Experts Live Austria

CISO's delight
SMB over QUIC meets iaKerb & Local KDC in Windows Server 2025

Didier Van Hoye

Technical Architect & Technology Strategist

Microsoft MVP Most Valuable Professional

VEEAM VANGUARD

Experts Live Austria

Thanks to our sponsors!

PLATINUM

ACP IT for innovators.

ConStraight

mann&mouse WE LIVE IT

base it

THOMAS KRENN® IT's people business

GOLD

CANCOM

DATACIDERS PASO

NiCE IT Management Solutions www.nice.de

INFOTECH [IT & Communication]

SEPP MAIL

ProLion

Agenda

- What is QUIC, what does it do, why, and how
- SMB over QUIC positioning and use cases
- Kerberos, NTLM, KDC Proxy, IAKerb & Local KDC
- Configuration tips & demos

QUIC

A quick word about QUIC

What is QUIC?

Started life at Google as gQUIC (Quick UDP Internet Connection)

Today QUIC is an IETF-standardized transport protocol

Wide, growing industry backing and support …

What is QUIC?

Replaces TCP with an (initially) Internet-oriented UDP mechanism that improves performance and congestion handling

QUIC strives to maintain TCP's reliability & broad applicability

QUIC is **always encrypted** and **requires TLS 1.3** with certificate authentication to establish the tunnel

Not just for “Internet browsers” => also **SMB**, DNS, SSH, SIP, WebSocket, MQTT, VPN, …

Microsoft created **MsQuic**, their open-source implemer the IETF QUIC transport protocol ➔ GitHub - microsof

MsQuic

What “caused” QUIC?

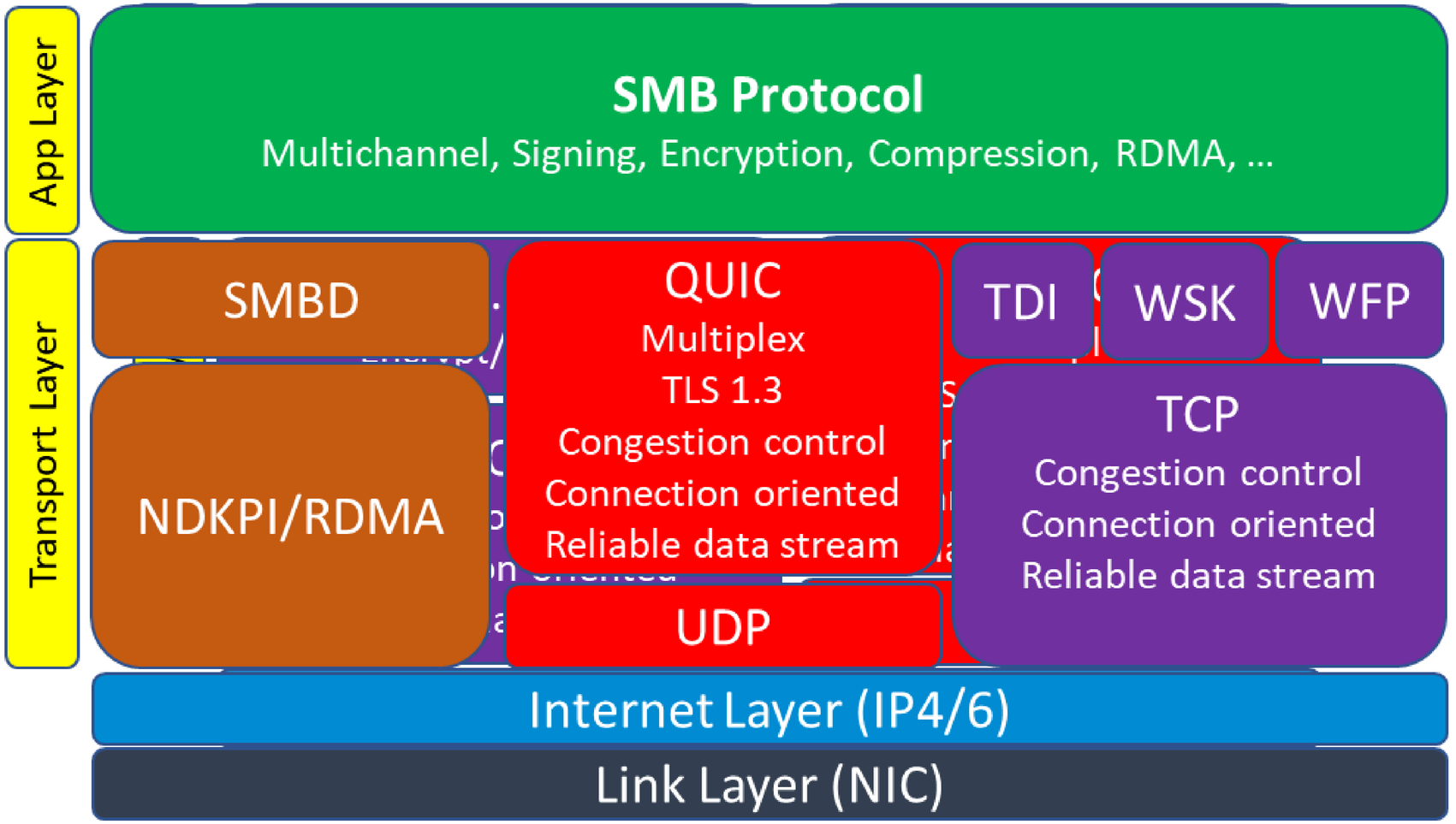
Too intimate coupling of HTTP/2 with TCP/IP

The “middle boxes” on the internet

- Routers
- Load Balancers
- Firewalls
- Proxies
- …

Both are slow to evolve and hinder progress

We got HTTP/3 in the process and it doesn’t exist without QUIC

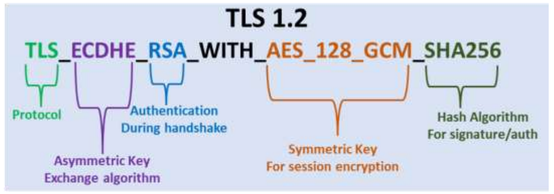


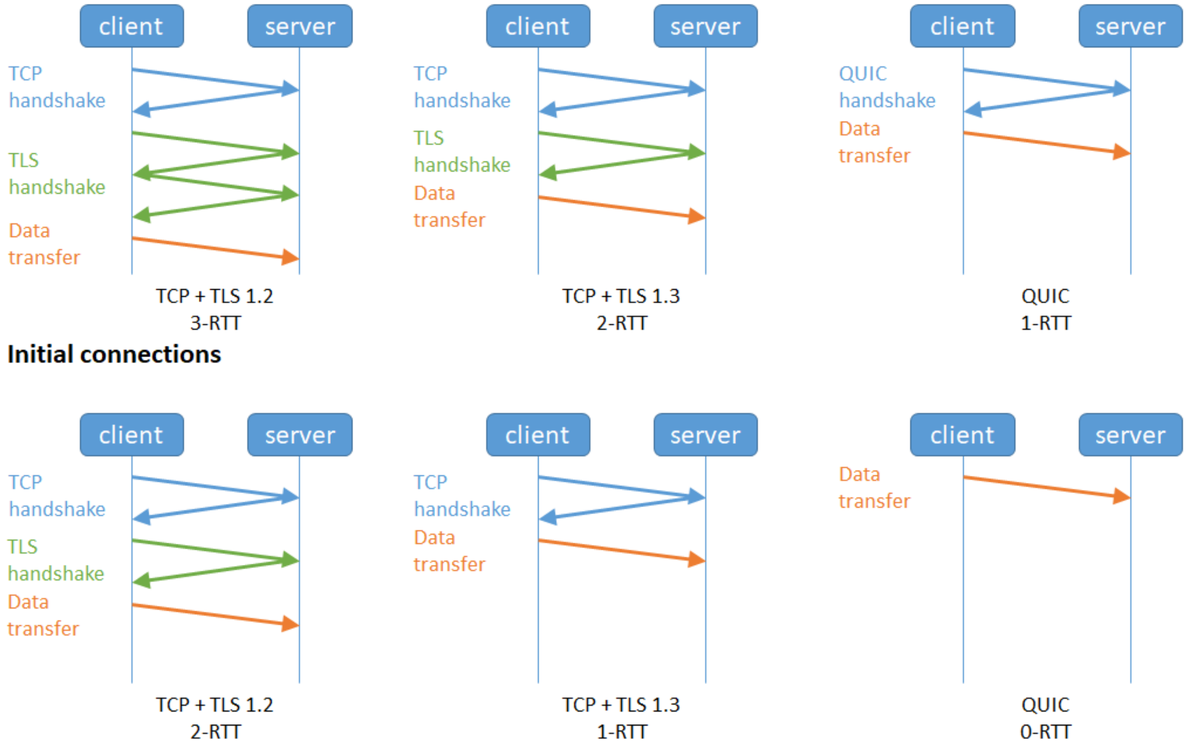
(Image by Dirk Van Hoye)

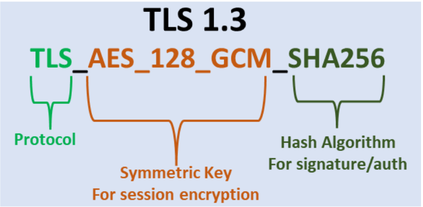
Goals of QUIC (1/4)

1. QUIC reduces connection times over TLS

- Replaces lengthy TCP & TLS handshake with a single handshake



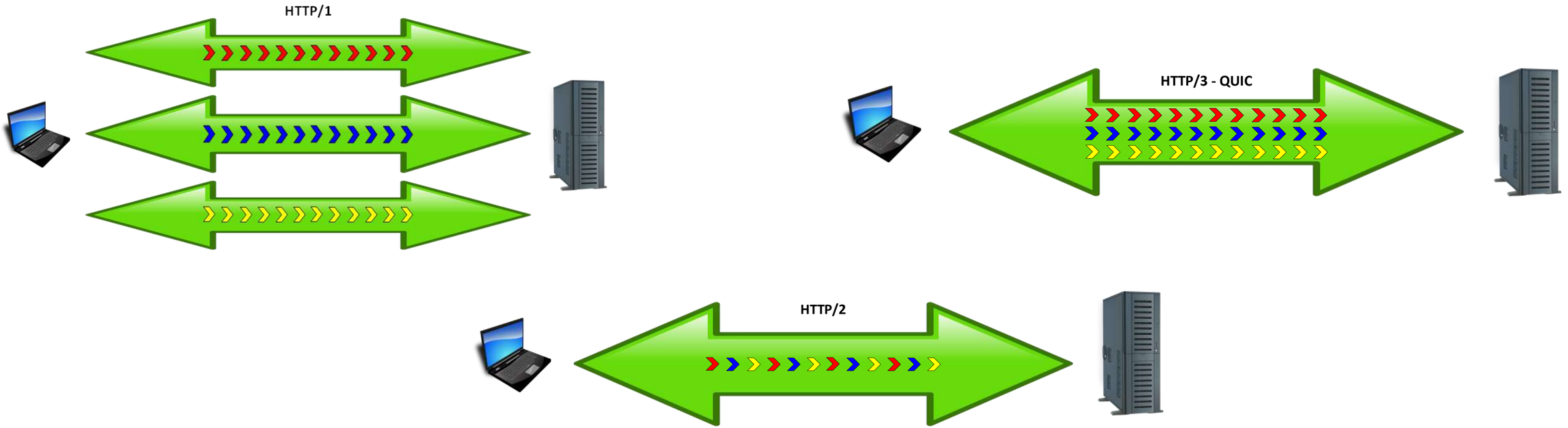




Images by Didier Van Hoye

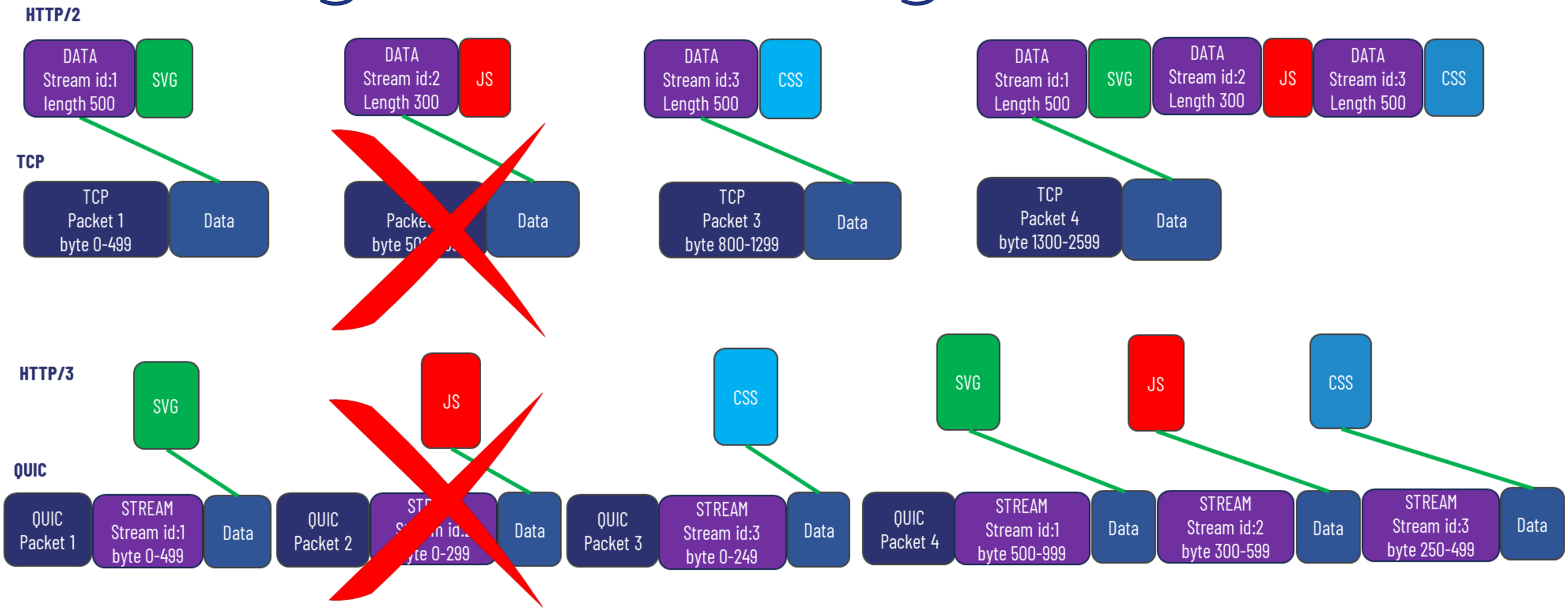
Goals of QUIC (2/4)

2. QUIC delivers better performance in case of data packet loss – Head of Line (HOL) blocking



Images by Didier Van Hoye

Solving HOL blocking



Goals of QUIC (3/4)

3. ~~Deal with the data transfer overhead of TCP, which QUIC with UDP avoids~~ Prevents the dependency on TCP and middle boxes delaying the progress in performance, features, and security
4. Better congestion control & loss detection
    - QUIC ACKs explicitly encode delay for precise RTT estimates
    - Accurate RTT estimations improve delay-sensing controllers
    - More resilient to loss & reordering
    - Prioritization of data
5. Connection reuse: server to client session ticket in TLS 1.3

Goals of QUIC (4/4)

6. Easy connection migration (network changes) = more stable connections.
   - With TCP, when your network changes your connection times out and needs to reestablish.
   - QUIC uses “unique identifiers” to make this process smoother. Reestablishing these is done by sending a packet instead of establishing a new connection, even when your IP address changes.
7. Easy development encourages adoption
   - QUIC can be implemented on the application level, making it easier to do and allowing for more flexibility.
   - TCP is part of the operating system kernel, you are dependent on that implementation.

Privacy Concerns

Image by Pete Linforth from Pixabay

Replay attacks via TLS session resumption (0-RTT)

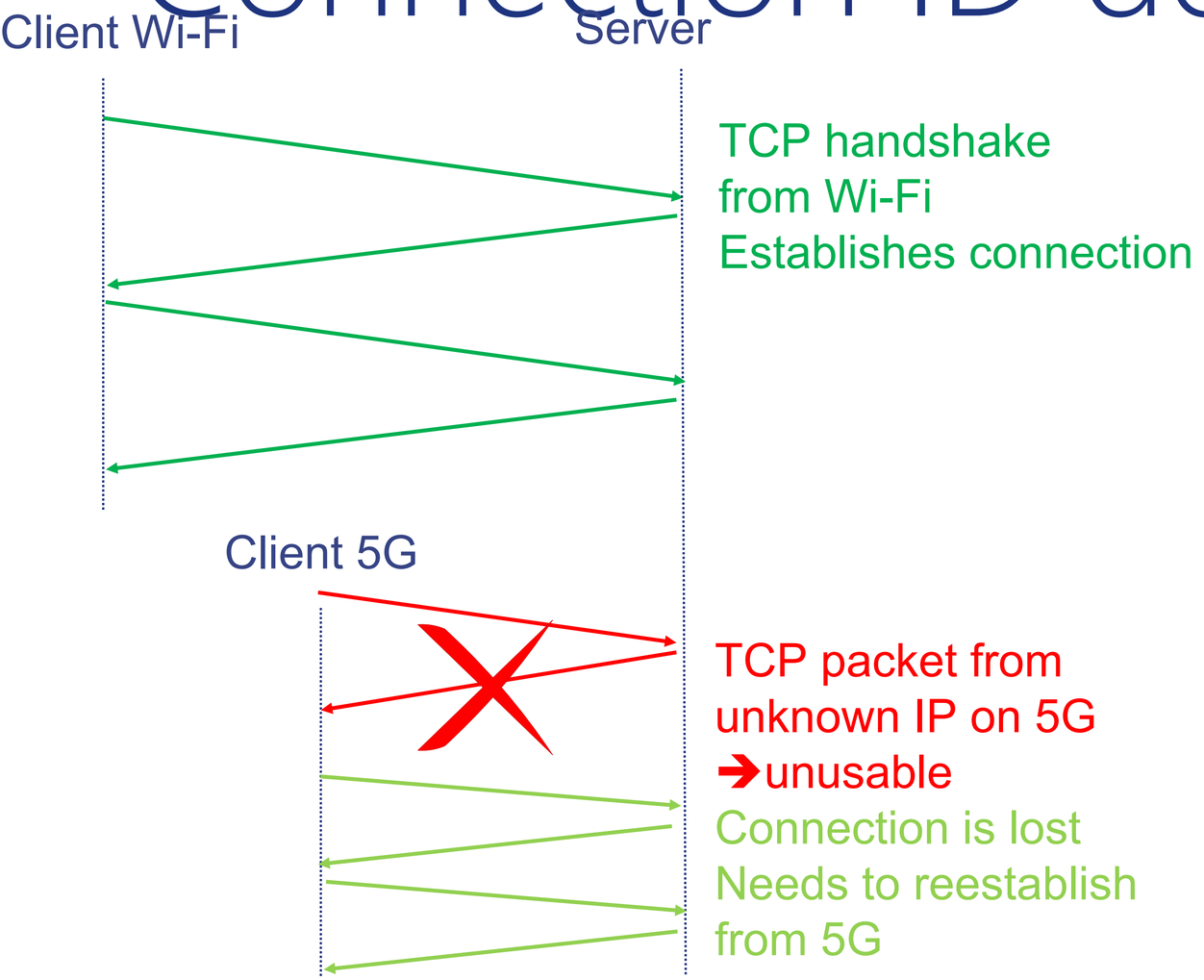
- Idempotency requirements
- App layer mitigations

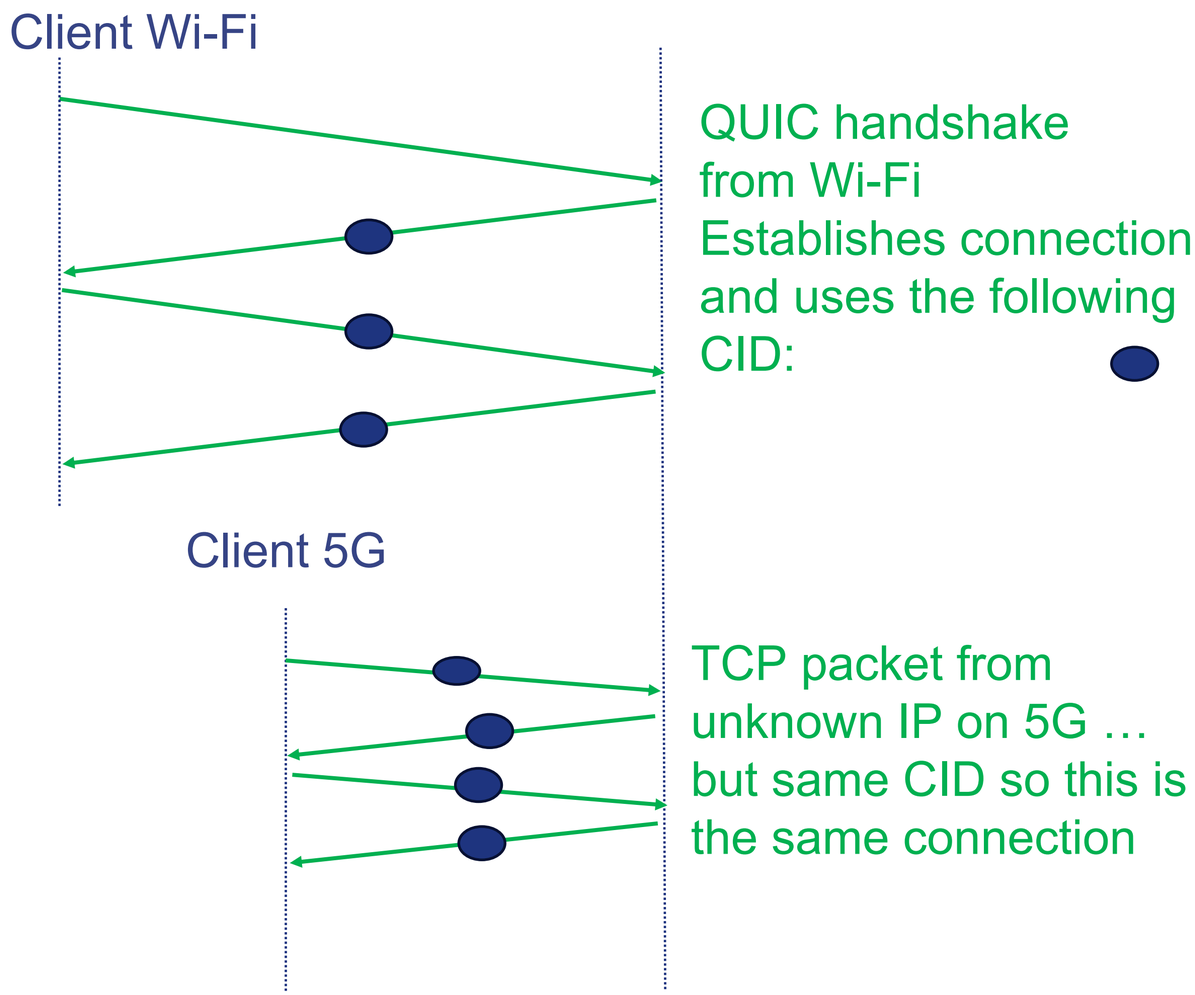
User tracking via Google's QUIC's (gQUIC) server config

