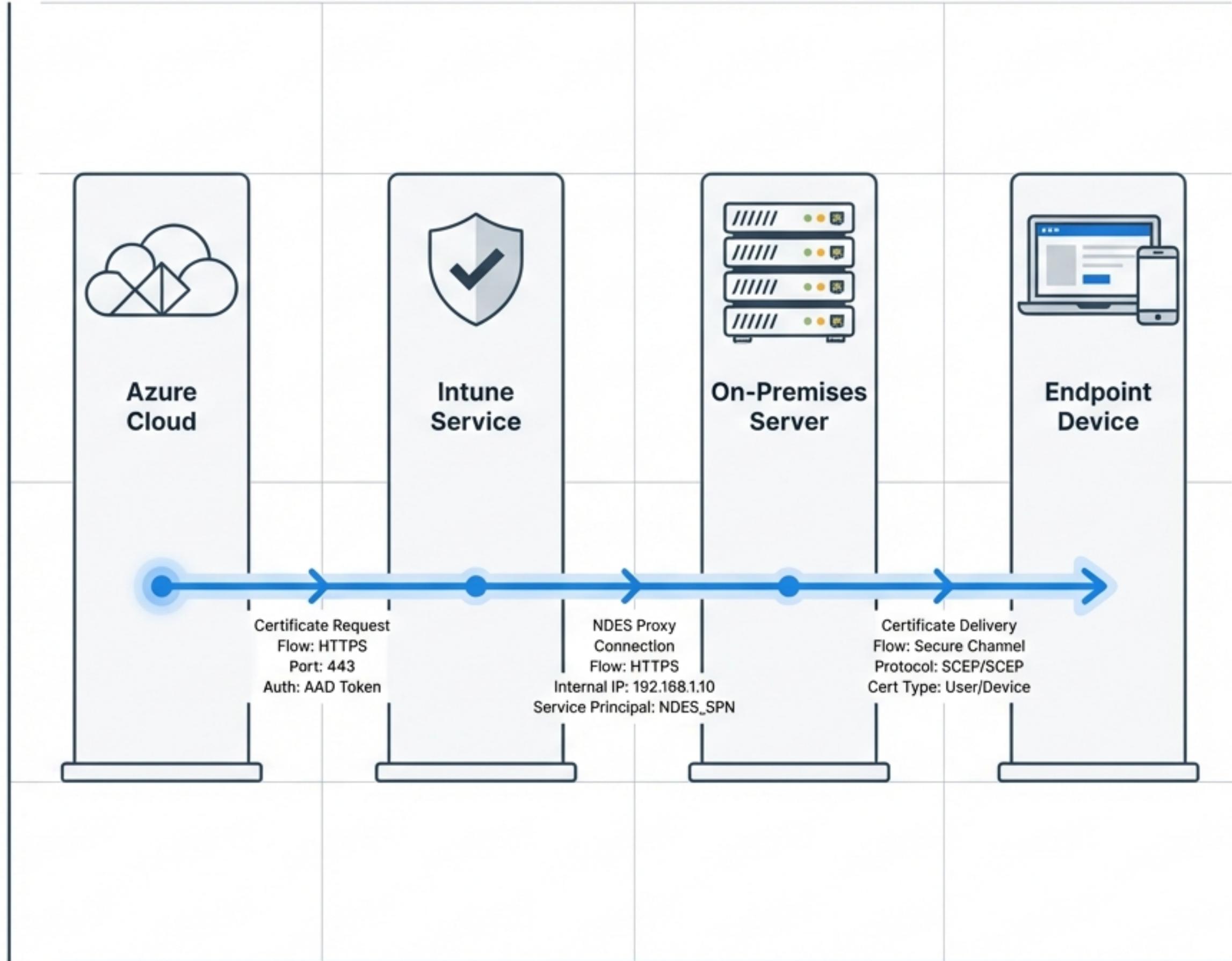


Modern PKI Architecture: Intune, NDES, & Azure App Proxy

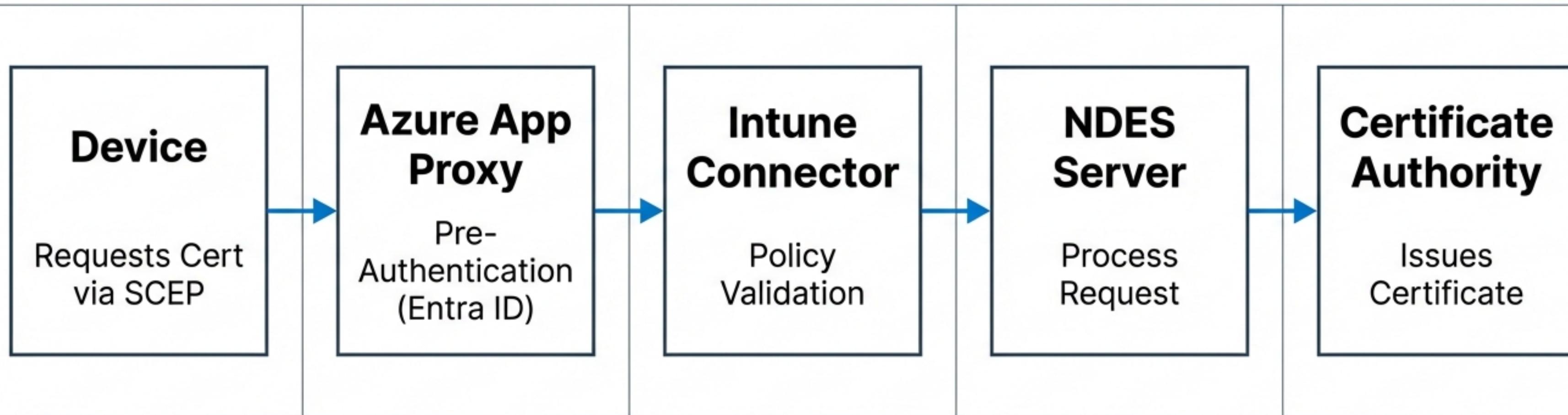
A Configuration Walkthrough
& Validation Guide for Secure
Certificate Deployment

Eliminating VPN dependencies for
certificate issuance by establishing a
secure, authenticated bridge between
Azure Active Directory and on-premises
Certificate Authorities.



The Architecture of Trust

Traffic & Trust Flow Logic



Architecture Note: Direct network exposure is eliminated. The NDES server is hidden behind the Azure App Proxy. Traffic is pre-authenticated via Entra ID before it ever touches the internal network boundary.

Identity Foundation: App Registration & Enterprise Applications

App Registration Definition

Search			
Display name ↑	Application (client) ID	Created on ↑	Certificates & secrets
N ndes-proxy	dd5c6d1e-857a-4893-9fa6-1f0ce7aee8c2	06/01/2026	Current

Service Principal Context

Name	Object ID	Application ID
N ndes-proxy	d17f0fc1-a49d-444e-95b8-478...	dd5c6d1e-857a-4893-9fa6-1f0ce7aee8c2

Critical Match: The App Registration defines identity; the Enterprise App enables operation. IDs must align.

Architecture Note: Direct network exposure is eliminated. The NDES server is hidden behind the Azure App Proxy. Traffic is pre-authenticated via Entra ID before it ever touches the internal network boundary.

The Secure Tunnel: Private Network Connectors

Private Network Connectors

Health Status	Groups	IP	Status	Country/Region
	▼ Default			
	NDES01.lab02.local	37.228.234.241	⚠ Inactive	Europe
	NDES02.lab02.local	37.228.234.241	✓ Active	Europe

Connector Details: NDES02.lab02.local

ID:
023b5807-40c5-400e-b968-9ac510062950

Status:
● Active

Machine Name:
NDES02.lab02.local

External IP:
37.228.234.241

Version:
1.5.4594.0

Connector Group:
Default - Europe

Note: Inactive status on NDES01 illustrates redundancy or maintenance. Check outbound 443 access if unexpected.

