



Secure MobiLink Synchronization using Microsoft IIS and the MobiLink Redirector

A whitepaper from Sybase iAnywhere

Author: Joshua Savill, Product Manager

Date: September 29th, 2008

**This whitepaper was written in the context of SQL Anywhere 10.
However, its content may be applicable to previous and future releases.**

Contents

Introduction	3
Prerequisites	3
Securing the Communication Stream	4
Configuring SSL on the Microsoft IIS Web Server	4
Create the Root Certificate.....	4
Create a Web Server Certificate.....	5
Sign the certreq.txt File	5
Install the rsa_iis.crt certificate.....	6
Verify the HTTPS Connection and Install the Certificate	6
Configuring the MobiLink Server and Redirector for HTTPS Communication.....	6
Setting Up the MobiLink Client	7
Additional Resources.....	7
Summary	8

Introduction

This document provides instructions for setting up secure MobiLink synchronization on a Microsoft Internet Information Services (IIS) web server. Although this document describes the methodology for SQL Anywhere 10.0.1, the procedures are applicable to all versions of SQL Anywhere.

For production systems, it is recommended that you purchase server certificates from a reputable Certificate Authority. The type of certificate required is dependent upon your unique business needs and encryption requirements.

Prerequisites

Before completing the procedures described in this document, it is recommended that you review the following information:

- Securing SQL Anywhere Server 10:
http://www.sybase.com/files/White_Papers/SecuringSA10.pdf
- Understanding Encryption and Transport-Layer Security
<http://www.sybase.com/detail?id=1035475>
- MobiLink transport-layer security and certificates:
<http://www.sybase.com/detail?id=1009621>
- Generating X.509 Certificates for Secure Communication in SQL Anywhere 10.0.1:
<http://www.sybase.com/detail?id=1055179>

The following software is required to complete the procedures in this document:

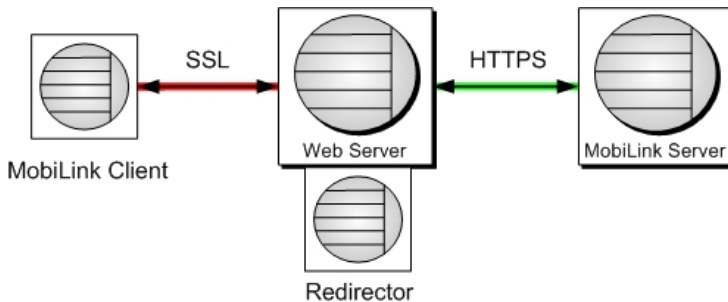
- Microsoft Windows 2000 Server or Microsoft Windows 2003 Server
- Microsoft Internet Information Services 5.0 or Microsoft Internet Information Services 6.0
- SQL Anywhere with MobiLink 10.0.1 and RSA encryption
- The SQL Anywhere 10.0.1 – Secure MobiLink Synchronization using Microsoft IIS code sample. The code sample is available for download from the following path:
<http://www.sybase.com/detail?id=1059364>

Securing the Communication Stream

To ensure the security of the communication stream, the procedures include the installation of the following security protocols:

- Transport Layer Security (TLS) for the entire MobiLink synchronization
- Secure Sockets Layer (SSL) and RSA encryption on the MobiLink client and Microsoft IIS web server.
- HTTPS and RSA encryption on the MobiLink Redirector and MobiLink Server

This diagram illustrates how the communication stream is configured for optimum security:



Configuring SSL on the Microsoft IIS Web Server

Create the Root Certificate

1. Install the `createcert` utility included with the RSA encryption option.
2. Run the following command:

```
"%SQLANY10%\win32\createcert"
```
3. Complete the following fields:

Field	Value
Choose encryption type ((R)SA or (E)CC)	R
Enter RSA key length (512-16384)	1024
Country Code	CA
State/Province	ON
Locality	Waterloo
Organization	Sybase
Organizational Unit	Sybase
Common Name	Sybase
Certificate valid for how many years (1-100)	10
Certificate Authority	Y
Key Usage [6,7]	6,7
Enter file path to save certificate	rsa_root.crt
Enter file path to save private key	rsa_key.key
Enter password to protect private key	pwd
Enter file path to save identity	id.pem

Create a Web Server Certificate

1. Open the Microsoft IIS Manager.
2. In the left pane, right-click **Default Web Site** and click **Properties**.
3. Click the **Web Site** tab.
4. In the **SSL Port** field, type **443**.
5. Click the **Directory Security** tab.
6. Click **Server Certificate**.
7. Click **Create a new certificate**. Click **Next**.
8. Click **Prepare the request now, but send it later**. Click **Next**.
9. In the **Name** field, type **Default Web Site** and on the **Bit length** list click **1024**. Click **Next**.
10. In the **Organization** and **Organizational unit** fields, type **Sybase**. Click **Next**.
11. In the **Common name** field, type **jsavill-iis**. Click **Next**.
12. Complete the following fields:
 - In the **Country/Region** list, click **CA**.
 - In the **State/province** field, type **ON**.
 - In the **City/locality** field, type **Waterloo**.
13. Accept the default location for the certreq.txt file. Click **Next**.
14. Click **Next**.
15. Click **Finish** and then click **OK**.