- Connection ID's are not static, differ from client and server and only the ones used publicly are non-encrypted

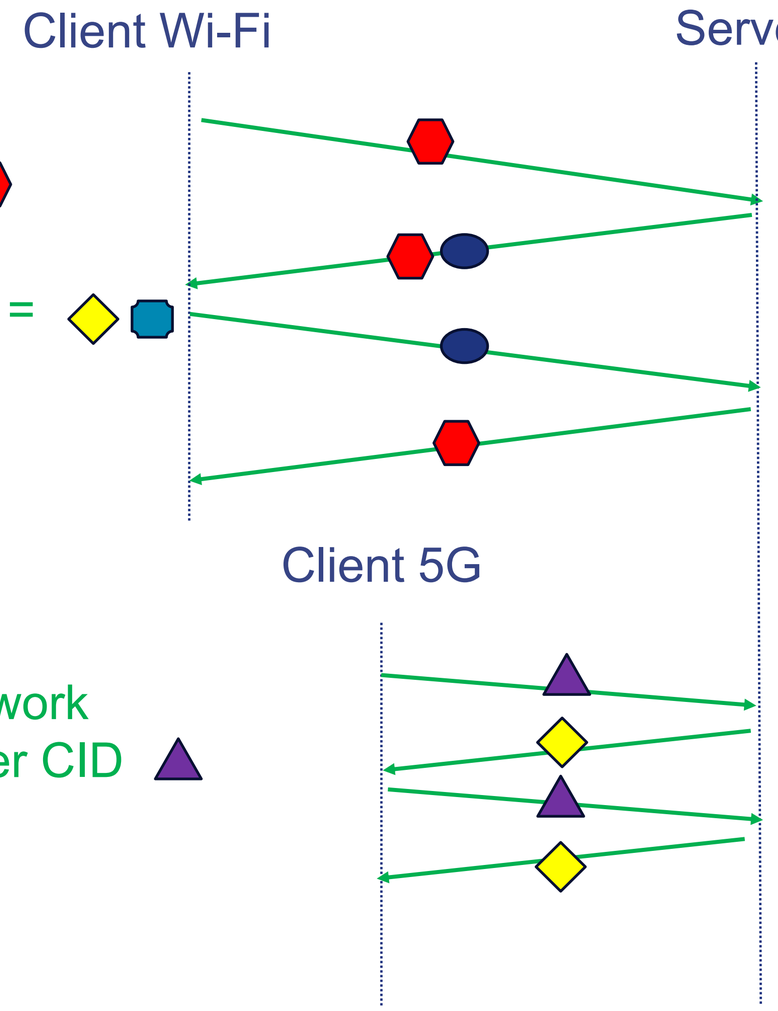
Web browsers will evolve to protect the user's privacy enough against these tracking mechanisms

Connection ID details





Asymmetric Linkability Prevention



Unencrypted:
My Client CID =

Encrypted:
Future Client CIDs =

QUIC handshake
from Wi-Fi
Establishes connection
Unencrypted:
Server CID =
Encrypted:
Future Server CIDs =

Each connection has multiple client and source CIDs associated

Client and serve choose their own CIDs

Connection IDs change over time (not just at reconnect)

Client switched network and now uses server CID

TCP packet from unknown IP on 5G … but it uses a communicated future server CID I know maps to
So this is the same connection
But I must switch to future client CID

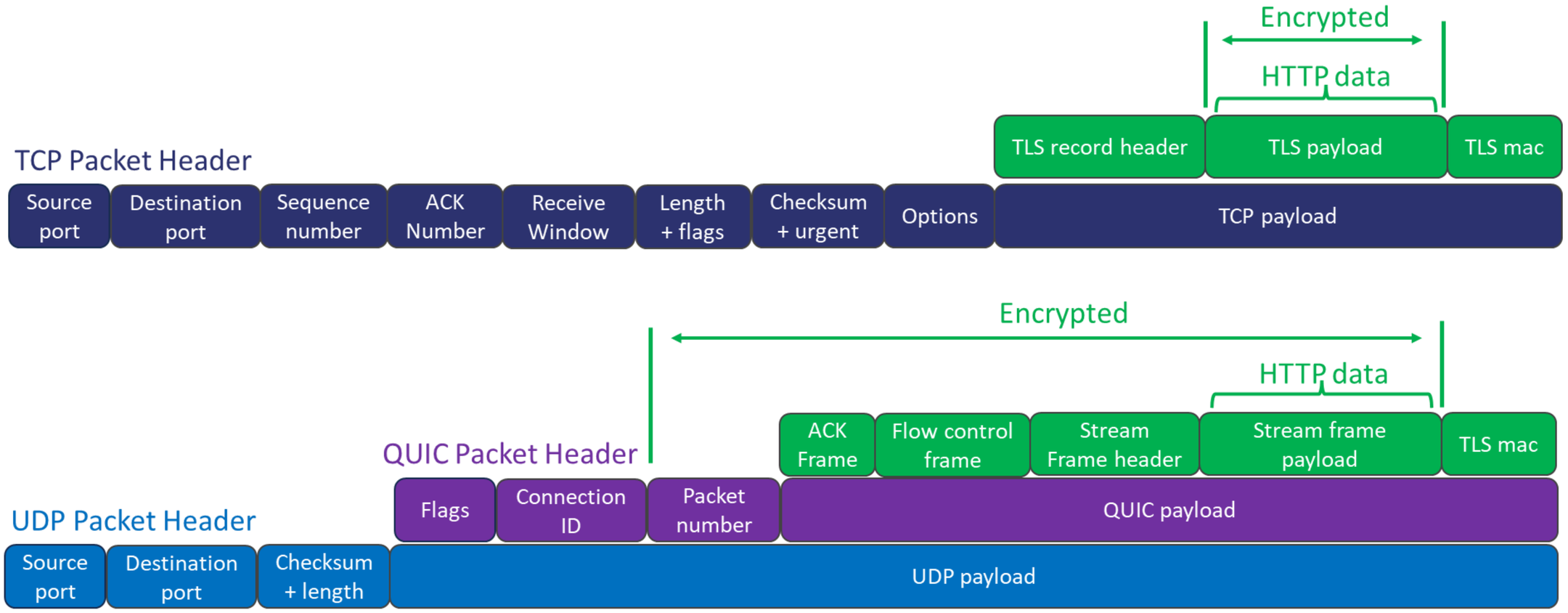
Client & Server future CIDs are communicated encrypted
The mapping to public original client/server CIDs is only known to client/server.

Security Critiques & FUDs

- Our firewalls are blind as a mole now
- TLS inspection is dead
- Bad for app visibility & control
- Breaks DDOS detection/prevention (UDP)
- Logging and Reporting
- Search term alerts, YouTube viewing lists

https://www.cleanpng.com/png-firewall-computer-icons-computer-network-clip-art-1182907/download-png.html
https://www.cleanpng.com/png-mole-cartoon-png-clipart-image-59940/download-png.html

Simplified TCP & UDP/QUIC header



Challenges, Inertia

QUIC doesn't make my app 3x faster ➔ Not meant to, performance gains at the provider & user side

I don't have issues with reconnection, HOL, … ➔ Me vs We discussion ;-)

QUIC doesn't do 25Gbps

- Does it have to do so for current use cases?
- Not yet. See Making MsQuic Blazing Fast - Microsoft Tech Community, https://microsoft.github.io/netperf/dist

Inertia

- If there is no need for the benefits of QUIC apps might forgo the effort
- Lots of endpoints in sensors & IoT barely speak TLS let alone can speak QUIC
- Security appliance's mental breakdown

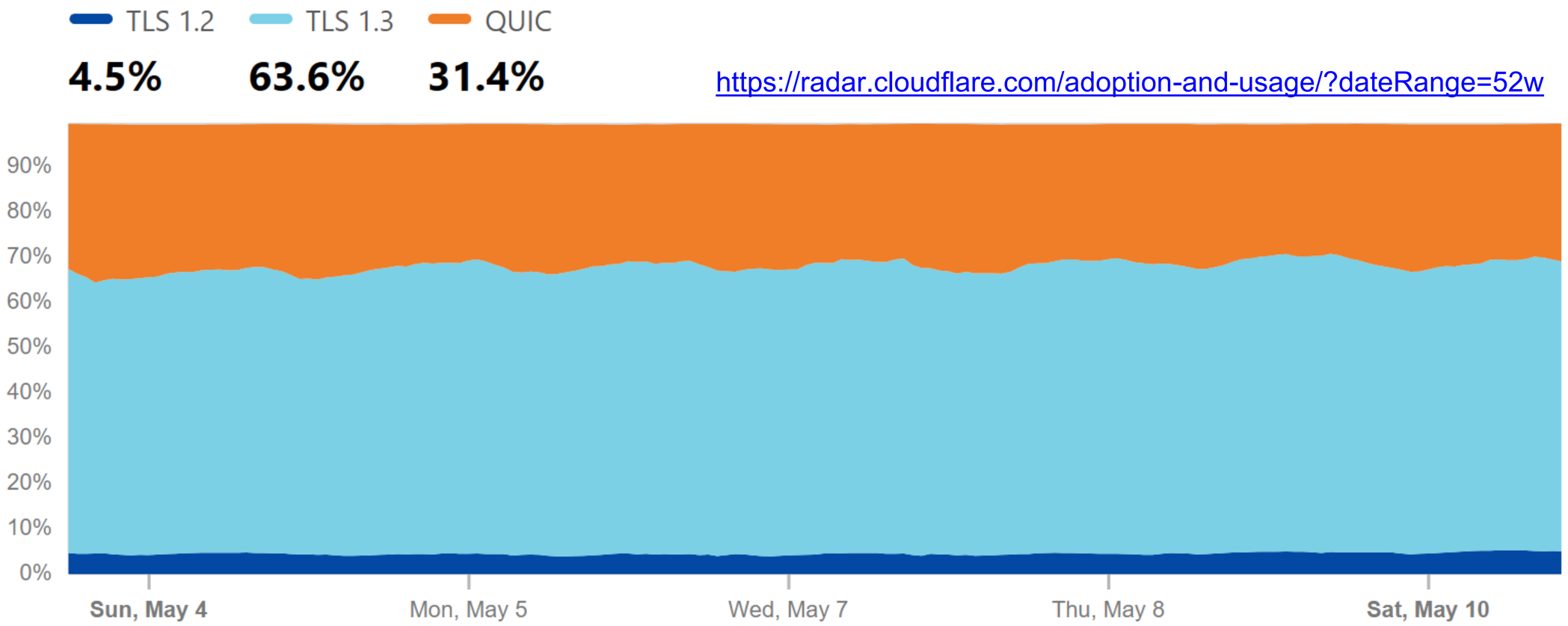
UDP: not all internet routers, and appliances are ready for this

NAT/ECMP (5 Tuple vs Connection ID)

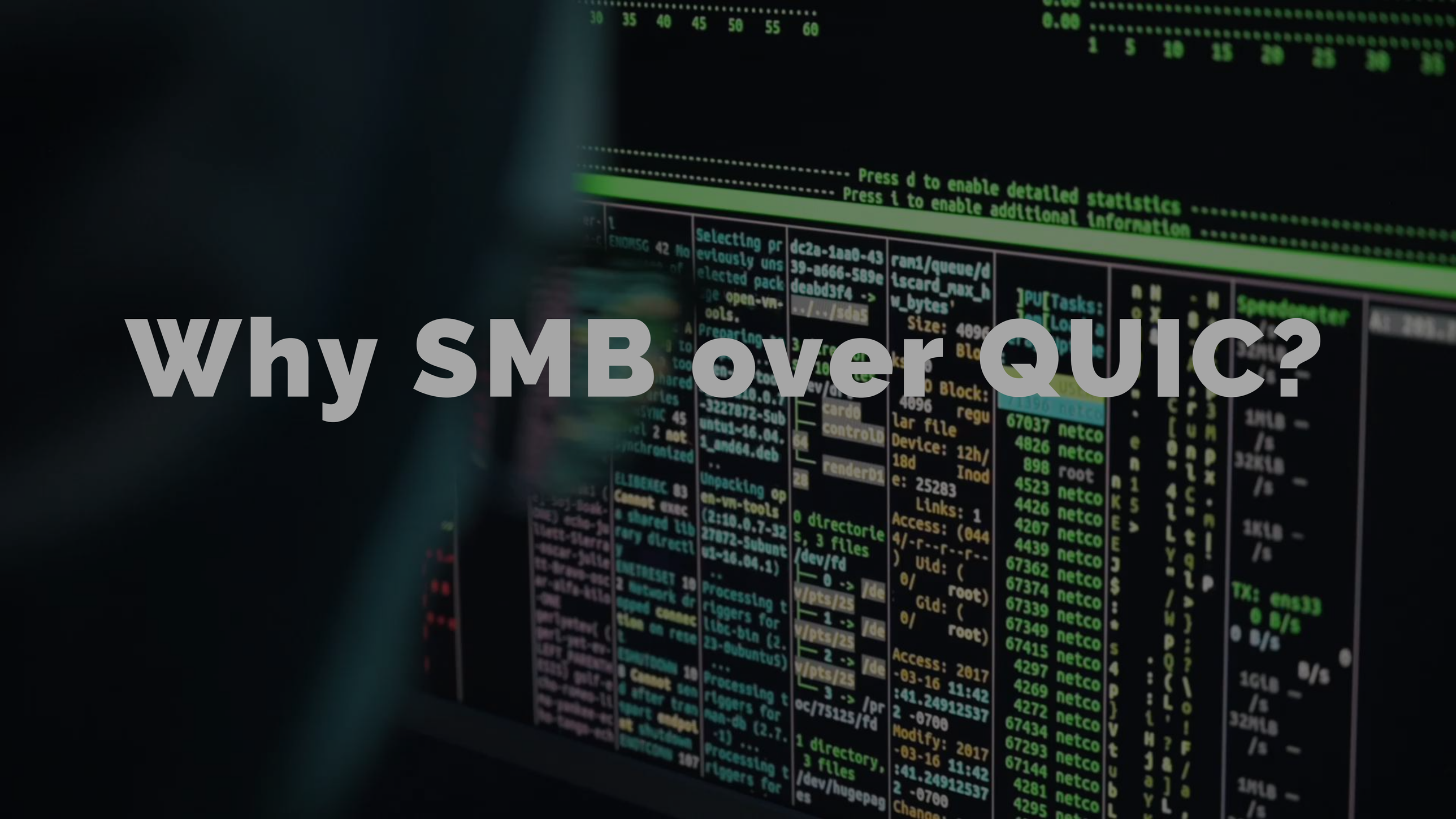
QUIC Adoption

TLS 1.2 vs. TLS 1.3 vs. QUIC

Distribution of secure HTTP requests by protocol



https://radar.cloudflare.com/adoption-and-usage/?dateRange=52w



Why SMB over QUIC?

Prime use case: Azure File Share

Accessing Azure File Shares from Servers, Clients, Smartphones, IoT, embedded devices, sensors, …

Israel Andrade on Unsplash

- Port 445 blocked Firewalls and by I
- Prevents Mapping Azure File Shares
- QUIC resolves this blocking factor securely and efficiently
- HTTPS/443 allowed on corporate firewall
- Add UPD and you're in business

Target Audiences

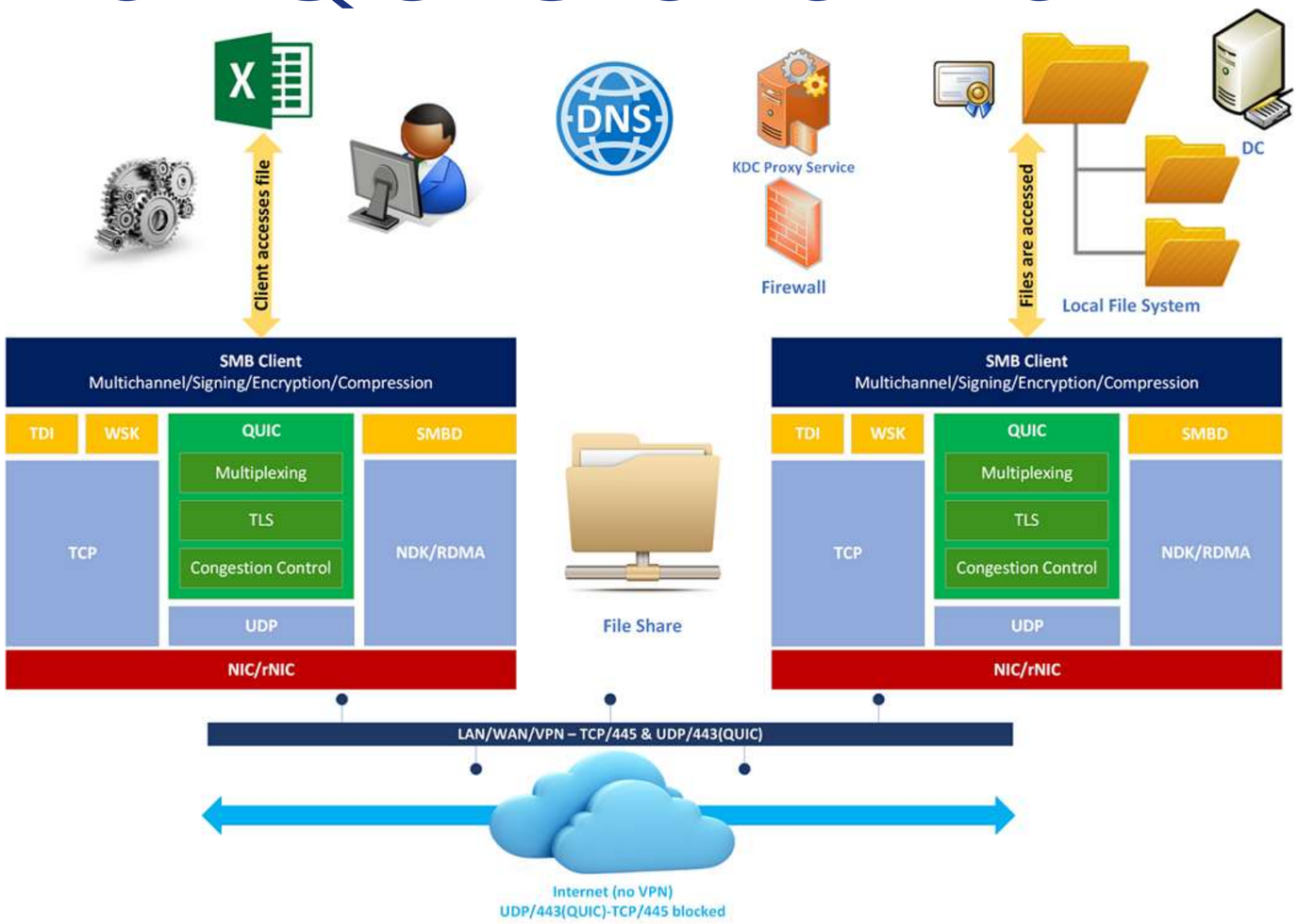
- Telecommuters
- Road Warriors
- Work From Anywhere
  - ➢ VPN free solution
  - ➢ Transparent Experience
  - ➢ No ISP/Firewall issues
  - ➢ No HOL blocking
  - ➢ TLS 1.3 benefits
    - ✓ Better congestion control
    - ✓ Easy network changes
    - ✓ Less RTTs = less latency, better performance
    - ✓ 0-RTT

