

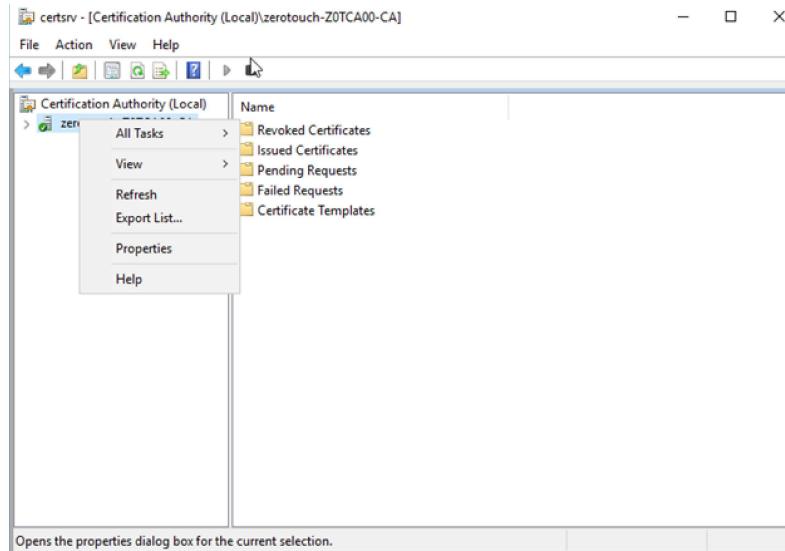


STEVE WEINER · MAY 10, 2021

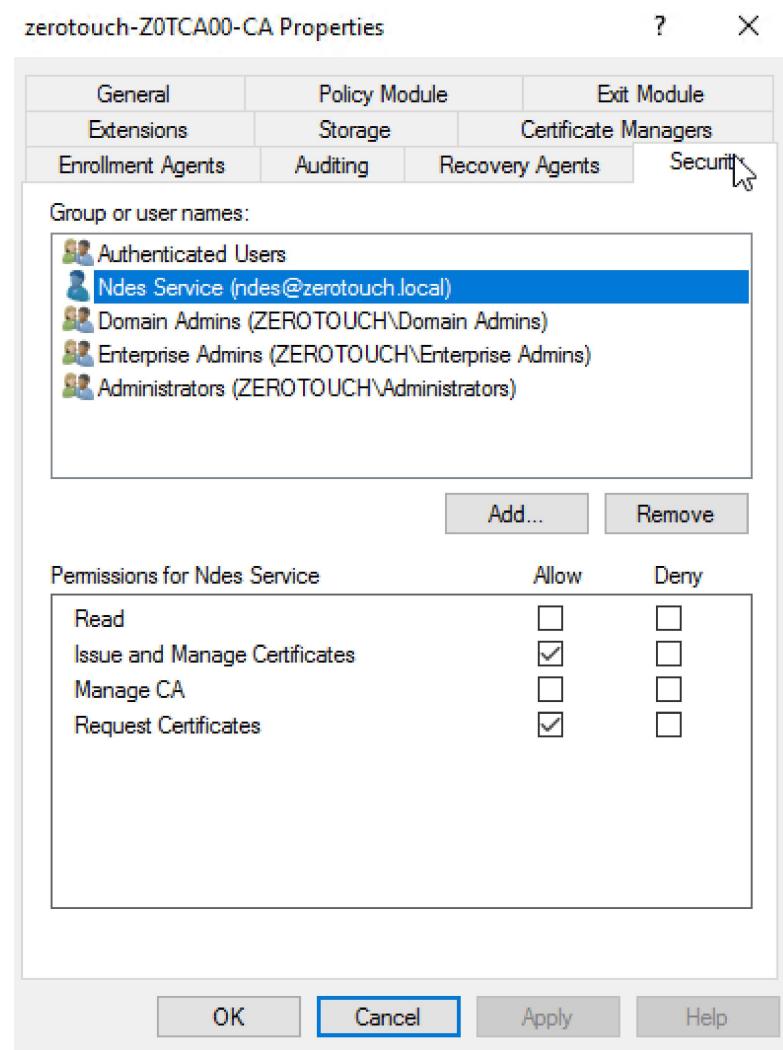
NDES and SCEP for Intune: Part 2

Before we move on to Part 2,
there are two tasks I should
have included in Part 1.

