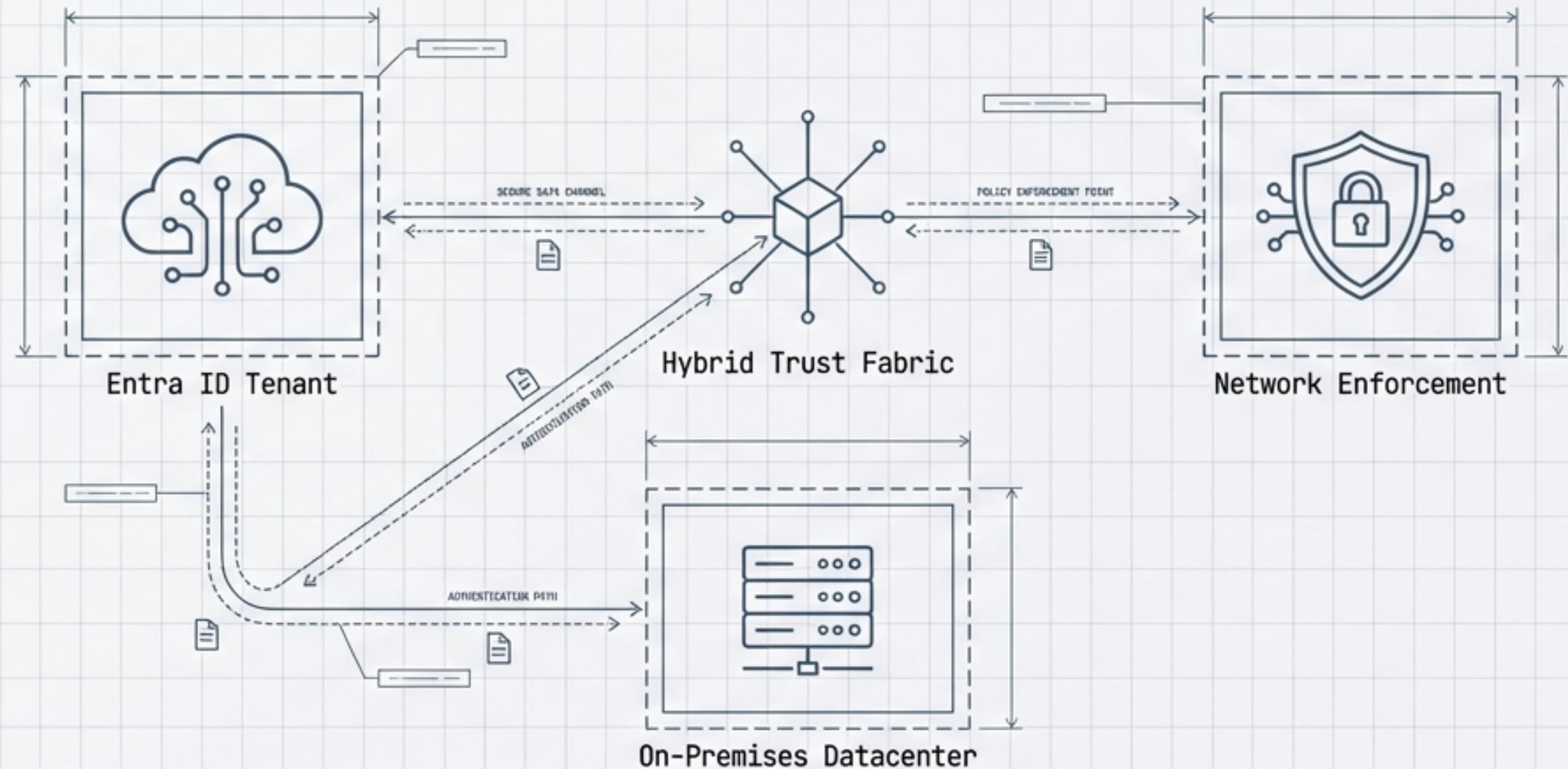


Zero Trust Hybrid Architecture: Identity, Connectivity, & Enforcement

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



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

The Cloud Identity Foundation: Entra ID Tenant Context

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Home, Entra agents, Favorites, Devices, App registrations, Enterprise apps, Users, Groups, Entra ID, ID Protection, ID Governance, Verified ID, Permissions Management, Global Secure Access, What's new, Billing, Diagnose & solve problems, and New support request. The main area displays tenant details for "Nfcloudlab.com". It shows the Tenant ID (b90cb652-f53e-4de1-93a3-53c6c90dd71), Primary domain (nfcloudlab.onmicrosoft.com), and user statistics (10 users, 10 groups, 11 devices, 5 apps). A user profile for "Nick Fennell" is shown with roles assigned. Below this, there are sections for Shortcuts (Add, User sign-ins, Audit logs, Authentication Methods, Tenant restrictions, Conditional Access Policies) and Deployment guides.

