RUBIX
Solving for the modern workplace

STEVE WEINER · MAY 10, 2021

NDES and SCEP for Intune: Part 1

Long time, no talk. But it's because I've been busy. And usually when I'm this busy it means I've got a lot to talk about. During three separate Endpoint Manager implementations, I've recently had to go outside my comfort zone and help folks troubleshoot Intune SCEP certificate profiles. That led to poking around the SCEP connector itself. Well, once I started looking there, it wasn't long before I pumped the breaks, took a deep breath, and figured out how to build the

whole thing from scratch. So, sit back and relax while I take you through the entire setup process of an Intune certificate connector on a fresh, new NDES server.

MINI SERIES

There's a lot of things that need to happen in order to get this working properly. Anyone who tells you it's 'painless' or 'no big deal' is a heartless liar. It's confusing, frustrating and worst of all, there's little documentation of the entire process in its entirety. I found very good pieces written by various tech resources detailing specific parts, often one blog had a piece missing from the other, all becoming pieces of the larger solution.

So, what I'll do here is break this into several parts of a whole series, each piece detailing their own part of the process. This way it can stay manageable, but all reside in the same place.

WORKFLOW

The high-level breakdown is as follows:

- NDES is a Windows Server joined to your Active Directory. DO NOT use a domain controller for this.
- NDES contains IIS role, which will handle incoming web requests from Intune asking for certs
- Azure application proxy is used to provide an external URL that points to the internal URL of the NDES
- Intune certificate connector is installed on NDES
- Intune SCEP profile makes request through Intune Certificate connector for cert. NDES asks for cert template from issuing CA and deploys through Intune

WHY DO I NEED THIS?

The Intune certificate connector lets you deploy certificates to devices that you would traditionally deploy to a domain joined PC via group policy. But we're not domain joined anymore, are we now? No, we're not. So we need a way to get those same certs from the Domain CA that are used for client authentication for VPN, MFA, and other fun things.

Alright, here we go. And for clarity, each section will have a location code so you know exactly where we're performing each step. Codes are as follows:

CA = Certificate Authority

NDES = Network Device Enrollment Service (server we're building)

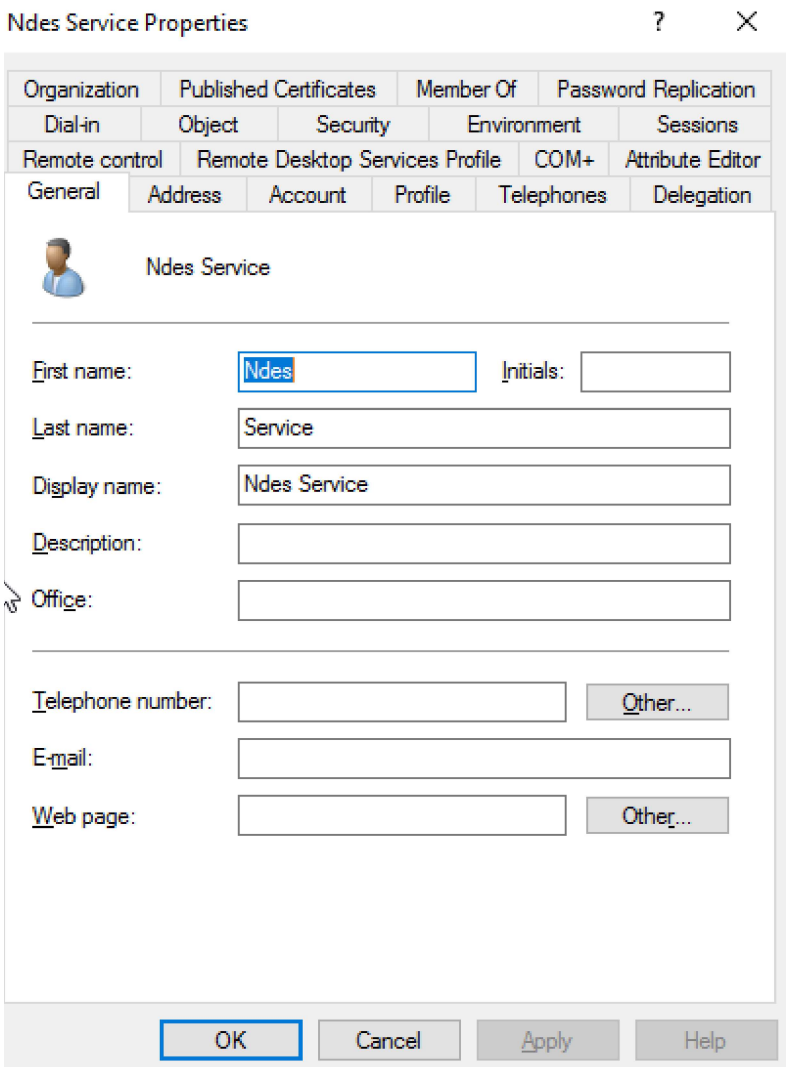
Intune = Microsoft Endpoint Manager (https://endpoint.microsoft.com)