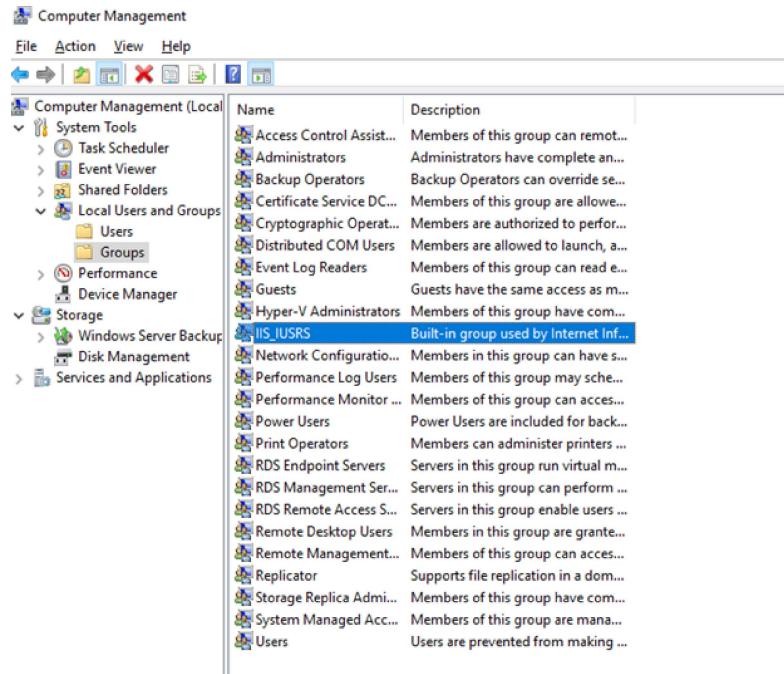
First, we need to give the NDES
service account permissions to
request and issue certificates.
Log into the CA and launch the
Certification Authority
console. Right click on the CA
and click **Properties**.



On the “Security” tab, add the NDES account and check the boxes for **Issue and Manage Certificates** and **Request Certificates** permissions.



Head back to the NDES server.
Launch “Computer
Management” and add the
NDES account to the
IIS_IUSRS group.



All good? Terrific. On to Part
2...

Part 2: IIS Filters, Azure App Proxy, and the Certificate with the external DNS

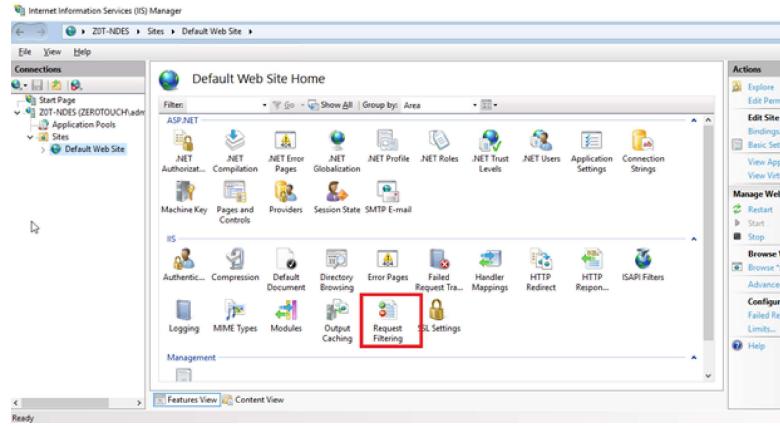
CONFIGURE REQUEST FILTERING (NDES)

Log into the NDES server and launch the IIS Manager.