TENANT:
Nfcloudlab.com

DOMAIN:
nfcloudlab.onmicrosoft.com

LICENSE:
Premium P1
(Required for Intune/CA)

ADMIN:
Nick Fennell

STATUS:
Healthy

The screenshot shows the Microsoft Azure portal overview for the tenant "Nfcloudlab.com". It includes a search bar, navigation links for Overview, Monitoring, Properties, Recommendations, and Setup guides, and a basic information section with the tenant name, tenant ID (b90cb652-f53e-4de1-93a3-53c6c90dd71), primary domain (nfcloudlab.onmicrosoft.com), and license (Microsoft Entra ID P1). There's also an Alerts section.

On-Premises Service Infrastructure: Preparing for Hybrid Access

The screenshot shows the Active Directory Users and Computers interface for the domain lab02.local. The left pane displays the organizational structure, and the right pane lists service accounts. Two accounts are visible: svc_ndes (User, Network Device Enrollment Service) and svc_palo (User, Palo Alto User-ID integration). The 'Managed Service Accounts' folder is selected in the navigation pane.

Name	Type	Description
svc_ndes	User	Network Device Enrollment Service
svc_palo	User	Palo Alto User-ID integration

The screenshot shows the Active Directory Users and Computers interface for the domain lab02.local. The left pane displays the organizational structure, and the right pane lists storage objects. Two computer accounts are visible: lazstore (Computer, Computer account object for storage) and nfstorage1 (Computer, Computer account object for storage). The 'storageaccounts' folder is selected in the navigation pane.

Name	Type	Description
lazstore	Computer	Computer account object for storage
nfstorage1	Computer	Computer account object for storage

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)

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

PHYSICAL LAYER: IPSEC TUNNEL STATUS [UP]

The screenshot shows a network management interface with a dark header bar containing the logo 'PA-VM' and navigation tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, and DEVICE. The DEVICE tab is selected. On the left, a sidebar lists 'Interfaces', 'Zones', 'VLANS', 'Virtual Wires', and 'Virtual Routers'. The main area displays a table titled 'IKE Gateway/Satellite' with columns: NAME, STATUS, TYPE, INTERFACE, LOCAL IP, PEER ADDRESS, and STATUS. Below it is a table titled 'Tunnel Interface' with columns: INTERFACE, VIRTUAL ROUTER, SECURITY ZONE, STATUS, and COMMENT. A search bar at the top right shows '3 items'.

IKE Gateway/Satellite						
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS
AE	Tunnel Info	Auto Key	ethernet1/6	192.168.0.117/24	51.105.182.158	IKE

INTERFACE	VIRTUAL ROUTER	SECURITY ZONE	STATUS	COMMENT
tunnel.200	default (Show Routes)	VPN		

LOGICAL LAYER: HYBRID DNS RESOLUTION

The screenshot shows a 'DNS Manager' window with a toolbar and a menu bar (File, Action, View, Help). The left pane is a tree view of DNS zones, including 'DCS2.leb62.lecal', 'Forward Lookup Zones' (with entries like '_msdcr.jeb02.lecal', 'duckdns.org', 'filecerewinews.net'), 'leb62.lecal' (with entries like '_msdcsl', '_sites', '_jrp', '_odp', 'DemsinDnsZones', 'ForestDnsZones', 'pivstelink.databases.windows.net', 'tenantbilevel'), 'Reverse Lookup Zones', 'Trust Points', 'Conditional Forwarders', and 'google.com'. The right pane displays a table with columns: Name, Type, Data, and Corruption. It lists several records:

Name	Type	Data	Corruption
(same as parent folder)	Start of Authority (SOA)	[16], dc02.lsb62.lecal, host...	
(same as parent folder)	Name Server (NS)	dc02.lsb62.lecal.	
(same as parent folder)	Name Server (NS)	dc01-lsb62.lecal.	
nfsql	Host (A)	172.16.0.6	

Secure Publishing: Microsoft Entra Application Proxy

Private Network connectors ...

