Mobile Solutions™
By Elliott Data Systems, Inc.

MOBILE SOLUTIONS DATABASE ENCRYPTION

Technical Guide

Version #2

Prepared By:
Elliott Data Systems, Inc.

17825 Edison Ave
Chesterfield, MO 63005
(636) 386-8400
Fax (636) 386-3072

Customer Service Support
1-888-345-8511

mobilesolutions@elliottdata.com
www.elliottmobilesolutions.com

Table of Contents

Overview

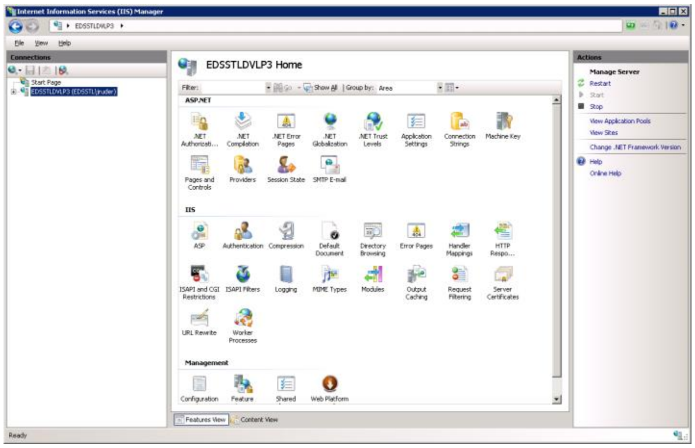
Mobile Solutions versions 7.6.21 and later have the ability to encrypt communications between the software and the database layers of the application using an SSL cert of any desired length. The software will passively encrypt communications regardless of any settings, but more options are available for increased security.

Creating a certificate on the server

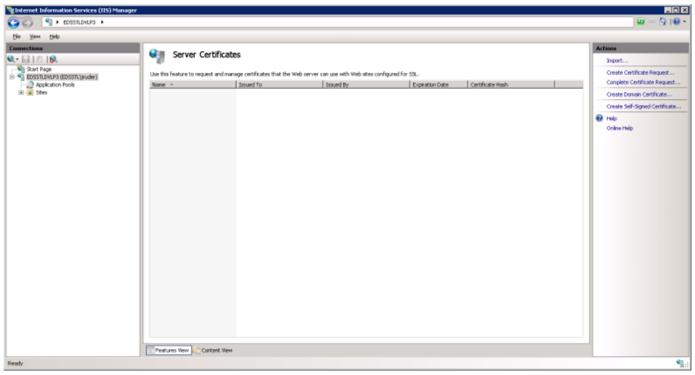
By creating a certificate for your SQL server, you can specify a particular certification to use, rather than a randomly generated cert. This section describes how to go about creating a self-signed cert, and configuring SQL Server to use the cert.

Creating a self-signed cert

1. Open IIS and select the root server from the navigation on the left

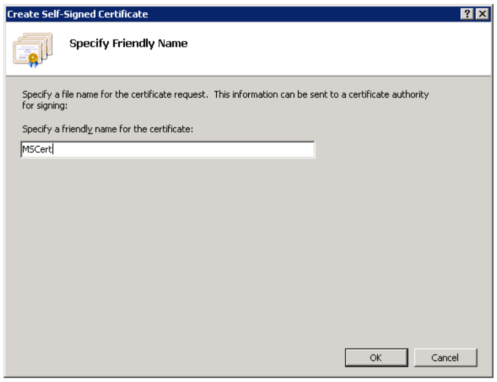


2. Open the Server Certificates area



Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

3. Click the “Create Self-Signed Certificate...” link from the actions menu on the right
4. Enter a name for your cert



Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

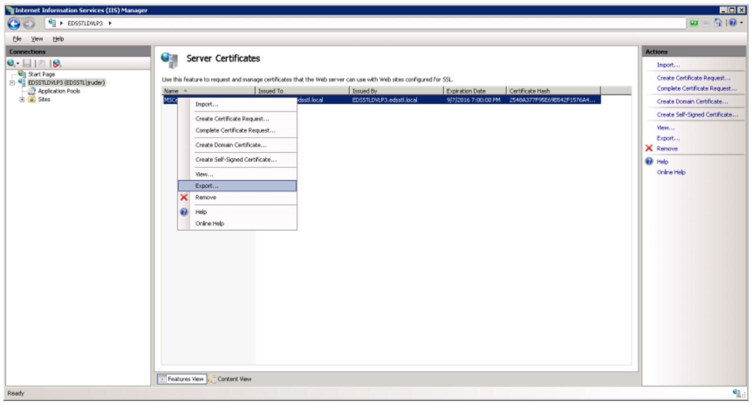
MSCert

5. The cert is now automatically installed in your cert store

Export the cert for clients

Client machines may enable options requiring that server certs be trusted, or they will not connect. In order for a client to trust a server’s cert, the server must first create a cert file, and the client must trust it. This is a manual process, and the cert file is recommended to be sent to client PCs via E-Mail or flash drive. This section outlines how to export the cert to a file.

