SYBASE®

An SAP® Company

Installation and Configuration Guide

Sybase Mobiliser Platform 5.1

Document ID: DC01871-01-0510-02

Last Revised: February 2013

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

Introduction

This document describes the process of installing and configuring the Sybase® Mobiliser Platform 5.1. The Mobiliser Platform consists of 3 components: Sybase Money Mobiliser (Core), Sybase Smartphone Mobiliser, and Sybase Brand Mobiliser.

- The Mobiliser Service Delivery Platform is a powerful infrastructure component in modern transaction processing suited to the needs of the mobilized world.
- The platform offers Telcos, Financial Institutions and Service Providers access to all necessary services required in transaction processing, namely authentication, authorization and accounting in one stop, and enables quick integration of any application.
- The platform is a key enabler for modern value added services offerings as the platform offers:
  - multiple communication channels (SMS, IVR, USSD, MMS, WAP, XML)
  - support for multiple languages and currencies
  - different payment and clearing protocols (e.g. ISO 8583, Edifact, SWIFT, CDR, TAP$, CIBER)

This document also provides guidance for monitoring and securing the Mobiliser Platform deployment.

Component Description

Money Mobiliser (Core)

The Mobiliser Platform is used to implement B2C solutions. Services to implement mobile payment and mobile banking services are already included. The Platform provides a framework to implement services, generate and process events, and run background jobs. The framework enforces conventions to implement/add services and logic and provides a strong but extensible security framework that is especially catered for B2C solutions. Services can be consumed by any kind of client over multiple protocols.

The mobile payment and mobile banking services are also accompanied by Web and mobile user interfaces (Smartphone Mobiliser) to cover the full customer life cycle (customer onboarding, customer self-care, customer care) and processing of financial transactions (person-2-person, merchant payments, airtime top-up, remittance). The system is completed by a built in Stored Value Account (SVA) that can be used as a standalone payment instrument.

Smartphone Mobiliser

The Mobiliser Smartphone application is a reference application framework that runs out-of-the-box with any Money Mobiliser server. The reference application comes pre-built with a set of features connected to the back-end server.

Brand Mobiliser

Brand Mobiliser is a high performance Mobile Messaging engine that can be used to quickly build and deploy messaging applications. The Brand Mobiliser user interface provides tools to visually *compose* a mobile interactive messaging application, *test* it using the built-in simulator, and *deploy* it to the processing engine for immediately ready to be consumed by the mobile consumers. The "*live*" applications can be easily modified in real time, to meet the changing business needs, and redeployed without disrupting the service availability.
More information can be found in the *Brand Mobiliser User Manual*.

Sybase Mobiliser Reporting Module (Optional)

The Sybase Mobiliser Reporting Module provides a way to utilize the integrated SAP® Crystal Reports functionality within Money Mobiliser Web portals. The option to use Mobiliser Reporting Module is not required for the Mobiliser Platform to function properly. The reports produced by Mobiliser Reporting include, and are not limited to, daily transaction, error overview, and fee/commission reports.

System Requirements

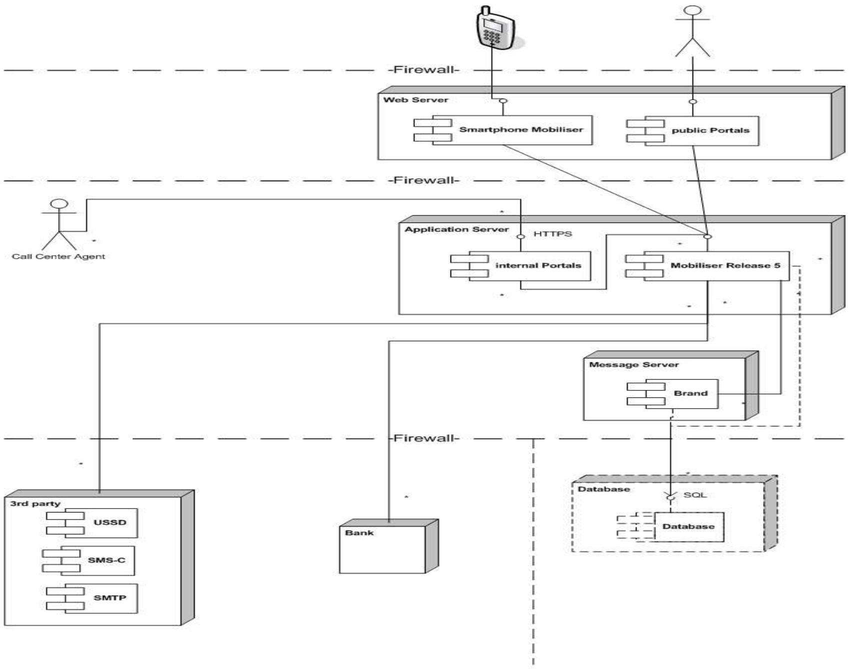
Standard Deployment Model

Each Sybase Mobiliser Platform host must meet the requirements for operating system and available disk space. The system can be installed on a single physical host or virtual machine for development or testing. In a production environment, the system can be deployed in a tiered manner to aid in administration, maintenance, and security.

See *Mobiliser Platform Supported Hardware and Software* for the most recent information on supported platforms and versions.

The standard Mobiliser Platform tiered architecture contains:

- Web layer - customer self-service portal
- Messaging layer - service access (SMS, USSD, and more)
- Application layer - Web service, back office
- Database layer



Supported Operating Systems

Operating System	Service Pack/Patch Level	CPU	JDK Version
IBM AIX 6.1		*64-bit*	*1.6 or 1.7 (latest patch)*
Red Hat Linux *EL5/POWER* *EL5/x86_64* *EL6/POWER* *EL6/x86_64*		*64-bit*	*1.6 or 1.7 (latest patch)*

Application, Messaging, and Web Tier minimum system requirements

- 2 CPU cores
- 2 GB memory
- 10 GB storage

Tip: Additional disk space, especially for the application and messaging layers, allows for more flexibility for troubleshooting purposes.

Supported Database Platforms

These database platforms have been certified and tested with Sybase® Mobiliser Platform components.

Database Platform	Brand Mobiliser	Money Mobiliser
Sybase Adaptive Server® Enterprise 15.5 or later	*No*	*Yes*
IBM DB2 9.7.4 or later	*Yes*	*Yes*
Oracle 11g Release 2	*Yes*	*Yes*

Database Tier minimum system requirements

- 2 CPU cores
- 8 GB memory
- 50 GB storage

For a vanilla implementation, the follow records require the specified amount of disk space; however, sizes reflect data file usage only and do not include other RDBMS control/system files, for example, redo, undo, temp, archive, and so on.

- Standard customer account record (4.0 KB)
- Standard authorization record (5.6 KB)

Installing the Mobiliser Platform Components

This section will describe how to set up application directories and accounts that are used to operate the Mobiliser Platform. Unless specified, directory structure, system accounts, and other such information is recommended. Please follow IT best practice or local system and security policies at all times.

- Installation also requires:
  - Internet Access
  - Sybase Product Download Center (confirm)
  - SAP Service Marketplace (confirm)

Creating Users and Groups

Use the proper command for the host operating system to create the groups and user accounts

Group	Description
sybase	*Group for Mobiliser Platform Users*

Username	Description	Shell	SSH	Group	Home	Host
Sybase	*Master Application User*	*bash*	*yes*	*sybase*	*/home/sybase*	*Web, Application, Messaging*
sap-mob	*Functional Owner*	*bash*	*yes*	*sybase*	*/home/sap-mob*	*Web, Application, Messaging*
sap-httpd	*Owner of http Server*	*nologin*	*no*	*sybase*	-	*Web*
sap-portal	*Owner of Portal Server*	*nologin*	*no*	*sybase*	-	*Web, Application*
sap-money	*Owner of OSGi Container*	*nologin*	*no*	*sybase*	-	*Application*
sap-brand	*Owner of OSGi Container*	*nologin*	*no*	*sybase*	-	*Messaging*

**/home/sybase may be referred to as {Mobiliser_Installation}*

For security reasons, it is recommended to use the *sudo* feature to restrict control and access of Mobiliser application users. As per recommendation, application users do not have a valid shell. Therefore, it is necessary to use sudo to manage an application with this user's privileges. *Sudo* also limits the commands that can be executed by a user.

Here an example for a sudoers entry:

- *sap-mob ALL=(sap-httpd) /opt/sybase/httpd/current/bin/apachectl*

Web Server		
User	act for	Command
sybase, sap-mob	*ALL=(sap-httpd)*	*ALL* *optional only: /opt/sybase/httpd/current/bin/apachectl*
sybase, sap-mob	*ALL=(sap-portal)*	*ALL* *optional only: /opt/sybase/portal/bin/catalina.sh, /opt/sybase/portal/bin/startup.sh, /opt/sybase/portal/bin/shutdown.sh*

Application Server		
User	act for	Command
sybase, sap-mob	*ALL=(sap-portal)*	*ALL* *optional only: /opt/sybase/portal/bin/catalina.sh, /opt/sybase/portal/bin/startup.sh, /opt/sybase/portal/bin/shutdown.sh*
sybase, sap-mob	*ALL=(sap-money)*	*ALL* *optional only: /opt/sybase/money/bin/mobiliser.sh, /opt/sybase/money/bin/startup.sh, /opt/sybase/money/bin/shutdown.sh*

For the database, use the default accounts as recommended by the respective User Manual.

Unpacking the Software

As the ‘sybase’ user, unpack the software into /home/sybase. This should create the following objects:

- Mobiliser Portals and pre-configured Tomcat instance (/applications/apache)
    - o *(/applications/apache/apache-tomcat-6.0.33 (Tomcat Container)*
    - o */applications/apache/com.sybase365.mobiliser.ui.web.application-5.1.0.RC1.war (WEB UI war file)*
- Container and Database scripts
    - ➢ Sybase (/applications/ase)
        - o */applications/ase/com.sybase365.mobiliser.vanilla.ase-5.1.0.RC1 (ASE Container)*
        - o */applications/ase/sql (ASE script archives)*
    - ➢ IBM (/applications/ibm)
        - o */applications/ibm/com.sybase365.mobiliser.vanilla.db2-5.1.0.RC1 (DB2 Container)*
        - o */applications/ibm/sql (IBM script archives)*
        - o */applications/ibm/create_jdbc_bundle.sh (Script to build DB2 driver jar)*
        - o */applications/ibm/db2manifest (Manifest to use with script)*
        - o */applications/ibm/MANIFEST.MF (Manifest to use with script)*
    - ➢ Oracle (/applications/oracle)
        - o */applications/oracle/com.sybase365.mobiliser.dist.oracle-5.1.0.RC1 (Oracle Container)*
        - o */applications/oracle/sql (Oracle script archives)*
        - o */applications/oracle/create_jdbc_bundle.sh (Script to build Oracle driver jar)*
        - o */applications/oracle/oraclemanifest (Manifest to use with script)*
        - o */applications/oracle/MANIFEST.MF (Manifest to use with script)*

Setting up the Database

[For all ASE 15.7 installations]
*Ensure that the page size selected, when creating the database, is 8K instead of the default value of 4K. *Note* If this setting is not set you will not be able create composite indexes more than 1250 bytes, resulting in an incomplete installation of Mobiliser 5.1 database scripts and making the overall Mobiliser 5.1 invalid.*

Using DBMaintain

The preferred way to install the database schema is by using dbmaintain. Dbmaintain can also be used to upgrade releases to a newer release. It will remember (in the database) which scripts have already been executed and only execute the new ones. If old scripts have been modified, it will not be able to do anything other than purging the DB completely. This feature can of course be disabled.

Dbmaintain is provided as an executable jar file that contains the DDL scripts (or script archive) as well as the Java classes required to execute the scripts. The location to the JDBC driver must be provided in the classpath. JDBC drivers for Oracle and DB2 databases must be downloaded from the respective websites or located within the database installation directory, while JDBC drivers for ASE databases are included in this software package.

- *The script archives are packaged as a jar files with the following names:*
    - ➢ *com.sybase365.mobiliser.vanilla.ase-5.1.0.RC1-scriptarchive-ase-upgrade-501-to-510.jar*
    - ➢ *com.sybase365.mobiliser.vanilla.ase-5.1.0.RC1-scriptarchive-ase.jar*
    - ➢ *com.sybase365.mobiliser.vanilla.db2-5.1.0.RC1-scriptarchive-db2-driverless.jar*
    - ➢ *com.sybase365.mobiliser.vanilla.db2-5.1.0.RC1-scriptarchive-db2-upgrade-500-to-510-driverless.jar*
    - ➢ *com.sybase365.mobiliser.vanilla.db2-5.1.0.RC1-scriptarchive-db2-upgrade-501-to-510-driverless.jar*
    - ➢ *com.sybase365.mobiliser.vanilla.oracle-5.1.0.RC1-scriptarchive-oracle-driverless.jar*
    - ➢ *com.sybase365.mobiliser.vanilla.oracle-5.1.0.RC1-scriptarchive-oracle-upgrade-500-to-510-driverless.jar*
    - ➢ *com.sybase365.mobiliser.vanilla.oracle-5.1.0.RC1-scriptarchive-oracle-upgrade-501-to-510-driverless.jar*

Running DBMaintain

1. Extract the Mobiliser user creation DDL script and the dbmaintain.properties files from the scriptarchive jar file:

   - *jar xvf com.sybase365.mobiliser.vanilla.oracle-<version>-scriptarchive-oracle-driverless.jar dbmaintain.properties (for Oracle, dbmaintain.properties.db2 (DB2) and dbmaintain.properties.ase (ASE))*
   - *jar -xvf com.sybase365.mobiliser.vanilla.oracle-<version>-scriptarchive-oracle-driverless.jar sql/001_MONEY/001_SETUP/001_MONEY_drop_and_create_user.DDL*

2. Creating the schema:
   a. Manually execute the following script as an administrative database user:
      - *sql/001_MONEY/001_SETUP/001_MONEY_drop_and_create_user.DDL*

   b. The purpose of running this script is to create the database schema that will hold all data/metadata, used by the Mobiliser container; this script also creates and assigns required roles/object owners in the database.
3. Modify the access and connection information in the dbmaintain.properties file (URL, user, password, etc.):
   a. Username and password can also be provided on the command line
   b. database.driverLocation=*</path/to/databaseDriver.jar>* must be provided when using the "driverless.jar" version of the installer
4. Set the dbmaintain installation mode (Production/Development):
   a. INSTALL: dbMaintainer.fromScratch.enabled – if this is set to "true", dbmaintain can delete all objects belonging to the specified schema and recreate everything from scratch (after command line approval). Always set this parameter to "false" in productive environments! Irregular script updates (in case of an update) must be resolved by the developer!
   b. DEVELOPMENT: dbMaintainer.alwaysDrop – Indicates if the db should be purged no matter if there were changes or not (for dev and test system use)
5. Please also read through the remaining settings in the property file (all are documented) and configure them according to your needs.

6. *Note for ASE 15.7 Installations* After executing the DBMaintain script for an ASE 15.7 database, you must enable the functionality group of the database with the following command:

sp_configure 'enable functionality group', 1

- *Here is a summary of what the functionality group change does for the database:*

  - *Enable permissive unicode for the database character set*
  - *Enables 'quoted identifier enhancements*
  - *Enables 'select for update' syntax when performing DB queries and updates*
  - *Enables streamlined dynamic SQL, that is useful for internal QP optimizations*
  - *Enables inline default sharing, which handles large numbers of defaults*

These are the supported command line parameters:

Parameter	Description
-c <arg>	*dbmaintain.properties configuration file location (if this is not specified the dbmaintain.properties file is expected to be in the current directory, otherwise in "/pbx_u01/conf/db/dbmaintain.properties")*
-clean	*cleans the db, purges the current contents, deletes all objects in the schema.*
-f <arg>	*specify external scriptarchive location e.g. archiveWithSqls.jar*
-h	*display help*
-preview	*Does nothing but to show what would be done and writes a delta file with all new changes to the tmp directory for review.*
-p <arg>	*dbPassword*

Parameter	Description
-u <arg>	*dbUsername*

- *Standard command line to run the dbmaintain tool:*
    - ➢ *java –classpath jconnect-osgi-7.0.5.jar -jar com.sybase365.mobiliser.vanilla.oracle-<version>-scriptarchive-ase-driverless.jar –c dbmaintain.properties.ase*

Creating Required Database Hash Values and Database Updates

For Mobiliser credentials:

The universal Mobiliser user, within the database, requires an encrypted hash in order for the Mobiliser container to function properly. The hashes are created using one of the tools packaged with Mobiliser; the tool is called com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.SP01-CLIPasswordEncoderClient.jar, and is located in the {MOBILISER_HOME}/tools directory.

