### TLS 1.2 Support on UC Suite's MS-SQL Server

#### **Applies to:**

Imagicle UC Suite rel. 2020.Winter.1 and above

#### **Description:**

This article explains the necessary steps to enable TLS. 1.2 secure connection to SQL Server. This is highly recommended if the SQL Server instance is running on a different server.

#### **Check Certificate requirements**

If you want to use a secure connection to SQL Server, a valid certificate must be used by SQL Server.

If you already have a trusted certificate for the Imagicle Server please skip this session. Otherwise you can build a self-signed certificate suitable for a SQL Server in a lab/test environment, by following this procedure:

- Login onto Imagicle Application Suite
- Open a command prompt and move into the following Directory:
- <StonevoiceAS>\System\SSL
- Launch the following command:

makecert -r -pe -n "CN=MININT-Q99PLQN.fareast.corp.microsoft.com" -b 10/16/2015 -e 12/01/2020 -eku 1.3.6.1.5.5.7.3.1 -ss my -sr localMachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 -a sha256

• The name of the certificate (CN=) must equal the server FQDN or full computer name of Imagicle Server

Following mandatory requirements of SQL certificate:

- It must be valid thus the current system date and time should be between the Valid From and Valid To properties of the certificate.
- It must be available into WCS "Personal" section (Computer account)
- The Common Name (CN) in the Subject property of the certificate must be the same as the fully qualified domain name (FQDN) of the server computer.
- It must be issued for server authentication so the Enhanced Key Usage property of the certificate should include 'Server Authentication (1.3.6.1.5.5.7.3.1)'.
- It must be created by using the KeySpec option of 'AT\_KEYEXCHANGE'.

Moreover, the certificate should be available in "Trusted root certification authorities". If not available, you can export it without a private key from **Personal** â **Certificates** and subsequently import it in **Trusted Root Certificaton Authorities** â **Certificates**. See below screenshots for the complete export/import procedure:

#### **Certificate Export**

👼 certin	n - [Certificates -	Local Compu	ter\Per	sonal\Cer	tificates]		x
File Action View Help							
🗢 🔿 🖄 🖬 🔏 🛱	) 🗟 🛛 🖬						
🗊 Certificates - Local Computer 🔺 🚞 Personal	Issued To 📩 🕈	ording	Issued Imagic	By Ie Call Reco	rding	Expiration Date 12/31/2035	Inte <al< td=""></al<>
Certificates	🕼 Imagicle Applicat	tionSuite	Imagic	leApplicatio	nSuite	1/1/2036	Sen
Trusted Root Certification Au	🙀 WIN-6EONT4KPI	PAS	WIN-6	EONT4KPPA	(S	12/1/2020	Sen
Certificates		Open					
Interprise Trust Intermediate Certification Au		All Tasks	•	Open			
<ul> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Third-Party Root Certification</li> <li>Trusted People</li> </ul>	Cut Copy Delete			Request Certificate with New Key Renew Certificate with New Key Manage Private Keys		nith New Key ith New Key s	
Client Authentication Issuers		Properties		Advar	nced Operation	ns	•
Remote Desktop		Help		Export	t		
<ul> <li>Trusted Devices</li> <li>Web Hosting</li> <li>Windows Live ID Token Issue</li> </ul>							
< III >	<	Ш					>
Export a certificate							

🕑 🍠 Certificate Export Wizard	
Export Private Key	
You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with certificate, you must type a password on a later page.	n the
Do you want to export the private key with the certificate?	
○ Yes, export the private key	
No, do not export the private key	
	-
Next	Cancel

Certificates ca	an be exported in a variety of file formats.
Select the for	mat you want to use:
DER er	ncoded binary X.509 (.CER)
O Base-6	4 encoded X.509 (.CER)
O Crypto	graphic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	lude all certificates in the certification path if possible
O Person	al Information Exchange - PKCS #12 (.PFX)
	lude all certificates in the certification path if possible
Del	lete the private key if the export is successful
Exp	port all extended properties
O Microso	oft Serialized Certificate Store (.SST)

ج چ	Certificate Export Wizard	×
	Completing the Certificate Ex	port Wizard
	You have successfully completed the Certificate	Export wizard
,	You have specified the following settings:	
	File Name	C:\Users\Administrator.WIN-6EONT4K
	Export Keys	No
	Include all certificates in the certification path	No
	File Format	DER Encoded Binary X.509 (*.cer)
	< 111	>
		Finish Cancel

#### **Certificate Import**

Import must be done on the machine where SQL Server instance is installed.

