802.1X Network Authentication

AD CS ile Kurumsal A■ Kimlik Do■rulama

Kablolu ve Kablosuz A■lar için Sertifika Tabanl■ EAP-TLS Da■■t■m■

Yazar	Kür■at Bal — System Engineer
■irket	VMind Bilgi ve Teknolojileri A.■.
Ortam	ortakvy.local — Active Directory Domain
Tarih	Haziran 2026
Versiyon	1.0

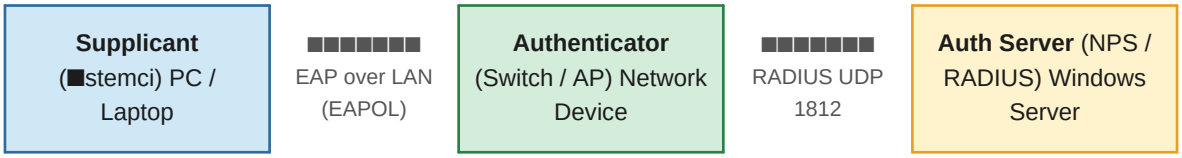
AD CS (PKI) | NPS (RADIUS) | GPO Da■■t■m■ | EAP-TLS | Wireless 802.1X | Wired 802.1X | Sertifika ■ablonlar■ | PowerShell

■çindekiler

1. Giri■ ve Mimari Genel Bak■■

1.1 802.1X Nedir?

IEEE 802.1X, a■ cihazlar■na eri■im öncesinde kimlik do■rulama zorunlulu■u getiren bir port tabanl■ eri■im kontrol standard■d■r. Kablosuz (Wi-Fi) ve kablolu (Ethernet) a■larda çal■■■r. Bir istemci a■a ba■lanmaya çal■■t■■■nda, switch veya Access Point bu iste■i do■rudan kar■■lamaz; kimlik do■rulama trafi■ini bir RADIUS sunucusuna (bu senaryoda NPS) yönlendirir. RADIUS sunucusu do■rulamay■ yapar ve eri■ime izin verir ya da reddeder.



■ekil 1 — 802.1X Üç Bile■en Mimarisi

1.2 EAP-TLS vs PEAP — Neden Sertifika Seçtik?

Özellik	PEAP-MSCHAPv2	EAP-TLS (Seçilen)
■stemci Kimlik Do■rulama	Kullan■c■ ad■ + Parola	X.509 Sertifikas■
Sunucu Kimlik Do■rulama	Sunucu Sertifikas■	Sunucu Sertifikas■
Parola Ele Geçirme Riski	Yüksek (offline brute-force)	Yok
Sertifika Altyap■s■ Gereksinimi	Sadece sunucu	Sunucu + ■stemci
Yönetim Karma■■kl■■■	Dü■ük	Orta (GPO ile otomatize)
Güvenlik Seviyesi	Orta	Yüksek (önerilen)

✓ **Best Practice:** EAP-TLS, sertifika tabanl■ kimlik do■rulama sayesinde parola güvenli■i sorununu ortadan kald■r■r. AD CS + GPO autoenrollment kombinasyonu ile istemci sertifikalar■ otomatik da■■t■l■r, yönetim yükü minimumdur.

1.3 Ortam Bilgileri

Bile■en	Detay
Domain	ortakvy.local
CA Sunucusu	Windows Server 2019 — Enterprise Root CA
NPS Sunucusu	Windows Server 2019 (CA ile ayn■ veya ayr■)
■stemciler	Windows 10/11 — Domain Member

Wireless Infrastructure	802.1X destekli Access Point'ler
Kablolu Infrastructure	802.1X destekli Cisco Switch'ler
Sertifika Geçerlilik Süresi	Bilgisayar: 2 y■l, Kullan■c■: 1 y■l

2. AD CS — Sertifika Altyap■s■ Kurulumu

2.1 CA Rolü Kurulumu (Enterprise Root CA)

Active Directory Certificate Services (AD CS), PKI altyap■s■n■n temelini olu■turur. Enterprise Root CA seçimi, sertifikalar■n Active Directory ile entegre çal■■mas■n■ ve autoenrollment özelli■inin kullan■labilmesini sa■lar.

