

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.

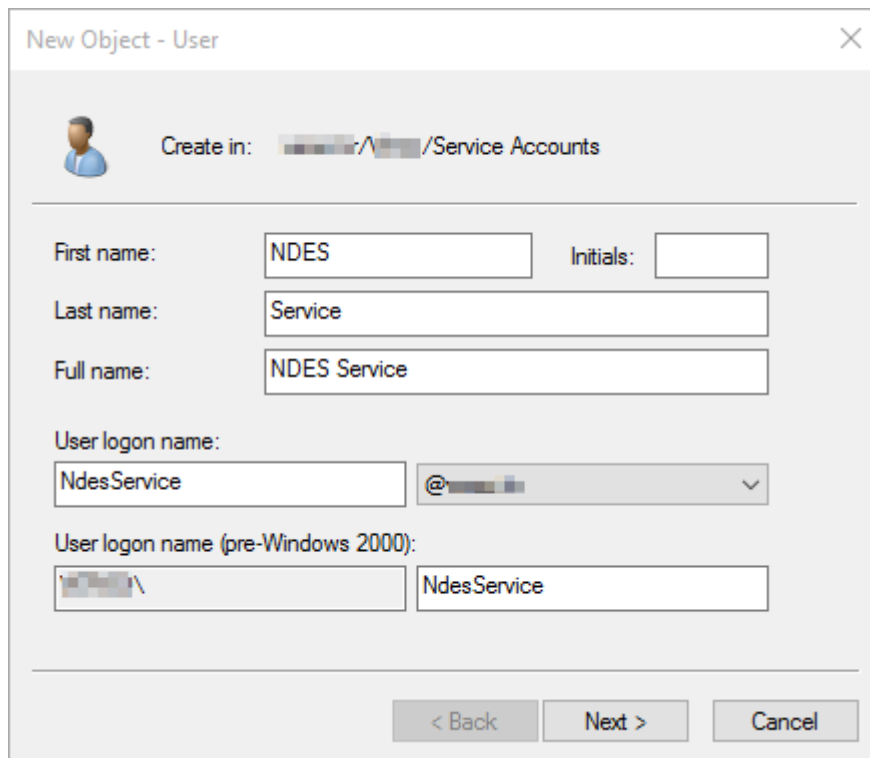
To request and enroll for a certificate by using the Network Device Enrollment Service

- 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:
 - 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:



New Object - User

Create in: /Service Accounts

First name: NDES Initials:

