

# Encrypt Those Connections!: Setting Up SQL Server to Use Encrypted Connections

Sharon Reid

[sharon.reid.harris@gmail.com](mailto:sharon.reid.harris@gmail.com)

<https://github.com/InfoJunkie1/EncryptConnections>

St. Louis SQL Server and Power BI User Group

11 June 2024





# About Me

- High school and then college writing instructor
- Needed full-time job!
- Went through LaunchCode SQL cohort
- Hired at NISA!
- Asked to come back and TA and then be a lead mentor
- Passionate about database security

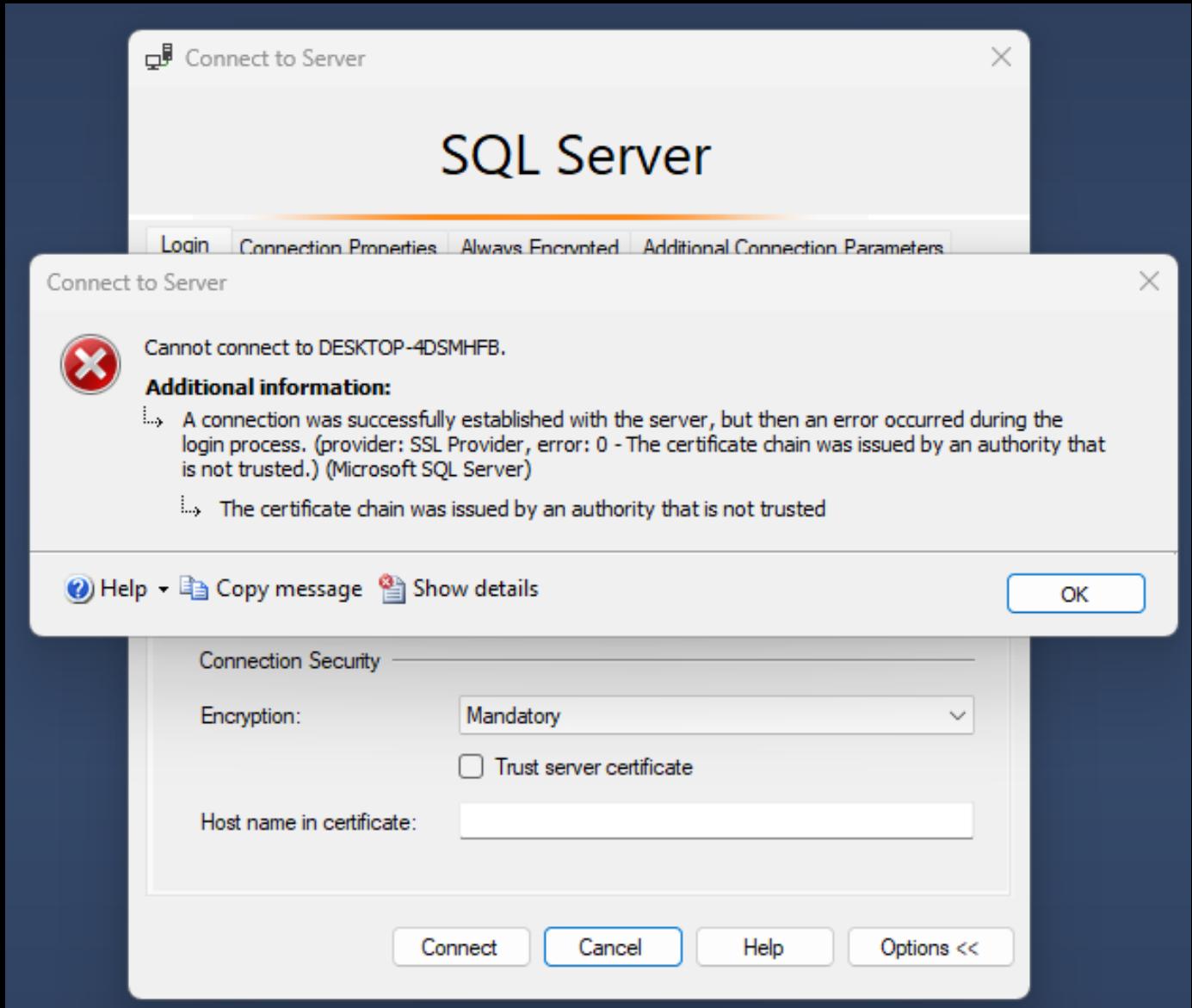
*(Everglades)*

# Expectations

- Not introductory, not in the weeds—passion to help others on the journey to improve database security
- Familiar with SQL Server but haven't yet set up environment to use encrypted connections
- Your friendly DBA is now after you to use encrypted connections, and you want to understand what you're doing

*(Yellowstone)*





Whaaaatttt?????

# Types of Encryption

- Data at Rest
- Data in Use
- Data in Transit

*Bryce Canyon*



## Data at Rest

- Where the database is stored
- TDE (Microsoft encryption option)
- Slight performance hit
- Storage layer partially addresses

*Yellowstone—The Narrows*

# Data in Use

- While data is actively used
- Always Encrypted (Microsoft encryption option)
- Can be by column
- Performance hit

*Yellowstone*





# Data in Transit

- Bytes of information go from one device or system to another
- Inherently vulnerable
- Seal the envelope
- Connection strings
- Slight performance hit—not noticeable
- Best practice!

*Zion—Allison Harris at Angel's Landing*

# SSL

- Secure Sockets Layer
- Used to encrypt data between SQL Server and the client application on the network
- Uses certificates to validate the server
- Used pre SQL Server 2016



*Valles Caldera National Preserve, New Mexico*

A scenic view of Bryce Canyon National Park. In the foreground, a woman wearing a white cap and sunglasses walks towards the camera. Behind her, a trail leads through a valley filled with numerous tall, thin rock formations called hoodoos, colored in shades of orange, red, and brown. The sky is clear and blue.

# TLS

- SSL>TLS
- Newer version of SSL with increased security
- TLS/SSL handshake
- [Microsoft link re authentication](#)

*Bryce Canyon*

