Configure the Network Device Enrollment Service In Pictures

The Network Device Enrollment Service performs the following functions

- Generates and provides one-time enrollment passwords to administrators.
- Submits SCEP enrollment requests to the CA.
- Retrieves enrolled certificates from the CA and forwards them to the network device.

To request and enroll for a certificate by using the Network Device Enrollment Service

- Run the software used to manage the network device, and use this software to generate an RSA public/private key pair configured for one of the following:
 - $\circ\,$ Signing and signature verification
 - Encryption and decryption
 - Signing, signature verification, encryption, and decryption
- The service will be available on url: http://localhost/certsrv/mscep_admin
- If the password table is not full, the Network Device Enrollment Service will create a random password and embed it in an HTML page that is returned to the caller.
 - Note: Every time you connect to this URL, a different challenge password is displayed. Each challenge password is valid for 60 minutes and can only be used once.
- Use the device software, along with the password, to submit a certificate request through the Network Device Enrollment Service, which relays the request to the CA.
- If the enrollment request is successful, the requested certificate is returned to the device from the CA through the Network Device Enrollment Service.

By default, the Network Device Enrollment Service can only cache five passwords at a time. If the password cache is full when you submit a password request, you must do one of the following before resubmitting your request:

- Wait until one of the passwords has expired before submitting a new request.
- Stop and restart Internet Information Services (IIS) to delete all passwords stored in the cache.
- Configure the service to cache more than five passwords at a time.

Here is how to configure the feature upon installation:

Last update: 2019/10/31 windows:servers:net_data_enrollment_service https://wiki.plecko.hr/doku.php?id=windows:servers:net_data_enrollment_service 09:06

lew Object - User		\times
Create in:	/Service Accounts	
First name:	NDES Initials:	
Last name:	Service	
Full name:	NDES Service	
User logon name:		
NdesService	@ ~	
User logon name (pre	-Windows 2000):	
	NdesService	
		_
	< Back Next > Cancel	

Create a new AD user named NdesService

New Object - User	×
Create in:	Service Accounts
Password: ••• Confirm password: •••	••••••
User must change password a User cannot change password Password never expires Account is disabled	t next logon
	< Back Next > Cancel

Set a strong password for the user and tick 'Password never expires'

General Organization	Addres	-	Security	00111	Autoute Luite
Organization	eral Address Account Profile		Telephones		
Organization Published Certificates			Member Of		
Member of:					
Name		Active Direc	tory Domain	Services Fo	older
Demain Lleam				0011100011	
		/Us	iltic		
IIS_IUSKS		/Bu	ilitin iltin		
Server Operato	015	/00	incur i		
			_		
			_		
			_		
			_		
			_		
	_				
Add	Re	emove			
Add	Re	move			
Add	Re	emove			
Add Primary group:	Re	emove main Users			
Add Primary group:	Re	emove nain Users			
Add Primary group: Set Primary G	Re Dor	move main Users There is	no need to d	change Prim	ary group unless

Add newly created user to Server Operators group, and to IIS_IUSRS group

Local Security Policy				
File Action View Help				
🗢 🔿 🙍 📰 🗙 🖾 😼 🛛 🖬				
 Security Settings Account Policies Local Policies Local Policy Audit Policy User Rights Assignment Security Options Windows Firewall with Advanced Security Opticies Public Key Policies Software Restriction Policies Software Restriction Policies Software Restriction Policies IP Security Policies on Local Compute Advanced Audit Policy Configuration 	Policy Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and user accounts to be trusted for delega Image: Enable computer and the trust and the trust accounts to be trusted for delega Image: Enable computer and the trust accounts to be trusted for delega Image: Enable computer and the trust accounts accounts accounts to be trust accounts account	Security Setting Administrators LOCAL SERVICE,NETWO LOCAL SERVICE,NETWO Users,Window Manager Administrators Administrators Administrators Administrators Administrators Administrators	^	
Advanced Audit Policy Configuration	 Modify an object label Modify firmware environment values Perform volume maintenance tasks Profile single process Profile system performance Remove computer from docking station Replace a process level token Restore files and directories Shut down the system Synchronize directory service data Take ownership of files or other objects 	Administrators Administrators Administrators Administrators,NT SERVI Administrators LOCAL SERVICE,NETWO Administrators,Backup Administrators,Backup	III	

Open 'Local Security policy' on the server where you installed the NDES and navigate to Local Policies \Rightarrow User Rights Assignment, and double-click 'Log on as a service'

Log on as a service Properties ?	x
Local Security Setting Explain	
Log on as a service	
IIS APPPOOL\DefaultAppPool NT SERVICE\ALL SERVICES \NdesService	
Add User or Group Remove	
OK Cancel Apply	,

Add the newly created domain user to the list

C:\.	Administrator: Command Prompt	D X
Microsoft Windows [(c) 2013 Microsoft	Version 6.3.9600] Corporation. All rights reserved.	^ =
C:\Users\administra The command complet	ator>net localgroup IIS_IUSRS\NdesService /ad ed successfully.	ld
C:\Users\administra	tor.	

