

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



Didier Van Hoye

Technical Architect & Technology Strategist



Thanks to our sponsors!

PLATINUM



GOLD





Agenda

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



QUIC

A quick word about QUIC

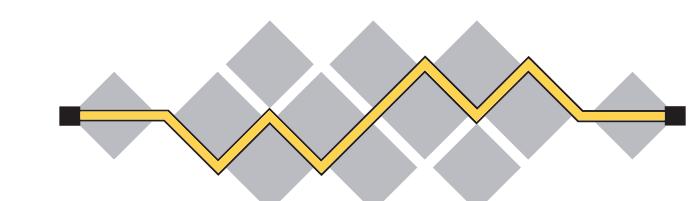


What is QUIC?

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

Today QUIC is an IETF-standardized transport protocol

Wide, growing industry backing and support ...



Google



fastly®

moz://a



trafficserver™

Microsoft

I E T F®



NGINX



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 implementation of the IETF QUIC transport protocol → [GitHub - microsoft/QuicLib](#)





What “caused” QUIC?

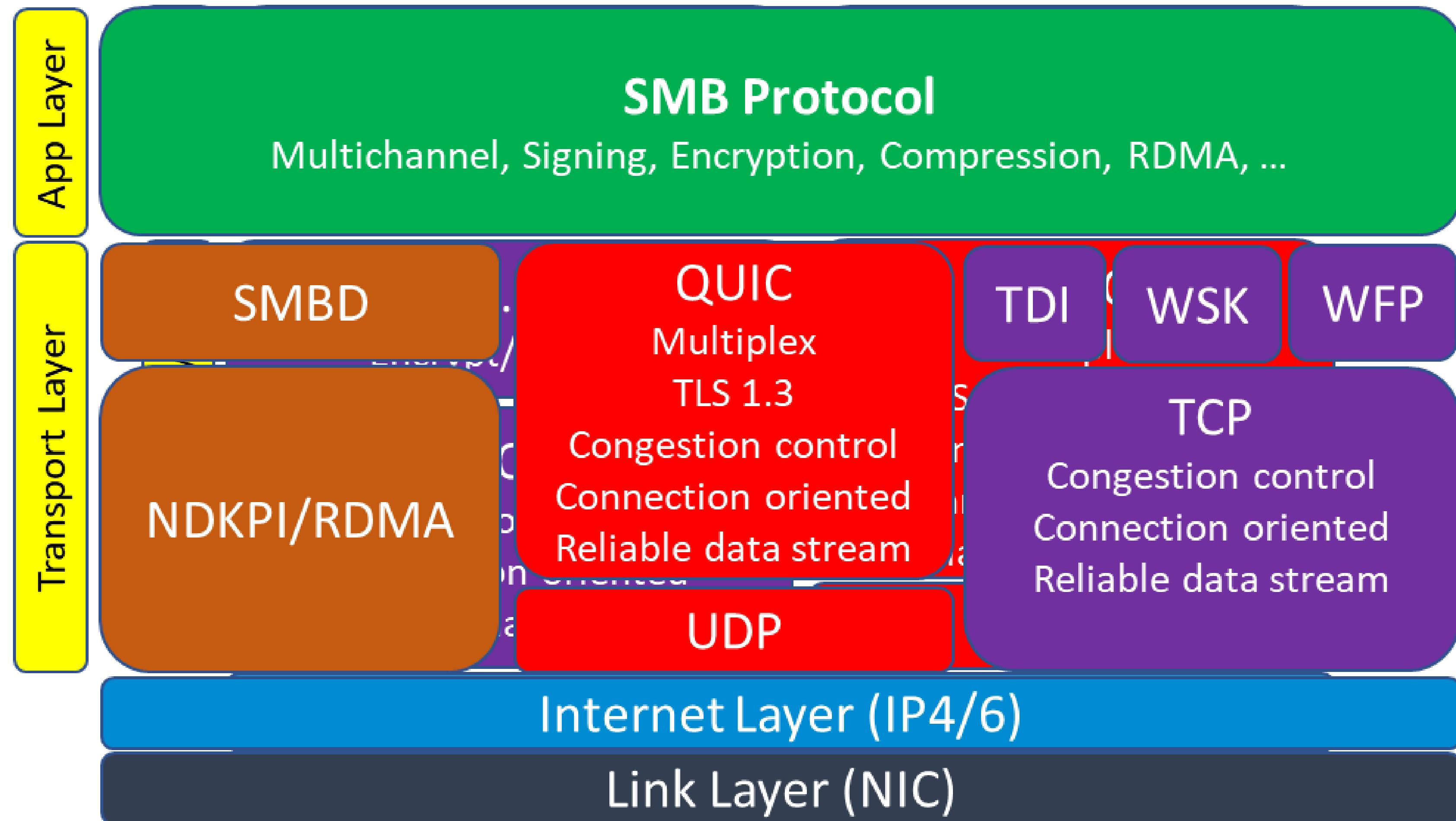
Too intimate coupling of HTTP/2 with TCP/IP

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



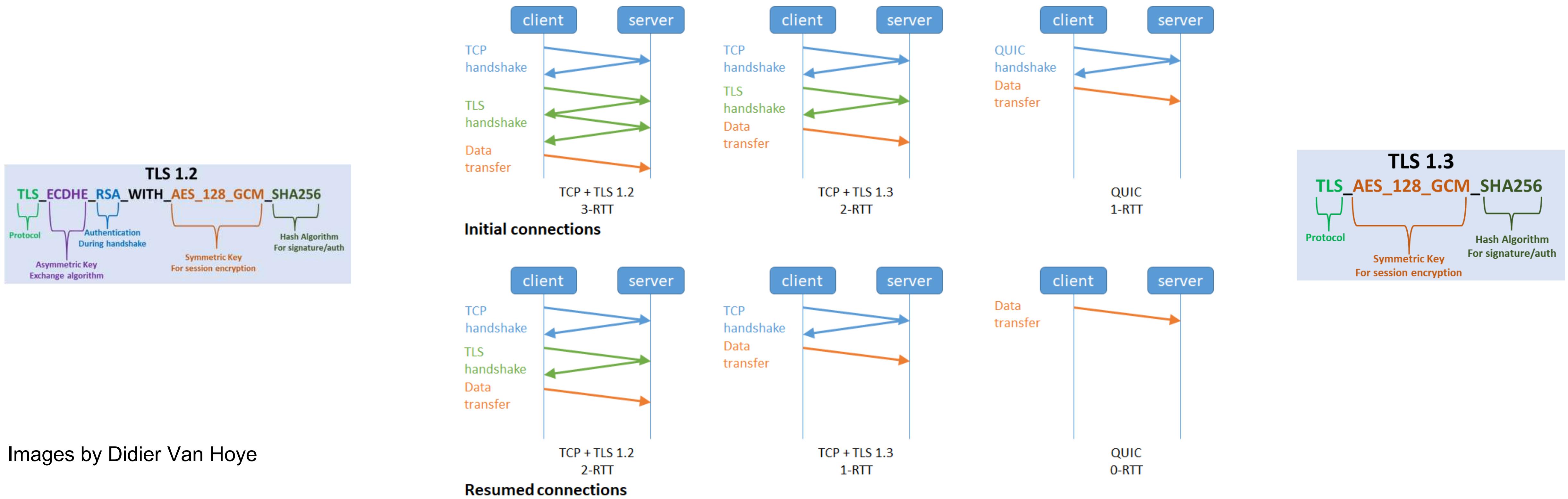
(Image by DidiVavahNeve)



Goals of QUIC (1/4)

1. QUIC reduces connection times over TLS

- Replaces lengthy TCP & TLS handshake with a single handshake

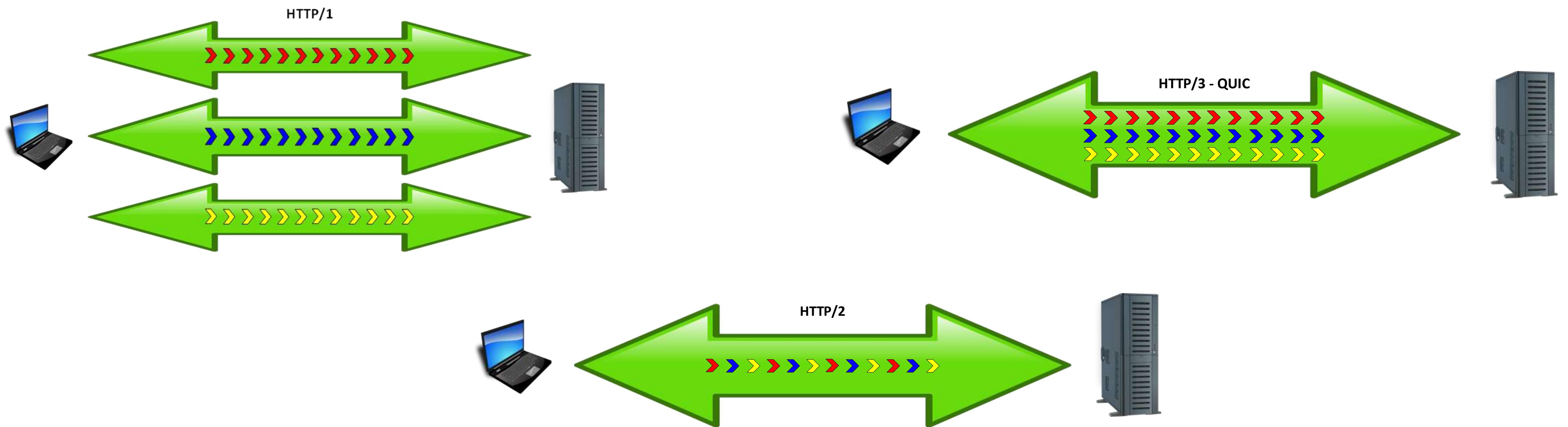


Images by Didier Van Hoye



Goals of QUIC (2/4)

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

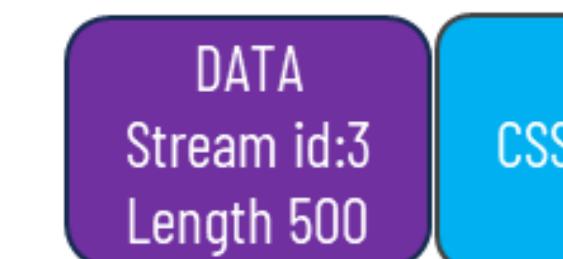
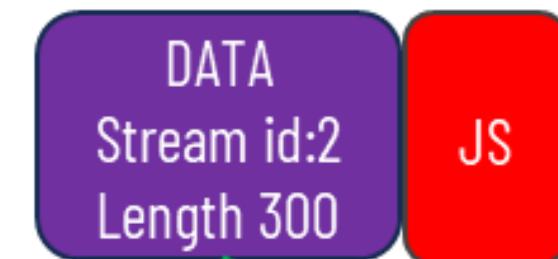
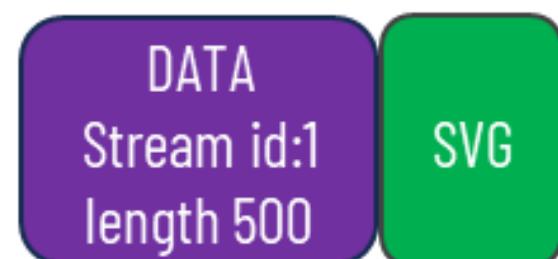


Images by Didier Van Hoye



Solving HOL blocking

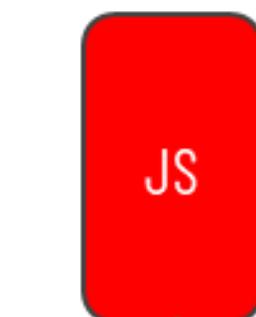
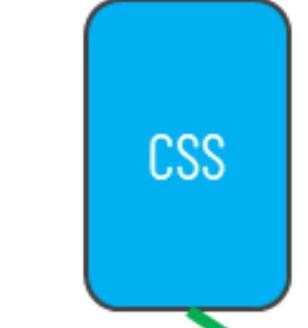
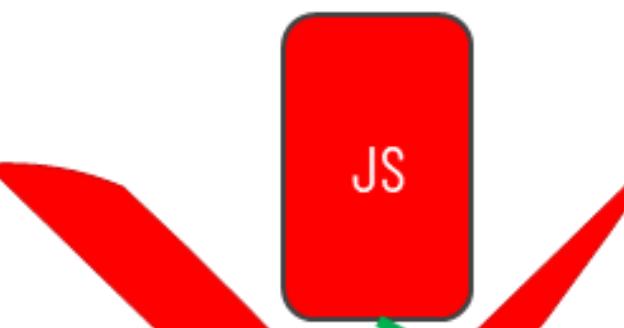
HTTP/2



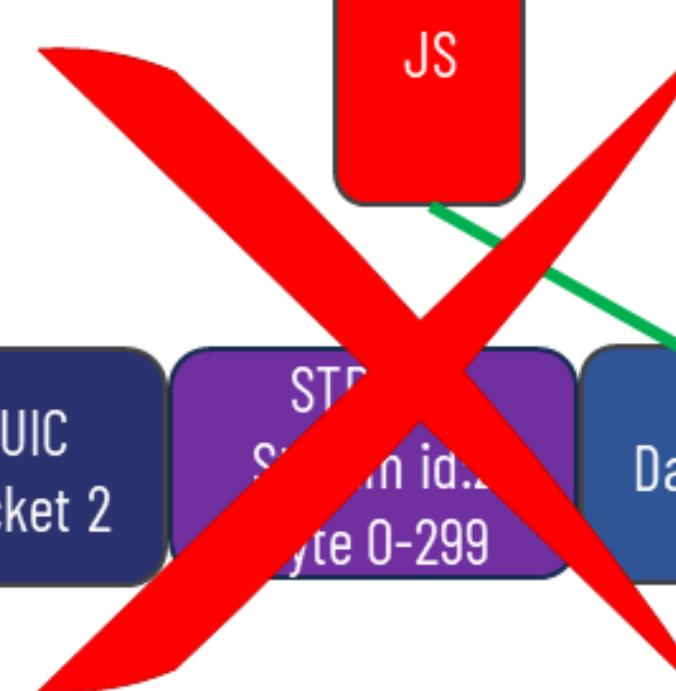
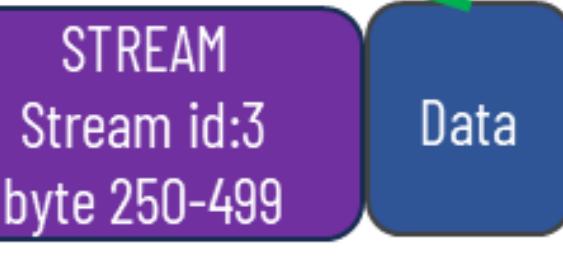
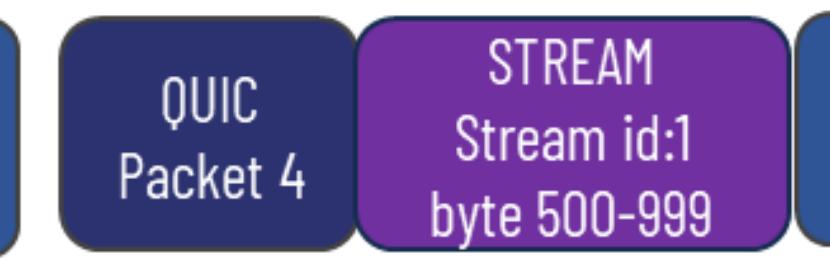
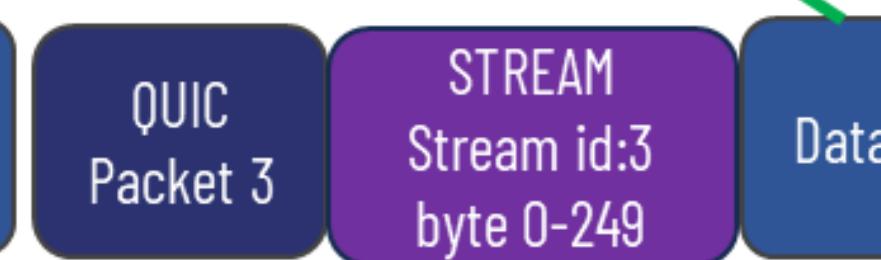
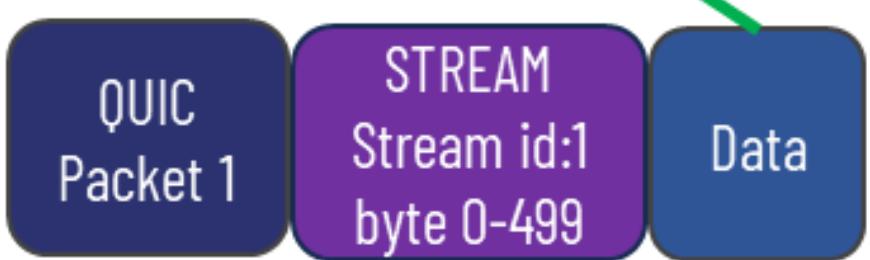
TCP



