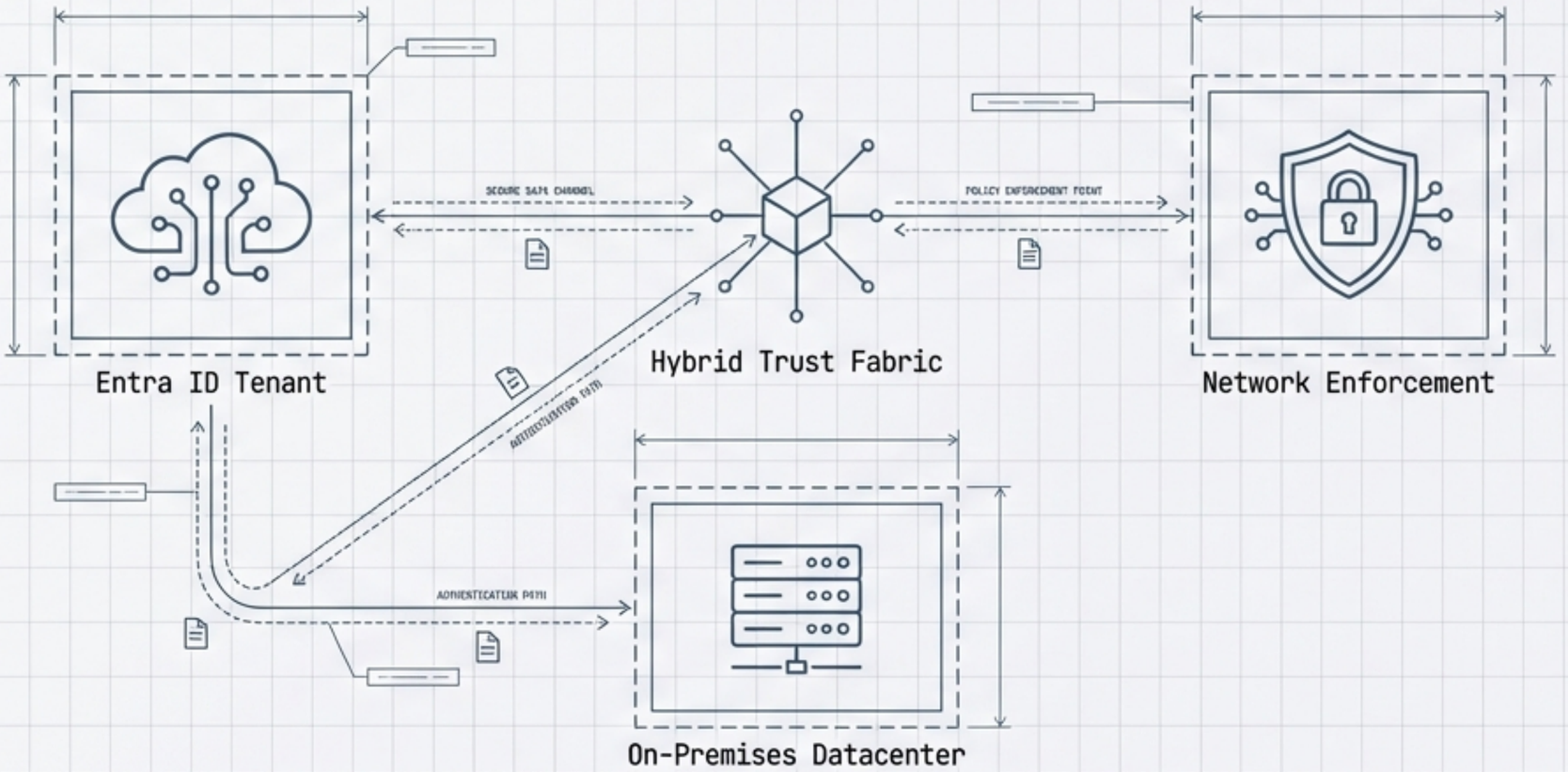
Zero Trust Hybrid Architecture: Identity, Connectivity, & Enforcement

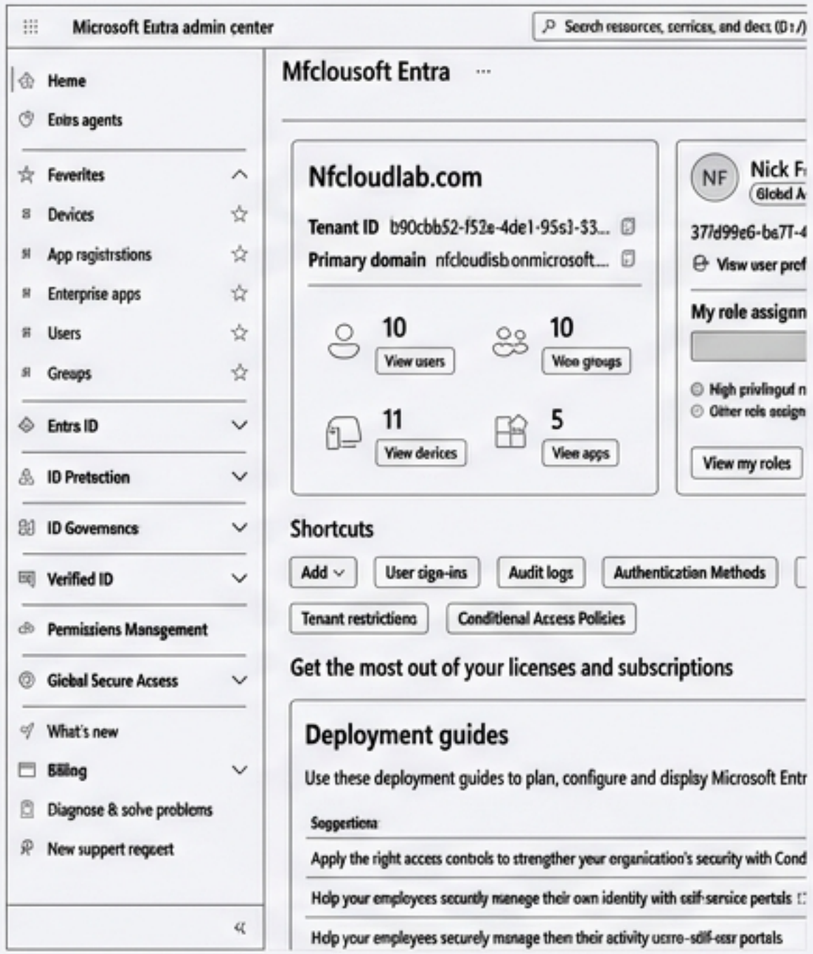
Deployment Verification and Configuration Review | Environment: Nfcloudlab (LAB02)