🗟 certlm - [Certific	tates - Loc	al Comp	outer\Trusted Root Cert	ification Authorities\Certificat	es] 🗕 🗖	x
File Action View Help						
🗔 Certificates - Local Co	omputer	Issued To	0 •	Issued By	Expiration Date	^
🔺 🚞 Personal		AddT	rust External CA Root	AddTrust External CA Root	5/30/2020	
🦰 Certificates		🗔 Baltin	nore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	
🔺 🧮 Trusted Root Cert	ification Au	🗔 Class	3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/2/2028	
📔 Certifica	All Tasks	•	Import	Copyright (c) 1997 Microsoft Corp.	12/31/1999	•
Enterprise T	AITON		reassureate toocea	DigiCert Assured ID Root CA	11/10/2031	
Intermediat	View	•	rt High Assurance EV Ro	DigiCert High Assurance EV Root	11/10/2031	
I Irusted Pub I Irusted Pub	Refresh		pot CA X3	DST Root CA X3	9/30/2021	
District Development	Export List		x Secure Certificate Auth	Equifax Secure Certificate Authority	8/22/2018	=
Fining Party			ust Global CA	GeoTrust Global CA	5/21/2022	
Figure 1 Client Authors and	Help		Sign	GlobalSign	12/15/2021	
Bemote Deskton	donnosacio	🗔 Globa	ISign Root CA	GlobalSign Root CA	1/28/2028	
b Smart Card Truste	ed Roots	🗔 Go Da	addy Class 2 Certification	Go Daddy Class 2 Certification Au	6/29/2034	
Trusted Devices		🗔 Imagi	icle Call Recording	Imagicle Call Recording	12/31/2035	
Web Hosting		🔄 Micro	osoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	1/1/2000	
Windows Live ID 1	Token Issue	🗔 Micro	soft Root Authority	Microsoft Root Authority	12/31/2020	
		🗔 Micro	soft Root Certificate Auth	Microsoft Root Certificate Authori	5/10/2021	
		🗔 Micro	soft Root Certificate Auth	Microsoft Root Certificate Authori	6/23/2035	
		🗔 Micro	soft Root Certificate Auth	Microsoft Root Certificate Authori	3/22/2036	
		🗔 NO LI	ABILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 V	1/8/2004	1
		🗔 Start 🤇	Com Certification Authority	StartCom Certification Authority	9/17/2036	
		Thaw	te Timestamning CA	Thawte Timestamning CA	1/1/2021	· Y
	>	<				2
Add a certificate to a store	2					

💿 🍠 Certificate Import Wizard	x
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location	
Current User     Ser     Local Machine	
To continue, click Next.	
Next Cance	:

×
📀 🍠 Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\Users\Administrator.WIN-6EONT4KPPAS\Desktop\cert.cer Browse
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next Cancel

	x
🛞 🍠 Certificate Import Wizard	
Cartificata Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
O Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities Browse	
Next Can	cel

	x
📀 🌛 Certificate Import Wizard	
Completing the Certifi	cate Import Wizard
The certificate will be imported after	r you click Finish.
You have specified the following set	ttings:
Certificate Store Selected by User	Trusted Root Certification Authorities
File Name	C:\Users\Administrator.WIN-6EONT4KPPAS\Desktop'
<	III >
	Finish Cancel

See this link for additional information.

Please notice that these requirements do not apply if you're going to establish a plain (unsecure) connection to SQL Server.

Also ensure the following:

- The certificate must be listed in "Personal" section of WCS (check using certIm.msc)
- The "Subject" property must equal server FQDN
- Server authentication (eku=1.3.6.1.5.5.7.3.1) must be enabled
- Must be created with KeySpec option set to "AT\_KEYEXCHANGE"
- Must also be listed in "Trusted root certification authority" section: if not listed, copy from "Personal/Certificates" section.
- Check certificate permissions: "NETWORK SERVICE" user must be present and have Full control



#### **SQL Server Engine Configuration**

To allow encrypted connections to SQL Server, you must configure a certificate. This is accomplished in two different ways:

- 1. Using own trusted certificate (in production environments):
- Pls. start SQL Server Configuration Manager and select "SQL Server Network Configuration" â "Protocols for IMAGICLE". Right-click on "Properties" and select "Certificate" tab. Here you can add your own trusted certificate.



- 2. Using a self-signed, auto-generated user's certificate (test environments):
- Pls. start SQL Server Configuration Manager and select "SQL Server Network Configuration" â "Protocols for IMAGICLE". Right-click on "Properties" and select "Certificate" tab. Here you can add new self-signed certificate (check certificate requirements for SQL Server).



#### Configure the UC Suite to use secure connection to SQL Server

Secure connection to SQL server is not mandatory for TLS setup. However, it is recommended when SQL server runs on a different server.

If you want to use a secure connection to the SQL Server, run the Imagicle Database Configuration tool (from Start Menu/Imagicle UC Suite), then select the "Use secure connection" checkbox and complete the procedure following the configuration wizard's instructions.

Billy Blue's setup wizard 📃 🗖 🗙					
Connecting to the SQL Server Enter the data to access Microsoft SQL Server. Click 'Next' to create the database and the DSN necessary to run BillyBlue's.					
SQL Server location:					
<ul> <li>On another computer (hostname or IP address):</li> </ul>					
SQL Server Instance name (if any):	IMAGICLE				
User name:	sa				
Password:	*****				
Database name:	BluesPro				
	Use secure connection				
	Next > Cancel				

If an external SQL Server is used, the FQDN must be entered in the SQL Server location

#### Adjust the UC Suite SQL client version

Regardless you are using or not a secure connection to SQL, you need to increase the SQL client version used by the Imagicle services to connect to the database:

- 1. Edit the file StonevoiceAS\System\SvSasDB.ini and replace the word 'SQLNCLI10 ' with 'SQLNCLI11'.
- 2. Save the file.
- 3. Stop and Start all Imagicle services or restart the server.

#### **Complete HA-related configurations**

In case of an HA environment, ensure <u>all</u> servers have <u>all</u> cluster certificates imported.