The Authority: Certificate Templates Configuration

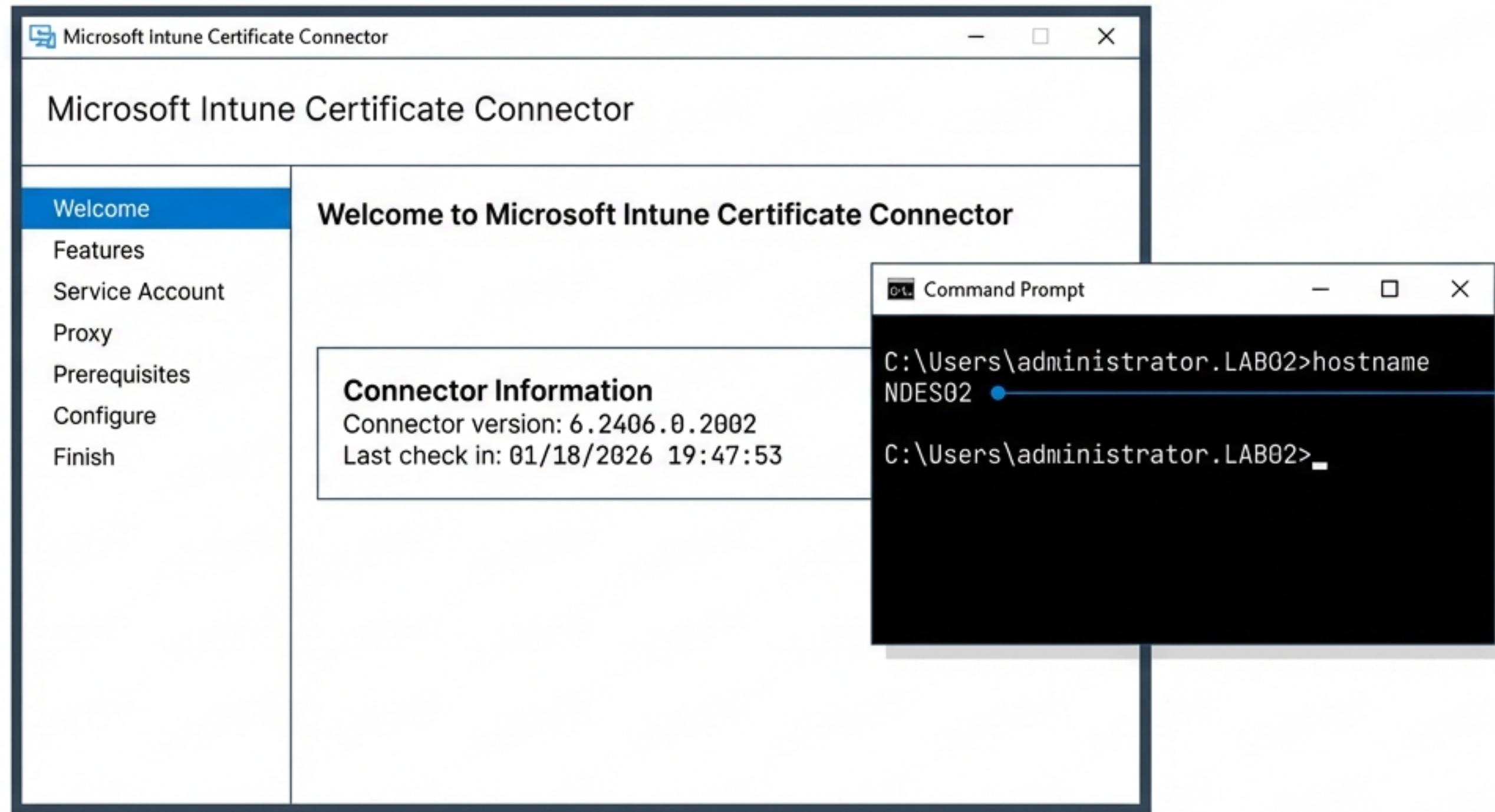
On-Premises CA Configuration (Host: interca)

