

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 ..

t all. recated



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

WPA(2)-PSK



- 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.

WPA-EAP



- 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.

Next problem.



Dynamic VLAN

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



Sounds complicated?



What we already have?

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







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

What we need?





- Configure CA
- Configure NPS RADIUS Server
- Reconfigure CAPsMAN
- Install CA on client device's only if not domain member

Next Steps



Add roles and features

Server Manager • Dashboard WELCOME TO SERVER MANAGER Dashboard Local Server All Servers AD DS 🖀 DNS QUICK START ■ File and Storage Services ▷ WHAT'S NEW 4 LEARN MORE ROLES AND SERVER GROUPS Roles: 3 | Server groups: 1 | Servers total: 1 ΕŤ. AD DS \odot Manageability Events Services Performance BPA results 🖶 🔎 🗆 🧲 🔚

🚡 Server Manager

 In Server Manager click Add roles and features"

- (2) |

Manage Tools View



5 Connect this server to cloud services







All Servers i AD DS 🔒 DNS ■ File and Storage Services ▷

🚡 Server Manager

Local Server



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

Install Roles

		- 0 ×
nager 🕨 Dash		🕶 🗭 🏲 Manage Tools View Help
WELCOME TO SERV	Add Roles and Features Wizard	
QUICK START	Before you begin Before You Begin	DC.lab0.ccisrd.eu This wizard helps you install roles, role services, or features. You determine which roles, role services, or
WHAT'S NEW	Installation Type Server Selection	features to install based on the computing needs of your organization, such as sharing documents, or hosting a website. To remove roles, role services, or features:
LEARN MORE	Server Roles Features Confirmation Results	Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed
ROLES AND SERVER Roles: 3 Server group		If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
AD DS Manageabilit Events Services		To continue, click Next.
Performance BPA results		Skip this page by default
		< Previous Next > Install Cancel
		^ 腔 30.02.2018 ♥



Install Roles - Installation Type

WELCOME TO SERVER MANAGER Local Server All Servers AD DS B DNS ■ File and Storage Services ▷ **ROLES AND SERVER** AD DS Manageabil Events Services Performance BPA results 🖶 🔎 🗆 🧲 🔚

🚡 Server Manager

 Select "Role-based or feature-based installation" and click "Next"

📥 Add Roles and Features Wizard DESTINATION SERVER Select installation type DC.lab0.ccisrd.eu Select the installation type. You can install roles and features on a running physical computer or virtual Before You Begin machine, or on an offline virtual hard disk (VHD). Installation Type Role-based or feature-based installation Server Selection Configure a single server by adding roles, role services, and features. Server Roles Remote Desktop Services installation Features Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based Confirmation or session-based desktop deployment. Results Next > < Previous Install





Install Roles - Select Server

WELCOME TO SEE Local Server All Servers i AD DS 🔒 DNS File and Storage Services ▷ ROLES AND SERV AD DS Manageab Events Performan **BPA** results 🚛 🔎 🗆 🥭 🔚

👝 Server Manager

 Select server, in our case there is only one server, and click "Next"

				Manage Tools
RVER MANAGER				- 0
Select destination	server			DESTINATION S DC.lab0.co
Before You Begin Installation Type Server Selection Server Roles Features	 Select a server or a virtual Select a server from Select a virtual hard Server Pool Filter: 	al hard disk on which the server pool disk	to install roles and features	n ha
Confirmation Results	Name DC.lab0.ccisrd.eu	IP Address 10.1.0.2	Operating System Microsoft Windows Serv	er 2016 Datacenter
ilit	1 Computer(s) found This page shows servers	that are running Wir	ndows Server 2012 or a new	er release of Windows S
ce	and that have been adde newly-added servers fro	ed by using the Add m which data collect	Servers command in Server ion is still incomplete are no	Manager. Offline servers t shown.
		< Pre	evious Next >	Install





Select Server Roles

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

		Server	Mar	nage		
	Dashboard			WELCO	ОМЕ ТО) SEI
	Local Server					
	All Servers					
i i	AD DS					
	DNS					
	File and Storag	ge Services	⊳			
				LEARN		
				ROLES Roles: 3	AND S	ERV er gro
				•	Manag Events Service Perforr BPA re	jeab es man sult:
		j 🬔		L		

👝 Server Manager

shboard

· 🕄 | 🚩

nage Tools







		Server	Mar	nag			23
				WEI	CC	ME TO S	E
	Dashboard						
	Local Server						
	All Servers						
	AD DS						
	DNS						
2	File and Stora	ge Services		WH	IAT':		
				ROL	. ES s: 3	AND SEF	Q I
					Ð	Managea Events Services Performa BPA resu	at
	_ 2	ı 🦲		r i	<u> </u>		

📥 Server Manager

Accept default and click "next"

Select features



< Previous

Next >

Install





AD Certificate Services

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



👝 Server Manager

shboard

WELCOME TO SERVER MANAGER 📥 Add Roles and Features Wizard Active Directory Certificate Services Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios Before You Begin such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Installation Type Access Protection (NAP), encrypting file system (EFS) and smart card log on. Server Selection Things to note: Server Roles • The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this Features server to a domain controller, complete these changes before installing the CA. For more AD CS information, see certification authority naming. Role Services Network Policy and Acces... Confirmation Results

< Previous Next > Install C





		📥 Server Manager			
		EO	Server I	Manage	
		Dashboard		WELO	OME TO S
		Local Server			
		An Servers			
		🚔 DNS			
•	Select "Certificate Auth	Ority",	ige Services 🖇	WHAT	
	"Certificate Enrollment				
	Web Service" and "Cert	ificate			
	Authority Web Service"			LEARN	
	Click "Next"			ROLES Roles: 3	S AND SER
				i iii	AD DS
				1	Managea
					Events
					Performa
					BPA resul
		ک	נ 🬔		

Install CA role



Ð		×	
View	He	lp	
SERVER cisrd.eu	<		
b nputers cates ot a omain- y of the icate s e to tic e users			
ancel]		
			\sim
9:42			

^ Ё 30.03.2018 ℃



Install NPS role



🚡 Server Manager

Click "Next"

			- 0 X
			Manage Tools View Help
Add Roles and Features Wizard	nd Access Services		- C X DESTINATION SERVER DC.lab0.ccisrd.eu
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Network Policy and Acces Web Server Role (IIS) Role Services Confirmation Results	 Network Policy and Access Services allows you to de authentication and authorization using Network Polic Things to note: You can deploy NPS as a Remote Authentication E After installing NPS using this wizard, you can cor NPS console. 	fine and enforce policie icy Server (NPS). Dial-In User Service (RA nfigure NPS from the N	DIUS) server and proxy. IPAS home page using the
	< Previous	Next >	Install Cancel 9:42 지 당 30.03.2018



		Server	Ma				Da	
	Dashboard			W	ELCO	ОМЕ ТО) S	ER
	Local Server							
	All Servers							
1	AD DS							
0	DNS							
P	File and Storag	ge Services	⊳					
				L	EARN			
				R	OLES	AND S	SER	V
					oles: 3	Serv	er g	
					iji	AD D	S	
					€	Manag	gea	bil
						Events	5	
						Servic	es	
						Perfor	ma	nc
						BPA re	sul	ts
	D D	1 🥖						

📥 Server Manager

Click "Next"

shboard



		þ	>	<
loois	Vie		нер	
_		×		
STINATI DC.la	ON SER\ b0.ccisrd	/ER l.eu		
h intrar hancec T, and \	nets and I securi Windov	d ty, vs		
services	s that and H	TTP		
	Cance	:I		
~ 또	9: 30.03	42 .2018	Ę	





Accept default and click "Next"

📥 Server Manager

	Ø		×	
View			lp	
SERVE	× R su			
for d Wel e the al or le an o ns.	D			
ancel				
9:42 30.03.2	2 2018	:	2	ĺ





🚡 Server Manager

Accept default and click "Install"

📥 Add Roles and Features Wizard DESTINATION Confirm installation selections DC.lab0.co To install the following roles, role services, or features on selected server, click Install. Before You Begin Restart the destination server automatically if required Installation Type Optional features (such as administration tools) might be displayed on this page because they have Server Selection been selected automatically. If you do not want to install these optional features, click Previous to Server Roles their check boxes. Features .NET Framework 4.6 Features AD CS ASP.NET 4.6 Role Services WCF Services Network Policy and Acces... HTTP Activation Web Server Role (IIS) Active Directory Certificate Services Role Services Certification Authority Confirmation Certificate Enrollment Web Service Results Network Policy and Access Services Remote Server Administration Tools Role Administration Tools Export configuration settings Specify an alternate source path Install < Previous Next >

	_	đ	×	
Tools			Help	
_		Х		
STINATI DC.lat	ON SERV 00.ccisrd.	'ER .eu		
use the Previou	y have us to cle	ear		
		^		
	Cance	~ I		
^ 또	9:4 30.03	42 .201 <u>8</u> _	5	



WELCOME TO SER Local Server All Servers AD DS 🔒 DNS ■ File and Storage Services ▷ **ROLES AND SERV** AD DS Manageabi Events Performan BPA results 🖶 🔎 🗆 🥭 🔚 📥

👝 Server Manager

 After installation is completed, click "Close"

		- 闭 🚩 Man	age Tools
۲v	ER MANAGER		
	Add Roles and Features Wizard		- 0
	Installation progre	SS	DESTINATION S DC.lab0.co
	Before You Beain	View installation progress	
	Installation Type	Eesture installation	
	Server Selection		
	Server Roles	Configuration required. Installation succeeded on DC.lab0.ccisrd.eu.	
	Features	Active Directory Certificate Services	
	AD CS	Additional steps are required to configure Active Directory Certificate Service	es on the
	Role Services	destination server	
	Network Policy and Acces	Configure Active Directory Certificate Services on the destination server	
EF	Web Server Role (IIS)	Certificate Enrollment Web Service	
pul	Role Services	.NET Framework 4.6 Features	
	Confirmation	ASP.NET 4.6	
_	Results	WCF Services HTTP Activation	
ilit		Network Policy and Access Services	
		page again by clicking Notifications in the command bar, and then Task	rogress or open Details.
ce		Export configuration settings	
;			
		< Previous Next >	Ca Ca





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

Next Steps



• In Server Manager Dashboard select "Configure Active **Directory Certificate** Services.."



