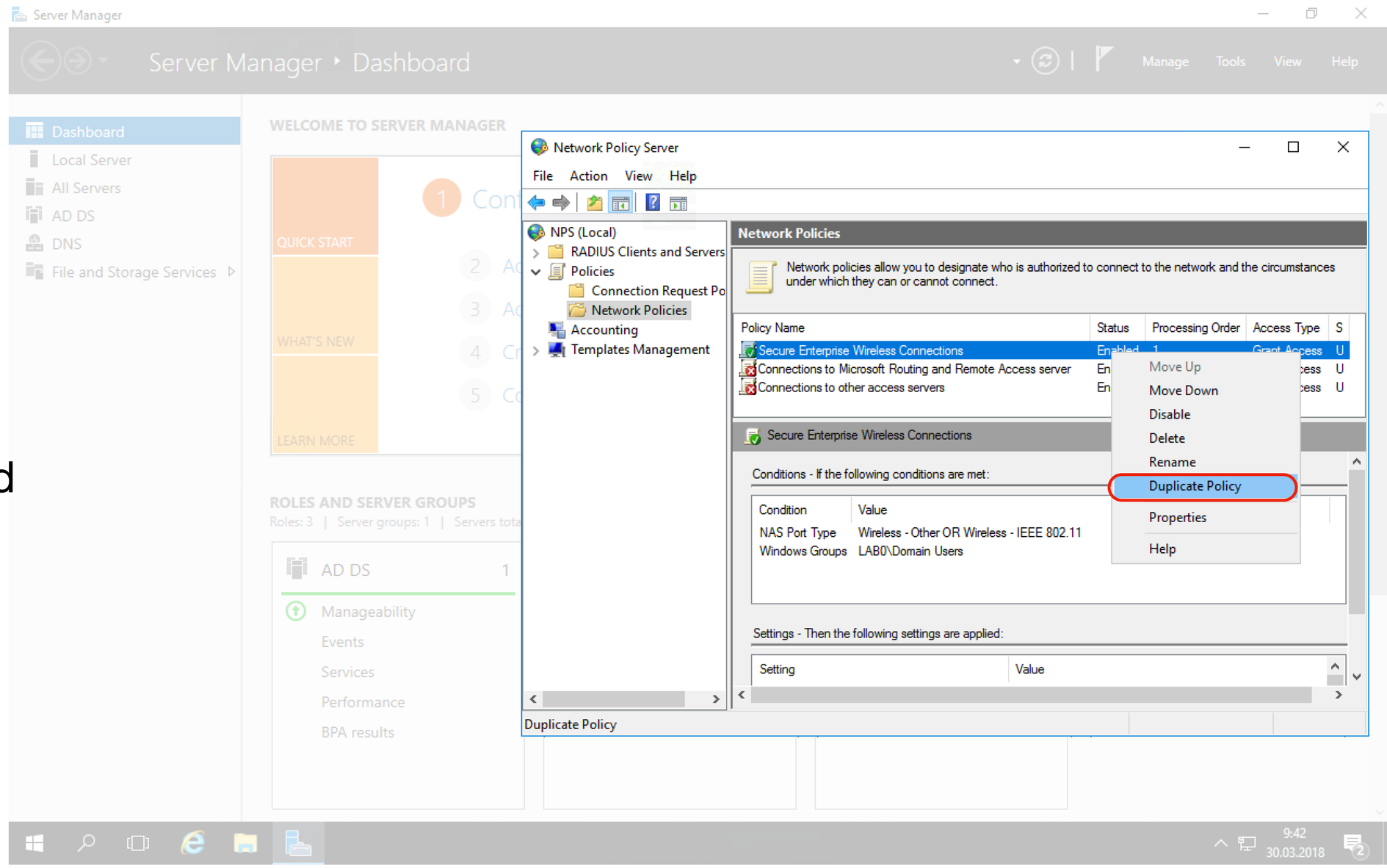
Configure NPS - Radius

- Review settings and click “Next”



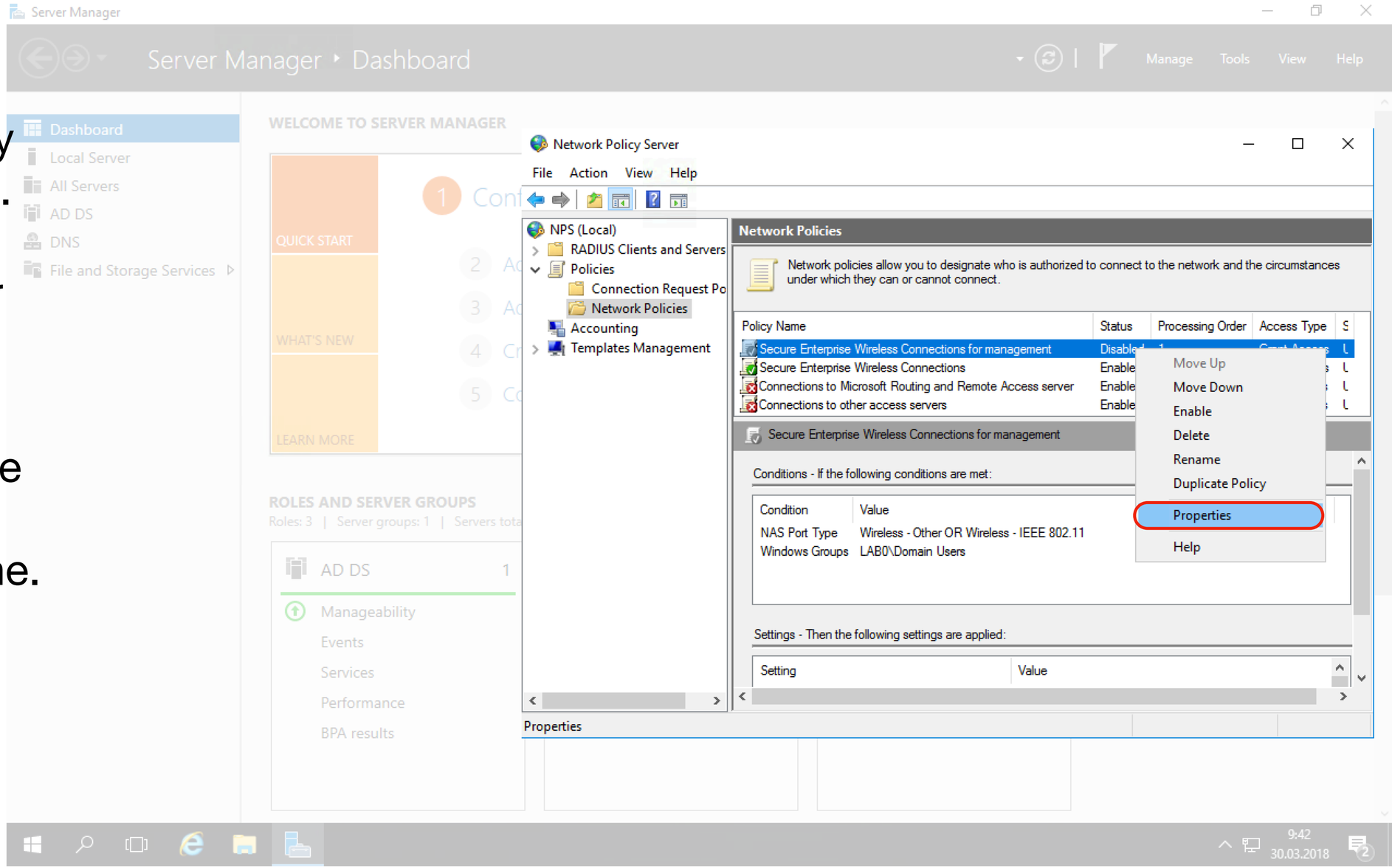
Configure NPS - Radius

- Now we create policies for privileged user groups.
- Duplicate newly created Network policy.



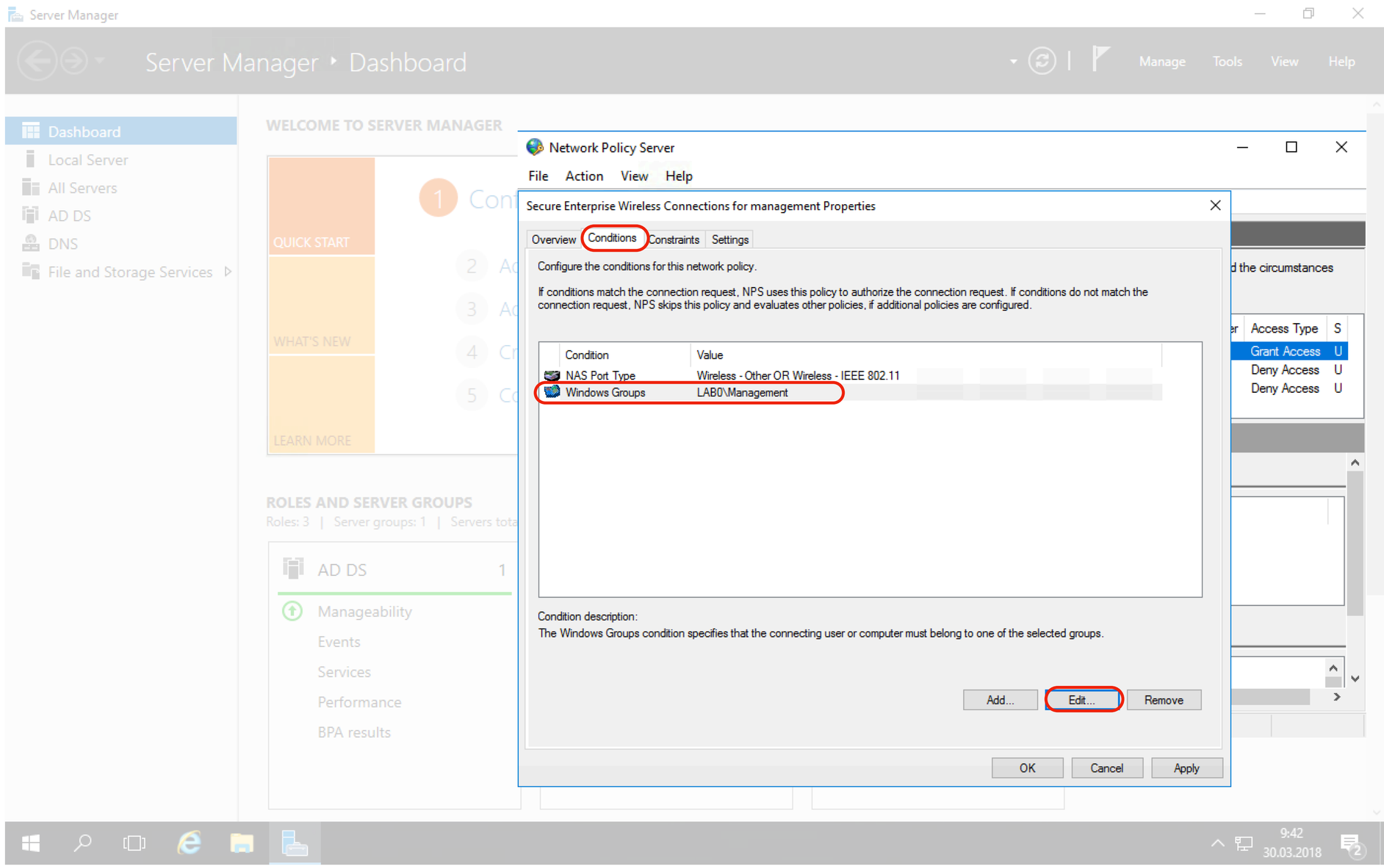
Configure NPS - Radius

- Give a duplicated policy a reasonable name (e.g. “Secure Enterprise Wireless connection for Management”
- Move this policy to the top. It must authenticate and accept privileged users before general one.
- Edit policy clicking “Properties”



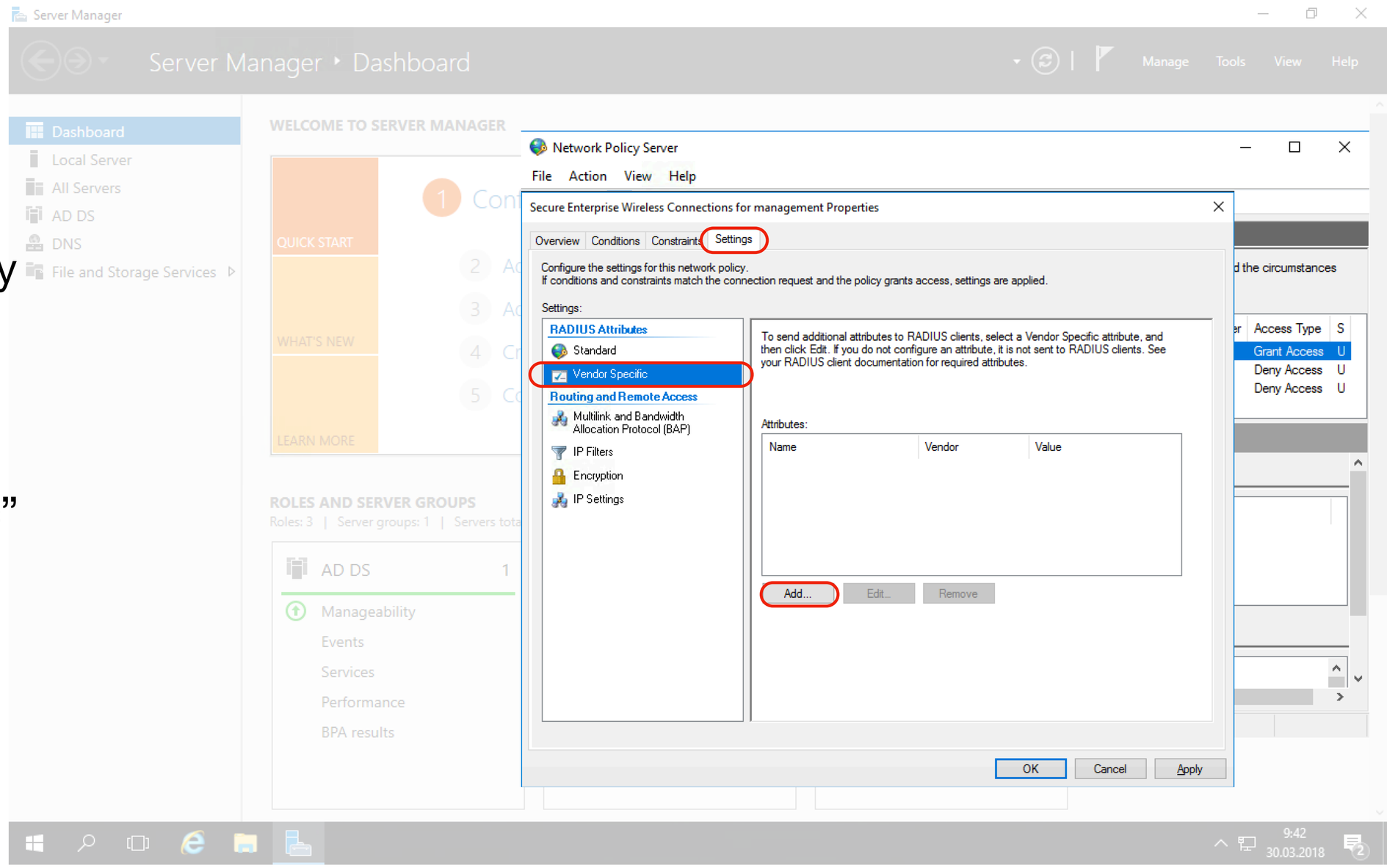
Configure NPS - Radius

- On “Conditions” tab replace Domain users with more specific / privileged user group by clicking “Edit”. (In our case group “Management”)



