

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 lose the key, we need to 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 users have several devices (laptop, smartphone and tablet)
- Cipher key is generated based on SSID and PSK. In the same network the generated key is always the same.
- No way to verify AP identity. We can create a fake AP and use special tools to steal information. Out of box tools cost ~100USD

- 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.

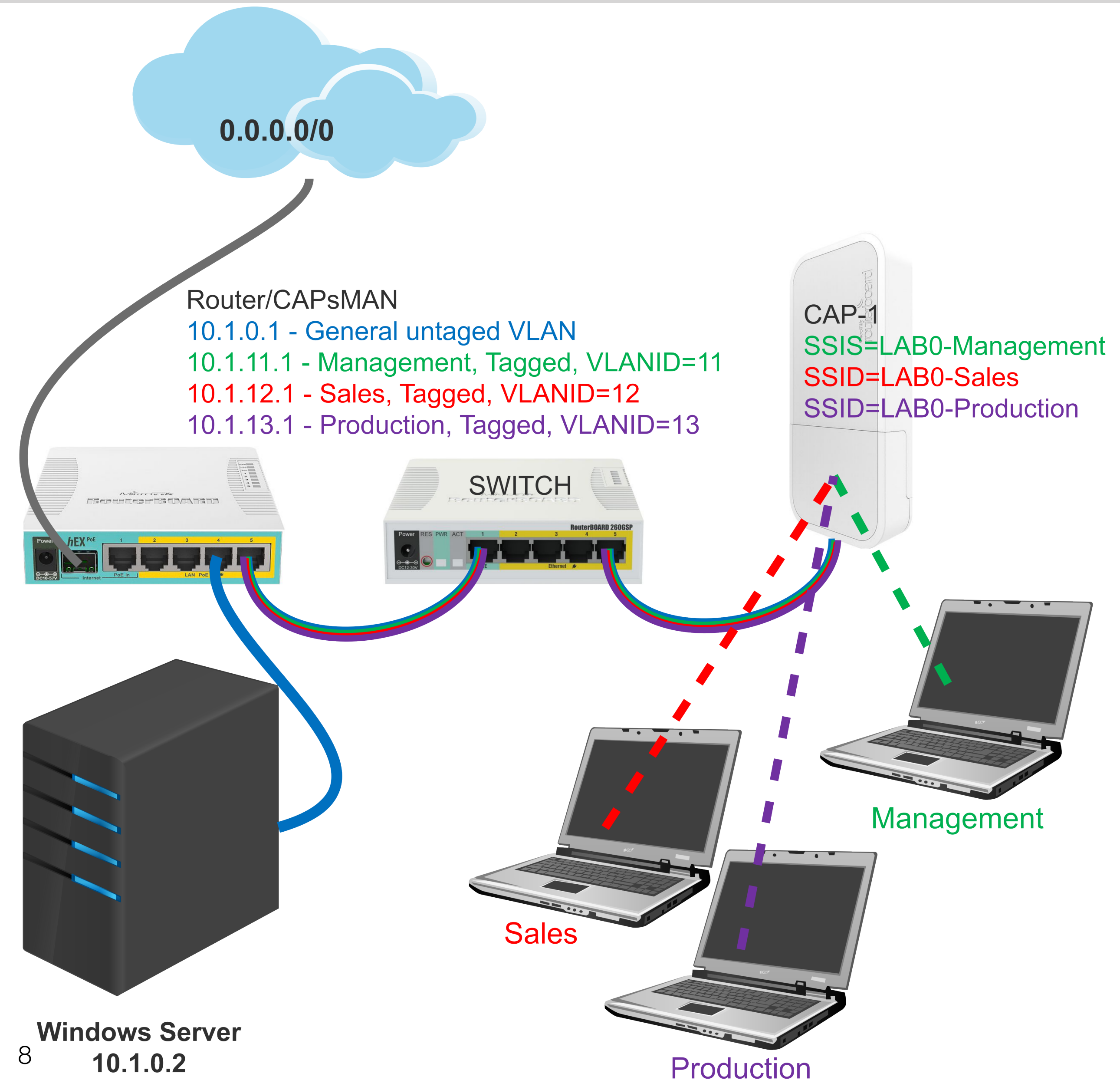
Dynamic VLAN

- 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 starting 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

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

Role	Count
AD DS	1
DNS	1
File and Storage Services	1

AD DS features: Manageability, Events, Services, Performance, BPA results

DNS features: Manageability, Events, Services, Performance, BPA results

File and Storage Services features: Manageability, Events, Services, Performance, BPA results

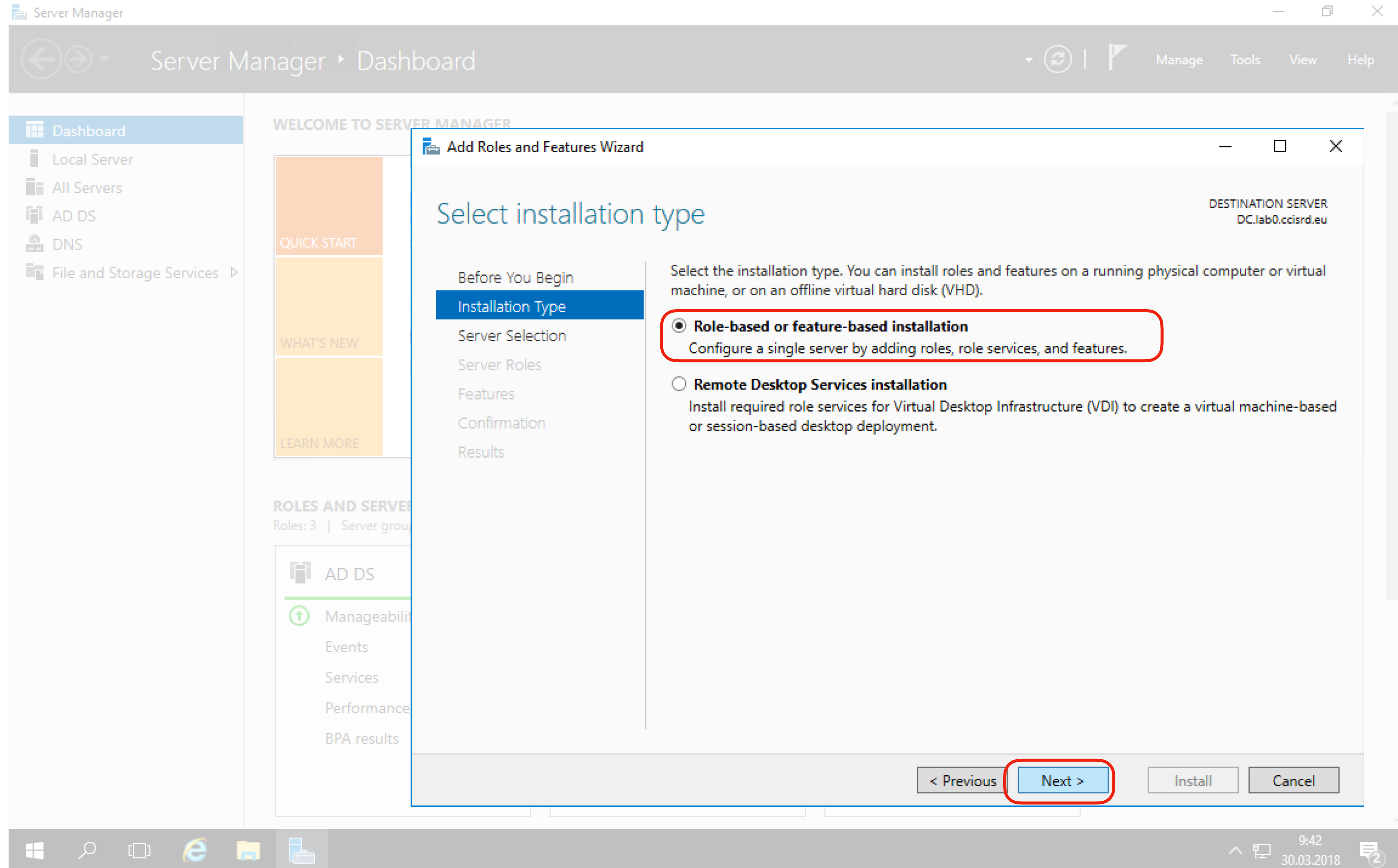
- In Server Manager click “Add roles and features”

Install Roles

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

The screenshot shows the Windows Server Manager interface. In the foreground, the 'Add Roles and Features Wizard' dialog box is open, titled 'Before you begin'. The wizard is for the destination server 'DC.lab0.ccisrd.eu'. The 'Before You Begin' step is selected in the left-hand navigation pane. The main content area provides instructions on how to use the wizard and lists prerequisites: a strong Administrator password, configured network settings, and the latest Windows updates. At the bottom of the dialog, the 'Next >' button is highlighted with a red circle, indicating the next step in the process. Other buttons visible include '< Previous', 'Install', and 'Cancel'. The background shows the Server Manager dashboard with a sidebar containing 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The 'ROLES AND SERVICES' section is partially visible, showing 'AD DS' and 'Manageability'.

Install Roles - Installation Type



Server Manager

Server Manager ▶ Dashboard

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 SERVICES

Roles: 3 | Server group

AD DS

Manageability

- Events
- Services
- Performance
- BPA results

Add Roles and Features Wizard

DESTINATION SERVER
DC.lab0.ccisrd.eu

Select installation type

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.

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

< Previous **Next >** Install Cancel

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

Install Roles - Select Server

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVICES

Roles: 3 | Server group

AD DS

Manageability

Events

Services

Performance

BPA results

Add Roles and Features Wizard

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.

< Previous **Next >** Install Cancel

- 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”

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVICES

Roles: 3 | Server group

AD DS

Manageability

Events

Services

Performance

BPA results

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Network Policy and Acces...

Confirmation

Results

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

DESTINATION SERVER
DC.lab0.ccisrd.eu

Roles	Description
<input checked="" type="checkbox"/> Active Directory Certificate Services	Network Policy and Access Services provides Network Policy Server (NPS), which helps safeguard the security of your network.
<input checked="" type="checkbox"/> Active Directory Domain Services (Installed)	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input checked="" type="checkbox"/> DNS Server (Installed)	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (2 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> MultiPoint Services	
<input type="checkbox"/> Network Controller	
<input checked="" type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	

< Previous **Next >** Install Cancel

Select features

- Accept default and click “next”

The screenshot shows the 'Add Roles and Features Wizard' in Windows Server Manager. The wizard is titled 'Add Roles and Features Wizard' and is running on the 'DESTINATION SERVER DC.lab0.ccisrd.eu'. The current step is 'Select features'. The left sidebar shows the 'Features' step is selected. The main area displays a list of features to be installed on the selected server. The 'Next >' button at the bottom right is highlighted with a red circle.

WELCOME TO SERVER MANAGER

Add Roles and Features Wizard

DESTINATION SERVER
DC.lab0.ccisrd.eu

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

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

< Previous **Next >** Install Cancel

AD Certificate Services

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

The screenshot shows the Windows Server Manager interface. On the left, a navigation pane lists 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with 'QUICK START', 'WHAT'S NEW', and 'LEARN MORE' sections. Below these is the 'ROLES AND SERVER' section, showing 'AD DS' and 'Manageability' (with sub-items: Events, Services, Performance, BPA results). A modal window titled 'Add Roles and Features Wizard' is open, showing 'Active Directory Certificate Services' for the 'DESTINATION SERVER DC.lab0.ccisrd.eu'. The wizard has a progress bar with steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services', 'Network Policy and Acces...', 'Confirmation', and 'Results'. The 'AD CS' step is currently selected. The 'Features' section is expanded, showing a list of features. At the bottom of the wizard, the '< Previous' button is disabled, the 'Next >' button is highlighted with a red circle, and 'Install' and 'Cancel' buttons are also visible. The Windows taskbar at the bottom shows the time as 9:42 on 30.03.2018.

Install CA role

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

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVICES

Roles: 3 | Server group

AD DS

Manageability

Events

Services

Performance

BPA results

Add Roles and Features Wizard

DESTINATION SERVER
DC.lab0.ccisrd.eu

Select role services

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 Active Directory Certificate Services

Role services	Description
<input checked="" type="checkbox"/> Certification Authority	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.
<input checked="" type="checkbox"/> Certificate Enrollment Policy Web Service	
<input checked="" type="checkbox"/> Certificate Enrollment Web Service	
<input checked="" type="checkbox"/> Certificate Authority Web Enrollment	
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	

< Previous **Next >** Install Cancel

Install NPS role

- Click “Next”

The screenshot shows the Windows Server Manager interface. In the background, the 'Server Manager Dashboard' is visible with a left-hand navigation pane containing 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' and 'ROLES AND SERVICES'.

In the foreground, the 'Add Roles and Features Wizard' is open. The title bar reads 'Add Roles and Features Wizard' and the destination server is 'DC.lab0.ccisrd.eu'. The wizard is titled 'Network Policy and Access Services'. The left-hand pane of the wizard lists the following steps: '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', and 'Results'. The 'Network Policy and Acces...' step is currently selected and highlighted in blue.

The right-hand pane of the wizard provides information about the service: '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.'

At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. The 'Next >' button is highlighted with a red circle, indicating the next step in the process.

Install NPS and CA role

The screenshot shows the Windows Server Manager interface. In the background, the 'Server Manager Dashboard' is visible with a left-hand navigation pane containing 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with 'QUICK START', 'WHAT'S NEW', and 'LEARN MORE' sections. Below these is the 'ROLES AND SERVICES' section, which lists 'AD DS', 'Manageability', 'Events', 'Services', 'Performance', and 'BPA results'. Overlaid on this is the 'Add Roles and Features Wizard' window. The wizard title is 'Web Server Role (IIS)' and the destination server is 'DC.lab0.ccisrd.eu'. The wizard's progress list includes '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', and 'Results'. The 'Web Server Role (IIS)' step is currently selected. The main content area of the wizard provides a description of web servers and a bullet point stating: '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.' At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. The 'Next >' button is highlighted with a red circle.

- Click “Next”

Install NPS and CA role

- Accept default and click “Next”

The screenshot shows the Windows Server Manager interface with the 'Add Roles and Features Wizard' open. The wizard is titled 'Select role services' and is for the 'Web Server (IIS)' role. The 'Role services' list is expanded, showing the following checked items:

- 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

The 'Description' on the right states: '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.'

At the bottom of the wizard, the 'Next >' button is highlighted with a red circle, indicating the next step in the installation process. Other buttons include '< Previous', 'Install', and 'Cancel'.

Install NPS and CA role

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVICES

Roles: 3 | Server group

AD DS

Manageability

Events

Services

Performance

BPA results

Add Roles and Features Wizard

DESTINATION SERVER
DC.lab0.ccisrd.eu

Confirm installation selections

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Network Policy and Access...

Web Server Role (IIS)

Role Services

Confirmation

Results

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

< Previous Next > **Install** Cancel

- Accept default and click “Install”

Install NPS and CA role

Server Manager

Server Manager Dashboard

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 SERVICES

Roles: 3 | Server group

- AD DS
- Manageability Tools
- Events
- Services
- Performance
- BPA results

Add Roles and Features Wizard

Installation progress

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

- Role Services

Network Policy and Access Services

Web Server Role (IIS)

- Role Services

Confirmation

Results

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](#)

< Previous Next > **Close** Cancel

9:42 30.03.2018

- 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

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD CS', 'AD DS', 'DNS', 'File and Storage Services', 'IIS', and 'NPAS'. The main area displays a 'WELCOME TO SERVER MANAGER' section with a 'QUICK START' list: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. A 'TASKS' window is open, showing a 'Post-deployment Configuration' task for 'Active Directory Certificate Services at DC'. The task progress bar is partially filled, and the task name 'Configure Active Directory Certificate Services on th...' is highlighted with a red circle. Below the tasks, the 'ROLES AND SERVER GROUPS' section shows three roles: AD CS, AD DS, and DNS, each with a 'Manageability' status and a list of sub-features like Events, Services, Performance, and BPA results.

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

Configure CA

- Accept default and click “Next”

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is at the 'Credentials' step, where the user is prompted to specify credentials for the destination server, DC.lab0.ccisrd.eu. The wizard lists the role services to be installed for the local Administrators group and the Enterprise Admins group. The 'Credentials' field is set to 'LAB0\administrator'. The 'Next >' button is highlighted with a red circle, indicating the next step in the configuration process.

Configure CA

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is at the 'Setup Type' step, where the user is prompted to specify the setup type of the CA. The 'Enterprise CA' option is selected and highlighted with a red box. The 'Next >' button at the bottom of the wizard is also highlighted with a red box. The background shows the Server Manager dashboard with a navigation pane on the left and a 'ROLES AND SERVER GROUPS' section at the bottom.

Server Manager Dashboard

WELCOME TO SERVER MANAGER

AD CS Configuration

Setup Type

DESTINATION SERVER
DC.lab0.ccisrd.eu

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

< Previous **Next >** Configure Cancel

ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1

AD DS	1
Manageability	
Events	
Services	
Performance	
BPA results	

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

Configure CA

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section containing '1 Configure AD CS', '2 Add Roles and Server Groups', '3 Add Roles', '4 Configure Roles', and '5 Complete Configuration'. Below this is a 'ROLES AND SERVER GROUPS' section showing 'AD DS' with a count of 1, and 'Manageability' with sub-items for 'Events', 'Services', 'Performance', and 'BPA results'. An 'AD CS Configuration' wizard window is open, showing the 'CA Type' step. The wizard has a 'DESTINATION SERVER' field set to 'DC.lab0.ccsird.eu'. The 'Specify the type of the CA' section contains two radio button options: 'Root CA' (selected and circled in red) and 'Subordinate CA'. The 'Root CA' option includes the text: 'Root CAs are the first and may be the only CAs configured in a PKI hierarchy.' The 'Subordinate CA' option includes the text: 'Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.' At the bottom of the wizard, the 'Next >' button is highlighted with a red box, along with '< Previous', 'Configure', and 'Cancel' buttons. The Windows taskbar at the bottom shows the time as 9:42 on 30.03.2018.