Configure CA

				_			
1		AD DS	1		0	DNS	1
bility	•	Manageability			€	Manageability	
		Events				Events	
		Services				Services	
nce		Performance				Performance	
ts		BPA results				BPA results	





	Server	Mar	nage		as
Dashboard			WELC	OME TO	SEI
 Dashboard Local Server All Servers AD DS DNS File and Storage 	ge Services		QUICK WHAT LEARN ROLES Roles: 3	START START SNEW MORE MORE MORE Manage Events Services Perform BPA res	RV grd an ults
	ı 🬔		L		

🚡 Server Manager

Accept default and click "Next"

Configure CA

RVER MANAGER 📥 AD CS Configuration — DESTINATION SERVER 1 Con Credentials DC.lab0.ccisrd.eu Specify credentials to configure role services Credentials Role Services 3 A To install the following role services you must belong to the local Administrators group: Confirmation Standalone certification authority Progress Certification Authority Web Enrollment Results 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... oility More about AD CS Server Roles Next > Configure < Previous



^ 뛰 9:42 30.03.2018 ₹



		Server	Mar	nage		
				WELCO	OME TO S	SE
T	Local Server					
ŝ.	All Servers					
а. С	AD DS					
0	DNS					
	File and Stora	ge Services	⊳			
				LEARN		
				ROLES Roles: 3	AND SEI	R V
				•	Manage	ab
					Events	
					Services	
					Performa	an
					BPA resu	lt
	<u> </u>		-			

👝 Server Manager

Select "Enterprise CA" as Setup Type and click "Next"

Configure CA

RVER MANAGER 📥 AD CS Configuration 1 Conf Setup Type DESTINATION DC.lab0.c Specify the setup type of the CA Credentials Role Services Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) Setup Type simplify the management of certificates. Standalone CAs do not use AD DS to issue or man СА Туре certificates. Private Key Enterprise CA Cryptography Enterprise CAs must be domain members and are typically online to issue certificates or CA Name certificate policies. Validity Period O Standalone CA Certificate Database Standalone CAs can be members or a workgroup or domain. Standalone CAs do not req DS and can be used without a network connection (offline). Confirmation Progress oility More about Setup Type Configure < Previous Next >

	đ		×	
View		He	lp	
]	×			
SERV	ER eu			
to nage				
Ţ				
quire A	D			
ancel				

· ^ 맏 9:42 30.03.2018 **문**



WELCOME TO SERVER MANAGER Local Server All Servers i AD DS B DNS File and Storage Services ▷ ROLES AND SERVER GROUPS AD DS Manageability Events Performance BPA results 🖶 🔎 🗆 🤶 🔚 🔚

👝 Server Manager

Select "Root CA" as CA type and click "Next"

Configure CA



	þ		\times	
View		He	lp	
	×			
I SERV ccisrd	/ER .eu			
ig a sues it the Pl	s Kl			
icates	by			
Cancel				
9:42	2			~
30.03.2	018		2	



		Server	Mar	nage		
				WELCO	ME TO S	2 5
	Dashboard			VVELCC	JWIE TO S	
	Local Server					
	All Servers					
	AD DS					
0	DNS					
P	File and Storag	ge Services	\triangleright			
				LEARN		
				ROLES Roles: 3	AND SEI	R\ gr
				€	Manage	ab
					Events	
					Services	
					Performa	an
					BPA resu	ilt
	2	ı 🦲		L		

🚡 Server Manager

• Select "Create a new private key" and click "Next"

Configure CA

RVER MANAGER 📥 AD CS Configuration DESTINATION SERVER 1 Conf Private Key Specify the type of the private key Credentials Role Services To generate and issue certificates to clients, a certification authority (CA) must have a private key. Setup Type СА Туре Create a new private key Private Key Use this option if you do not have a private key or want to create a new private key. Cryptography Use existing private key CA Name Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Validity Period 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 Certificate Database import a certificate and use its associated private key. Confirmation Select an existing private key on this computer Progress Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source. oility More about Private Key < Previous Next > Configure





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



📥 Server Manager

Configure CA

📥 AD CS Configuration DESTINATION Con Cryptography for CA DC.lab0. Specify the cryptographic options Credentials Role Services Select a cryptographic provider: Key length: Setup Type × 2048 RSA#Microsoft Software Key Storage Provider СА Туре Private Key Select the hash algorithm for signing certificates issued by this CA: Cryptography SHA256 CA Name SHA384 SHA512 Validity Period SHA1 Certificate Database MD5 Confirmation Allow administrator interaction when the private key is accessed by the CA. Progress Results More about Cryptography Configure < Previous Next >

	þ		\times	
View		Helj	p	
	×			
SERV	ER .eu			
	<u>·</u>			
Cancel				

〜 EP <u>9:42</u> 30.03.2018 **見**





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



🚡 Server Manager

Configure CA

		🕶 🧭 🚩 Manage Tools
RVER MANAGER	AD CS Configuration	—
1 Cont	CA Name	DESTINATION DC.lab0.c
2 Ac	Credentials Role Services	Specify the name of the CA
3 Ad 4 Cr 5 Cd /ER GROUPS oups: 1 Servers tota	Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	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 be modified. Common name for this CA: Iab0-MUM2008-CA Distinguished name suffix: DC=Iab0,DC=ccisrd,DC=eu Preview of distinguished name: CN=Iab0-MUM2008-CA,DC=Iab0,DC=ccisrd,DC=eu
oility		More about CA Name < Previous Next > Configure C
S		





		Server	Mar	nage		
				WELC	OME TO S	SE
	Local Server					
	All Sonvore					
3						
P	File and Storag	ge Services	⊳			
		2				
				LEARN		
				ROLES Roles: 3	AND SE	R\ gr
				i i i	AD DS	
				•	Manage Events	ab
					Services	
					Perform	an
					BPA resu	ılt
	⊡_ Q	1 🥖				

🚡 Server Manager

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

Configure CA

RVER MANAGER 📥 AD CS Configuration DESTINATION SERVER Con Validity Period DC.lab0.ccisrd.eu Specify the validity period Credentials Role Services 3 A Select the validity period for the certificate generated for this certification authority (CA): Setup Type 5 Years СА Туре CA expiration Date: 30.03.2023 10:48:00 Private Key Cryptography The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue. CA Name Validity Period Certificate Database Confirmation Progress Results bility More about Validity Period Next > Configure < Previous ts





ᡖ Server Manager

Server Ma	anager 🕨 Dashboard		- 🕄 🏲 Manage Tool	5
Dashboard	WELCOME TO SERVER MAN	AGER	_	
Local Server All Servers AD DS	1	Conf CA Database	DESTINA DC.I	TION lab0.
B DNS File and Storage Services ▷		 Ac Credentials Role Services Ac Setup Type CA Type Private Key Cc Cryptography CA Name 	Specify the database locations Certificate database location: C:\Windows\system32\CertLog Certificate database log location: C:\Windows\system32\CertLog	
	ROLES AND SERVER GROUP Roles: 3 Server groups: 1 Se	Validity Period Certificate Database Confirmation Progress Results		
	 Manageability Events Services Performance BPA results 		More about CA Database < Previous	(
🖶 🔎 🗆 🬔 📑				<u> </u>

Accept default and click "Next"

Configure CA



9:42 30.03.2018 🔁



	Server	Mar	nage		as
Dashboard			WELC	OME TO	SEI
 Dashboard Local Server All Servers AD DS DNS File and Storage 	ge Services		QUICK WHAT LEARN ROLES Roles: 3	START START SNEW MORE MORE MORE Manage Events Services Perform BPA res	RV grd an ults
	ı 🬔		L		

🚡 Server Manager

Accept default and click "Next"

Configure CA

RVER MANAGER 📥 AD CS Configuration — 1 Con DESTINATION SERVER CA Database DC.lab0.ccisrd.eu Specify the database locations Credentials Role Services 3 A Certificate database location: Setup Type C:\Windows\system32\CertLog СА Туре Private Key Certificate database log location: Cryptography C:\Windows\system32\CertLog CA Name Validity Period Certificate Database Confirmation Progress Results bility

More about CA Database

ice Next > Configure < Previous ts



^ 문 ^{9:42} 30.03.2018 €



WELCOME TO SERVER MANAGER Local Server All Servers i AD DS B DNS ■ File and Storage Services ▷ ROLES AND SERVER GROUPS AD DS Manageability Events Performance BPA results 🖶 🔎 🗆 🤶 🔚 🔚

🚡 Server Manager

Accept default and click "Configure"

Configure CA

📥 AD CS Configuration DESTINATION SERVER Cor Confirmation DC.lab0.ccisrd.eu To configure the following roles, role services, or features, click Configure. Credentials Role Services Active Directory Certificate Services Setup Type **Certification Authority** СА Туре CA Type: Enterprise Root Private Key RSA#Microsoft Software Key Storage Provider Cryptographic provider: Cryptography Hash Algorithm: SHA256 Key Length: 2048 CA Name Allow Administrator Interaction: Disabled Validity Period Certificate Validity Period: 30.03.2023 10:48:00 Certificate Database Distinguished Name: CN=lab0-MUM2008-CA,DC=lab0,DC=ccisrd,DC=eu Confirmation C:\Windows\system32\CertLog Certificate Database Location: Progress Certificate Database Log C:\Windows\system32\CertLog Location: Results Configure < Previous Next >





		Server	Mar	nage		
	Dashboard			WELCO	OME TO :	SEI
i i: i:	Local Server All Servers AD DS					
4	DNS File and Stora	ge Services	⊳			
				LEARN ROLES Roles: 3	MORE AND SE	RV
				ij.	AD DS	
				1	Manage Events Services Perform BPA resi	an an
	_ D (ı 🬔		-		

👝 Server Manager

• After configuration complete, click "Close"

Configure CA

RVER MANAGER 📥 AD CS Configuration _ 1 Con DESTINATION SERVER Results DC.lab0.ccisrd.eu The following roles, role services, or features were configured: 2 A Credentials Role Services Active Directory Certificate Services 3 A Setup Type Configuration succeeded Certification Authority CA Type More about CA Configuration Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results bility ice < Previous Close Next > ts






 When asked to configure additional role services, click "Yes"

Configure CA



	Server	Mar	nage		as
Dashboard			WELC	OME TO	SEI
 Dashboard Local Server All Servers AD DS DNS File and Storage 	ge Services		QUICK WHAT LEARN ROLES Roles: 3	START START SNEW MORE MORE MORE Manage Events Services Perform BPA res	RV grd an ults
	ı 🬔		L		

🚡 Server Manager

Accept default and click "Next"

Configure CA







🚘 Server Manager

Dashboard	WELCOME TO SERVE	R MANAGER	AD CS Carlinuation		
Local Server All Servers AD DS DNS	QUICK START	1 Conf	Role Services		DESTINATION DC.lab0.4
■ File and Storage Services ▷	WHAT'S NEW LEARN MORE ROLES AND SERVER C Roles: 3 Server groups: Coles: 3 Server groups: Manageability Events Services	2 Ac 3 Ac 4 Cr 5 Cc state stat	Credentials Role Services CA for CES Authentication Type for C Service Account for CES Server Certificate Confirmation Progress Results	 Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service 	
	Performance BPA results			< Previous Next	> Configure C