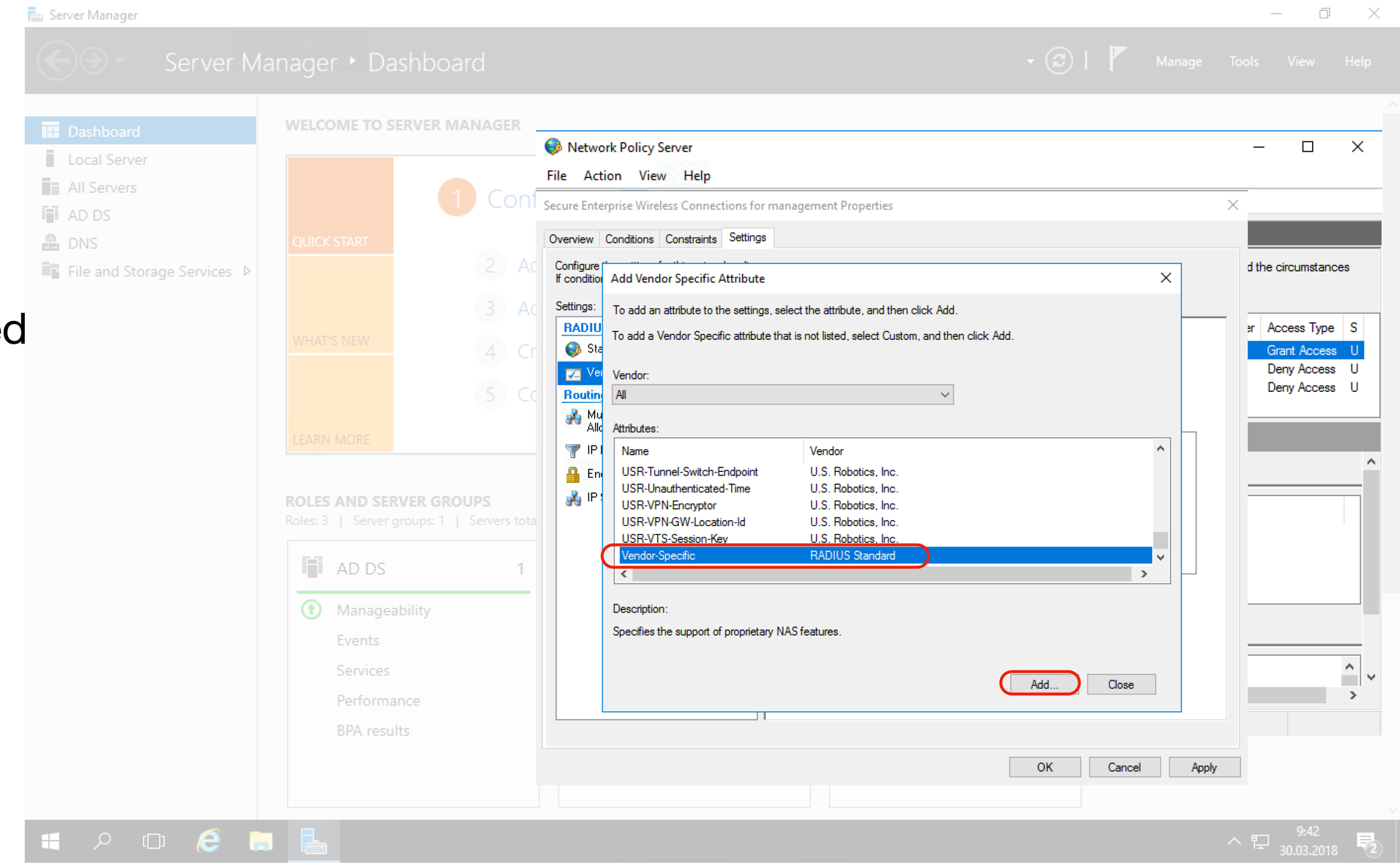
Configure NPS - Radius

- Now we need to specify VLAN ID for this group.
- Select “Settings” tab
- In Settings section select “Vendor Specific” and click “Add”



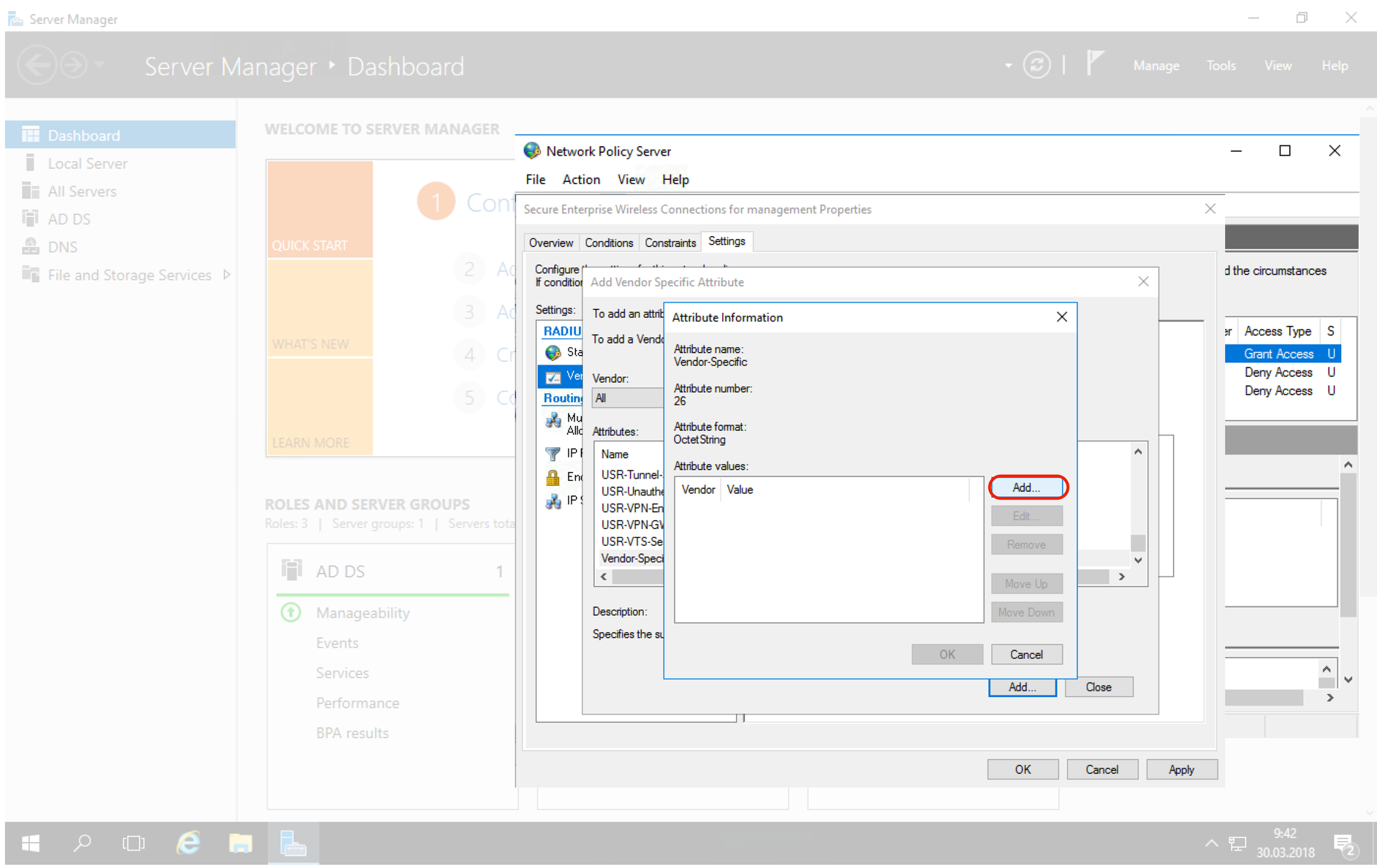
Configure NPS - Radius

- As MikroTik is not listed here, we need to use “Vendor Specific”
- Click “Add”



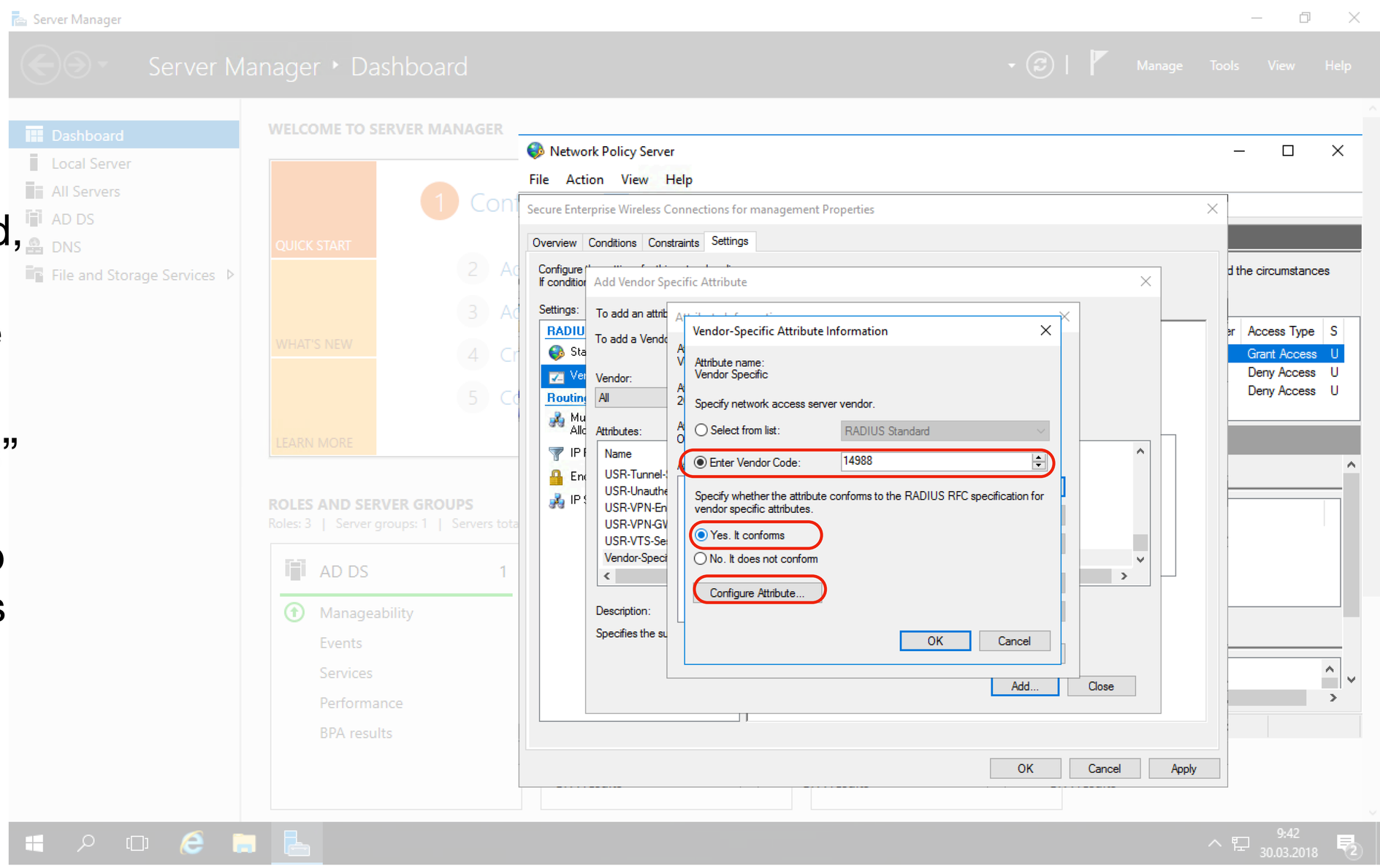
Configure NPS - Radius

- Click “Add”