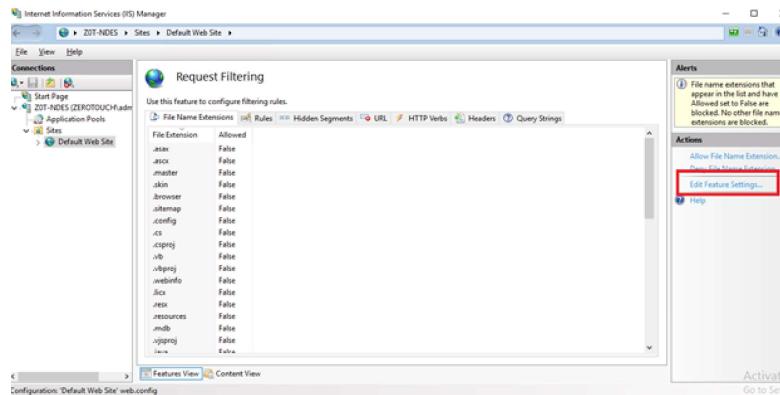
Navigate to the “Default Web

Site” and select Request

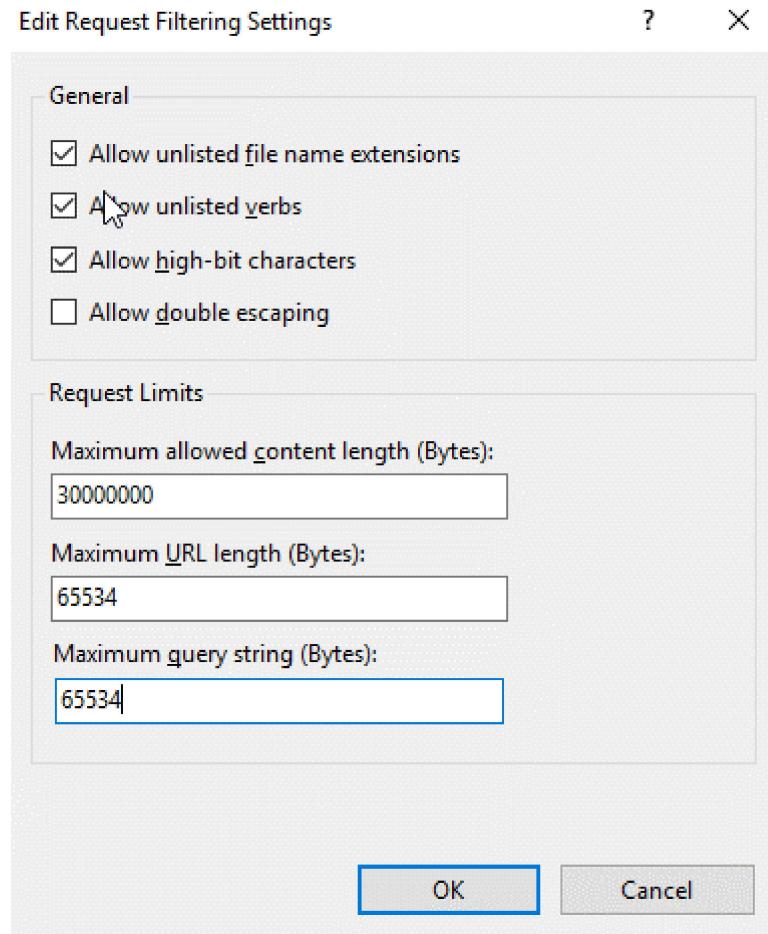
Filtering.



Click Edit Feature Settings...



Change the value for
Maximum URL length (Bytes)
and Maximum query string
(Bytes) to 65534.

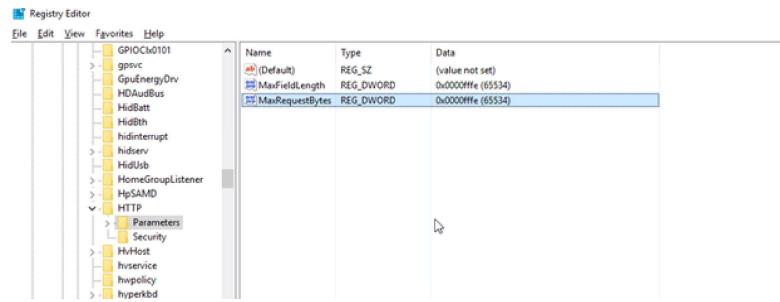


The requests for certs coming through the Intune connector can get quite lengthy, and we don't want them getting stuck at the door with the bouncer.

