Houston, We Have a Solution: Microsoft Cloud PKI

04-12-2024

Zurich, We Have a Solution: Microsoft Cloud PKI

04-12-2024

Thank you Sponsors

#WPNinjaCH

Microsoft

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

EPIC FUSION
BRING IT ALL TOGETHER

About Jeroen Burgerhout

Focus

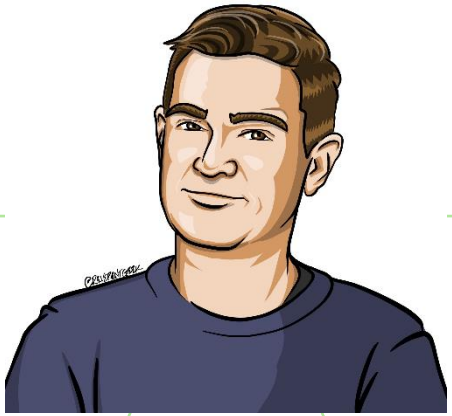
Microsoft Intune

From

Nieuwkoop, The Netherlands

My Blog

https://burgerhout.org



Certifications

A lot. MVP & MCT

Hobbies

Craft beer

Contact

https://burgerhou.tj/connect

What is Cloud PKI?

What is Cloud PKI?

Microsoft’s solution for certificate management in the Cloud!

Questions?

?