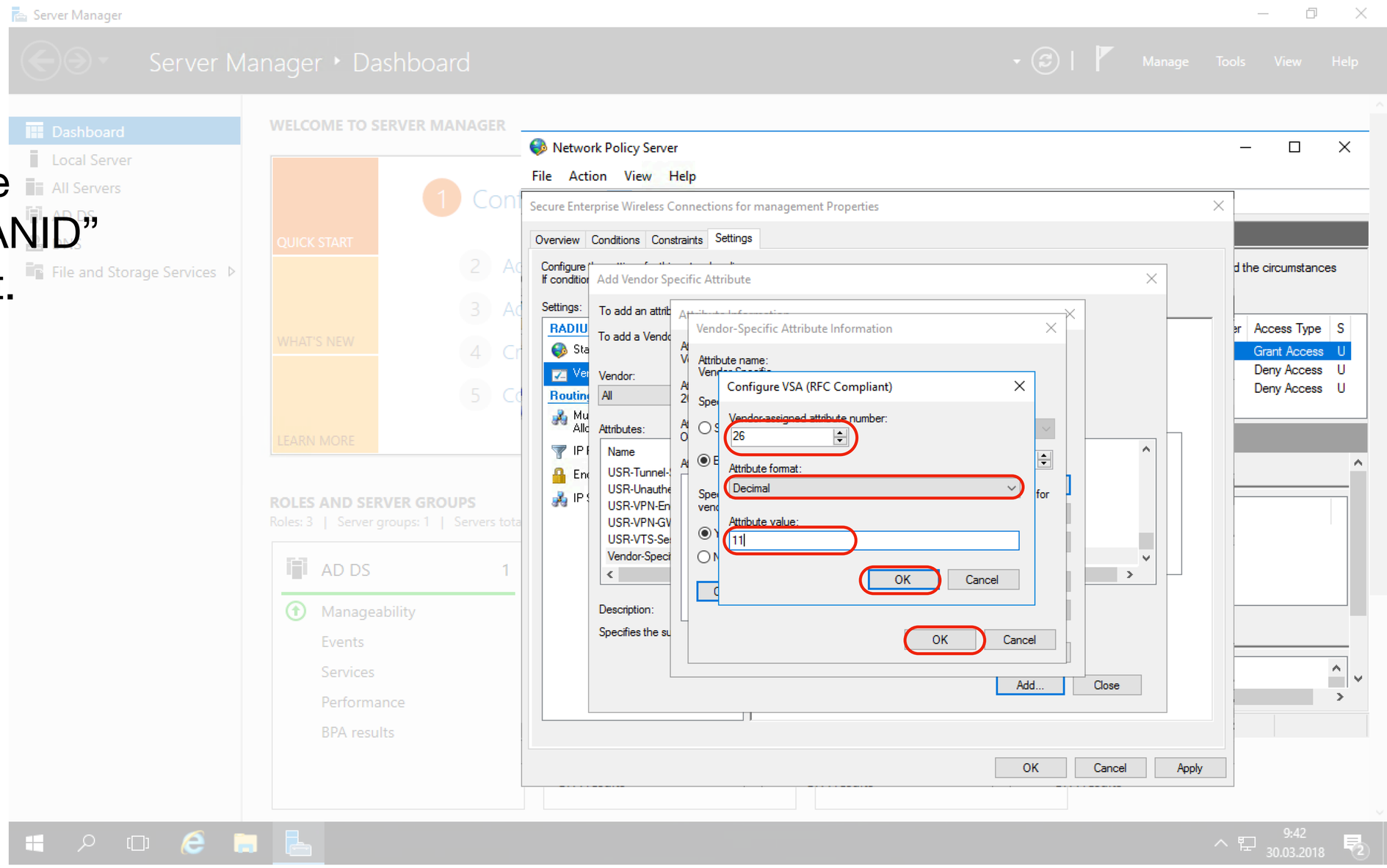
Configure NPS - Radius

- As MikroTik is not listed, we need to enter MikroTik's vendor code 14988 manually.
- Select "Yes it conforms" and click "Configure Attribute" to specify VLAN attributes



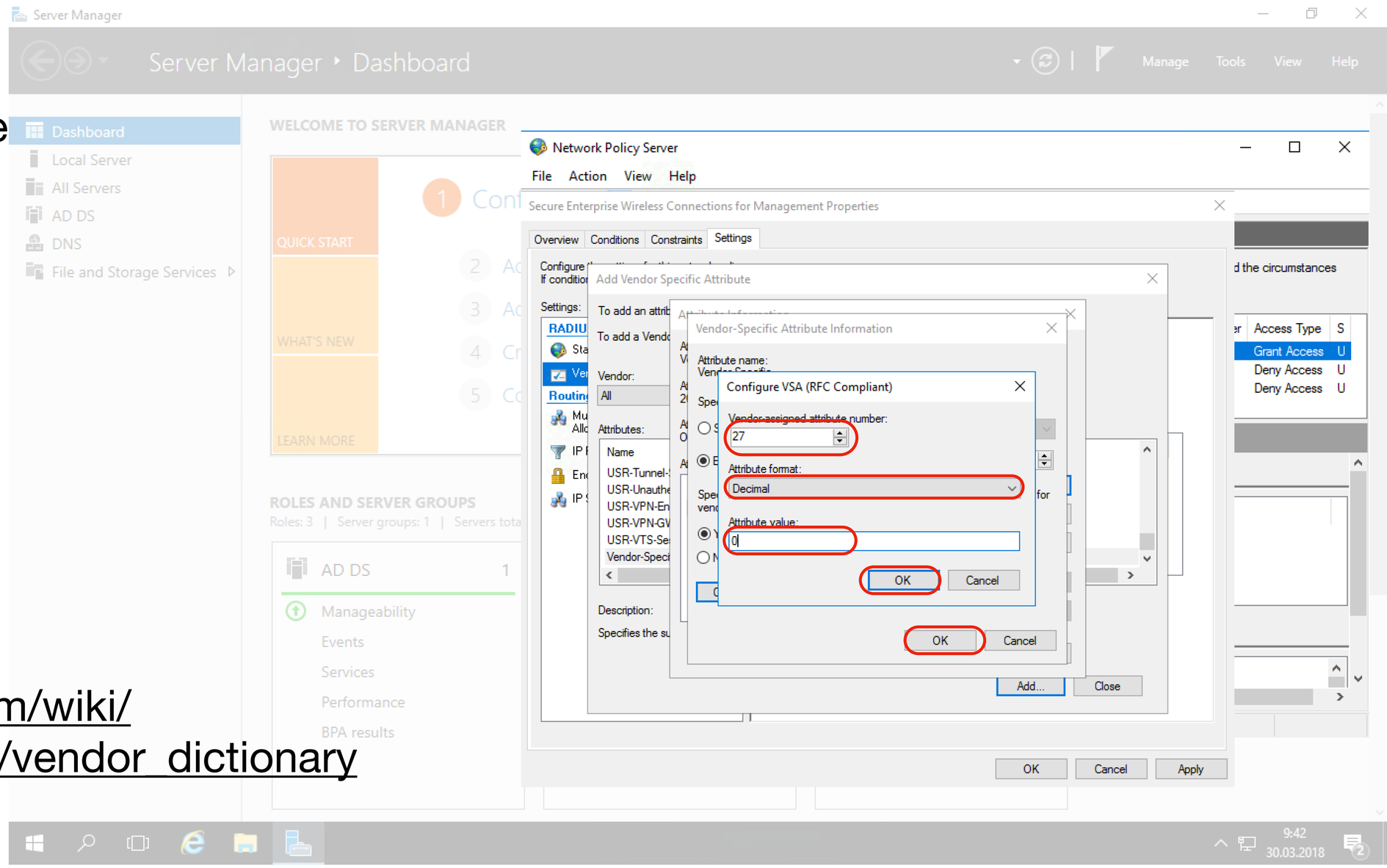
Configure NPS - Radius

- Vendor-assigned attribute number for the “Mikrotik_Wireless_VLANID” is 26. Therefore insert it.
- Attribute format for VLAN id is “Decimal”
- Field “Attribute value” specifies the VLAN ID value. In or case it is 11 (Management).
- Click “OK”, “OK”



Configure NPS - Radius

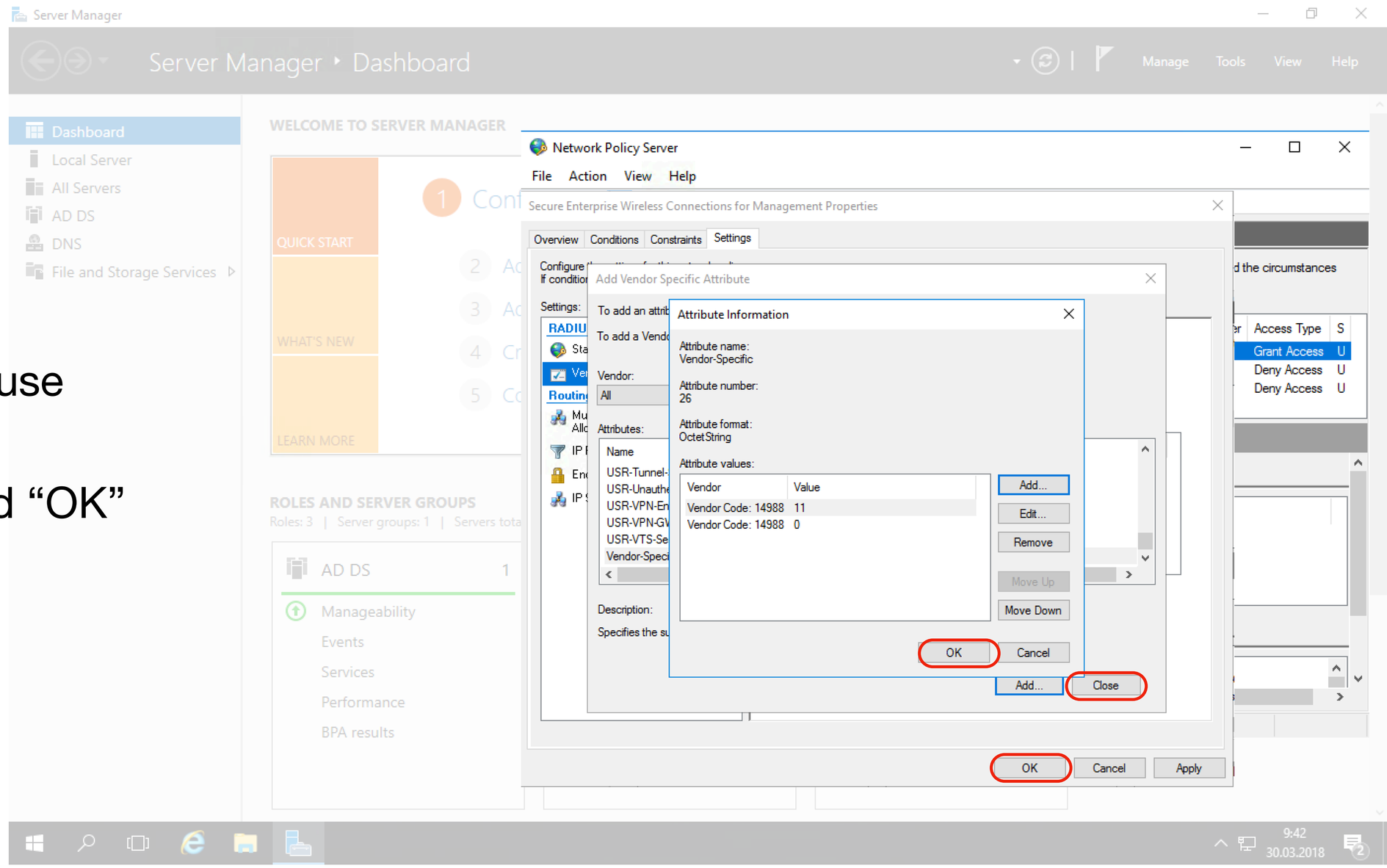
- Add option 27, which specifies VLAN type we will use (value 0 = 802.1q).
- Click “OK”, “OK”



- For more options see https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client/vendor_dictionary

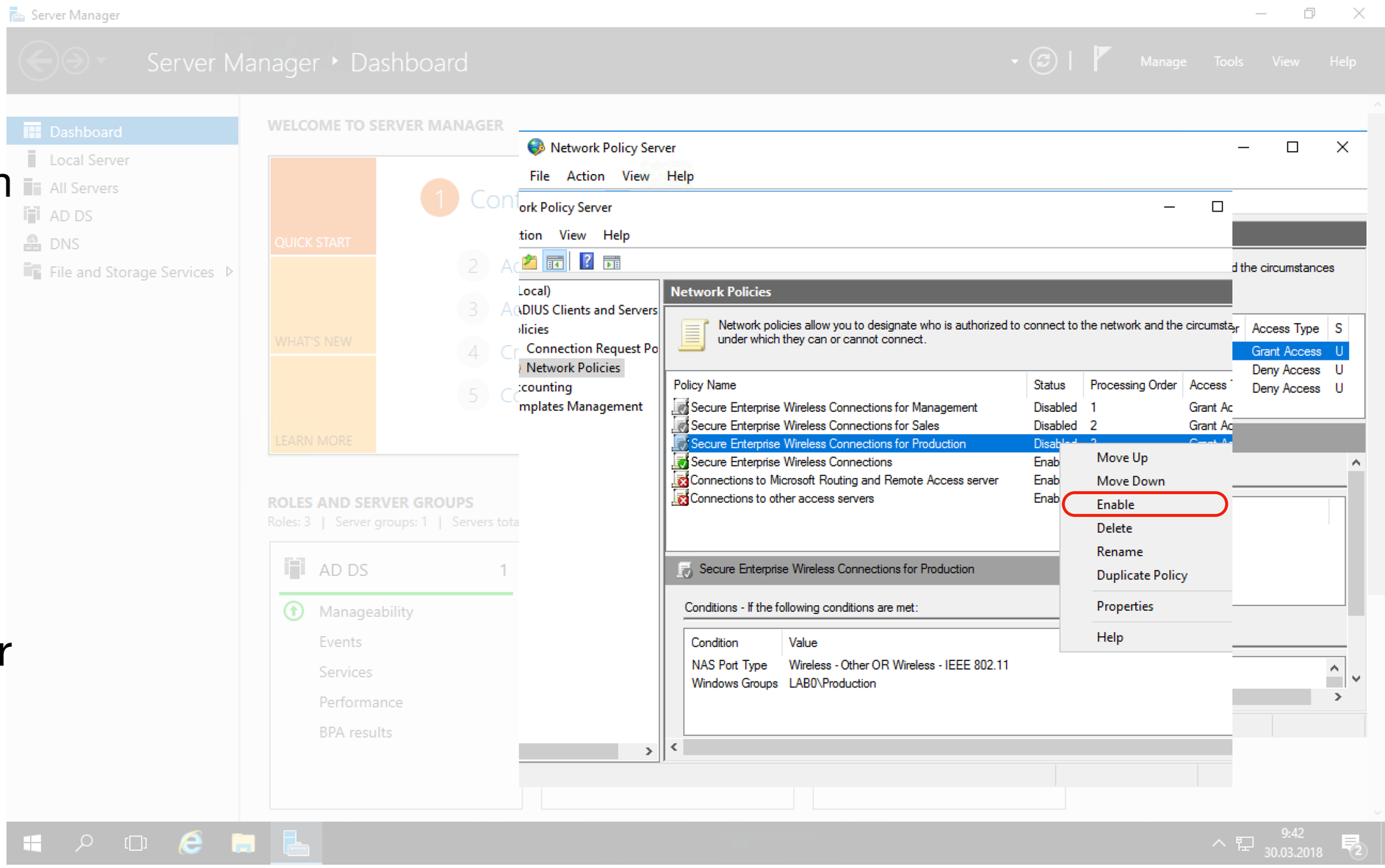
Configure NPS - Radius

- Now we have specified which VLAN ID we will use for specific group.
- Click “OK”, “Close” and “OK”



Configure NPS - Radius

- Repeat last steps for each Group/VLAN, from “duplicate policy” to “specify VLAN ID”.
- More precise policies must be on top of the Policy list, they will be applied first.
- Enable created policies
- General policy, for other users, must be the last.