whereslugo on Unsplash

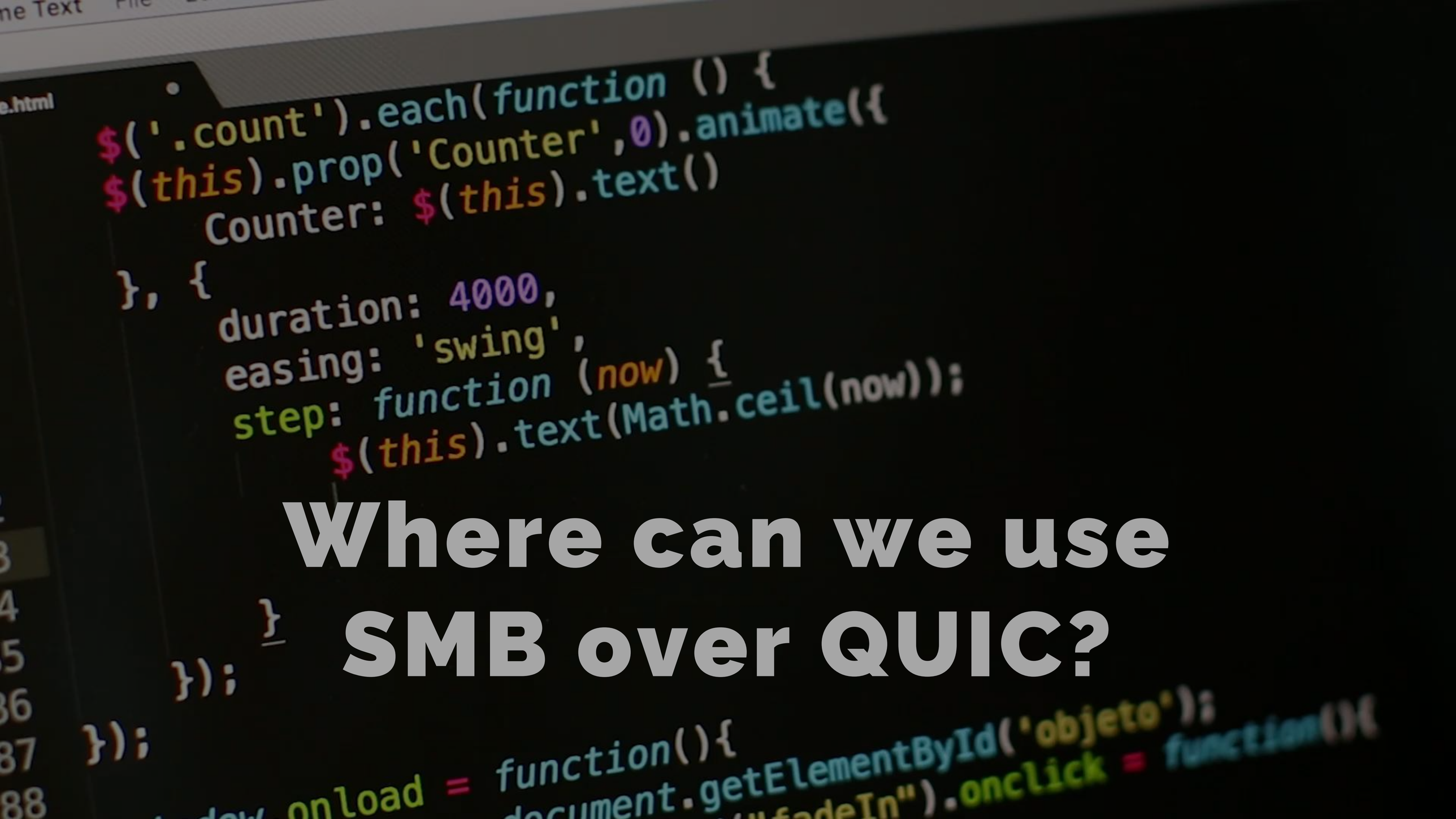
Standsome Worklifestyle on Unsplash

Helena Lopes on Unsplash

SMB over QUIC overview



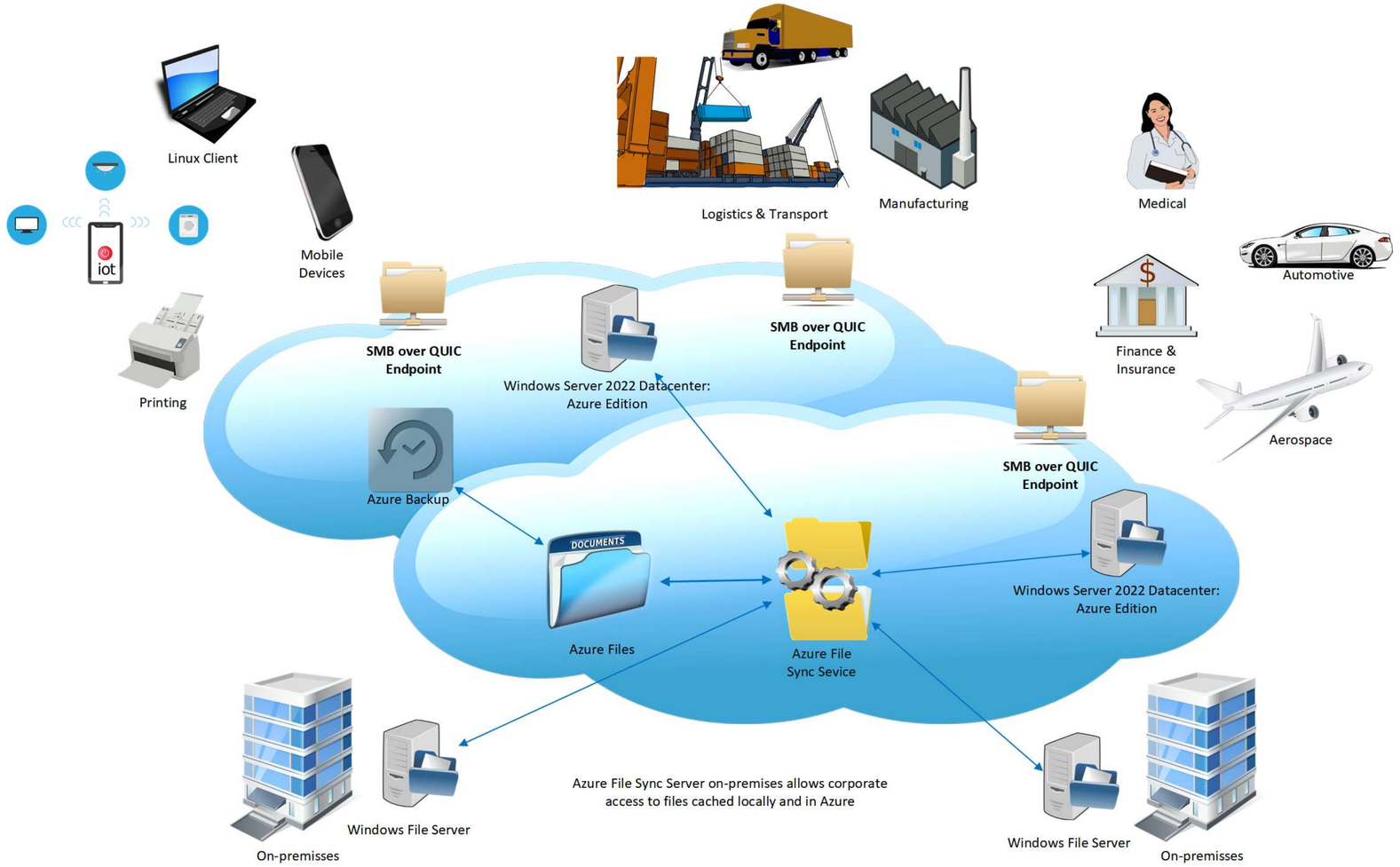
Images by Didier Van Hoye


Where can we use
SMB over QUIC?

Support for SMB over QUIC?

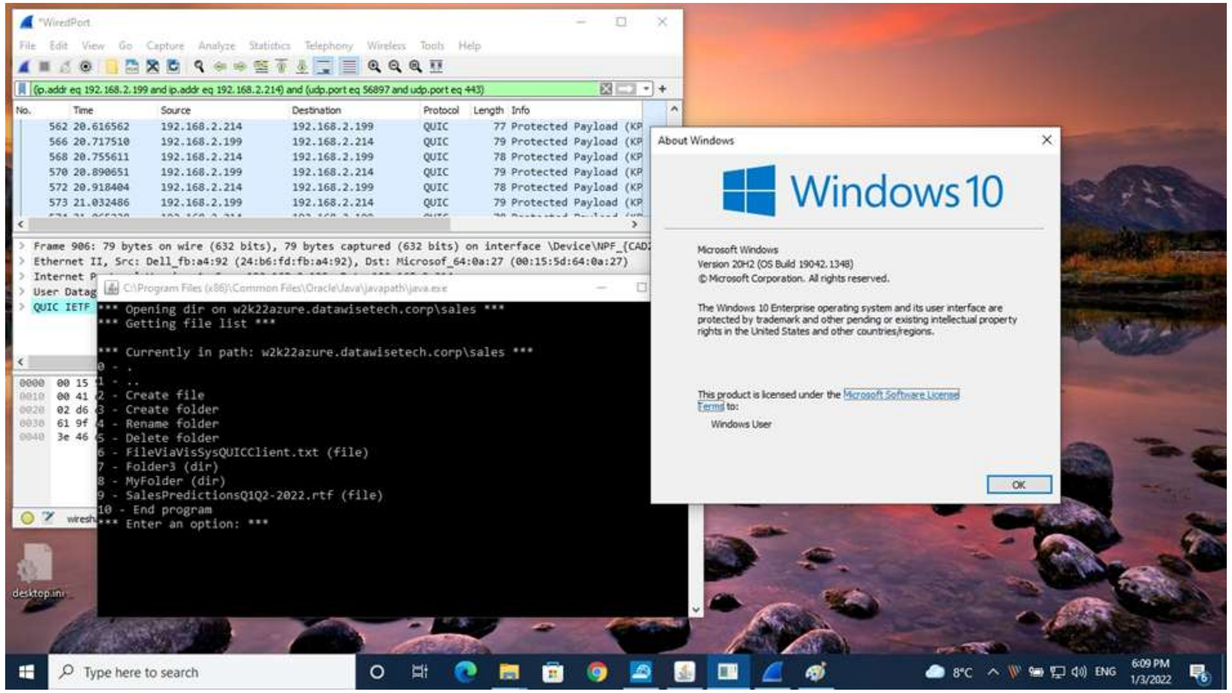
- Windows Server 2022 Datacenter: Azure Edition
  - Runs in Azure IaaS and Azure Stack HCI – nowhere else
- Windows Server 2025 – **all SKUs**
  - Runs anywhere ☺
- Windows 11
- Is that it?
  - Lack of clients is a roadblock to adoption
  - Luckily, it is not! 3rd party expert solutions fill the gap!
- Sadly missing in Azure Files!

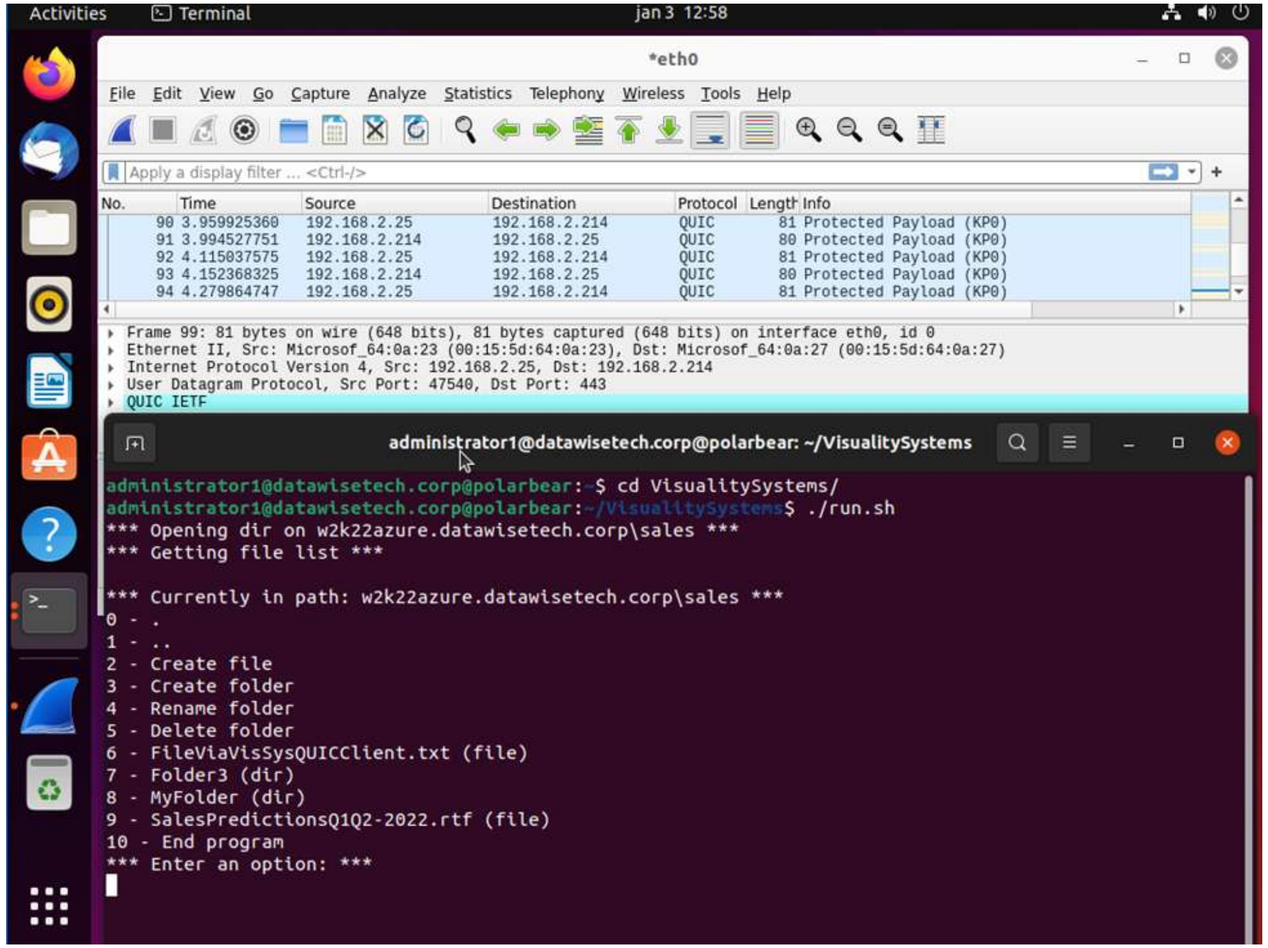
Servers, Clients, Smartphones, IoT, embedded devices, sensors, …



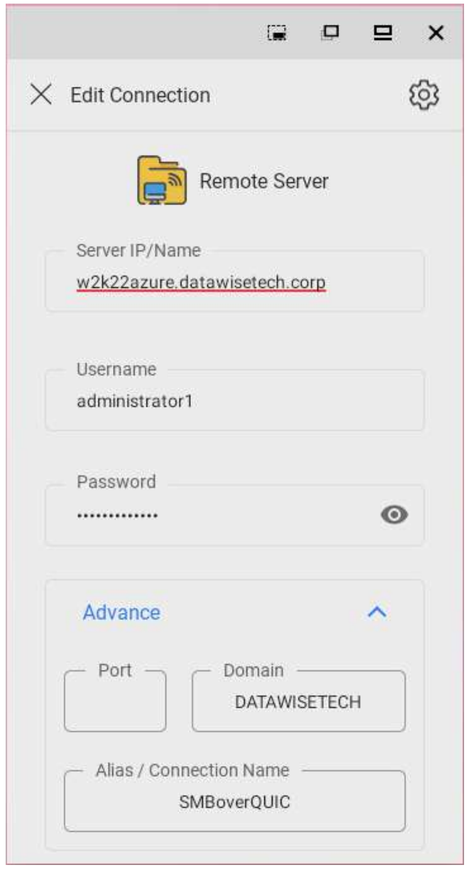
Images by Didier Van Hoye

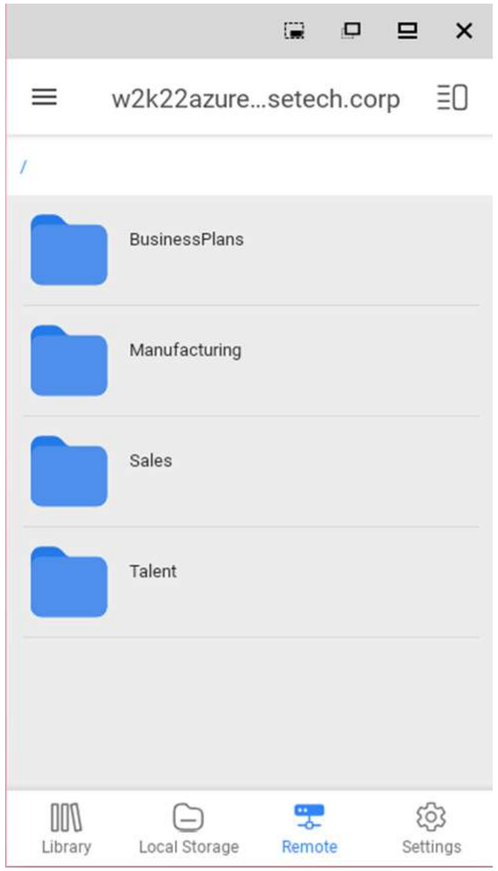
Other operating systems

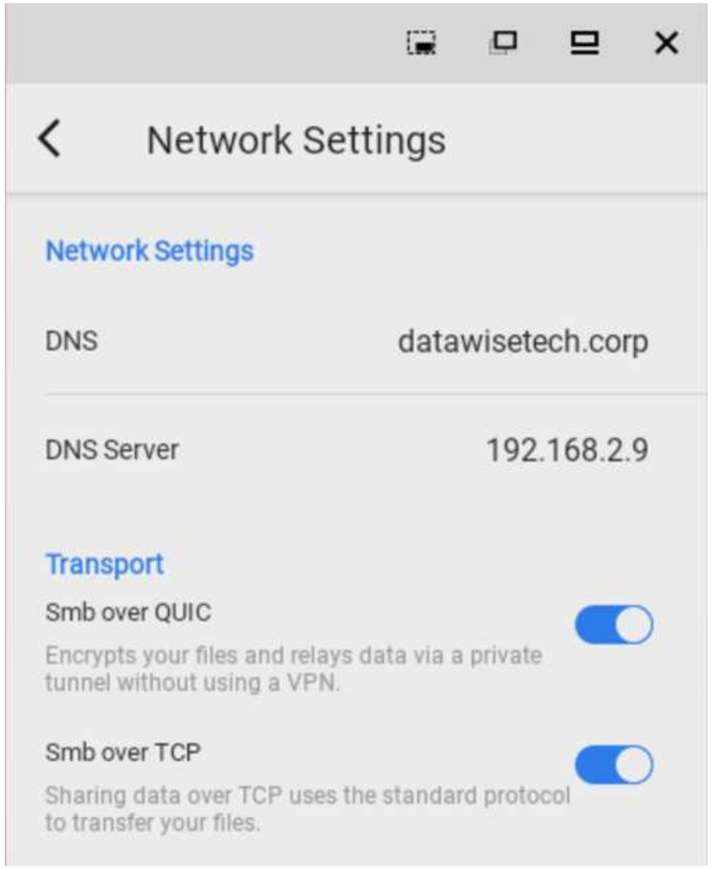




Android







https://vqr.vc/QQSd1ebRc

Libraries

YNQ

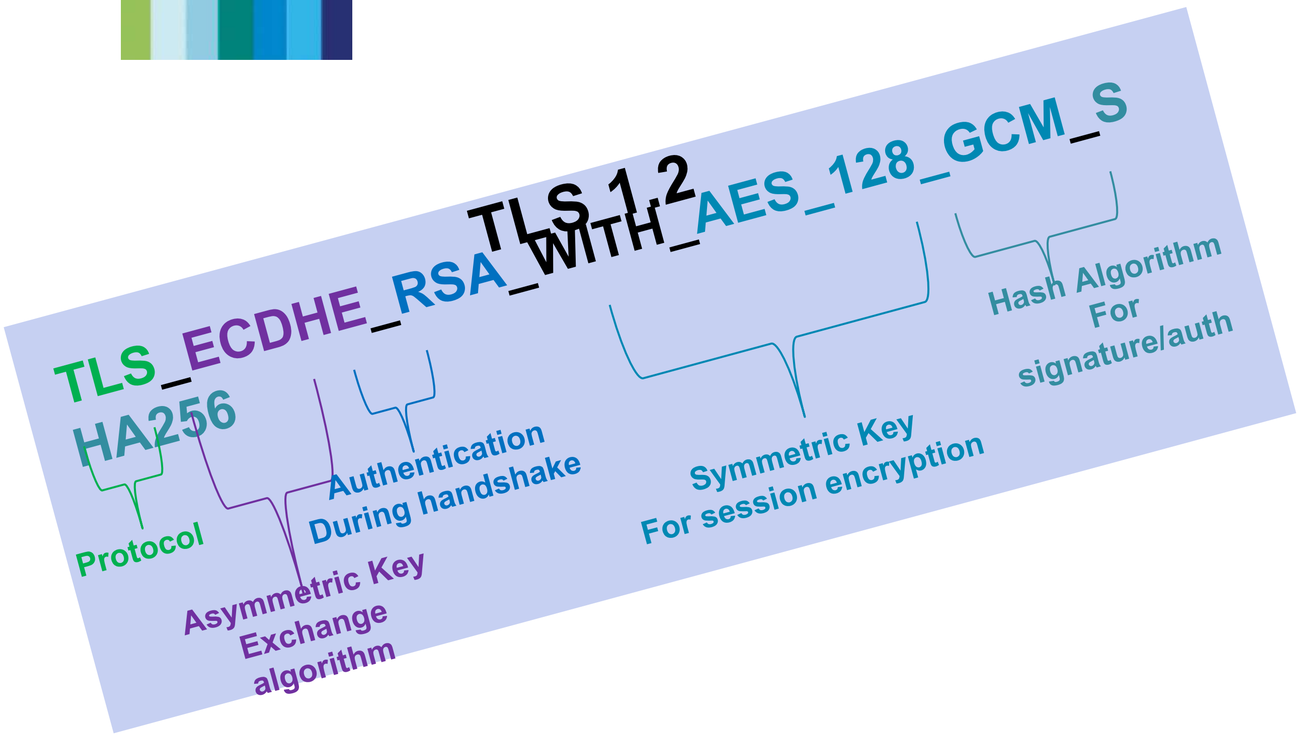
Portable SMB Server, Client, and system driver solution for various devices

For more info: https://visualitynq.com
info@visualitynq.com

jNQ

Fully scalable, robust, continually updated Pure Java SMB library

Configuration



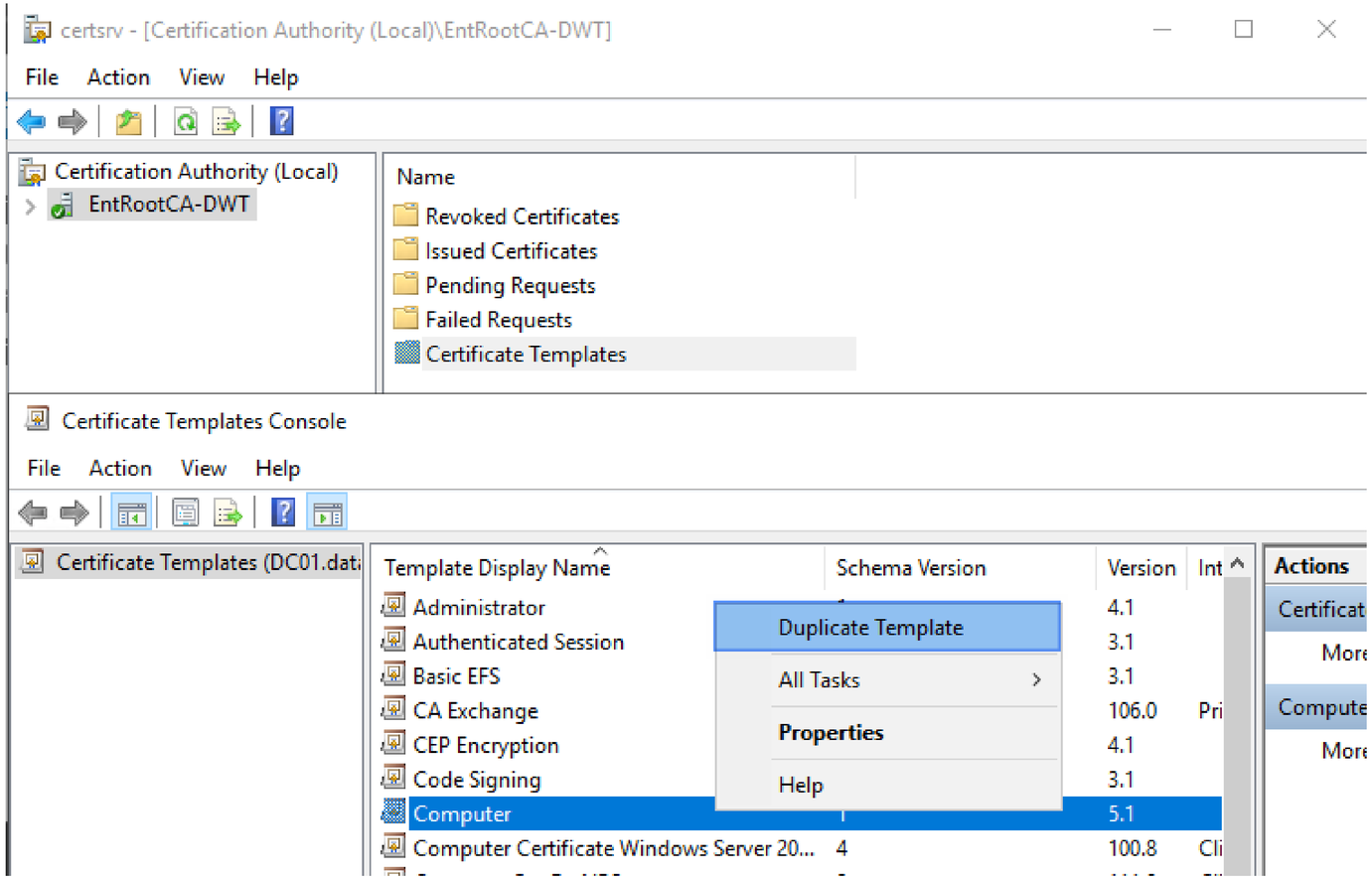
Get a certificate

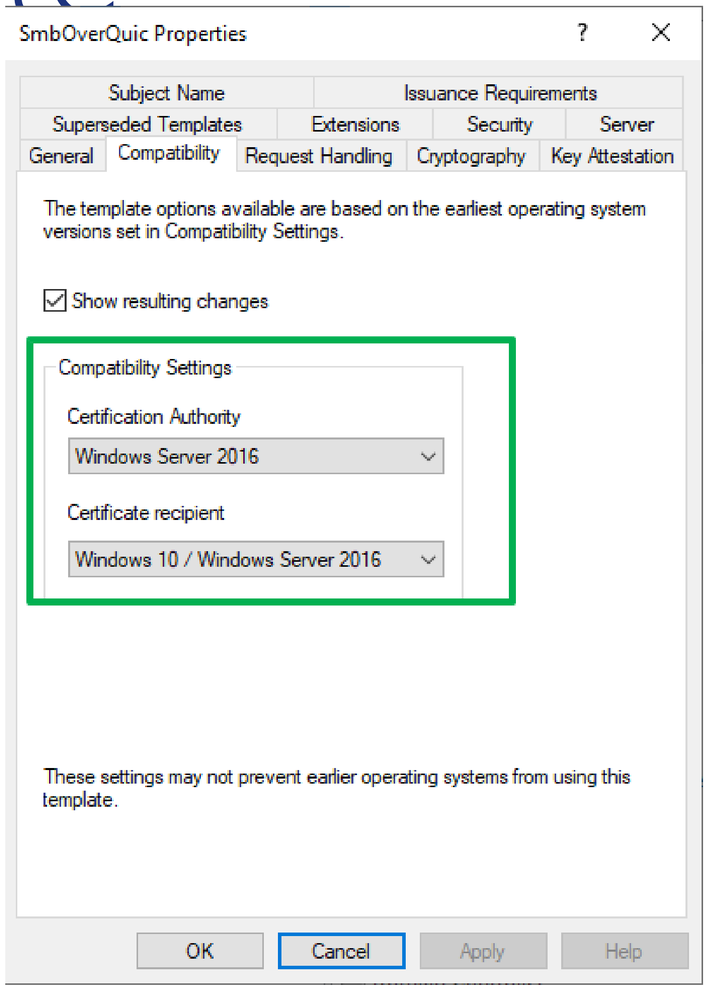
Watch Ned Pyle's video on this subject:

SMB over QUIC certificate issuance - YouTube

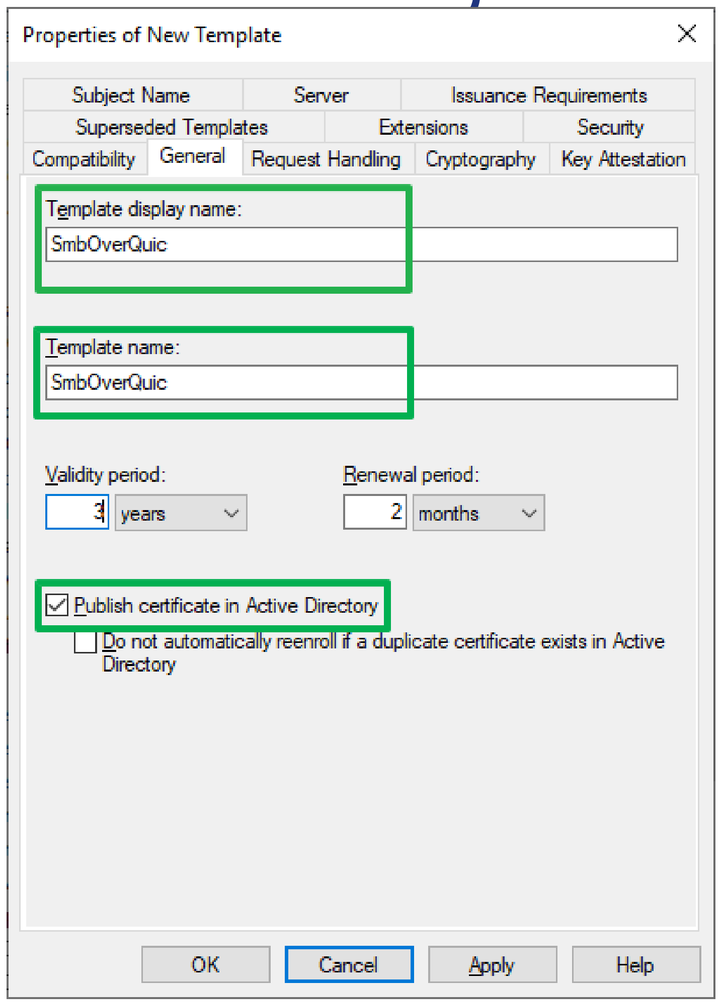
Images by Didier Van Hoye

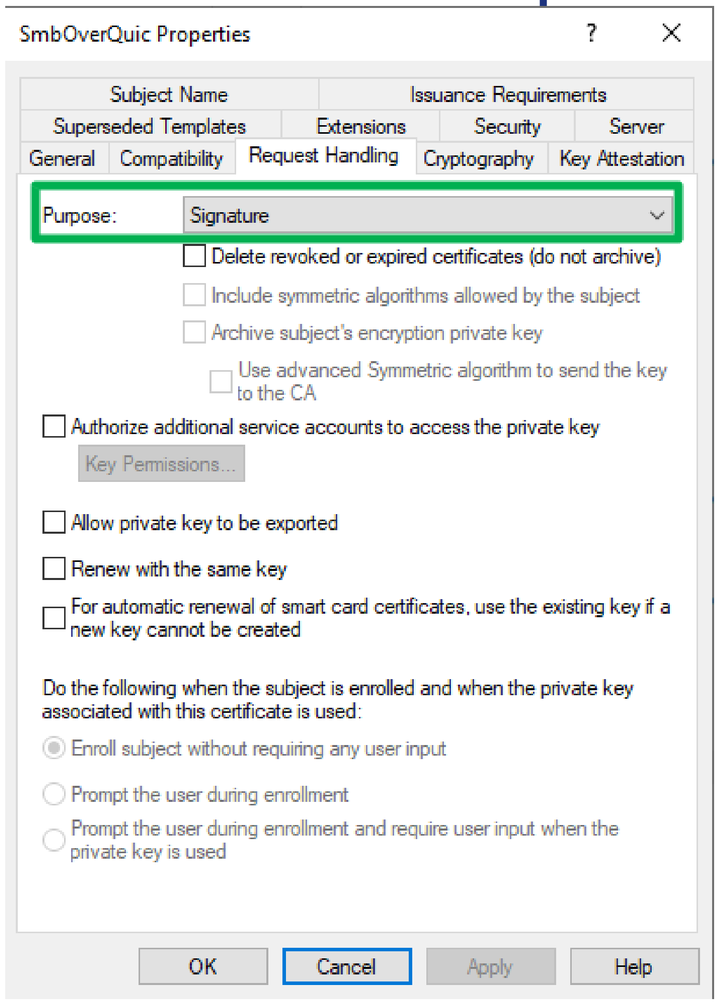
Configure Cert Template

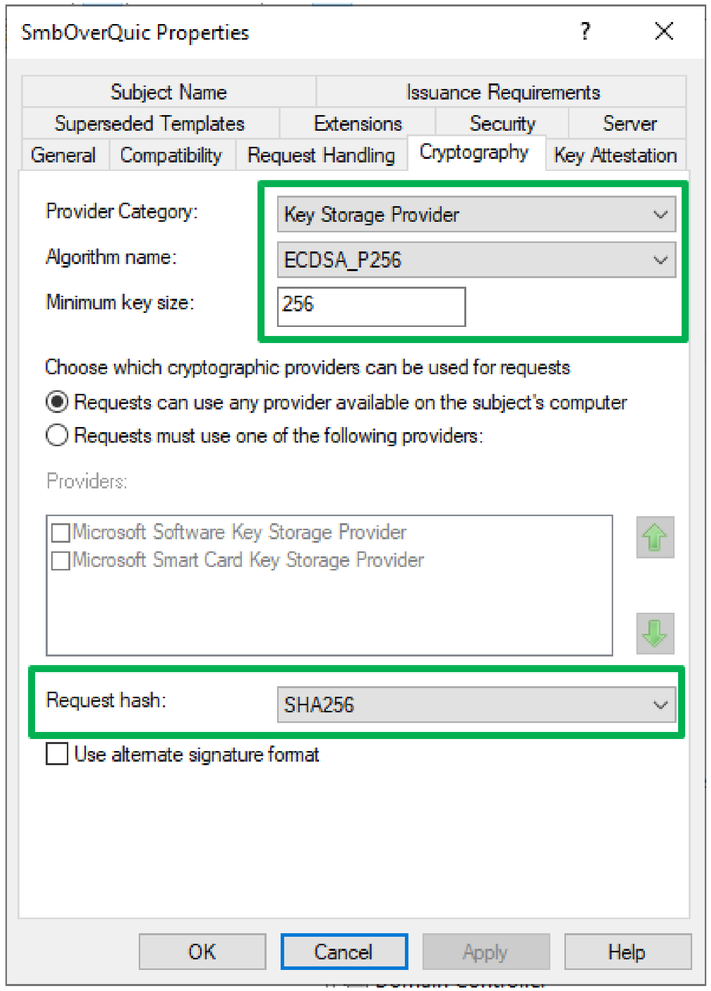




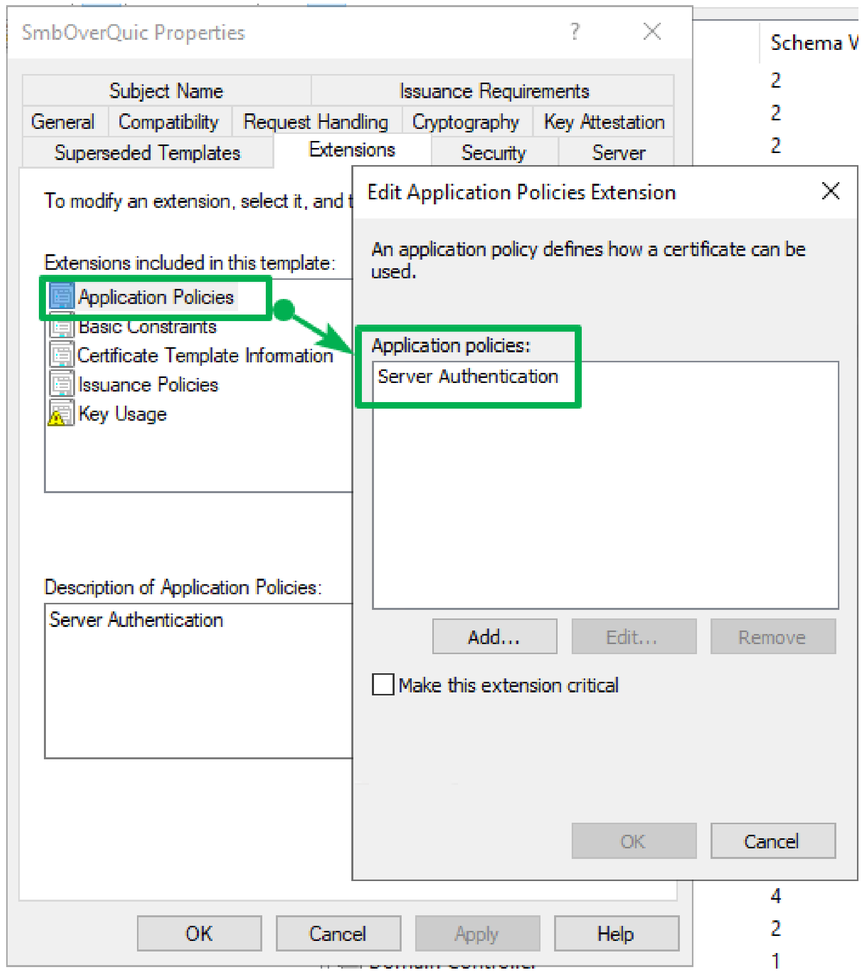
Configure Cert Template

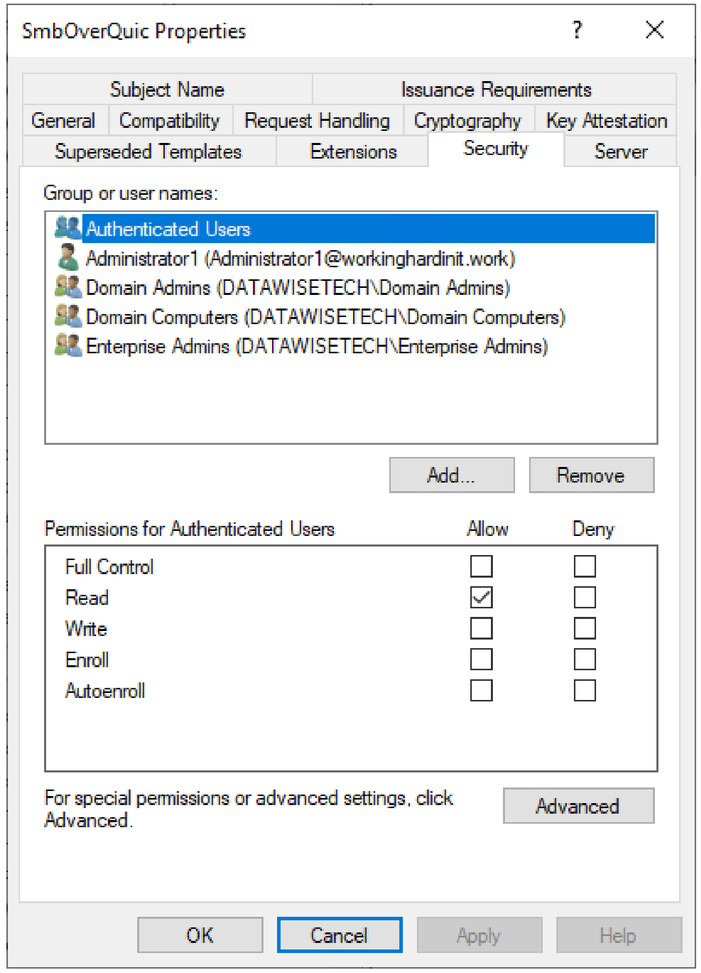


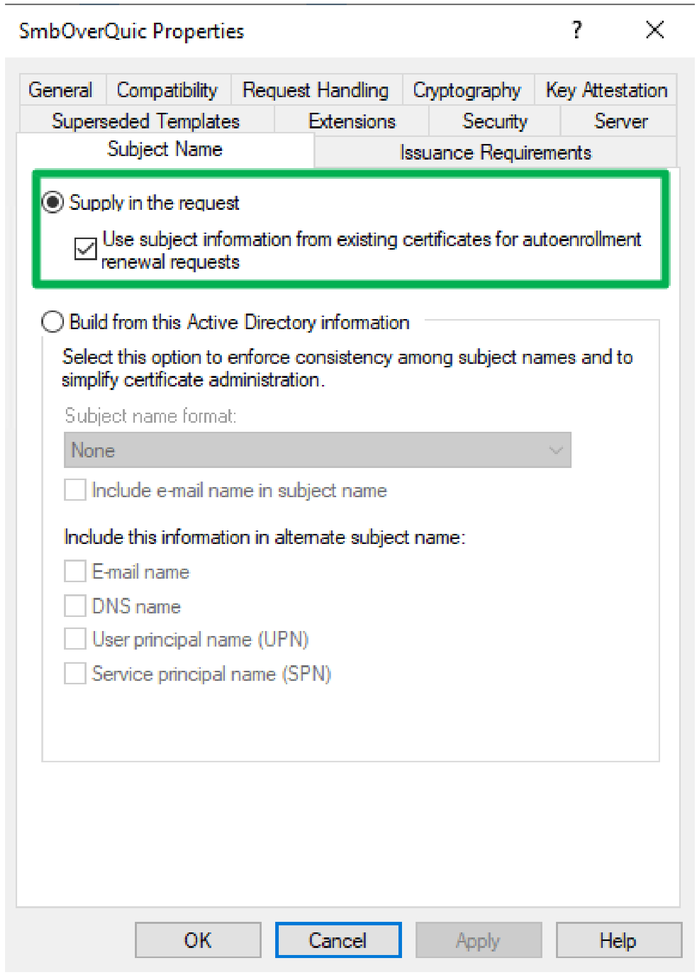




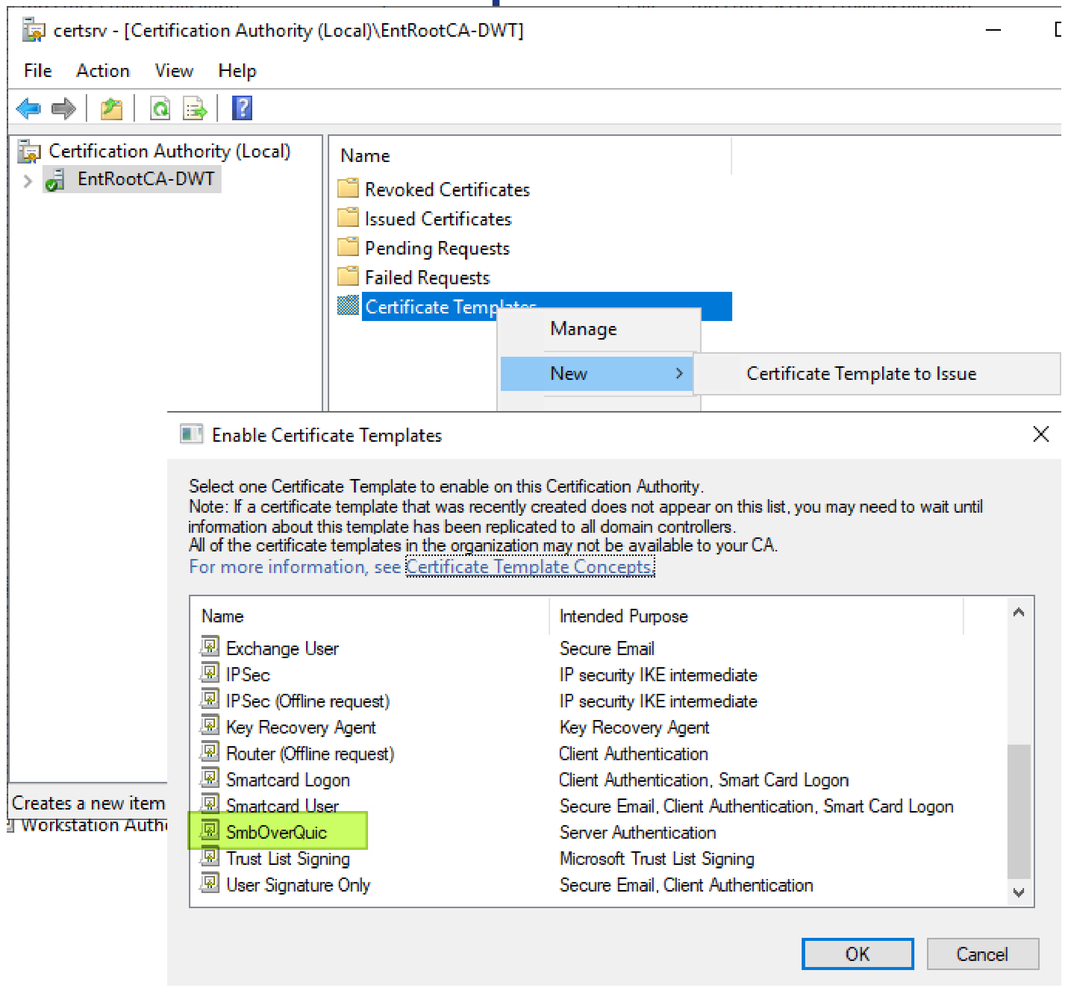
Configure Cert Template



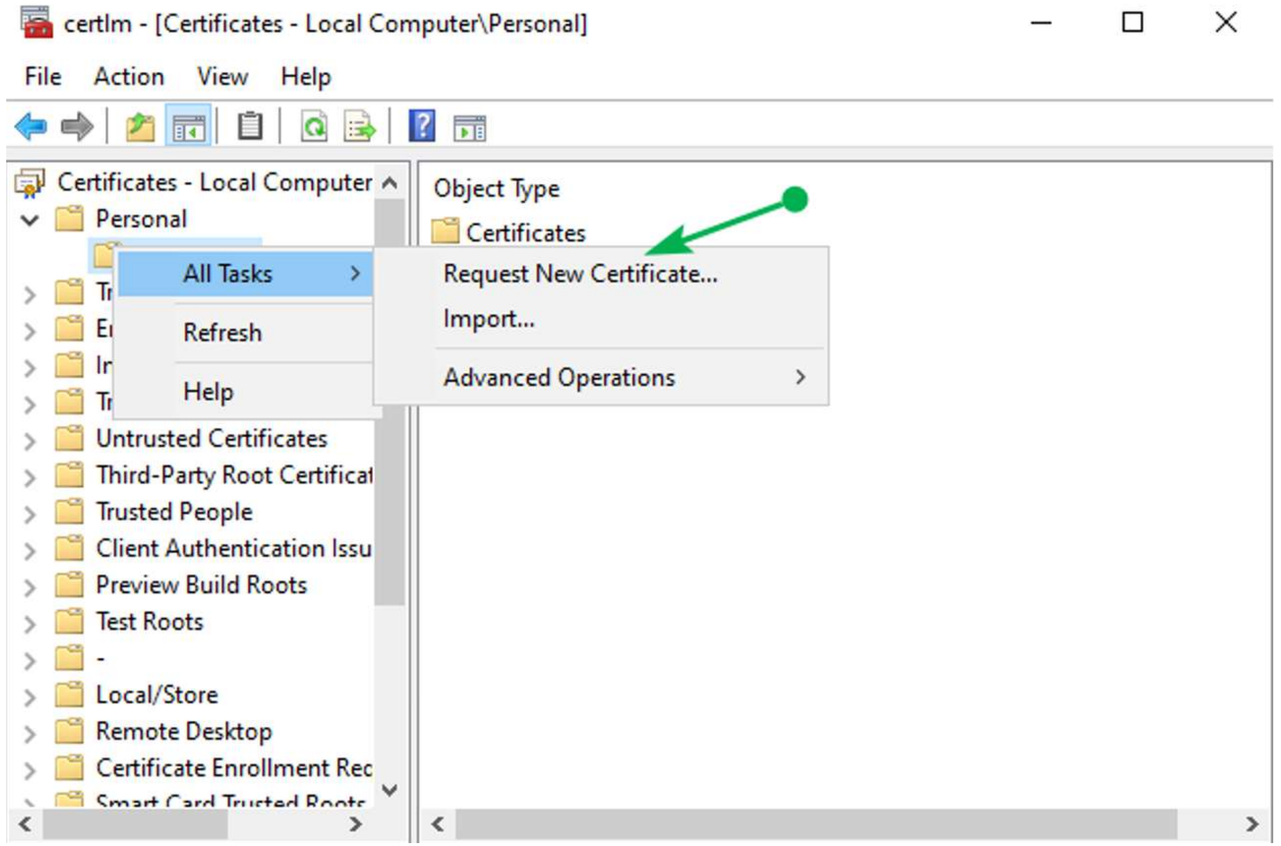




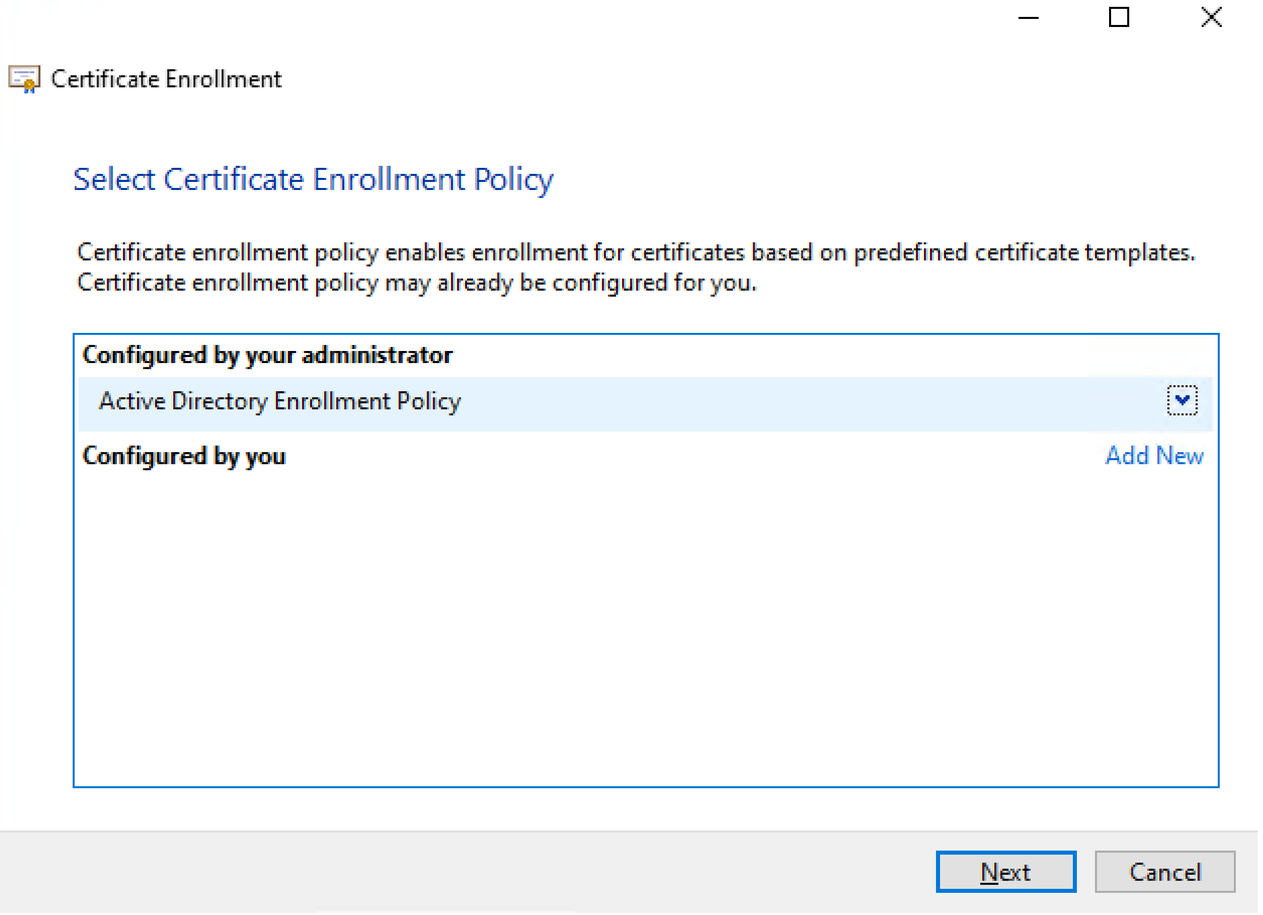
Enable Cert Template on CA

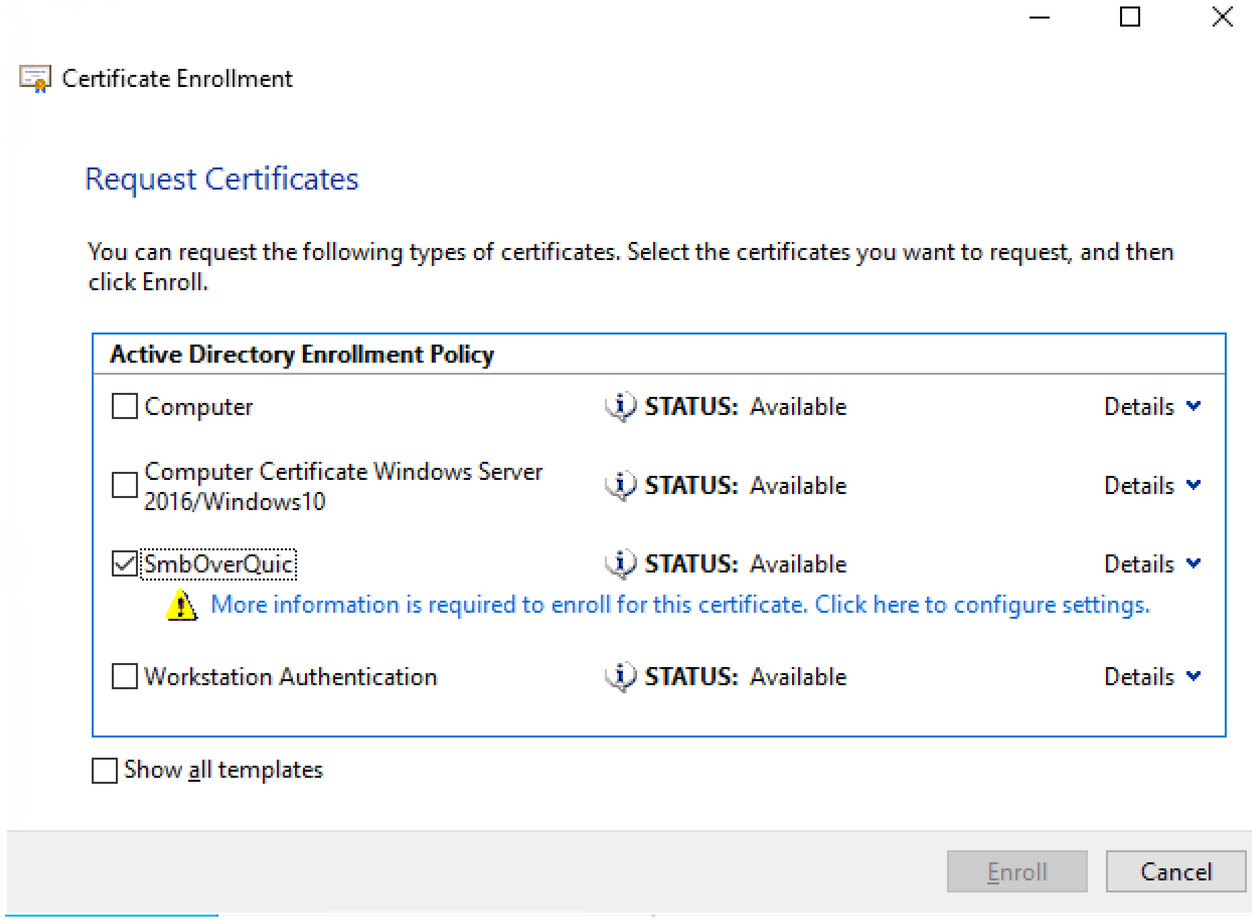


Requesting a certificate

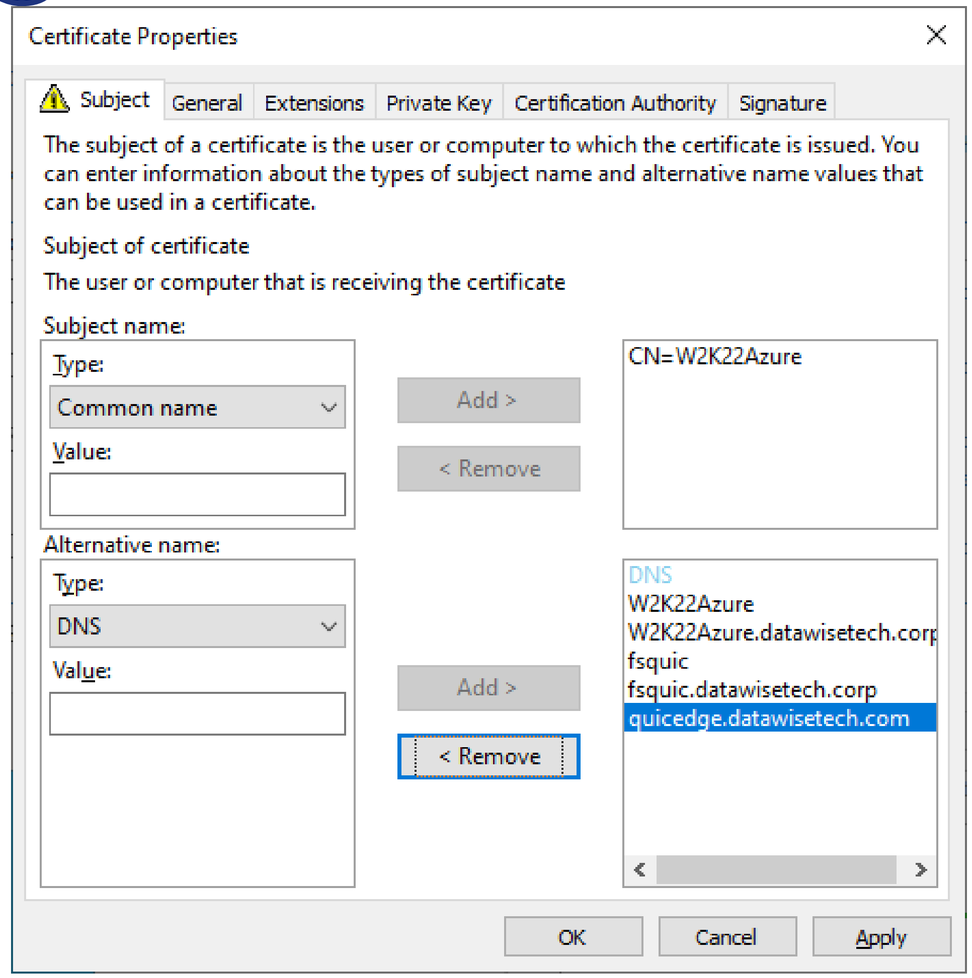


Requesting a certificate

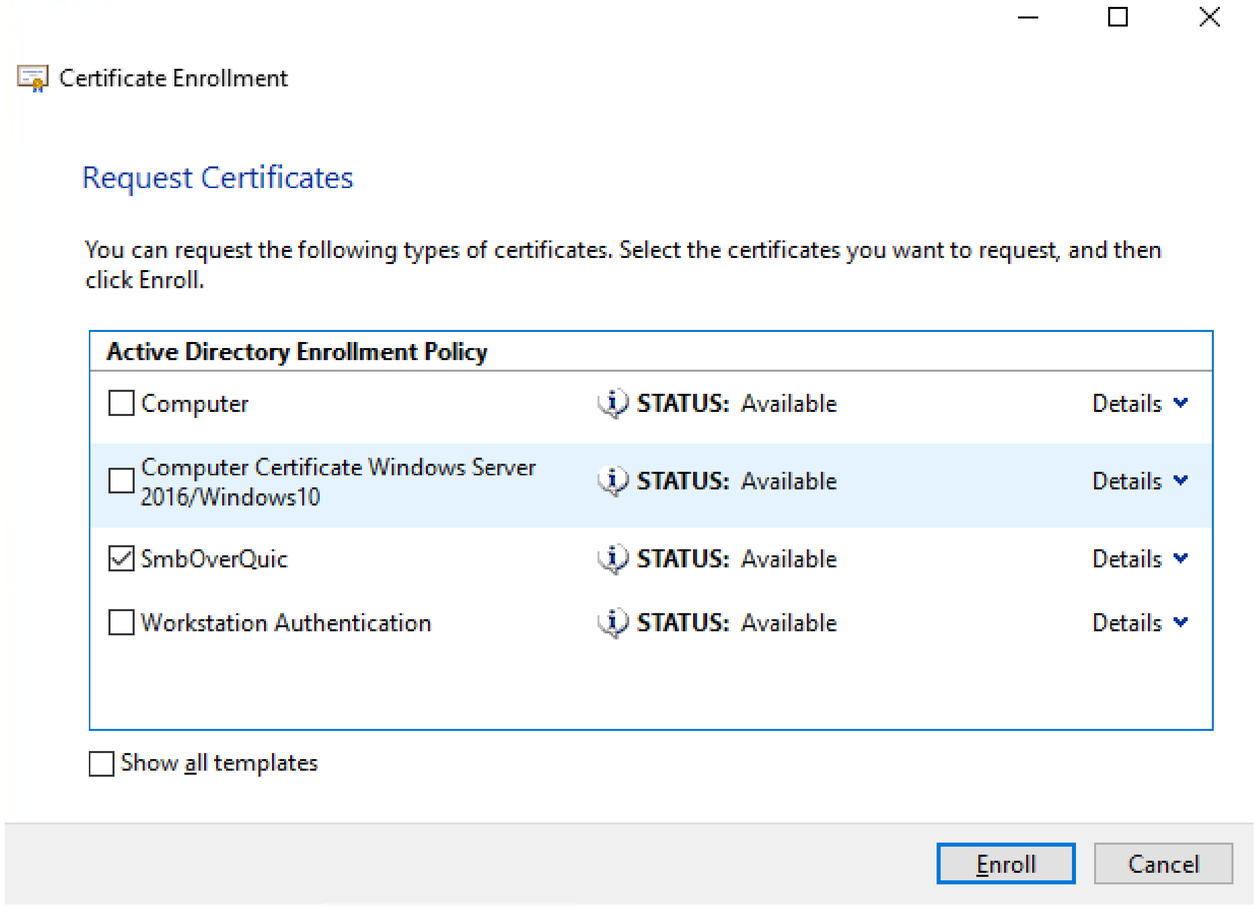


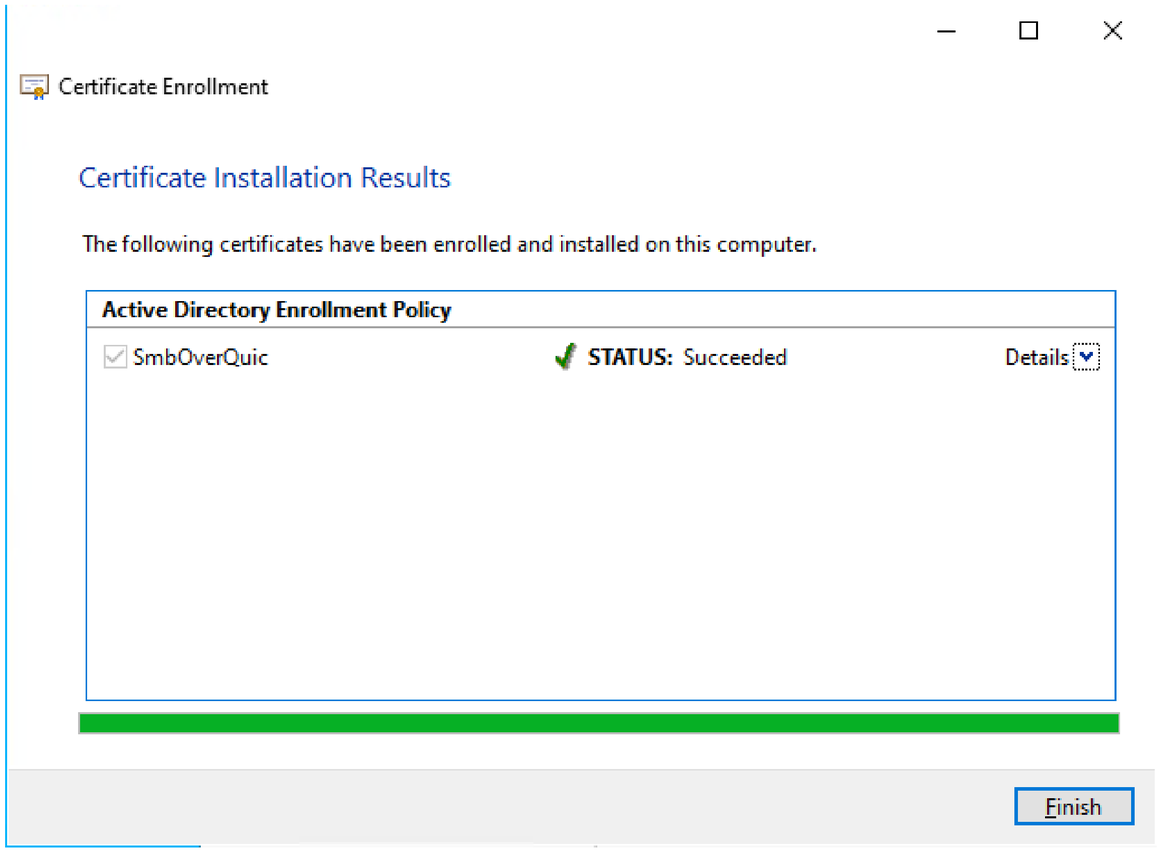


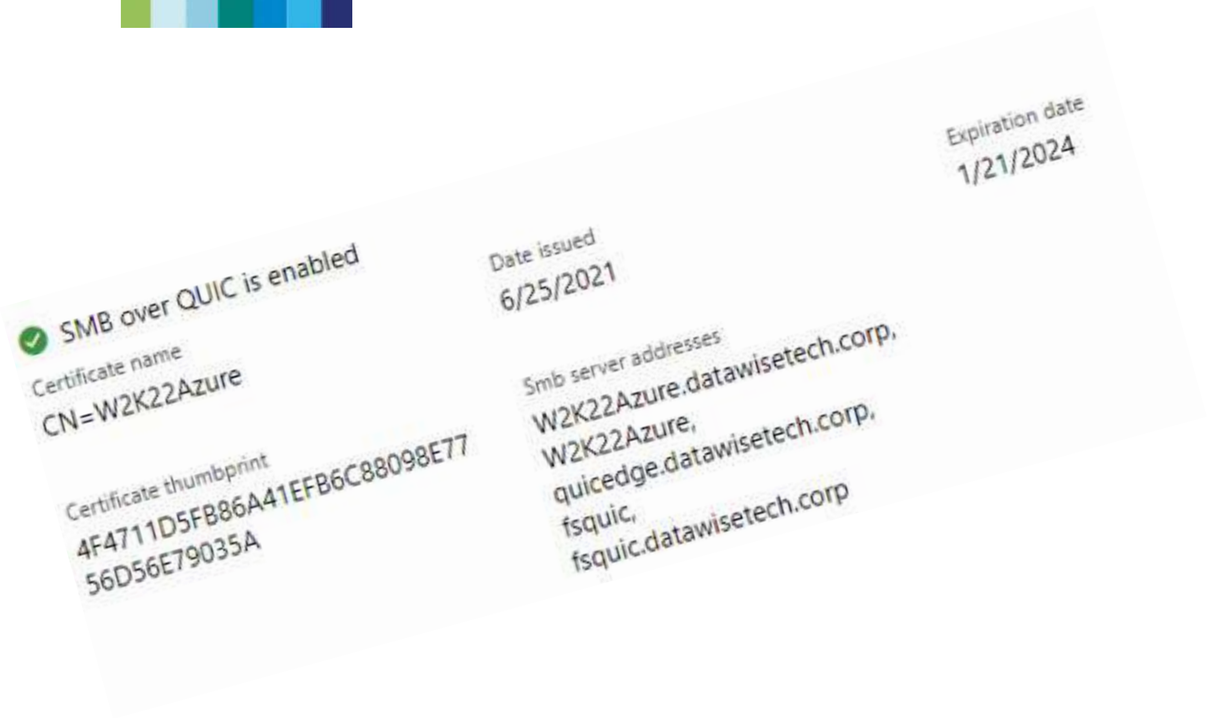
Requesting a certificate

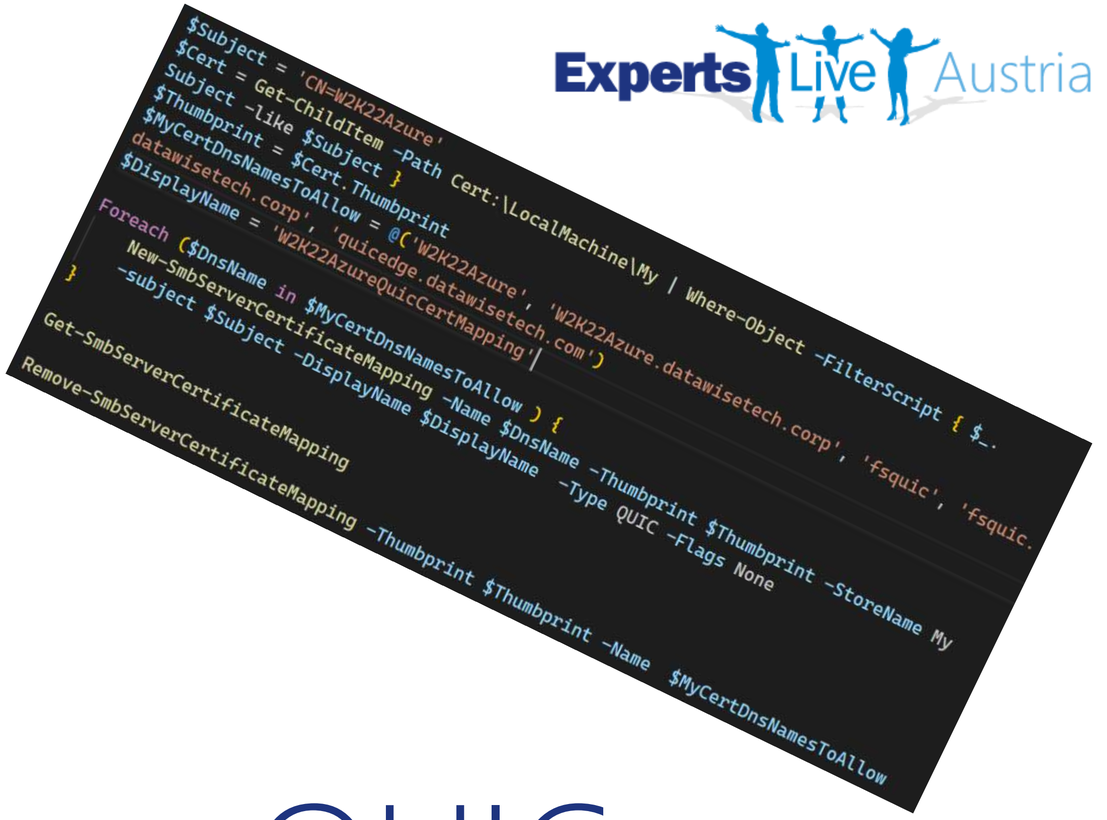


Requesting a certificate





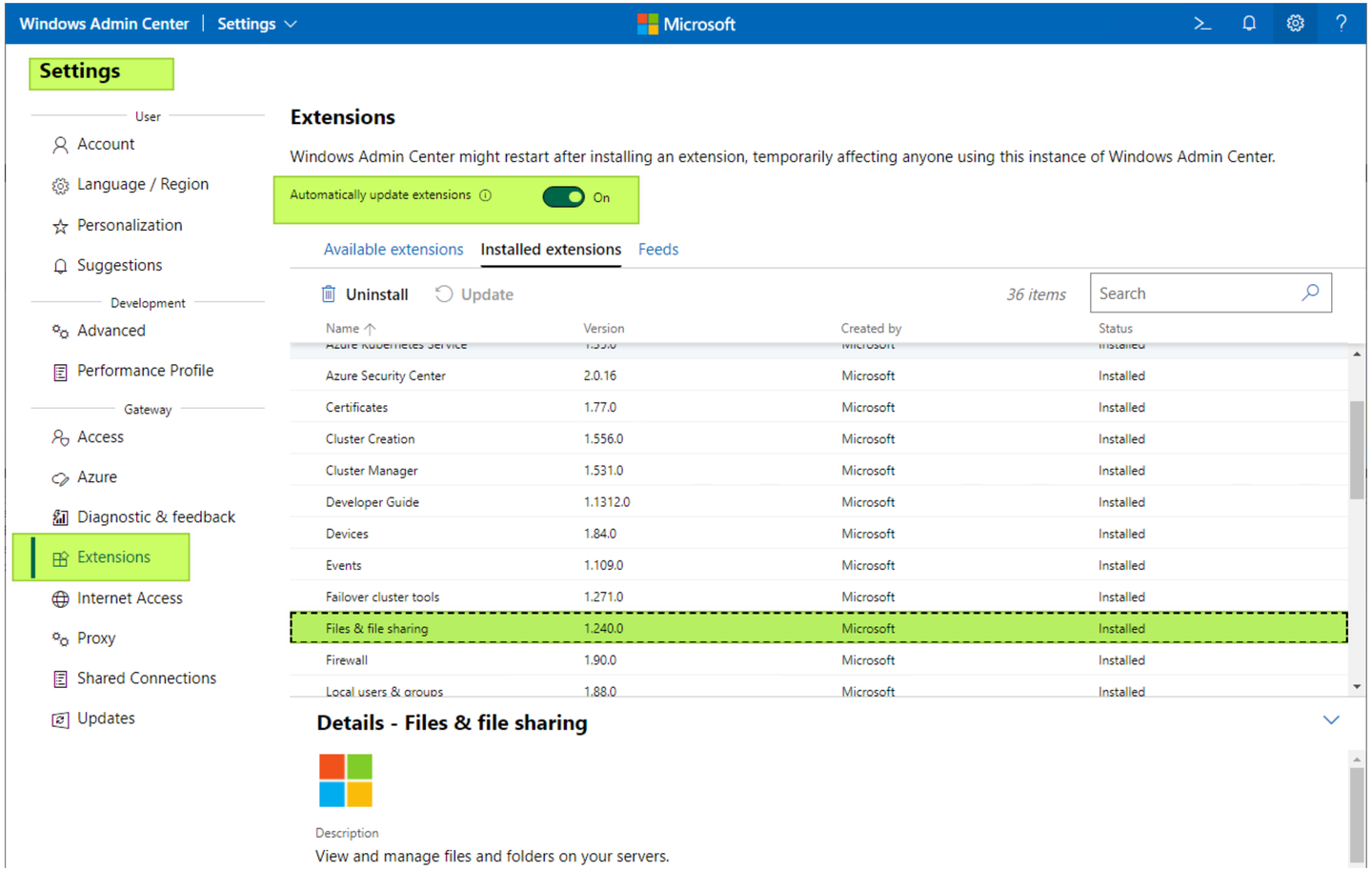




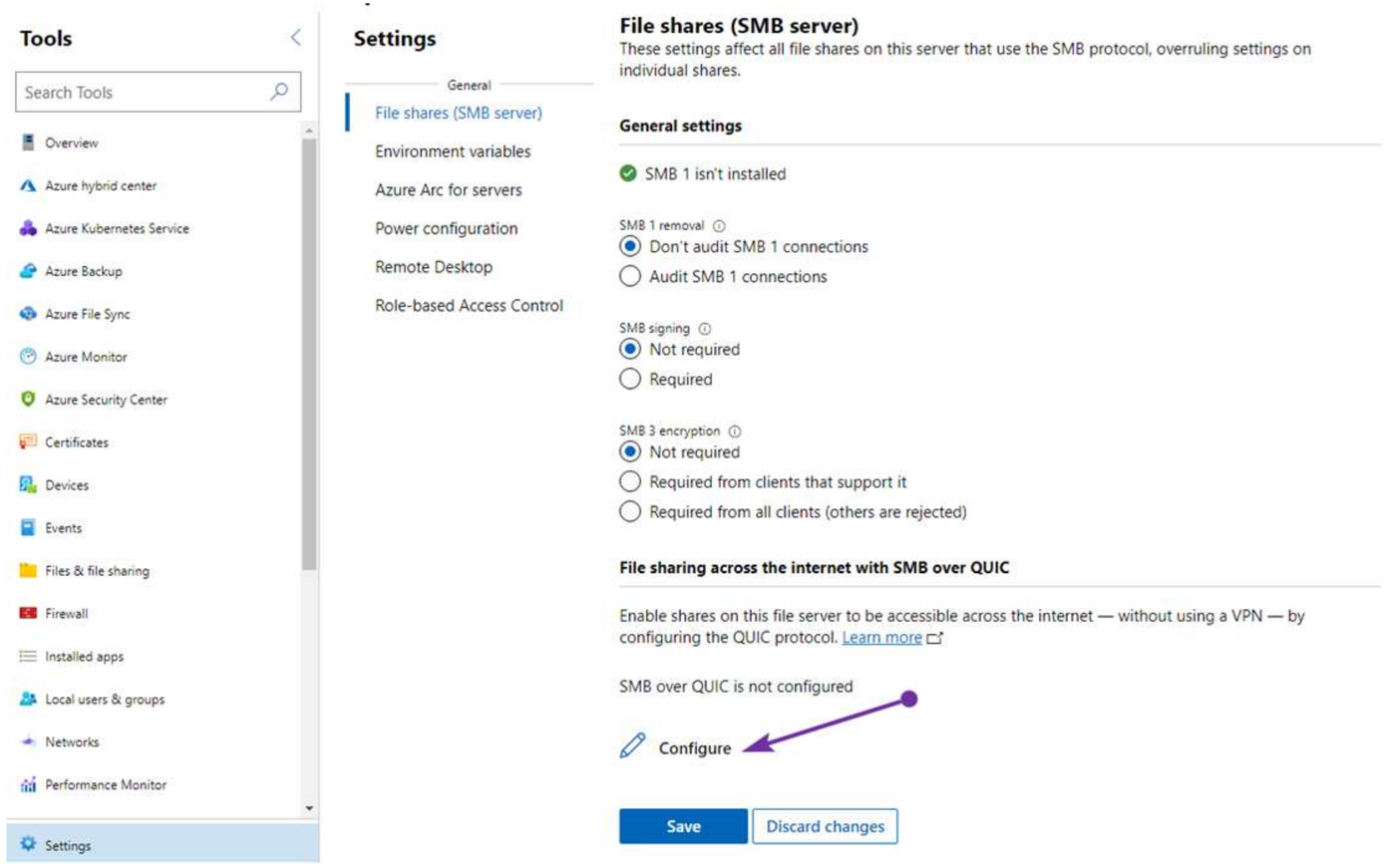
```
$Subject = 'CN=W2K22Azure'
$Cert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object -FilterScript { $_.
Subject -like $Subject }
$Thumbprint = $Cert.Thumbprint
$MyCertDnsNamesToAllow = @('W2K22Azure', 'W2K22Azure.datawisetech.corp', 'fsquic', 'fsquic.
datawisetech.corp', 'quicedge.datawisetech.com')
$DisplayName = 'W2K22AzureQuicCertMapping'
Foreach ($DnsName in $MyCertDnsNamesToAllow ) {
    New-SmbServerCertificateMapping -Name $DnsName -Thumbprint $Thumbprint -StoreName My
    -subject $Subject -DisplayName $DisplayName  -Type QUIC -Flags None
}
Get-SmbServerCertificateMapping
Remove-SmbServerCertificateMapping -Thumbprint $Thumbprint -Name  $MyCertDnsNamesToAllow
```

Configuring SMB over QUIC

Windows Admin Center (1/5)



Windows Admin Center (2/5)



Windows Admin Center (3/5)

Configure file sharing across the Internet with SMB over QUIC

Select a certificate (from the Local Machine\My certificate store) that identifies this server and is trusted by the server and clients. The server name must also be resolvable by client devices. Learn more

Certificate name	Status	Date issued	Expiration date	Thumbprint	Friendly name	Issuer	Signature algorithm
CN=W2k22Azure	Healthy	8/29/2023	1/28/2028	BE9BF0EE34C47021415C66804D3D88...	SMBOverQuicCert	CN=EntRootCA-DWT, DC=datawisete...	sha256RSA
[redacted]							
[redacted]							

Addresses that SMB over QUIC clients can connect to *

- [x] Select All
- [x] W2K22Azure.datawisetech.corp
- [x] W2K22Azure
- [x] fsquic.datawisetech.corp
- [x] fsquic
- [x] quicedge.datawisetech.com

Kerberos support through KDC Proxy (requires client configuration changes)

- (•) Enabled (Recommended)
- ( ) Disabled for SMB over QUIC
- ( ) Disabled