Execute the com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.SP01-CLIPasswordEncoderClient.jar file by typing the following command:

- java –jar com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.SP01-CLIPasswordEncoderClient.jar
- Choose the desired encryption method
- Enter the plain text password that you would like to create the hash of
- Enter the salt for the universal mobiliser user. (This value will be 100)
- Update the hash value in the database by running the following statement on the database
    - ➢ UPDATE "MOBR5"."MOB_CUSTOMERS_CREDENTIALS" SET STR_CREDENTIAL = '<Hash Value>' WHERE ID_CUSTOMER = '100'
    - ➢ Note The SQL script specified above is for Oracle databases, SQL syntax may change for DB2 and ASE databases
- Update the creation date for the universal mobiliser user and sysmgr user by running the following statements on the database:
    - ➢ UPDATE "MOBR5"."MOB_CUSTOMERS_CREDENTIALS" SET DAT_CREATION = TO_TIMESTAMP('<Current Date> 12.00.00.000000000 AM', 'DD-MON-RR HH.MI.SS.FF AM') WHERE ID_CUSTOMER = '100'
    - ➢ UPDATE "MOBR5"."MOB_CUSTOMERS_CREDENTIALS" SET DAT_CREATION = TO_TIMESTAMP('<Current Date> 12.00.00.000000000 AM', 'DD-MON-RR HH.MI.SS.FF AM') WHERE ID_CUSTOMER = '106'
    - ➢ Note The SQL scripts specified above are for Oracle databases, SQL syntax may change for DB2 and ASE databases

For preferences:

Mobiliser preferences are accessed by the Mobilser WebUI via a successful Money Mobiliser installation. The preferences entries in the database also require created hash entries. The hashes are created using another encryption tool packaged with Mobiliser; the tool is called com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.SP01-CLIEncrypterClient.jar. The com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.SP01-CLIEncrypterClient.jar tool requires arguments in order to be used correctly (Please reference Security Settings: JDK and Configuration files section for details on how to use this tool).

Once the hash has been created successfully update the database with the following SQL statements in order to update the preferences:

- UPDATE "MOBR5"."MOB_PREFERENCES" SET STR_VALUE = '{AES-128-PBKDF2}<created hash value>' WHERE ID_PREFERENCE = '402'
- UPDATE "MOBR5"."MOB_PREFERENCES" SET STR_VALUE = '{AES-128-PBKDF2}<created hash value>' WHERE ID_PREFERENCE = '426'
- Note The SQL scripts specified above are for Oracle databases, SQL syntax may change for DB2 and ASE databases

Sybase Brand Mobiliser Installation and Configuration

For installation and configuration information for Brand Mobiliser, see the *Sybase Brand Mobiliser User Manual* on Sybase Product Documentation:

Click here to view the Sybase Brand Mobiliser documentation set.

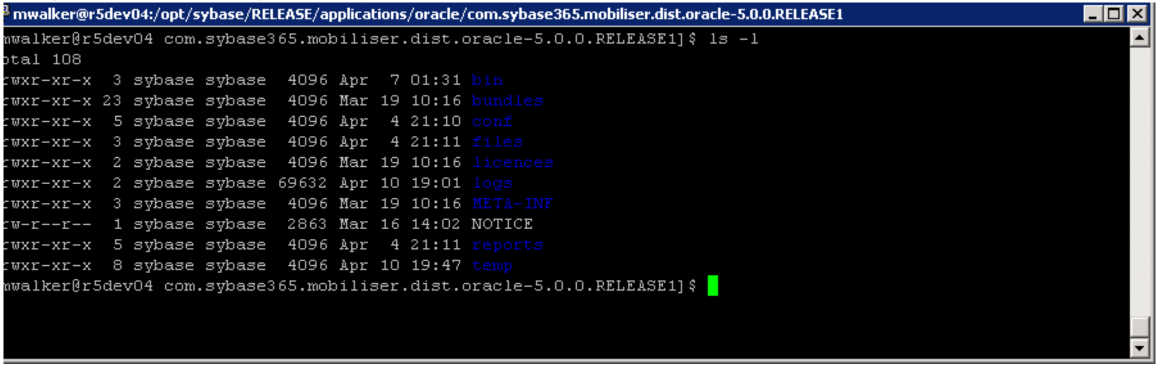
Initializing the Mobiliser Platform Container

The Mobiliser Platform container comes preconfigured and can essentially be unpacked and started up. To perform minimal functional testing, the network settings (for Web portals, database, etc) must be updated. There are also a few 3rd party components that must be downloaded and installed. For this reason, it is ideal to allow internet access during installation.

Server Setup: Deploying the Container

The following procedure is used to setup and initialize the Mobiliser core server.

1. Navigate to the {Mobiliser_Installation}/applications/<target_database> directory
2. Unpack the com.sybase365.mobiliser.dist.<target_database>-xxx-dist.zip file. This action will create a com.sybase365.mobiliser.dist.<target_database>-xxx directory
3. Copy the com.sybase365.mobiliser.dist.<target_database>-xxx directory to /opt/sybase/ to create the {MOBILISER_HOME} directory



mwalker@r5dev04:/opt/sybase/RELEASE/applications/oracle/com.sybase365.mobiliser.dist.oracle-5.0.0.RELEASE1

```
mwalker@r5dev04 com.sybase365.mobiliser.dist.oracle-5.0.0.RELEASE1]$ ls -l
otal 108
rwxr-xr-x  3 sybase sybase  4096 Apr  7 01:31 bin
rwxr-xr-x 23 sybase sybase  4096 Mar 19 10:16 bundles
rwxr-xr-x  5 sybase sybase  4096 Apr  4 21:10 conf
rwxr-xr-x  3 sybase sybase  4096 Apr  4 21:11 files
rwxr-xr-x  2 sybase sybase  4096 Mar 19 10:16 licences
rwxr-xr-x  2 sybase sybase 69632 Apr 10 19:01 logs
rwxr-xr-x  3 sybase sybase  4096 Mar 19 10:16 META-INF
rw-r--r--  1 sybase sybase  2863 Mar 16 14:02 NOTICE
rwxr-xr-x  5 sybase sybase  4096 Apr  4 21:11 reports
rwxr-xr-x  8 sybase sybase  4096 Apr 10 19:47 temp
mwalker@r5dev04 com.sybase365.mobiliser.dist.oracle-5.0.0.RELEASE1]$
```

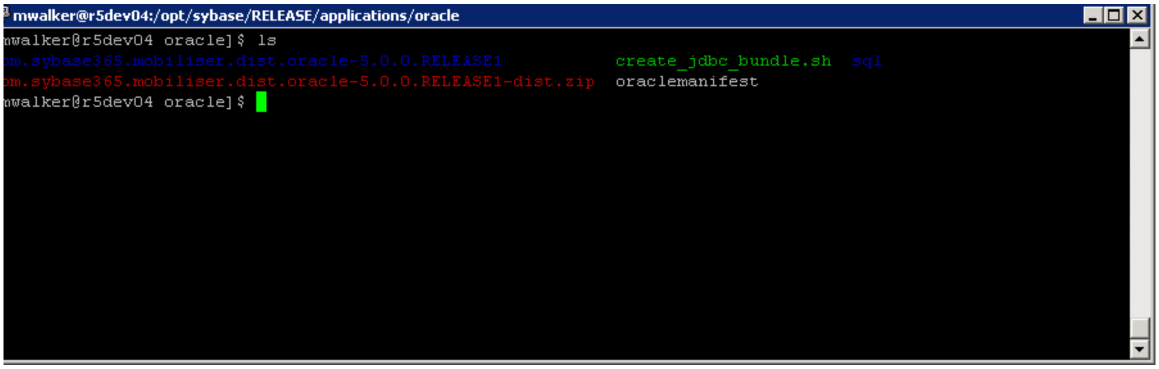
Server Setup: Third Party Software Installation

There are a variety of required third party jar files that are required for normal operation. This software can be obtained from the respective vendors and deployed directly onto the OSGi container.

JDBC Driver Bundle

The JDBC jar for the respective database provider must be packaged in an OSGi bundle. Once the JDBC driver is available on the system (download from database provider), use the 'create_jdbc_bundle.sh' utility to create the necessary bundle.

1. Navigate to the {MOBILISER_INSTALLATION}/applications/oracle directory. (For DB2 database configurations navigate to {MOBILISER_HOME}/applications/ibm



```
mwalker@r5dev04 oracle]$ ls
om.sybase365.mobiliser.dist.oracle-5.0.0.RELEASE1           create_jdbc_bundle.sh  sql
om.sybase365.mobiliser.dist.oracle-5.0.0.RELEASE1-dist.zip  oraclemanifest
mwalker@r5dev04 oracle]$ 
```

2. Download an Oracle or DB2 JDBC driver that is compatible with the JRE that was installed onto your system (http://www.oracle.com) or (http://www.ibm.com)
3. Run ./create_jdbc_bundle.sh script using (for ex. Oraclemanifest) and JDBC jar as input variables
   - *ex: ./create_jdbc_bundle.sh oraclemanifest ojdbc6.jar (Oracle)*
   - *ex: ./create_jdbc_bundle.sh db2manifest db2jcc4.jar (DB2)*
4. Rename created jar file bundle_<name of jdbc> to oracle-jdbc-osgi_11.2.0.2.0-1.0.1.jar (com.sybase365.com.ibm.db2jcc4-9.7.4.jar for DB2)
5. Copy oracle-jdbc-osgi_11.2.0.2.0-1.0.1.jar or com.sybase365.com.ibm.db2jcc4-9.7.4.jar to {MOBILISER_HOME}/bundles/07-frameworks

This completes the database configuration

Springsource (http://www.springsource.org)
- Download and copy into {MOBILISER_HOME}/bundles/07-frameworks directory:
  - com.springsource.org.jgroups-2.2.8.jar

Springsource (http://www.springsource.org)
- Download and copy into {MOBILISER_HOME}/bundles/16-framework-reports directory:
  - com.springsource.javax.media.jai.codec-1.1.3.jar
  - com.springsource.javax.media.jai.core-1.1.3.jar

Sybase Mobiliser Reporting Module 5.1 (Available at Sybase Product Download Center)
- Download and copy into {MOBILISER_HOME}/bundles/17-crystalreports directory:
  - com.businessobjects.cvom_12.2.212.1346-1.0.1.jar
  - com.businessobjects.foundation.logging_12.2.212.1346-1.0.1.jar
  - com.businessobjects.reports.jdbinterface_12.2.212.1346-1.0.1.jar
  - com.businessobjects.visualization.pfjgraphics_12.2.212.1346-1.0.1.jar
  - com.crystaldecisions.common.keycode_12.2.212.1346-1.0.1.jar
  - com.crystaldecisions.reports.runtime_12.2.212.1346-1.0.1.jar

Sybase Mobiliser Reporting Module 5.1 (Available at Sybase Product Download Center)
- Download and copy into {MOBILISER_HOME}/bundles/20-mobiliser-reports-services directory:
  - com.sybase365.mobiliser.util.report.crystalreports.impl-5.1.0.RELEASE.jar
  - com.sybase365.mobiliser.util.report.crystalreports.util-5.1.0.RELEASE.jar
  - com.sybase365.mobiliser.util.report.crystalreports.web-5.1.0.RELEASE.war
  - com.sybase365.mobiliser.util.report.watcher-5.1.0.RELEASE.jar

Sybase Mobiliser Reporting Module 5.1 (Available at Sybase Product Download Center)
- Download and copy into {MOBILSER_HOME}/bundles/18-report-fragments directory:
  - com.azalea.ufl.barcode_1.0-1.0.1.jar

Security Settings: JDK and Configuration Files

Security settings that are managed via configuration files require a restart of the container to take effect.

Enabling Strong Encryption in JDK

Per default a JDK installation only supports AES encryption with 128 bit keylength, which is considered to be insecure. To enable strong cryptography on your JVM, please download the 'JCE unlimited strength jurisdiction policy file' from the vendor of your JDK. For Oracle and IBM JDKs, this will provide two files:

- *local_policy.jar*
- *US_export_policy.jar*

Replace these files in your JDK installation directory at /jre/lib/security. Refer to the accompanying installation instructions for JVM-specific hints.

Encryption in Configuration Files

All configuration files in the ./conf/cfgbackup folder support encrypted configuration values. The master key for encryption of these values is stored in the ./conf/system.properties file:

- *com.sybase365.arf.container.system.decryptionkey=<PASSWORD>*
- *com.sybase365.arf.container.system.decryptionkeylength=<128|256>*

The 256 bit key length will only work if you replaced the JVM's encryption policy files. Any configuration value in the property files at ./conf/cfgbackup can be encrypted. The decryption of these values will happen transparently to the Mobiliser application (using the key configured in ./conf/system.properties). This also means that inside the Mobiliser container, encrypted values will be visible in clear text (this includes the Web console). To indicate that a value is encrypted, it must be prefixed with '{enc}' (without quotes). An entry must look like:

- *<KEY>={enc}<ENCRYPTED-VALUE>*

If you want to disable encryption support in a single configuration file explicitly, simply add this key/value pair into that particular property file:

- *com.sybase365.arf.container.system.configadmin.decryptproperties=false*

We use AES/CBC/PKCS5Padding encryption; the encrypted value is expected to be base64 encoded, the first 16 bytes are interpreted as the initialization vector (IV). The encryption key is derived from the password using PBKDF2HmacWithSHA1 hashing with the static salt {97,101,105,111,117,85,79,73,69} and 65536 iterations. The Mobiliser container includes a executable JAR in the ./tools folder to encrypt configuration values according to this specification. Simply run:

- *./tools> java -jar com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.RELEASE-CLIEncrypterClient.jar <KEY> <TEXT> [<KEYLENGTH>]*

Note In Mobiliser Platform 5.1 installations, this tool requires the installation of X Windows in the system environment in order to execute properly; however, for Mobiliser Platform 5.1 SP01 installations, this tool can be run without X Windows capability. The <KEY> must match the configured key from ./conf/system.properties, <KEYLENGTH> is optional and defaults to 128 bits - 256 will only work if you've updated your Java encryption policy file. *Note* If using this tool to create hash values for Preferences, make note of the <key> value used to create the hash because it will need to be used in future configuration of the context.xml (JDNI Entry) specified in the next section.

Encryption in Mobiliser Platform Preferences

Preferences configuration values can be stored encrypted in the MOB_PREFERENCES table. Encrypted preferences values must be prefixed with the used encryption algorithm, i.e.:

- *{AES-128-PBKDF2}<ENCRYPTED-VALUE>*
- *{AES-256-PBKDF2}<ENCRYPTED-VALUE>*

Decryption happens transparently to the using application; however, the developer using a particular preferences node must enable encryption-support for this node explicitly. Hence, unlike configuration property file encryption, this will only work if the developer has set it up like that.

For the Mobiliser Platform container, the en/decryption key is configured in ./conf/cfgbackup/com.sybase365.mobiliser.util.prefs.encryption.aes.properties:

- *preferencesEncryptionKey=<KEY>*

For applications using remote access to preferences, the en/decryption is configured through on of these (descending priority):

- *system property: -Dcom.sybase365.mobiliser.money.prefs.secret=<KEY>*
- *JNDI entry: <Environment description="Preferences key" name="prefs/secret" type="java.lang.String" value="<KEY>" /> (usually configured in <TOMCAT_HOME>/conf/server.xml)*
- *property file on class path: sybase-preferences.properties with this line: encryption-secret=<KEY>*

We use AES/CBC/PKCS5Padding encryption; the encrypted value is expected to be base64 encoded, the first 16 bytes are interpreted as the initialization vector (IV). The encryption key is derived from the password using PBKDF2HmacWithSHA1 hashing with the static salt {97,101,105,111,117,85,79,73,69} and 65536 iterations. The Mobiliser Platform container includes a executable JAR in the ./tools folder to encrypt configuration values according to this specification. Simply run:

- *./tools> java -jar com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.RELEASE-CLIEncrypterClient.jar <KEY> <TEXT> [<KEYLENGTH>]*

Note In Mobiliser Platform 5.1 installations, this tool requires the installation of X Windows in the system environment in order to execute properly; however, for Mobiliser Platform 5.1 SP01 installations, this tool can be run without X Windows capability. The <KEY> must match the configured key from one of the configuration places mentioned above, <KEYLENGTH> is optional and defaults to 128 bits - 256 will only work if you've updated your Java encryption policy file.
Alternatively, once your system is up and running you can also log in to the dashboard (per default with the 'opsmgr' user), and change preferences through the UI. Remember to use the consistent encryption key there as well.

Security Settings: Database and Preferences

Security settings which are managed via database and preferences do not require a restart of the container to take effect.

Hashing Customer Credentials

Any customer (consumer, merchant, agent, system user) credentials are stored hashed in MOB_CUSTOMER_CREDENTIALS. Mobiliser Platform supports using different hashing algorithms. The STR_CREDENTIAL is always prefixed with the used hashing algorithm in curly brackets, ie.:

- *{<HASH-ALGORITH>}<HASHVALUE>*

Configuration of hashing algorithms is controlled through preferences. Update the following node:

- *com.sybase365.mobiliser.money.businesslogic.umgr.impl.SmartPasswordEncoder*

Key	Description
Algorithms	*comma-separated list of supported hashing algorithms; the default list is SHA,SHA-256,SHA-512,SHA-512:1,SHA-512:10000,PBKDF2WithHmacSHA1:10000,BCRYPT:10,SSHA-512:10000,SPBKDF2WithHmacSHA1:10000*
encodeAlgorithm	*the algorithm to use for storing and encoding new credentials; default is SSHA-512:10000*
defaultAlgorithm	*the algorithm to use for credential validation if the algorithm is not specified with the stored credential; default is SHA*

You can change these default configurations within certain boundaries. You may only add actual new hashing algorithms when they are provided through JCE (i.e., they either come with your JDK or you've installed an extension like bouncycastle into your JDK), however, you can freely change the number of iterations / strength (which is the numeric value after the colon) to either increase performance or security if required. Be aware that BCrypt is decreasing performance tremendously, so only use that if this is a strong security requirement.