• Select "Certificate **Enrollment Web Service**" and Click "Next"

Configure CA



9:42 0.03.2018 🔁



		Server	Mar	nage		
				WELCO	OME TO S	SEI
ï	Local Server					
i.	All Servers					
	AD DS					
0	DNS					
	File and Storag	ge Services	⊳			
				LEARN		
				ROLES Roles: 3	AND SE	RV gro
				ij	AD DS	
				1	Manage Events Services Perform	ab
					BPA resu	ults
		1 (C				

👝 Server Manager

Select "CA Name" and Click "Next"

Configure CA

RVER MANAGER 📥 AD CS Configuration _ 1 Con DESTINATION SERVER CA for CES DC.lab0.ccisrd.eu Specify CA for Certificate Enrollment Web Services Credentials Role Services Select the certification authority (CA) that you want to use for issuing certificates requested CA for CES through this Certificate Enrollment Web Service (CES). Authentication Type for C... -Select: Service Account for CES Occession CA name Server Certificate Computer name Confirmation Target CA: DC.lab0.ccisrd.eu\lab0-MUM2008-CA Select... Progress Results Configure the Certificate Enrollment Web Service for renewal-only mode. Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2. oility More about CA for CES Configure < Previous Next >





👝 Server Manager

Server Ma	anager • Dashboard		- 🍘 🚩 Manage Tools
 Server Ma Dashboard Local Server All Servers AD DS DNS File and Storage Services > 	Anager Dashboard WELCOME TO SERVER MANA	Image: Service Account for CES Confirmation Credentials Role Services CA for CES Authentication Type for C Service Account for CES Confirmation Progress Results	• (2) Manage Tools - E DESTINATION DC.IabO.C ntication
	Services Performance BPA results		< Previous Next > Configure C
📲 🔎 🗆 🥭 🔚			~ 洰 :

• Select "Windows integrated authentication" and Click "Next"

Configure CA



9:42 0.03.2018 尾





- 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"



🚡 Server Manager

Configure CA

ERVER MANAGER			
	📥 AD CS Configuration	_	
1 Conf Service Account for		or CES DESTIN	IATIO C.lab(
 2 Ac 3 Ac 4 Cr 	Credentials Role Services CA for CES Authentication Type for C	Specify the service account Select the identity that the Certificate Enrollment Web Service (CES) uses when com with the certification authority (CA) and other services on the network.	ımuni
5 Co	Service Account for CES Server Certificate Confirmation Progress Results	 Specify service account (recommended) The account selected must be a member of the IIS_IUSRS group. If Kerberos is seauthentication type, a service principal name is required for the service account. Use the built-in application pool identity 	electer Se
VER GROUPS groups: 1 Servers tota			
ability		More about Service Account for CES	
ince Its		< Previous Next > Configure	

_	ð		×	
View		Help		
	×			
N SER\ 0.ccisrd	/ER .eu			
cating				
d as the	e			
elect				
Cancel				

· ^ 문 9:42 30.03.2018 ₹2



- 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	Mar	age		
Dashboard			WELCO	OME TO S	SER
Local Server All Servers AD DS DNS File and Stora	ige Services		QUICK WHAT'		
;)			ROLES Roles: 3	AND SE	gro
			Ŧ	Manage Events Services Perform BPA resu	anc Ilts
	ו 🔎 ו				

👝 Server Manager

Configure CA

VER MANAGER 📥 AD CS Configuration DESTINATION Cor Server Certificate DC.lab0. Specify a Server Authentication Certificate Credentials Role Services 3 A When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) prote CA for CES encrypt network traffic. Authentication Type for C... Choose an existing certificate for SSL encryption (recommended) Service Account for CES Issued To Issued By Expiration Date Server Certificate lab0-MUM2008-CA 29.03.2020 dc.lab0.ccisrd.eu Confirmation lab0-MUM2008-CA lab0-MUM2008-CA 30.03.2023 Progress Refresh Properties O Choose and assign a certificate for SSL later A For this role service to function, you must configure this server with a valid certificat ity More about Server Certificate < Previous Next > Configure

	Ø		\times	
View		He	lp	
	Х			
SERV	ER .eu			
ocol to	þ			
te.				
Cancel				

へ EP <u>9:42</u> 30.03.2018 **見**



• Open "Internet Information Services (IIS) Manager".

🚡 Server Manager Server Manager • Dashboard WELCOME TO SERVER MANAGER Dashboard Local Server All Servers AD CS AD DS QUICK START 2 🔒 DNS ■ File and Storage Services ▷ 3 IIS 🕲 WHAT'S NEW **P**NPAS 4 5 LEARN MORE ROLES AND SERVER GROUPS Roles: 6 | Server groups: 1 | Servers total: 1 AD CS \odot Manageability Events Services Performance **BPA** results 🚛 🔎 🗆 🧲 🔚

Configure CA



- (2) |

Ŧ

			-	-	o ×	
ÐI	P _	Manage	Tools	View	Help	
Active Directory Administrative Center						

Active Directory Domains and Trusts

^ 닫 30.03.2018 10:55



💐 Internet Information Services (IIS) Manager Dashboard Local Server (🛀 🕨 DC 🔸 All Servers File View Help AD CS Connections AD DS 🔍 - 🕞 🖄 🔗 🔒 DNS 💐 Start Page 🗸 📲 DC (LAB0\administrator) File and Sto Application Pools IIS 🕲 Expand Your server and > 🐻 Sites **P**NPAS select "Server Certificates" on the features view pane. Ready Performance BPA results 🕂 🔎 🗆 🧲 🔚

📥 Server Manager









• In Action pane click "Create Domain Certificate ..."

				Manage Tools
RVER MANAGER				
ormation Services (IIS) N	Manager			- 0
to the test the test test test test test t				🏧 🖾 🟠
Help				
ge (0\administrator)	Server Certifica Use this feature to request and m configured for SSL.	Actions Import Create Certificate Reque Complete Certificate Reque		
	Filter:	Go 🕞 😽 Show All Group by:	No Grouping 👻	Create Domain Certificat
	Name	Issued To Iab0-MUM2008-CA	Issued By Iab0-MUM2008-CA	Create Self-Signed Certificate Enable Automatic Rebin Renewed Certificate



ヘ 記 9:42 30.03.2018 見



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



					-
formation Services (Create Certificate		?	×	
€ DC → Help	Distinguished Name Properties				× 6
ge BO\administrator) lication Pools s	Specify the required information for the certificate official names and they cannot contain abbreviati Common name: Organization: Organizational unit: City/locality State/province: Country/region:	e. State/province and City/locality must be specified as ons.	Cancel		e Reque cate Rec ertifica d Certif c Rebin ate



ヘ 記 9:42 30.03.2018 見



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



👝 Server Manager

formation Services (Create Certificate	?	×	
¶ ⊨ DC →	Online Certification Authority			🛛 🏠
Help				
	Specify the certification authority within your domain that will sign the certificate. A friendly name is re and should be easy to remember.	equired		
B0\administrator)	Specify Online Certification Authority:			: Reque cate Re
olication Pools s	lab0-MUM2008-CA\DC.lab0.ccisrd.eu	Select		ertifica
	Example: CertificateAuthorityName\ServerName			d Certi
	Friendly name:			c Rebin ate
	DC.lab0.ccisrd.eu			
	Previous Next Finish	Cancel		



- へ EP <u>9:42</u> 30.03.2018 **号**2



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



RVER MANAGER				
ormation Services (IIS	5) Manager			— 🗆
∎ ► DC ►				🌆 🔤 🏠
Help				
8	Server Cert	ificates		Actions Import
e 0\administrator) ication Pools	Use this feature to request configured for SSL.	and manage certificates that the We	eb server can use with websites	Create Certificate Reque Complete Certificate Rec
	Filter:	👻 🖤 Go 👒 🥁 Show All 🗌 Group	by: No Grouping -	Create Domain Certificat
	Name	Issued To	Issued By	Create Self-Signed Certif
	DC.lab0.ccisrd.eu	dc.lab0.ccisrd.eu	lab0-MUM2008-CA lab0-MUM2008-CA	View Export Renew Remove Enable Automatic Rebin Renewed Certificate
	< <p>Features View Contended</p>	ent View		Help



ヘ 記 9:42 30.03.2018 見





- 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"

		,	WELCO	ME TO S	
	Dashboard		WELCO	JME TO 3	
2	Local Server				
	All Servers				
	AD DS				
	DNS				
P	File and Storage Services ▷				
			LEARN		
			ROLES	AND SE	RV
r			Roles: 3	Server	gro
1-					
				AD DS	
				Manage	ab
			Ŭ	Events	
				Sonvicos	
				Derf	
				Performa	an:
				BPA resu	ilts
	נו 📿 🕻		r de la com		

📥 Server Manager

Configure CA

RVER MANAGER 📥 AD CS Configuration DESTINATION Con Server Certificate DC.lab0. Specify a Server Authentication Certificate Credentials Role Services 3 A When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) proto CA for CES encrypt network traffic. Authentication Type for C... Choose an existing certificate for SSL encryption (recommended) Service Account for CES Issued To Issued By Expiration Date Server Certificate lab0-MUM2008-CA 29.03.2020 dc.lab0.ccisrd.eu Confirmation lab0-MUM2008-CA lab0-MUM2008-CA 30.03.2023 Progress Properties Refresh O Choose and assign a certificate for SSL later A For this role service to function, you must configure this server with a valid certificat oility More about Server Certificate < Previous Next > Configure

	Ø		\times	
View		He	lp	
	Х			
SERV	ER .eu			
ocol to	þ			
te.				
Cancel				

· ^ 문 <u>9:42</u> 30.03.2018 **문**



WELCOME TO S Local Server All Servers i AD DS 🔒 DNS ■ File and Storage Services ▷ **ROLES AND SER** AD DS Managea Events Services Performa BPA resu = 🔎 🗆 🧲 🔚

👝 Server Manager

• Click "Configure"

Configure CA

FRVFR MANAGER			
ERVERMANAGER	📥 AD CS Configuration		
1 Cor	Confirmation		DESTINATIO DC.lab
2 A	Credentials	To configure the following rol	les, role services, or features, click Configure.
3 A	CA for CES	Active Directory Certifi	cate Services
4 0	Authentication Type for C Service Account for CES Server Certificate Confirmation Progress	Certificate Enrollment Web CA Name: Renewal Only Mode: Authentication Type: Allow Key-based Renewal: Account:	Service DC.lab0.ccisrd.eu\lab0-MUM2008-CA False Windows Integrated Authentication False Application Pool Identity
RVER GROUPS groups: 1 Servers to 1	ta	Server Authentication Certificate:	D89FE6FADAB5F1173C57569D314C2E11C3EB9C1E
ability			
ance			< Previous Next > Configure
lts			