Open command prompt and add the newly created domain user to local IIS_IUSRS group by issuing the command: net localgroup IIS_IUSRS DOMAIN\NdesService /add

a	Add Roles and Features Wizard
Installation progre	CSS DESTINATION SERVER
Before You Begin	View installation progress
Installation Type	Feature installation
Server Roles	Configuration required. Installation succeeded on
Features Confirmation	Active Directory Certificate Services Additional steps are required to configure Active Directory Certificate Services on the destination
Results	Configure Active Directory Certificate Services on the destination server Network Device Enrollment Service Image: Service
	< <u>P</u> revious <u>N</u> ext > Close Cancel

After you have finished installing the Network Device Enrollment Service role, click 'Configure Active Directory Certificate Services on the destination server'

Last update: 2019/10/31 09:06 windows:servers:net_data_enrollment_service https://wiki.plecko.hr/doku.php?id=windows:servers:net_data_enrollment_service

2	AD CS Configuration
Credentials	DESTINATION SERVER
Credentials Role Services	Specify credentials to configure role services
Confirmation Progress Results	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:
	More about AD CS Server Roles
	< Previous Next > Configure Cancel

Make sure that you have the adequate credentials and click 'Next'



Tick the 'Network Device Enrollment Service' and click 'Next'

Last update: 2019/10/31 windows:servers:net_data_enrollment_service https://wiki.plecko.hr/doku.php?id=windows:servers:net_data_enrollment_service 09:06

<u> </u>	AD CS Configuration	
Service Account f	or NDES	DESTINATION SERVER
Credentials Role Services	Specify the service account	
Service Account for NDES	Select the identity the Network Device Enrollment Service (NDES) will u	ise.
Cryptography for NDES Confirmation	 Specify service account (recommended) The account must be a member of the domain and must be added 	to the local IIS_IUSRS group. Select
Progress Results	O Use the built-in application pool identity	
	More about Service Account for NDES	
	< Previous Next >	Configure Cancel
Click 'Select'		
Wi	ndows Security	
AD CS Configuration Type the name and password selected servers.	of an account with user rights on the	
For example, user@example.c	contoso.com, or domain\user name.	
NdesService	2	
M	•••	
Domain:	87 E	
Connect a	smart card	
	OK Cancel	
Enter the credentials of the	e newly created domain user and click 'OK'	

https://wiki.plecko.hr/

a	AD CS Configuration	_ D ×
Service Account f	or NDES	ESTINATION SERVER
Credentials Role Services Service Account for NDES RA Information Cryptography for NDES Confirmation Progress Results	Specify the service account Select the identity the Network Device Enrollment Service (NDES) will use. Specify service account (recommended) The account must be a member of the domain and must be added to the low NdesService Use the built-in application pool identity	ocal IIS_IUSRS group. Select
	More about Service Account for NDES < Previous	gure Cancel

Now that we have selected the user, click 'Next'

<u></u>	AD C	S Configuration
RA Information		DESTINATION SERVER
Credentials Role Services	Type the request	ed information to enroll for an RA certificate
Service Account for NDES RA Information	A registration authority (certificate requests.	RA) is required to manage the Network Device Enrollment Service (NDES)
Cryptography for NDES	Required information	
Confirmation	RA N <u>a</u> me:	MSPCA01-MSCEP-RA
Progress	Co <u>u</u> ntry/Region:	HR (Croatia) 🔻
Results	Optional information	
	<u>E</u> -mail:	dc@hr
	C <u>o</u> mpany:	d.o.o.
	Department:	П
	<u>C</u> ity:	Zagreb
	State/Province:	Croatia
	More about RA Informat	ion
		< <u>P</u> revious <u>N</u> ext > <u>C</u> onfigure Cancel

Enter the required details in the form and click 'Next'

a	AD CS Configuration	_ □	x
Cryptography for	NDES	DESTINATION SER	VER
Credentials Role Services	Configure CSPs for the RA		
Service Account for NDES RA Information	Select the registration authority (RA) cryptographic service provide the signature and encryption keys.	ers (CSPs) and key lengths for	
Cryptography for NDES	Signature key provider:	Key length:	
Confirmation	Microsoft Strong Cryptographic Provider	▼ 2048	•
Progress	Encryption key provider:	Key length:	
Results	Microsoft Strong Cryptographic Provider	▼ 2048	•
	More about Cryptography for NDES		
	< Previous Next >	Configure Cance	ł

You can leave this as-is and click 'next'. Or you can change the providers and key lengths, but this is OK

Last update: 2019/10/31 09:06 windows:servers:net_data_enrollment_service https://wiki.plecko.hr/doku.php?id=windows:servers:net_data_enrollment_service

🖹 AD CS Configuration 📃 🗖 🗙				
Confirmation		DESTINATION SERVER		
Credentials Role Services	To configure the following roles, role services, or features, click Configure. Active Directory Certificate Services 			
Service Account for NDES RA Information Cryptography for NDES Confirmation Progress Results	Network Device Enrollmen Account: RA Information: Name: Country/Region: Email: Company: Department: City: State/Province: Signature Key Provider: Signature Key Length: Exchange Key Length:	At Service NdesService MSPCA01-MSCEP-RA HR dc@hr IT Zagreb Croatia Microsoft Strong Cryptographic Provider 2048 Microsoft Strong Cryptographic Provider 2048		
		< Previous Next > Configure Cancel		

Confirm that all data is correct and click 'Configure'

2025/04/15 20:12 13/1	Configure the Network Device Enrollment Service In Picture				
à	AD CS Configuration	on	_ D X		
Results			DESTINATION SERVER		
Credentials	The following roles, role services, or featur	es were configured:			
Role Services	 Active Directory Certificate Services 				
Service Account for NDES	Network Device Enrollment Service	Configuration succ	eeded		
RA Information	More about NDES Configuration	Configuration succ	leeueu		
Cryptography for NDES					
Confirmation					
Progress					
Results					
	< Previ	ious Next >	Close Cancel		

Close the wizzard and you're done!