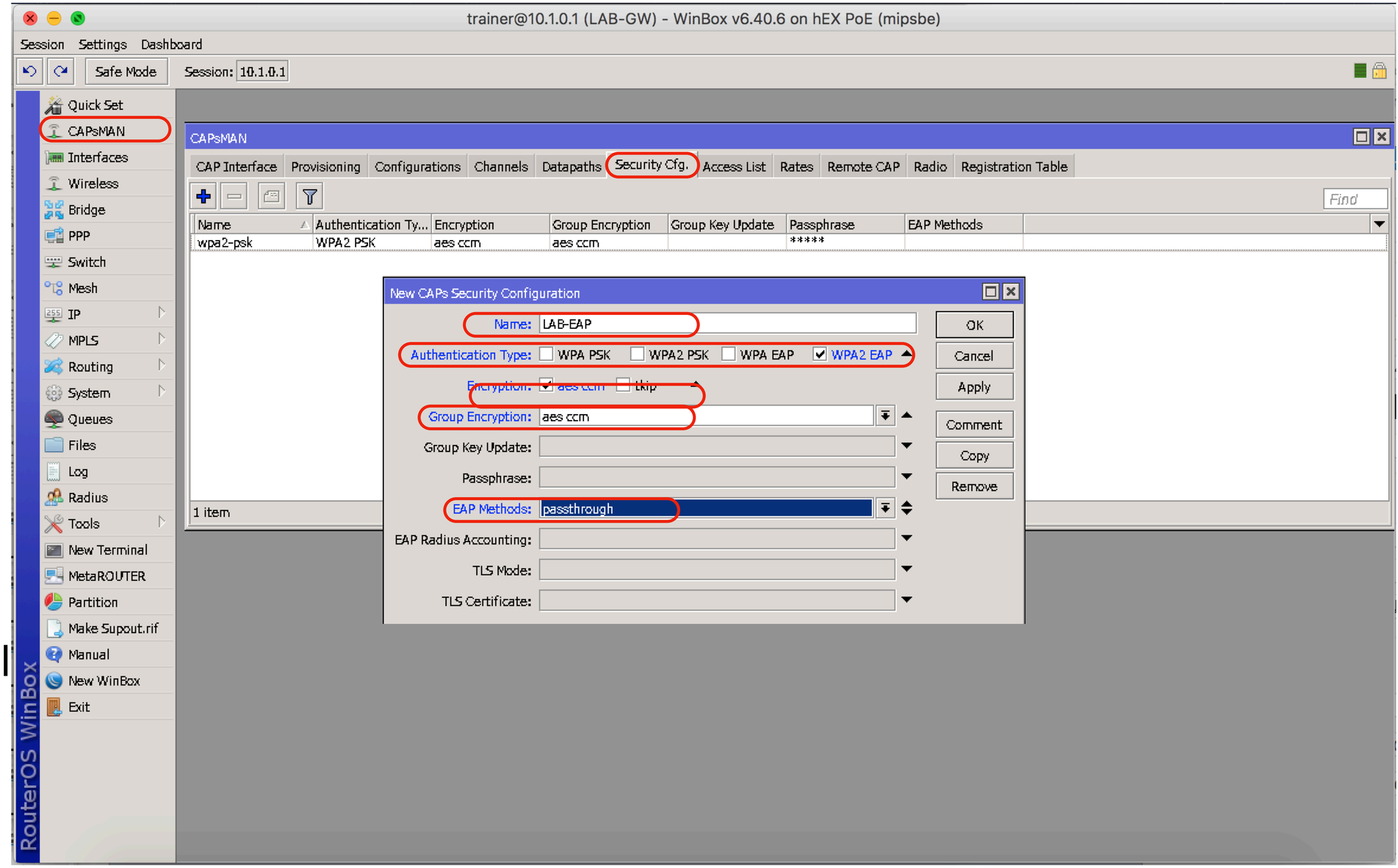


Next Steps

- ~~Install NPS and CA roles on Windows Server~~
- ~~Configure CA~~
- ~~Configure NPS - RADIUS Server~~
- **Reconfigure CAPsMAN**
- Install CA on client device's

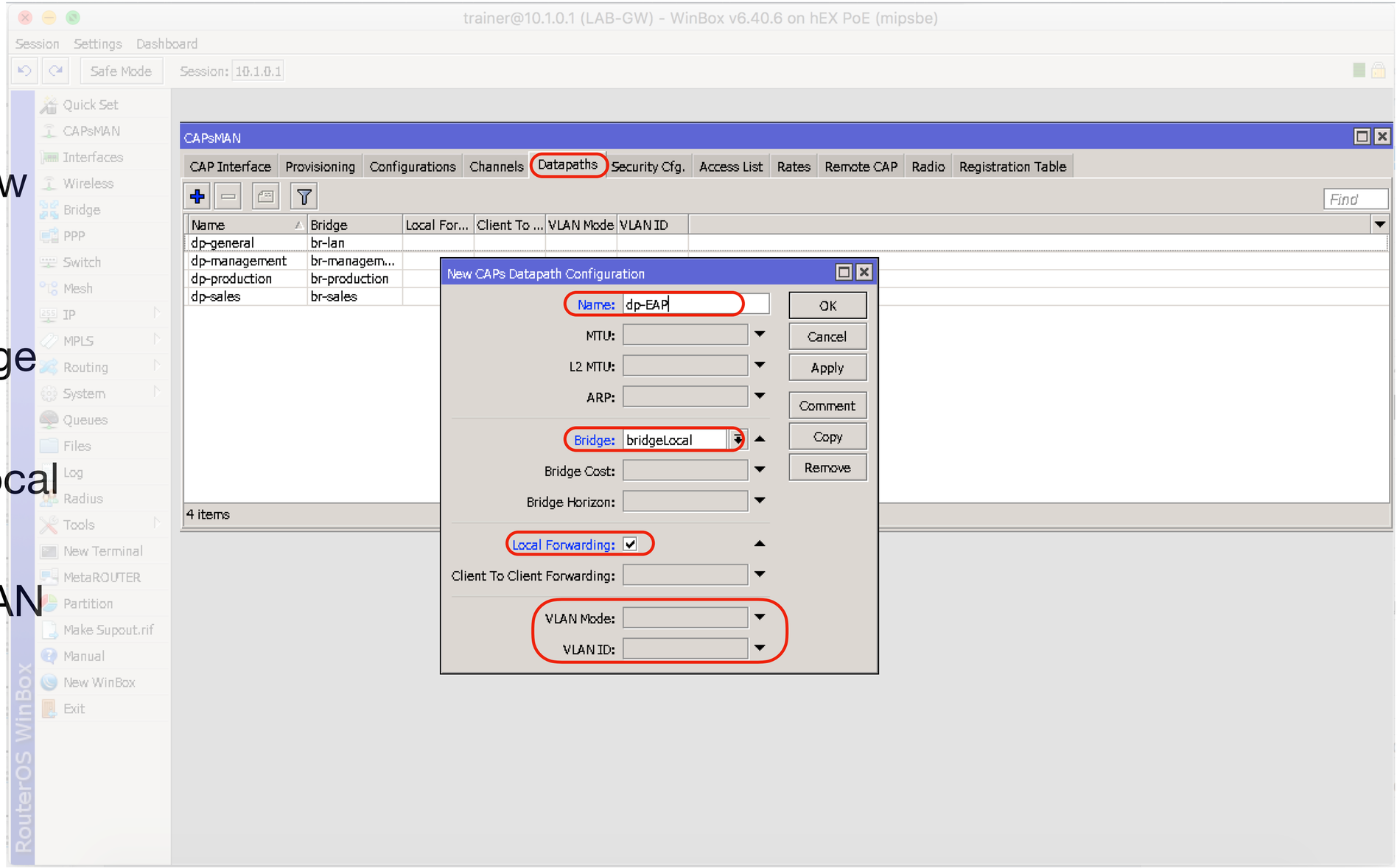
Add New Security Configuration

- In CAPsMAN select “Security cfg” and click “Add”
- Name “LAB-EAP”
- Authentication type “WAP2-EAP”
- Encryption “aes ccm”
- Group Encryption “aes ccm”
- EAP Method “passthrough” - we will authenticate in RADIUS



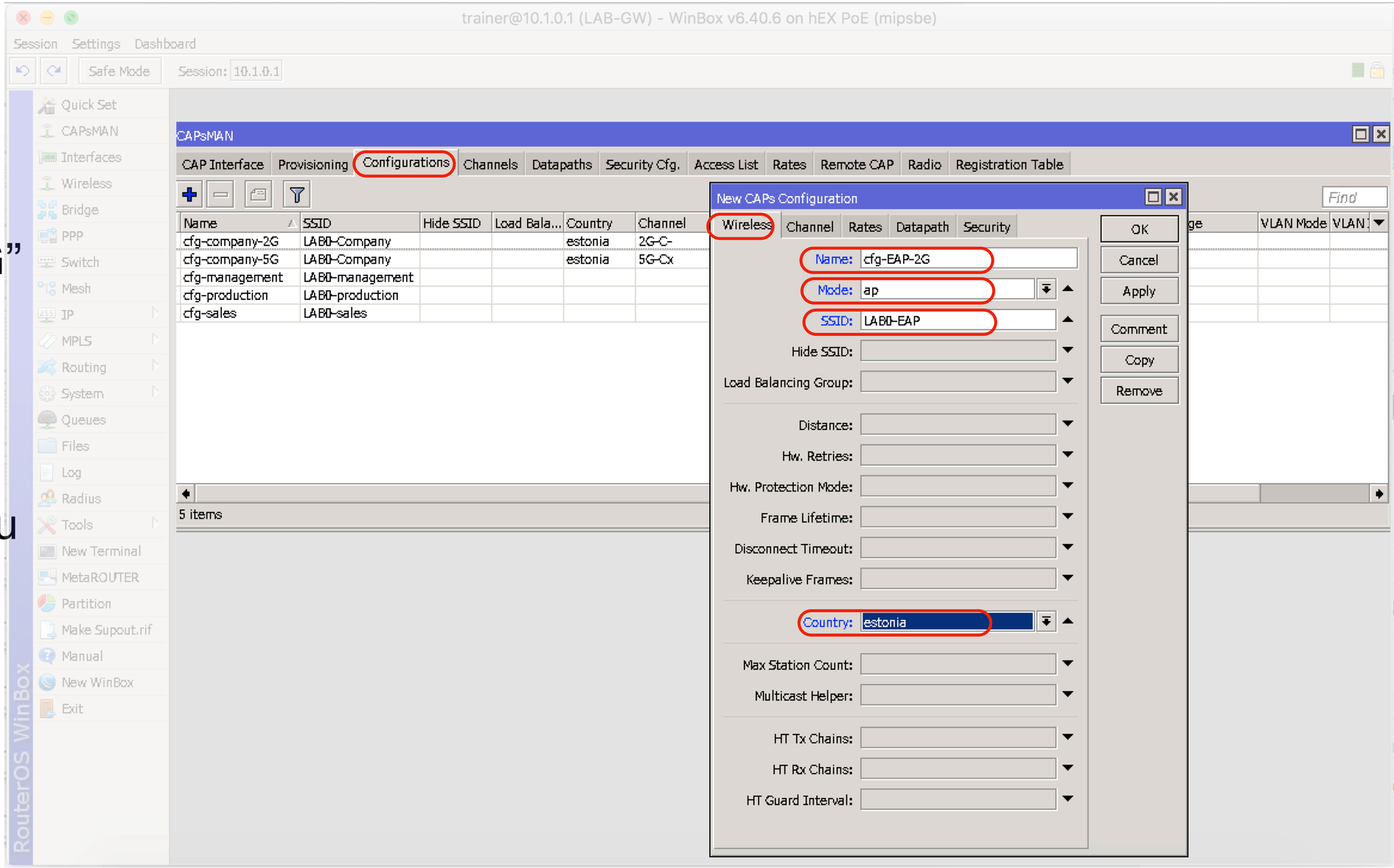
Add New Datapath

- Select “Datapath” tab and click “Add”.
- Give a name for the new datapath - “dp-EAP”
- Select bridge - it must correspond to the bridge name on CAP’s
- In our case, enable “Local Forward”
- We do not specify “VLAN Mode” and “VLAN ID” as they come from RADIUS