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

Configure CA

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

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is at the 'Private Key' step, where the user is prompted to 'Specify the type of the private key'. The 'Create a new private key' option is selected and highlighted with a red box. The 'Next >' button at the bottom of the wizard is also highlighted with a red box. The destination server is identified as DC.lab0.ccisrd.eu.

Server Manager Dashboard

WELCOME TO SERVER MANAGER

AD CS Configuration

DESTINATION SERVER
DC.lab0.ccisrd.eu

Private Key

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

< Previous **Next >** Configure Cancel

Configure CA

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

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is titled "Cryptography for CA" and is currently on the "Specify the cryptographic options" step. The "DESTINATION SERVER" is identified as "DC.lab0.ccisrd.eu".

The "Specify the cryptographic options" section includes the following settings:

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

The "Next >" button at the bottom right of the wizard is highlighted with a red box, indicating the next step in the configuration process.

Configure CA

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

The screenshot displays the Windows Server Manager interface. On the left, a navigation pane shows 'Server Manager' with options for 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area shows 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section containing '1 Configure AD CS', '2 Active Directory Certificate Services', '3 Active Directory Certificate Services', '4 Certificate Services', and '5 Certificate Services'. Below this is a 'ROLES AND SERVER GROUPS' section showing 'AD DS' with a count of 1, and 'Manageability' with sub-items for 'Events', 'Services', 'Performance', and 'BPA results'. The 'AD CS Configuration' wizard is open, showing a list of steps: 'Credentials', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name' (highlighted), 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The 'CA Name' step is active, with the 'DESTINATION SERVER' set to 'DC.lab0.ccisrd.eu'. The wizard prompts the user to 'Specify the name of the CA' and provides instructions: '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.' The 'Common name for this CA:' field contains 'lab0-MUM2008-CA'. The 'Distinguished name suffix:' field contains 'DC=lab0,DC=ccisrd,DC=eu'. The 'Preview of distinguished name:' field shows 'CN=lab0-MUM2008-CA,DC=lab0,DC=ccisrd,DC=eu'. At the bottom of the wizard, the 'Next >' button is highlighted with a red circle.

Configure CA

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

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section and a 'ROLES AND SERVER GROUPS' section. The 'AD CS Configuration' wizard is open, showing the 'Validity Period' step. The wizard is titled 'AD CS Configuration' and 'DESTINATION SERVER DC.lab0.ccsird.eu'. The 'Validity Period' section asks to 'Specify the validity period for the certificate generated for this certification authority (CA):' and shows a dropdown menu with '5' selected and 'Years' as the unit. Below this, it displays 'CA expiration Date: 30.03.2023 10:48:00' and a note: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom of the wizard, the 'Next >' button is highlighted with a red circle, along with 'Previous <', 'Configure', and 'Cancel' buttons. The Windows taskbar at the bottom shows the time as 9:42 on 30.03.2018.

Configure CA

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is titled "AD CS Configuration" and is currently on the "CA Database" step. The "DESTINATION SERVER" is set to "DC.lab0.ccsird.eu". The "Specify the database locations" section has two text boxes, both containing the default path "C:\Windows\system32\CertLog". The "Next >" button at the bottom right of the wizard is highlighted with a red circle. The background shows the Server Manager dashboard with a navigation pane on the left and a "WELCOME TO SERVER MANAGER" section in the center.

- Accept default and click “Next”

Configure CA

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is titled "AD CS Configuration" and is currently on the "CA Database" step. The "DESTINATION SERVER" is set to "DC.lab0.ccisrd.eu". The "Specify the database locations" section has two text boxes, both containing the default path "C:\Windows\system32\CertLog". The "Certificate Database" option in the left-hand menu is selected. At the bottom of the wizard, the "Next >" button is highlighted with a red circle, indicating the next step in the configuration process. Other buttons visible are "< Previous", "Configure", and "Cancel".

- Accept default and click “Next”

Configure CA

- Accept default and click “Configure”

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section and a 'ROLES AND SERVER GROUPS' section. The 'AD DS' role is listed with a '1' next to it. The 'AD CS Configuration' wizard is open, showing the 'Confirmation' step. The wizard title bar indicates the 'DESTINATION SERVER' is 'DC.lab0.ccisrd.eu'. The 'Confirmation' step lists the following roles, role services, or features to be configured: 'Active Directory Certificate Services'. The 'Confirmation' step is highlighted in blue. The 'Configure' button at the bottom right of the wizard is circled in red. The wizard also shows the following configuration details:

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

The screenshot shows the Windows Server Manager interface. On the left, a navigation pane lists 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section and a 'ROLES AND SERVER GROUPS' section. The 'ROLES AND SERVER GROUPS' section shows 'AD DS' with a count of 1, and sub-items for 'Manageability', 'Events', 'Services', 'Performance', and 'BPA results'. An 'AD CS Configuration' wizard window is open, showing the 'Results' step. The 'Results' window lists the following roles, role services, or features that were configured: 'Active Directory Certificate Services', 'Certification Authority', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', and 'Progress'. The 'Active Directory Certificate Services' section shows 'Configuration succeeded' with a green checkmark. The 'Close' button at the bottom right of the wizard window is highlighted with a red circle.

- After configuration complete, click “Close”

Configure CA

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

AD CS Configuration

Do you want to configure additional role services?

Yes No

ROLES AND SERVER GROUPS

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

Role Service	Count
AD DS	1
DNS	1
File and Storage Services	1

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

Configure CA

- Accept default and click “Next”

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is titled "AD CS Configuration" and is currently on the "Credentials" step. The "DESTINATION SERVER" is set to "DC.lab0.ccsird.eu". The "Credentials" field contains "LAB0\administrator". The "Next >" button is highlighted with a red circle, indicating the next step in the wizard. The "Configure" and "Cancel" buttons are also visible.

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

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

AD DS 1

Manageability

Events

Services

Performance

BPA results

AD CS Configuration

Credentials

Role Services

Confirmation

Progress

Results

DESTINATION SERVER
DC.lab0.ccsird.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...

More about AD CS Server Roles

< Previous Next > Configure Cancel

Configure CA

The screenshot shows the Server Manager interface with the AD CS Configuration wizard open. The wizard is at the 'Role Services' step. The 'Destination Server' is identified as 'DC.lab0.ccsird.eu'. In the 'Select Role Services to configure' section, the 'Certificate Enrollment Web Service' checkbox is checked and circled in red. The 'Next >' button at the bottom of the wizard is also circled in red. The background shows the 'ROLES AND SERVER GROUPS' section with 'AD DS' listed as a role on 1 server.

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

Configure CA

The screenshot shows the Windows Server Manager interface with the 'AD CS Configuration' wizard open. The wizard is titled 'CA for CES' and is currently on the 'Specify CA for Certificate Enrollment Web Services' step. The 'DESTINATION SERVER' is 'DC.lab0.ccisrd.eu'. The 'Select:' section has two radio buttons: 'CA name' (selected and circled in red) and 'Computer name'. Below this, the 'Target CA' field contains 'DC.lab0.ccisrd.eu/lab0-MUM2008-CA'. There is a 'Select...' button next to the field. A checkbox for 'Configure the Certificate Enrollment Web Service for renewal-only mode.' is present, with a note that 'Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.' At the bottom of the wizard, the '< Previous' button is disabled, the 'Next >' button is highlighted with a red circle, and the 'Configure' and 'Cancel' buttons are also visible. The background shows the Server Manager dashboard with a 'QUICK START' section and a 'ROLES AND SERVER GROUPS' section.

- Select “CA Name” and Click “Next”

Configure CA

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section and a 'ROLES AND SERVER GROUPS' section. The 'AD DS' role is listed with a count of 1. A task pane on the right shows the 'AD CS Configuration' wizard steps: 1. Configuration, 2. Credentials, 3. Role Services, 4. CA for CES, 5. Authentication Type for CES, 6. Service Account for CES, 7. Server Certificate, 8. Confirmation, 9. Progress, 10. Results. The 'Authentication Type for CES' step is selected, and the wizard window is open. The wizard title is 'AD CS Configuration' and the destination server is 'DC.lab0.ccisrd.eu'. The 'Authentication Type for CES' step is active, and the user is prompted to 'Select the type of authentication'. Three options are available: 'Windows integrated authentication' (selected and circled in red), 'Client certificate authentication', and 'User name and password'. At the bottom of the wizard, the '< Previous' button is disabled, the 'Next >' button is highlighted with a red circle, and the 'Configure' and 'Cancel' buttons are visible. The Windows taskbar at the bottom shows the time as 9:42 on 30.03.2018.

- 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”

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is titled "Service Account for CES" and is for the destination server "DC.lab0.ccisrd.eu". The "Specify the service account" section has two radio button options: "Specify service account (recommended)" and "Use the built-in application pool identity". The second option is selected and circled in red. Below the options is a text input field and a "Select..." button. At the bottom of the wizard, the "Next >" button is also circled in red. The background shows the Server Manager dashboard with a navigation pane on the left and a "WELCOME TO SERVER MANAGER" section with a "QUICK START" card.

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 Manager Dashboard

WELCOME TO SERVER MANAGER

AD CS Configuration

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

< Previous **Next >** Configure Cancel

Configure CA

The screenshot shows the Windows Server Manager interface. On the left, a navigation pane lists various server components: Dashboard, Local Server, All Servers, AD CS, AD DS, DNS, File and Storage Services, IIS, and NPAS. The main area displays a 'WELCOME TO SERVER MANAGER' section with a 'QUICK START' guide. The first step is 'Configure this local server', followed by 'Add roles and features', 'Add other servers to manage', 'Create a server group', and 'Connect this server to cloud services'. Below this, the 'ROLES AND SERVER GROUPS' section shows three roles: AD CS, AD DS, and DNS, each with a count of 1. Each role has a list of sub-items: Manageability, Events, Services, Performance, and BPA results. On the right, a 'Tools' menu is open, listing various administrative tools. The 'Internet Information Services (IIS) Manager' option is highlighted with a red box.

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: 6 | Server groups: 1 | Servers total: 1

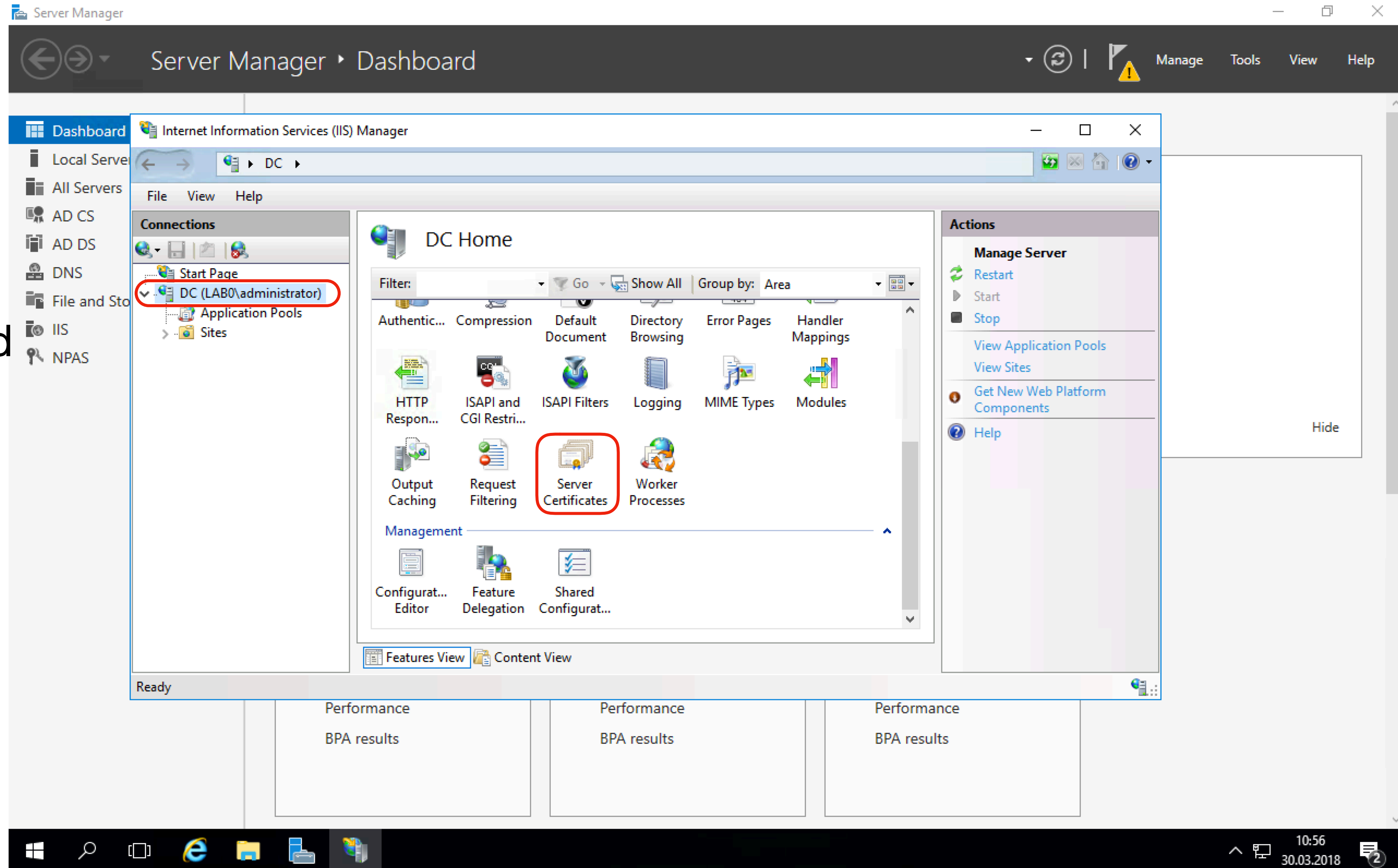
Role	Count
AD CS	1
AD DS	1
DNS	1

Tools menu items:

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Module for Windows PowerShell
- Active Directory Sites and Services
- Active Directory Users and Computers
- ADSI Edit
- Certification Authority
- Component Services
- Computer Management
- Defragment and Optimize Drives
- Disk Cleanup
- DNS
- Event Viewer
- Group Policy Management
- Internet Information Services (IIS) Manager**
- iSCSI Initiator
- Local Security Policy
- Microsoft Azure Services
- Network Policy Server
- ODBC Data Sources (32-bit)
- ODBC Data Sources (64-bit)
- Performance Monitor
- Print Management
- Resource Monitor
- Services
- System Configuration
- System Information
- Task Scheduler
- Windows Firewall with Advanced Security
- Windows Memory Diagnostic
- Windows PowerShell

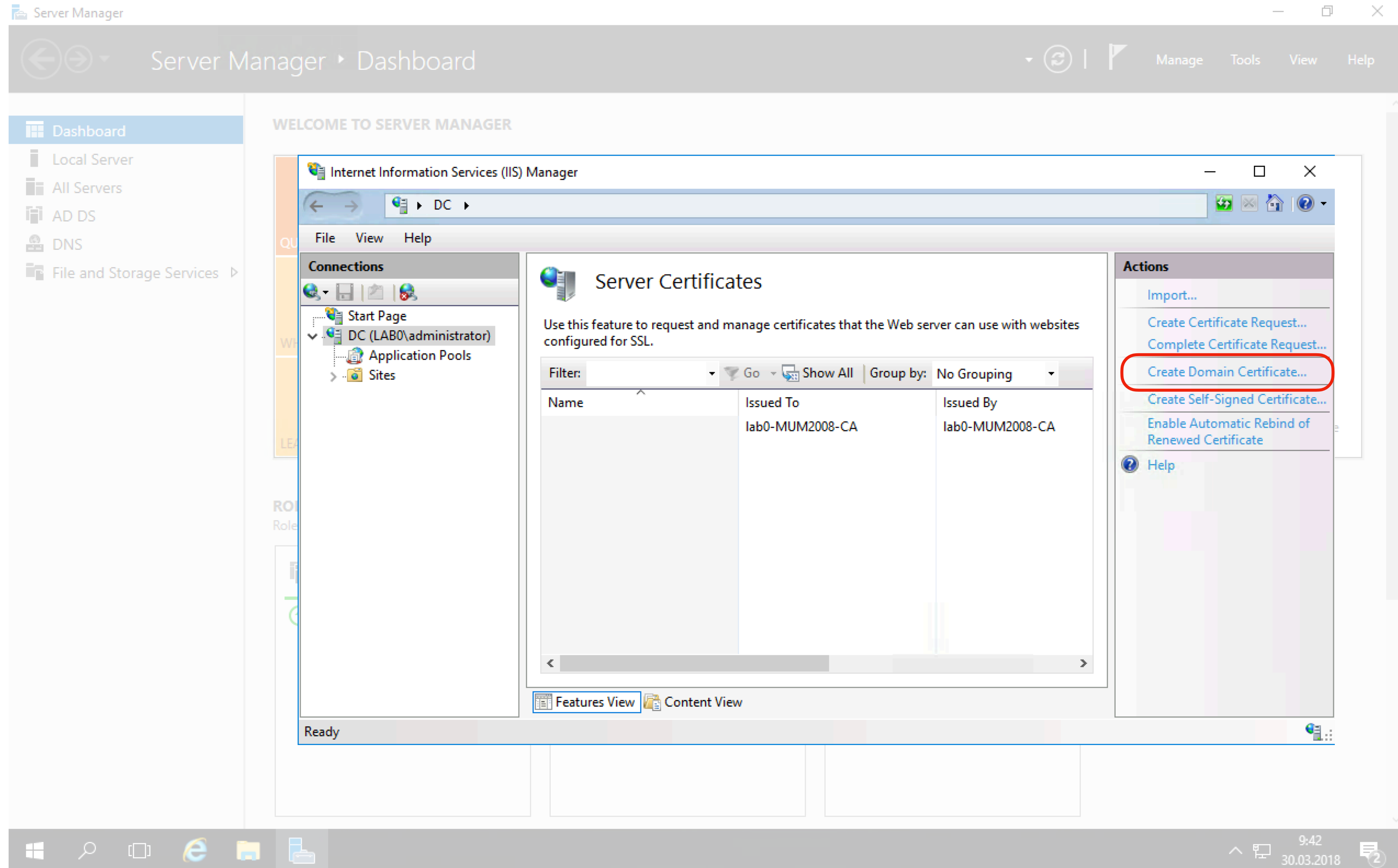
- Open “Internet Information Services (IIS) Manager”.