Technical Documentation Series
Status: VERIFIED
Doc ID: REF-ZTA-01

NotebookLM

The Cloud Identity Foundation: Entra ID Tenant Context



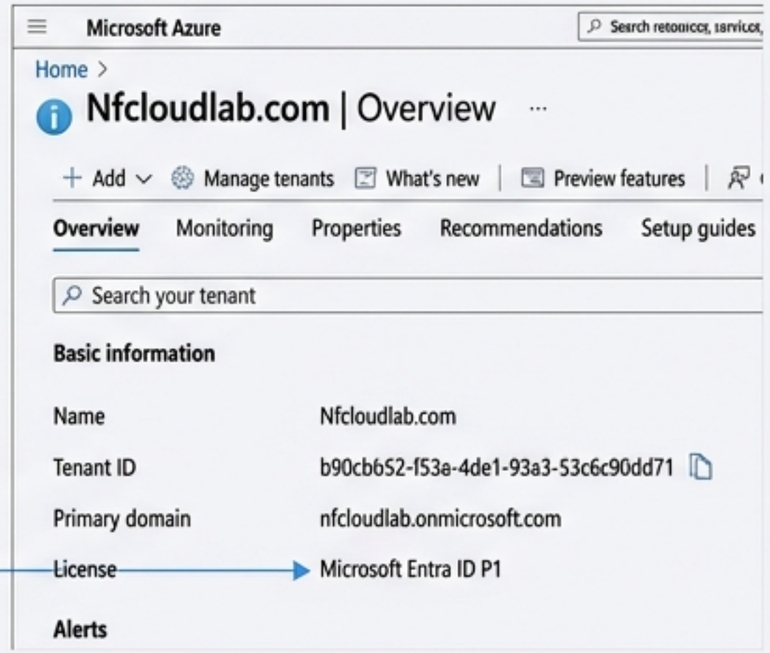
TENANT:
Nfcloudlab.com

DOMAIN:
nfcloudlab.onmicrosoft.com

LICENSE:
Premium P1
(Required for Intune/CA)