Microsoft Cloud PKI

General Available since 1st of March 2024

Simplify certificate delivery to Intune clients

Set up a PKI in minutes instead of weeks

Improve security more easily than ever

Part of Intune Suite or Single license

Microsoft Cloud PKI

RSA 2048/3072/4096

SHA 256/384/512

Licensed CA -> HSM

Trial CA -> Software keys

2-Tier PKI

BYOCA

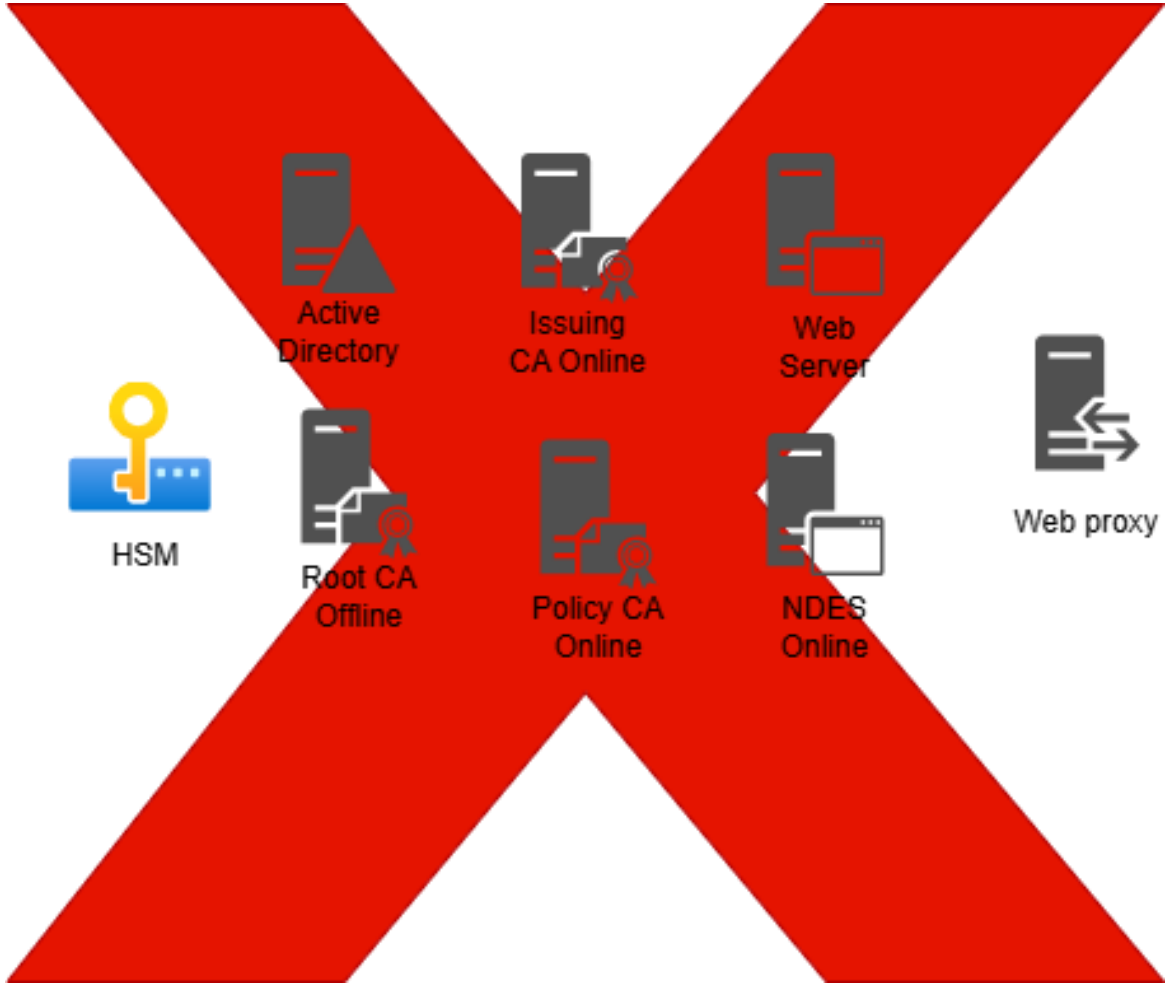
No need for on-prem PKI

Don’t need on-prem servers, like:

- Root CA
- Issuing CA
- Web
- NDES
- Web proxy
- Policy CA

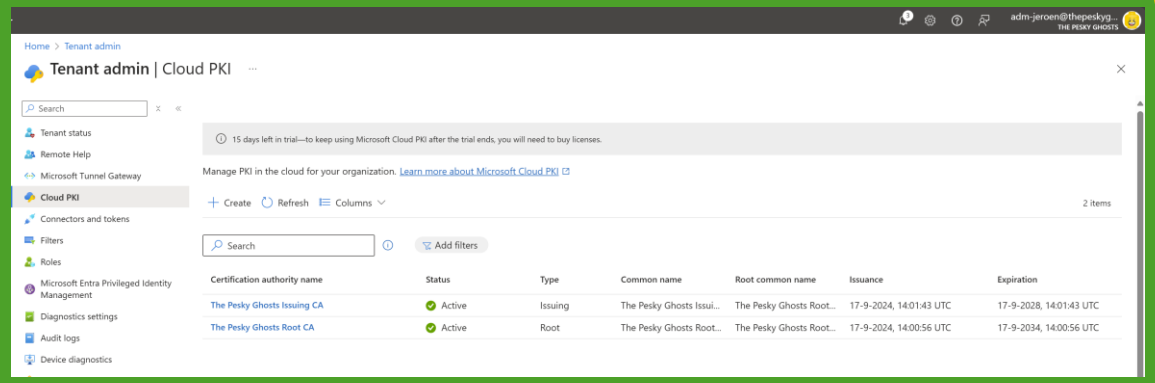
Also

- a dedicated HSM
- No firewall/port maintenance



Demo Setting it up

#WPNinjaCH



PKI Services

- CRL (Certificate Revocation List)
  - For each CA
  - Validity period is 7 days. Publishing and refresh happens every 3,5 days. After every revocation, the CRL is updated

- AIA (Authority Information Access)
  - For each Issuing CA
  - Endpoint can be used by relying parties to retrieve parent certificates