PowerShell ile CA Kurulumu:

```
# AD CS rolünü kur
Install-WindowsFeature -Name AD-Certificate -IncludeManagementTools

# Enterprise Root CA olarak yap■land■r
Install-AdcsCertificationAuthority `
-CAType EnterpriseRootCa `
-CACommonName 'OrtakVY-Root-CA' `
-KeyLength 2048 `
-HashAlgorithmName SHA256 `
-ValidityPeriod Years `
-ValidityPeriodUnits 10 `
-Force
```

■ **Dikkat:** Production ortam■nda Root CA'y■ offline tutmak best practice'tir. Ancak SMB ölçe■indeki ortamlarda online Enterprise Root CA kabul edilebilir bir trade-off'tur.

2.2 Sertifika ■ablonlar■ Olu■turma

802.1X için iki ayr■ sertifika ■ablonu olu■turulur: biri NPS sunucusu (Bilgisayar/Sunucu kimlik do■rulama), di■eri domain istemcileri için (Bilgisayar kimlik do■rulama). Mevcut ■ablonlar kopyalanarak özelle■tirilir.

■ablon 1 — NPS Server Sertifikas■:

NPS Server Sertifikas■ Ayarlar■

- Kaynak ■ablon: Computer (Windows Server 2003 veya üstü)
- ■ablon Ad■: NPS-Server-Auth
- Subject Name: Build from Active Directory (DNS name dahil)
- Key Usage: Digital Signature, Key Encipherment

- Extended Key Usage: Server Authentication (1.3.6.1.5.5.7.3.1)
- Validity Period: 2 Years | Renewal: 6 Weeks
- Permissions: NPS sunucu bilgisayar hesab■na Read + Enroll
- Publish to AD: Hay■r (sunucu sertifikas■, istemciler taraf■ndan do■rulan■r)

■ablon 2 — ■stemci Bilgisayar Sertifikas■:

Client Computer Sertifikas■ Ayarlar■

- Kaynak ■ablon: Computer (mevcut ■ablonu kopyala)
- ■ablon Ad■: 8021X-Computer-Auth
- Subject Name: Build from Active Directory
- Key Usage: Digital Signature, Key Encipherment
- Extended Key Usage: Client Authentication (1.3.6.1.5.5.7.3.2)
- Validity Period: 2 Years | Renewal: 6 Weeks
- Request Handling: Allow private key to be exported (HAYIR — güvenlik)
- Permissions: Domain Computers grubuna Read + Enroll + Autoenroll

2.3 ■ablonlar■n Yay■nlanmas■

Olu■turulan ■ablonlar■n CA üzerinden yay■nlanmas■ gerekir. Bu i■lem Certification Authority konsolundan yap■l■r.

```
# certutil ile ■ablon yay■nlama
certutil -SetCAtemplates +NPS-Server-Auth
certutil -SetCAtemplates +8021X-Computer-Auth

# Alternatif: CA MMC > Certificate Templates > New > Certificate Template to
Issue
# NPS-Server-Auth ve 8021X-Computer-Auth ■ablonlar■n■ seç
```

✓ **Best Practice:** ■ablon de■i■ikliklerinin AD'ye yay■lmas■ için CA servisini yeniden ba■lat■n veya gpupdate /force çal■■t■r■n. Propagation süresi genellikle 15-30 dakikad■r.