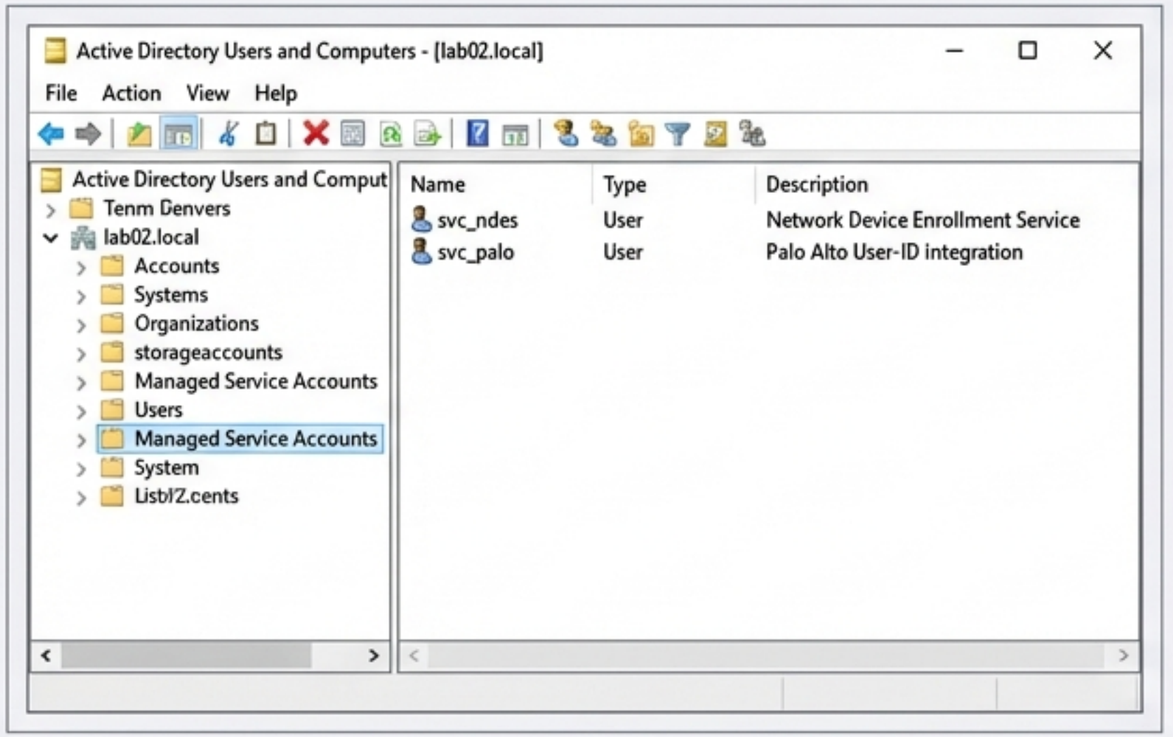
ADMIN:
Nick Fennell

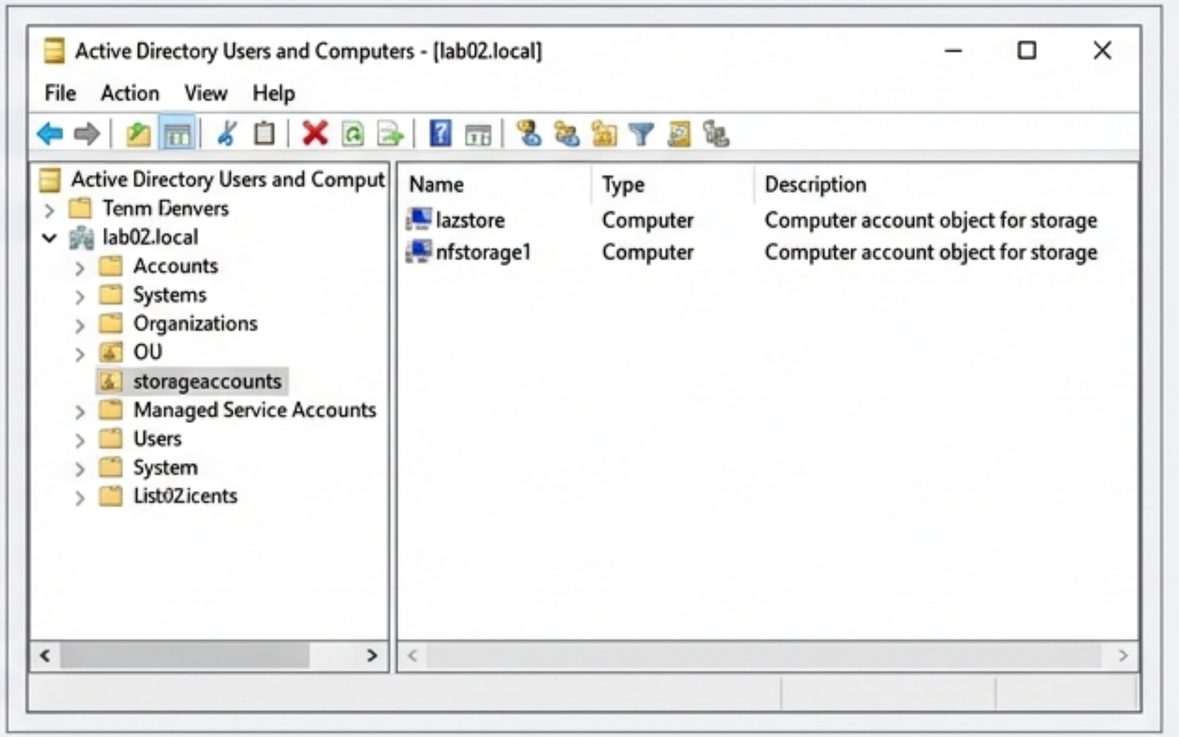
STATUS:
Healthy



NotebookLM

On-Premises Service Infrastructure: Preparing for Hybrid Access





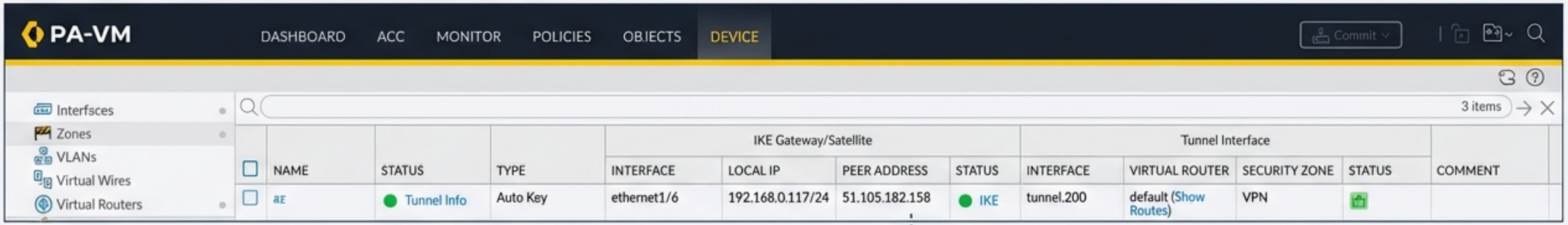
Configuration Notes

```
DOMAIN CONTEXT: lab02.local
SERVICE ACCOUNTS:
  > svc_ndes (Network Device Enrollment Service)
  > svc_palo (Palo Alto User-ID Integration)
STORAGE OBJECTS:
  > lazstore / nfstorage1 (Hybrid Data Link)
```

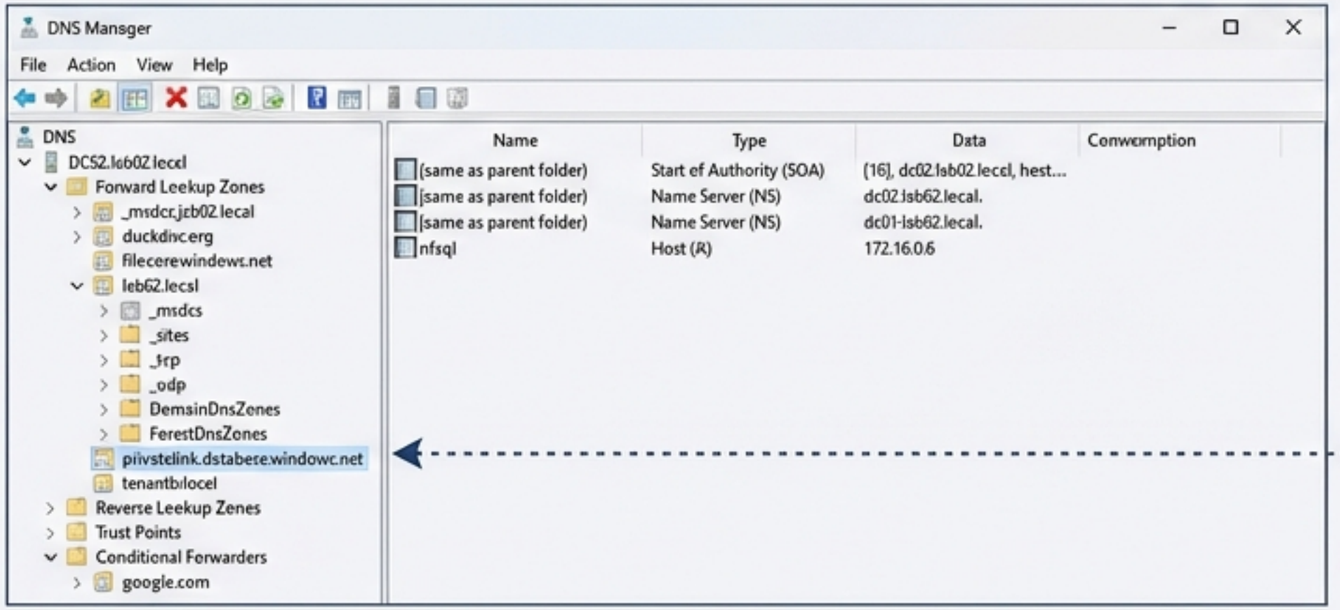
NotebookLM

Hybrid Connectivity Layer: Site-to-Site VPN & Private DNS

PHYSICAL LAYER: IPSEC TUNNEL STATUS [UP]

