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.

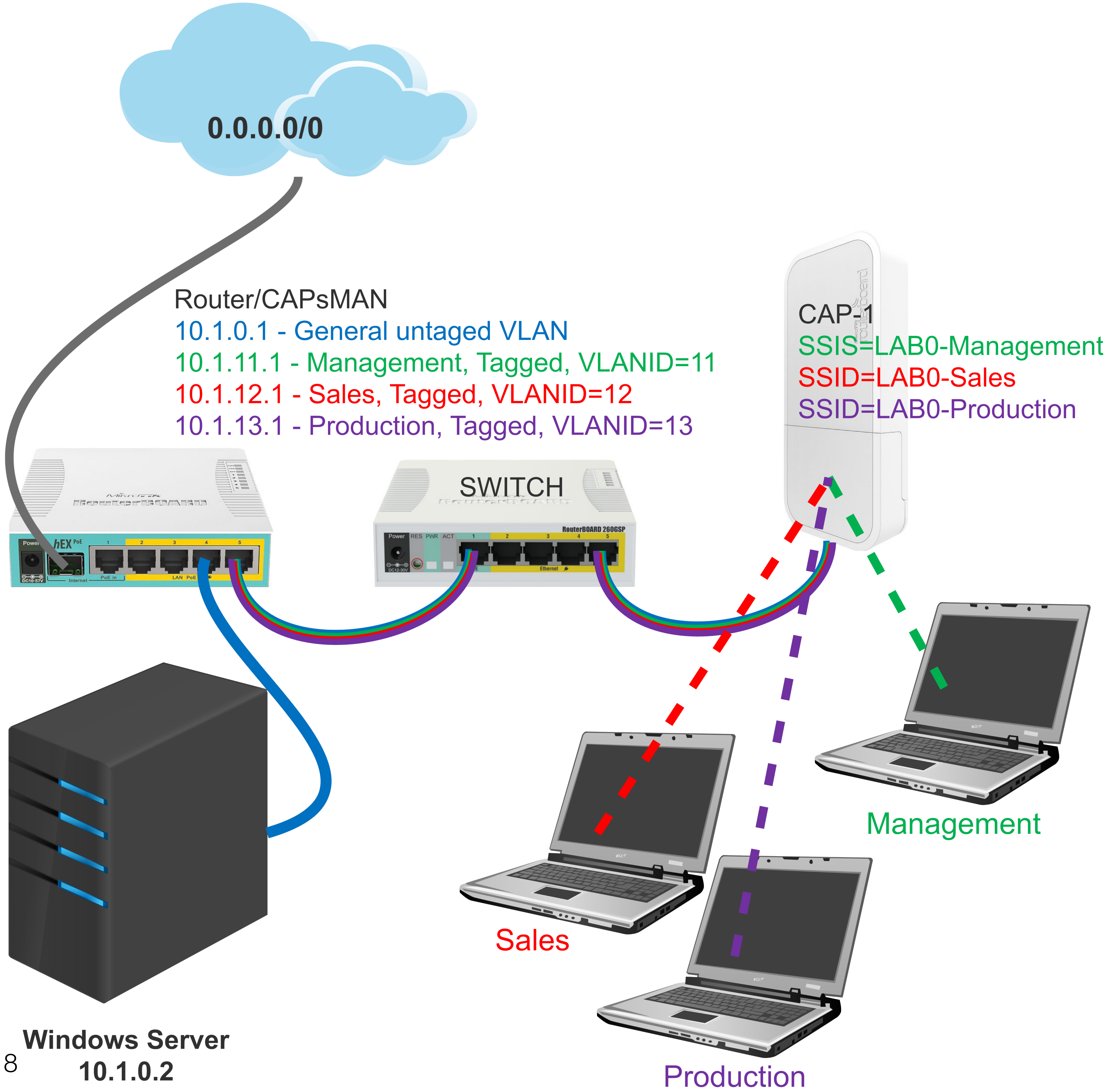
Dynamic VLAN

- 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

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



0.0.0.0/0
Router/CAPsMAN
10.1.0.1 - General untaged VLAN
10.1.11.1 - Management, Tagged, VLANID=11
10.1.12.1 - Sales, Tagged, VLANID=12
10.1.13.1 - Production, Tagged, VLANID=13
SWITCH
CAP-1
SSIS=LAB0-Management
SSID=LAB0-Sales
SSID=LAB0-Production
Management
Sales
Production
Windows Server
10.1.0.2

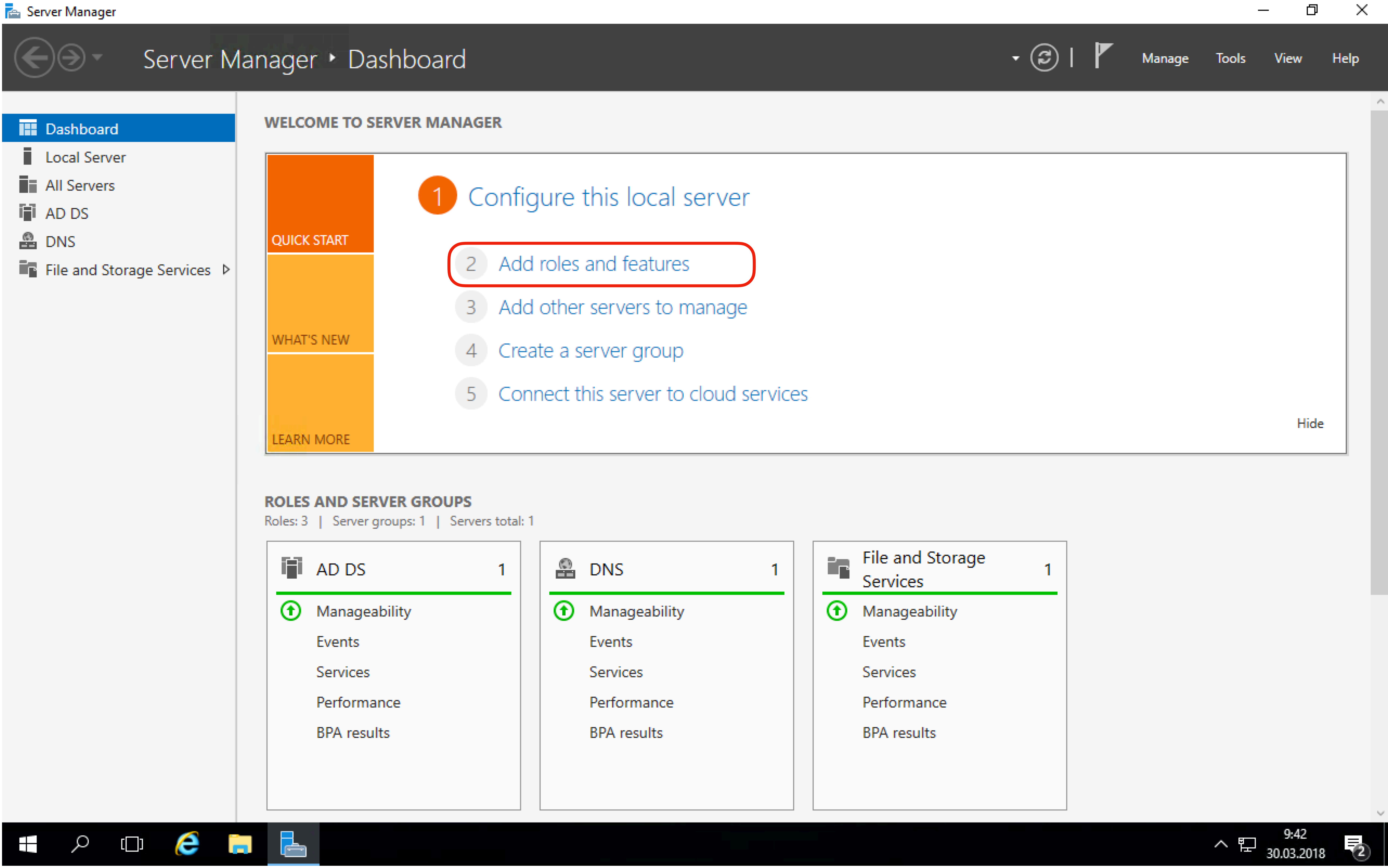
What we need?

- 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



Server Manager

Server Manager ‣ Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

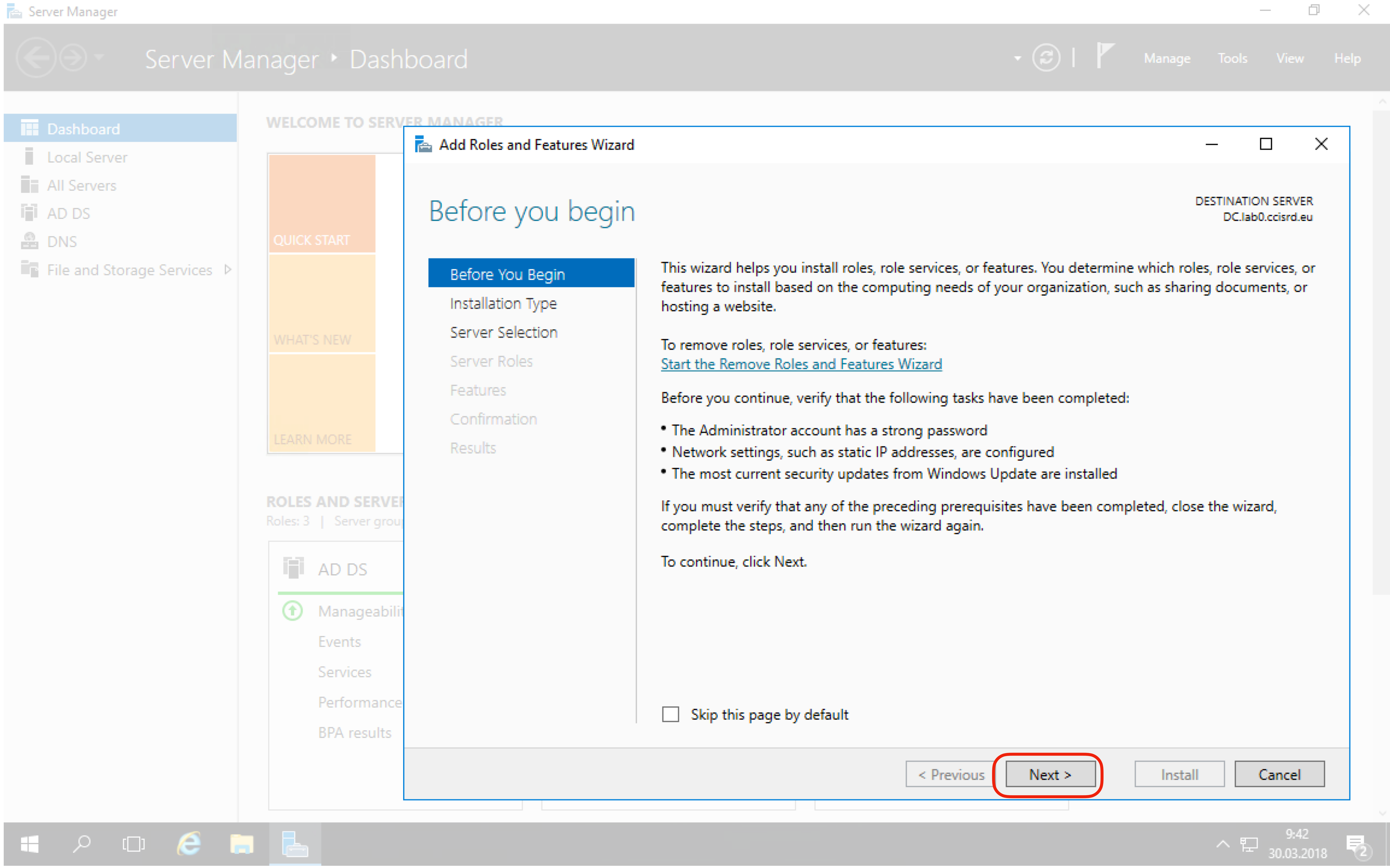
AD DS 1	DNS 1	File and Storage Services 1
Manageability	Manageability	Manageability
Events	Events	Events
Services	Services	Services
Performance	Performance	Performance
BPA results	BPA results	BPA results

9:42
30.03.2018

- In Server Manager click Add roles and features”

Install Roles

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



Before you begin

DESTINATION SERVER
DC.lab0.ccisrd.eu

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

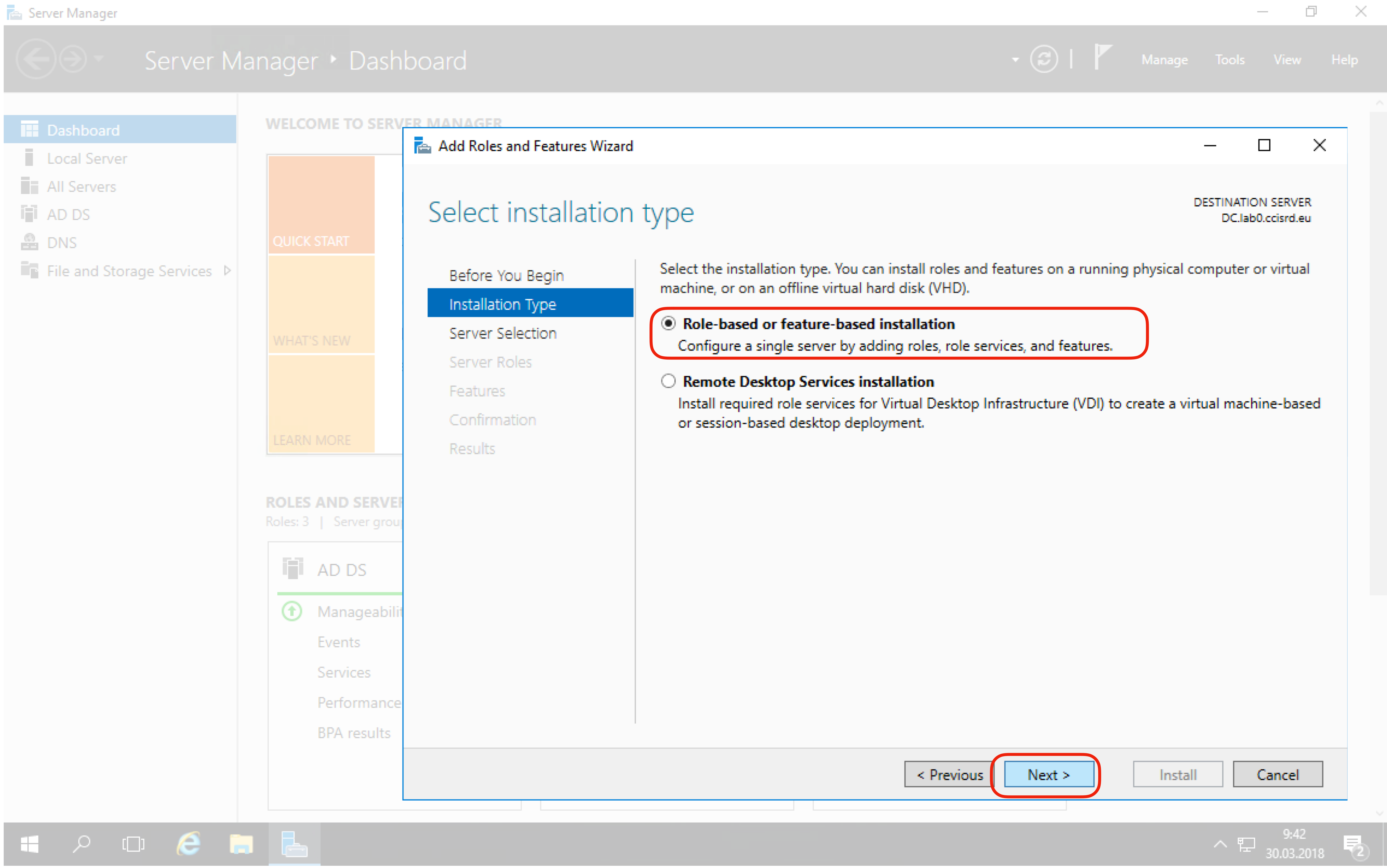
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Install Roles - Installation Type

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



Select installation type

DESTINATION SERVER
DC.lab0.ccisrd.eu

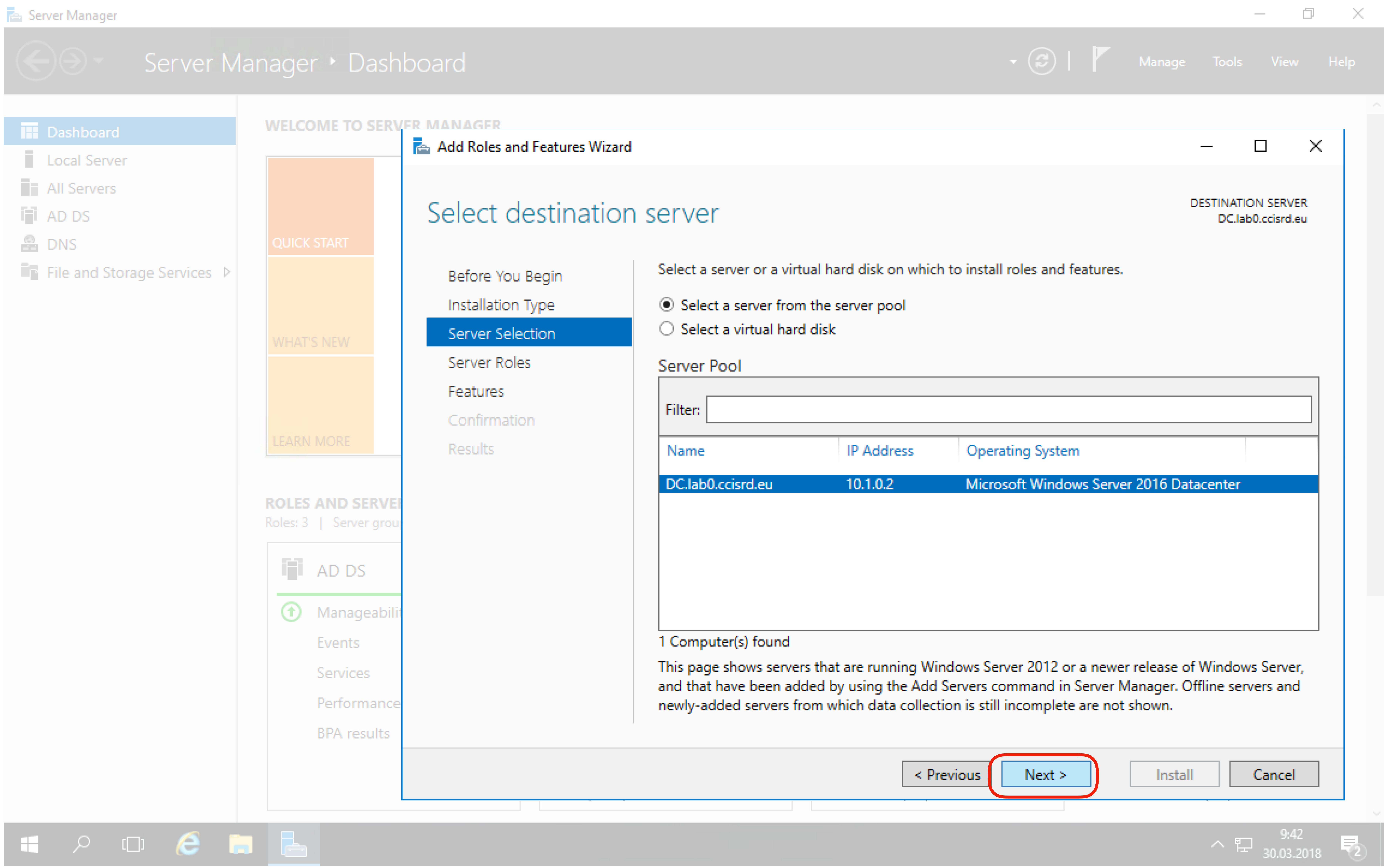
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **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.

Install Roles - Select Server

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



Select destination server

DESTINATION SERVER
DC.lab0.ccisrd.eu

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:

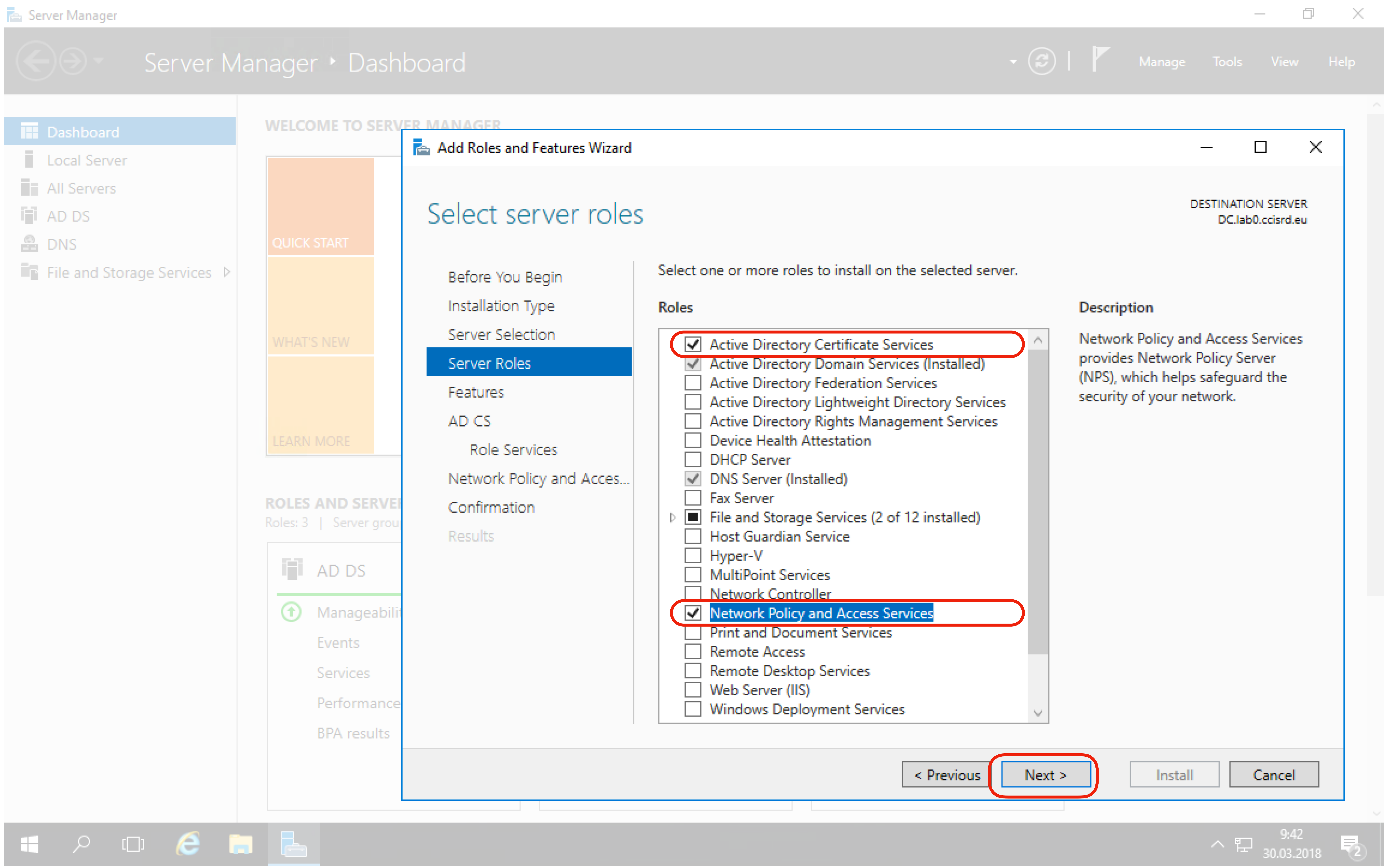
Name	IP Address	Operating System
DC.lab0.ccisrd.eu	10.1.0.2	Microsoft Windows Server 2016 Datacenter

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.

Select Server Roles

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



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
DC.lab0.ccisrd.eu

Select one or more roles to install on the selected server.

Roles

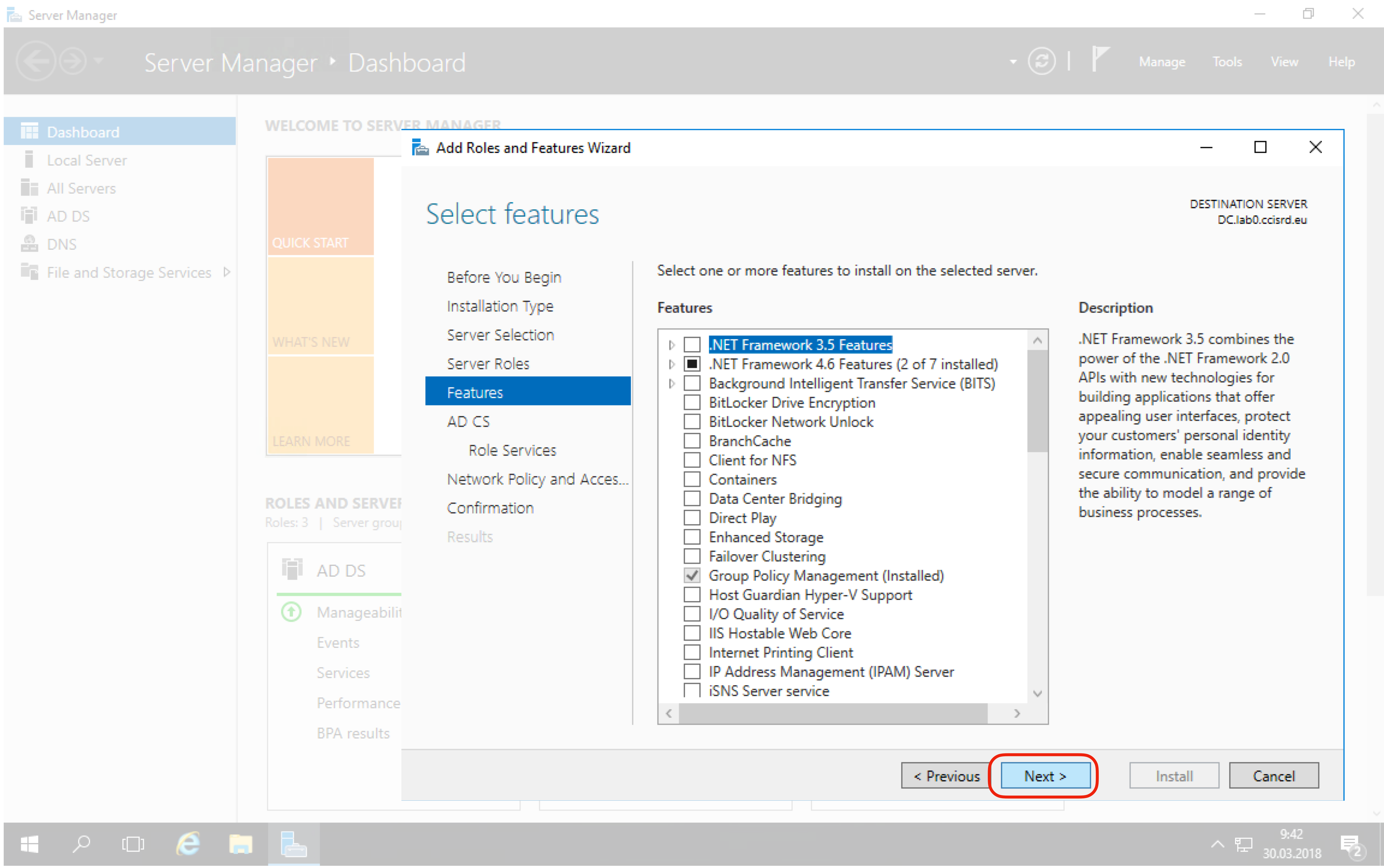
- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Controller
- ☑ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services

Description

Network Policy and Access Services provides Network Policy Server (NPS), which helps safeguard the security of your network.

Select features

- Accept default and click “next”



Add Roles and Features Wizard

Select features

DESTINATION SERVER
DC.lab0.ccisrd.eu

Select one or more features to install on the selected server.

Features

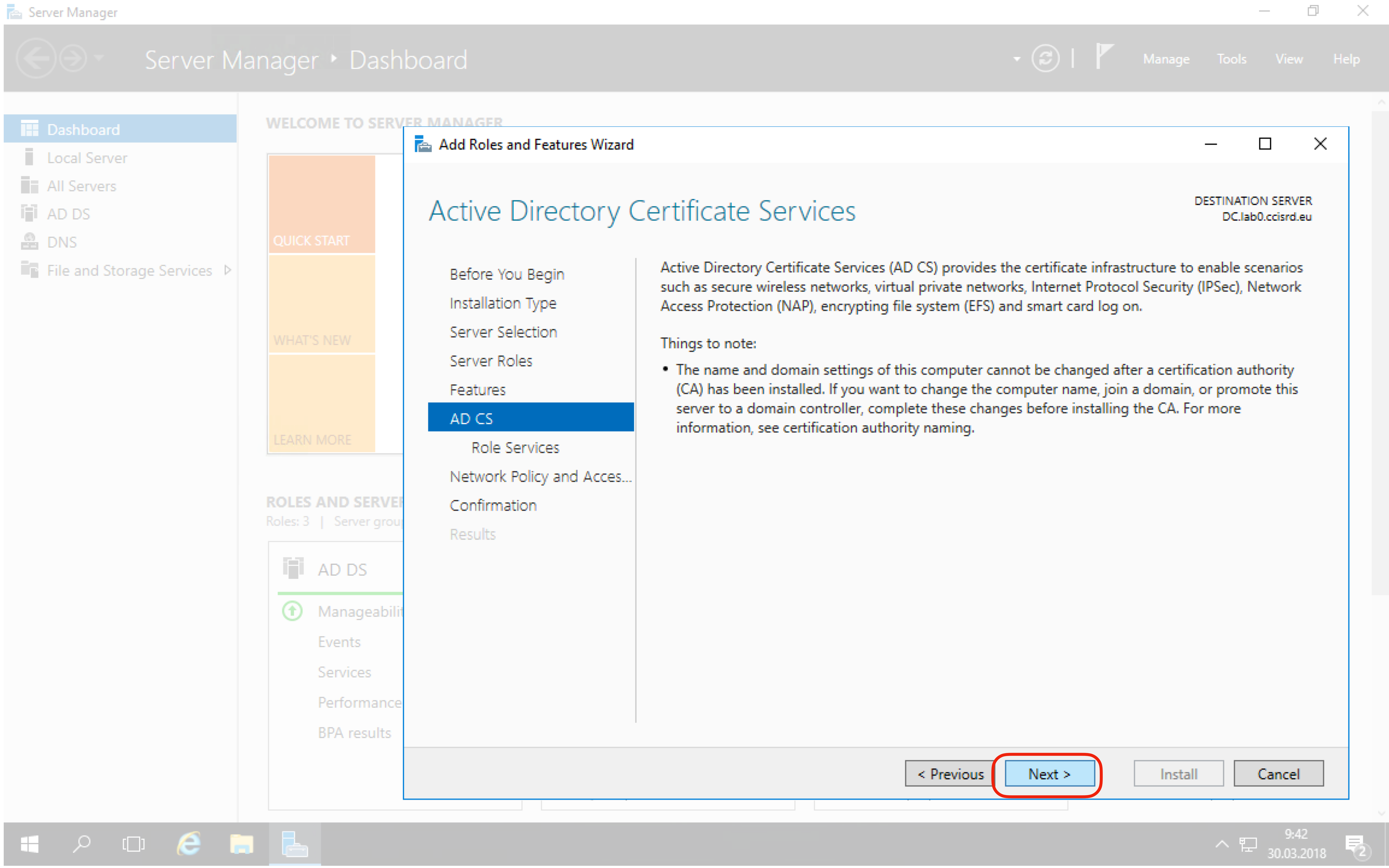
- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.6 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ Host Guardian Hyper-V Support
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

AD Certificate Services

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



Add Roles and Features Wizard

Active Directory Certificate Services

DESTINATION SERVER
DC.lab0.ccisrd.eu

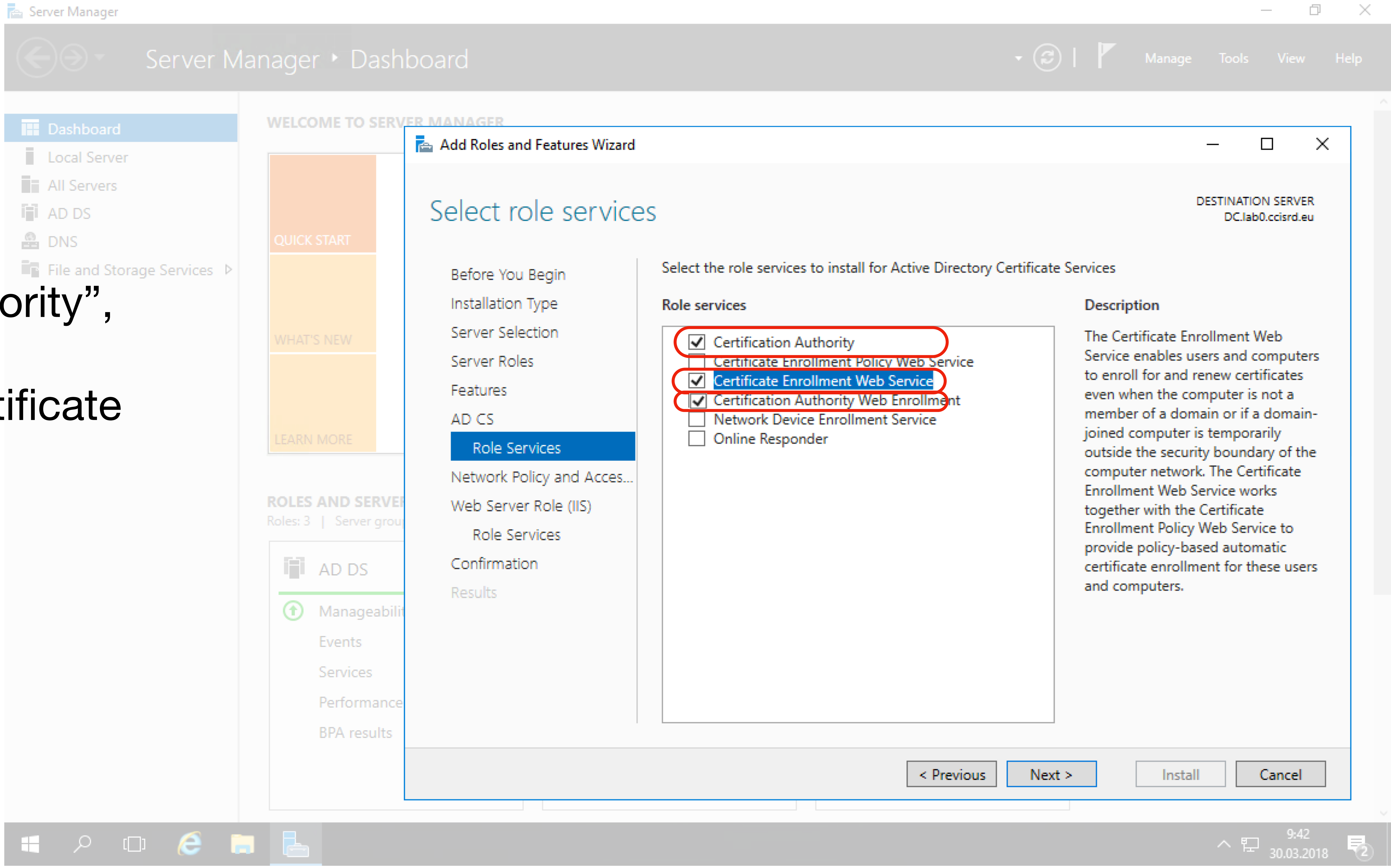
Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Install CA role

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



Select role services

DESTINATION SERVER
DC.lab0.ccisrd.eu

Select the role services to install for Active Directory Certificate Services

Role services

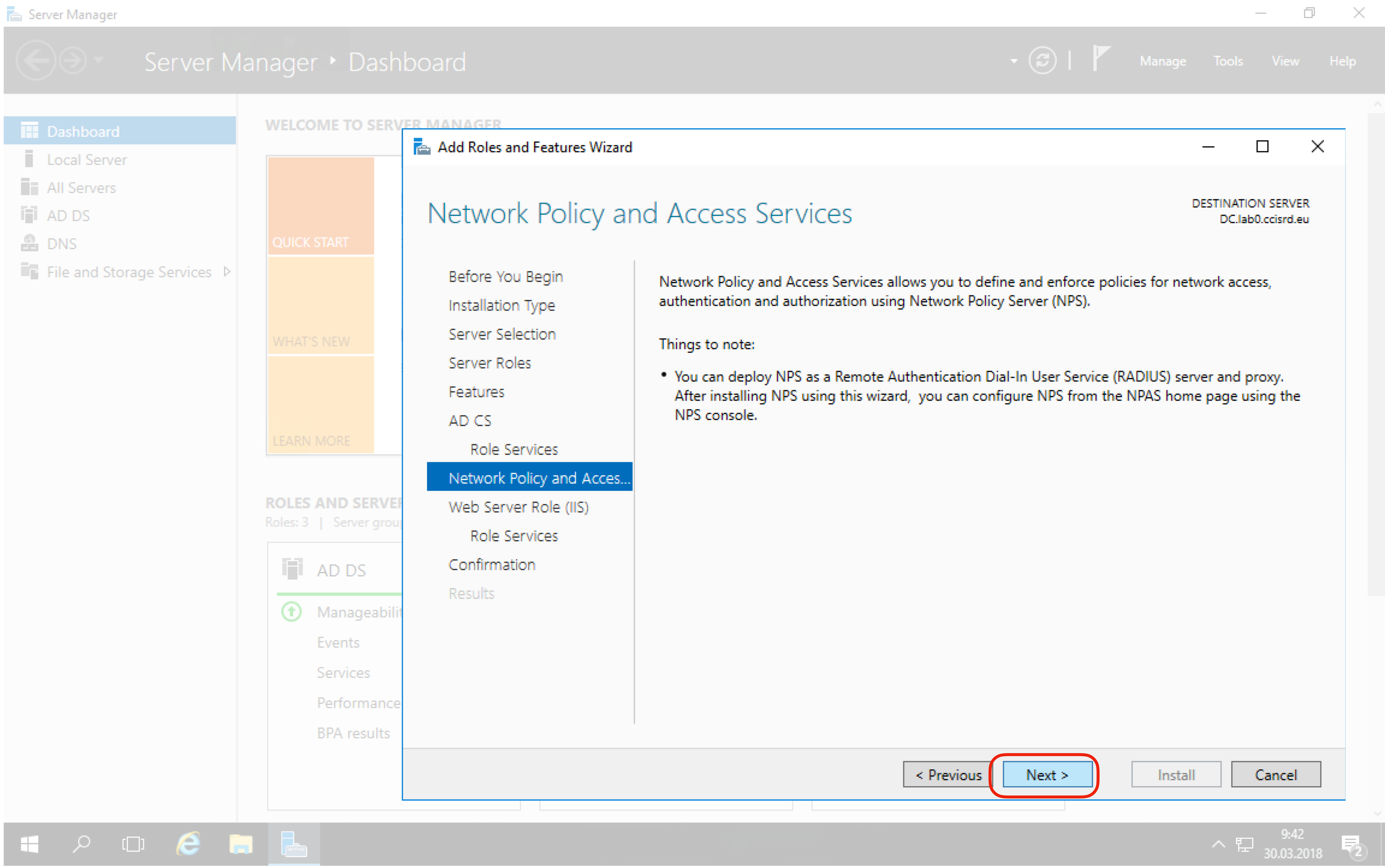
- ☑ Certification Authority
- □ Certificate Enrollment Policy Web Service
- ☑ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- □ Network Device Enrollment Service
- □ Online Responder

Description

The Certificate Enrollment Web Service enables users and computers to enroll for and renew certificates even when the computer is not a member of a domain or if a domain-joined computer is temporarily outside the security boundary of the computer network. The Certificate Enrollment Web Service works together with the Certificate Enrollment Policy Web Service to provide policy-based automatic certificate enrollment for these users and computers.

Install NPS role

- Click “Next”



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).

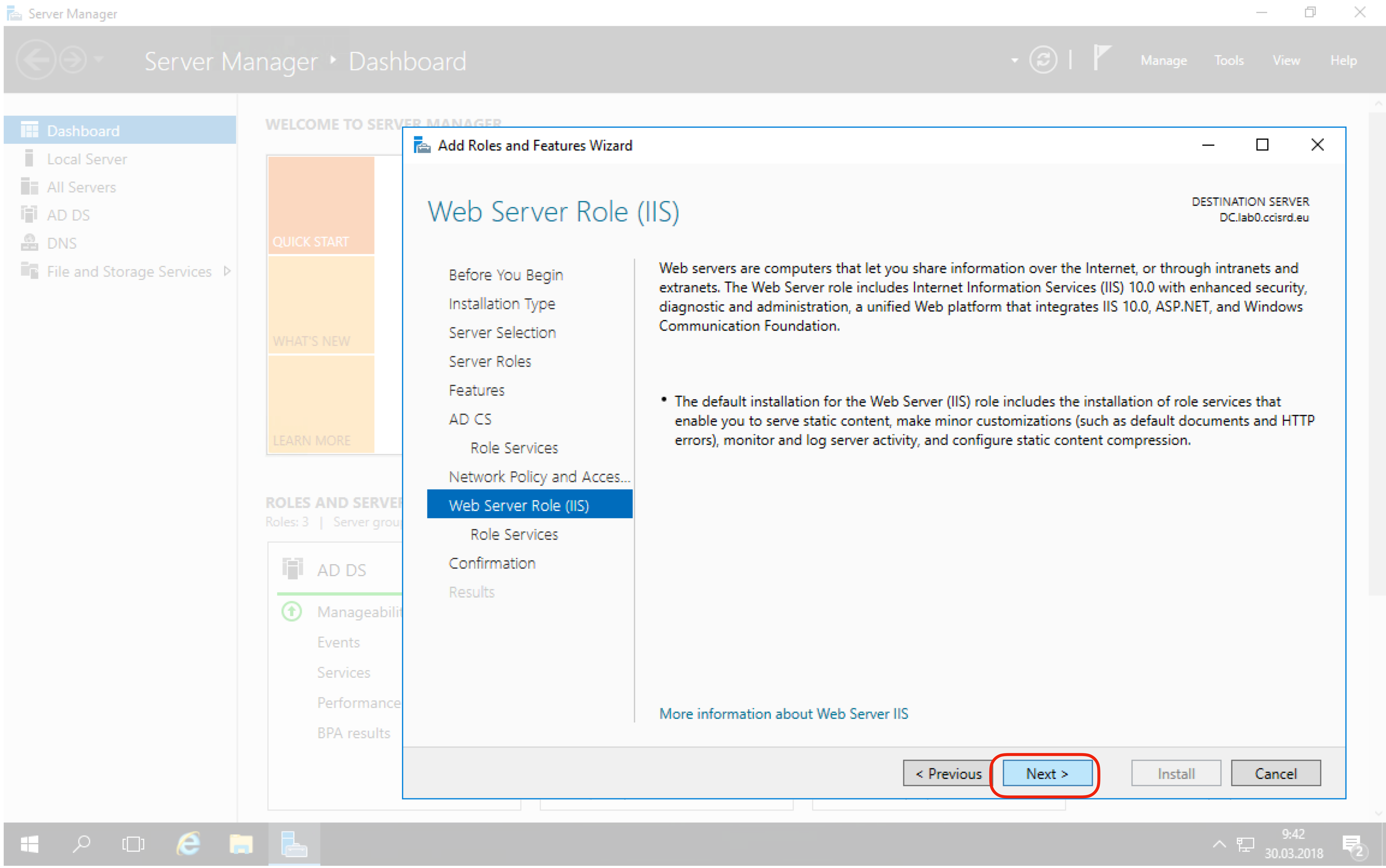
Things to note:

- 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.