Last name: Service

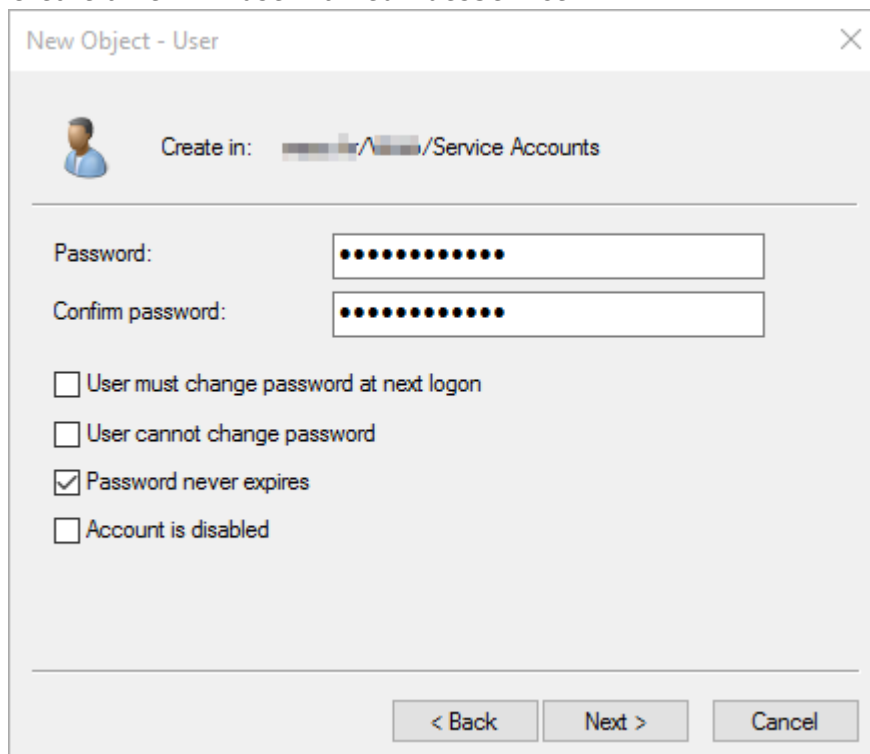
Full name: NDES Service

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 at next logon

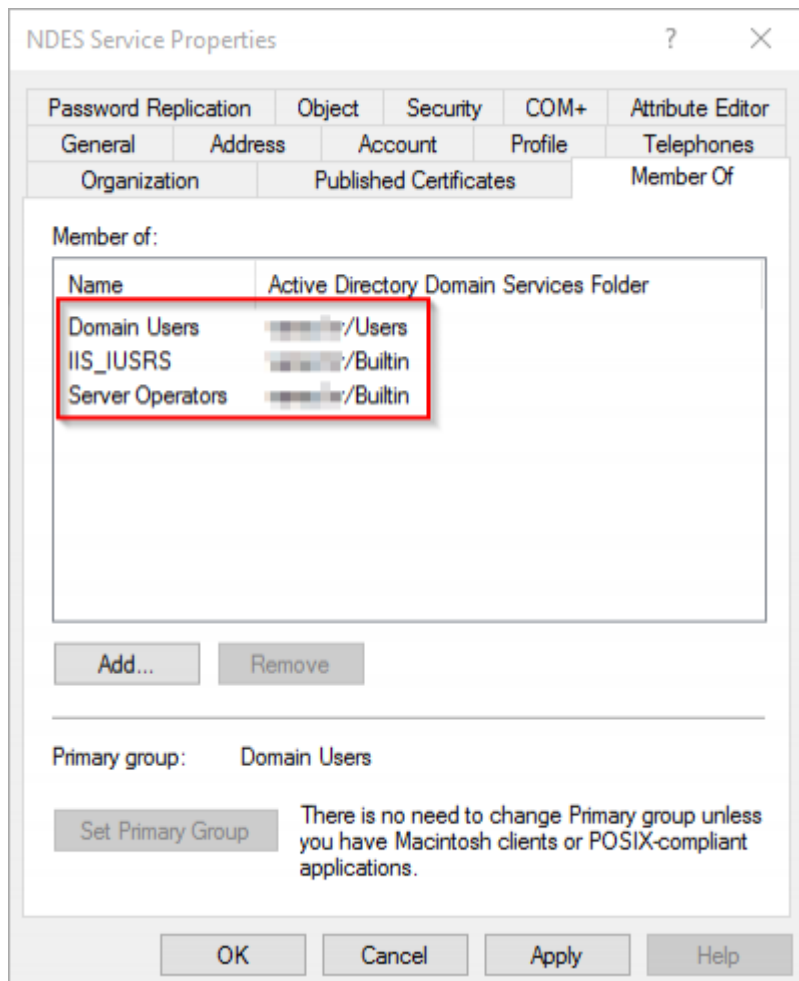
☐ User cannot change password

☒ Password never expires

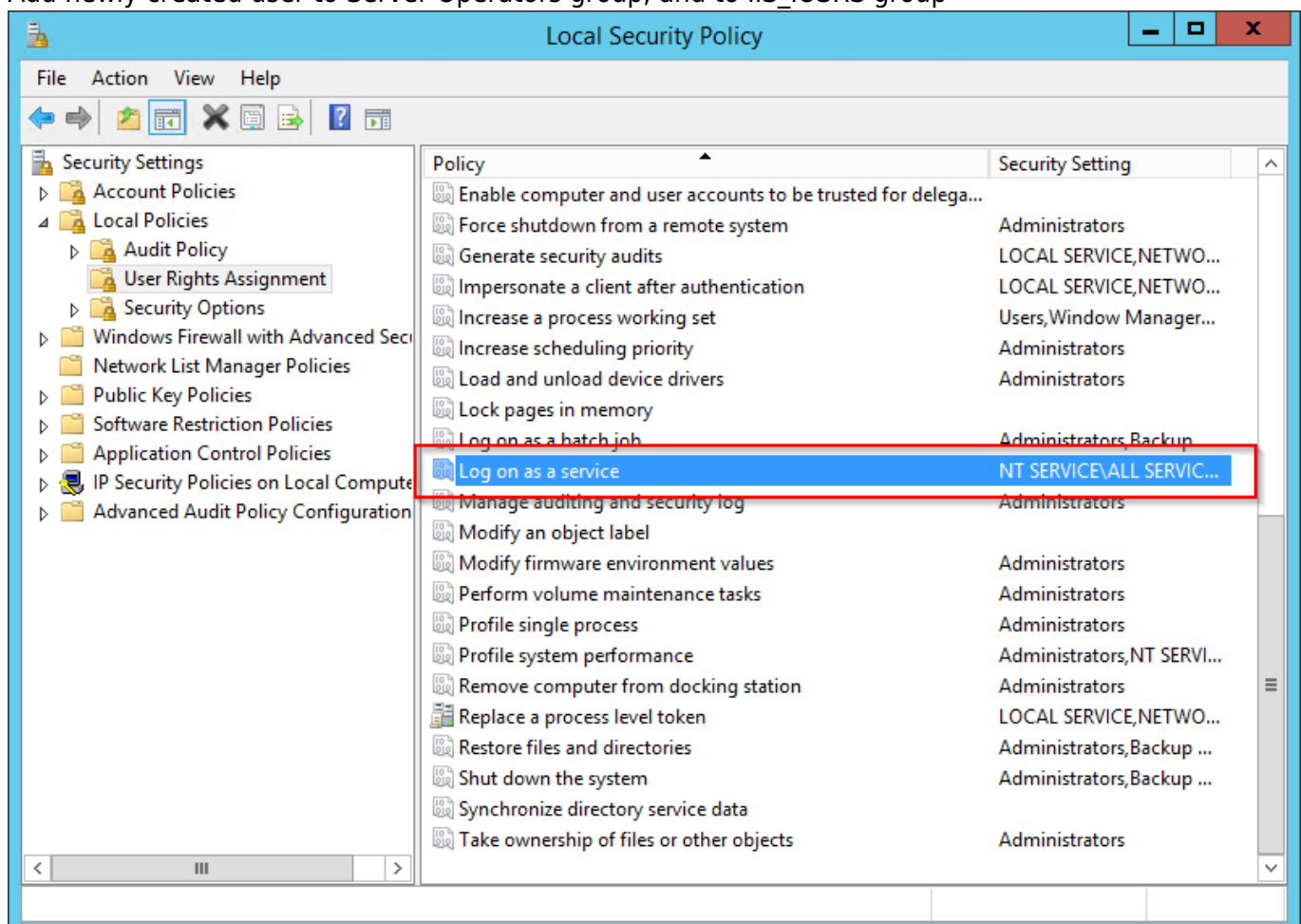