A photograph of a woman with long red hair, wearing a dark cap and a black long-sleeved shirt, sitting on a large, light-colored rock. She is looking towards the camera. The background is the vast, layered landscape of the Grand Canyon under a blue sky with some clouds.

# Can we use encrypted connections?

- No—environment not set up
- Sometimes—allows for use of encrypted connections
  - SQL Server security certs required
  - Connection strings updated
- Yes—forces use of encrypted connections
  - Goal!

*Allison Harris at Grand Canyon*

# Create a security cert

- Self-signed
  - Encrypts connection but still must check Trust Server
  - Not signed by a trusted authority
- Company's own cert authority
  - Active Directory domain
- 3<sup>rd</sup> party Certificate Authority such as DigiCert

*(Bryce Canyon)*



A wide-angle aerial photograph of Horseshoe Bend, a famous geological feature in the Colorado River. The river forms a sharp, sweeping bend that resembles a horseshoe. The surrounding terrain is composed of layered red and orange sandstone cliffs. The water of the river is a deep blue-green color. The sky above is dark, creating a strong contrast with the bright, textured rock surfaces.

# Steps to create a security cert

- Create the cert
- Grant SQL Server rights to read private key
- Configure SQL Server to use this cert

- *(Horseshoe Bend)*

# Creating self-signed cert in PowerShell

- Use DBATools!

```
Administrator: C:\Program Files\WindowsApps\Microsoft.PowerShell_7.4.2.0_x64_8wekyb3d8bbwe\pwsh.exe
PowerShell 7.4.2
PS C:\Windows\System32> New-DBACertificate -SelfSigned

FriendlyName : SQL Server
DnsNameList  : {DESKTOP-4DSMHFB.WORKGROUP, DESKTOP-4DSMHFB}
Thumbprint    : A7975A6819AE93B0BA06DE32E4B1ACA3E479CC59
NotBefore    : 6/5/2024 9:50:13 PM
NotAfter     : 6/5/2025 10:10:13 PM
Subject       : CN=DESKTOP-4DSMHFB.WORKGROUP
Issuer        : CN=DESKTOP-4DSMHFB.WORKGROUP

PS C:\Windows\System32>
```

# Grant SQL Server rights to read private key

- Super important step!
- SQL Server service can't start otherwise
- MMC>Personal>Certificates
- Certificate>rt click>All Tasks>Manage Private Keys
- Confirm in Configuration Manager the service account for your instance

The image shows two screenshots of Windows management consoles.