CCISRD
Center for Communication and Informationsecurity Research and Development

Install NPS and CA role

- Click “Next”



Add Roles and Features Wizard

Web Server Role (IIS)

DESTINATION SERVER
DC.lab0.ccisrd.eu

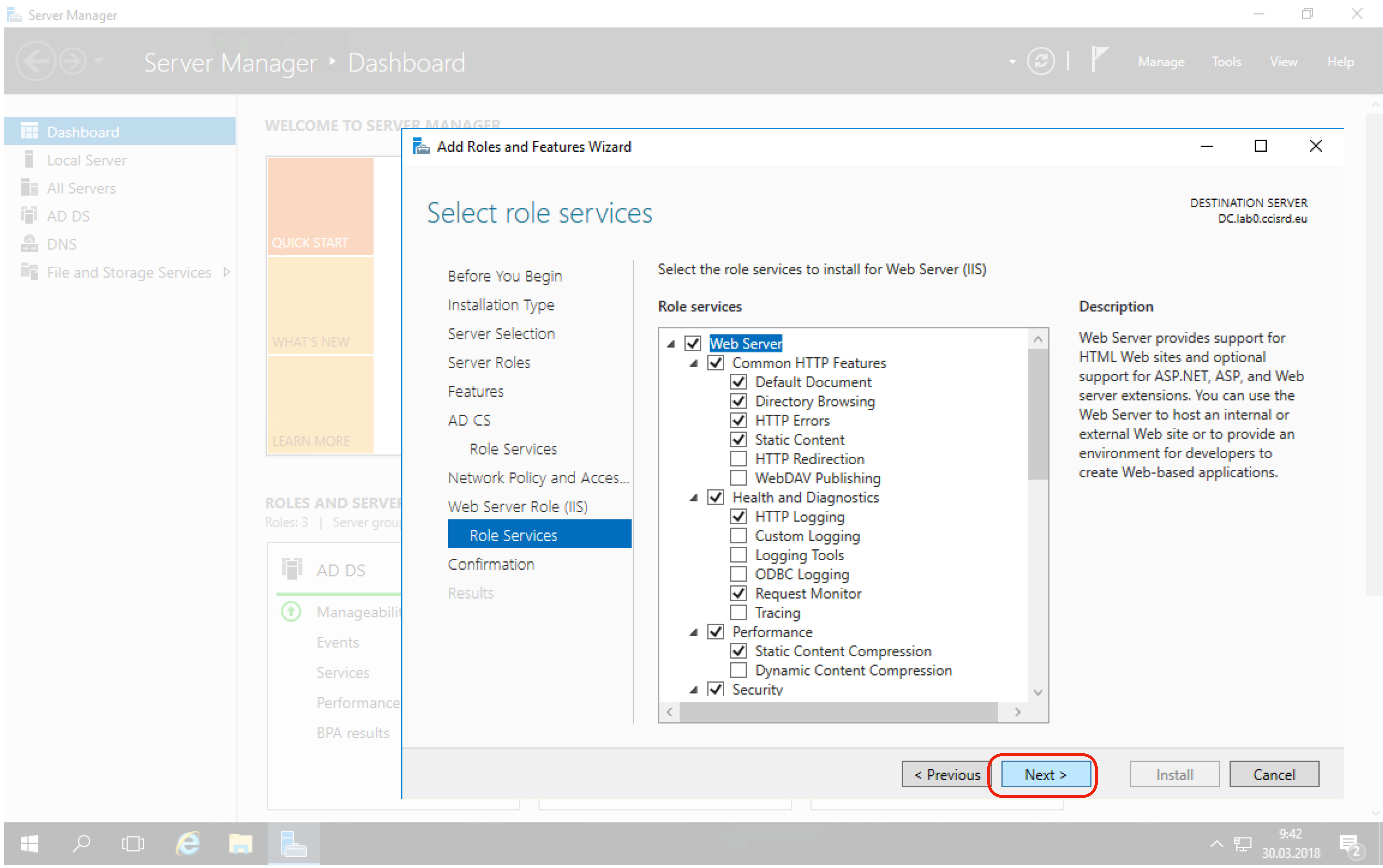
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

Install NPS and CA role

- Accept default and click “Next”



Server Manager

Server Manager ▸ Dashboard

Manage Tools View Help

Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services

WELCOME TO SERVER MANAGER

QUICK START
WHAT'S NEW
LEARN MORE

ROLES AND SERVER
Roles: 3 | Server grou

AD DS
Manageabili
Events
Services
Performance
BPA results

Add Roles and Features Wizard

Select role services

DESTINATION SERVER
DC.lab0.ccisrd.eu

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Network Policy and Acces...
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - □ Logging Tools
    - □ ODBC Logging
    - ☑ Request Monitor
    - □ Tracing
  - ☑ Performance
    - ☑ Static Content Compression
    - □ Dynamic Content Compression
  - ☑ Security

Description

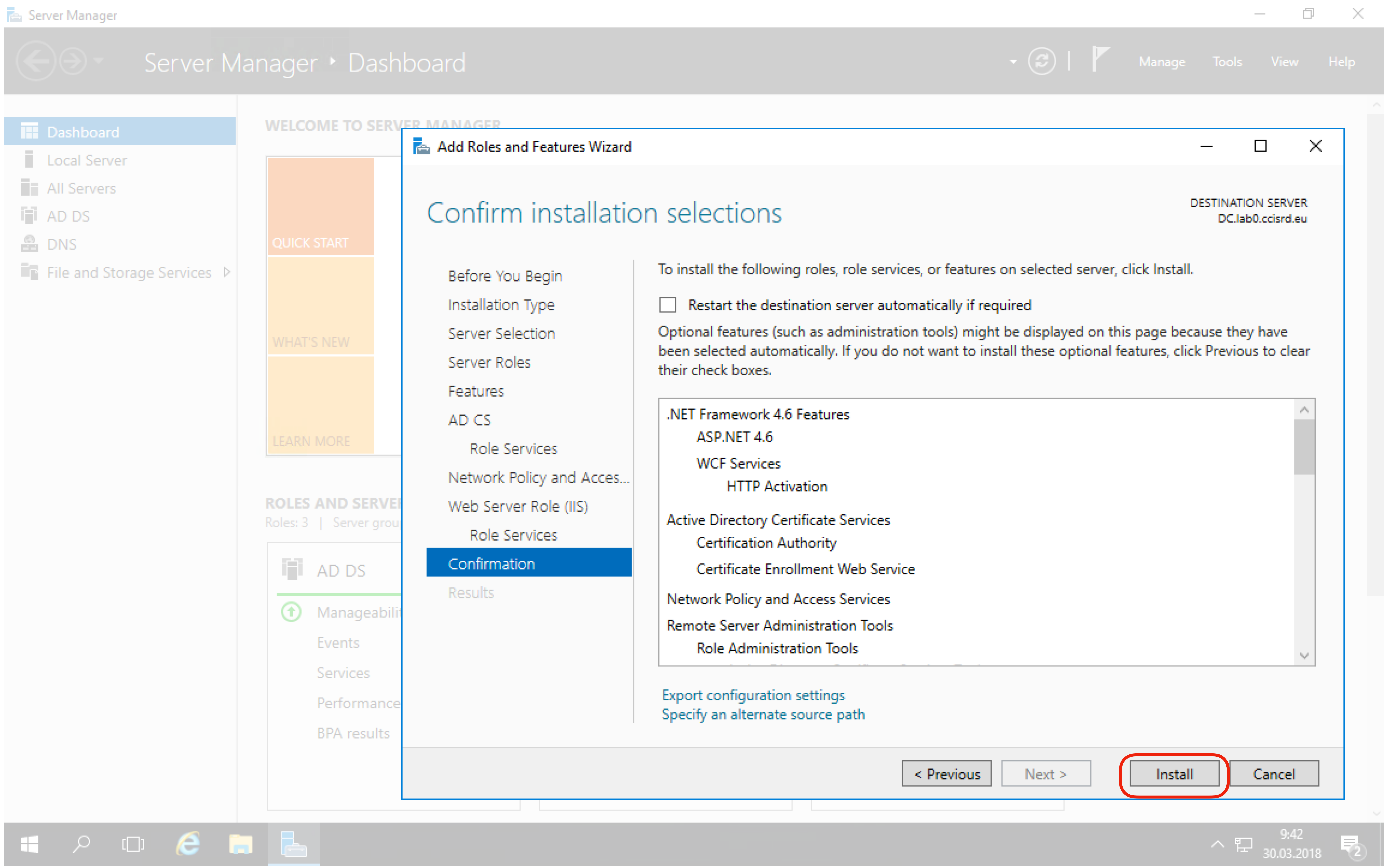
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

< Previous | Next > | Install | Cancel

9:42
30.03.2018

Install NPS and CA role

- Accept default and click “Install”



Confirm installation selections

DESTINATION SERVER
DC.lab0.ccisrd.eu

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

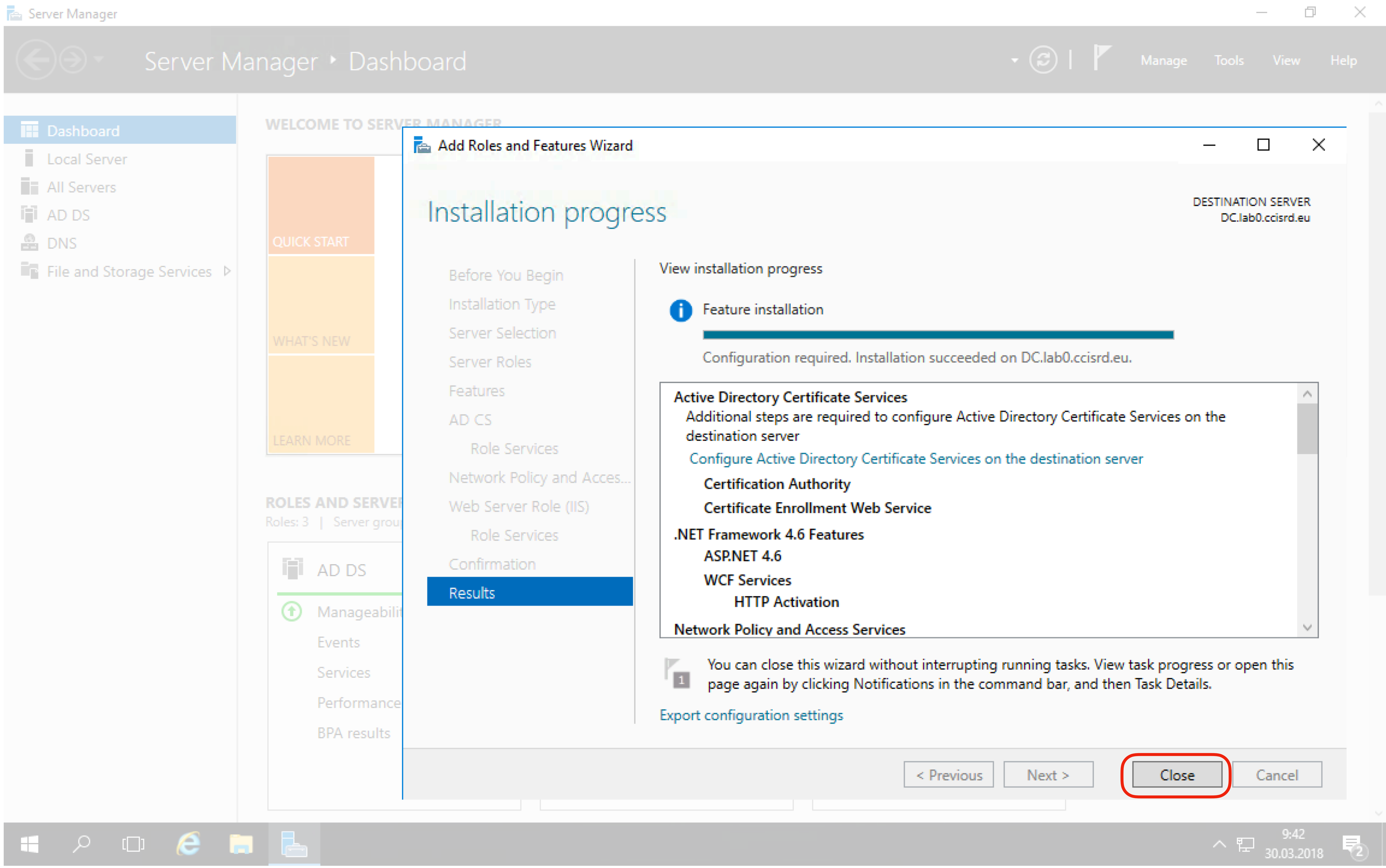
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

.NET Framework 4.6 Features
    ASP.NET 4.6
    WCF Services
        HTTP Activation
Active Directory Certificate Services
    Certification Authority
    Certificate Enrollment Web Service
Network Policy and Access Services
Remote Server Administration Tools
    Role Administration Tools

Export configuration settings
Specify an alternate source path

Install NPS and CA role

- After installation is completed, click “Close”



Installation progress

DESTINATION SERVER
DC.lab0.ccisrd.eu

View installation progress

Feature installation

Configuration required. Installation succeeded on DC.lab0.ccisrd.eu.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Certificate Enrollment Web Service
.NET Framework 4.6 Features
ASP.NET 4.6
WCF Services
HTTP Activation
Network Policy and Access Services

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

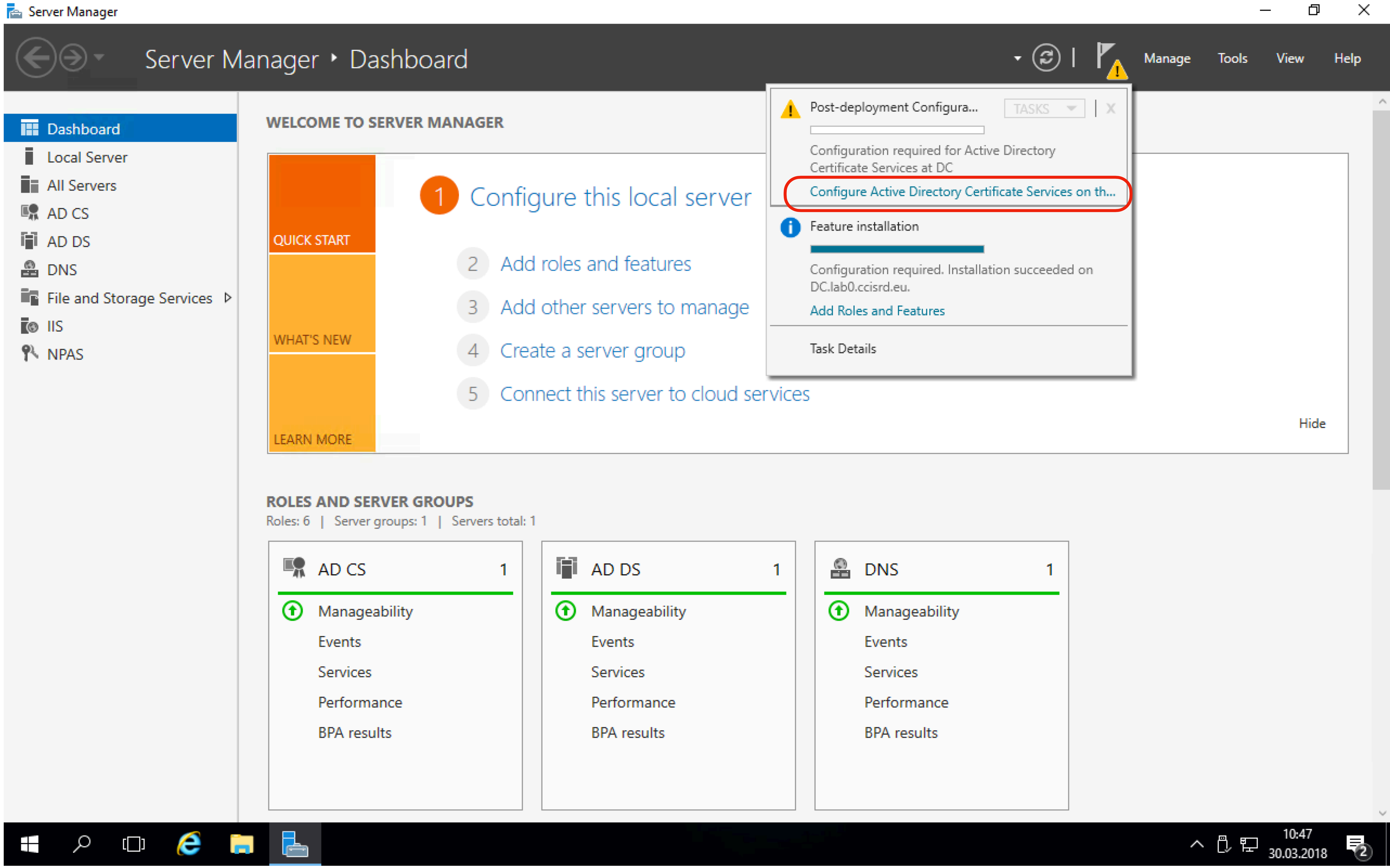
Export configuration settings

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 ..”



Post-deployment Configura...

TASKS

Configuration required for Active Directory Certificate Services at DC

Configure Active Directory Certificate Services on th...

Feature installation

Configuration required. Installation succeeded on DC.lab0.ccisrd.eu.

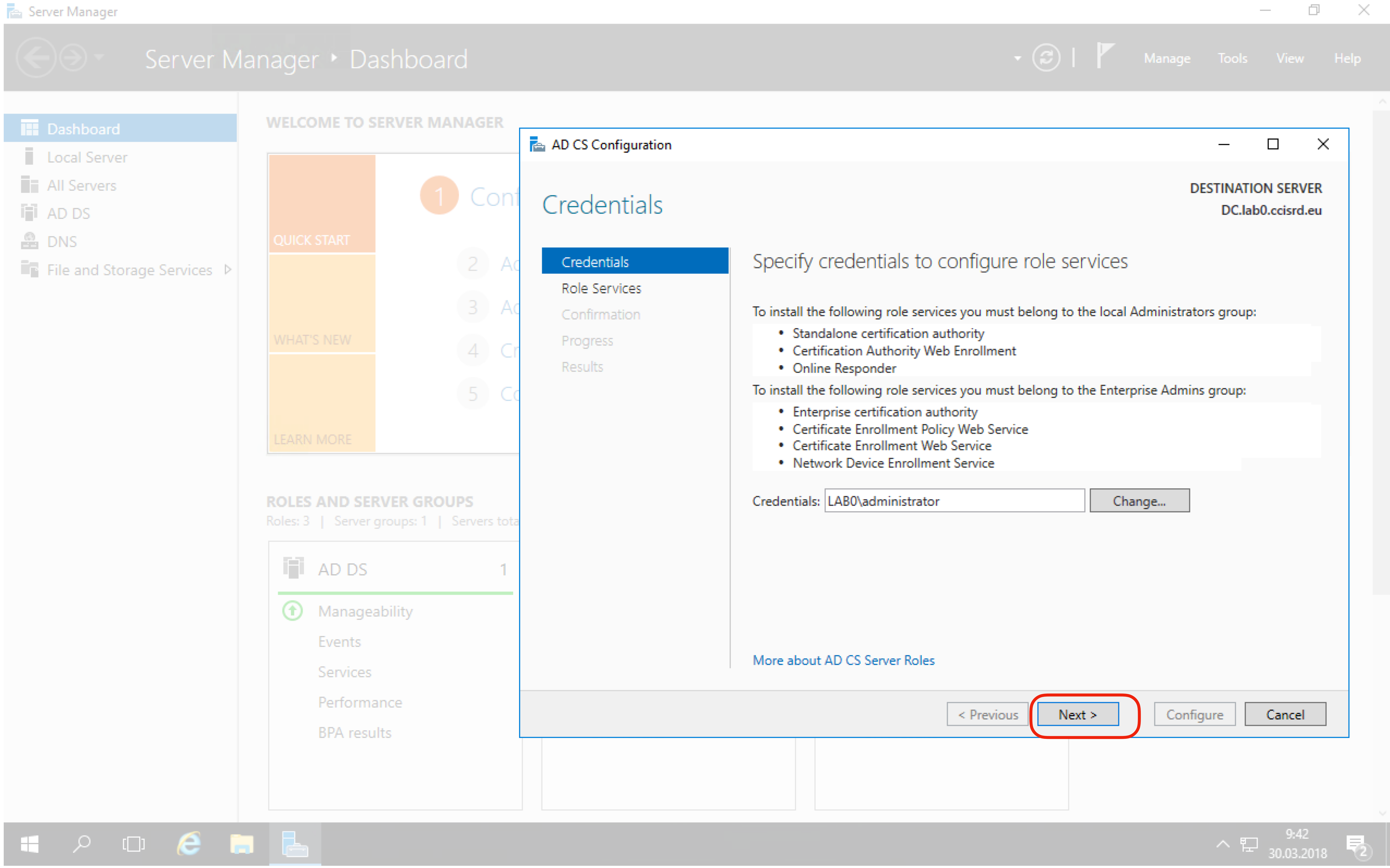
Add Roles and Features

Task Details

CCISRD
Center for Communication and Informationsecurity Research and Development

Configure CA

- Accept default and click “Next”



AD CS Configuration

DESTINATION SERVER
DC.lab0.ccisrd.eu

Credentials

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

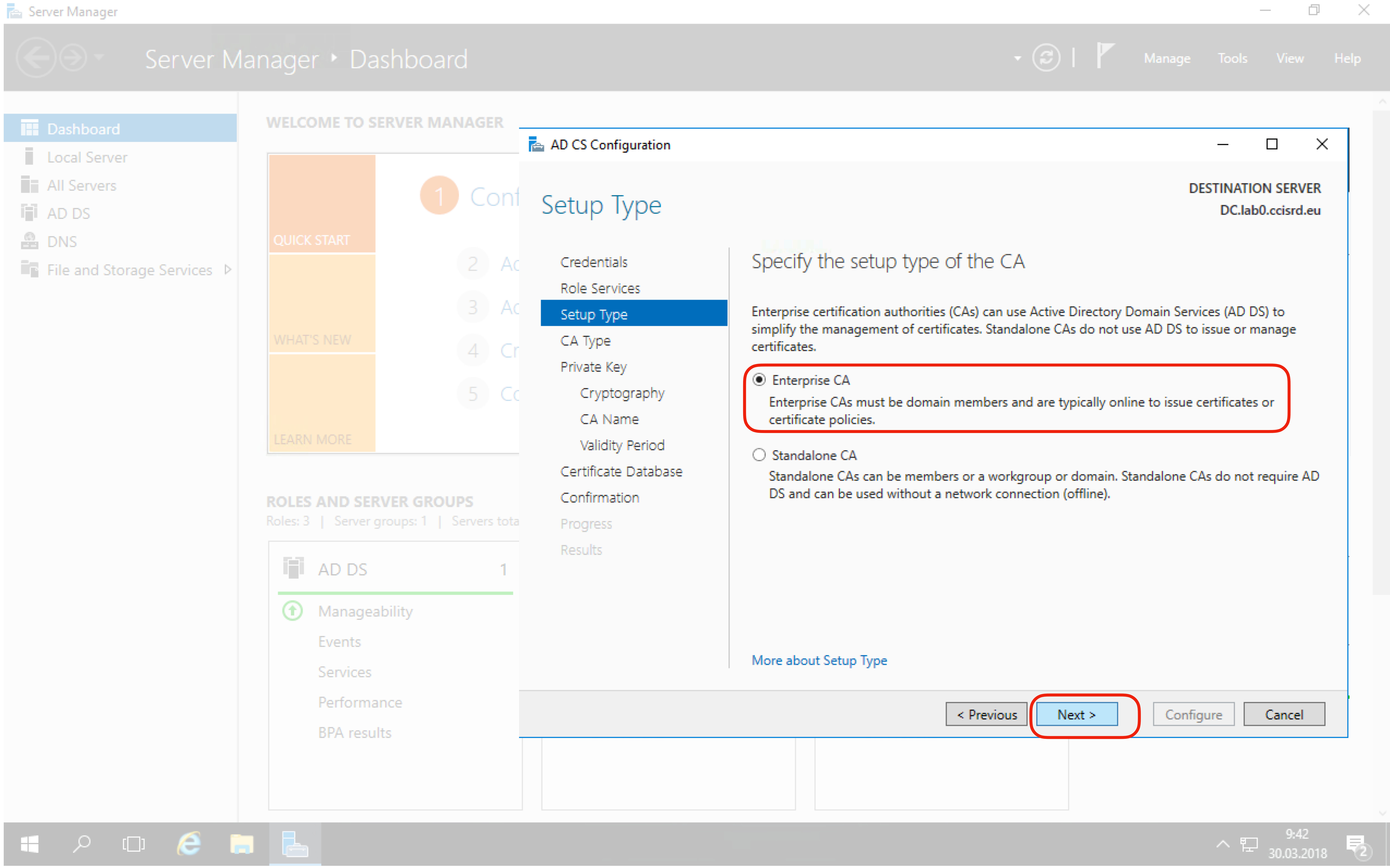
- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: LAB0\administrator

More about AD CS Server Roles

Configure CA

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



AD CS Configuration

DESTINATION SERVER
DC.lab0.ccisrd.eu

Setup Type

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA

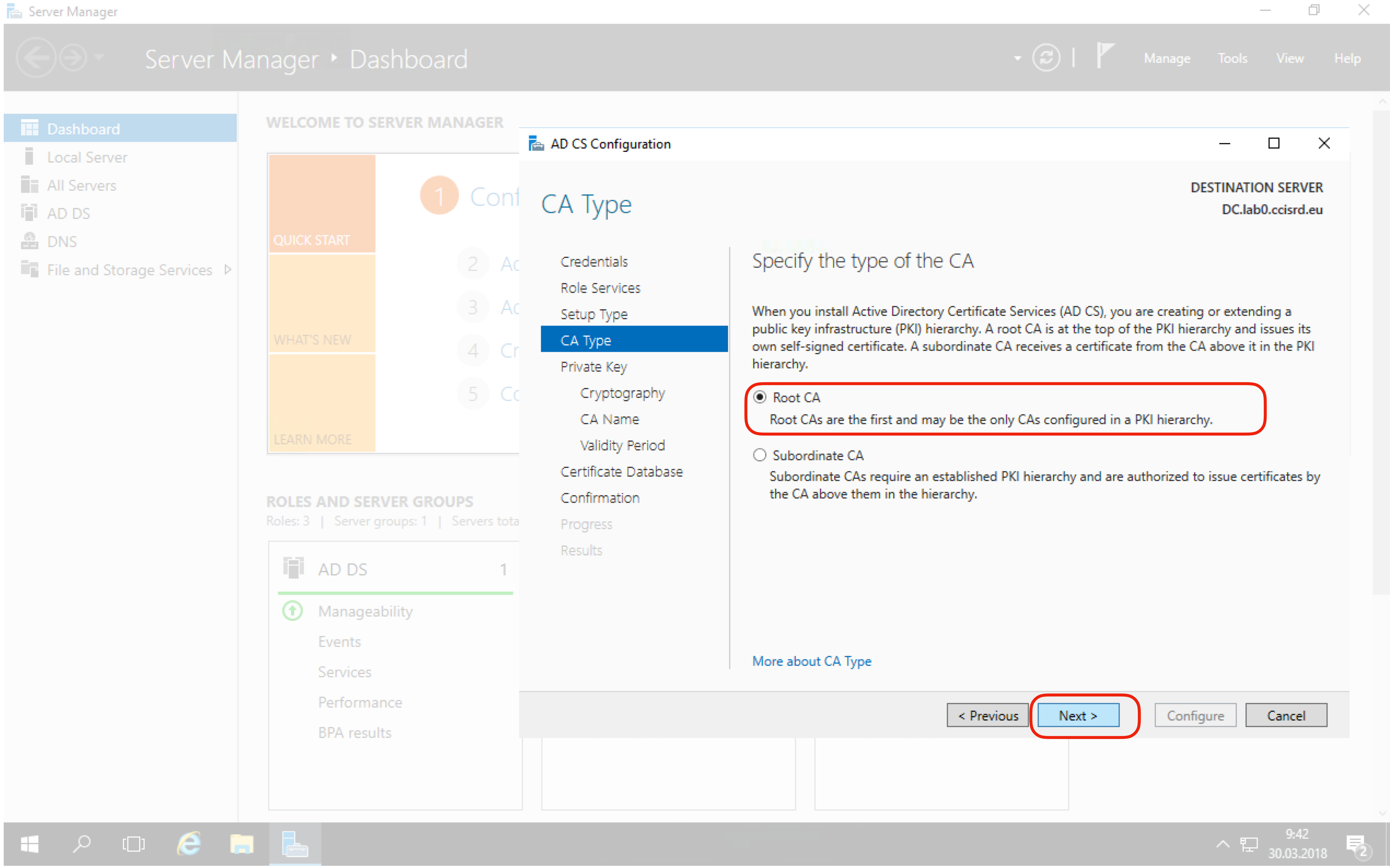
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

CCISRD
Center for Communication and Informationsecurity Research and Development

Configure CA

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



CA Type

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify the type of the CA

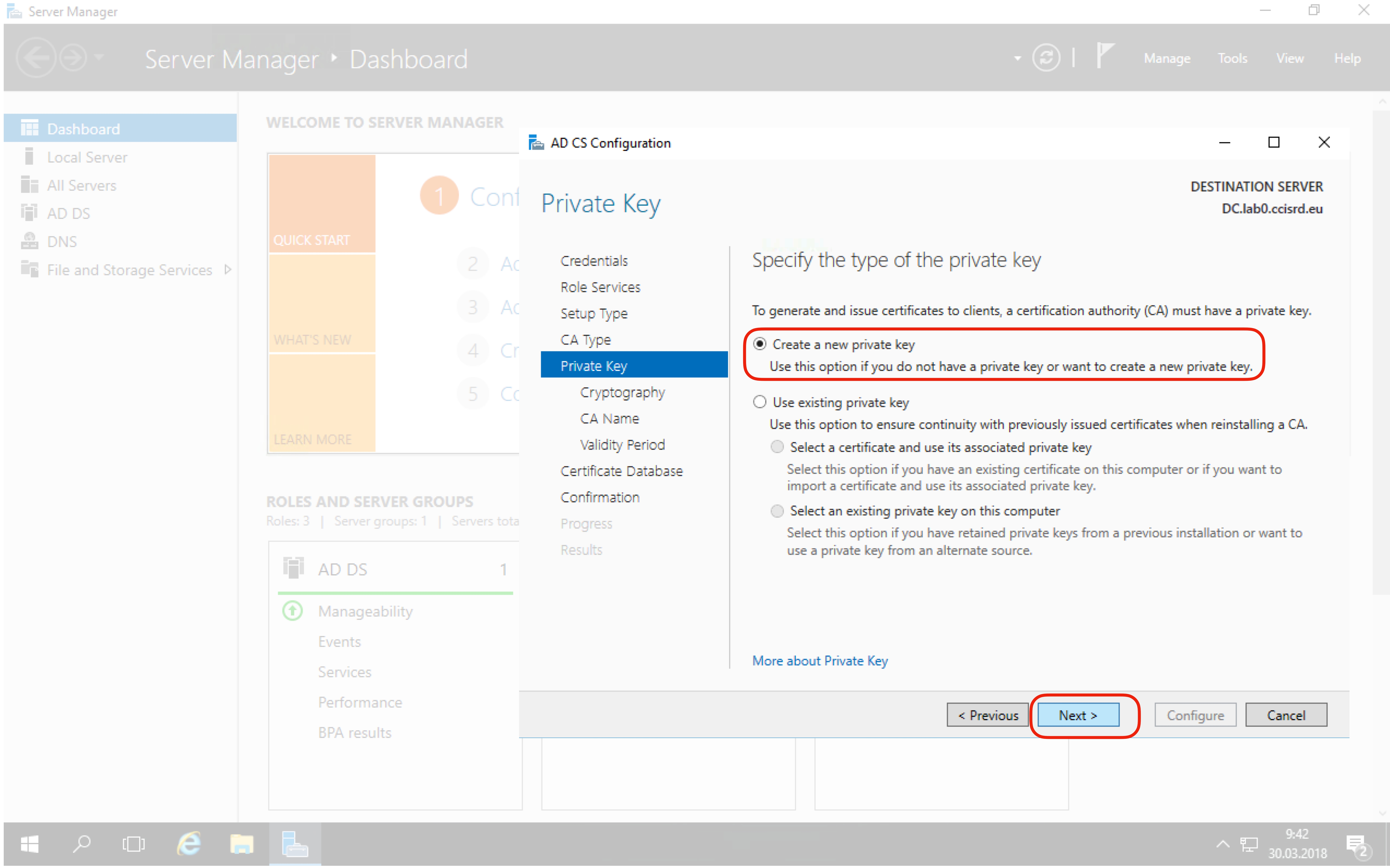
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

Configure CA

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



AD CS Configuration

Private Key

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

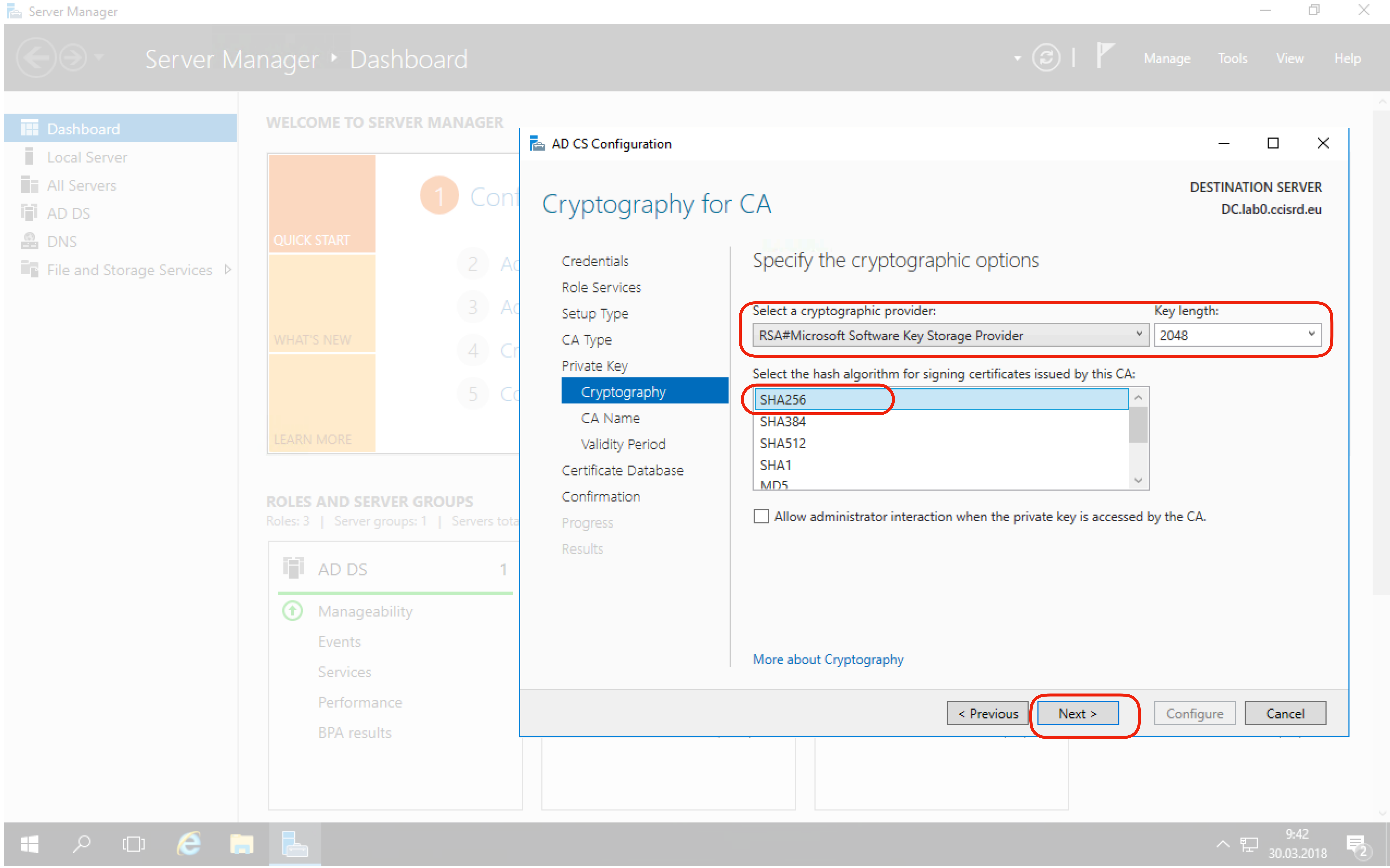
○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about Private Key

Configure CA

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



Cryptography for CA

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

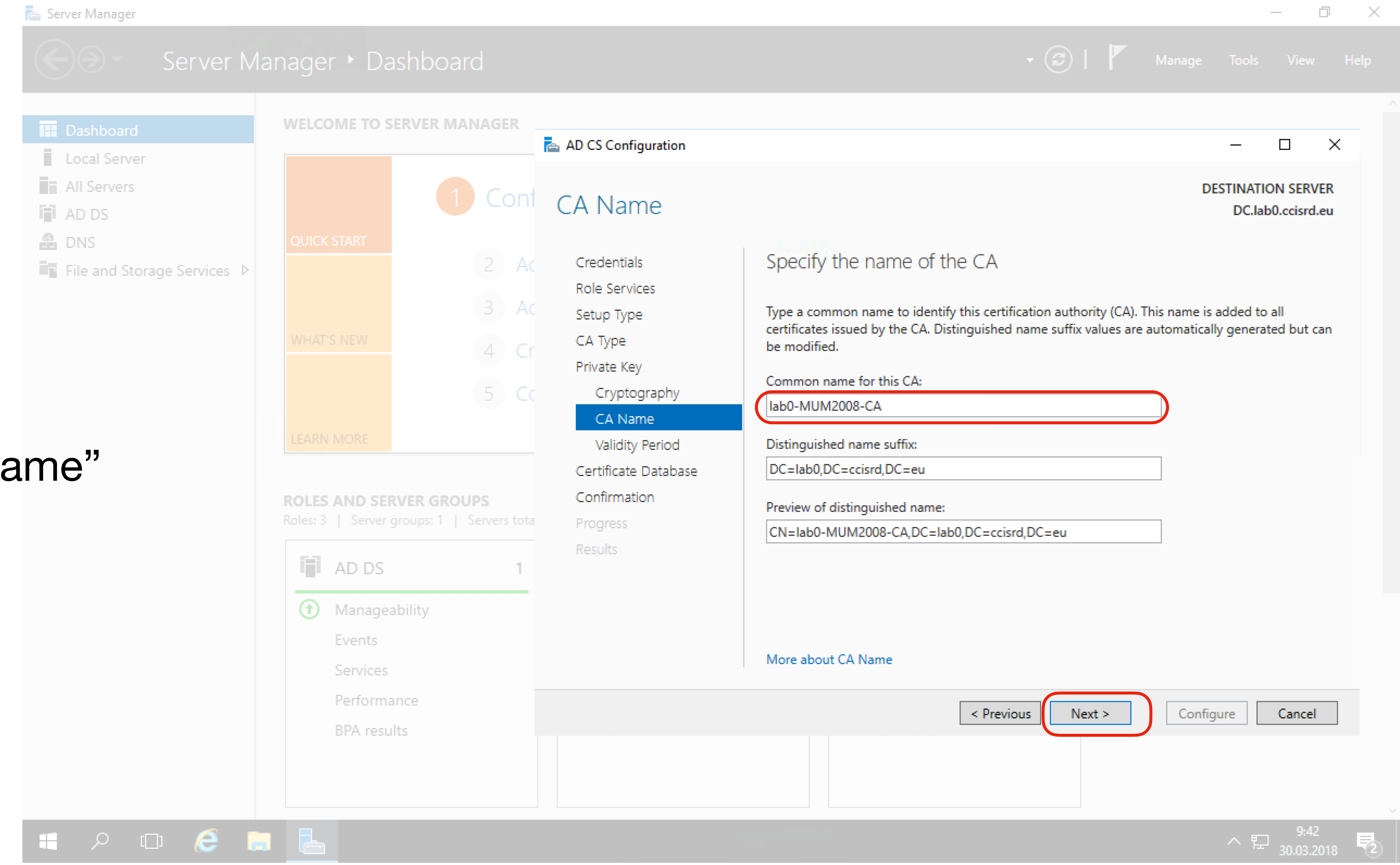
Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