- SCEP (PKCS#7)
  - Intune only enrolled devices
  - https://{{CloudPKIFQDN}}/TrafficGateway/PassThroughRoutingService/CloudPki/CloudPkiService/Scep/9028deb3-4647-40fe-b92a-31c3d95459d7/eeefafda-cb0c-4bf1-98f9-16fce4ca6529

Planning

Validity Period (Root CA)

- 5 Year Minimum
- 25 Year Maximum

Validity Period (Issuing CA)

- 2 Year Minimum
- 10 Year Maximum

Best Practice

- Issuing CA Half Lifetime of Root CA
- Example: 20 Year Root > 10 Year Issuing

Planning

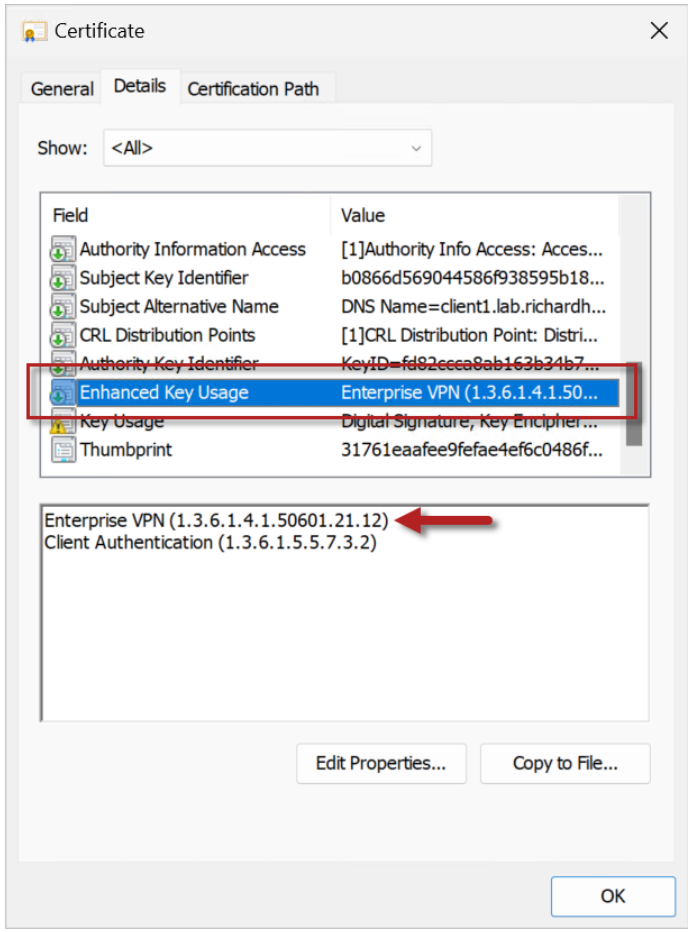
Extended Key Usages (OIDs)