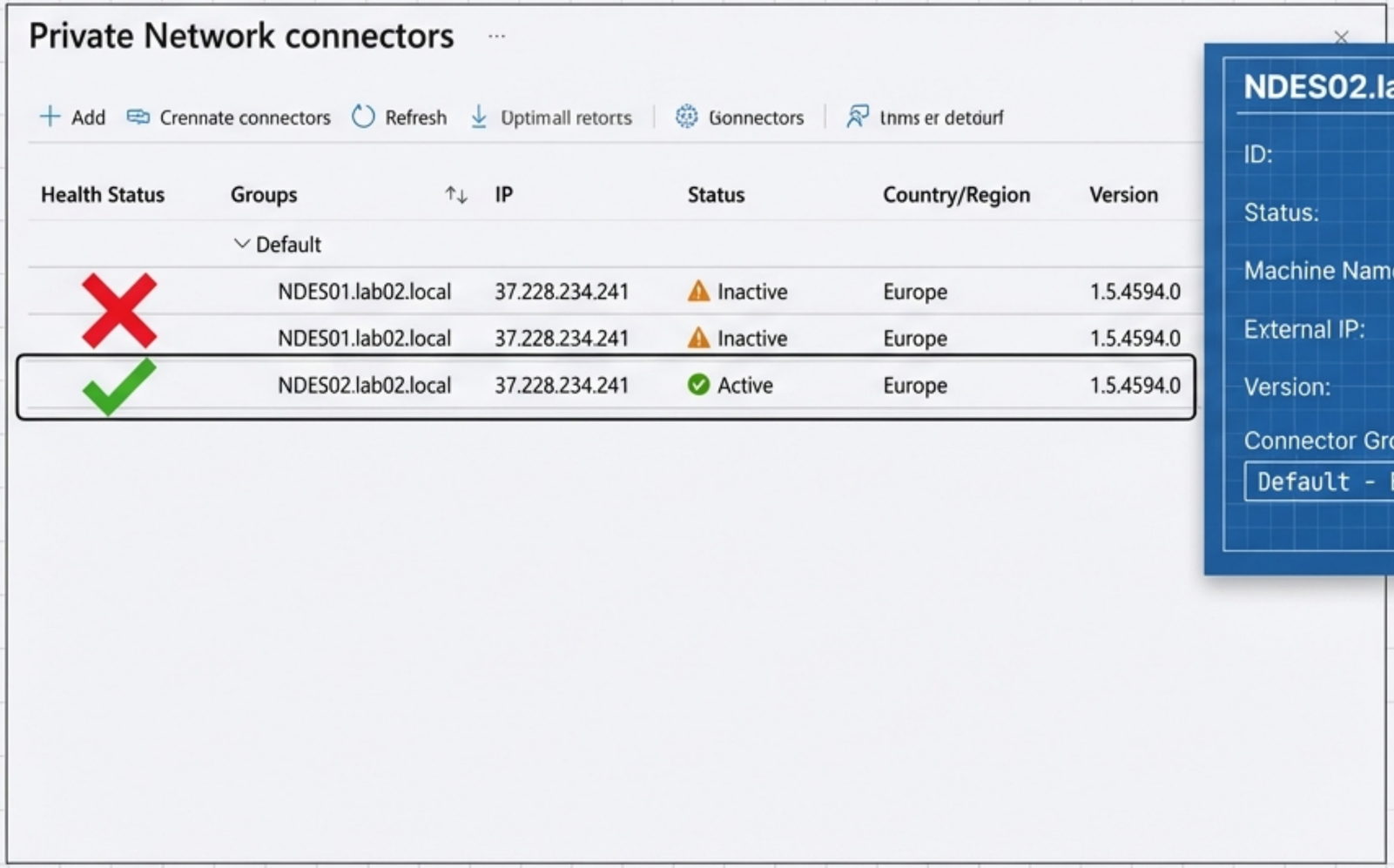


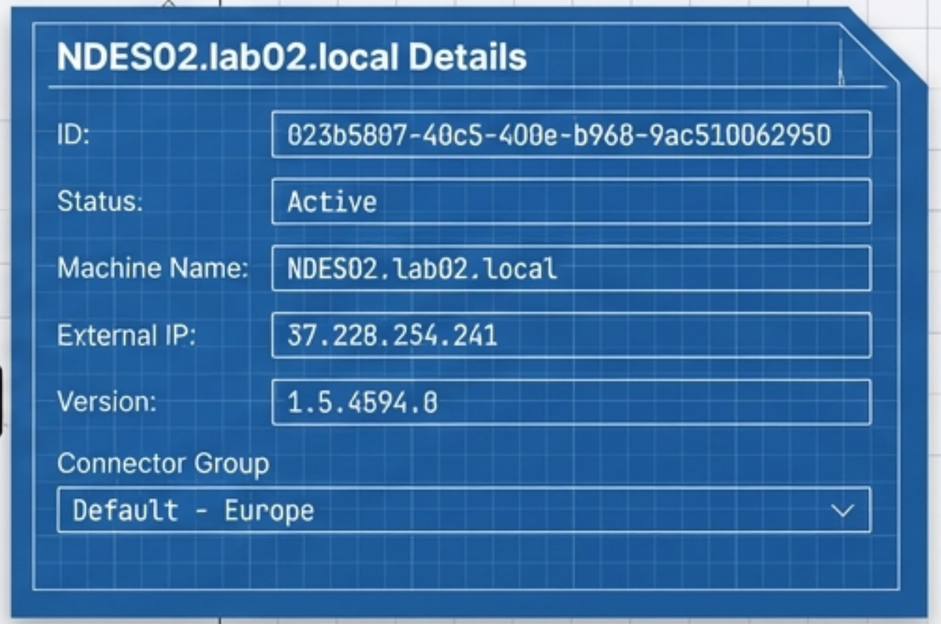
LOGICAL LAYER: HYBRID DNS RESOLUTION

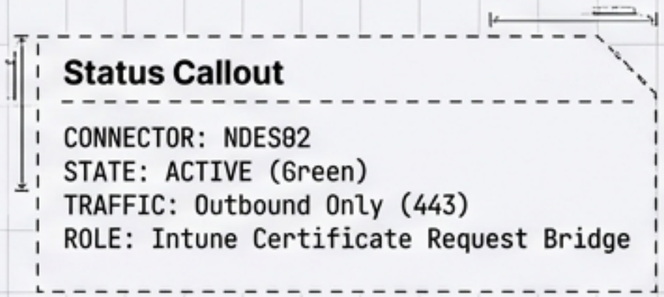


NotebookLM

Secure Publishing: Microsoft Entra Application Proxy

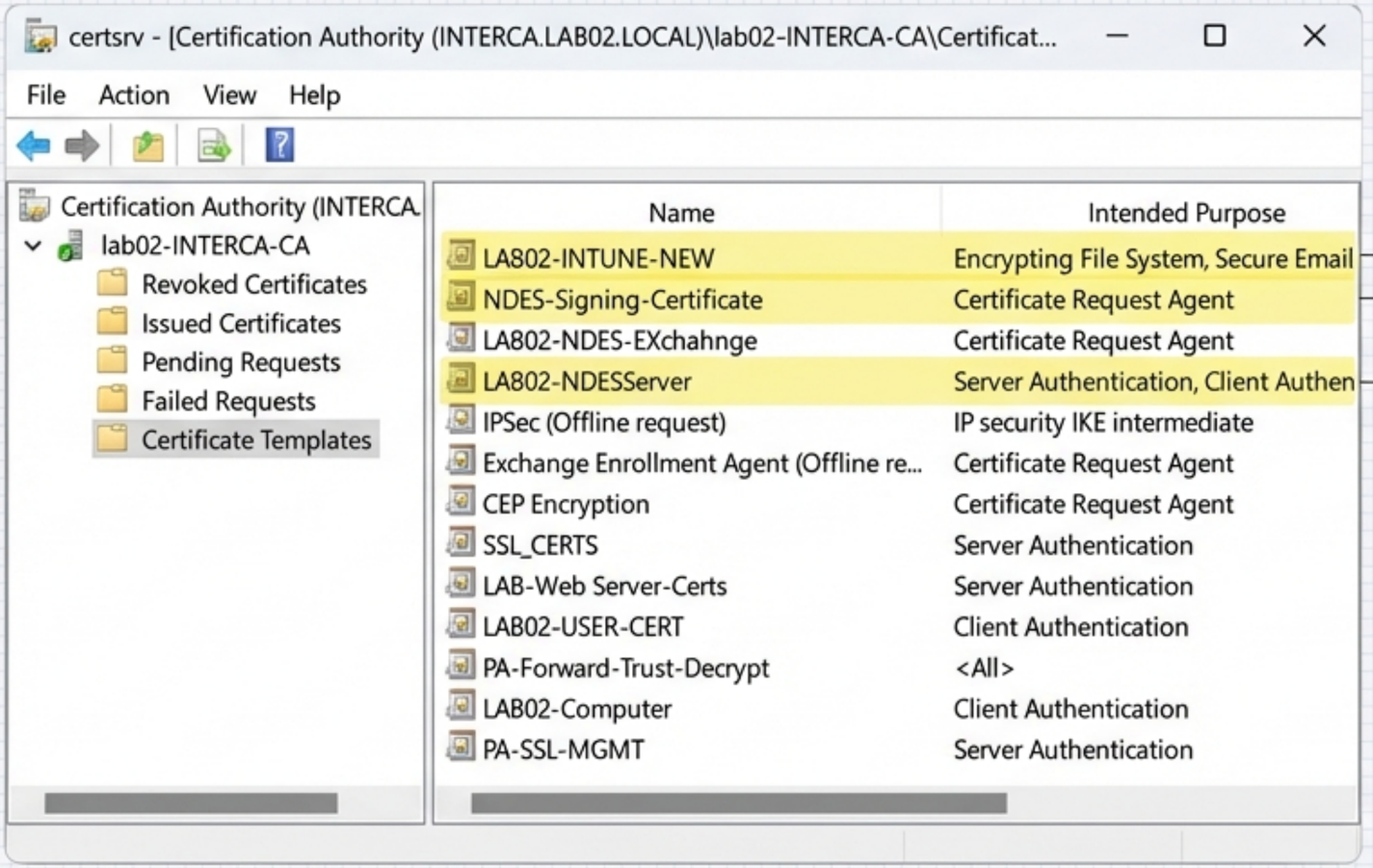






NotebookLM

The Trust Fabric: PKI & Certificate Templates



TECHNICAL LEGEND: TEMPLATE PURPOSE & USAGE

