



STEVE WEINER · MAY 12, 2021

NDES and SCEP for Intune: Part 4

Can you smell that? It's the smell of almost being done deploying SCEP certificates to Windows 10 devices from Intune via the Intune SCEP connector and NDES server.

In case you missed it, you can start from Part 1, [here](#).

Part 4: Adding the root, deploying SCEP and achieving victory

EXPORT THE ROOT CERTIFICATE (CA)

Log into the CA and open an elevated CMD prompt. Type the following:

```
certutil -ca.cert C:\root
```



```
C:\Users\administrator.ZEROTOUCH>certutil -ca.cert C:\root.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDFTCCAmBgAwIBAgIQQG1rNB4eH+FY1vqTANBgkqhkiG9w0BAQsFADBR
MRUwEVYKZCImIZPyLQGBGRYFBg9jYwvxGTAXBgjKiaJk/TsZA2FgI6ZXvG91
YzgxKHTAbBgNVBANTP0l1o0b3V/a1aMRDwRmLNUmQHTE5IzHDE4NDeY
M1oXnTB0fT0fLQGBGRY3eayjy1oUWtGmGmJ0mT81xKMRMqdtYV/FsPRHdWPK
Cj1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1zIz1z
NC1DQTCASImQYJko2IkvcNAQEBOBQDggEPADCAQcCgeBALauY2hCH.dnV3co
dJBRn4wSL2vcl4lnhh4v8fQ6EvSV/SehpKvYf1phpldrqV1YSPCU7krXpI7STCL
ypV7p0Gg08HKxfUh88+hx1sTDDGavlamap0nZ13NQ5uMs0z0oZ1HuuvvPMI
1shLuiuGbwuHFjGkhmo83h02V0drd1MBcCnTY80+8nArwv5zPwCJAzc2V1sdfQ
cvMg2UxF6MOMuabRo7ye81McnNzdsJHD/mFNGLh1c3Rwn1qxwHMz2vzs
XyyvNLSv*#16]1nr8+gsP1M+&F2Xwlb1btz1x8dr1hdNb1GzciujfKwlPaxCR
RoV1o8CawEAoJRNIEBnwDVROpBAQAgGGMA0GA1ueWeB/QfMANBFAwHQYD
VR00BBYEFkTQ075757Rn2M0Ep5a15Cu/eBGMBAGC5sGAQQBgjcVAQQAgaEAAQG
Csqg51bDQ0EBcWm41BAQCKhFl1rBBNm4dUf1M4mf6sJDxJ0fLX9cZXY3C9u
tivS51DQ0EBcWm41BAQCKhFl1rBBNm4dUf1M4mf6sJDxJ0fLX9cZXY3C9u
US1f3fegL09E/Y7u3ec0QaFO/G1G02yaaEnG74K/B7fFzJ7Q313ju3dgpm0FH
Rzyyvymw0FzcuFwB0p0uVrbh6cvol7jeV1kh2nDrfa7aLL7mrlD0eCqr05H7
7FU1ABRX1C/WKSYiwhlREExshG6hEwcl0/Hdnby6e/PcLUwdXaoJVBShEgnV7F
M7TNwBprccy95Y4BpcUllwjjf+3GRQVHgkDr1HGFIyXq
-----END CERTIFICATE-----
CertUtil: -ca.cert command completed successfully.

C:\Users\administrator.ZEROTOUCH>
```

Obviously, feel free to use whatever path you're comfortable with for the root certificate.

DEPLOY TRUSTED ROOT CERTIFICATE PROFILE (INTUNE)

Log into Intune at

<https://endpoint.microsoft.com>

and navigate to Devices ->

Windows -> Configuration profiles and click +Create profile. Choose Windows 10 - > Templates -> Trusted certificate.

In the “Certificate file” field, navigate to your root.cer you exported in the last step and upload it.

In “Destination store”, select **Computer certificate store – Root**.

Assign this profile to a device group.