HTTP/3



QUIC





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

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



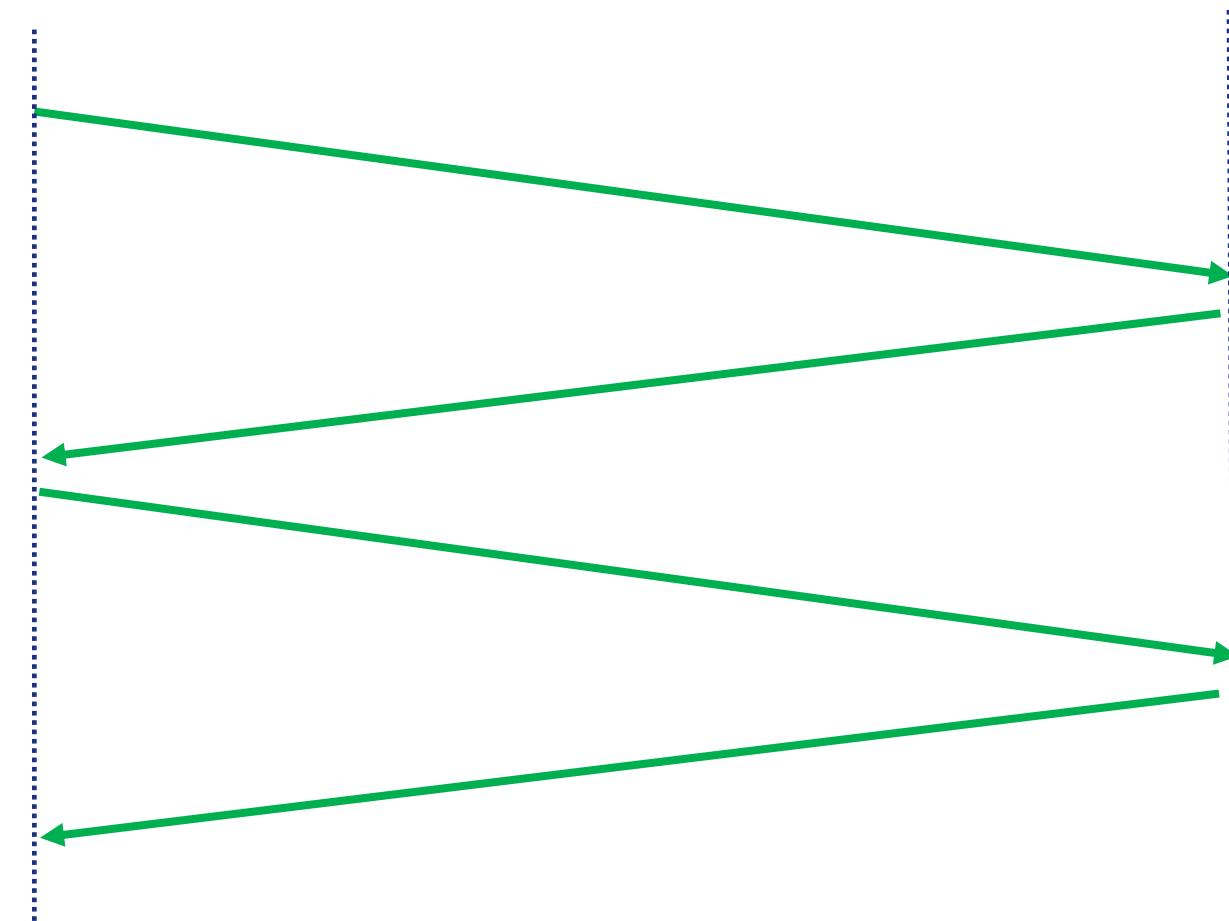
Image by [Pete Linforth](#) from [Pixabay](#)



Connection ID details

Client Wi-Fi

Server

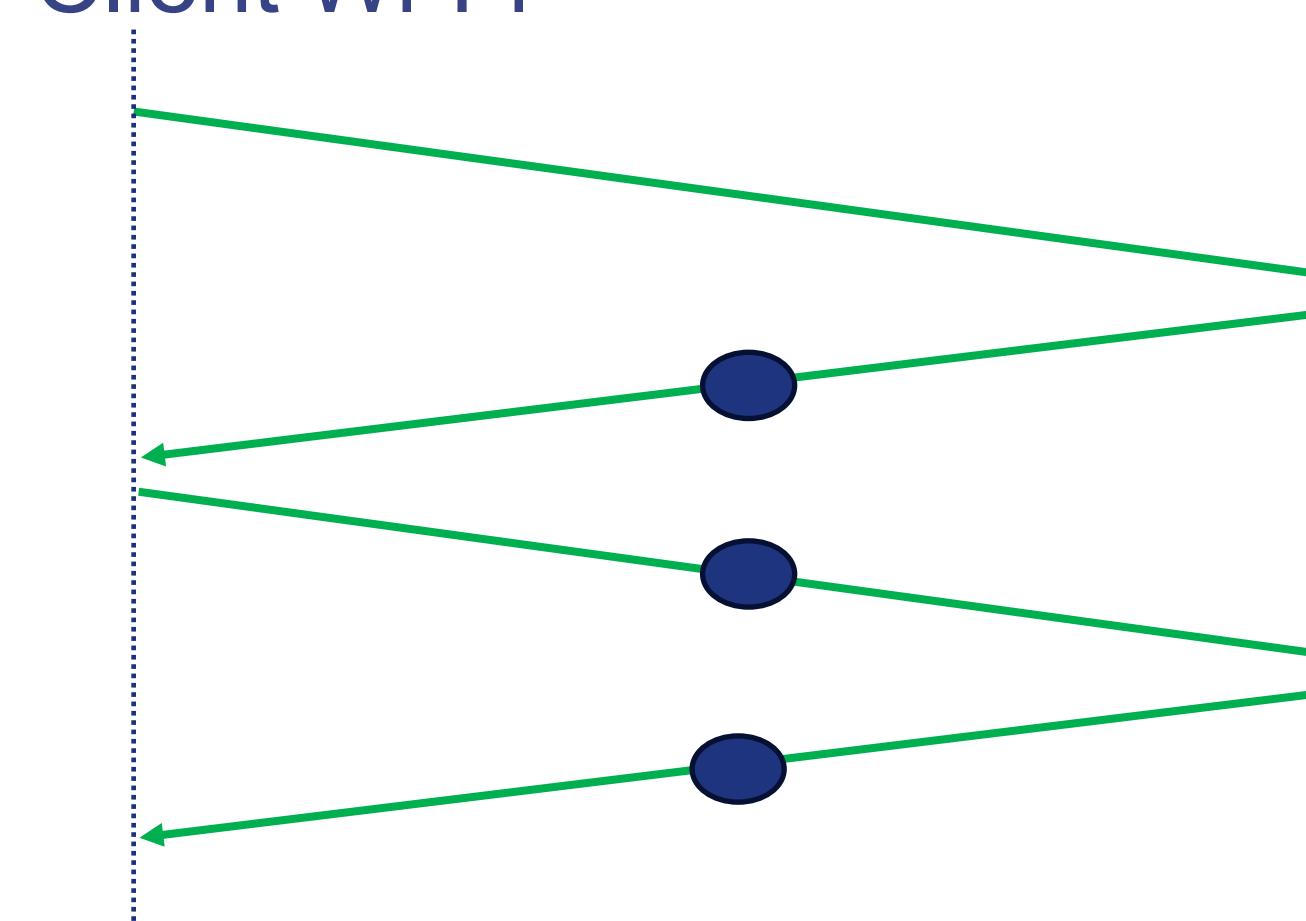


TCP handshake
from Wi-Fi
Establishes connection

Client 5G

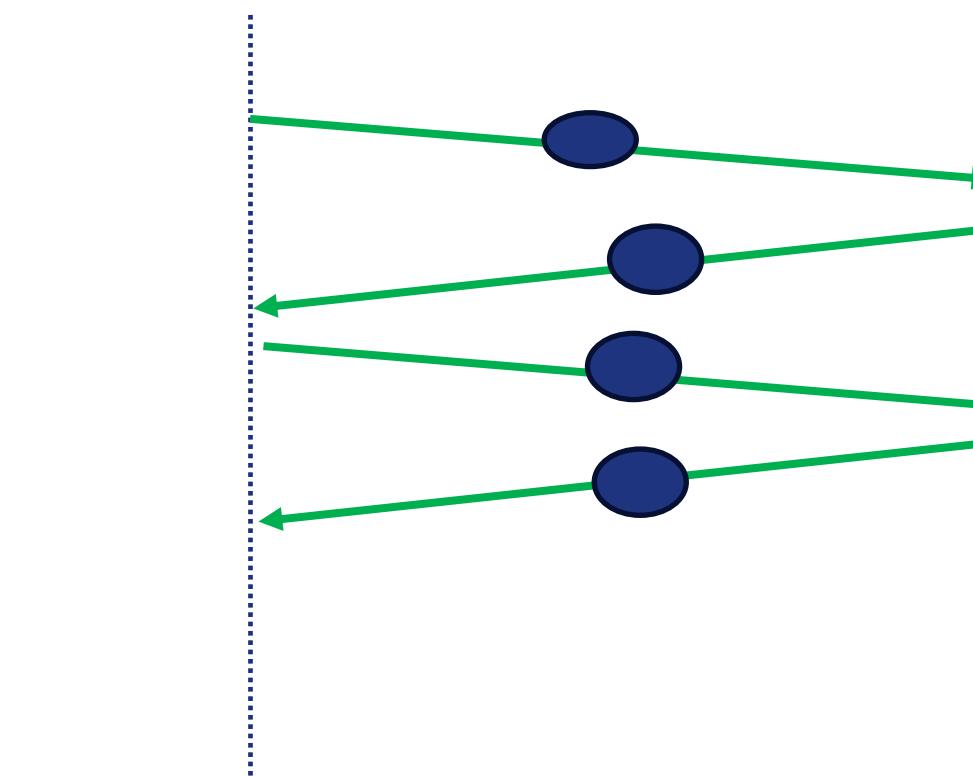
TCP packet from
unknown IP on 5G
➔ unusable
Connection is lost
Needs to reestablish
from 5G

Client Wi-Fi



QUIC handshake
from Wi-Fi
Establishes connection
and uses the following
CID:

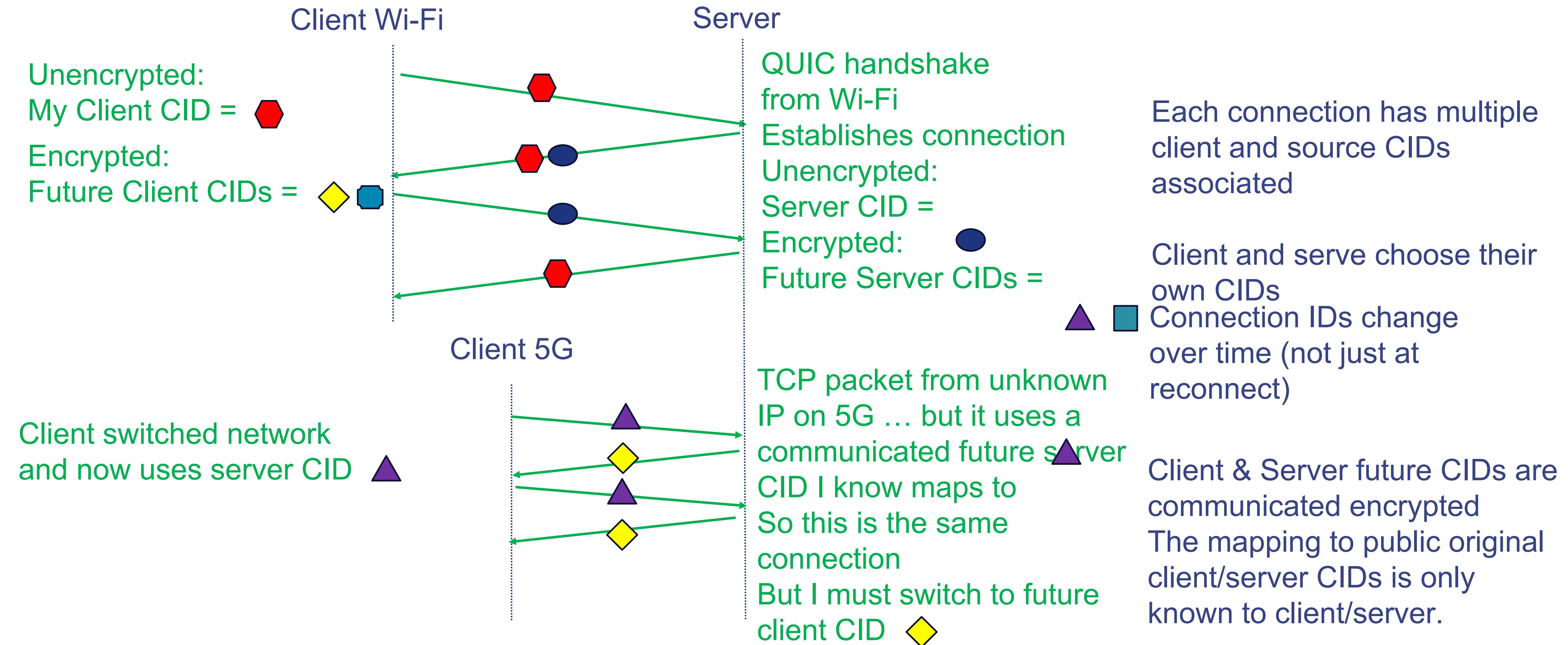
Client 5G



TCP packet from
unknown IP on 5G ...
but same CID so this is
the same connection



Asymmetric Linkability Prevention





Security Critiques & FUDs

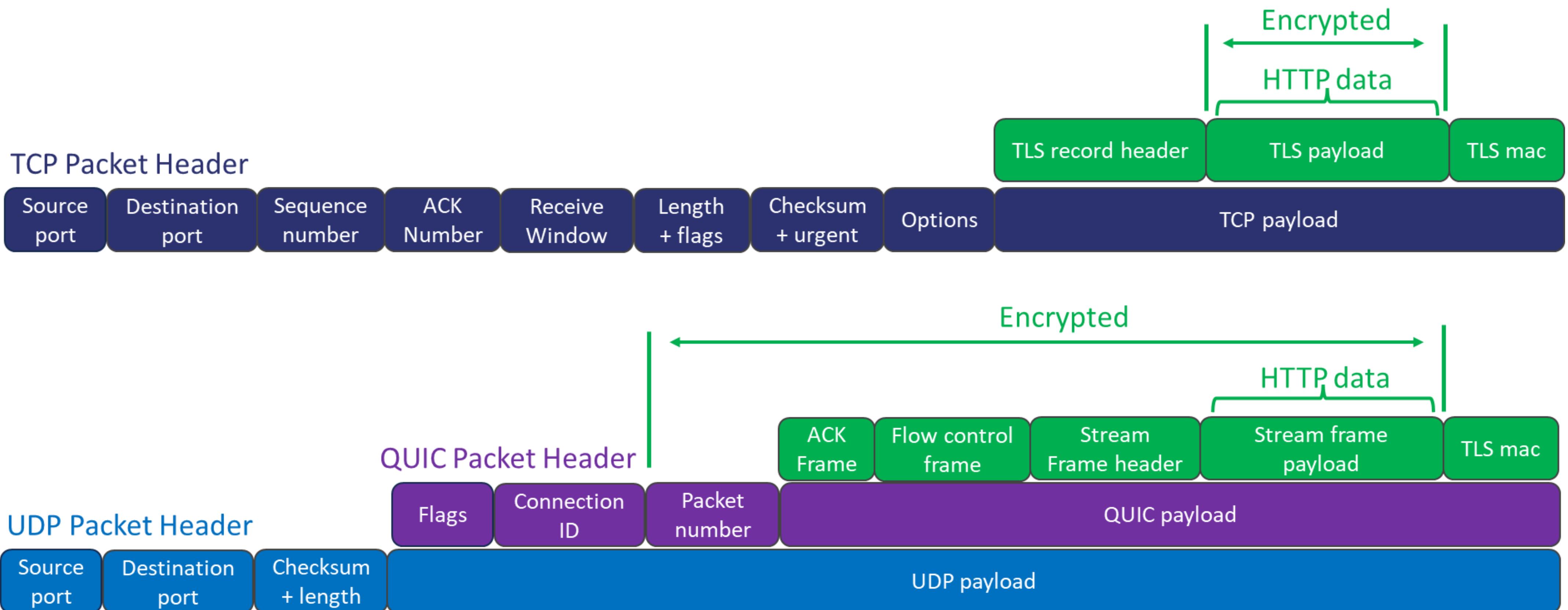
- Our firewalls are blind as a mole now
- TLS inspection is dead
- Bad for app visibility & control
- Breaks DDOS detection/prevention (UDP)
- Logging and Reporting
- Search term alerts, YouTube viewing lists



<https://www.cleapng.com/png-firewall-computer-icons-computer-network-clip-art-1182907/download-png.html>
<https://www.cleapng.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](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 ? 🔍 🔗