Mobiliser Platform also supports an upgrade of the used hash algorithm, i.e. each time a customer's credential gets checked, Mobiliser Platform can also validate if the used hashing algorithm is configured to be updated with the configured 'encodeAlgorithm'. Update the following node:

- *com.sybase365.mobiliser.money.businesslogic.umgr.impl.SecurityLogic:*

Key	Description
hashUpgradePattern	*this is a Java regex pattern; if this is <null>, no password upgrade will be performed, otherwise any hashed password that matches this pattern will be re-hashed using the current 'encodeAlgorithm'; per default this value is not configured.*

The actual value stored in STR_CREDENTIAL depends on the used hashing algorithm. All hash values are base64 encoded. For all algorithms, which do not use random salts, the customer id is used as the salt value. Random salts are always 16 byte.

- *SHA: BASE64(HASH(<SALT>|<HASH>))*
- *SSHA: BASE64(<SALT>HASH(<SALT><HASH>))*
- *PBKDF2: BASE64(HASH(<SALT>,<HASH>))*
- *SPBKDF2: BASE64(<SALT>HASH(<SALT>,<HASH>))*
- *BCrypt: $2a$<ROUNDS#>$BASE64(<SALT><HASH>)*

Mobiliser Platform comes with a Java executable to compute hash values, simply run:

- *./tools> java-jar com.sybase365.mobiliser.vanilla.cli-tools-5.1.0.RELEASE-CLIPasswordEncoderClient.jar*

Security Settings: Creating a KeyStore

The Vanilla Mobiliser Platform installation uses asymmetric encryption to secure credit card and bank account information in the front-end and decrypt it again in a dummy payment handler implementation in the back-end for credit card payments. Follow these steps to create a keystore for public and one holding the private keys.

1. Create the first key pair. You can use different names, but have to use them in the appropriate places below as well, also remember the passwords you choose for keystore password and key password for later configuration:
    - *keytool -genkey -alilas mobiliser_card -keyalg RSA -keystore mobiliser.jks -keysize 2048*

2. Export the public key:
   - *keytool -export -alias mobiliser_card -file mobiliser_card.crt -keystore mobiliser.jks*
3. Import the certificate into a new separate keystore:
   - *keytool -import -alias mobiliser_card -file mobiliser_card.crt -keystore mobiliser_pub.jks*
4. Now, the same steps again for a second key pair:
   - *keytool -genkey -alias mobiliser_bank -keyalg RSA -keystore mobiliser.jks -keysize 2048*
   - *keytool -export -alias mobiliser_bank -file mobiliser_bank.crt -keystore mobiliser.jks*
   - *keytool -import -alias mobiliser_bank -file mobiliser_bank.crt -keystore mobiliser_pub.jks*

Depending on the project, there might be additional keys required, or none at all. Above description reflects the keystore creation process for the Vanilla Mobiliser Platform installation.

Mobile Web and Smartphone Client Installation/Configuration

Mobile Web

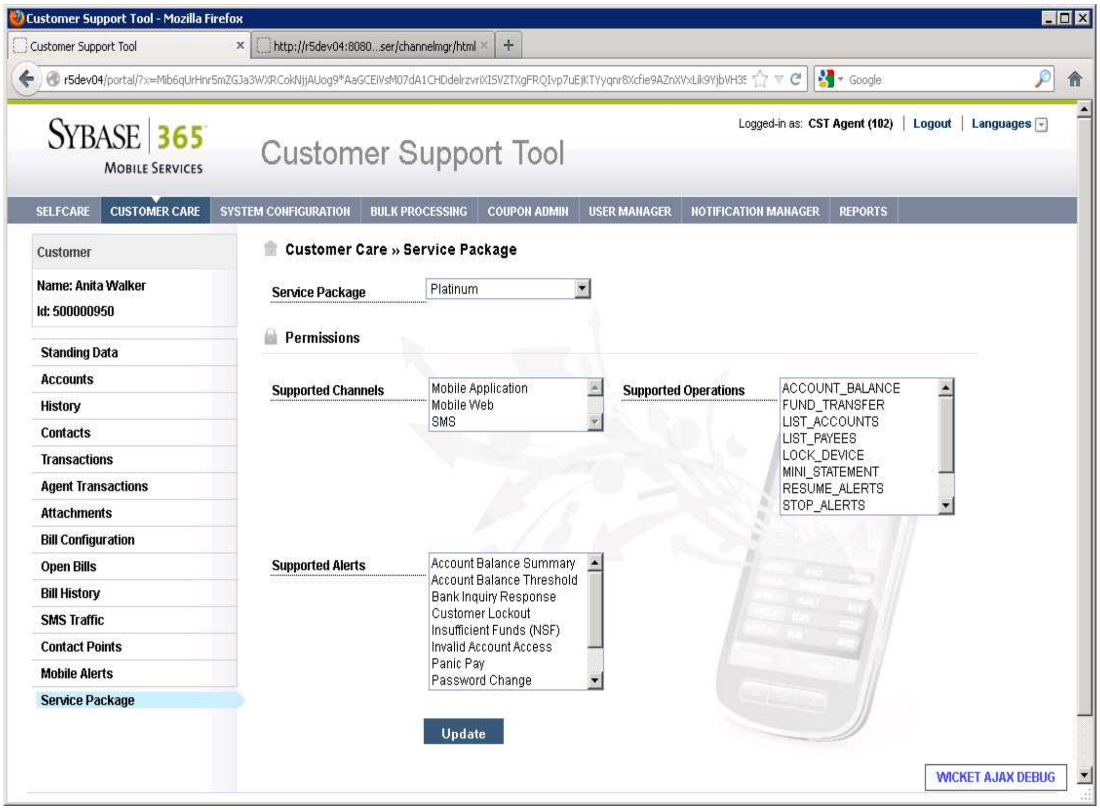
Mobile Web is intended to be installed as an extension to the current webUI container, referred to earlier in this document as {TOMCAT_HOME}. In order to install Mobile Web follow these instructions:

1. If currently running, stop the Web UI container using the {TOMCAT_HOME}/bin/shutdown.sh script.
2. Navigate to {TOMCAT_HOME}/webapps directory and create a directory named "mobileweb"
   a. mkdir mobileweb
3. Download the Smartphone Mobiliser package and unzip it in a desired location. The directory created as a result of the unpacking is SmartphoneMobiliser-5.1.RELEASE; this directory will be known as {SMARTPHONE_HOME}
4. Navigate to {SMARTPHONE_HOME}/WebApp/Mobiliser/trunk directory. Copy the ENTIRE contents of the folder to the {TOMCAT_HOME}/webapps/mobileweb directory created in step 2.
5. Open the SY_Data_Objects.js located at {TOMCAT_HOME}/webapps/mobileweb/mobiliser, and configure the following section to specify the proxy port and IP address of the system that {MOBILISER_HOME} resides, while leaving other values the same:

```
function Setting() {
   this.protocol = 'http://';
   this.ipaddress = '216.207.70.198';
   this.port = '80';
   this.wsname = 'mobiliser/rest/smartphone';
   this.jsonws = 'mobiliser/rest/smartphone';
   this.origin = "MAPP";
}
```

6. Make sure that the reverse proxy settings specified in the Proxy Setup section have been completed
7. Initialize the webUI container using the {TOMCAT_HOME}/bin/startup.sh script. Mobileweb login page will be available http://<system>:<port>/mobileweb.

- By default, only MBanking customers have access to login to mobileweb portal, after a vanilla install. If you attempt to login to the Mobileweb portal as a Money customer you will receive an error message after a lengthy timeout. In order to allow an MBanking customer to access both mobilie Web and Smartphone client, they must be assigned to the 'Premium' or 'Platinum' service tier within the Customer Support Tool (CST)
  - Steps to assign consumer tier
    - Login to WebUI as cstfull administrative user
    - Click Customer Care then Find Customer
    - Enter data to search for desired customer then click on customer Id number
    - Select 'Service Package' on left side of screen



Name: Anita Walker
Id: 500000950

Service Package: Platinum

Supported Channels: Mobile Application, Mobile Web, SMS

Supported Operations: ACCOUNT_BALANCE, FUND_TRANSFER, LIST_ACCOUNTS, LIST_PAYEES, LOCK_DEVICE, MINI_STATEMENT, RESUME_ALERTS, STOP_ALERTS

Supported Alerts: Account Balance Summary, Account Balance Threshold, Bank Inquiry Response, Customer Lockout, Insufficient Funds (NSF), Invalid Account Access, Panic Pay, Password Change

- Choose the desired Service Package tier from the dropdown list. The default tier for MBanking consumers is ‘Basic’, which only provides access to Mobileweb login.

Smartphone Mobiliser Client

The Smartphone Mobiliser clients for the various mobile devices are packaged as source code and require compilation after customer customization has been performed to the source code. Customization to the source code is not required for the source code to compile successfully, but the client will contain default SAP branding.

The source code for all devices is located at {SMARTPHONE_HOME}/client

Provisioning the finalized application after development is usually done through the official distribution marketplace for each mobile platform:

- iPhone, iPad –App Store
- BlackBerry – BlackBerry App World
- Android – Android Market, Google Play Store

Follow the instructions and policy for each of these distribution channels for provisioning your application through that specific channel. More information can be found in *Developer Guide: Smartphone Mobiliser Applications*:

http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc01866.0510/html/title.htm

Security Settings: First Installation Checklist

There are a couple of pre-configured values that you want to change on a fresh install for security reasons. For some of these steps, please consult the description above on the details how an where to change things.
The system is installed with an invalid password for the user “mobiliser”. It is required to set a new password for this user and to also configure the password in the preferences (see below).

1. Change the master password for configuration file encryption in ./conf/system.properties.   This step is optional and is only required if password encryption is needed in Mobiliser Platform configuration.
2. Update configuration property files. The Vanilla distribution comes with only database passwords pre-encrypted, change them according to your DB password, and use the newly configured master password. The two files holding database passwords are:
    - *com.sybase365.mobiliser.framework.persistence.jdbc.<bonecp|c3p0>.pool.properties*
    - *com.sybase365.mobiliser.util.report.crystalreports.properties.*

**Note* for ASE 15.7 Installations only:*

- Uncomment the following lines in the com.sybase365.mobiliser.framework.event.scheduler.quartz.properties file

** #jobStore.selectWithLockSQL=SELECT * FROM {0}LOCKS WHERE LOCK_NAME = ? FOR UPDATE*
** #jobStore.lockHandlerClass=*

- Uncomment the following line in the com.sybase365.mobiliser.framework.persistence.hibernate.sessionfactory.properties file

**#hibernate.dialect=com.sybase365.mobiliser.framework.persistence.hibernate.ase.MobiliserSybase157Dialect*

3. Change the passwords in MOB_CUSTOMER_CREDENTIALS for these preconfigured users:
    - *[REQUIRED] #100: mobiliser (Internal Mobiliser user for service calls from Web UI)*
    - *#101: usermgr (User Manager portal login)*
    - *#102: cstfull (CST Agent portal login)*
    - *#103: selfcare Selfcare and Signup*
    - *#104: opsmgr (Operations Manager portal login)*
    - *#105: notifmgr (Notification Manager portal login)*
    - *#106: sysmgr (System Manager Felix Web Console login)*
    - *#203: Headquarter (Money Headquarter portal login)*

    If you choose not to update the passwords for all users, with the exception of “mobiliser”, the default password is ‘secret’ and you will be asked to change the password upon first login to the Web UI.

4. Set a new preferences master password in the Web UI context.xml as well as the container property file (you may opt to store this password encrypted itself in the property file for local access). Please refer to the Encryption in Mobiliser preferences section and reference the JNDI entry to perform this step. This step is REQUIRED if preferences hashes are created with any key that differs from the default “paybox”.
5. Update preferences configuration which hold 'mobiliser' user password (remember to use your new preferences master key for encryption. This step can be skipped if the database was updated with the scripts specified in the Creating required Database Hash Values and required Database Updates (for preferences) section. The Vanilla installation has these two configuration nodes; in order to reach these nodes you will need to log into the webUI as the opsmgr user, and select ‘Preferences’ on the left side of the scrren. Update the 2 preference keys 'mobiliser.password' located in the mobr5.mob_preferences table (str_name column)::
    - */presentationlayer/system/com/sybase365/mobiliser/web/util/Configuration/*
    - */presentationlayer/system/com/sybase365/mobiliser/web/util/DynamicServiceConfiguration/*

6. Create a new pair of keystores, place the public keystore in the Web portal's WEB-INF/classes and the private keystore in the Mobiliser Platform container's ./conf/keys. Update the preferences configuration for the new keystore:
    - *Node: /presentationlayer/system/com/sybase365/mobiliser/web/util/Configuration/*
        - *Property: bankAccKeyAlias - the key alias for the public key to be used for bank account encryption; default: mobiliser_bank*
        - *Property: creditCardKeyAlias - the key alias for the public key to be used for card number encryption; default: mobiliser_card*
        - *Property: keyStorePw - the password for the public key store*
        - *Property: publicKeyStore - the public key store's name; default: mobiliser_pub.jks*
    - *Node: /businesslayer/com/sybase365/mobiliser/money/businesslogic/payment/handlers/card/impl/DummyCardPaymentHandler/*
        - *Property: key.store - the private key store's name;*
          default: ${mobiliser.home}/conf/keys/mobiliser.jks
        - *Property: key.store.password - the private key store's password*
        - *Property: key.alias - the alias for the private key to be used for card decryption;*
          default: mobiliser_card
        - *Property: key.password - the private key password*
    - *Node: /businesslayer/com/sybase365/mobiliser/mbanking/businesslogic/openbank/api/OpenBankConfiguration/*
        - *Property: key.alias - the private key to be used for bank decryption; default: mobiliser_bank*
        - *Property: key.password - the private key password*
        - *Property: key.store - the private key store's name;*
          default: ${mobiliser.home}/conf/keys/mobiliser.jks
        - *Property: key.store.password - the private key store's password*

7. If Mobileweb and/or Smartphone access is necessary for your Mobiliser Platform installation please follow the steps provided in the Mobileweb & Smartphone Client Installation/Configuration section.

System Hardening

As stated above, there are certain configuration files on the file system that contain sensitive information (such as keys used for encryption for example). Access to those files cannot be monitored or controlled from the Mobiliser Platform application and are therefore subject to OS level system hardening. Access must be limited to the user who is used to run the respective server and all read and write access should be logged. The relevant files and directories are:

- {MOBILISER_HOME}/conf/
- {TOMCAT_HOME}/conf/

The user used for starting the servers (user sybase) does not require any elevated privileges (e.g. super user, sudoers list).

Web / Jetty

You can configure the HTTP Port and other settings regarding the build in Jetty HTTP server in the file

- *{MOBILISER_HOME}/conf/jetty.xml*

You can also configure SSL (keystore) and various other settings (DoS / QoS filters). Please refer to

- *http://wiki.eclipse.org/Jetty/Reference/jetty.xml_syntax*
- *http://wiki.eclipse.org/Jetty/Howto/Configure_SSL*

Logging

Logging is configured in

- *{MOBILISER_HOME}/conf/org.ops4j.pax.logging.properties*

It is a standard log4j configuration file. For details on configuration please refer to:

- *http://logging.apache.org/log4j/1.2/manual.html*

Mobiliser Platform has its own log appender. This has two changes to the default daily rolling file appender:

- *The context name (last part of the URL when a service is called) is added to the name of the log file*
- *The "conversationId" which is part of each MobiliserReqeust is included in each line of the log file that deals with handling the corresponding request*

To enable request / response tracing, update the following values:

- *log4j.logger.com.sybase365.mobiliser.framework.service.jsonaudit.JsonAuditManager.log=TRACE, JSON*
- *log4j.additivity.com.sybase365.mobiliser.framework.service.jsonaudit.JsonAuditManager.log=true*

It will log all requests and responses in JSON still into the file json.log (configurable) indepdendently of the original protocol used (SOAP, plain XML, JSON). Sensitive information (PINs, passwords, etc) is masked.

Database Configuration

The database coordinates must be configured in two separate files (one of them is only used for the reporting framework):

- *{MOBILISER_HOME}/conf/cfgbackup*
  - *com.sybase365.mobiliser.framework.persistence.jdbc.bonecp.pool.properties*
  - *com.sybase365.mobiliser.util.report.crystalreports.properties*

In both files you need to make sure that the following parameters are set correct:

- *jdbcUrl=jdbc:oracle:thin:@localhost:1521:orcl (Oracle example, may vary slightly for DB2 and ASE)*
-
- *username=mobr5*
- *password={enc}nsoVN/2Kv4askDeZiY+DH8KYDseo0Jd5C8CJNlKpGIA=*

Refer to the previous section to learn how to encrypt passwords (and other configuration data).

The other parameters can influence the performance of the system.
The parameters you might want to check are:

- *maxConnectionsPerPartition=5*
- *partitionCount=2*

The product of these two values is the maximum number of parallel connections to the database. All other parameters should only be changed if you know exactly what you are doing.

