**Intune NDES Guide**

## **Introduction**

NDES (Network Device Enrolment Service) is a feature of AD Certificate Services (CS) and provides an implementation of the Simple Certification Enrolment Protocol (SCEP).The NDES Connector basically allows the AD Certificate Services to validate if the device is trusted/authorized for certificate issues (as opposed to authentication which is handled in SCEP).

## **Purpose**

The purpose of the document is to provide Intune NDES (Microsoft Network Device Enrollment Service) install instruction, Prerequisites, and procedures to the Support Team.

This document will be a reference guide for Intune team members to handle SCEP certificate related issue and future upgrades

## **Scope**

This section describes an overview of the scope of the document. The document is of below list are the areas covered within this document

* Microsoft Network Device Enrollment Service
* Prerequisites
* NDES Role setup
* NDES Post Deployment Configuration
* Microsoft Intune Certificate Connector
  1. Prerequisites
* Ensure to have NDES server RDP and admin access
* Please have Latest AD DS and AD CS servers list from required stakeholders
* Network firewall port opening between NDES server to AD DS, AD CS and Microsoft services. Please refer the below URL

We allowed firewall port mentioned in the article below along with list we have in this document.

[**https://support.microsoft.com/en-in/help/179442/how-to-configure-a-firewall-for-domains-and-trusts**](https://support.microsoft.com/en-in/help/179442/how-to-configure-a-firewall-for-domains-and-trusts)

<https://learn.microsoft.com/en-us/mem/intune/protect/certificate-connector-prerequisites>

* Ensure required SSL certificates are available and active, if not ensure to renew or create with respective template
* Service Account is required for NDES configuration (New account created ex: SVC\_INTUNE\_NDES).
* Service Account should be allowed **“Allow Login Locally, Log on as a service and Log on as batch job policies**” via Local Security Policy on server
* Ensure **SVC\_Intune\_NDES account and NDES server “NDESxx.domain.com h**aving READ and ENROLL permission on NDES\_Server\_SSL template

Graphical user interface, application

Description automatically generated

* Ensure **SVC\_Intune\_NDES account and NDES server “NDESxx.domain.com** having READ and ENROLL permission on NDES certificate template
* Add NDES service Account into IIS\_USRS and Administrator group
* Please have Domain Enterprise Admin account for login or EA privilege with logon account
  1. NDES Role setup

1. Please login NDES server “**NDESxx.domain.com,** ensure you have required privilege ( Enterprise Admin or Domain Admin) to configure the NDES.
2. Launch Server Manager and then use the Add Roles and Features Wizard to install NDES
3. In the Wizard, select Active Directory Certificate Services to gain access to the AD CS Role Services. Select Network Device Enrollment Service, uncheck Certification Authority, and then complete the wizard

Graphical user interface, application

Description automatically generated

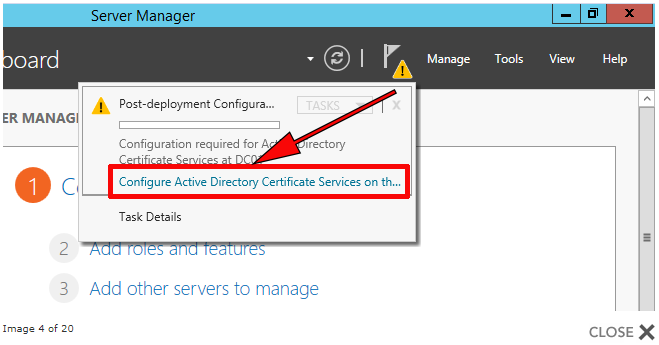
1. When NDES role is added to the server, the wizard also installs IIS. Confirm that IIS has the following configurations:

* Web Server > Security > Request Filtering
* Web Server > Application Development > ASP.NET 3.5
* Installing ASP.NET 3.5 installs .NET Framework 3.5. When installing .NET Framework 3.5, install both the core .NET Framework 3.5 feature and HTTP Activation.
* Web Server > Application Development > ASP.NET 4.7.2
* Installing ASP.NET 4.7.2 installs .NET Framework 4.7.2.
* When installing .NET Framework 4.7.2, install the core .NET Framework 4.7.2 feature, ASP.NET 4.7.2, and the WCF Services > HTTP Activation feature.
* Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility.
* Management Tools > IIS 6 Management Compatibility > IIS 6 WMI Compatibility
* On the server, add the NDES service account as a member of the local IIS\_IUSR group.
* On the NDES server “NDES.EXAMPLE.COM” run the following command in an elevated command prompt. The following command sets the SPN of the NDES Service account:

