# Network Device Enrollment Service (NDES) Installation Guide

# Contents

Prerequisites	. 2
Configuring NDES	. 2
Step 1: Deploy Active Directory Certificate services	. 2
Step 2: Configure Active Directory Certificate services	.7
Step 2a: Configure Certification Authority	.8
Step 2b: Configure Network Device Enrollment Service (NDES)	13
Verify NDES Service configuration1	17
NDES Service Challenge Password configuration1	19
Default behaviors1	19
To change the maximum number of passwords cached by NDES (PasswordMax)1	19
To change the challenge password validity period (PasswordValidity)1	19
To reuse the same challenge password (UseSinglePassword)1	19
References2	20

## Network Device Enrollment Service (NDES)

Network Device Enrollment Service (NDES) - Microsoft's implementation of SCEP



## Prerequisites

The following are the prerequisites to install NDES server.

- A service account for NDES server
  - New user to be created (Example: ndesadmin@\_\_\_\_.com)
  - Must be a domain user account
  - Must be a member of local IIS\_IUSRS group
- Admin user credentials with Enterprise administrator privileges and local administrator privileges to the server where NDES will be installed (i.e. in dev-m\_\_\_\_\_\_x.com)

## **Configuring NDES**

To configure NDES, complete the following steps:

#### Step 1: Deploy Active Directory Certificate services

1. From Microsoft Windows Server Manager dashboard, click Manage and select Add Roles and Features.

Server Ma	anager • Dashboard			• ©   <b>ľ</b>	Manage Tools View Help Add Regrand Features
III Dashboard	WELCOME TO SERVER MANAGER				Remove Roles and Features
Local Server					Add Servers Create Server Group
All Servers	1 Conf	iqure this local server			Server Manager Properties
■ File and Storage Services ▷	0.000	gure uns local ser rer			
LO IIS	2 AC	ld roles and features			
		Id ather concerns to many or			
	3 AC	lo other servers to manage			
	4 Cr	eate a server group			
	5 Cc	nnect this server to cloud service	95		
	(EAD) MODE				Hide
	Roles: 2   Server groups: 1   Servers tota	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Local Server 1	All Servers 1	
	Manageability	Manageability	Manageability	Manageability	
	Events	Events	Events	Events	
	Performance	Services	2 Services	2 Services	
	BPA results	Performance	Performance	Performance	
		BPA results	BPA results	BPA results	
			5/27/2022 10:27 AM	5/27/2022 10:27 AM	

2. Read the content in the **Before You Begin** page and click **Next**.

Dashboard	WELCOME TO S	ERVER MANAGER		
.ocal Server All Servers File and Storage Services		La Add Roles and Features Wizard	- n x	
s	QUICK START	Before you begin Before You Begin Installation Type Server Selection Server Robe	This wards helps you initial roles, role services, or halances. You determine which roles, role services, or features to initial based on the computing needs of your organization, such as sharing documents, or helps are based on the computing needs of your organization, such as sharing documents, or helps are based on the computing needs of your organization.	
	LEARN MORE Roles AND SEF Roles 2   Server File and Services Manager Events Performa		Before you continue, weinfy that the following tasks have been completed: • The d-inimization account has a storing parsonnel • The most handle and the storing barbones of the storing • The most current security updates from Windows Update are installed • Thy you must weight have of the preseding particular have been completed, close the witard, complete the storp, and then run the witard again. To continue, click Next.	168
	8PA resu		Skip this page by default	
			5/27/2022 10:27 AM 5/27/	8022 10:27 AM

3. For Installation Type, select 'Role-based or feature-based installation' and click Next.

I Local Server         All Servers         I Is         I Is         All Servers         I Is         Servers Services In         VILLIST NEW         Servers Selection         Servers S	Server Manager	anager • Dashboard	• @   <b>/</b>	Manage	Tools View	D X
< Previous	Iteration         Iteration           Iteration         Local Server           Iteration         All Servers           Iteration         Storage Services           Iteration         Iteration           Iteration         Iteration	WELCOME TO SERVER MANAGER         CUCK STANT         CUCK STANT         Select installation type         UNATES NEW         Before You Begin         Installation Type         DETINATION SERVER         Detination Server         Fore You Begin         Installation Type         Detination Server         Detination Server         Fore Select         Confirmation         Revise         Confirmation         Revise         Pristallation         Pristallation Type         Detrive Factor         Factors         Confirmation         Revise         Pristallation         Results         Pristallation         Results         Pristallation         Results         Pristallation         Results         Performs         BPA ress	1			Hide
		< Previous	27/2022 10:27 AM			