Create web server certificate



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

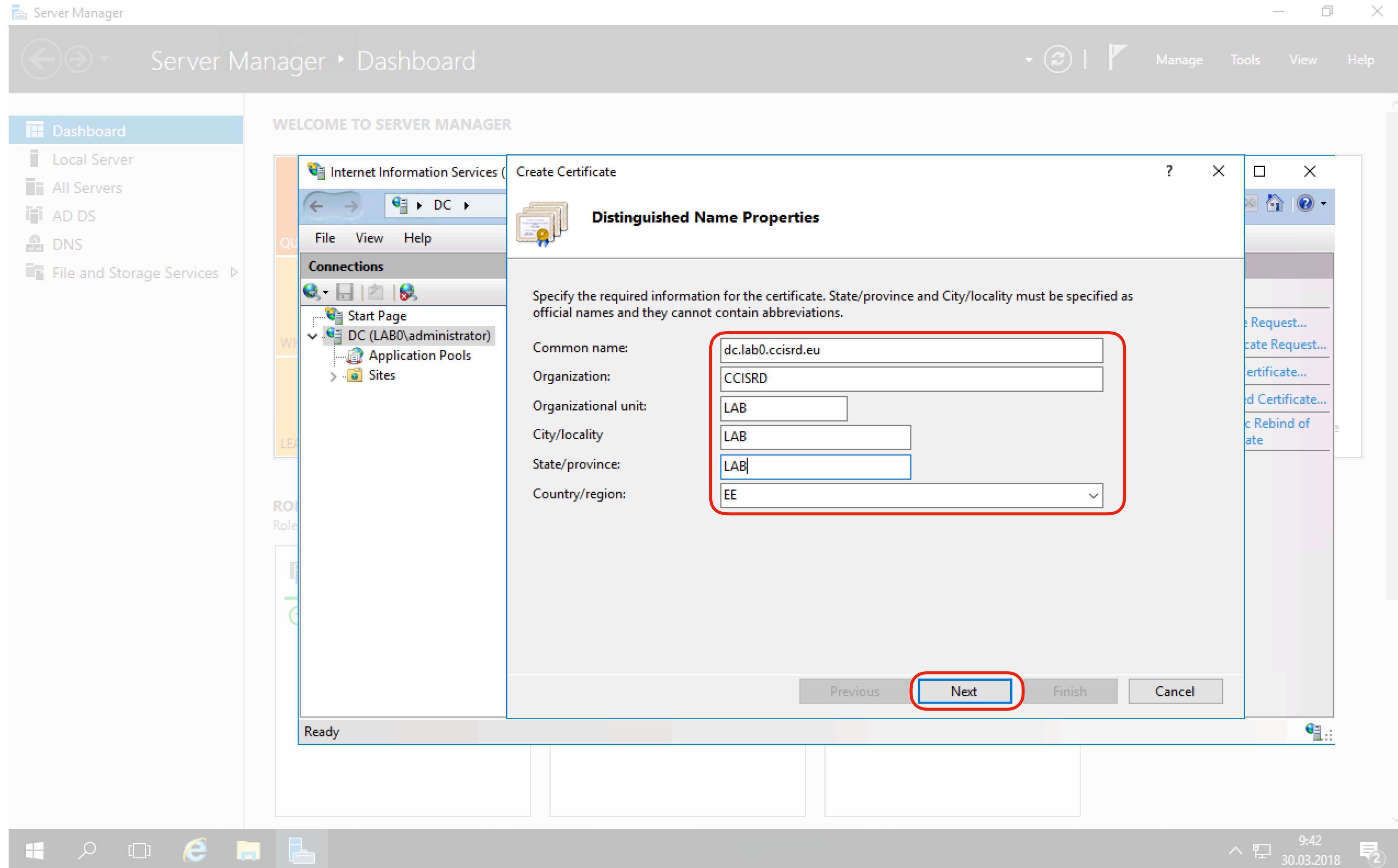
Create web server certificate



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

Create web server certificate

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



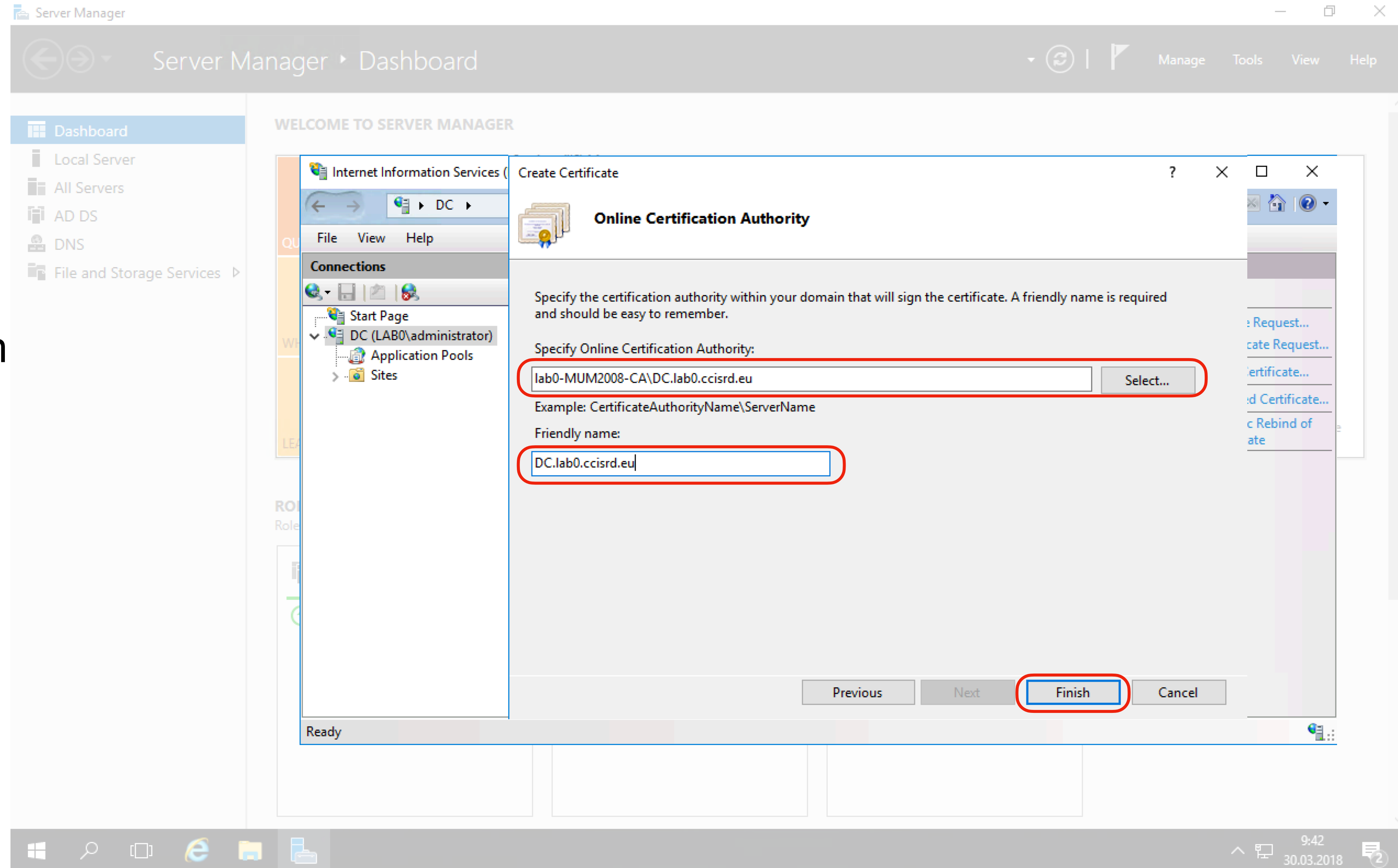
The screenshot shows the Windows Server Manager interface. On the left, the navigation pane shows 'Server Manager' > 'Dashboard' > 'Local Server' > 'All Servers' > 'AD DS' > 'DNS' > 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' and 'Internet Information Services (IIS) Manager'. The 'Create Certificate' wizard is open, showing the 'Distinguished Name Properties' dialog. The dialog contains the following fields:

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

The 'Next' button at the bottom of the dialog is highlighted with a red circle. The status bar at the bottom of the window shows 'Ready'.

Create web server certificate

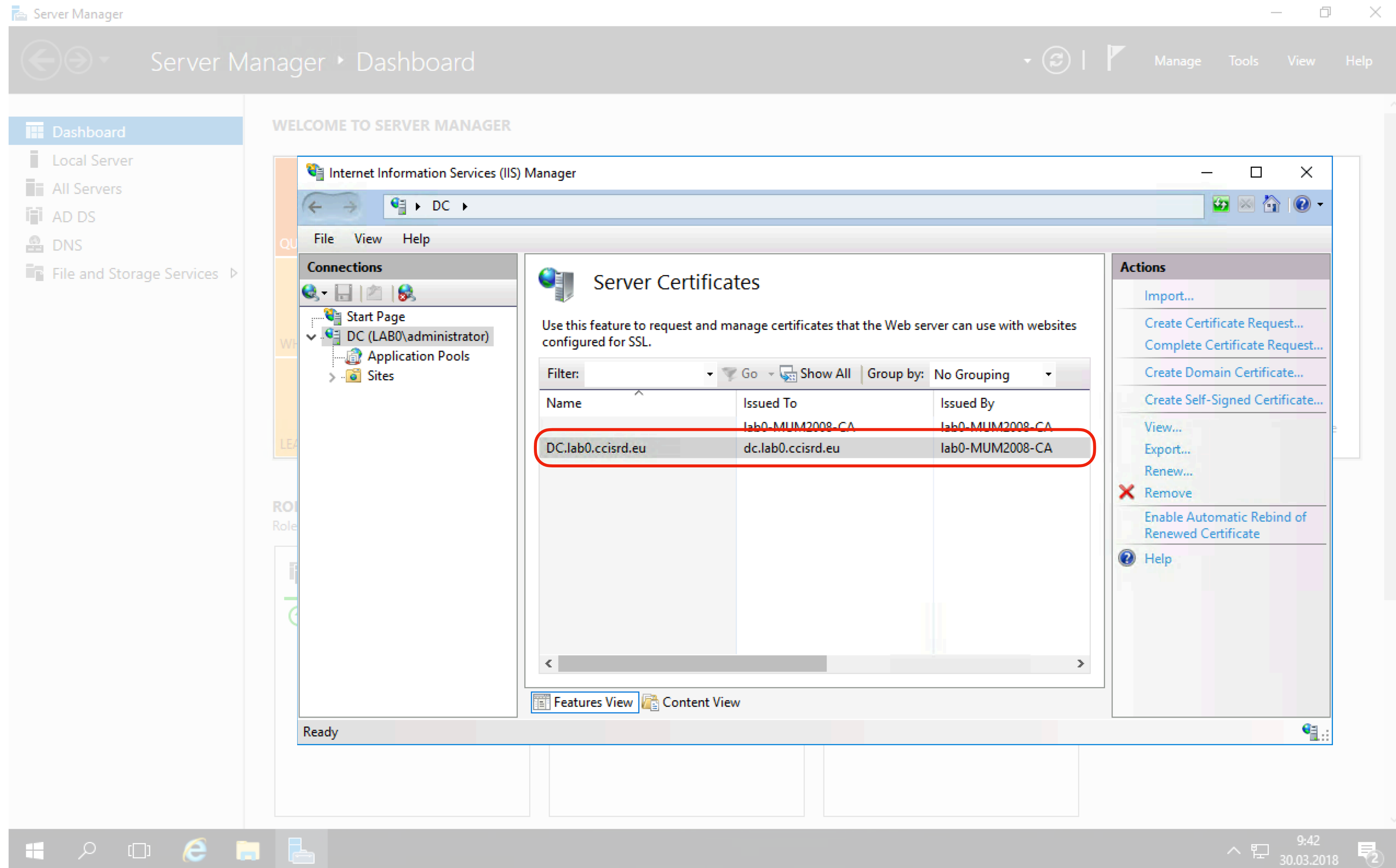
- Specify Online Certificate Authority by clicking “Select” button
- Insert a friendly name for the certificate. It can be any name.
- Click “Finish”



The screenshot shows the Server Manager console with the 'Create Certificate' wizard open. The wizard is titled 'Online Certification Authority' and is located within the 'Internet Information Services (IIS) Manager' window. The wizard's progress bar shows that the 'Specify Online Certification Authority' step is the current step. The 'Specify Online Certification Authority' field contains the text 'lab0-MUM2008-CA\DC.lab0.ccisrd.eu' and is highlighted with a red box. The 'Select...' button next to it is also highlighted with a red box. The 'Friendly name' field contains the text 'DC.lab0.ccisrd.eu' and is also highlighted with a red box. The 'Finish' button at the bottom of the wizard is highlighted with a red box. The 'Previous' and 'Next' buttons are disabled. The 'Cancel' button is also visible. The background shows the Server Manager dashboard with a navigation pane on the left and a 'WELCOME TO SERVER MANAGER' message at the top.

Create web server certificate

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



The screenshot shows the Windows Server Manager interface. The 'Server Manager' window is open, displaying the 'Dashboard' and 'Local Server' sections. The 'Internet Information Services (IIS) Manager' window is also open, showing the 'Server Certificates' section. A table of certificates is displayed, with one certificate highlighted in red:

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

The 'Actions' pane on the right side of the IIS Manager window shows various options for managing certificates, including 'Import...', 'Create Certificate Request...', 'Complete Certificate Request...', 'Create Domain Certificate...', 'Create Self-Signed Certificate...', 'View...', 'Export...', 'Renew...', 'Remove', 'Enable Automatic Rebind of Renewed Certificate', and 'Help'.

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”

The screenshot shows the Server Manager interface with the AD CS Configuration wizard open. The wizard is at the 'Server Certificate' step for the 'DESTINATION SERVER DC.lab0.ccisrd.eu'. The 'Specify a Server Authentication Certificate' section is active, showing a table of certificates. The first certificate is selected, with its 'Issued To' field highlighted in red. A 'Refresh' button is also highlighted in red. At the bottom of the wizard, the 'Next >' button is highlighted in red.

Server Manager Dashboard

WELCOME TO SERVER MANAGER

AD CS Configuration

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

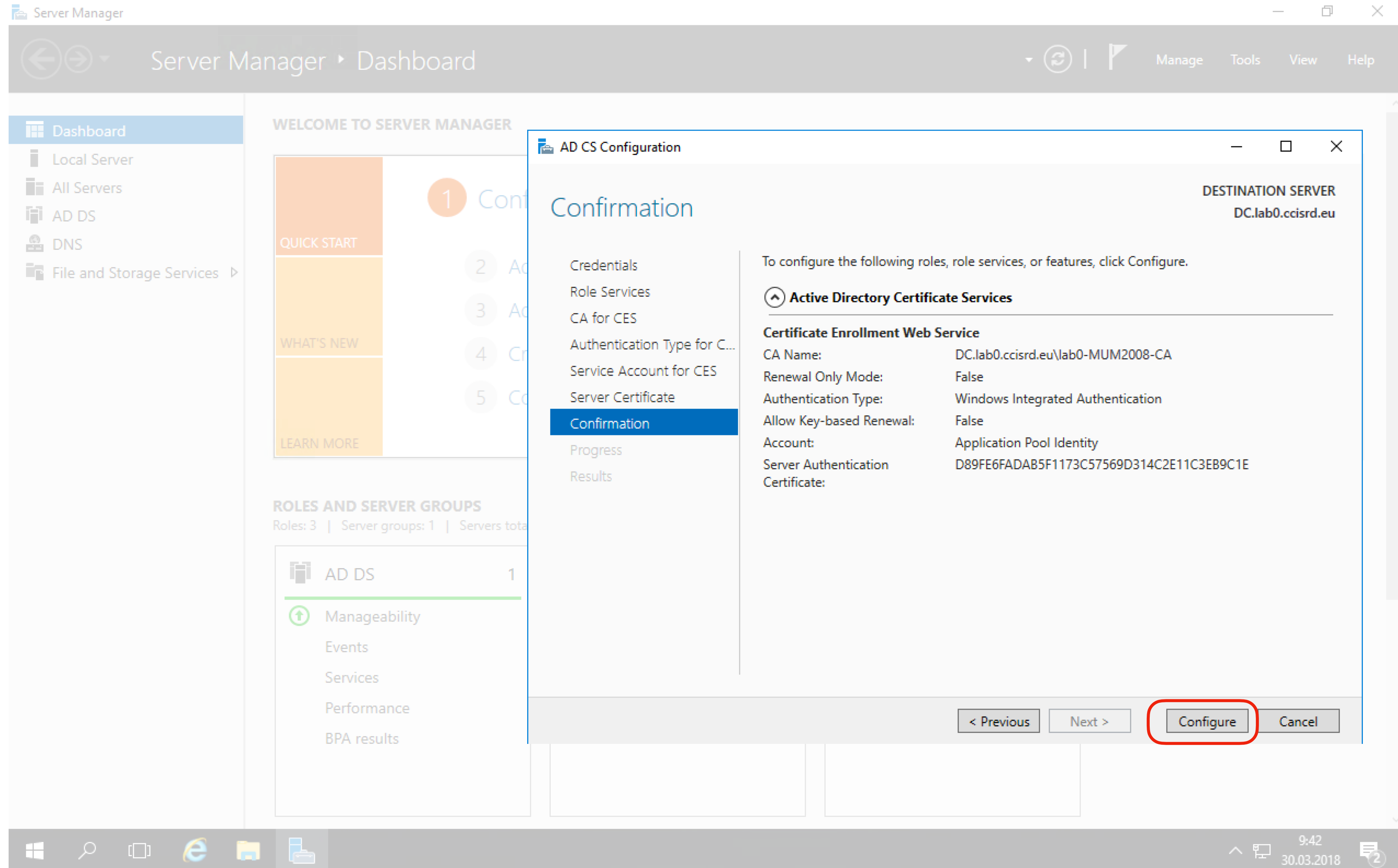
Properties Refresh

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

< Previous Next > Configure Cancel

Configure CA



The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section containing '1 Configure', '2 Add Roles and Server Groups', '3 Add Roles', '4 Configure Roles', and '5 Configure Server Groups'. Below this is the 'ROLES AND SERVER GROUPS' section, showing 'AD DS' with a count of 1, and sub-items for 'Manageability', 'Events', 'Services', 'Performance', and 'BPA results'. A dialog box titled 'AD CS Configuration' is open, showing a 'Confirmation' step. The dialog lists the following roles and services to be configured: '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'. The 'DESTINATION SERVER' is listed as 'DC.lab0.ccisrd.eu'. At the bottom of the dialog, the 'Configure' button is highlighted with a red circle.