AD = anywhere in your Active Directory

Part 1 – The service account, certificate templates, and NDES role.

MAKE AN NDES ACCOUNT AND SERVER (AD)

In your on-premises Active Directory, create a new user that we will use as a service account for our NDES activities.



For the server, just spin up a fresh Windows Server 2016 or later physical or virtual machine and join it to your domain. DO NOT promote it to a domain controller.

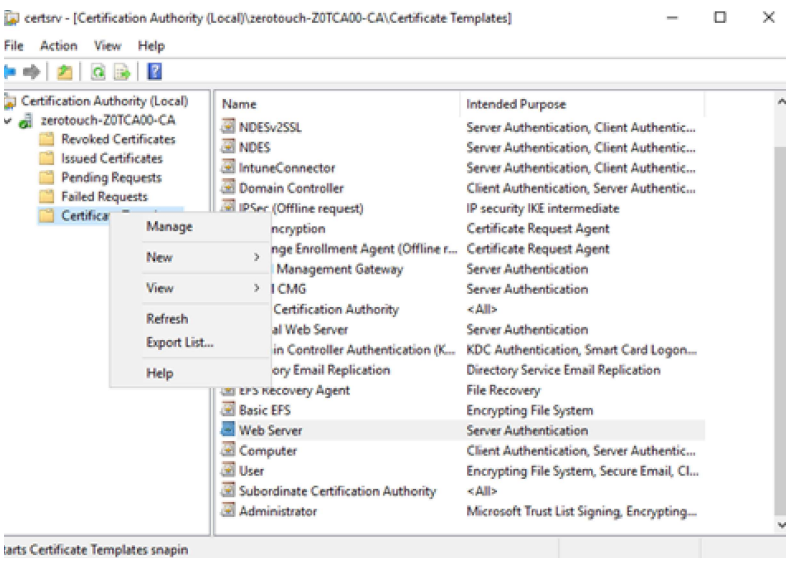
CERTIFICATE TEMPLATES (CA)

We will make two certificate templates. First will be the Web Server template used for NDES