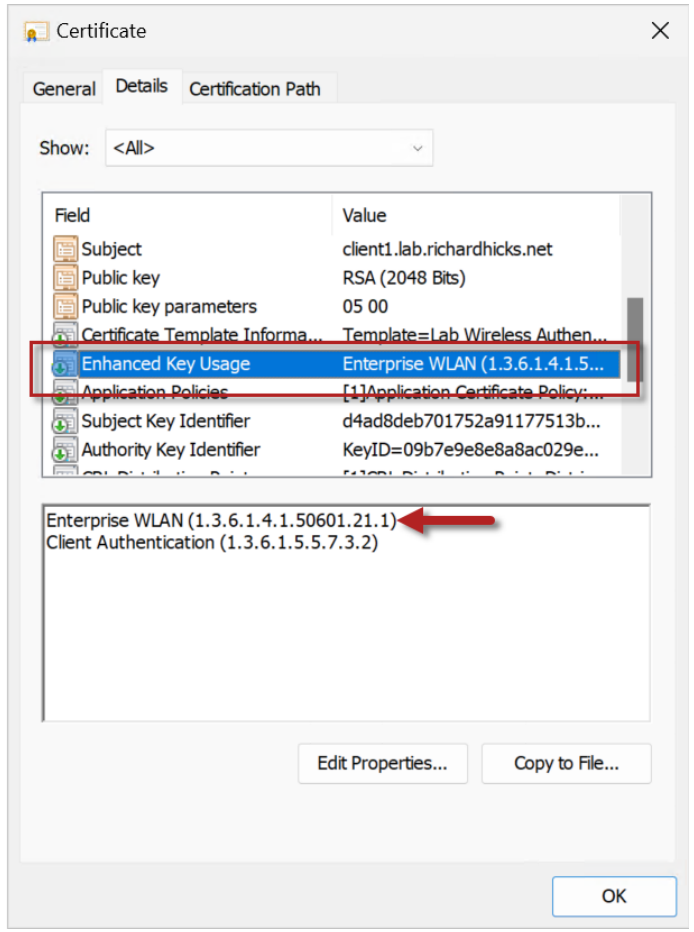
- Client Authentication (1.3.6.1.5.5.7.3.2)
- Server Authentication (1.3.6.1.5.5.7.3.1)
- Smartcard logon (1.3.6.1.4.1.311.20.2.2)
- Code Signing (1.3.6.1.5.5.7.3.3)
- Email Protection (1.3.6.1.5.5.7.3.4)
- And more…

Issuing CA

- Limited to EKUs of Root CA

Private Enterprise Number





http://burgerhou.tj/pen

WARNING

Settings Cannot Be Changed After Deployment!

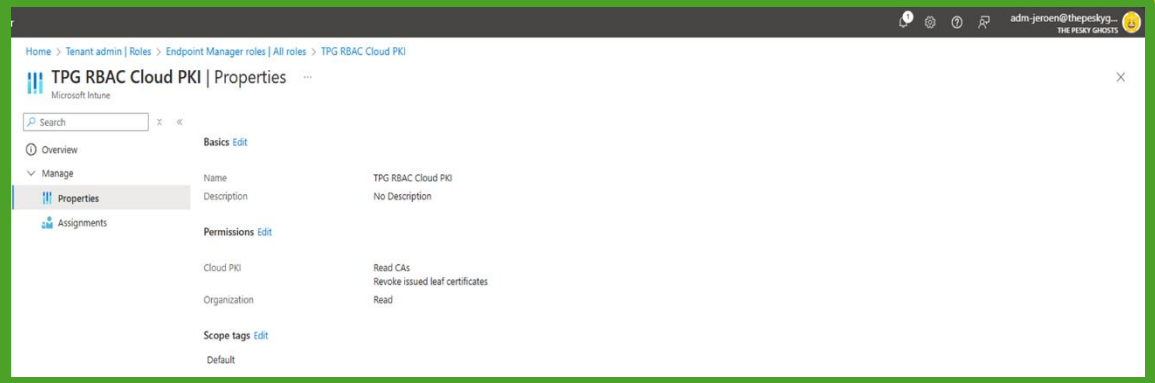
Limit access

Global Administrator

Intune Administrator

Custom Intune role

Demo RBAC


adm-jeroen@thepeskyg...
THE PESKY GHOSTS
Home > Tenant admin | Roles > Endpoint Manager roles | All roles > TPG RBAC Cloud PKI
TPG RBAC Cloud PKI | Properties
Microsoft Intune
Search
Overview
Manage
Properties
Assignments
Basics Edit
Name
TPG RBAC Cloud PKI
Description
No Description
Permissions Edit
Cloud PKI
Read CAs
Revoke issued leaf certificates
Organization
Read
Scope tags Edit
Default

Use cases

- VPN
- Wi-Fi
- Certificate Based Authentication (CBA)
- Sensitive Data/Application Access
- Code Signing Scripts/powershell