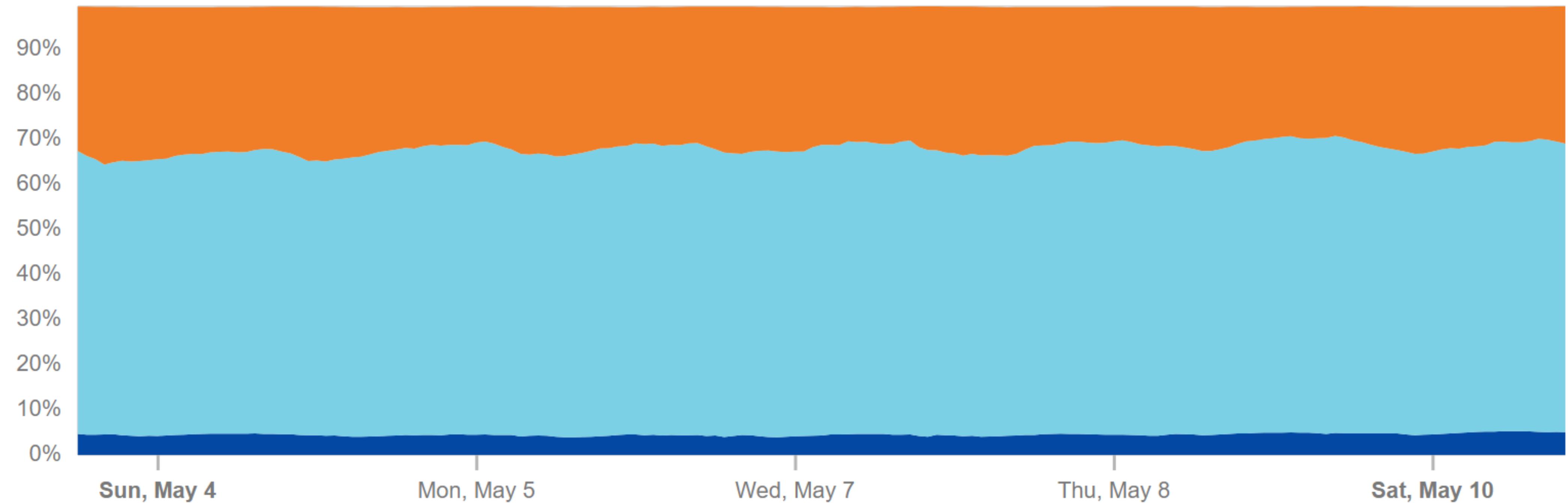
— TLS 1.2 — TLS 1.3 — QUIC

4.5%

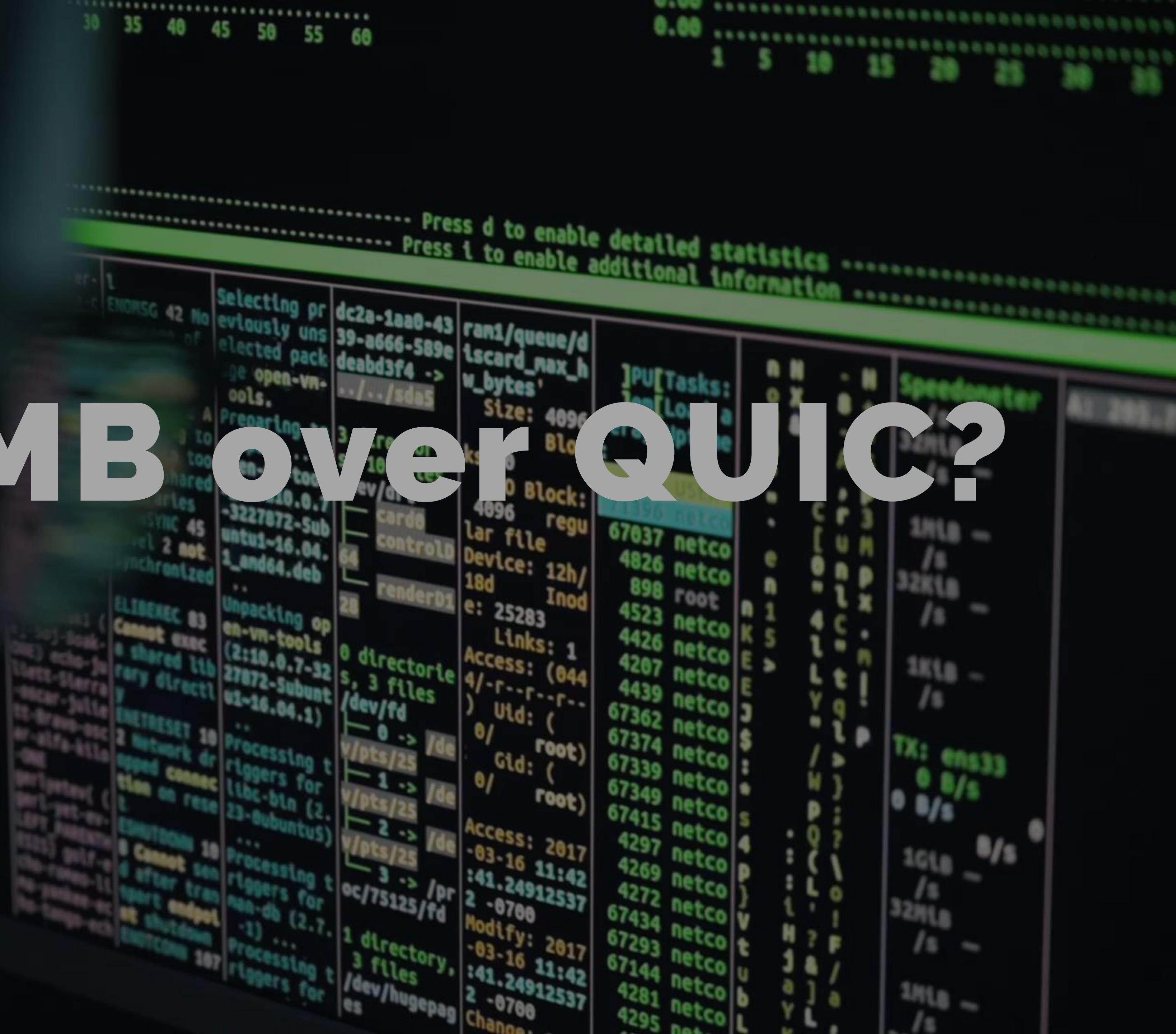
63.6%

31.4%

<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, ...

- Port 445 blocked Firewalls and by Law
- 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



Azure File Share



[Israel Andrade](#) on [Unsplash](#)



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](#)

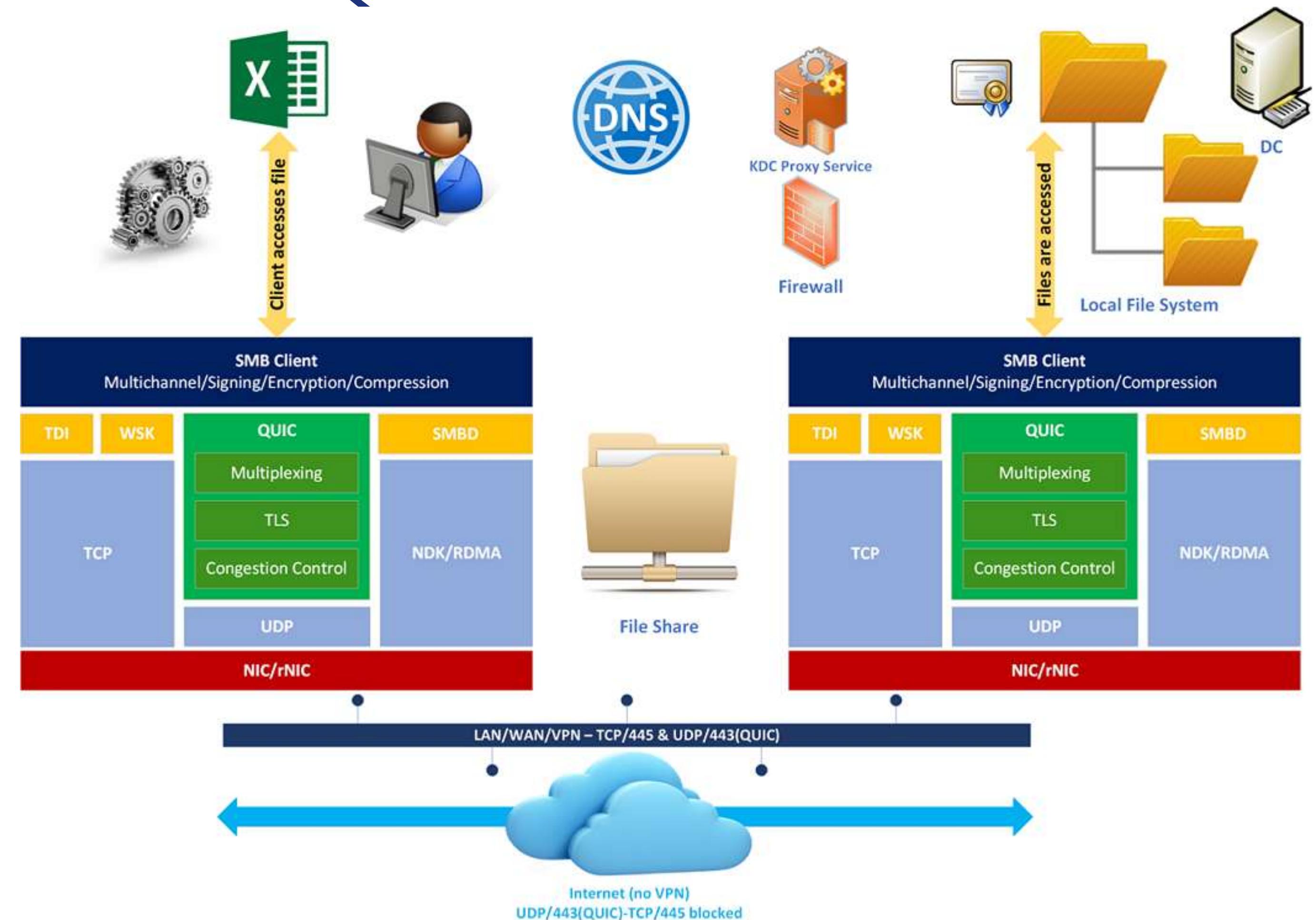


[Standsome Worklifestyle](#) on [Unsplash](#)



[Helena Lopes](#) on [Unsplash](#)

SMB over QUIC overview



Images by Didier Van Hoye

Where can we use SMB over QUIC?

```
ne Text File e.html
8. count').each(function () {
  $(this).prop('Counter', 0).animate({
    Counter: $(this).text()
  }, {
    duration: 4000,
    easing: 'swing',
    step: function (now) {
      $(this).text(Math.ceil(now));
    }
  });
  document.onload = function(){
    document.getElementById('objeto').onclick = function(){
      $( "#fadeIn" ).fadeIn();
    }
  }
});
```



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 ☺

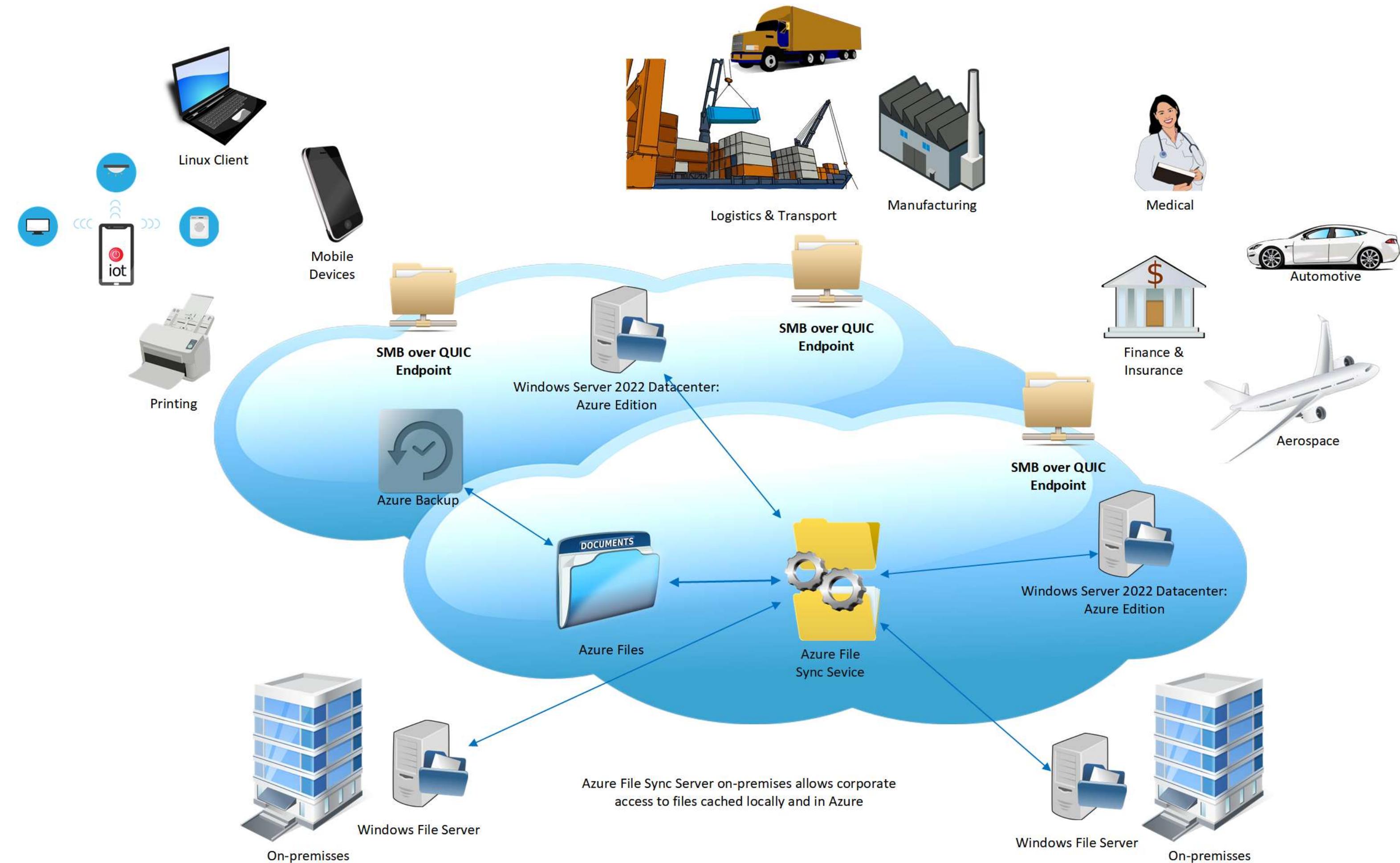
Windows 11

Is that it?

- Lack of clients is a roadblock to adoption
- Luckily, it is not! 3rd party expert solutions fill the gap!

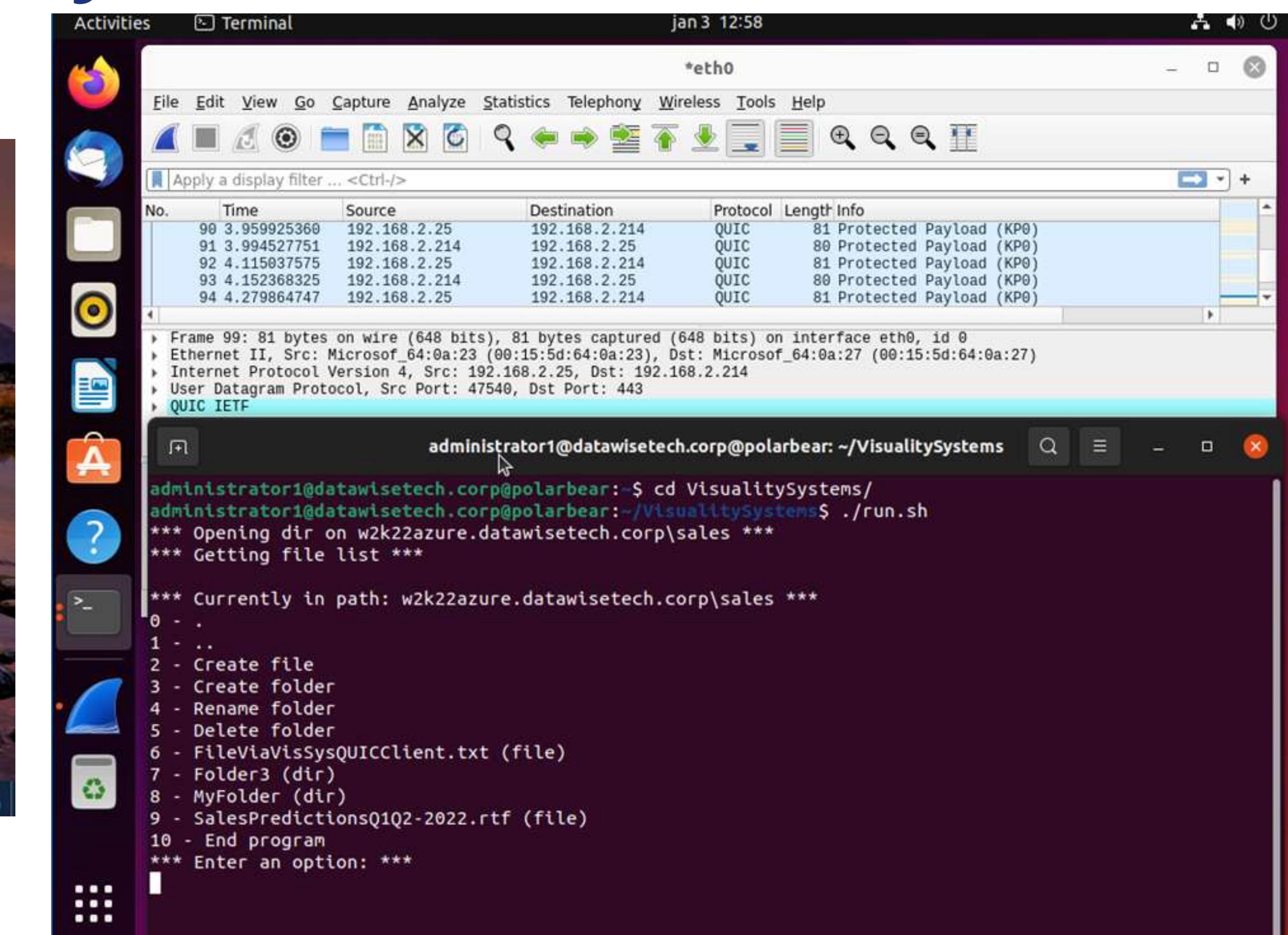
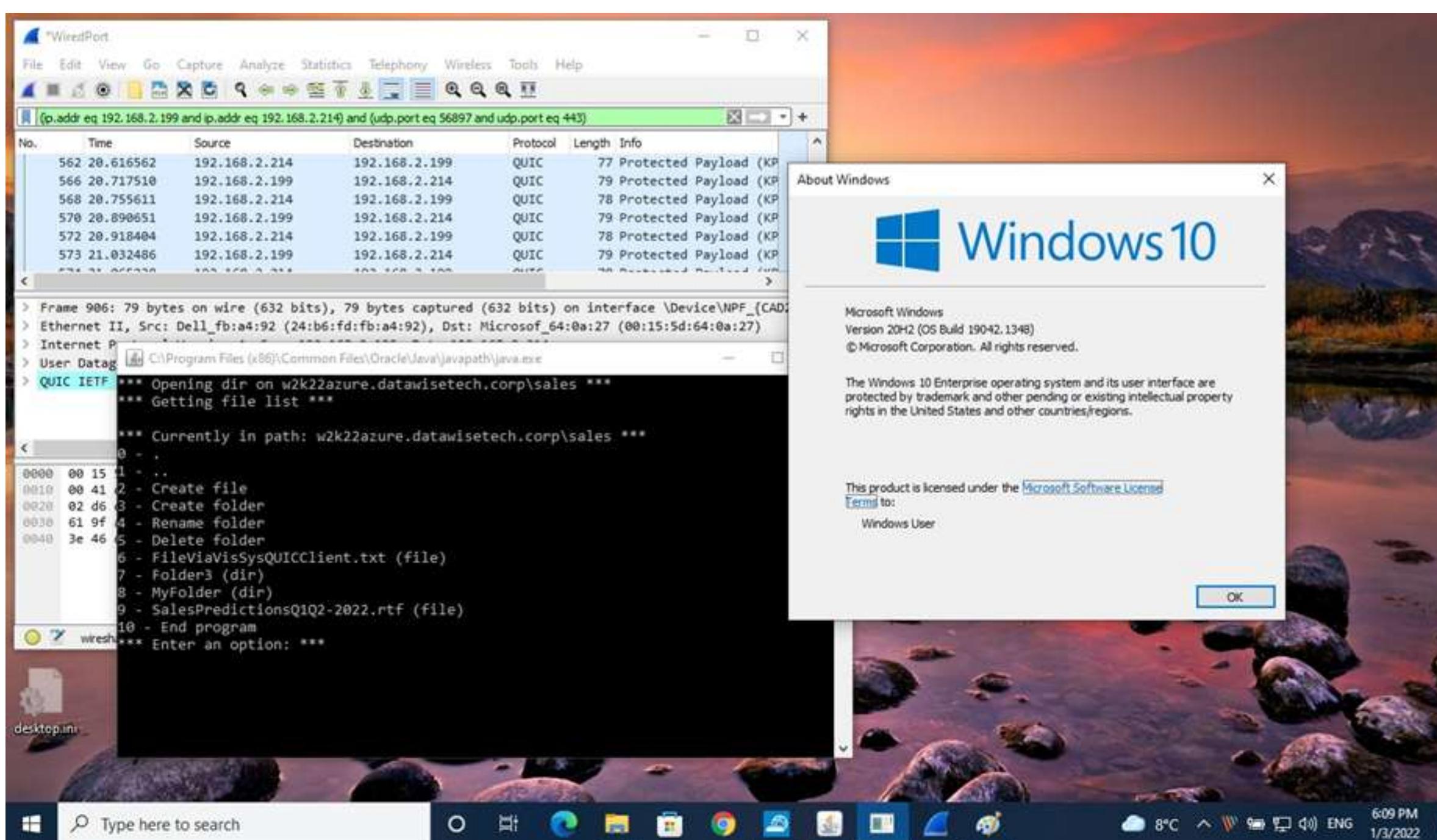
Sadly missing in Azure Files!

