IDENTITY INTUNE ENTERPRISE MOBILITY ARCHITECTURE SECURITY

Intune NDES & SCEP explained

by **Niklas Tinner** 9 months ago 7 MIN READ

Introduction

Introduction

This post is intended to give a technical concept guidance with a focus on security about **certificate deployment** with **Intune** (cloud-only/Azure AD only clients) and **NDES + SCEP**. (not PKCS with PFX)

This scenario is applicable, if you run an internal certificate authority in your domain and want to issue internally signed certificates to clients that are in any internal or external network. If you don't require internally signed certificates, you can also consider a cloud certificate authority such as SCEPman.

From an identity security perspective, leveraging certificates, can be used for **client authentication** or **user authentication** to distributed resources. This is considered as strong authentication.

Use cases

Certificate-based authentication (CBA) to on-premises resources is the most common use case, such as:

- Authentication to domain server hosting services
- Network authentication to WiFi 802.1X / VPN > RADIUS server

The client will send its own signed certificate, requested through NDES & SCEP and issued by your internal CA to any authentication service which trusts your internal root CA.

Technologies

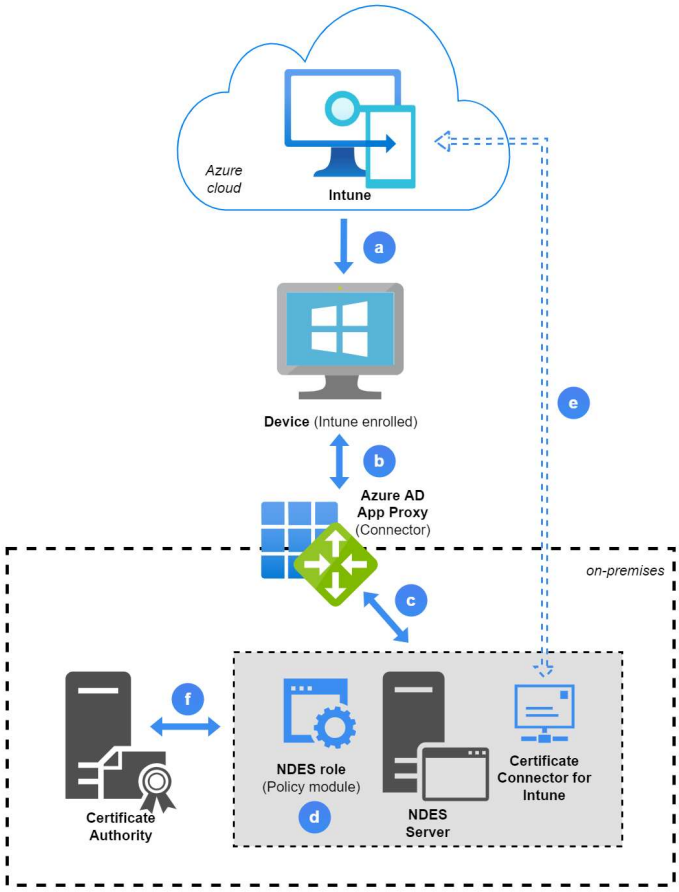
- **SCEP -** Simple Certificate Enrollmer
  Standardization of certificate mana
  exchange with certificate authority

- **NDES -** Network Device Enrollment Service: Microsoft service that allows network devices to obtain digital certificates for secure communication with other devices on a network.

Solution concept

This is a best practice SCEP/NDES architecture with Azure AD App Proxy:

a. An Intune SCEP configuration profile is applied to a device. The policy includes information to let the device create a challenge CSR (including public/private key), based on different device/user declarations. The most important information in the profile is the NDES URL.
b. The NDES URL is externally published through Azure AD App Proxy, the device will retrieve the URL and send its challenge CSR request.
c. The internal URL is an IIS server, that runs on the NDES Server. Some NDES components are available through an application pool for the client request.
d. The NDES policy module verifies the request in combination with step e.
e. The certificate connector sends the challenge CSR to Intune to validate it. (signature, payload and integrity-check information) If this is successful, step f. will continue.
f. NDES contacts the CA to issue a certificate.
-> The certificate is now issued to the d



Components list

Name	Use
NDES Server	-NDES Server role -Webserver to p where clients wi -Policy module t enrolled client c

Name	Use
	-Intune Certificate Connector, for the communication between on-premises components and Intune
Intune	-Trusted root certificate device configuration profile, will be needed in the SCEP profile -SCEP device configuration profile that forms the subject request on the client
PKI	-Certificate issuance and revocation -Prepare certificate templates that will later be issued to the clients/users from NDES -There is always a 1:1 relationship between an issuing/subordinate CA and an NDES server
Reverse/Web proxy (Azure AD Application Proxy)	-Provide the NDES Webserver service to external networks, so clients can request certificates from any network

Security

PKCS/PFX vs. SCEP

Intune also supports PKCS (public key a
PFX (personal information exchange) c

This includes no NDES components and the Intune certificate connector directly communicates with the CA and requests certificates on behalf of Intune. Please consider that the private key is in transit and communication could be infiltrated.