TEMPLATE: NDES-Signing-Certificate
> **Usage:** Registration Authority (RA)
> **Usage:** Registration Authority (RA)
> **Function:** Signs requests on behalf of devices

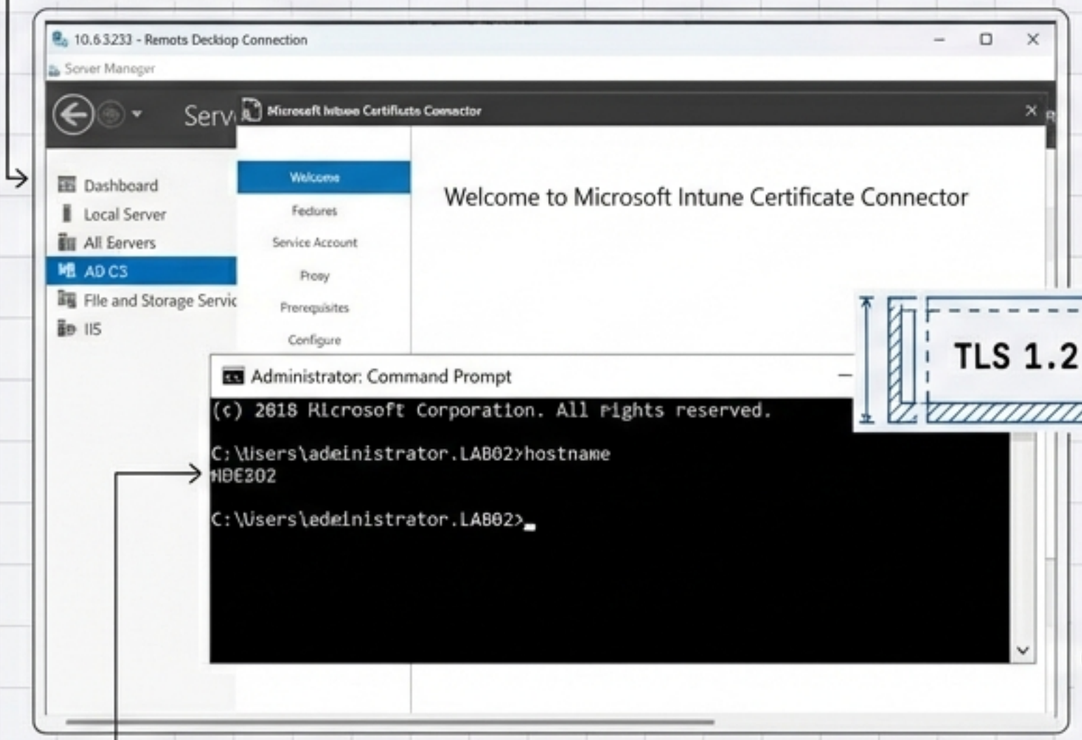
TEMPLATE: LAB02-INTUNE-NEW
> **Usage:** End-User Identity
> **Function:** SCEP/PKCS Profile for Zero Trust

NotebookLM

Bridging Trust: The Intune Certificate Connector

SERVER-SIDE SETUP (CAUSE)