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

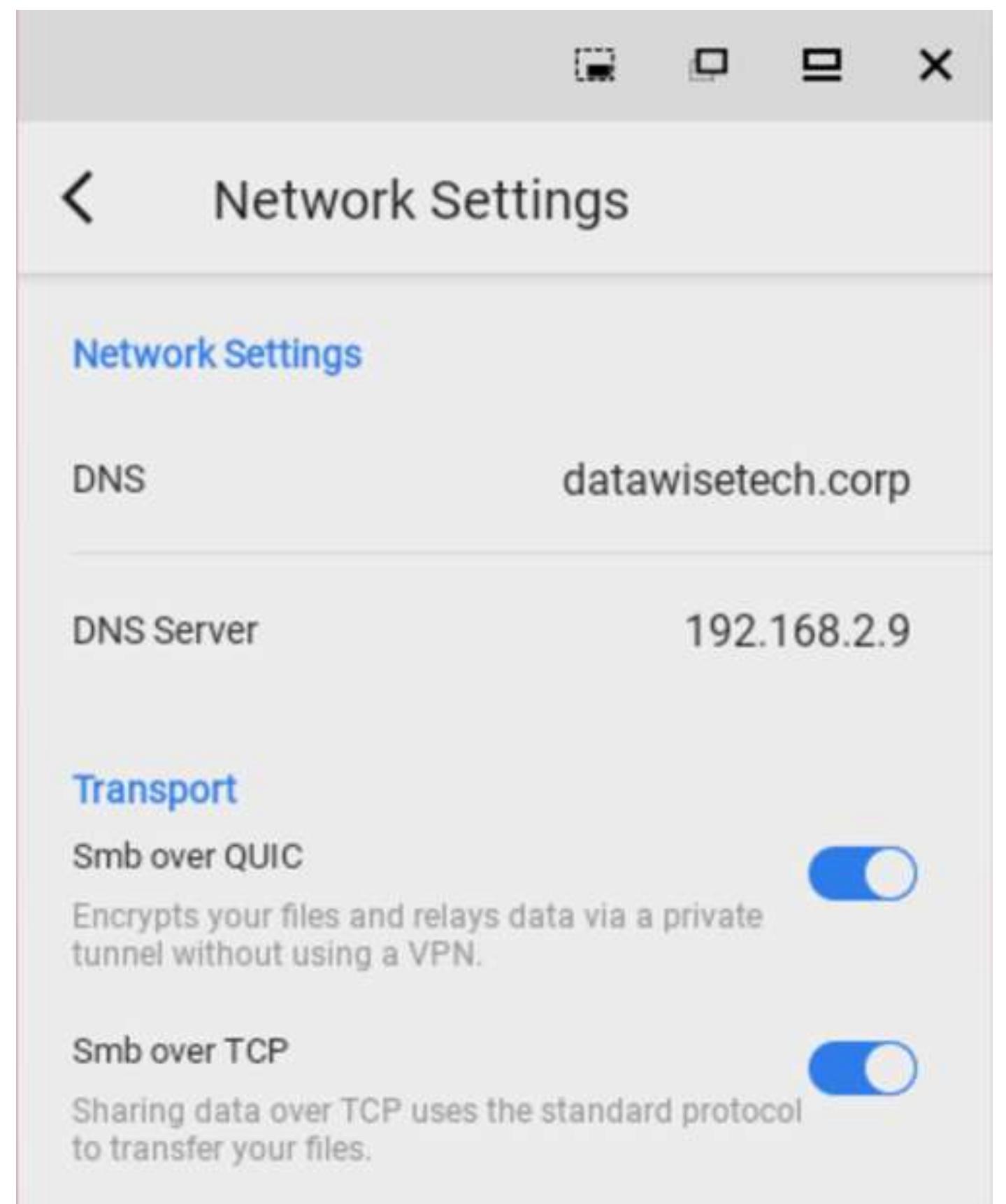
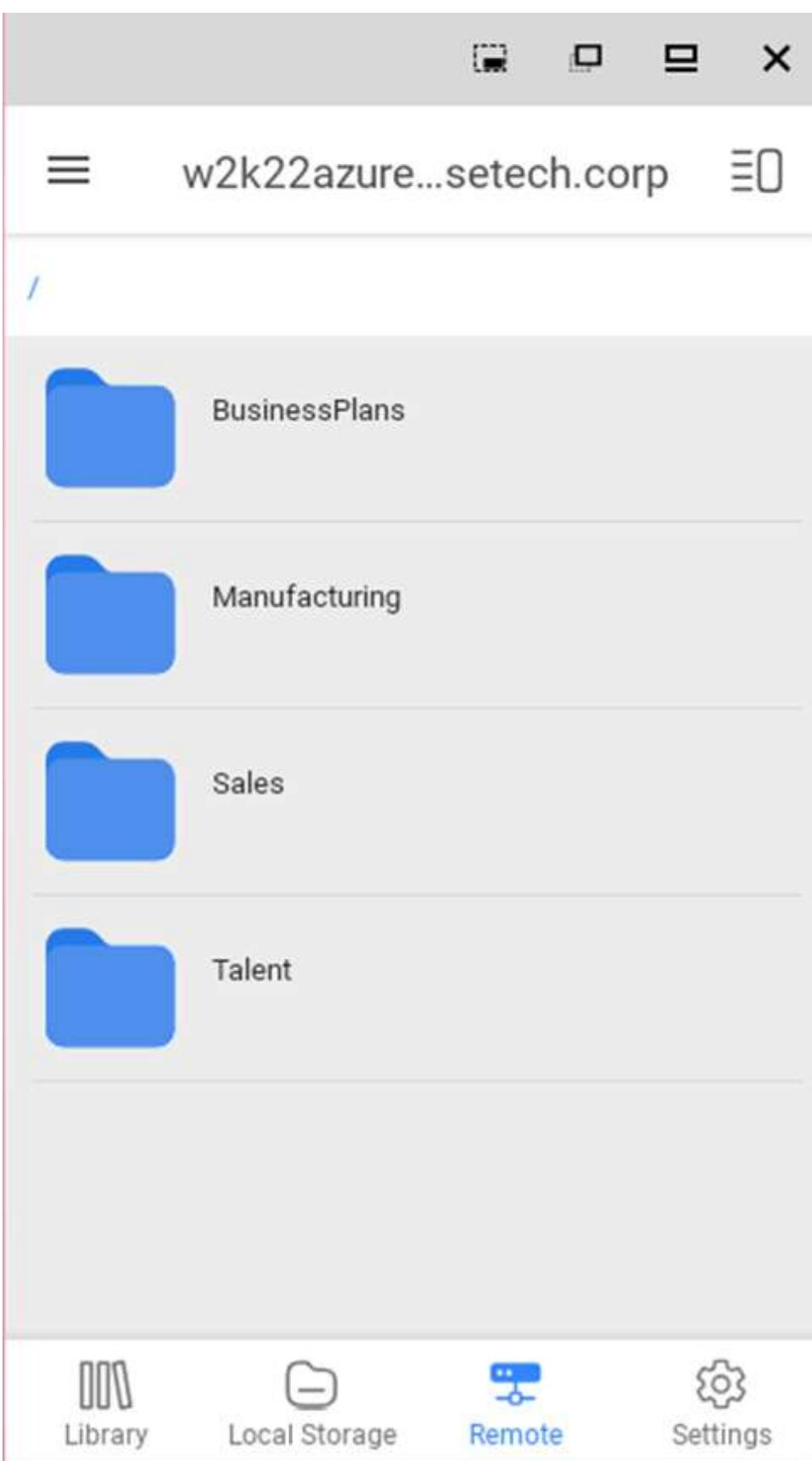
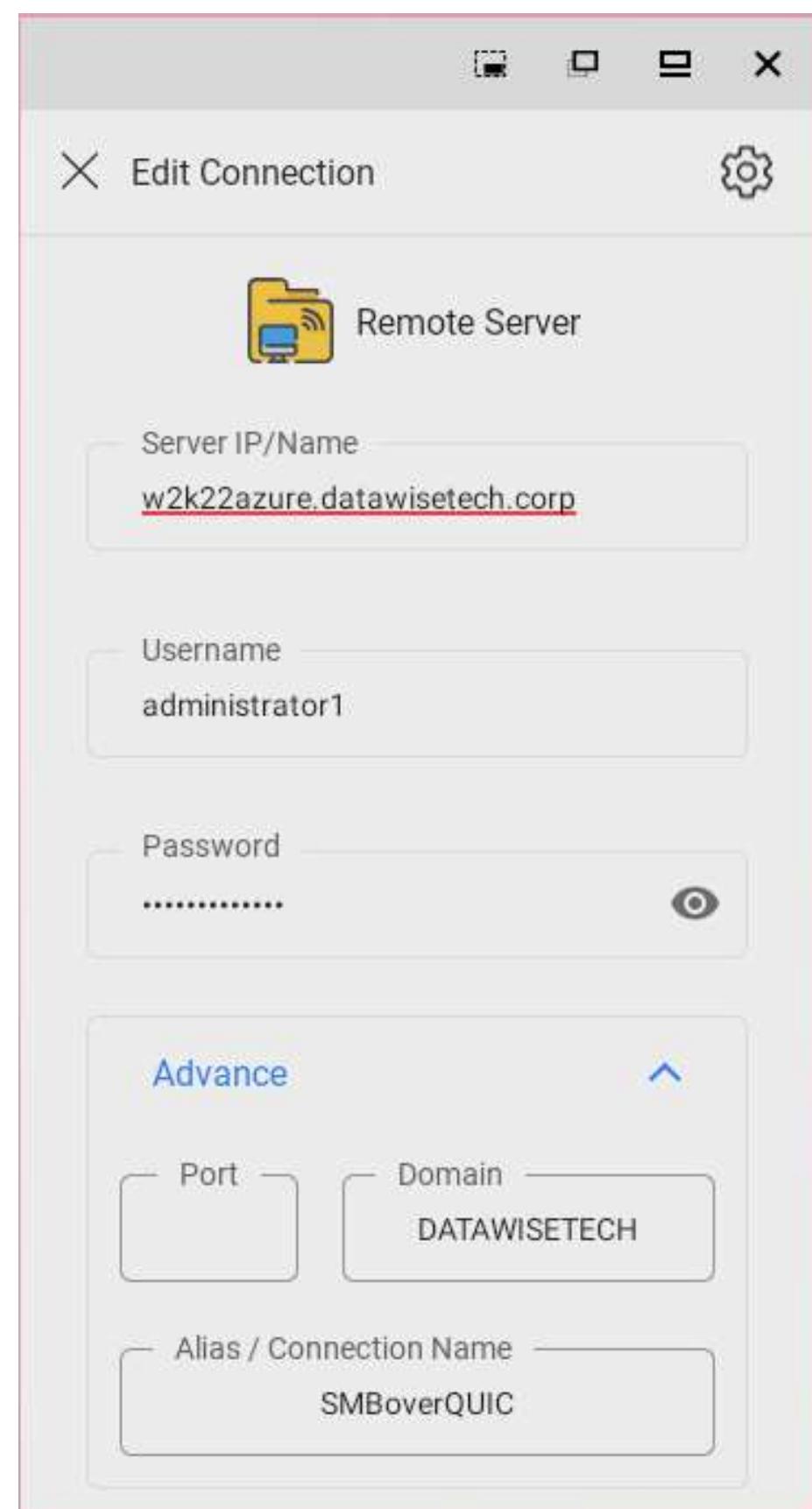


Images by Didier Van Hoye

Other operating systems



Android



<https://vqr.vc/QQSd1ebRc>



Libraries

YNQ



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

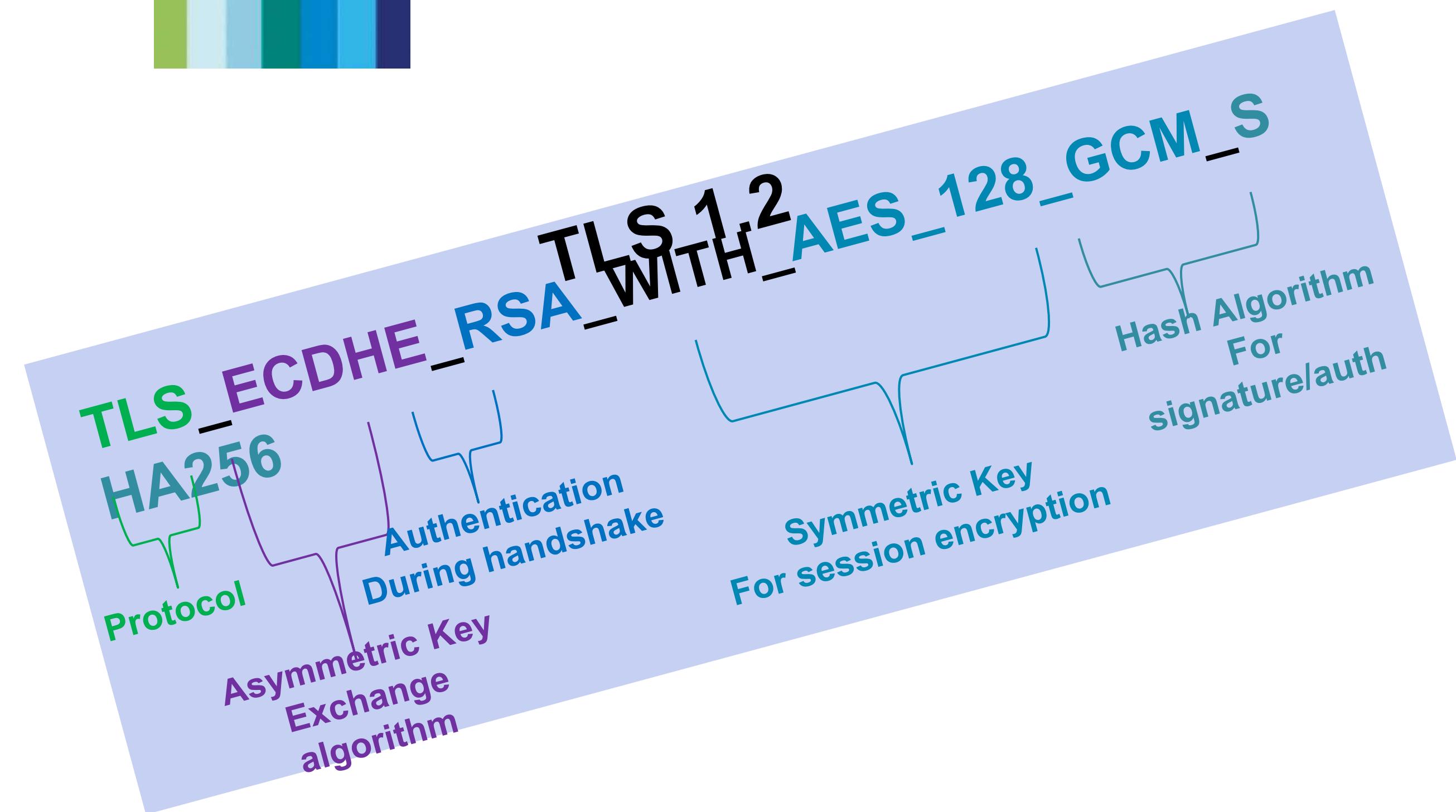
For more info: <https://visualitynq.com>
info@visualitynq.com

jNQ



Fully scalable, robust, continually updated Pure Java SMB library

Configuration



Get a certificate

Watch Ned Pyle's video on this subject:

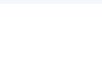
[SMB over QUIC certificate issuance - YouTube](#)

Images by Didier Van Hoye

Configure Cert Template

Certsrv - [Certification Authority (Local)\EntRootCA-DWT]

File Action View Help

← → |     | ?