4. In the Server Selection section, retain the defaults and click Next.

Local Server										
All Servers		퉖 Add Roles and Features Wizard	(			( <u>—</u>				
File and Storage Services ▷	CHINEY CTADT					DES	INATION SERVER			
115	QUICK START	Select destination	server			dev	com			
		Before You Begin	Select a server or a vin	tual hard disk on which	to install roles and feat	ures.				
	WHAT'S NEW	Installation Type	Select a server from	n the server pool						
		Server Selection Server Roles	Senior Pool	a aisk						
		Features	Filter							1.6
	LEARN MORE	Confirmation	Filter:							н
		, Mesolita:	Name	IP Address	Operating System	Server 2019 Datace	oter			
	ROLES AND SE Roles: 2   Server	1								
	File and	d						1		
	- Service	e e								
	Manage     Events	56	1 Computer(s) found				(			
	Perform	a	This page shows serve	rs that are running Wir Ided by using the Add	ndows Server 2012 or a Servers command in Se	newer release of Wi ver Manager, Offlin	ndows Server, e servers and			
	BPA res		newly-added servers fi	rom which data collect	ion is still incomplete ar	e not shown.				
						C. In some				
				< 21	5/27/2022	10:27 AM	Cancel 5/2	7/2022 10:27 AM		
					276776066		-91-	The contract for the second		

5. In the Server Roles section, select 'Active Directory Certificate Services' and click Next.

Dashboard	WELCOME TO S	ERVER MANAGER				
All Servers		LAdd Roles and Features Wizard		- 🗆 X		
■ File and Storage Services ™ IIS	QUICK START	Select server roles		devLcom		
	WHAT'S NEW	Before You Begin Installation Type Server Folection Server Roles Features AD CS Role Services Confirmation Results	Select one or more roles to install on the selected server.  Roles  Active Decotory Centrical Services  Active Directory Rolation Services  Active Directory Rolation Brevices  Active Directory Rolation Brevices  Directo	Description Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.	1	Hide
			< Previous Nex 5/2	t > Install Cancel 7/2022 10:27 AM 5/21	7/2022 10:27 AM	

6. In the Features section, retain the defaults and click Next.

Local Server						
All Servers		📠 Add Roles and Features Wizard		- 🗆 ×		
File and Storage Services IIS	QUICK START	Select features		DESTINATION SERVER		
	MULATIC NEW	Before You Begin Installation Type	Select one or more features to install on the selected server.	Description		
	I FARN MORE	Server Selection Server Roles Features AD CS	NET Framework 3.5 Features     NET Framework 4.7 Features (2 of 7 installed)     Background Intelligent Transfer Service (BITS)     BitLocker Drive Encryption     BitLocker Network Unlock	NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect		Hic
	ROLES AND SEI Roles: 2   Server	Role Services Confirmation Results	BranchCache  Client for NFS  Containers (Installed)  Data Center Bridging  Direct Play  Ephaneed Storage	your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.		
	File and Services		Financed solvage     Failure Clustering     Group Policy Management     Host Guardian Hyper-V Support     I/O Quality of Service		1	
	Events Performa	z	IIS Hostable Web Core Internet Printing Client IP Address Management (IPAM) Server ISNS Server service			
	BPA resu					
			< Previous Next	2022 10:35 AM 5/	27/2022 10:35 AM	

7. In the **AD CS** section, click Next. From **Role Services**, select 'Certificate Authority' and 'Network Device Enrollment Services' and click **Next**.

Server Ma	anager • Da	ashboard Server Manager					• @	Manage	Tools View Help
■ Local Server ■ All Servers ■ File and Storage Services ▷ ■ IIS	QUICK START	Add Roles and Features Wizar	d es						
	WHAT'S NEW LEARN MORE Roles 2   Sener Roles 2   Sener Manage Events Performs BPA resu	Before You Begin Installation Type Server Roles Features ADICS Role Services Confirmation Results	Select the role services to install fo Role services           Certification Authonity           Certificate Evolument Polic           Certificate Evolument Polic           Certification Authority           Certification Authority           Orbine Responder	r Active Directory Certificat (y Web Service Service 5 Ervicient 5 Ervice	e Services Description Network Device Enrollment makes it possible to suse a manage certificates for rou other network devices that have network accounts.	Service nd ers and do not	1		Hide
				< Previous Ne	t > Install	Cancel 5/27/4	022 10:35 AM		
ा २ म <b>ह</b>								^ <b>(</b>	₽ 🖵 4 🔒 10:37 AM 💭