☐ Account is disabled

< Back Next > Cancel

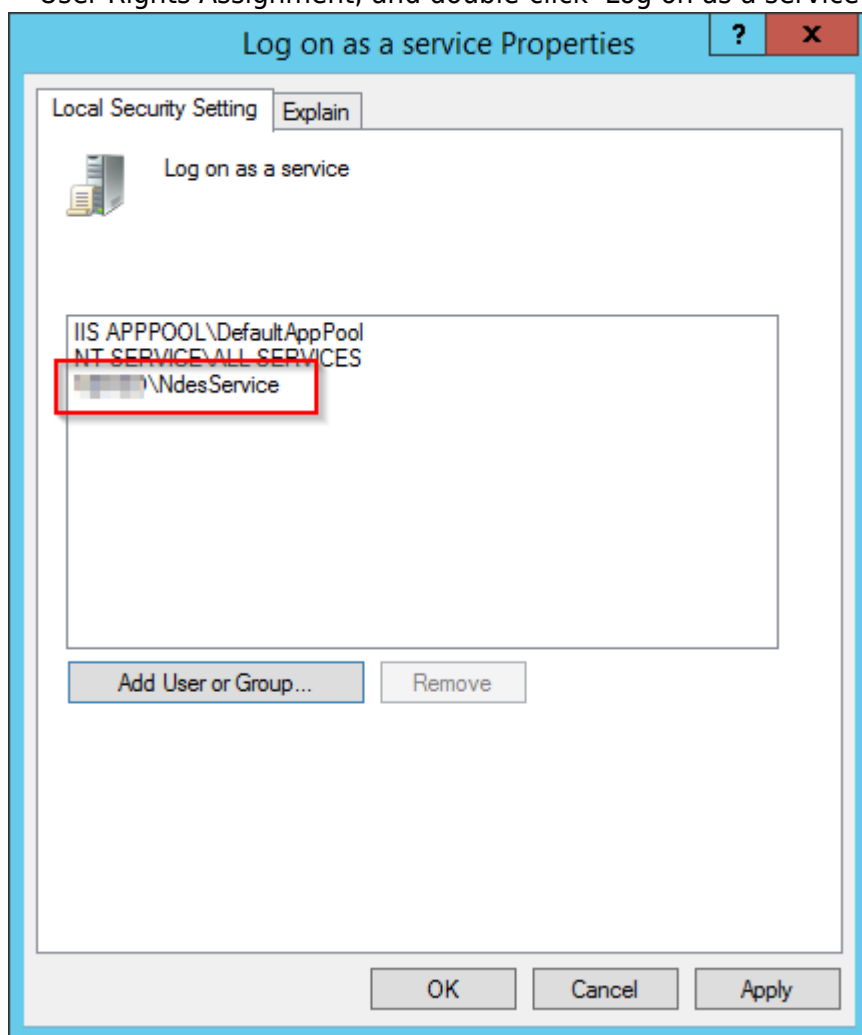
Set a strong password for the user and tick 'Password never expires'



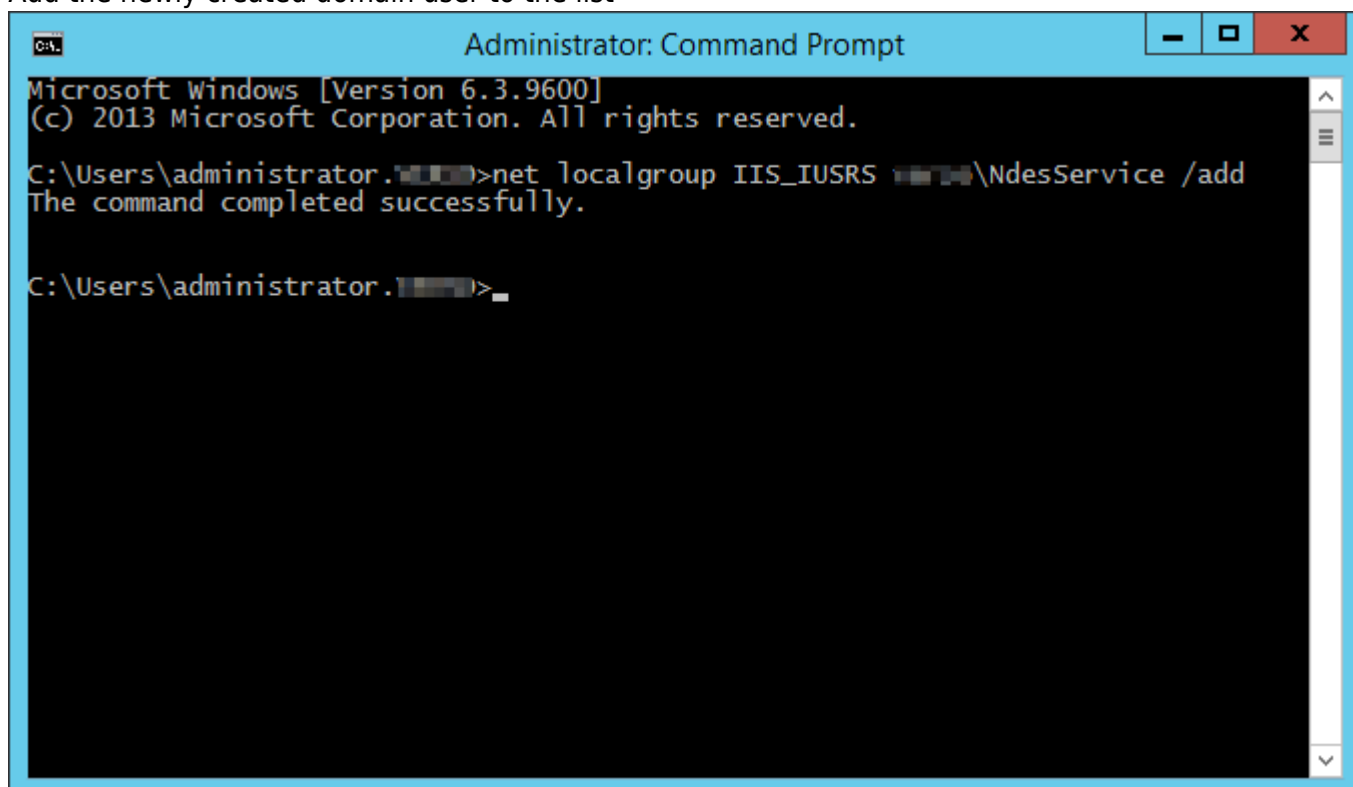
Add newly created user to Server Operators group, and to IIS_IUSRS group