To further solidify those values, open the Registry Editor on the NDES and navigate to **COMPUTER\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters** and add the following DWORD values:

- Name: *MaxFieldLength*
 - Base: Decimal
 - Value data: 65534

- Name: *MaxRequestBytes*
 - Base: Decimal
 - Value data: 65534



DOWNLOAD THE AZURE APP PROXY CONNECTOR (AZURE AD)

Login to Azure AD with global administrator rights at
<https://aad.portal.azure.com>
 and navigate to **Azure Active Directory -> Application Proxy -> Download connector service.**

Accept the terms and download.

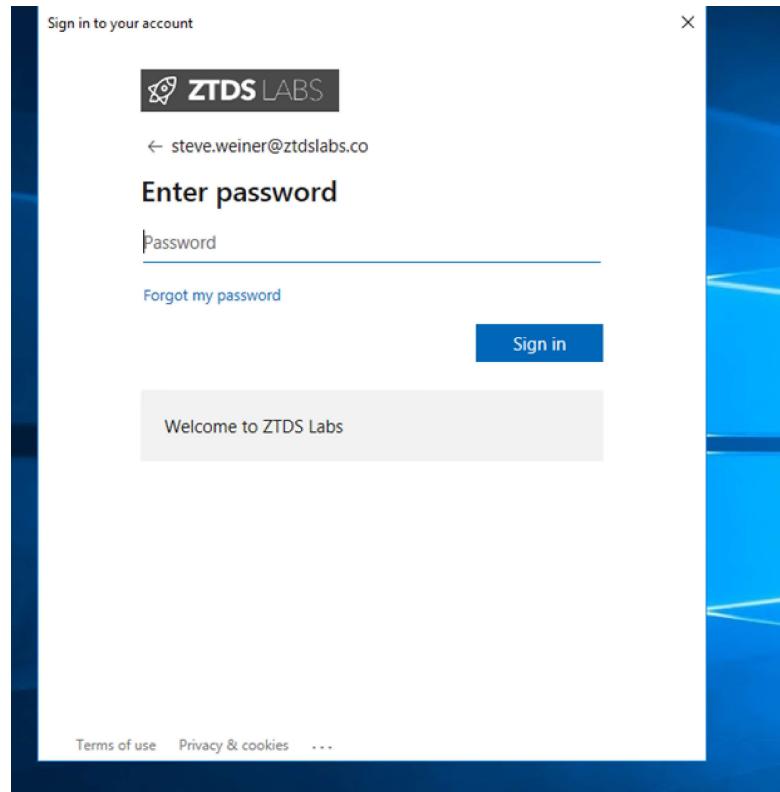
The screenshot shows the Azure Active Directory admin center with the 'Application proxy' section selected. A table lists a single connector named 'Default'. The connector's IP address is 71.172.1.115, it is marked as 'Active', and it is associated with the 'North America' region.

INSTALL THE AZURE APP PROXY CONNECTOR (NDES)

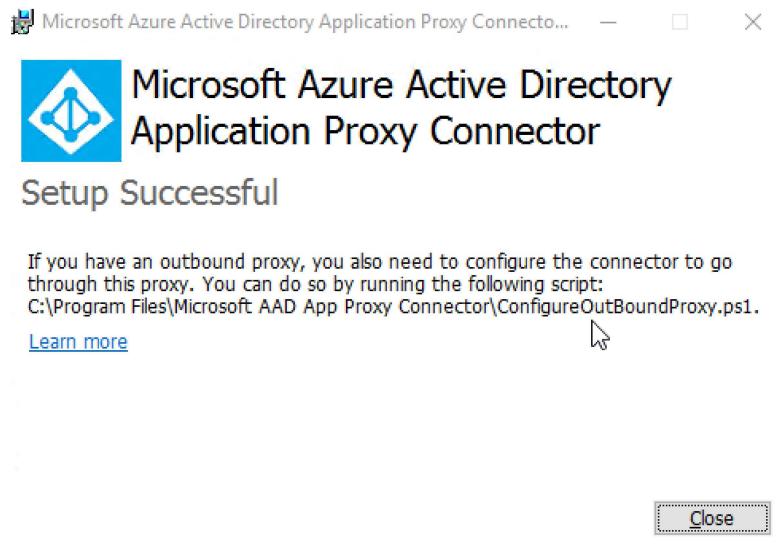
On the NDES server, launch the *AADApplicationProxyConnectorInstaller.msi*. Agree to the terms and click “Install”.