3. NPS (Network Policy Server) Yap■land■rmas■

3.1 NPS Rolü Kurulumu

```
# NPS rolünü kur
Install-WindowsFeature -Name NPAS -IncludeManagementTools

# NPS'i AD'ye kaydet (RADIUS isteklerinin AD hesaplar■na eri■ebilmesi için)
netsh nps add registeredserver domain=ortakvy.local server=

# Alternatif: NPS MMC > NPS (Local) > Register server in Active Directory
```

■ **Dikkat:** NPS sunucusunun AD'ye kay■t i■lemi kritiktir. Kay■t yap■lmadan NPS, kullan■c■/bilgisayar hesaplar■n■ do■rulayamaz ve tüm 802.1X istekleri 'Access-Reject' döner.

3.2 RADIUS Client Tan■mlar■

Her switch ve Access Point, NPS'e RADIUS client olarak eklenir. Shared secret, network cihaz■ ile NPS aras■nda payla■■lan gizli anahtard■r.

```
# PowerShell ile RADIUS Client ekleme
New-NpsRadiusClient `
-Name 'Core-Switch-01' `
-Address '192.168.1.1' `
-SharedSecret 'Guclu_Shared_Secret_2026!' `
-VendorName 'Cisco'

New-NpsRadiusClient `
-Name 'AP-Floor1' `
-Address '192.168.1.10' `
-SharedSecret 'Guclu_Shared_Secret_2026!' `
-VendorName 'Standard'
```

✓ **Best Practice:** Her cihaz için ayn■ shared secret kullanmak yönetimi kolayla■t■r■r. Kritik ortamlarda her switch/AP grubu için farkl■ secret kullan■n. Minimum 22 karakter, karma■■k secret önerilir.

3.3 Connection Request Policy

Connection Request Policy Ayarlar■

- Policy Name: 802.1X-CRP
- Policy Type: Grant access
- Condition — NAS Port Type: Ethernet VEYA IEEE 802.11 Wireless
- Authentication: Authenticate requests on this server (lokal NPS i■ler)
- S■ra (Order): 1 (en yüksek öncelik)

3.4 Network Policy — EAP-TLS

Network Policy, hangi ko■ullarda eri■ime izin verilece■ini tan■mlar. EAP-TLS için sertifika do■rulama zorunlu tutulur.

Network Policy Ayarlar■

- Policy Name: 802.1X-EAP-TLS-Computers
- Access Permission: Grant access
- Condition — Windows Groups: Domain Computers
- Condition — NAS Port Type: Ethernet + Wireless
- Authentication Method: EAP — Microsoft: Smart Card or other certificate
- EAP Type Sertifikas■: NPS-Server-Auth sertifikas■ (CA'dan al■nan)
- Certificate Validation: Verify issuer = ortakvy.local CA
- Constraints — Authentication Methods: SADECE EAP (PEAP/MSCHAPv2 i■aretlenmez)
- Settings — VLAN: Opsiyonel — Tunnel-Type=VLAN, Tunnel-Medium-Type=802, Tunnel-Pvt-Group-ID=

■ **Dikkat:** EAP-TLS policy'de 'Less secure authentication methods' seçeneklerini (MSCHAPv2, PAP) kesinlikle i■aretlemeyin. Bu seçenekler güvenlik modelini bozar.

4. GPO ile Sertifika Otomatik Da■■t■m■

GPO Autoenrollment, domain üyesi bilgisayarlar■n sertifika ■ablonlar■ndan otomatik sertifika talep etmesini sa■lar. Kullan■c■ müdahalesi gerekmez; sertifikalar arka planda al■n■r ve yenilenir.