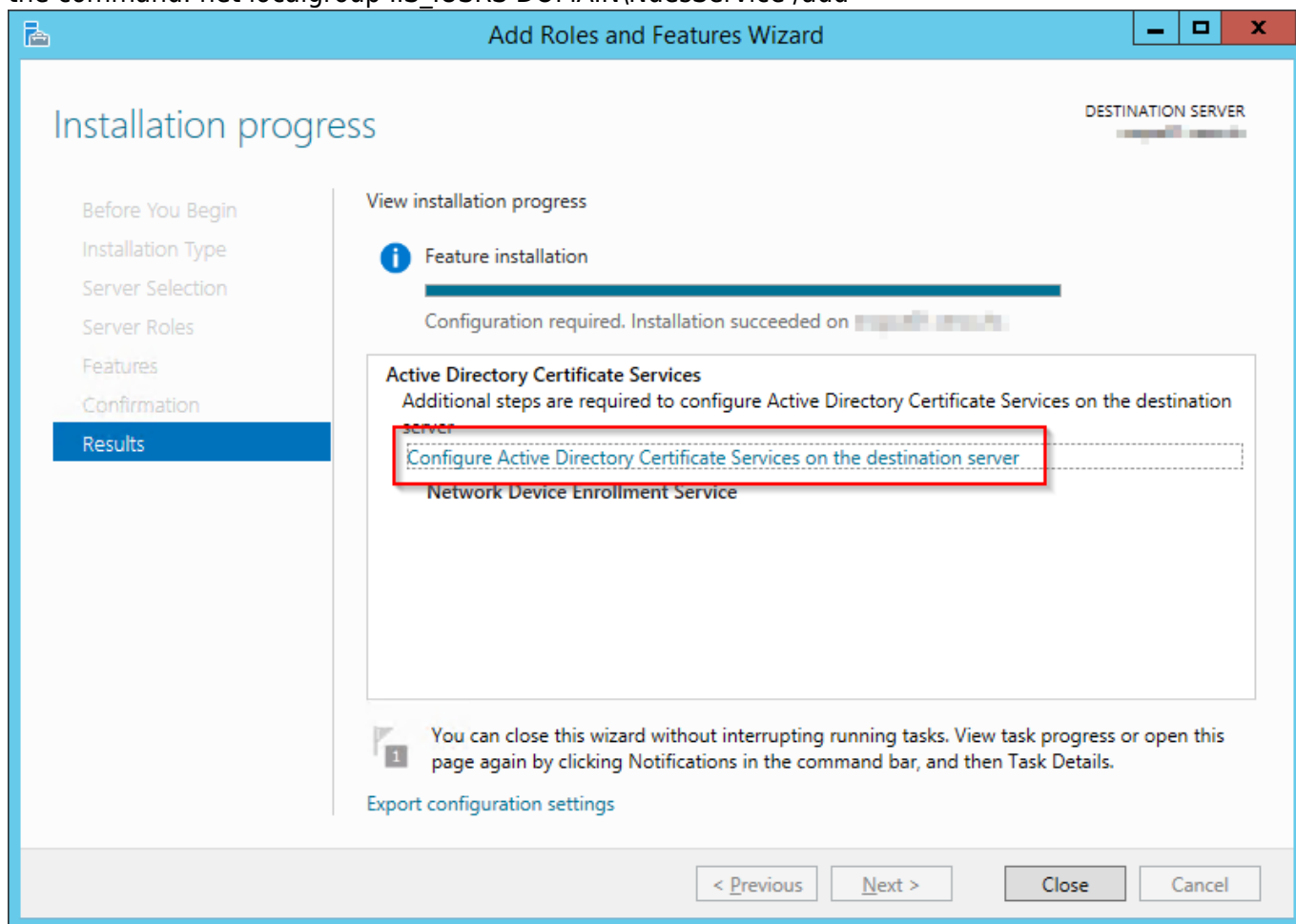
Open 'Local Security policy' on the server where you installed the NDES and navigate to Local Policies ⇒ User Rights Assignment, and double-click 'Log on as a service'