Registration authority

A registration authority (RA) validates the requestors identity and puts another digital signature on the certificate and forwards certificate signing requests (CSR) to the CA.

Best practices

- Two-Tier PKI hierarchy and all the PKI infrastructure should be treated as TIER 0
- Deploy NDES with a group-managed service account (gMSA)
- Install the Intune Certificate Connector on the NDES server, which is separate from the CA
- The private key can not be exported from the device

Default measurements

- NDES URL can't be directly accessed
- Intune generates a custom encrypted and signed challenge blob, which is only readable by the policy module, but not by the device. The device blob includes the CSR details
- A certificate request compares bot
  the device CSR, only Intune enrolle
  validation and are issued a certifica

More information from the Microsoft Tech Community: NDES Security Best Practices | Enrollment Options for End-Entity Certificates

Prerequisites

- Healthy PKI infrastructure
- NDES Windows server + Intune Certificate Connector
- Network endpoints for Microsoft Intune must be accessible
- Access to Intune Endpoint Manager admin center
- Azure AD Application Proxy (recommended) for creating an App registration, Learn more (alternative: Web Application Proxy or Third-pary reverse proxy)
- Certificate revocation lists (CRL) from the CA must be available externally
- Workloads that leverage certificates (e.g. Wifi, VPN, RADIUS server) must be capable to check the public CRL's and verify/merge the certificate through the subject name

Privileged accounts

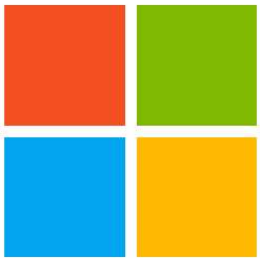
- Application Administrator role for AAD App Proxy and App registration
- Intune Administrator role, with assigned Intune license to register the Intune Certificate Connector and create certificate profiles
- Enterprise Administrator (*on-prem*) the NDES AD CS role services
- Domain account with sufficient pe CA, usually Domain Administrator

Official Microsofot prerequisites

Configure infrastructure to support SCEP certificate profiles with Microsoft Intune

To use Simple Certificate Enrollment Protocol (SCEP) with Microsoft Intune, configure your on-...

Microsoft Learn • Brenduns



Deployment in a nutshell

A straight forward functional tutorial is found on the Tech Community.

Prerequisites

- Create a service account or gMSA
- Add the NDES service account to *IIS_IUSRS* local group on NDES server and make sure the same account can request certificates on the Issuing CA
- Set the service principal name (SPN) on the NDES server
- Azure AD App Proxy deployed and functional

Key steps

1. **Create certficate templates**

Basically two templates need to be crea

- Client authentication - this will be later used to issue to the end-entities/devices.
- Web server - is used for the Web (NDES) server to secure the NDES URL with *https*.

3. **Install the NDES server and service**

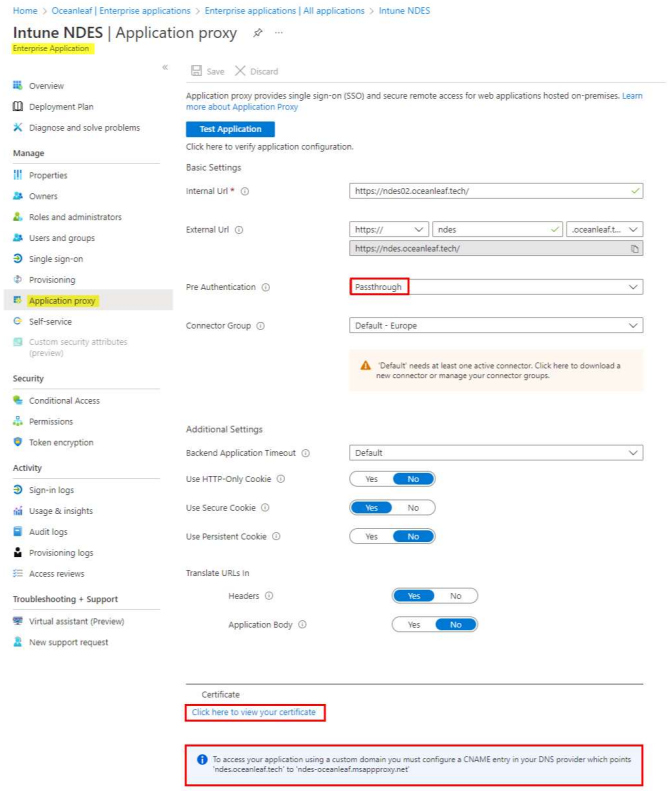
Install the NDES roles and configure it: choose an issuing CA and set RA details and cryptography settings.