1. From the IIS Certifications page, right click the cert that you wish to export from the list



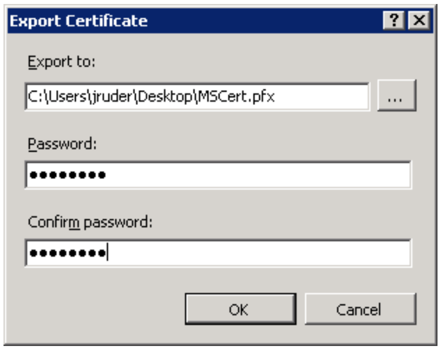
Internet Information Services (IIS) Manager
EDSSTLDVLP3
File
View
Help
Connections
Start Page
EDSSTLDVLP3 (EDSSTL\jruder)
Application Pools
Sites
Server Certificates
Name
Issued To
Issued By
Expiration Date
Certificate Hash
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Help
Online Help
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Help
Online Help
Features View
Content View
Ready

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash
MSC	dsstl.local	EDSSTLDVLP3.edsstl.local	9/7/2016 7:00:00 PM	2548A377F95E698542F1576A4...

2. Select “Export...” from the drop down

3. Select an export location to create the file, and create a password. Each client installing this cert will be required to know the password you enter here.



Export to: C:\Users\jruder\Desktop\MSCert.pfx

Password: ••••••••

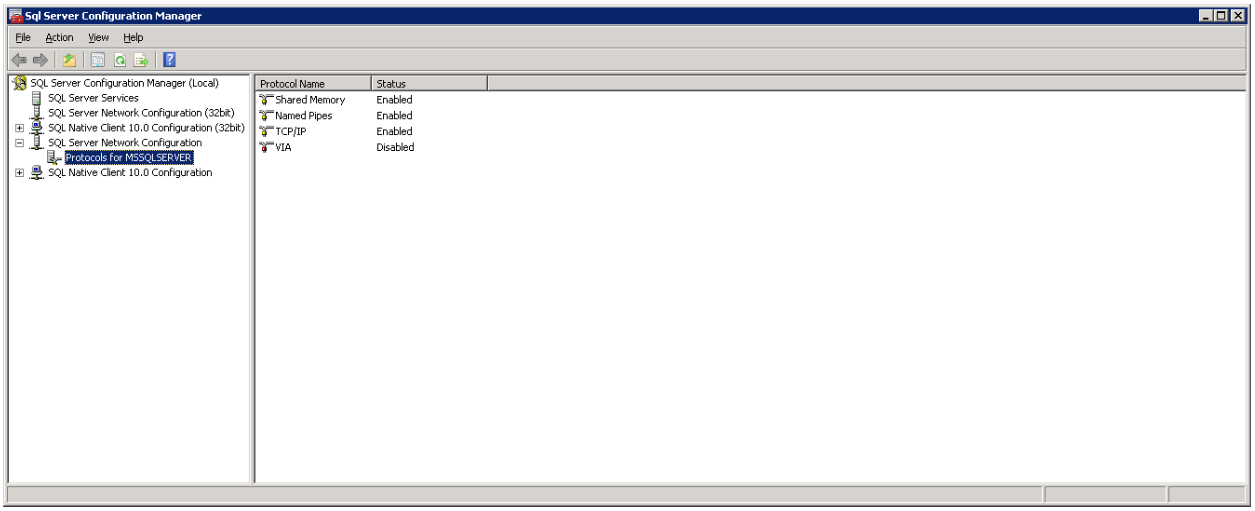
Confirm password: ••••••••

4. You can now send the pfx file to the desired clients

Configuring SQL Server to use the cert

If your IIS and SQL Server are on the same PC/Server, then the cert will automatically be installed in the store. If your SQL Server and IIS Server are different physical devices however, you will need to install the cert onto the SQL Server computer. See the client cert installation section for details on installing the cert from the cert file.