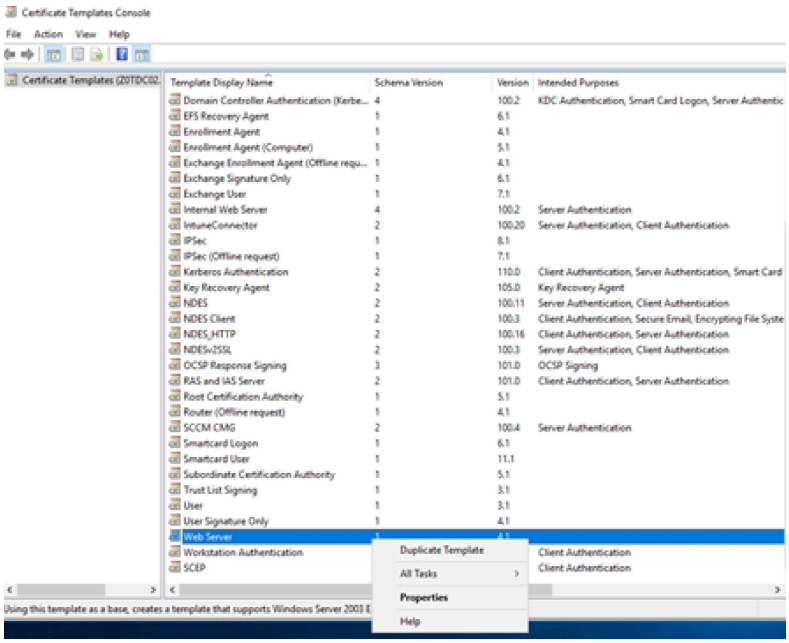
and Intune connector authentication to the CA.

Next is the SCEP template for client authentication- this will be the certificate that gets issued to Intune devices via connector.

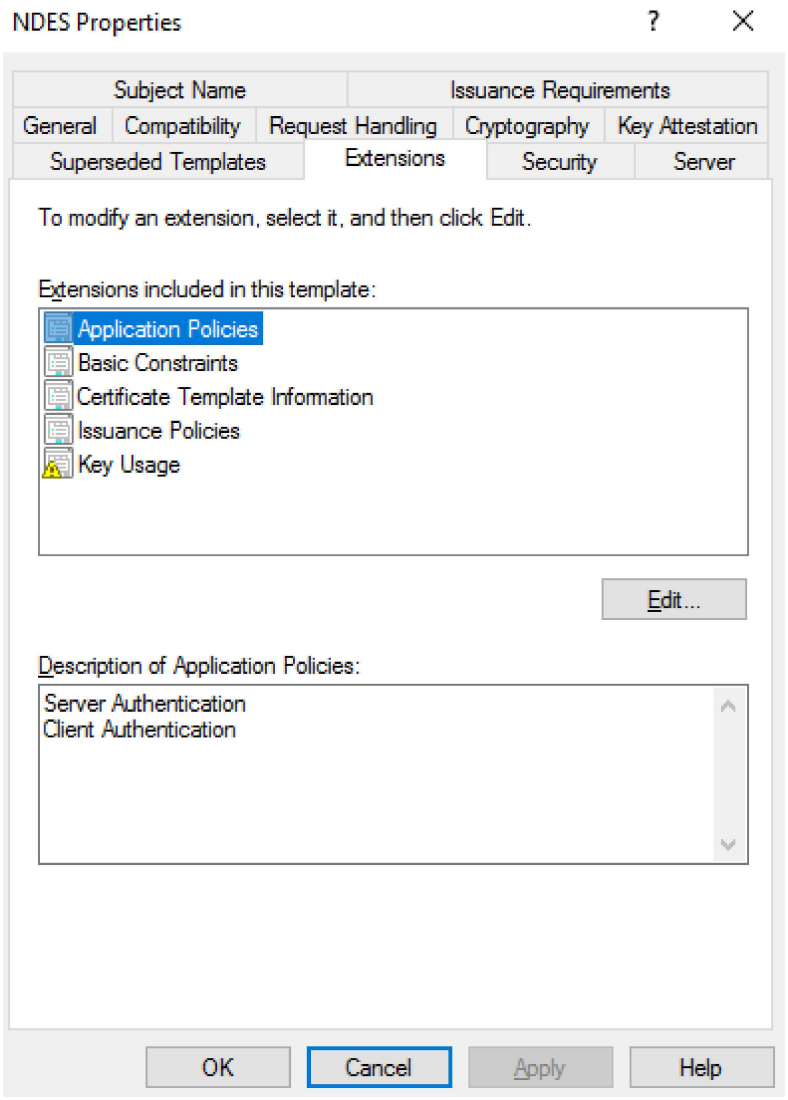
Log into your CA open the Certification Authority. Expand the CA and right-click Certificate Templates. Click "Manage"