+ Add Crennate connectors Refresh Optimall retorts | Connectors Ihmser detourf

Health Status	Groups	IP	Status	Country/Region	Version	
✗	Default	NDES01.lab02.local	37.228.234.241	Inactive	Europe	1.5.4594.0
✗	Default	NDES01.lab02.local	37.228.234.241	Inactive	Europe	1.5.4594.0
✓	Default	NDES02.lab02.local	37.228.234.241	Active	Europe	1.5.4594.0

NDES02.lab02.local Details

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

Status: Active

Machine Name: NDES02.lab02.local

External IP: 37.228.254.241

Version: 1.5.4594.0

Connector Group: Default - Europe

Status Callout

CONNECTOR: NDES02
STATE: ACTIVE (Green)
TRAFFIC: Outbound Only (443)
ROLE: Intune Certificate Request Bridge

NotebookLM

The Trust Fabric: PKI & Certificate Templates

The screenshot shows the Windows Certificates snap-in window. The title bar reads "certsrv - [Certification Authority (INTERCA.LAB02.LOCAL)\lab02-INTERCA-CA\Certificat...". The menu bar includes File, Action, View, Help, and standard navigation icons. On the left, a tree view shows the Certification Authority (INTERCA) and its sub-node "lab02-INTERCA-CA", which contains Revoked Certificates, Issued Certificates, Pending Requests, Failed Requests, and Certificate Templates. The main pane displays a table of certificate templates:

Name	Intended Purpose
LA802-INTUNE-NEW	Encrypting File System, Secure Email
NDES-Signing-Certificate	Certificate Request Agent
LA802-NDES-EXchahnge	Certificate Request Agent
LA802-NDESServer	Server Authentication, Client Authen
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
LAB02-USER-CERT	Client Authentication
PA-Forward-Trust-Decrypt	<All>
LAB02-Computer	Client Authentication
PA-SSL-MGMT	Server Authentication

TECHNICAL LEGEND: TEMPLATE PURPOSE & USAGE

TEMPLATE: NDES-Signing-Certificate

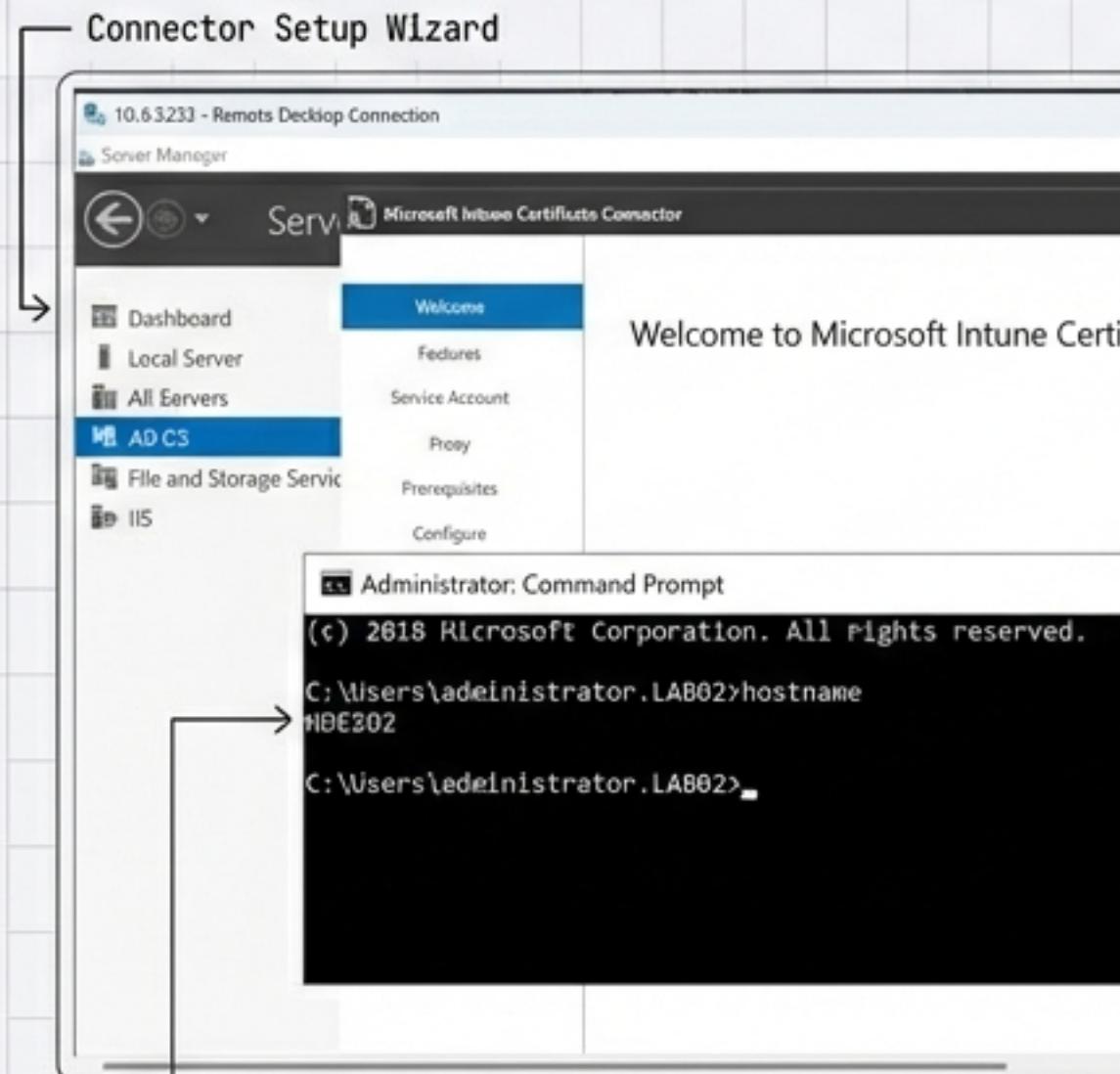
- > Usage: Registration Authority (RA)
- > Usage: Registration Authority (RA)
- > Function: Signs requests on behalf of devices