Connector Setup Wizard

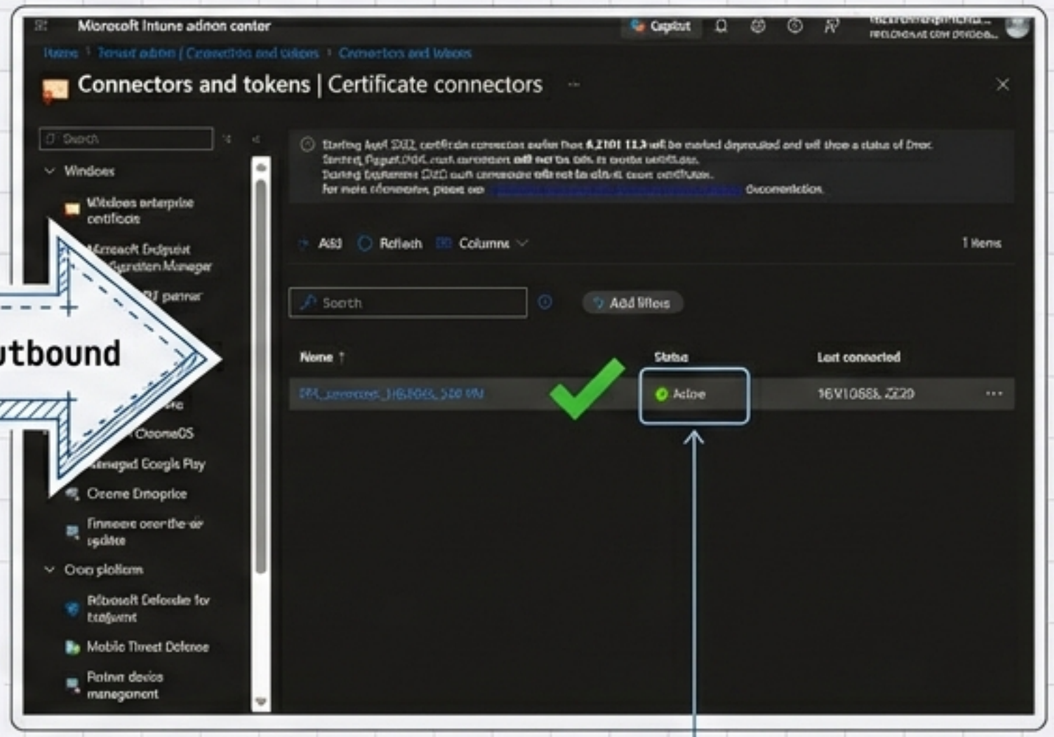


Hostname Verification

TLS 1.2 / HTTPS Outbound

Secure Encrypted Communication

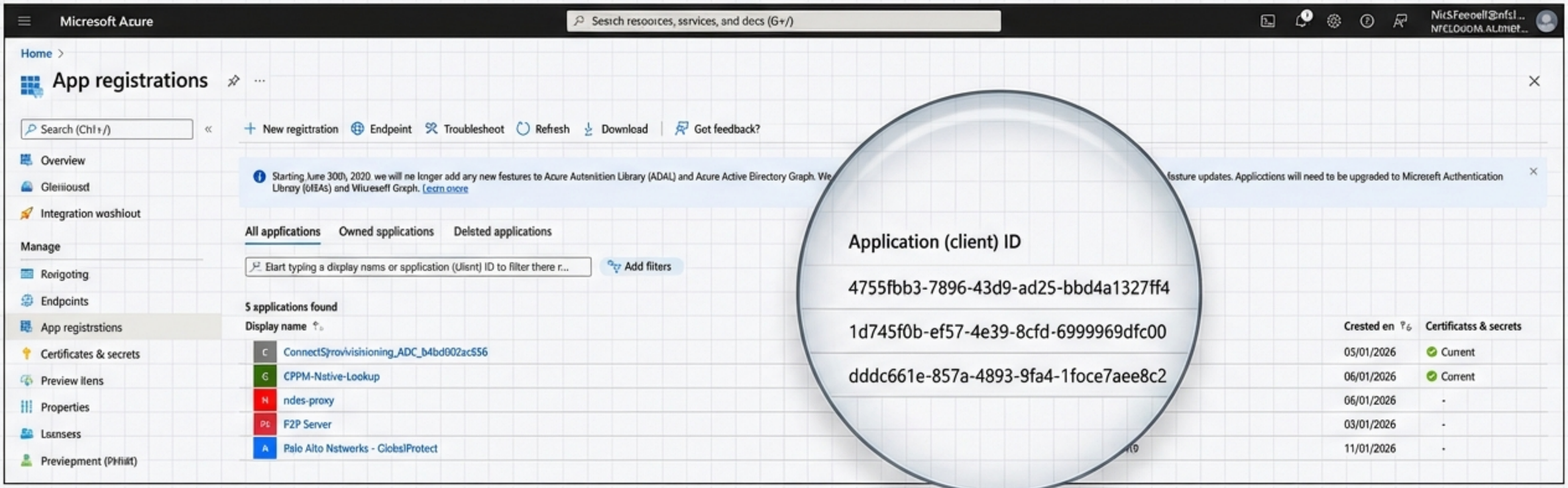
CLOUD CONSOLE STATUS (EFFECT)