8. In the **Confirmation** section, read and verify the information and click **Install.** 

oard Server	WELCOME TO SI	ERVER MANAGER				
vers		La Add Roles and Features Wizard		- 🗆 ×	1	
id Storage Services ♪	QUICK START	Confirm installatio	n selections 🛶	DESTINATION SERVER		
	WHAT'S NEW	Before You Begin Installation Type Server Selection Server Roles	To install the following roles; role services; or features on selected server, click insta Bestart the destination server automatically if required Optional features (such as administration toold) might be displayed on this page by been selected automatically. If you do not want to install these optional features, d their check boxes.	ll. Icause they have lick Previous to clear		
	LEARN MORE	Features AD CS Role Services	Active Directory Certificate Services Certification Authority			
I	ROLES AND SER	Confirmation Results	Network Jewice Enrollment Service Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools		1	
	Services     Managea     Events				,	
	Performa BPA resu		Export configuration settings Specify an alternate source path			
			< Previous Next >	all Cancel		
			5/27/2022 10:35 AM	5/	27/2022 10:35 AM	

#### Step 2: Configure Active Directory Certificate services

1. To configure Active Directory Certificate Services, from the Server Manager Dashboard, click and select **Post-deployment Configuration**.

Server Ma	anager • Dashboard			• ©   🍢	Manage Tools View Help
Dashboard	WELCOME TO SERVER MANAGER		4	Post-deployment Configuration	
All Servers	1 Config	gure this local server		Services at W 19 Promote this server to a domain controller	
AD DS	QUICK START	roles and features		Configuration required for Active Directory Certificate	
■ File and Storage Services ▷ ∎ ■ IIS	3 Add	other servers to manage ate a server group		Configure Active Directory Certificate Services on th Task Details	
	5 Cor	nect this server to cloud services	_		Hide
	ROLES AND SERVER GROUPS Roles: 5   Server groups: 1   Servers total:	1 ad ds 1	DNS 1	File and Storage	
	Manageability     Events     Services	Manageability     Events     Services	Manageability Events Services	Services     Manageability     Events     Services	
	Performance BPA results	Performance BPA results	Performance BPA results	Performance BPA results	
		Local Server 1	All Servers 1		

2. Under ROLES AND ERVER GROUPS, select AD CS. In the **Credentials** section, enter the Server Manager Administrator credentials, and click **Next**.

🗲 Э 🗝 Ser	rver Manager 🕨 Da	shboard	• 🕄   🖡
Dashboard	WELCOME TO SE	RVER MANAGER	
<ul> <li>Local Server</li> <li>All Servers</li> <li>AD CS</li> <li>AD DS</li> <li>DNS</li> <li>File and Storage Set</li> <li>IIS</li> </ul>	AD CS Configuration Credentials Role Services Confirmation Progress Results	DESTINATION SERVER WIN- DESTINATION SERVER WIN- Destination services Specify credentials to configure role services To install the following role services you must belong to the local Administrators group:     Standalone certification authority     Certificate favoliment Policy Web Service     Certificate Enrollment Veb Service     Certificate Enrollment Service Credentiats: SCEPV Change.	1       File and Storage       1         Image: Services       1         Image: Manageability       Events
		More about AD CS Server Roles	Performance BPA results

## Step 2a: Configure Certification Authority

Dashboard	WELCOME TO	SERVER MANAGER			
Local Server All Servers AD CS		AD CS Configuration		DESTINATION SERVER	
AD DS     DNS	QUICK START	Credentials	Select Role Services to configure	WIDCal	
I∎ File and Storage Services ▷ In IIS	WHAT'S NEW	Role Services Setup Type CA Type Private Key	Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service	1	
	LEARN MORE	Cryptography CA Name Certificate Request	Certificate Enrollment Web Service		
	ROLES AND Roles: 5   Se	Certificate Database Confirmation Progress			
	AD C				nd Storage 1
	① Man				geability

