Microsoft NDES

NDES

Windows Server 2019

Integration Guide

CryptoServer HSM

SecurityServer 4.45.5

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-03-27
Status	PUBLISHED
Document No.	IG-2026-0017

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All Utimaco SecurityServer product documentation is available from Utimaco's web site at https://utimaco.com/.

1.1 About This Guide

This guide describes how to enable HSM integration with Microsoft NDES. Utimaco HSM secures the signing private keys used by Microsoft NDES.

1.1.1 Target Audience for This Guide

This guide is intended for Microsoft NDES and HSM administrators.

1.1.2 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the OK button.
Monospaced	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file example.conf in the /exmp/demo/ directory.
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *CryptoServer - csadm Manual* or [CSADMIN].

Table 1: Document conventions

Special icons are used to highlight the most important notes and information.

Here you find important safety information that should be followed.

Here you find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
AD CS	Active Directory Certificate Services
CA	Certificate Authority
CNG	Cryptography API Next Generation
CSADM	CryptoServer Command-line Administration Tool
CSP	Cryptographic Service Provider
CXI	Cryptographic eXtended Services Interface
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface

Abbreviation	Meaning
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
IIS	Internet Information Service
IP	Internet Protocol
LAN	Local Area Network
MBK	Master Backup Key
NDES	Network Device Enrollment Service
PCIe	PCI Express Interface
PIN	Personal Identification number
RA	Registration Authority
SCEP	Simple Certificate Enrollment Protocol
SSL	Secure Sockets Layer
VPN	Virtual Private Network
URL	Uniform Resource Locator

Table 2: List of Abbreviations

2 Overview

2.1 Microsoft Network Device Enrollment Service

The Network Device Enrollment Service (NDES) is one of the role services of the Active Directory Certificate Services (ADCS) role in Windows server. It implements the Simple Certificate Enrollment Protocol (SCEP). SCEP was originally designed to semi-automatically enroll certificates to Cisco network devices in a closed network where all endpoints are trusted, like routers or VPN concentrators.

SCEP does not include any mechanisms of verifying the certificate requestor's identity, instead it relies on a Registration Authority (RA) to handle this sensitive task.

The Network Device Enrollment Service performs the following functions:

a) Generates and provides one-time enrollment passwords to administrators.

b) Submits enrollment requests to the CA.

c) Retrieves enrolled certificates from the CA and forwards them to the network device.

Refer to the Microsoft documentation, for more information about Microsoft NDES.

2.2 Utimaco CryptoServer HSM

CryptoServer is a hardware security module developed by Utimaco IS GmbH. CryptoServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using, meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured required software.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with Microsoft NDES.

Operating System	Utimaco Security Server Version	Utimaco HSM
Windows Server 2019	SecurityServer 4.45.5	CryptoServer CSe-Series/Se-Series

Table 3: List of Tested Versions

3.2 Software Requirements

Software	Software Requirements
HSM Interfaces	CryptoServer CSP/CNG Provider

Table 4: List of Software Requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.45.5 or higher

Hardware	Hardware Requirements
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.45.5 or higher

Table 5: List of Hardware Requirements

3.4 Prerequisites

Before you begin, please ensure that you have installed/set up:

- CryptoServer. Refer to the CryptoServer documentations to setup the HSM.
- The operating system listed in Tested Versions.
- The SecurityServer version listed in Tested Versions.
- CryptoServer Default Admin – this should be replaced with a new admin user.
- The MBK – must be created and stored onto each HSM. Refer to the CryptoServer documentation to set up the MBK.
- If you are using Smartcard Authentication – install PIN PAD Driver through the SecurityServer software file, configure PIN PAD, and start PIN Pad Daemon. Refer to the CryptoServer documentation for more information about PIN PAD driver installation and configuration.
- Following machines to demonstrate the NDES Integration:
    - A Domain Controller.
    - CA Server with joined to domain and ADCS Installed.
    - A server joined to the domain. This will be used for installing NDES and configuring it as part of the integration process in next chapter.
    - A Client machine without joined to domain.

Ensure that your domain controller and ADCS server is up and running before proceeding ahead. The steps for creating a domain controller and setting up ADCS is out of scope of this document. You can refer to ADCS with OCSP Integration Guide with Utimaco HSM for steps to install and configure ADCS for setting up a Certificate Authority.

4 Configuring the CSP-CNG Provider

4.1 Introduction and Prerequisites

A CSP (Cryptographic Service Provider) is a general-purpose cryptography standard, developed by Microsoft. On one side it defines a cryptographic interface to be used by applications (CryptoAPI). On the other side it defines an interface to be used by manufacturers to integrate their cryptographic hardware.

A CNG (Cryptography API Next Generation) is the second-generation cryptographic interface, developed by Microsoft. It offers updated cryptographic algorithms and is intended for a longterm replacement of CSP.

When installing the CryptoServer Setup make sure to select the CPS/CNG - Cryptographic Service Provider (Microsoft) interface. A Cryptographic User should be created as well as an MBK should be generated.

Generating the MBK is necessary for the HSM to become operational. Without the MBK one cannot run any cryptographic operations.

4.2 Creating HSM Users

Start the CryptoServer Administration Tool and login a user with the permission level of at least 02000000.

4.2.1 Creating a Key Manager User

If the Key manager and Crypto user roles are separated, a Key Manager user might need to be created.

More users with the permission level 00000010 might be needed (Group 1) to enforce "m of n" security policy for the key management and smart card authentication might need to be used.

For this guide only one Key Manager User will be created.

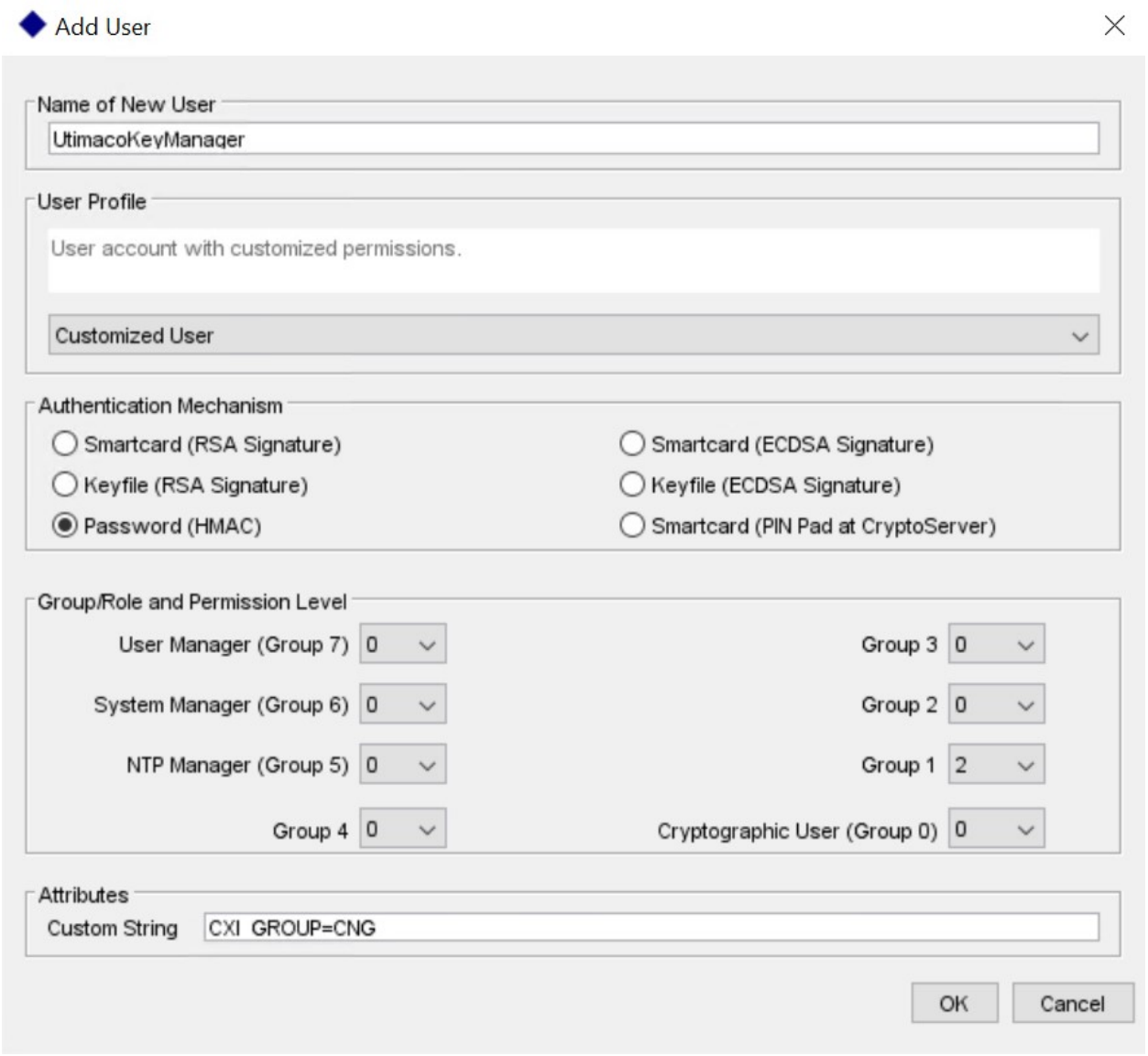

Figure 1 : Creating Key Manager User

4.2.2 Creating a Crypto User

Crypto Users with permission level of 00000002 will have to be created. Use encrypted passwords. For this guide, a user with permission level of 00000002, CXI Group "CNG" and HMAC password will be created.