Certificate Deployment

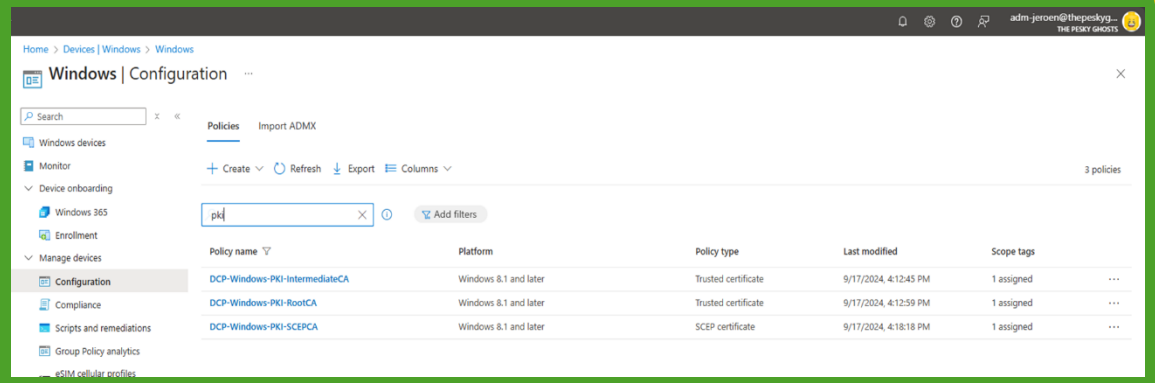
Device Configuration Policies

- Trusted certificate
  - Deploy Root CA Certificate
  - Deploy Issuing CA Certificate

SCEP Certificate

- Entity certificate
  - User
  - Device

Demo deployment



Known issues

- EKU
  - Must be set at Root and Issuing CA
  - EKU **Any Purpose** is blocked
  - Issuing CA can only contain EKU from Root CA
  - Once created, cannot be changed

- A maximum of 6 CAs in an Intune tenant
  - Licensed: Azure mHSM keys can used for 6 CAs
  - Trial: Up to 6 CAs can be created