Sign the certreq.txt File

1. Run the following command:

```
"SQLANY10%\win32\createcert" -s certreq.txt
```
2. Complete the following fields:

Field	Value
Enter file path of signer's certificate	rsa_root.crt
Enter file path of signer's private key	rsa_key.key
Enter password for signer's private key	pwd
Certificate valid for how many years (1-100)	10
Certificate Authority (Y/N)	N
Key Usage [3,4,5]	3,4,5
Enter file path to save certificate	rsa_iis.crt

3. Run the following command:

```
"%SQLANY10%\win32\viewcert" rsa_iis.crt
```
4. Verify the certificate information is correct.

Install the *rsa_iis.crt* certificate

1. Open the Microsoft IIS Manager.
2. In the left pane, right-click **Default Web Site** and click **Properties**.
3. Click the **Directory Security** tab.
4. Click **Server Certificate**. Click **Next**.
5. Click **Process the pending request and install the certificate**. Click **Next**.
6. In the **Path and file name** field, browse to the location of the *rsa_iis.crt* file. Click **Next**.
7. In the **SSL Port** field, type **443**. Click **Next**.
8. Review your settings. Click **Next**.
9. Click **Finish**.

Verify the HTTPS Connection and Install the Certificate

1. Open your Internet browser.
2. In the **Address** field, type <https://servername>. Press **Enter**.
3. Click **Continue to this website**.

The Under Construction page appears indicating the certificate installed correctly.

Configuring the MobiLink Server and Redirector for HTTPS Communication

1. Run the following command:

```
"%SQLANY10%\win32\createcert"
```
2. Complete the following fields:

Field	Value
Choose encryption type ((R)SA or (E)CC)	R
Enter RSA key length (512-16384)	1024
Country Code	CA
State/Province	ON
Locality	Waterloo
Organization	Sybase
Organizational Unit	Sybase
Common Name	Sybase
Certificate valid for how many years (1-100)	10
Certificate Authority	Y
Key Usage [3,4,5]	3,4,5
Enter file path to save certificate	rsa_ml.crt
Enter file path to save private key	rsa_ml_key.key
Enter password to protect private key	pwd
Enter file path to save identity	id_ml.pem

3. Run the *setup.bat* file located in the **cons** folder. This file:

- Initializes a new SQL Anywhere consolidated database
- Creates the data source name
- Spawns the database server
- Sets up the MobiLink system tables
- Inserts test data into the database
- Starts the MobiLink Server with the following command line message:

```
"%SQLANY10%\win32\mlsrv10" -v+ -o mlsrv.out -zs ml_https -c
"DSN=https_cons" -dl -zu+ -x
https{port=2439;tls_type=RSA;certificate=..\certs\id_ml.pem;certif
icate_password=pwd}
```

4. Open the *redirector.config* file in your text editor. The file is saved to the following path:
c:\inetpub\scripts directory.

5. Complete the following section:

```
# Properties
# -----
SLEEP=1800
ML_CLIENT_TIMEOUT=1800
LOG_LEVEL=1
#
# List of servers
# -----
ML="https=true;host=localhost;port=2439;tls_type=RSA;fips=n;truste
d_certificates=C:\\HTTPS_Redirector_IIS\\certs\\rsa_ml.crt"
```

6. Save your changes to the *redirector.config* file.
7. Open the Microsoft IIS Manager.
8. Right-click **Default Web Site**, and click **Stop**.
9. Right-click **Default Web Site**, and click **Start**.

Setting Up the MobiLink Client

Run the *setup.bat* file located in the **rem** folder. This file:

- Initializes a new SQL Anywhere remote database
- Creates the data source name
- Spawns the database server
- Inserts test data into the database
- Starts the MobiLink Server with the following command line message:

```
"%SQLANY10%\win32\dbmlsync" -c "DSN=https_rem" -mp sql -v+ -o rem.txt
-e "ctp=https;adr='host=jsavill-
IIS;port=443;url_suffix=/scripts/iaredirect.dll/ml/;trusted_certifica
tes=..\certs\rsa_root.crt'"
```

Additional Resources

For information about the `createcert` utility, see: <http://www.sybase.com/detail?id=1055179>.

For assistance configuring the MobiLink Redirector using Microsoft IIS, see The MobiLink Redirector using Microsoft Internet Information Services.

For information about the MobiLink Redirector, see
<http://dcx.sybase.com/index.php#http%3A%2F%2Fdcx.sybase.com%2Fhtml%2Fdbmlen10%2Fml-isapi-config-iadeploy.html>.

For assistance installing SQL Anywhere 10.0.1, see
<http://dcx.sybase.com/index.php#http%3A%2F%2Fdcx.sybase.com%2Fhtml%2Fdbdaen10%2Fda-environment-variables.html>.

Summary

This document has outlined the steps required to configure the MobiLink Redirector using Microsoft IIS to complete secure MobiLink synchronizations. Provided with this document is a demonstration of how the MobiLink client, MobiLink server, Redirector, and Microsoft IIS need to be configured. After finishing this document you should have a complete synchronizing system using SSL communication between the MobiLink client and Microsoft IIS Web Server. The communication stream between the MobiLink Redirector and MobiLink server is encrypted with RSA using HTTPS.

Copyright © 2008 iAnywhere Solutions, Inc. All Rights Reserved. Sybase, Afaia, SQL Anywhere, Adaptive Server Anywhere, MobiLink, UltraLite, and M-Business Anywhere are trademarks of Sybase, Inc. All other trademarks are property of their respective owners.