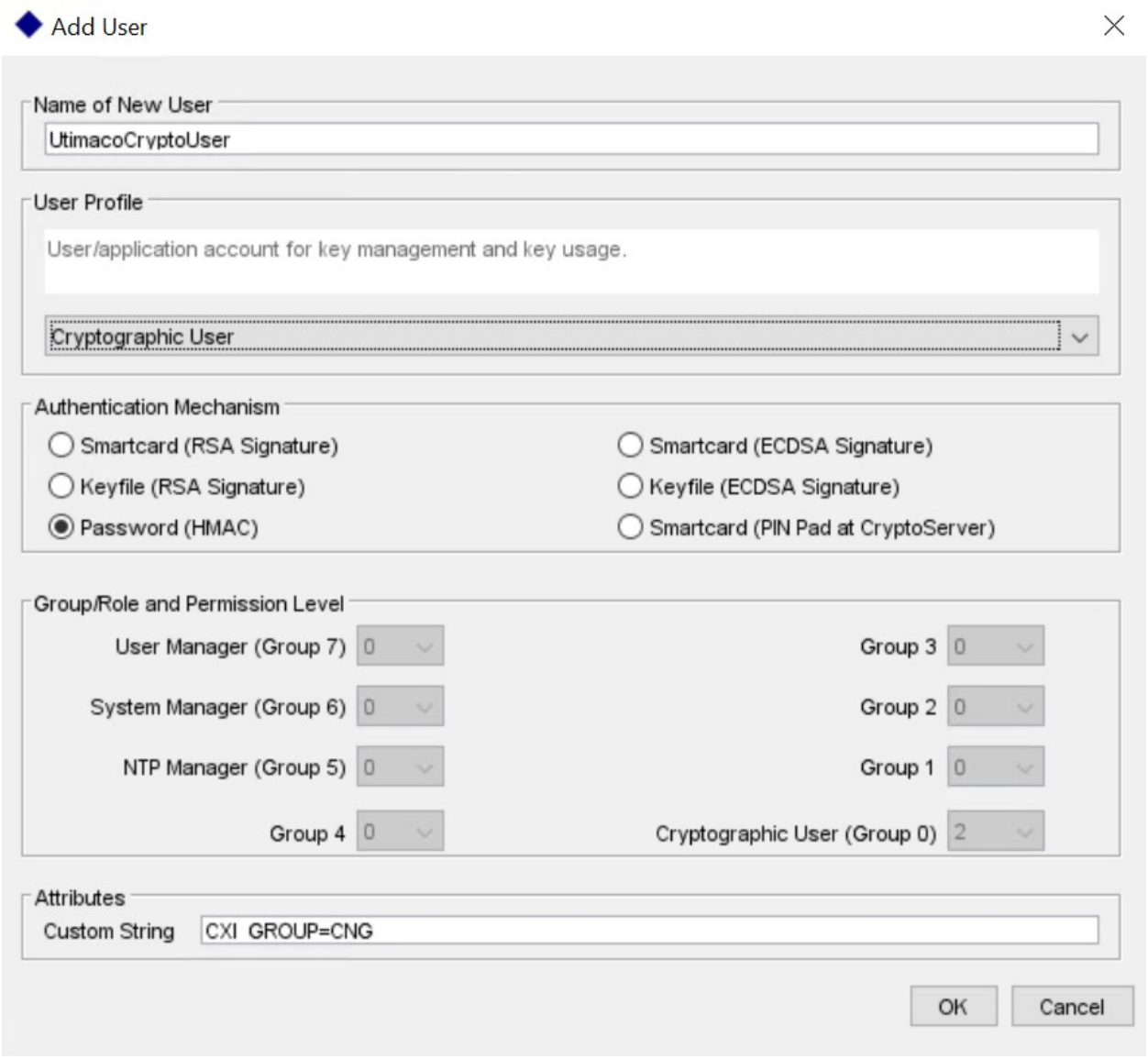

Figure 2 : Creating a Crypto User

Based on your requirement, the user can use Password (HMAC), Smart Card or KeyFile protection type. If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

4.3 Setting Up the CSP/CNG Provider

The `CS_CNG_CFG` environment variable contains the path and name of the configuration file.

By default, it is located at C:\ProgramData\Utimaco\CNG\cs_cng.cfg.

For more advanced configuration, refer to [CspCng];

1. Open the cs_cng.cfg file with an appropriate text editor.

›_ Console

```
> notepad %CS_CNG_CFG%
```

2. For this installation set the path to the log file and set the log level to "ERROR".

cs_cng.cfg

```
# Path to the logfile (name of logfile is attached by the API)
Logpath = C:\ProgramData\Utimaco\CNG\log
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1
```

To make your testing easier, it would be good to enable the CNG log file. That can be enabled by editing the Logging Loglevel. Set the LogPath and Logging Loglevel to 1. For testing you may want to increase it to 4.

The added LogPath points to a writable directory, not to a file.

If you encounter problems, check the log file named cs_cng.log in the LogPath defined directory. When you are done testing, you should change Logging to 1 or 2. This will limit the logging to only critical and important messages.

3. Set the Login. In this case, the name of the Cryptographic User is "UtimacoCryptoUser" with an HMAC password "Utimaco19".

cs_cng.cfg

```
Login = UtimacoCryptoUser,HMACPwd=Utimaco19
```

If using Smartcard or KeyFile protection make the appropriate change in the Login Section as shown below:

Login = username,RSASign=filename#password

Login = "SmartCardUser,RSASign=:cs2:auto:USB0@<HSM-IP>"

For additional information refer **CryptoServer_csadm_Manual_Systemadministrators.pdf** document, found on the product CD in the Documentation directory.

4. Set the IP address of the HSM.

cs_cng.cfg

```
# default device and fallback devices
Device = 10.44.223.141
```

For more information regarding the commands and command parameters please check the Utimaco documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

Device = 288@<HSM IP address> Hardware (LAN) HSM

OR

Device = /dev/cs2.0 Hardware (PCIe) HSM

4.3.1 Testing Connection

To enumerate providers, use the following command:

›_ Console

```
> cngtool EnumProvider
Microsoft Key Protection Provider
Microsoft Passport Key Storage Provider
Microsoft Platform Crypto Provider
Microsoft Primitive Provider
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Microsoft SSL Protocol Provider
Windows Client Key Protection Provider
Utimaco CryptoServer Key Storage Provider
```

To get the provider information, use the following command:

›_ Console

```
>cngtool ProviderInfo
Provider : Utimaco CryptoServer Key Storage Provider
Device : 10.44.223.141
Group : CNG
Mode : Internal Key Storage
------------------------------------------------------------
Name : Utimaco CryptoServer Key Storage Provider
Name : Utimaco CryptoServer Key Storage Provider
Version : 0x02010000
Impl. -Type : 0x00000011
MaxNameLength : 0x00000104  Device : 10.44.223.141
Group : CNG
Mode : Internal Key Storage
```

5 Adding Users and Assigning Permission for NDES

5.1 Creating User Accounts for NDES

1. Login to the Domain Controller with Domain Administrator account.
2. Open Active Directory Users and Computers from the Server Manager Tools menu.
3. For demonstration purpose create three user accounts NDESAdmin, NDESService, NDESDeviceAdmin.
4. Click <domain_name>.com to expand, then right-click on Users and select New > User.
5. Enter the name NDESAdmin and select Next.
6. Set a strong password.
7. Check Password Never expires option.