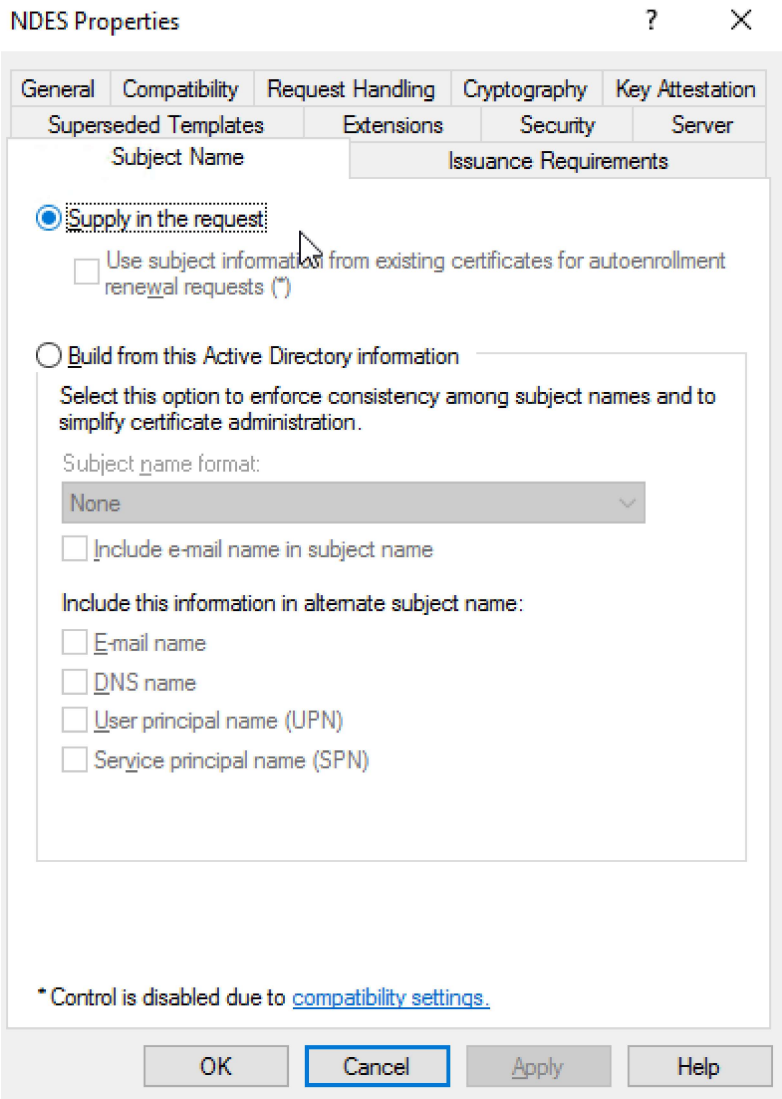
The Certificate Templates Console opens. Right click on "Web server" and select **Duplicate Template**.