Add New Configuration

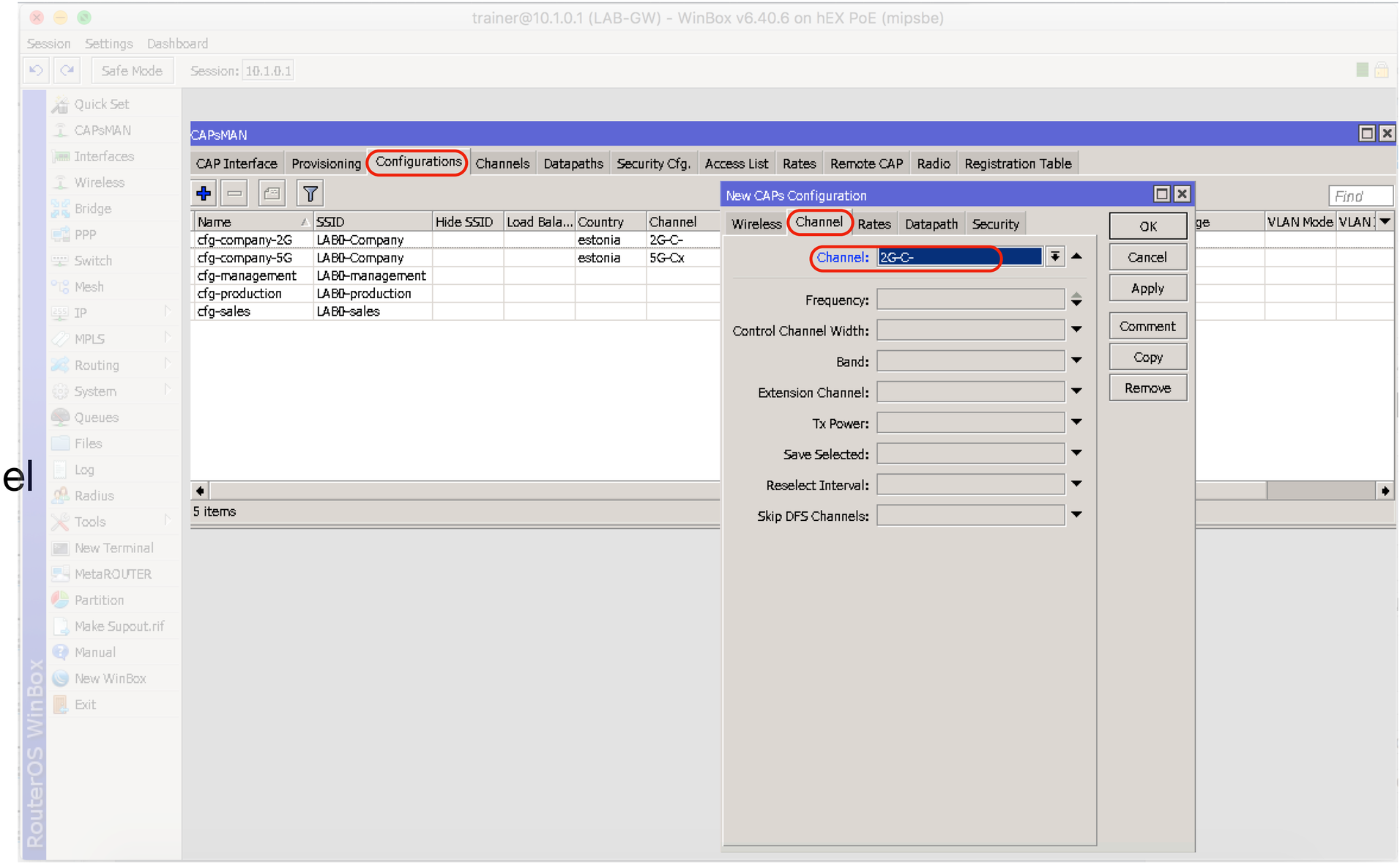
- In “Wireless” tab set
  - Name = “cfg-EAP-2G”
  - Mode = “ap”
  - SSID = “LAB0-EAP”
  - Country - in our case it is “Estonia”, but You need to choice a proper one



Add New Configuration

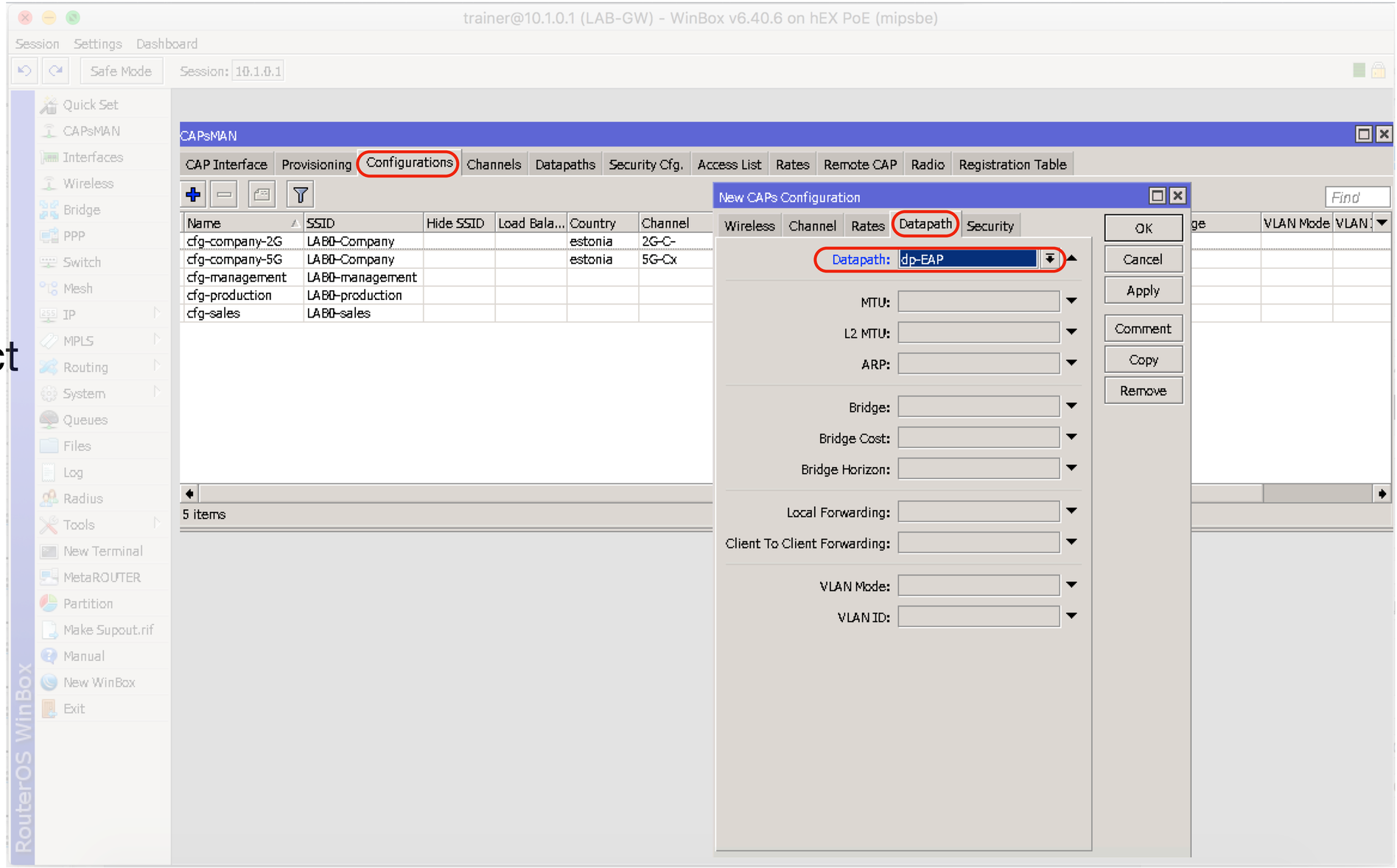
- In “Channel” tab set
  - Channel = 2G-C-

In our case it is pre defined frequency/channel with no extension



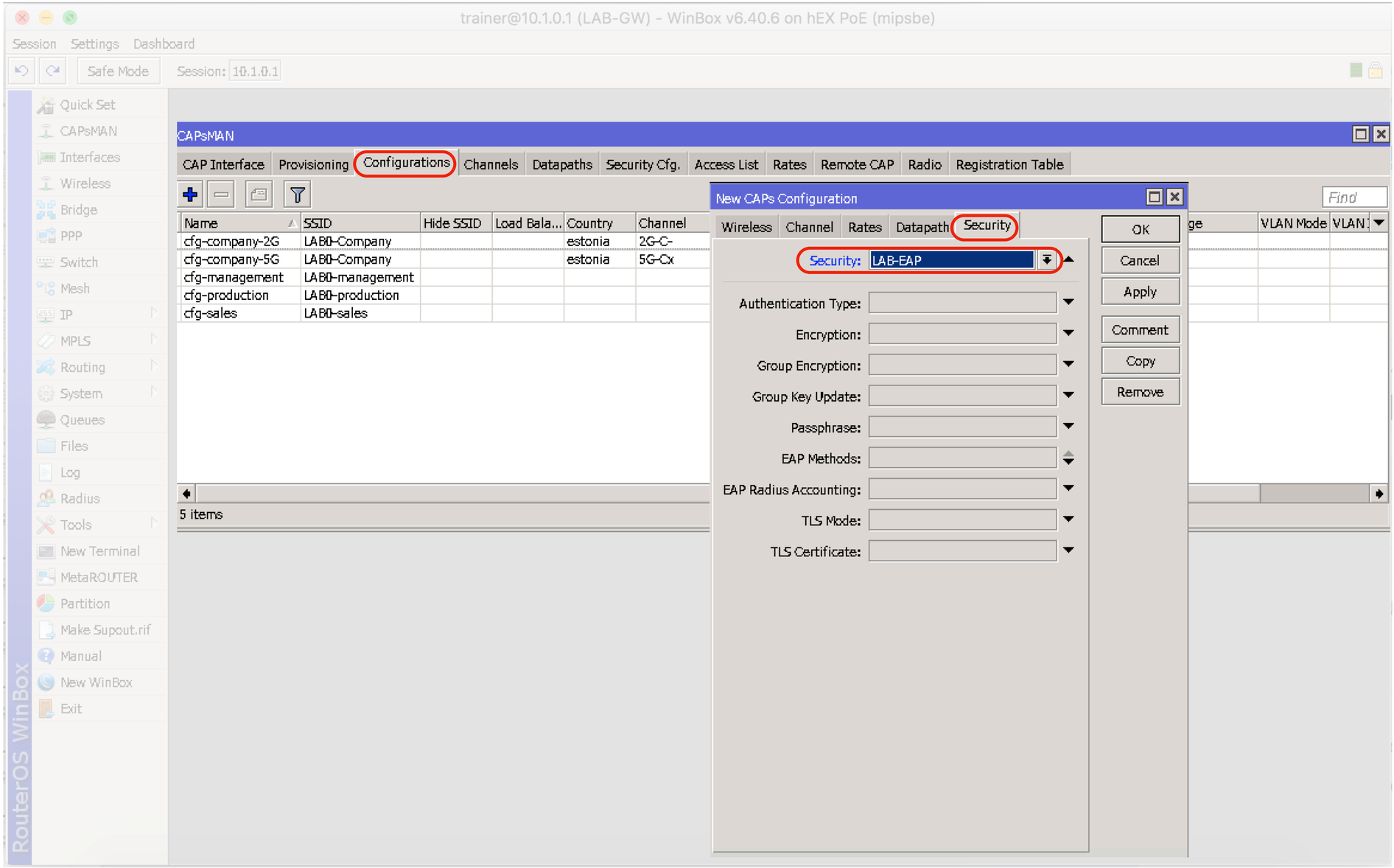
Add New Configuration

- In “Datapath” tab select previously created datapath “dp-EAP”



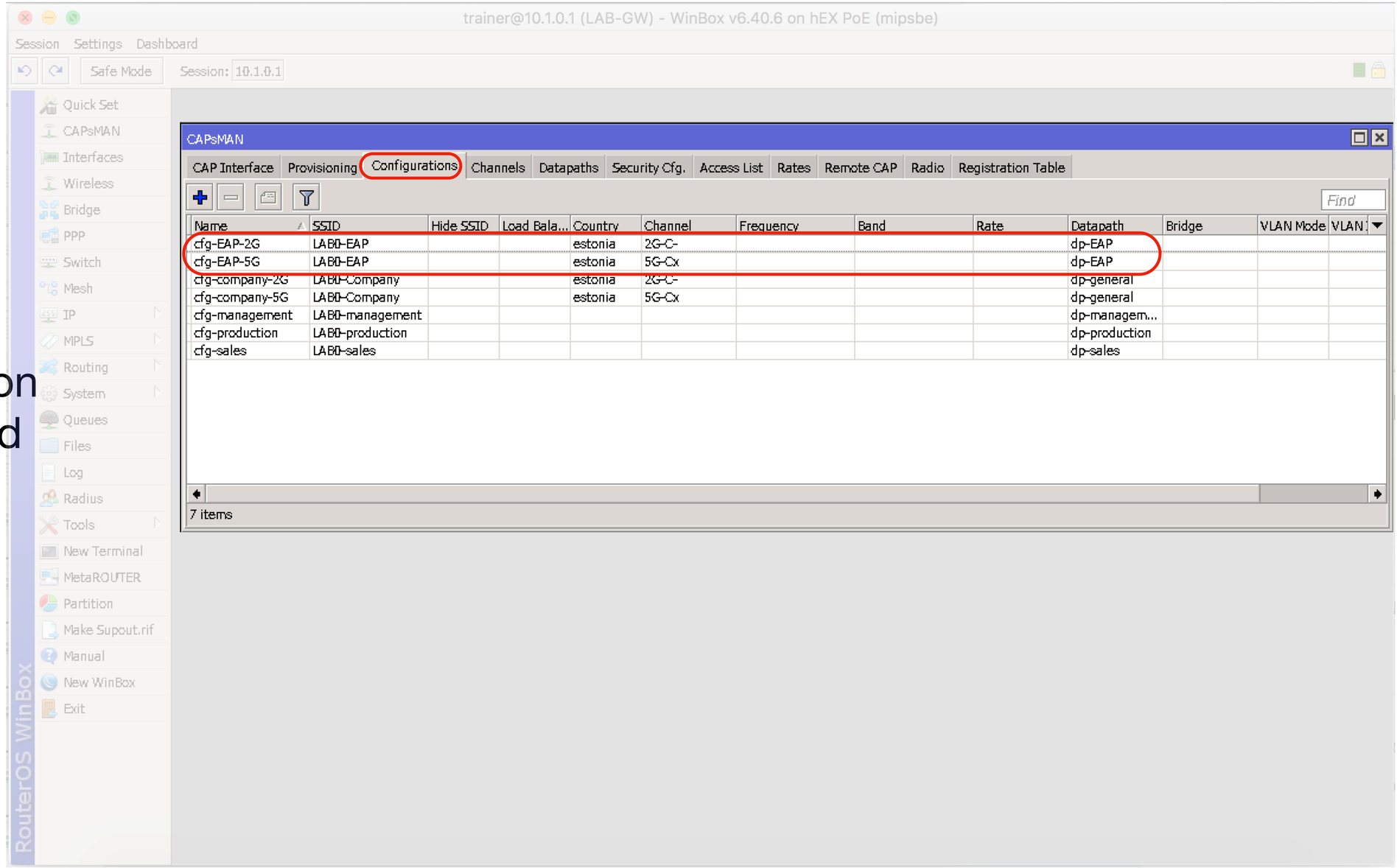
Add New Configuration

- In “Security” tab select previously created Security configuration “LAB-EAP”
- Save configuration clicking “OK”