Virus Protection

SAP NetWeaver VCA

Mobiliser Platform 5.1 introduces the SAP NetWeaver Virus Scan Adapter that scans all files upload to the mobiliser platform via Web services. The Virus Scan Adaptor uses plug in to connect to various virus scan engines that are used to scan the binary data. Please find details here:

- *http://help.sap.com/saphelp_nw04/helpdata/EN/ca/7cb340be761b07e10000000a155106/frameset.htm*

Installation

1. Install/copy the NetWeaver Virus Scan adapter for your Virus Scanner. This is provided by most Virus Scan vendors.
2. The NW-VSI integration bundle comes with a graphical configuration and test GUI. This is part of the vsi bundle

   ➢ *{$MOBILISER_HOME}/bundles/07-frameworks/com.sap.security.vsi${version}.jar.*

3. Start the gui:

   ➢ *$>java –jar $MOBILISER_HOME/bundles/07-frameworks/com.sap.security.vsi${version}.jar*
   ➢ *Test the connection with the EICAR test pattern and mark the provides as default provider. The mobiliser engine will always use the default provider only.*

4. Open the mobiliser configuration file:

   ➢ *${mobiliser_home}/conf/cfgbackup/com.sybase365.mobiliser.framework.vsi.properties and vsi.properties*
   ➢ *Copy all lines from the vsi.properties file and replace the similar ones in the mobiliser configuration file.*

5. Restart the mobiliser bundle (or the complete container) and examine the mobiliser.log file. Please make sure that there is no WARN entry like:

```
2012-08-28 08:22:10,768 [aims-init-10] WARN com.sybase365.mobiliser.framework.vscan.impl.VScanImpl - Cannot initialize
Virus Scan Service. The following service exception occured: Virus scan provider VSA_DEFAULT does not exist.
2012-08-28 08:22:10,890 [aims-init-10] INFO com.sybase365.mobiliser.framework.vscan.impl.VScanImpl - No virus scan will be performed
```

Clam AV

One widely used virus scan engine on Unix systems is ClamAV and you can use the ClamSAP library to connect the Virus Scan Adapter with the ClamAV engine. This document lists the mandatory steps to install and configure the mobiliser 5.1 virus scan adapter with ClamAV on a Linux Server.

Installation

1. The mobiliser 5.1 virus scan adapter with ClamAV requires 3 packages:
   a. ClamAV virus scan engine
   b. ClamAV development package
   c. libclamsap
2. The first two packages are usually available via the Linux distributor, while libclamsap may not. But you can still download the library from http://sourceforge.net/projects/clamsap/files/
3. Use the libclamsap when the mobiliser can access a local clamav engine.

Configure VSI

1. The configuration of the clamav adapter is straight forward. Please enable the default adapter and edit the adaptor path to point to the libclamsap shared library.:

   ➢ *com.sybase365.mobiliser.framework.vsi.properties*

   ```
   (...)
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT=VSA_DEFAULT
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT.Active=true
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT.AdapterPath=/home/sybase/libclamsap.so
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT.Description=DEFAULT PROVIDER
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT.Group=DEFAULT
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT.PoolInstanceTimeOut=3600
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT.PoolMaxInstances=50
   vsi.provider.Virus_Scan_Adapter.Adapters.VSA_DEFAULT.ReInitTime=0
   (...)
   ```

2. Restart the mobiliser instance and examine the log. The adapter is loaded successfully when you see the following log lines in the mobiliser.log:

   ```
   (...)
   2012-09-06 08:43:48,747 [aims-init-15] DEBUG com.sybase365.mobiliser.framework.vscan.scanner.impl.VScanImpl - VSI Virus Scan Service initialization was
   successfull
   (...)
   ```

Proxy Setup

As described in a previous section, it is strongly recommended to not place the Mobiliser Core in the DMZ. It is best to use a proxy in the DMZ to provide restricted access to the services provided by Mobiliser Core. This can either be done by using a standard reverse proxy or by using the Mobiliser Validating Proxy.

Reverse Proxy

The example here is provided for an Apache with proxy modules installed. The full installation and configuration of the Apache server is not covered in this document.

```
<Proxy *>
        Order deny,allow
        Allow from all
</Proxy>

ProxyPass /mobiliser http://localhost:8080/mobiliser
ProxyPassReverse /mobiliser http://localhost:8080/mobiliser

ProxyPass /system http://localhost:8080/system
ProxyPassReverse /system http://localhost:8080/system
```

Validating Proxy

The validating proxy is a specially assembled OSGi container that contains a subset of the Mobiliser Core bundles. It is provided as a zip file that must be extracted into an appropriate directory:

- */opt/Sybase/mobiliser_proxy*

The Validating Proxy contains the same Jetty specific configuration options as the Mobiliser Core container, which are documented in a previous section. In addition there is a configuration file which contains the URL for the Mobiliser Core to which the requests are forwarded (after successful validation). This file is located under:

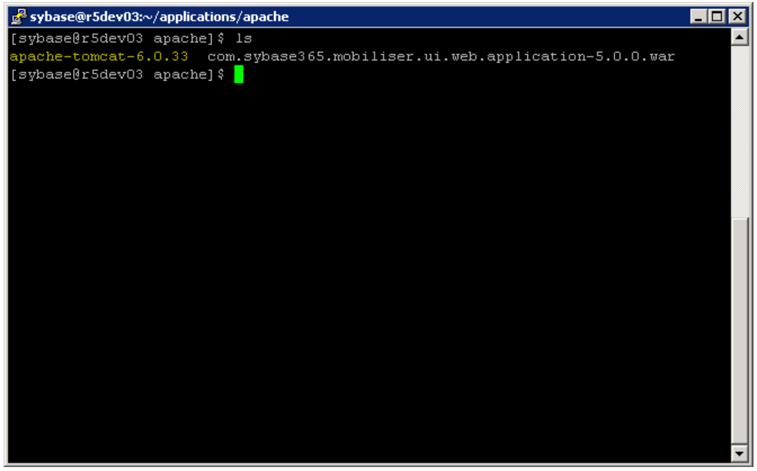
- *{MOBILISER_HOME}/conf/cfgbackup/ com.sybase365.mobiliser.framework.service.proxy.properties.*

UI Setup

UI Setup - Tomcat

The UI will be deployed on Tomcat (6.0.33) or later. The UI provides access to End User and Administrative Portals. As shown in the deployment diagram in a previous section, there is usually a public portal and an internal portal providing access to different functions for different types of users. The internal portal contains, for example functions to make modifications to vital system configuration and to monitor the server. This is also protected by privileges and roles, but should not be exposed to the public Internet anyway. The source code for both portals is usually identical. They only differ by a configuration file located in the WEB-INF/ folder of the jar file. In standard projects, two different WAR files should be provided that have the correct configuration file included. The public portal is to be installed on the DMZ, the internal portal on the application server tier. Otherwise, the structure of Tomcat and the WAR file is identical.

The Tomcat Container and UI application are located at {MOBILISER_INSTALLATION}/applications/apache



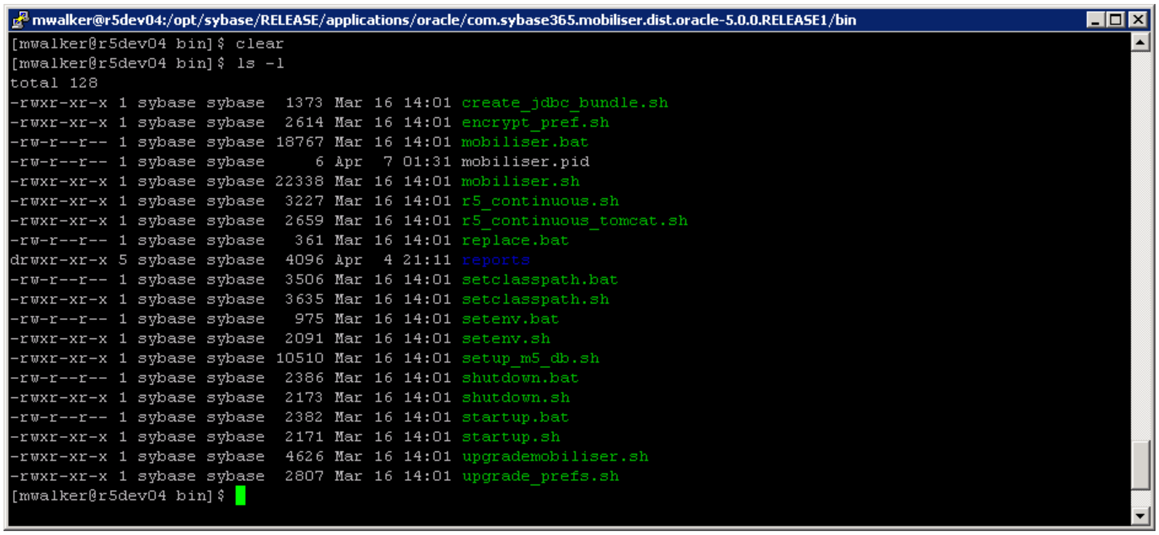
```
[sybase@r5dev03 apache]$ ls
apache-tomcat-6.0.33  com.sybase365.mobiliser.ui.web.application-5.0.0.war
[sybase@r5dev03 apache]$
```

1. Copy the Tomcat Container from {MOBILISER_INSTALLATION}/applications/apache/apache-tomcat-6.0.33 to /opt/sybase to create the {TOMCAT_HOME} directory
    a. Note: It is useful to create a symbolic link ‘tomcat’ to the {TOMCAT_HOME} directory
    b. Note: All other necessary application directories are generated automatically on start up by Tomcat
2. Copy the UI application ‘com.sybase365.mobiliser.ui.web.application-5.1.war’ to the {TOMCAT_HOME}/webapps directory and rename it to ROOT.war

Initialization and System Check (Mobiliser 5.1 Core)

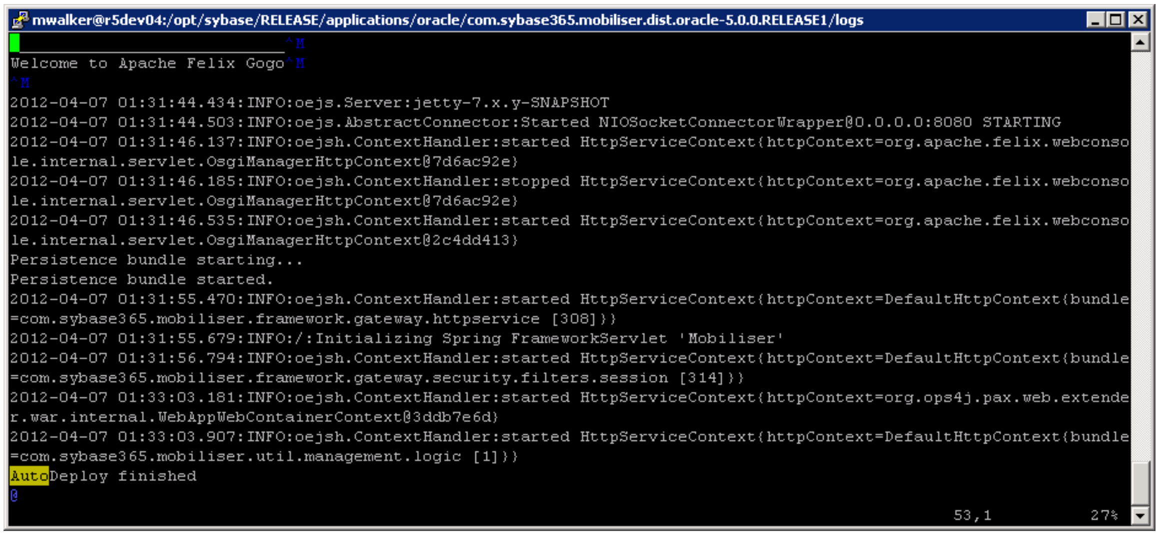
Start Server and UI

1. Execute the following start script {MOBILISER_HOME}/bin/startup.sh to start the Server *(note: shutdown.sh and other admin scripts are also located in this directory).*



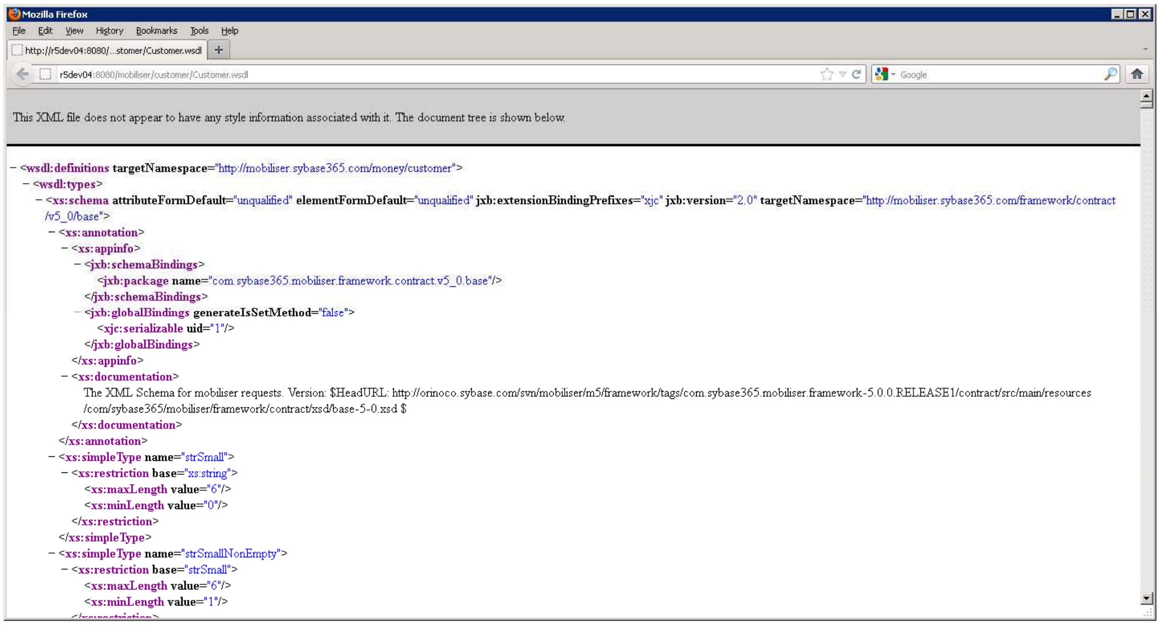
```
mwalker@r5dev04:/opt/sybase/RELEASE/applications/oracle/com.sybase365.mobiliser.dist.oracle-5.0.0.RELEASE1/bin
[mwalker@r5dev04 bin]$ clear
[mwalker@r5dev04 bin]$ ls -l
total 128
-rwxr-xr-x 1 sybase sybase  1373 Mar 16 14:01 create_jdbc_bundle.sh
-rwxr-xr-x 1 sybase sybase  2614 Mar 16 14:01 encrypt_pref.sh
-rw-r--r-- 1 sybase sybase 18767 Mar 16 14:01 mobiliser.bat
-rw-r--r-- 1 sybase sybase     6 Apr  7 01:31 mobiliser.pid
-rwxr-xr-x 1 sybase sybase 22338 Mar 16 14:01 mobiliser.sh
-rwxr-xr-x 1 sybase sybase  3227 Mar 16 14:01 r5_continuous.sh
-rwxr-xr-x 1 sybase sybase  2659 Mar 16 14:01 r5_continuous_tomcat.sh
-rw-r--r-- 1 sybase sybase   361 Mar 16 14:01 replace.bat
drwxr-xr-x 5 sybase sybase  4096 Apr  4 21:11 reports
-rw-r--r-- 1 sybase sybase  3506 Mar 16 14:01 setclasspath.bat
-rwxr-xr-x 1 sybase sybase  3635 Mar 16 14:01 setclasspath.sh
-rw-r--r-- 1 sybase sybase   975 Mar 16 14:01 setenv.bat
-rwxr-xr-x 1 sybase sybase  2091 Mar 16 14:01 setenv.sh
-rwxr-xr-x 1 sybase sybase 10510 Mar 16 14:01 setup_m5_db.sh
-rw-r--r-- 1 sybase sybase  2386 Mar 16 14:01 shutdown.bat
-rwxr-xr-x 1 sybase sybase  2173 Mar 16 14:01 shutdown.sh
-rw-r--r-- 1 sybase sybase  2382 Mar 16 14:01 startup.bat
-rwxr-xr-x 1 sybase sybase  2171 Mar 16 14:01 startup.sh
-rwxr-xr-x 1 sybase sybase  4626 Mar 16 14:01 upgrademobiliser.sh
-rwxr-xr-x 1 sybase sybase  2807 Mar 16 14:01 upgrade_prefs.sh
[mwalker@r5dev04 bin]$
```