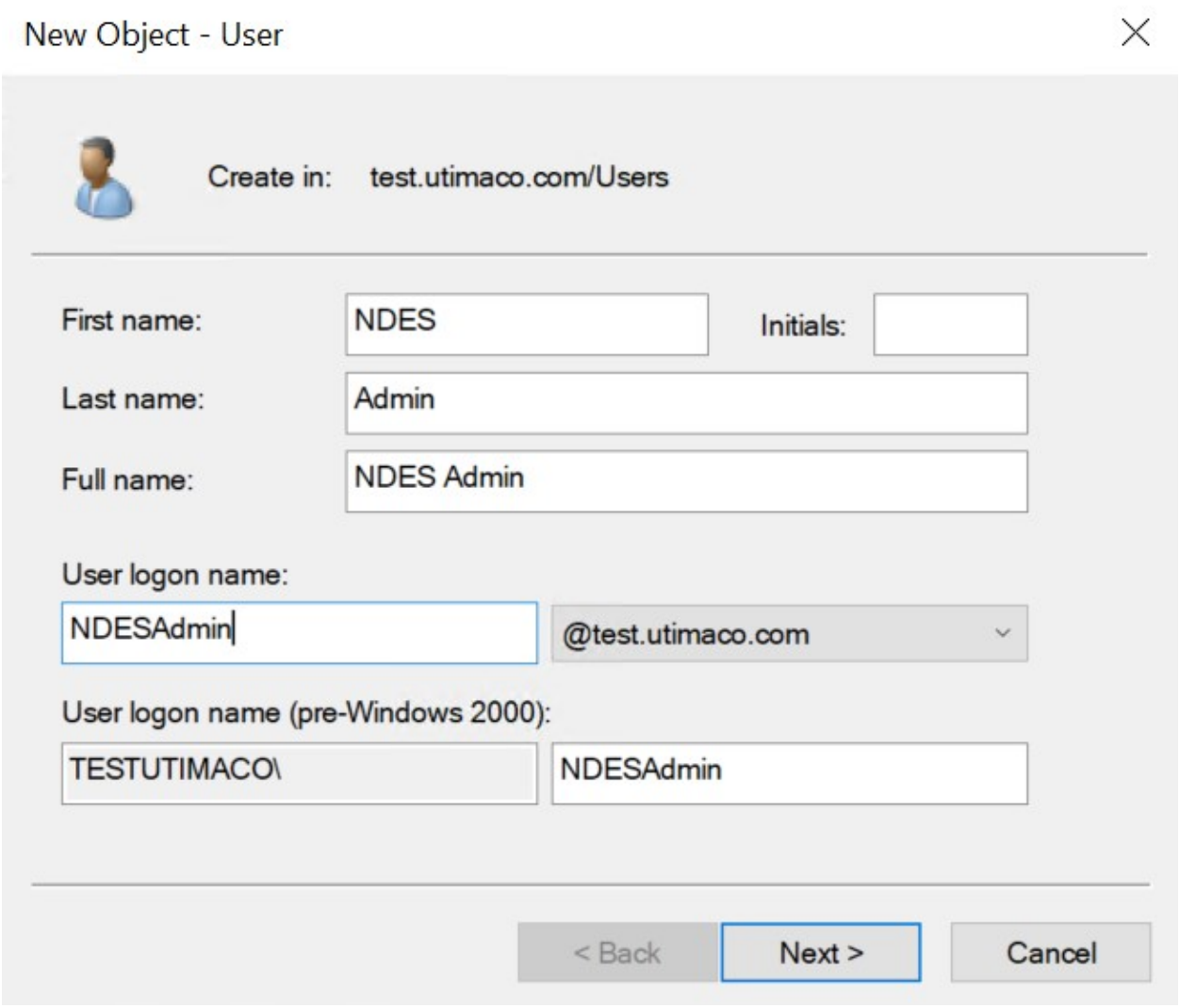

Figure 3 : New Object - User Window

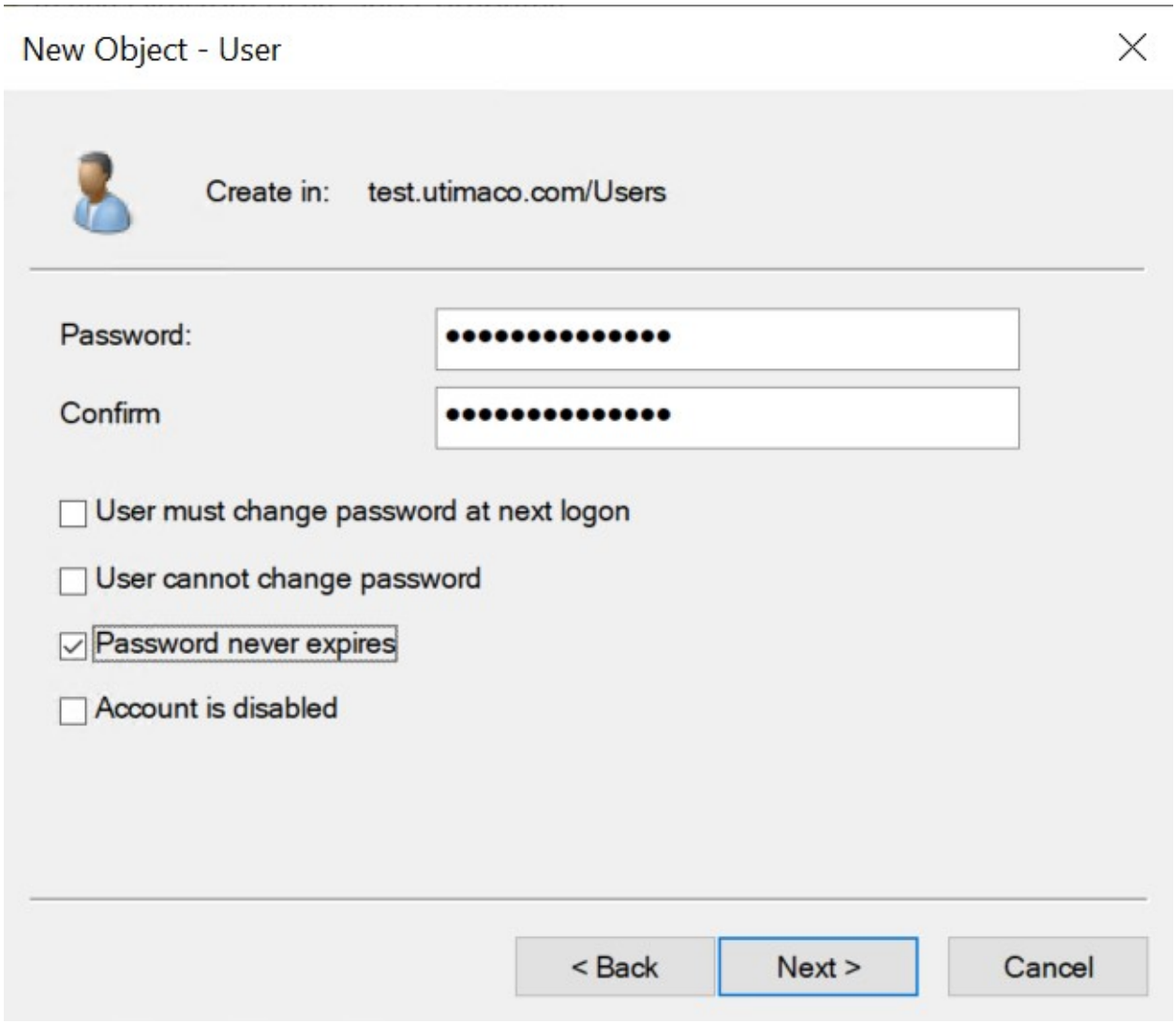

Figure 4 : New Object - User Window

8. By repeating the previous steps create new users for NDESService and NDESDeviceAdmin.

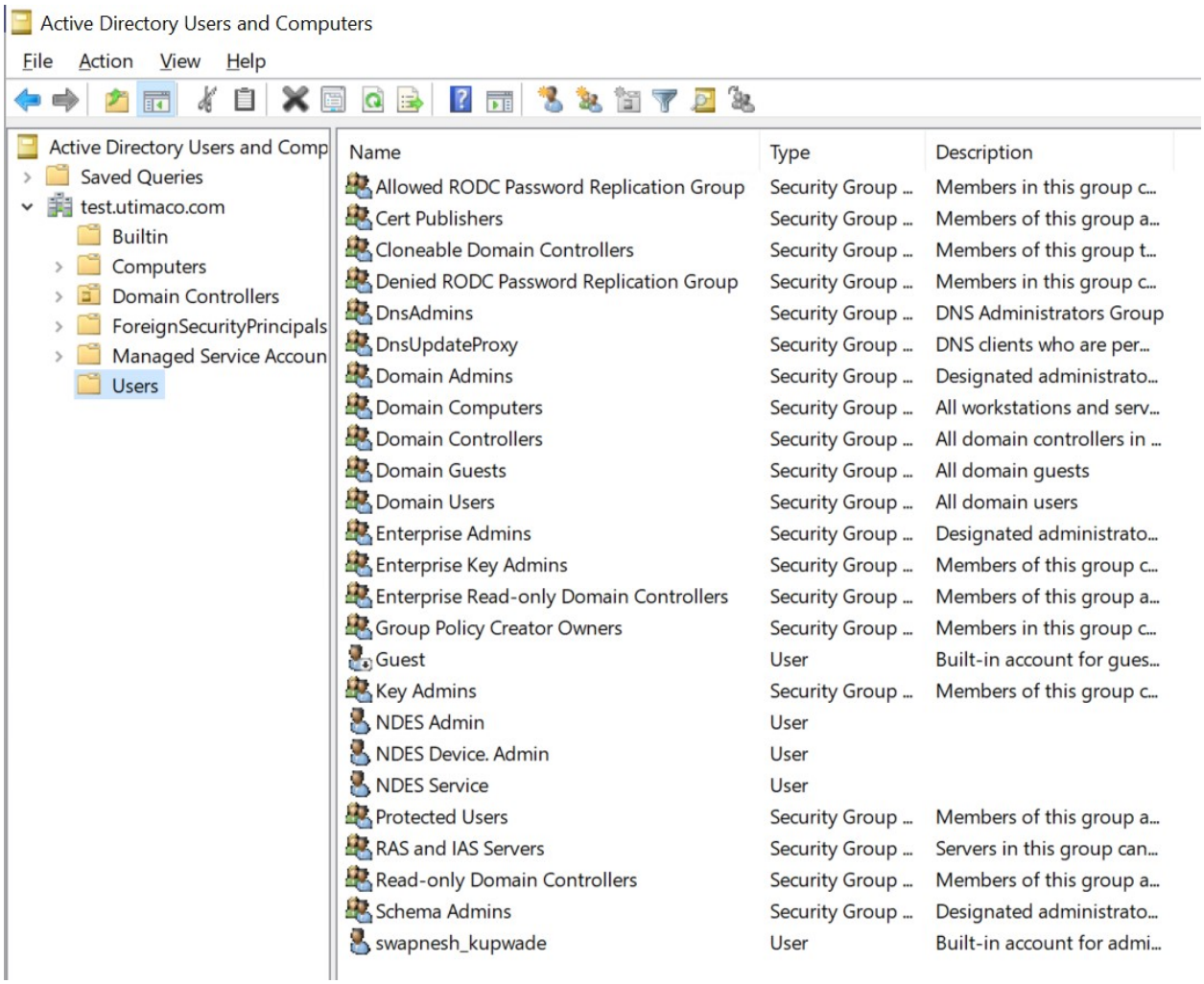

Figure 5 : Active Directory Users and Computers Window

5.2 Add NDESAdmin User to the Enterprise Admins and Domain Admins Groups

1. Right-click on Enterprise Admins on the right pane from Active Directory users and Computers, and select Properties.
2. Select the Members tab and then select Add.
3. Enter the NDESAdmin account, select Check Names, and if found then select OK.
4. Select Apply and OK.