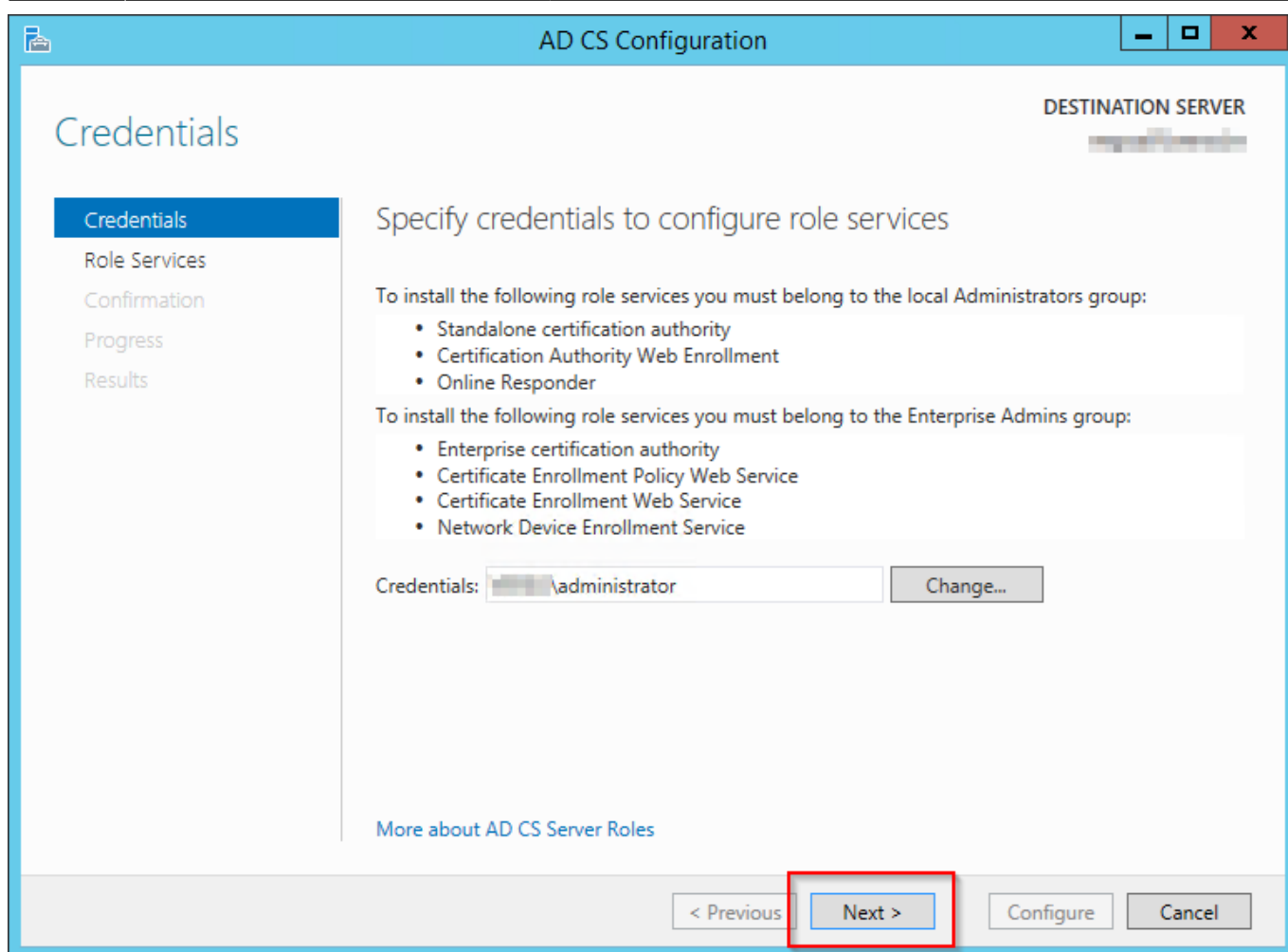
Add the newly created domain user to the list



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`



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



The screenshot shows the 'AD CS Configuration' window with the 'Credentials' step selected in the left-hand navigation pane. The main area is titled 'Specify credentials to configure role services'. It lists two groups of services that require specific permissions: 'local Administrators group' (Standalone certification authority, Certification Authority Web Enrollment, Online Responder) and 'Enterprise Admins group' (Enterprise certification authority, Certificate Enrollment Policy Web Service, Certificate Enrollment Web Service, Network Device Enrollment Service). Below this, a 'Credentials' field shows '\administrator' and a 'Change...' button. At the bottom, the 'Next >' button is highlighted with a red rectangle, indicating the next step in the wizard. Other buttons include '< Previous', 'Configure', and 'Cancel'.