2. Monitor the Server log at {MOBILISER_HOME}/logs/felix.log until the log specifies that “AutoDeploy finished”.



```
mwalker@r5dev04:/opt/sybase/RELEASE/applications/oracle/com.sybase365.mobiliser.dist.oracle-5.0.0.RELEASE1/logs
 ____________________________^M
Welcome to Apache Felix Gogo^M
^M
2012-04-07 01:31:44.434:INFO:oejs.Server:jetty-7.x.y-SNAPSHOT
2012-04-07 01:31:44.503:INFO:oejs.AbstractConnector:Started NIOSocketConnectorWrapper@0.0.0.0:8080 STARTING
2012-04-07 01:31:46.137:INFO:oejsh.ContextHandler:started HttpServiceContext{httpContext=org.apache.felix.webconso
le.internal.servlet.OsgiManagerHttpContext@7d6ac92e}
2012-04-07 01:31:46.185:INFO:oejsh.ContextHandler:stopped HttpServiceContext{httpContext=org.apache.felix.webconso
le.internal.servlet.OsgiManagerHttpContext@7d6ac92e}
2012-04-07 01:31:46.535:INFO:oejsh.ContextHandler:started HttpServiceContext{httpContext=org.apache.felix.webconso
le.internal.servlet.OsgiManagerHttpContext@2c4dd413}
Persistence bundle starting...
Persistence bundle started.
2012-04-07 01:31:55.470:INFO:oejsh.ContextHandler:started HttpServiceContext{httpContext=DefaultHttpContext{bundle
=com.sybase365.mobiliser.framework.gateway.httpservice [308]}}
2012-04-07 01:31:55.679:INFO:/:Initializing Spring FrameworkServlet 'Mobiliser'
2012-04-07 01:31:56.794:INFO:oejsh.ContextHandler:started HttpServiceContext{httpContext=DefaultHttpContext{bundle
=com.sybase365.mobiliser.framework.gateway.security.filters.session [314]}}
2012-04-07 01:33:03.181:INFO:oejsh.ContextHandler:started HttpServiceContext{httpContext=org.ops4j.pax.web.extende
r.war.internal.WebAppWebContainerContext@3ddb7e6d}
2012-04-07 01:33:03.907:INFO:oejsh.ContextHandler:started HttpServiceContext{httpContext=DefaultHttpContext{bundle
=com.sybase365.mobiliser.util.management.logic [1]}}
AutoDeploy finished
@
                                                                                         53,1          27%
```

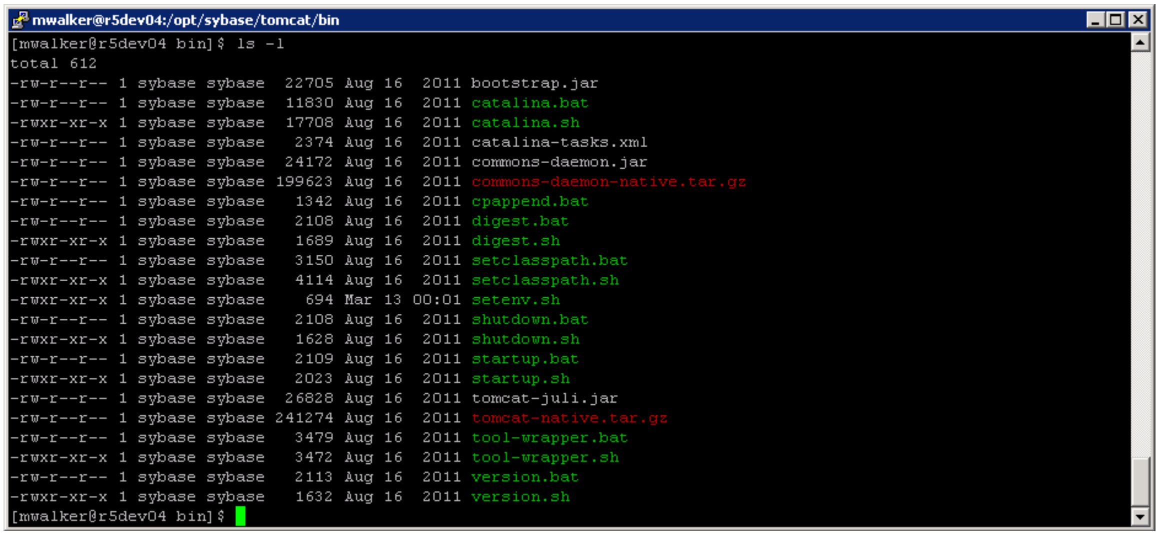
3. Verify that the Mobiliser Platform console has initialized successfully by viewing the customer WSDL via Web browser (http://localhost:8080/mobiliser/customer/Customer.wsdl).


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://r5dev04:8080/...stomer/Customer.wsdl
r5dev04:8080/mobiliser/customer/Customer.wsdl
Google

This XML file does not appear to have any style information associated with it. The document tree is shown below.

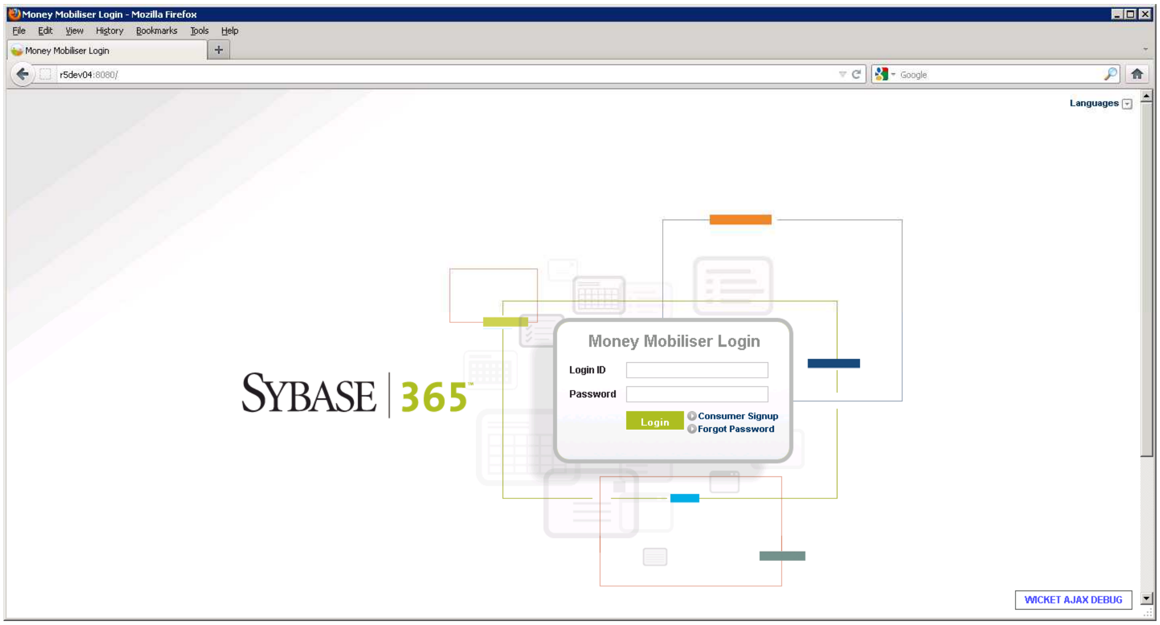
```
– <wsdl:definitions targetNamespace="http://mobiliser.sybase365.com/money/customer">
  – <wsdl:types>
    – <xs:schema attributeFormDefault="unqualified" elementFormDefault="unqualified" jxb:extensionBindingPrefixes="xjc" jxb:version="2.0" targetNamespace="http://mobiliser.sybase365.com/framework/contract
      /v5_0/base">
      – <xs:annotation>
        – <xs:appinfo>
          – <jxb:schemaBindings>
              <jxb:package name="com.sybase365.mobiliser.framework.contract.v5_0.base"/>
            </jxb:schemaBindings>
          – <jxb:globalBindings generateIsSetMethod="false">
              <xjc:serializable uid="1"/>
            </jxb:globalBindings>
          </xs:appinfo>
        – <xs:documentation>
            The XML Schema for mobiliser requests. Version: $HeadURL: http://orinoco.sybase.com/svn/mobiliser/m5/framework/tags/com.sybase365.mobiliser.framework-5.0.0.RELEASE1/contract/src/main/resources
            /com/sybase365/mobiliser/framework/contract/xsd/base-5-0.xsd $
          </xs:documentation>
        </xs:annotation>
      – <xs:simpleType name="strSmall">
        – <xs:restriction base="xs:string">
            <xs:maxLength value="6"/>
            <xs:minLength value="0"/>
          </xs:restriction>
        </xs:simpleType>
      – <xs:simpleType name="strSmallNonEmpty">
        – <xs:restriction base="strSmall">
            <xs:maxLength value="6"/>
            <xs:minLength value="1"/>
          </xs:restriction>
```

4. Execute the following startup script {TOMCAT_HOME}/bin/startup.sh to start the UI *(note: shutdown.sh and other admin scripts are also located in this directory).*



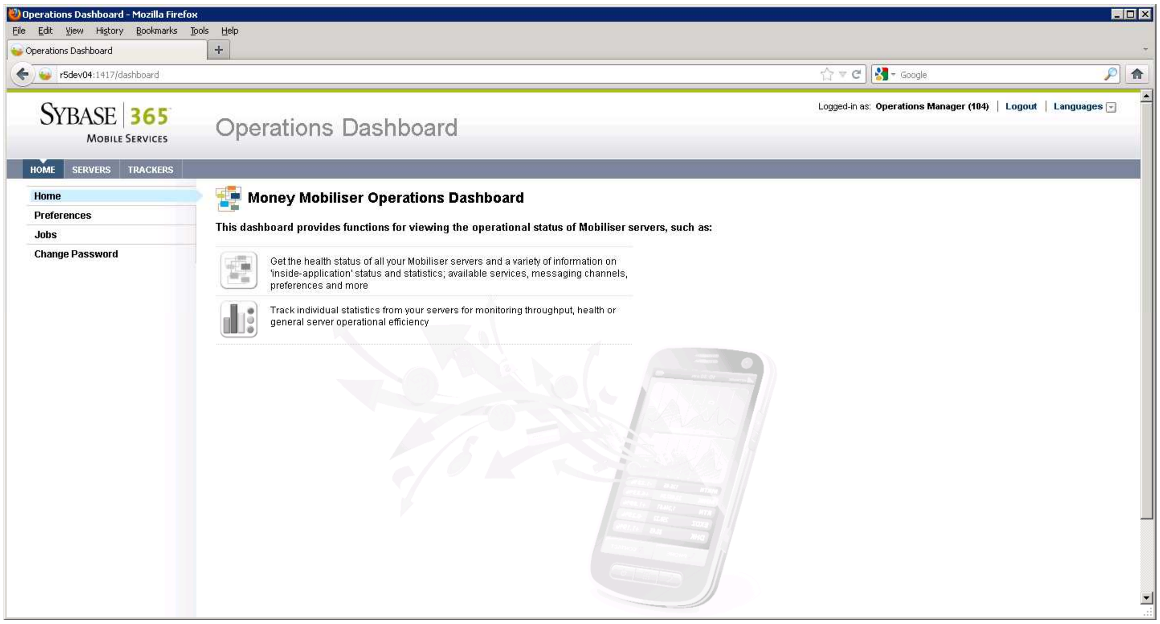
```
[mwalker@r5dev04 bin]$ ls -l
total 612
-rw-r--r-- 1 sybase sybase  22705 Aug 16  2011 bootstrap.jar
-rw-r--r-- 1 sybase sybase  11830 Aug 16  2011 catalina.bat
-rwxr-xr-x 1 sybase sybase  17708 Aug 16  2011 catalina.sh
-rw-r--r-- 1 sybase sybase   2374 Aug 16  2011 catalina-tasks.xml
-rw-r--r-- 1 sybase sybase  24172 Aug 16  2011 commons-daemon.jar
-rw-r--r-- 1 sybase sybase 199623 Aug 16  2011 commons-daemon-native.tar.gz
-rw-r--r-- 1 sybase sybase   1342 Aug 16  2011 cpappend.bat
-rw-r--r-- 1 sybase sybase   2108 Aug 16  2011 digest.bat
-rwxr-xr-x 1 sybase sybase   1689 Aug 16  2011 digest.sh
-rw-r--r-- 1 sybase sybase   3150 Aug 16  2011 setclasspath.bat
-rwxr-xr-x 1 sybase sybase   4114 Aug 16  2011 setclasspath.sh
-rwxr-xr-x 1 sybase sybase    694 Mar 13 00:01 setenv.sh
-rw-r--r-- 1 sybase sybase   2108 Aug 16  2011 shutdown.bat
-rwxr-xr-x 1 sybase sybase   1628 Aug 16  2011 shutdown.sh
-rw-r--r-- 1 sybase sybase   2109 Aug 16  2011 startup.bat
-rwxr-xr-x 1 sybase sybase   2023 Aug 16  2011 startup.sh
-rw-r--r-- 1 sybase sybase  26828 Aug 16  2011 tomcat-juli.jar
-rw-r--r-- 1 sybase sybase 241274 Aug 16  2011 tomcat-native.tar.gz
-rw-r--r-- 1 sybase sybase   3479 Aug 16  2011 tool-wrapper.bat
-rwxr-xr-x 1 sybase sybase   3472 Aug 16  2011 tool-wrapper.sh
-rw-r--r-- 1 sybase sybase   2113 Aug 16  2011 version.bat
-rwxr-xr-x 1 sybase sybase   1632 Aug 16  2011 version.sh
[mwalker@r5dev04 bin]$
```

5. Verify that the Tomcat Web UI application has initialized successfully by viewing it in Web browser (http://localhost:8082).



Preferences Configuration

1. Log into the UI (Operations Dashboard) as the opsmgr user (opsmgr: secret). You will be prompted to change the password for the user before you are logged in.



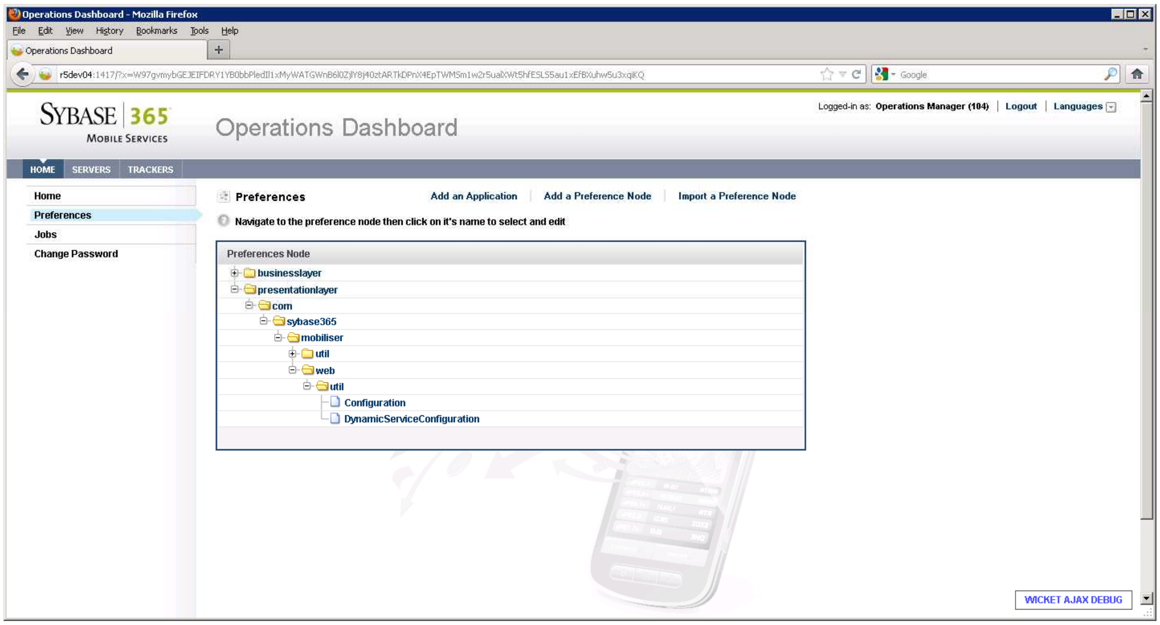
Money Mobiliser Operations Dashboard

This dashboard provides functions for viewing the operational status of Mobiliser servers, such as:

Get the health status of all your Mobiliser servers and a variety of information on 'inside-application' status and statistics; available services, messaging channels, preferences and more

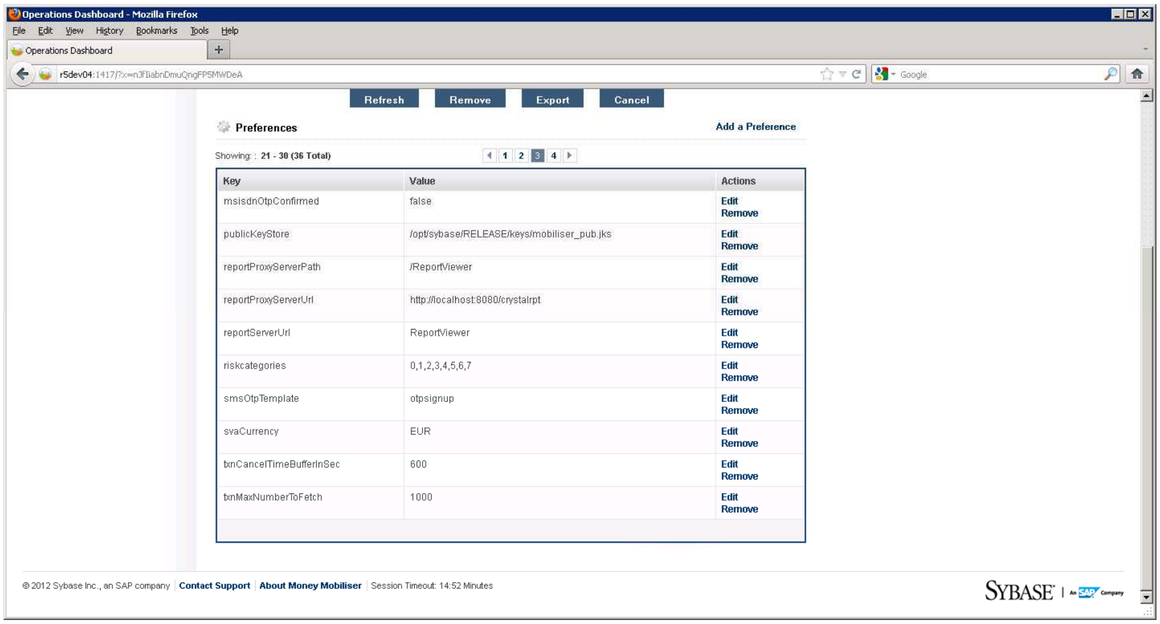
Track individual statistics from your servers for monitoring throughput, health or general server operational efficiency

2. Select Preferences on the left side of the screen, expand to the following path /presentationlayer/com/sybase365/mobiliser/util/web/util and select the Configuration file.