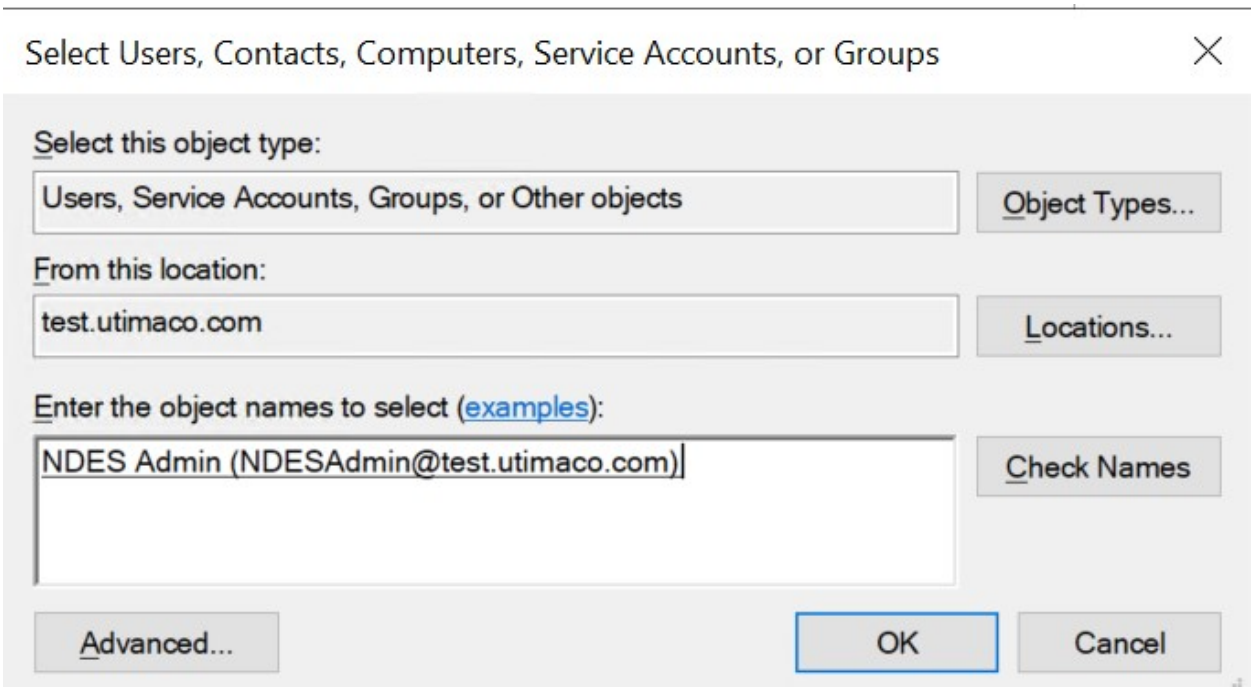

Figure 6 : Select Users, Contacts, Computers, Service Accounts, or Groups Window

5. Repeat the above steps for the Domain Admins group.

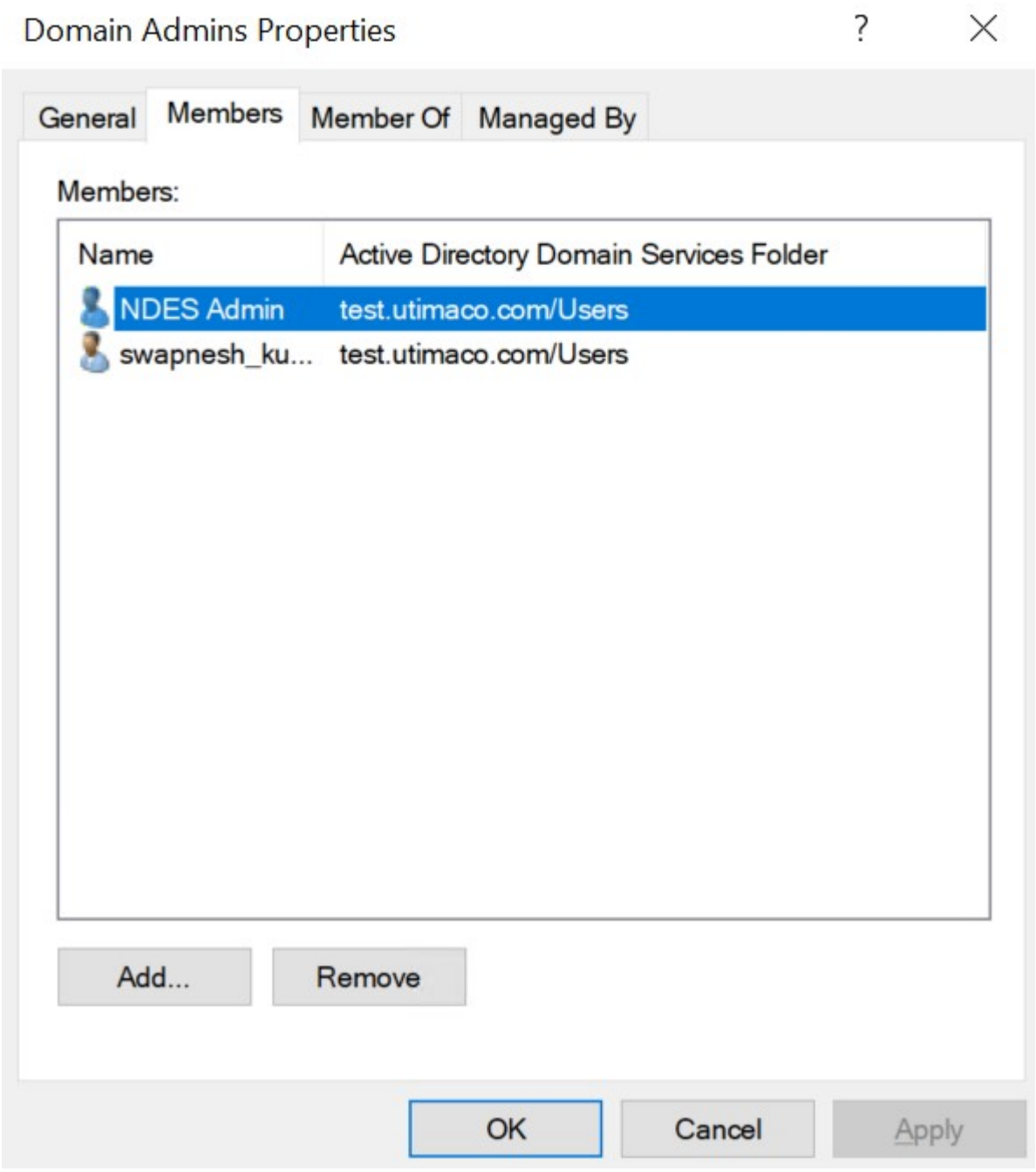

Figure 7 : Domain Admin Properties Window

5.3 Add the NDESAdmin and NDESService Account to the Local IIS_IUSERS Group

1. Login to the NDES server using the domain\Administrator.
2. Click start, Open Run and type compmgmt.msc to open Computer Management.

3. Expand Local User and Groups on the Computer Management console tree, under System Tools. Select Groups.
4. Double-click IIS_IUSRS.
5. Click on Add on the IIS_IUSRS Properties window.
6. Enter the NDESAdmin account, select Check Names, and if found then select OK.
7. Select Apply and OK.