🚡 Server Manager

• Click "Close"

Configure CA

		- 0 >
		🗝 🍞 🚩 Manage Tools View Help
RVER MANAGER	AD CS Configuration	— 🗆 X
1 Cont	Results	DESTINATION SERVER DC.lab0.ccisrd.eu
2 Ad 3 Ad 4 Cr 5 Co VER GROUPS roups: 1 Servers tota 1 pility	Credentials Role Services CA for CES Authentication Type for C Service Account for CES Server Certificate Confirmation Progress Results	The following roles, role services, or features were configured:
ice Is		< Previous Next > Close Cancel

^ 문 ^{9:42} 30.03.2018 ₹2





📥 Server Manager

• In Server Manager Dashboard, click to configure "Active **Directory Certificate** Services"



Configure Web Service





WELCOME TO SERVER MANAGER Local Server All Servers i AD DS 🔒 DNS File and Storage Services ROLES AND SERVER GROUPS AD DS Manageability Events Performance BPA results 🚛 🔎 🗆 🥭 🔚 🔚

🚡 Server Manager

Verify username and click "Next"

Configure CA

📥 AD CS Configuration — DESTINATION SERVER Con Credentials DC.lab0.ccisrd.eu Specify credentials to configure role services Credentials Role Services 3 A To install the following role services you must belong to the local Administrators group: Confirmation Standalone certification authority Progress Certification Authority Web Enrollment Results 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 Next > Configure < Previous



· ^ 문 9:42 30.03.2018 ₹2



🚘 Server Manager	
Server Mar	nager 🕨 Das
Dashboard	WELCOME TO SEF
 Local Server All Servers AD DS DNS File and Storage Services 	QUICK START
ority ick	WHAT'S NEW
	Roles: 3 Server gro
	Manageab Events Services Performane BPA results
📲 🔎 🗔 🥭 🔚	E.

Select "Certificate Authorit Web Enrollment" and click "Next"

Configure CA

RVER MANAGER 📥 AD CS Configuration — 1 Cor DESTINATION SERVER **Role Services** DC.lab0.ccisrd.eu Select Role Services to configure Credentials Role Services Certification Authority Confirmation Certification Authority Web Enrollment Progress Online Responder Results Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service oility More about AD CS Server Roles ce < Previous Configure Next >





WELCOME TO SE Local Server All Servers i AD DS 🔒 DNS ■ File and Storage Services ▷ **ROLES AND SERV** AD DS Manageal Events Services Performar BPA result 🖶 🔎 🗆 🥭 🔚

🚡 Server Manager

- Click "Close"
- Now is CA configured.

Configure CA

			🕝 🚩 Manage Tools
RVER MANAGER	AD CS Configuration		— [
1 Con	Results		DESTINATION DC.lab0.
2 A	C Credentials Role Services	The following roles, role services, or features we	ere configured:
3 A 4 C 5 C	Confirmation Progress Results C	Certification Authority Web Enrollment More about Web Enrollment Configuration	Configuration succeeded
VER GROUPS roups: 1 Servers tot 1			
bility			
ts		< Previous	Next > Close (



9:42 1 30.03.2018



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

Next Steps



• From Server Manager open "Network Policy Server.





Select "RADIUS server for 802.1X Wireless or Wired Connections

Click "Configure 802.1X"



👝 Server Manager

B DNS

Network Policy Server File Action View Help 🚯 NPS (Local) NPS (Local) > ADIUS Clients and Servers Getting Started > I Policies Network Accounting Network Policy Server (NPS) allows you to create and enforce organization-wide network acce 🛃 Templates Management connection request authentication, and connection request authorization. Standard Configuration Select a configuration scenario from the list and then click the link below to open the scenario wizard RADIUS server for 802.1X Wireless or Wired Connections RADIUS server for 802.1X Wireless or Wired Connections When you configure NPS as a RADIUS server for 802.1X connections, you create network policies th NPS to authenticate and authorize connections from wireless access points and authenticating switch called RADIUS clients). Configure 802.1X Learn more Advanced Configuration Templates Configuration

	þ		\times	
View		He	p	
		×		,
ss polic	cies f	or		
	-	•		
hat allo nes (als	W io			
	•	•		
		•		

- へ EP <u>9:42</u> 30.03.2018 **見**



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



📥 Server Manager

RVER MANAGER		Configure 802.1X	×	
1 Con	File Action	Select 802.1X Connections Type		_
2 Ac 3 Ac	 NPS (Local) RADIUS C Policies Accountint Templates 	Type of 802.1X connections: Secure Wireless Connections When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.		rk acce
4 Cr 5 Cc		 Secure Wired (Etnemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Name: This default text is used as part of the name for each of the policies created with this wizard. You can use the default text as made by an authentication of the name for each of the policies created with this wizard. You can use the default text as made by a second secon		wizard
VER GROUPS roups: 1 Servers tota	3	Secure Enterprise Wireless Connections	\supset	olicies t g switc
1 bility				
Dinty				
nce ts	<	Previous Next Finish Cancel		

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

ヘ EP <u>9:42</u> 30.03.2018 **長**



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



📥 Server Manager

X Configure 802.1X 🚯 Network Poli Specify 802.1X Switches File Action Please specify 802.1X switches or Wireless Access Points (RADIUS Clients) 🚯 NPS (Local) > I RADIUS CI RADIUS clients are network access servers, such as authenticating switches and wireless access point. RADIUS clients are not client computers Policies Network Accountin To specify a RADIUS client, click Add rk acce Templates RADIUS clients: Add... Edit... wizard. Remove \sim plicies th g switch Previous Next Finish Cancel <

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

· ^ 문 9:42 30.03.2018 ₹2



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".



= 🔎 🗆 🤶 🔚 📥

📥 Server Manager

Configu New RADIUS Client Х 🚯 Network Poli Settings File Action Select an existing template: NPS (Local) > I RADIUS CI RADIUS Name and Address point Policies RADIU Friendly name: Accountin CAPsMAN To spec rk acce 🌉 Templates Address (IP or DNS): RADIU 10.1.0.1 Verify... Shared Secret Select an existing Shared Secrets template wizard None \sim To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive plicies th a switch Manual Generate Shared secret: Confirm shared secret: OK Cancel <

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

へ EP <u>9:42</u> 30.03.2018 号2



Select "Microsoft" Protected EAP (PEAP) as Type.

Click "Configure"



📥 Server Manager

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

· ^ 문 9:42 30.03.2018 ₹2



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



📥 Server Manager

Configure 802.1X WELCOME TO SERVER MANAGER 🚯 Network Poli Edit Protected EAP Properties Х File Action (= -) 🗖 Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request NPS (Local) Policy will override this certificate. > iii RADIUS CI. Certificate issued to: DC.lab0.ccisrd.eu \sim > I Policies National Accounting Friendly name: DC.lab0.ccisrd.eu rk acce 🌉 Templates Configure.. lab0-MUM2008-CA Issuer: Expiration date: 30.03.2019 10:51:47 Enable Fast Reconnect wizard. Disconnect Clients without Cryptobinding Eap Types \sim ecured password (EAP-MSCHAP v2 Move Up Move Down plicies the a switch Add OK Edit Remove Cancel Previous Next Finish Cancel <

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

· ^ 문 9:42 30.03.2018 ₹2



 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"



📥 Server Manager

age	Tools

	Carta	- 902.1V				~	
	twork Doli	e 002.1X				^	
Vie		Specify L	lser Groups				
File /	Action	Users that are	members of the selecte	ed group or groups will b	e allowed or de	nied access	
		based on the r	etwork policy Access Pe	ermission setting.			
S NPS	S (Local)						
2 AC .	RADIUS CI To select	User Groups, click Add	l. If no groups are selecte	ed, this policy applies to all	users.		
	Accountin						de nonce
3 Ac 🔊 🜉	Templates Groups					Add	IK acce:
	LABO)omain Users				Pamaya	
4 Cr						Nemove	
E CC							
							wizard.
							~
							×
VER GROUPS							plicies th g switch
roups: 1 Servers tota							
1							
bility							
-							
			-		D ()		
nce <			Previous	Next	Finish	Cancel	
ts							

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

· ^ 문 ^{9:42} 30.03.2018 **₹**2



WELCOME TO SE Local Server All Servers i AD DS 🔒 DNS File and Storage Services **ROLES AND SER** AD DS Managea Events Performa BPA resul 🚛 🔎 🗆 🥭 🔚 🔚

👝 Server Manager

Accept default and Click "Next"

TUUIS

ERVER MANAGER			Configure 802.1X	<
	ا 🌍	Network Poli	i Configuro Troffic Controls	-
	File	Action \		
1 Conf	•	⇒ 📰 🕻	Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.	
	🌍 N	VPS (Local)		
2 Ac	> [RADIUS CI	CI If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes	
3 Ac	<u>ا</u> ا < ا	🚪 Accountin Į Templates	in NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.	rk acce
4 Cr			If you do not use traffic controls or you want to configure them later, click Next.	
5 Cc			Traffic control configuration To configure traffic control attributes, click Configure.	wizard
			Configure	~
VER GROUPS				olicies t g switc
1				
bility				
nce	<		Previous Next Finish Cancel	
ts				

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

· ^ 문 9:42 30.03.2018 ₹2



WELCOME TO SI Local Server All Servers i AD DS 🔒 DNS File and Storage Services **ROLES AND SER** AD DS Managea Events Performa **BPA** resul 🚛 🔎 🗆 🧲 🔚 🔚

👝 Server Manager

Review settings and click "Next"

DVD MANACED		Canfinuar 902.1V	$\overline{}$	
	Sile Action	Compute SU2.1X Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients		
2 Ad 3 Ad	 NPS (Local) RADIUS CI Policies Accountint Templates 	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.		rk acce
4 Cr 5 Cc		RADIUS clients: CAPsMAN (10.1.0.1) Connection Request Policy: Secure Enterprise Wireless Connections Network Policies: Secure Enterprise Wireless Connections		wizard
VER GROUPS proups: 1 Servers tota				olicies t g switc
bility		Configuration Details		
nce	<	Previous Next Finish Cancel		

ſ	7	×	
View	He	lp	
	×	(
ss polici	es for		
	•		
nat allov nes (also	V)		
	•		
	•		

ヘ E→ 9:42 30.03.2018 - 見



Now we create policies for privileged user groups.

 Duplicate newly created Network policy.