Configure CA

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



CA Name

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

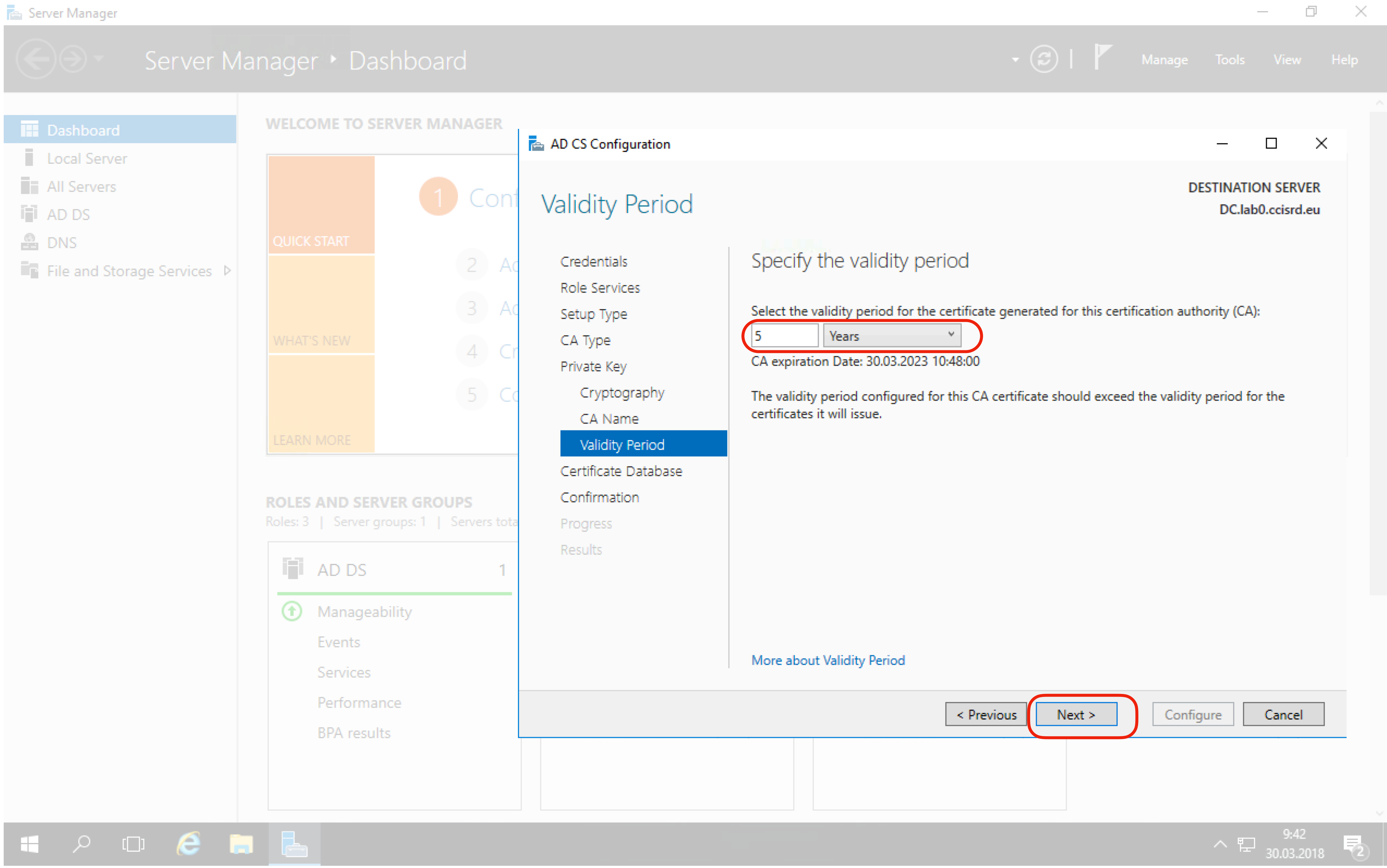
Common name for this CA:
lab0-MUM2008-CA

Distinguished name suffix:
DC=lab0,DC=ccisrd,DC=eu

Preview of distinguished name:
CN=lab0-MUM2008-CA,DC=lab0,DC=ccisrd,DC=eu

Configure CA

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



AD CS Configuration

Validity Period

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years

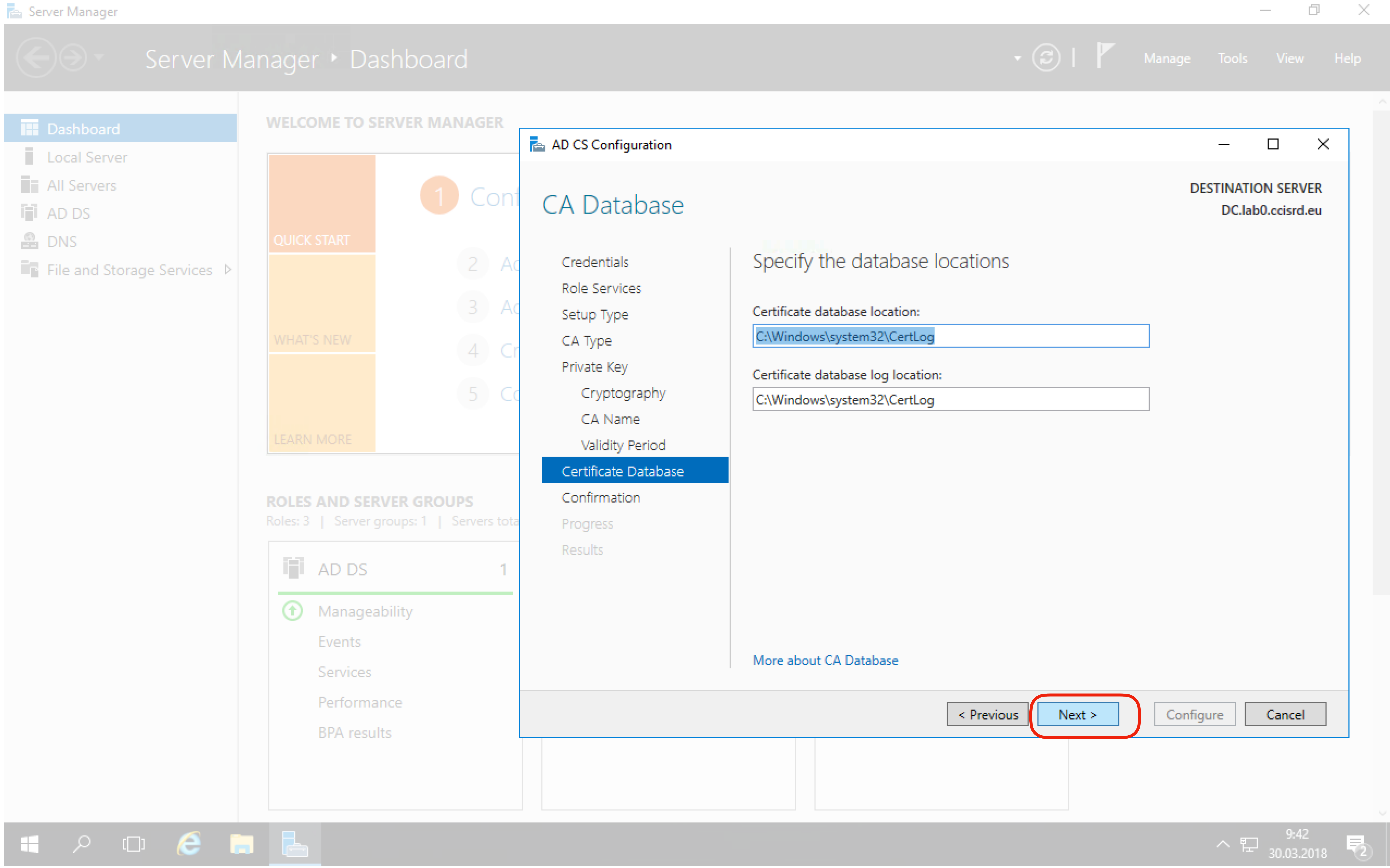
CA expiration Date: 30.03.2023 10:48:00

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

More about Validity Period

Configure CA

- Accept default and click “Next”



CA Database

DESTINATION SERVER
DC.lab0.ccisrd.eu

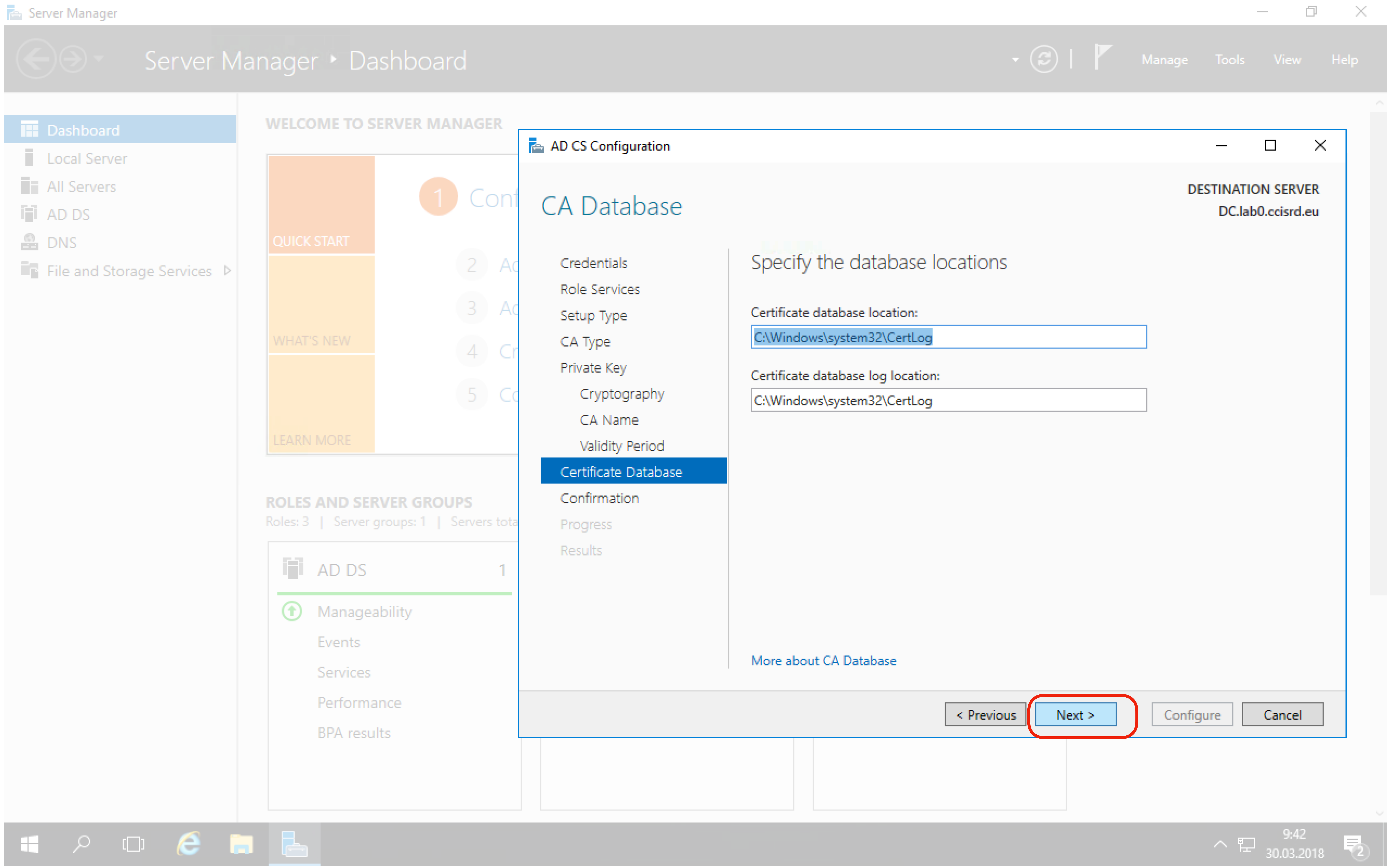
Specify the database locations

Certificate database location: C:\Windows\system32\CertLog

Certificate database log location: C:\Windows\system32\CertLog

Configure CA

- Accept default and click “Next”



AD CS Configuration

CA Database

DESTINATION SERVER
DC.lab0.ccisrd.eu

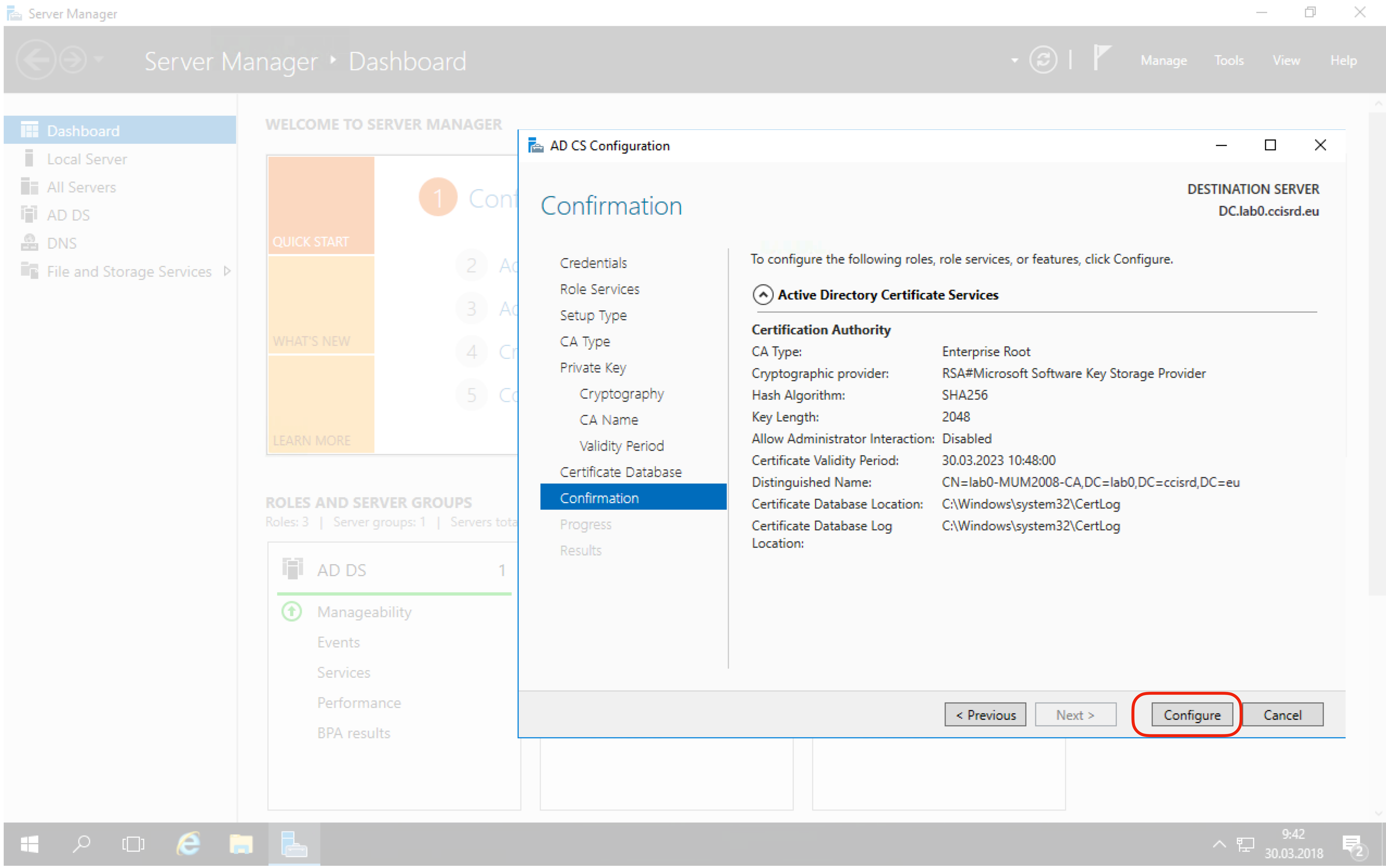
Specify the database locations

Certificate database location: C:\Windows\system32\CertLog

Certificate database log location: C:\Windows\system32\CertLog

Configure CA

- Accept default and click “Configure”



Confirmation

DESTINATION SERVER
DC.lab0.ccisrd.eu

To configure the following roles, role services, or features, click Configure.

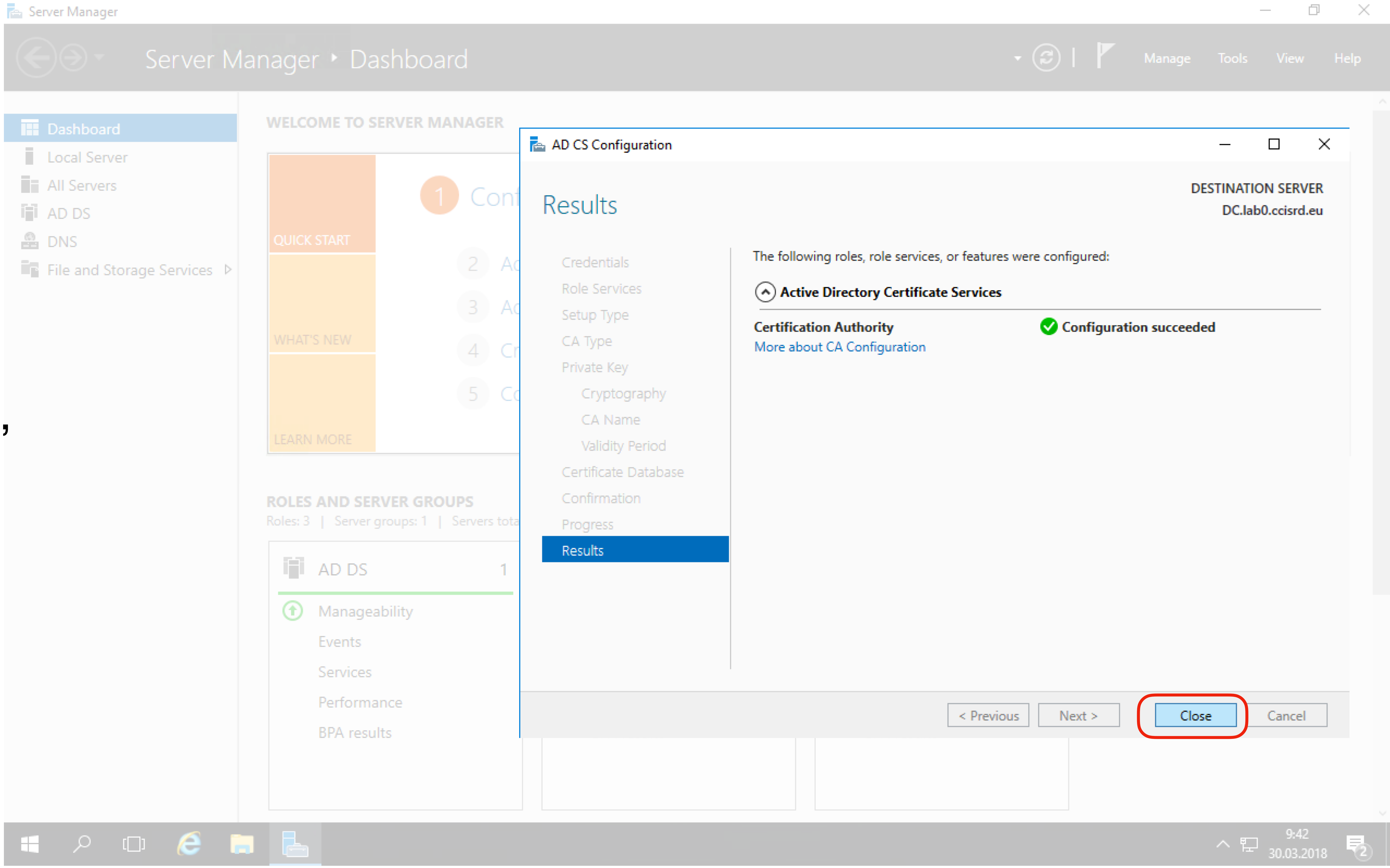
Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	30.03.2023 10:48:00
Distinguished Name:	CN=lab0-MUM2008-CA,DC=lab0,DC=ccisrd,DC=eu
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Configure CA

- After configuration complete, click “Close”



AD CS Configuration

Results

DESTINATION SERVER
DC.lab0.ccisrd.eu

The following roles, role services, or features were configured:

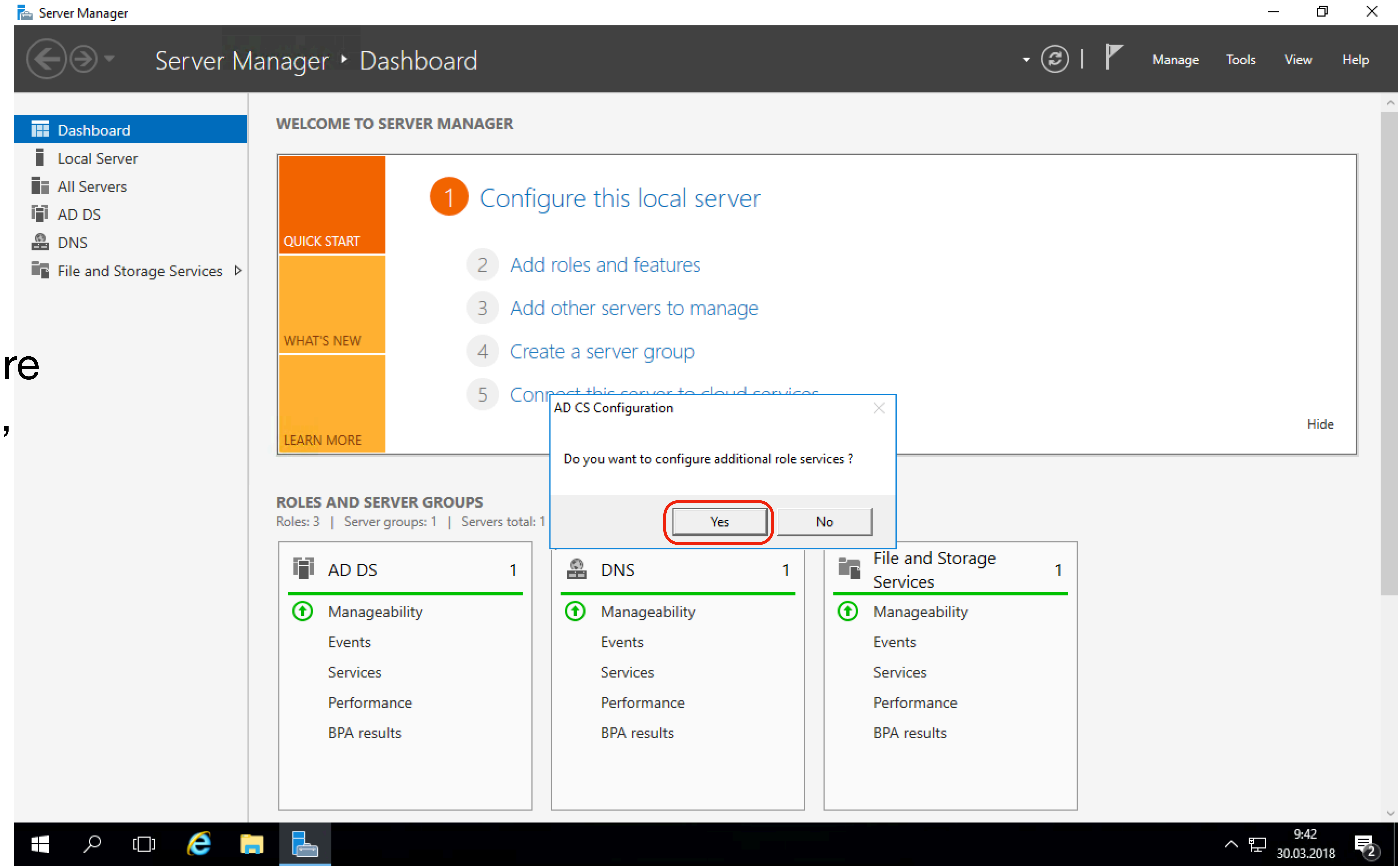
Active Directory Certificate Services

Certification Authority — ✓ Configuration succeeded

More about CA Configuration

Configure CA

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

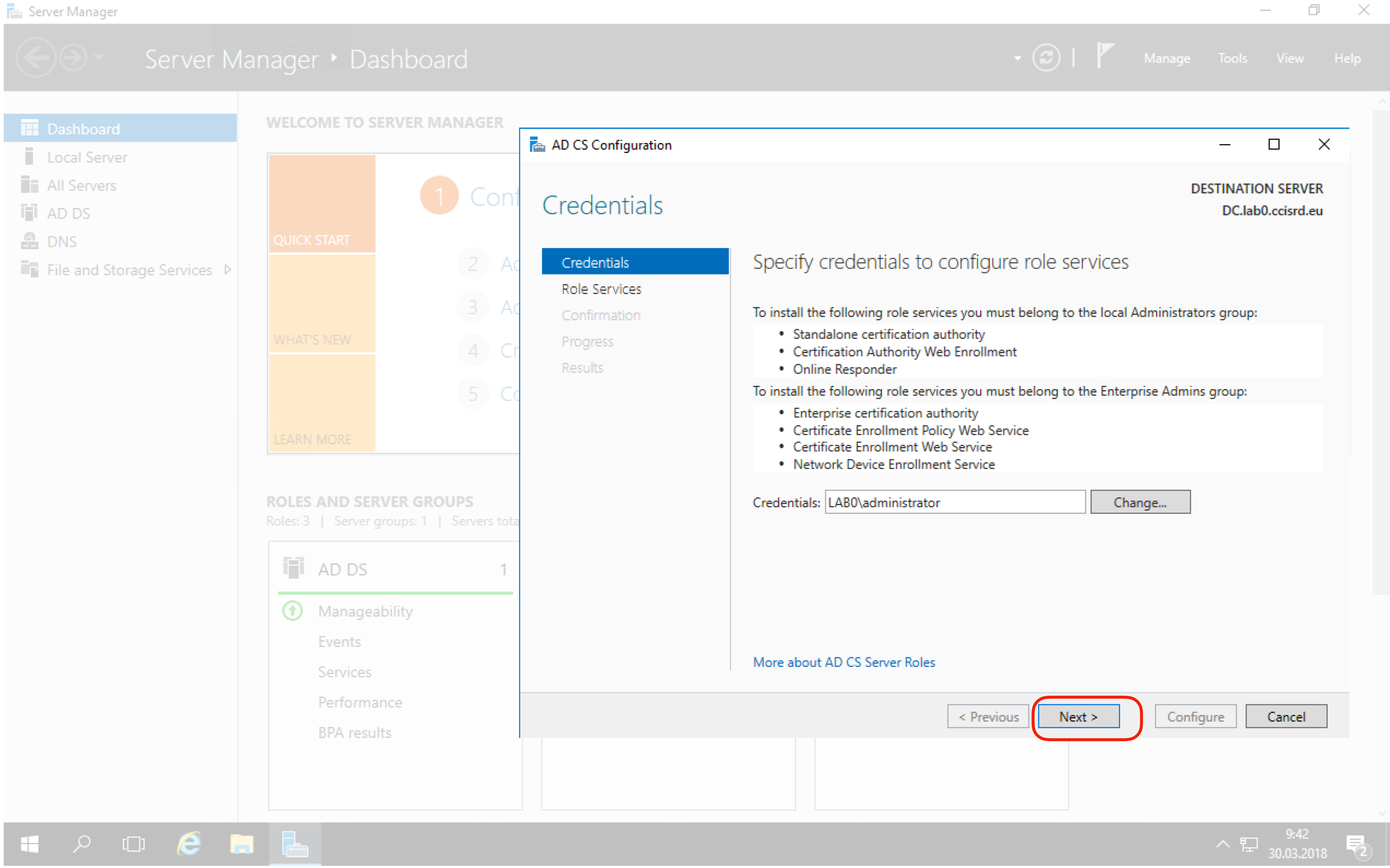


AD CS Configuration

Do you want to configure additional role services ?

Configure CA

- Accept default and click “Next”



Credentials

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

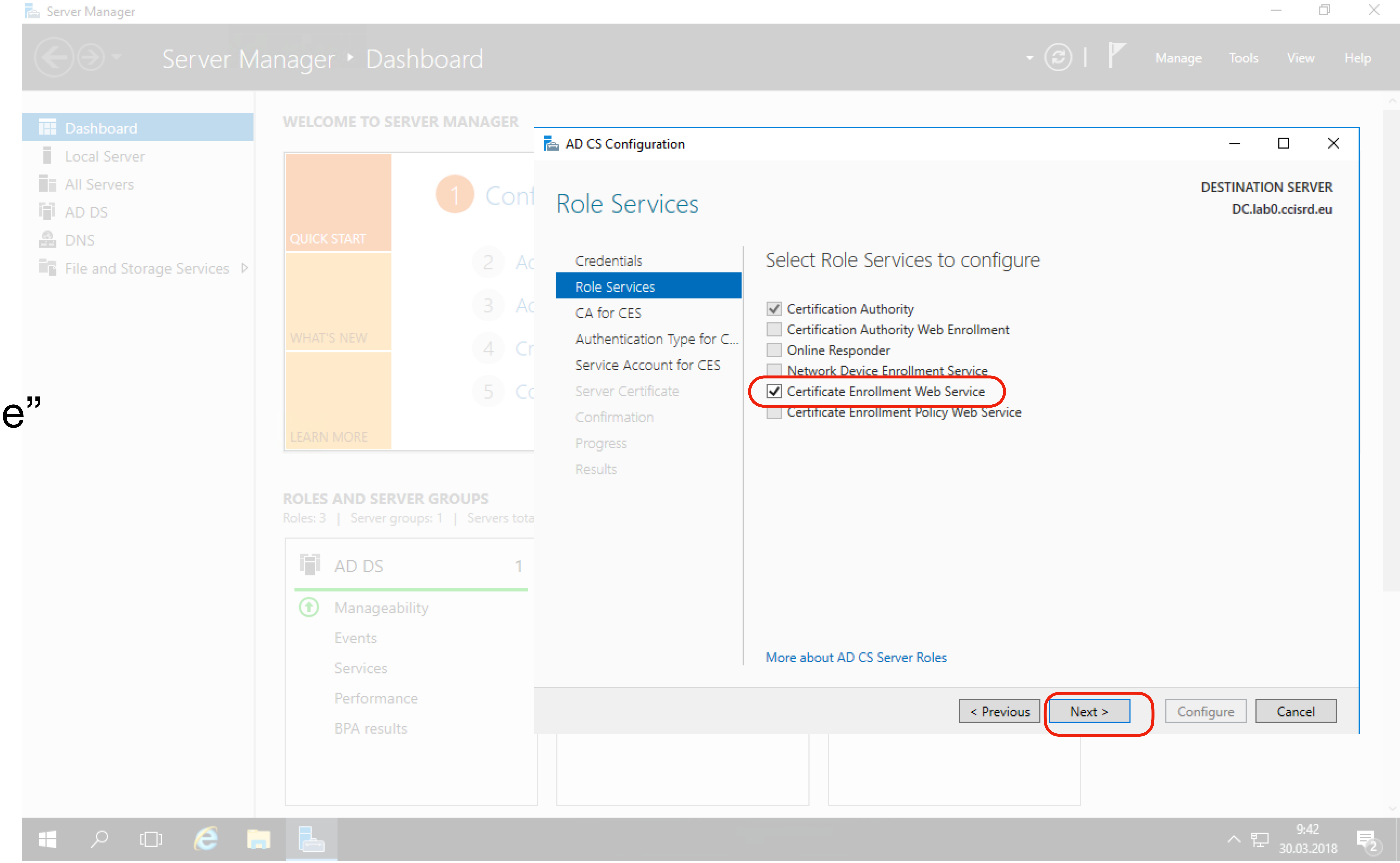
To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: LAB0\administrator [Change...]

Configure CA

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



AD CS Configuration

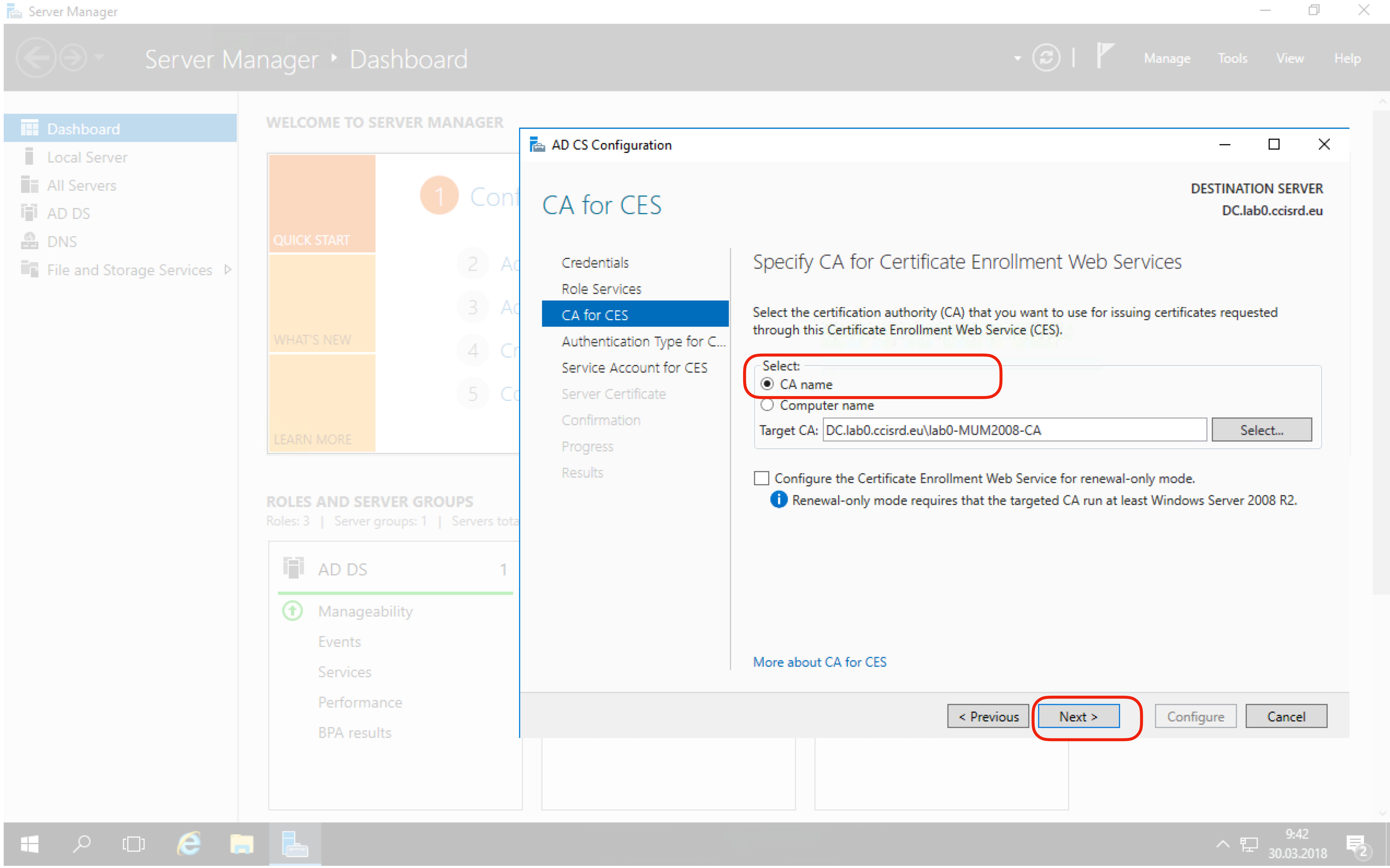
DESTINATION SERVER
DC.lab0.ccisrd.eu

Role Services

Select Role Services to configure

☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
☑ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

Configure CA



AD CS Configuration

DESTINATION SERVER
DC.lab0.ccisrd.eu

CA for CES

Specify CA for Certificate Enrollment Web Services

Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).

Select:
● CA name
○ Computer name

Target CA: DC.lab0.ccisrd.eu\lab0-MUM2008-CA

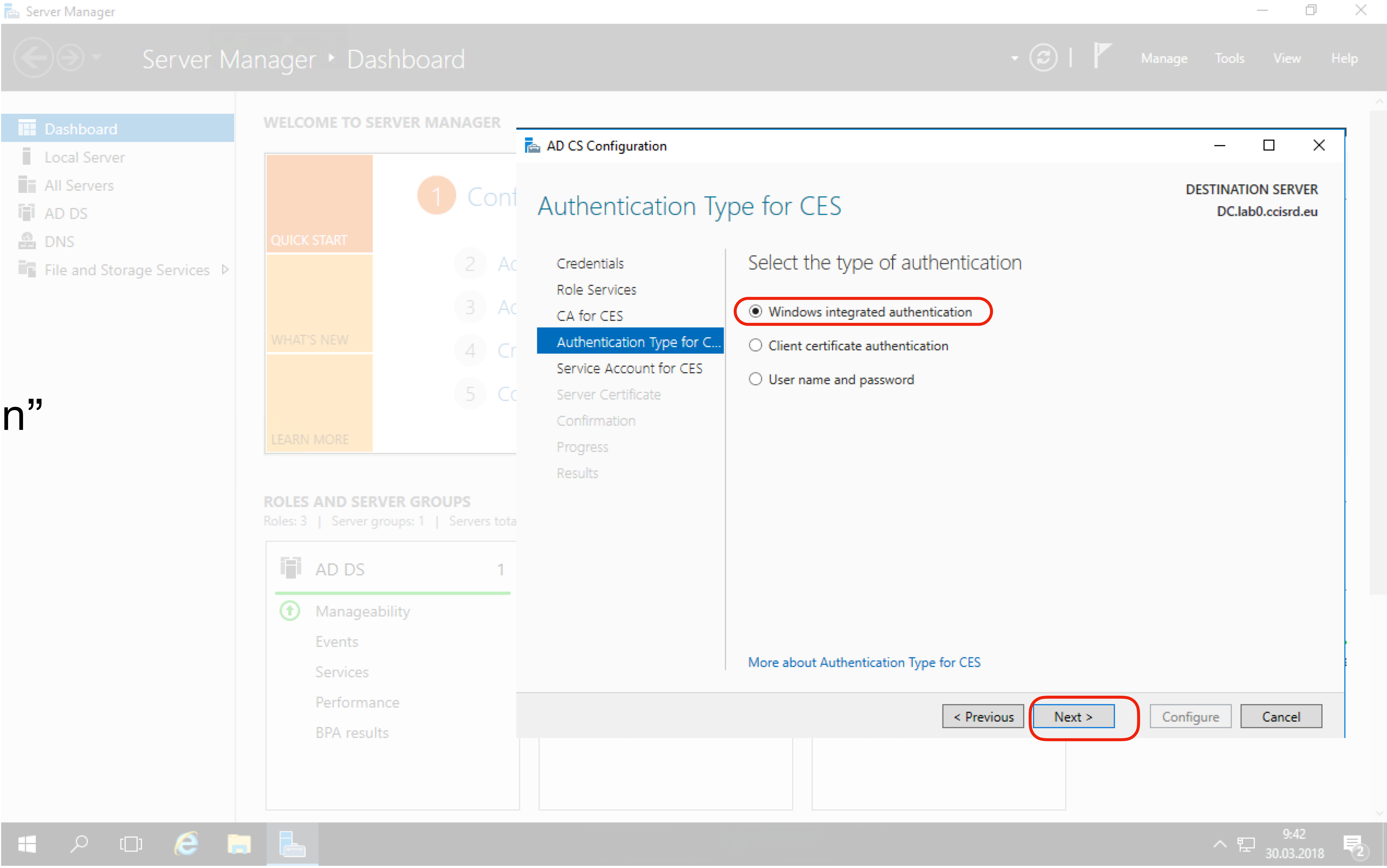
□ Configure the Certificate Enrollment Web Service for renewal-only mode.

Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.

- Select “CA Name” and Click “Next”

Configure CA

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



AD CS Configuration

DESTINATION SERVER
DC.lab0.ccisrd.eu

Authentication Type for CES

Select the type of authentication

● Windows integrated authentication

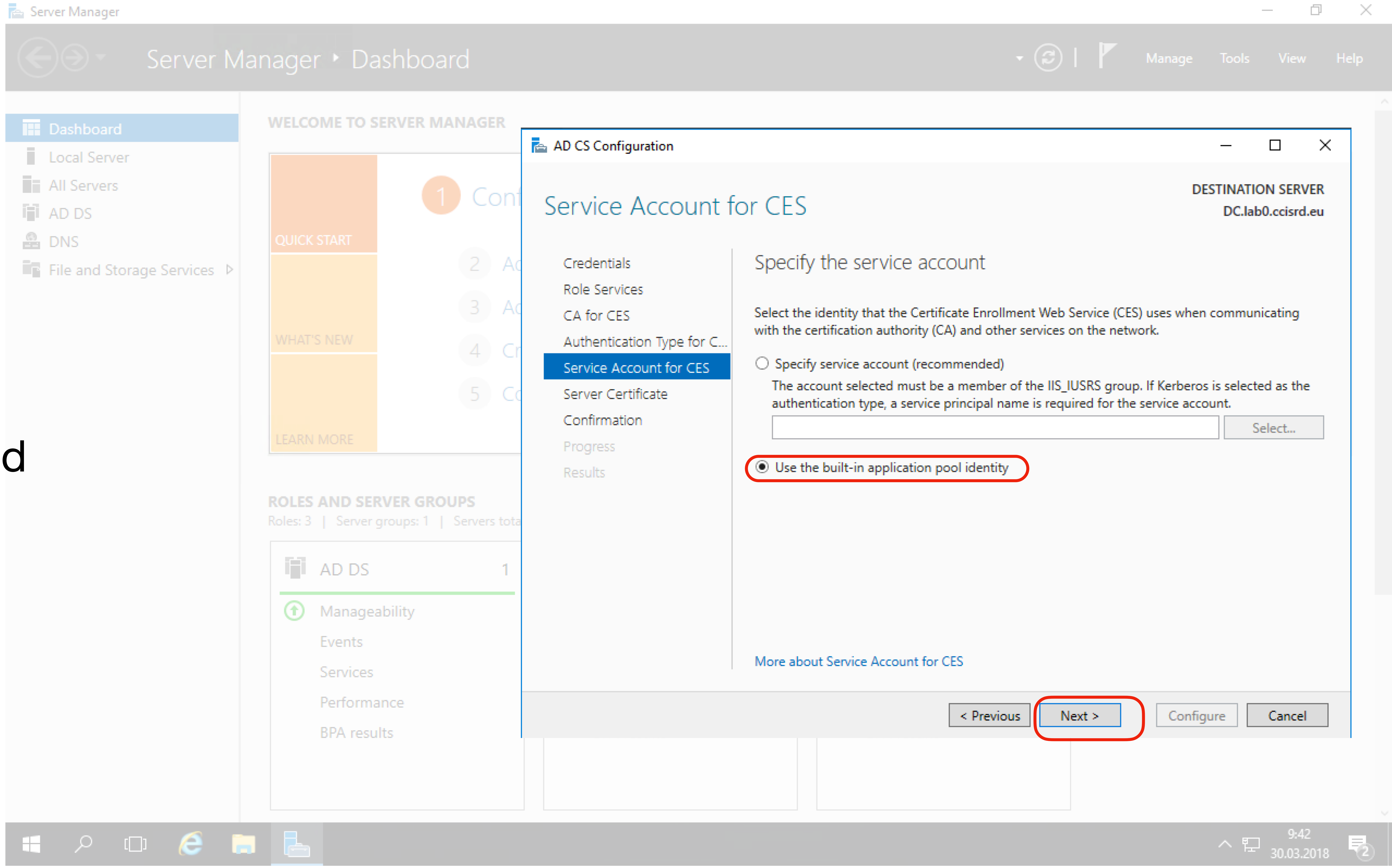
○ Client certificate authentication

○ User name and password

More about Authentication Type for CES

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”



AD CS Configuration

DESTINATION SERVER
DC.lab0.ccisrd.eu

Service Account for CES

Specify the service account

Select the identity that the Certificate Enrollment Web Service (CES) uses when communicating with the certification authority (CA) and other services on the network.