AD CS Configuration

Credentials

DESTINATION SERVER

Specify credentials to configure role services

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

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

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

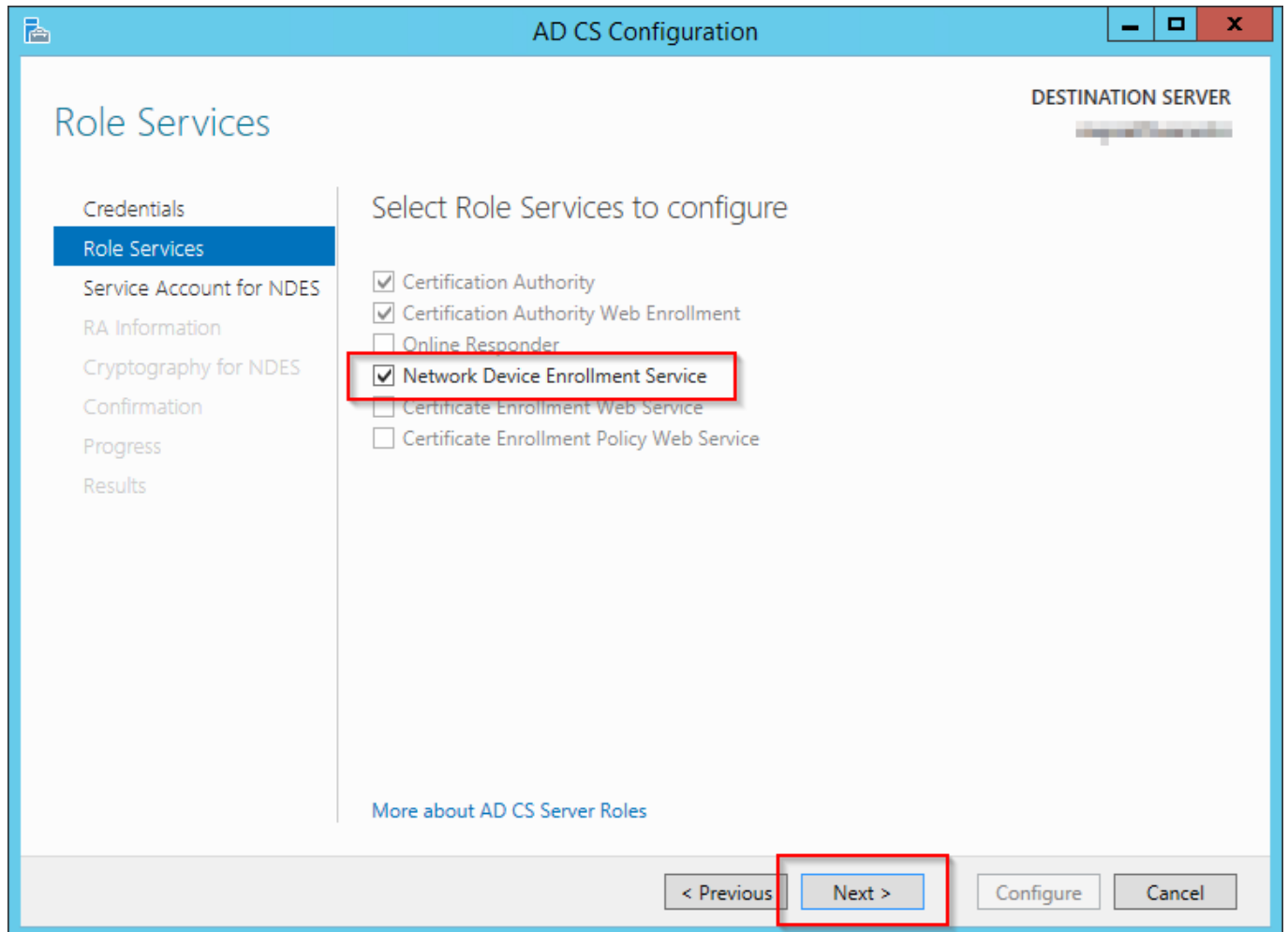
- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: \administrator Change...

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'

The screenshot shows the 'AD CS Configuration' window with the 'Service Account for NDES' step selected in the left-hand navigation pane. The main area is titled 'Specify the service account' and contains the instruction: 'Select the identity the Network Device Enrollment Service (NDES) will use.' There are two radio button options. The first option, 'Specify service account (recommended)', is selected and highlighted with a red rectangle. Below this option is a text box and a 'Select...' button. The second option is 'Use the built-in application pool identity'. At the bottom of the window are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER

Service Account for NDES

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 local IIS_IUSRS group.

☐ Use the built-in application pool identity

[More about Service Account for NDES](#)

< Previous Next > Configure Cancel


Click 'Select...'

The screenshot shows a 'Windows Security' dialog box titled 'AD CS Configuration'. It contains the instruction: 'Type the name and password of an account with user rights on the selected servers. For example, user@example.contoso.com, or domain\user name.' Below this is a light blue box with a user icon, a text field containing 'NdesService', a password field with masked characters, and a 'Domain:' label followed by a masked text field. Below the blue box is a smart card icon and the text 'Connect a smart card'. At the bottom are 'OK' and 'Cancel' buttons.


Windows Security

AD CS Configuration

Type the name and password of an account with user rights on the selected servers.
For example, user@example.contoso.com, or domain\user name.