Navigate to the preference node then click on it's name to select and edit

3. Navigate to the Key named publicKeyStore (Page 3) and edit the value to “{MOBILISER_HOME}/keys/mobiliser_pub.jks”
    a. This will allow Mobiliser Platform to use the test keystore that comes with the package.



Operations Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operations Dashboard
Refresh
Remove
Export
Cancel
Preferences
Add a Preference
1 2 3 4
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser
SYBASE An SAP Company

Showing: : 21 - 30 (36 Total)

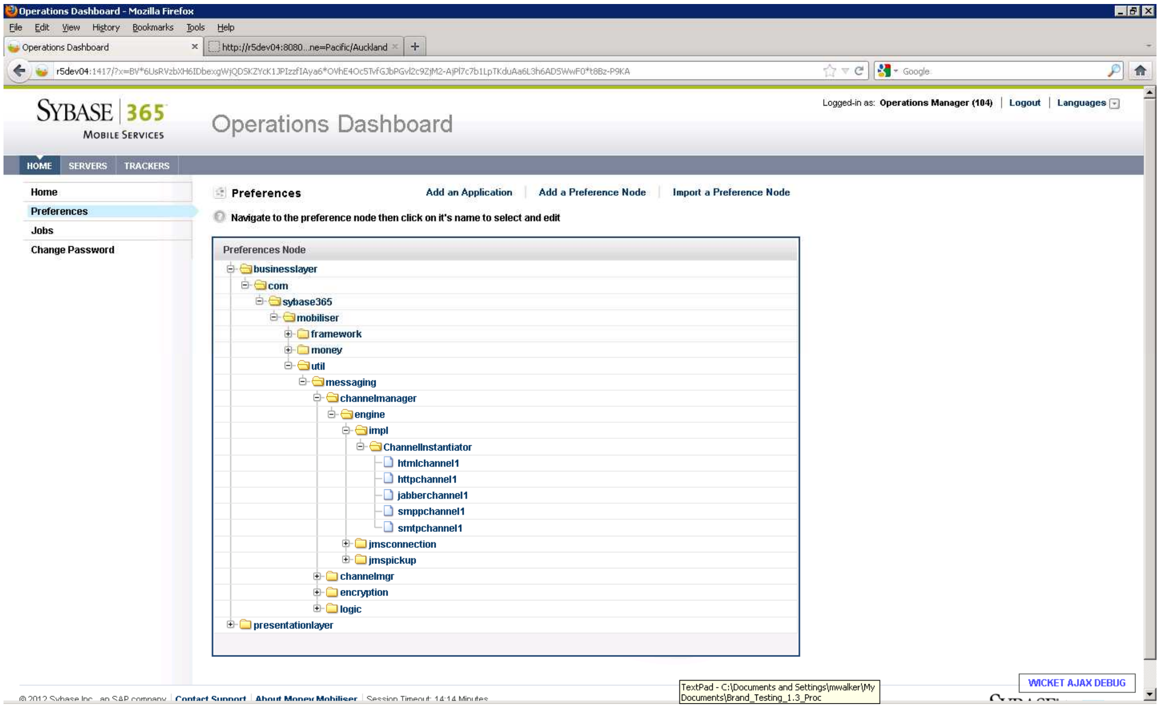
Key	Value	Actions
msisdnOtpConfirmed	false	Edit Remove
publicKeyStore	/opt/sybase/RELEASE/keys/mobiliser_pub.jks	Edit Remove
reportProxyServerPath	/ReportViewer	Edit Remove
reportProxyServerUrl	http://localhost:8080/crystalrpt	Edit Remove
reportServerUrl	ReportViewer	Edit Remove
riskcategories	0,1,2,3,4,5,6,7	Edit Remove
smsOtpTemplate	otpsignup	Edit Remove
svaCurrency	EUR	Edit Remove
txnCancelTimeBufferInSec	600	Edit Remove
txnMaxNumberToFetch	1000	Edit Remove

Session Timeout: 14:52 Minutes

4. Click Refresh to assure that preferences changes were committed.

SMPP Configuration (Optional)

1. Log into the UI (Operations Dashboard) as the opsmgr user
2. Select Preferences on the left side of the screen, expand to the following path com/sybase365/mobiliser/util/messaging/channelmanager/engine/impl/ChannelInstantiator/ and select the smppchannel1 node file.



Operations Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operations Dashboard
http://r5dev04:8080...ne=Pacific/Auckland
r5dev04:1417/?x=BY*6UsRVzbXH6IDbexgWjQDSKZYcK1JPIzzfIAya6*OVhE4Oc5TvFGJbPGvl2c9ZjM2-AjPl7c7b1LpTKduAa6L3h6AD5WwF0*t8Bz-P9KA
Google
SYBASE 365 Mobile Services
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME SERVERS TRACKERS
Home
Preferences
Jobs
Change Password
Preferences
Add an Application | Add a Preference Node | Import a Preference Node

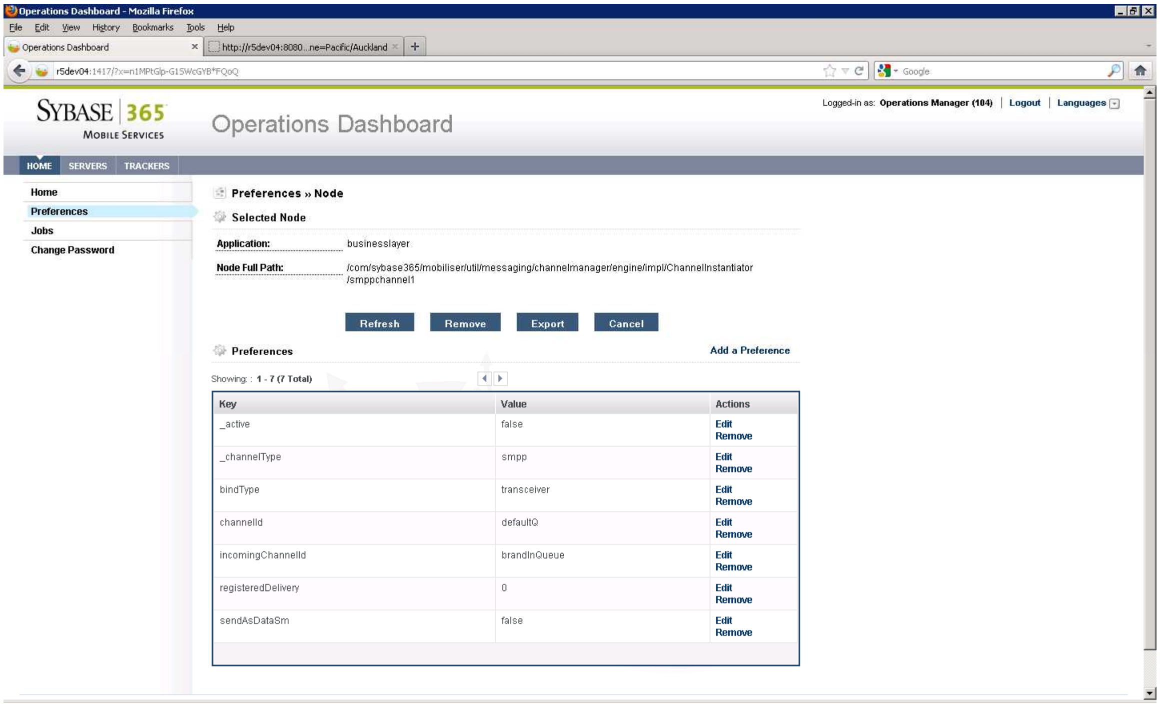
Navigate to the preference node then click on it's name to select and edit

Preferences Node

```
⊟ businesslayer
  ⊟ com
    ⊟ sybase365
      ⊟ mobiliser
        ⊞ framework
        ⊞ money
        ⊟ util
          ⊟ messaging
            ⊟ channelmanager
              ⊟ engine
                ⊟ impl
                  ⊟ ChannelInstantiator
                      htmlchannel1
                      httpchannel1
                      jabberchannel1
                      smppchannel1
                      smtpchannel1
                ⊞ jmsconnection
                ⊞ jmspickup
            ⊞ channelmgr
            ⊞ encryption
            ⊞ logic
⊞ presentationlayer
```

© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:14 Minutes
TextPad - C:\Documents and Settings\mwalker\My Documents\Brand_Testing_1.3_Proc
WICKET AJAX DEBUG

3. Navigate through all of the node preferences, and enter all relevant SMPP account information.



Operations Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operations Dashboard
http://r5dev04:8080...ne=Pacific/Auckland
r5dev04:1417/?x=n1MPtGlp-G15WcGYB*FQoQ
Google
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME SERVERS TRACKERS
Home
Preferences
Jobs
Change Password

Preferences » Node

Selected Node

Application:	businesslayer
Node Full Path:	/com/sybase365/mobiliser/util/messaging/channelmanager/engine/impl/ChannelInstantiator /smppchannel1

Refresh
Remove
Export
Cancel

Preferences

Showing: : 1 - 7 (7 Total)

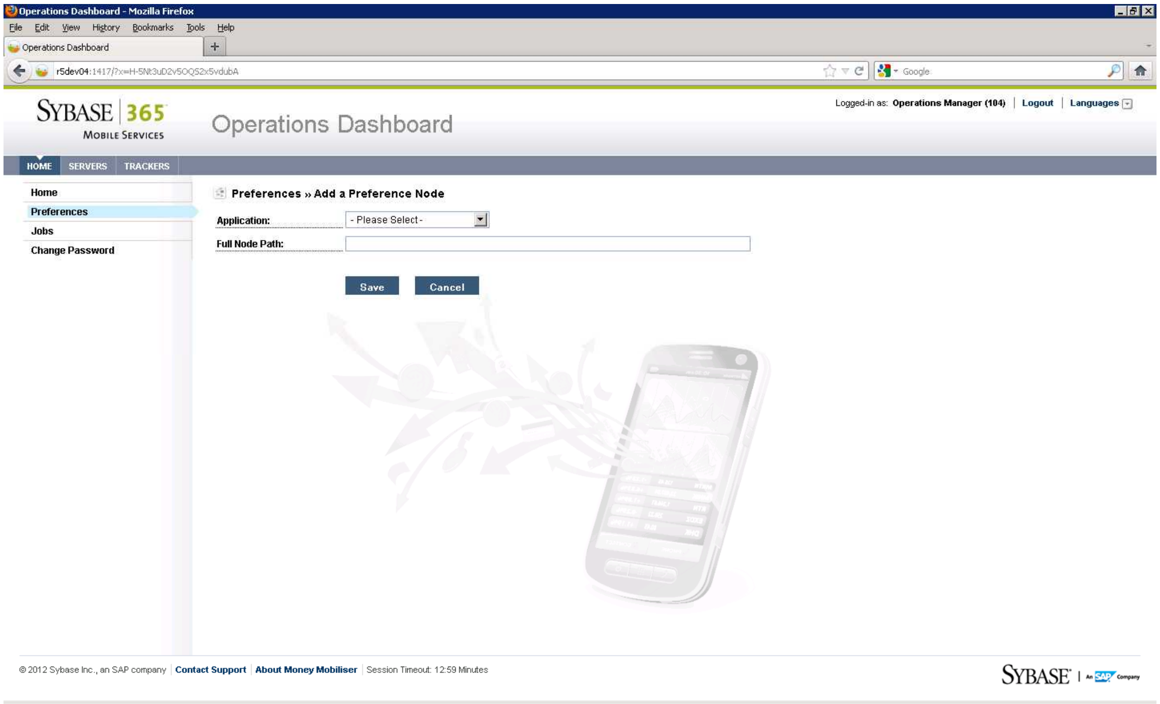
Key	Value	Actions
_active	false	Edit Remove
_channelType	smpp	Edit Remove
bindType	transceiver	Edit Remove
channelId	defaultQ	Edit Remove
incomingChannelId	brandInQueue	Edit Remove
registeredDelivery	0	Edit Remove
sendAsDataSm	false	Edit Remove

4. Click Refresh to assure that preferences changes were committed

SMTP Configuration (Optional)

Log into the UI (Operations Dashboard) as the opsmgr user

1. Select Preferences on the left side of the screen, the select “Add a Preference Node”



Operations Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operations Dashboard
r5dev04:1417/?x=H-5Nt3uD2v5OQS2x5vdubA
Google
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME SERVERS TRACKERS
Home
Preferences
Jobs
Change Password

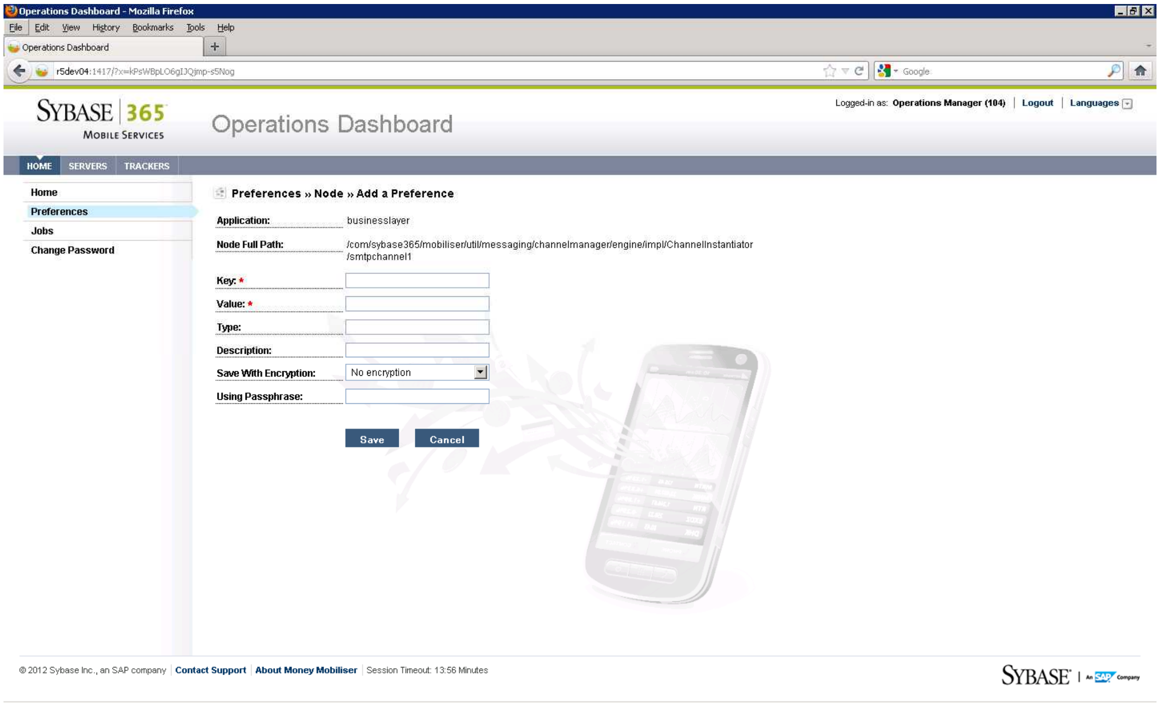
Preferences » Add a Preference Node

Application:	- Please Select -
Full Node Path:	

Save
Cancel
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 12:59 Minutes
SYBASE An SAP Company

2. Select businesslayer in the Application drop down list and enter the following path in the Full Node Path field: com/sybase365/mobiliser/util/messaging/channelmanager/engine/impl/ChannelInstantiator/smtpchannel1, then click Save.