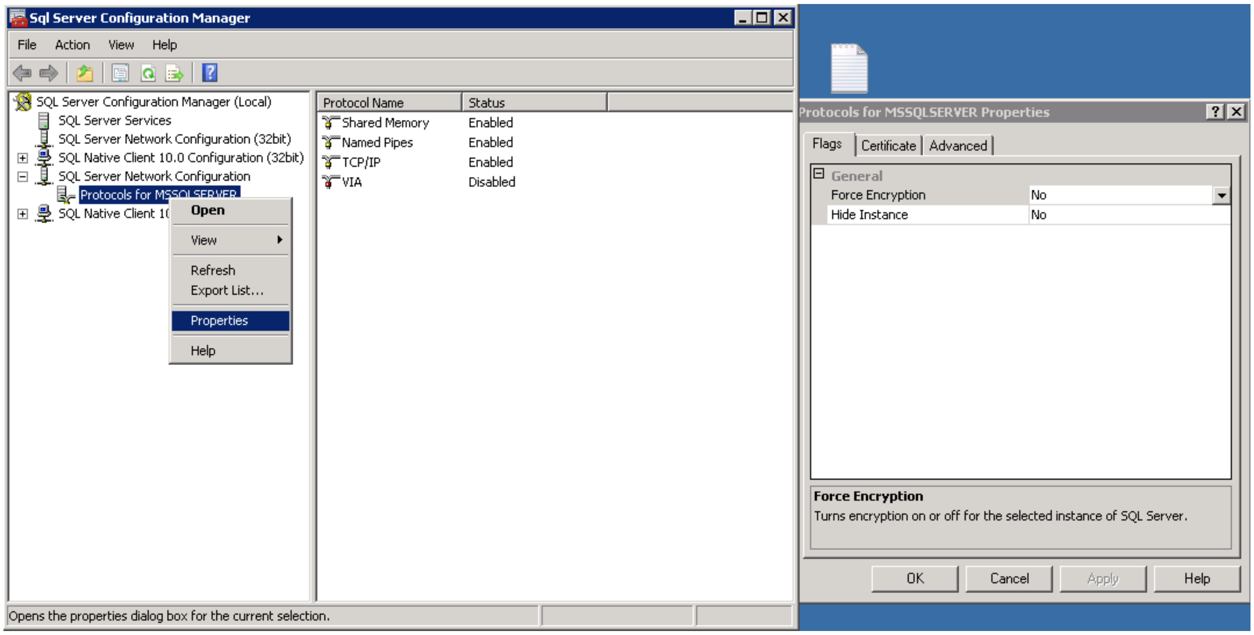
1. Open the Sql Server Configuration Manager, and select the protocols for your SQL server



- SQL Server Configuration Manager (Local)
  - SQL Server Services
  - SQL Server Network Configuration (32bit)
  - SQL Native Client 10.0 Configuration (32bit)
  - SQL Server Network Configuration
    - Protocols for MSSQLSERVER
  - SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

2. Right click “Protocols for <servername>” and select properties


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for MSSQLSERVER
SQL Native Client 10
Open
View
Refresh
Export List...
Properties
Help
Protocols for MSSQLSERVER Properties
Flags
Certificate
Advanced
General
OK
Cancel
Apply
Help

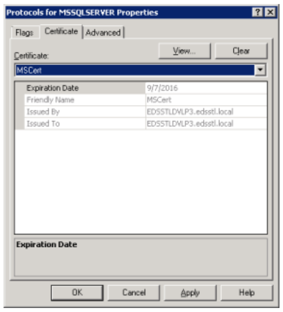
Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

Force Encryption	No
Hide Instance	No

Force Encryption
Turns encryption on or off for the selected instance of SQL Server.

Opens the properties dialog box for the current selection.

3. Open the Certificate tab, and use the drop down to select the cert you created earlier. This will only display certs already installed into the computer’s cert store.



Certificate: MSCert

Expiration Date	9/7/2016
Friendly Name	MSCert
Issued By	EDSSTLDVLP3.edsstl.local
Issued To	EDSSTLDVLP3.edsstl.local

4. Click OK. You will get a warning stating that you need to restart SQL Server.
5. Restart SQL Server by doing one of the following
    a. Reboot the computer
    b. Restart the windows service named “SQL Server (<instancename>)”
    c. Open SSMS, connect to the server, right click the server instance in the navigation and select “Restart”
    d. IMPORTANT NOTE: Sometimes when attempting to restart the service after selecting the cert, the service will be unable to start due to user rights. It is often necessary to enter the windows services page and select a new user with higher rights to run the SQL Server instance.

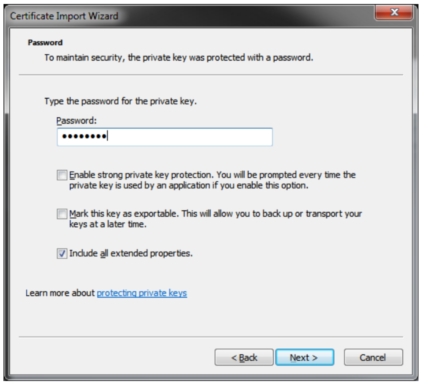
Using certificate on client computers

In order for a client and server computers to have the same certs installed, the .pfx file must be installed on the local client. The only two things you need for this are the actual PFX file, and the password that the creator used to export it.