Certification Authority (Local) > EntRootCA-DWT

- Name
- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests
- Certificate Templates

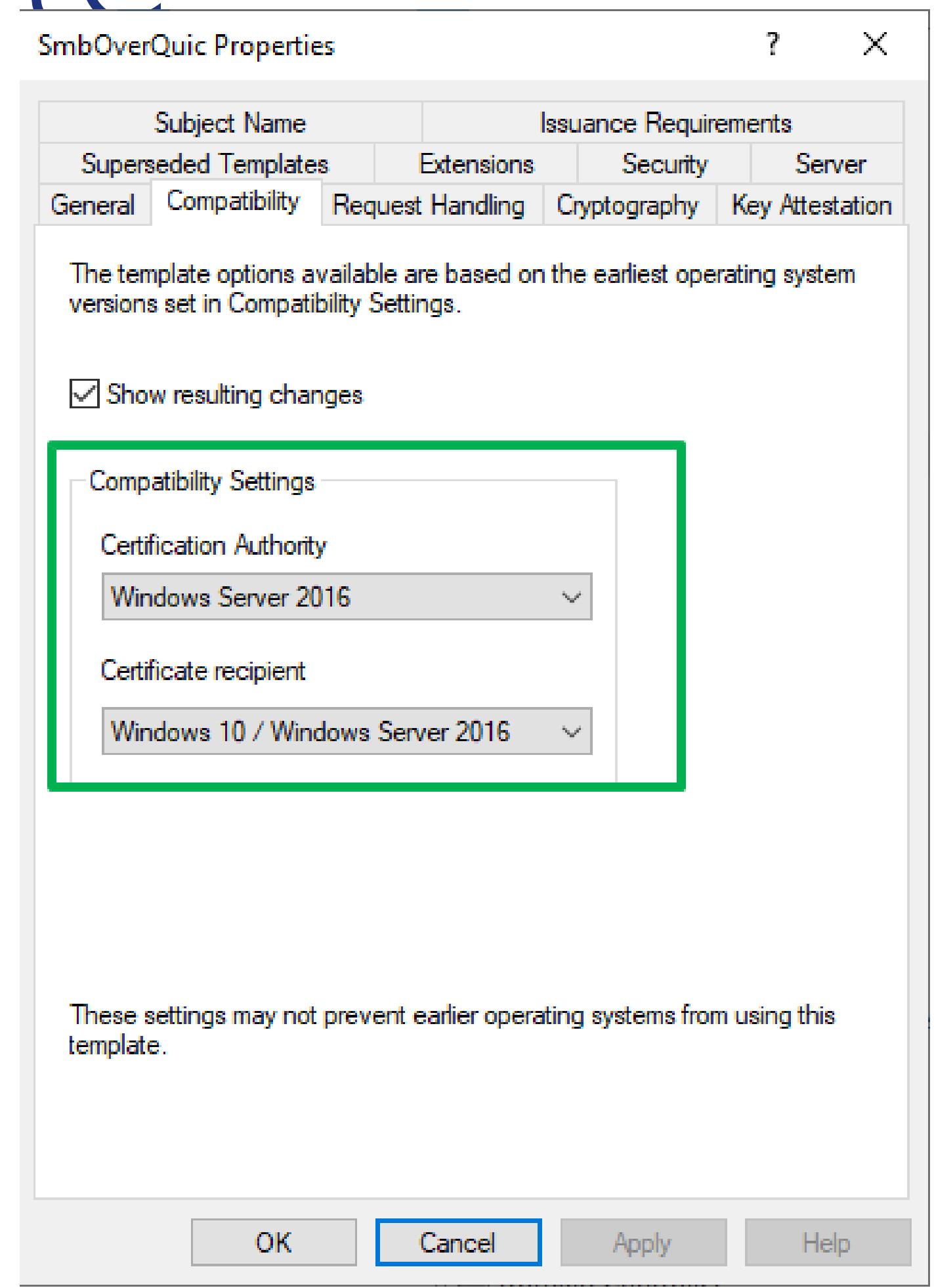
Certificate Templates Console

File Action View Help

← → |     | ?

Certificate Templates (DC01.dat)

Template Display Name	Schema Version	Version	Int	Actions
Duplicate Template	4.1			Certificat
All Tasks	3.1			More
Properties	3.1	106.0	Pr	Compute
Help	4.1			More
	3.1			
	5.1			
Computer Certificate Windows Server 20...	4	100.8	Cli	



Configure Cert Template

Properties of New Template

Subject Name	Server	Issuance Requirements	
Superseded Templates	Extensions	Security	Server
Compatibility	General	Request Handling	Cryptography
Template display name:		SmbOverQuic	
Template name:		SmbOverQuic	
Validity period:		Renewal period:	3 years
		2 months	
<input checked="" type="checkbox"/> Publish certificate in Active Directory <input type="checkbox"/> Do not automatically reenroll if a duplicate certificate exists in Active Directory			

OK Cancel Apply Help

SmbOverQuic Properties

Subject Name	Issuance Requirements			
Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation
Purpose: Signature				
<input type="checkbox"/> Delete revoked or expired certificates (do not archive) <input type="checkbox"/> Include symmetric algorithms allowed by the subject <input type="checkbox"/> Archive subject's encryption private key <input type="checkbox"/> Use advanced Symmetric algorithm to send the key to the CA <input type="checkbox"/> Authorize additional service accounts to access the private key Key Permissions...				
<input type="checkbox"/> Allow private key to be exported <input type="checkbox"/> Renew with the same key <input type="checkbox"/> For automatic renewal of smart card certificates, use the existing key if a new key cannot be created				
Do the following when the subject is enrolled and when the private key associated with this certificate is used: <input checked="" type="radio"/> Enroll subject without requiring any user input <input type="radio"/> Prompt the user during enrollment <input type="radio"/> Prompt the user during enrollment and require user input when the private key is used				

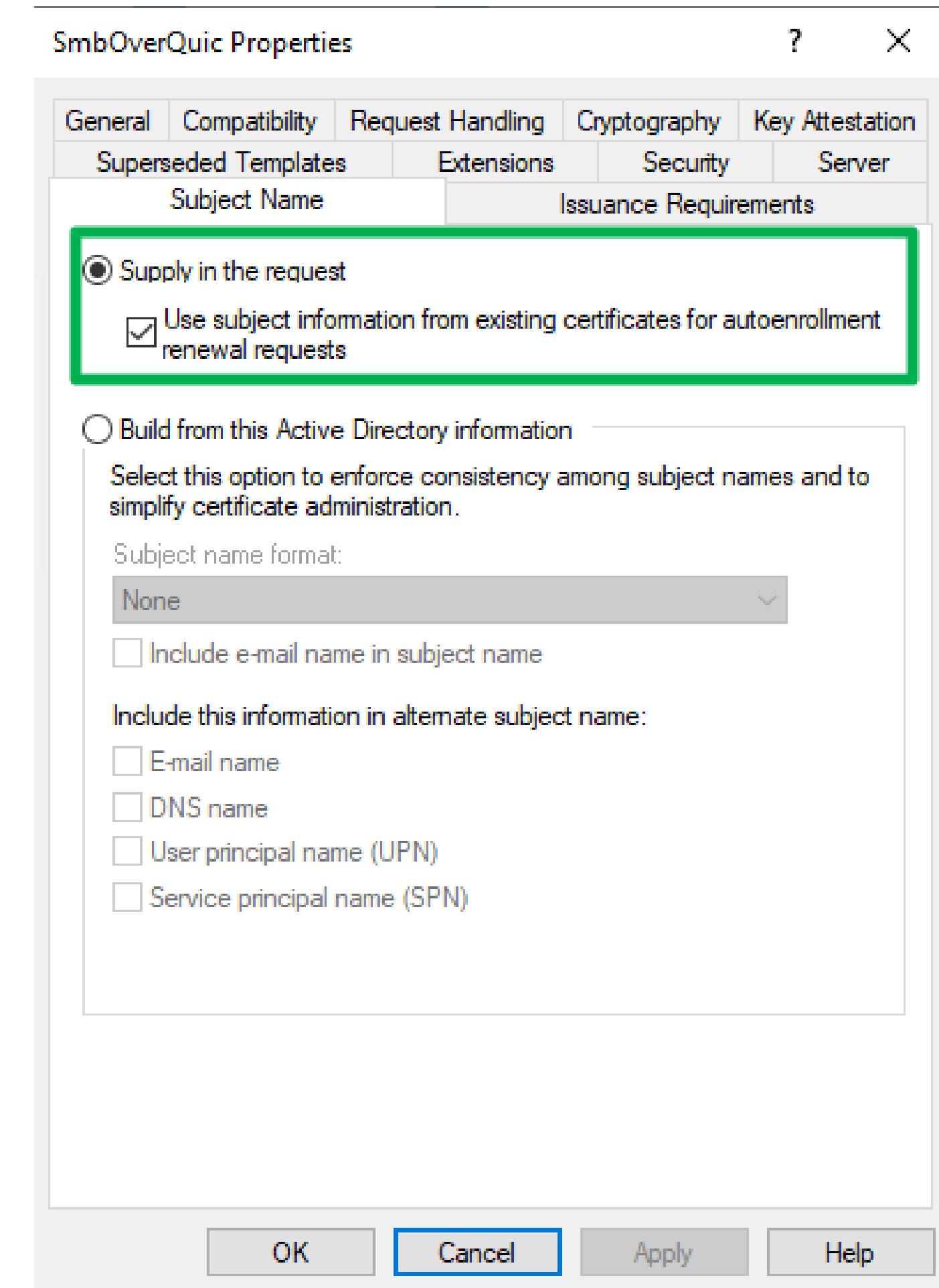
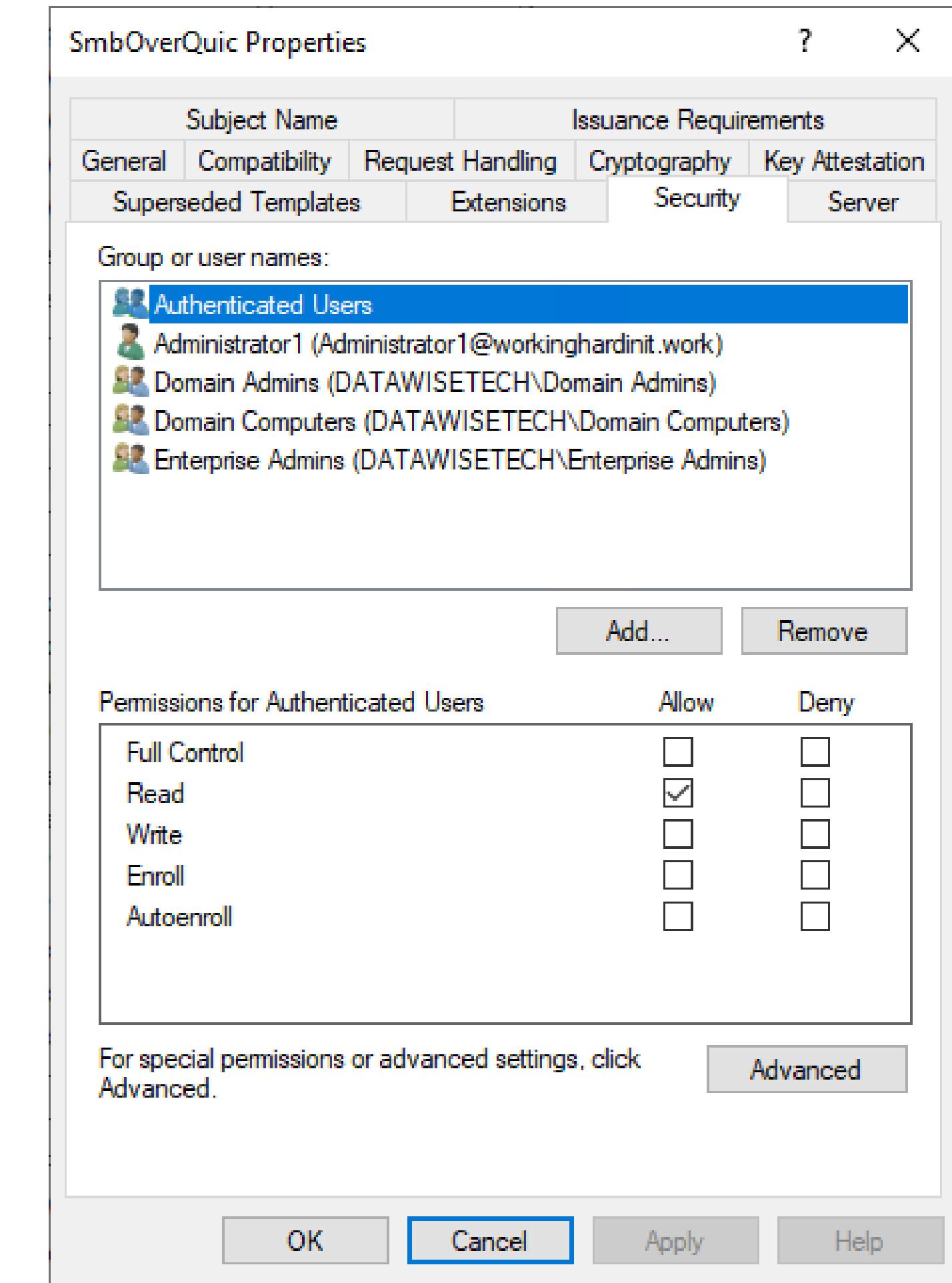
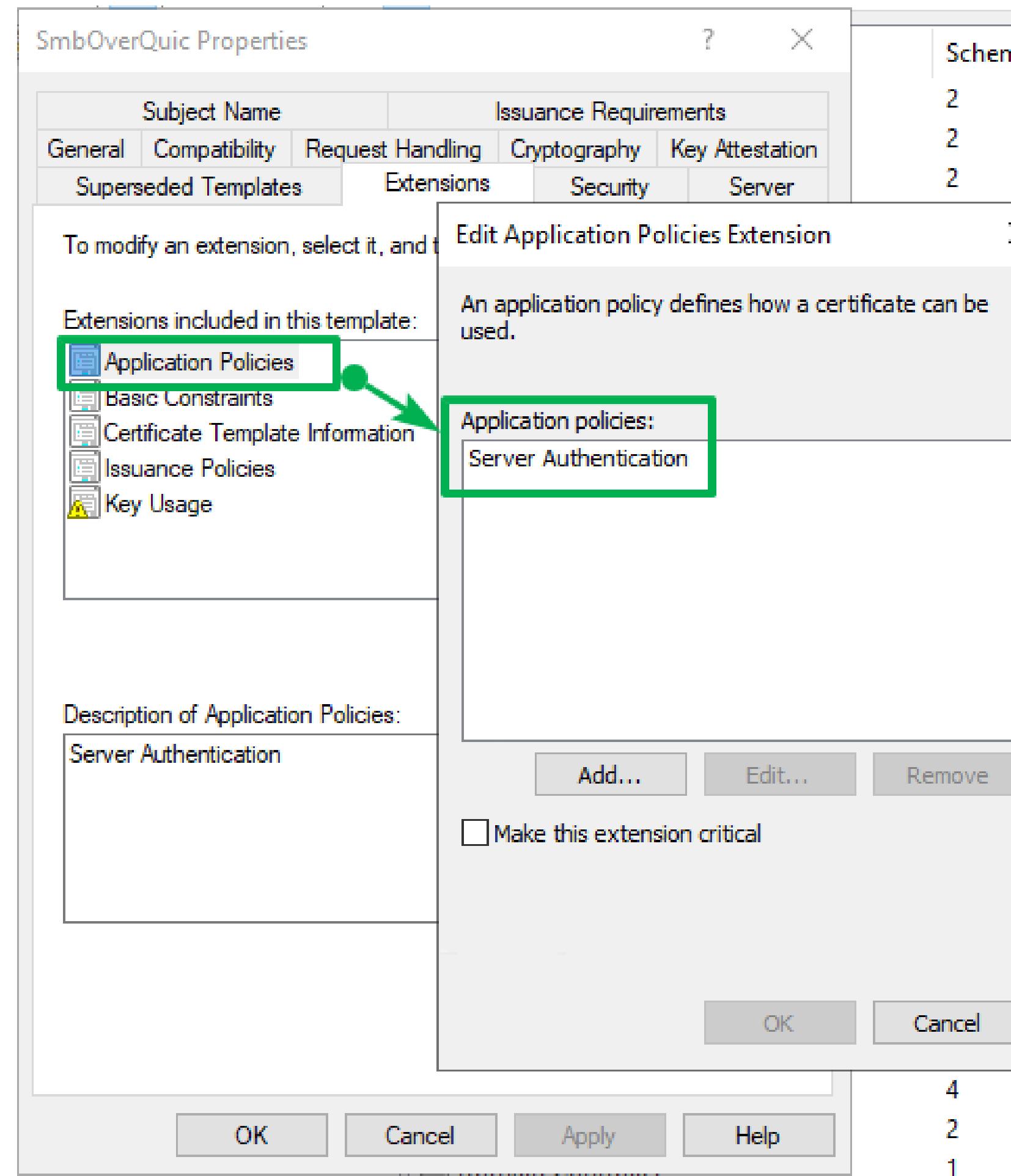
OK Cancel Apply Help

SmbOverQuic Properties

Subject Name	Issuance Requirements			
Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation
Provider Category: Key Storage Provider				
Algorithm name: ECDSA_P256 Minimum key size: 256				
Choose which cryptographic providers can be used for requests <input checked="" type="radio"/> Requests can use any provider available on the subject's computer <input type="radio"/> Requests must use one of the following providers: Providers: <input type="checkbox"/> Microsoft Software Key Storage Provider <input type="checkbox"/> Microsoft Smart Card Key Storage Provider				
Request hash: SHA256 <input type="checkbox"/> Use alternate signature format				