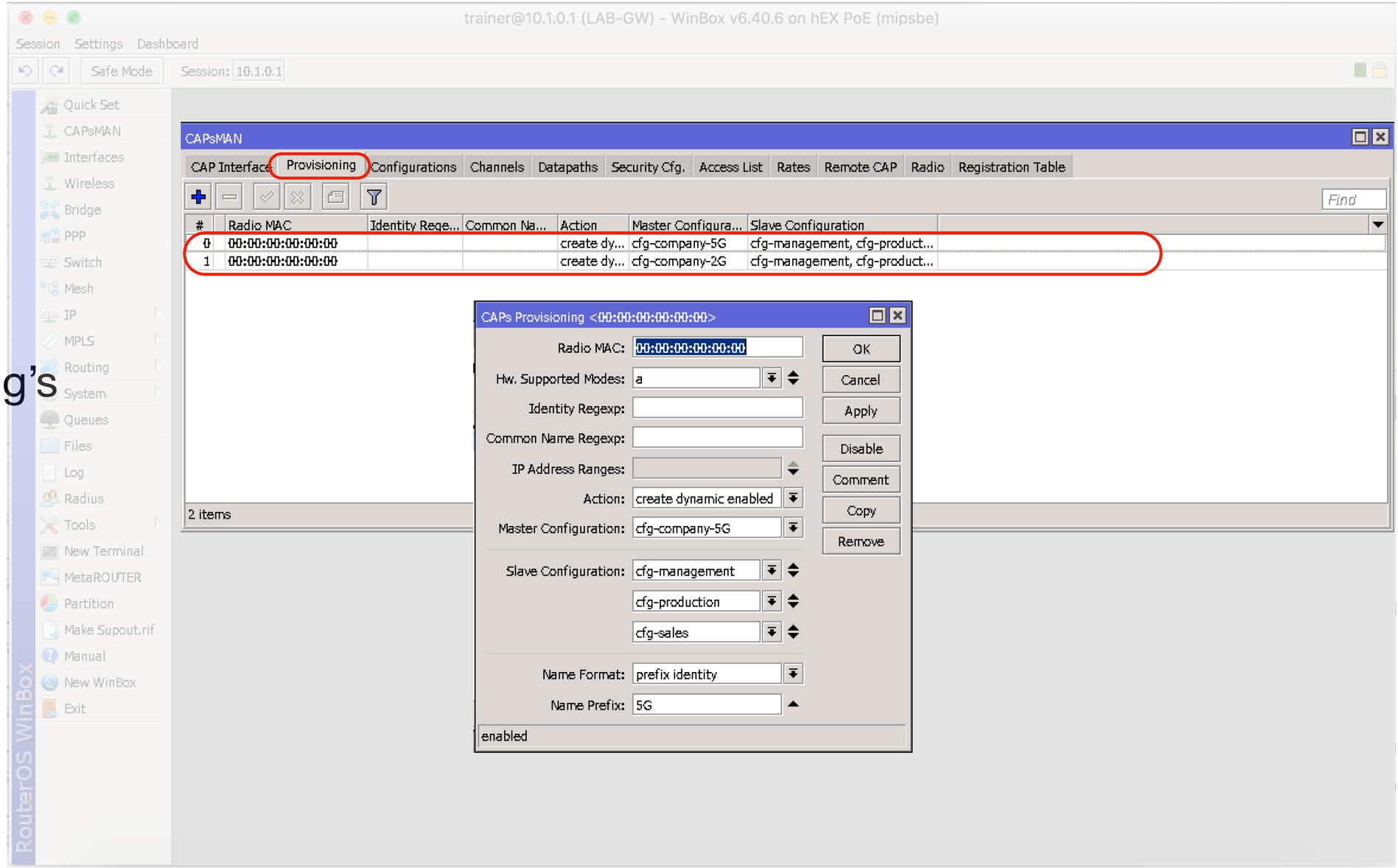
Add New Configuration

- Add similar configuration for 5GHz (A/N/AC) band



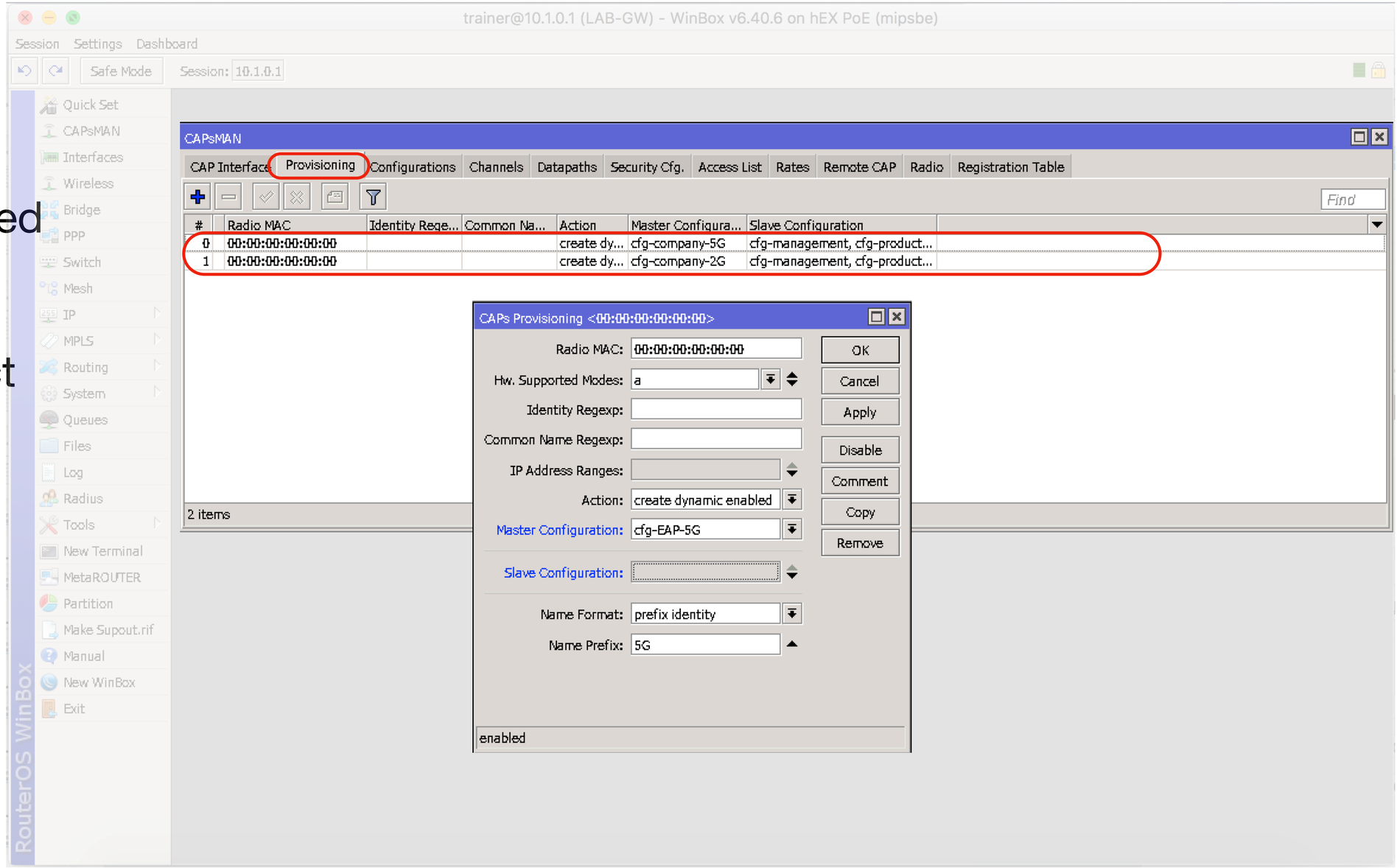
Update Provisioning's

- Select provisioning tab
- Edit current provisioning's
- Remove unnecessary configurations



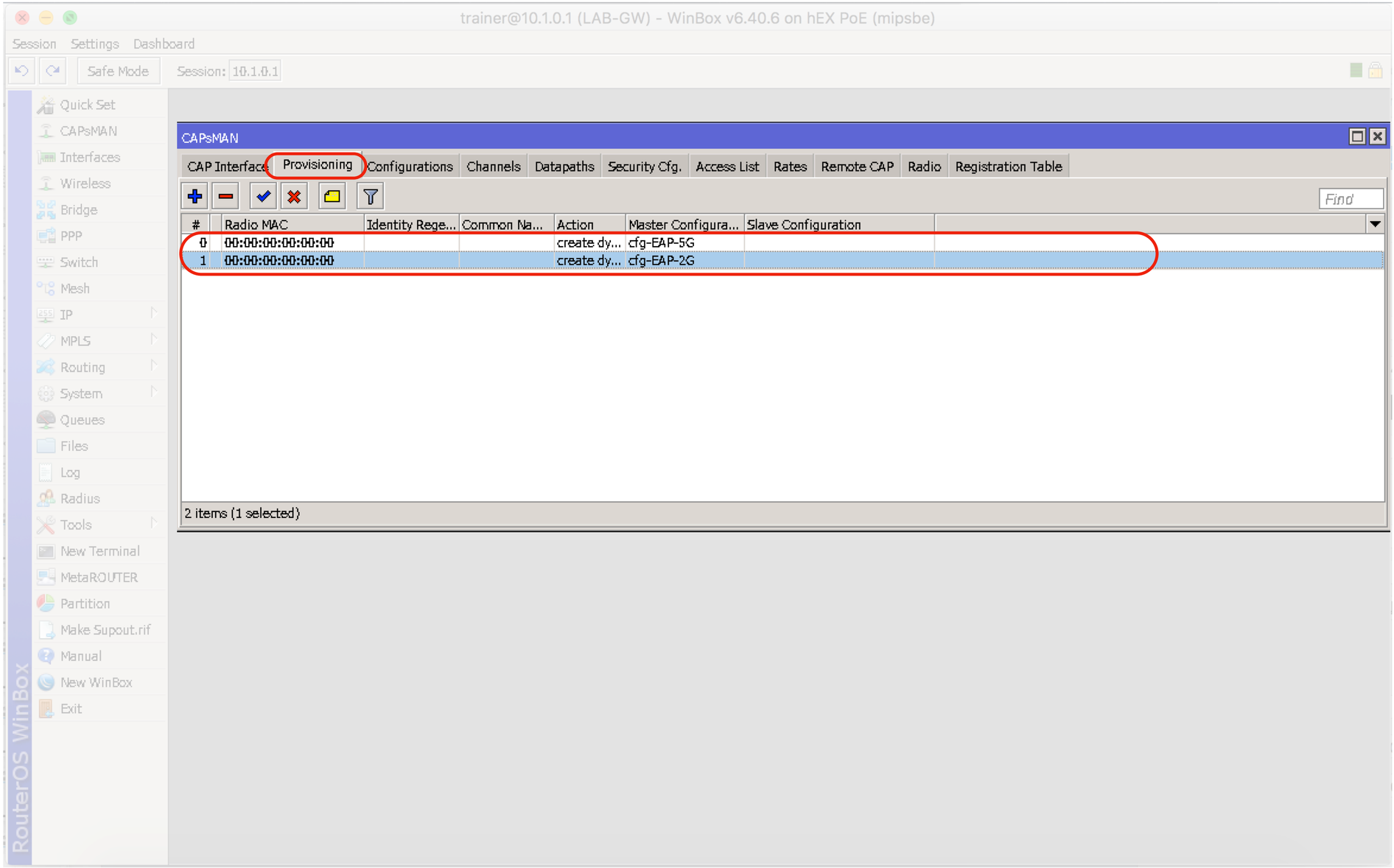
Update Provisioning's

- Select previously created EAP configuration.
  As we have hardware filter for "A" here, select matching - in our case "cfg-EAP-5G"
- Save Provisioning