Kerberos support through KDC Proxy (requires client configuration changes): 443

Advanced Settings

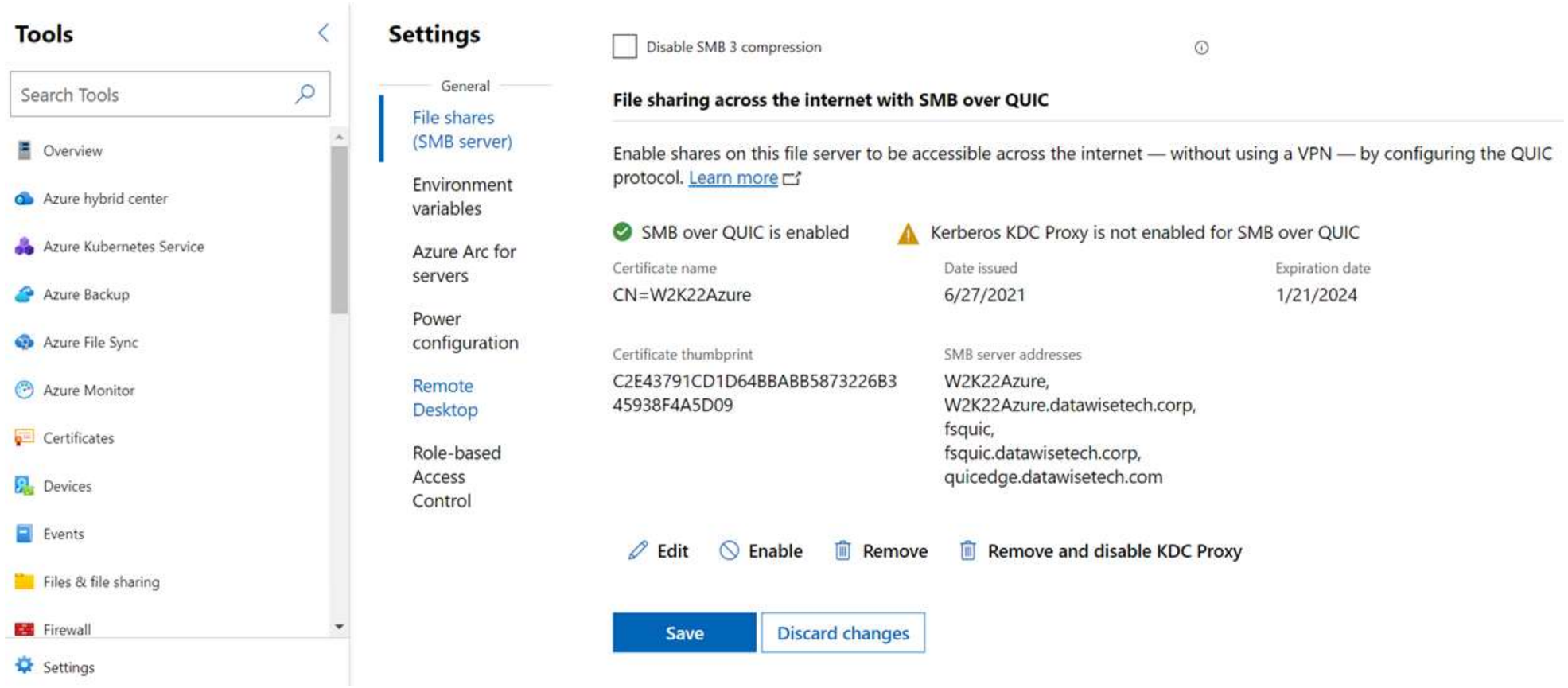
SMB encryption (in addition to QUIC encryption)

- (•) Disabled (Recommended)
- ( ) Enabled

Access to named pipes

- (•) Disabled (Recommended)
- ( ) Enabled

Windows Admin Center (4/5)



Windows Admin Center (5/5)

File sharing across the internet with SMB over QUIC

Enable shares on this file server to be accessible across the internet — without using a VPN — by configuring the QUIC protocol. Learn more

SMB over QUIC is enabled

Kerberos KDC Proxy is enabled for SMB over QUIC

Certificate name	Date issued	Expiration date
CN=W2K22Azure	6/27/2021	1/21/2024

Certificate thumbprint	SMB server addresses
C2E43791CD1D64BBABB587322 6B345938F4A5D09	W2K22Azure, W2K22Azure.datawisetech.corp, fsquic, fsquic.datawisetech.corp, quicedge.datawisetech.com

Edit Enable Remove Remove and disable KDC Proxy

Automate with PowerShell

```
$Subject = 'CN=file01'
$Cert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object -FilterScript {
$_.Subject -like $Subject }
$Thumbprint = $Cert.Thumbprint
$MyCertDnsNamesToAllow = @('file01', 'file01.datawisetech.corp', 'fsquic',
'fsquic.datawisetech.corp', 'fsquic.datawisetech.com','fsquic.workinghardinit.work')
$DisplayName = 'file01'

Foreach ($DnsName in $MyCertDnsNamesToAllow ) {
   New-SmbServerCertificateMapping -Name $DnsName -Thumbprint $Thumbprint -StoreName My
-subject $Subject -DisplayName $DisplayName  -Type QUIC -Flags None
}

Get-SmbServerCertificateMapping

Remove-SmbServerCertificateMapping -Thumbprint $Thumbprint -Name  $MyCertDnsNamesToAllow
```

Forcing SMB over QUIC at client

Net Use

```
NET USE * \\ quicedge.datawisetech.com \sales /TRANSPORT:QUIC
```

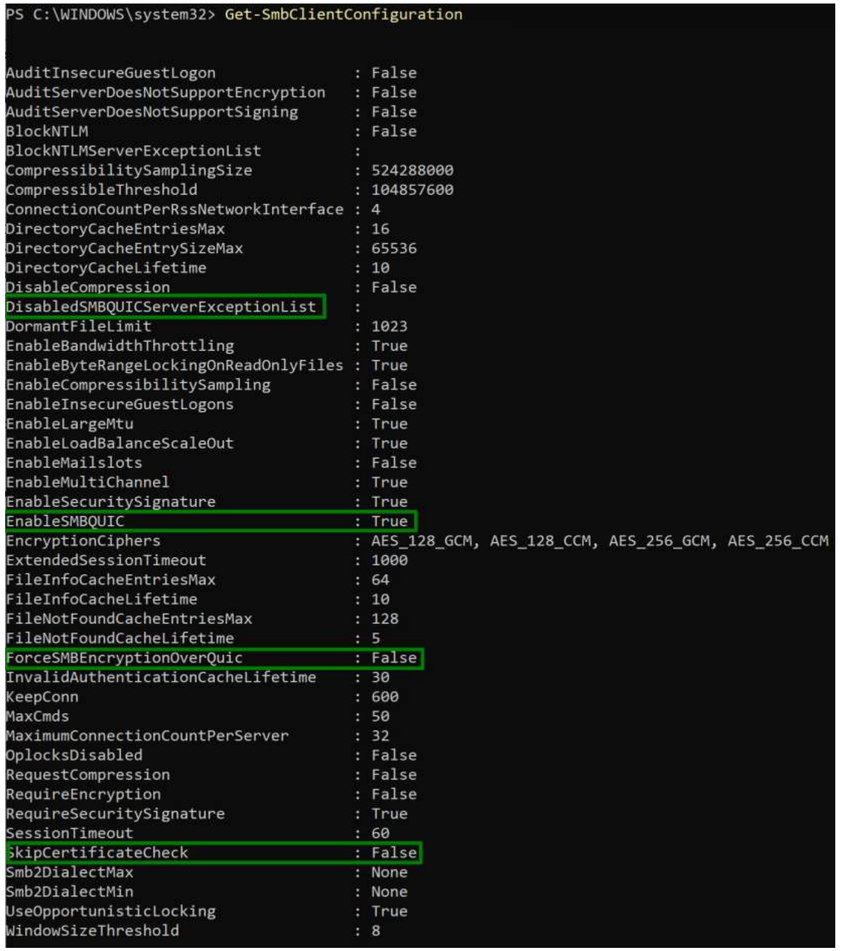
PowerShell

```
New-SmbMapping -LocalPath 'Z:' -RemotePath
'\\quicedge.datawisetech.com\BusinessPlans' -TransportType QUIC
```

SMB Client Configuration

- SkipCertificateCheck
- ForceSMBEncryptionOverQuic
- EnableSMBQUIC
- DisabledSMBQUICServerExceptionList
  This setting allows administrators to opt specific servers into SMB over QUIC access, even when the client's policy disables it.

```
Set-SmbClientConfiguration -DisabledSMBQUICServerExceptionList "<Server01>, <Server02>, <Server03>"
```



SMB Server Configuration

DisableSmbEncryptionOnSecureConnection

RestrictNamedPipeAccessViaQuic

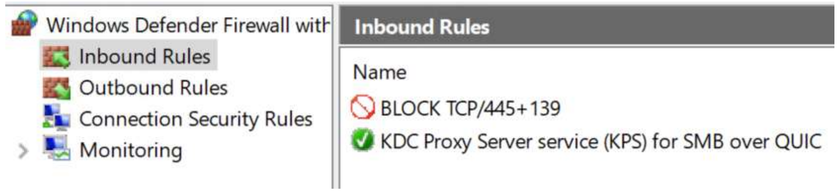
EnableSMBQUIC

NEW: AuditClientCertificateAccess

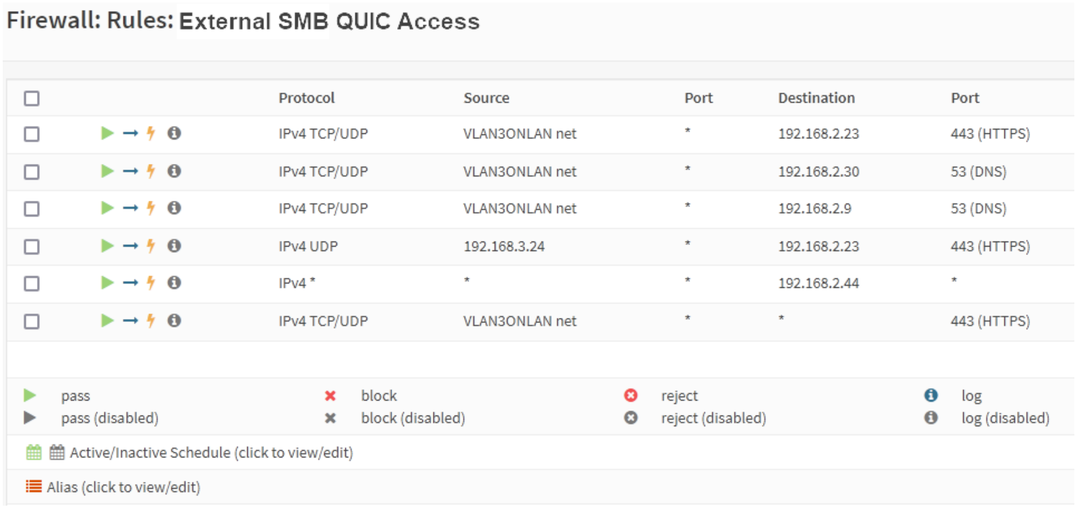
```
PS C:\Users\administrator1> Get-SmbServerConfiguration

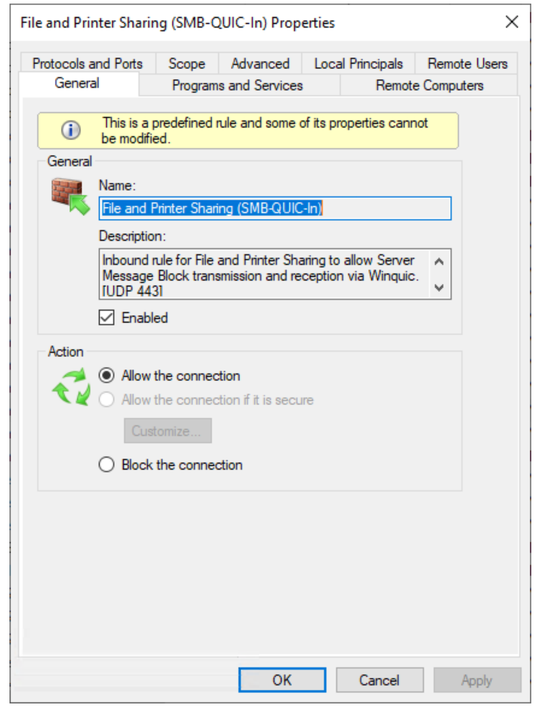
AnnounceComment                           :
AnnounceServer                            : False
AsynchronousCredits                       : 512