👝 Server Manager

ERVER MANAGER					
	🚳 Network Policy Server			-	_
	File Action View Help				
1 Con	🗢 🔿 🙋 📅 🚺				
	NPS (Local)	Network Policies			
2 A(RADIUS Clients and Servers	Network policies allow you to designate who is authorized to	connect	to the network and i	the
	Connection Request Po	under which they can or cannot connect.			
3 A0	Metwork Policies		. .		
4.5	Accounting	Policy Name	Status	Processing Order	Ac
4 C	> 🜉 Templates Management	Connections to Microsoft Routing and Remote Access server	Enables	Move Up	
5 C		Connections to other access servers	En	Move Down	
			_	Disable	
		Secure Enterprise Wireless Connections		Delete	
		Conditions - If the following conditions are met:		Rename	
				Duplicate Policy	
groups: 1 Servers tota		Condition Value		Properties	
		Windows Groups LAB0\Domain Users		Help	
1					
- 1.112					
ability		Settings - Then the following settings are applied:			
		Setting Value			
ince	< >	<			
lts	Duplicate Policy				

	D		\times	
View			lp	
		×		
ircums	tance	es		
cess T	уре	S		
nt Ac	cess	U		
	ess ess	U U		
			•	
			11	
		^	¥	
		>		

· ^ 문 9:42 30.03.2018 ₹2



👝 Server Manager

 Give a duplicated policy a reasonable name (e.g. AD DS "Secure Enterprise 🔒 DNS Wireless connection for Management"

- Move this policy to the top. It must authenticate and accept privileged users before general one.
- Edit policy clicking "Properties"



Network Policy Server File Action View Help 🗢 🄿 🞽 🚾 🛛 🖬 NPS (Local) **Network Policies** > ADIUS Clients and Servers Network policies allow you to designate who is authorized to connect to the network and the ci under which they can or cannot connect. Connection Request Po 3 A Network Policies Policy Name Status Processing Order Ac Network Accounting 🌉 Templates Management Secure Enterprise Wireless Connections for management Disable Move Up Secure Enterprise Wireless Connections Enable Connections to Microsoft Routing and Remote Access server Enable Move Down Enable Connections to other access servers Enable Secure Enterprise Wireless Connections for management Delete Rename Conditions - If the following conditions are met: Duplicate Policy Condition Value Properties NAS Port Type Wireless - Other OR Wireless - IEEE 802.11 Help Windows Groups LAB0\Domain Users Settings - Then the following settings are applied: Value Setting Properties

Ē	×	
View	Help	
	×	
ircumstand	285	
reamstant	.63	
cess Туре	e S	
^	s L s L	
	i L	
	; [
	^	
	>	

へ EP <u>9:42</u> 30.03.2018 号2



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



📥 Server Manager

shboard

- (2) I

age Too

Network Policy Server File Action View Help Configure the conditions for management Properties Configure the conditions for this network policy. Configure the conditions for this network policy to authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. NPS wips this policy or authorize the connection request. If conditions do not match the connection request. IEEE 802.11 Weters GROUPS VER GROUPS Troupp: 1 Servers tot Ince ts Ordition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. OK Cancel Add Edit. Pendore OK Cancel Apply	ERVER MANAGER		
File Action View Help 1 Conditions Secure Entreprise Wireless Connections for management Properties X 2 Action Conditions Conditions Ontraineris Settings 2 Action Conditions Conditions Conditions Ontraineris Settings 3 Action Conditions Conditions The conditions do not match the connection request. If condition do not match the connection request. If condition description: 1 Condition Condition description: 1 Condition descript		Network Policy Server	—
Secure Enterprise Wireless Connections for management Properties X 2 Ac 2 Ac 2 Ac 4 Configure the conditions for this network policy. 4 Condition match the connection request. MPS uses this policy to authorize the conditional do not match the connection request. MPS skips this policy and evaluates other policies, if additional policies are configured. 4 Condition 5 Condition 7 NAS Port Type Wireless - Other OR Wreless - IEEE 802.11 9 Windows Groups 1 Delitivy 1 Condition description: 1 The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. 1 OK		File Action View Help	
Verview Conditions onstraints Settings d	1 Conf	Secure Enterprise Wireless Connections for management Properties X	
2 Ac 2 Ac 3 Ac 3 Ac 4 Cr 5 Cr 1 5 Cr 1 bility 1 condition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. Add Edt Remove 0K Cancel Apty		Overview Conditions Constraints Settings	
3 Act 3 Act 4 Cr 5 Cr 5 Cr Wretess - Other OR Wretess - Other OR Wretess - IEEE 802.11 Wretess - Other OR Wretess - Other OR Wretess - IEEE 802.11 Wretess - Other OR Wretess - Other OR Wretess - IEEE 802.11 Wretess - Other OR Wretess - Other OR Wretess - IEEE 802.11 Wretess - Other OR Wretess - Other OR Wretess - IEEE 802.11 Wretess - Other OR Wretess - Other OR Wretess - IEEE 802.11 Wrete GROUPS rougs: 1 Servers tota 1 bility Condition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. Add Edt Remove Add OK Cancel	2 Ac	Configure the conditions for this network policy.	d the c
4 C 5 C 5 C Windows Groups LABO/Management 0 LABO/Management 0 Condition description: 1 Condition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. Add Edt Remove Mdd Concel Add 0K Cancel 0K Cancel	3 Ac	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.	er Ac
S C VER GROUPS roups: 1 Servers tota 1 bility Condition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. Add Edt Remove 0K Cancel	4 Cr	Condition Value	Gr
S Cd Windows Groups LAB0\Management De VER GROUPS roups: 1 Servers tota Image: Condition description: Image: Condition		Search Strate St	De
VER GROUPS roups: 1 Servers tota 1 bility Condition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. Add Edit Remove ts OK Cancel Apply	5 00	Windows Groups LAB0\Management	De
bility Condition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups. Add Edit Remove ts OK Cancel Apply	VER GROUPS roups: 1 Servers tota 1		
nce ts OK Cancel Apply	bility	Condition description: The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.	
nce Add Edit Remove OK Cancel Apply			
ts OK Cancel Apply	nce	Add Edit Remove	
OK Cancel Apply	ts		
		OK Cancel Apply	

Ø		×	
View	He	р	
	×	:	
ircumstanc	es		
cess Type	S		
ant Access	U		
ny Access ny Access	U		
		^	
	^	v	
	>		
			~

へ 記 <u>9:42</u> 30.03.2018





👝 Server Manager

Local Server

File and Storage Services ▷

🖶 🔎 🖽 🥭 🔚 🔚

All Servers

AD DS

🔒 DNS Now we need to specify VLAN ID for this group.

- Select "Settings" tab
- In Settings section select "Vendor Specific" and click "Add"

		Network Policy Server				_
	F	File Action View Help				
	Cont _s	ecure Enterprise Wireless Connectior	ns for management Propert	ies		×
		Overview Conditions Constraints Se	ettings			
	2 Ac	Configure the settings for this network p If conditions and constraints match the	olicy. connection request and the po	licy grants access, settings a	are applied.	d the
	3 Ac	Settings:				
	4 Cr	BADIUS Attributes	To send additional attr then click Edit. If you o	ibutes to RADIUS clients, sel lo not configure an attribute, i	ect a Vendor Specific attribute, and it is not sent to RADIUS clients. See	er
	(🗾 Vendor Specific	your RADIUS client do	ocumentation for required attri	ibutes.	I
	5 Co	Routing and Remote Access				
		Allocation Protocol (BAP)	Attributes:	Vendor	Value	
		Allocation Protocol (BAP)	Attributes: Name	Vendor	Value	
MORE	s	Allocation Protocol (BAP) IP Filters IP Settings	Attributes: Name	Vendor	Value	
N MORE S AND SERVER GROUPS 3 Server groups: 1 Ser	S rvers tota	Allocation Protocol (BAP) IP Filters IP Settings	Attributes: Name	Vendor	Value	
ND SERVER GROUPS Server groups: 1 Ser	s rvers tota	Allocation Protocol (BAP) IP Filters IP Settings	Attributes: Name	Vendor	Value	
ERVER GROUPS er groups: 1 Ser	s rvers tota 1	Allocation Protocol (BAP) IP Filters IP Settings	Attributes: Name Add	Edit Remove	Value	
SERVER GROUPS ver groups: 1 Ser	s rvers tota 1	Allocation Protocol (BAP) IP Filters IP Settings	Attributes: Name Add	Edit Remove	Value	
SERVER GROUPS ver groups: 1 Ser OS ageability ts	s rvers tota 1	Allocation Protocol (BAP) IP Filters Encryption IP Settings	Attributes: Name	Edit Remove	Value	
MORE AND SERVER GROUPS Server groups: 1 Ser AD DS Manageability Events Services	s rvers tota 1	Allocation Protocol (BAP) IP Filters Encryption IP Settings	Attributes: Name Add	Edit Remove	Value	
RN MORE ES AND SERVER GROUPS 3 Server groups: 1 Ser AD DS Manageability Events Services Performance	s rvers tota 1	Allocation Protocol (BAP)	Attributes: Name Add	Edit Remove	Value	
MORE AND SERVER GROUPS I Server groups: 1 Ser AD DS Manageability Events Services Performance BPA results	s rvers tota	Allocation Protocol (BAP)	Attributes: Name Add	Edit Remove	Value	

Configure NPS - Radius

Ø		×	
View	He	р	
	×	:	
ircumstanc	es		
cess Type	S		
ant Access	U		
ny Access ny Access	U		
		^	
	^	v	
	>		
			~

· ^ 문 30.03.2018





👝 Server Manager

🔒 DNS As MikroTik is not listed here, we need to use "Vendor Specific"

Click "Add"



Configure NPS - Radius

ERVER MANAGER						
	🥪 Netwo	ork Policy Server				_
	File Act	tion View Help				
1 Cont	Secure Ente	erprise Wireless Connections for ma	nagement Properties		×	
	Overview	Conditions Constraints Settings				
2.44						
2 AC	If condition	Add Vendor Specific Attribute			×	d the c
3 Ac	Settings:	To add an attribute to the settings, se	lect the attribute, and then click	: Add.		
	RADIU	To add a Vendor Specific attribute the	at is not listed select Custom an	nd then click Add		ar Ac
4 Cr	🌍 🌍 Sta					Gr
	🔽 Vei	Vendor:				De
5 Co	Routin	All		~		De
	🖂 Mu Alla	Attributes:				_
		Name	Vandar			
	<u>т</u> "	USP. Tuppel, Switch, Endpoint	U.S. Pabatica Inc.			
	🏥 En	USB-Unauthenticated-Time	U.S. Robotics, Inc.			
VER GROUPS	🛛 🛃 IP i	USR-VPN-Encryptor	U.S. Robotics, Inc.			
groups: 1 Servers tota		USR-VPN-GW-Location-Id	U.S. Robotics, Inc.			
		USR-VTS-Session-Key	U.S. Robotics, Inc.			
		Vendor-Specific	RADIUS Standard		▼	
1		<			>	
bility		Description:				
		Specifies the support of proprietary N	AS features.			
0.00				Add	ose	
Ince	l					_
lts						
				ОК	ancel Apply	

Ø		×	
View	He	р	
	×	:	
ircumstanc	es		
cess Type	S		
ant Access	U		
ny Access ny Access	U		
		^	
	^	v	
	>		
			~

· ^ 문 30.03.2018


Configure NPS - Radius

📥 Server Manager Local Server All Servers i AD DS 🔒 DNS ■ File and Storage Services ▷ ROLES AND SERVER GROUPS AD DS Manageability Events Services Performance **BPA** results 🚛 🔎 🗔 🥭

Click "Add"



đ		×	
View	He	lр	
	×	:	
ircumstanc	es		
cess Type	S		
ant Access	U		
ny Access ny Access	U		
		^	
	^	v	
	>		
			~



Configure NPS - Radius 📥 Server Manager

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



	a		~	
View		He	p	
		×		
ircums	tance	es		
cess T	уре	S		
ant Aco	cess	U		
ny Acc	cess	U		
_			^	
		Q	¥	



Configure NPS - Radius

Vendor-assigned
 attribute number for the
 "Mikrotik_Wireless_VLANID"
 is 26. Therefore insert it.