When prompted, login with Azure AD global administrator rights.



Assuming you know the
password, you should be all set.



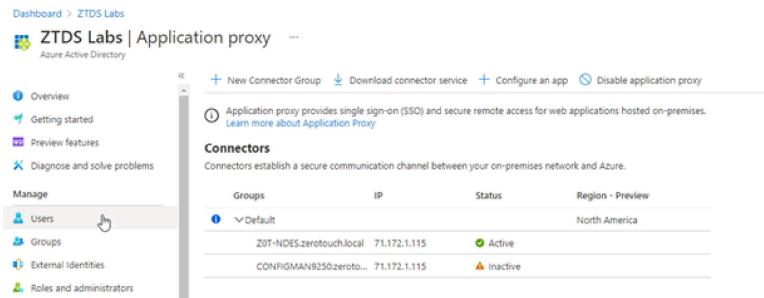
Go ahead and close the
installer.

ADD THE ON-PREMISE APPLICATION (AZURE AD)

Log back into

<https://aad.portal.azure.com>

and make your way back to the app proxy. You should now see the healthy connection as active and pointing to your NDES server.



The screenshot shows the 'ZTDS Labs | Application proxy' page in the Azure Active Directory portal. The left sidebar has links for Overview, Getting started, Preview features, Diagnose and solve problems, Manage (with sub-links for Users, Groups, External identities, and Roles and administrators), and a 'New Connector Group' button. The main content area has buttons for New Connector Group, Download connector service, Configure an app, and Disable application proxy. A note says 'Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises.' Below this is a 'Connectors' section with a table:

Groups	IP	Status	Region - Preview	
Default	ZOT-NDES.zerotouch.local	71.172.1.115	Active	North America
	CONFIGMAN9250.zeroto...	71.172.1.115	Inactive	

Select + Configure an app.

Give the application a friendly name (I chose “SCEP”) and then specify the <<http://FQDN>> of your NDES.

The screenshot shows the configuration interface for adding an on-premises application. Key settings include:

- Name:** SCEP
- Internal Url:** http://z0tndes.zerotouch.local
- External Url:** https://httpz0tndeszerotouchlocal-m365x934446.msappproxy.net/
- Pre Authentication:** Passthrough
- Connector Group:** Default - North America
- Additional Settings:**
 - Backend Application Timeout: Default
 - Use HTTP-Only Cookie: Yes
 - Use Secure Cookie: Yes
 - Use Persistent Cookie: Yes
- Translate URLs In:**
 - Headers: Yes
 - Application Body: No

Azure will automatically
concatenate the external URL.
Copy that into a notepad or
sticky cause we're going to need
it a few times later.

Set “Pre-Authentication” to
Passthrough. Leave the other
values as defaults. Click **+Add**
when you’re done to save the
application.

*TROUBLESHOOTING TIP

Be sure the internal URL name
does not have any wrong
characters or spelling errors, as
that will ruin the whole thing.
Like the brilliant mind that I

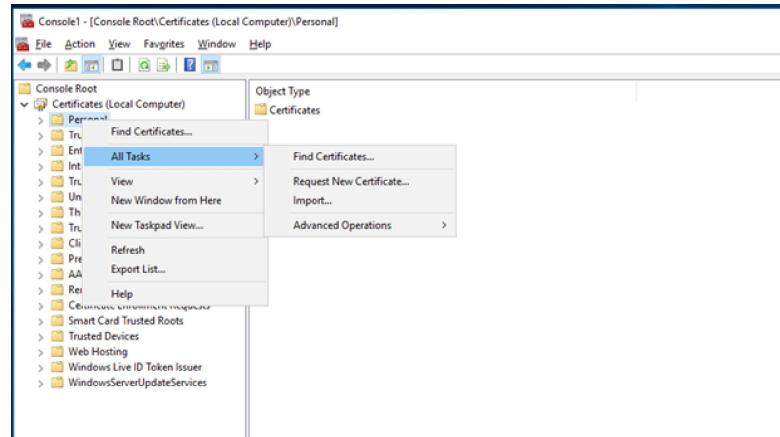
am, I initially entered my internal URL as **http://z0tndes.zerotouch.local** and in reality, it is **http://z0t-ndes.zerotouch.local.**

