RUBIX
Solving for the modern workplace

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.

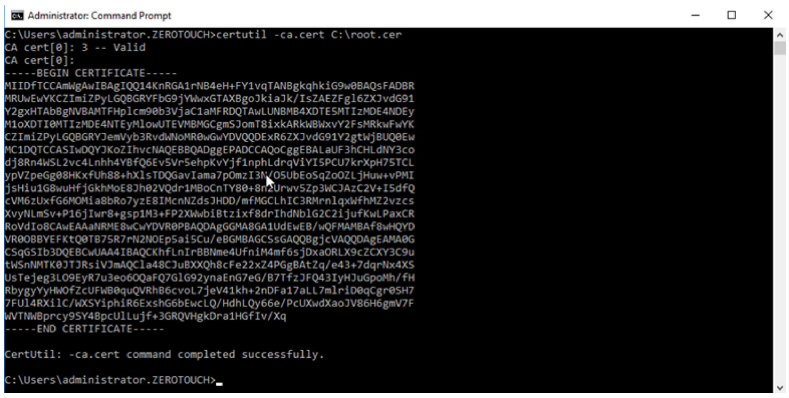
In case you missed it, you can start from Part 1, here.

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:

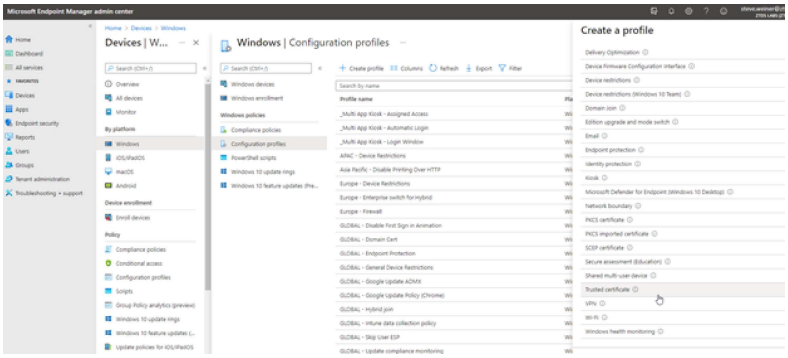
```
certutil -ca.cert C:\roo
```



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

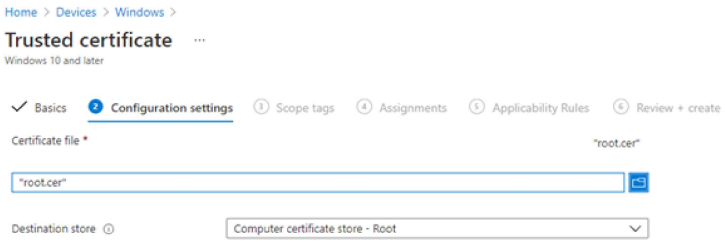
DEPLOY TRUSTED ROOT CERTIFICATE PROFILE (INTUNE)