1. In the **Role Services** section, select 'Certification Authority' and click **Next**.

2. For Setup Type, select 'Enterprise CA' and click **Next**.

1

Local Server

Ever Serv Perf

BPA

IIS 🗊

🗰 Dashboard	WELCOME TO SERVER MANAGER		
Local Server     All Servers     All Servers     All CS     D     AD CS     D     D     D     D     D     D     T     File and Storage Services      IIS	CURCK START COLICK START WHAT'S NEW	-       -       -       -       -       -       -	
	CA Name Cartificate Request Certificate Database Confirmation Progress Results Man Even Serv Perfc BPA	certificate policies.  Sundatione CA Sundatione CA Subartic CA Subartic CA Subartic CA Subartic Connection (offline).  More about Setup Type	nd Storage 1 ces 1 geability 2 ses mance 2 soults

< Previous Next >

All Servers

Configure Cancel

3. For **CA Type**, select 'Root CA' and click **Next**.

Server M	lanager 🕨	Dashboard		- 🕄   🍢 Manage
<ul> <li>Server M</li> <li>Dashboard</li> <li>Local Server</li> <li>All Servers</li> <li>AD DS</li> <li>DNS</li> <li>File and Storage Services P</li> <li>IIS</li> </ul>	Unager → WELCOME T QUICK START WHAT'S NEW LEARN MORE ROLES AND ROLES AND ROLES AND CO Mana EVen Sand	Dashboard	DESTINATION SERVER     WIN     DESTINATION SERVER     WIN     Specify the type of the CA     Specify the type of the CA     Won you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its ours self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI     hierarchy.     P Root CA     Root CA are the first and may be the only CAs configured in a PKI hierarchy.     Subordinate CA require an established PKI hierarchy and are authorized to issue certificates by     the CA above them in the hierarchy.	res 1 peability
	Servi Perfo		More about CA Type	es mance
	BPA		<pre></pre>	sults

4. For **Private Key**, select 'Create a new private key' option and click Next.

Dashboard	WELCOME TO	D SERVER MANAGER			
Local Server		AD CS Configuration	- 🗆 X		
AD CS AD DS	QUICK START	Private Key	DESTINATION SERVER WIL		
DNS		Credentials	Specify the type of the private key		
File and Storage Services ▷		Role Services			
IIS	WHAT'S NEW	Setup Type	To generate and issue certificates to clients, a certification authority (CA) must have a private key.		
		CA Type Private Key	Ocreate a new private key Use this option if you do not have a private key or want to create a new private key.		
	LEARN MORE ROLES AND Roles: 5   Ser	Cryptography CA Name Validity Period Certificate Database Confirmation Progress	<ul> <li>Use existing private key</li> <li>Use this option to ensure continuity with previously issued certificates when reinstalling a CA.</li> <li>Select a certificate and use its associated private key</li> <li>Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.</li> <li>Select an existing private key on this computer</li> <li>Select this option if you have retained private keys from a previous installation or want to</li> </ul>		
	MR AD C		use a private key from an alternate source.	tes 1	
	① Mana			geability	
	Event Servio Porto		More about Private Key	25	
	BPA r		< Previous Next > Configure Cancel	sults	

5. Cryptography: Specify the cryptographic options as required and click Next.

Server Ma	∕lanager + Dashboard	• 🗭   🍢 Manage Tools View
<ul> <li>Construction</li> <li>Construction</li> <li>Construction</li> <li>Construction</li> <li>AD CS</li> <li>AD CS</li> <li>AD DS</li> <li>DNS</li> <li>File and Storage Services ▷</li> <li>IS</li> </ul>	Velcome to server MANAGER         Welcome to server MANAGER         Cryptography for CA         Cryptography for CA         WHATS NEW         Credentials         Roles Services         Setup Type         CA Type         Private Key         Vidity Period         Certificate Database         Vidity Period         Roles S 1 Ser         Roles S 1 Ser         Allow administrator interaction when the private key is accessed by the CA.	View
	AD C     Results     More about Cryptography     Perfo     BPA r     Configure     Can     Configure     Can     Can	nd Storage 1 res 1 reability ss mance sults

6. For **CA Name**, configure the settings as required and click **Next**.

Server M	lanager 🕨 [	Dashboard		• @   🍢	Manage
Dashboard Local Server All Servers AD CS AD DS DNS File and Storage Services IS	UNDER START	Dashboard	DESTINATION SERVER      DESTINATION SERVER      WI      Specify the name of the CA      Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.      Common name for this CA:     scc      CA      Distinguished name suffic:     DC=scep.DC=bigfix.DC=local      Preview of distinguished name:     (N=scep-V)	• @   M	Manage
	AD C Mana Event Servic Perfo BPA r	RESUIS	More about CA Name	es 1 jeability 25 nance sults	