TEMPLATE: LAB02-INTUNE-NEW

- > Usage: End-User Identity
- > Function: SCEP/PKCS Profile for Zero Trust

Bridging Trust: The Intune Certificate Connector

SERVER-SIDE SETUP (CAUSE)

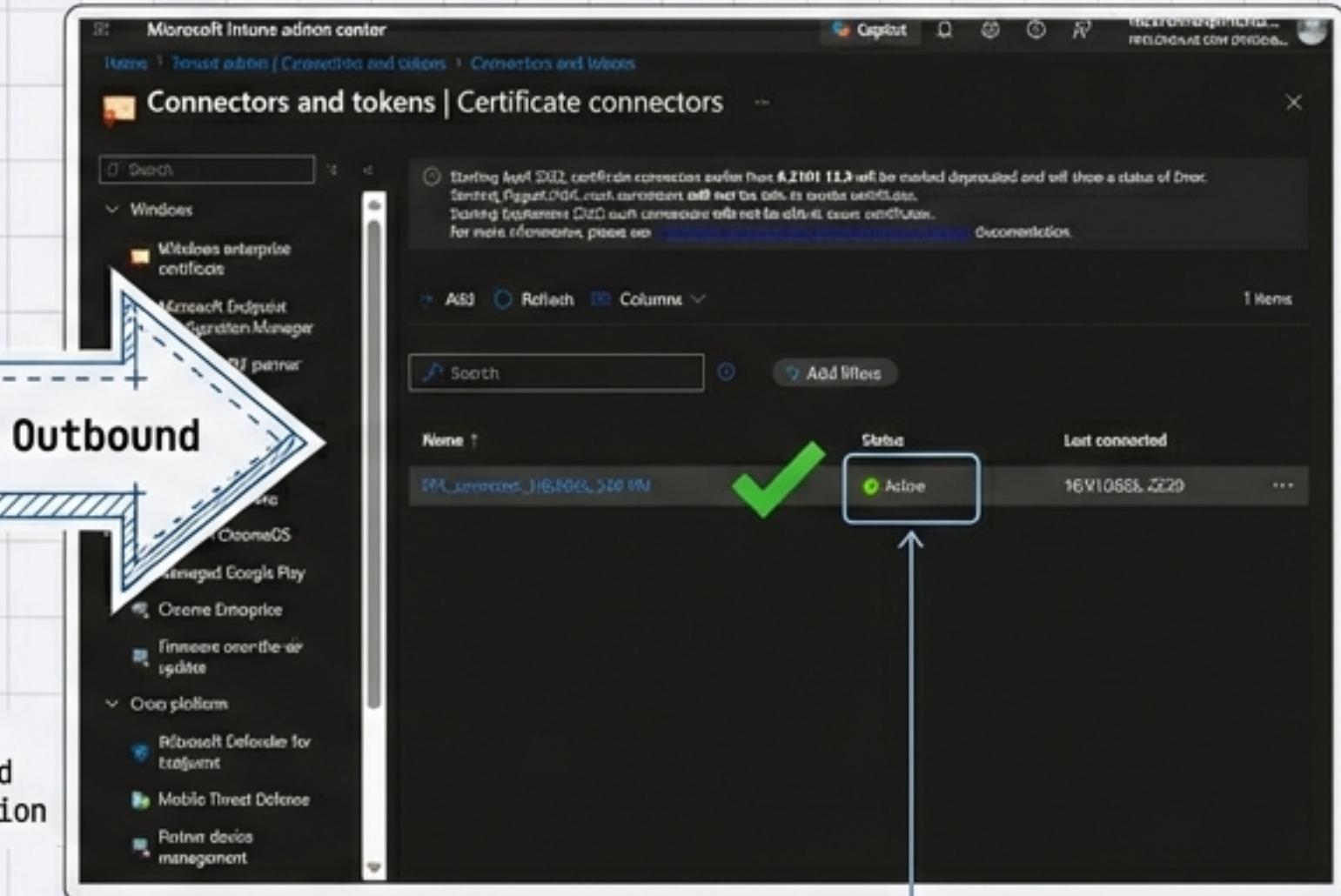


Hostname Verification

Secure
Encrypted
Communication

TLS 1.2 / HTTPS Outbound

CLOUD CONSOLE STATUS (EFFECT)



Active

Integrated Ecosystem: App Registrations & Service Principals

The screenshot shows the Microsoft Azure portal's App registrations page. The left sidebar includes links for Overview, Global usage, Integration health, Manage (Revolving, Endpoints, App registrations, Certificates & secrets, Preview items, Properties, Licenses, Previewment (Phaset)), and a Search bar. The main area displays a message about the end of support for ADAL and AAD Graph. It lists five applications under 'All applications':

Display name	Application (client) ID	Created on	Certificates & secrets
ConnectSprovisioning_ADC_b4bd002ac556	4755fbb3-7896-43d9-ad25-bbd4a1327ff4	05/01/2026	Current
CPPM-Native-Lookup	1d745f0b-ef57-4e39-8cf8-6999969dfc00	06/01/2026	Current
ndes-proxy	dddc661e-857a-4893-9fa4-1fce7aee8c2	06/01/2026	-
F2P Server		03/01/2026	-
Palo Alto Networks - GlobalProtect		11/01/2026	-