- Click “Configure”

Configure CA

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

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

AD DS 1

Manageability

Events

Services

Performance

BPA results

AD CS Configuration

Results

Credentials

Role Services

CA for CES

Authentication Type for C...

Service Account for CES

Server Certificate

Confirmation

Progress

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

< Previous Next > Close Cancel

- Click "Close"

Configure Web Service

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

The screenshot shows the Windows Server Manager interface. The top navigation bar includes 'Server Manager' and 'Dashboard'. A task notification window is open, titled 'Post-deployment Configuration', with a yellow warning icon. The notification text reads: 'Configuration required for Active Directory Certificate Services at DC'. Below this, a link is highlighted in red: 'Configure Active Directory Certificate Services on the destination server'. Other text in the notification includes 'Configuration required. Installation succeeded on DC.lab0.ccisrd.eu.' and a link 'Add Roles and Features'. The main dashboard area shows a 'WELCOME TO SERVER MANAGER' section with a 'QUICK START' list: 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. Below this is the 'ROLES AND SERVER GROUPS' section, which lists three roles: AD CS, AD DS, and DNS, each with a 'Manageability' status and a list of sub-items (Events, Services, Performance, BPA results). The Windows taskbar at the bottom shows the time as 15:04 on 01.04.2018.

Configure CA

- Verify username and click “Next”

The screenshot shows the Windows Server Manager interface with the AD CS Configuration wizard open. The wizard is titled "AD CS Configuration" and is currently on the "Credentials" step. The "DESTINATION SERVER" is set to "DC.lab0.ccisrd.eu". The "Credentials" field contains "LAB0\administrator" and is highlighted with a red circle. The "Next >" button at the bottom of the wizard is also highlighted with a red circle. The background shows the Server Manager dashboard with a navigation pane on the left and a main content area with a "QUICK START" section and a "ROLES AND SERVER GROUPS" section.

Configure CA

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section containing a '1' in a circle, 'WHAT'S NEW', and 'LEARN MORE'. Below this is the 'ROLES AND SERVER GROUPS' section, showing 'AD DS' with a count of 1, and sub-items for 'Manageability', 'Events', 'Services', 'Performance', and 'BPA results'. An 'AD CS Configuration' wizard window is open, showing the 'Role Services' tab. The 'Select Role Services to configure' list includes: 'Certification Authority' (checked), 'Certification Authority Web Enrollment' (checked and circled in red), 'Online Responder' (unchecked), 'Network Device Enrollment Service' (unchecked), 'Certificate Enrollment Web Service' (checked), and 'Certificate Enrollment Policy Web Service' (unchecked). The 'DESTINATION SERVER' is 'DC.lab0.ccsird.eu'. At the bottom of the wizard, the '< Previous' and 'Next >' buttons are visible, with 'Next >' circled in red. The Windows taskbar at the bottom shows the time as 9:42 on 30.03.2018.

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

Configure CA

The screenshot displays the Windows Server Manager interface. On the left, a navigation pane shows 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area is titled 'WELCOME TO SERVER MANAGER' and contains a 'QUICK START' section with a numbered list (1-5) and a 'WHAT'S NEW' section. Below this is the 'ROLES AND SERVER GROUPS' section, which lists 'AD DS' with a count of 1, and sub-items for 'Manageability', 'Events', 'Services', 'Performance', and 'BPA results'. An 'AD CS Configuration' dialog box is open in the foreground, showing a 'Results' tab. The dialog title is 'AD CS Configuration' and the destination server is 'DC.lab0.ccsird.eu'. The results section states: 'The following roles, role services, or features were configured: Active Directory Certificate Services'. Below this, 'Certification Authority Web Enrollment' is listed with a green checkmark and the text 'Configuration succeeded'. At the bottom of the dialog, there are buttons for '< Previous', 'Next >', 'Close' (highlighted with a red circle), and 'Cancel'. The Windows taskbar at the bottom shows the time as 9:42 on 30.03.2018.

- 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

The screenshot shows the Windows Server Manager interface. The top navigation bar includes 'Server Manager' and 'Dashboard'. The left-hand navigation pane lists various server roles: Dashboard, Local Server, All Servers, AD CS, AD DS, DNS, File and Storage Services, IIS, and NPAS. The main content area is titled 'WELCOME TO SERVER MANAGER' and features a 'QUICK START' section with a numbered list of tasks: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is the 'ROLES AND SERVER GROUPS' section, which displays three role cards: AD CS, AD DS, and DNS. Each card shows a 'Manageability' icon and a list of sub-features: Events, Services, Performance, and BPA results. A red circle highlights the 'Network Policy Server' role in the right-hand pane, which is currently hidden. The taskbar at the bottom shows the Windows logo, search icon, and several application icons, along with the system tray displaying the time as 11:03 and the date as 30.03.2018.

- From Server Manager open “Network Policy Server”.

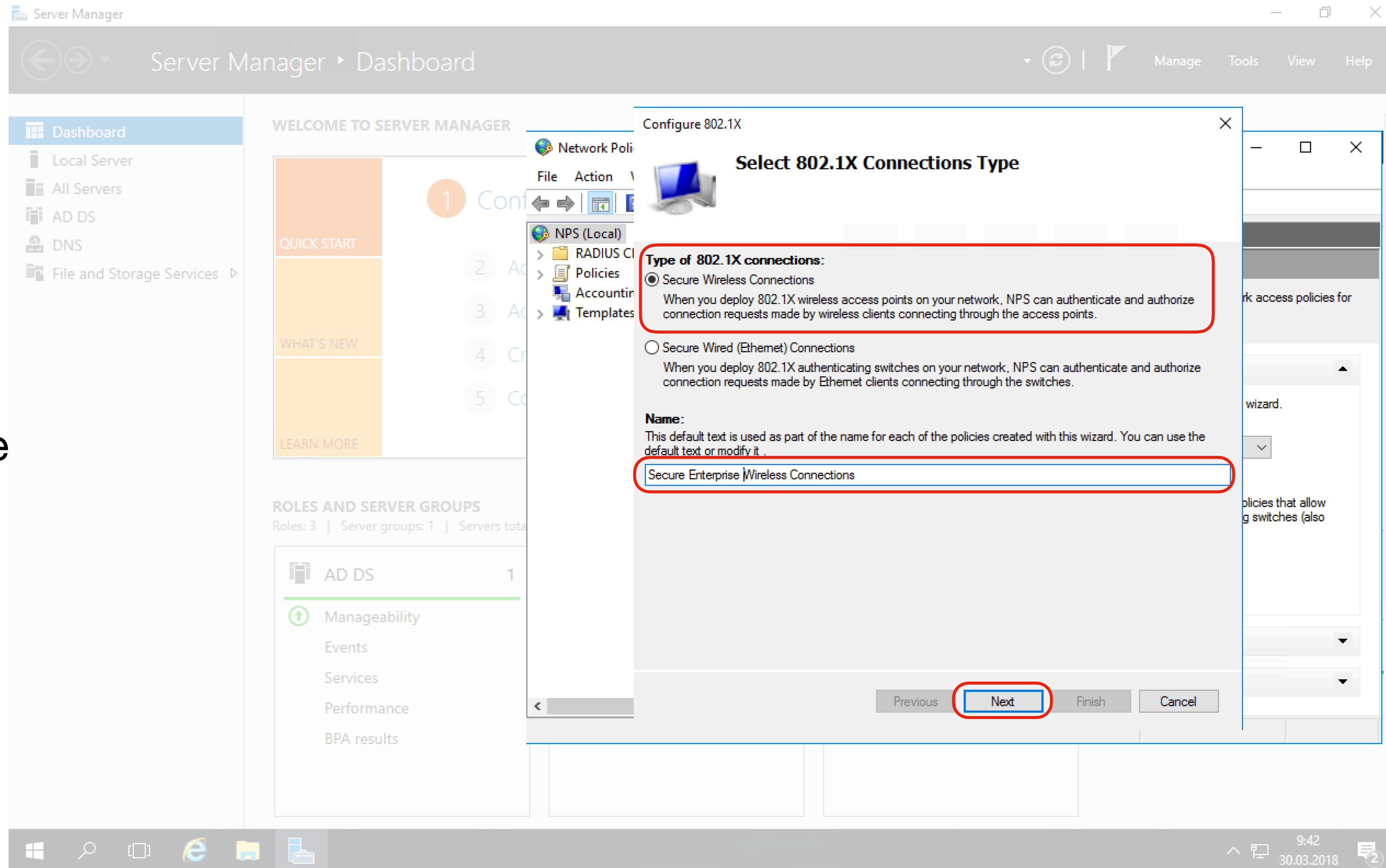
Configure NPS - Radius

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

The screenshot displays the Windows Server Manager interface. The 'Server Manager' window is open, showing the 'Dashboard' for a 'Local Server'. The 'Network Policy Server' (NPS) console is also open, showing the 'Getting Started' page. The 'Standard Configuration' section is expanded, and the 'RADIUS server for 802.1X Wireless or Wired Connections' option is selected in the dropdown menu. The 'Configure 802.1X' button is highlighted with a red circle. The 'Advanced Configuration' and 'Templates Configuration' sections are also visible.

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

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

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

AD DS 1

Manageability

Events

Services

Performance

BPA results

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:

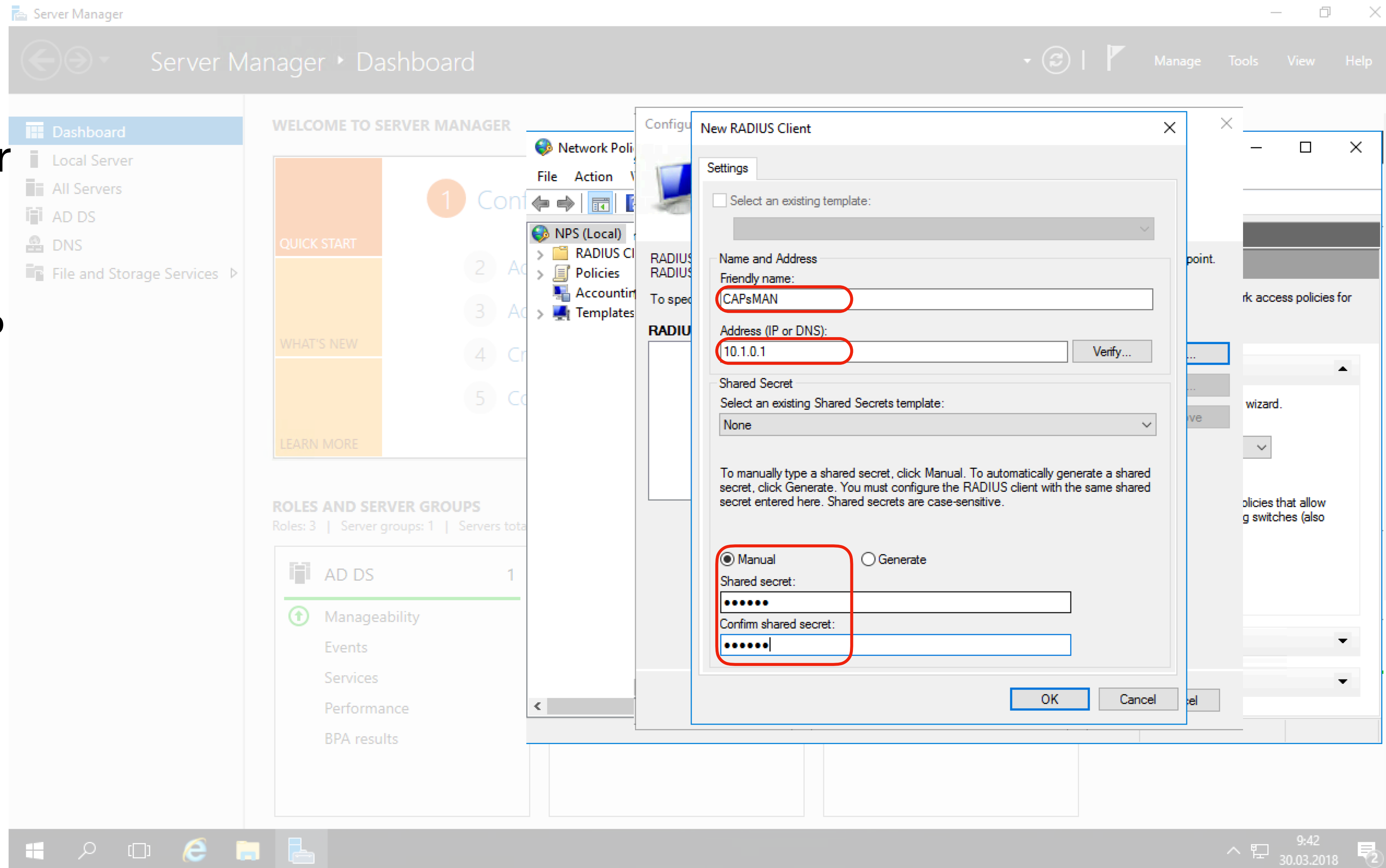
Add... Edit... Remove

Previous Next Finish Cancel

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

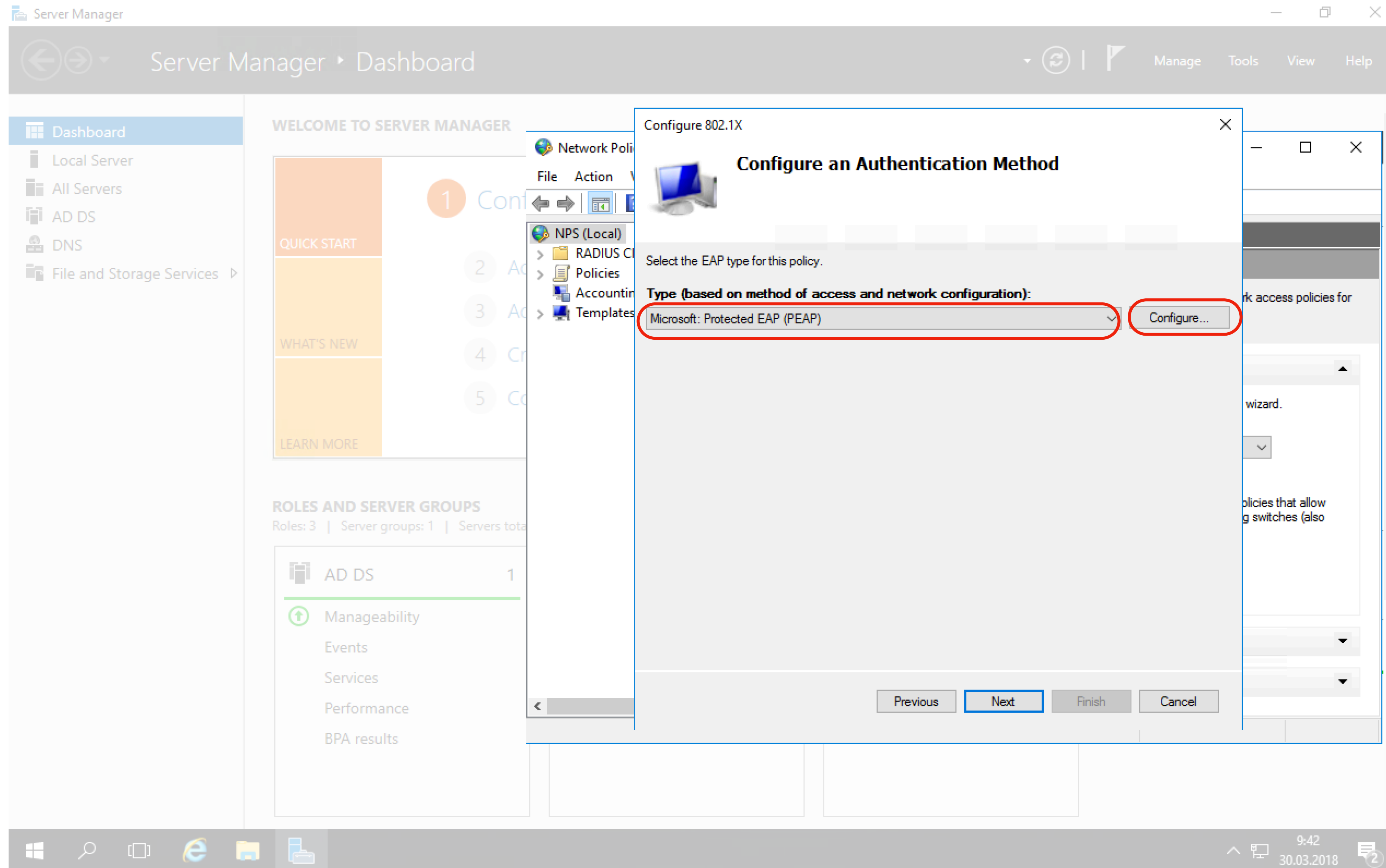
Configure NPS - Radius

- 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”