AuditClientCertificateAccess              : True
AuditClientDoesNotSupportEncryption       : False
AuditClientDoesNotSupportSigning          : False
AuditInsecureGuestLogon                   : False
AuditSmb1Access                           : False
AutoDisconnectTimeoutInMinutesV1          : 15
AutoDisconnectTimeoutInSecondsV2          : 900
AutoShareServer                           : True
AutoShareWorkstation                      : True
CachedOpenLimit                           : 10
DisableCompression                        : False
DisableSmbEncryptionOnSecureConnection    : True
DurableHandleV2TimeoutInSeconds           : 180
EnableAuthenticateUserSharing             : False
EnableAuthRateLimiter                     : True
EnableDirectoryHandleLeasing              : True
EnableDownlevelTimewarp                   : False
EnableForcedLogoff                        : True
EnableLeasing                             : True
EnableMailslots                           : False
EnableMultiChannel                        : True
EnableOplocks                             : True
EnableSecuritySignature                   : False
EnableSMB1Protocol                        : False
EnableSMB2Protocol                        : True
EnableSMBQUIC                             : True
EnableStrictNameChecking                  : True
EncryptData                               : False
EncryptionCiphers                         : AES_128_GCM, AES_128_CCM, AES_256_GCM, AES_256_CCM
InvalidAuthenticationDelayTimeInMs        : 2000
IrpStackSize                              : 15
KeepAliveTime                             : 2
MaxChannelPerSession                      : 32
MaxMpxCount                               : 50
MaxSessionPerConnection                   : 16384
MaxThreadsPerQueue                        : 20
MaxWorkItems                              : 1
NullSessionPipes                          :
NullSessionShares                         :
OplockBreakWait                           : 35
PendingClientTimeoutInSeconds             : 120
RejectUnencryptedAccess                   : True
RequestCompression                        : False
RequireSecuritySignature                  : False
RestrictNamedpipeAccessViaQuic            : True
ServerHidden                              : True
Smb2CreditsMax                            : 8192
Smb2CreditsMin                            : 512
Smb2DialectMax                            : None
Smb2DialectMin                            : None
SmbServerNameHardeningLevel               : 0
TreatHostAsStableStorage                  : False
ValidateAliasNotCircular                  : True
ValidateShareScope                        : True
ValidateShareScopeNotAliased              : True
ValidateTargetName                        : True
```