CONFIGURE SCEP PROFILE (INTUNE)

Assuming you’re still logged into the Endpoint Manager, create another configuration profile. Choose **Windows 10 –**

> Templates -> SCEP
certificate.

Create a profile

Custom ⓘ
Delivery Optimization ⓘ
Device Firmware Configuration Interface ⓘ
Device restrictions ⓘ
Device restrictions (Windows 10 Team) ⓘ
Domain Join ⓘ
Edition upgrade and mode switch ⓘ
Email ⓘ
Endpoint protection ⓘ
Identity protection ⓘ
Kiosk ⓘ
Microsoft Defender for Endpoint (Windows 10 Desktop) ⓘ
Network boundary ⓘ
PKCS certificate ⓘ
PKCS imported certificate ⓘ
SCEP certificate ⓘ 
Secure assessment (Education) ⓘ
Shared multi-user device ⓘ
Trusted certificate ⓘ

Fill out the following fields in
the SCEP certificate profile:

- **Certificate type:** Device
- **Subject name format:**
CN={{AAD_Device_ID}}
- **Certificate validity period:** 2 Years
- **Key storage provider (KSP):** Enroll to Trusted

Platform Module (TPM)

KSP if present, otherwise

Software KSP

- **Key usage:** Key encipherment, Digital signature
- **Key size (bits):** 2048
- **Hash algorithm:** SHA-2
- **Root Certificate:** <NAME OF ROOT CERT FROM PREVIOUS STEP>
- **Extended key usage:** Client Authentication
- **SCEP Server URLs:**
`https://<NAME OF YOUR EXTERNAL URL FROM AZURE APP PROXY>/certsrv/mscep/mscep.dll`

The screenshot shows the configuration of an SCEP certificate profile. Key settings include:

- Certificate type:** Device
- Subject name format:** CN=|AAD_Device_ID|
- Certificate validity period:** 2 Years
- Key storage provider (KSP):** Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software K...
- Key usage:** 2 selected
- Key size (bits):** 2048
- Hash algorithm:** SHA-2
- Root Certificate:** ZTD-NDES-Root Cert (selected)
- Extended key usage:** Client Authentication (selected), Object Identifier: 1.3.6.1.5.7.3.2, Predefined values: Client Authentication (1.3.6.1....)
- Enrollment Settings:**
 - Renewal threshold (%):** 20
 - SCEP Server URLs:** https://https://ndeszerotouchlocal-m365x93446.msappproxy.net/certsrv/mscep/mscep.dll

Buttons at the bottom include **Previous**, **Next**, and **Export**.

Assign the SCEP profile to a device group, and watch it deploy.

EPILOGUE: Troubleshooting

You should feel proud. That was a convoluted and painful process, but you did it. Now if for some reason the SCEP cert doesn't deploy, there's a few good steps you can take to troubleshoot.

VALIDATE NDES POWERSHELL SCRIPT.