4.1 Computer Sertifikas■ Autoenrollment GPO

GPO Yolu ve Ayarlar

- GPO Ad■: 8021X-Certificate-Autoenrollment
- Ba■lant■: Domain kök veya hedef OU (örn: OU=Computers,DC=ortakvy,DC=local)
- Yol: Computer Configuration > Windows Settings > Security Settings
- > Public Key Policies > Certificate Services Client - Auto-Enrollment
- Ayar: Enabled
- Seçenek 1: Renew expired certificates... (Süresi dolan sertifikalar■ yenile — ■■ARETLE)
- Seçenek 2: Update certificates that use certificate templates (■■ARETLE)

4.2 User Sertifikas■ Autoenrollment GPO (Opsiyonel)

User Autoenrollment Ayarlar■

- GPO Yolu: User Configuration > Windows Settings > Security Settings
- > Public Key Policies > Certificate Services Client - Auto-Enrollment
- Ayar: Enabled (ayn■ seçenekler i■aretlenir)
- Not: EAP-TLS'yi bilgisayar sertifikas■yla yapt■ysan■z bu ad■m opsiyoneldir
- Kullan■m senaryosu: Kullan■c■ bazl■ kimlik do■rulama isteniyorsa aktif edin

4.3 Trusted Root CA Da■■t■m■

■stemcilerin NPS sertifikas■na güvenebilmesi için CA sertifikas■ tüm bilgisayarlara da■■t■lmal■d■r. Enterprise CA ile kurulumda bu genellikle otomatik gerçekle■ir, ancak manuel kontrol önerilir.

Trusted Root CA GPO Ayarlar■

- GPO Yolu: Computer Configuration > Windows Settings > Security Settings
- > Public Key Policies > Trusted Root Certification Authorities

- ■■lem: Import > CA sertifikas■n■ içe aktar (ortakvy-Root-CA.cer)
- Kontrol: certmgr.msc > Trusted Root Certification Authorities > Certificates
- OrtakVY-Root-CA burada görünüyor olmal■

Sertifika Da■■t■m■ Do■rulama:

```
# ■stemci üzerinde - sertifikalar■ listele
certutil -store My

# Bilgisayar sertifika deposunu kontrol et
Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object {
$_.EnhancedKeyUsageList -like '*Client Authentication*'
} | Select-Object Subject, NotAfter, Thumbprint

# Autoenrollment'■ manuel tetikle (test için)
certutil -pulse
# veya
gpupdate /force
```

5. Kablosuz A■ (Wireless) 802.1X Yap■land■rmas■

5.1 GPO ile Wireless Profile Da■■t■m■

GPO ile istemcilere 802.1X yap■land■r■lm■■ Wi-Fi profili otomatik da■■t■l■r. Bu sayede kullan■c■lar■n manuel a■ yap■land■rmas■ yapmas■ gerekmez.

Wireless Profile GPO Ayarlar■

- GPO Yolu: Computer Configuration > Windows Settings > Security Settings
- > Wireless Network (IEEE 802.11) Policies
- ■■lem: Yeni policy olu■tur — 'Add' > Infrastructure
- Network Name (SSID): Kurumsal Wi-Fi SSID ad■ (örn: ORTAKVY-CORP)
- Connection Type: ESS (Infrastructure Mode)
- Security: WPA2-Enterprise
- Encryption: AES (CCMP)
- Authentication: EAP
- Protected EAP Properties > Authentication Method: Smart Card or other certificate
- Certificate Issuer: OrtakVY-Root-CA (CA'n■z■ seçin)
- Connect automatically: Evet
- Connect even if network is not broadcasting: Opsiyonel

■ **Dikkat:** Wireless GPO'da 'Validate server certificate' seçene■i mutlaka i■aretli olmal■d■r. Bu seçenek devre d■■■ b■rak■l■rsa rogue AP sald■r■lar■na kar■■ koruma ortadan kalkar.

5.2 Access Point Taraf■ Yap■land■rmas■

AP taraf■nda RADIUS sunucu bilgileri ve SSID güvenlik ayarlar■ yap■land■r■l■r. A■a■■daki örnek genel 802.1X destekli AP web arayüzü için geçerlidir.