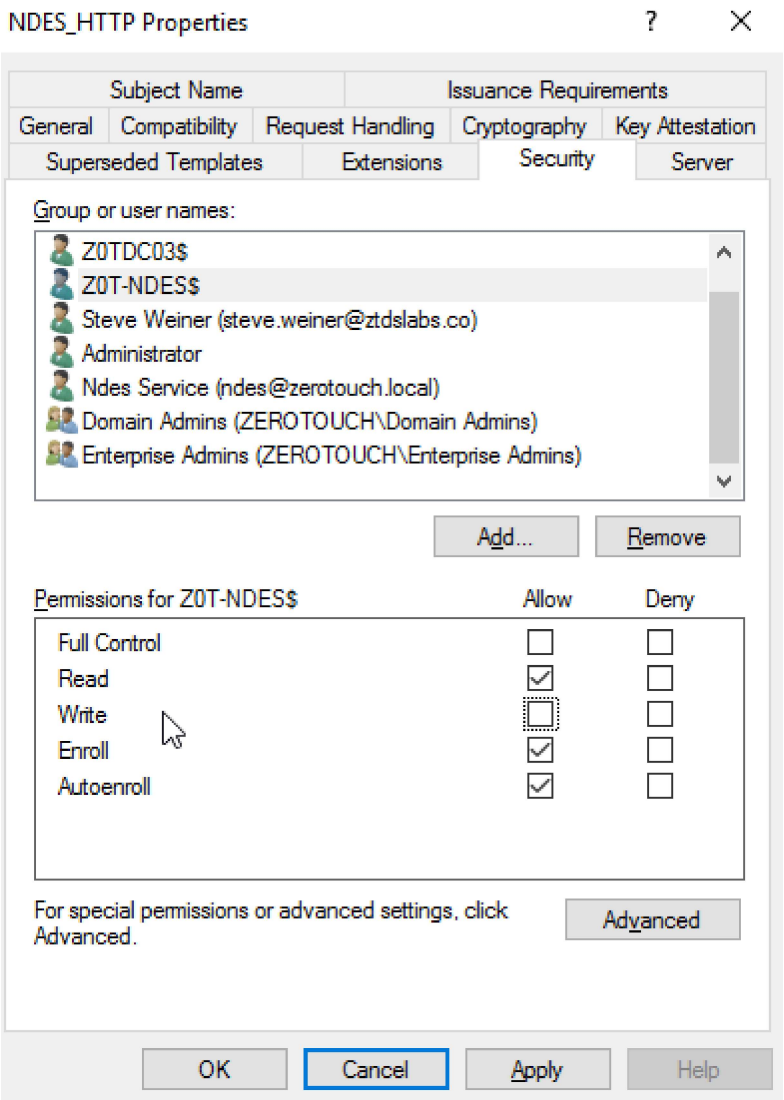
In the “Extensions” tab, edit Application Policies to contain Server Authentication and Client Authentication.



In the “Subject Names” tab, ensure that **Supply in the request** is selected.



In the “Security” tab, add the name of the NDES server you just made and give it **Read, Enroll** and **Autoenroll** permissions.

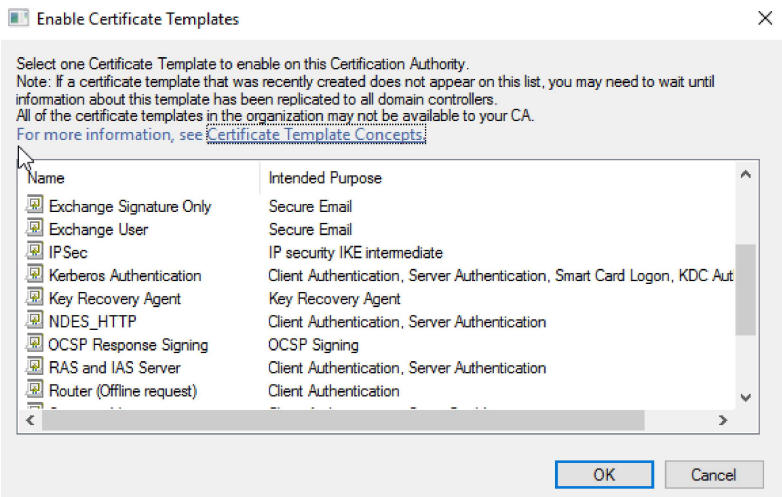


Make sure to give it a clear name in the "General" tab. I just use "NDES". Click **Apply** and **OK** to close.

Use the above flow to make another certificate. This one will be used as the client authentication template issued to Intune. Make the following changes:

- Duplicate from “User” template
- Extensions -> Application Policies -> add **Client Authentication**
- Security -> add NDES user -> enable permissions for **Read, Enroll**, **Write and Autoenroll**
- Subject Name -> select **Supply in the request**
- Click and Apply and OK to save certificate. Close the Certificate Template Console.