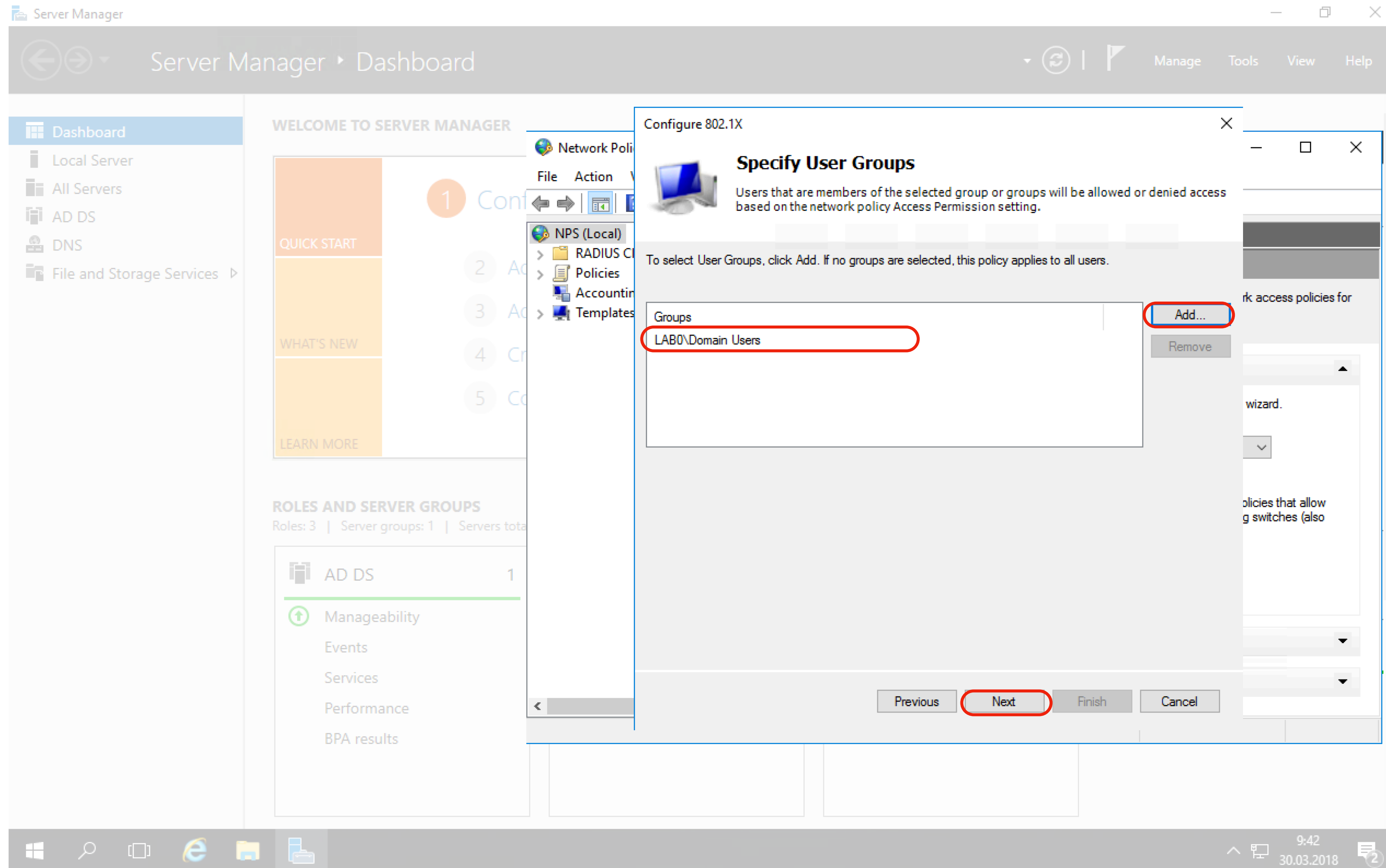
The screenshot displays the Windows Server Manager interface. In the left-hand navigation pane, 'NPS (Local)' is selected under 'Network Policy Server'. The main area shows the 'Configure 802.1X' wizard. The 'Edit Protected EAP Properties' dialog box is open, showing the following configuration:

- 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)

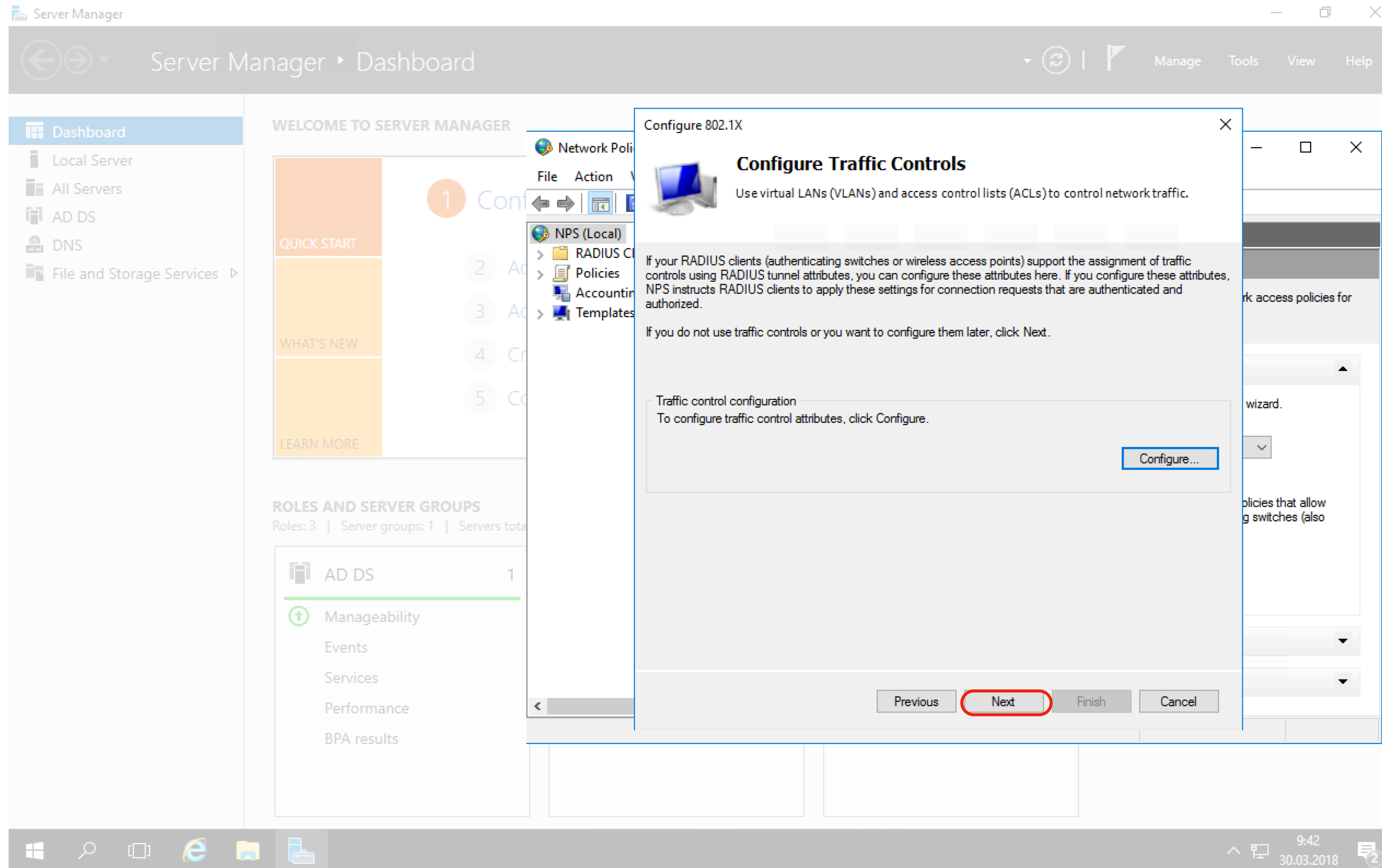
The 'OK' button at the bottom of the dialog is highlighted with a red circle. The 'Next' button in the wizard is also visible.

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

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

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

- AD DS 1
- Manageability
- Events
- Services
- Performance
- BPA results

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

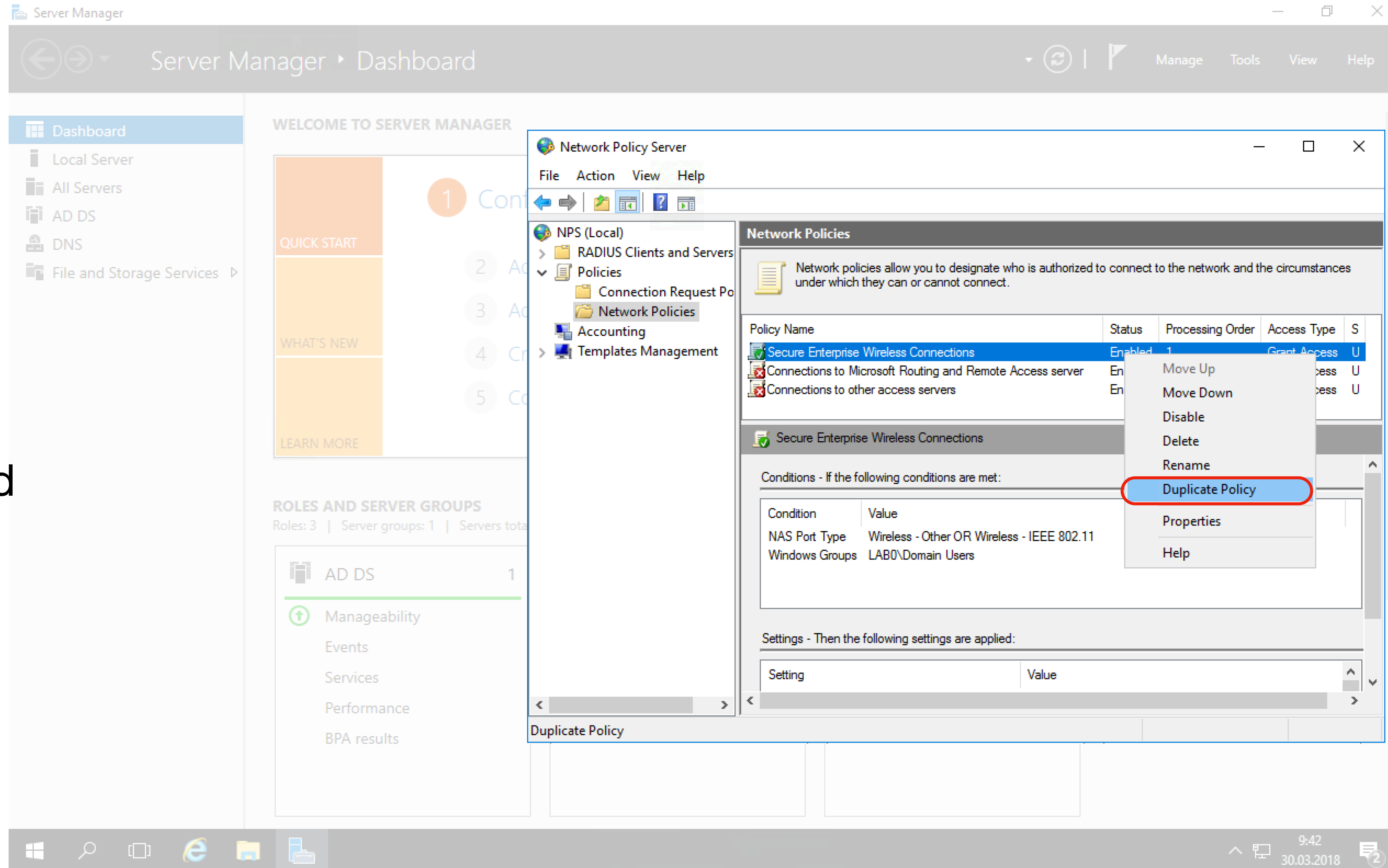
[Configuration Details](#)

Previous Next **Finish** Cancel

- Review settings and click “Next”

Configure NPS - Radius

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



The screenshot shows the Windows Server Manager interface. The left sidebar contains navigation options: Dashboard, Local Server, All Servers, AD DS, DNS, and File and Storage Services. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section containing a numbered list (1-5) and a 'WHAT'S NEW' section. Below this is the 'ROLES AND SERVER GROUPS' section, showing 'AD DS' with 1 server and 'Manageability' with 1 server. The 'Network Policy Server' console tree is expanded to 'Policies > Network Policies'. The 'Network Policies' pane shows a table of policies:

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		Access	U
Connections to other access servers	En		Access	U

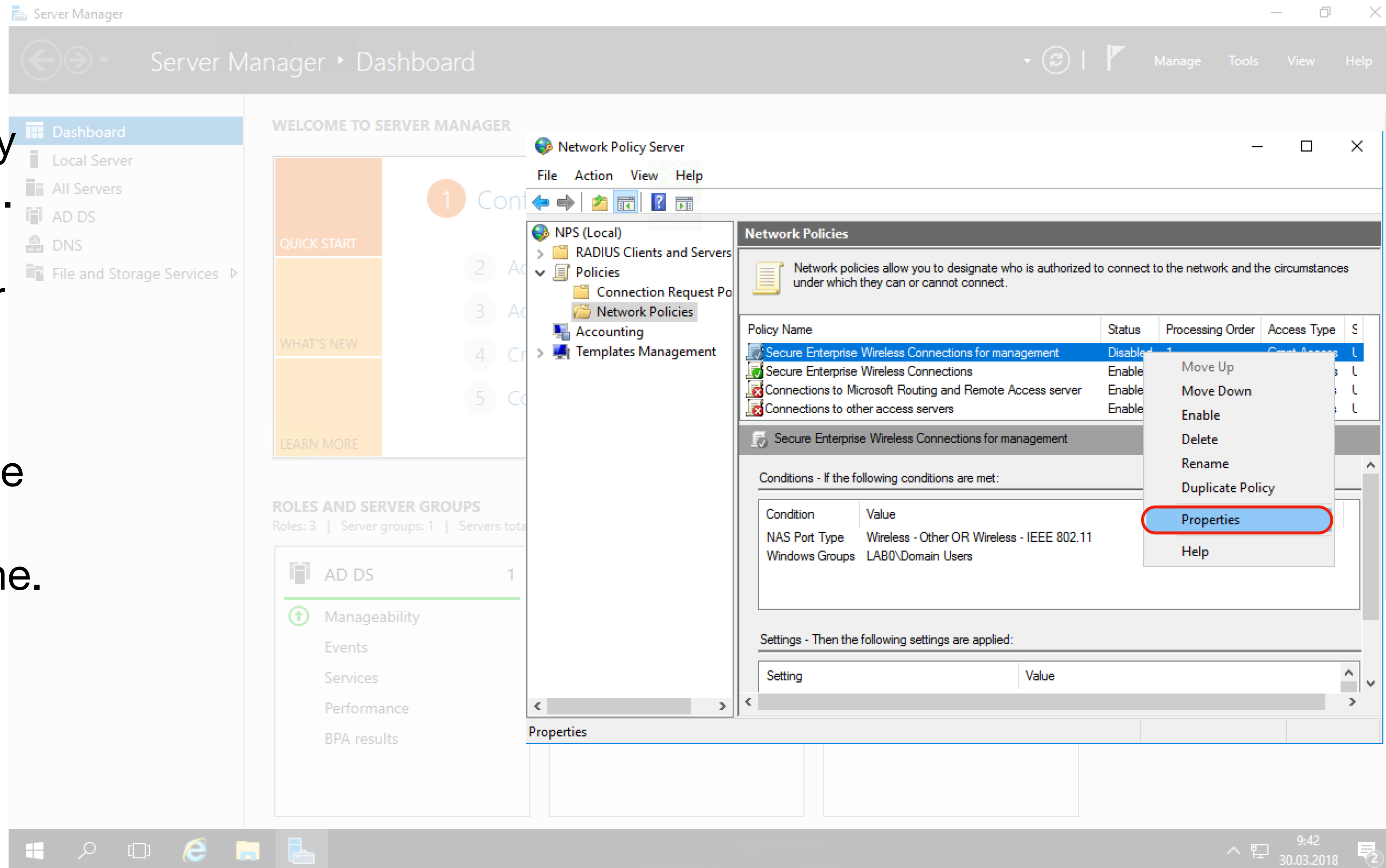
The 'Secure Enterprise Wireless Connections' policy is selected, and a context menu is open over it. The menu items are: Move Up, Move Down, Disable, Delete, Rename, Duplicate Policy (highlighted in red), Properties, and Help. Below the table, the 'Conditions' section is visible, showing a table:

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

The 'Settings' section is also visible, showing a table with columns for Setting and Value.