7. Validity Period: Configure the CA certificate validity period and click Next.

€∋- Server	Manager 🕨 [	Dashboard		🕶 🍘   🍢 Manage Tools
📰 Dashboard	WELCOME TO	O SERVER MANAGER		
Local Server		L AD CS Configuration	- 🗆 🗙	
All Servers				
R AD CS		Validity Period	WI Col	
AD DS	QUICK START	· · · · · · · · · · · · · · · · · · ·		
B DNS		Credentials	Specify the validity period	
File and Storage Services	Þ	Role Services		
IIS	WHAT'S NEW	Setup Type	Select the validity period for the certificate generated for this certification authority (CA):	
		CA Type	5 Years  CA expiration Date: 27.05.2027 16-20:00	
		Private Key	CM expiration Date: 27-03-2027 10:33:00	
		CA Name	The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.	
	LEARN MORE	Validity Period		
		Certificate Database		
	ROLES AND	Confirmation		
	Koles. 5   Sel			
	🛤 AD C			nd Storage 1
	<u></u>			es
	U Mana			jeability
	Event			
	Servic		More about Validity Period	25
	Perfor			nance
	BPA r		< Previous Next > Configure Cancel	sults

8. Certificate Database: Configure the certificate database location and click Next.

Server M	lanager 🕨 [	Dashboard			• 闭   🍢 Manage
🗰 Dashboard	WELCOME TO	O SERVER MANAGER			
Local Server		L AD CS Configuration		- 🗆 X	}
All Servers					
💀 AD CS		CA Database		DESTINATION SERVER	
🖬 AD DS	QUICK START	0.100000000		in clocal	
🖴 DNS		Credentials	Specify the database locations		
■ File and Storage Services ▶		Role Services			
IIS	WHAT'S NEW	Setup Type	Certificate database location:		
	WIDT STILL	СА Туре	C:\Windows\system32\CertLog		
		Private Key	Certificate database log location:		
		Cryptography	C:\Windows\system32\CertLog		
	LEARN MORE	CA Name			
		Validity Period			
	ROLES AND	Certificate Database			
	Roles: 5   Sen	Progress			
					nd Storage
	-A ADC				es
	🛈 Mana				eability
	Event				
	Servic		More about CA Database		rs
	Perfor				nance
	BPA re		< Previous New	t > Configure Cancel	sults
					L

9. Verify the configuration and click Configure.

Server N	lanager 🕨 [	Dashboard	• ②	🍢 Manage
📰 Dashboard	WELCOME TO	O SERVER MANAGER		
Local Server		L AD CS Configuration	- 🗆 X	
All Servers				
R AD CS		Confirmation	WIN local	
I AD DS	QUICK START			
DNS		Credentials	To configure the following roles, role services, or features, click Configure.	
■ File and Storage Services ▶		Role Services	Active Directory Certificate Services	
∎© IIS	WHAT'S NEW	Setup Type	Certification Authority	
		CA Type	CA Type: Enterprise Root	
		Crustography	Cryptographic provider: RSA#Microsoft Software Key Storage Provider	
		CA Name	Key Length: 2048	
	LEARIN MORE	Validity Period	Allow Administrator Interaction: Disabled	
		Certificate Database	Certificate Validity Period: 27-05-2027 16:39:00	
	ROLES AND : Roles: 5   Sen	Confirmation	Certificate Database Location: C:\Windows\system32\CertLog	
		Progress	Certificate Database Log C:\Windows\system32\CertLog	
	🖳 AD C	Results	Location: Id Storage 1	
	① Mana		ability	
	Uniditia		eability	
	Event			
	Servic		S	
	Perfor		hance	
	BPA re	·	< Previous Next > Configure Cancel sults	

10. Close after configuration succeeds, and click **Yes** to configure additional role services.

Server M	anager • Dashboard		🕄   🍢 Manage 1
📰 Dashboard	WELCOME TO SERVER MANAGER		
Local Server     All Servers     AD CS	1 Configure this local server		
AD DS DNS	QUICK START 2 Add roles and features		
<ul> <li>File and Storage Services P</li> <li>IIS</li> </ul>	WHAT'S NEW         3         Add other servers to manage           4         Create a server group		
	5 Connect this server AD cs Configuration	×	
	Do you want to configure addit ROLES AND SERVER GROUPS Roles 5   Server groups: 1   Servers total: 1 Ves	onal role services ?	
	AD CS 1 AD DS 1	DNS 1 File and Storage Services	1
	Manageability     Manageability       Events     Events       Services     Services	Manageability ① Manageability Events Events Services Services	
	Performance Performance BPA results BPA results	Performance Performance BPA results BPA results	

#### Step 2b: Configure Network Device Enrollment Service (NDES)

1. On the AD CS Configuration page, in the **Credentials** section, verify the logged in Administrator credentials, and click **Next**.