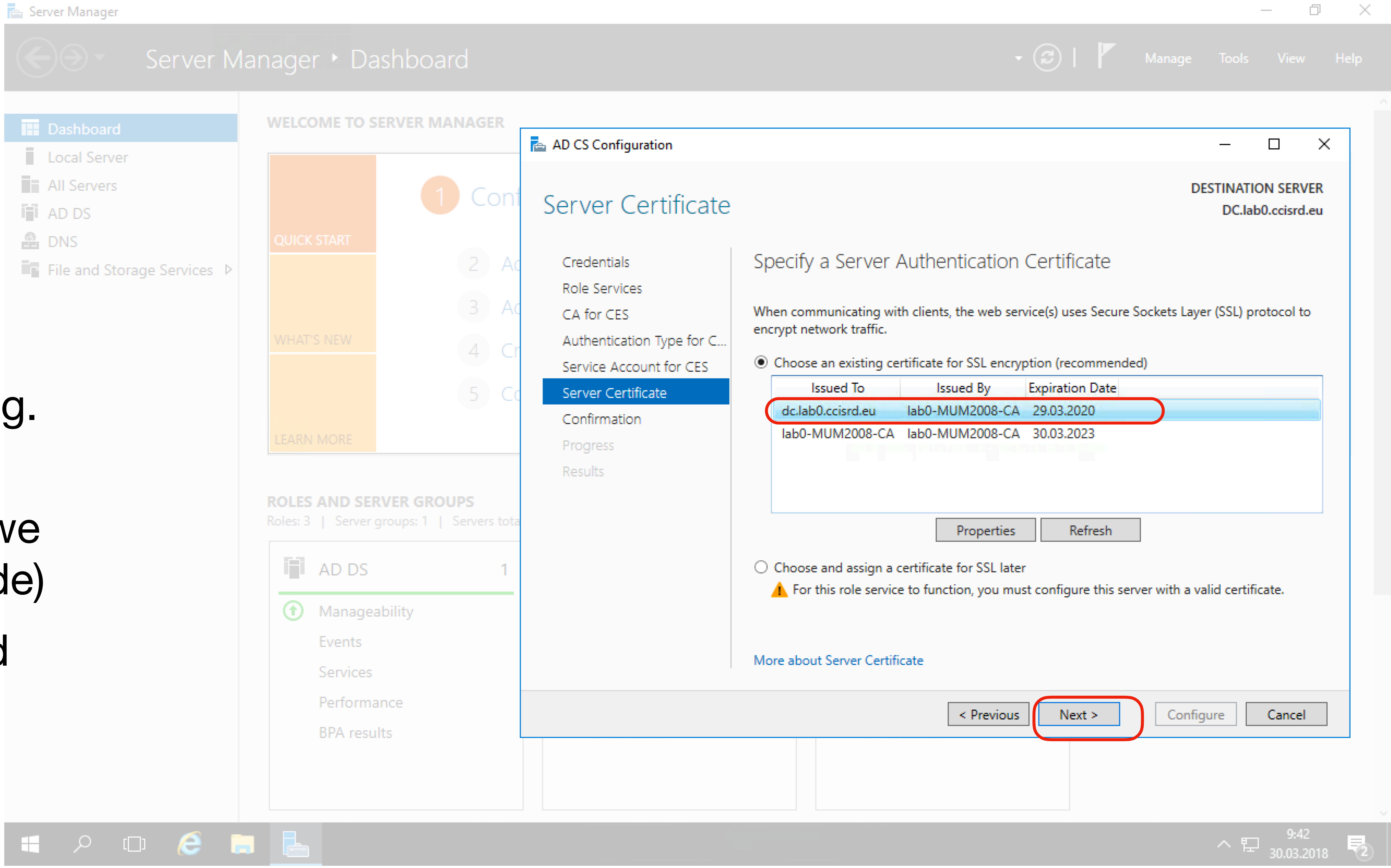
○ Specify service account (recommended)

The account selected must be a member of the IIS_IUSRS group. If Kerberos is selected as the authentication type, a service principal name is required for the service account.

● Use the built-in application pool identity

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



Server Certificate

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify a Server Authentication Certificate

When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.

● Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date
dc.lab0.ccisrd.eu	lab0-MUM2008-CA	29.03.2020
lab0-MUM2008-CA	lab0-MUM2008-CA	30.03.2023

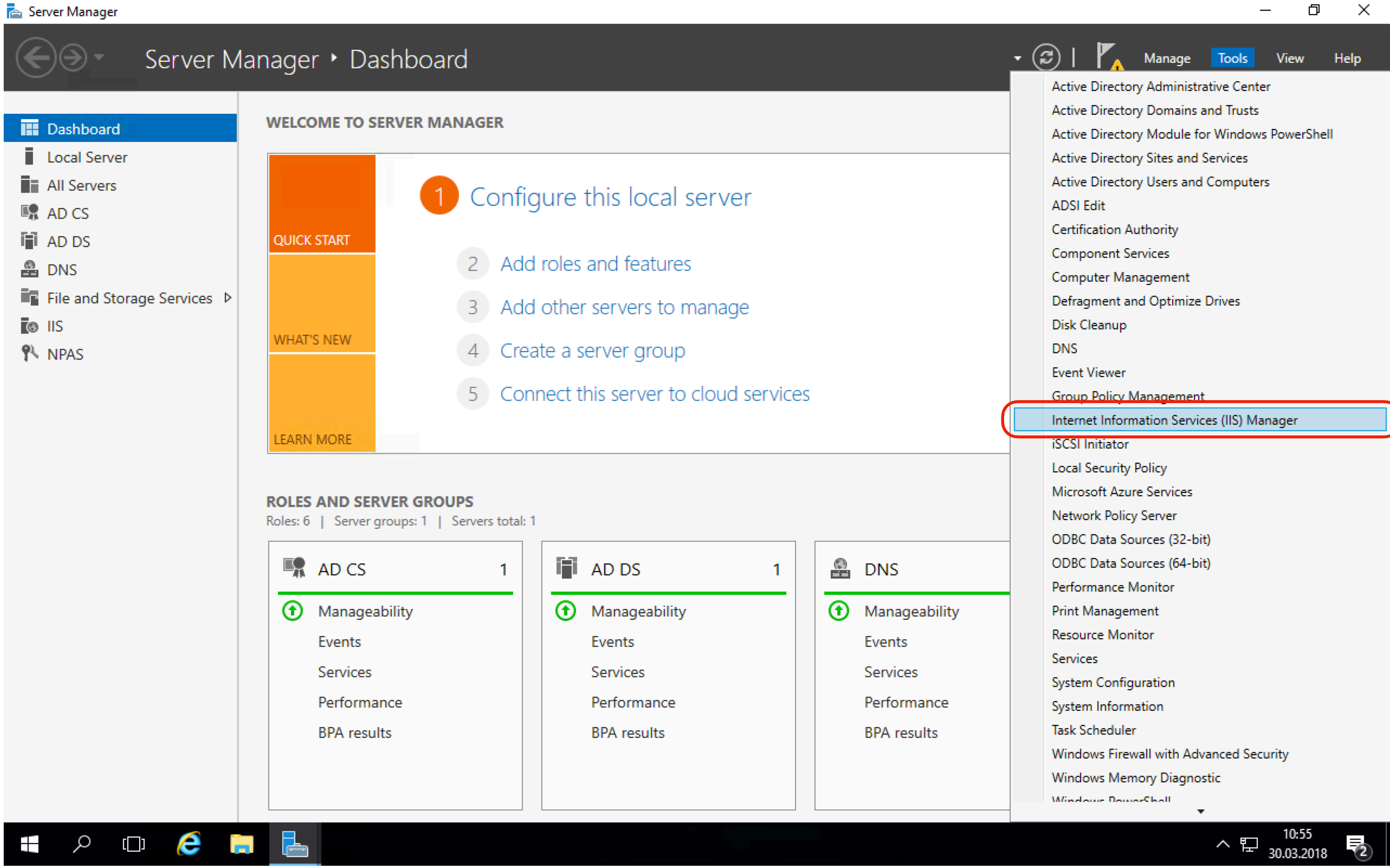
○ Choose and assign a certificate for SSL later

⚠ For this role service to function, you must configure this server with a valid certificate.

More about Server Certificate

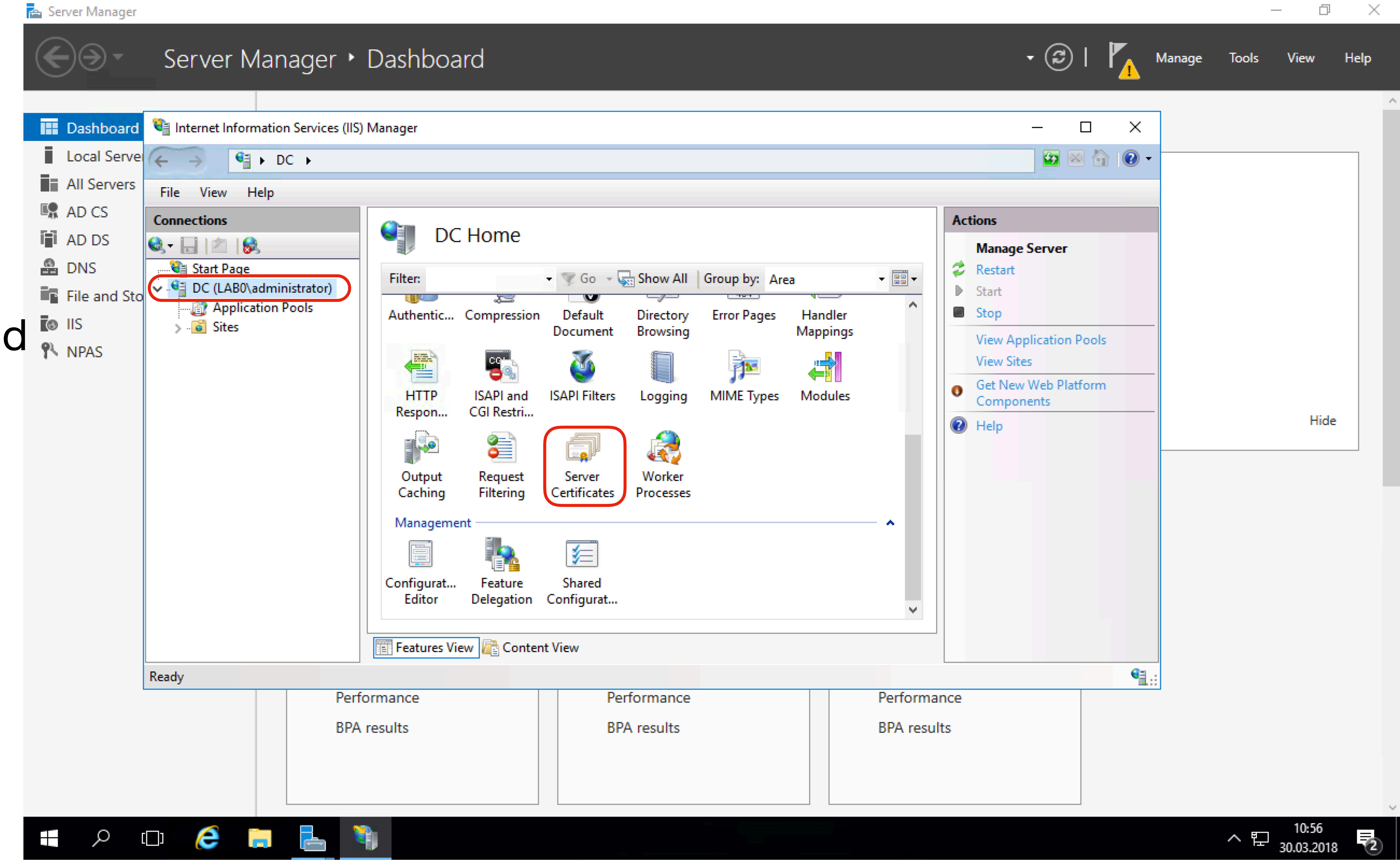
Configure CA

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



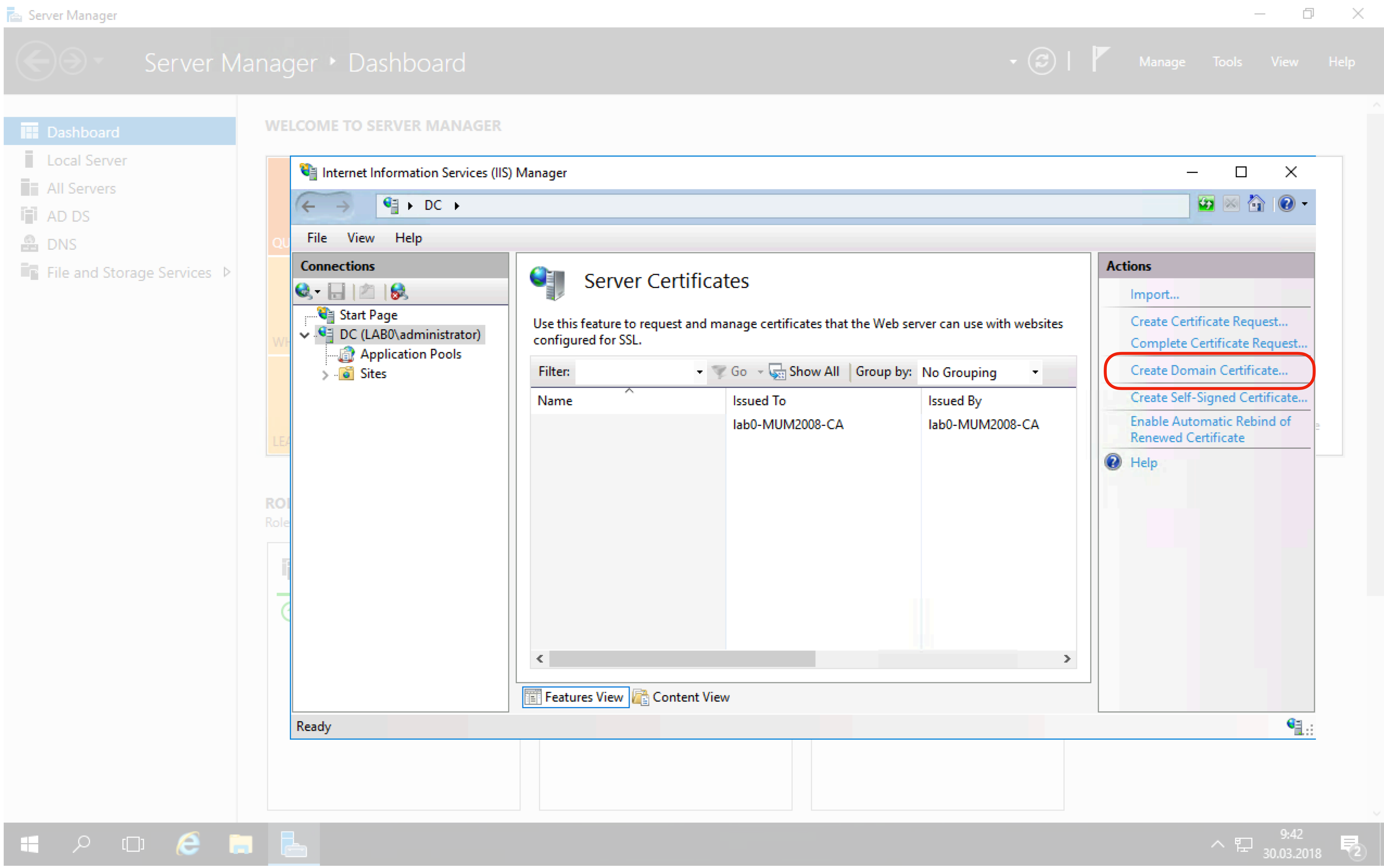
Create web server certificate

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



Create web server certificate

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


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
Internet Information Services (IIS) Manager
DC
File
View
Help
Connections
Start Page
DC (LAB0\administrator)
Application Pools
Sites
Filter:
Go
Show All
Group by:
No Grouping
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready
9:42
30.03.2018

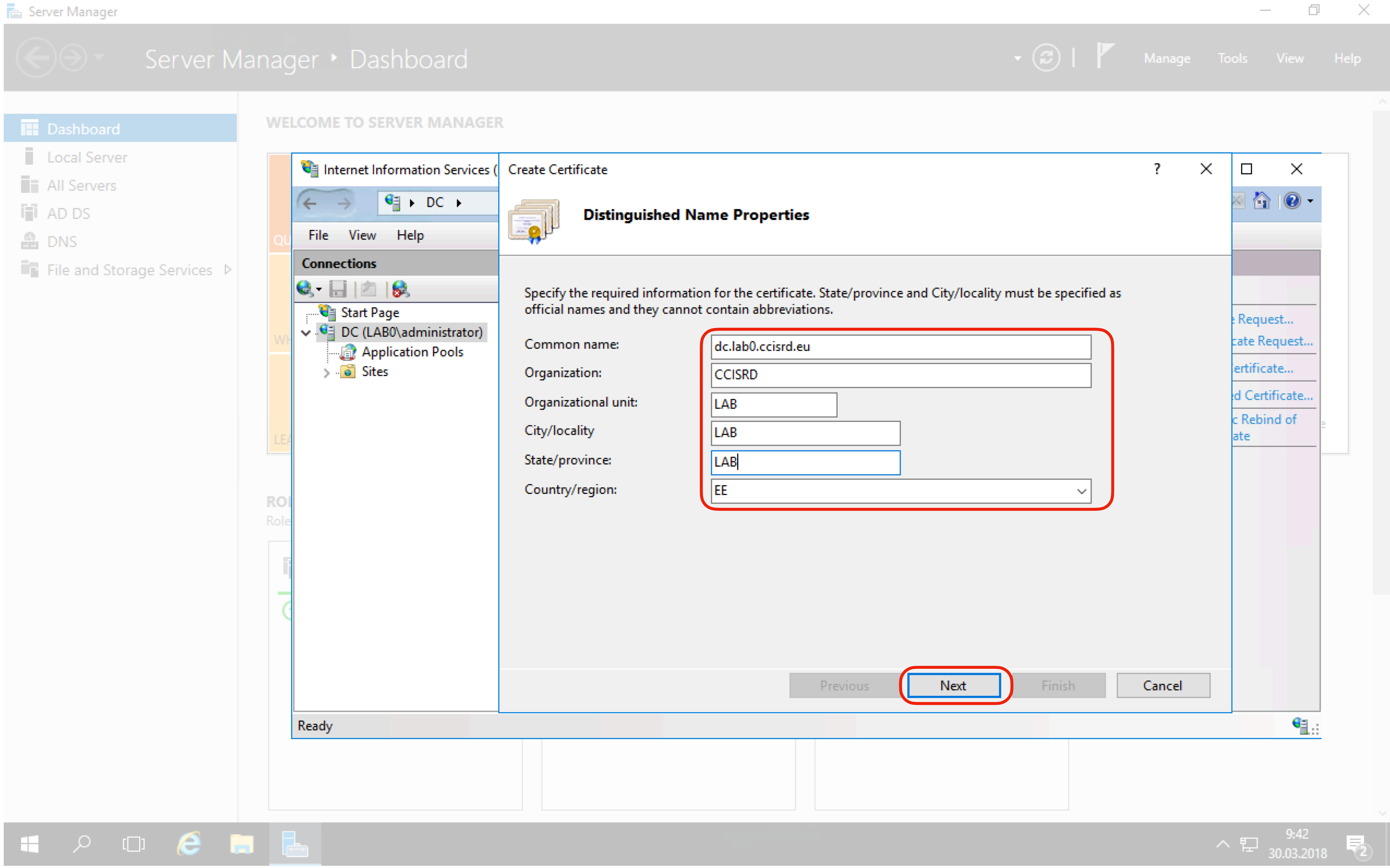
Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By
	lab0-MUM2008-CA	lab0-MUM2008-CA

Create web server certificate

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



Create Certificate

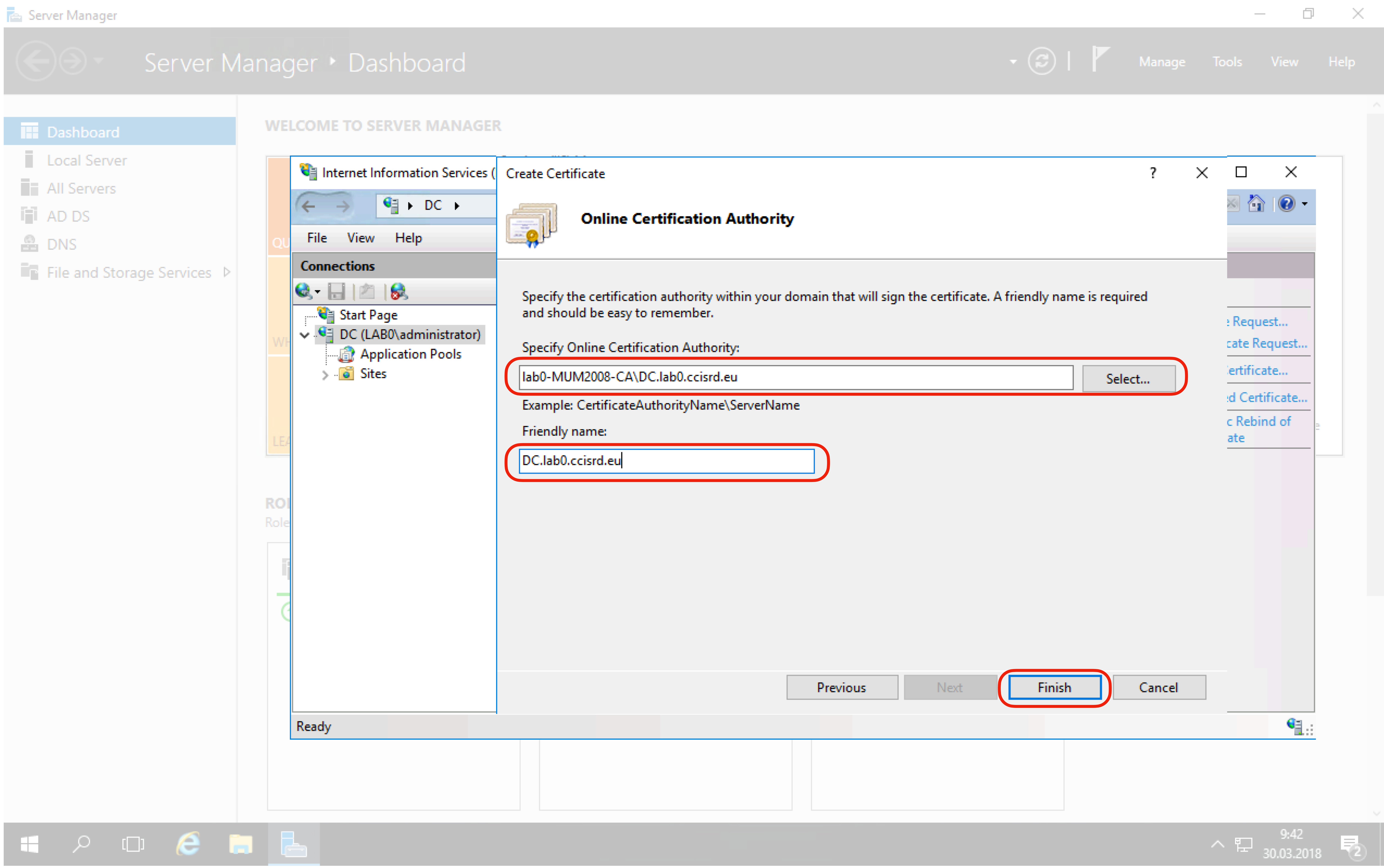
Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	dc.lab0.ccisrd.eu
Organization:	CCISRD
Organizational unit:	LAB
City/locality	LAB
State/province:	LAB
Country/region:	EE

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 Certificate

Online Certification Authority

Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.

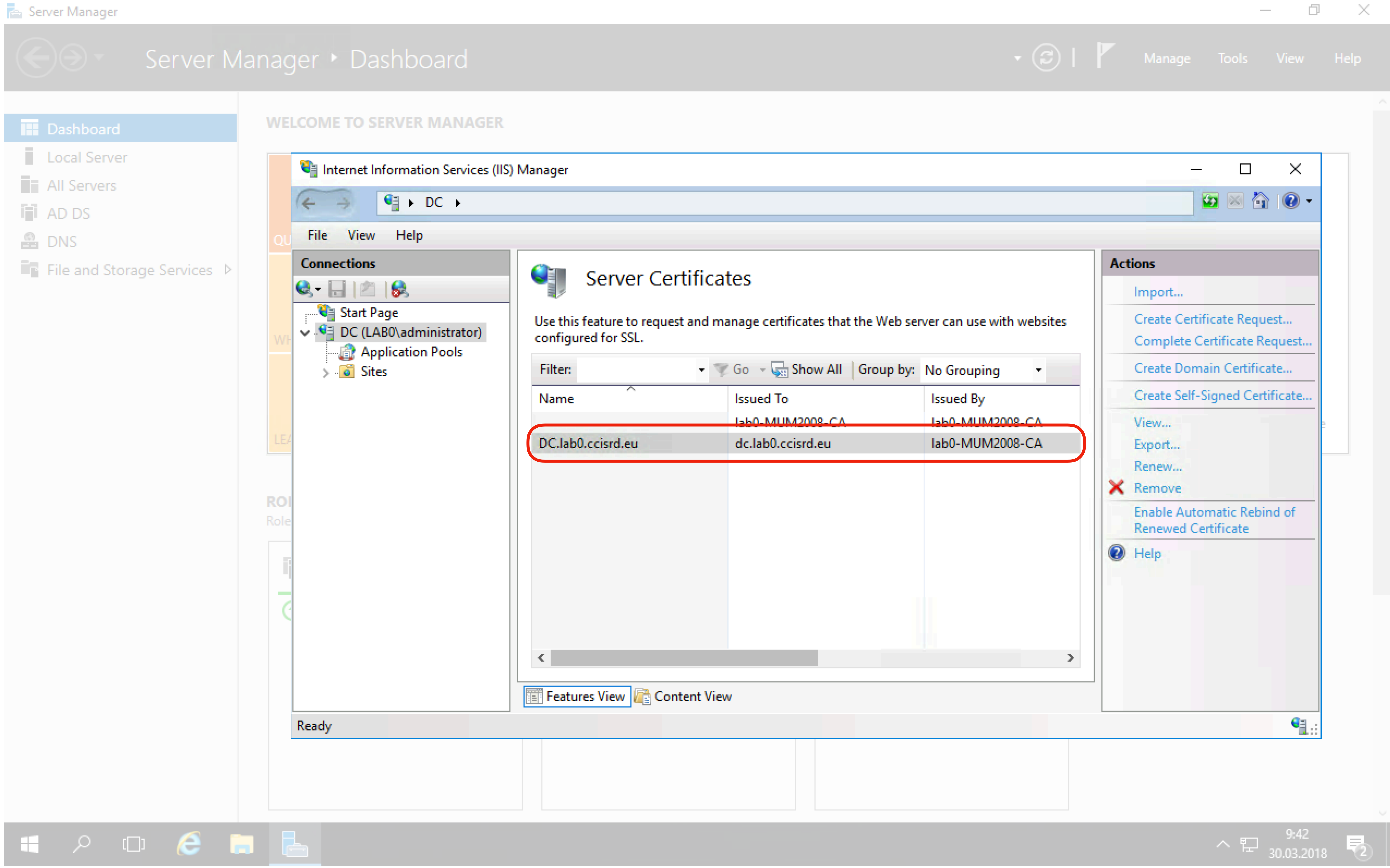
Specify Online Certification Authority: lab0-MUM2008-CA\DC.lab0.ccisrd.eu

Example: CertificateAuthorityName\ServerName

Friendly name: DC.lab0.ccisrd.eu

Create web server certificate

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


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
Internet Information Services (IIS) Manager
DC
File
View
Help
Connections
Start Page
DC (LAB0\administrator)
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
9:42
30.03.2018

Server Certificates

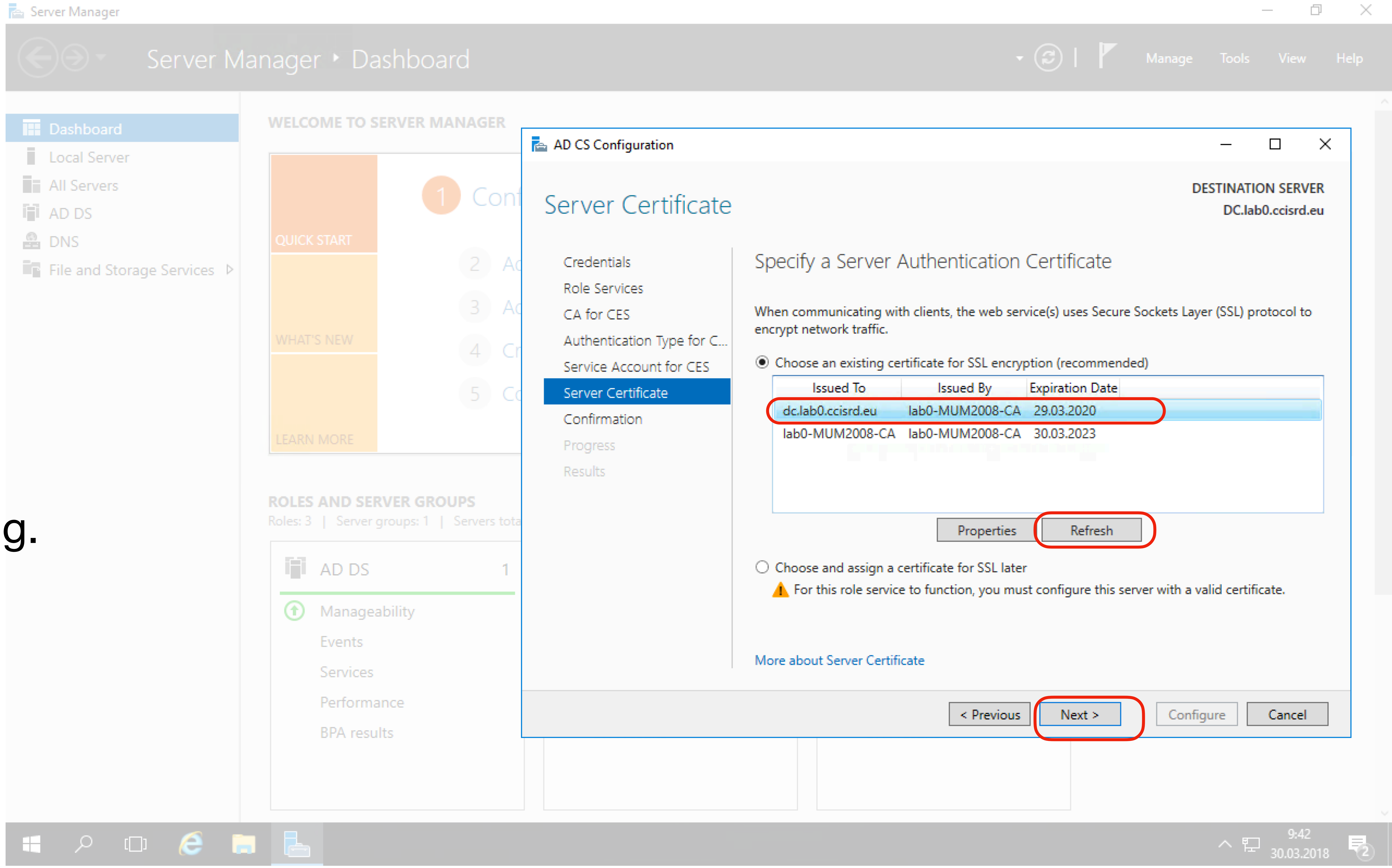
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All Group by: No Grouping

Name	Issued To	Issued By
	lab0-MUM2008-CA	lab0-MUM2008-CA
DC.lab0.ccisrd.eu	dc.lab0.ccisrd.eu	lab0-MUM2008-CA

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”



Server Certificate

Specify a Server Authentication Certificate

When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.

● Choose an existing certificate for SSL encryption (recommended)

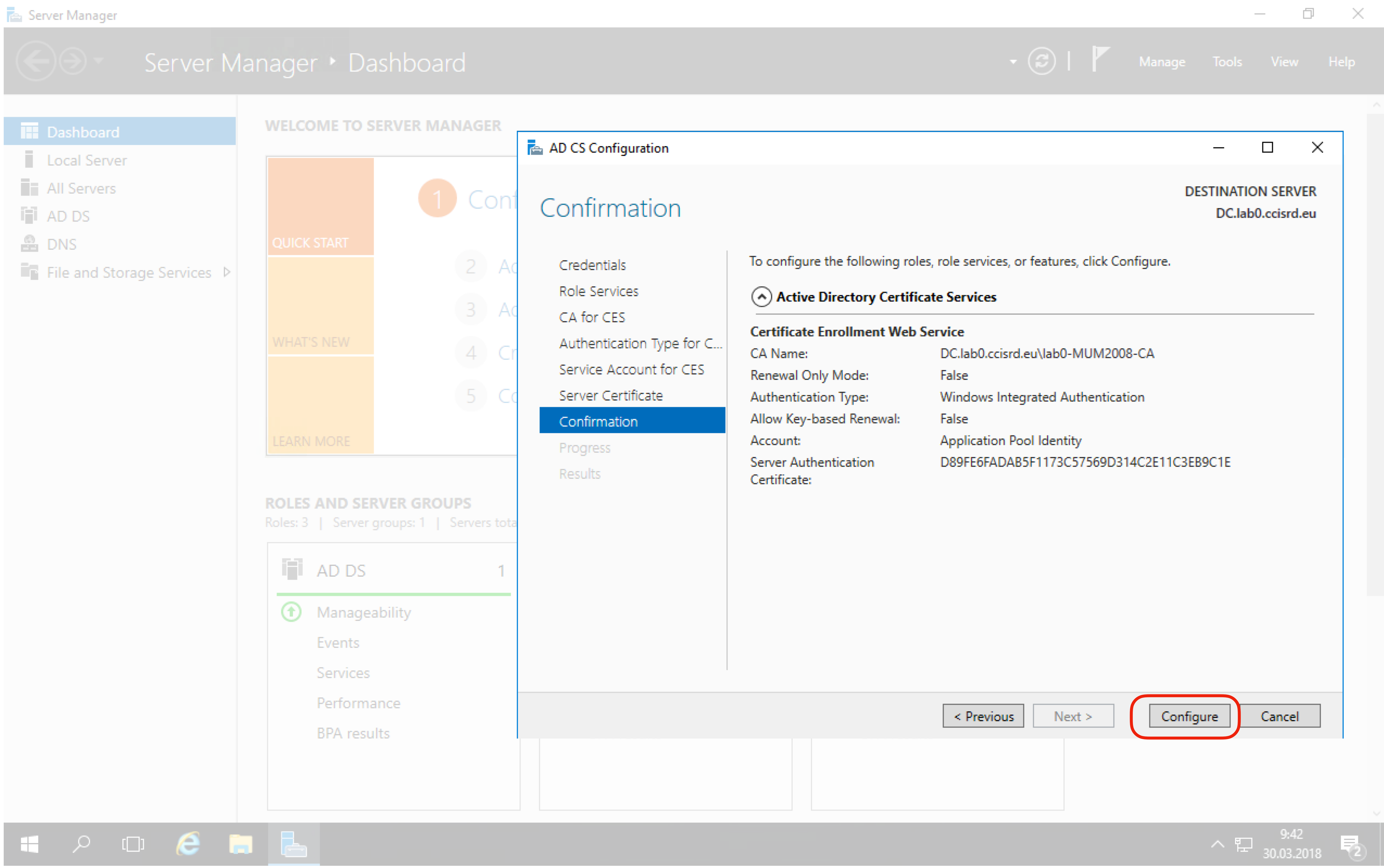
Issued To	Issued By	Expiration Date
dc.lab0.ccisrd.eu	lab0-MUM2008-CA	29.03.2020
lab0-MUM2008-CA	lab0-MUM2008-CA	30.03.2023

○ Choose and assign a certificate for SSL later

For this role service to function, you must configure this server with a valid certificate.

Configure CA

- Click “Configure”



AD CS Configuration

Confirmation

DESTINATION SERVER
DC.lab0.ccisrd.eu

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Server Certificate
Confirmation
Progress
Results

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

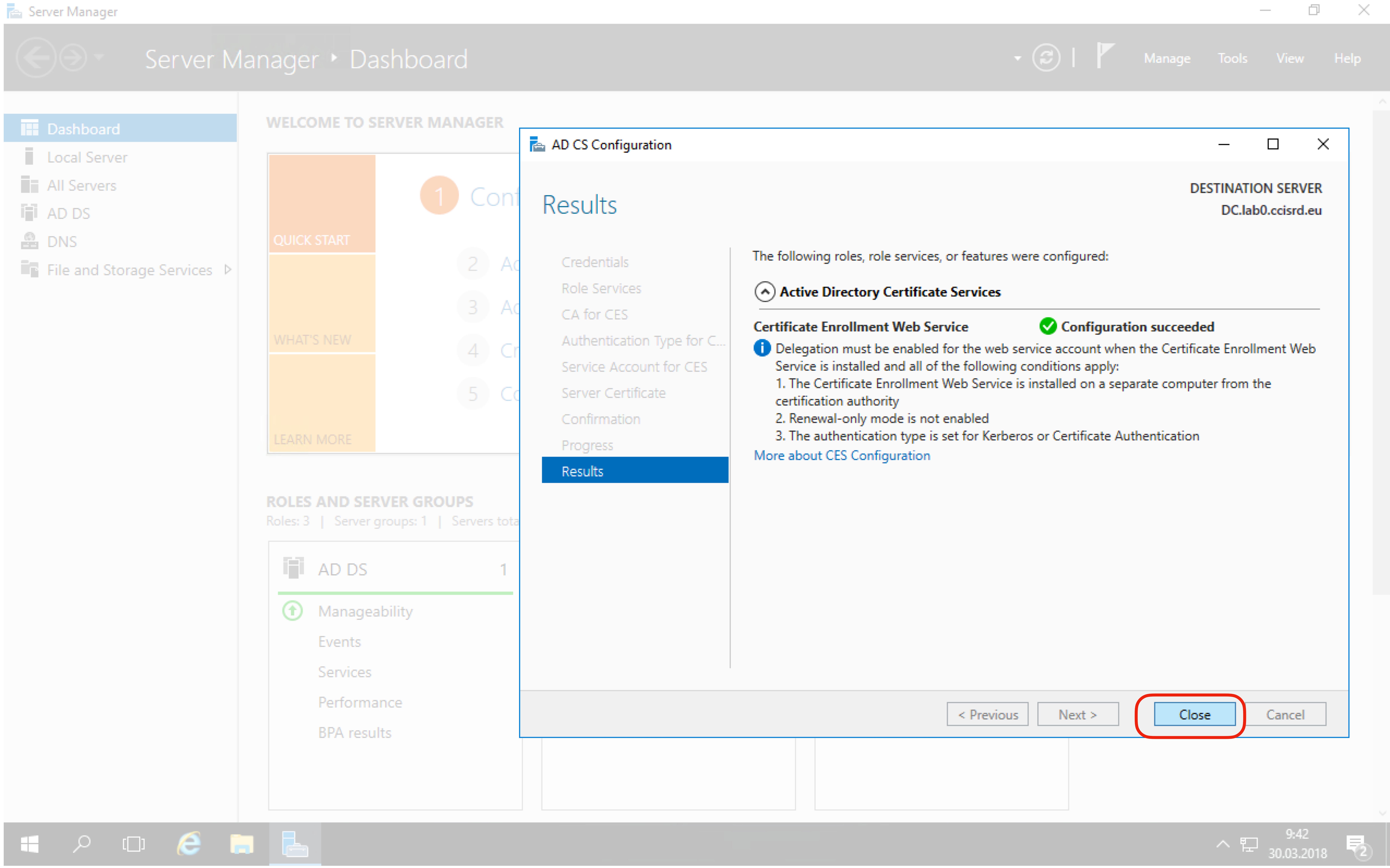
Certificate Enrollment Web Service

CA Name:	DC.lab0.ccisrd.eu\lab0-MUM2008-CA
Renewal Only Mode:	False
Authentication Type:	Windows Integrated Authentication
Allow Key-based Renewal:	False
Account:	Application Pool Identity
Server Authentication Certificate:	D89FE6FADAB5F1173C57569D314C2E11C3EB9C1E

< Previous | Next > | Configure | Cancel

Configure CA

- Click “Close”



Results

DESTINATION SERVER
DC.lab0.ccisrd.eu

The following roles, role services, or features were configured:

Active Directory Certificate Services

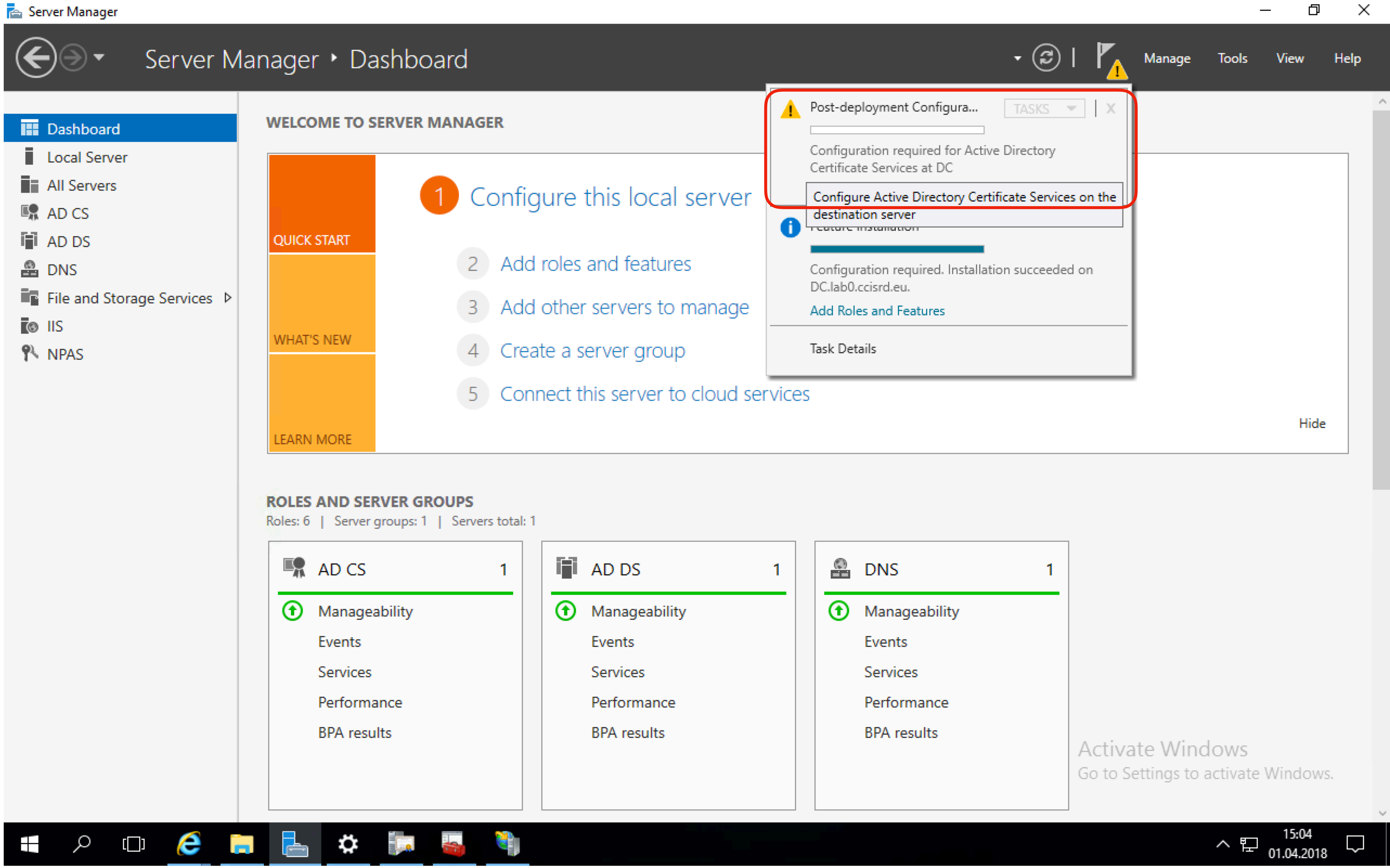
Certificate Enrollment Web Service ✓ Configuration succeeded

Delegation must be enabled for the web service account when the Certificate Enrollment Web Service is installed and all of the following conditions apply:
1. The Certificate Enrollment Web Service is installed on a separate computer from the certification authority
2. Renewal-only mode is not enabled
3. The authentication type is set for Kerberos or Certificate Authentication

More about CES Configuration

Configure Web Service

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



Server Manager › Dashboard

Post-deployment Configura...