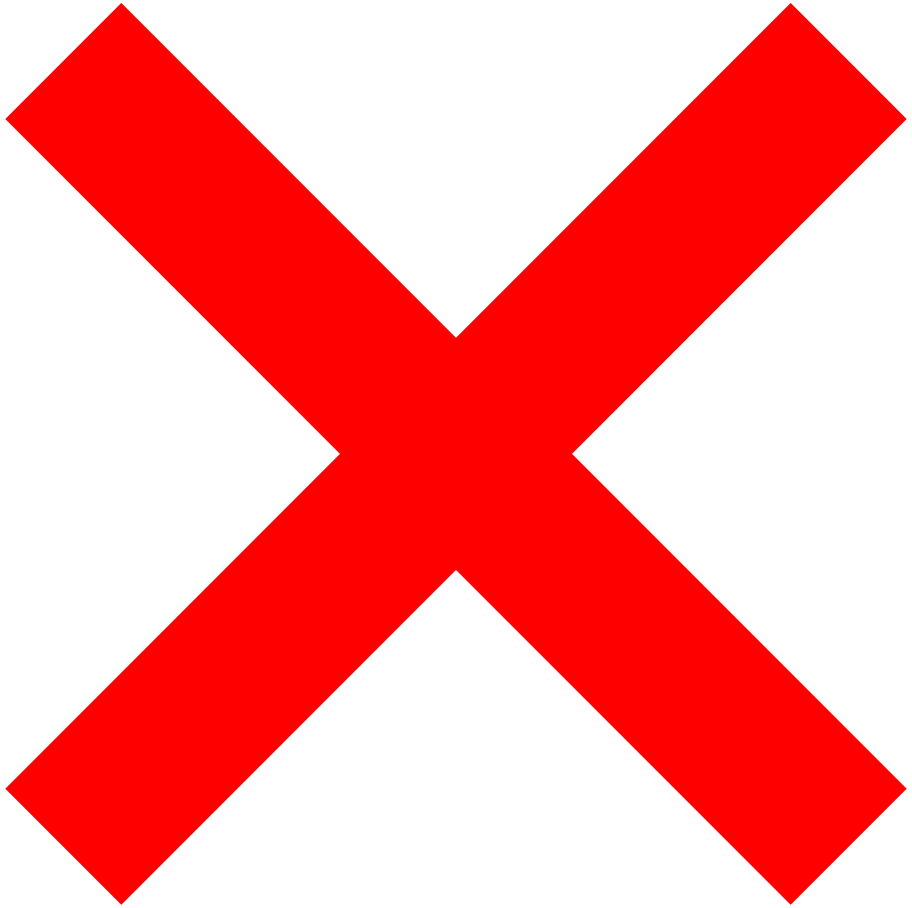
Known issues

- CA types count towards the capacity:
  - Cloud PKI Root CA
  - Cloud PKI Issuing CA
  - BYOCA Issuing CA

- In the Intune admin center, only the first 1000 issued certificates are shown. As a workaround, go to **Devices** > **Monitor**. To view all issued certificates, select **Certifications**

What about radius?

What about radius?



What about radius?

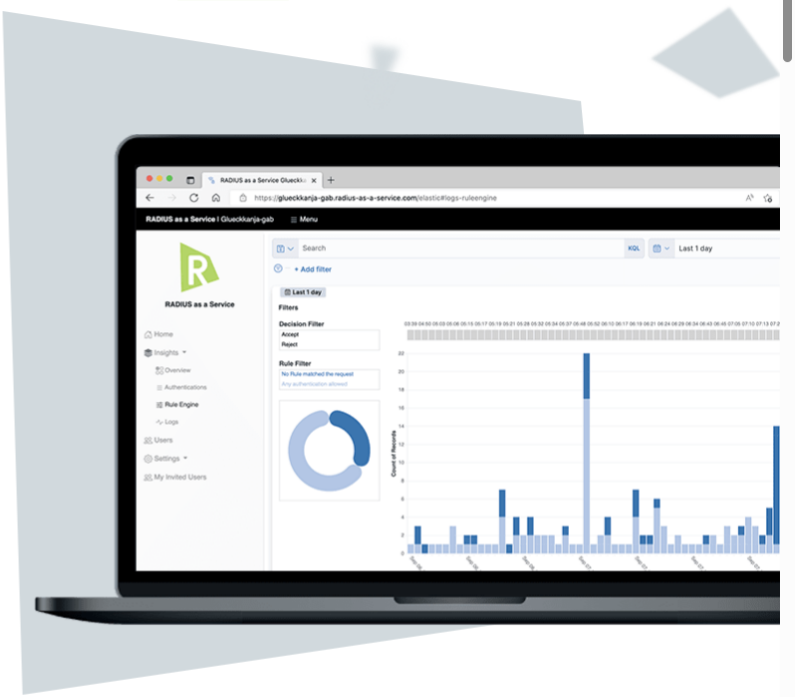
RADIUSaaS

Home Pricing Partners Docs Help About us Start now

RADIUSaaS

Authentication Service for Your Network

Try RADIUSaaS now



RADIUSaaS is a cloud-based RADIUS service that offers easy and secure authentication for network resources. It delivers the comfort, reliability, and scalability of a native cloud SaaS without the hassle of installing,

Bring your own CA

Extending Your Existing On-Premises AD CS Infrastructure to Cloud PKI for Intune

Cloud PKI Issuing CA

Chained to On-Premises Root CA

Benefits

- Control Root of Trust
- Extend AD CS to Cloud
- Eliminate Need for Intune Certificate Connector
  - No PKCS
  - No NDES/SCEP

Questions?

?

Session Feedback

#WPNinjaCH

Thank you