👝 Server Manager

🚛 🔎 🗆 🥭 🔚 🔚

- 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"



shboard

- (B) | |

age Too

	_	- 🗇		\times
Тос	ols	View	Hel	P
				_
	—		×	
				_
\times				_
	d the c	circumstan	ces	
-	er Ac	cess Type	s S	
	Gr	ant Acces	s U	
	De	eny Acces	s U	
	De	eny Acces	s U	
			~	
			>	×
		9.42		Ň
	即	30.03.201	8	2



Configure NPS - Radius

• Add option 27, which

📥 Server Manager

- specifies VLAN type we will use (value 0 = 802.1q).
- Click "OK", "OK"



🚛 🔎 🗆 🧲 🔚 🔚

• For more options see https://wiki.mikrotik.com/wiki/ Manual:RADIUS Client/vendor dictionary

WELCOME TO SERVER MANAGER 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 attrib RADIU Vendor-Specific Attribute Information To add a Vendo - 🚯 Sta Attribute name **-**Vendor: \times Configure VSA (RFC Compliant) AI Routin 2 Spe 💑 Mu Allo de number Attributes: 💎 IP 🛛 Name ΘE Attribute format: 🔒 Enc USR-Tunnel-USR-Unauthe Decimal 💑 IP Spe USR-VPN-En USR-VPN-GV Attribute value \odot USR-VTS-Se Vendor-Speci < > OK Cancel Description: Specifies the su OK Cancel Add.. Close OK Cancel Apply

· 문 30.03.2018 €

	_	ð		×	
ols	View		Hel	Р	
	. 🗆		×		
		_			
-				_	
a tri	ie circumsi	ance	5		
er	Access T	уре	S		
	Grant Acc	ess	U		
	Deny Acc	ess	U		
1				^	
-					
_					
-			^		
			>	Ť	
	0.45				





🚛 🔎 🗆 🧲 🔚

📥 Server Manager

Local Server

All Servers

AD DS

B DNS

• Now we have specified which VLAN ID we will use for specific group.

Click "OK", "Close" and "OK"



Configure NPS - Radius

WELCOME TO SERVER MANAGER 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 To add an attrib Attribute Information Settings: Х RADIU To add a Vendo Attribute name: 🌍 Sta Vendor-Specific **-**Vendor: Attribute number: AIL Routin 26 Alle Attributes: Attribute format: OctetString 💎 IP F Name Attribute values: 🔒 Eng USR-Tunnel Add... Value Vendor USR-Unauthe 💑 IP USR-VPN-En Vendor Code: 14988 11 Edit.. USR-VPN-GV Vendor Code: 14988 0 USR-VTS-Se Remove Vendor-Speci < > Description: Move Down Specifies the su Cancel Add. Close

Apply

OK

Cancel

_	_	ð		×	
ols	View		Hel	р	
_			X		
d the (circums	tance	S		
ar Ac	ccess T	уре	s		
G	rant Aco	cess	U		
	eny Acc eny Acc	cess cess	U		
		_			
				~	
1			ļ	¥	
			-		
					~



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.



🚘 Server Manager

			Manag	e Tools	
RVER MANAGER	er				_
File Action View	Help				
CON ^{ork} Policy Server			_		
2 Ac 2 III 2 III				d ;	the c
Local) 3 AQDIUS Clients and Servers vicies 4 Cr Connection Request Po	Network Policies Network policies allow you to designate who is authorized under which they can or cannot connect.	to connect to t	the network and the	e circumsta _{er}	Ac
5 Cc:counting mplates Management	Policy Name Secure Enterprise Wireless Connections for Management Secure Enterprise Wireless Connections for Sales Secure Enterprise Wireless Connections for Production Secure Enterprise Wireless Connections	Status Disabled Disabled Disabled Enab	Processing Order 1 2 Move Up	Access Grant Ac Grant Ac	De
/ER GROUPS oups: 1 Servers tota	Connections to Microsoft Routing and Remote Access server Connections to other access servers	Enab Enab	Move Down Enable Delete		
1	Secure Enterprise Wireless Connections for Production		Duplicate Polic	y	
pility	Conditions - If the following conditions are met: Condition Value Value Value		Properties Help		
ce	NAS Port Type Wireless - Other OR Wireless - IEEE 802.11 Windows Groups LAB0\Production				
>	<				

đ		×	
View	He	lр	
	×	:	
ircumstanc	es		
cess Type	S		
ant Access	U		
ny Access ny Access	U		
		^	
	^	v	
	>		
			~

へ
に 30.03.2018



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

Next Steps



ISRD ACCO NEW Set

- 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



ecu	Irity		; Or	ן	fi	JU	r 8	DN
trainer@10.	.1.0.1 (LAB-GW) - V Datapaths Security Cf	Access List Ra	on hEX PoE (mi	P Rad) io Registratio	on Table		
n Ty Encryption aes.ccm	Group Encryption G aes com	roup Key Update	Passphrase ****	EAPI	Methods			Find
Name: Name: Authentication Type: Encryption: Group Encryption: Group Key Update: Passphrase: EAP Methods: TLS Mode: TLS Certificate:	AB-EAP WPA PSK WPA PSK WPA 2 AB-EAP WPA PSK WPA 2 AB-EAP WPA PSK WPA 2 AB-EAP WPA PSK WPA 2 AB-EAP WPA 2 WPA 2 <td></td> <td>• • • • • • • • • • • • • • • • • • •</td> <td> → →</td> <td>OK Cancel Apply Comment Copy Remove</td> <td></td> <td></td> <td></td>		• • • • • • • • • • • • • • • • • • •	 → →	OK Cancel Apply Comment Copy Remove			





Add New Datapath

nfiguratio	ons Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP	Radio	Registration Table	
Local I	For Client To	o VLAN Mode	VLANID						
	New CAPs Da	tapath Configui	ration						
		Name:	dp-EAP			ок			
		MTUS		•		ancel			
		LZ MIO.	•		р р				
		ARP:	:	~	Col	mment			
		Bridge:	bridgeLoca	-		Сору			
		Bridge Cost:	:		Re	emove			
		Bridge Horizon:	:						
						_			
	Lo	xal Forwarding:		*					
	Client To Clie	ent Forwarding:	:	•					
		VLAN Mode:							
		VIANTO							
		V DAIN 1D:	•						

Find	
• •	
	ŀ
i	





- 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

Settings Dashord Settings Das	×	⊖ 🔕	trainer@10.1.0.1 (LAB-GW) - WinBox v6.40.6 on hEX PoE (mipsbe)			
Safe Mode Safe Mode Control Control Control Control </td <td>Ses</td> <td>sion Settings Dashb</td> <td>bard</td> <td></td> <td></td> <td></td>	Ses	sion Settings Dashb	bard			
CADADAN C	ю	🖓 🛛 Safe Mode	Session: 10.1.0.1			
CAPHNAN CAPINE CAPINAN CAPINE CAPINAN CAPINE CAPINAN CAPINE CAPINAN CAPINE CAPINAN CAPINE CAPINA CAPINE CAPINE CAPINE CAPINE CAPINE CAPINE CAPINE CAPINE CAPINE CA		A Quick Set				
Statuty Statuty <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<>						
Wieleso CAP Interface Provisioning Contigurations Channels Datapaths Security (7g. Access List Rates Renote CAP Radio Registration Table Wieleso Image: Cap Interface Provisioning Contigurations Channels Datapaths Security (7g. Access List Rates Datapath Security (7g. Ac						
Vertices Interest Interes			CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table			
Billinge Hane SSD Helde SSDD Lode SSD Channel Rates Datapath Security OK Pe Billinge channel channel Rates Datapath Channel Rates Datapath Channel Security OK Pe Billinge channel channel Abel Company Security Security Channel Rates Datapath Channel Abel PP-26 Cancel Apply Company channel channel channel channel Channel Abel PP-26 Apply Comment Company Cancel Apply Comment Company Comment Comment Company Comment Company Comment Company Comment Company Comment Company Comment Company Comment Comment Comment Comment Comment <		Store Decidere	🕂 🖃 🖾 🝸			
Image: cdg-company-S2 LABC-company estonia 25-C- Image: cdg-company-S2 LABC-company estonia 55-Cx Image: cdg-company-S2 LABC-company estonia File Image: cdg-company-S2 LABC-company estonia File Image: cdg-company-S2 LABD-coluce Image: cdg-company-Cdg-cdg-cdg-cdg-cdg-cdg-cdg-cdg-cdg-cdg-c		and and a	Name 🛆 SSID Hide SSID Load Bala Country Channel Wireless Channel Rates Datapath Security	ак	ge '	VI
Control Contro Control Control	"		cfg-company-2G LABD-Company estonia 2G-C-			
View WinBox Weikand Opportunition LABB-sales Mode: apply Gamea Gamea Piles Log System Log Stance: Log Stance: View VinBox Partilion MetaRUTTR Partilion Multicast Helper: HT Ta Chains: HT Guard Interval:		🛫 Switch	crg-company-5G LABU-company estonia 5G-CX Name: crg-EAP-2G	Cancel		
Image: Problem in the series in t		°T¦8 Mesh	cfg-production LAB0-production	Apply		
MPLS Routing System Queues Files Log Radus Sitems Files New Tortion MakeSupoutrif		255 IP D	cfg-sales LABD-sales	Comment		
Routing System Queues Files Load Balancing Group: Waters: Steme Frame Lifetime: Steme Frame Lifetime: VetaROUTER Make Supout If		🖉 MPLS 🛛 🔿	Hide SSID:			
System Image: Cool Belaicing strupp: Queues Files Log Radius Radius Image: Cool Belaicing strupp: Files Log Max Retries: Image: Cool Belaicing strupp: Hw. Retries: Hw. Retries: Image: Cool Belaicing strupp: Image: Cool Belaicing strupp: <		🍂 Routing 💦 🖹		Сору		
Queues Files Ico Atadius Siteme		🚱 System 👘 🕑		Remove		
Files Log Radius Tools Interval: Interval: Hw. Retries: Hw. Protection Mode: Hw. Protection Mode: Hw. Protection Mode: Hw. Protection Mode: Interval: Interval: Hw. Protection Mode: Hw. Protection Mode: Interval: Interval: <td></td> <td>👰 Queues</td> <td>Distance:</td> <td></td> <td></td> <td></td>		👰 Queues	Distance:			
Log Radius Tools Sitems Frame Lifetime: Disconnect Timeout: WetaROUTER Partition Make Supout rif Manual Manual New WinBox Exit Hit Hit Chains: HT Tx Chains: HT Rx Chains: HT Rx Chains: HT Guard Interval:		📄 Files	Hu Batrias			
Radius Image: Radius Image: Tools Image: Tools <tr< td=""><td></td><td>Log</td><td></td><td></td><td></td><td></td></tr<>		Log				
New Terminal MetaROUTER Partition Make Supout.rif Manual New WinBox E bit Mature Station Count: Mitticast Helper: HT Tx Chains: HT Rx Chains: HT Guard Interval:		🧟 Radius	Hw. Protection Mode:			
New Terminal MetaROUTER Partition Make Supput.rif Manual New WinBox E bit HT Tx Chains: HT Rx Chains: HT Guard Interval:	L	💥 Tools 🛛 🔿	5 items Frame Lifetime:			
MetaROUTER Partition Make Suport.rif Manual Manual Mew WinBox Exit Multicast Helper: HT Tx Chains: HT Rx Chains: HT Suard Interval:	1	New Terminal	Disconnect Timeout:			
Partition Make Suport.rif Manual New WinBox Exit Multicast Helper: HT Tx Chains: HT Rx Chains: HT Guard Interval:			Keepalive Frames:			
Make Supout.rif Manual New WinBox Exit Multicast Helper: HT Tx Chains: HT Rx Chains: HT Guard Interval:		Partition				
Image: Station Count: Image: Station Coun		A Make Supout.rif	Country: estonia			
Max Station Count:		Manual				
Multicast Helper: HT Tx Chains: HT Guard Interval:		New WinBoy	Max Station Count:			
HT Tx Chains: HT Rx Chains: HT Guard Interval: HT Guard Interval:	ğ	Evit	Multicast Helper:			
HT Tx Chains: HT Rx Chains: HT Guard Interval:						
HT Rx Chains: Translerval:			HT Tx Chains:			
HT Guard Interval:			HT Rx Chains:			
- Second Se	ð		HT Guard Interval:			