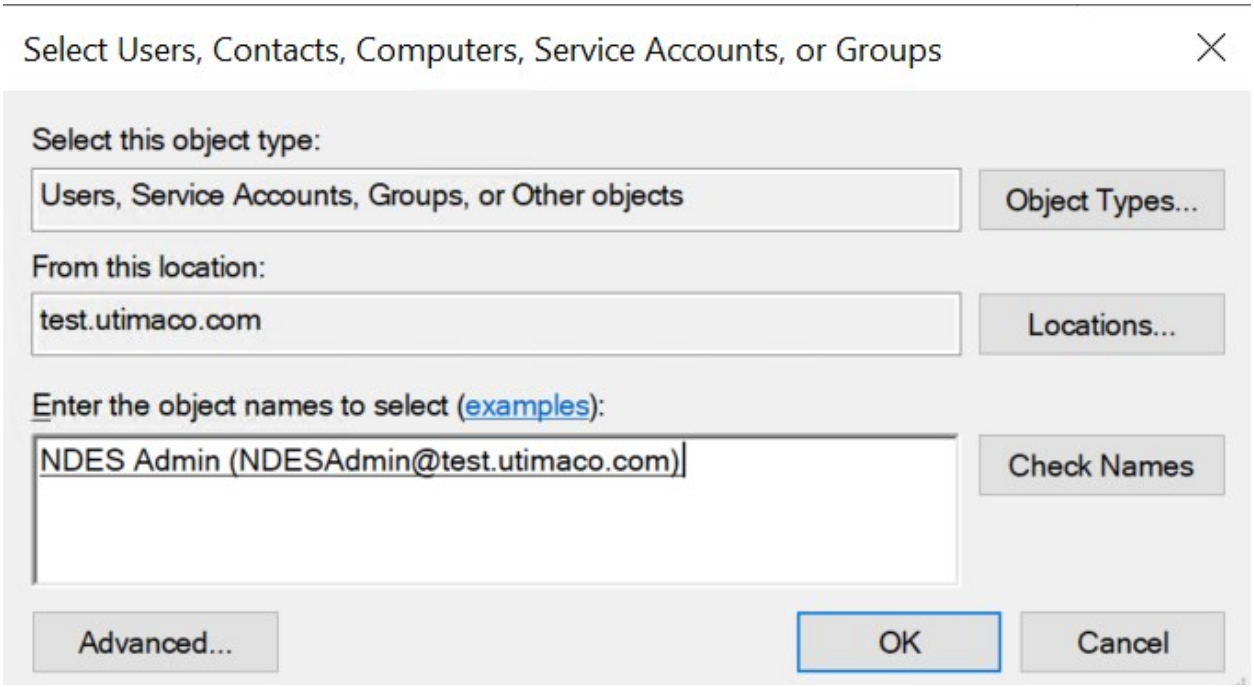

Figure 8 : Select Users, Contacts, Computers, Service Accounts, or Groups Window

8. Repeat above steps to add the NDESService account to IIS_IUSRS groups.

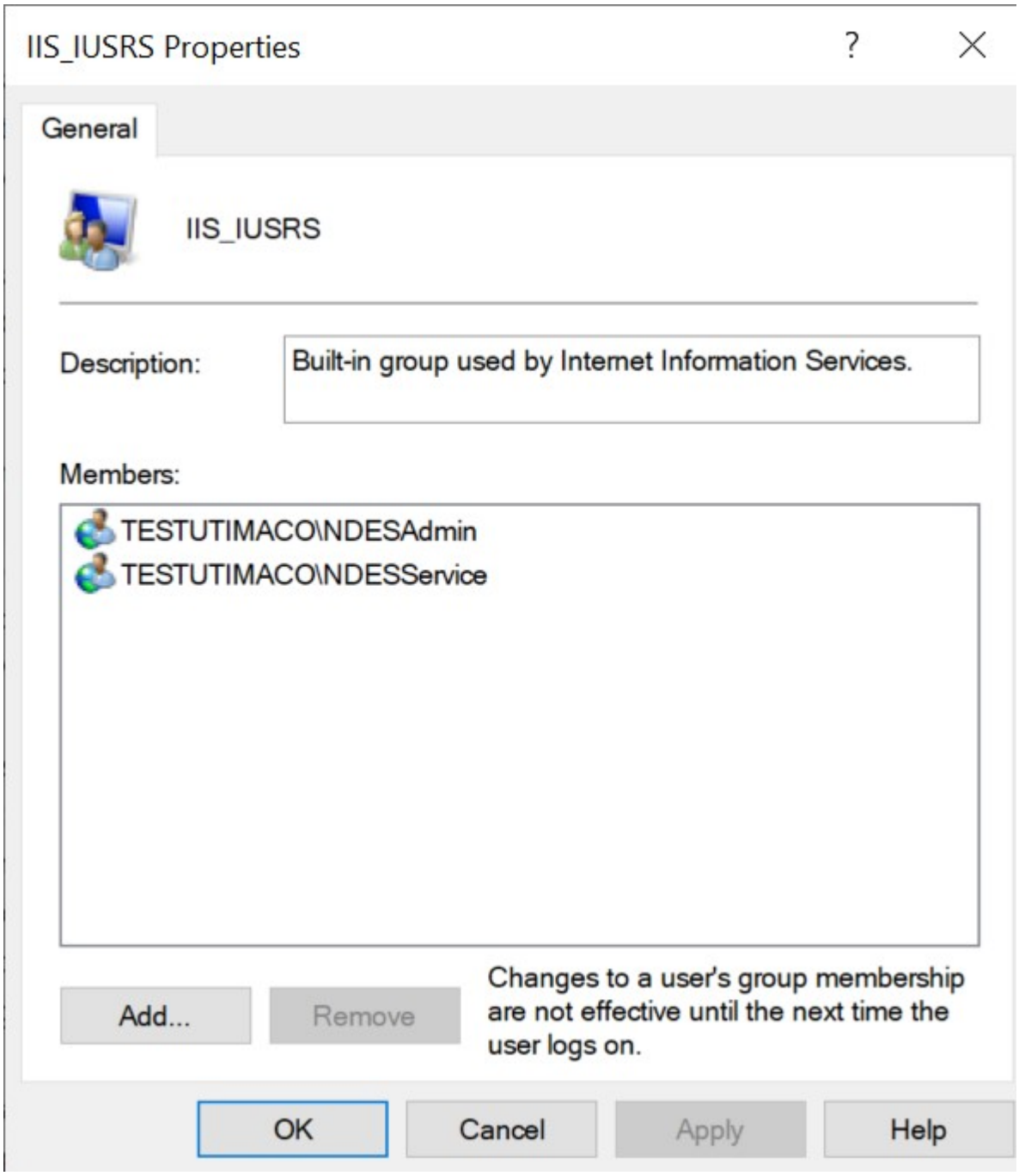

Figure 9 : IIS_IUSRS Properties Window

5.4 Providing Request Permission on the CA for NDESAdmin and NDESService Account

1. Log into the CA server using the domain account.
2. On the Server Manager window Select Certification Authority from the Tools menu.

3. Right-click the certification authority, and then select Properties.
4. Click on Security tab.
5. Click on Add button.
6. On the Select Users, Computers, Service Accounts, or Groups text box, type the name of the NDESAdmin account, select Check Names, and if found then select OK.
7. Select the NDESAdmin account and click on the Allow check box to Request Certificates. Select Apply and then select OK.
8. Repeat the above steps to add the NDESService account.

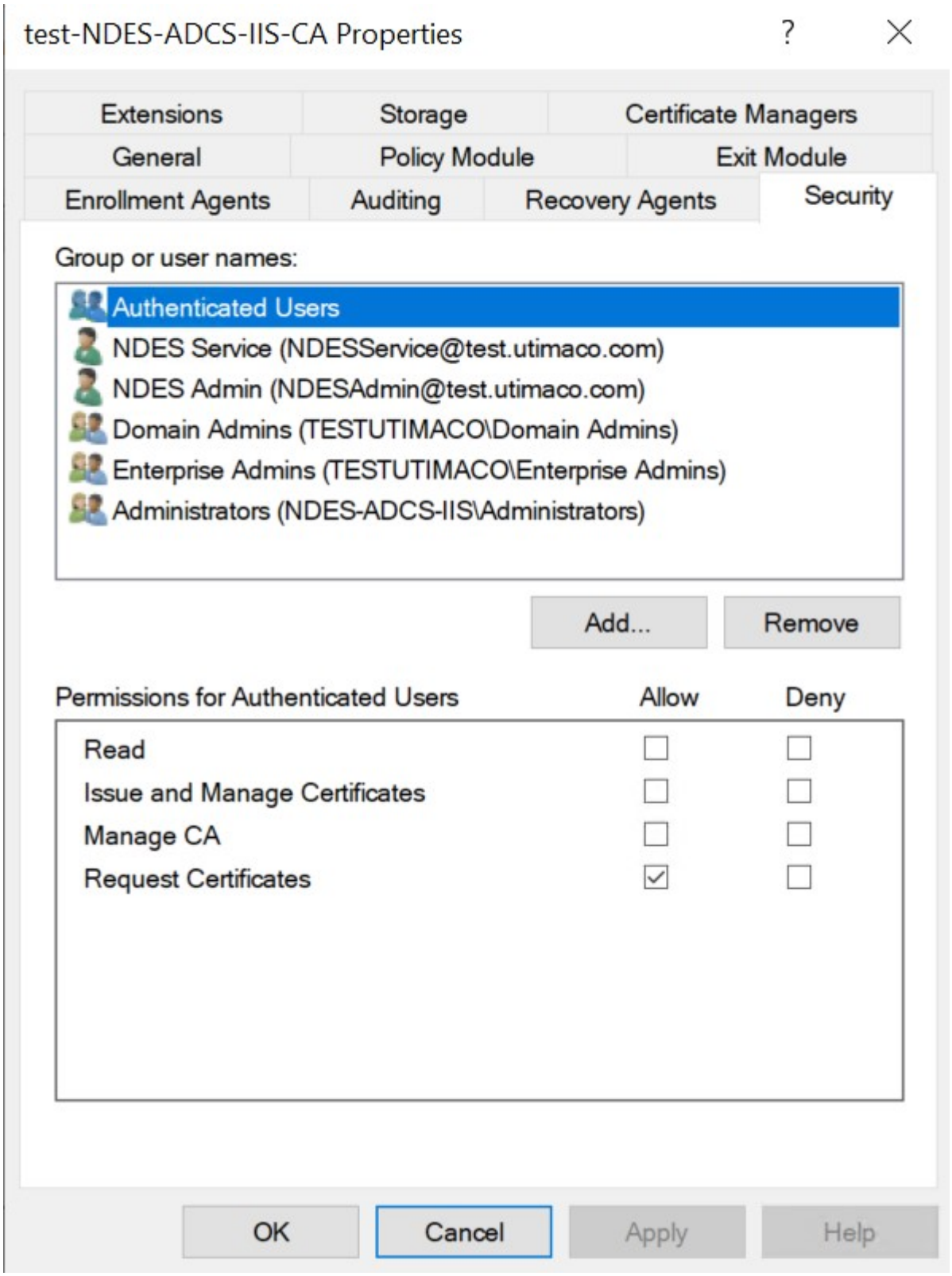

Figure 10 : test-NDES-ADCS-IIS-CA Properties Window

5.5 Configure the NDESDeviceAdmin Account with Enroll Permission to the IPsec (Offline Request) Certificate

1. Log into the CA server using the domain account.
2. Select Certification Authority from the Tools menu on the Server Manager window.
3. Expand the server on the left pane, then right-click on Certificate Templates and select Manage.