+

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

The Decision Engine: Conditional Access Policies

Validation Mode Tag

Microsoft Azure

Home > Conditional Access

Conditional Access | Policies

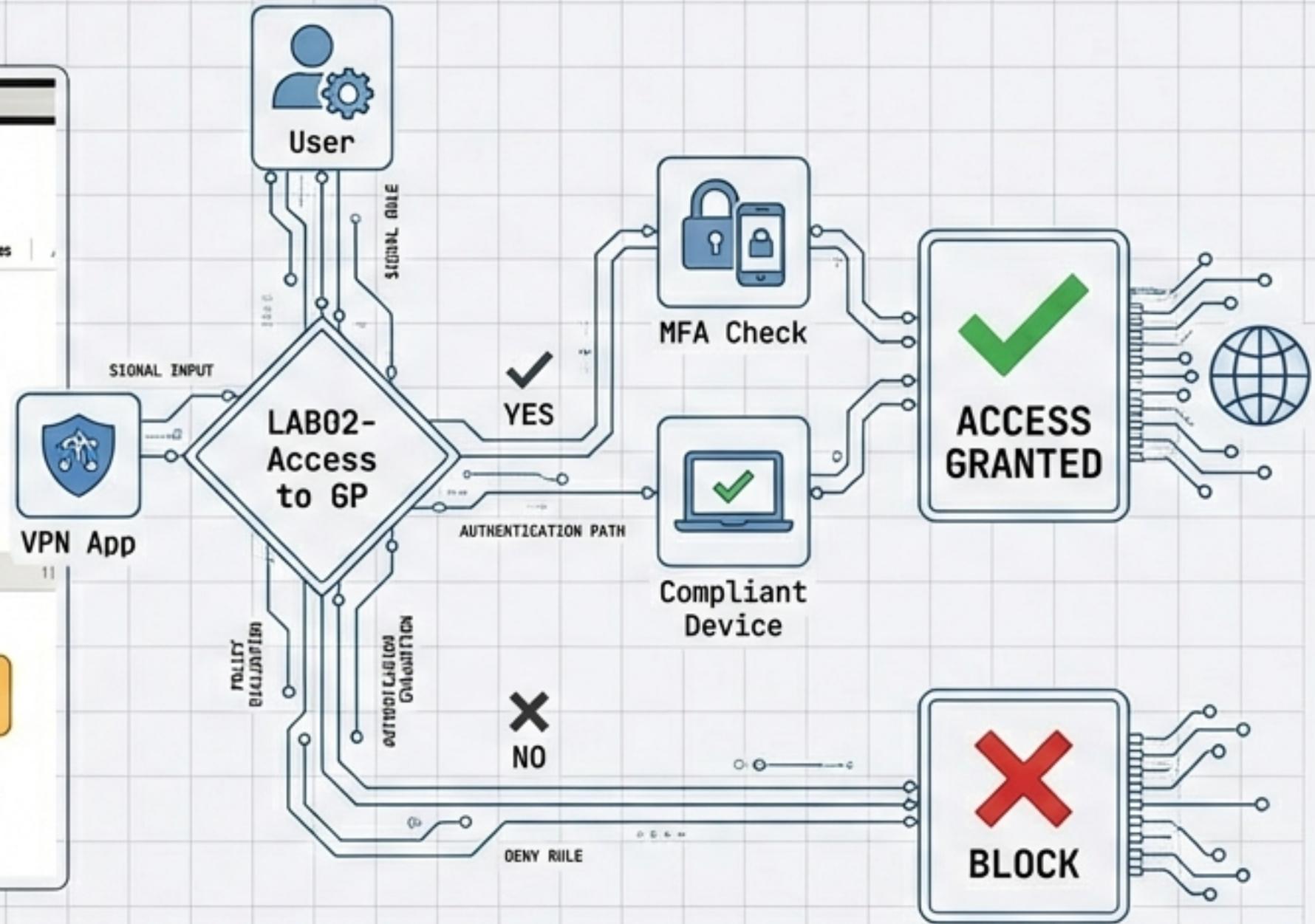
All policies Microsoft managed policies

1 Total 80 out of 1

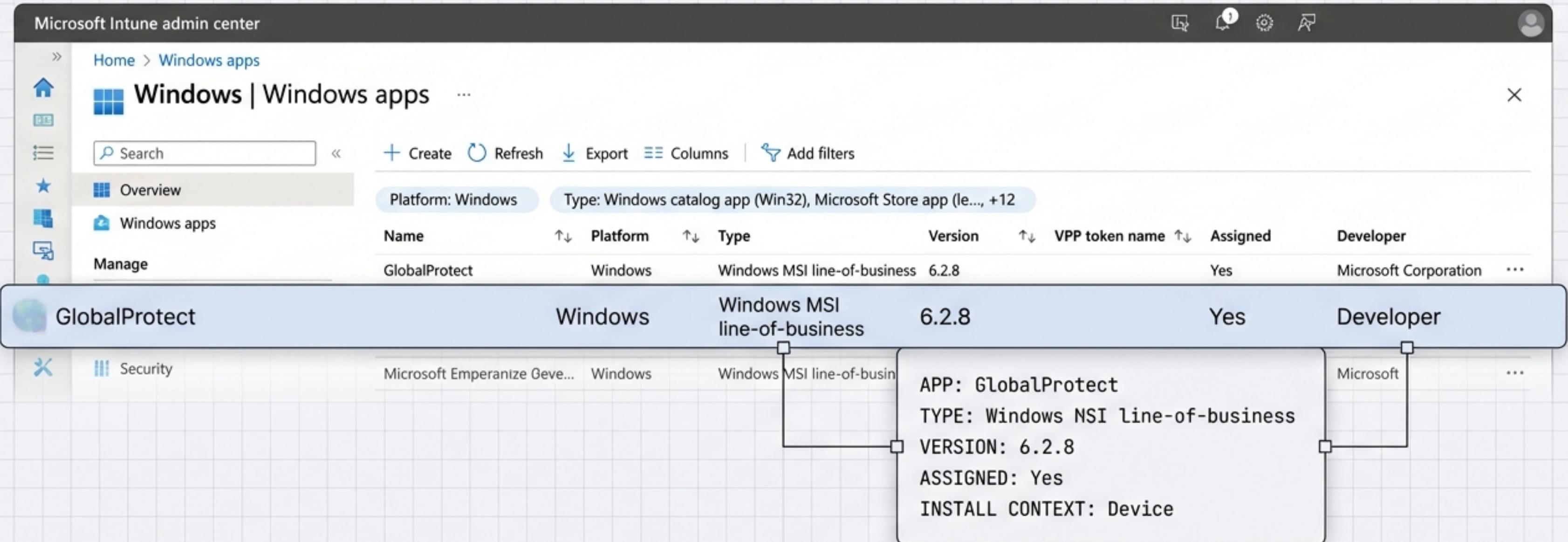
Policy name: LAB02-Access to GP

State: Report-only Creation date: 11/01/2025, 13:47:20

Validation Mode Active



Endpoint Management: Automated Security Tool Delivery



The screenshot shows the Microsoft Intune admin center interface. The left sidebar has icons for Home, Windows apps, Overview, and Manage. The main area title is "Windows | Windows apps". It includes a search bar, "Create", "Refresh", "Export", "Columns", and "Add filters" buttons. Filter options show "Platform: Windows" and "Type: Windows catalog app (Win32), Microsoft Store app (le..., +12)". A table lists apps with columns: Name, Platform, Type, Version, VPP token name, Assigned, and Developer. One row is selected for "GlobalProtect". A tooltip box over the GlobalProtect row displays detailed information: APP: GlobalProtect, TYPE: Windows MSI line-of-business, VERSION: 6.2.8, ASSIGNED: Yes, and INSTALL CONTEXT: Device.

Name	Platform	Type	Version	VPP token name	Assigned	Developer
GlobalProtect	Windows	Windows MSI line-of-business	6.2.8		Yes	Microsoft Corporation

GlobalProtect
Windows
Windows MSI line-of-business
6.2.8
Yes
Developer

APP: GlobalProtect
TYPE: Windows MSI line-of-business
VERSION: 6.2.8
ASSIGNED: Yes
INSTALL CONTEXT: Device

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