4. **Configure the Web server**

Install the Internet Information Service (IIS) role, request a certificate, based on the Web server template and export it with the private key. (This file needs to be uploaded to the App registration. Also configure the bindings with this certificate. Furthermore adjust the maximum URL length and query string.

5. **Create the App registration**

Create an App registration, specify the internal NDES URL, external URL, set the pre-authentication to *passthrough* and upload the Web server certificate (including the private key). Also create a CNAME to point to the *msappproxy*-URL.



6. **Intune Certificate connector**

Download the connector, install it on the NDES server and configure it with *SCEP* and *Certificate revocation* the corresponding accounts.

8. **Deploy the trusted certificate**

Trusted root/intermediate certificate
Platform: Windows 10 and later
Profile type: Templates
Template name: Trusted certificate

Upload both the Trusted root and inter
profiles only needed in a two-tier hiera

7. **Intune SCEP profile**

SCEP

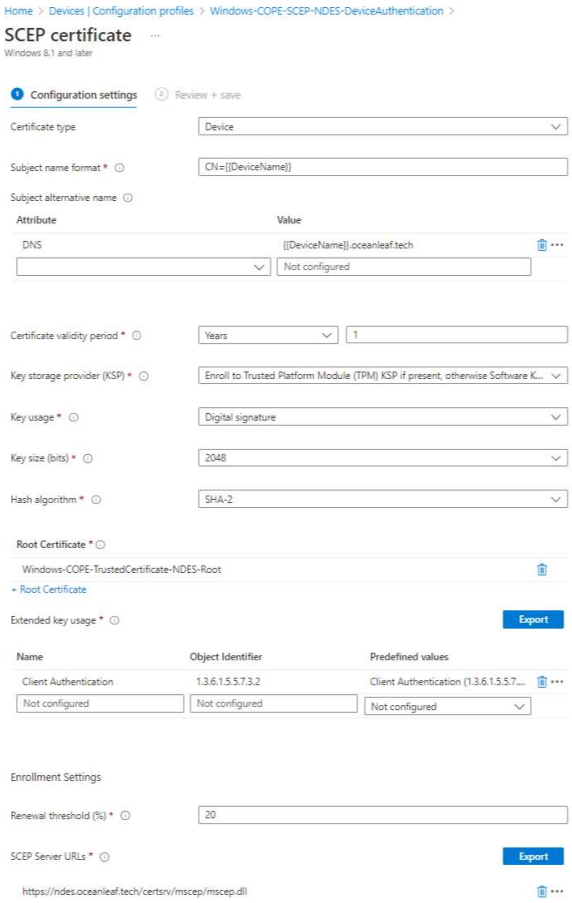
Platform: Windows 10 and later

Profile type: Templates

Template name: SCEP certificate

Configure the profile (view image for a sample). It is important that you specify the the correct Root Certificate.