AP Ayar■	De■er
SSID	ORTAKVY-CORP
Security Mode	WPA2-Enterprise
Encryption	AES
RADIUS Server IP	NPS sunucu IP adresi

RADIUS Port (Auth)	1812
RADIUS Port (Accounting)	1813
Shared Secret	NPS'e girilen shared secret (ayn■ de■er)
RADIUS Accounting	Opsiyonel — aktif edilebilir
MAC Auth Bypass	Devre d■■■ (EAP-TLS kullan■ld■■■nda gereksiz)

6. Kablolu A■ (Wired) 802.1X Yap■land■rmas■

6.1 GPO ile Wired Autoconfig Servisi

Kablolu 802.1X için öncelikle 'Wired AutoConfig' servisinin çal■■mas■ gerekir. GPO ile bu servis otomatik ba■lat■l■r.

Wired AutoConfig GPO Ayarlar■

- Servis GPO Yolu: Computer Configuration > Windows Settings > Security Settings > System Services
- Servis: Wired AutoConfig (dot3svc) — Startup: Automatic
- Wired Policy GPO Yolu: Computer Configuration > Windows Settings > Security Settings
- > Wired Network (IEEE 802.3) Policies
- ■■lem: Yeni policy olu■tur
- Security Type: 802.1X
- Authentication: User or Computer authentication (veya Computer only)
- EAP Type: Smart Card or other certificate
- Validate server certificate: Evet
- Trusted Root CA: OrtakVY-Root-CA

6.2 Switch Port Yap■land■rmas■ (Cisco)

Cisco switch üzerinde her port için 802.1X aktif edilir. Kritik portlar için (yaz■c■, IP telefon) MAB (MAC Authentication Bypass) ek olarak yap■land■r■labilir.

```
! Global RADIUS yap■land■rmas■
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

radius server NPS-Primary
address ipv4 auth-port 1812 acct-port 1813
key Guclu_Shared_Secret_2026!

! 802.1X global aktivasyon
dot1x system-auth-control
```

```
! Access port yap■land■rmas■
interface GigabitEthernet1/0/1
description Workstation-Port
switchport mode access
switchport access vlan 10
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast

! Opsiyonel: Unauthorized VLAN (kimlik do■rulama ba■ar■s■zsa)
authentication event fail action authorize vlan 999
authentication event no-response action authorize vlan 999
```

✓ **Best Practice:** Guest VLAN ve Auth-Fail VLAN yap■land■rmas■, domain d■■■ cihazlar■n s■n■rl■ a■a eri■imini sa■lar. Bu sayede misafir cihazlar tamamen bloke edilmek yerine yönlendirilebilir.

7. Test ve Do■rulama

7.1 NPS Event Log Kontrolü

NPS tüm kimlik do■rulama i■lemlerini Event Log'a yazar. Ba■ar■l■ ba■lant■lar Event ID 6272, ba■ar■s■zlar 6273 olarak loglan■r.

```
# PowerShell ile NPS loglar■n■ sorgula
Get-WinEvent -LogName 'Security' | Where-Object {
$_.Id -in @(6272, 6273)
} | Select-Object TimeCreated, Id, Message | Format-List

# Son 50 NPS event
Get-WinEvent -LogName 'Security' -MaxEvents 50 | Where-Object { $_.Id -in
@(6272,6273) }

# Event Viewer > Security Log > Filter: Event ID 6272 (success), 6273 (failure)
```

NPS Log Analizi:

Event ID	Anlam	Kontrol Edilecek Alan
6272	Network Policy Server granted access (Ba■ar■l■)	Account Name, Policy Name
6273	Network Policy Server denied access (Reddedildi)	Reason Code — hata sebebi
6274	Network Policy Server discarded request	NPS'e ula■an ama i■lenemeyen istek
6278	NPS granted full access (quarantine sonras■)	NAP kullan■l■yorsa

7.2 ■stemci Taraf■ Do■rulama

```
# Sertifika deposunu kontrol et
certmgr.msc
# Personal > Certificates > 8021X-Computer-Auth sertifikas■ görünmeli

# A■ ba■lant■ durumu
netsh lan show interfaces
netsh wlan show interfaces

# EAP durumu
netsh eap show interface
```

```
# gpupdate ile policy ve sertifika yenile
gpupdate /force
certutil -pulse # Autoenrollment tetikle
```