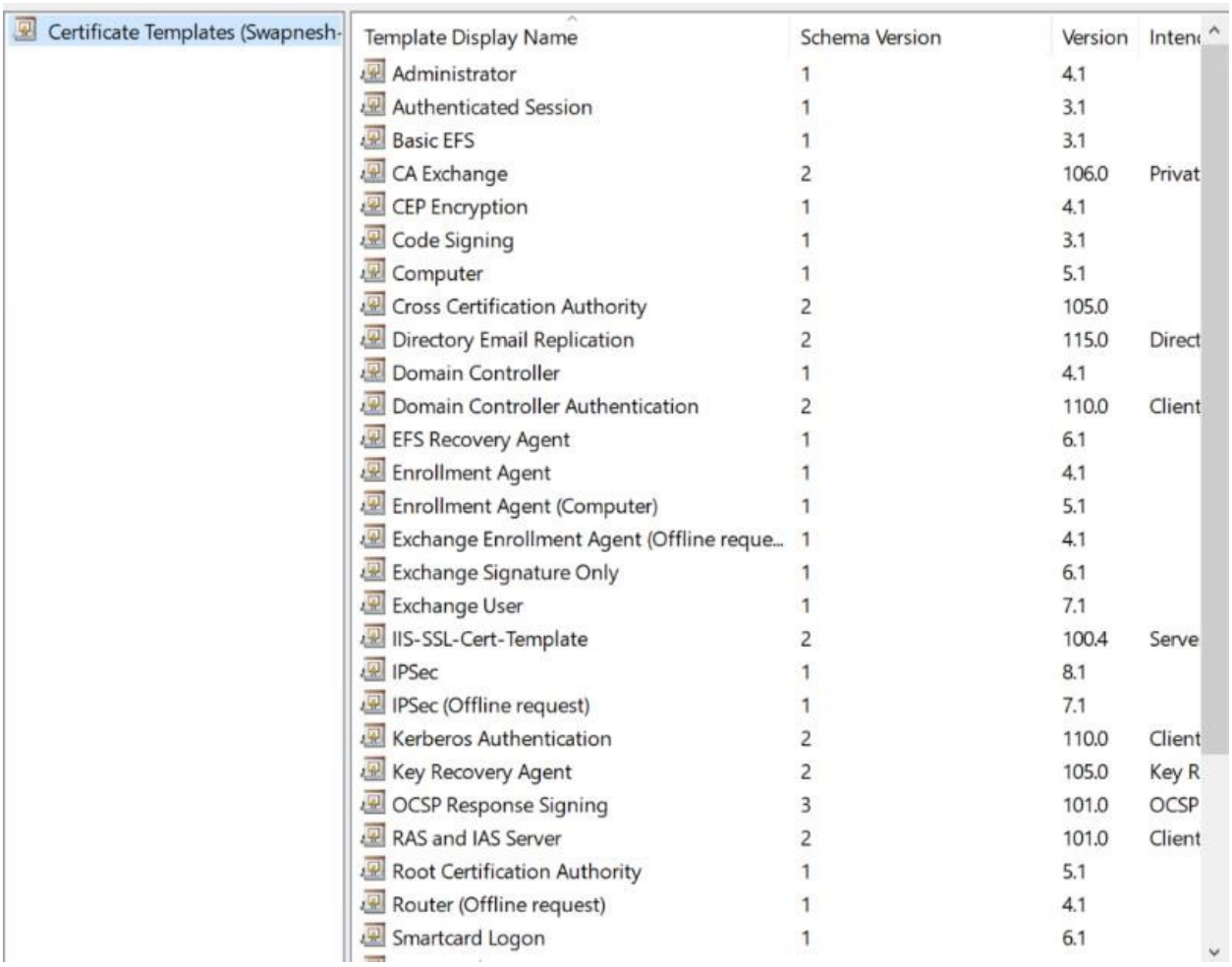

Figure 11 : Certificates Templates Window

4. Right-click on IPSec (offline request) Template Display Name and select Properties.
5. Click on the Security tab and select Add button.

6. On the Select Users, Computers, Service Accounts, or Groups text box, type the name of the NDESDeviceAdmin account, select Check Names, and after finding select OK.

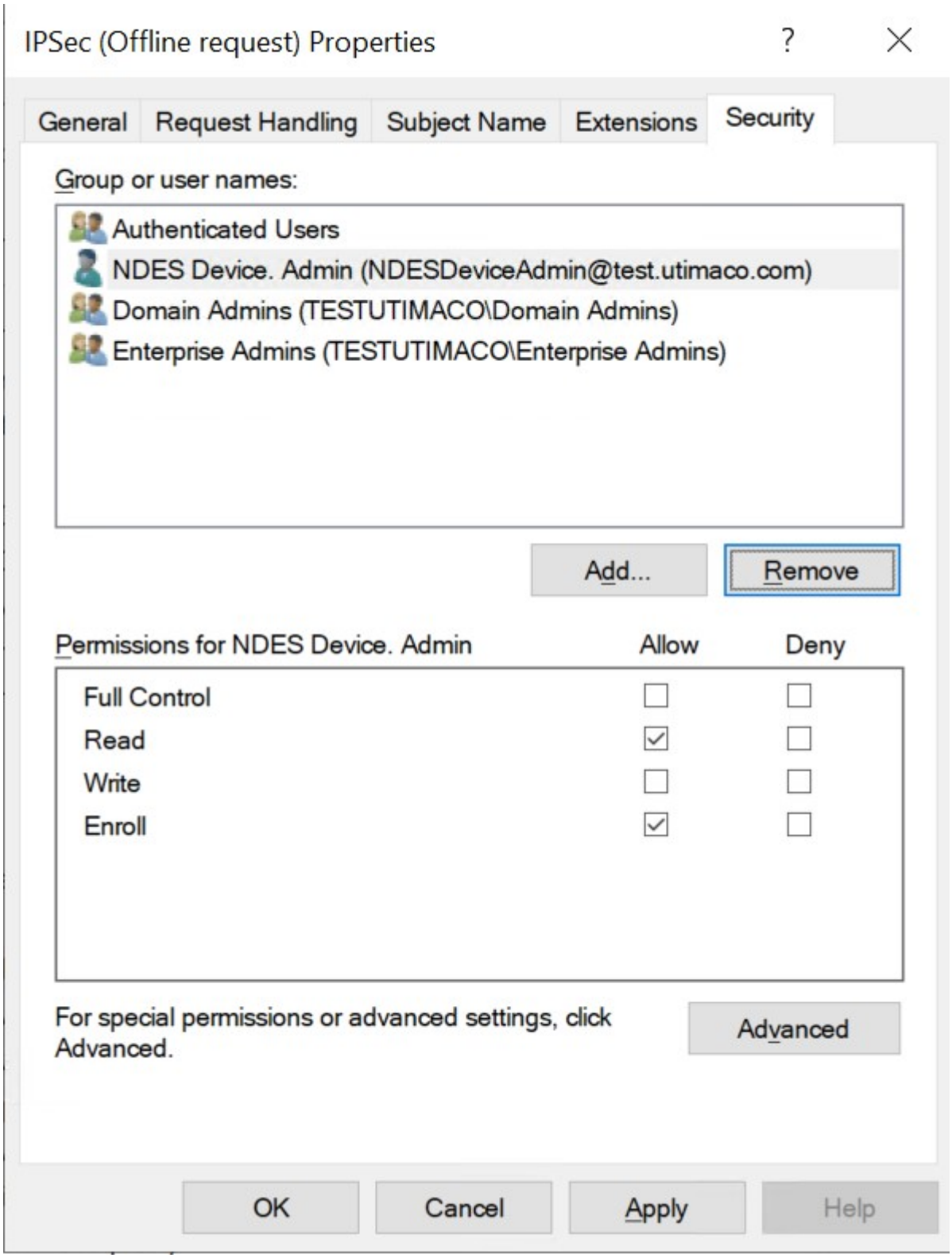

Figure 12 : IPSec (Offline request) Properties Window

7. Select the NDESDeviceAdmin account and verify the Allow check box that corresponds to Enroll is selected.

8. Select Apply and then select OK.

6 Installing and Configuring NDES

6.1 Installing NDES

1. Log into the NDES server using the domain account.
2. Open Server Manager.
3. Select Manage, then select Add Roles & Features. The Before you begin window opens. Select Next.
4. Select Role-based or feature-based installation on the Select installation type Window and click Next.
5. Select the server from the pool on the Select destination server window and click Next.
6. Select Active Directory Certificate Services role on the Select server roles window. The Add Roles and Features Wizard appears. Select Add Features and then select Next.
7. Click Next on the Select features window.
8. Select Next on the Active Directory Certificate Services window.
9. Uncheck Certification Authority and check Network Device Enrollment Service on the Select role services window. The Add Roles and Features Wizard will appear.
10. Select Add Features and then select Next on the Select role services window.
11. Click Install on the Confirm installation selections window.
12. Do not select Close on the Installation progress windows once the installation is complete.

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

6.2 Configuring NDES

1. On the open Window from previous step select the Configure Active Directory Certificate Services on the destination server link instead.
2. Change the Credentials to <domain_name>\NDESAdmin on the Credentials windows. Select Change, enter new credential, then select Next.
3. Check Network Device Enrollment Service on the Credential window, then select Next.

4. Select the Specify service account on the Service Account window, then click Select.
5. Enter the credential for the NDESService account and then select OK and Next.

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

6. Select CA name on the CA for NDES windows, then click Select.
7. Choose the CA server that you already have on the Select Certificate Authority window, then select OK and Next.
8. Note the specified Registration Authority (RA Name) on the RA Information window. Complete any of the optional information as required. Then click Next.