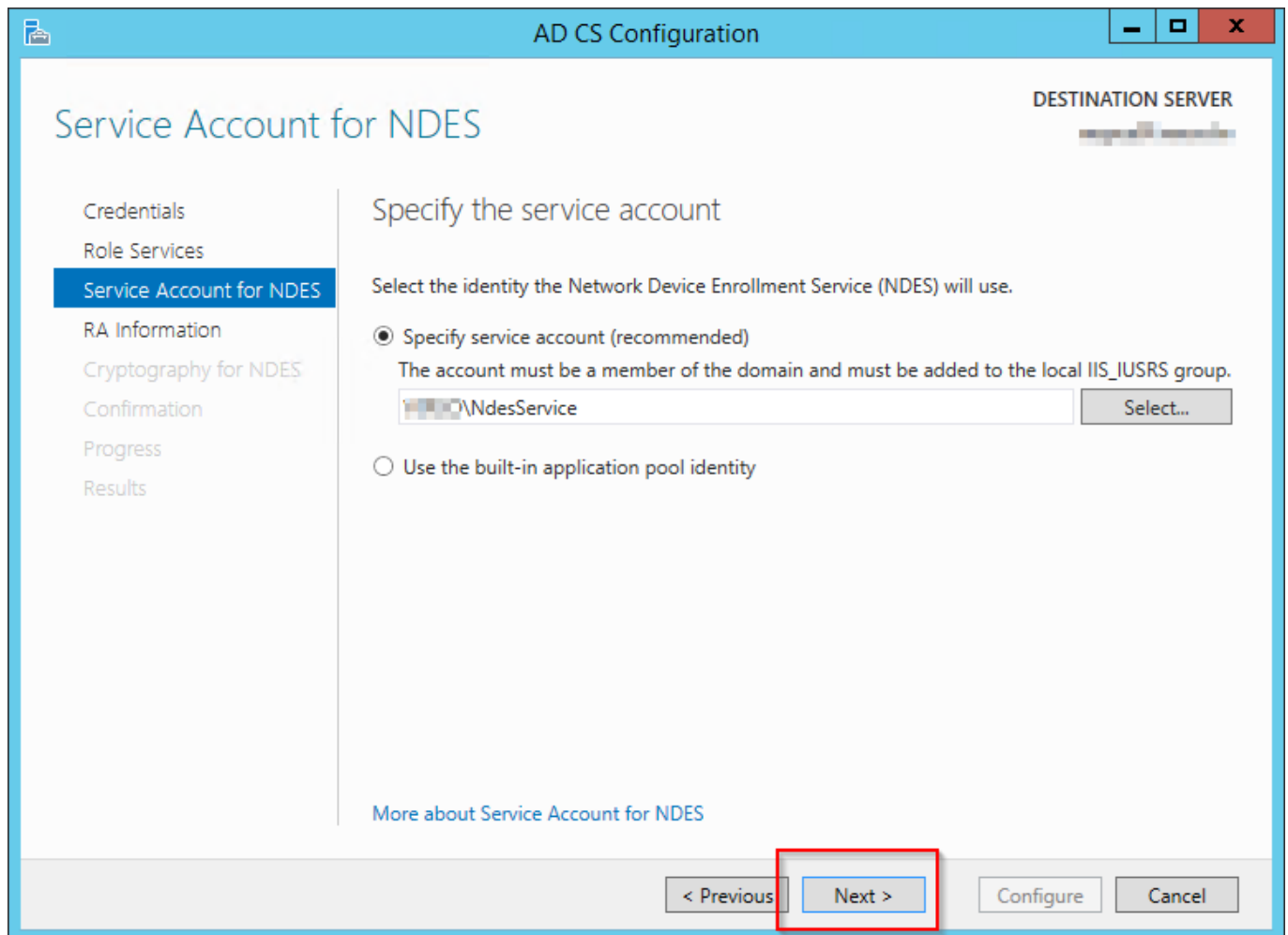


Domain:

 Connect a smart card

OK Cancel

Enter the credentials of the newly created domain user and click 'OK'



The screenshot shows the 'AD CS Configuration' console window. The title bar reads 'AD CS Configuration'. The main heading is 'Service Account for NDES'. On the left, a navigation pane lists: 'Credentials', 'Role Services', 'Service Account for NDES' (highlighted), 'RA Information', 'Cryptography for NDES', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Specify the service account' and contains the text: 'Select the identity the Network Device Enrollment Service (NDES) will use.' Below this are two radio buttons: 'Specify service account (recommended)' (selected) and 'Use the built-in application pool identity'. Under the selected option, it says 'The account must be a member of the domain and must be added to the local IIS_IUSRS group.' A text box contains 'NdesService' and a 'Select...' button is to its right. At the bottom right, the 'Next >' button is highlighted with a red rectangle. Other buttons at the bottom include '< Previous', 'Configure', and 'Cancel'. A link 'More about Service Account for NDES' is at the bottom left of the main area.

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

The screenshot shows the 'AD CS Configuration' window with the 'RA Information' step selected in the left-hand navigation pane. The main area is titled 'RA Information' and contains a description of the Registration Authority (RA) and its role in managing the Network Device Enrollment Service (NDES). Below the description, there are two sections: 'Required information' and 'Optional information'. The 'Required information' section includes fields for 'RA Name' (MSPCA01-MSCEP-RA) and 'Country/Region' (HR (Croatia)). The 'Optional information' section includes fields for 'E-mail' (dc@...hr), 'Company' (... d.o.o.), 'Department' (IT), 'City' (Zagreb), and 'State/Province' (Croatia). At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle.

AD CS Configuration

DESTINATION SERVER

RA Information

Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results

Type the requested information to enroll for an RA certificate

A registration authority (RA) is required to manage the Network Device Enrollment Service (NDES) certificate requests.

Required information

RA Name: MSPCA01-MSCEP-RA

Country/Region: HR (Croatia)

Optional information

E-mail: dc@...hr

Company: ... d.o.o.

