MICRO FOCUS

ZENworks Mobile Workspace
TLS Setup Guide

September 2017

Legal Notice

TABLE OF CONTENTS

1 ENABLE TLS CONNECTION BETWEEN ZENWORKS MOBILE WORKSPACE AND A REVERSE PROXY

This section aims to describe how to install a certificate on ZENworks Mobile Workspace in order to allow TLS connection from a reverse proxy.

1.1 Generate a self-signed certificate

1. Start the application *portecle* provided with ZENworks Mobile Workspace installer package (SENSE_INSTALLER/tools/portecle-launcher.bat)
2. Create a new keystore (File -> New keystore) and select JKS.
3. Generate a key pair (Tools -> Generate Key Pair)
4. Use RSA algorithm with a key size of 4096.
5. Enter the required information.
6. Enter an alias name (senseserver) and a password.
7. Save (File -> Save Keystore) the generated keystore with the same password used for generation as jks file.

1.2 Install the certificate

1. Copy the Keystore in the folder ZMW_HOME/conf
2. Edit the following lines in the file ZMW_HOME /conf/server.xml

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
           port="8443" address="${jboss.bind.address}"
           scheme="https" secure="true" clientAuth="false"
           keystoreFile="<SENSE_HOME>/conf/mykeystore.jks"
           keystorePass="mypassword" sslProtocol = "TLS"

          ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA"/>
```

3. Set the path TLS to the keystore file for the variable keystoreFile and the keystore password (defined at step 2.1.6) for the variable keystorePass

If you want to use the TLS connection between the security server and the application server, your certificate must be added in the ZENworks Mobile Workspace truststore as well.

1.3 Restart the server

1. Press the Windows button and enter "services" as the keyword.
2. Select the program "Services".
3. Find the service SENSE-SERVER.
4. Right click on it and press Restart.

2 ADDING BACK-END TLS CERTIFICATES IN THE ZENWORKS MOBILE WORKSPACE TRUST STORE

This section aims to help IT administrator to properly configure TLS connections between ZENworks Mobile Workspace and back-end systems.

2.1 Creating a ZENworks Mobile Workspace trust store

The first time you need to add a certificate, you need to create a trust store for ZENworks Mobile Workspace. This store will contains all the certificates that must be trusted by ZENworks Mobile Workspace. To ensure that ZENworks Mobile Workspace will trust standard certificates and propriety ones, we will take the JAVA trust store as the basis.

2.1.1 Copy the JAVA trust store

1. Copy the file ZMW _HOME/jdk/jre/lib/security/cacerts
2. Past it in the folder ZMW_HOME/conf and rename to sense.jks

2.1.2 Change the trust store password

3. Start the application portecle provided with the ZENworks Mobile Workspace installer package (ZENworks_Mobile_Workspace __INSTALLER/tools/portecle-launcher.bat)
4. Open sense.truststore (File -> Open keystore file) and enter the password "changeit".
5. Change the password (Tools -> Set Keystore Password) and keep it safely.
6. Save it (File -> Save Keystore)

2.1.3 Enable the trust store

Windows

- Start the SENSE service manager (ZMW_HOME/services/SENSE-SERVER_service_manager.bat)
- On the Java tab, add the following lines and **set the path and the password**:

  -Djavax.net.ssl.trustStore=file:///SENSE_HOME/conf/sense.jks
  -Djavax.net.ssl.trustStorePassword=thepassword

- Apply and restart the SENSE service

Linux

- Edit the file *ZENworks_Mobile_Workspace* _HOME/bin/setenv.sh

- Remove the # before the line where trust store options are defined and **set the path and the password**:

  JAVA_OPTS="$JAVA_OPTS -
  Djavax.net.ssl.trustStore=file:///SENSE_HOME/conf/sense.jks -
  Djavax.net.ssl.trustStorePassword=thepassword"

- Save the file and restart the SENSE service

2.2 Add a certificate in the ZENworks Mobile Workspace trust store

When the trust store has been created and referenced in ZENworks Mobile Workspace, you can add your back-end certificates that ZENworks Mobile Workspace must trust.

1. Start the application *portecle* provided with ZENworks Mobile Workspace installer package (ZMW _INSTALLER/tools/portecle-launcher.bat) Start the application *portecle.*
2. Open sense.truststore (File -> Open keystore file) and enter the password you set during installation.
3. If you have the certificate (*.pem, *.cer, *.crt, *.cert), go to step 8.
4. *Portecle* provides a tool to retrieve the certificate that has to be added (Examine -> Examine SSL/TLS Connection).
5. Enter the back-end hostname or IP address and the port number.
6. Select the certificate you want to add and click "PEM Encoding".
7. Click "Save", browse to ZMW_HOME/conf and save.
8. Import the certificate (Tools -> Import Trusted Certificate).
9. Save (File -> Save Keystore)
10. Restart the SENSE service.

3 ENABLE TLS CONNECTION BETWEEN ZENWORKS MOBILE WORKSPACE AND IBM DOMINO

This section describes how to setup ZENworks Mobile Workspace to enable the TLS connection and how to add the Domino certificate that has to be trusted by ZENworks Mobile Workspace.

3.1 Enable TLS on ZENworks Mobile Workspace

1. Using a WEB browser, get to the PIM configuration administration console. (https://<your_ip>/sense/pim/).
2. Click on the server button and select the "PIM Parameters" tab.
3. On the Mail server section, select the checkbox "**Connect using TLS?**"

3.2 Create a key ring on Domino

Open the Server Certificate Admin (certsrv.nsf) database on a Domino server and use its forms to create and populate a key ring. See *Administering the Domino System, Volume 2* or the Domino Administrator Help for detailed information. For testing purposes, you can use the CertAdminCreateKeyringWithSelfCert form to create a key ring with a self-certified certificate.

3.3 Move the keyring to the server

The keyring consists of a keyring file (KYR file) and stash file (STH file). These files are generated on the computer from which you're accessing the Server Certificate Admin database. Move or copy the two keyring files to the computer containing the Domino server. Place them in the server's data directory. For example, if you create a keyring with a self-certified certificate using default names and copy the files to a computer with a server whose data files are installed at C:\Lotus\Domino\Data, the server files would be:

```
C:\Lotus\Domino\Data\selfcert.kyr
C:\Lotus\Domino\Data\selfcert.sth
```

3.4 Enable SSL on Domino

In the Server document in the server's Domino Directory, go to the Ports tab, then the Internet Ports tab. Under SSL settings, specify the SSL key file name (for example, selfcert.kyr). Go to the DIIOP tab. Ensure that the SSL port number is correct-it defaults to 63149. Enable the SSL port. Set Name & password and Anonymous authentication as desired.

3.5 Install the certificate on ZENworks Mobile Workspace

Once the keyring files are on the server, starting or restarting the DIIOP task generates a file named TrustedCerts.class in the Domino data directory. Copy that file to SENSE_HOME/lib.

Steps 3.2 to 3.4 has been copied form the following site:
http://blueteetech.wordpress.com/2007/08/02/configure-ssl-on-domino/

3.6 Restart the SENSE service

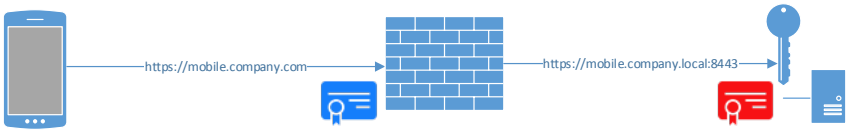
4 MIGRATE FROM HTTP TO HTTPS

When the security server has been installed and setup without SSL for convenience reason, it is wise to move to SSL when starting production. This should be done only if you have a SSL certificate that have been signed by a well-known CA.

Current infrastructure

Trusted SSL connection provided by Zenworks Mobile Workspace Server

Trusted SSL connection provided by FW or reverse proxy



4.1 Updating the keystore (Only if ZMW is not behind a reverse proxy or FW)

Even if Zenworks Mobile Workspace server has been installed without SSL connection, a SSL interface has been configured anyway with an auto generated self-signed certificate. To enable SSL with a trsuted certificate, we only need to replace it.

1. Start the application portecle provided with SENSE installer package (ZMW_INSTALLER/tools/portecle-launcher.bat)
2. Open the keystore file (ZMW_HOME/conf/keystore.jks)
3. Enter the auto generated password at installation. It can be found in the file ZMW_HOME/conf/server.xml in the attribute keystorePass of the SSL Connector.
4. Remove the auto generate certificate
5. Import the trusted key pair (Tools -> Import Key Pair)
6. Enter the password of the key pair
7. Save the keystore

4.2 Force SSL connection for mobile client

When installed without SSL, the URL Proxy set in your domain configuration starts with http:// on the port 8080. This value is read be the public store Workspace and updated if different than the one entered by the user at first installation. To force them to connect to https interface, follow the steps bellows:

1. Update the Proxy URL to https://mobile.company.com:8443/appserver/Server *
2. Wait for all users to connect. This will update the mobile client with the new URL.
3. If behind a reverse proxy or FW, remove access on http. **Warning**: If a user did not connect to the server before this step, they will be forced to reinstall the application to setup the new URL.

**The port may be different if behind a reverse proxy or a FW*