The top screenshot is titled "Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]". It displays a list of certificates under "Issued To" (localhost) and "Issued By" (DESKTOP-4DSMHFB.WORKGROUP). A context menu is open over the first certificate, listing options: All Tasks, Open, Cut, Copy, Delete, Properties, Request Certificate with New Key..., Renew Certificate with New Key..., Manage Private Keys..., Advanced Operations, and Export... The "Open" option is highlighted.

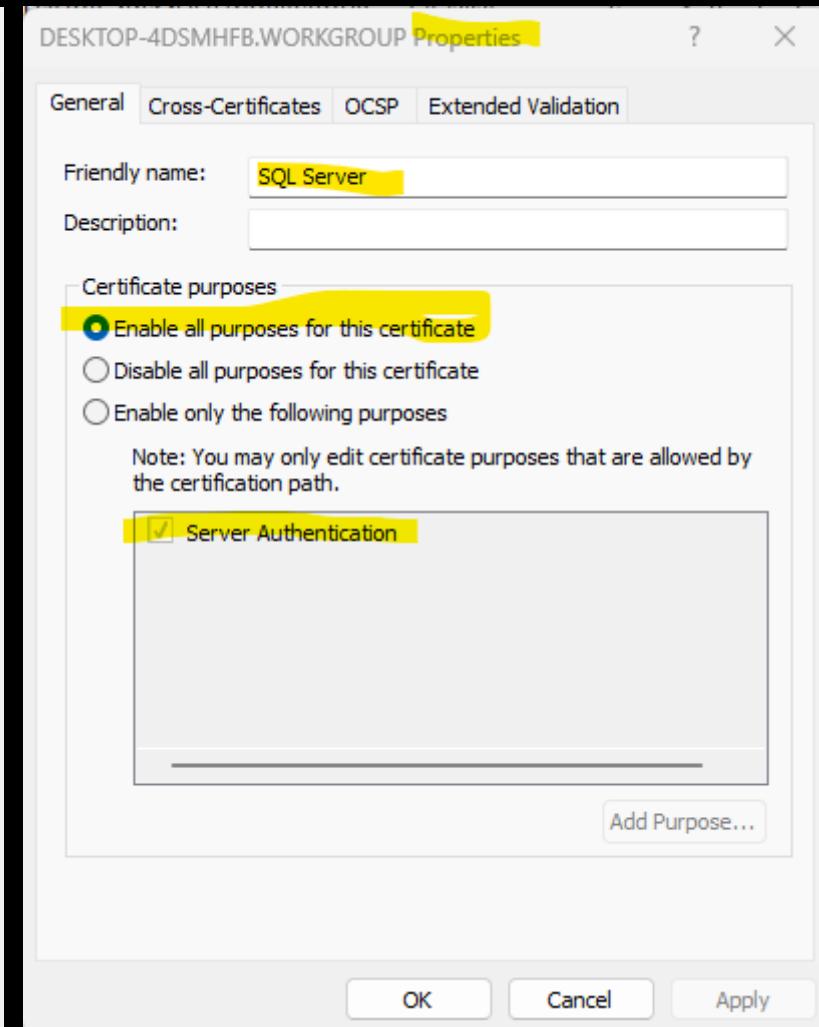
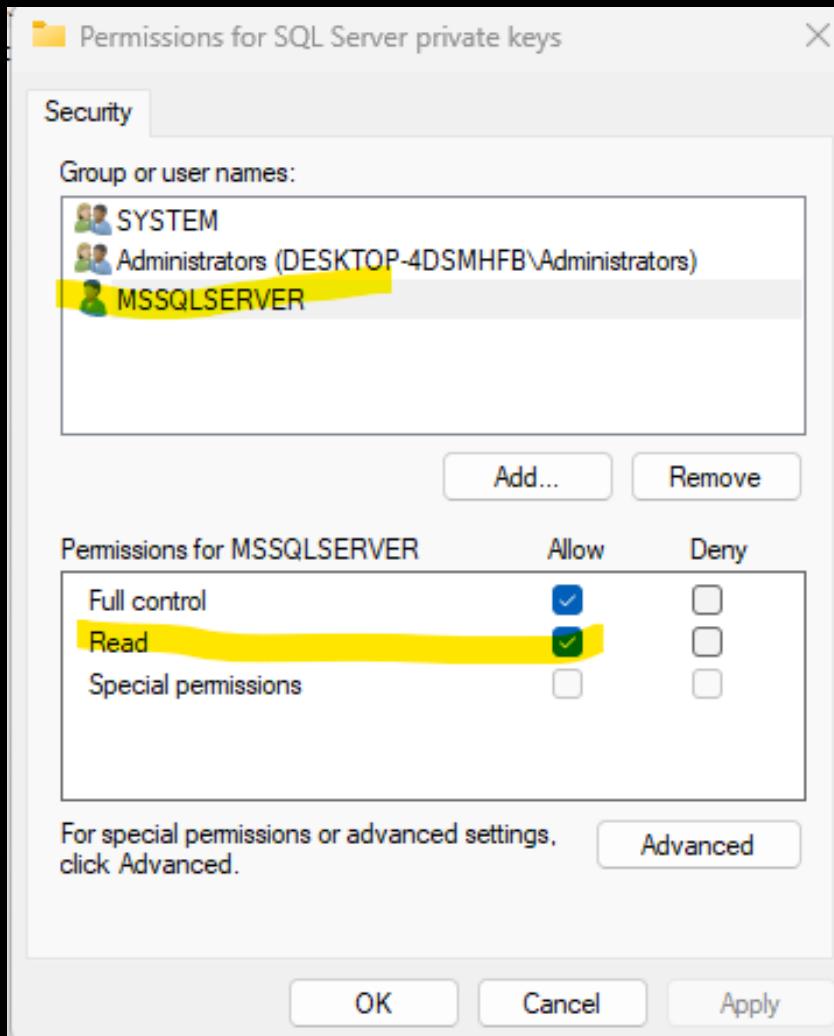
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
localhost	DESKTOP-4DSMHFB.WORKGROUP	6/5/2025	Server Authentication	SQL Server
		12/19/2027	Server Authentication	IIS Express Develop...