That lack of a hyphen sank the whole ship later until I went back and corrected it.

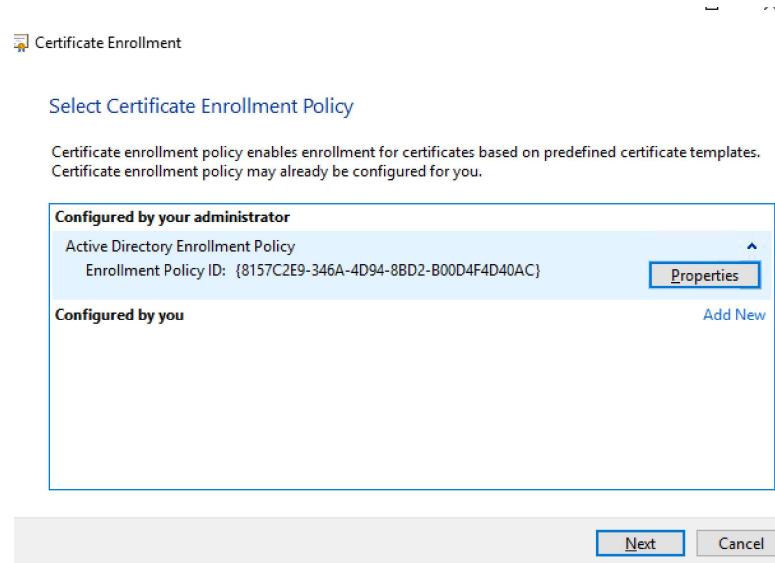
REQUEST THE NDES CERTIFICATE (NDES)

We're going to use the same client/server authentication template we made originally, based off the web server template, to authenticate both the NDES to the CA and for the Intune SCEP connector in Part 3.

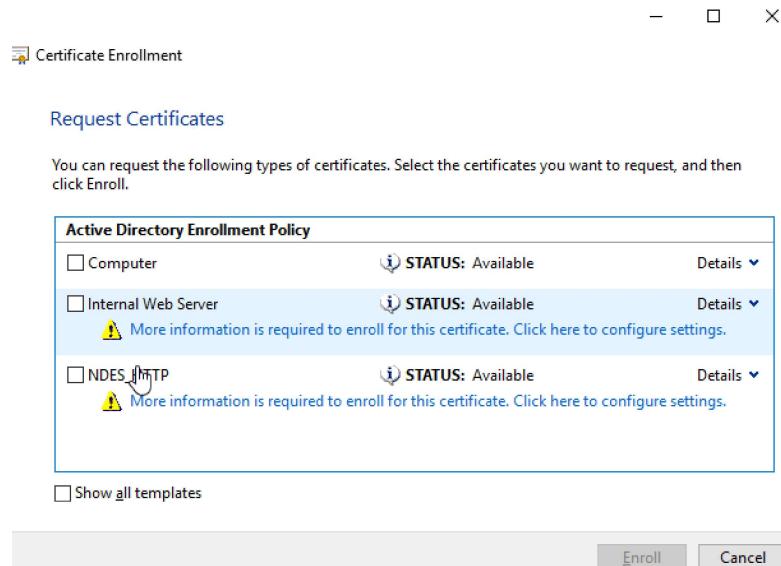
On your NDES server, launch MMC and add the local computer certificate snap in. Right click on “Personal” and select **All tasks -> Request New Certificate.**



Select “Active Directory Enrollment Policy” and click Next.