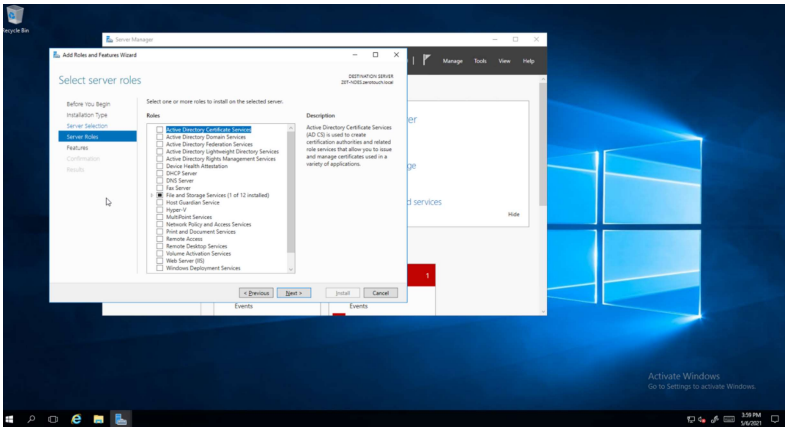
Back in the Certification Authority console, right click on **Certificate Templates** and select **New -> Certificate Template to Issue**.



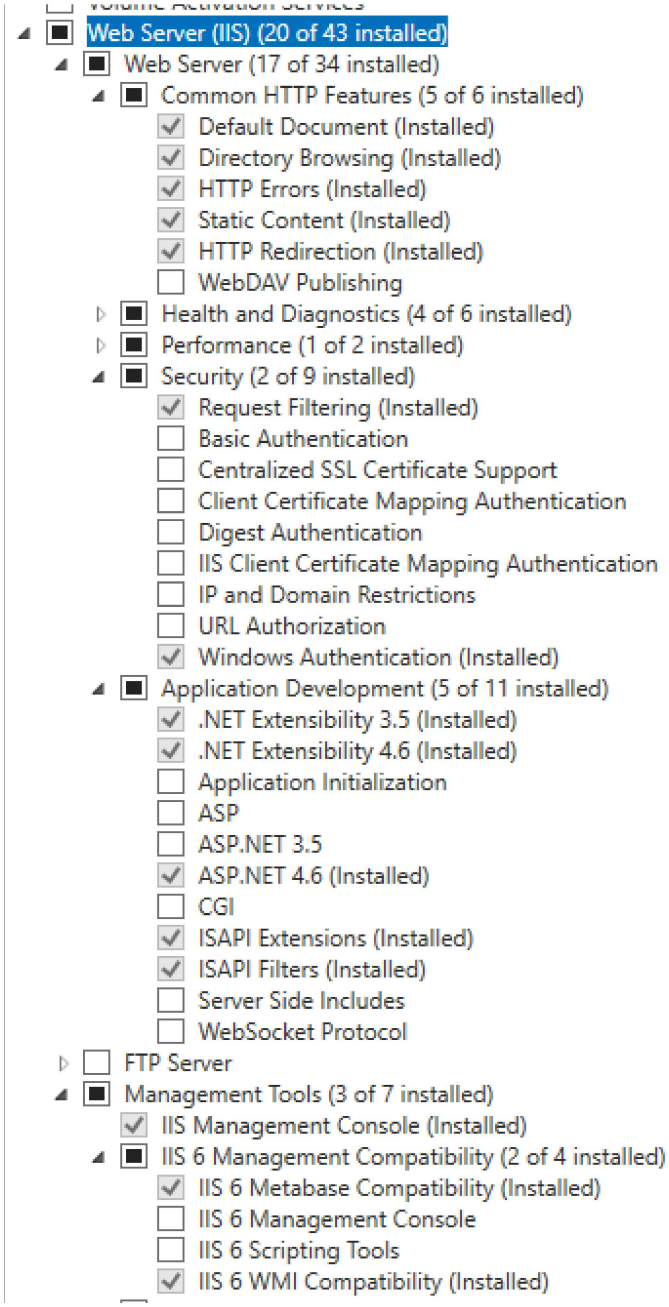
Choose the two we just created and select **OK.**