The bottom screenshot is titled "Computer Management". It shows the "Services and Applications" section with a list of services. The "SQL Server (MSSQLSERVER)" service is highlighted in yellow. The table below lists the services:

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server (MSSQLSERVER)	Running	Automatic	NT Service\MSSQLSERVER	5868	SQL Server
SQL Server Browser	Stopped	Other (Boot, Syste...)	NT AUTHORITY\LOCALSERVICE	0	
SQL Server Agent...	Running	Manual	NT Service\SQLSERVERAGENT	17596	SQL Agent

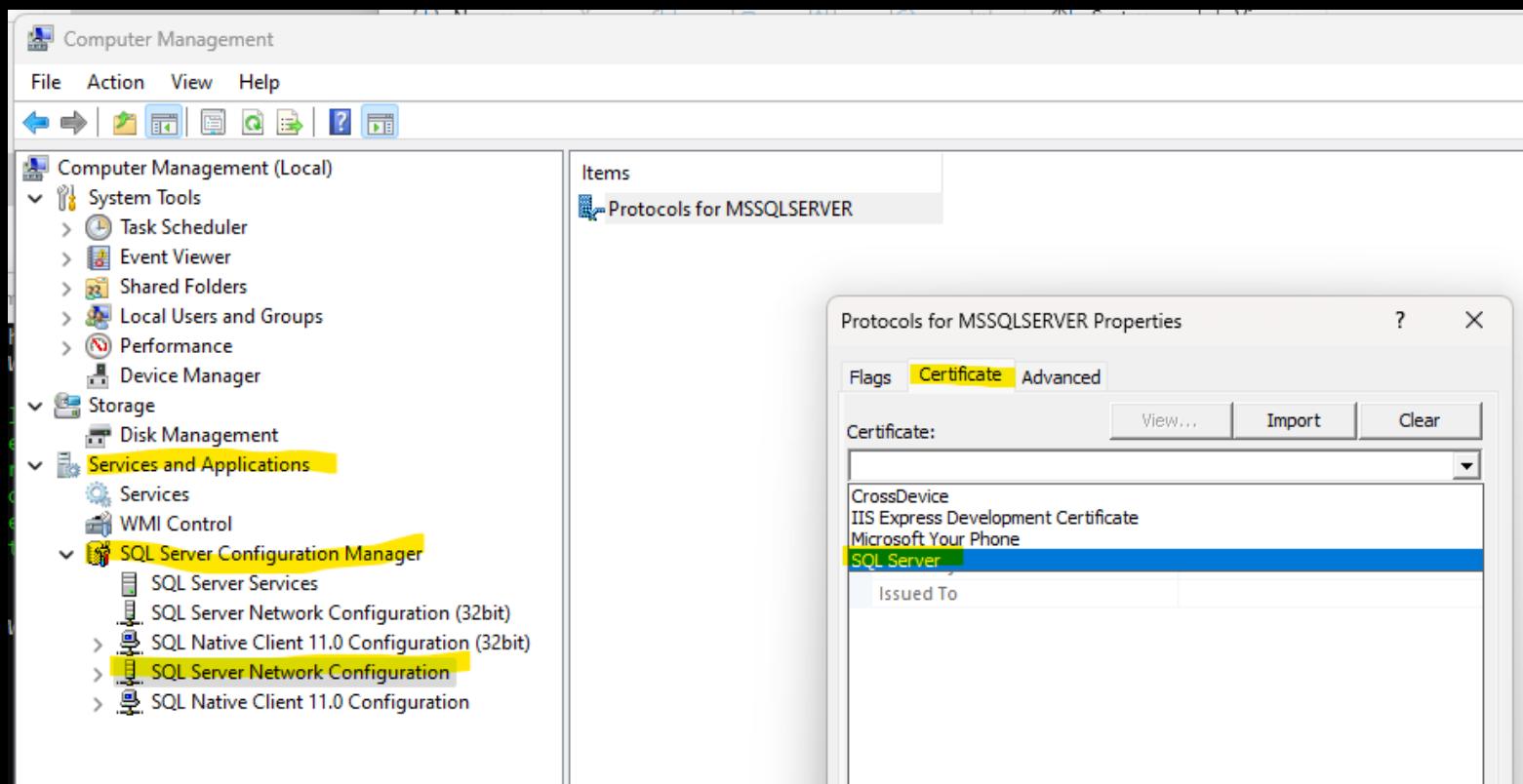
# Grant SQL Server rights to read private key (pt. 2)