			_
			×
Г	Find	1	
∟ AN Mode	VIA	N	-
			-
			•



- In "Channel" tab set
 - Channel = 2G-C-

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

		0			trair	ner@10.1.0).1 (LAB-(GW) – WinE	ox v6.40.6 on hEX PoE (mipsbe)				
s	ssio	on Sett ings Dashb	oard											
		CM Safe Mode	Session: 10.1.0.1											
5	2	Quick Set												
	1	CAPSMAN	CAPSMAN											
e		Interfaces	CAP Interface Pr	rovisioning Configura	tions) Cha	nnels Data	upaths Sev	curity Cfg. A	ccess List Rates Remote C	AP Radio Registration	Table			
	î	Wireless							New CAPs Capfiguration					
		🖁 Bridge					0		New CAPS Configuration					
3		PPP	cfo-company-2G	A SSID LABD-Company	HIde SSID	Load Bala	estonia	2G-C-	Wireless Channel Rates	s Datapath Security		ОК	ge	VI
		Switch	cfg-company-5G	LABO-Company			estonia	5G-Cx	Channel: 2	6-0-	₹ ▲	Cancel		
		8 Mesh	cfg-management	LABO-management								Apply		
		S TP D	cfg-sales	LABO-sales					Frequency:		÷			
	=	2 MPIS D							Control Channel Width:		-	Comment		
		Routing							Band:		•	Сору		
		System							Extension Channel:		•	Remove		
		Queues												
e		Files												
		Log												
ブ	de la	Radius	•						Reselect Interval:					
		Tools	5 items						Skip DFS Channels:		•			
		New Terminal												
		MetaROUTER												
		Partition												
		Make Supout.rif												
		Manual												
		New WinBox												
		, Exit												
1×														
v														
ĮČ														
1														
Ī														





In "Datapath" tab select previously created datapath "dp-EAP"

×		trainer@10.1.0.1 (LAB-GW) - WinBox v6.40.6 on hEX PoE (mipsbe)			
Sec	ssion <mark>Sett</mark> ings Dashb	xoard			
ю	CM Safe Mode	Session: 10.1.0.1			
s	🚰 Ouick Set				
	î CAPSMAN				
¢	Interfaces				
	î Wireless	CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table			
	Se Bridge	Image: Provide state Image: Provide state Image: Provide state Image: Provide state			
3	PPP	Name SSID Hide SSID Load Bala Country Channel Wireless Channel Rates Datapath Security	ОК	ge	VI
2 1	Switch	crg-company-2G LABL-Company estonia 2G-C- cfg-company-5G LABL-Company estonia 5G-Cx Datapath: dp-EAP	Cancel		
	PTS Mesh	cfg-management LABO-management	Apply		
4	255 TP	tig-production LAB0-production tig-production LAB0-production TU: ▼	Арріу	<u> </u>	
_		L2 MTU:	Comment		
t	Routing	ARP:	Сору		
	83 System		Remove		
	Cueues	Bridge:			
4	Files	Bridge Cost:			
6 19 19		Bridge Horizon:			
	CA Padius	•			
	Trole	5 items Local Forwarding:			
	Naw Terminal	Client To Client Forwarding:			
		VLAN Mode:			
	Make Support rif	VLAN ID:			
	Manual				
	May Min Bay				
Ĭŏ	Evit				
Ξ					
ι σ					
Q					
ē					
no					
2					





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

×			trainer@10.1.0.1 (LAB-	GW) - WinB	ox v6.40.6 on hEX PoE (mipsbe)				
Se	ssion Sett ings Das	iboard							
×0	Safe Mode	Session: 10.1.0.1							
5	🚔 Ouick Set								
	T CAPSMAN	CAD-MAN							
e		CAPSMAN							
	T Wireless	CAP Interface Provisioning Configuration:	Channels Datapaths Se	scurity Cfg. A	ccess List Rates Remote CAP Radio Registration T	able		_	
	See Bridge				New CAPs Configuration				
3	PDP	Name 🛆 SSID Hide	SSID Load Bala Country	Channel	Wireless Channel Rates Datapath Security		ОК	ge ۱	V
	En Switch	cfg-company-2G LABL-Company cfg-company-5G LABL-Company	estonia	2G-C- 5G-Cx	Security: LAB-EAP	Ŧ.	Cancel		
	OT ⁰ Mach	cfg-management LAB0-management							
		cfg-production LAB0-production			Authentication Type:	•	Apply		
					Encryption:	•	Comment		
					Crows Essentiant	- _	Copy		
4	Routing								
	tge System				Group Key Update:	_	Kemove		
	Queues				Passphrase:	•			
	Files				EAP Methods:	†			
	Log				EAP Radius Accounting:	_			_
	2 Radius	▼ 5 items				<u> </u>			
	🔀 Tools 🛛 🗋								_
	🔄 New Terminal				TLS Certificate:				
	🕗 Partition								
	[] Make Supout.rif								
	🕜 Manual								
	🔘 New WinBox								
Ē	📙 Exit								
N N									
L 2									
Ľ,									
l õ									





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

X	- 0								
Sessi	ion :	Settinas D.	ashb	oard					
ю	QI	Safe Mod	8	Ses	sion: 1	0.1.0.1			
	🔆 01	uick Set							
	î d	APSMAN							
	In In	terfaces			IPSMAIN		-		6
	î.w	ireless			AP Inte	ertace	Prov	isionin T	g Col
	Br	idge				1	T		
	🔹 PP	P		Ν	lame fa EAD	20	Δ	SSID	- 4 0
	₩ Sv	vitch			fg-EAP-	-23 -5G		LABO-E	сар Бар
	te Ma	esh		C	tg-com	pany-24	G		Compar
	55 IP				tg-com fg-man	pany-5« ageme	G nt	LАВ0-К LAB0-г	Compar nanaos
-	22 MI	215		c	fg-prod	uction	-	LABO-p	product
	R	outina			tg-sale:	5		LABD-s	ales
٦,	8) Sv	stem							
6	, o	Jeues							
	Fi	les							
	E Lo	g							
3	🔒 Ra	idius		•					
	<i>R</i> То	ols		7	items				
	Ne	w Terminal							
	- Mk	etaROUTER							
	🕒 Pa	irtition							
	🔒 Ma	ake Supout.r	if						
	Ma	anual							
	S Ne	w WinBox							
	В	it							
S									
Le Le									
Ľ									
2									

figura	tions Cha	nnels Dat	tapaths	Securi	ity Cfg.	Access	List	Rates	Rema	ote CAP	Radio	Regi	stration Ta	ible				
	Hide SSID	Load Bala	a Count	ry (Channel	F	Freque	элсу		Band		R	ate		Datapath	Bridge	۱	٧LA
			estoni	ia 🛛	2G-C-									•	dp-EAP			
			estoni	ia S	5G-Cx									•	dp-EAP			
/			eston	ia 2	2G-C-										dp-general			
/			estoni	ia S	5G-Cx									•	dp-general			
nent														•	dp-managem			
л															dp-production			
															dp-sales			

Find
AN Mode VLAN 🔻
•



Update Provisioning's

- Select provisioning tab
- Edit current provisionin
- Remove unnecessary configurations