Closing the Loop: ClearPass & Intune Attribute Exchange

aruba

ClearPass Policy Manager

Administration > Dictionaries > Dictionary Attributes

Dictionary Attributes

The Attributes dictionary page allows you to specify unique sets of criteria for local users, guest users, endpoints, and devices.

Filter: Name | Contains | Go | Clear Filter

#	Name	Entity	Is Mandatory	Allow Multiple
61.	Intune Eas Activated	Endpoint	No	Yes
62.	Intune Eas Activation Date Time	Endpoint	No	Yes
63.	Intune Eas Device ID	Endpoint	No	Yes
64.	Intunes Email Address	Endpoint	No	Yes
65.	Intuns Enrolled Dste Time	Endpoint	No	Yes
66.	Intune Etherest MAC Address	Endpoint	No	Yes
67.	Intune Exchange Access Seon	Endpoint	No	Yes
68.	Intune Exchange Access Stats Reason	Endpoint	No	Yes
69.	Intune Exchange Last Succesful Sync Date Time	Endpoint	No	Yes
70.	Intune Fres Storage Space in Bytes	Endpoint	No	Yes
71.	Intune ID	Endpoint	No	Yes
72.	Intune isCompliant	Endpoint	No	Yes
73.	Intune is Encrypted	Endpoint	No	Yes
74.	Intuns Is Supervised	Endpoint	No	Yes
75.	Intune Jall Broken	Endpoint	No	Yes
76.	Intone Last Sync Date Times	Endpoint	No	Yes
77.	Intune Last Updats	Endpoint	No	Yes
77.	Intune Managed	Endpoint	No	Yes
78.	Intune Managed Device Name	Endpoint	No	Yes
79.	Intane Managed Device Owner Type	Endpoint	No	Yes
80.	Intuns Matflexed Device Owner Type	Endpoint	No	Yes

14 t Showing 61-80 of 130 + |

INTUNE ATTRIBUTES
In JetBrains Mono

NETWORK ENFORCEMENT

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

Architecture Summary: The Verified Flow



CONFIGURATION STATUS: VALIDATED
ENVIRONMENT: LABG2
ARCHITECT: N. FENNELL