Microsoft offers a PowerShell script called “Validate-NDESConfiguration.ps1” that can be found [here](#). It’s a very useful script that you run on your NDES server to make sure all your ducks are in a row. It will very clearly point out if you missed a step or something isn’t configured correctly.

```
Checking Windows OS version...
Success: OS Version 10.0.14393 supported.

-----
Checking NDES Service Account properties in Active Directory...
Success: NDES Service Account seems to be in working order:

SamAccountName      : ndes
Enabled             : True
AccountExpirationDate : 9223372036854775807
AccountExpires       :
AccountLockoutTime   :
PasswordExpired      : False
PasswordLastSet       : 4/26/2021 9:21:48 AM
PasswordNeverExpires  : True
Lockedout            : False

-----
Checking if NDES server is the CA...
Success: NDES server is not running on the CA

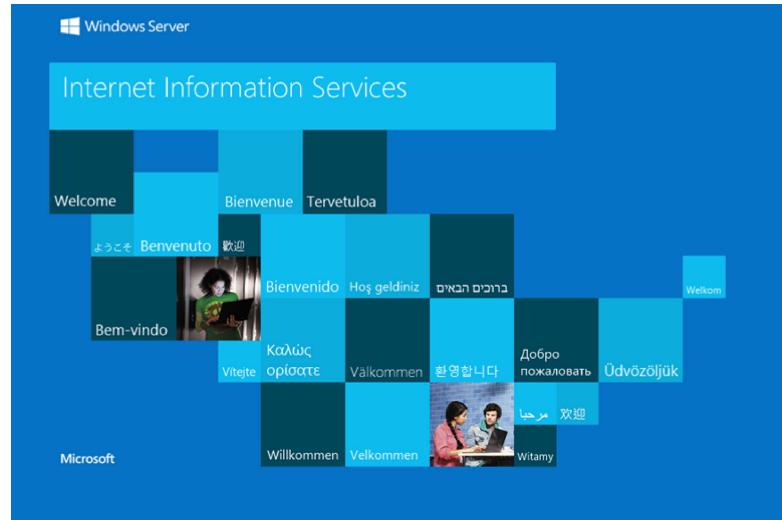
-----
Checking NDES Service Account Local permissions...
Success: NDES Service account is not a member of the Local Administrators group
Checking NDES Service account is a member of the IIS_IUSR group...
Success: NDES Service Account is a member of the local IIS_IUSR group

-----
Checking Windows Features are installed...
Success: Request Filtering Feature Installed
Success: .NET Extensibility 4.6 Feature Installed
Success: .NET Framework 4.6 Feature Installed
Success: HTTP Activation Feature Installed
```

TEST THE AZURE APP PROXY

Before deploying anything, you should ensure the Azure App Proxy is doing its job. To do that, just navigate to the external URL from any browser. You should see the

Windows IIS page coming from
the NDES:



Next, verify that the full
MSCEP path works by
navigating to the full path in
your SCEP profile. It should be
[https://<yourExternalURL>/ce
rtsrv/mscep/mscep.dll](https://<yourExternalURL>/certsvr/mscep/mscep.dll). While
it looks scary, be happy if you
see this:

HTTP Error 403.0 – Forbidden (0x8000ffff)
You do not have permission to view this directory or page.

Most likely causes:
• This is a generic 403 error and means the authenticated user is not authorized to view the page.

Things you can try:
• Create a tracing rule to track failed requests for this HTTP status code. For more information about creating a tracing rule for failed requests, click [here](#).

Detailed Error Information:

Module	IISAPI Module	Requested URL	http://20-ndes.zerotouch.local:80/certsrv/mscep/mscep.dll
Notification	ExecuteRequestHandler	Physical Path	C:\Windows\system32\CertSrv\mscep.dll
Handler	IISAPI-dll	Logon Method	Anonymous
Error Code	0x00000000	Logon User	Anonymous

More Information:
This generic 403 error means that the authenticated user is not authorized to use the requested resource. A substatus code in the IIS log files should indicate the reason for the 403 error. If a substatus code does not appear above, gather more information about the source of the error.
[View more information](#)...
...or [View less information](#).

That's because this is a service
and not a website to go

browsing on.

**IF HYBRID JOINING

If you're using Autopilot to perform a Hybrid Azure AD join for Windows 10, and you plan to deploy a SCEP cert, you need to make one important change.

For Subject name format, use
CN=
{{FullyQualifiedDomainName}}
}}.



RE-TRACE YOUR STEPS

If things aren't working the way they should, don't worry. There are a lot of steps in this process that will have you bouncing back and forth between AD servers, Azure sites and Intune. Even if you don't nail it on the first shot, don't get down. Just going through the whole process several times, you'll feel

more comfortable and have a better understanding of how the pieces work together.

Reach out if you hit a snag at
steve@getrubix.com.

Thanks for hanging in there with me.



PREVIOUS

Home Office and Geek Cave Tour

NEXT

NDES and SCEP for Intune: Part 3