Forcing SMB over QUIC



- Block TCP/445 on Windows & 3rd party firewall
- Allow UDP/443 on Windows & 3rd party firewall
  - Check out the new File and Printer Sharing (SMB-QUIC-in) rule

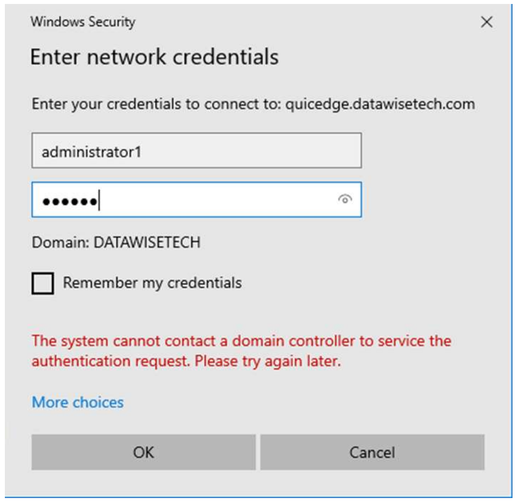




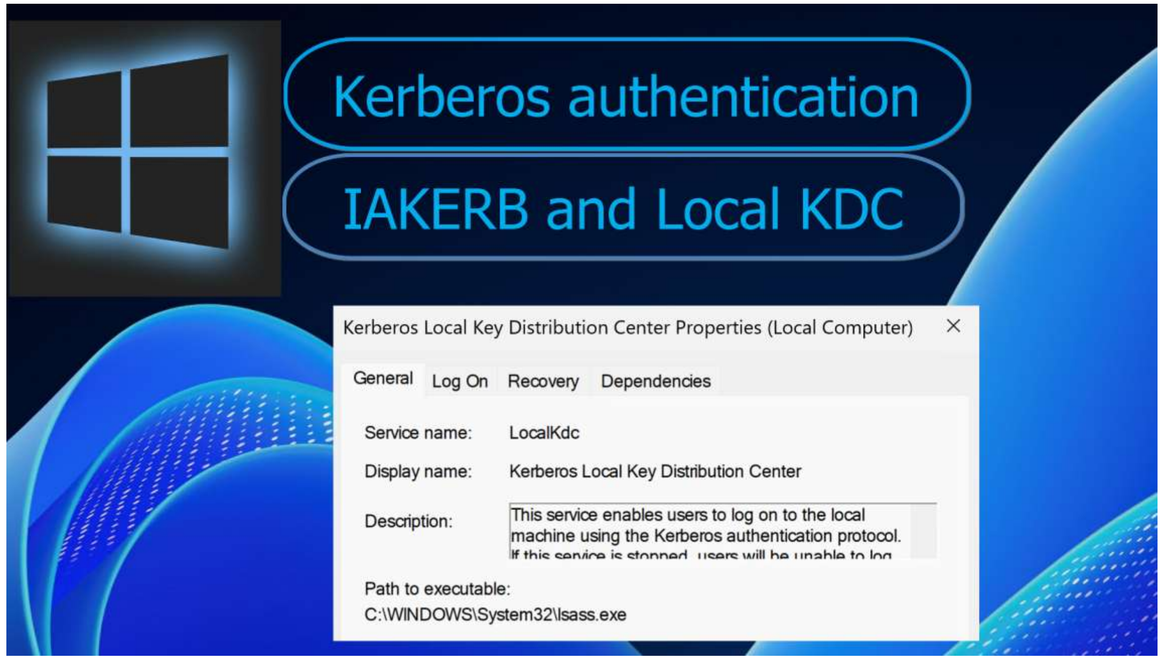
SMB over QUIC can use NTLMv2

Falling back to NTLMv2 is very convenient (for bad actors to)
Only option without line of sight to a domain controller
Leveraging NTLMv2 is considered regression
You want Kerberos, Active Directory domain controllers (DCs)
You must not expose your DCs to the internet!
KDC proxy to the rescue!

https://www.trustedsec.com/blog/making-smb-accessible-with-ntlmquic/



IaKerb & Local KDC



5% No line of sight

29% Local Account

14% Unknown Servers

52% Hard Coded!

SMB over QUIC IaKerb & Local KDC

Next to KDC Proxies, we'll have in Windows Server 2025

- IaKerb => if no line of sight to a domain controller
- Local KDC to provide Kerberos on Local Systems
- Even hard-coded NTLM can be redirected to see if Kerberos will work

SMB over QUIC Auditing

- SMB now supports auditing SMB over QUIC.
- Both at the SMB server and client levels.
- Helps determine if Windows client & server are establishing SMB over QUIC connections.

SMB over QUIC Custom Port 1/2

- ```
  #Lists all available alternative ports
  Get-SmbServerAlternativePort
  ```
- ```
  #Creates a new alternative port
  New-SmbServerAlternativePort -TransportType QUIC -Port 44344 -EnableInstances Default
  ```
- ```
  #Deletes an alternative port
  Remove-SmbServerAlternativePort
  ```
- ```
  #Configures SMB to use a specific port
  Set-SmbServerAlternativePort
  ```
- ```
  #Configures SMB to use a specific port
  New-SmbMapping -LocalPath F: -RemotePath \fsquic.datawisetech.com\finances -QuicPort 44344
  ```
- Configure alternative SMB ports for Windows Server 2025 | Microsoft Learn
  ```

SMB over QUIC Custom Port 2/2

Group Policy/PowerShell cmdlets to configure SMB client QUIC bindings

- PowerShell
  ```
  New-SmbClientBindingPolicy -TransportType QUIC -Port 44344 -ServerName fsquic.contoso.com
  ```

- Registry
  ```
  HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\SmbClientBindingPolicies
  ```

SMB over QUIC client access control

- Leverages a shared trusted CA, both client and server trust
- Restrict which clients can access SMB over QUIC
- Client access control creates allow & block lists for clients connecting to the file server
- Based on client certificates (mTLS-like)
- Supports subject alternative names

SMB over QUIC client access control

File Server

```
$DnsName = "fsquic.datawisetech.com"
Set-SmbServerCertificateMapping -Name $DnsName -RequireClientAuthentication $true -Thumbprint $ThumbPrint
```

Client

```
Get-ChildItem -Path Cert:\LocalMachine\My
$clientCert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object {$_.Subject -Match "CN=dwtws-101"}
$clientCert.GetCertHashString("SHA256") #SHA256 value needed for server config
New-SmbClientCertificateMapping -Namespace $DnsName -Thumbprint $clientCert.Thumbprint -StoreName My
Get-SmbClientCertificateMapping  #Verify your work
```

```
Namespace              Thumbprint                               StoreName IssuerName    Subject      DisplayName
---------              ----------                               --------- ----------    -------      -----------
fsquic.datawisetech.com 046E88B5B0B3A738D2BE74B3C976B0F5127A2B87 My        EntRootCA-DWT CN=dwtws-101 dwtws-101
```

```
#Try it – without further the server-side config, this won't work
New-SmbMapping -RemotePath \\fsquic.datawisetech.com\finance -TransportType QUIC
```

over QUIC client access control

File Server

```
$Subject = 'CN=file01'
$Cert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object -FilterScript { $_.Subject -like $Subject}
$Thumbprint = $Cert.Thumbprint
$DnsName = "fsquic.datawisetech.com"
$DisplayName = "file01" #Only with New-SmbServerCertificateMapping

Set-SmbServerCertificateMapping -Name $DnsName -RequireClientAuthentication $true -Thumbprint $Thumbprint
#or
New-SmbServerCertificateMapping -Name $DnsName -Thumbprint $Thumbprint -StoreName My -subject $Subject -
DisplayName $DisplayName -Type QUIC -Flags None

Get-SmbServerCertificateMapping #Check your work.
```

Name	Subject	Thumbprint	DisplayName	StoreName	Type	Flags	RequireClientAuthentication	SkipClientCertificateAccessCheck
file01	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	False	False
file01.workinghardinit.work	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	False	False
file01.datawisetech.corp	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	False	False
file01.datawisetech.com	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	False	False
fsquic	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	False	False
fsquic.datawisetech.corp	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	False	False
fsquic.datawisetech.com	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	True	False
fsquic.workinghardinit.work	CN=file01	E6D246062EF2D8F478C1D652EE9EF85E4E6FA935	file01	My	QUIC	None	False	False

over QUIC client access control

On the File Server

```
#We either use -SkipClientCertificateAccessCheck in the SmbServerCertificateMapping or we configure client access control
$SmbClientCertSha256Hash = "5ABB94D9D279DCA88C0BAE8805C9C5FB7B2F786F3FC415A1F9FC208E3808FAD7" #SHA256 Hash
$SmbClientCertIssuer = "CN = EntRootCA-DWT,DC = datawisetech,DC = corp"
Grant-SmbClientAccessToServer -Name $DnsName -IdentifierType SHA256 -Identifier $SmbClientCertSha256Hash
#or
Grant-SmbClientAccessToServer -Name $DnsName -IdentifierType ISSUER -Identifier $SmbClientCertIssuer

Get-SmbClientAccessToServer -Name $DnsName #Chek your work
```

```
Name              : fsquic.datawisetech.com
AccessControlType : Allow
IdentifierType    : SHA256
Identifier        : 5ABB94D9D279DCA88C0BAE8805C9C5FB7B2F786F3FC415A1F9FC208E3808FAD7
Description       :
```

```
Set-SmbServerConfiguration -AuditClientCertificateAccess $true # Enable auditing for client certificate access

#Try it – without the server-side config, this won't work
New-SmbMapping -RemotePath \\fsquic.datawisetech.com\finance -TransportType QUIC
```

Configure SMB over QUIC client access control in Windows Server | Microsoft Learn


Show me a demo!

KDC Proxy Service

Kerberos over the internet!?

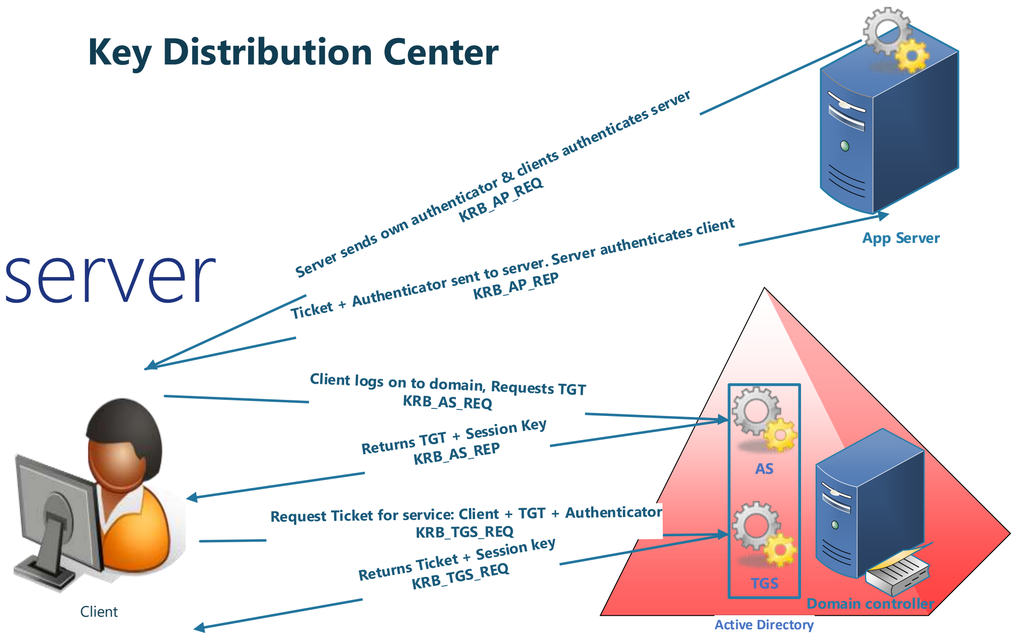
Kerberos: Key Distribution Center

Domain service that runs on every domain controller

Provides 2 services

- Authentication Service (AS)
- Ticket-Granting Service (TGS)

Used to mutually authenticate client & server



Images by Didier Van Hoye

See for more details https://en.wikipedia.org/wiki/Kerberos_(protocol)

The KDC Proxy Service

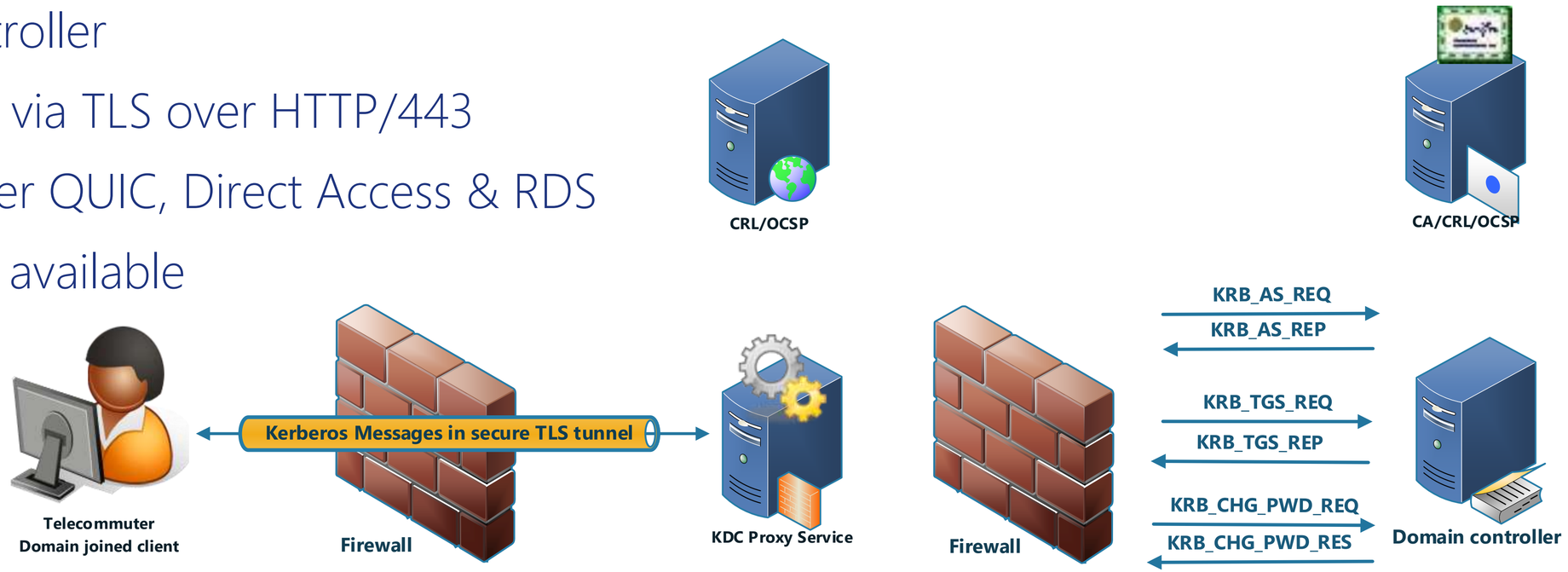
KDC Proxy Service

Provides KDC services to clients that have no line of sight to a domain controller

Secured by encryption via TLS over HTTP/443

Supported for SMB over QUIC, Direct Access & RDS

Publish CRL – must be available



Images by Didier Van Hoye

Configuring the KDC Proxy Service

Configure file sharing across the Internet with SMB over QUIC

Select a certificate (from the Local Machine\My certificate store) that identifies this server and is trusted by the server and clients. The server name must also be resolvable by client devices. Learn more

Certificate name	Status	Date issued	Expiration date	Thumbprint	Friendly name	Issuer	Signature algorithm
CN=W2k22Azure	Healthy	8/29/2023	1/28/2028	BE9BF0EE34C47021415C66804D3D88...	SMBOverQuicCert	CN=EntRootCA-DWT, DC=datawisete...	sha256RSA
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]

Addresses that SMB over QUIC clients can connect to *

- [x] Select All
- [x] W2K22Azure.datawisetech.corp
- [x] W2K22Azure
- [x] fsquic.datawisetech.corp
- [x] fsquic
- [x] quicedge.datawisetech.com

Kerberos support through KDC Proxy (requires client configuration changes)

- (•) Enabled (Recommended)
- ( ) Disabled for SMB over QUIC
- ( ) Disabled

Kerberos support through KDC Proxy (requires client configuration changes): 443

Advanced Settings

SMB encryption (in addition to QUIC encryption)

- (•) Disabled (Recommended)
- ( ) Enabled

Access to named pipes

- (•) Disabled (Recommended)
- ( ) Enabled

Configuring the KDC Proxy Service

File sharing across the internet with SMB over QUIC

Enable shares on this file server to be accessible across the internet — without using a VPN — by configuring the QUIC protocol. Learn more

SMB over QUIC is enabled

Kerberos KDC Proxy is enabled for SMB over QUIC

Certificate name	Date issued	Expiration date
CN=W2K22Azure	6/27/2021	1/21/2024

Certificate thumbprint	SMB server addresses
C2E43791CD1D64BBABB5873226B345938F4A5D09	W2K22Azure, W2K22Azure.datawisetech.corp, fsquic, fsquic.datawisetech.corp, quicedge.datawisetech.com

Edit Enable Remove Remove and disable KDC Proxy

Configuring the KDC Proxy Service

```
# 1 Configure a URL ACL for the endpoint
NETSH http add urlacl url=https://+:443/KdcProxy user="NT authority\Network Service"

# 2 Disable smartcard / Windows Hello certificates
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings" /v HttpsClientAuth
/t REG_DWORD /d 0x0 /f
Or
New-ItemProperty -Path
HKLM:\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings -Name
HttpsClientAuth -Type Dword -Value 0x0 -Force

# 3 Allwow password authentication (we are not using a cert for that)
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings" /v
DisallowUnprotectedPasswordAuth /t REG_DWORD /d 0x0 /f
Or
New-ItemProperty -Path
HKLM:\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings -Name
DisallowUnprotectedPasswordAuth -Type Dword -Value 0x0 -Force
```

Configuring the KDC Proxy Service

```
#Associate the certificate for QUIC with the endpoint ➔ tells HTTP.SYS to use the
certificate when you connect over HTTPS

$KpsFqdn = “kps.datawisetech.com”
$KpsPort = 443
$Guid = [Guid]::NewGuid().ToString("B")

$Cert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object -FilterScript { $_.Subject -
like “file01" }

#Netsh is still your best friend
$SslCertCommand = 'netsh http add sslcert hostnameport={0}:{1} certhash={2} appid={3}
certstorename=MY' -f $KpsFqdn, $KpsPort, $Cert.Thumbprint, $Guid
cmd /c $SslCertCommand
netsh http show sslcert

#Or
Add-NetIPHttpsCertBinding -ipport 0.0.0.0:443 -CertificateHash $Cert.Thumbprint -
CertificateStoreName "MY" -ApplicationId $Guid -NullEncryption $false
```

Configuring the KDC Proxy Service

```
#Add Computer Name Aliases for Kerberos
NETDOM computername file01.datawisetech.corp /add file01.datawisetech.com
NETDOM computername file01.datawisetech.corp /add fsquic.datawisetech.com
NETDOM computername file01.datawisetech.corp /add fsquic.datawisetech.corp
```

```
PS C:\Users\administrator1> NETDOM computername file01.datawisetech.corp /enum
All of the names for the computer are:

FILE01.datawisetech.corp
file01.datawisetech.com
fsquic.datawisetech.com
fsquic.datawisetech.corp
The command completed successfully.
```

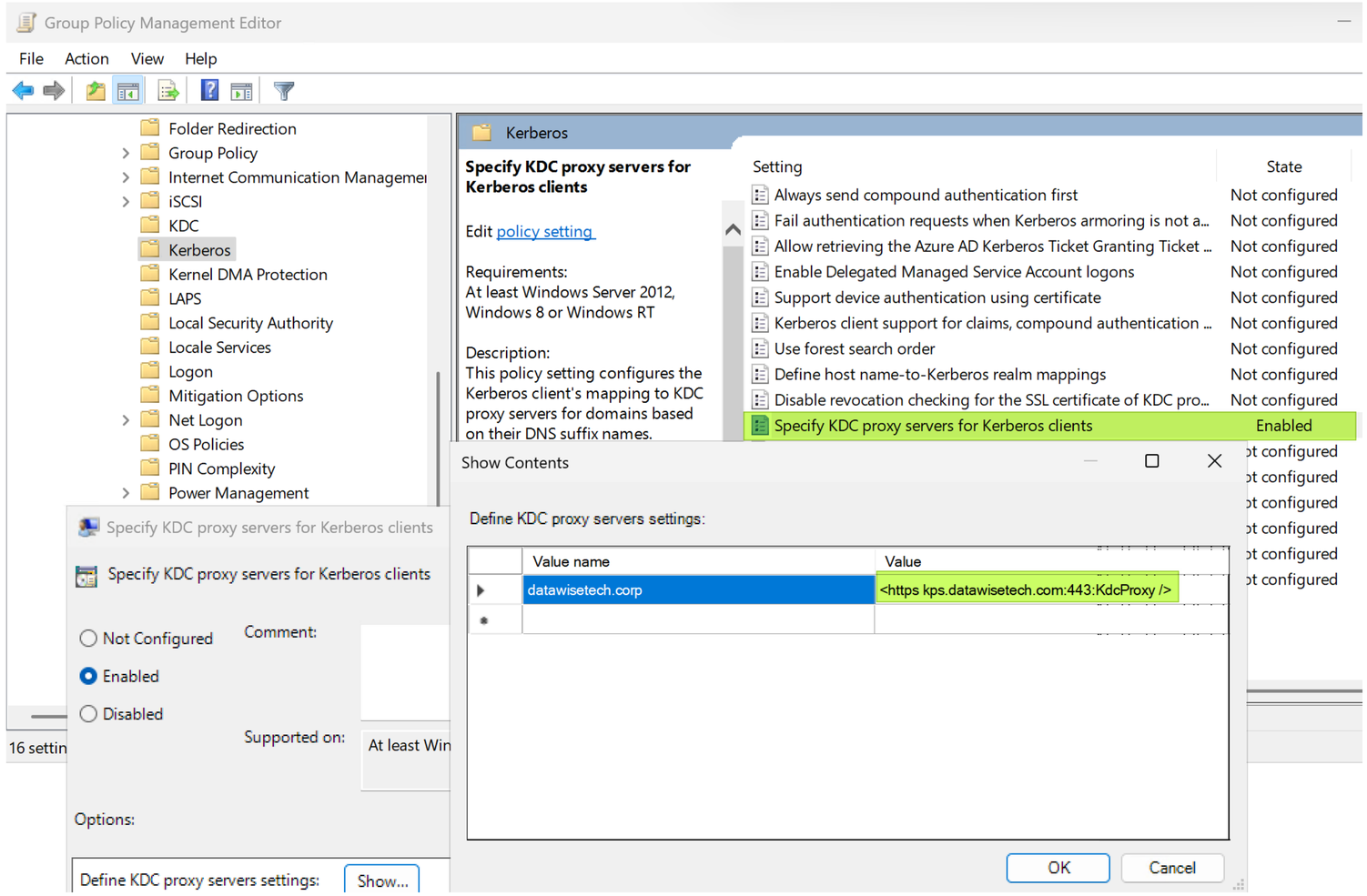
```
setspn -S HOST/file01.datawisetech.com file01
setspn -S HOST/fsquic.datawisetech.com file01
setspn -S HOST/fsquic.datawisetech.corp file01

#Set the KDC Proxy Service to start automatically
Set-Service -Name kpssvc -StartupType Automatic

#Start the KDC Proxy Service
Start-Service -Name kpssvc
```

```
C:\Users\administrator1>setspn -L File01
Registered ServicePrincipalNames for CN=FILE01,CN=Computers,DC=datawisetech,DC=corp:
        HOST/fsquic
        HOST/fsquic.datawisetech.corp
        HOST/fsquic.datawisetech.com
        http/kps.datawisetech.com
        TERMSRV/KPS
        TERMSRV/kps.datawisetech.com
        WSMAN/KPS
        WSMAN/kps.datawisetech.com
        RestrictedKrbHost/KPS
        HOST/KPS
        RestrictedKrbHost/kps.datawisetech.com
        HOST/kps.datawisetech.com
        TERMSRV/file01.datawisetech.com
        WSMAN/file01.datawisetech.com
        RestrictedKrbHost/file01.datawisetech.com
        HOST/file01.datawisetech.com
        TERMSRV/FILE01
        TERMSRV/FILE01.datawisetech.corp
        WSMAN/FILE01
        WSMAN/FILE01.datawisetech.corp
        RestrictedKrbHost/FILE01
        HOST/FILE01
        RestrictedKrbHost/FILE01.datawisetech.corp
        HOST/FILE01.datawisetech.corp
```

Specify KDC Proxy Server for clients

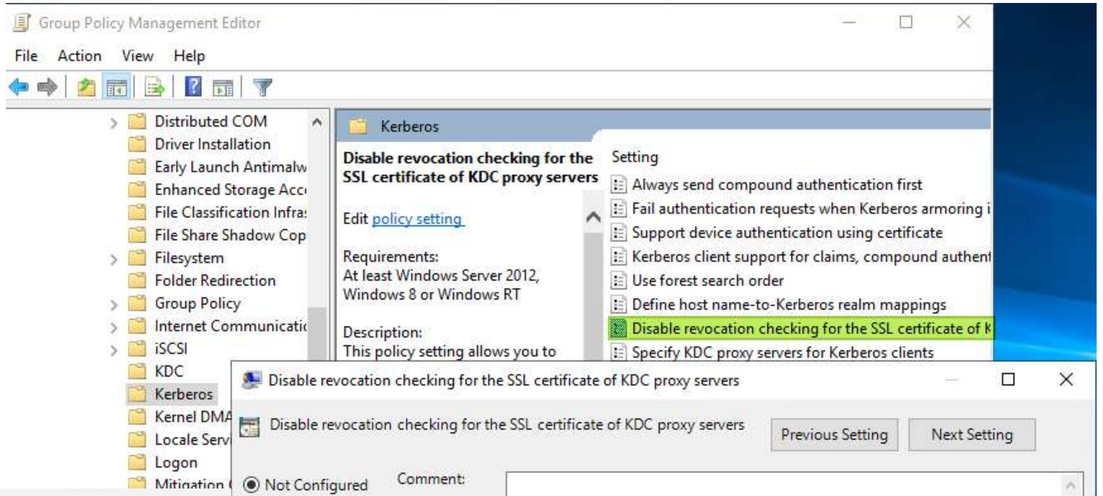


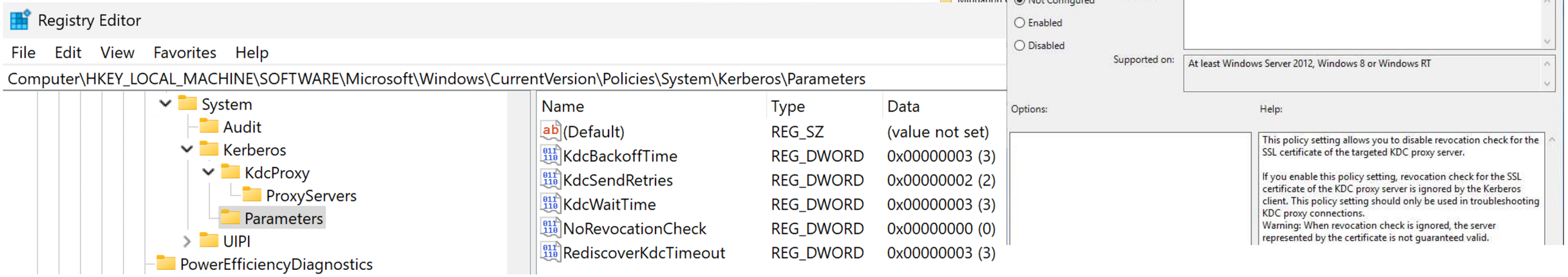
Disable revocation checking on client

You need to be able to check the CRL/OCSP for the certificate

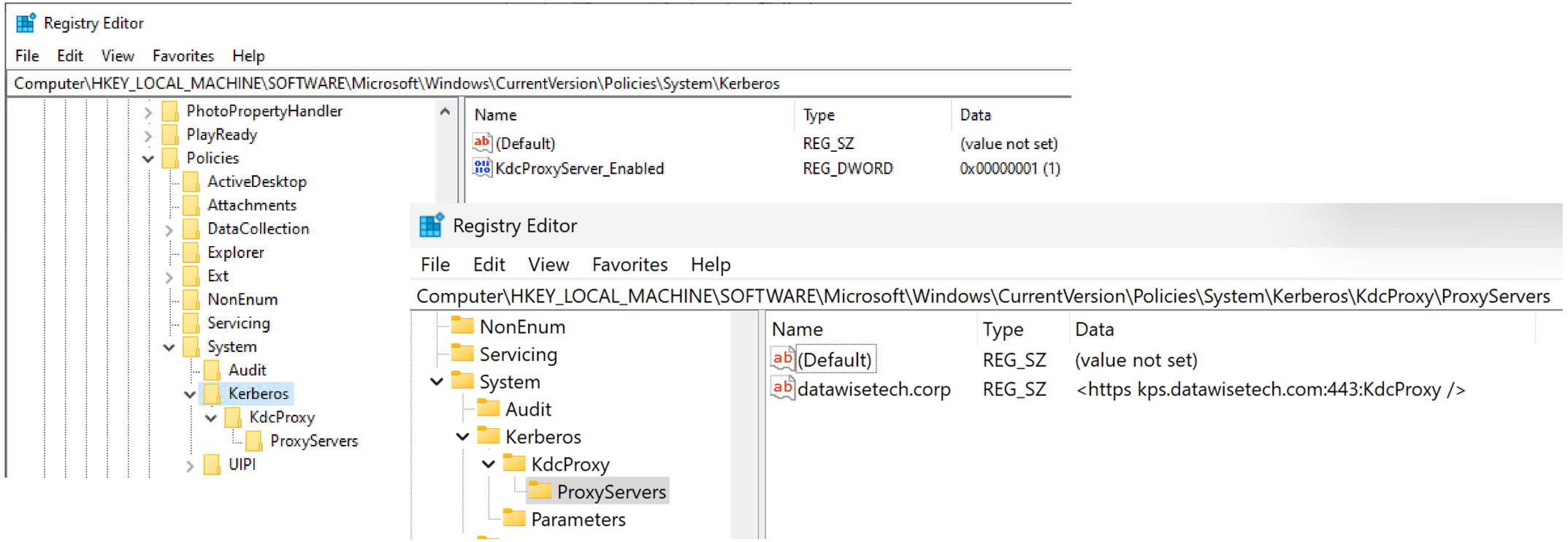
Disable this for lab/troubleshooting

Tune KDC params when needed





Specify KDC Proxy Server for clients



[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos]
"KdcProxyServer_Enabled"=dword:00000001

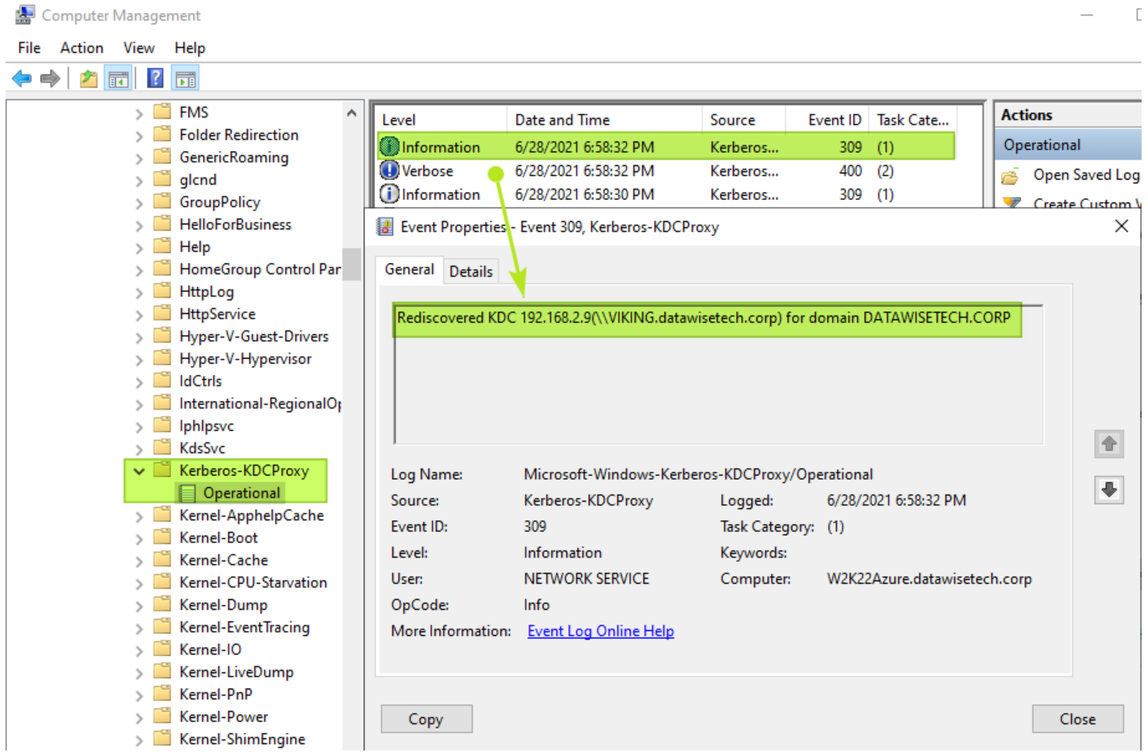
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\KdcProxy\ProxyServers]
“datawisetech.corp"="<https kps.datawisetech.com:443:kdcproxy />"

Demo
KDC Proxy Service

Is the KDC Proxy being used?

Kerberos-KDCProxy\Operational log

Enable “Show Analytic and Debug Logs.”



View those Kerberos tickets appear

klist get krbtgt

```
Cached Tickets: (3)

#0>     Client: administrator1 @ DATAWISETECH.CORP
        Server: krbtgt/DATAWISETECH.CORP @ DATAWISETECH.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 5/29/2025 11:01:20 (local)
        End Time:   5/29/2025 21:01:20 (local)
        Renew Time: 6/3/2025 10:16:21 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DC01

#1>     Client: administrator1 @ DATAWISETECH.CORP
        Server: cifs/NPS01 @ DATAWISETECH.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 5/29/2025 11:16:33 (local)
        End Time:   5/29/2025 21:01:20 (local)
        Renew Time: 6/3/2025 10:16:21 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DC01

#2>     Client: administrator1 @ DATAWISETECH.CORP
        Server: cifs/NPS02 @ DATAWISETECH.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 5/29/2025 11:16:33 (local)
        End Time:   5/29/2025 21:01:20 (local)
        Renew Time: 6/3/2025 10:16:21 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DC01
```

```
C:\Users\quicdemo>klist

Current LogonId is 0:0x1b5d6e

Cached Tickets: (4)

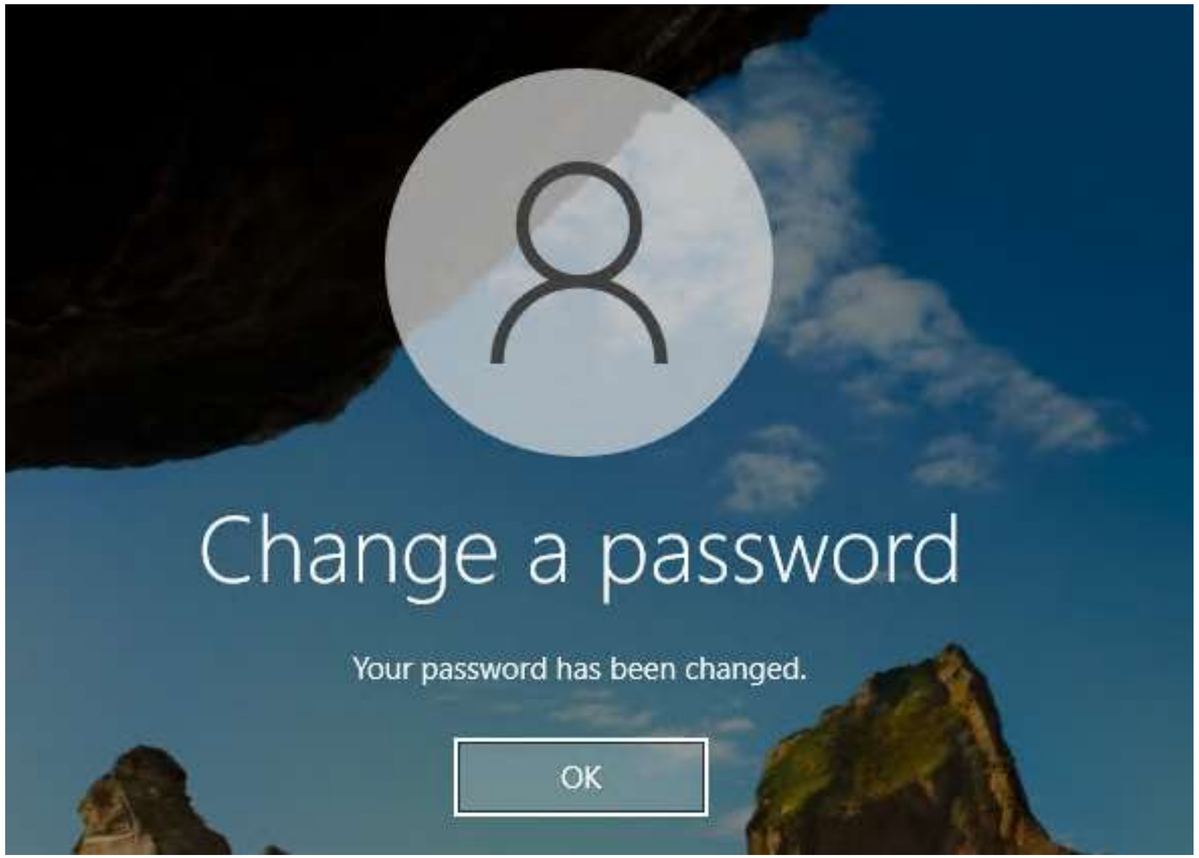
#0>     Client: quicdemo @ DATAWISETECH.CORP
        Server: krbtgt/DATAWISETECH.CORP @ DATAWISETECH.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 5/29/2025 13:12:11 (local)
        End Time:   5/29/2025 23:12:11 (local)
        Renew Time: 6/5/2025 13:12:11 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: KdcProxy:kps.datawisetech.com

#1>     Client: quicdemo @ DATAWISETECH.CORP
        Server: cifs/fsquic.datawisetech.com @ DATAWISETECH.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 5/29/2025 13:19:01 (local)
        End Time:   5/29/2025 23:12:11 (local)
        Renew Time: 6/5/2025 13:12:11 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: KdcProxy:kps.datawisetech.com

#2>     Client: quicdemo @ DATAWISETECH.CORP
        Server: cifs/file01.datawisetech.corp @ DATAWISETECH.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 5/29/2025 13:12:52 (local)
        End Time:   5/29/2025 23:12:11 (local)
        Renew Time: 6/5/2025 13:12:11 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: KdcProxy:kps.datawisetech.com

#3>     Client: quicdemo @ DATAWISETECH.CORP
        Server: cifs/fsquic.datawisetech.corp @ DATAWISETECH.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 5/29/2025 13:12:14 (local)
        End Time:   5/29/2025 23:12:11 (local)
        Renew Time: 6/5/2025 13:12:11 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: KdcProxy:kps.datawisetech.com
```

Change your password over internet



Conclusion

QUIC is a fast-rising layer 4 network prot

SMB over QUIC is a foundational te , Client as well as on other operating systems vi

File Servers & file sharing ar ybrid or cloud.

Setting & configuratio Center

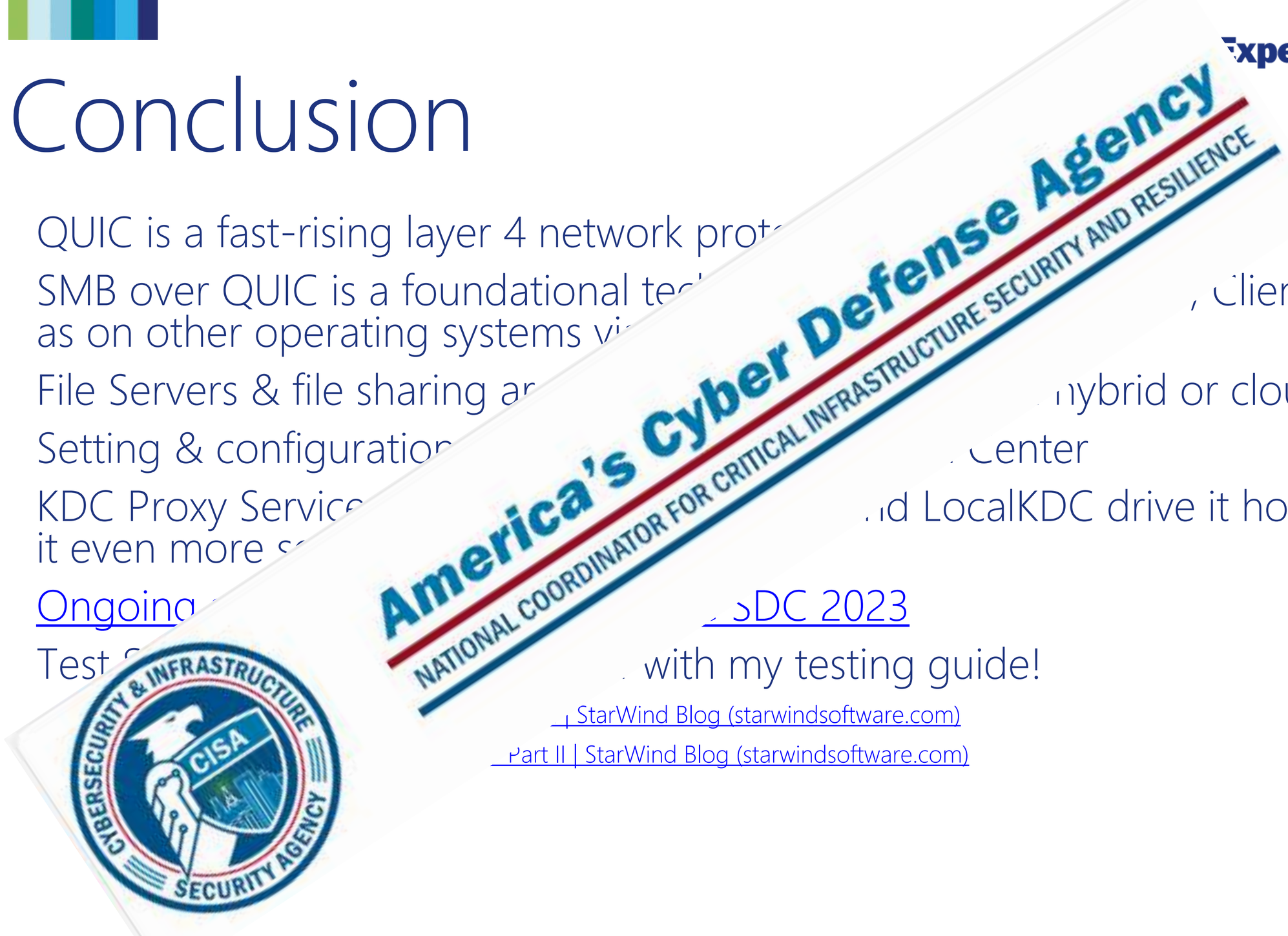
KDC Proxy Servic d LocalKDC drive it home make it even more s

Ongoing sDC 2023

Test with my testing guide!

StarWind Blog (starwindsoftware.com)

Part II | StarWind Blog (starwindsoftware.com)



Experts Live Austria

Thanks to our sponsors!

PLATINUM

ACP IT for innovators.

ConStraight

mann&mouse
WE LIVE IT

base it

THOMAS KRENN®
IT's people business

GOLD

CANCOM

INFOTECH
[IT & Communication]

ProLion

DATACIDERS
PASO

NiCE
IT Management Solutions
www.nice.de

SEPP MAIL

Questions & Answers