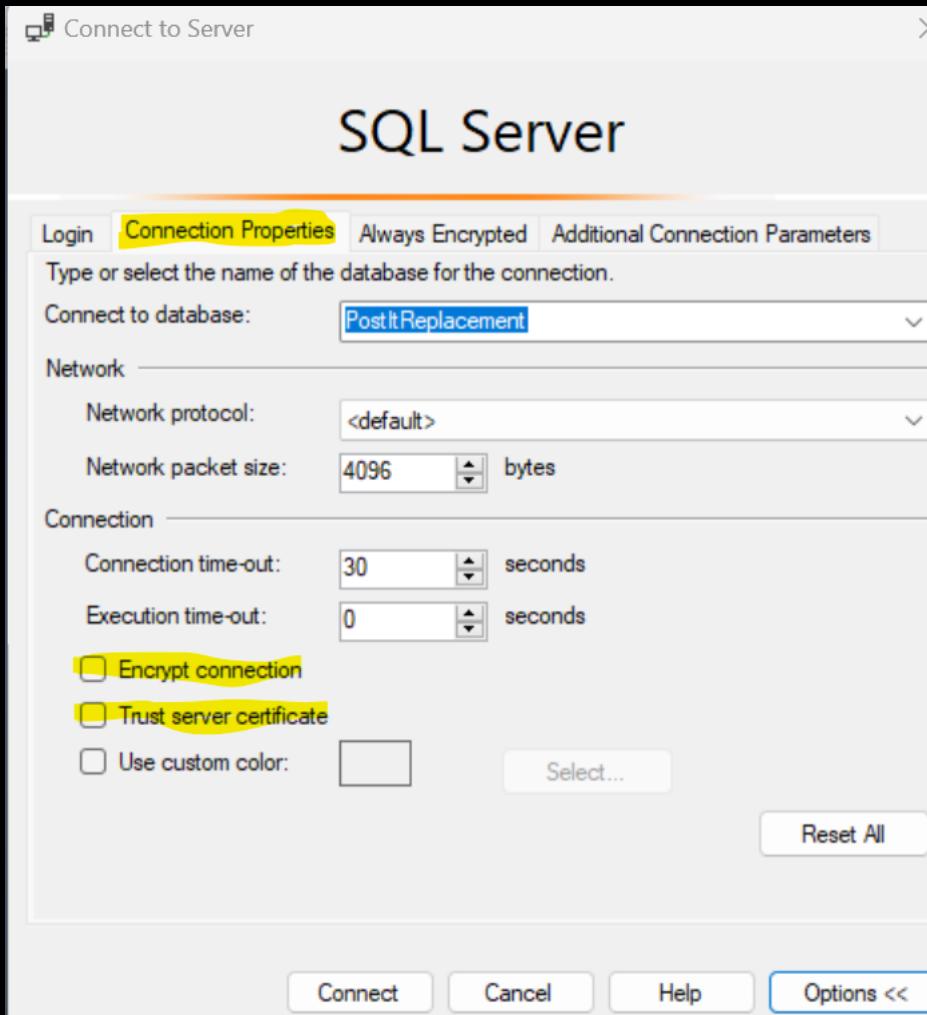
- Give service account Read permissions
- Make sure Server Authentication is selected in Properties