Name	Intended Purpose
NDES-Signing-Certificate	Certificate Request Agent
LAB02-SCEP-MACHINE	Server Authentication, Client Authentication
LAB02-USER-CERT	Client Authentication
LAB02-INTUNE-NEW	Encrypting File System, Secure Email...
LAB02-NDES-Exchahnge	Certificate Request Agent
LAB02-NDESServer	Server Authentication, Client Authent...
IPSec (Offline request)	IP security IKE intermediate
Exchange Enrollment Agent (Offline re...	Certificate Request Agent
CEP Encryption	Certificate Request Agent
SSL_CERTS	Server Authentication
LAB-Web Server-Certs	Server Authentication
PA-Forward-Trust-Decrypt	<All>
LAB02-Computer	Client Authentication
PA-SSL-MGMT	Server Authentication

CRITICAL: Used by the NDES server to sign and vouch for incoming requests.

The payload template distributed to endpoints.

The Bridge: Intune Certificate Connector



Service Verification:
The connector runs locally on the NDES02 host. It polls Intune for requests and communicates directly with the CA.

Policy Definition: Establishing Trust

1

Policy name	Platform	Policy type
LA02-INTER-CA-CERT	Windows 8.1 and later	Trusted certificate
LAB02-SCEP-MACHINE	Windows 8.1 and later	SCEP certificate
LAB02-SCEP-USER	Windows 8.1 and later	SCEP certificate

Prerequisite: The Trusted Certificate profile pushes the Public Key of Lab02-INTERCA-CA to the device's Trusted Root Store. The device must trust the issuer before requesting a personal certificate.

Policy Definition: SCEP Configuration

2

Policy name	Platform	Policy type	Configuration Details
LA02-INTER-CA-CERT	Windows 8.1 and later	Trusted certificate	
LAB02-SCEP-MACHINE	Windows 8.1 and later	SCEP certificate	Contains External URL: The Azure App Proxy address configured in Phase 1.
LAB02-SCEP-USER	Windows 8.1 and later	SCEP certificate	Contains Template Ref: Matches LAB02-SCEP- MACHINE on the CA.

Operational Validation: Deployment Status

Policy Profile: LAB02-SCEP



1

Succeeded

0

Error

0

Conflict

0

Not applicable

This metric confirms the device successfully:
1. Received Policy,
2. Contacted App Proxy,
3. Authenticated,
4. Received Certificate.

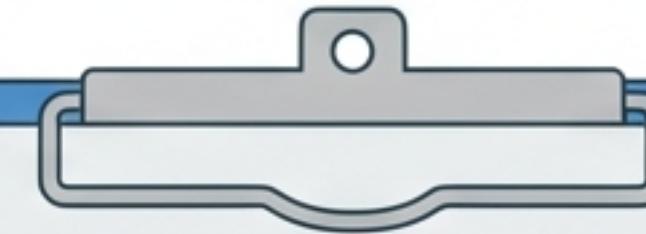


Endpoint Verification: Issued Certificates

Device name	Thumbprint	Serial number	Issuer	Key usage
DESKTOP-GM7NF61	C5D1F11A61F9822D0F26...	1A0000006BA620B66AA0A154FE...	CN=Lab02-INTERCA-CA, DC=lab02, DC=local	160

Proof of Trust: The Cloud-joined device holds a certificate signed by the internal On-Premises CA.

Implementation Checklist & Summary



1. **Identity Confirmed** - App Registration & Enterprise App IDs match (ndes-proxy).
2. **Tunnel Established** - App Proxy Connector Group is active (Default - Europe).
3. **Infrastructure Ready** - CA Templates (NDES-Signing) published on CA.
4. **Bridge Installed** - Intune Connector Service running on NDES02.
5. **Trust Established** - Trusted Root profile deployed before SCEP profile.
6. **Validation Complete** - Intune reports 'Succeeded: 1'.

Final State: Secure, certificate-based authentication without VPN.