3. Navigate to the newly created preference node in the preference tree, and double click on the smtpchannel1 node. Then select "Add a Preference"


Operations Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operations Dashboard
r5dev04:1417/?x=kPsWBpLO6gIJQjmp-s5Nog
Google
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME SERVERS TRACKERS
Home
Preferences
Jobs
Change Password

Preferences » Node » Add a Preference

Application: businesslayer

Node Full Path: /com/sybase365/mobiliser/util/messaging/channelmanager/engine/impl/ChannelInstantiator/smtpchannel1

Key: *

Value: *

Type:

Description:

Save With Encryption: No encryption

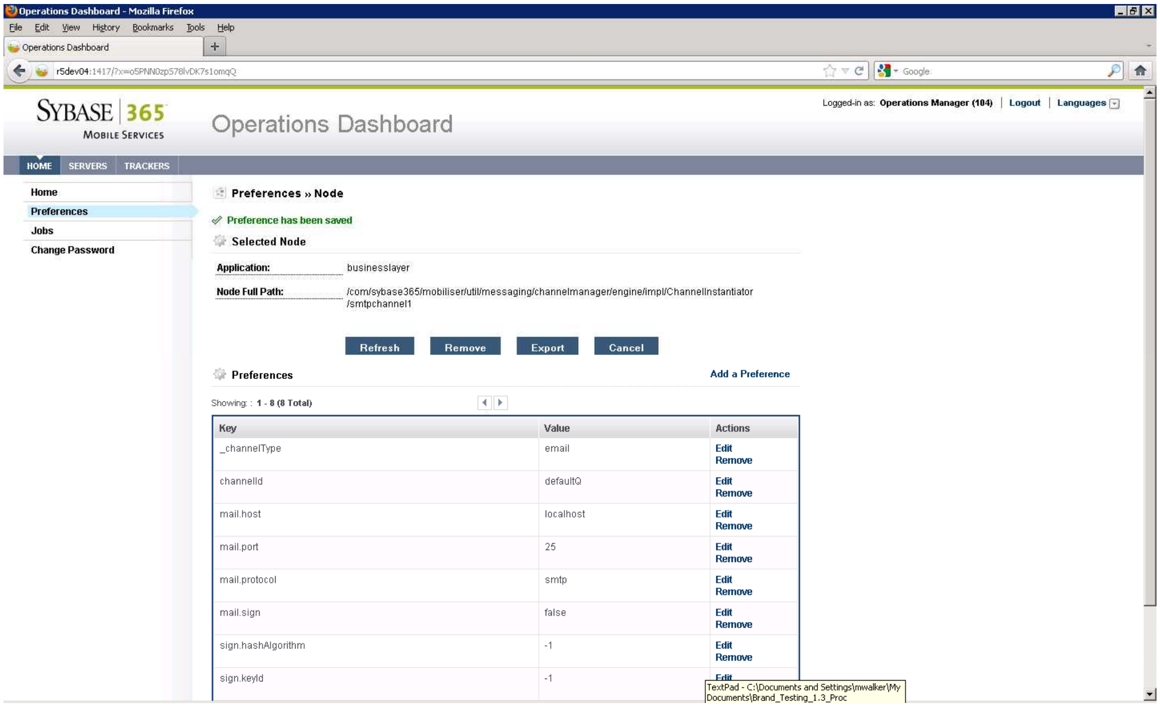
Using Passphrase:

Save
Cancel
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 13:56 Minutes
SYBASE | An SAP Company

4. In the Key field enter _channelType, in the Value field enter email, in the Type field enter java.lang.String. Click Save.

5. Repeat previous step to enter the following values
   a. Key: channeled, Value: default, Type: java.lang.String
   b. Key: mail.host, Value: localhost, Type: java.lang.String
   c. Key: mail.port, Value: 25, Type: java.lang.String
   d. Key: mail.protocol, Value: smtp, Type: java.lang.String
   e. Key: mail.sign, Value: false, Type: java.lang.String
   f. Key: sign.hashAlgorithm, Value: -1, Type: java.lang.String
   g. Key: sign.keyId, Value: -1, Type: java.lang.String

6. Click Refresh to assure that preferences changes were committed


Operations Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Operations Dashboard
r5dev04:1417/?x=o5PNN0zp578lvDK7s1omqQ
Google
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
Home
Preferences
Jobs
Change Password
Refresh
Remove
Export
Cancel
Add a Preference

Preferences » Node

✓ Preference has been saved

Selected Node

Application:	businesslayer
Node Full Path:	/com/sybase365/mobiliser/util/messaging/channelmanager/engine/impl/ChannelInstantiator /smtpchannel1

Preferences

Showing: : 1 - 8 (8 Total)

Key	Value	Actions
_channelType	email	Edit Remove
channelId	defaultQ	Edit Remove
mail.host	localhost	Edit Remove
mail.port	25	Edit Remove
mail.protocol	smtp	Edit Remove
mail.sign	false	Edit Remove
sign.hashAlgorithm	-1	Edit Remove
sign.keyId	-1	Edit

TextPad - C:\Documents and Settings\mwalker\My Documents\Brand_Testing_1.3_Proc

Default (Administrative) Web UI Accounts

The following user accounts are the administrative accounts that are created after a Mobiliser Platform Installation. Note: After the first successful attempt to log in with these accounts you will be prompted to change the password for the account before proceeding

Customer Support Accounts

Customer Support Tool – cstfull: secret
Manager User Accounts – usermgr: secret
Manage Notifications and Alerts – notifmgr:secret

Distribution Partner Portal Account

Create and Manage Merchants – Headquarter:secret

Operations Dashboard Admin Account

View and Manage System Configuration – opsmgr:secret

System Console

This console is used to monitor all of the functions of the Mobiliser Platform container

1. Default url = http://<localhost>:8080/system/console
2. Default Account – sysmgr:secret
    a. Note: This password may have been updated on first attempt to log into the Operations Dashboard.

Accessing Mobiliser Platform through JMX

Mobiliser Platform exposes various information through JMX. Local access directly connecting to the Java process is unlimited (per JMX specification), i.e., you can start jconsole (or any other JMX front-end) and connect to the running process. In addition, Mobiliser Platform also exposes JMX through RMI. The access details are configured in the com.sybase365.mobiliser.framework.gateway.security.authentication.jmx.properties file, located in ./conf/cfgbackup. When changing the configured port, make sure to adjust both properties, jmxPort as well as serviceUrl.

Any remote access is secured with username and password, which is validated using the standard Mobiliser Platform authentication mechanisms. The property file also allows configuration of a required access role. Per default, the sysmgr user has the pre-configured JMX_ACCESS role.

Exposed Information

Mobiliser Platform exposes standard JMX statistics and operations from the embedded Jetty servlet container ehcache, which provides the underlying caching implementation for Hibernate the database connection pool implementation BoneCP. In addition there are a couple of Mobiliser Platform specific MBeans available.

- *Framework components expose statistics and configuration:*
  - *com.sybase365.mobiliser.framework.event: provides statistics and details on the event processing framework and registered handlers*
  - *com.sybase365.mobiliser.framework.service.audit.jmx: basic request auditor, exposing very high-level statistics on processed Mobiliser service calls*
  - *com.sybase365.mobiliser.util.messaging.channelmanager: statistics on channels and messages*
  - *com.sybase365.mobiliser.util.prefs: read and write access to preferences as well as basic preference service configuration*
- *Brokers expose the list of available handlers:*
  - *com.sybase365.mobiliser.mbanking.businesslogic.openbank.impl*
  - *com.sybase365.mobiliser.money.businesslogic.authentication.impl*
  - *com.sybase365.mobiliser.money.businesslogic.billpayment.impl*
  - *com.sybase365.mobiliser.money.businesslogic.bulkprocessing.impl*
  - *com.sybase365.mobiliser.money.businesslogic.payment.impl*
  - *com.sybase365.mobiliser.money.businesslogic.transaction.flow.impl*
- *Hibernate DAOs allow changing the behavior on query caching and ordering:*
  - *com.sybase365.mobiliser.mbanking.persistence.dao.hibernate*
  - *com.sybase365.mobiliser.money*
  - *com.sybase365.mobiliser.money.persistence.hibernate.dao.customer*
  - *com.sybase365.mobiliser.money.persistence.hibernate.dao.job*
  - *com.sybase365.mobiliser.money.persistence.hibernate.dao.pi*
  - *com.sybase365.mobiliser.money.persistence.hibernate.dao.system*
  - *com.sybase365.mobiliser.money.persistence.hibernate.dao.transaction*
  - *com.sybase365.mobiliser.util.alerts.persistence.dao.hibernate*
  - *com.sybase365.mobiliser.util.messaging.dao.impl.hibernate*
  - *com.sybase365.mobiliser.util.prefs.persistence.dao.hibernate*

Data Archiving, Retention, and Deletion

In the current release 5.1 (or older), Mobiliser Platform does not support data archiving out of the box, neither do we have data retention and deletion policies implemented. Hence, it is a system engineer's task to set up means using default database technology implementing any desired procedures.

Data Archiving

Transactional data can be moved out of the online transaction database safely. We do not recommend moving out customer data since this information is required in the online transaction database to ensure referential integrity. This should not be a problem since the portion of customer data should be small compared to the amount of transactional data in a system. When archiving data out of the online database, obviously this data will not be visible through the standard Mobiliser Platform user interfaces anymore.

When moving out transactional data, please be aware of foreign key constraints on transaction data; make sure to move the full information belonging to a transaction.

A Mobiliser Platform transaction stores data in these tables:

- *MOB_TXNS*
- *MOB_SUB_TXNS.ID_TXN->MOB_TXNS.ID_TXN*
- *MOB_TXN_ATTRIBUTES.ID_TXN->MOB_TXNS.ID_TXN*
- *MOB_FEES.ID_SUB_TXN->MOB_SUB_TXNS.ID_SUB_TXN*

In case the transaction is an invoice payment, the invoice must be moved as well:

- *MOB_INVOICES*
- *MOB_INV_TXNS.ID_TXN->MOB_TXNS.ID_TXN*
- *MOB_INV_TXNS.ID_INVOICE->MOB_INVOICES.ID_INVOICE*
- *MOB_INV_ATTRIBUTES.ID_INVOICE->MOB_INVOICES.ID_INVOICE*

Additionally there is some audit/logging data created in the following tables:

- *MOB HISTORY – tracks changes to individual columns in the database.*
- *MOB_AUDIT_LOGS – each remote service call is tracked in this table.*
- *MOB_TRACEABLE_REQUESTS – stores data for non-repudiation and response dehydration. Usually not more than 24 hours of data is required in this table.*

Data Retention and Deletion

Mobiliser Platform does not have automated procedures to implement data retention and deletion policies. Hence, it must be part of the system setup to install jobs (or manually perform tasks) to delete data after the retention period is expired. Since the Mobiliser database holds many referential integrity constraints binding a customer record to transactions and other entities, we recommend to scramble customer data instead of physically deleting it, i.e. any personally identifiable information should be overwritten with random text (or a specific string ex. –DELETED--) in order to delete the customer record from the system.

Customer data is stored in these tables (customization project may have introduced further tables holding PII):

- *MOB_CUSTOMERS*
- *MOB_CUSTOMERS_IDENTIFICATIONS.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_CUSTOMERS_CREDENTIALS.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_CUSTOMERS_IDENTITIES.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_CUSTOMERS_ATTRIBUTES.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_ADDRESSES.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_ATTACHMENTS.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_NOTES.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*

- *MOB_PIS.ID_CUSTOMER->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_PIS.ID_PI<-MOB_WALLET->MOB_CUSTOMER.ID_CUSTOMER*
- *MOB_SVA.ID_PI->MOB_PIS.ID_PI*
- *MOB_CREDIT_CARDS.ID_PI->MOB_PIS.ID_PI*
- *MOB_BANK_ACCOUNTS.ID_PI->MOB_PIS.ID_PI*
- *MOB_EXTERNAL_ACCOUNTS.ID_PI->MOB_PIS.ID_PI*

Deletion Script

Execute this script to obfuscate all PIs of a customer. Use with care! Also all payment instruments related information is removed. Further processing of financial transactions will not be possible.

```
-- delete information about bank accounts
UPDATE MOB_BANK_ACCOUNTS SET STR_NAME = '###', STR_NAME_BANK = '###', STR_CITY_BANK = '###', STR_INSTITUTION_CODE = '###',
STR_BRANCH_CODE = '###', STR_ACCOUNT_NUMBER = '###', STR_DISPLAY_NUMBER = '###' WHERE
ID_PI in (SELECT ID_PI FROM MOB_PIS WHERE ID_CUSTOMER = ?);
-- delete information about "other" financial accounts
UPDATE MOB_EXTERNAL_ACCOUNTS SET STR_ID1 = '###', STR_ID2 = '###', STR_ID3 = '###', STR_ID4 = '###',
STR_ID8 = '###', STR_ID7 = '###', STR_ID6 = '###', STR_ID5 = '###' WHERE
ID_PI in (SELECT ID_PI FROM MOB_PIS WHERE ID_CUSTOMER = ?);
-- delete credit card information
UPDATE MOB_CREDIT_CARDS SET STR_CARD_NUMBER = '###', STR_CARD_HOLDER_NAME = '###', STR_DISPLAY_NUMBER = '###' WHERE
ID_PI in (SELECT ID_PI FROM MOB_PIS WHERE ID_CUSTOMER = ?);
-- delete names of accounts
UPDATE MOB_WALLET SET STR_ALIAS = '###' WHERE ID_CUSTOMER = ?;
-- mark all accounts as inactive
UPDATE MOB_PIS SET BOL_IS_ACTIVE = 'N' WHERE ID_CUSTOMER = ?;
-- delete all identifications, such as mobile phone number and make them inactive
UPDATE MOB_CUSTOMERS_IDENTIFICATIONS SET STR_IDENTIFICATION = '###', BOL_IS_ACTIVE = 'N' WHERE ID_CUSTOMER = ?;
-- delete all passwords and PINs and make them inactive
UPDATE MOB_CUSTOMERS_CREDENTIALS SET STR_CREDENTIAL = '###', BOL_IS_ACTIVE = 'N' WHERE ID_CUSTOMER = ?;
-- delete all identity (e.g. passport) information
UPDATE MOB_CUSTOMERS_IDENTITIES SET STR_IDENTITY = '###', STR_ISSUE_PLACE = '###', STR_ISSUER = '###', BOL_IS_ACTIVE = 'N' WHERE ID_CUSTOMER = ?;
-- delete all general purpose attributes
UPDATE MOB_CUSTOMERS_ATTRIBUTES SET STR_VALUE = '###' WHERE ID_CUSTOMER = ?;
-- delete all binary attachments
UPDATE MOB_ATTACHMENTS SET STR_NAME = '###', BIN_CONTENT = null WHERE ID_CUSTOMER = ?;
-- delete all notes (system generated or manually entered)
UPDATE MOB_NOTES SET STR_SUBJECT = '###', STR_TEXT = '###' WHERE ID_CUSTOMER = ?;
-- mark customer as inactive
UPDATE MOB_CUSTOMERS SET STR_DISPLAY_NAME = '###', STR_SECURITY_QUESTION = '###', STR_SECURITY_ANSWER = '###', STR_REFERRAL_CODE = '###', BOL_IS_ACTIVE = 'N',
DAT_DATE_OF_BIRTH = null WHERE ID_CUSTOMER = ?;
-- delete all address information
UPDATE MOB_ADDRESSES SET STR_FIRST_NAME = '###', STR_MIDDLE_NAME = '###', STR_LAST_NAME = '###', STR_TITLE = '###', STR_COMPANY1 = '###', STR_COMPANY2 = '###',
STR_COMPANY_SHORTNAME = '###', STR_POSITION = '###', STR_STREET1 = '###', STR_STREET2 = '###', STR_HOUSE_NUMBER = '###', STR_ZIP = '###', STR_CITY = '###',
STR_STATE = '###', STR_PHONE1 = '###', STR_PHONE2 = '###', STR_FAX = '###', STR_EMAIL = '###', STR_URL = '###', STR_NAME_ADDRESS = '###' WHERE ID_CUSTOMER = ?;
-- delete all information regarding change history
UPDATE MOB_HISTORY SET STR_OLD_VALUE = '###', STR_NEW_VALUE = '###' WHERE ID_OBJECT = ?;
UPDATE MOB_HISTORY SET STR_OLD_VALUE = '###', STR_NEW_VALUE = '###' WHERE ID_OBJECT in (SELECT ID_PI FROM MOB_PIS WHERE ID_CUSTOMER = ?);
UPDATE MOB_HISTORY SET STR_OLD_VALUE = '###', STR_NEW_VALUE = '###' WHERE ID_OBJECT in (SELECT ID_ADDRESS FROM MOB_ADDRESSES WHERE ID_CUSTOMER = ?);
UPDATE MOB_HISTORY SET STR_OLD_VALUE = '###', STR_NEW_VALUE = '###' WHERE ID_OBJECT in (SELECT ID_IDENTITY FROM MOB_CUSTOMERS_IDENTITIES WHERE ID_CUSTOMER = ?);
UPDATE MOB_HISTORY SET STR_OLD_VALUE = '###', STR_NEW_VALUE = '###' WHERE ID_OBJECT in (SELECT ID_CUSTOMER_IDENTIFICATION FROM MOB_CUSTOMERS_IDENTIFICATIONS
WHERE ID_CUSTOMER = ?);
UPDATE MOB_HISTORY SET STR_OLD_VALUE = '###', STR_NEW_VALUE = '###' WHERE ID_OBJECT in (SELECT ID_CUSTOMER_CREDENTIAL FROM MOB_CUSTOMERS_CREDENTIALS WHERE
ID_CUSTOMER = ?);
UPDATE MOB_HISTORY SET STR_OLD_VALUE = '###', STR_NEW_VALUE = '###' WHERE ID_OBJECT in (SELECT ID_NOTE FROM MOB_NOTES WHERE ID_CUSTOMER = ?);
-- commit all data
commit;
```

Auditing Information

All tables in the Mobiliser database schema have 4 columns that track the date and user who created the record and the date and user of the last update to the record.