Configuration required for Active Directory Certificate Services at DC

Configure Active Directory Certificate Services on the destination server

Feature installation

Configuration required. Installation succeeded on DC.lab0.ccisrd.eu.

Add Roles and Features

Task Details

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

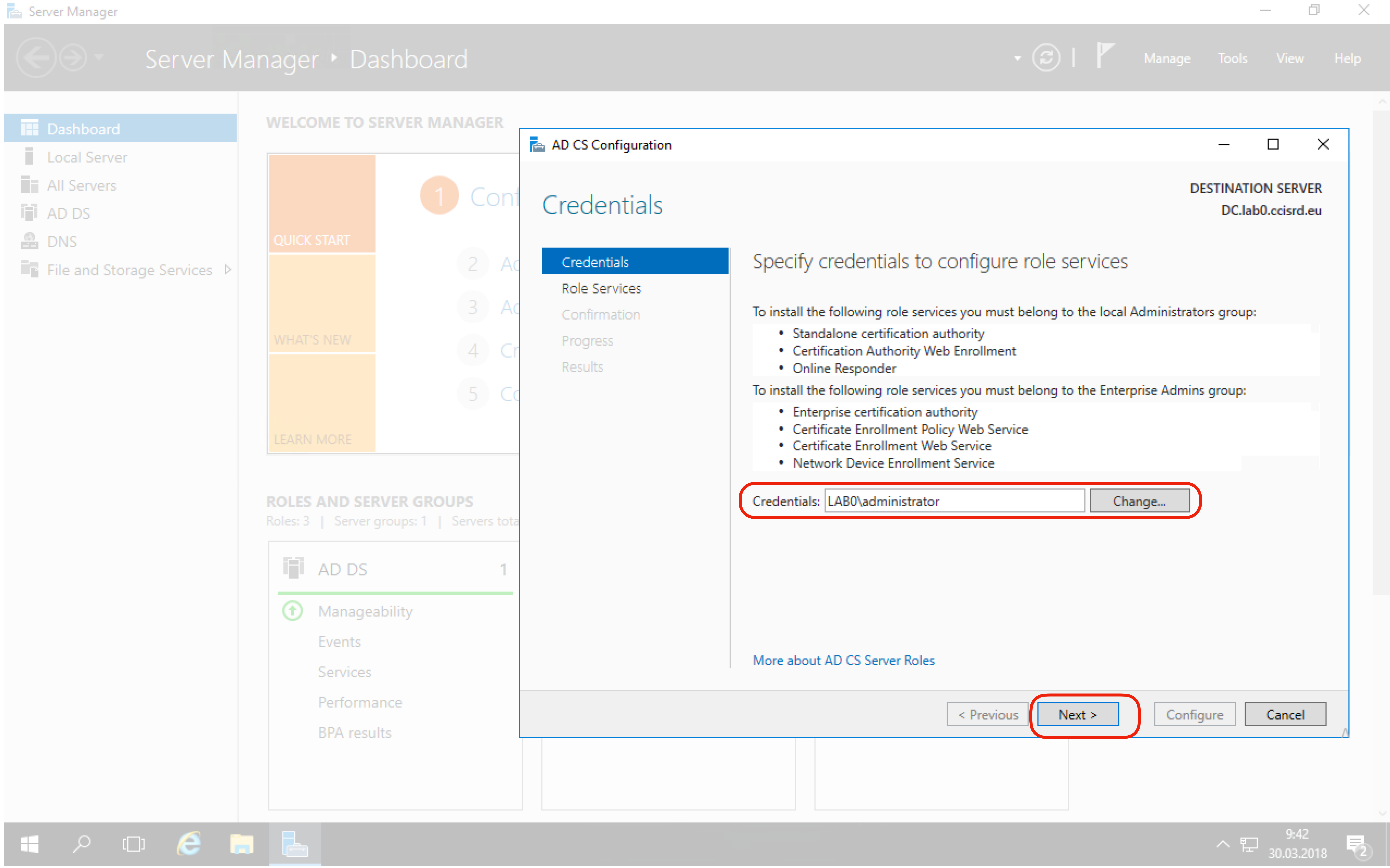
4 Create a server group

5 Connect this server to cloud services

ROLES AND SERVER GROUPS
Roles: 6 | Server groups: 1 | Servers total: 1

Configure CA

- Verify username and click “Next”



AD CS Configuration

Credentials

DESTINATION SERVER
DC.lab0.ccisrd.eu

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

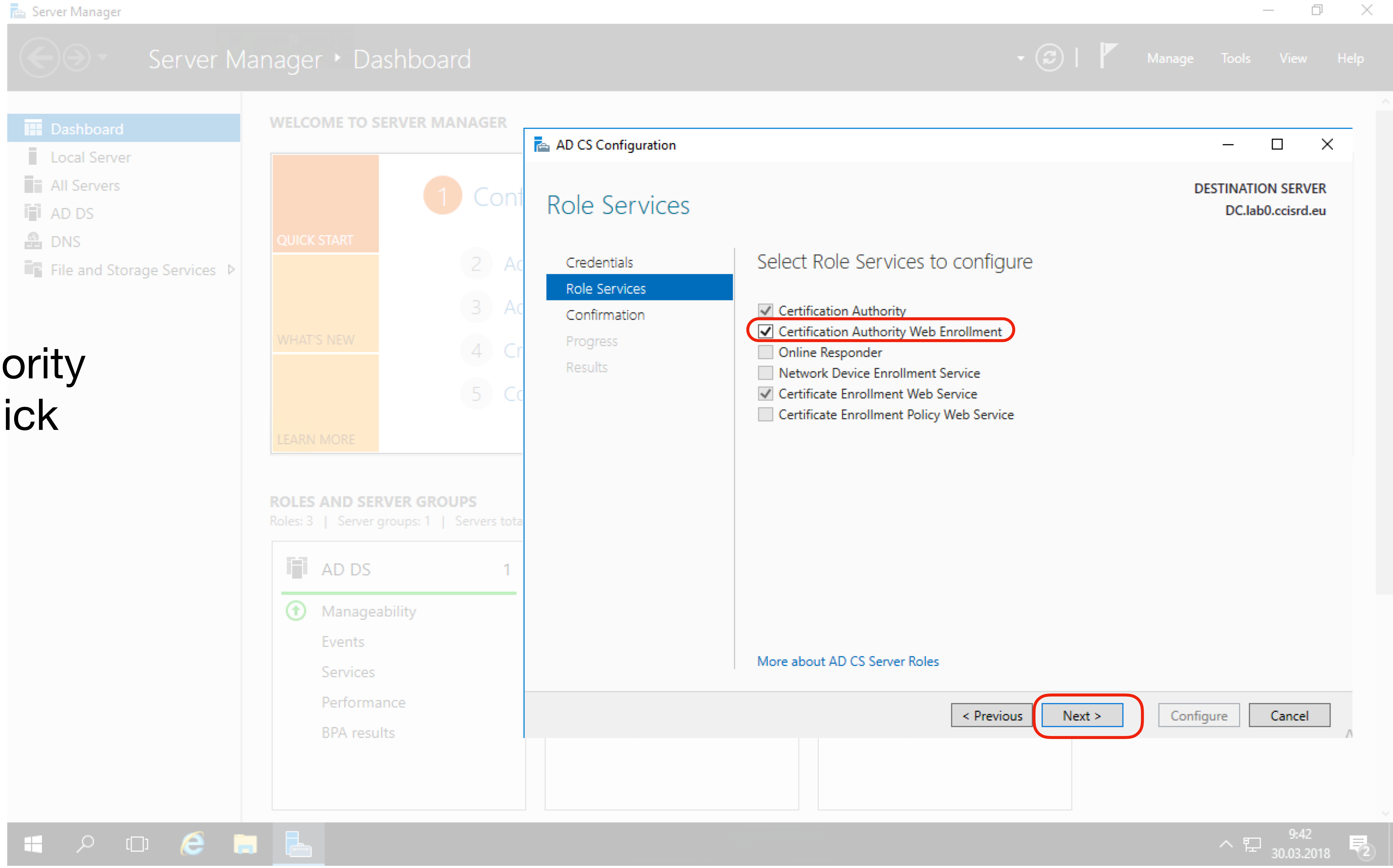
To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: LAB0\administrator

More about AD CS Server Roles

Configure CA



AD CS Configuration

Role Services

DESTINATION SERVER
DC.lab0.ccisrd.eu

Select Role Services to configure

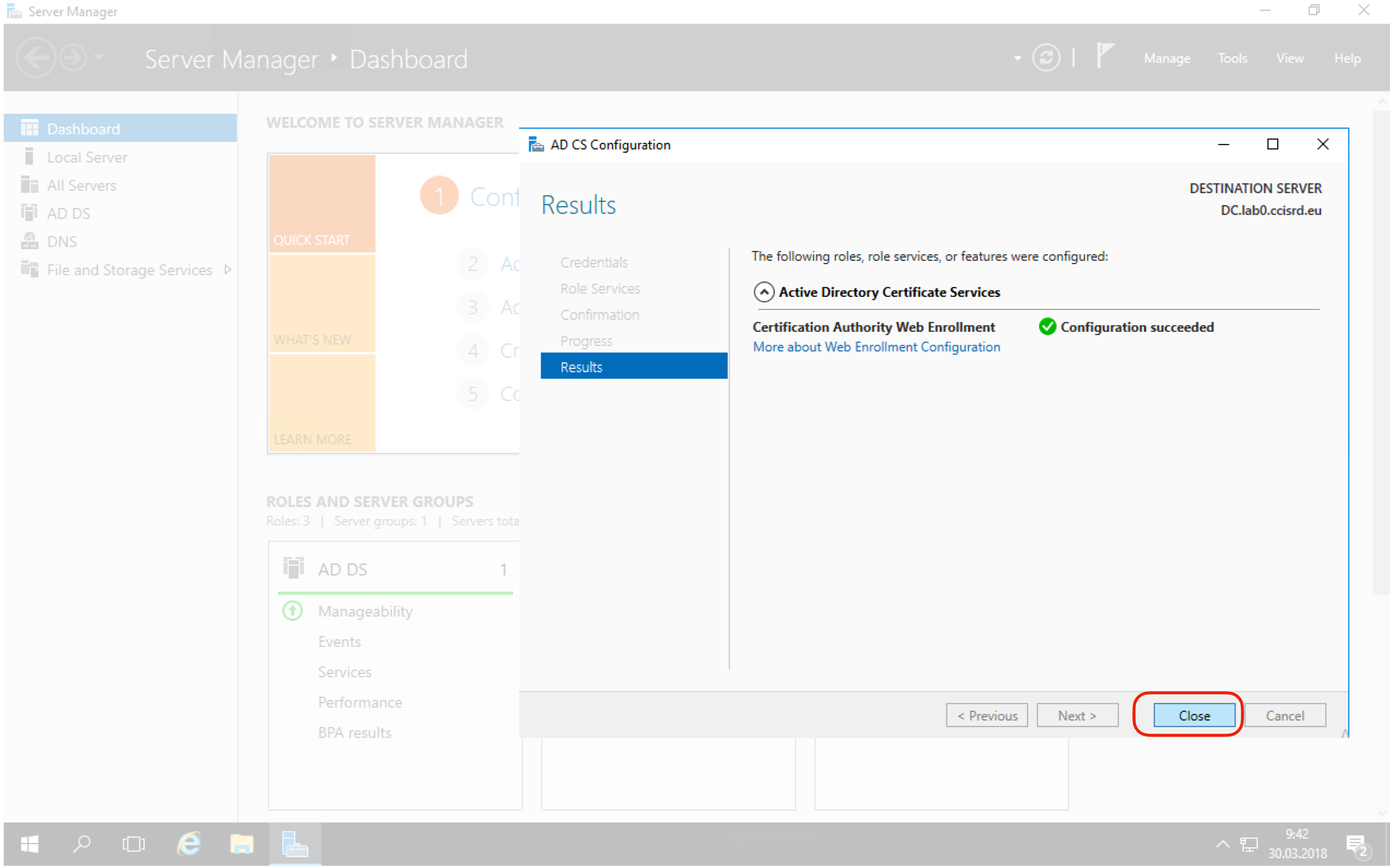
- ☑ Certification Authority
- ☑ Certification Authority Web Enrollment
- □ Online Responder
- □ Network Device Enrollment Service
- ☑ Certificate Enrollment Web Service
- □ Certificate Enrollment Policy Web Service

More about AD CS Server Roles

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

Configure CA

- Click “Close”
- Now is CA configured.



Results

DESTINATION SERVER
DC.lab0.ccisrd.eu

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority Web Enrollment — Configuration succeeded

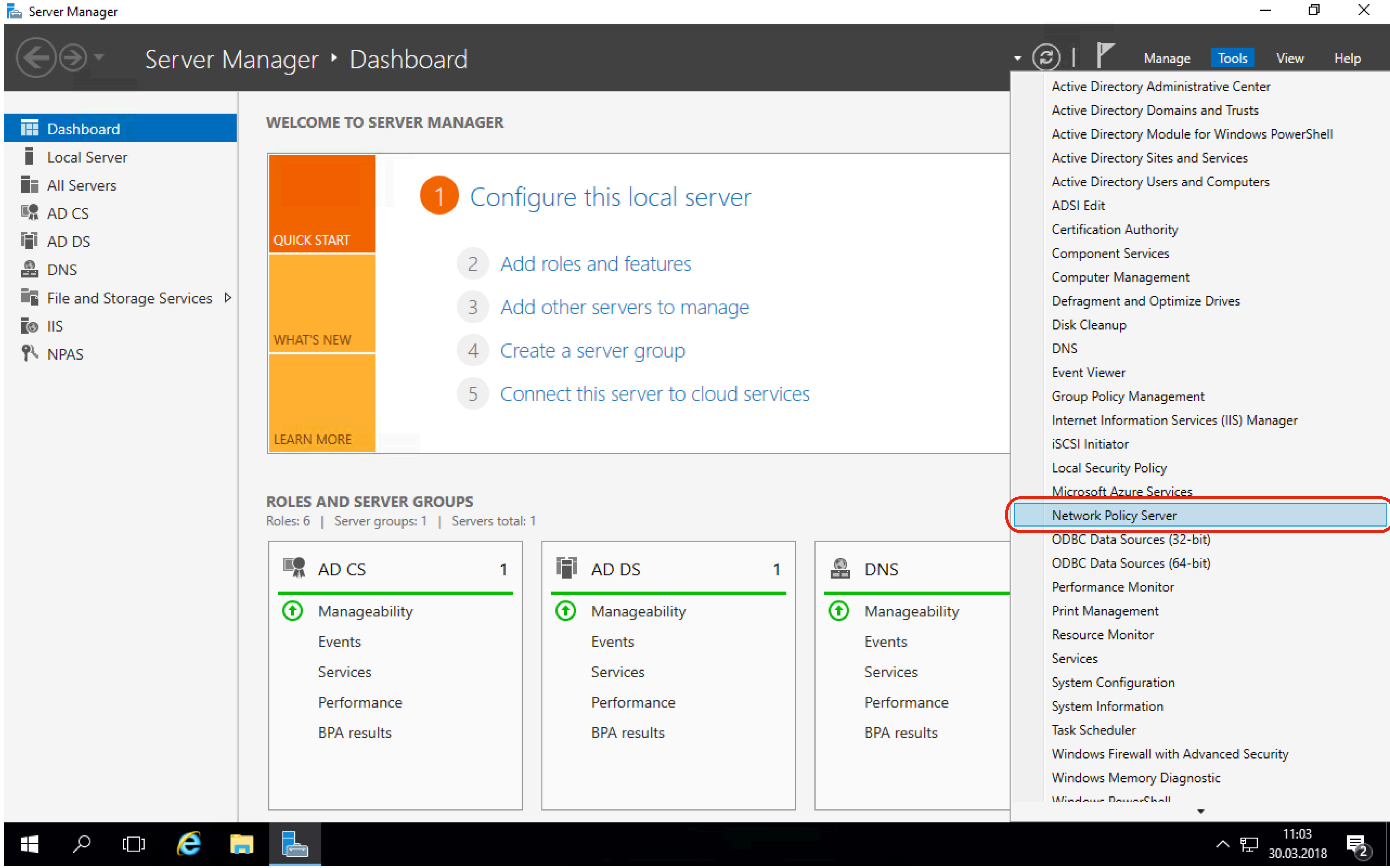
More about Web Enrollment Configuration

Next Steps

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

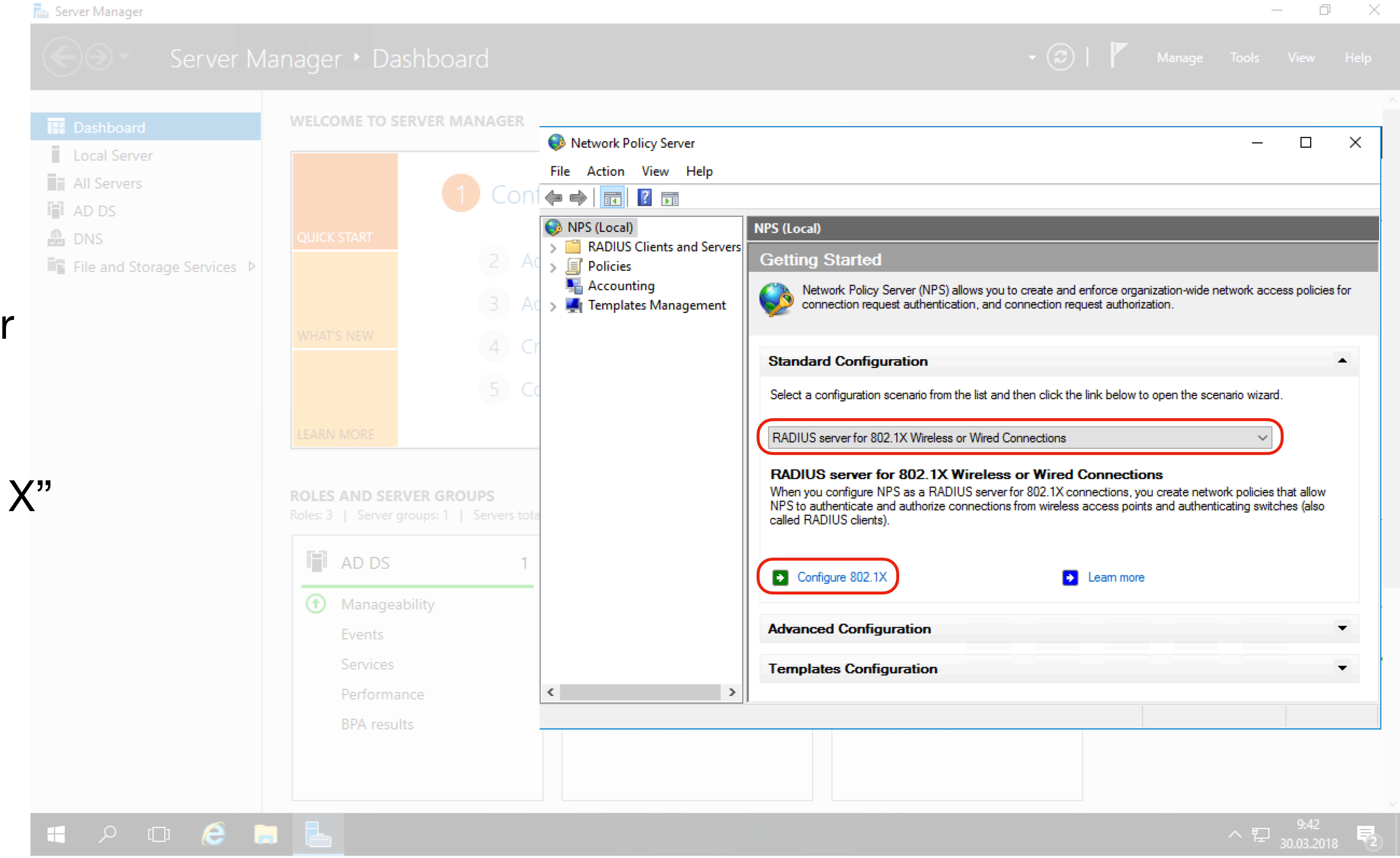
Configure NPS - Radius

- From Server Manager open “Network Policy Server.



Configure NPS - Radius

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



Network Policy Server

Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

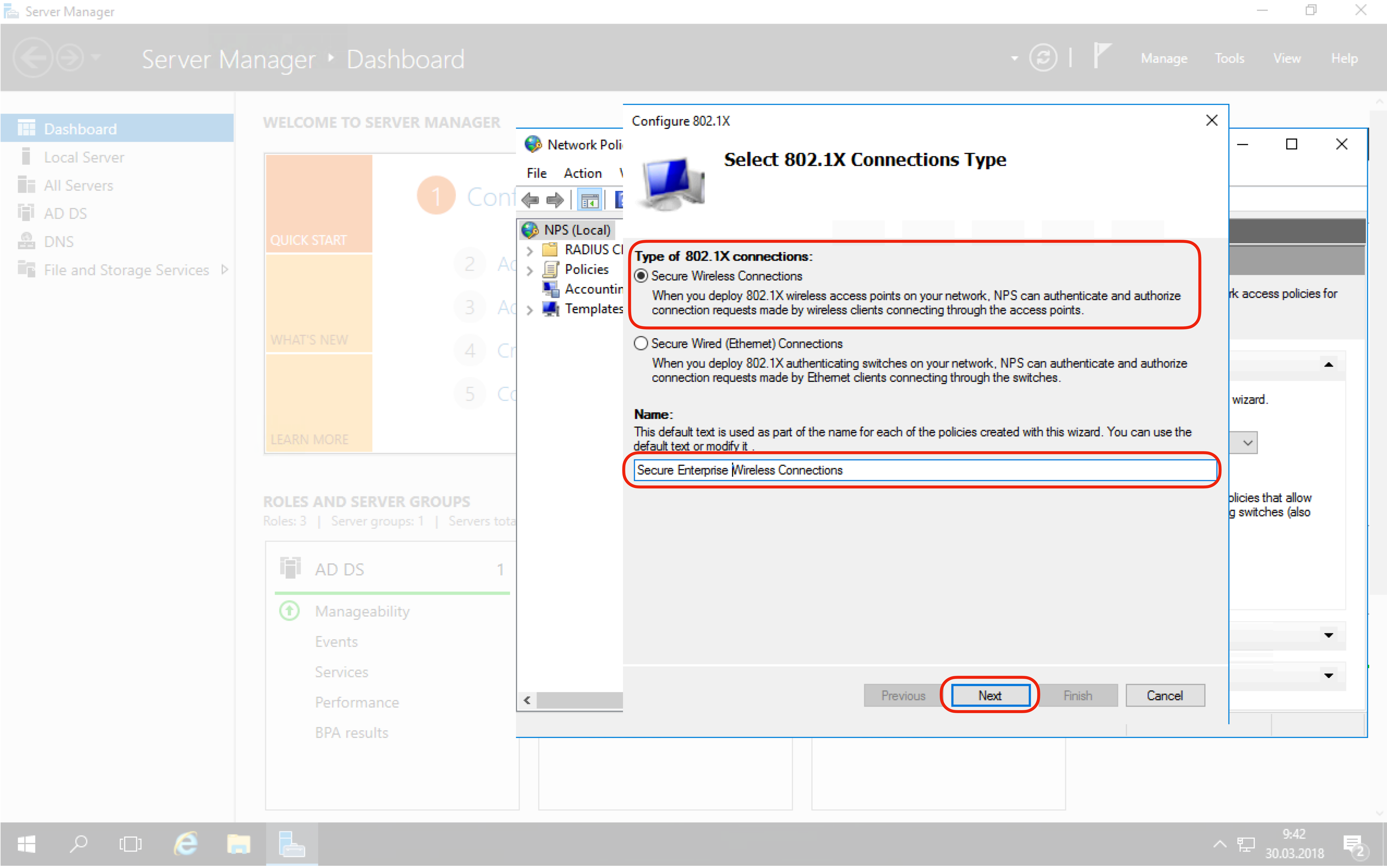
RADIUS server for 802.1X Wireless or Wired Connections

RADIUS server for 802.1X Wireless or Wired Connections

When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

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 802.1X

Select 802.1X Connections Type

Type of 802.1X connections:

● Secure Wireless Connections

When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

○ Secure Wired (Ethernet) Connections

When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

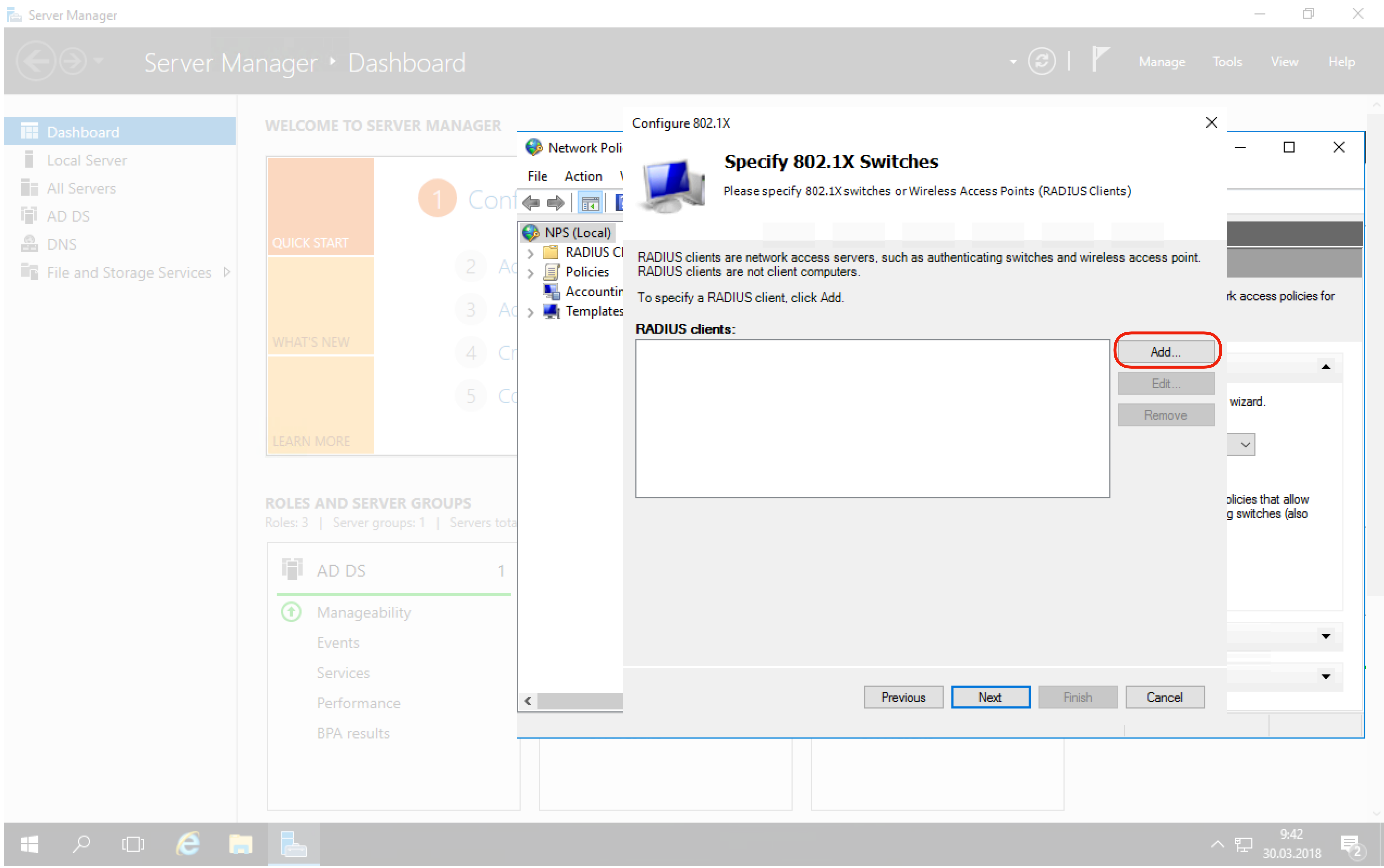
Name:

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .

Secure Enterprise Wireless Connections

Configure NPS - Radius

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



Configure 802.1X

Specify 802.1X Switches

Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)

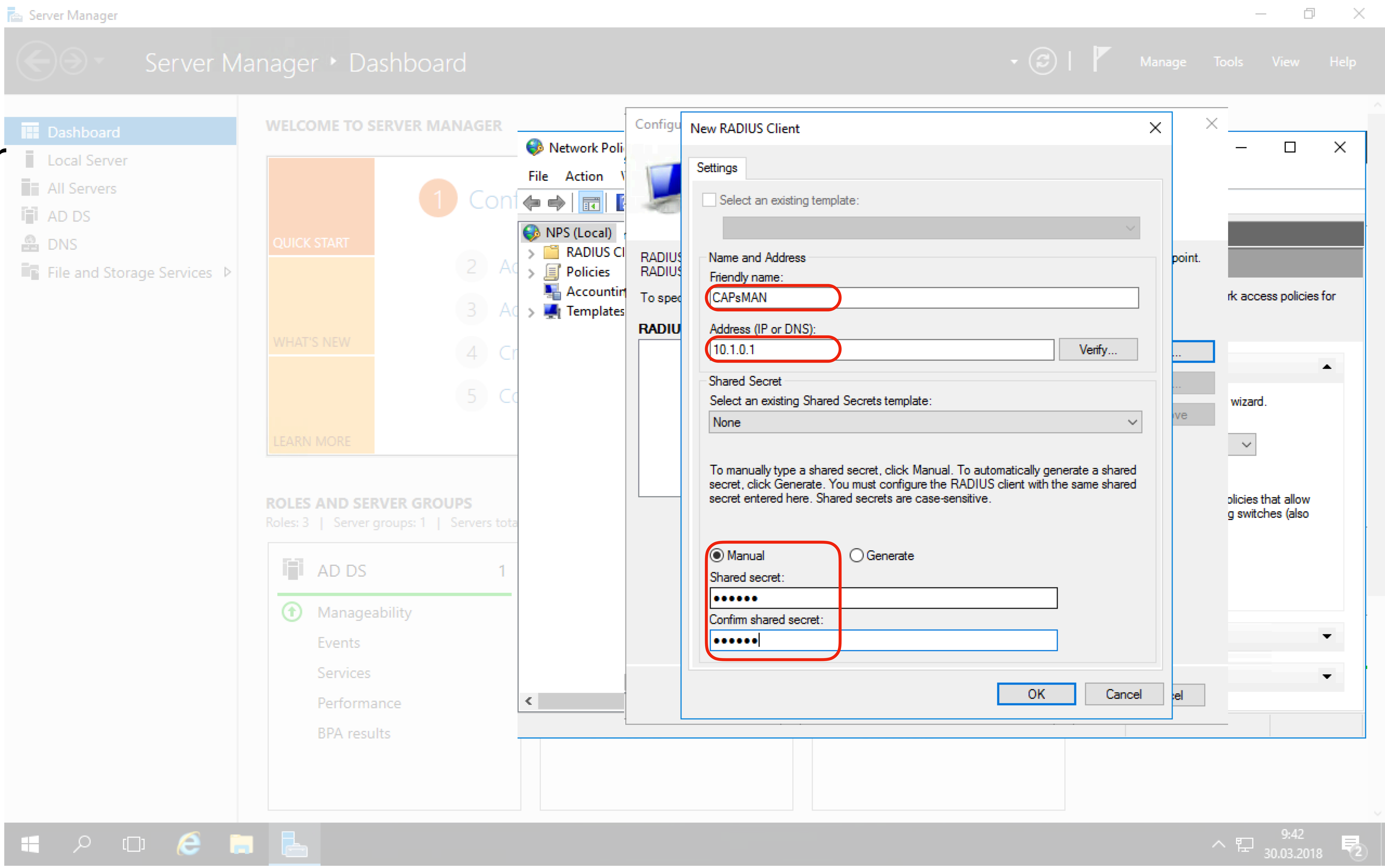
RADIUS clients are network access servers, such as authenticating switches and wireless access point. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

RADIUS clients:

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”.



New RADIUS Client

Settings

□ Select an existing template:

Name and Address

Friendly name: CAPsMAN

Address (IP or DNS): 10.1.0.1

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.

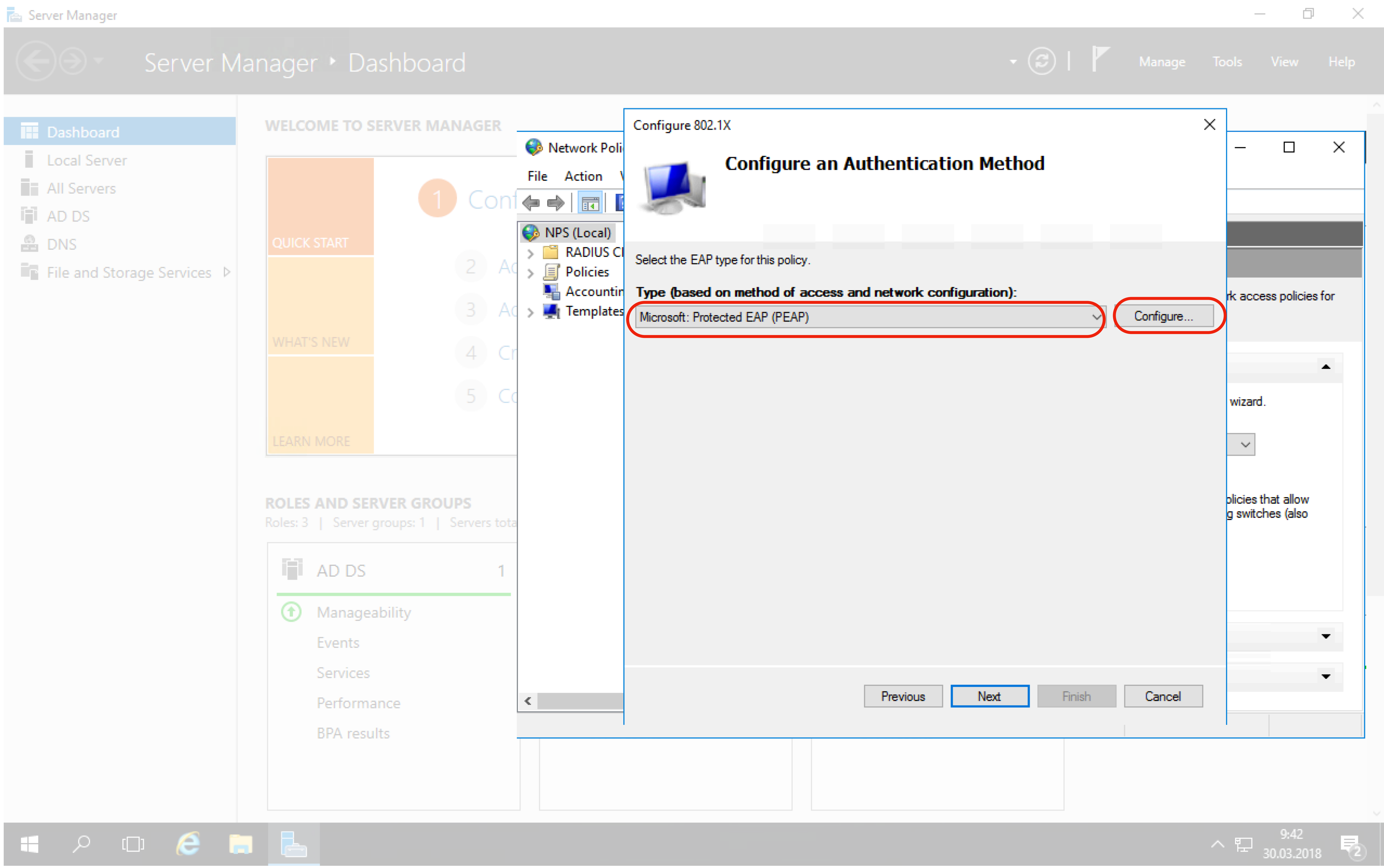
● Manual ○ Generate

Shared secret: ••••••

Confirm shared secret: ••••••

Configure NPS - Radius

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



Configure 802.1X

Configure an Authentication Method

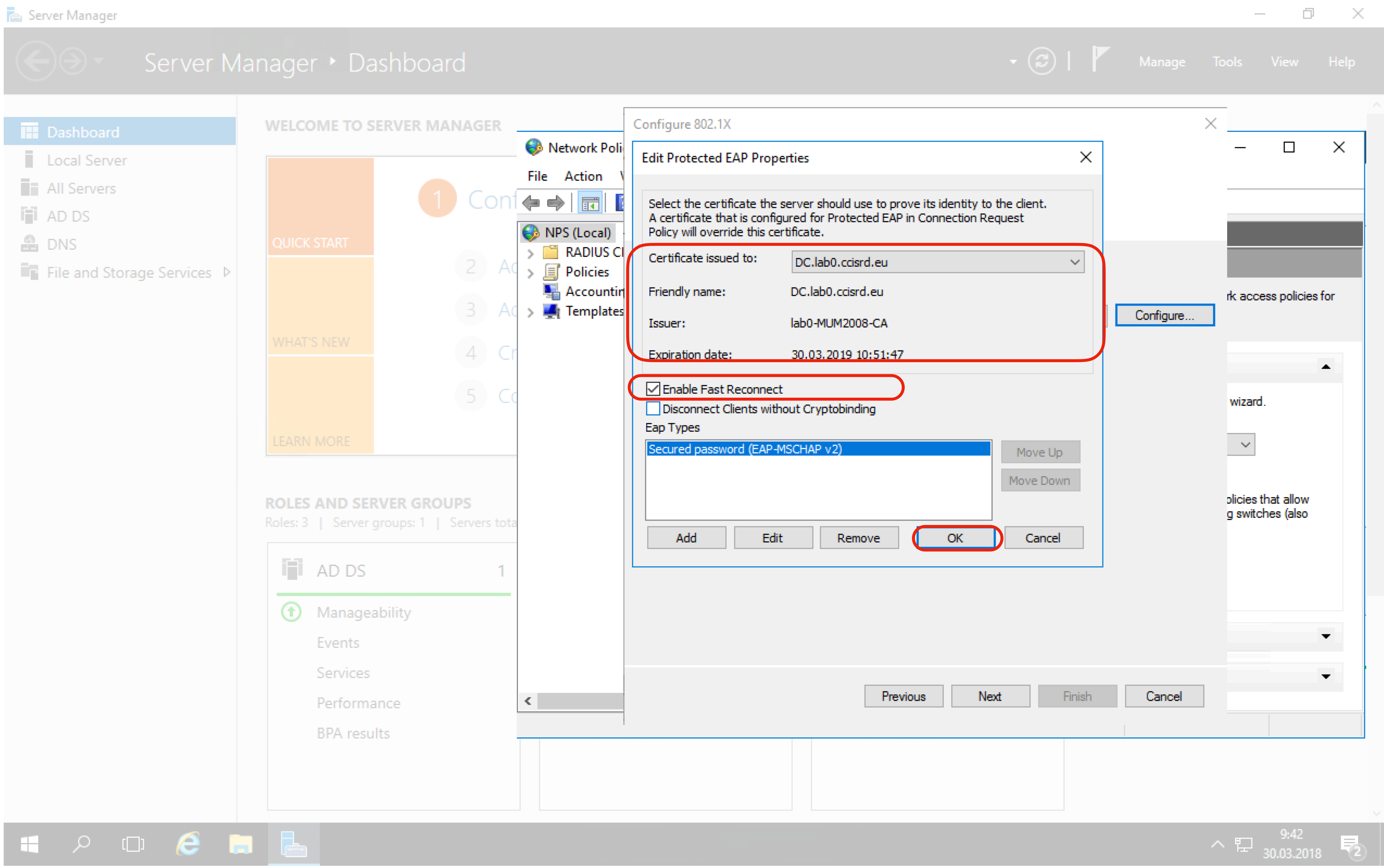
Select the EAP type for this policy.