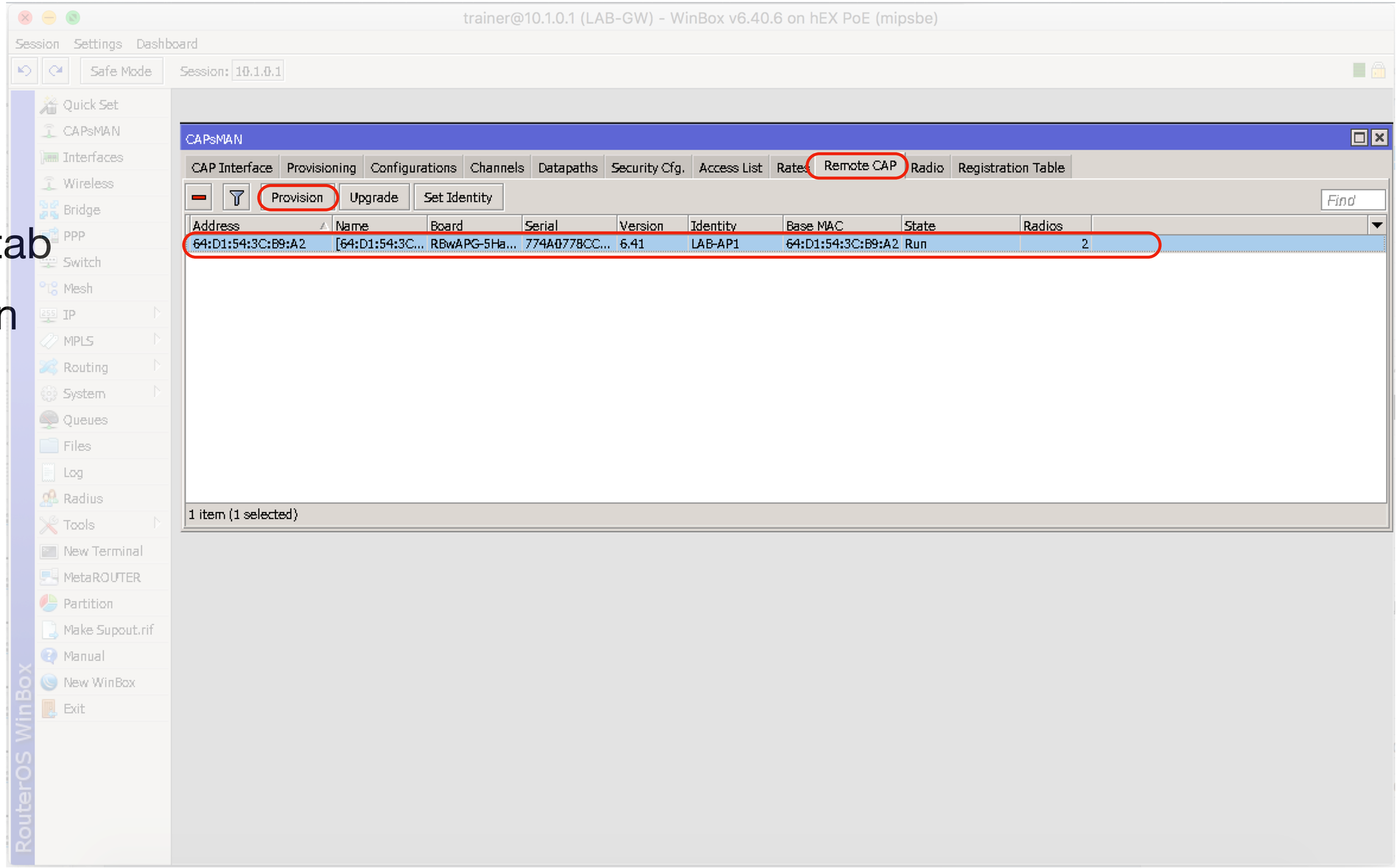
Provisioning

- Correct also the 2GHz provisioning - remove old, unneeded and add new matching EAP configuration



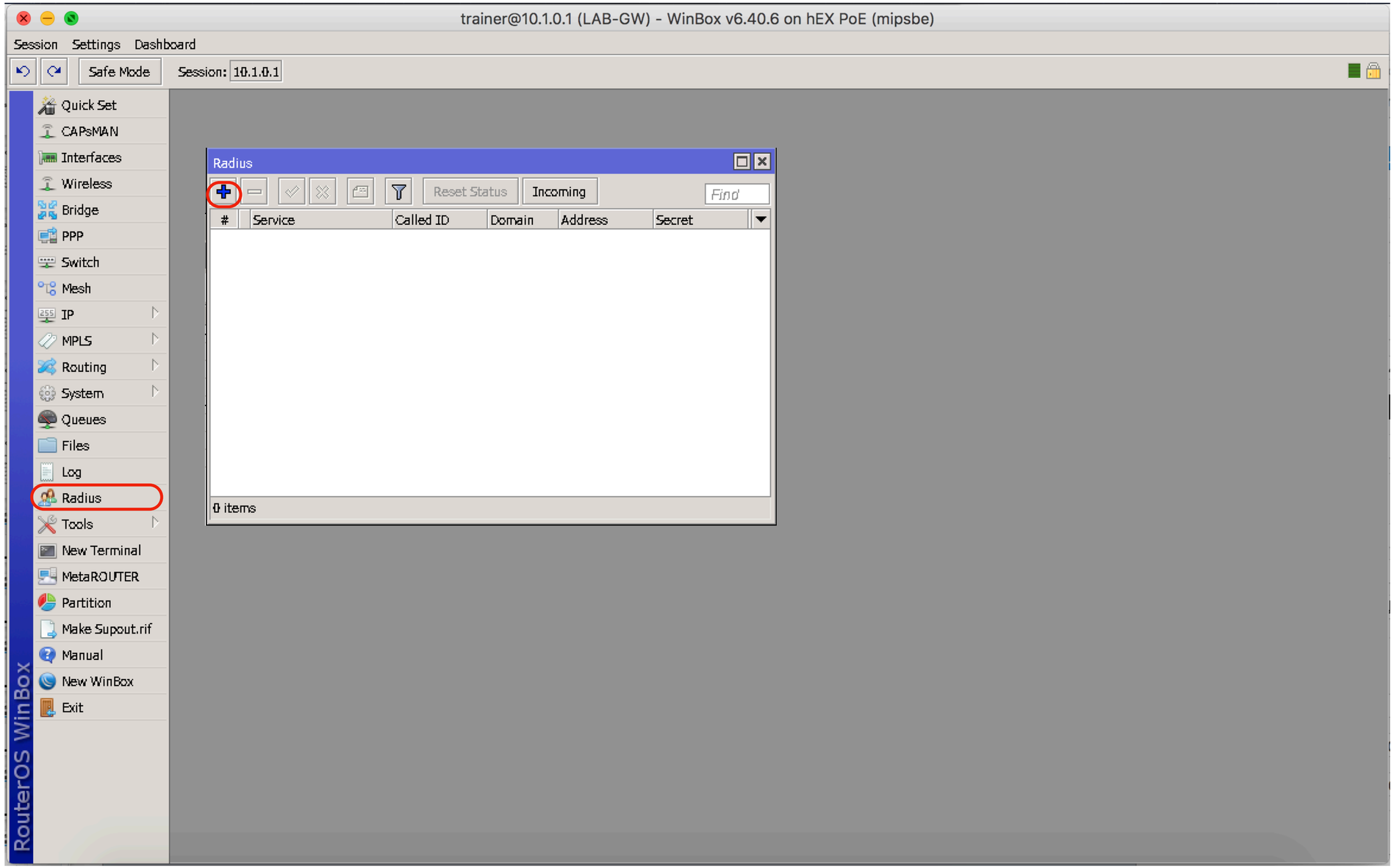
Reconfigure CAP’s

- Select “Remote CAP” tab
- Select access points on the list and click “Provision” - Now we have reconfigured all CAP’s to use EAP



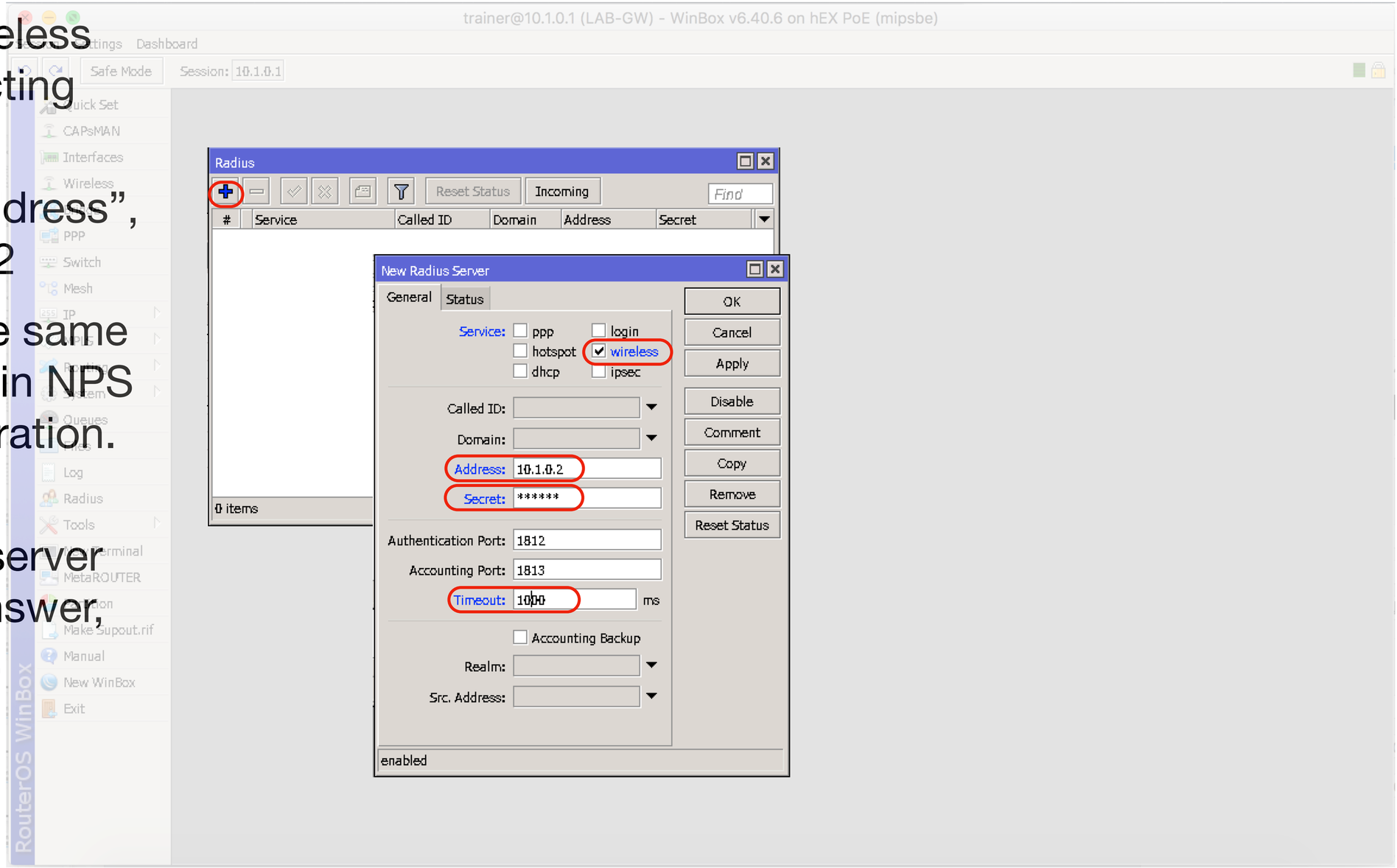
Configure RADIUS Client

- In the end we need to configure RADIUS Client.
- Open “Radius” and click “Add”



Configure RADIUS Client

- Enable RADIUS for wireless authentication by selecting “service” “wireless”
- Set RADIUS server “address”, in our case it is 10.1.0.2
- Set Shared Secret - the same secret that we created in NPS RADIUS Client configuration.
- Based on my personal experience, Windows server need a more time to answer, set timeout to 1000ms.
- Save Radius settings.

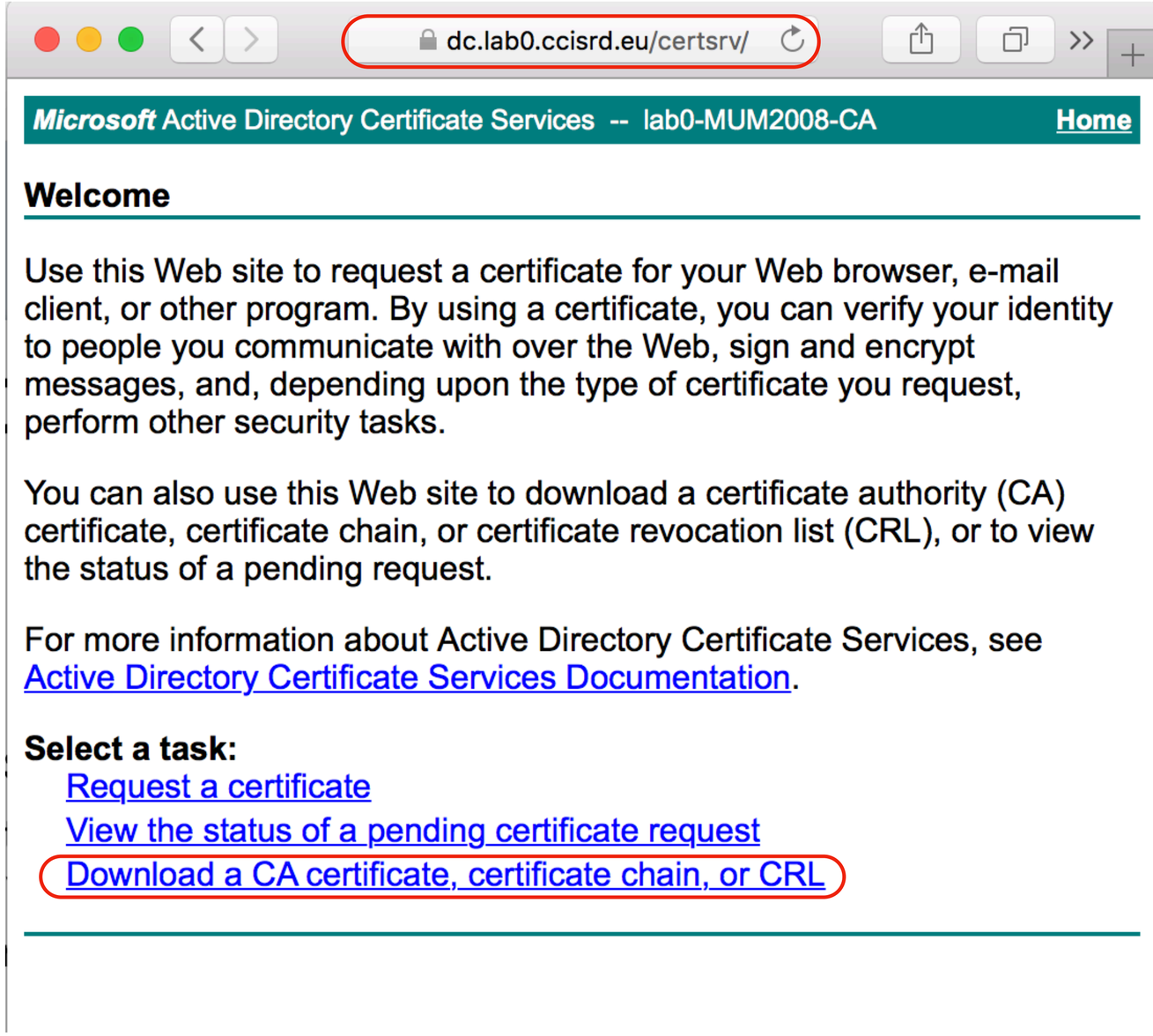


Next Steps

- ~~Install NPS and CA roles on Windows Server~~
- ~~Configure CA~~
- ~~Configure NPS - RADIUS Server~~
- ~~Reconfigure CAPsMAN~~
- **Install CA on client device that are not domain members**