NDES ROLE (NDES)

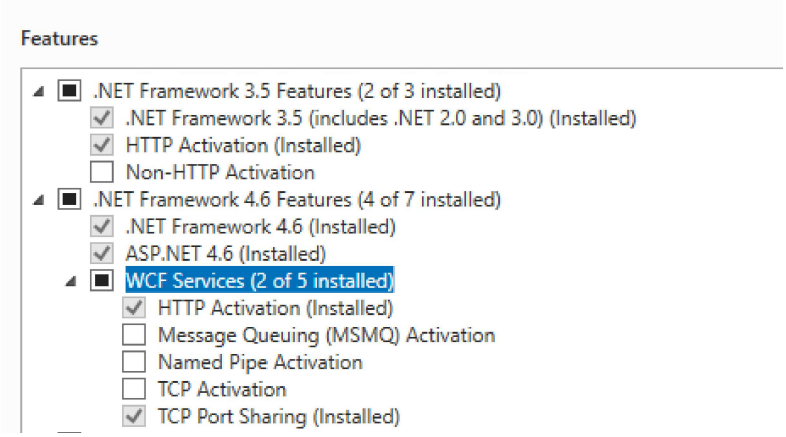
Log into the NDES server you created. Launch Server Manager and click **Manage -> Add Roles and Features.** Add the **Active Directory Certificate Services** and **Web Server (IIS)** roles.



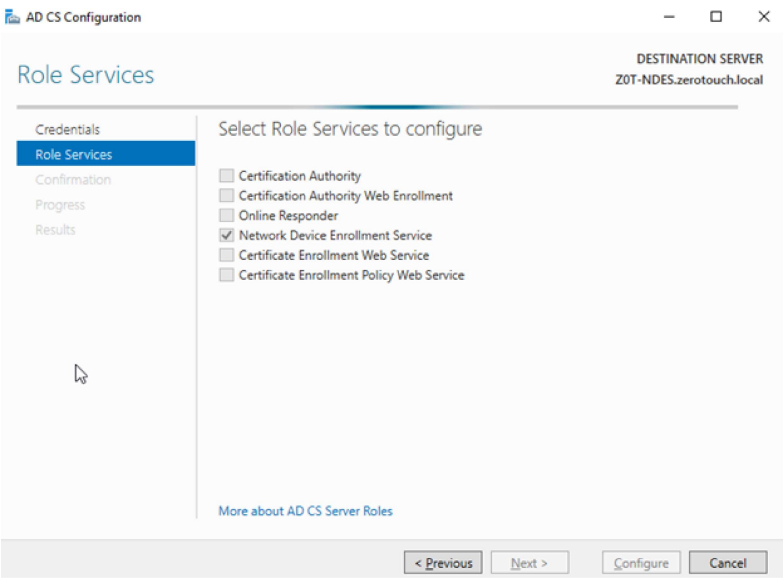
Web Server needs everything and the kitchen sink, so make sure these are selected:



On the “Features” menu, check the following options:



On the menu for role services for Active Directory Certificate Services, uncheck all but **Network Device Enrollment Service.**



When prompted for the Service Account, enter the NDES user we created in the first section. When prompted for the certificate authority, choose

Computer name and enter the FQDN of your CA.

Click **Next** until the role has been installed. Restart your NDES server.

Congratulations- you've completed part 1. Better get some rest before part 2.

PREVIOUS

NDES and SCEP for Intune: Part 2

NEXT

Troubleshooting Hardware Failure