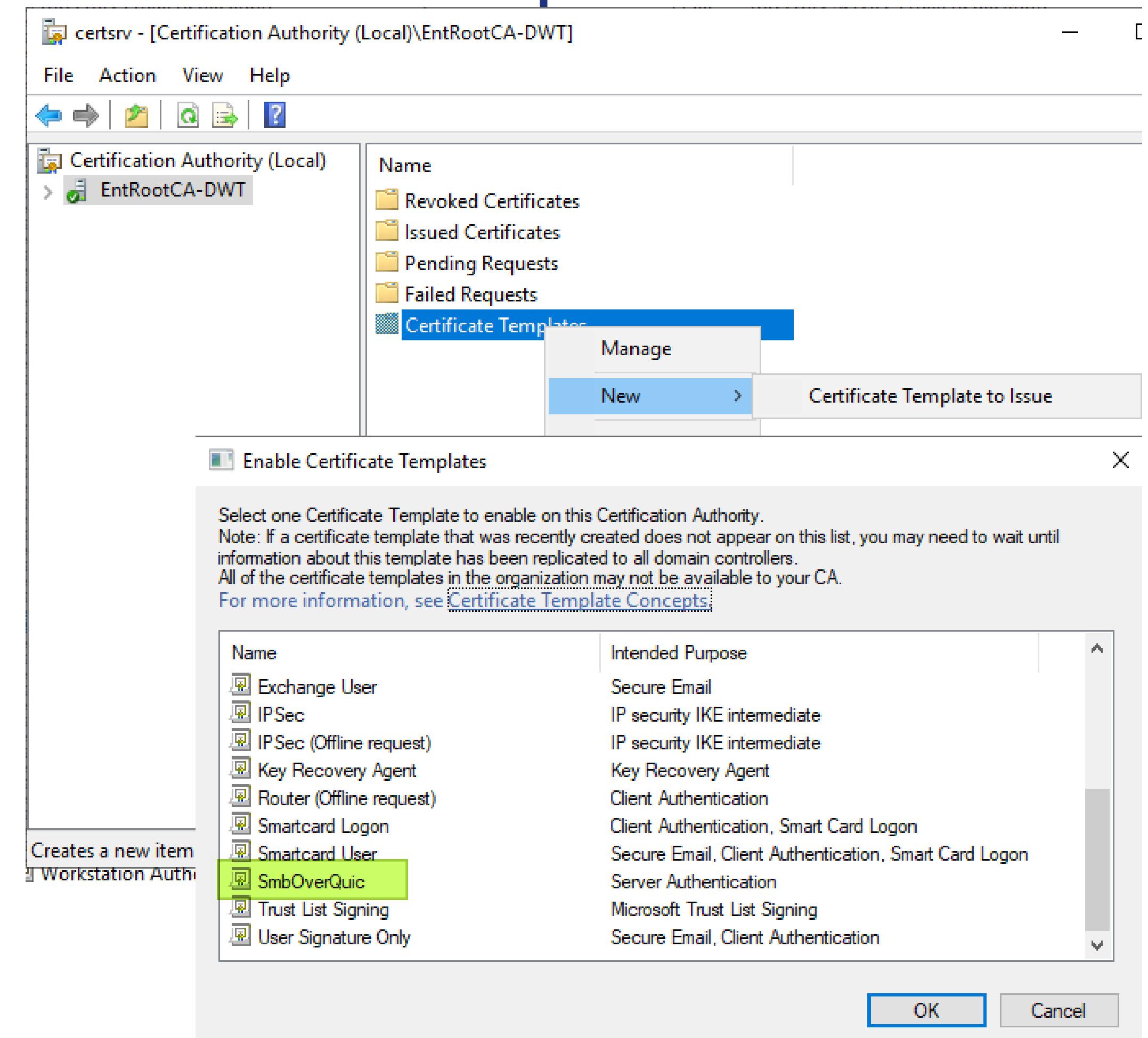
OK Cancel Apply Help

Configure Cert Template



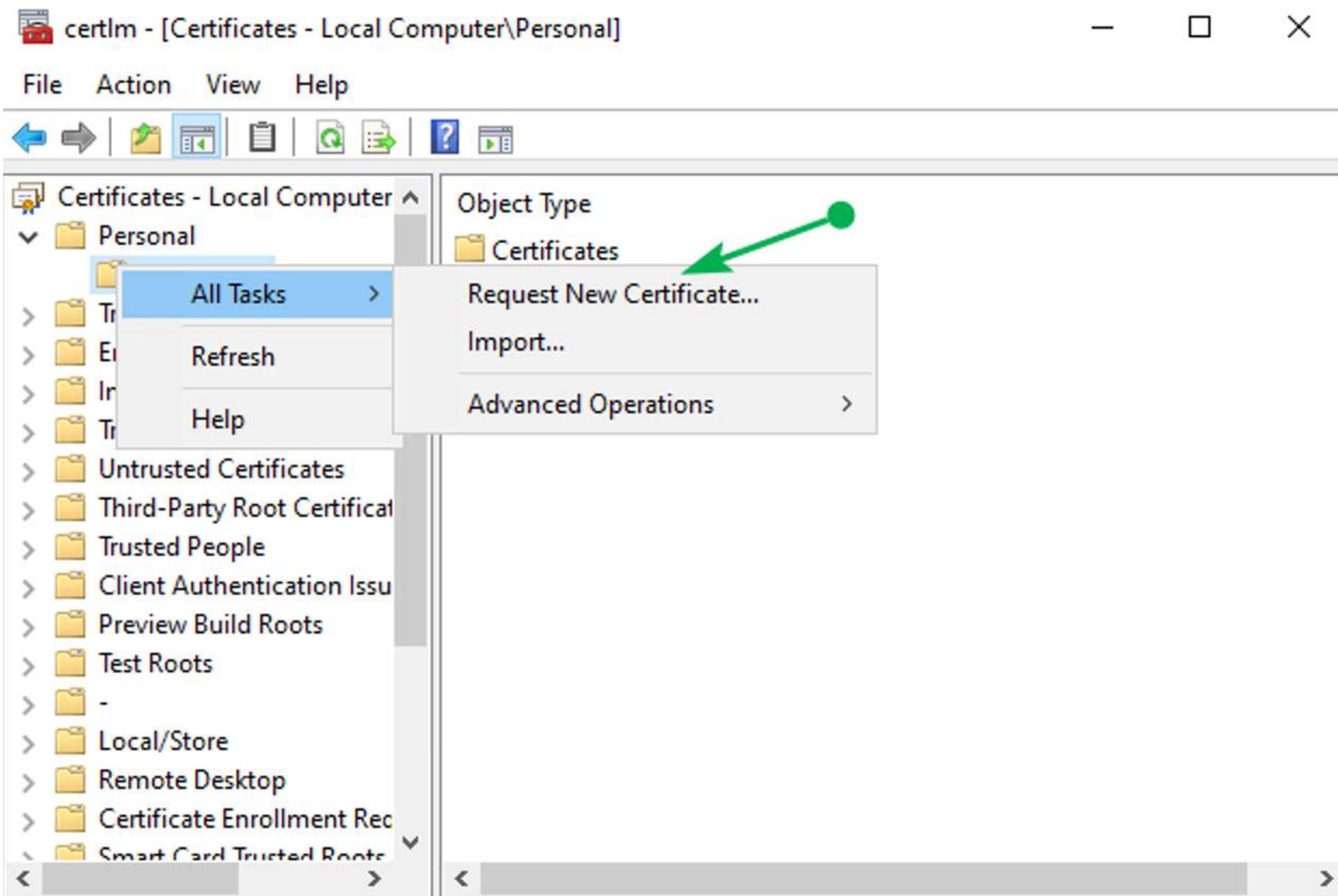


Enable Cert Template on CA





Requesting a certificate



Requesting a certificate

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates.
Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy



Configured by you

Add New

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

Computer

 STATUS: Available

Details ▾

Computer Certificate Windows Server
2016/Windows10

 STATUS: Available

Details ▾

SmbOverQuic

 STATUS: Available

Details ▾

Workstation Authentication

 STATUS: Available

Details ▾

Next

Cancel

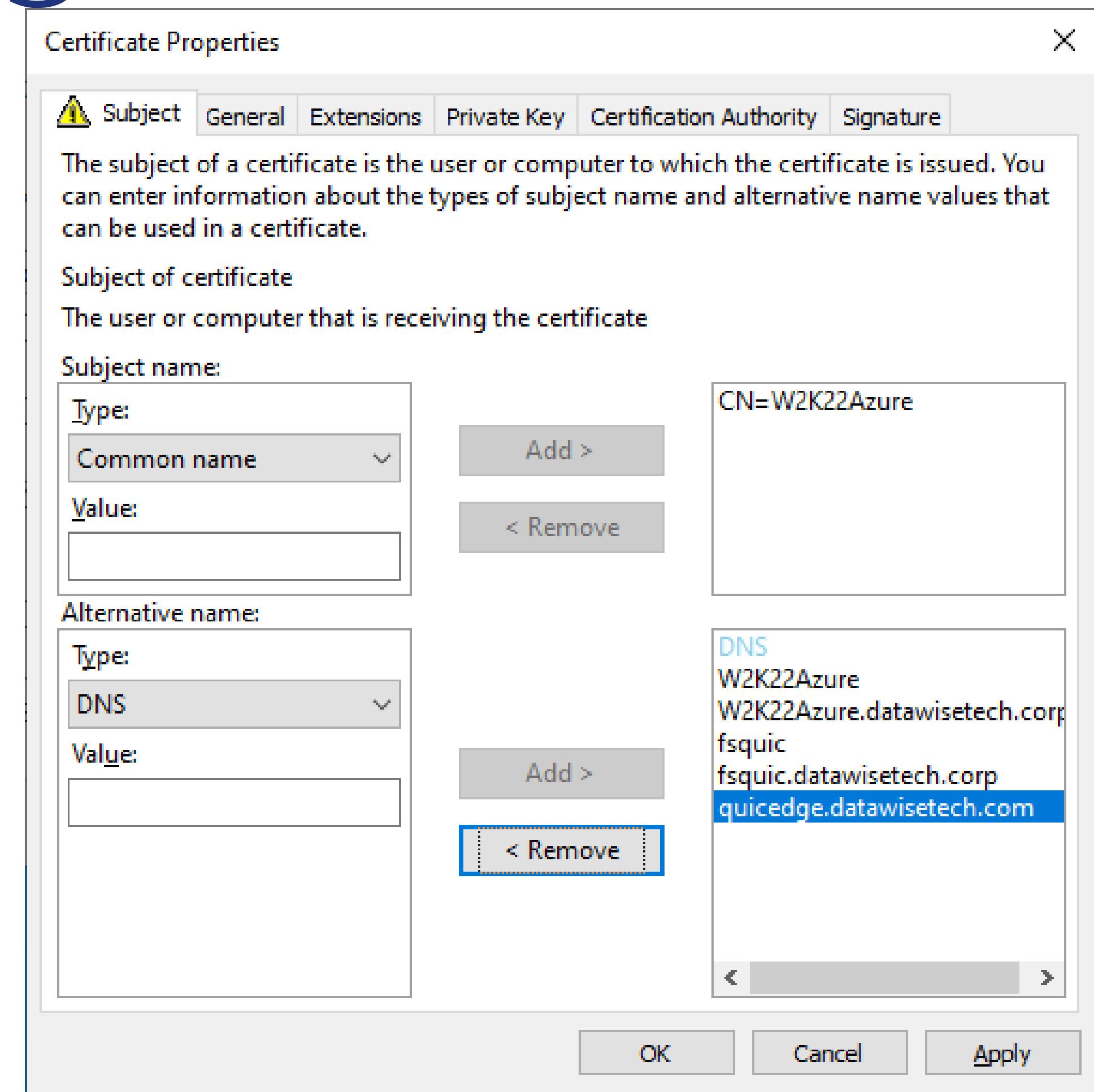
Show all templates

Enroll

Cancel



Requesting a certificate





Requesting a certificate

— □ ×

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy		
<input type="checkbox"/> Computer	 ⓘ STATUS: Available	Details ▾
<input type="checkbox"/> Computer Certificate Windows Server 2016/Windows10	 ⓘ STATUS: Available	Details ▾
<input checked="" type="checkbox"/> SmbOverQuic	 ⓘ STATUS: Available	Details ▾
<input type="checkbox"/> Workstation Authentication	 ⓘ STATUS: Available	Details ▾

Show all templates

Enroll Cancel

— □ ×

Certificate Enrollment

Certificate Installation Results

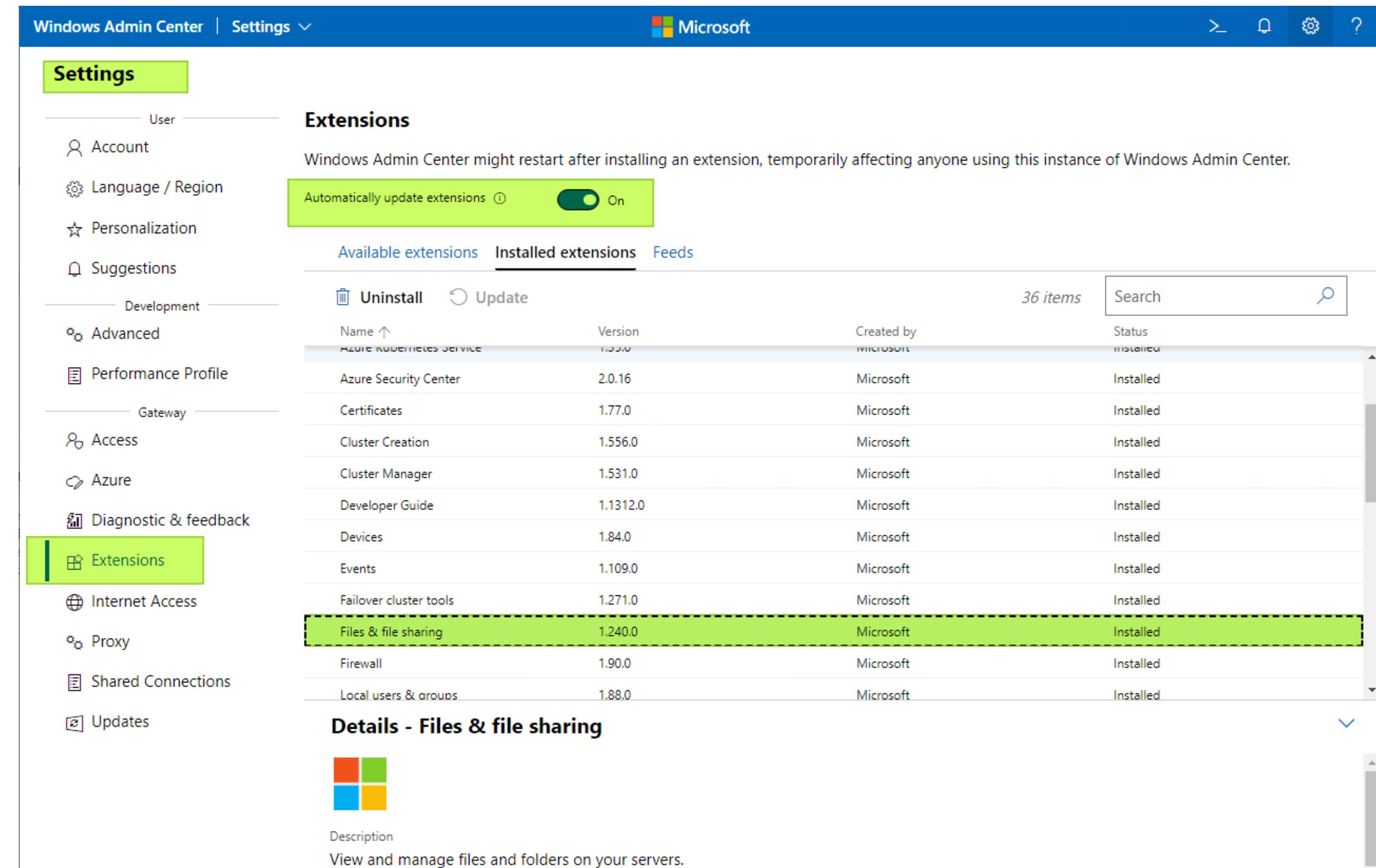
The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy		
<input checked="" type="checkbox"/> SmbOverQuic	 ✓ STATUS: Succeeded	Details ▾

Finish



Windows Admin Center (1/5)



The screenshot shows the Windows Admin Center Settings page. The left sidebar has a 'Settings' tab selected, with 'Extensions' highlighted. The main content area is titled 'Extensions' and contains a note about potential restarts after installation. A toggle switch for 'Automatically update extensions' is set to 'On'. Below this are three tabs: 'Available extensions', 'Installed extensions' (which is selected), and 'Feeds'. A table lists 36 installed items, including Azure Kubernetes Service, Azure Security Center, Certificates, Cluster Creation, Cluster Manager, Developer Guide, Devices, Events, Failover cluster tools, Files & file sharing (which is highlighted with a dashed green border), Firewall, and Local users & groups. The 'Files & file sharing' row shows version 1.240.0, created by Microsoft, and a status of 'Installed'. At the bottom, a 'Details - Files & file sharing' section provides a description: 'View and manage files and folders on your servers.'

Name	Version	Created by	Status
Azure Kubernetes Service	1.55.0	Microsoft	Installed
Azure Security Center	2.0.16	Microsoft	Installed
Certificates	1.77.0	Microsoft	Installed
Cluster Creation	1.556.0	Microsoft	Installed
Cluster Manager	1.531.0	Microsoft	Installed
Developer Guide	1.1312.0	Microsoft	Installed
Devices	1.84.0	Microsoft	Installed
Events	1.109.0	Microsoft	Installed
Failover cluster tools	1.271.0	Microsoft	Installed
Files & file sharing	1.240.0	Microsoft	Installed
Firewall	1.90.0	Microsoft	Installed
Local users & groups	1.88.0	Microsoft	Installed

Windows Admin Center (2/5)

Tools

- Search Tools
- Overview
- Azure hybrid center
- Azure Kubernetes Service
- Azure Backup
- Azure File Sync
- Azure Monitor
- Azure Security Center
- Certificates
- Devices
- Events
- Files & file sharing
- Firewall
- Installed apps
- Local users & groups
- Networks
- Performance Monitor
- Settings

Settings

General

File shares (SMB server)

These settings affect all file shares on this server that use the SMB protocol, overruling settings on individual shares.