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”



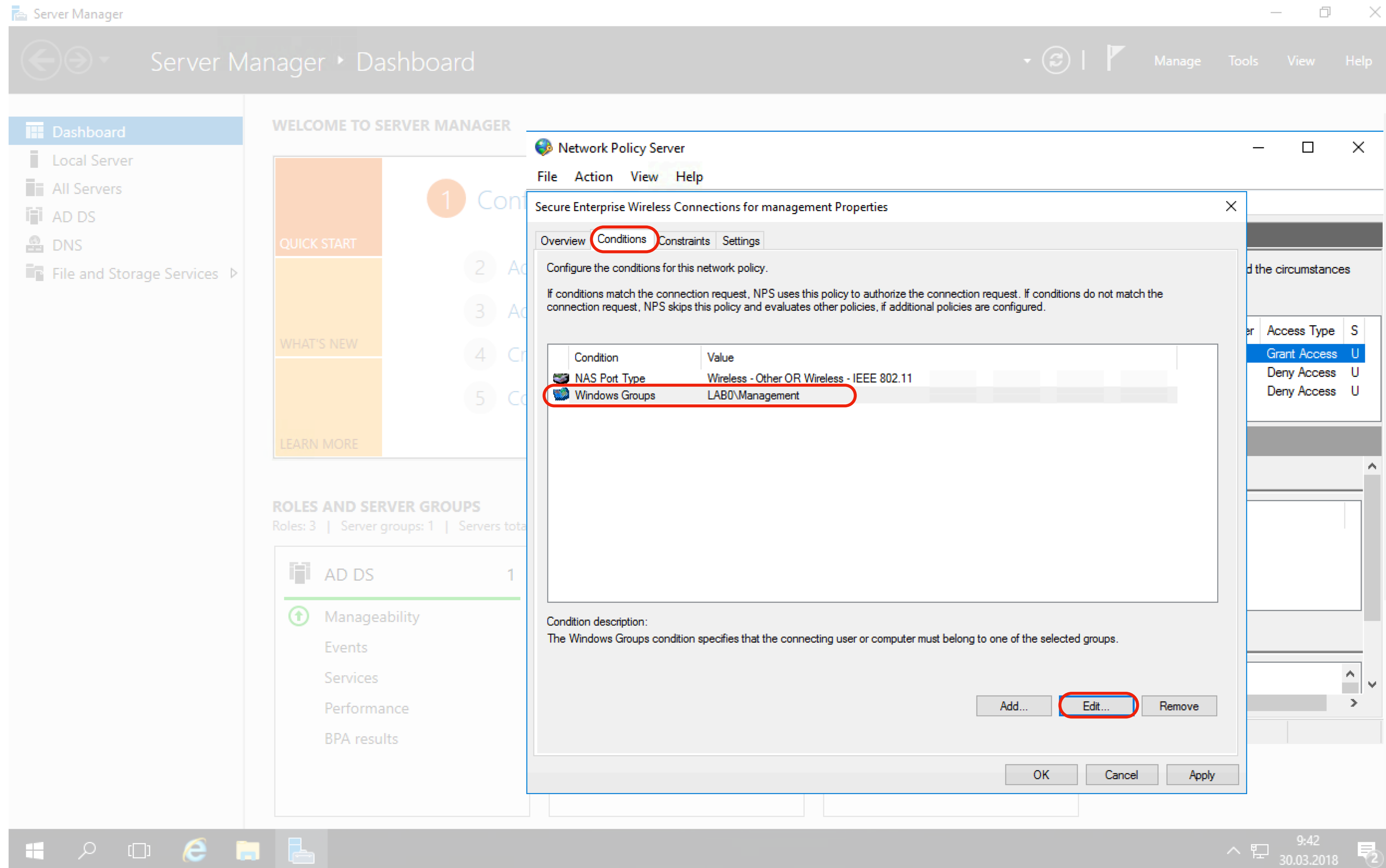
The screenshot shows the Windows Server Manager interface for a Network Policy Server. The left sidebar shows the navigation pane with 'Network Policy Server' selected. The main area displays the 'Network Policies' list. A context menu is open over the policy 'Secure Enterprise Wireless Connections for management', with the 'Properties' option highlighted in blue. The policy details pane on the right shows the following configuration:

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

The 'Settings' section below the conditions is also visible, showing a table with 'Setting' and 'Value' columns.

Configure NPS - Radius

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



The screenshot shows the Windows Server Manager interface. The 'Network Policy Server' console tree is expanded to 'Secure Enterprise Wireless Connections for management Properties'. The 'Conditions' tab is selected, showing a table of conditions. The 'Windows Groups' condition is highlighted with a red circle, and its 'Edit...' button is also circled in red. The 'Edit...' button is highlighted with a red circle.

Network Policy Server
File Action View Help

Secure Enterprise Wireless Connections for management Properties

Overview **Conditions** Constraints Settings

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.

Add... **Edit...** Remove

OK Cancel Apply

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”

The screenshot shows the Windows Server Manager interface. In the background, the 'Network Policy Server' console is open, displaying the 'Settings' tab for a policy. The 'RADIUS Attributes' section is expanded, and 'Vendor Specific' is selected. The 'Add...' button is highlighted with a red circle. In the foreground, a 'Secure Enterprise Wireless Connections for management Properties' dialog box is open, showing a table of attributes. The 'Add...' button in this dialog is also highlighted with a red circle.

Name	Vendor	Value

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

Configure NPS - Radius

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

The screenshot shows the Windows Server Manager interface with the Network Policy Server (NPS) configuration window open. The 'Secure Enterprise Wireless Connections for management Properties' dialog is displayed, with the 'Settings' tab selected. The 'Add Vendor Specific Attribute' dialog is open, showing a list of attributes. The 'Vendor-Specific' attribute under the 'RADIUS Standard' vendor is selected. The 'Add...' button is highlighted with a red circle.

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

Configure NPS - Radius

The screenshot displays the Windows Server Manager interface for configuring a Network Policy Server (NPS). The main window is titled "Network Policy Server" and has tabs for "Overview", "Conditions", "Constraints", and "Settings". The "Settings" tab is active, showing "Secure Enterprise Wireless Connections for management Properties". A dialog box titled "Add Vendor Specific Attribute" is open, with the "Attribute Information" sub-dialog also open. The "Attribute Information" dialog shows "Attribute name: Vendor-Specific", "Attribute number: 26", and "Attribute format: OctetString". The "Attribute values" table is empty, and the "Add..." button is highlighted with a red circle. The background shows the "Roles and Server Groups" section with "AD DS" selected.

Name	Vendor	Value
USR-Tunnel-		
USR-Unauth-		
USR-VPN-En-		
USR-VPN-GV-		
USR-VTS-Se-		
Vendor-Spec-		

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

- 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

The screenshot displays the Windows Server Manager interface for configuring a Network Policy Server (NPS). The main window is titled "Network Policy Server" and shows the "Secure Enterprise Wireless Connections for management Properties" dialog box. The "Settings" tab is selected, and the "Add Vendor Specific Attribute" dialog box is open. In this dialog, the "Vendor" is set to "All", and the "Attributes" list includes "Vendor-Specific". The "Enter Vendor Code" field is highlighted with a red box and contains the value "14988". Below this, the "Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes" section has the "Yes, it conforms" radio button selected, also highlighted with a red box. A "Configure Attribute..." button is also highlighted with a red box. The background shows the "Secure Enterprise Wireless Connections for management Properties" dialog box with the "Settings" tab active, and the "Add Vendor Specific Attribute" dialog box is open over it. The "Vendor-Specific Attribute Information" dialog box is also open over the "Add Vendor Specific Attribute" dialog box. The "Enter Vendor Code" field is highlighted with a red box and contains the value "14988". Below this, the "Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes" section has the "Yes, it conforms" radio button selected, also highlighted with a red box. A "Configure Attribute..." button is also highlighted with a red box. The background shows the "Secure Enterprise Wireless Connections for management Properties" dialog box with the "Settings" tab active, and the "Add Vendor Specific Attribute" dialog box is open over it.

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”

The screenshot displays the Windows Server Manager interface for configuring a Network Policy Server (NPS). The 'Settings' tab is selected, and the 'Add Vendor Specific Attribute' dialog is open. Within this dialog, the 'Configure VSA (RFC Compliant)' sub-dialog is also open, showing the following configuration:

- Vendor: All
- Vendor-assigned attribute number: 26
- Attribute format: Decimal
- Attribute value: 11

Red circles highlight the 'Vendor-assigned attribute number' field, the 'Attribute format' dropdown, the 'Attribute value' field, and the 'OK' buttons in both dialog boxes. The background shows the 'ROLES AND SERVER GROUPS' section with 'AD DS' and 'Manageability' listed.

Configure NPS - Radius

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

The screenshot shows the Windows Server Manager interface for configuring a Network Policy Server (NPS). The 'Vendor-Specific Attribute Information' dialog box is open, showing the configuration for a Vendor-Specific Attribute (VSA). The 'Vendor assigned attribute number' is set to 27, the 'Attribute format' is set to Decimal, and the 'Attribute value' is set to 0. The 'OK' button is highlighted with a red circle. The background shows the 'Secure Enterprise Wireless Connections for Management Properties' window with the 'Settings' tab selected.

- For more options see [https://wiki.mikrotik.com/wiki/Manual:RADIUS Client/vendor dictionary](https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client/vendor_dictionary)

Configure NPS - Radius

Server Manager Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

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

AD DS 1

Manageability

Events

Services

Performance

BPA results

Network Policy Server

File Action View Help

Secure Enterprise Wireless Connections for Management Properties

Overview Conditions Constraints Settings

Configure If condition

Add Vendor Specific Attribute

Settings:

To add an attribute

To add a Vendor

Vendor: All

Attributes:

Name	Attribute values:
USR-Tunnel	
USR-Unauth	
USR-VPN-En	
USR-VPN-GV	
USR-VTS-Se	
Vendor-Spec	

Description: Specifies the su

Attribute Information

Attribute name: Vendor-Specific

Attribute number: 26

Attribute format: OctetString

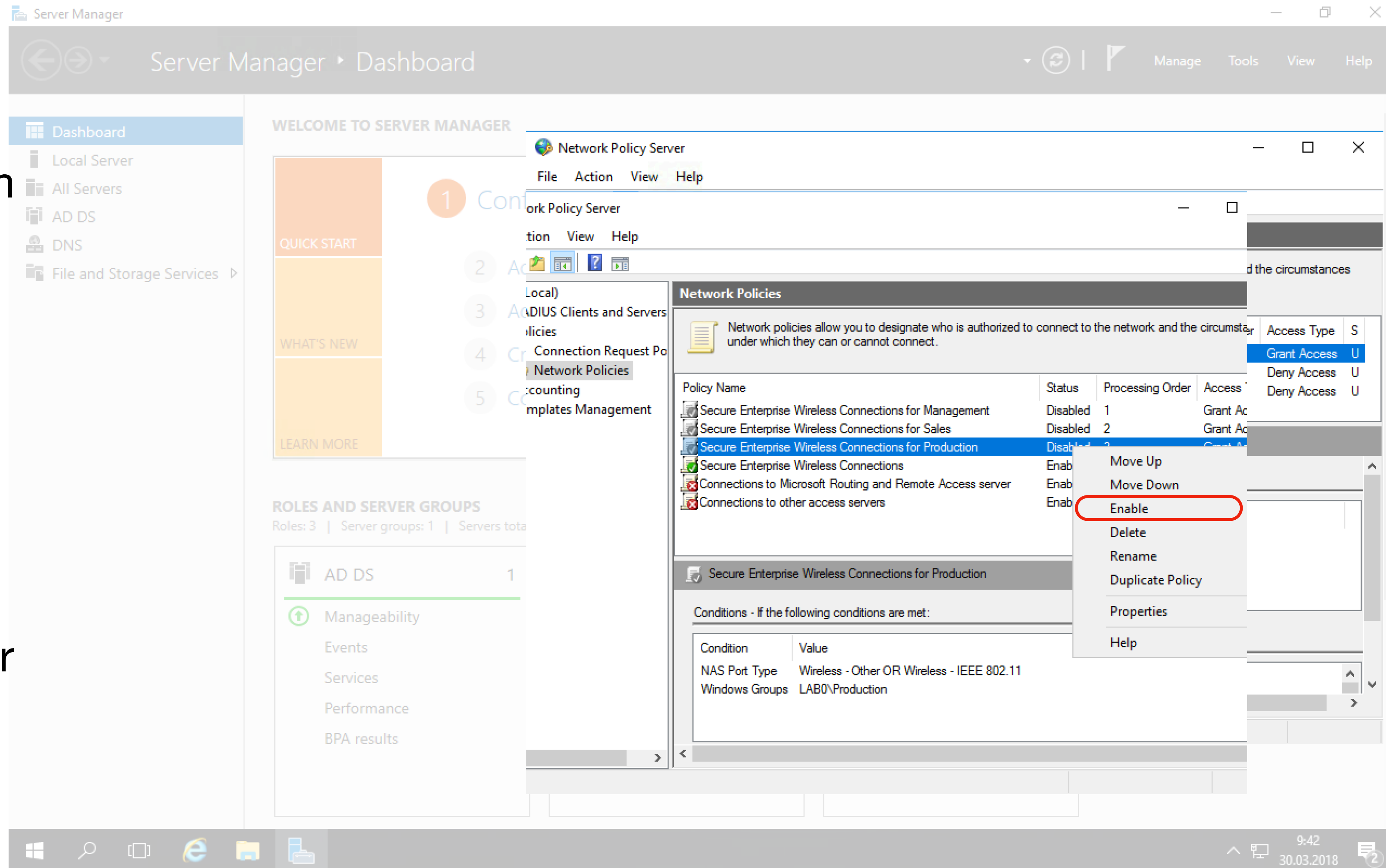
Vendor	Value
Vendor Code: 14988	11
Vendor Code: 14988	0

Buttons: Add..., Edit..., Remove, Move Up, Move Down, OK, Cancel, Add..., Close

- 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.



The screenshot shows the Windows Server Manager interface for a Network Policy Server. The 'Network Policies' list is displayed with the following items:

Policy Name	Status	Processing Order	Access Type
Secure Enterprise Wireless Connections for Management	Disabled	1	Grant Access
Secure Enterprise Wireless Connections for Sales	Disabled	2	Grant Access
Secure Enterprise Wireless Connections for Production	Disabled	3	Grant Access
Secure Enterprise Wireless Connections	Enabled		
Connections to Microsoft Routing and Remote Access server	Enabled		
Connections to other access servers	Enabled		

The context menu for the 'Secure Enterprise Wireless Connections for Production' policy is open, showing the following options:

- Move Up
- Move Down
- Enable** (highlighted with a red circle)
- Delete
- Rename
- Duplicate Policy
- Properties
- Help

The 'Conditions' section for the selected policy is also visible:

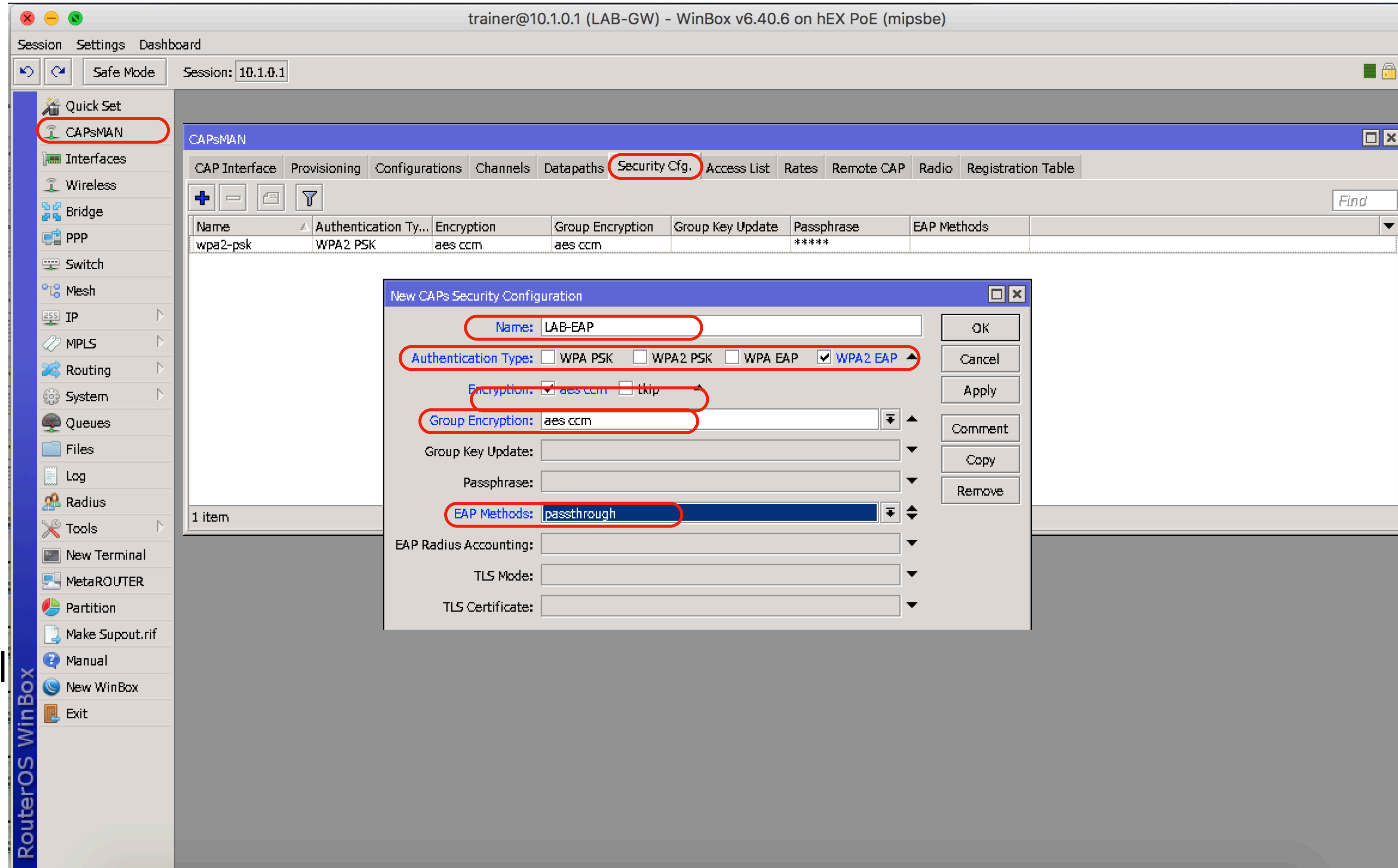
Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	LAB0\Production