Server Ma	anager • Dashboar	d		• @   <b> </b>	Manage	Tools
📰 Dashboard	WELCOME TO SERVER MA	NAGER				
<ul> <li>Local Server</li> <li>Al Servers</li> <li>AD CS</li> <li>AD DS</li> <li>DNS</li> <li>File and Storage Services ▷</li> <li>IIS</li> </ul>	QUICK START WHAT'S NEW LEARN MORE ROLES AND SERVER GROO Roles: 5   Server groups: 1   AD CS Manageability Events Services Performance BPA results	AD CS Configuration Credentials Credentials Role Services Confirmation Progress Results	Credentials: SCEPV     Credentials     Credentials: SCEPV     Credentials: SCEPV     Credentials: SCEPV     Configure Roles	1		

2. From **Role Services**, select 'Network Device Enrollment Service' and click **Next**.

Server Ma	anager • Dashboard		🕶 🗭   🍢 Manage Tools Vie
Dashboard	WELCOME TO SERVER MANAGER		
Local Server     All Servers     AD CS     AD DS	AD CS Configuration QUICK START Role Services	- D DESTINATION SERVE	R H
mi UNS mi File and Storage Services ▷ io IIS	LEARN MORE 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	
	ROLES AND SERVER GROU Roles: 5   Server groups: 1   AD CS Manageability Events Services Performance BPA results	More about AD CS Server Roles	1

3. In the **Service Account for NDES** section, select the 'Specify service account recommended' option and enter the credentials of the service account created for NDES. Click **Next**.

Important: The service account created must be a part of the local IIS\_IUSRS group from Server Manager > Tools > Computer Management > Local Users and Groups > Groups > IIS\_USRS > Add to Group menu.

⊖	anager • [	Dashboard		• 🕄   🍢 Manage
Local Server		L AD CS Configuration	- 🗆 X	]
All Servers				
AD CS		Service Account	for NDES with the server	
AD DS	QUICK START			
DNS		Credentials	Specify the service account	
File and Storage Services 👂		Role Services		
D IIS		Service Account for NDES	Select the identity the Network Device Enrollment Service (NDES) will use.	
	WHAT S NEW	RA Information	<ul> <li>Specify service account (recommended)</li> </ul>	
		Cryptography for NDES	The account must be a member of the domain and must be added to the local IIS_IUSRS group.	
	LEARN MORE	Progress Results	Use the built-in application pool identity	
	ROLES AND 3 Roles: 5   Serv Roles: 5   Service Roles: 5   Service Roles: 5   Service Roles: 5   Service Roles: 5   Service Roles: 6   Service Roles: 6   Service Roles: 6   Service Roles: 7   Servic		More about Service Account for NDES	d Storage 1 es 1 eability s hance tults

4. **RA Information**: Configure Registration Authority (RA) Information (update only if required) and click **Next**.

Server M	anager • Dashboard	🔹 🍘   🍢 Manage Tools
Dashboard	WELCOME TO SERVER MANAGER	
<ul> <li>Local Server</li> <li>All Servers</li> <li>AD CS</li> <li>DNS</li> <li>File and Storage Services ▷</li> <li>IIS</li> </ul>	CLICK START  CAUCK START  WHAT'S NEW  LEARN MORE  ROLES AND SERVER GROU Roles: 5   Server groups: 1   S  AD CS  Manageability Events Services Performance BPA results	1

5. **Cryptography for NDES**: Update cryptographic details for NDES (update only if required) and click **Next**.

Server Ma	anager • Dashboard	Ł			• 🕲 I	Мап.	age Tools	View
Dashboard	WELCOME TO SERVER MAN	IAGER						
All Servers AD CS AD DS DNS	QUICK START	L AD CS Configuration	NDES w	DESTINATION SERVER VIN-				
III File and Storage Services ▷ IIIS	WHAT'S NEW	Credentials Role Services Service Account for NDES RA Information	Configure CSPs for the RA Select the registration authority (RA) cryptographic service provi signature and encryption keys.	iders (CSPs) and key lengths for the				
	LEARN MORE  ROLES AND SERVER GROUP Roles: 5   Server groups: 1   S  AD CS  Manageability Events	Crofirmation Progress Results	Microsoft Strong Cryptographic Provider Encryption Rey provider: Microsoft Strong Cryptographic Provider	v         2048         ∨           Key length:         ∨           2048         ∨	1			1
	Services Performance BPA results		More about Cryptography for NDES	Configure Cancel				