- List of available subject name formats

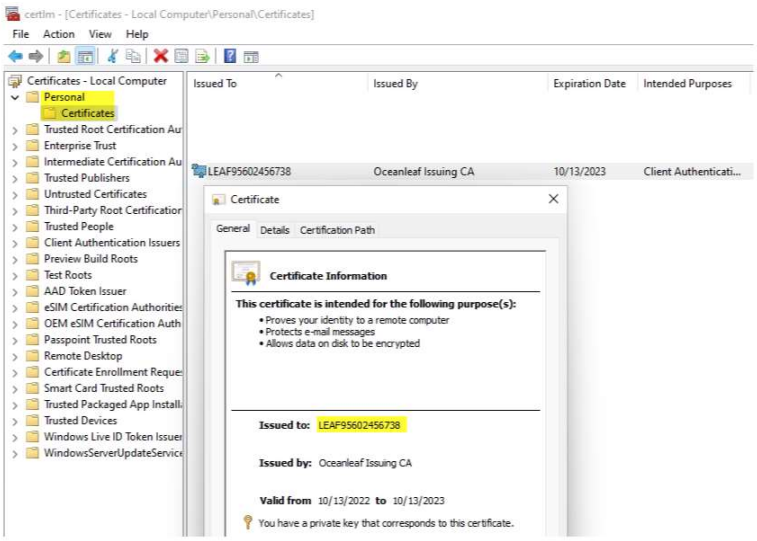


Fragments of the de

Certificates

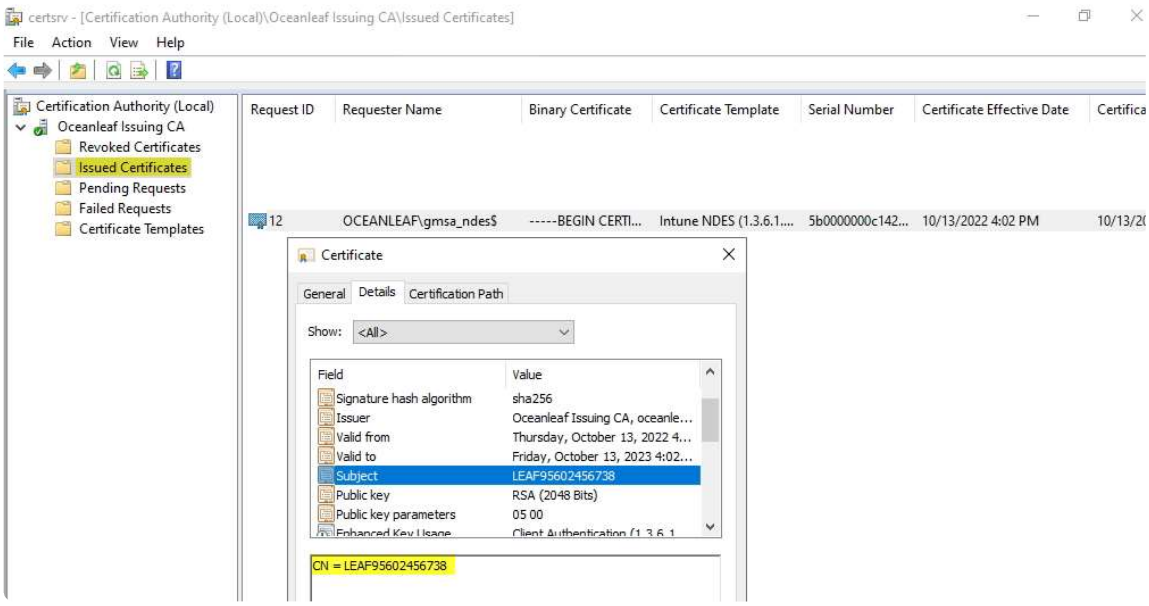
End-entity/device

Open **certlm.msc**, go to Certificates>Personal to view the requested certificate from your internal issuing CA through NDES. (Root and intermediate trusted certificates are also stored on the machine)



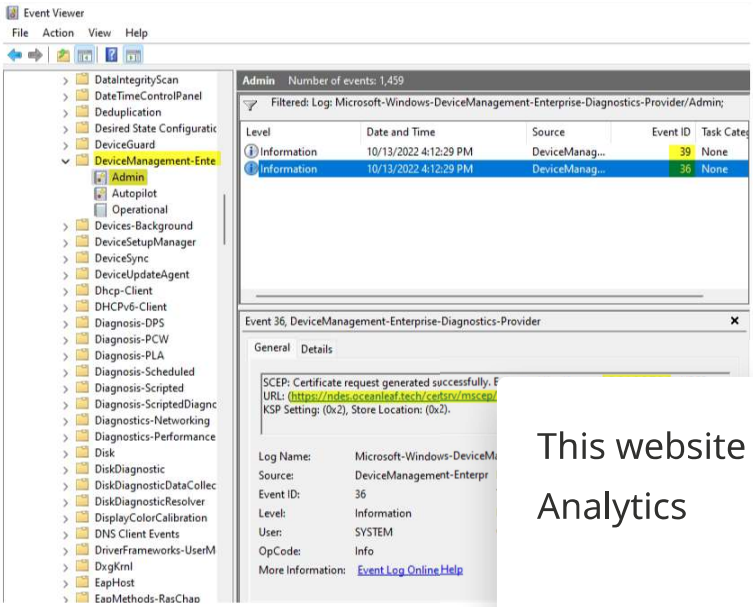
Issuing certificate authority

From **certsrv.msc**, you can check the issued certificates. There you can also see that the requestor is the NDES service account, because the request came through NDES.



Logs

From the event viewer you can find SCEP events under **Applications and Services Logs>Microsoft>Windows>DeviceManagement-Enterprise-Diagnostics-Provider>Admin**



Notes from the field

- If you use split-DNS, make sure that you also add the NDES service DNS records internally (ADDS DNS).
- Certificate chain always must be completely present on the end device.
- Use an Azure Storage account container to make CRL and public certificates (CRT) available externally.
- The certificate for the Web server is usually valid for 2 years. Afterwards it must be renewed and newly uploaded to AAD App Proxy.

Endpoint Management with Microsoft Intune

Ever wanted a full tutorial how to deal with Microsoft Autopilot Intune Technology? Well here...

Oceanleaf • Niklas Tinner

Special thanks to Nicola for explaining me these concepts! Visit his blog

READ MORE POSTS BY THI

Niklas Tinner

NEWER POST

Intune challenges (community edition)

OLDER POST

Intune change tracking (Azure Workbook)