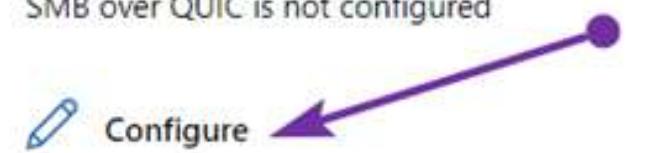
General settings

- SMB 1 isn't installed
- SMB 1 removal
 - Don't audit SMB 1 connections
 - Audit SMB 1 connections
- SMB signing
 - Not required
 - Required
- SMB 3 encryption
 - Not required
 - Required from clients that support it
 - Required from all clients (others are rejected)

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 not configured



Configure

Save **Discard changes**



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]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Addresses that SMB over QUIC clients can connect to * ⓘ Select All

W2K22Azure.datawisetech.corp
 W2K22Azure
 fsquic.datawisetech.corp
 fsquic
 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](#)

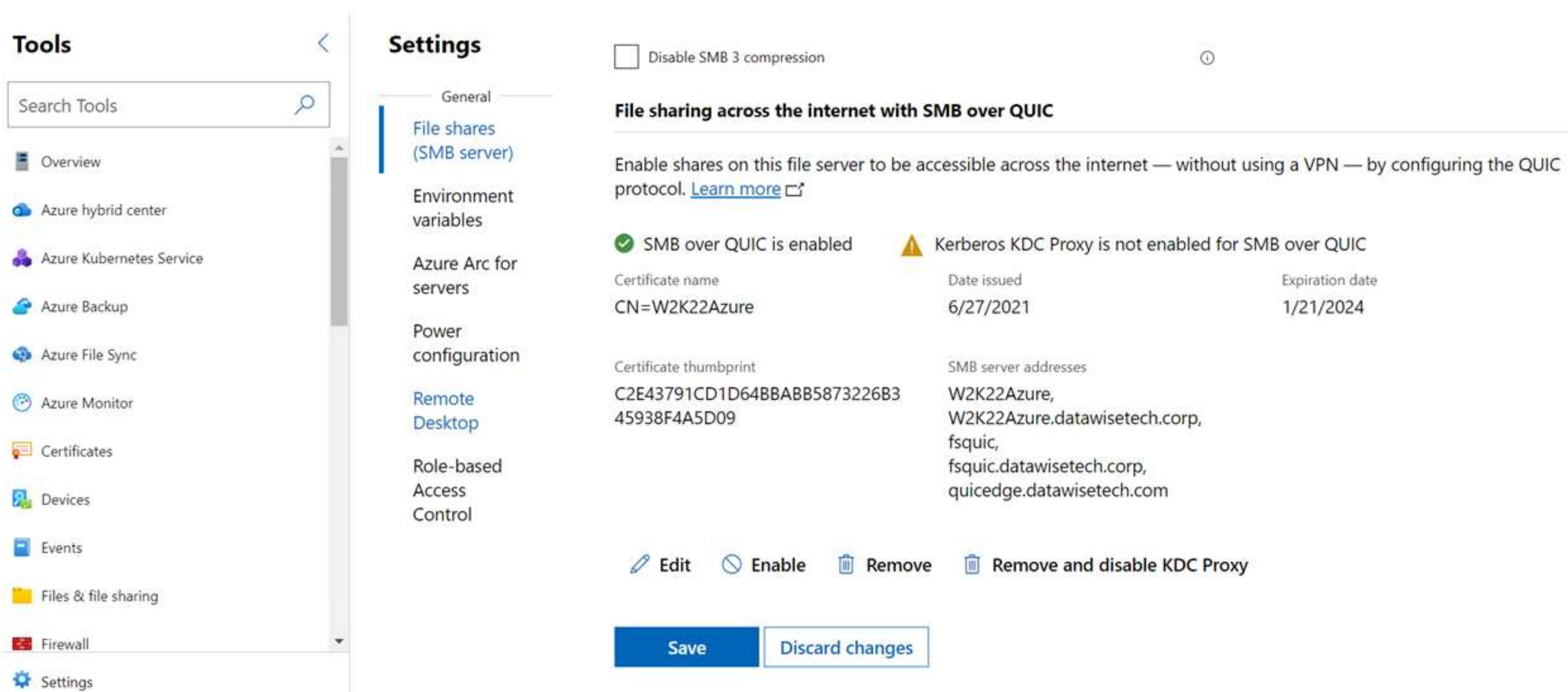
SMB encryption (in addition to QUIC encryption) ⓘ

- Disabled (Recommended)
 Enabled

Access to named pipes ⓘ

- Disabled (Recommended)
 Enabled

Windows Admin Center (4/5)



The screenshot shows the Windows Admin Center interface with the title "Tools" in the top left. The main content area is titled "Settings" under "File shares (SMB server)". A sub-section titled "File sharing across the internet with SMB over QUIC" is displayed. It includes a checkbox for "Disable SMB 3 compression" and a note about enabling shares across the internet using the QUIC protocol. A status message indicates "SMB over QUIC is enabled" with a green checkmark. A warning message states "Kerberos KDC Proxy is not enabled for SMB over QUIC". Below this, certificate details are shown: "CN=W2K22Azure", "Date issued: 6/27/2021", and "Expiration date: 1/21/2024". The "Certificate thumbprint" is listed as "C2E43791CD1D64BBABB5873226B3 45938F4A5D09". The "SMB server addresses" listed are "W2K22Azure", "W2K22Azure.datawisetech.corp", "fsquic", "fsquic.datawisetech.corp", and "quicedge.datawisetech.com". At the bottom, there are buttons for "Edit", "Enable", "Remove", and "Remove and disable KDC Proxy". A "Save" button is highlighted in blue, and a "Discard changes" button is also present.

Tools

Search Tools

Overview

Azure hybrid center

Azure Kubernetes Service

Azure Backup

Azure File Sync

Azure Monitor

Certificates

Devices

Events

Files & file sharing

Firewall

Settings

General

File shares (SMB server)

Environment variables

Azure Arc for servers

Power configuration

Remote Desktop

Role-based Access Control

Disable SMB 3 compression

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 not enabled for SMB over QUIC

Certificate name: CN=W2K22Azure

Date issued: 6/27/2021

Expiration date: 1/21/2024

Certificate thumbprint: C2E43791CD1D64BBABB5873226B3 45938F4A5D09

SMB server addresses: W2K22Azure, W2K22Azure.datawisetech.corp, fsquic, fsquic.datawisetech.corp, quicedge.datawisetech.com

Edit Enable Remove Remove and disable KDC Proxy

Save Discard changes



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

Certificate name

CN=W2K22Azure

 Kerberos KDC Proxy is enabled for SMB over QUIC

Date issued

6/27/2021

Expiration date

1/21/2024

Certificate thumbprint

C2E43791CD1D64BBABB587322

6B345938F4A5D09

SMB server addresses

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>"](#)

```
PS C:\WINDOWS\system32> Get-SmbClientConfiguration

AuditInsecureGuestLogon          : False
AuditServerDoesNotSupportEncryption : False
AuditServerDoesNotSupportSigning  : False
BlockNTLM                         :
BlockNTLMServerExceptionList      :
CompressibilitySamplingSize       : 524288000
CompressibleThreshold             : 104857600
ConnectionCountPerRssNetworkInterface : 4
DirectoryCacheEntriesMax          : 16
DirectoryCacheEntrySizeMax        : 65536
DirectoryCacheLifetime            : 10
DisableCompression                 : False
DisabledSMBQUICServerExceptionList :
DormantFileLimit                  : 1023
EnableBandwidthThrottling         : True
EnableByteRangeLockingOnReadOnlyFiles : True
EnableCompressibilitySampling     : False
EnableInsecureGuestLogons          : False
EnableLargeMtu                      : True
EnableLoadBalanceScaleOut          : True
EnableMailslots                     : False
EnableMultiChannel                 : True
EnableSecuritySignature             : True
EnableSMBQUIC                       : True
EncryptionCiphers                  : AES_128_GCM, AES_128_CCM, AES_256_GCM, AES_256_CCM
ExtendedSessionTimeout              : 1000
FileInfoCacheEntriesMax            : 64
FileInfoCacheLifetime              : 10
FileNotFoundExceptionsMax           : 128
FileNotFoundCacheLifetime          : 5
ForceSMBEncryptionOverQuic         : False
InvalidAuthenticationCacheLifetime : 30
KeepConn                           : 600
MaxCmds                            : 50
MaximumConnectionCountPerServer    : 32
OlocksDisabled                      : False
RequestCompression                  : False
RequireEncryption                   : False
RequireSecuritySignature            : True
SessionTimeout                      : 60
SkipCertificateCheck                : False
Smb2DialectMax                     : None
Smb2DialectMin                     : None
UseOpportunisticLocking             : True
WindowSizeThreshold                 : 8
```



SMB Server Configuration

DisableSmbEncryptionOnSecureConnection

RestrictNamedPipeAccessViaQuic

EnableSMBQUIC

NEW: AuditClientCertificateAccess

```
PS C:\Users\administrator> 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                :
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                :
NullSessionPipes           :
NullSessionShares          :
OplockBreakWait            : 35
PendingClientTimeoutInSeconds : 120
RejectUnencryptedAccess    : True
RequestCompression          : False
RequireSecuritySignature   : False
RestrictNamedpipeAccessViaQuic : True
ServerHidden                :
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

Firewall: Rules: External SMB QUIC Access

	Protocol	Source	Port	Destination	Port
<input type="checkbox"/>	IPv4 TCP/UDP	VLAN3ONLAN net	*	192.168.2.23	443 (HTTPS)
<input type="checkbox"/>	IPv4 TCP/UDP	VLAN3ONLAN net	*	192.168.2.30	53 (DNS)
<input type="checkbox"/>	IPv4 TCP/UDP	VLAN3ONLAN net	*	192.168.2.9	53 (DNS)
<input type="checkbox"/>	IPv4 UDP	192.168.3.24	*	192.168.2.23	443 (HTTPS)
<input type="checkbox"/>	IPv4 *	*	*	192.168.2.44	*
<input type="checkbox"/>	IPv4 TCP/UDP	VLAN3ONLAN net	*	*	443 (HTTPS)

█ pass ✘ block
 ▶ pass (disabled) ✘ block (disabled)
 ✘ reject ⓘ log
 ✘ reject (disabled) ⓘ log (disabled)

ⓘ Active/Inactive Schedule (click to view/edit)
 ⓘ Alias (click to view/edit)

Windows Defender Firewall with Advanced Security

Inbound Rules

- Name: BLOCK TCP/445+139
- KDC Proxy Server service (KPS) for SMB over QUIC

File and Printer Sharing (SMB-QUIC-In) Properties

This is a predefined rule and some of its properties cannot be modified.

General

Name: File and Printer Sharing (SMB-QUIC-In)

Description: Inbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Winquic. (UDP 443)

Enabled:

Action:

Allow the connection

Allow the connection if it is secure

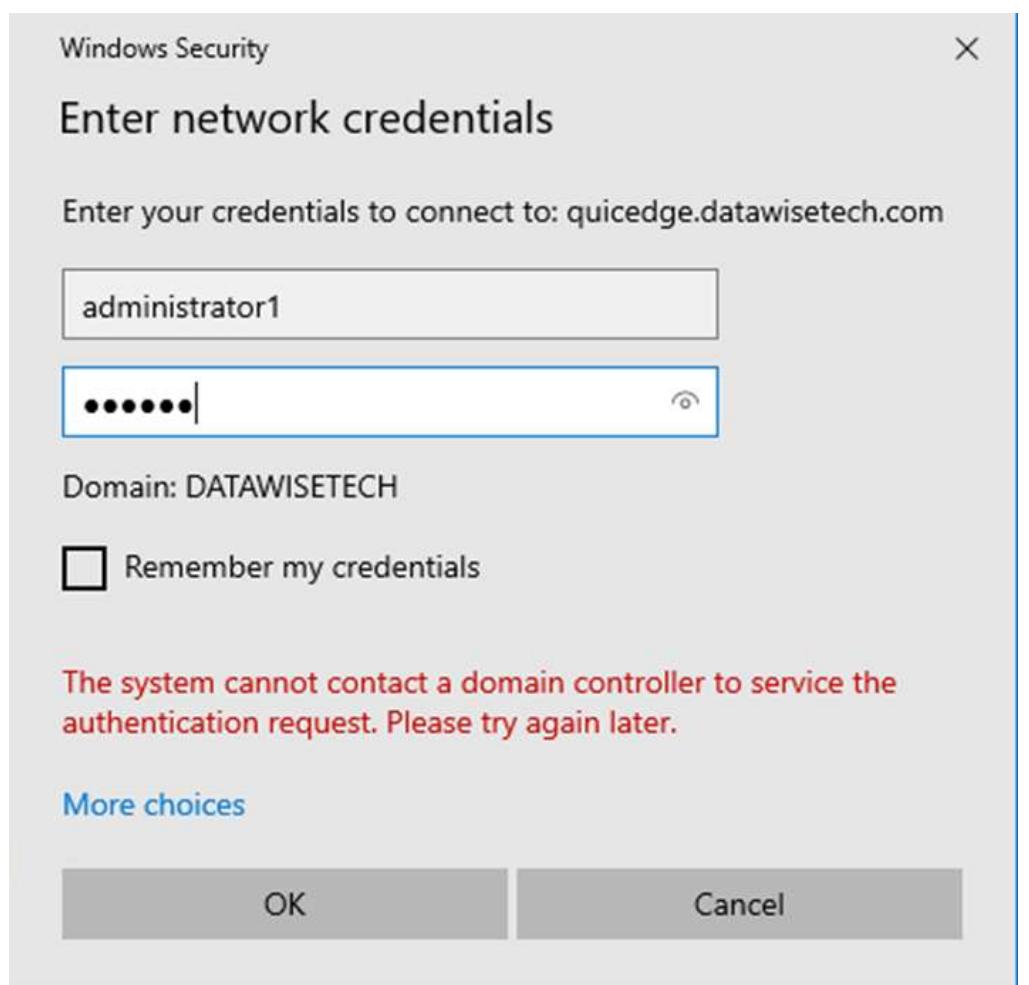
Block the connection

OK Cancel Apply

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

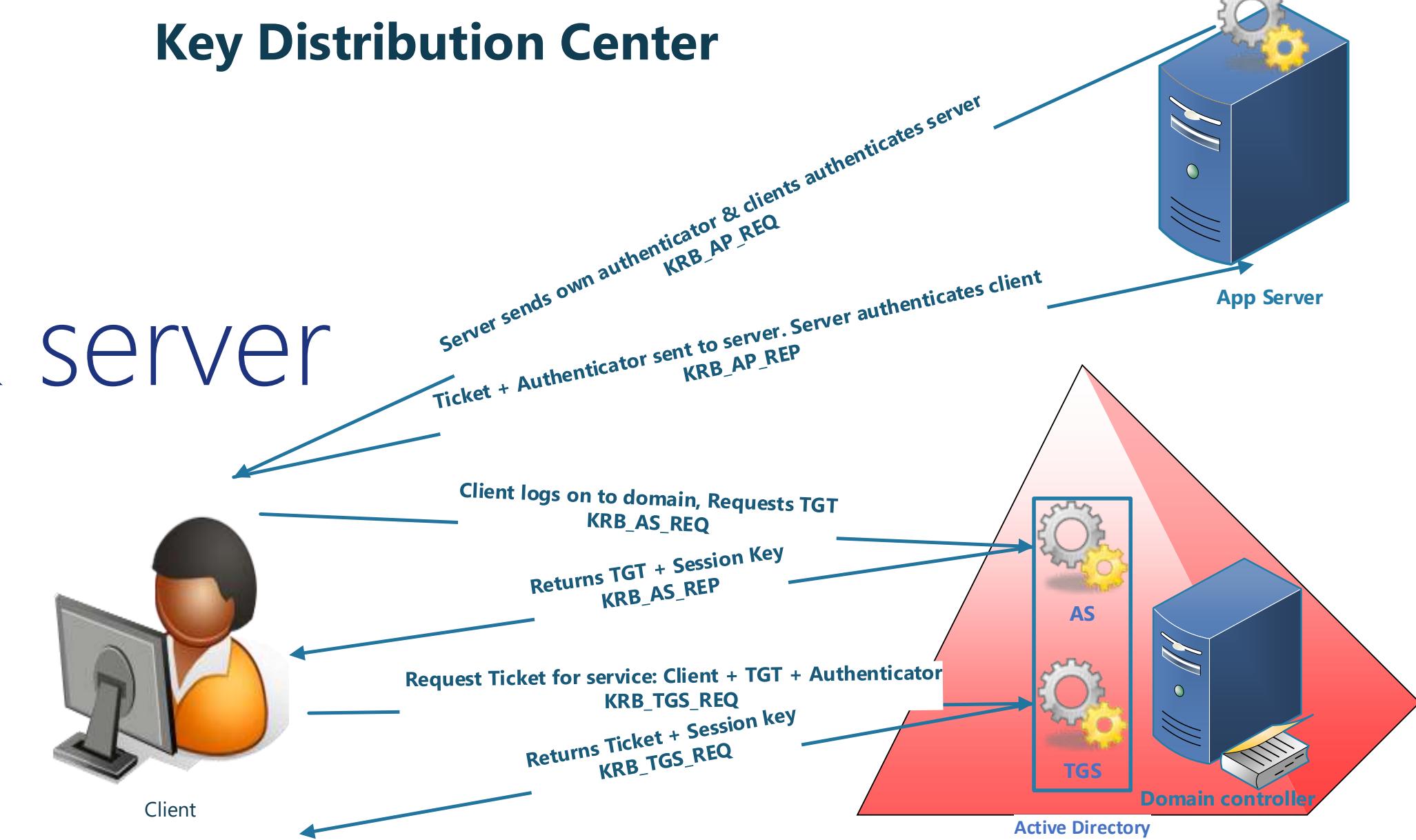
Provides 2 services

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

Used to mutually authenticate client & server

Images by Didier Van Hove

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





The KDC Proxy Service

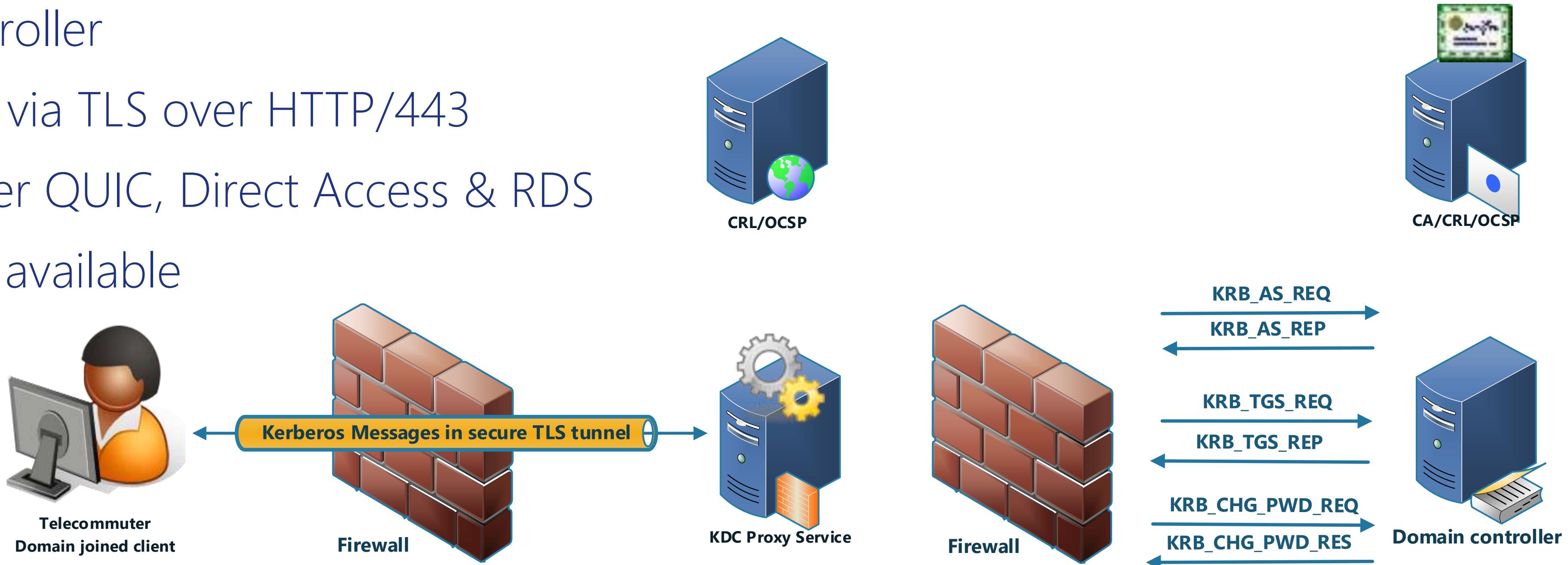
KDC Proxy Service

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=datawisetech...	sha256RSA
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Addresses that SMB over QUIC clients can connect to * ⓘ Select All

W2K22Azure.datawisetech.corp
 W2K22Azure
 fsquic.datawisetech.corp
 fsquic
 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

Certificate name

CN=W2K22Azure

 Kerberos KDC Proxy is enabled for SMB over QUIC

Date issued

6/27/2021

Expiration date

1/21/2024

Certificate thumbprint

C2E43791CD1D64BBABB587322

6B345938F4A5D09

SMB server addresses

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 Allow 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
```