6. Verify the details and click **Configure.** 

🕤 🕘 - 🛛 Server M	lanager 🕨 Dash	board				• 🕲	Manage	Tools
Image: Cool Server         Image: All Servers         Image: All Servers	WELCOME TO SERV	ER MANAGER CS Configuration CS Configuration Credentials tole Services iervice Account for NDES tA Information Cryptography for NDES Confirmation Confirmation	To configure the following rol Configure the following rol Active Directory Certific Network Device Enrollment Account: RA Information: Name: Country/Region: Enrol		ANATION SERVER bigfix.local			
	ROLES AND S Roles: 5   Serv AD CS Manag Events Servico Perfor BPA re	lesults	Company: Company: Department: City: Sitate/Province: Signature Key Provider: Signature Key Length: Exchange Key Length: Exchange Key Length:	<pre></pre> <pre>&lt;</pre>	Cancel	d Storage <u>1</u> 25 2ability 5 Nance ults		

7. Close after configuration succeeds.



## Verify NDES Service configuration

To verify if the SCEP services are running and working as expected, to the following:

1. Open the Internet Information Services (IIS) Manager and check if SCEP service is started.

)))•	Server Manager + IIS	5						• 3	Mar
Dashboard	All servers	1 total							
Local Server									
All Soniors	Filter	م	• (=) •	• (11) •					-
An Servers	Internet Information Services (IIS) N	Manager						- 🗆 ×	
ADICS		19 Application Pools	5					😰 🖂 🔂 🔞 •	
AD DS	File View Help								
DNS	Connections							Actions	
llS	Start Page       WIN-1       P\Adi       Application Pools	This page lets you view processes, contain one	ION POOI w and manag e or more app	S e the list of a plications, and	oplication pools on I provide isolation a	the server. Application among different applic	pools are associated with worker ations.	Add Application Pool Set Application Pool Defaults Application Pool Tasks  Start	2
	> - 💽 Sites	Flitter:	• 40	30 * 🚛 Sho	W All Group by:	No Grouping	•	Stop	
		Name	Status	NET CLR V	Managed Pipel	Identity	Applications	😂 Recycle	
		MET v2.0	Started	v2.0	Integrated	ApplicationPoolId	0	Edit Application Pool	
		.NET v4.5	Started	v4.0	Integrated	ApplicationPoolld	0	Basic Settings	
		.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolld	0	Recycling	
		Classic .NET Ap	Started	v2.0	Classic	ApplicationPoolld	0	Advanced Settings	
		DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolld	1		
		U SCEP	Started	v4.0	Classic	scepadmin@scep	<u> </u>	Kemove	-
								View Applications	-
		Features View - C	Content View					W Hep	
	>		STATE TROUT					87	_
	Keady							•	

2. Verify SCEP admin app page to get challenge password and CA Thumbprint. Use SCEP service account to authenticate the request.

.125/certsrv/mscep_a				
$\leftrightarrow$ $\rightarrow$ $C$ (i) 19	/certsrv/mscep_admin/			
		Sign in http://19 Your connec	125 tion to this site is not private	
		Username	ndesadmin@scep.bigfix.local	
		Password		
			Sign in Cancel	

← → C A Not secure   1
Network Device Enrollment Service
Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).
To complete certificate enrollment for your network device you will need the following information:
The thumbprint (hash value) for the CA certificate is: 5D837 BF78C
The enrollment challenge password is: 933 B39
This password can be used only once and will expire within 60 minutes.
Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.
For more information see Using Network Device Enrollment Service.

3. CA Certificate templates can be configured from the Certification authority service (Windows > Run > certsrv.msc) > Certificate Templates.

File Action View Help			
Þ 🤿 🖄 🔤 🔯			
Certification Authority (Local) Scep-Wi Revoked Certificates Pending Requests Failed Requests Certificate Templates	Name IPSec (Offline request) IPSec (Offline request) IPSec (Offline request) IPSec (Offline r IPSec Addition IPSec Controller Authentication IPSec Corey Agent IPSec Authentication IPSec Corey Agent IPSEC IPSIC IPS	Intended Purpose IP security IKE intermediate Certificate Request Agent Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all> Microsoft Trust List Signing, Encrypting</all>	

4. You can check the certificates issued from Certification authority service (Windows > Run > certsrv.msc) > Issued Certificates.