**“setspn -s http//NDES.EXAMPLE.com EXAMPLE.COM\Svc\_intune\_ndes”**

* 1. NDES Post Deployment Configuration

1. From within Server Manager, launch the post deployment configuration wizard. Ensure to login with Domain Enterprise Admin account to proceed the post deployment configuration. (LOGIN account was provided with EA access by AD team for this installation)



1. Next,

Graphical user interface, text, application

Description automatically generated

1. Then Select the EXAMPLE.COM Issuing server which is “CertficateIssueing.exmaple.com”.
2. Next
3. Select the “Country region “

Graphical user interface, text, application, email

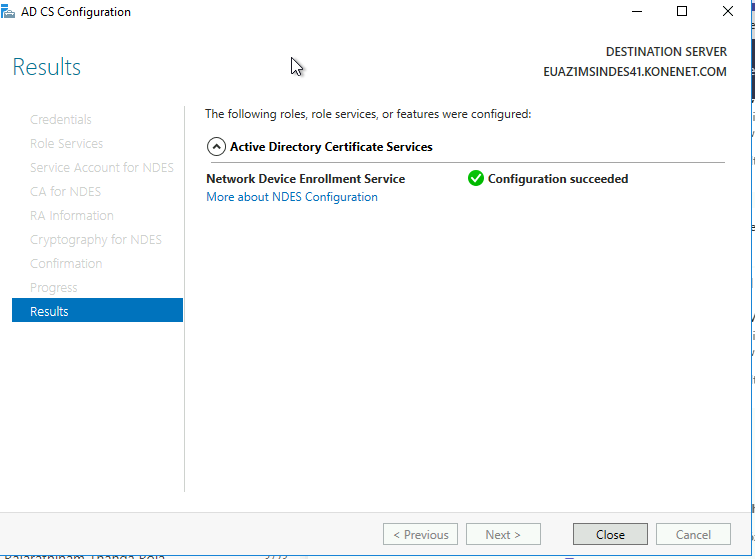
Description automatically generated

1. Next
2. Accept the defaults > Next

Graphical user interface, text, application

Description automatically generated

1. Verify the configuration and Click Configure .
2. Once the configuration is successful, Click Close



* 1. NDES Server Registry Changes

Now we need to let NDES know what certificate template to use when it reaches out to the Certificate Authority to request certificates. We have to make these changes in the newly created MSCEP.

1. Open registry with Administrator privilege and navigate to :

HKLM/Software/Microsoft/Cryptography/MSCEP

1. On the right hand side update the Template values into “\_Intune\_Managed\_Devices” like below.

Graphical user interface, table

Description automatically generated

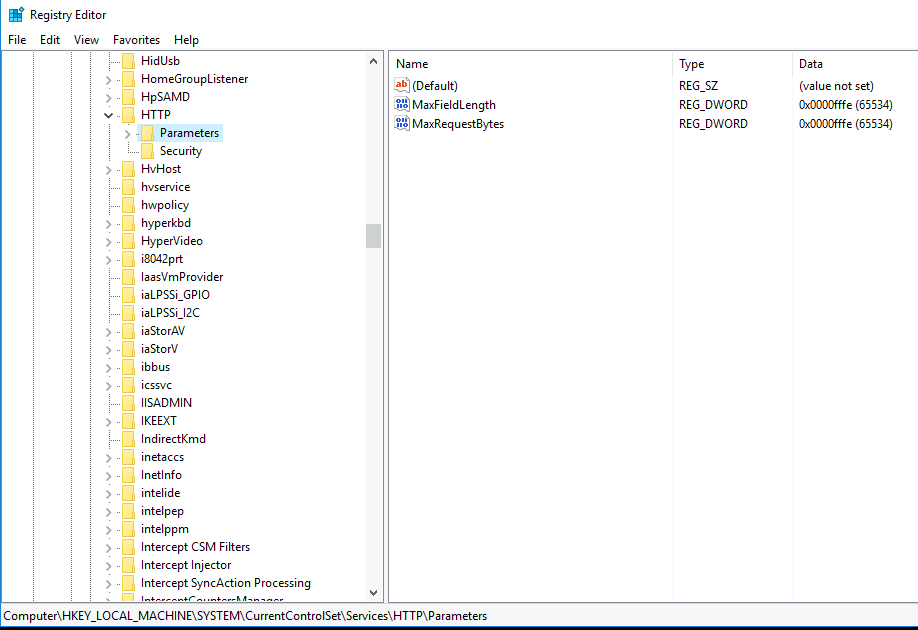
1. Then Navigate to HKLM/SYSTEM/CurrentControSet\Services\

HTTP\Parameter and

Add these two DWORD value registry keys, both with a decimal value of 65534:

MaxFieldLength

MaxRequestBytes



1. Then restart the server.
   1. NDES IIS Configuration

Please do ensure NDES SSL certificates NDES.EXAMPLE.COM IS valid.