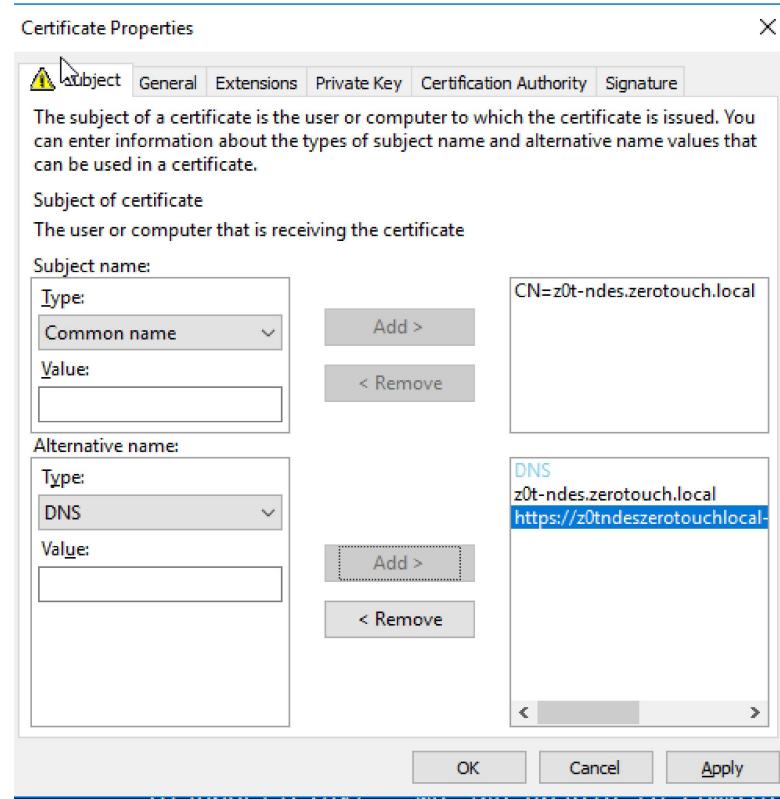


Find the NDES template you made and click the “More information is required...” link

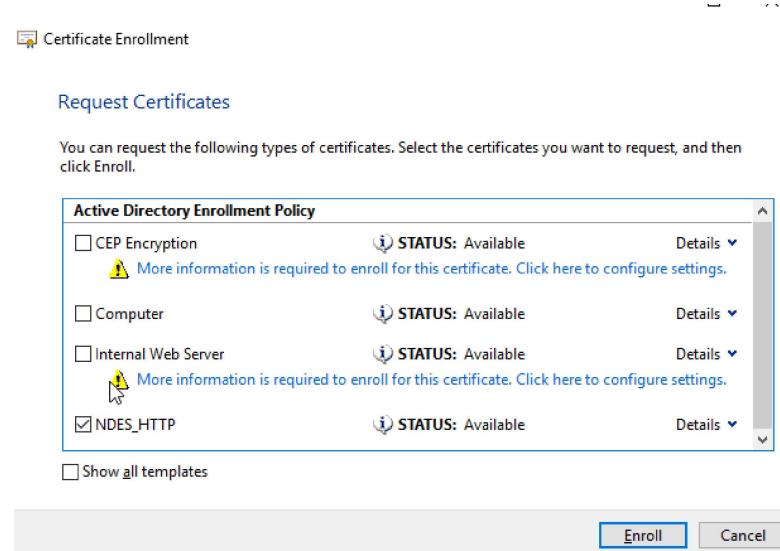


For the “Subject name”, select **Common name** from the drop down. Add the FQDN of your NDES server as the value and click **Add>**

For “Alternative name”, select **DNS** from the drop down. Again, add the FQDN as the value, and then add the external URL of the app proxy from the previous step as the second value. It should look like this:



Select **OK**, and then check the
box next to the template and hit
Enroll.



The NDES server will now have
the client/server authentication

certificate in the “Personal” certificate store.

Alright, I think we’ve all earned a little rest before Part 3. See you soon.



PREVIOUS

NDES and SCEP for Intune: Part 3

NEXT

NDES and SCEP for Intune: Part 1