Active

NotebookLM

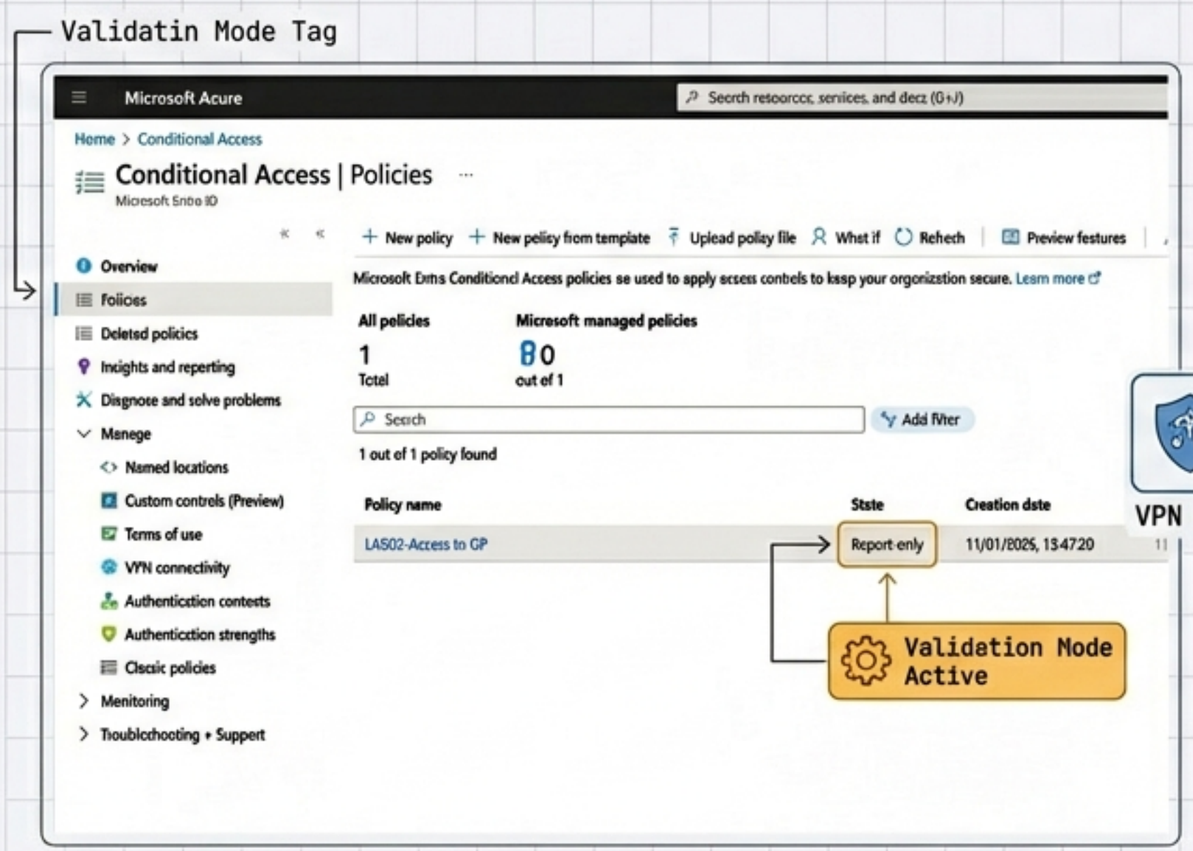
Integrated Ecosystem: App Registrations & Service Principals

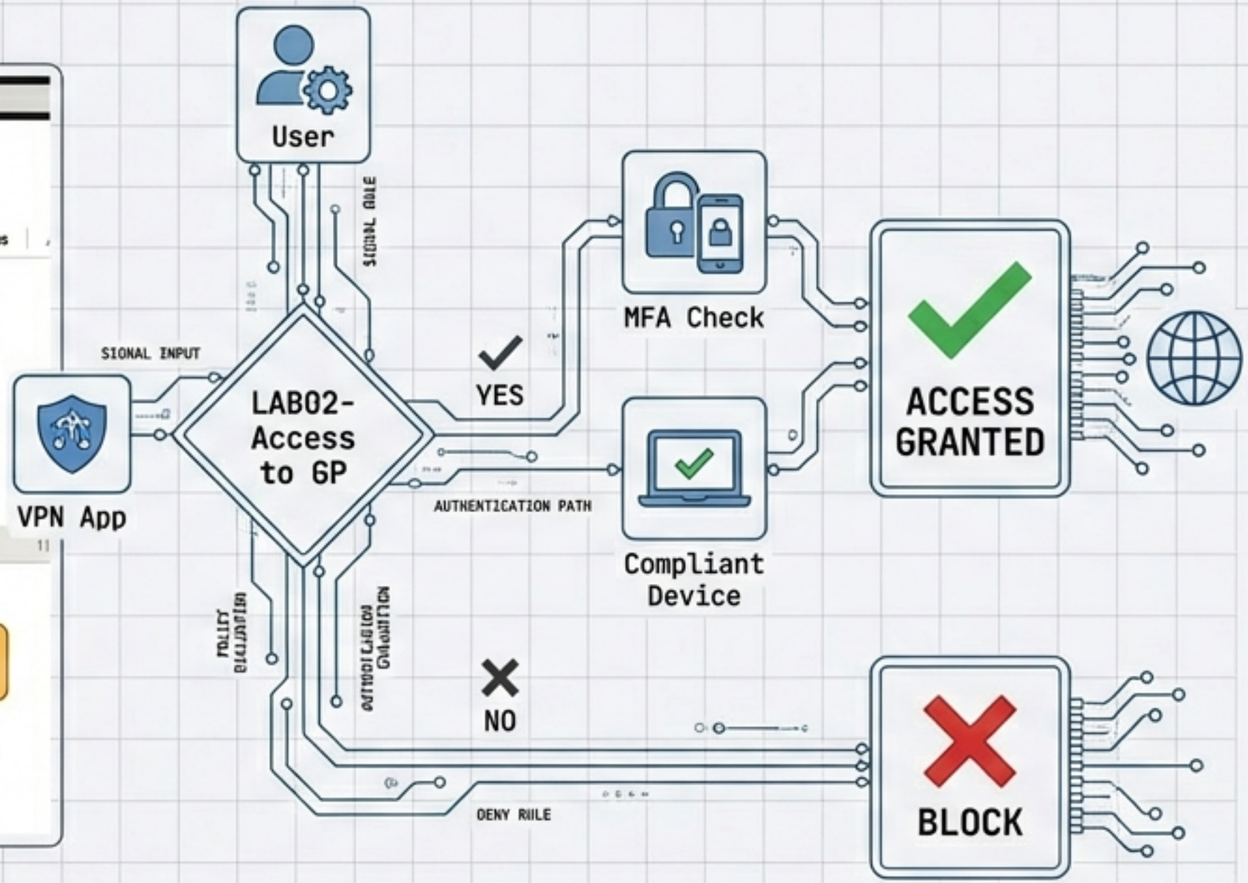


APPLICATION ID	ROLE	AUTH PROTOCOL
Palo Alto GlobalProtect	VPN Client	SAML / OIDC
CPPM-Native-Lookup	Network Access Control	Graph API
ndes-proxy	PKI Bridge	App Proxy