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



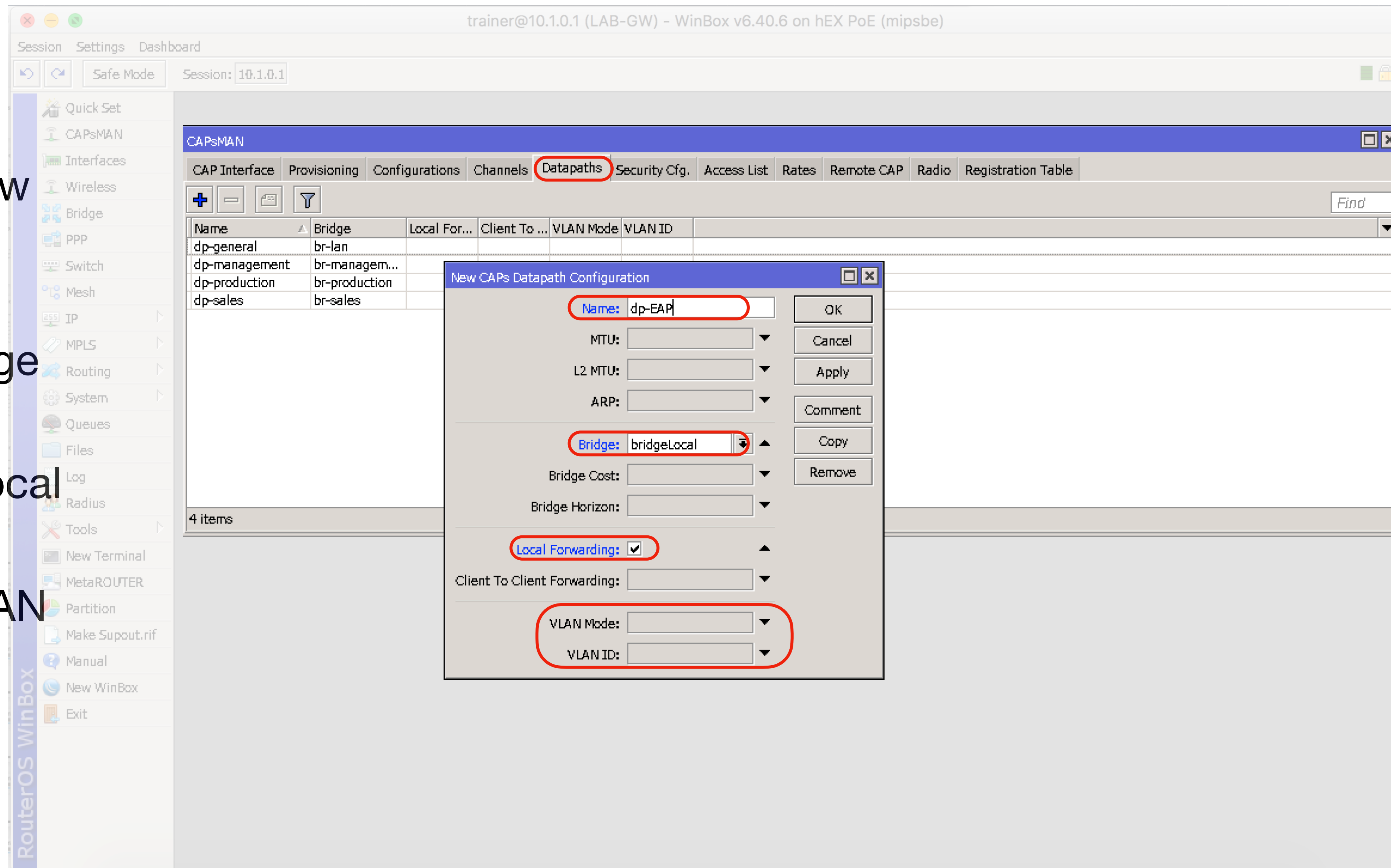
The screenshot shows the RouterOS WinBox interface. The CAPsMAN configuration page is open, and the 'Security Cfg.' tab is selected. A table lists existing configurations, including 'wpa2-psk'. A 'New CAPs Security Configuration' dialog box is open, showing the following settings:

- Name: LAB-EAP
- Authentication Type: WPA2 EAP
- Encryption: aes ccm
- Group Encryption: aes ccm
- EAP Methods: passthrough

The dialog also includes fields for Group Key Update, Passphrase, EAP Radius Accounting, TLS Mode, and TLS Certificate, along with OK, Cancel, Apply, Comment, Copy, and Remove buttons.

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



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

Session Settings Dashboard

Safe Mode Session: 10.1.0.1

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit

CAPsMAN

CAP Interface Provisioning Configurations Channels **Datapaths** Security Cfg. Access List Rates Remote CAP Radio Registration Table

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: []

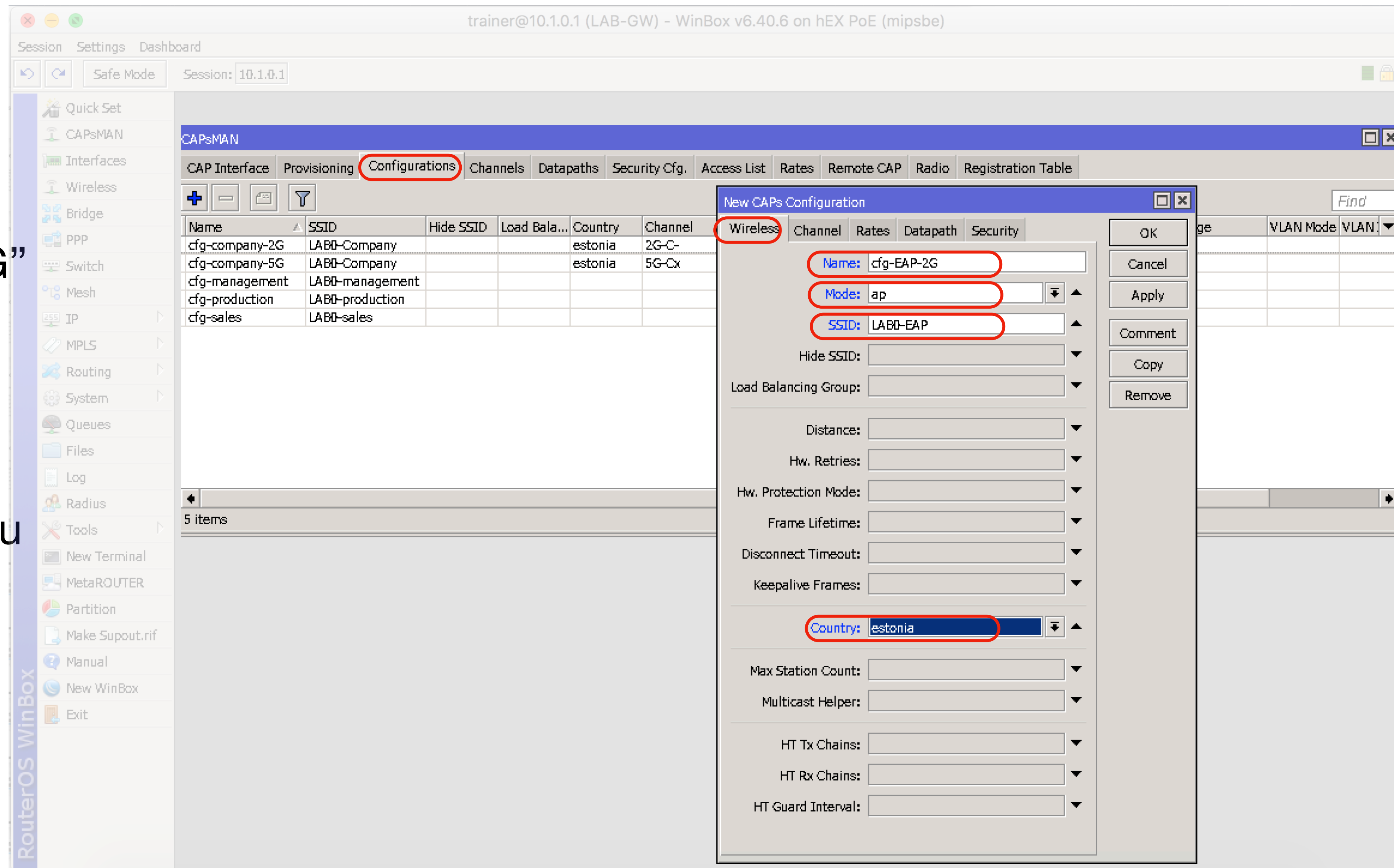
VLAN Mode: []

VLAN ID: []

OK
Cancel
Apply
Comment
Copy
Remove

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



The screenshot shows the RouterOS WinBox interface. The main window is titled "CAPsMAN" and has several tabs: CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. The "Configurations" tab is active, displaying a table of existing configurations:

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				

A "New CAPs Configuration" dialog box is open, showing the "Wireless" tab. The fields are filled with the following values:

- Name: cfg-EAP-2G
- Mode: ap
- SSID: LAB0-EAP
- Country: estonia

Other fields like Hide SSID, Load Balancing Group, Distance, Hw. Retries, Hw. Protection Mode, Frame Lifetime, Disconnect Timeout, Keepalive Frames, Max Station Count, Multicast Helper, HT Tx Chains, HT Rx Chains, and HT Guard Interval are empty.

Add New Configuration

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

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

The screenshot shows the RouterOS WinBox interface. The main window is titled "CAPsMAN" and has several tabs: CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. The "Configurations" tab is active, displaying a table of configurations:

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

A "New CAPs Configuration" dialog box is open, showing the "Channel" tab. The "Channel" dropdown menu is set to "2G-C-". Other fields in the dialog include Frequency, Control Channel Width, Band, Extension Channel, Tx Power, Save Selected, Reselect Interval, and Skip DFS Channels. The dialog also has buttons for OK, Cancel, Apply, Comment, Copy, and Remove.

Add New Configuration

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

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

Session Settings Dashboard

Safe Mode Session: 10.1.0.1

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit

CAPsMAN

CAP Interface Provisioning **Configurations** Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

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

New CAPs Configuration

Wireless Channel Rates **Datapath** Security

Datapath: dp-EAP

MTU:

L2 MTU:

ARP:

Bridge:

Bridge Cost:

Bridge Horizon:

Local Forwarding:

Client To Client Forwarding:

VLAN Mode:

VLAN ID:

OK
Cancel
Apply
Comment
Copy
Remove

Add New Configuration

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

The screenshot shows the RouterOS WinBox interface. The main window is titled "CAPsMAN" and has several tabs: CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. The "Configurations" tab is active, displaying a table with the following data:

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				

A "New CAPs Configuration" dialog box is open, showing the "Security" tab. The "Security" dropdown menu is set to "LAB-EAP". Other fields in the dialog include Authentication Type, Encryption, Group Encryption, Group Key Update, Passphrase, EAP Methods, EAP Radius Accounting, TLS Mode, and TLS Certificate. The "OK" button is highlighted.

Add New Configuration

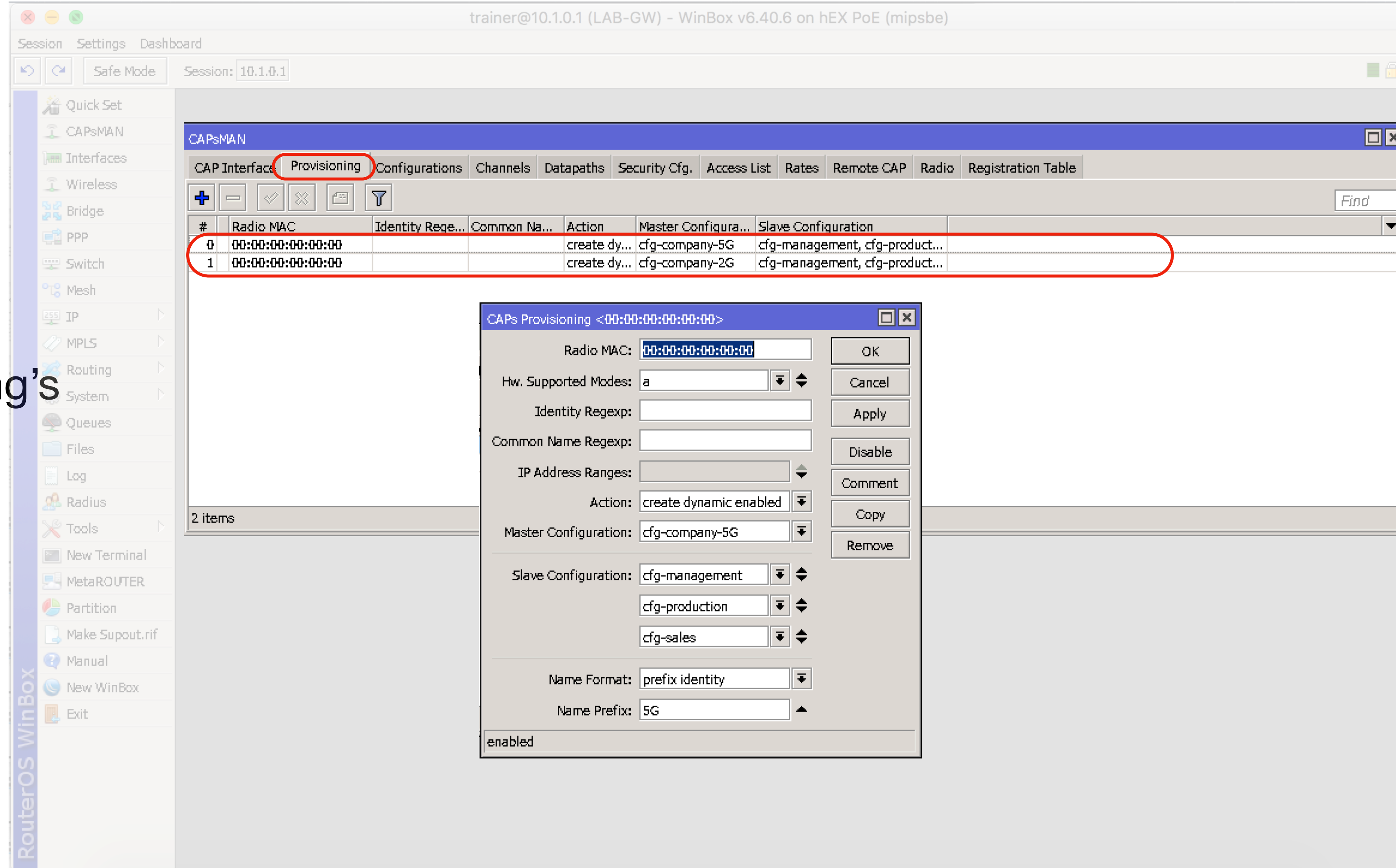
The screenshot shows the WinBox interface for a RouterOS device. The 'CAPsMAN' configuration window is open, and the 'Configurations' tab is selected. A table lists various configurations, with 'cfg-EAP-5G' highlighted by a red circle. The table has the following columns: Name, SSID, Hide SSID, Load Bala..., Country, Channel, Frequency, Band, Rate, Datapath, Bridge, VLAN Mode, and VLAN. The 'cfg-EAP-5G' row shows 'LAB0-EAP' as the SSID, 'estonia' as the country, '5G-Cx' as the channel, and 'dp-EAP' as the datapath.

Name	SSID	Hide SSID	Load Bala...	Country	Channel	Frequency	Band	Rate	Datapath	Bridge	VLAN Mode	VLAN
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			

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

Update Provisioning's

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



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

Session Settings Dashboard

Safe Mode Session: 10.1.0.1

RouterOS WinBox

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

#	Radio MAC	Identity Regexp	Common Name	Action	Master Configuration	Slave Configuration
0	00:00:00:00:00:00			create dynamic enabled	cfg-company-5G	cfg-management, cfg-production, cfg-sales
1	00:00:00:00:00:00			create dynamic enabled	cfg-company-2G	cfg-management, cfg-production, cfg-sales

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

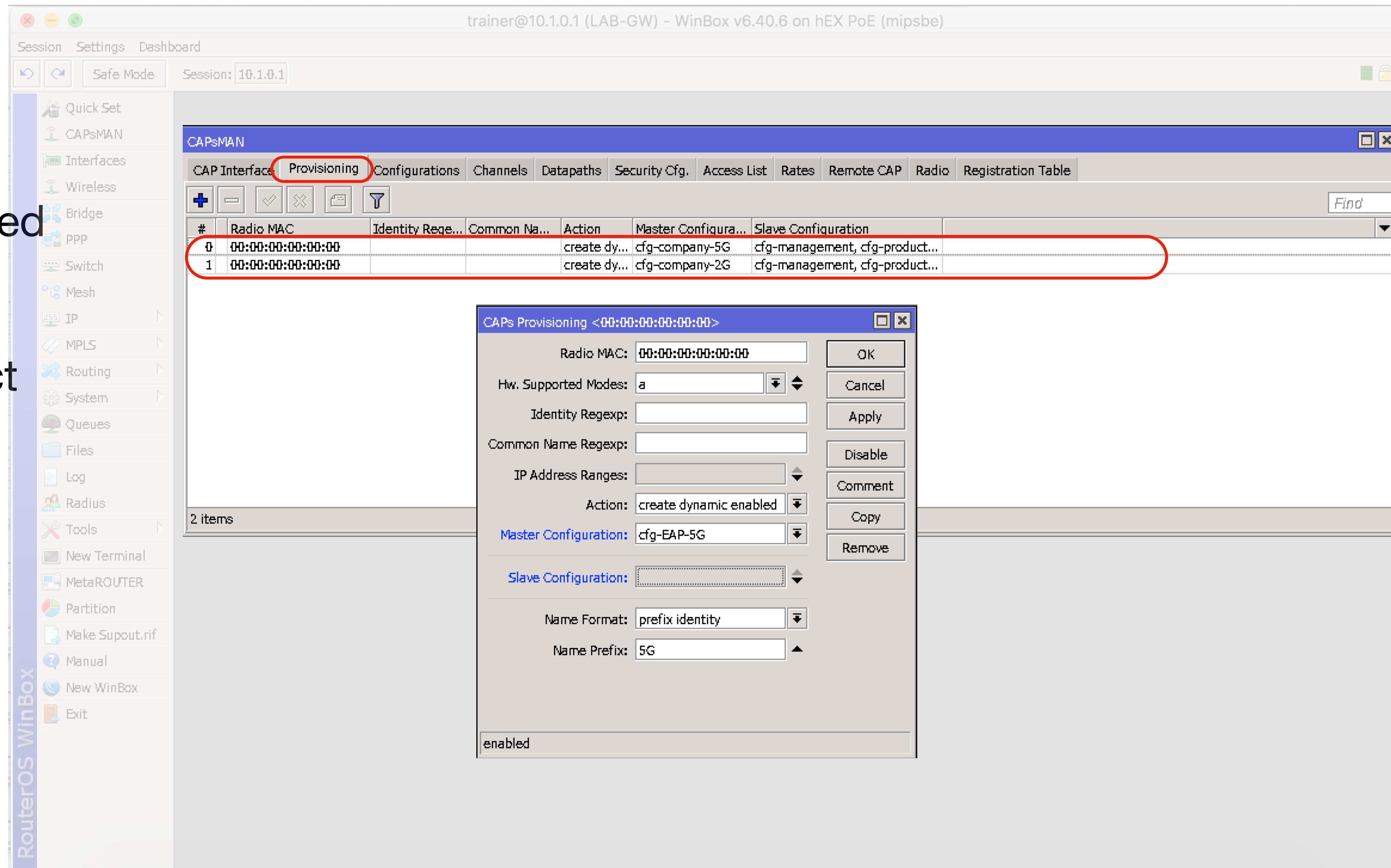
Name Prefix: 5G

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

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



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

Session Settings Dashboard

Safe Mode Session: 10.1.0.1

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

#	Radio MAC	Identity Regexp	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

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Provisioning

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

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

Session Settings Dashboard

Safe Mode Session: 10.1.0.1

RouterOS WinBox

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

#	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

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

Session Settings Dashboard

Safe Mode Session: 10.1.0.1

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates **Remote CAP** Radio Registration Table