Then Access IIS manager 🡪 Default Website🡪SSL Certificate 🡪 Binding🡪then select https🡪 and select NDES IIS Certificate and click OK

Graphical user interface, text, application, email

Description automatically generated

1. Microsoft Intune Certificate Connector

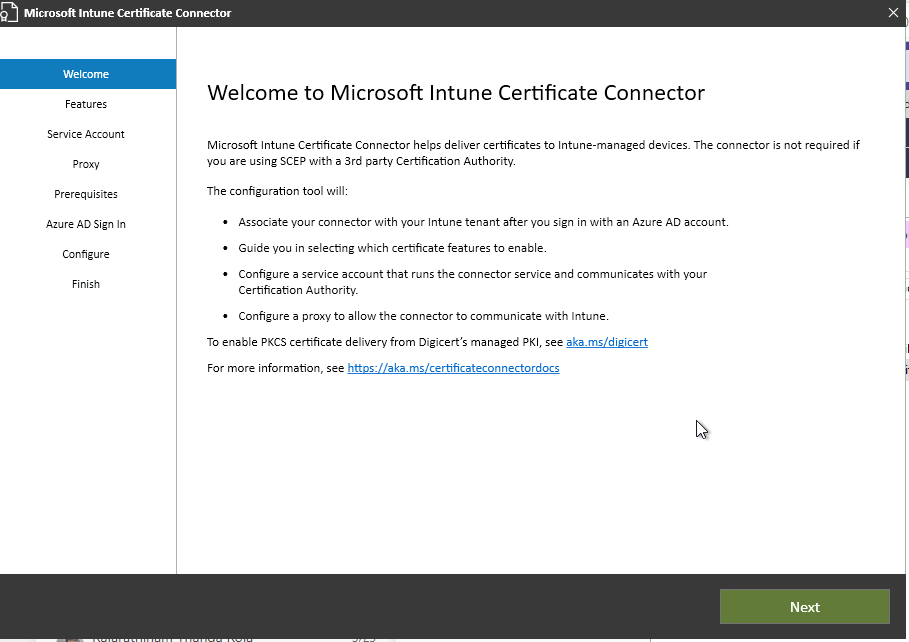
The certificate connector is software to be installed on an on-premises server to help deliver and manage certificates for our Intune-managed devices.

* 1. Install and Configure Intune Certificate Connector

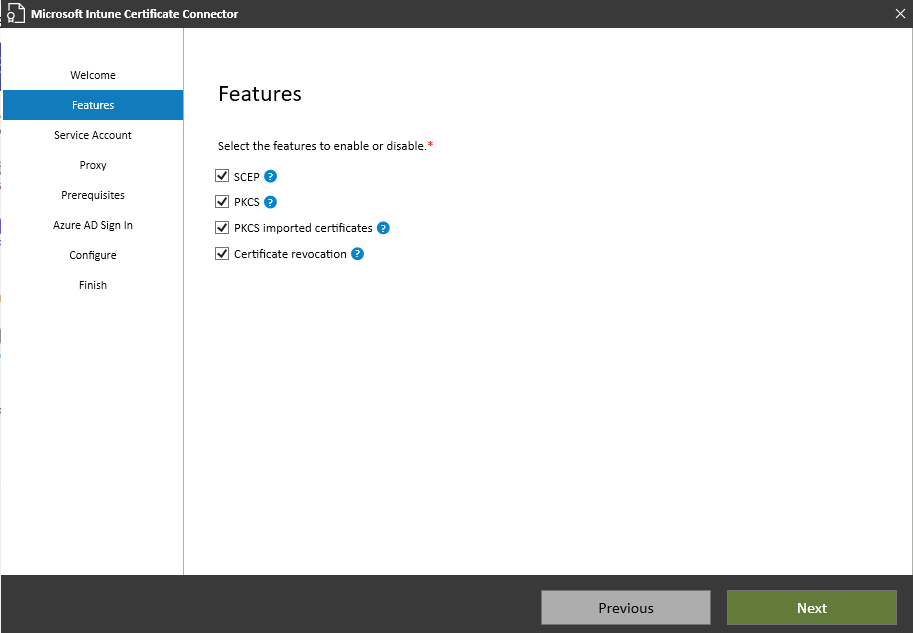
The Intune Certificate connector can be downloaded from Intune portal 🡪 **Tenant administration** > **Connectors and tokens** > **Certificate connectors** > **Add**.