NotebookLM

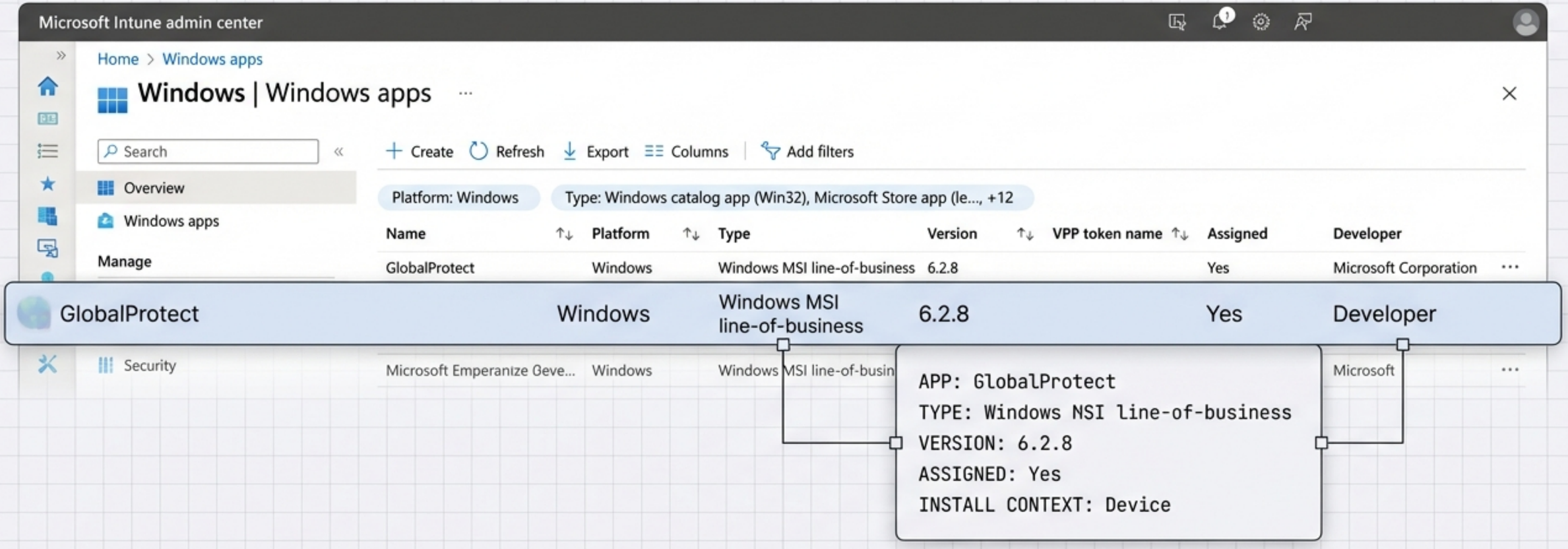
The Decision Engine: Conditional Access Policies





NotebookLM

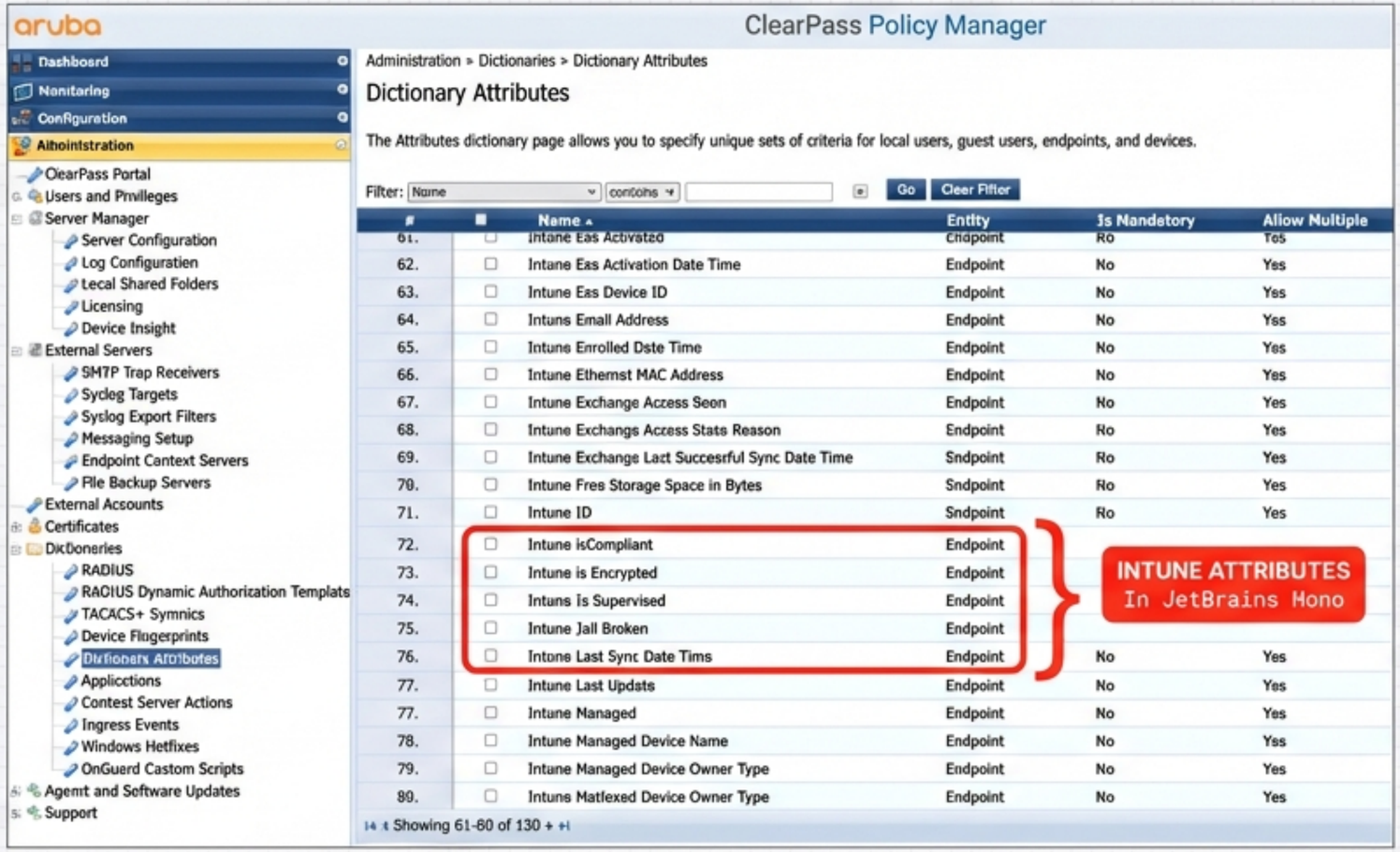
Endpoint Management: Automated Security Tool Delivery



Workflow: Intune automatically installs the VPN client (GlobalProtect) required to access the network. This ensures no unmanaged devices can attempt connection.

NotebookLM

Closing the Loop: ClearPass & Intune Attribute Exchange



NETWORK ENFORCEMENT

The firewall now reads the cloud. If “Intune isCompliant” = False, Network Access = Denied.

NotebookLM

Architecture Summary: The Verified Flow

CONFIGURATION STATUS: VALIDATED
ENVIRONMENT: LAB02
ARCHITECT: N. FENNELL

NotebookLM