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.**

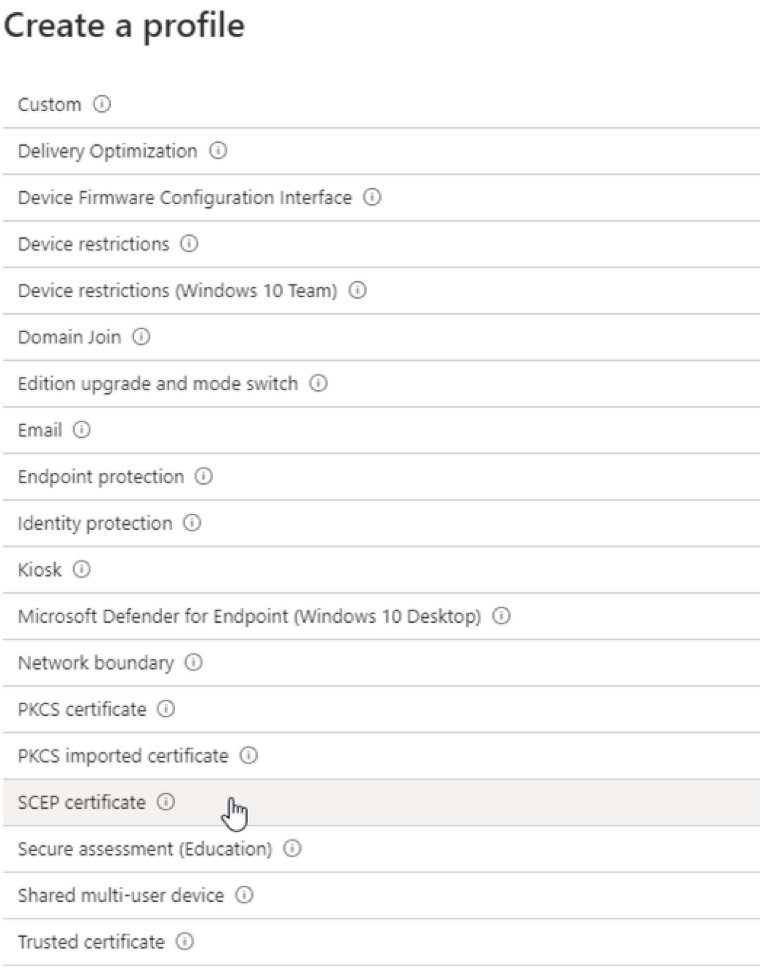


Assign this profile to a device group.

CONFIGURE SCEP PROFILE (INTUNE)

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

> Templates -> SCEP certificate.

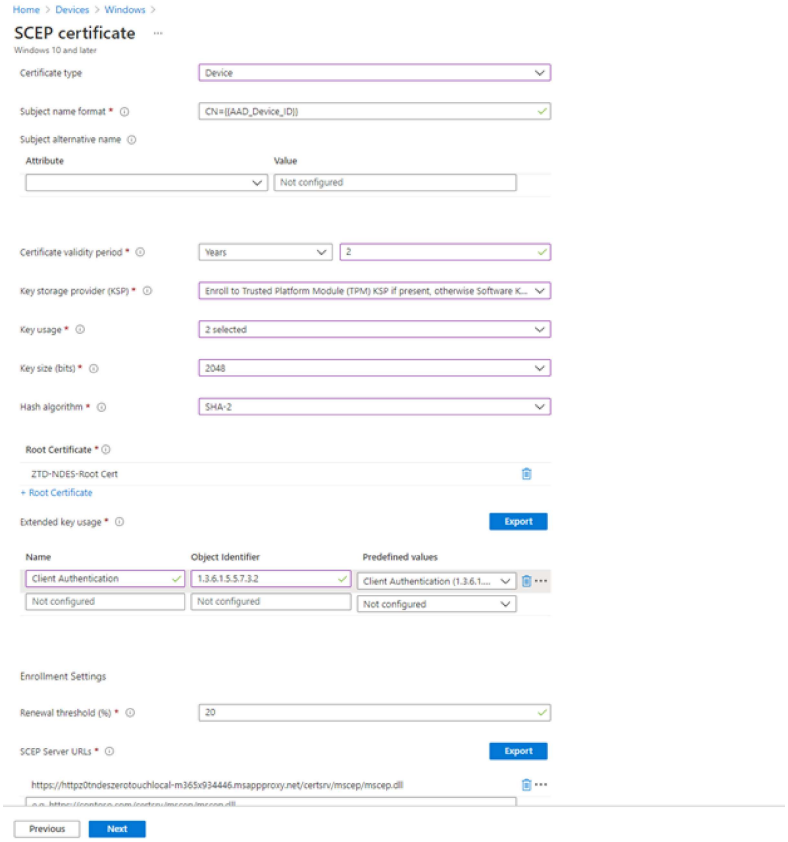


Fill out the following fields in the SCEP certificate profile:

- **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



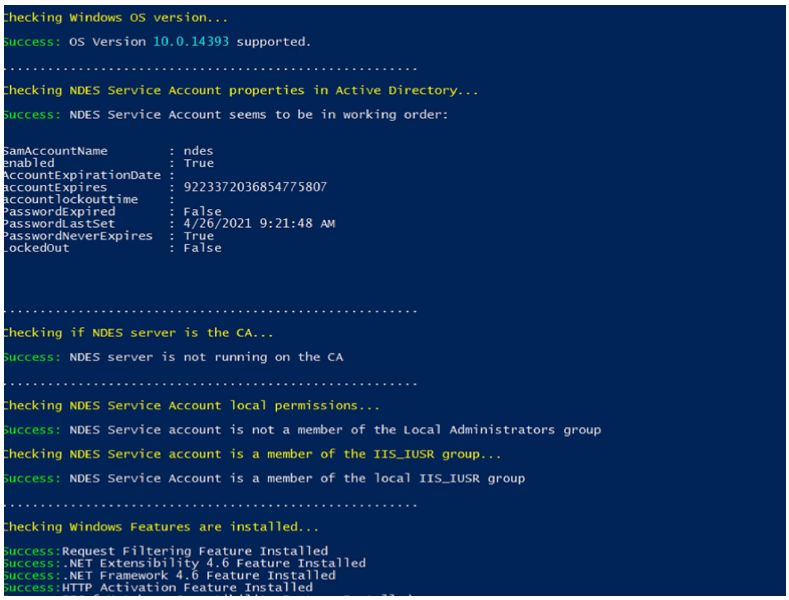
Assign the SCEP profile to a device group, and watch it deploy.

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.

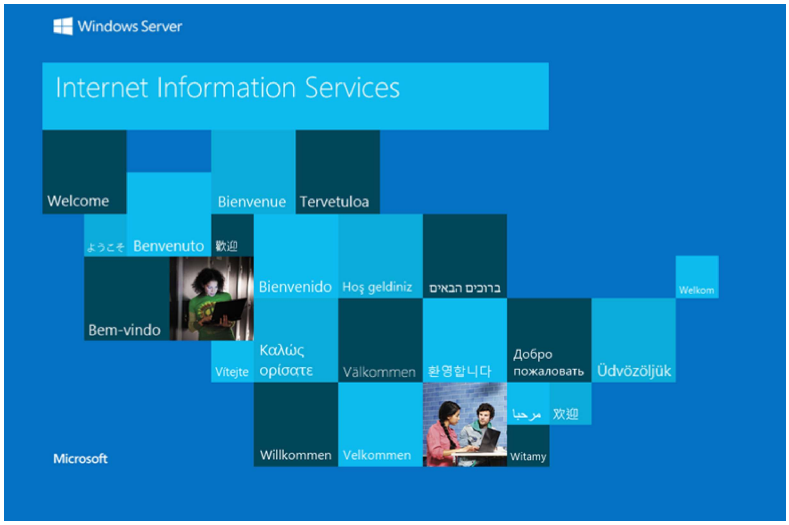
Microsoft offers a PowerShell script called "Validate-NDESConfiguration.ps1" that can be found here. It's a very useful script that you run on your NDES server to make sure all your ducks are in a row. It will very clearly point out if you missed a step or something isn't configured correctly.



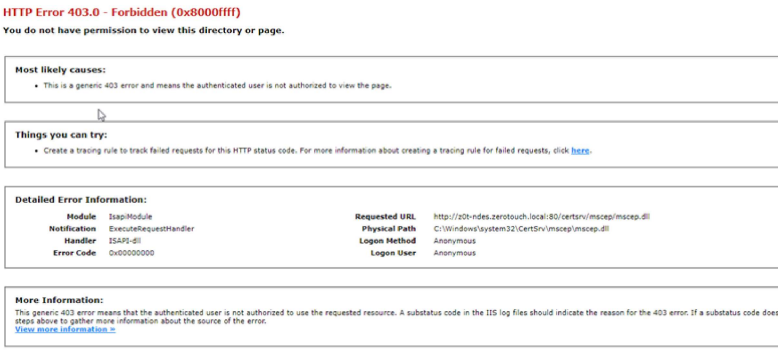
TEST THE AZURE APP PROXY

Before deploying anything, you should ensure the Azure App Proxy is doing it's 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>/certsrv/mscep/mscep.dll**. While it looks scary, be happy if you see this:



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