Type (based on method of access and network configuration):

Microsoft: Protected EAP (PEAP)

Configure NPS - Radius

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



Edit Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued to: DC.lab0.ccisrd.eu

Friendly name: DC.lab0.ccisrd.eu

Issuer: lab0-MUM2008-CA

Expiration date: 30.03.2019 10:51:47

☑ Enable Fast Reconnect

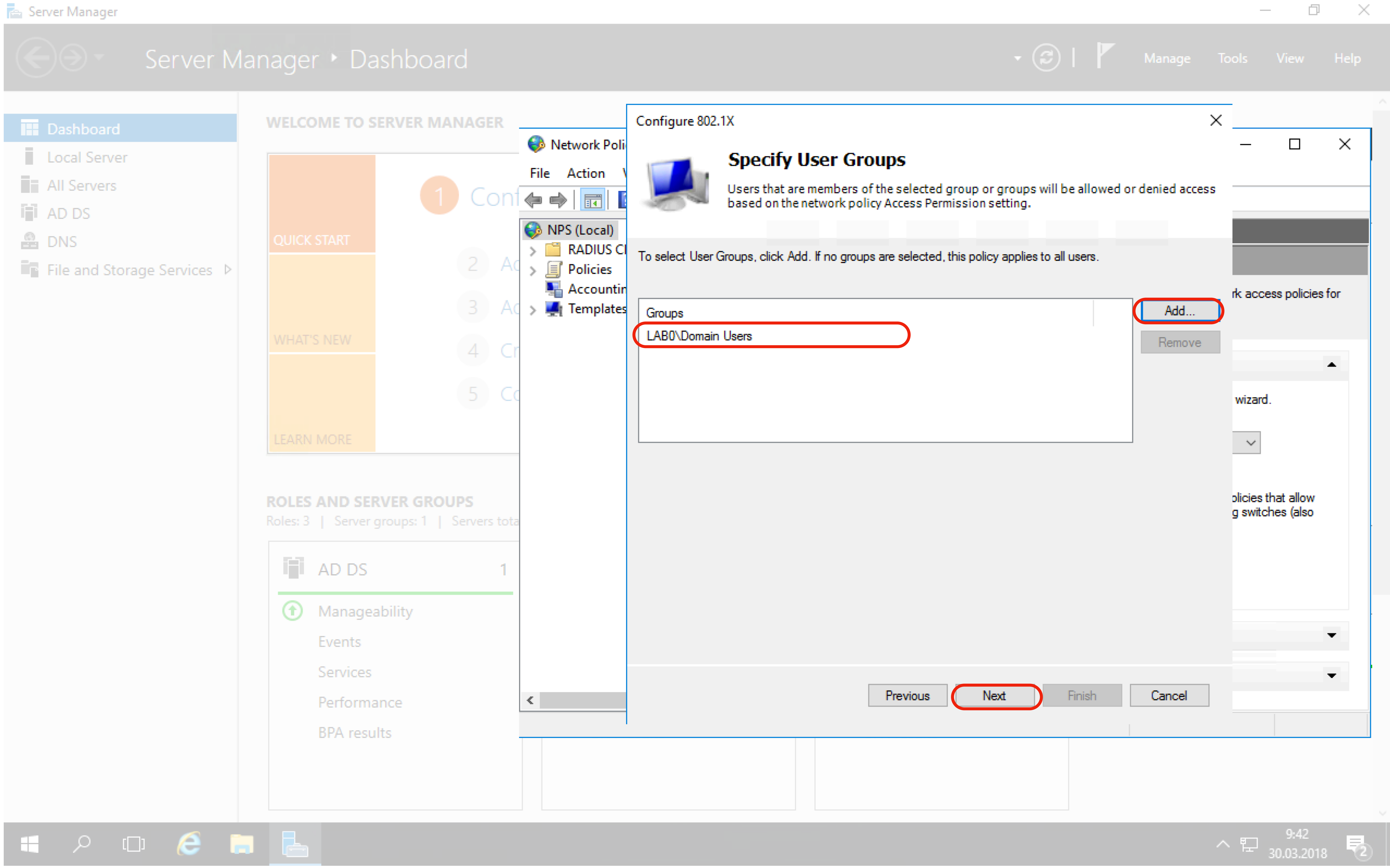
☐ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

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 802.1X

Specify User Groups

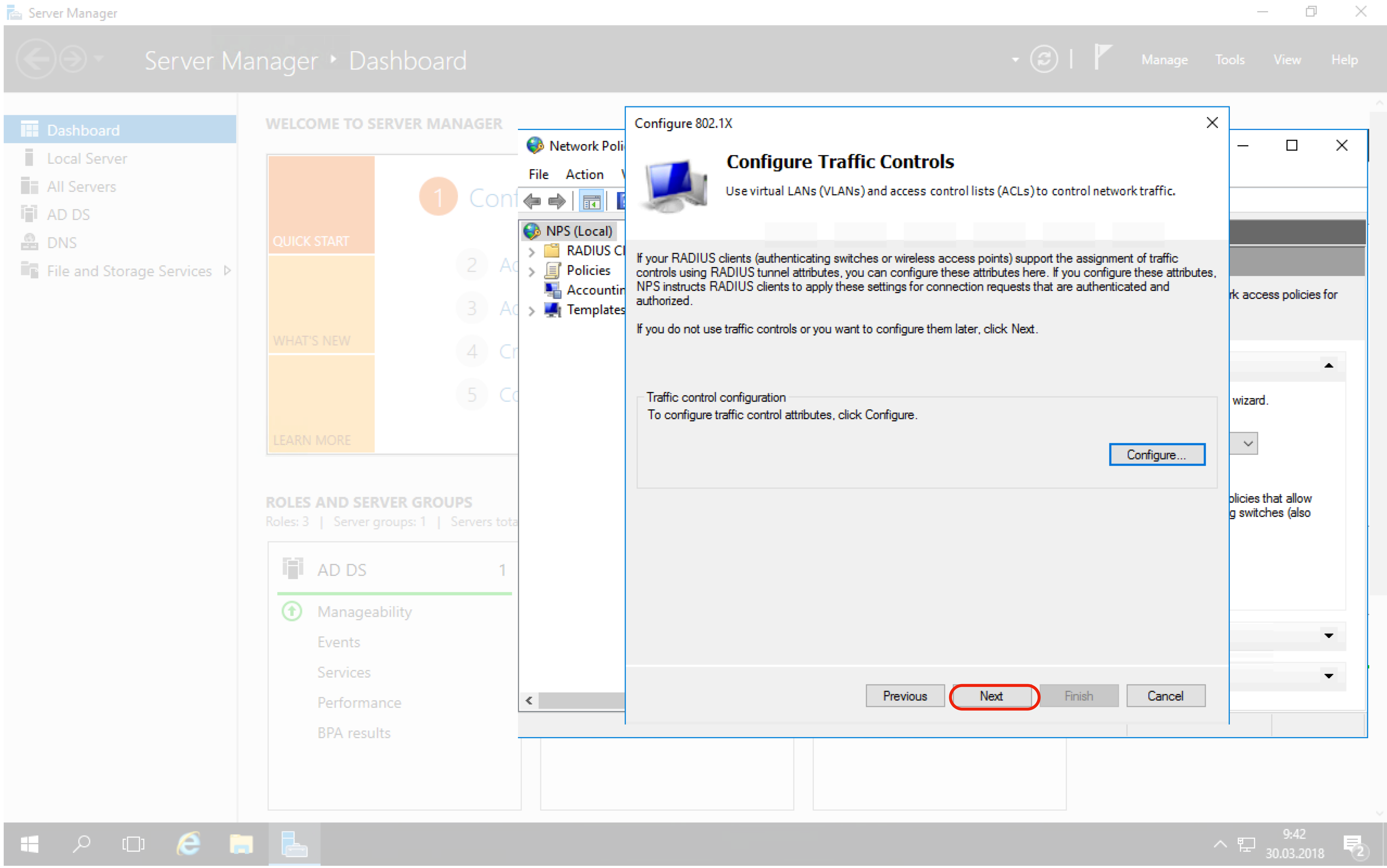
Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Groups
LAB0\Domain Users

Configure NPS - Radius

- Accept default and Click "Next"



Configure 802.1X

Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.

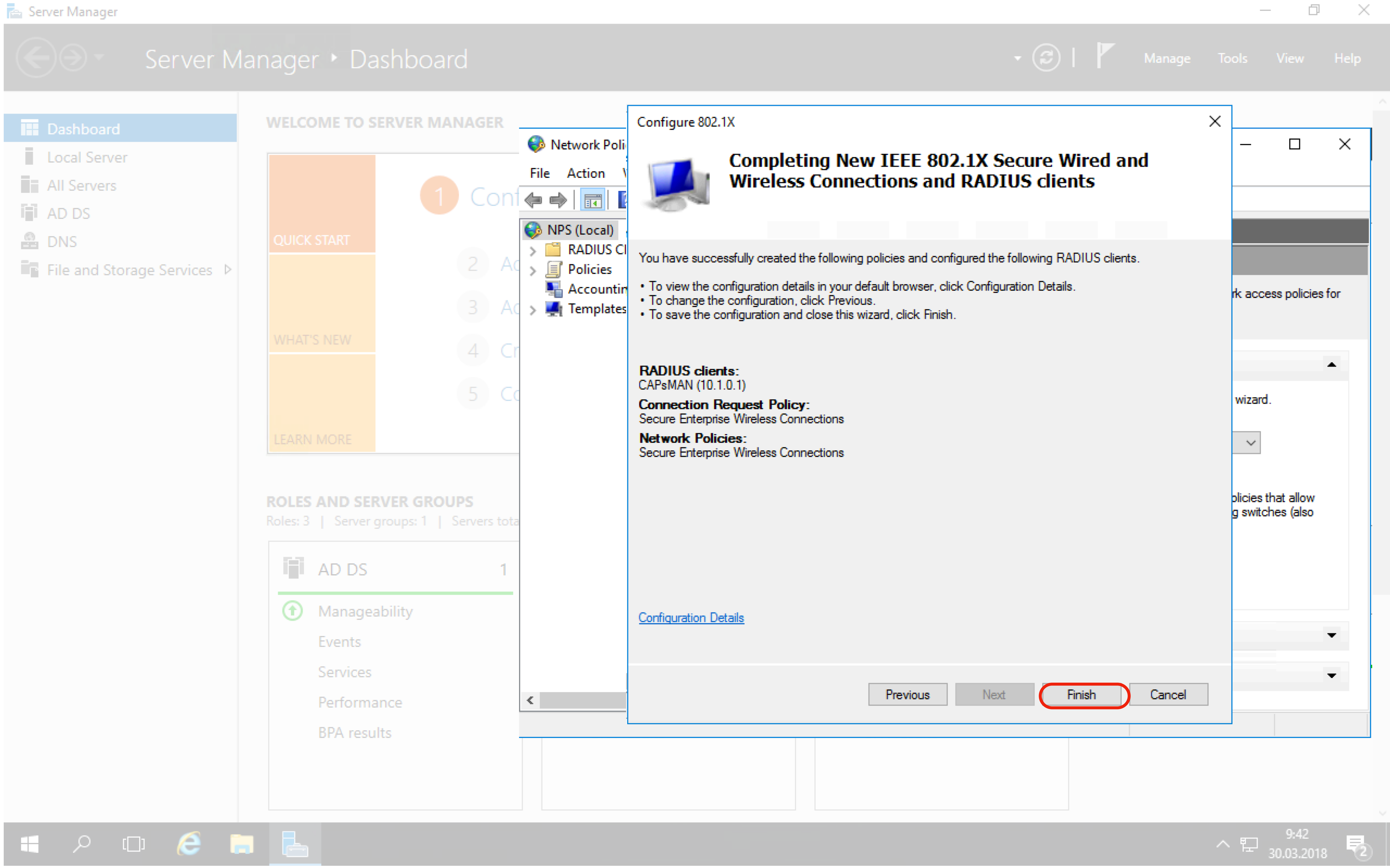
If you do not use traffic controls or you want to configure them later, click Next.

Traffic control configuration

To configure traffic control attributes, click Configure.

Configure NPS - Radius

- Review settings and click “Next”



Configure 802.1X

Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

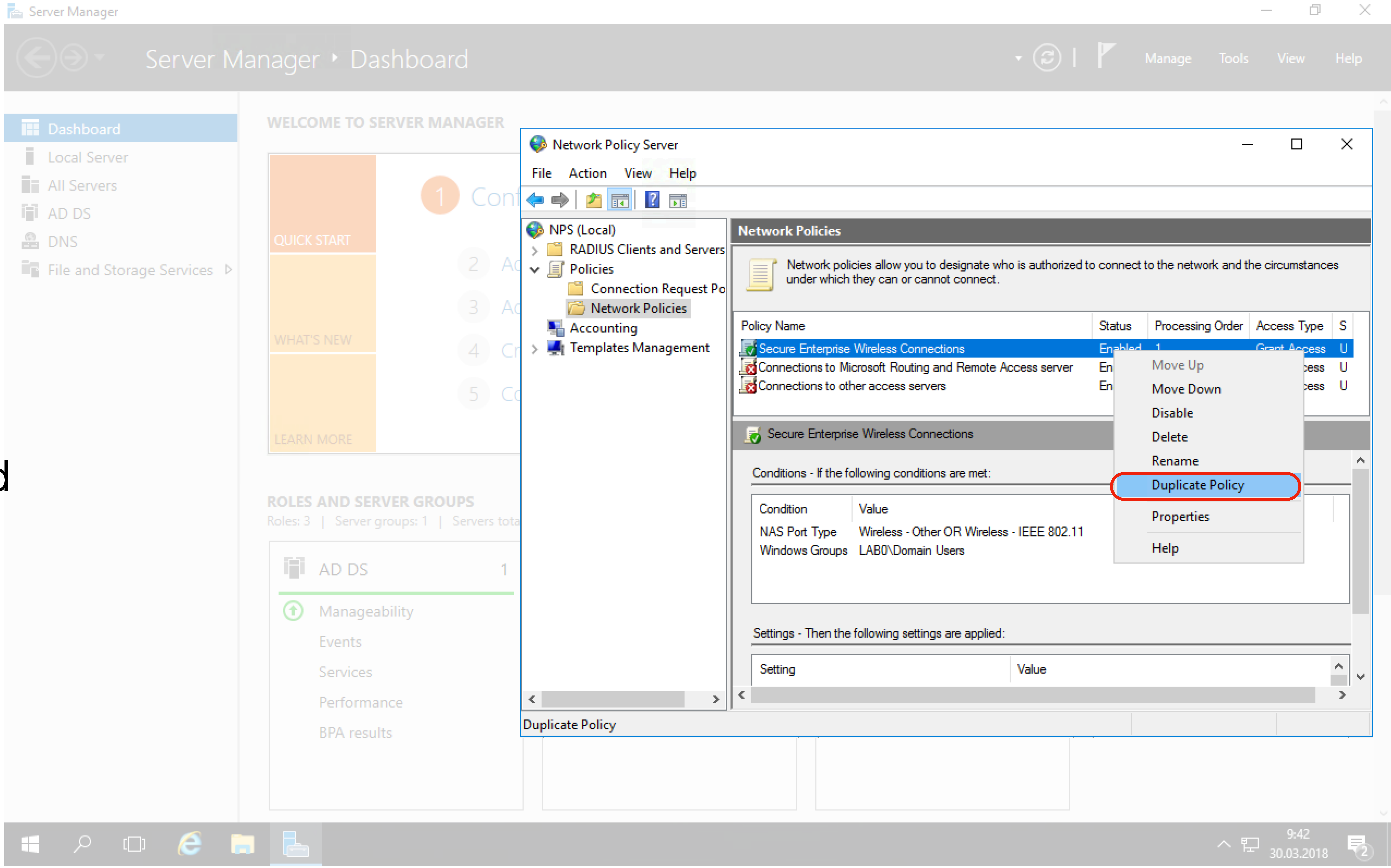
RADIUS clients:
CAPsMAN (10.1.0.1)

Connection Request Policy:
Secure Enterprise Wireless Connections

Network Policies:
Secure Enterprise Wireless Connections

Configure NPS - Radius

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



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	S
Secure Enterprise Wireless Connections	Enabled	1	Grant Access	U
Connections to Microsoft Routing and Remote Access server	En		cess	U
Connections to other access servers	En		cess	U

Secure Enterprise Wireless Connections

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	LAB0\Domain Users

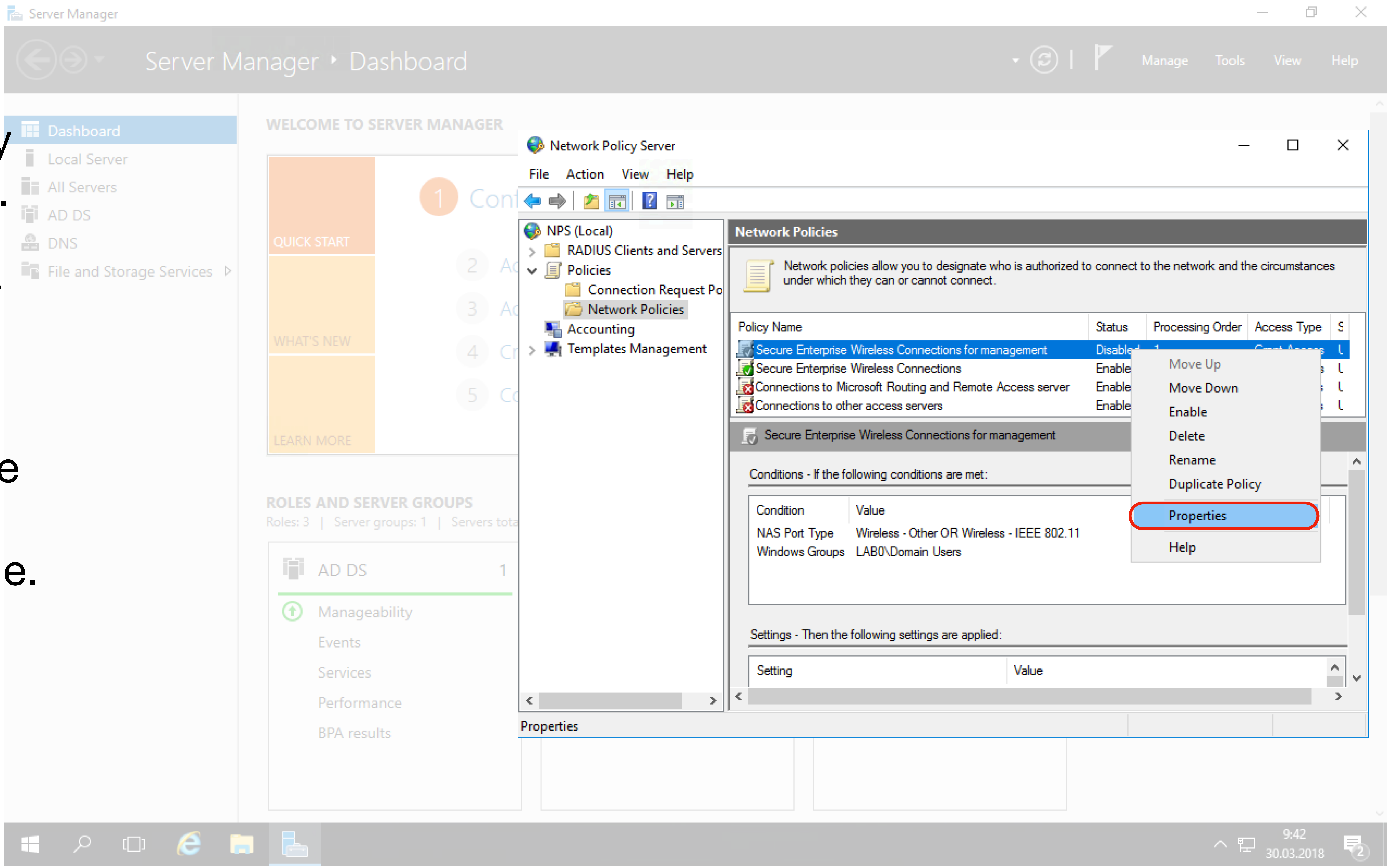
Settings - Then the following settings are applied:

Setting	Value

Duplicate 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”



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type
Secure Enterprise Wireless Connections for management	Disabled	1	Grant Access
Secure Enterprise Wireless Connections	Enable		
Connections to Microsoft Routing and Remote Access server	Enable		
Connections to other access servers	Enable		

Secure Enterprise Wireless Connections for management

Conditions - If the following conditions are met:

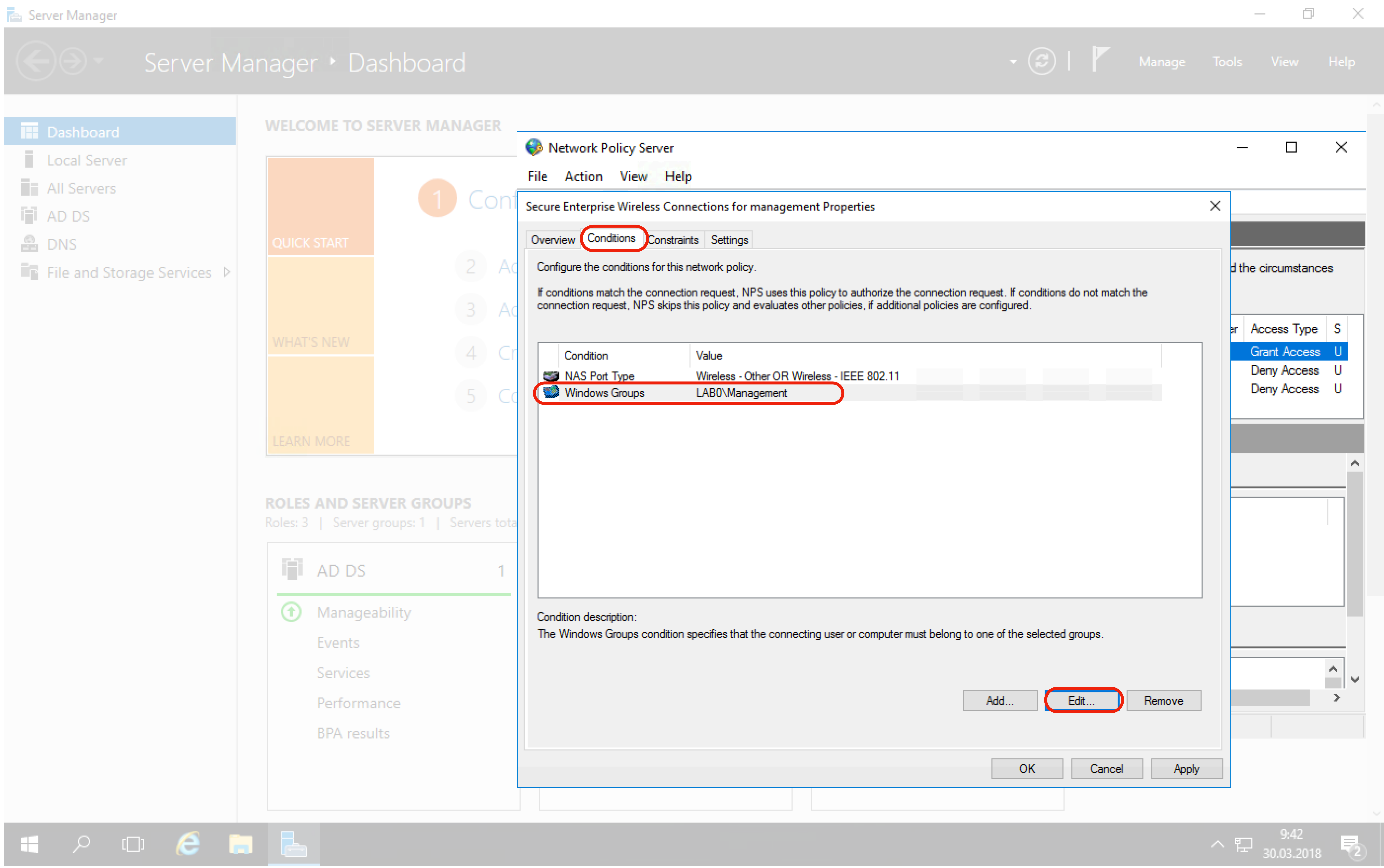
Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	LAB0\Domain Users

Settings - Then the following settings are applied:

Setting	Value

Configure NPS - Radius

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



Secure Enterprise Wireless Connections for management Properties

Configure the conditions for this network policy.

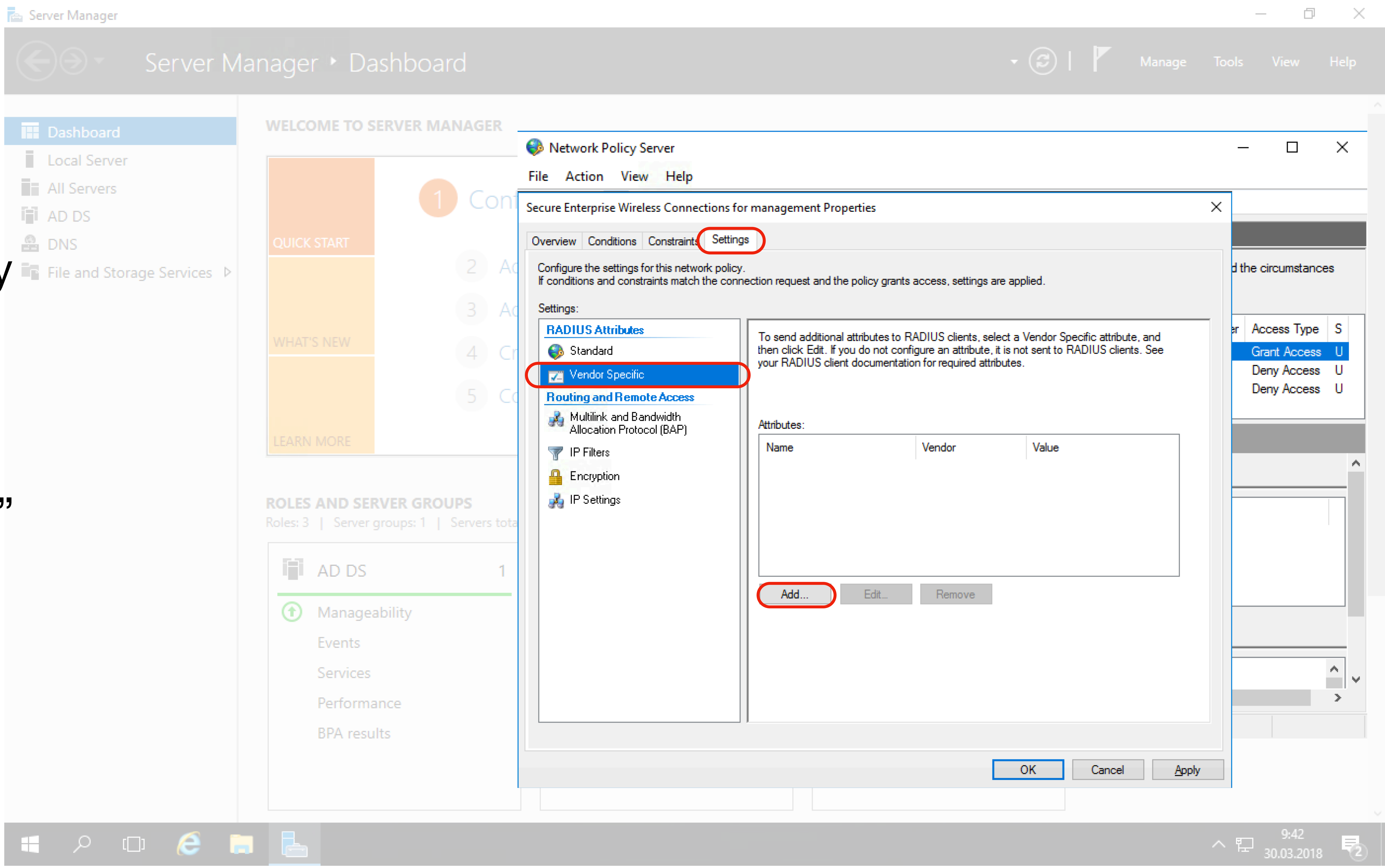
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	LAB0\Management

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

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”

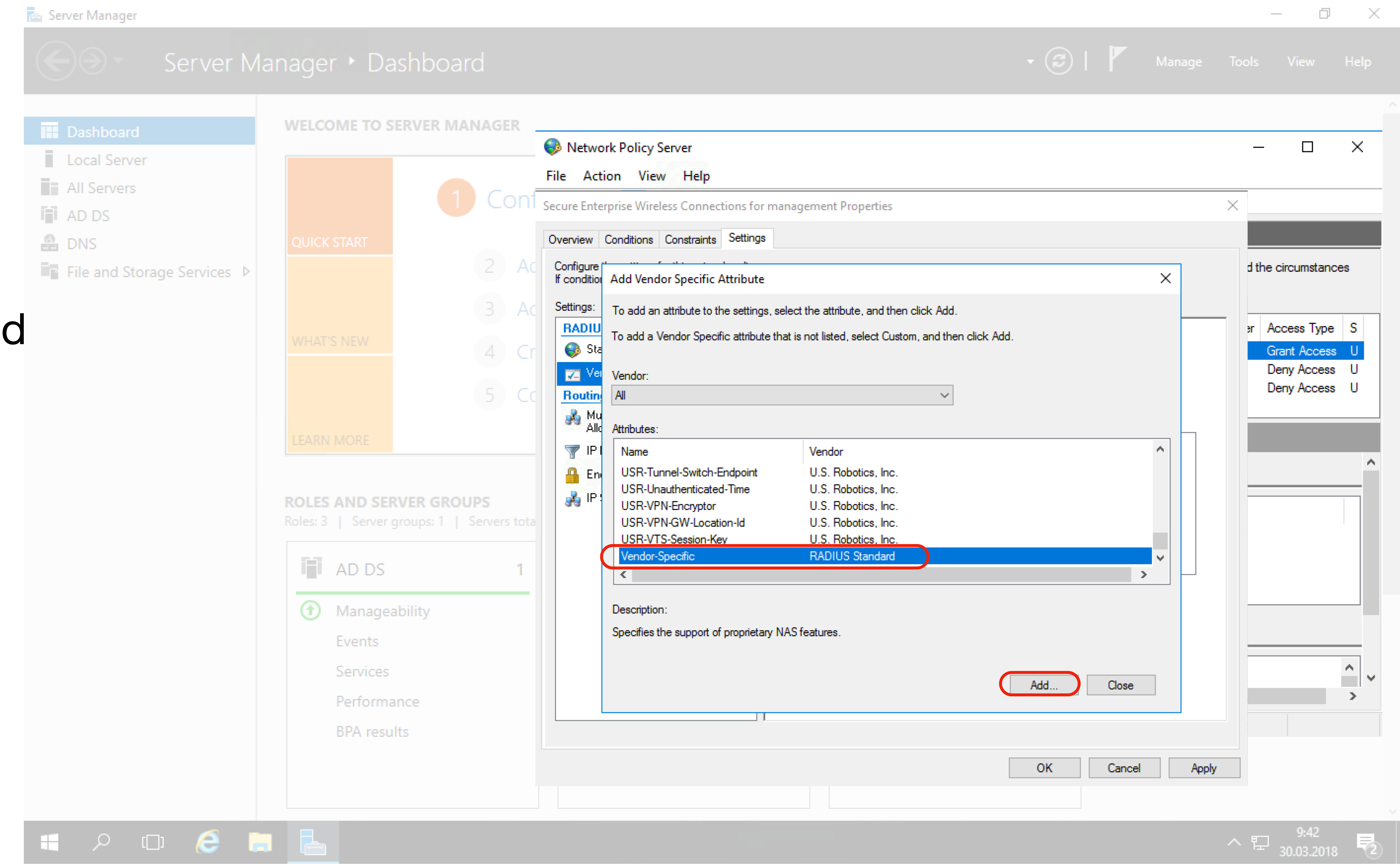


Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a Vendor Specific 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.

Configure NPS - Radius

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



Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor: All

Attributes:

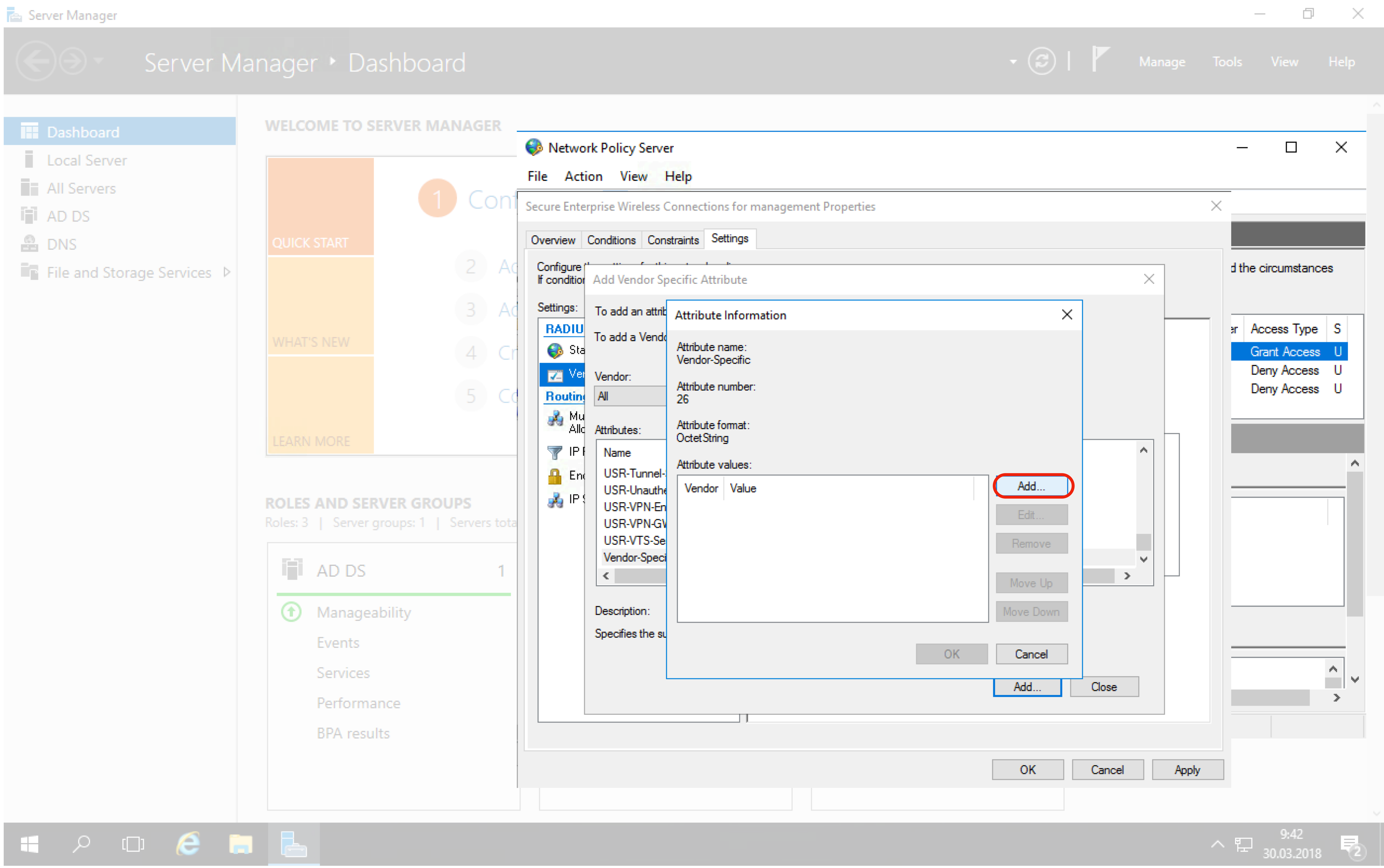
Name	Vendor
USR-Tunnel-Switch-Endpoint	U.S. Robotics, Inc.
USR-Unauthenticated-Time	U.S. Robotics, Inc.
USR-VPN-Encryptor	U.S. Robotics, Inc.
USR-VPN-GW-Location-Id	U.S. Robotics, Inc.
USR-VTS-Session-Key	U.S. Robotics, Inc.
Vendor-Specific	RADIUS Standard

Description:

Specifies the support of proprietary NAS features.