Department: IT

City: Zagreb

State/Province: Croatia

[More about RA Information](#)

< Previous Next > Configure Cancel

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

AD CS Configuration

DESTINATION SERVER

Cryptography for NDES

- Credentials
- Role Services
- Service Account for NDES
- RA Information
- Cryptography for NDES**
- Confirmation
- Progress
- Results

Configure CSPs for the RA

Select the registration authority (RA) cryptographic service providers (CSPs) and key lengths for the signature and encryption keys.

Signature key provider: Key length:

Encryption key provider: Key length:

[More about Cryptography for NDES](#)

< Previous **Next >** Configure Cancel

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

The screenshot shows the 'AD CS Configuration' window with the 'Confirmation' step selected in the left-hand navigation pane. The main area displays the configuration details for the 'Network Device Enrollment Service'. The 'Configure' button at the bottom right is highlighted with a red rectangle.

AD CS Configuration

Confirmation

DESTINATION SERVER

Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results

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

Active Directory Certificate Services

Network Device Enrollment Service

Account: \NdesService

RA Information:

Name: MSPCA01-MSCEP-RA

Country/Region: HR

Email: dc@.hr

Company:

Department: IT

City: Zagreb

State/Province: Croatia

Signature Key Provider: Microsoft Strong Cryptographic Provider

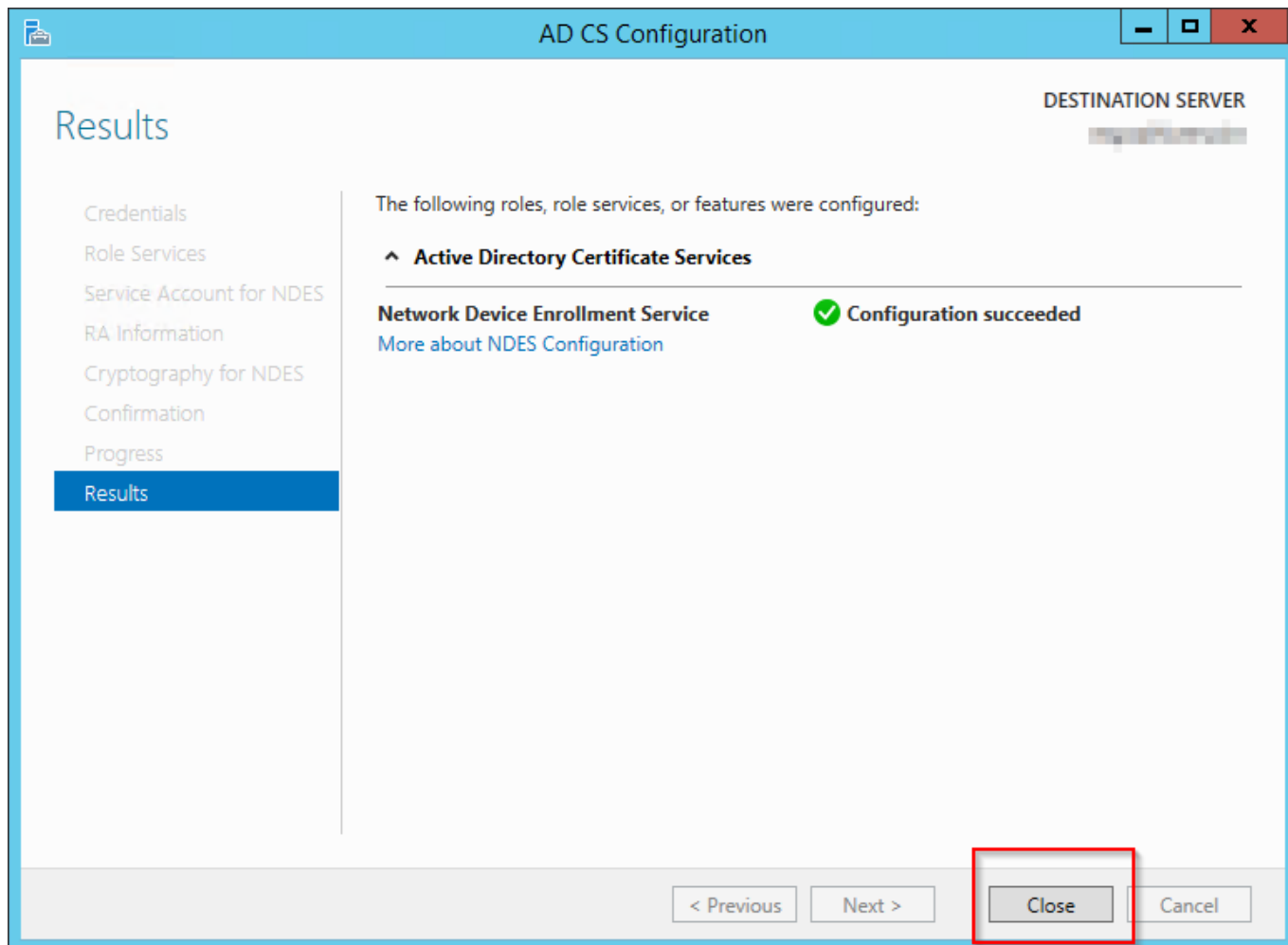
Signature Key Length: 2048

Exchange Key Provider: Microsoft Strong Cryptographic Provider

Exchange Key Length: 2048

< Previous Next > **Configure** Cancel

Confirm that all data is correct and click 'Configure'



Close the wizzard and you're done!

From:
<https://wiki.plecko.hr/> - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=windows:servers:net_data_enrollment_service

Last update: **2019/10/31 09:06**