9	0	Safe Mox	le	Session: 10.1.0.1	
	h	Quick Set			
	Î	CAPSMAN		CAPSMAN	
		Interfaces		CAP Interfact Provisioning	Cor
	1	Wireless		+ - / × a	$\overline{\mathbf{T}}$
		Bridge		# Radio MAC	Ide
		PPP		0 00:00:00:00:00:00	
	-8-	Switch		1 00:00:00:00:00:00	
		Mesh			
	255	IP			
		MPLS			
, 7	S	Routing			
		System			
	2	Queues			
		Files			
		Log			
	25 3.6	Radius		2 items	
		I DOIS		<u></u>	
		Partition			
		Make Supout	rif		
		Manual	1 1 1		
		New WinBox			
		Exit			
6					
9					
õ					

figurations	Channels	Dat	apaths S	ecurity Cfg.	Access I	ist Rates	Remote CAP	Radio	Registration Table	
tity Dana	Common Na		Action	Master Co.	ofioura	Slave Conf	iouration			
ILLY NOYON]	ACTON				iguration			
			create dy	. ctg-compa	пу-5G	ctg-manage	ement, ctg-prod	luct		
			create dy	. cfg-compa	ny-2G	cfg-manag	ement, cfg-prod	luct		

trainer@10.1.0.1 (LAB-0	GW) - WinBox v6.40.6 on l	nEX PoE (mip	sbe)			
S Channels Datapaths Sex	curity Cfg. Access List Rates	Remote CAP	Radio Reg	istration Table		
						Find
Common Na Action	Master Configura Slave Conf	iguration			 	•
create dy create dy	cfg-company-5G cfg-manag- cfg-company-2G cfg-manag-	ement, cfg-produ ement, cfg-produ	uct		 	
CAPs Provisioning <00:00	:00:00:00:00>					
Radio MAC:	00:00:00:00:00	ОК				
Hw. Supported Modes:	a 두 🖨	Cancel				
Identity Regexp:		Apply				
Common Name Regexp:		Disable				
IP Address Ranges:	\$	Comment				
Action:	create dynamic enabled F	Сору				
Master Configuration:	cfg-company-5G Ŧ	Remove			 	
Slave Configuration:	cfg-management 🔻 🜩					
	cfg-production 🔻 🜩					
	cfg-sales 🗧 🗧					
Name Format:	prefix identity					
Name Prefix:	5G 🔺					
enabled						
<u>.</u>			-			



Update Provisioning's

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

Ses	sion	Settings D	asht	board				
ю	0	Safe Mod	e	Session	10.1.0.1	L		
	14	Quick Set						
	Î	CAPSMAN		CAPsN	IAN			
		Interfaces		CAPI	Interface	Provisio	pning	Сол
	Î	Wireless					-a	∇
0	5 P 2 5	Bridge		T				U
	¢,	PPP		÷ Ū	00:00:00	 ::00::00:0	ю	TOGI
		Switch		1	00:00:00	:00:00:0	Ю	
		Mesh						
	255	IP						
		MPLS						
		Routing						
		System						
	\$	Queues						
		Files						
		Log						
	2	Radius		2 item	's			
		Tools		<u> </u>				
		New Terminal						
	23	MetaROUTER						
		Partition						
		Make Supout.r	TT					
	9	Manual						
ň								
		EXIL						
<u>></u>								
õ								
ē								
0 D								
R.								

figurations	Channels	Data	apaths	Secu	rity Cfg.	Access L	ist F	Rates	Remote CAP	Radio	Registration Table		
tity Reae	Common Na	I	Action	M	laster Cor	ifiqura	Slave	Confie	ouration				 _
			create dy	/ ɗ	fg-compai	пу-5G	cfg-п	vanage	ement, cfg-prox	luct			
			create dy	/ d	fg-compai	ny-2G	cfg-п	vanage	ement, cfg-prox	luct		 /	

t	rainer@10.1.0.1 (LAB-0	GW) - WinBox v6.40.6 (on h	EX PoE (mip	sbe)				
s	Channels Datapaths Sex	curity Cfg. Access List Ra	tes	Remote CAP	Radio	Registration Table			
						, , , , , , , , , , , , , , , , , , ,			Find
C	Common Na Action	Master Configura Slave C	onfi	guration					•
	create dy create dy	cfg-company-5G cfg-ma cfg-company-2G cfg-ma	nage nage	ement, cfg-prod ement, cfg-prod	uct		 	 	
	CAPs Provisioning <00:00):00:00:00:00>			1				
	Radio MAC:	00:00:00:00:00		ОК					
	Hw. Supported Modes:	a 🗧 🗧	•	Cancel					
	Identity Regexp:			Apply					
	Common Name Regexp:			Disable					
	IP Address Ranges:	4	•	Comment					
	Action:	create dynamic enabled	F	Сору					
	Master Configuration:	cfg-EAP-5G	F	Remove			 	 	
	Slave Configuration:		•						
	Name Format:	prefix identity	F						
	Name Prefix:	5G	•						
	enabled								
-									



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



Provisioning

figurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP	Radio	Registration Table	
ntity Rege	Common Na	a Action	Master Co	nfigura Sla	ave Confi	iguration			
		create	dy cfg-EAP-5	G					
		create	dy cfg-EAP-2	G					

Find	
FIND	



Reconfigure CAP's

- Select "Remote CAP" ta
- Select access points of the list and click
 "Provision" - Now we have reconfigured all CAP's to use EAP

Session Settin	gs Dashbo	ard		
හි 🖓 Saf	e Mode	Session: 10.1.0.1	1	
he wick St	et			
1 CAPSMA	N	CAPSMAN		
🔚 Interfac	æs	CAP Interface	Provisioning	Con
🧘 Wireles	S			ncadu
👷 Bridge				grade
h ^{PPP}		64:D1:54:3C:B	9:A2 [64:D	;)1:54
🛫 Switch				
°T¦8 Mesh				
255 IP				
MPLS				
🎉 Routing				
System				
Queues				
📄 Files				
E Log				
🧟 Radius		1 item (1 select		
🔀 Tools				
New Ter	minal			
MetaRO	UTER			
Partitio	1			
🛄 Make Su	pout.rif			
× 📿 Manual				
🛯 🕓 New Wi	nBox			
Exit				
\leq				
<u>Ö</u>				
Ē				
no				

nfigura	tions Channe	els Datapaths	Security Cfg.	Access List	Rate: Remote CAP	Radio	Registration Table		
le 1	Set Identity								
	Board	Serial	Version	Identity	Base MAC	State	Radios		
4 : 3C	RBwAPG-5Ha.	. 774A0778CC	6.41	LAB-AP1	64:D1:54:3C:B9:A2	Run		2	

[×]
Fino		•	
	_		



Configure RADIUS Client

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

Session Settings Dashboard Session: 10.1.0.1 Quick Set CAPsMAN	8 - 8		
Safe Mode Session: 10.1.0.1 Quick Set CAPSMAN	Session Setting	js Dashb	xoard
Auick Set CAPSMAN Im Interfaces Wireless Bridge PPP Switch Mesh Im PP Mesh Im News Routing Mess Im New Terminal Im New Terminal Im New Terminal Im Make Supput.rif Make Supput.rif Im New WinBox	🔊 (🍳 Saf	e Mode	Session: 10.1.0.1
	Vireless CAPsMA CAPsMA Interface Vireless Switch PP Switch Nesh IP NPL5 Nouting System Polacues Interface Nesh IP Nesh IP Nesh IP Nesh IP Interface IP Interface Inte	t N es b b b b b b b b b b b b b b b b b b	Radius * Service * items









📙 Exit i

- 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. 🥖 Manual 🔄 New WinBox
- Save Radius settings.

on: 10.1.0.1	
Radius	
# Service	
	_
	Ne
	G
	_
0 items	
	A
	-
	1
	en

Configure RADIUS Client





- 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

Next Steps



- 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.

Install CA Certificate $\bullet \bullet \bullet < >$ dc.lab0.ccisrd.eu/certsrv/ Û Microsoft Active Directory Certificate Services -- lab0-MUM2008-CA 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 <u>View the status of a pending certificate request</u> Download a CA certificate, certificate chain, or CRL





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







×	-	8								trainer
æs	sion	Settings Da	ashb	oard						
9	0	Safe Mode	3	Sessi	on: 1	0.1.0.	1			
	2	Quick Set		CAPsN	1AN					
	ŝ	CAPSMAN		CAP	Interf	ace	Provisioning) Configui	ations	Channel
]	Interfaces			7		APs Scanner	1		
	Î	Wireless		Toter	face				MAC	Address
	50	Bridge		5G-L	AB-AP	21-2	LABILE	AP	34:AE	3:37:19:37
	F	PPP		5G-L	AB-AP	21-2	LABD-E/	AP	3C:28	:FF:0D:2
		Switch		(5G-L	AB-AP	2 -2	LABD-E/	4P	AC:B	C:32:D0:8
	°tô	Mesh								
	255	IP	\triangleright							
	$\overline{\mathcal{O}}$	MPLS	⊳							
	Ż	Routing	\triangleright	3 iten	ne					
	683	System	\triangleright							
		Queues			DH	CP Se	erver			
	ì	Files			DH	ЮР	Networks	Leases	Optie	ons Op
		Log						_ >> [45]		
	<u>e</u>	Radius							U	
	$\overline{\mathbb{X}}$	Tools	\triangleright			A	ddress	MAC	Addres	8
		New Terminal				1	3.1.13.252	34:AE	:37:19	37:75
		MetaROLITER				14	3.1.0.204 3.1.11.251	30:05 30:05	- 60:22	2:00:FU
		Partition			D	1	3.1.12.251	3C:2E	FF:00	D:28:5D
	-				D	1	3.1.11.254	64:D1	:54:19):FB:88
		маке Supout.n	IT		D	1	3.1.13.254	64:D1	:54:19):FB:88
×	~	Manual			D	1	3.1.12.254	64:D1	:54:19):FB:88
g	<u>_</u>	New WinBox				1	3.1.0.252	64:D1	:54:30	D:89:A2
2	4	Exit				11	3.1.12.252 3.1.0.250		-132:D •D7•D	0:00:F5 2-8F-31
3					Ľ	1	5,1,0,200	01.01		2.01.01
20										
ā					•					
Inc					10	item	S			
ř										

Verify connected users

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

ls	Data	paths	Security	Cfg.	Access	s List	Rates	Remot	te C	АР	Radio	Reg	istratio	n Tabl	le					
	Δ	EAP I	dentity	Tx Ra	ate	Rx Rat	te	Tx Signa	I	Rx S	iignal	Uptin	ne	Tx/Rx	: Pack	ets	T×	(/Rx Byt	es.	
7:7	5	llab0\i	ohn	6Mbp	26	270Mb	ops		Ð		-55	00:03	1:01	71/16	4		15	i.4 KiB/	2 8 .5 KiB	
B:5	D	llab0\v	alice	6Мbр	26	400Mb	pps		Ð		-46	00:00	0:4 3	42/99	ŀ		12	2.8 KiB/	17.1 KiB	
1 9: F	-5	lab0\i	mike	9Мbp	7 5	405 Mb	ops		Ð		-55	00:1	0:20	293/2	51		17	7.7 KiB/.	37.1 KiB	

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

Find
-

•





- 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

Future options



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

Summary



CAPsMAN configuration

/caps-man channel add band=2ghz-b/g/n control-channel-width=20mhz extension-channel=disabled name=2G-Cadd 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 nam prefix-identity name-prefix=5G
	add action=create-dynamic-enabled hw-supported-modes=gn master-configuration=cfg-EAP-2G nar 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