Certification Authority (Local)	r Name	Binary Certificate	Certificate Template	Serial Num	ber	Certificate Effective Date	Certificate Expiration Date	Issued Country/Region	Issued Organization	Issued Organization Unit	Issued Common I	Name
Scep-wij pis-CA	ministra	BEGIN CERTI	Exchange Enrollment	26	d4	27-05-2022 16:52	26-05-2024 16:52	IN			WIN-	MS
Revoked Certificates	ministra	BEGIN CERTI	CEP Encryption (CEP	26	6e	27-05-2022 16:52	26-05-2024 16:52	IN			WIN-	MS
issued Certificates	ministra	BEGIN CERTI	Exchange Enrollment	26	736	27-05-2022 17:07	26-05-2024 17:07	IN			WIN-	MS
Ending Requests	ministra	BEGIN CERTI	CEP Encryption (CEP	26	925	27-05-2022 17:07	26-05-2024 17:07	IN			WIN-	MS
Certificate Templates	esadmin	BEGIN CERTI	IPSec (Offline reques	260000000	óf7	27-05-2022 17:19	26-05-2024 17:19				Vijesl	

In the endpoint, you can check the certificates issued from certmgr (Windows > Run > certmgr.msc)

acertmgr - [Certificates - Current User/Personal\Certificates]									
File Action View Help									
⋥ Certificates - Current User	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem		
Personal	2 V	scer 5UI9-CA	5/26/2024	IP security IKE inter	<none></none>		IPSec (Offline r		
Certificates				,					
> Invited Root Certification Aut									
> Enterprise Trust									
Intermediate Certification Aut									
> Active Directory User Object									
Trusted Publishers									
> Intrusted Certificates									
> Inited Party Root Certification									
> Invited People									
> In Client Authentication Issuers									
> Certificate Enrollment Reques									
> Smart Card Trusted Roots									

# NDES Service Challenge Password configuration

#### Default behaviors

The following are the default NDES behavior with respect to the challenge password:

- Password cannot be reused for certificate enrollment requests. Every request to the NDES admin service (<u>http://ndes\_service/certsrv/mscep\_admin</u>) shall generate a new password.
- The maximum number of passwords that will be cached in the server is 5.
- The password validity is 60 minutes.

With the above default behavior, only maximum of 5 certificate enrollment requests per hour can be processed by NDES service.

All of these can be overridden with below registry configurations.

To change the maximum number of passwords cached by NDES (PasswordMax)

You can update the maximum number of passwords that can be cached by NDES through the following steps:

- 1. Run Registry editor (Regedit)
- 2. Go to HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\MSCEP
- 3. Create a new Key named PasswordMax
- 4. Under the *PasswordMax* key, create a new *DWORD* with the same name *PasswordMax* and set the value in decimals. The value will decide the number of passwords that can be cached.
- 5. Restart IIS

#### To change the challenge password validity period (PasswordValidity)

You can change the challenge password validity period from 60 minutes through the following steps:

- 1. Run Registry editor (Regedit)
- 2. Go to HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\MSCEP
- 3. Create a new Key named PasswordValidity
- 4. Under the *PasswordValidity* key, create a new *DWORD* with the same name *PasswordValidity* and set the value in decimals. The value will decide the password validity in minutes for which it should be cached.
- 5. Restart IIS

#### To reuse the same challenge password (UseSinglePassword)

To allow reusing the same challenge password for every certificate enrollment request, the following registry key needs to be updated. This prevents the NDES admin service from generating new challenge passwords.

- 1. Run Registry editor (Regedit)
- 2. Go to HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\MSCEP
- 3. Modify the value of the key UseSingePassword as 1
- 4. Restart IIS

Note: If the SCEP services fails to start due to above change, configure the following:

- 1. Open IIS Manager.
- 2. In the navigation pane, click Application Pools.

- 3. In Application Pools, click SCEP.
- 4. In the Actions pane, click Advanced Settings.
- 5. Under *Process Model*, click *Load User Profile*. Set to **True**.
- 6. Click OK to all dialog boxes.
- 7. Restart IIS

## References

- <u>http://everythingaboutintune.com/2020/07/ndes-and-scep-setup-for-intune-a-complete-guide/</u>
- <u>https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-how-to-configure-ndes-for-scep-certificate/ba-p/455125</u>