Configure NPS - Radius

- Click “Add”



Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

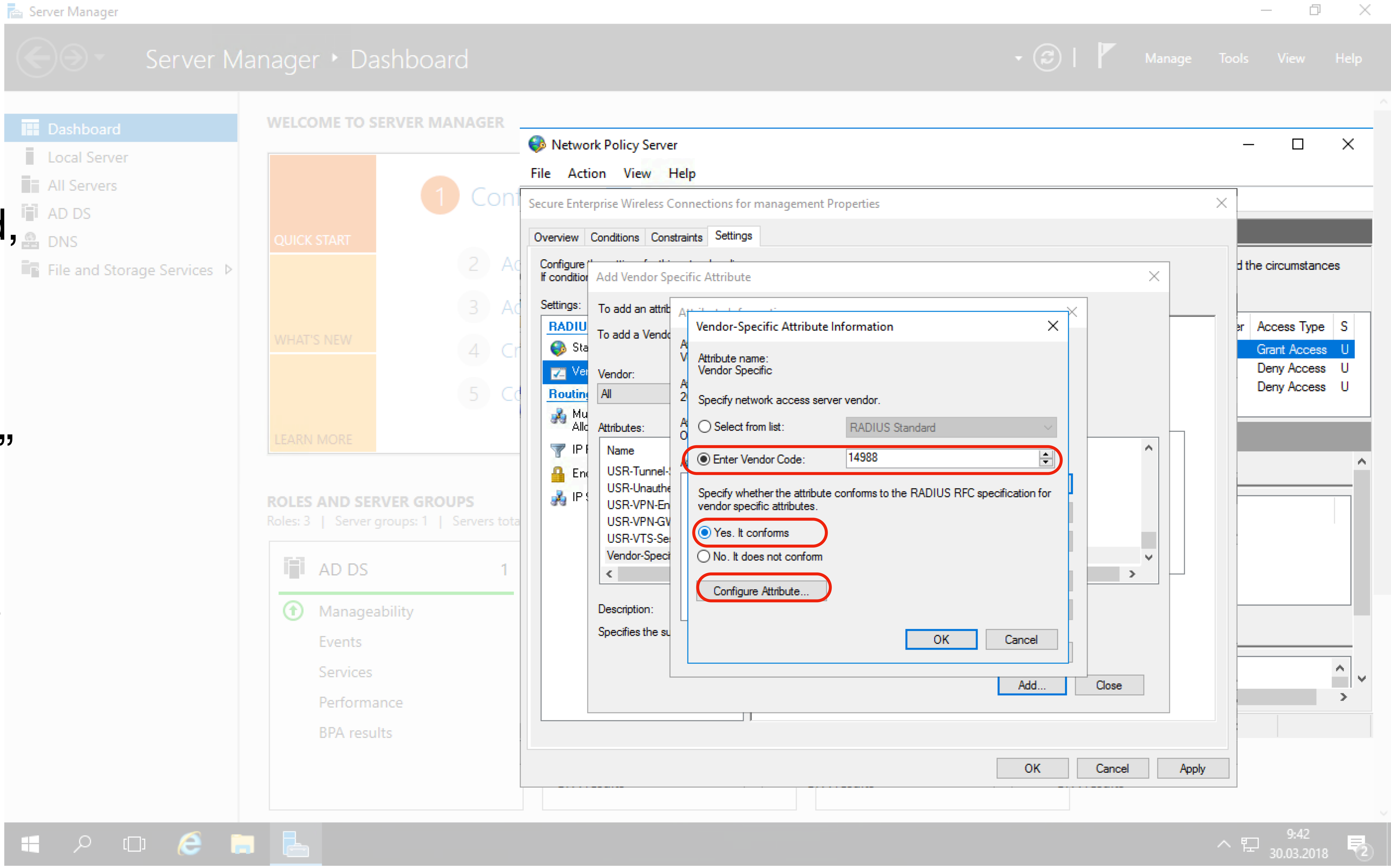
Attribute format:
OctetString

Attribute values:

Vendor	Value

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



Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 14988

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

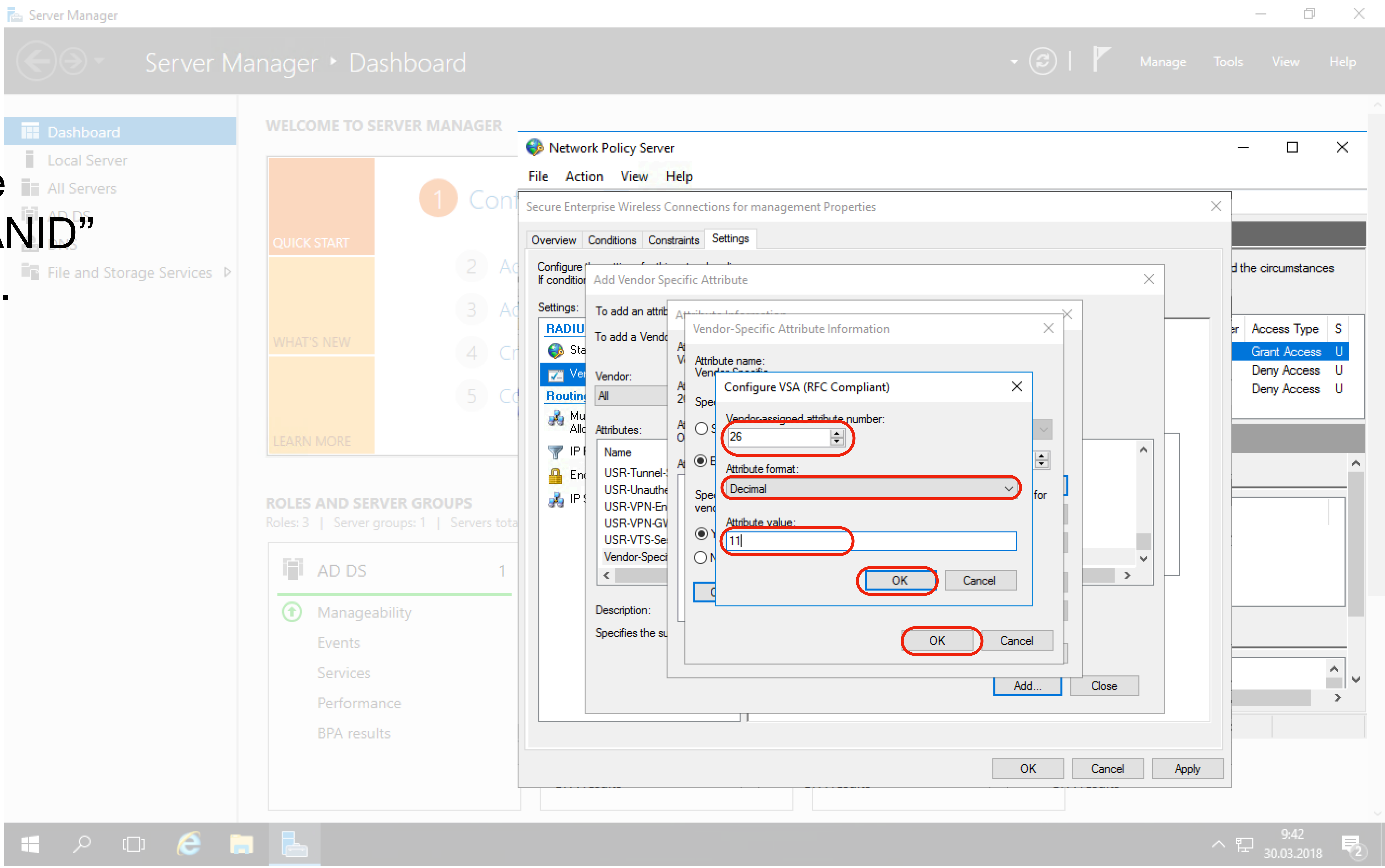
● Yes. It conforms

○ No. It does not conform

CCISRD
Center for Communication and Informationsecurity Research and Development

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 VSA (RFC Compliant)

Vendor-assigned attribute number: 26

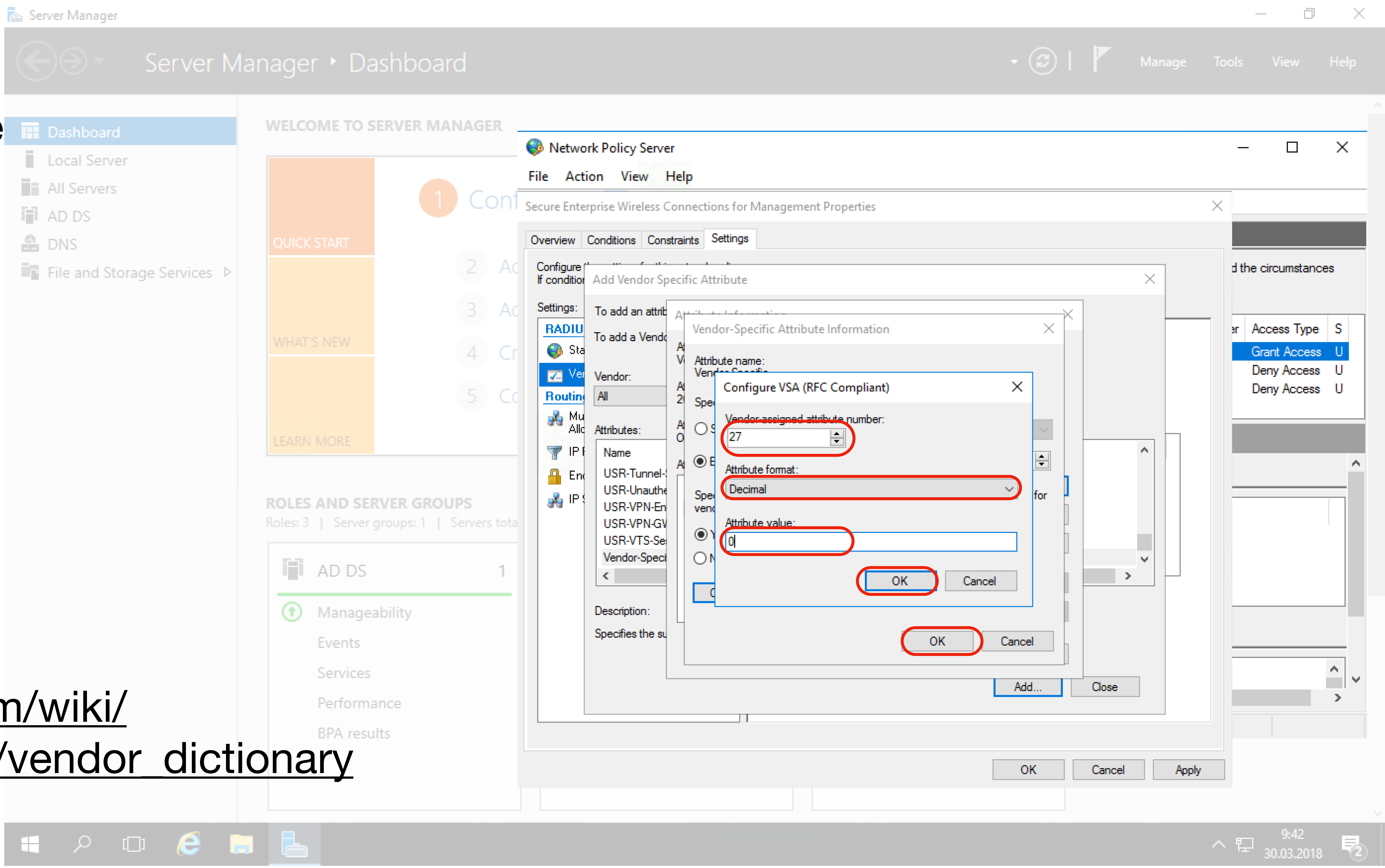
Attribute format: Decimal

Attribute value: 11

OK Cancel

Configure NPS - Radius

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



Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 27

Attribute format: Decimal

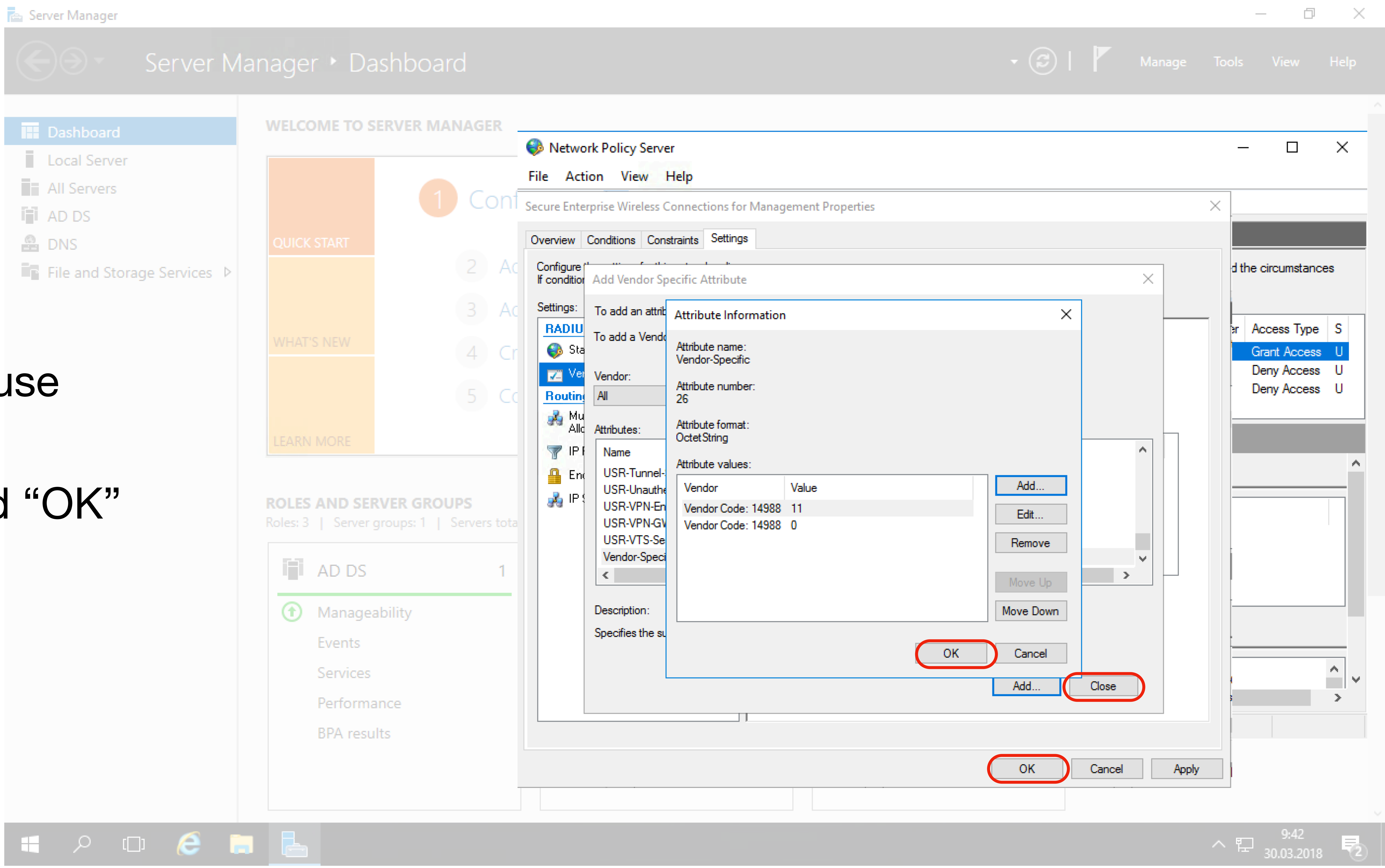
Attribute value: 0

OK Cancel

- 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”



Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

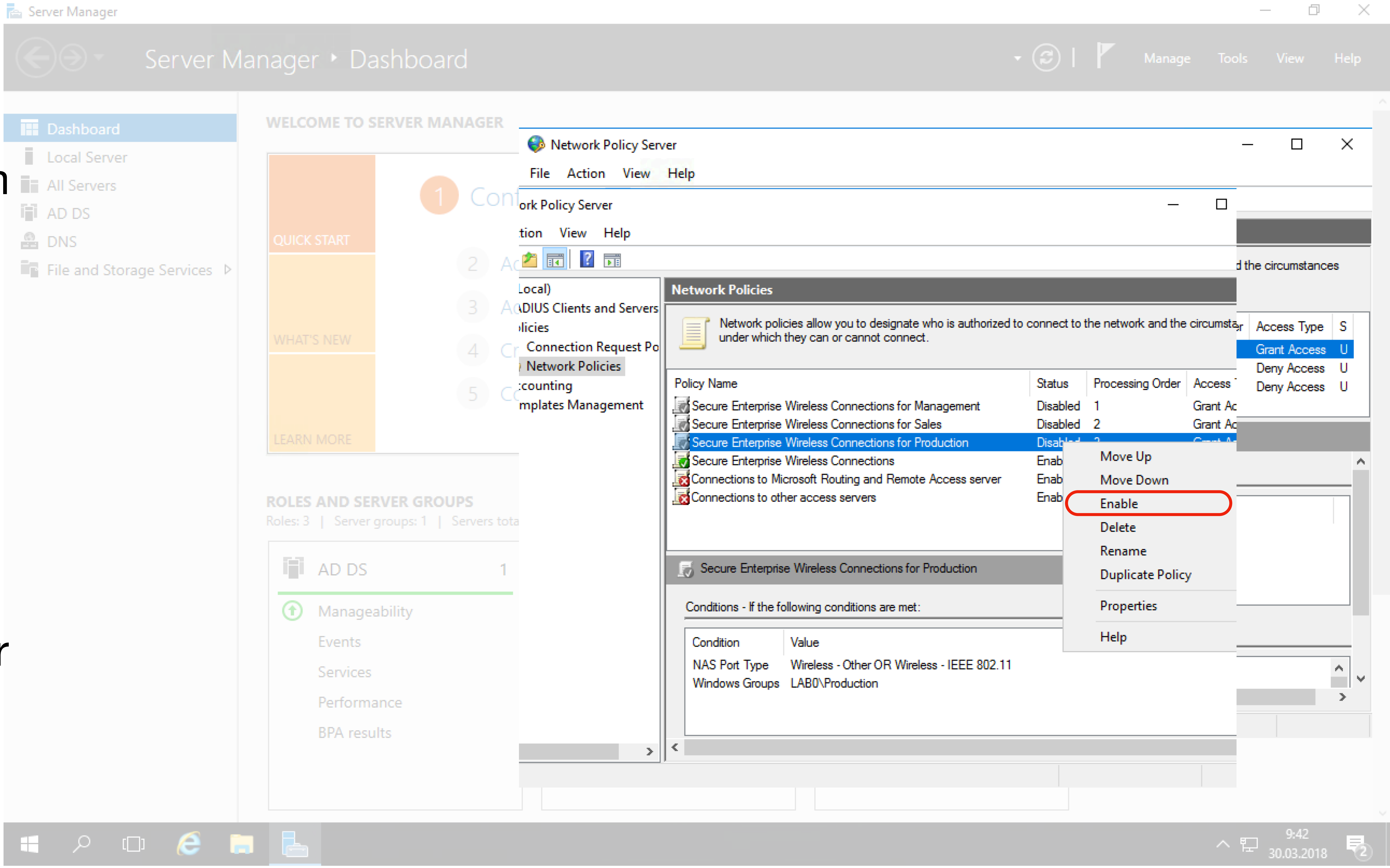
Attribute format:
OctetString

Attribute values:

Vendor	Value
Vendor Code: 14988	11
Vendor Code: 14988	0

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.



Network Policy Server

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access
Secure Enterprise Wireless Connections for Management	Disabled	1	Grant Ac
Secure Enterprise Wireless Connections for Sales	Disabled	2	Grant Ac
Secure Enterprise Wireless Connections for Production	Disabl		
Secure Enterprise Wireless Connections	Enab		
Connections to Microsoft Routing and Remote Access server	Enab		
Connections to other access servers	Enab		

Secure Enterprise Wireless Connections for Production

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	LAB0\Production

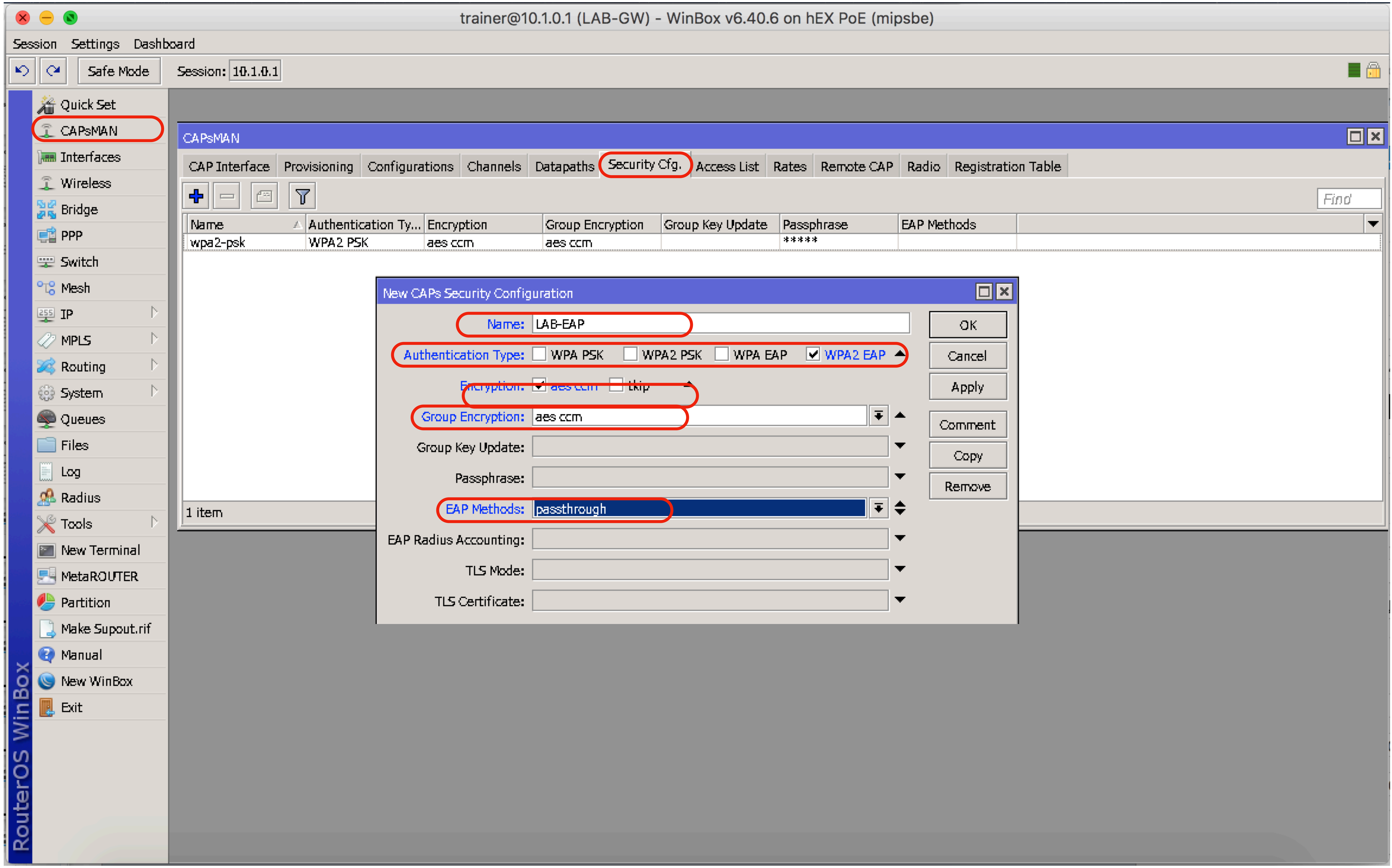
Access Type	S
Grant Access	U
Deny Access	U
Deny Access	U

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



trainer@10.1.0.1 (LAB-GW) - WinBox v6.40.6 on hEX PoE (mipsbe)

Session: 10.1.0.1

CAPsMAN

Name	Authentication Ty...	Encryption	Group Encryption	Group Key Update	Passphrase	EAP Methods
wpa2-psk	WPA2 PSK	aes ccm	aes ccm		*****	

1 item

New CAPs Security Configuration

Name: LAB-EAP

Authentication Type: □ WPA PSK □ WPA2 PSK □ WPA EAP ☑ WPA2 EAP

Encryption: ☑ aes ccm □ tkip

Group Encryption: aes ccm

Group Key Update:

Passphrase:

EAP Methods: passthrough

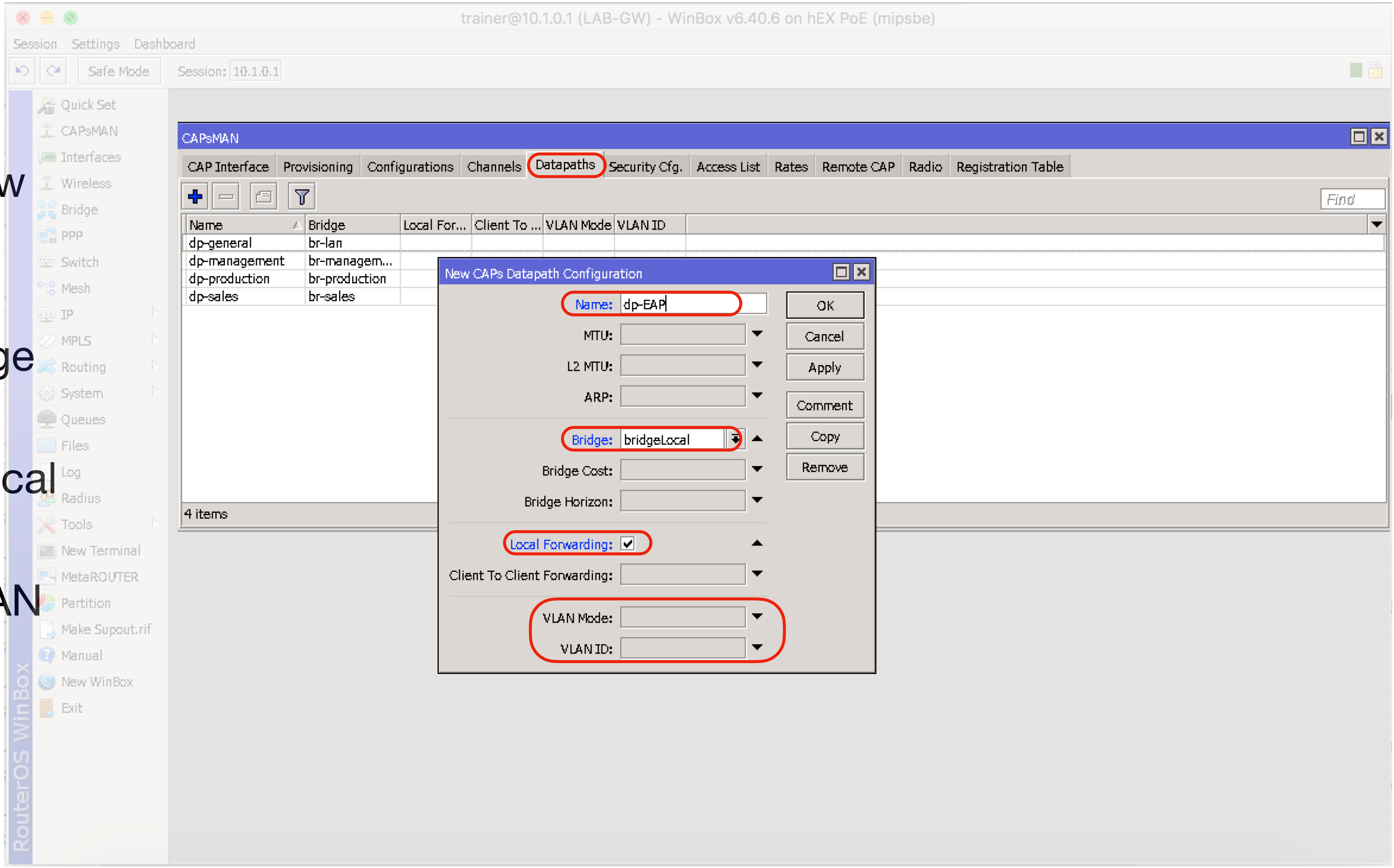
EAP Radius Accounting:

TLS Mode:

TLS Certificate:

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



Name	Bridge	Local For...	Client To ...	VLAN Mode	VLAN ID
dp-general	br-lan				
dp-management	br-managem...				
dp-production	br-production				
dp-sales	br-sales				

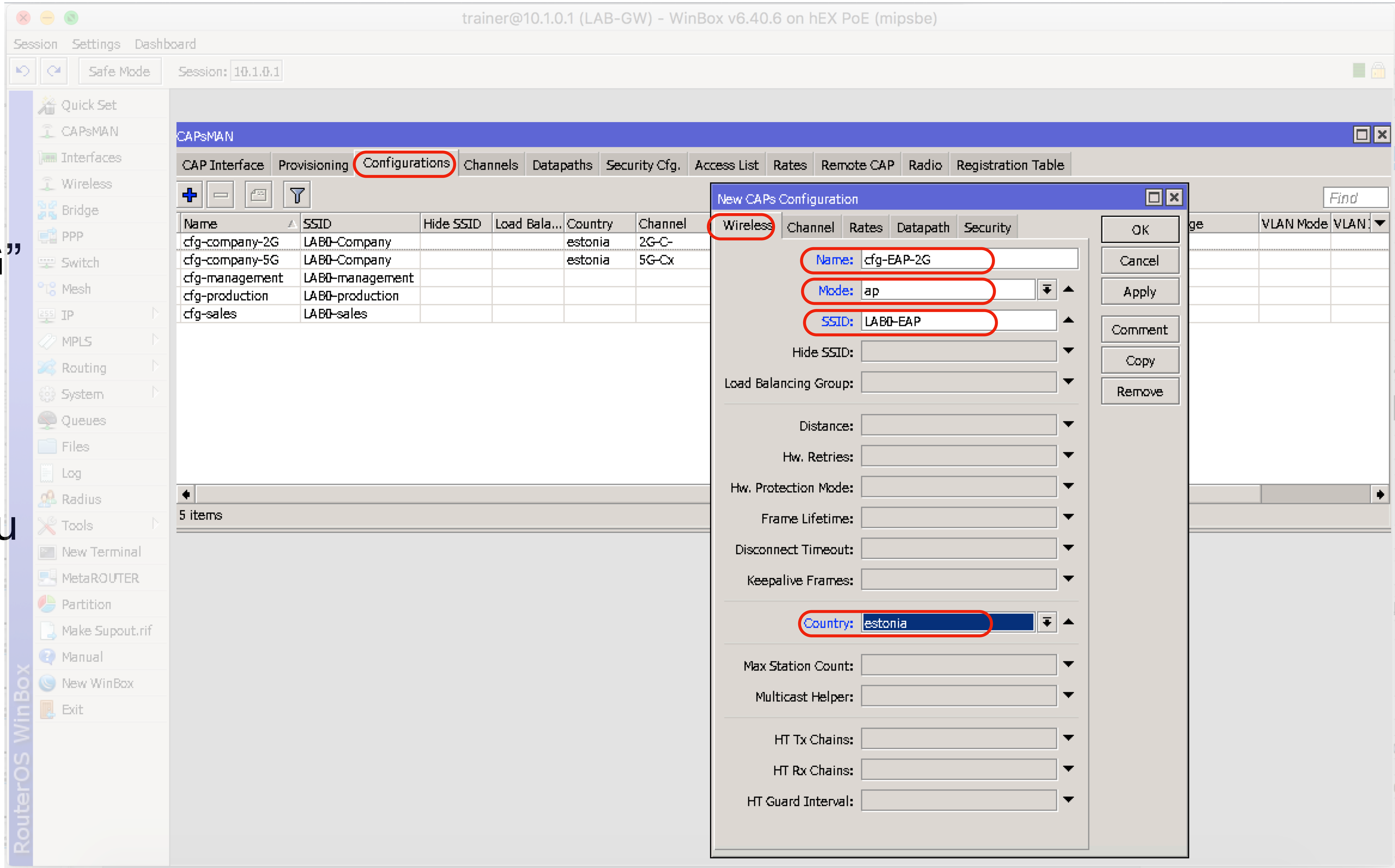
4 items

New CAPs Datapath Configuration

Name: dp-EAP
MTU:
L2 MTU:
ARP:
Bridge: bridgeLocal
Bridge Cost:
Bridge Horizon:
Local Forwarding: ☑
Client To Client Forwarding:
VLAN Mode:
VLAN ID:

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



Name	SSID	Hide SSID	Load Bala...	Country	Channel
cfg-company-2G	LAB0-Company			estonia	2G-C-
cfg-company-5G	LAB0-Company			estonia	5G-Cx
cfg-management	LAB0-management				
cfg-production	LAB0-production				
cfg-sales	LAB0-sales				

ge VLAN Mode VLAN I

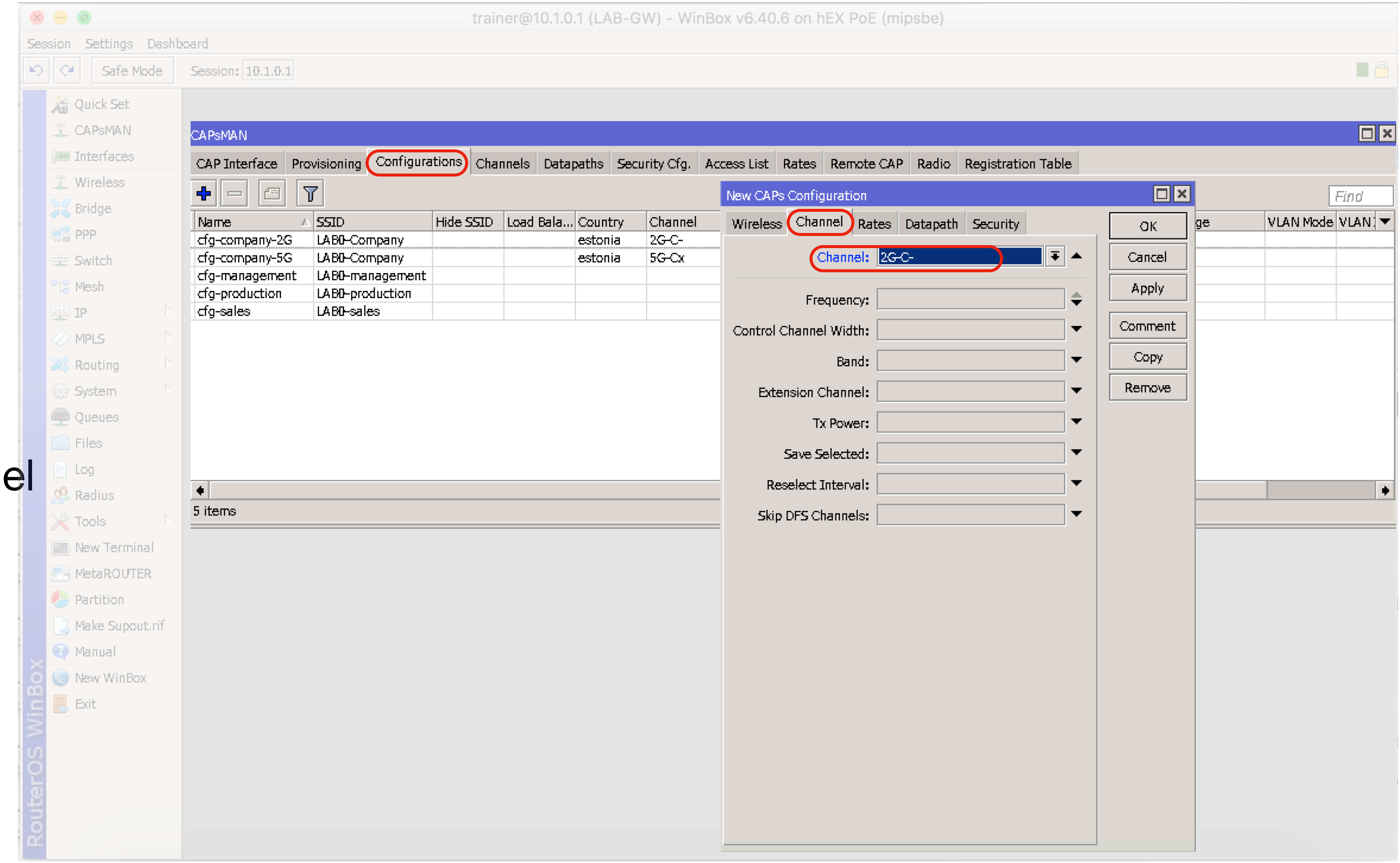
5 items

Name: cfg-EAP-2G
Mode: ap
SSID: LAB0-EAP
Hide SSID:
Load Balancing Group:
Distance:
Hw. Retries:
Hw. Protection Mode:
Frame Lifetime:
Disconnect Timeout:
Keepalive Frames:
Country: estonia
Max Station Count:
Multicast Helper:
HT Tx Chains:
HT Rx Chains:
HT Guard Interval:

Add New Configuration

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

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



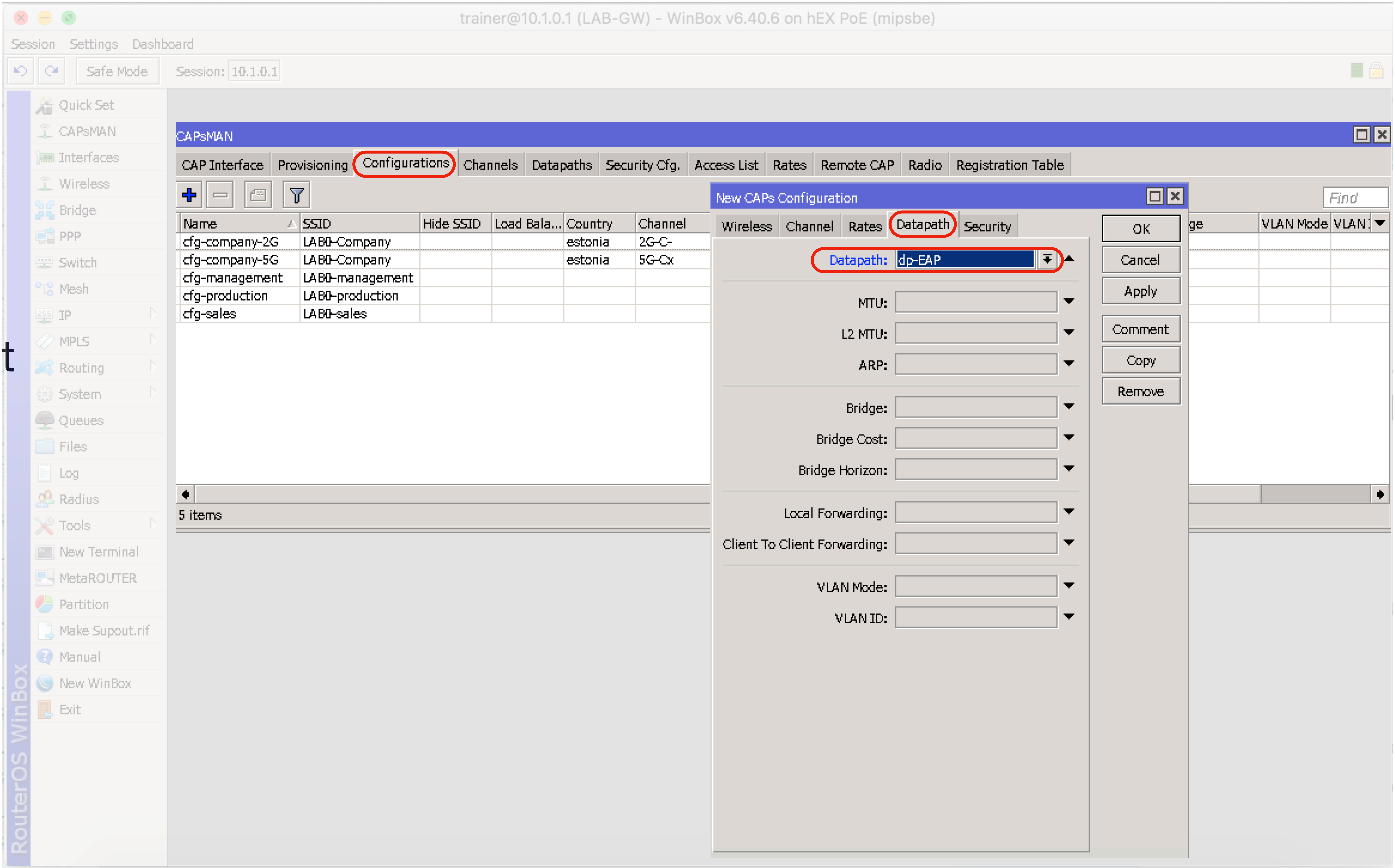
Name	SSID	Hide SSID	Load Bala...	Country	Channel
cfg-company-2G	LAB0-Company			estonia	2G-C-
cfg-company-5G	LAB0-Company			estonia	5G-Cx
cfg-management	LAB0-management				
cfg-production	LAB0-production				
cfg-sales	LAB0-sales				

5 items

Channel: 2G-C-
Frequency:
Control Channel Width:
Band:
Extension Channel:
Tx Power:
Save Selected:
Reselect Interval:
Skip DFS Channels:

Add New Configuration

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



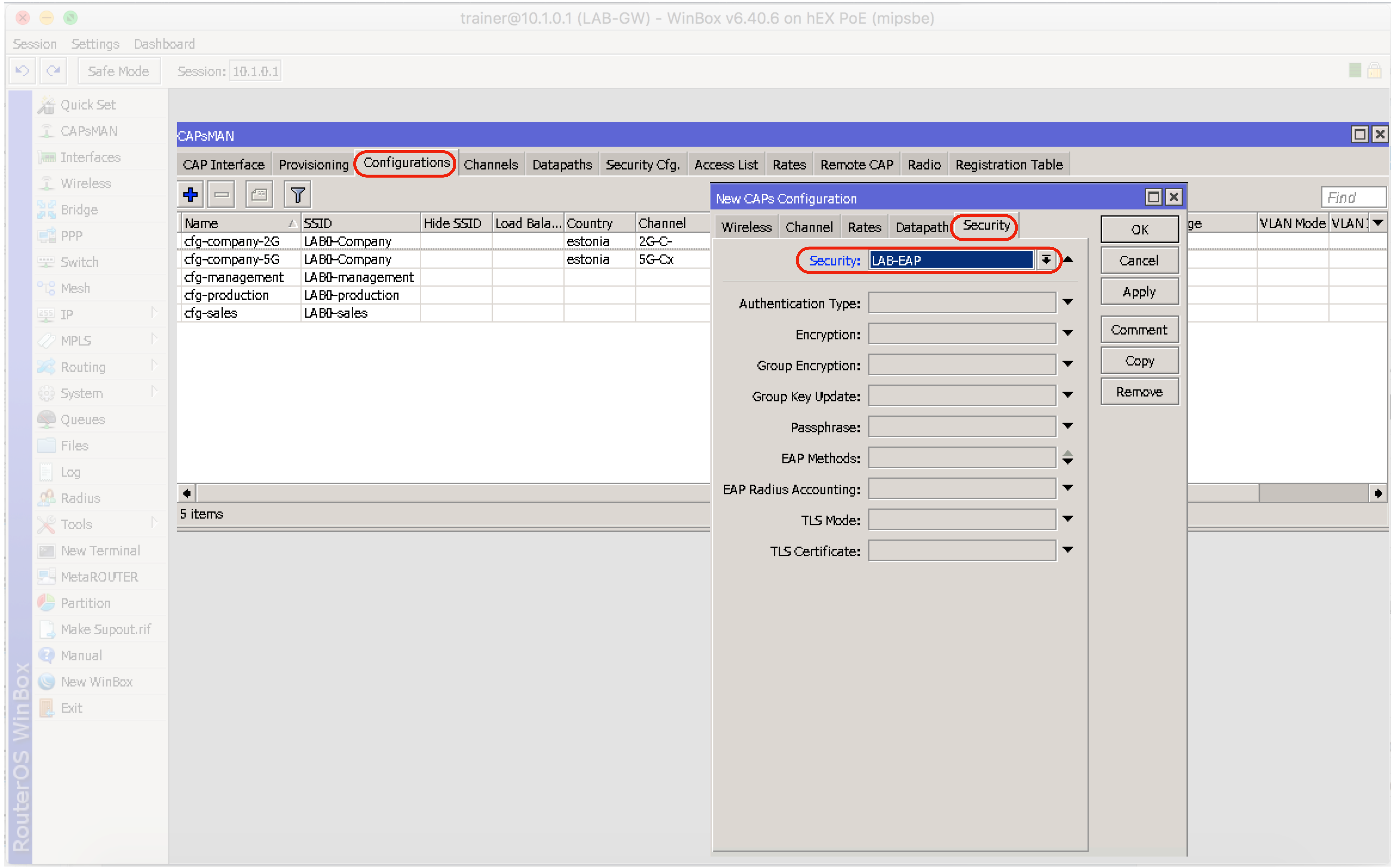
Name	SSID	Hide SSID	Load Bala...	Country	Channel
cfg-company-2G	LAB0-Company			estonia	2G-C-
cfg-company-5G	LAB0-Company			estonia	5G-Cx
cfg-management	LAB0-management				
cfg-production	LAB0-production				
cfg-sales	LAB0-sales				

5 items

Datapath: dp-EAP
MTU:
L2 MTU:
ARP:
Bridge:
Bridge Cost:
Bridge Horizon:
Local Forwarding:
Client To Client Forwarding:
VLAN Mode:
VLAN ID:

Add New Configuration

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



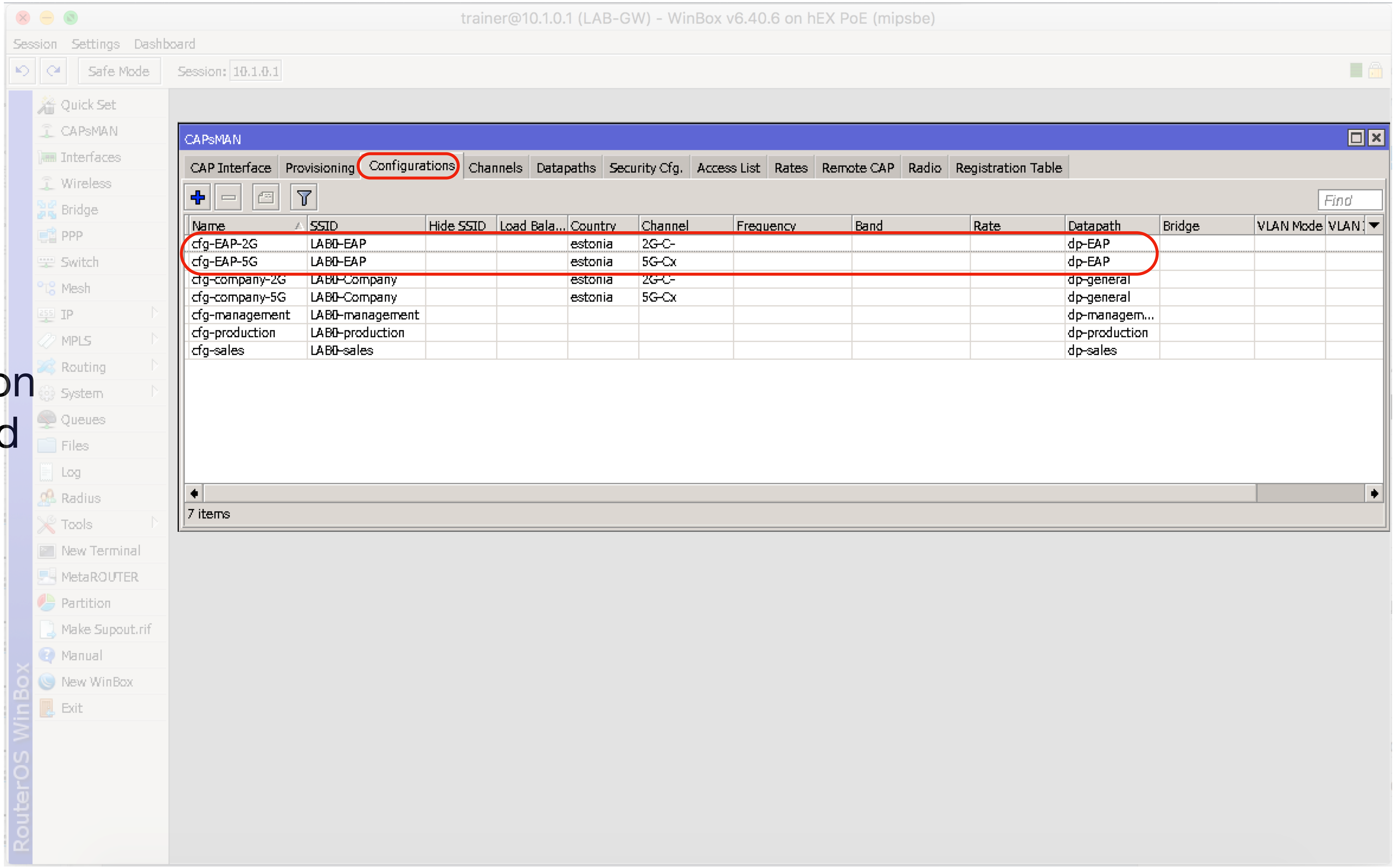
Name	SSID	Hide SSID	Load Bala...	Country	Channel
cfg-company-2G	LAB0-Company			estonia	2G-C-
cfg-company-5G	LAB0-Company			estonia	5G-Cx
cfg-management	LAB0-management				
cfg-production	LAB0-production				
cfg-sales	LAB0-sales				

5 items

Security: LAB-EAP
Authentication Type:
Encryption:
Group Encryption:
Group Key Update:
Passphrase:
EAP Methods:
EAP Radius Accounting:
TLS Mode:
TLS Certificate:

Add New Configuration

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

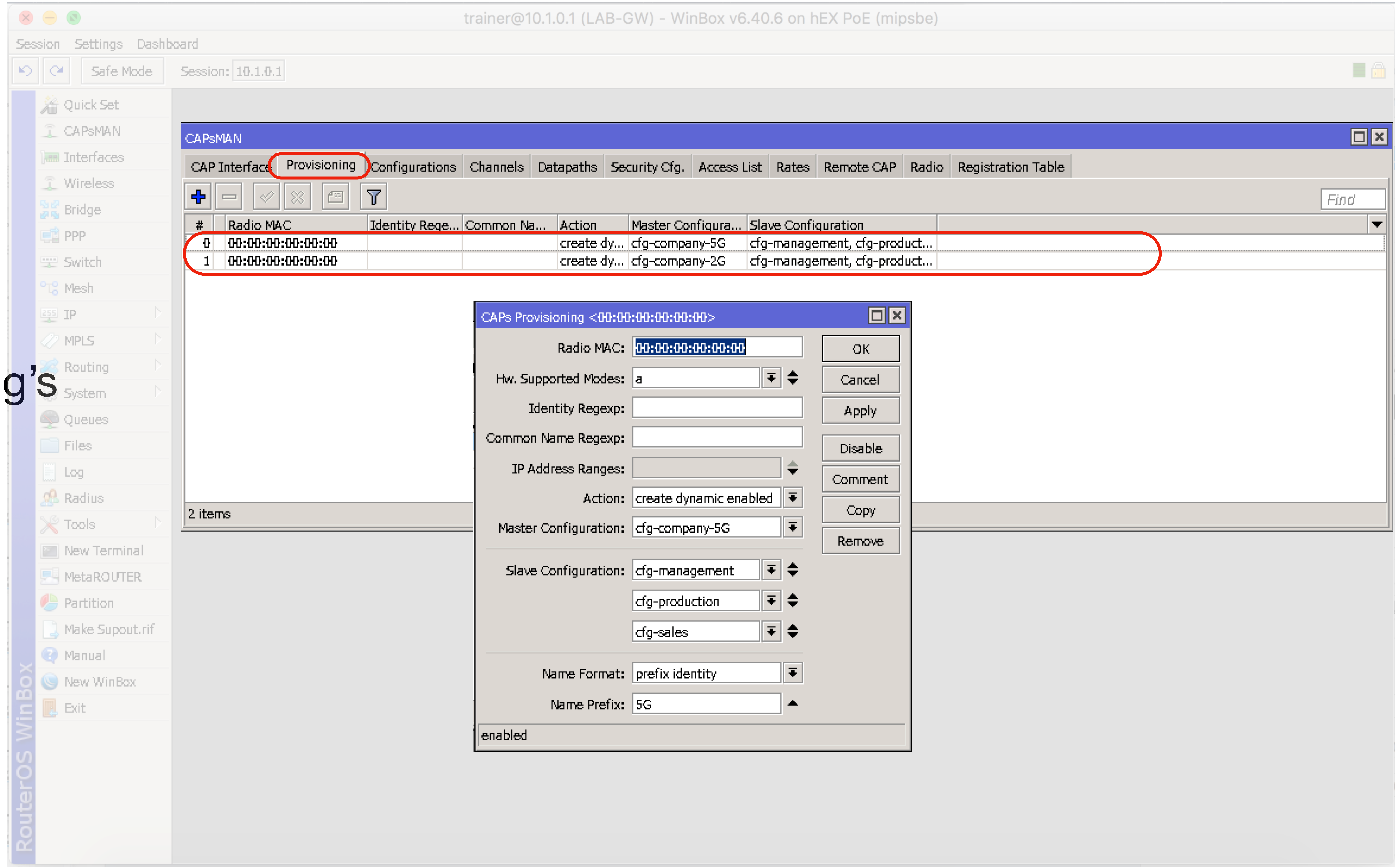


Name	SSID	Hide SSID	Load Bala...	Country	Channel	Frequency	Band	Rate	Datapath	Bridge	VLAN Mode	VLAN I
cfg-EAP-2G	LAB0-EAP			estonia	2G-C-				dp-EAP			
cfg-EAP-5G	LAB0-EAP			estonia	5G-Cx				dp-EAP			
cfg-company-2G	LAB0-Company			estonia	2G-C-				dp-general			
cfg-company-5G	LAB0-Company			estonia	5G-Cx				dp-general			
cfg-management	LAB0-management								dp-managem...			
cfg-production	LAB0-production								dp-production			
cfg-sales	LAB0-sales								dp-sales			

7 items

Update Provisioning’s

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



#	Radio MAC	Identity Rege...	Common Na...	Action	Master Configura...	Slave Configuration
0	00:00:00:00:00:00			create dy...	cfg-company-5G	cfg-management, cfg-product...
1	00:00:00:00:00:00			create dy...	cfg-company-2G	cfg-management, cfg-product...

2 items

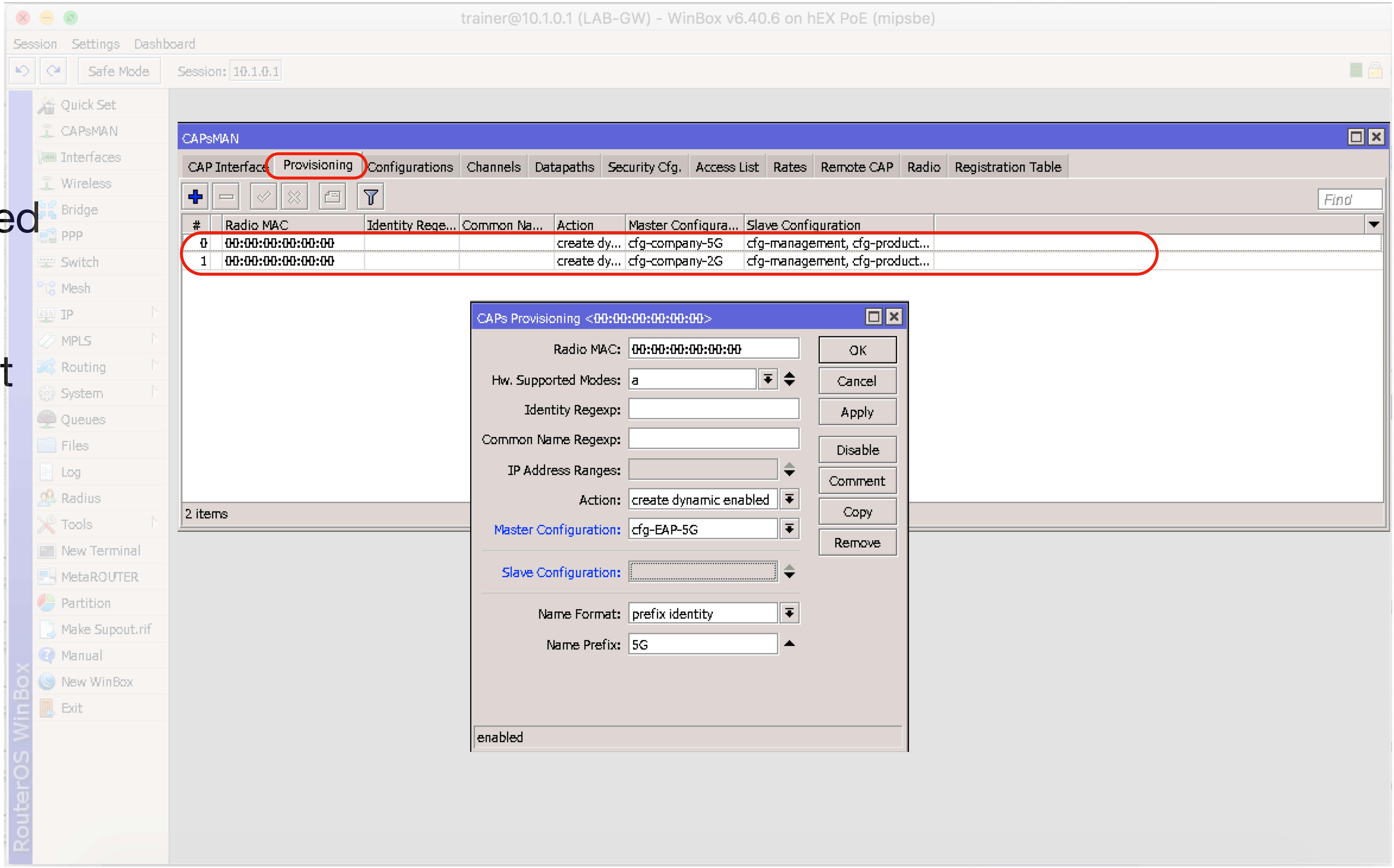
CAPs Provisioning <00:00:00:00:00:00>

Radio MAC: 00:00:00:00:00:00
Hw. Supported Modes: a
Identity Regexp:
Common Name Regexp:
IP Address Ranges:
Action: create dynamic enabled
Master Configuration: cfg-company-5G
Slave Configuration: cfg-management
cfg-production
cfg-sales
Name Format: prefix identity
Name Prefix: 5G

enabled

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



#	Radio MAC	Identity Rege...	Common Na...	Action	Master Configura...	Slave Configuration
0	00:00:00:00:00:00			create dy...	cfg-company-5G	cfg-management, cfg-product...
1	00:00:00:00:00:00			create dy...	cfg-company-2G	cfg-management, cfg-product...

2 items

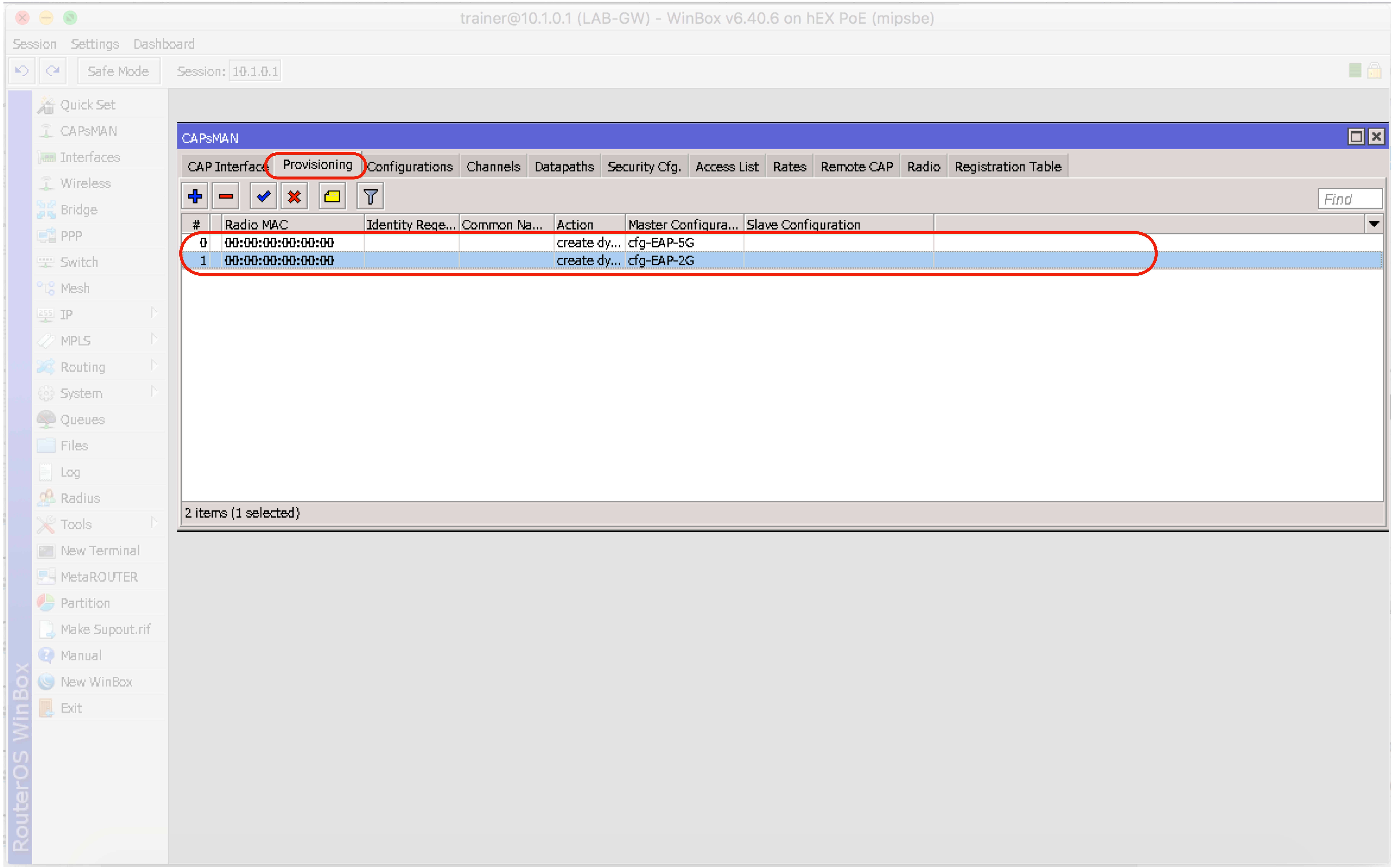
CAPs Provisioning <00:00:00:00:00:00>

Radio MAC: 00:00:00:00:00:00
Hw. Supported Modes: a
Identity Regexp:
Common Name Regexp:
IP Address Ranges:
Action: create dynamic enabled
Master Configuration: cfg-EAP-5G
Slave Configuration:
Name Format: prefix identity
Name Prefix: 5G

enabled

Provisioning

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

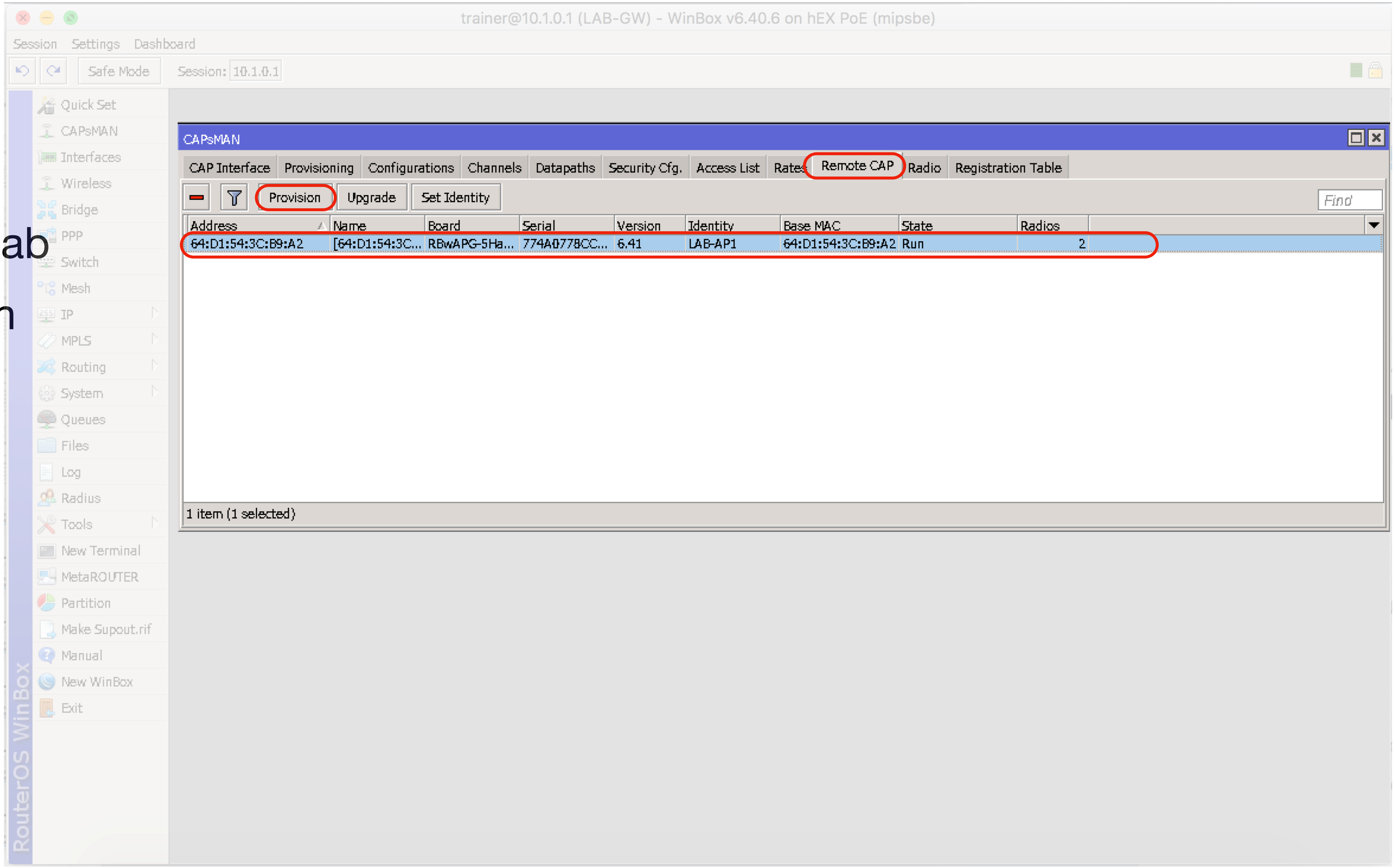


#	Radio MAC	Identity Rege...	Common Na...	Action	Master Configura...	Slave Configuration
0	00:00:00:00:00:00			create dy...	cfg-EAP-5G	
1	00:00:00:00:00:00			create dy...	cfg-EAP-2G	

2 items (1 selected)

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

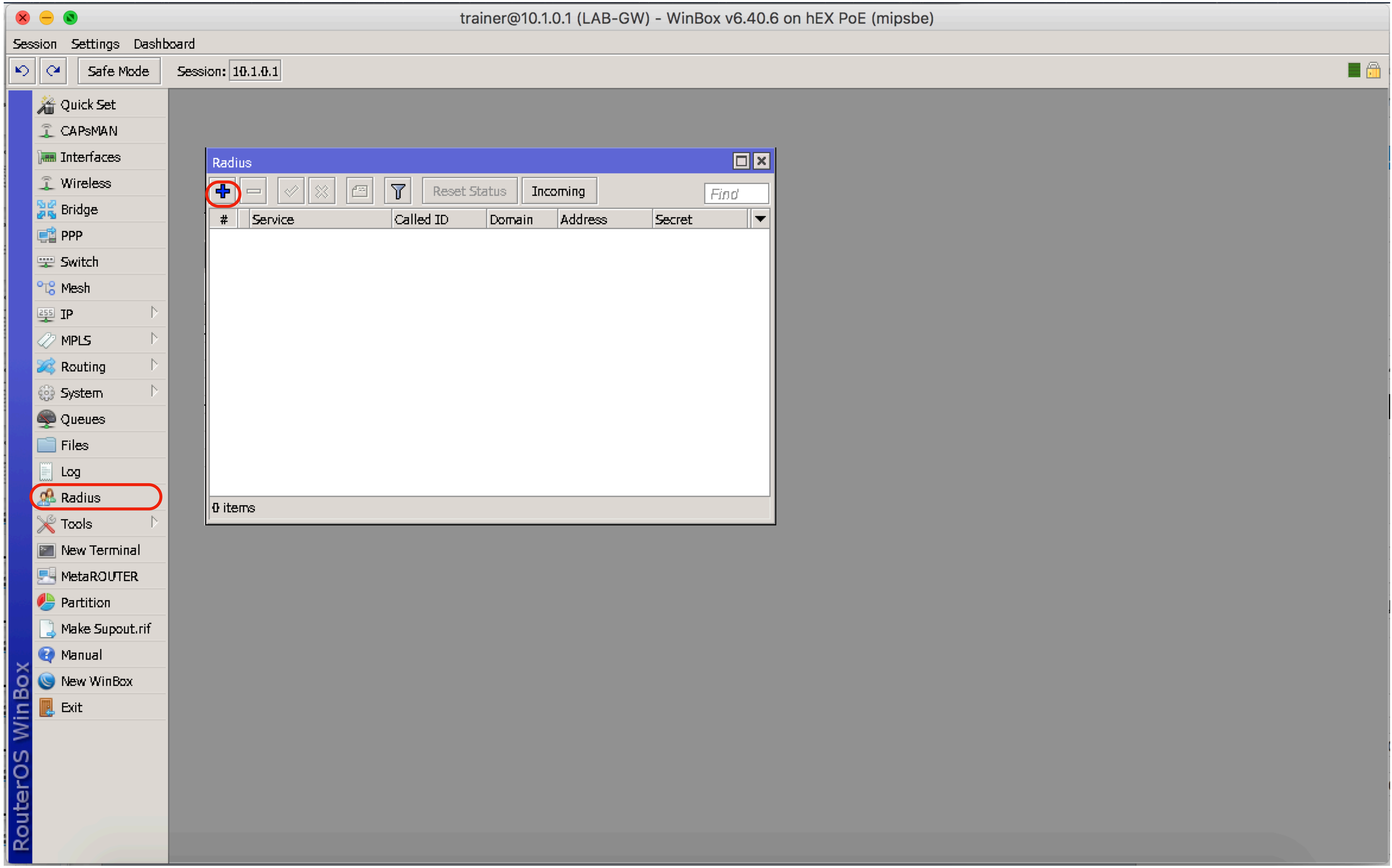


Address	Name	Board	Serial	Version	Identity	Base MAC	State	Radios
64:D1:54:3C:B9:A2	[64:D1:54:3C...	RBwAPG-5Ha...	774A0778CC...	6.41	LAB-AP1	64:D1:54:3C:B9:A2	Run	2

1 item (1 selected)

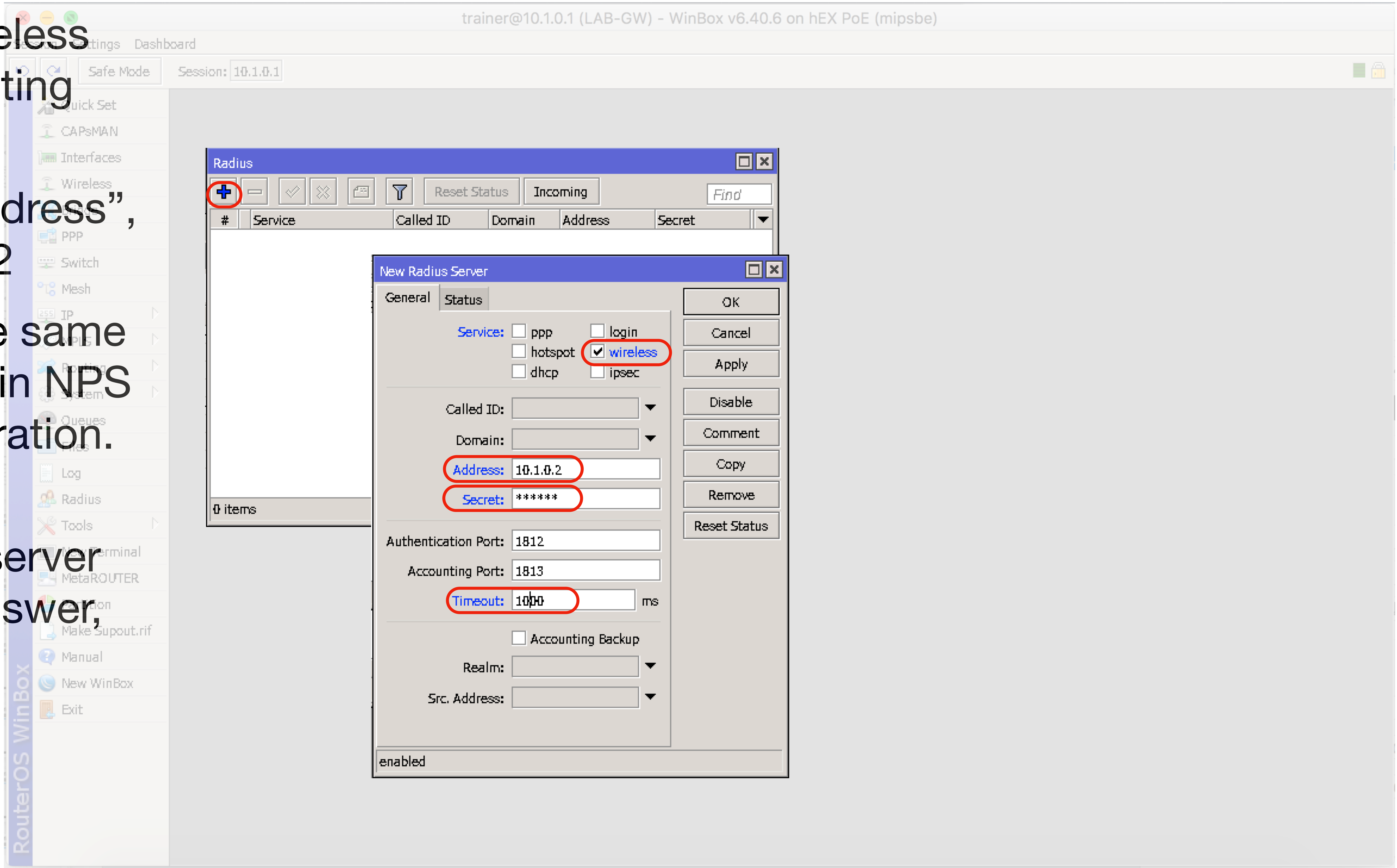
Configure RADIUS Client

- 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.



trainer@10.1.0.1 (LAB-GW) - WinBox v6.40.6 on hEX PoE (mipsbe)

Radius

#	Service	Called ID	Domain	Address	Secret

0 items

New Radius Server

Service: □ ppp ☐ login
□ hotspot ☑ wireless
□ dhcp □ ipsec

Called ID:

Domain:

Address: 10.1.0.2

Secret: ******

Authentication Port: 1812

Accounting Port: 1813

Timeout: 1000 ms

□ Accounting Backup

Realm:

Src. Address:

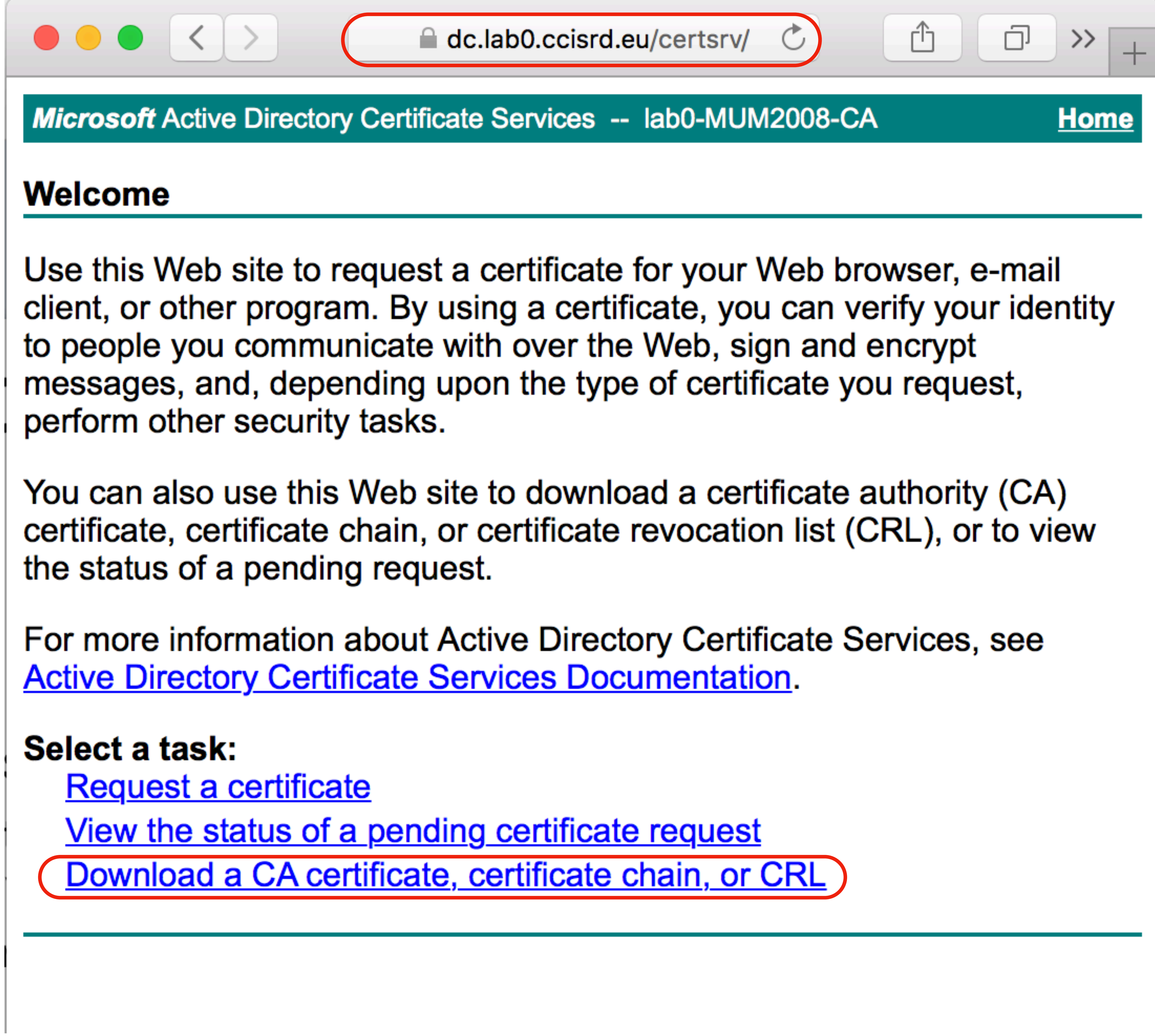
enabled

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.



Microsoft Active Directory Certificate Services -- lab0-MUM2008-CA **Home**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

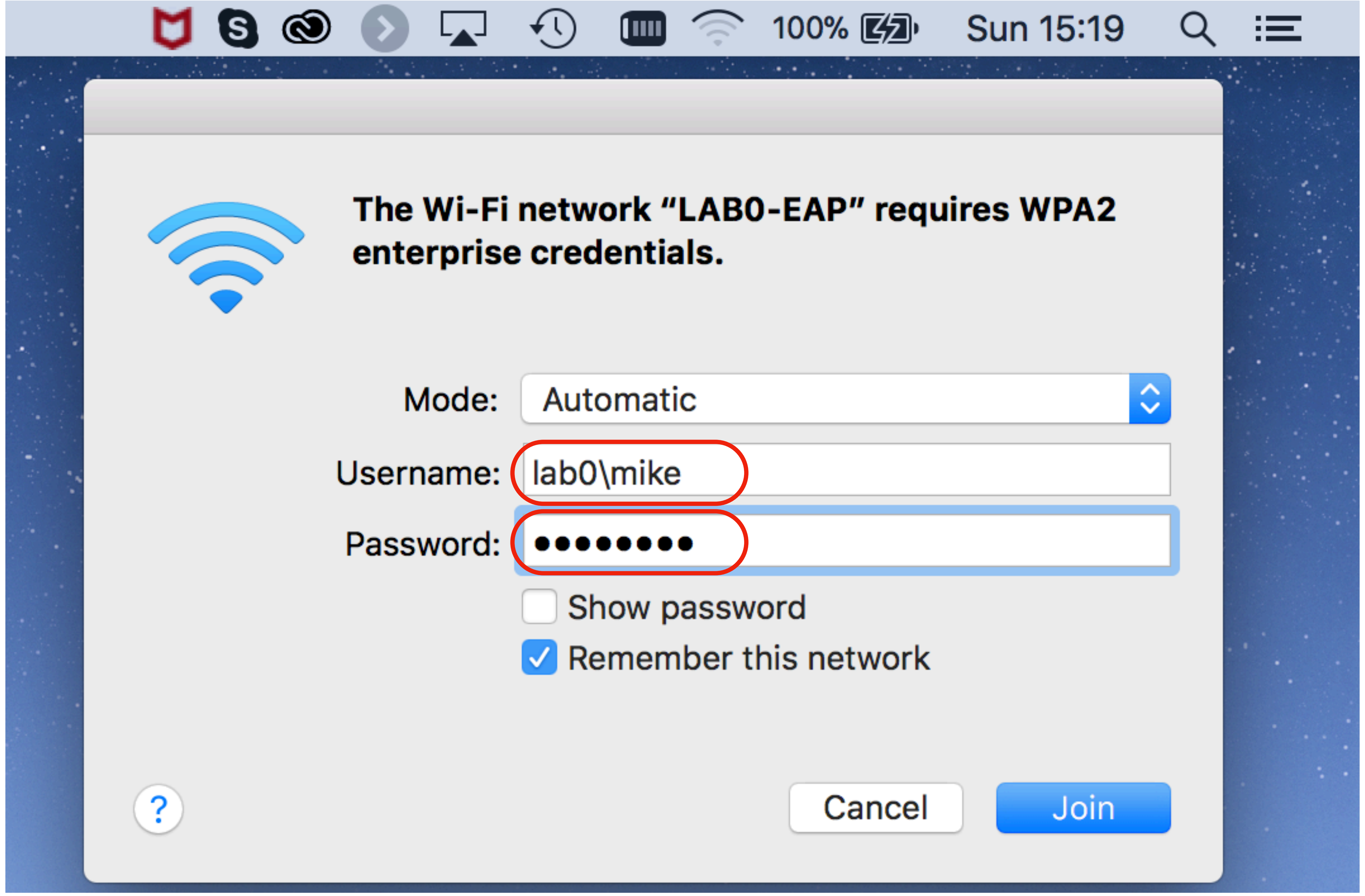
Request a certificate

View the status of a pending certificate request

Download a CA certificate, certificate chain, or CRL

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.



The Wi-Fi network “LAB0-EAP” requires WPA2 enterprise credentials.

Mode: Automatic

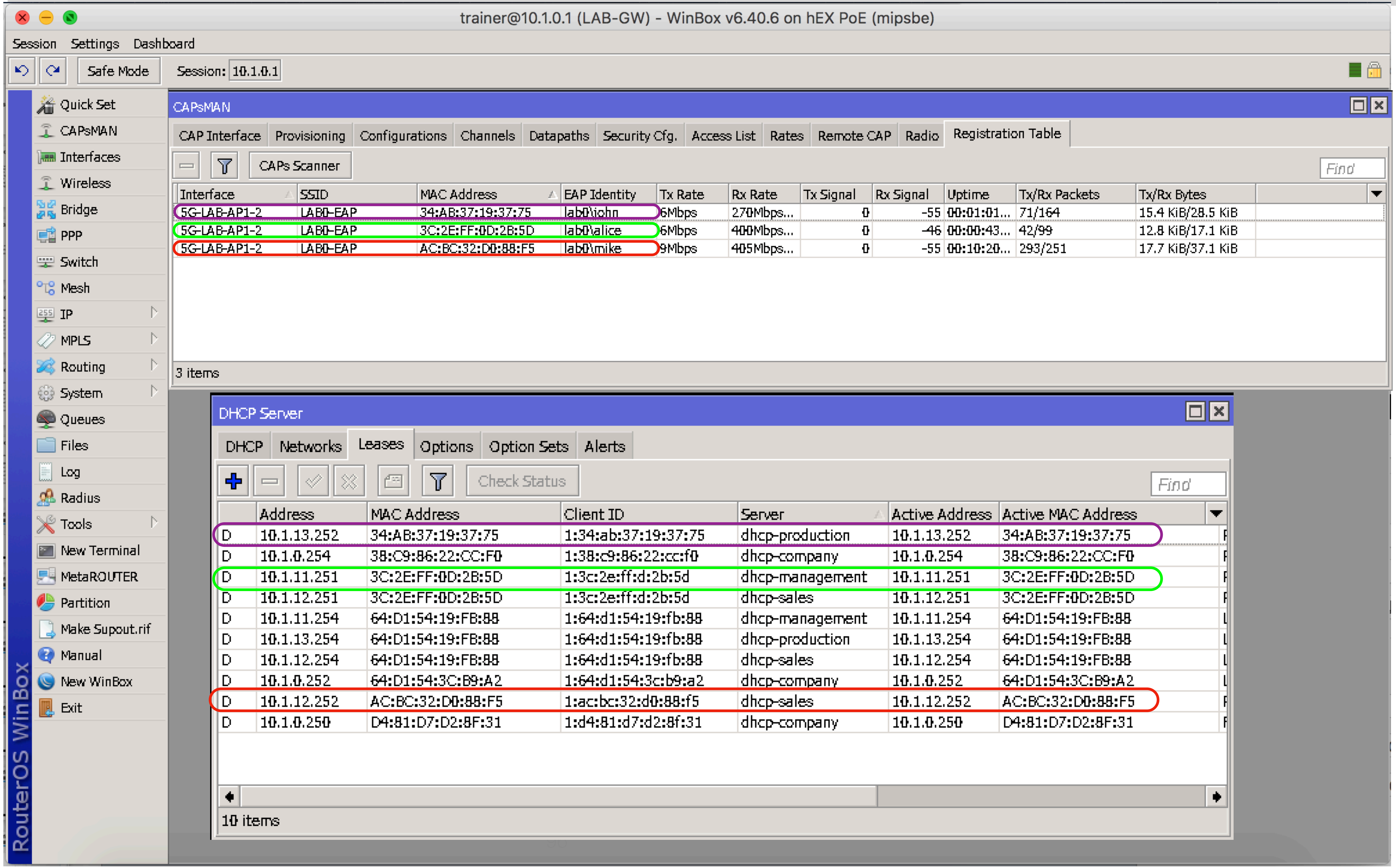
Username: lab0\mike

Password: ●●●●●●●●●

□ Show password

☑ Remember this network

Verify connected users



Interface	SSID	MAC Address	EAP Identity	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	Tx/Rx Packets	Tx/Rx Bytes
5G-LAB-AP1-2	LAB0-EAP	34:AB:37:19:37:75	lab0\john	6Mbps	270Mbps...	0	-55	00:01:01...	71/164	15.4 KiB/28.5 KiB
5G-LAB-AP1-2	LAB0-EAP	3C:2E:FF:0D:2B:5D	lab0\alice	6Mbps	400Mbps...	0	-46	00:00:43...	42/99	12.8 KiB/17.1 KiB
5G-LAB-AP1-2	LAB0-EAP	AC:BC:32:D0:88:F5	lab0\mike	9Mbps	405Mbps...	0	-55	00:10:20...	293/251	17.7 KiB/37.1 KiB

3 items

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address
D	10.1.13.252	34:AB:37:19:37:75	1:34:ab:37:19:37:75	dhcp-production	10.1.13.252	34:AB:37:19:37:75
D	10.1.0.254	38:C9:86:22:CC:F0	1:38:c9:86:22:cc:f0	dhcp-company	10.1.0.254	38:C9:86:22:CC:F0
D	10.1.11.251	3C:2E:FF:0D:2B:5D	1:3c:2e:ff:d:2b:5d	dhcp-management	10.1.11.251	3C:2E:FF:0D:2B:5D
D	10.1.12.251	3C:2E:FF:0D:2B:5D	1:3c:2e:ff:d:2b:5d	dhcp-sales	10.1.12.251	3C:2E:FF:0D:2B:5D
D	10.1.11.254	64:D1:54:19:FB:88	1:64:d1:54:19:fb:88	dhcp-management	10.1.11.254	64:D1:54:19:FB:88
D	10.1.13.254	64:D1:54:19:FB:88	1:64:d1:54:19:fb:88	dhcp-production	10.1.13.254	64:D1:54:19:FB:88
D	10.1.12.254	64:D1:54:19:FB:88	1:64:d1:54:19:fb:88	dhcp-sales	10.1.12.254	64:D1:54:19:FB:88
D	10.1.0.252	64:D1:54:3C:B9:A2	1:64:d1:54:3c:b9:a2	dhcp-company	10.1.0.252	64:D1:54:3C:B9:A2
D	10.1.12.252	AC:BC:32:D0:88:F5	1:ac:bc:32:d0:88:f5	dhcp-sales	10.1.12.252	AC:BC:32:D0:88:F5
D	10.1.0.250	D4:81:D7:D2:8F:31	1:d4:81:d7:d2:8f:31	dhcp-company	10.1.0.250	D4:81:D7:D2:8F:31

10 items

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
```

Thank You!

rein.podra@ccisrd.eu