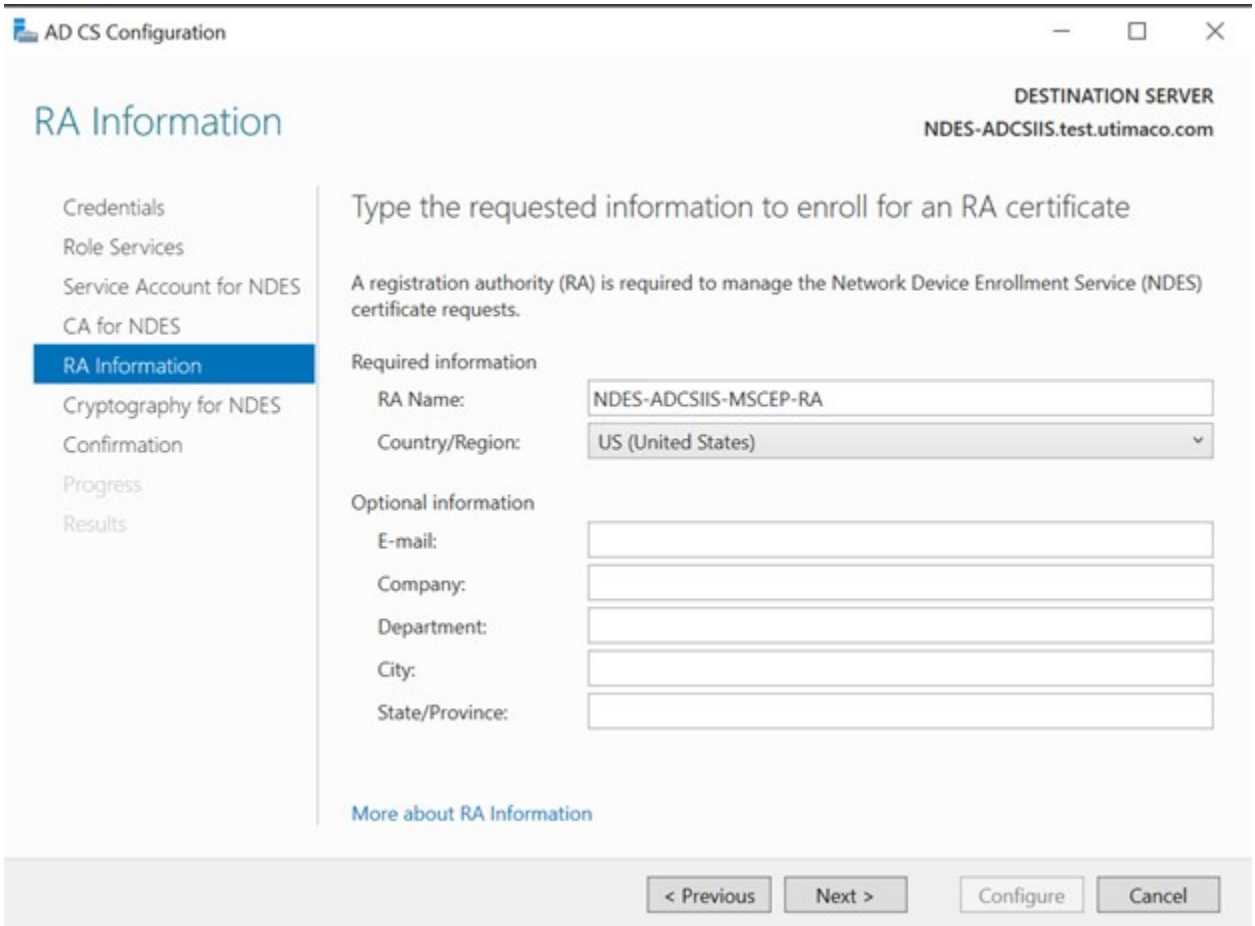

Figure 13 : AD CS Configuration Window

9. Choose the Uitmaco CryptoServer CSP on the Cryptography for NDES window. A key size of 2048 or larger is recommended.

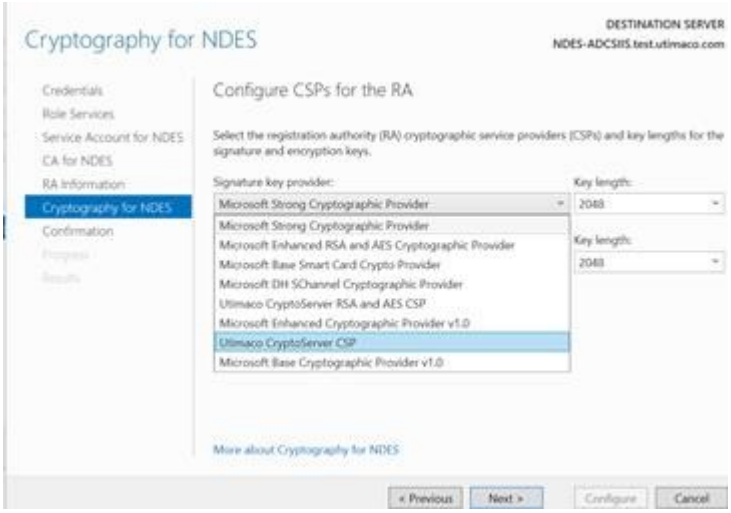

Figure 14 : Cryptography for NDES

10. Click Next and then click Configure.

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

11. Go back to the NDES server. Notice the Configuration succeeded message on the Results window. Then select Close.
12. Open any the browser and go to the following address: http://<NDES-server-address>/CertSrv/msecp_admin. Log in as <domain-name>\NDESService.
13. Notice the hash value of the CA certificate and the challenge password. Refreshing the browser generates a new enrollment challenge password.

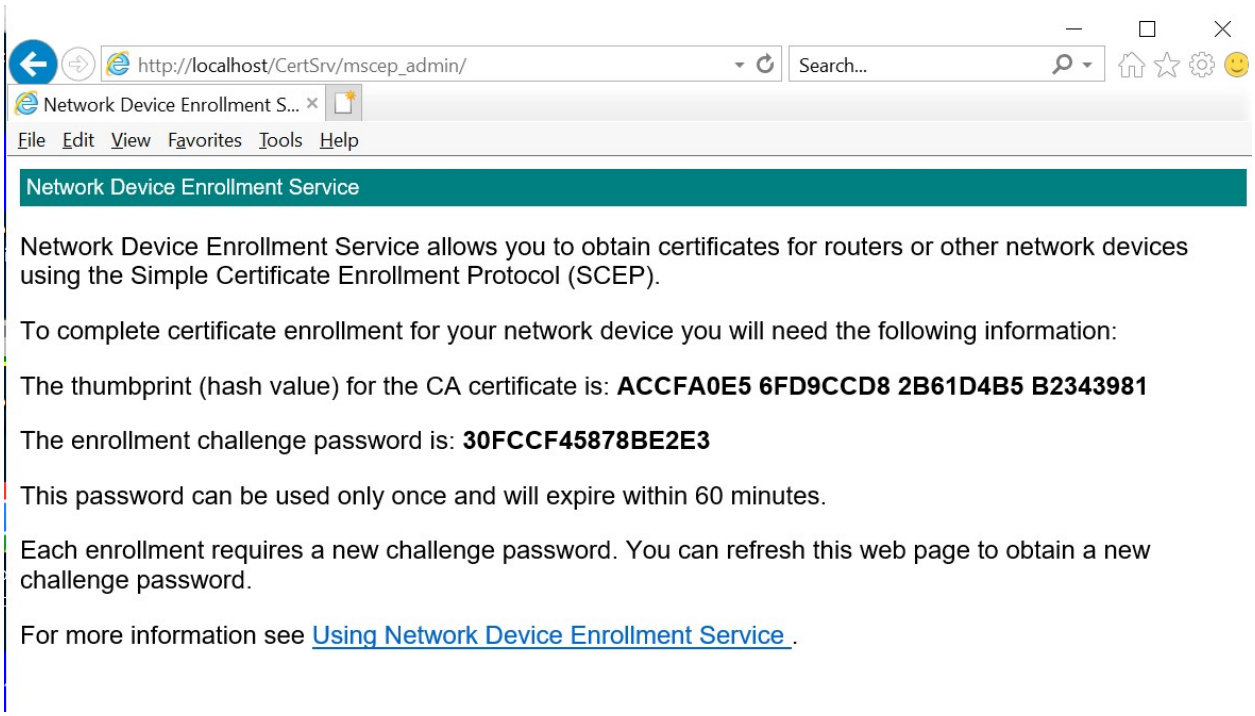

Figure 15 : Network Device Enrollment Service Window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

7 Configuring the NDES Admin Page to Use SSL Certificate

7.1 Generate SSL Certificate for IIS

To generate SSL certifcate for IIS Server follow these steps:

1. Log into the NDES server using the <domain_name>\Administrator.
2. Create a NDES-SSL-Cert.inf file using a text editor as follows. Change the Subject field to the Fully Qualified Domain Name (FQDN) of the NDES Server.

›_ Console

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "CN= NDES-ADCSIIS.test.utimaco.comutimaco-NDES-CA.com "
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "Utimaco CryptoServer Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
```

3. Open cmd and create a Certificate request file by running the following command.

›_ Console

```
certreq -new NDES-SSL-Cert.inf NDES-SSL-Cert.req
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

4. Copy the above certificate request file and send it to the CA for signing.
5. Once signed by CA paste the certificate back to NDES Server

6. Install the certificate by running the following command

›_ Console

```
certreq -accept IIS-SSL-Cert.cer
```

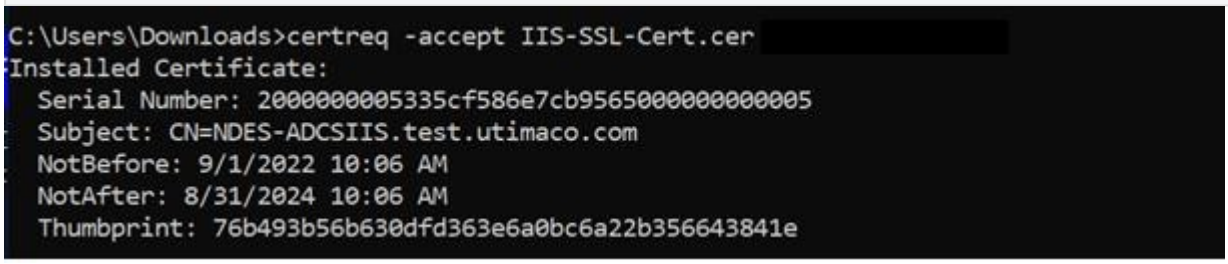

Figure 16 : Output Window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

7.2 Configure IIS to Use the SSL Certificate

1. Open the IIS manager, expand the server and Sites on the Connections pane and select Default Web Site.
2. Select Bindings on the Actions pane.
3. Select Add on the Site Bindings dialog.
4. Select https in Type: on the Add Site Binding dialog. Choose the certificate previously created in SSL certificate. Then select OK and Close.