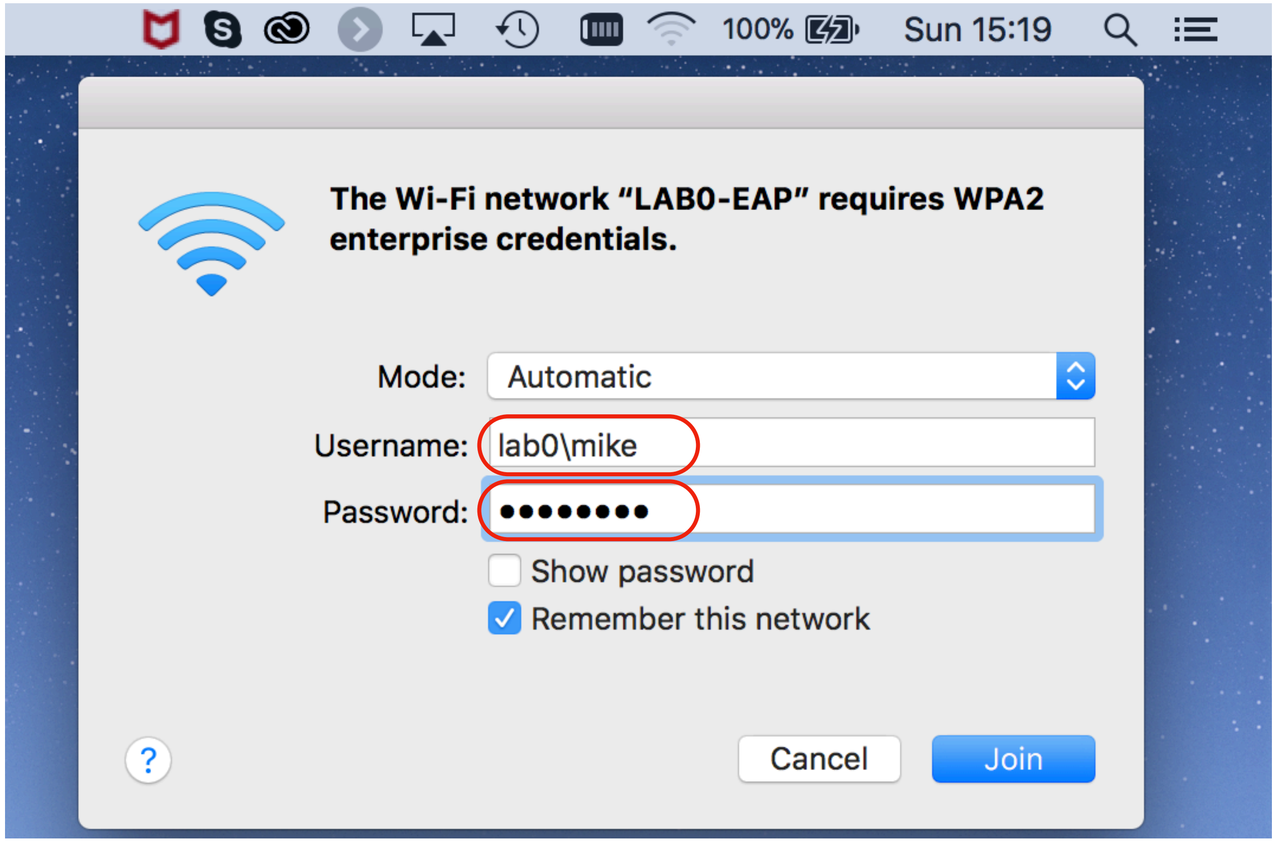
Install CA Certificate

- Open certificate server URL via browser. In our case it is https://dc.lab0.ccisrd.eu/certsrv
- Download and install CA certificate into your computer (Trusted Root) certificate store.

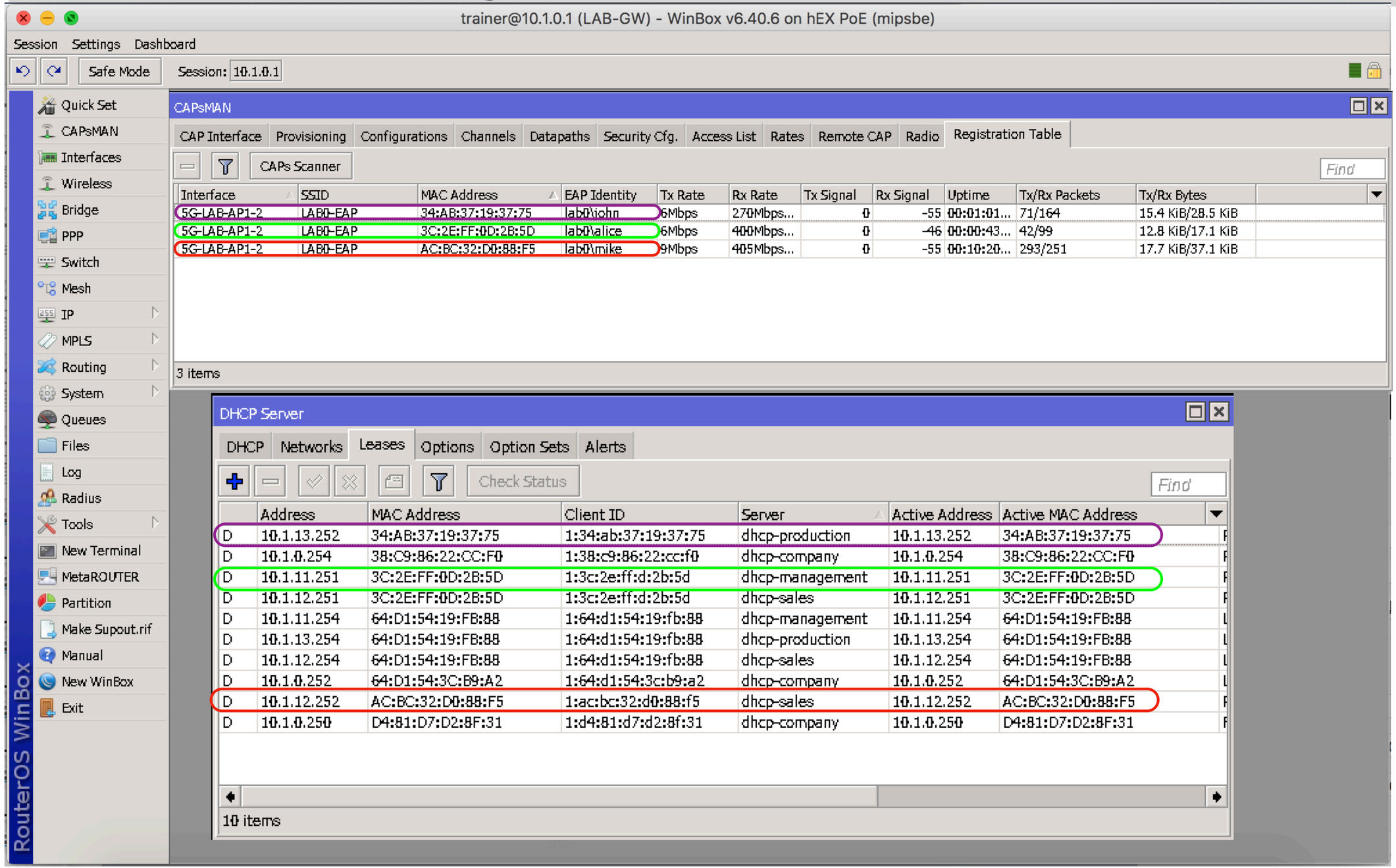


Connect to Wireless

- Connect to the LAB0-EAP network and specify username and password.
- Now you are connected.
- In Windows it works in asimilar way.
- If Your computer is a domain member, CA certificate will be installed automatically.



Verify connected users



Future options

- Configure 2FA on NPS
- Provide user certificates via GPO or install user certificates manually on client devices
- Use computer account if possible instead user account

Summary

- EAP + Dynamic VLAN assignment is not complicated
- We need to
  - Install and configure NPS and CS
  - (Re)configure CAPsMAN
- Start using

CAPsMAN configuration

```
/caps-man channel
add band=2ghz-b/g/n control-channel-width=20mhz extension-channel=disabled name=2G-C-
add band=5ghz-a/n/ac control-channel-width=20mhz extension-channel=XX name=5G-Cx
/interface bridge
add name=br-lan
add comment=vlan-11 name=br-management
add comment=vlan-13 name=br-production
add comment=vlan-12 name=br-sales
add comment=CAPsMAN name=bridgeLocal
/interface vlan
add comment=management interface=ether5 name=vlan11-ether5 vlan-id=11
add comment=Sales interface=ether5 name=vlan12-ether5 vlan-id=12
add comment=Production interface=ether5 name=vlan13-ether5 vlan-id=13
/caps-man datapath
add bridge=br-lan name=dp-general
add bridge=br-sales name=dp-sales
add bridge=br-management name=dp-management
add bridge=br-production name=dp-production
add bridge=bridgeLocal local-forwarding=yes name=dp-EAP
/caps-man security
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm name=wpa2-psk passphrase=\
    Training-2018
add authentication-types=wpa2-eap eap-methods=passthrough encryption=aes-ccm group-encryption=aes-ccm \
    name=LAB-EAP
/caps-man configuration
add channel=2G-C- country=estonia datapath=dp-general mode=ap name=cfg-company-2G security=wpa2-psk ssid=\
    LAB0-Company
add channel=5G-Cx country=estonia datapath=dp-general mode=ap name=cfg-company-5G security=wpa2-psk ssid=\
    LAB0-Company
add datapath=dp-management mode=ap name=cfg-management security=wpa2-psk ssid=LAB0-management
add datapath=dp-production mode=ap name=cfg-production security=wpa2-psk ssid=LAB0-production
add datapath=dp-sales mode=ap name=cfg-sales security=wpa2-psk ssid=LAB0-sales
add channel=2G-C- country=estonia datapath=dp-EAP mode=ap name=cfg-EAP-2G security=LAB-EAP ssid=LAB0-EAP
add channel=5G-Cx country=estonia datapath=dp-EAP mode=ap name=cfg-EAP-5G security=LAB-EAP ssid=LAB0-EAP
/ip pool
add name=dhcp_pool_0_company ranges=10.1.0.2-10.1.0.254
add name=dhcp_pool_11_management ranges=10.1.11.2-10.1.11.254
add name=dhcp_pool_12_sales ranges=10.1.12.2-10.1.12.254
add name=dhcp_pool_13_production ranges=10.1.13.2-10.1.13.254
/ip dhcp-server
add address-pool=dhcp_pool_0_company disabled=no interface=br-lan name=dhcp-company
add address-pool=dhcp_pool_11_management disabled=no interface=br-management name=dhcp-management
add address-pool=dhcp_pool_12_sales disabled=no interface=br-sales name=dhcp-sales
add address-pool=dhcp_pool_13_production disabled=no interface=br-production name=dhcp-production
/system logging action
add name=radiuslog target=memory
/caps-man manager
set enabled=yes
/caps-man provisioning
add action=create-dynamic-enabled hw-supported-modes=a master-configuration=cfg-EAP-5G name-format=\
    prefix-identity name-prefix=5G
add action=create-dynamic-enabled hw-supported-modes=gn master-configuration=cfg-EAP-2G name-format=\
    prefix-identity name-prefix=5G
/interface bridge port
add bridge=br-lan interface=ether2
add bridge=br-lan interface=ether3
add bridge=br-lan interface=ether4
add bridge=br-lan interface=ether5
add bridge=br-management interface=vlan11-ether5
add bridge=br-sales interface=vlan12-ether5
add bridge=br-production interface=vlan13-ether5
/ip address
add address=10.1.0.1/24 interface=br-lan network=10.1.0.0
add address=10.1.11.1/24 interface=br-management network=10.1.11.0
add address=10.1.12.1/24 interface=br-sales network=10.1.12.0
add address=10.1.13.1/24 interface=br-production network=10.1.13.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=ether1
/ip dhcp-server network
add address=10.1.0.0/24 dns-server=10.1.0.1 gateway=10.1.0.1
add address=10.1.11.0/24 dns-server=10.0.0.2 domain=lab0.ccisrd.eu gateway=10.1.11.1
add address=10.1.12.0/24 dns-server=10.0.0.2 domain=lab0.ccisrd.eu gateway=10.1.12.1
add address=10.1.13.0/24 dns-server=10.0.0.2 domain=lab0.ccisrd.eu gateway=10.1.13.1
/ip dns
set allow-remote-requests=yes servers=10.0.0.1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/radius
add address=10.1.0.2 secret=Security service=wireless timeout=1s
/system clock
set time-zone-name=Europe/Tallinn
/system identity
set name=LAB-GW
/system logging
add topics=radius
```

CCISRD
Center for Communication and Informationsecurity
Research and Development

Thank You!

rein.podra@ccisrd.eu