To configure Intune Certificate Connector , we must to have AD account with Global Admin Privilege to sync with Azure AD

1. Once Application is downloaded and installed launch the Intune Certificate connector with “Run As Administrator”



1. Click Next
2. Select required Features on below screen, Ensure SCEP and PKCS



1. Select Service Account to configure Connector

Graphical user interface, text, application

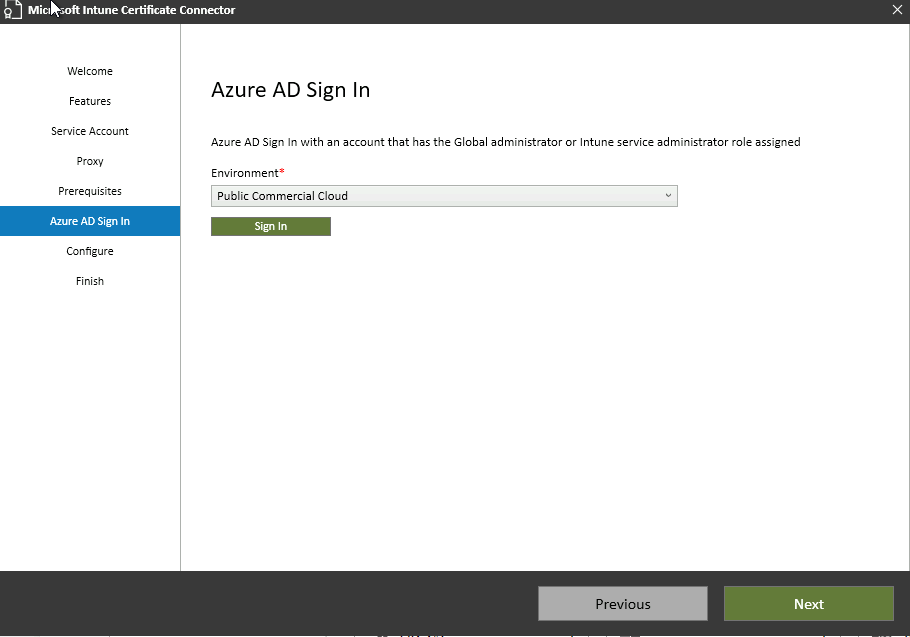
Description automatically generated

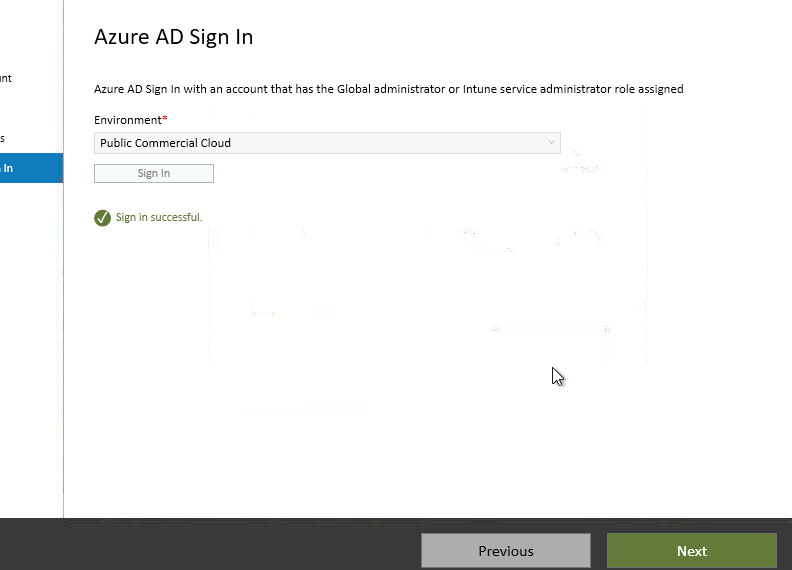
1. Click Next, Add Proxy details based on infra update.
2. Then verify prerequisites is completed successfully, Then click Next