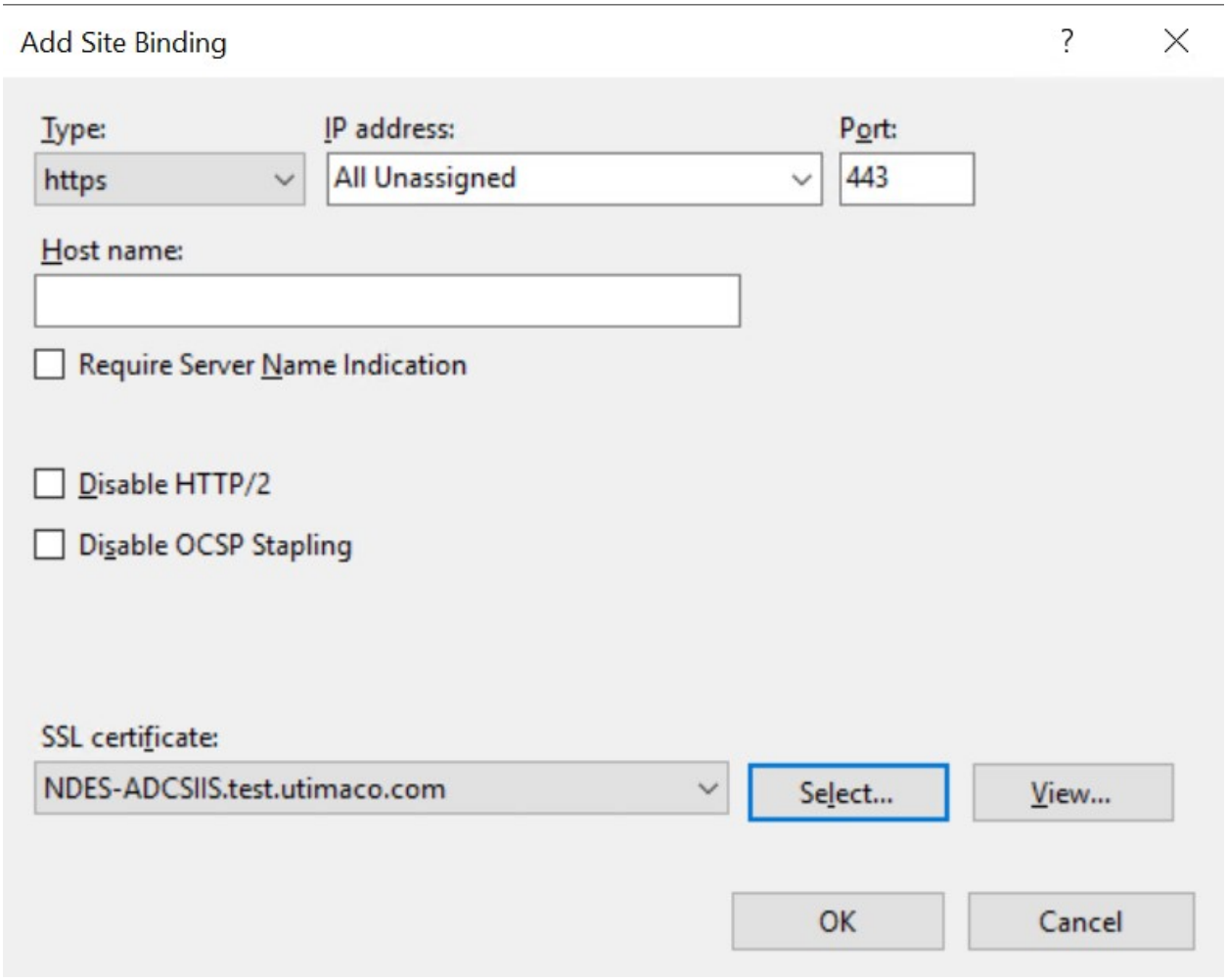

Figure 17 : Add Site Binding Window

Provide password as and when it is asking, if you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

5. Open any browser and go to the following address: https://<NDES-serveraddress>/CertSrv/mscep_admin. Log in as <domain-name>\NDESService.

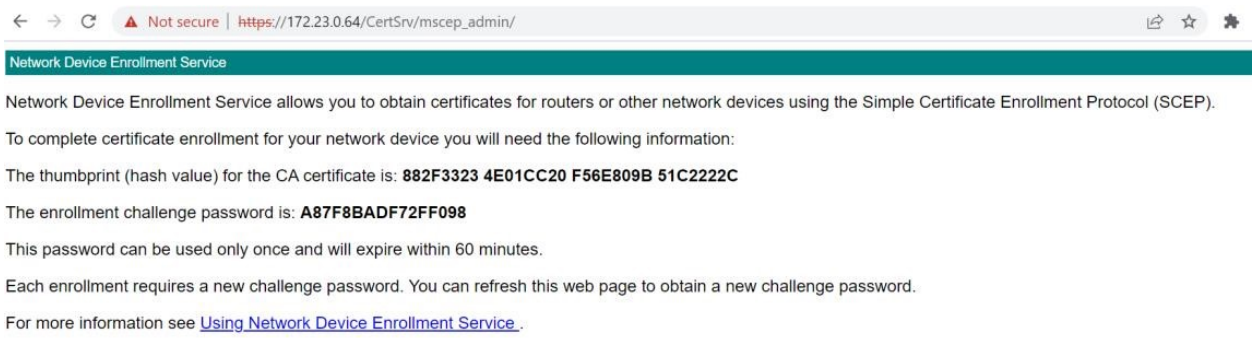

Figure 18 : Accessing NDES Admin Page

6. The page will load over HTTPS. Notice the hash value of the CA certificate and the challenge password. Refreshing the browser generates a new enrollment challenge password.

Unique password will be generated only 5 times by default. You can increase the maximum number of allowed unique passwords generated by the NDES service based on the requirement.

8 Verifying Microsoft NDES

1. Log on to the client machine that is not the part of domain.
2. Download the Microsoft SCEP utility from http://secadmins.com/index.php/ndes-scepwindows-test-tool/. Extract the file downloaded.
3. Open https://<NDES-serveraddress>/CertSrv/mscep_admin from any browser.
4. Enter the credentials for NDESAdmin and click OK. You will see the MSCEP Admin page with the challenge password for device certificate enrollment.
5. Open the command prompt and go to the directory where you extracted the MS SCEP utility.
6. Run the following command to generate a certificate request providing a Common Name and the Challenge Password when prompted by openssl.

›_ Console

```
openssl.exe req -config scep.cnf -new -key priv.key -out output.csr
```

```
C:\Users\Downloads\scep\scep>openssl.exe req -config scep.cnf -new -key priv.key -out output.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg, your name) []:Utimaco

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:5C799D82EB80673A
```

Figure 19 : Output Window

7. Retrieve the CA and RA certificates from your SECP/NDES server using the command.

›_ Console

```
sscep.exe getca -u http://<NDES-serveraddress>/CertSrv/mscep/ -c ca.cr
```

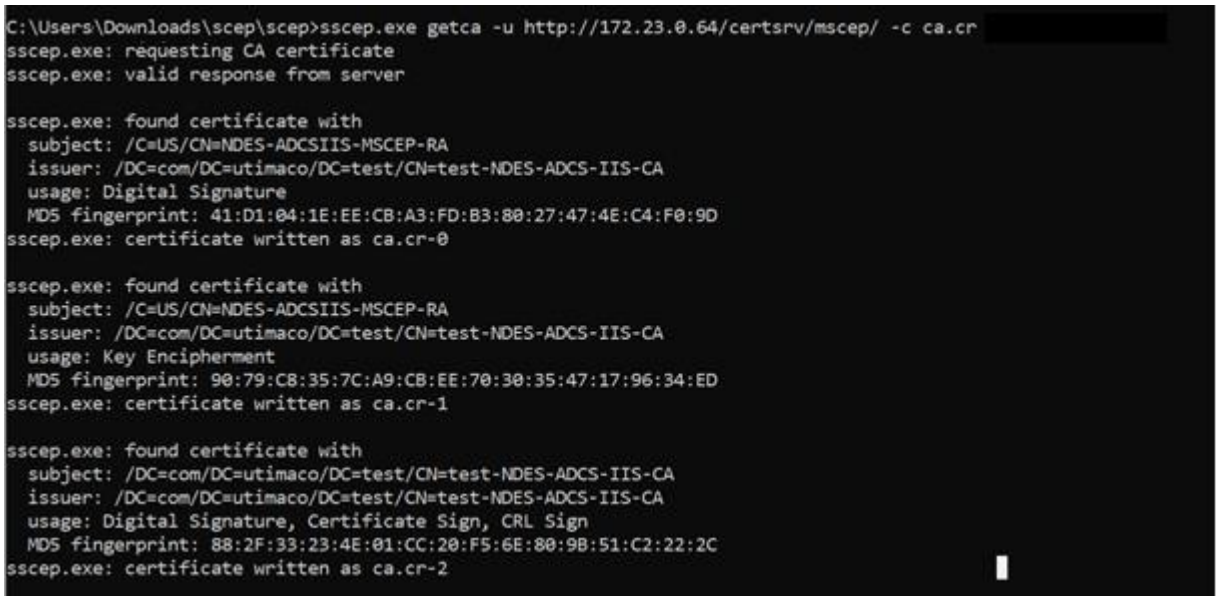

Figure 20 : Output Window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

8. Enroll a new certificate and make sure to specify the correct RA (-c flag) & CA (-e flag) certificates using the command below.

›_ Console

```
sscep.exe enroll -u https://<NDES-serveraddress>/CertSrv/mscep/ -k
priv.key -r output.csr -l output.crt -c ca.cr-0 -e ca.cr-1
```

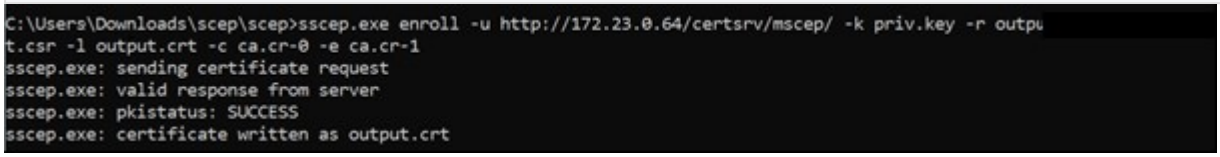

Figure 21 : Output Window

Provide password as and when it is asking, if you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

9. Open the output.crt file to verify that the certificate is signed by your CA.

This completes the integration of Microsoft NDES with Utimaco HSM.

9 Troubleshooting

Error	Diagnosis
Using the certreq -new <.req file here> command returns an Invalid Provider Specified error.	Ensure that the Utimaco CNG/CSP providers are correctly installed and set.
The AD CS Configuration Wizard does not detect the Smartcard Device.	Install the PPD drivers using SecurityServer latest version.

Table 6: List of Errors and their Diagnoses

10 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website:

https://utimaco.com/.

11 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSLAN]	CryptoServerLAN_V5_Manual_Systemadministrators.pdf	2018-0010
[CSP-CNG]	CryptoServer_Manual_CSP_CNG.pdf	2008-0002

12 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.