Installing a cert into the cert store on a client computer

1. Start by double-clicking the cert file on the local PC

2. Click Next when prompted about installing certs
3. Click Next when prompted to enter the cert location (it's already entered)
4. Type in the password that was used during the export and click Next


Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: ••••••••

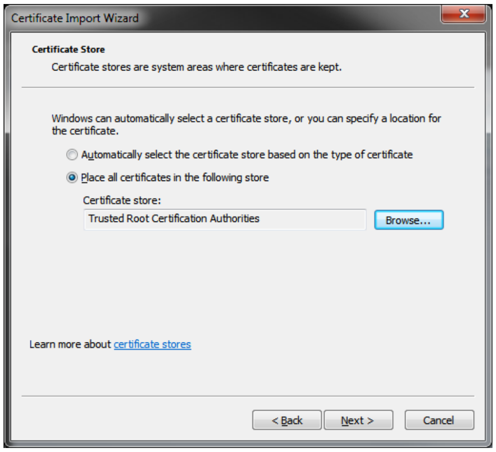
☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

5. Select "Place all certificates in the following store" radio option, then select "Trusted Root Certification Authorities" from the browse menu. Then click Next.


Certificate Import Wizard

Certificate 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.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

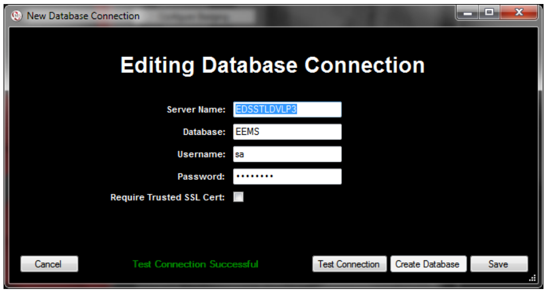
Learn more about certificate stores

6. Click Finish on the verification screen
7. You will likely get a security warning since this will likely be a self-signed cert. Click Yes to accept the cert.

Enabling "Required Trusted SSL Cert" on Mobile Solutions software

Mobile solutions software released after 7.6.21 have checkboxes on their database connection pages that allow you to “Require Trusted SSL Certs”. This means that when you check this check box, the client software using this connection will refuse to connect to the server, unless the server is using one of the certs installed in the local PC’s cert store. This may seem like a backwards concept at first. But it is used to prevent a hacker from impersonating the SQL server with another server aliasing the same name.

1. Open the database connection page in any client-side software in Mobile Solutions

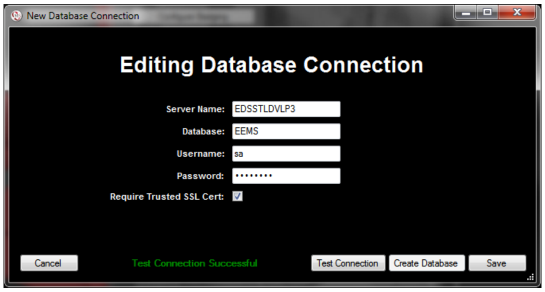


Editing Database Connection

Server Name: EDSSTLDVLP3
Database: EEMS
Username: sa
Password: ••••••••
Require Trusted SSL Cert: ☐

Test Connection Successful

2. Check the Require Trusted SSL Cert option

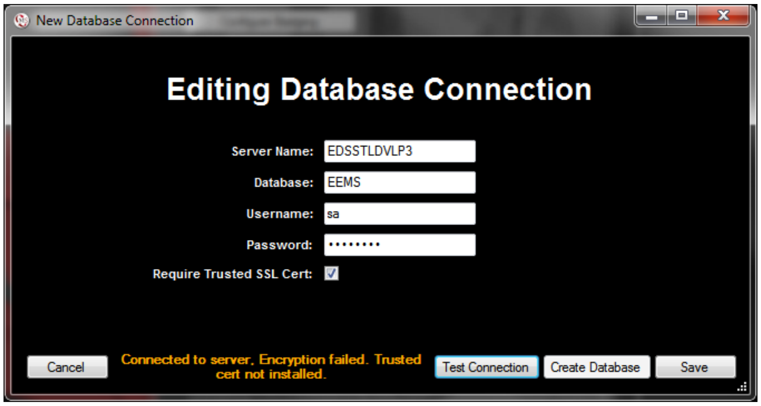


Editing Database Connection

Server Name: EDSSTLDVLP3
Database: EEMS
Username: sa
Password: ••••••••
Require Trusted SSL Cert: ☑

Test Connection Successful

3. Test the connection, or click OK. If the cert verification fails, you will receive a message stating that something went wrong and needs to be diagnosed.



Editing Database Connection

Server Name: EDSSTLDVLP3
Database: EEMS
Username: sa
Password: •••••••••
Require Trusted SSL Cert: ☑

Connected to server. Encryption failed. Trusted cert not installed.