7.3 S■k Kar■■la■■lan Hatalar ve Çözümleri

Hata / Belirti	Muhtemel Sebep	Çözüm
Event 6273 Reason 16	Authentication failed — sertifika yok veya geçersiz	■stemcide sertifika kontrolü: certmgr.msc > Personal
Event 6273 Reason 22	Sertifika süresi dolmu■	CA'da renewal kontrol et, autoenrollment GPO'yu do■rula
Event 6273 Reason 48	CA'ya güven yok	Trusted Root CA GPO'nun uyguland■■■n■ do■rula
NPS sertifika görmüyor	NPS sunucusu CA'dan sertifika almam■■	certmgr.msc (Local Computer) > Personal'da NPS-Server-Auth olmal■
Switch port aç■lm■yor	Shared secret uyu■muyor	NPS RADIUS client ve switch config'deki secret'■ kar■■la■t■r
Wired 802.1X çal■■m■yor	dot3svc servisi çal■■m■yor	services.msc > Wired AutoConfig > Automatic + Start
GPO uygulanm■yor	gpresult /r ç■kt■s■nda policy yok	OU ba■lant■s■n■ ve filtre ayarlar■n■ kontrol et

8. Sonuç ve Best Practice Özeti

802.1X + AD CS + NPS kombinasyonu, kurumsal a■larda port tabanl■ eri■im kontrolü için en olgun ve güvenilir çözümlerden birini sunmaktad■r. Sertifika tabanl■ kimlik do■rulama sayesinde parola odakl■ sald■r■ vektörleri devre d■■■ kal■r; GPO autoenrollment ile operasyonel yük minimumdur.

Best Practice Kontrol Listesi:

AD CS

- ■ Enterprise Root CA — SHA256, 2048-bit minimum
- ■ Sertifika ■ablonlar■nda minimum gerekli izinler (Domain Computers: Enroll + Autoenroll)
- ■ ■ablon geçerlilik süresi makul (bilgisayar 2 y■l, kullan■c■ 1 y■l)
- ■ Private key export izni kapal■

NPS

- ■ NPS'i AD'ye kay■t et (netsh nps add registeredserver)
- ■ Her RADIUS client için güçlü ve benzersiz shared secret
- ■ Sadece EAP-TLS kabul et, zay■f metodlar■ devre d■■■ b■rak
- ■ NPS sertifikas■n■n FQDN'i ile uyumlu SAN içermesini sa■la

GPO

- ■ Autoenrollment her iki kutucu■u da i■aretli olmal■
- ■ Wireless/Wired policy'de 'Validate server certificate' aç■k
- ■ Trusted Root CA GPO ile da■■t■lm■■
- ■ Wired AutoConfig servisi otomatik ba■latma

Network

- ■ Switch/AP'lerde auth-fail VLAN tan■ml■ (misafir/bilinmeyen cihaz izolasyonu)
- ■ NPS sunucusuna eri■im için güvenlik duvar■: UDP 1812, 1813
- ■ Printers, IP phones için MAB (MAC Auth Bypass) ek önlem olarak yap■land■r■l
- ■ NPS log'lar■n■ düzenli izle (SIEM entegrasyonu önerilir)

Mimari Özeti:

Katman	Bile■en	Görev
PKI	AD CS — Enterprise Root CA	Sertifika üretimi ve yönetimi
Auth Server	NPS (Network Policy Server)	RADIUS — kimlik do■rulama karar■
Policy	Active Directory + GPO	Sertifika da■■t■m■ + network profile

Authenticator	Switch / Access Point	Port eri■im kontrolü
Supplicant	Windows 10/11 Domain PC	EAP-TLS ile kimlik kan■tlama