# Configure SQL Server to use our new cert

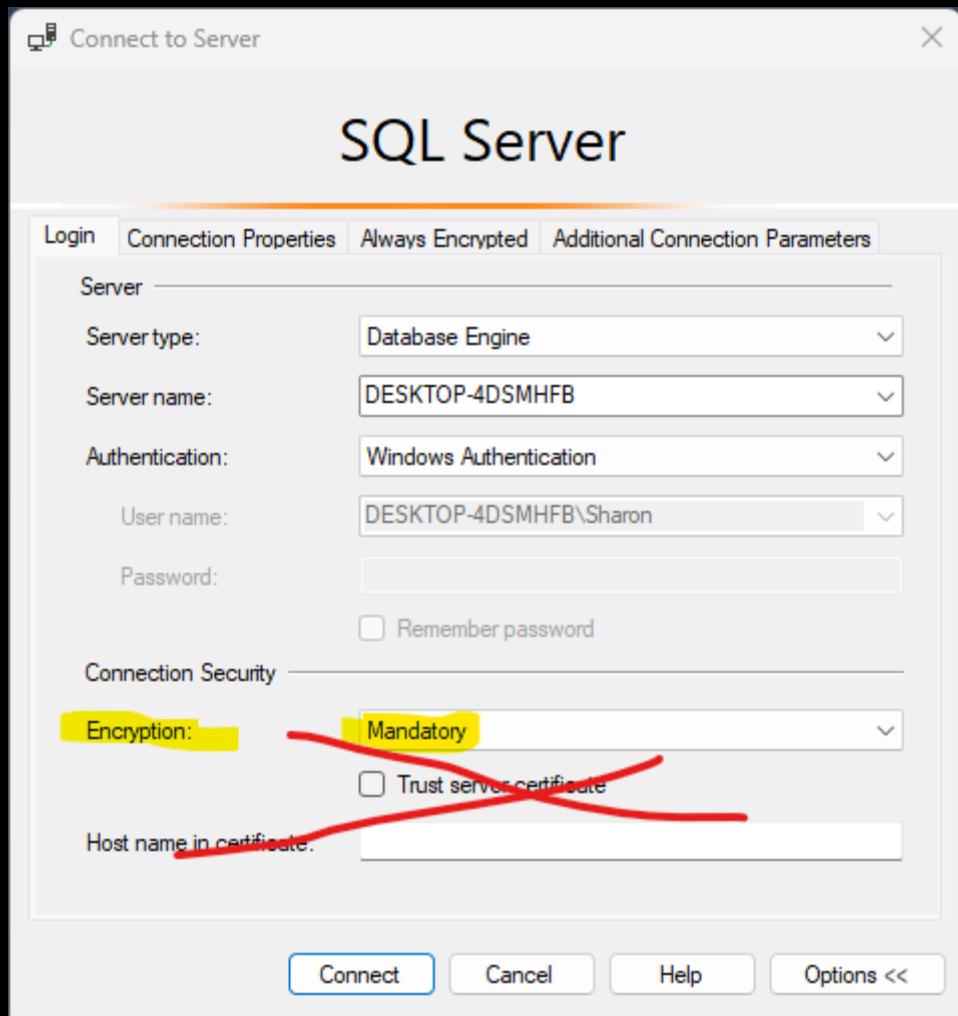
- SQL Server Configuration Manager
- SQL Server Network Configuration
- Select instance
- Right click>Properties>Certificate
- Choose cert
- Restart service