Graphical user interface, text, application, email

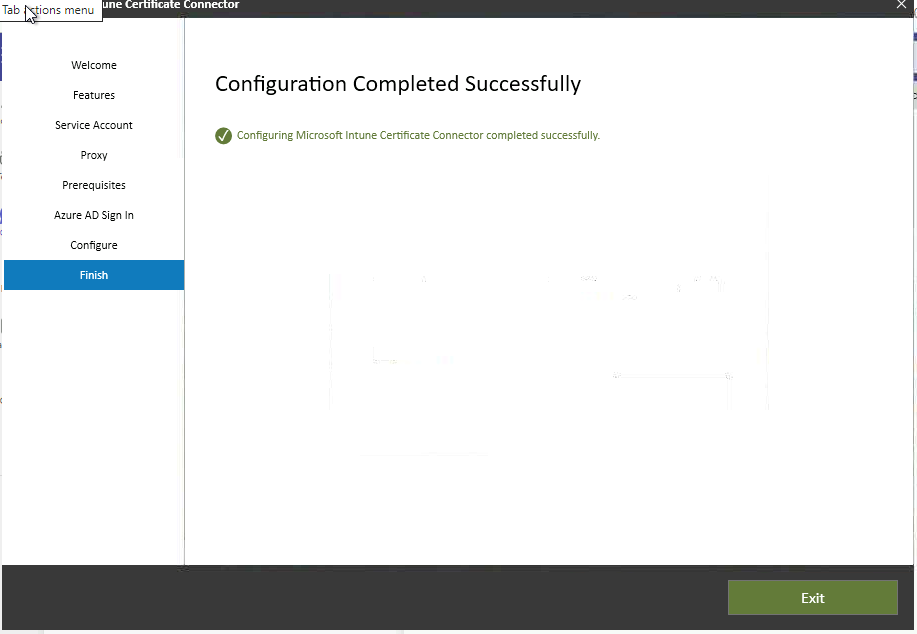
Description automatically generated

1. Select Public Commercial Cloud then click sign in. Please do ensure that you are login with AD account which is having Global Admin privilege with Intune License.



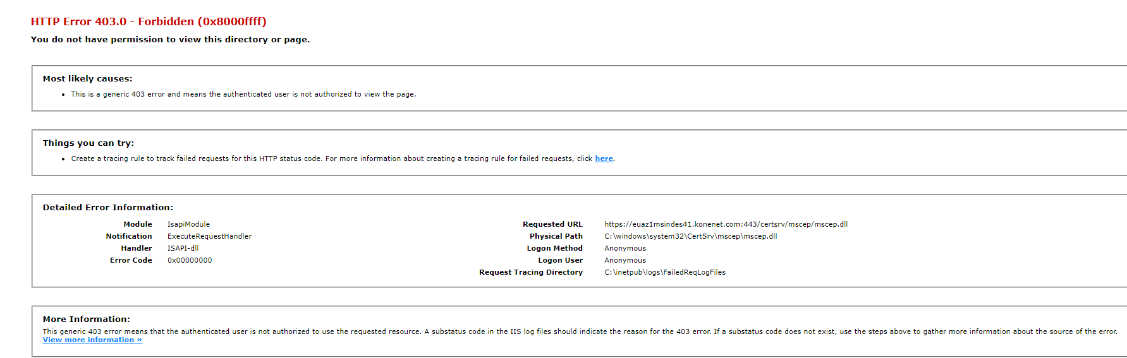


1. Once the signing is successful, Click Next
2. Then configuration part will be completed successfully and Exit.



1. Then try to access below url, the output should be like below

<http://ndes.example.com/certsrv/mscep/mscep.dll>



1. Then do the necessary configuration in Intune side and test the certificat
2. The completed NDES configurations is :

Install-AdcsNetworkDeviceEnrollmentService -Force -ServiceAccountName "example.com\SVC\_INTUNE\_NDES" -ServiceAccountPassword "System.Security.SecureString" -RAName "NDES-MSCEP-RA" -RACountry "FI" -SigningProviderName "Microsoft Strong Cryptographic Provider" -SigningKeyLength "2048" -EncryptionProviderName "Microsoft Strong Cryptographic Provider" -EncryptionKeyLength "2048" -CAConfig "CAIssueingServer.example COM\_Issuing\_CA2"

1. Microsoft Intune Connector should be updated to the latest version every six months, either automatically or manually.

SOME REFRECE:

<https://www.getrubix.com/blog/ndes-and-scep-for-intune-part-1>

<https://www.getrubix.com/blog/ndes-and-scep-for-intune-part-2>

<https://www.getrubix.com/blog/ndes-and-scep-for-intune-part-3>