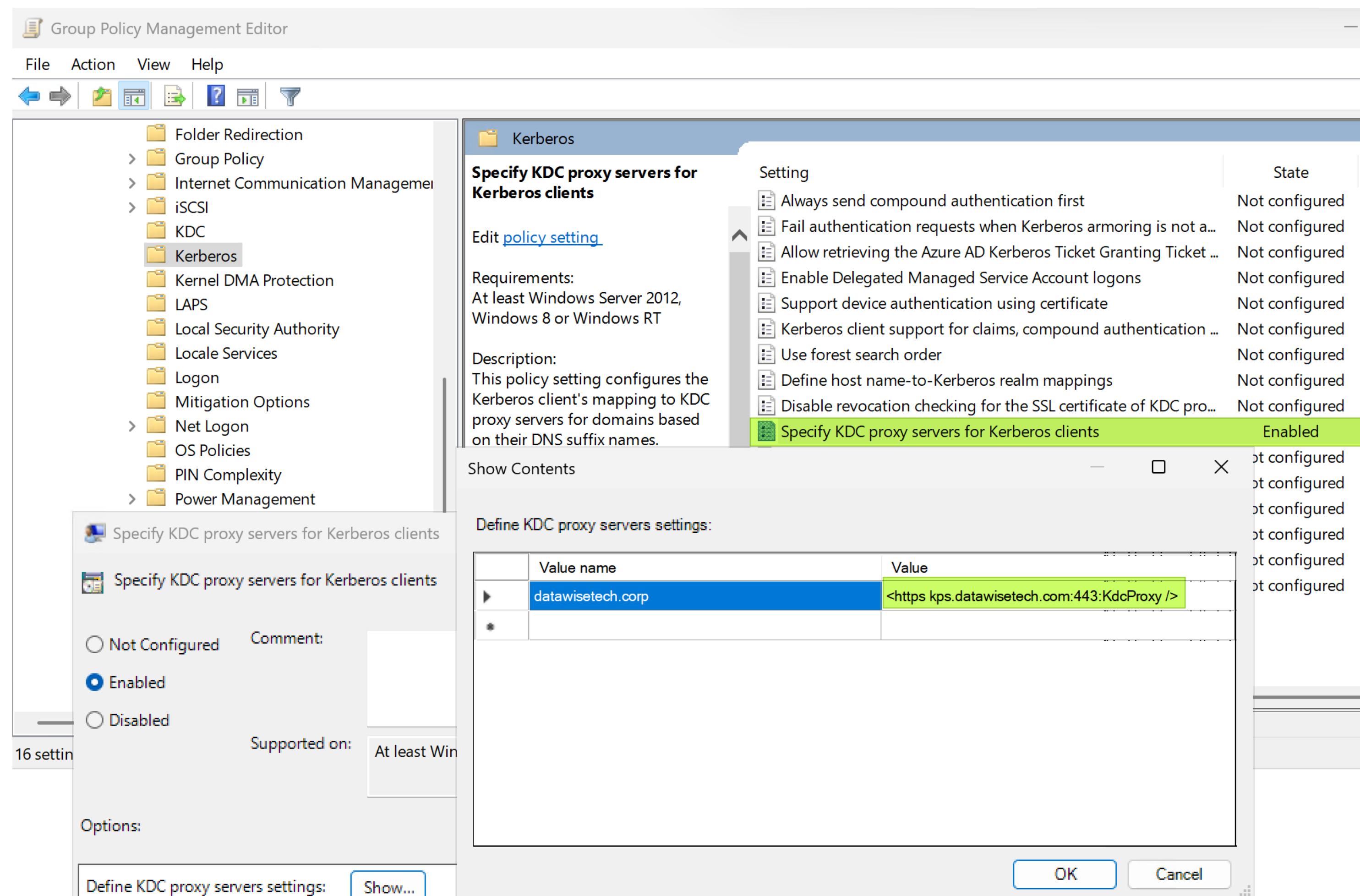
```
Set-Service -Name kpssvc -StartupType Automatic
```

```
#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

 Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters

Name	Type	Data
ab(Default)	REG_SZ	(value not set)
0110 KdcBackoffTime	REG_DWORD	0x00000003 (3)
0110 KdcSendRetries	REG_DWORD	0x00000002 (2)
0110 KdcWaitTime	REG_DWORD	0x00000003 (3)
0110 NoRevocationCheck	REG_DWORD	0x00000000 (0)
0110 RediscoverKdcTimeout	REG_DWORD	0x00000003 (3)

System
Audit
Kerberos
KdcProxy
ProxyServers
Parameters
UIPI
PowerEfficiencyDiagnostics

 Group Policy Management Editor

File Action View Help

Kerberos

Disable revocation checking for the SSL certificate of KDC proxy servers

[Edit policy setting](#)

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:
This policy setting allows you to

Setting:

- Always send compound authentication first
- Fail authentication requests when Kerberos armoring is used
- Support device authentication using certificate
- Kerberos client support for claims, compound authentication, and Kerberos delegation
- Use forest search order
- Define host name-to-Kerberos realm mappings
- Disable revocation checking for the SSL certificate of KDC proxy servers**
- Specify KDC proxy servers for Kerberos clients

Disable revocation checking for the SSL certificate of KDC proxy servers

Disable revocation checking for the SSL certificate of KDC proxy servers

Previous Setting Next Setting

Comment:

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Not Configured
 Enabled
 Disabled

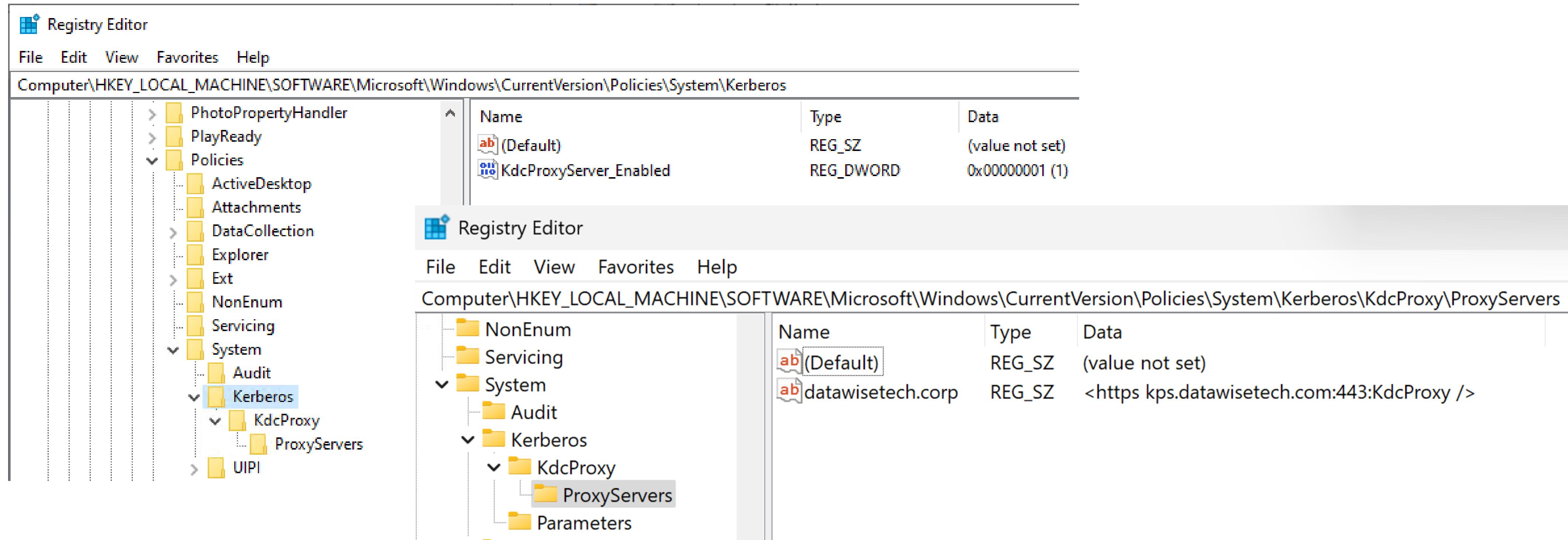
Options:

This policy setting allows you to disable revocation check for the SSL certificate of the targeted KDC proxy server.

If you enable this policy setting, revocation check for the SSL certificate of the KDC proxy server is ignored by the Kerberos client. This policy setting should only be used in troubleshooting KDC proxy connections.

Warning: When revocation check is ignored, the server represented by the certificate is not guaranteed valid.

Specify KDC Proxy Server for clients



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

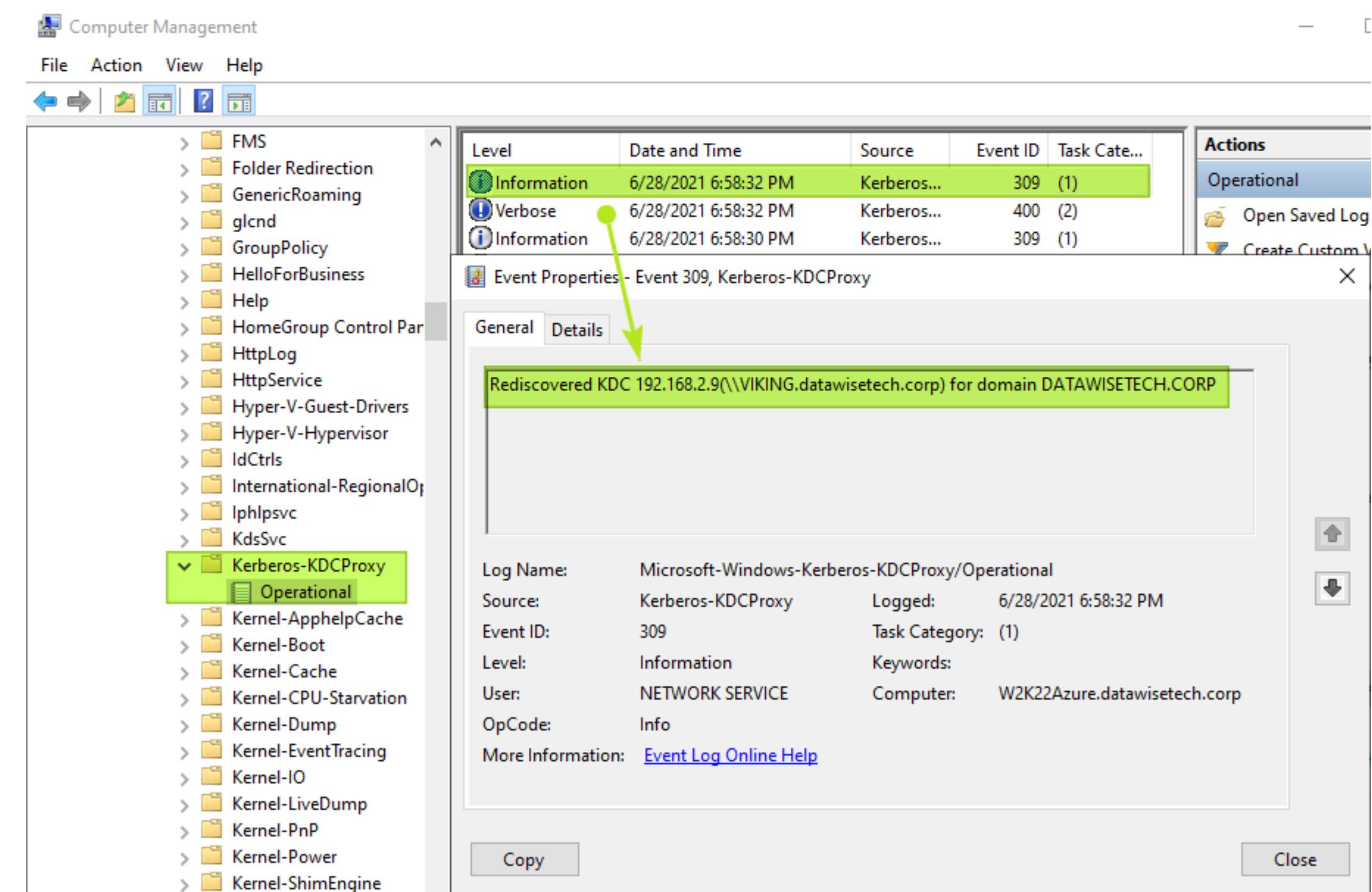
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\KdcProxy\ProxyServers]
 "datawisetech.corp"=<https kps.datawisetech.com:443:kdcproxy />"

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)

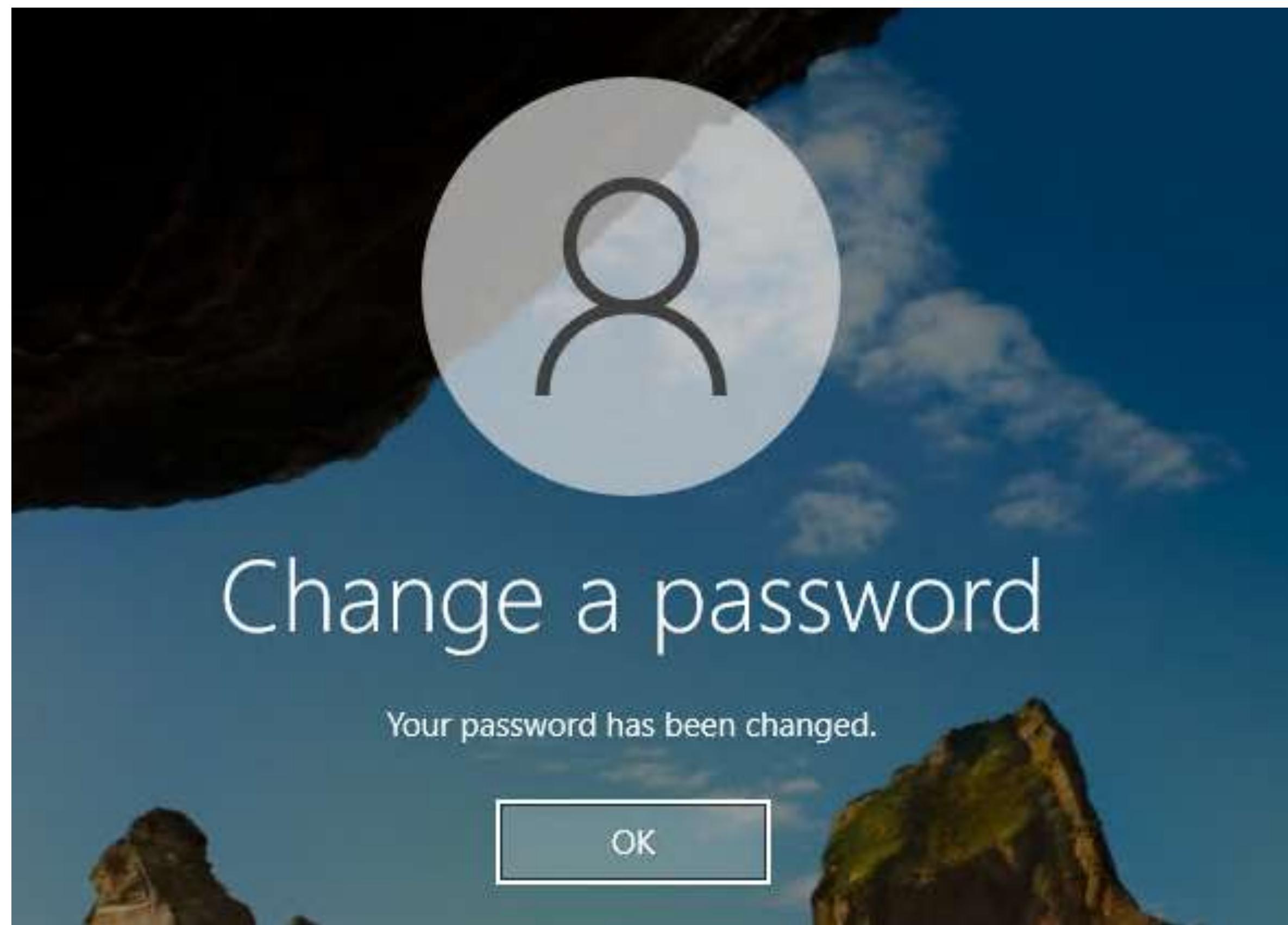
#0> Client: quicdemo @ DATAWISETECH.CORP
Server: krbtgt/DATAWISETECH.CORP @ DATAWISETECH.CORP
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 5/29/2025 13:12:11 (local)
End Time: 5/29/2025 23:12:11 (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 protocol.

SMB over QUIC is a foundational technology as on other operating systems via SMB3.

File Servers & file sharing are

Setting & configuration

KDC Proxy Service makes it even more secure.

Ongoing

Test Suite

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

client as well

hybrid or cloud.

Cloud Center

and LocalKDC drive it home make

sDC 2023

with my testing guide!

[Part I | StarWind Blog \(starwindsoftware.com\)](#)

[Part II | StarWind Blog \(starwindsoftware.com\)](#)



Thanks to our sponsors!

PLATINUM



GOLD



Questions & Answers