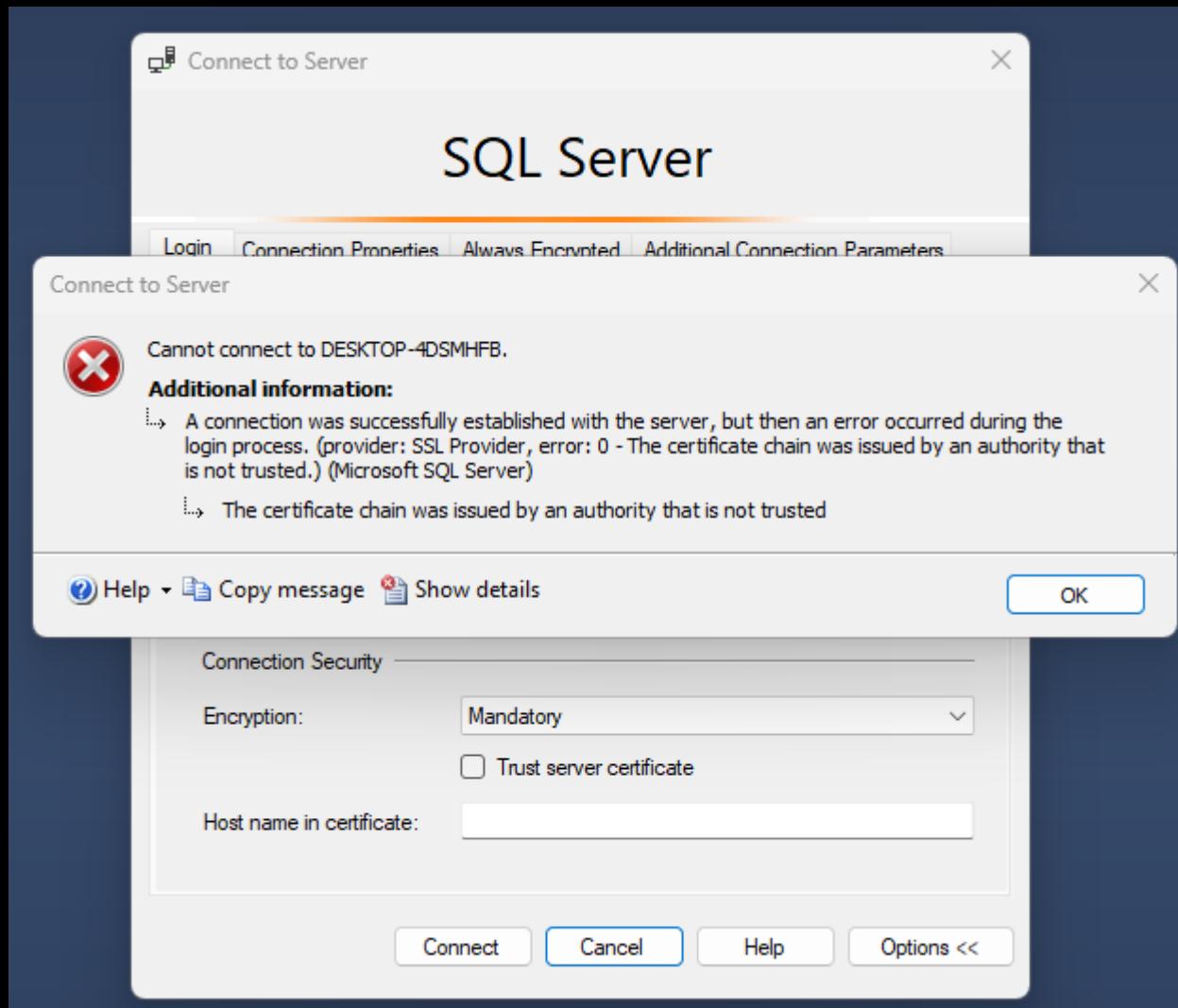
## SSMS 18 or 19

- Encryption options on 2<sup>nd</sup> tab
- Defaults to not using Encrypt Connection
- Offers Trust Server option



# SSMS 20

- Moved Encryption checkbox to first tab
- Defaults to Mandatory
  - Means to encrypt that connection
- Offers Trust Server option
  - Not secure
  - Susceptible to man-in-the-middle attacks



## SSMS 20

- Not set up for encrypted connections
- Can switch to Encryption Optional
- Can check Trust Server option

# Connection strings

- Add Encrypt=Yes to your connection string
- Can add Trust Server Certificate=Yes but  
DON'T
- [Microsoft link on encryption connection  
strings](#)

*(Grand Canyon North Rim—Allison Harris)*

# Resources

[www.sqlshack.com/how-to-set-and-use-encrypted-sql-server-connections](http://www.sqlshack.com/how-to-set-and-use-encrypted-sql-server-connections)  
[www.mssqltips.com/sqlservertip/3299/how-to-configure-ssql-encryption-in-sql-server](http://www.mssqltips.com/sqlservertip/3299/how-to-configure-ssql-encryption-in-sql-server)  
[www.mssqltips.com/sqlservertip/3408/how-to-troubleshoot-ssl-encryption-issues-in-sql-server](http://www.mssqltips.com/sqlservertip/3408/how-to-troubleshoot-ssl-encryption-issues-in-sql-server)  
[www.dataversity.net/securing-data-in-transit-for-analytics-operations](http://www.dataversity.net/securing-data-in-transit-for-analytics-operations)  
[www.digicert.com/faq/cryptography/what-is-ssl-cryptography](http://www.digicert.com/faq/cryptography/what-is-ssl-cryptography)  
[msurasky.wordpress.com/2017/02/27/encryption-in-transit/](http://msurasky.wordpress.com/2017/02/27/encryption-in-transit/)



*(Grand Canyon—my daughter Allison Harris)*

# Contact info

- sharon.reid.harris@gmail.com
- <https://github.com/InfoJunkie1/EncryptConnections>
- @Edudiva on Twitter
- @edudiva@dataplatform.social on Mastodon
- @edudiva.bsky.social on Bluesky
- [linkedin.com/in/Sharon-reid-44433654](https://linkedin.com/in/Sharon-reid-44433654) on LinkedIn



(Grand Canyon—North Rim)