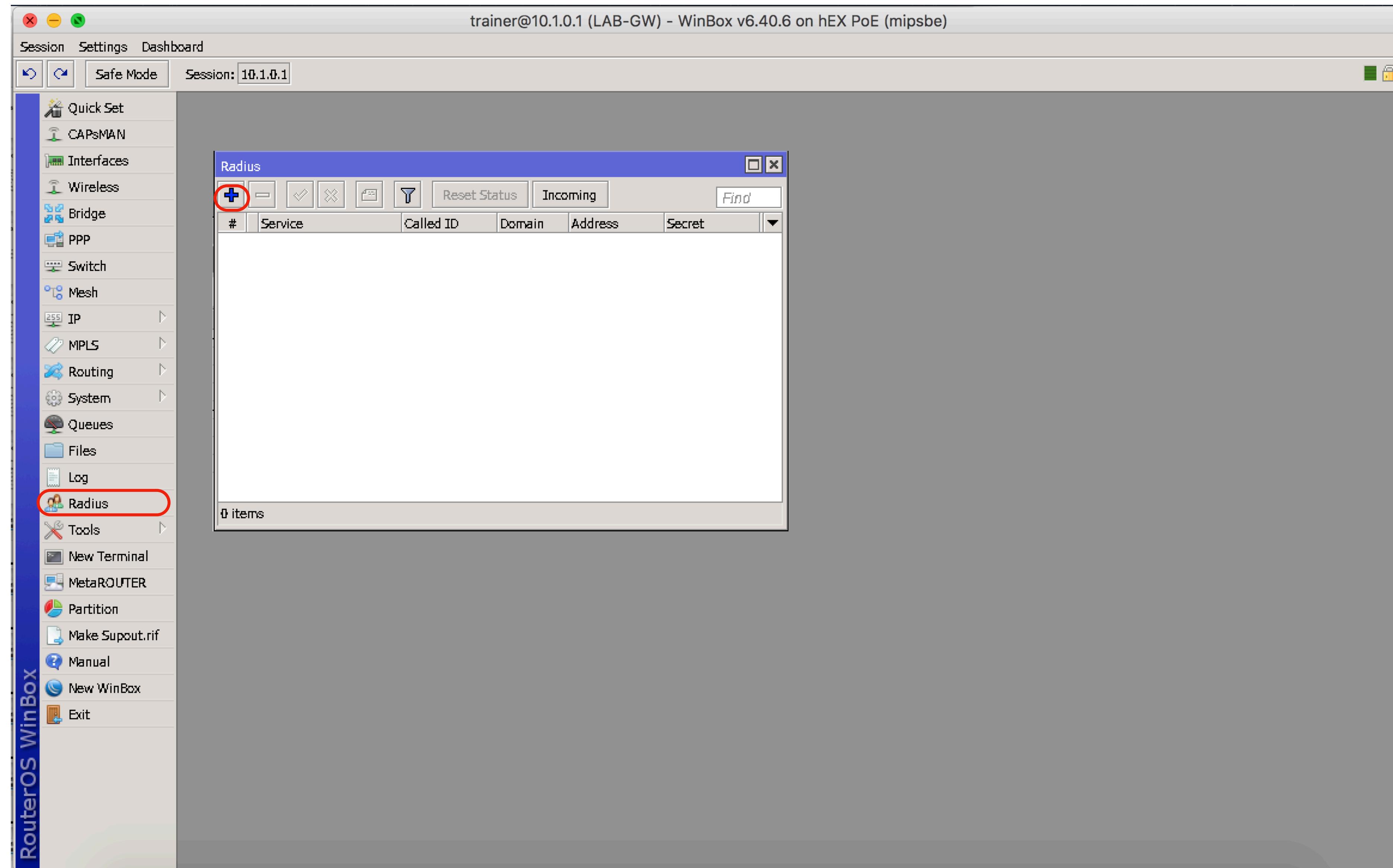
Provision Upgrade Set Identity Find

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)

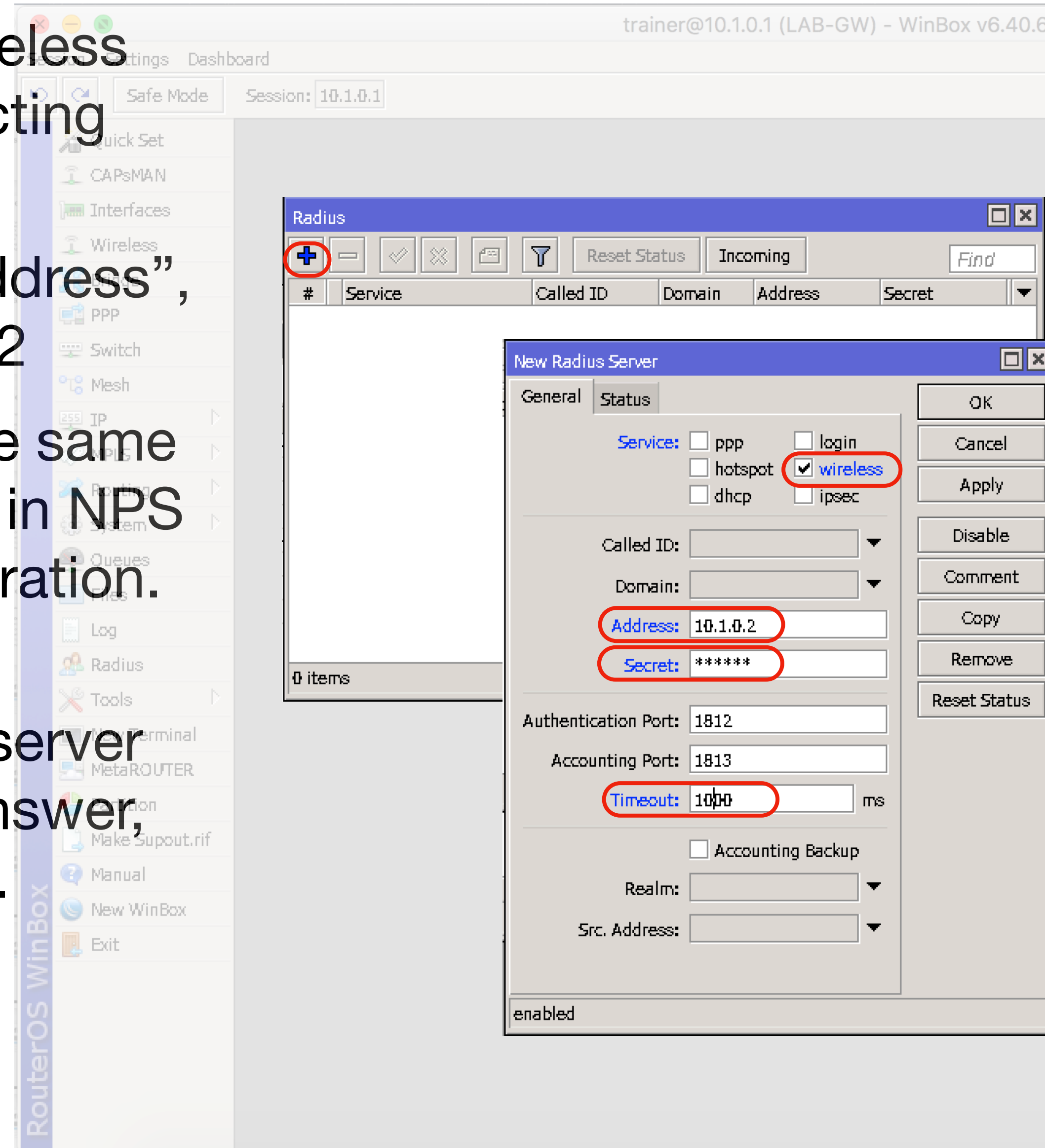
Configure RADIUS Client

- 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.



The screenshot shows the RouterOS WinBox interface. The 'Radius' window is open, displaying a table with columns: #, Service, Called ID, Domain, Address, Secret. A red circle highlights the '+' button in the top-left corner of the table. The 'New Radius Server' dialog is open, showing the following configuration:

- Service:** wireless (highlighted with a red circle)
- Address:** 10.1.0.2 (highlighted with a red circle)
- Secret:** ***** (highlighted with a red circle)
- Timeout:** 1000 ms (highlighted with a red circle)

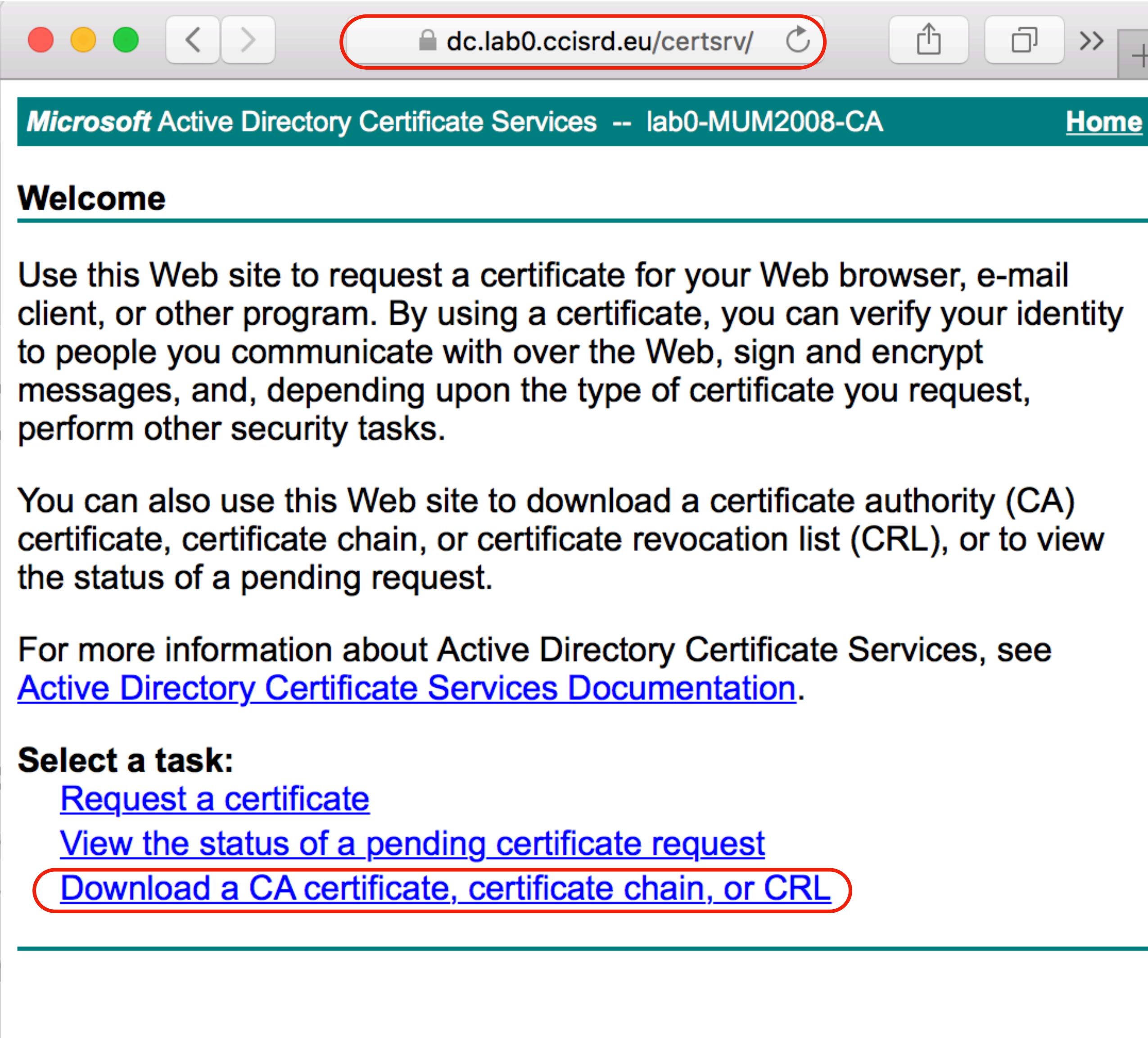
Other fields in the dialog include: Called ID, Domain, Authentication Port (1812), Accounting Port (1813), and Src. Address. The dialog is set to 'enabled'.

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.



dc.lab0.ccisrd.eu/certsrv/

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.

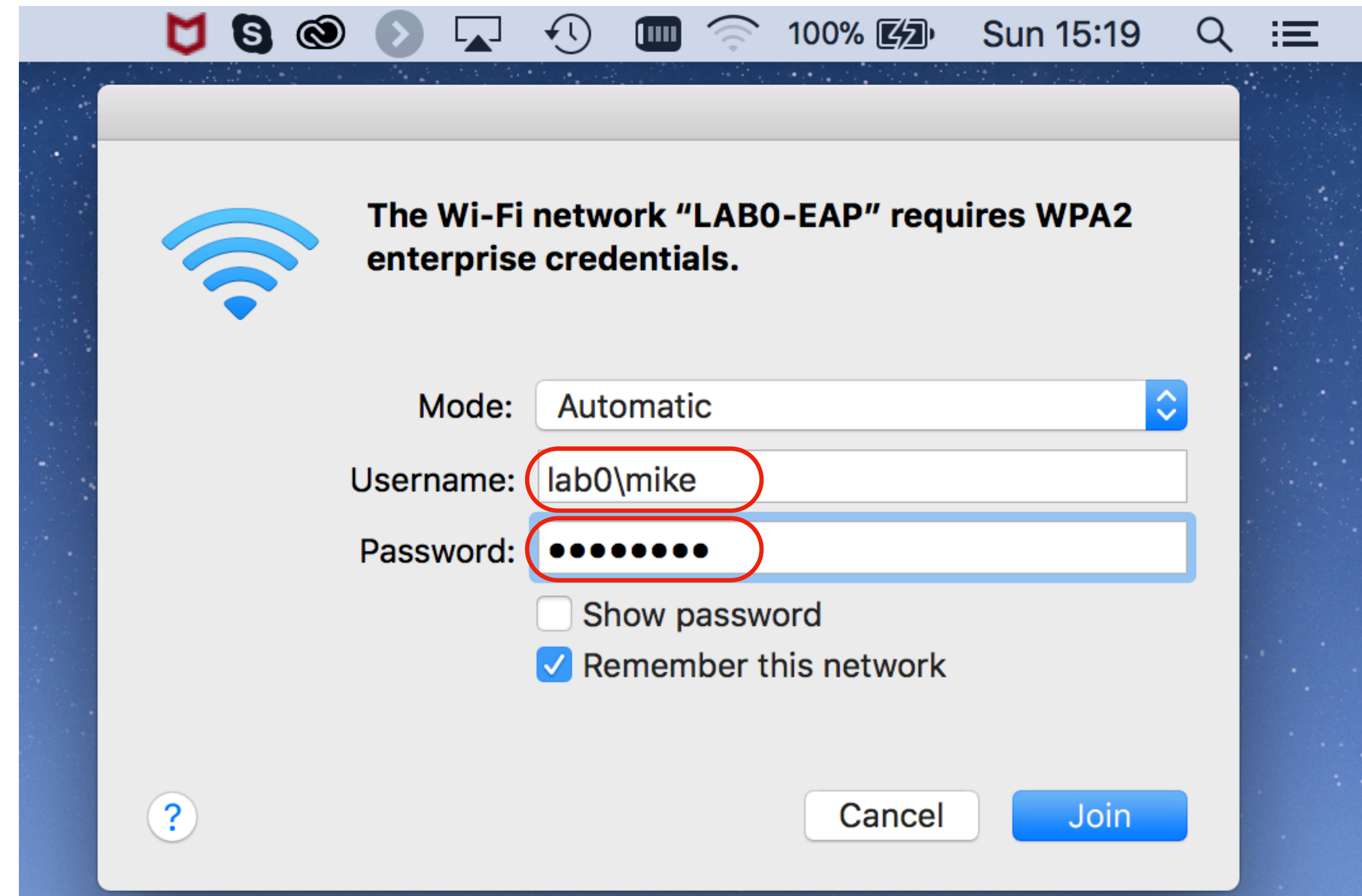
For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

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 a similar way.
- If your computer is a domain member, CA certificate will be installed automatically.



Verify connected users

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

Session Settings Dashboard

Safe Mode Session: 10.1.0.1

RouterOS WinBox

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

CAPs Scanner Find

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

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

Check Status Find

	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

```

/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