Table	Description
MOB_AUDIT_LOGS	*Access to each service call in Mobiliser Platform is logged to the Database and to the log file. The service call is logged in this table. The name of the service, the ID of the caller, the return, and other relevant information are logged into this table. This applies to services related to customers but also to internal configurations that are accessible.*
MOB_PREFERNCES_HISTORY	*Changes to the configuration (Preferences) that is stored in the database is tracked additionally. This table contains previous entries along with the user who performed the update on the configuration.*
MOB_HISTORY	*Changes to customer and potentially other data is tracked in the table MOB_HISTORY. It contains the name of the field, the old and new value, the timestamp and the ID of the user who has done the change. This data is provided by database triggers on individual columns and is provided on an is-needed basis for each project.*

Security Considerations

In case any services of the Mobiliser Core need to exposed to the public Internet (e.g. for consumption by Smartphone Mobiliser) it is essential that only a subset of the services offered by Mobiliser Platform are exposed on the Internet. The privilege and role based security concept of Mobiliser Platform only grants access to services for users on an as-needed basis but there is no need to expose all of the services on the Internet.

Services in Mobiliser Platform are always attached to a "context" that, among other things, defines the last section of the URL to address a specific service.

Exposing Web Service Endpoints Securely:
http://localhost:8080/mobiliser/customer - is the default context for generic customer related services.
http://localhost:8080/mobiliser/smartphone - is the default context for services to be consumed by Smartphone Mobiliser Platform.

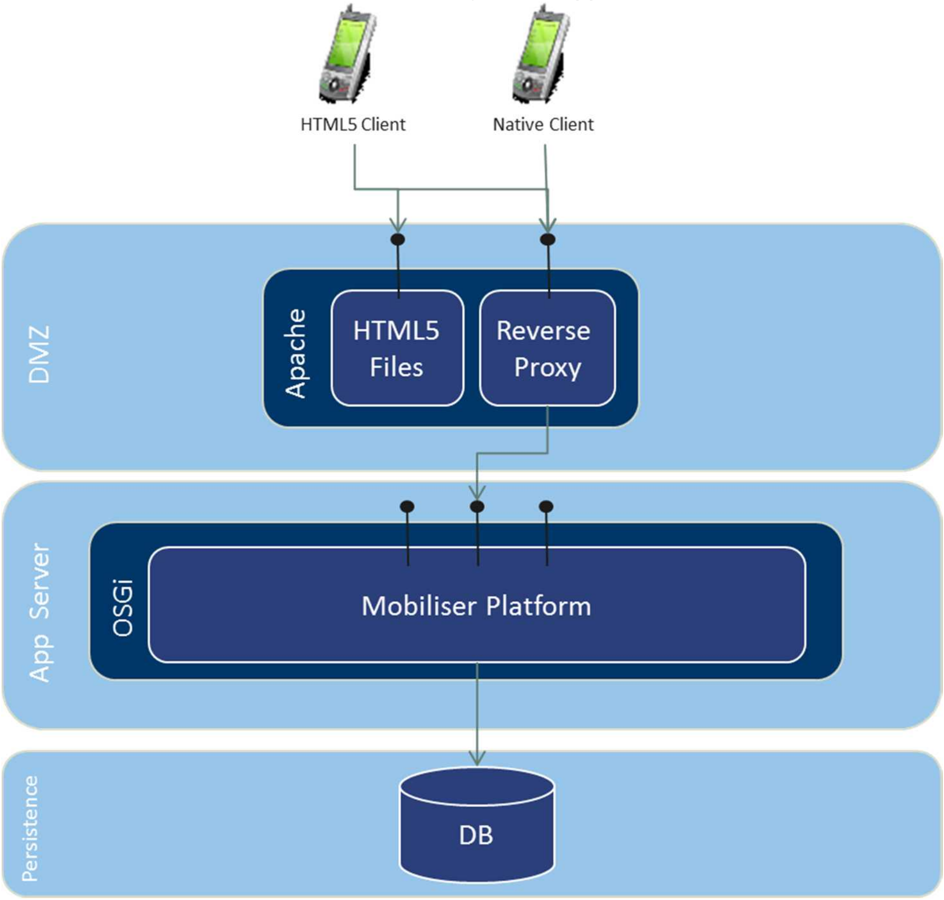
Mobiliser Platform supports various transport protocols (on top of HTTP). The JSON services are exposed under a slightly different URL. The JSON variants to the two examples mentioned above are:
http://localhost:8080/mobiliser/rest/customer
http://localhost:8080/mobiliser/rest/smartphone

So in most cases it is sufficient to expose the following URLs from the Mobiliser Core
http://localhost:8080/mobiliser/smartphone
http://localhost:8080/mobiliser/rest/smartphone

(Some customized projects might use other/additional URLs).

There are two alternatives to grant access to the services.

Standard Reverse Proxy
Any reverse proxy (e.g. Apache) can be used to accept incoming requests from the Internet in the DMZ and to forward them to the Mobiliser Core running on the application server tier.



Additionally to shielding direct access to the Mobiliser Core, the Apache can also be used to provide access to the HTML5 version of Smartphone Mobiliser or any other HTML5 application. Because of the "Same origin policy" (http://en.wikipedia.org/wiki/Same_origin_policy) the HTML files and the AJAX services must be provided by the same server (hostname + port).
The Reverse Proxy can also be used for the SSL termination.

In order for the Mobiliser Platform 5.1 platform to be deployed in the Standard Reverse Proxy model, configuration changes need to be made on the Apache Web UI container (located on the DMZ layer) and one of the database preferences (located in the Persistence layer).

Updating the WebUI container:

- Open the context.xml file in the {TOMCAT_HOME}/conf/ directory of the DMZ system.
- Update the value in the context.xml file to point to the {MOBILISER_HOME} instance on the App Server.

Example: value="prefs://prefsread:notsosecret@my_app_server:8080/mobiliser/rest/prefs?pollInterval=60000&amp;clientType=json&amp;applicationIdentifier=presentationlayer" />

Where "my_app_server" is your node where the mobiliser container is installed

Updating the database preferences

- Connect to the database with your choice of application that can run SQL/PL-SQL against the database
- Run the following SQL scripts against the database to update required preferences (syntax may vary slightly depending on database platform, the examples provided are for ASE 15.7 databases)

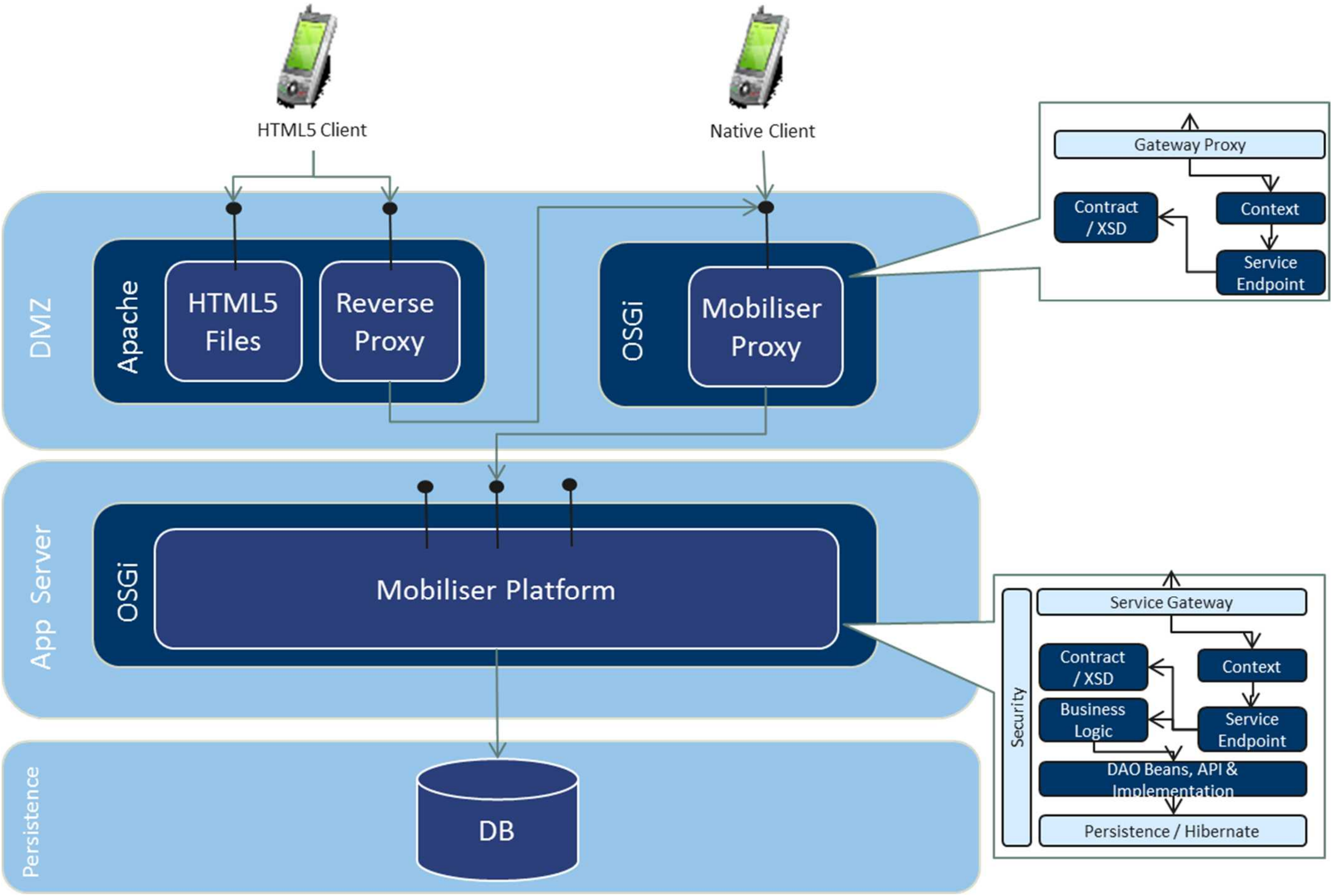
UPDATE MOB_PREFERENCES SET STR_VALUE='http:// my_app_server:8080/mobiliser' where ID_PREFERENCE=403
UPDATE MOB_PREFERENCES SET STR_VALUE='http:// my_app_server:8080/crystalrpt' where ID_PREFERENCE=437

Where "my_app_server" is your node where the mobiliser container is installed

Validating Proxy

Alternatively to a Reverse Proxy the Mobiliser Validating Proxy can be used.
In addition to restricting access to certain services, the validating proxy will make sure that the incoming request corresponds to the contract (XSD) defined for the appropriate service. This check can be applied on all supported protocols (SOAP, plain XML, JSON).

The validating proxy contains a subset of the bundles from the original Mobiliser Core. It only contains the contract definitions (XSD) and the context and endpoint information.
When the request was validated successfully it is forwarded to the Mobiliser Platform in its original format.

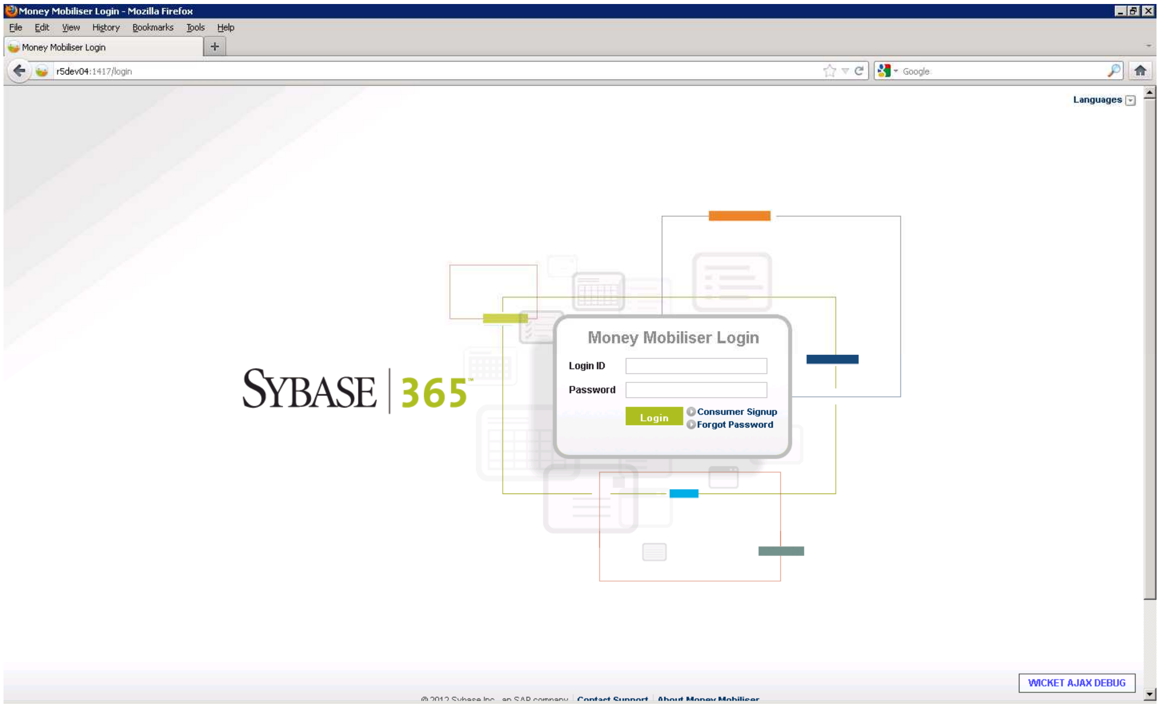


If there is also an HTML5 client in the mix, an additional Apache with reverse proxy (or similar HTTP server) needs to be added to support the Same Origin Policy.
The validating proxy provides an additional security layer.

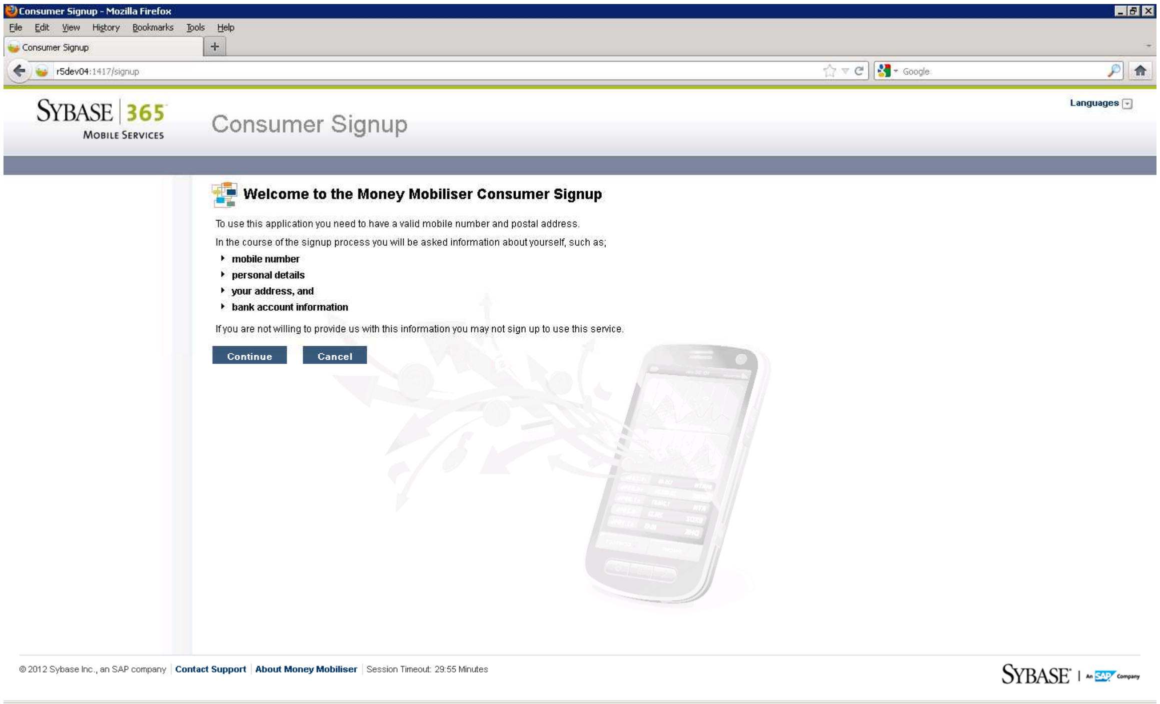
End-to-End Test (Mobiliser Platform 5.1 Core)

Add Customer

1. The consumer signup process begins at the Web UI login screen. Click on the link that says “Consumer Signup.”



2. Click Continue to move on to the Consumer Signup form for new Mobiliser Platform customers


Consumer Signup - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Consumer Signup
r5dev04:1417/signup
Google
SYBASE 365
MOBILE SERVICES
Languages

Consumer Signup

Welcome to the Money Mobiliser Consumer Signup

To use this application you need to have a valid mobile number and postal address.

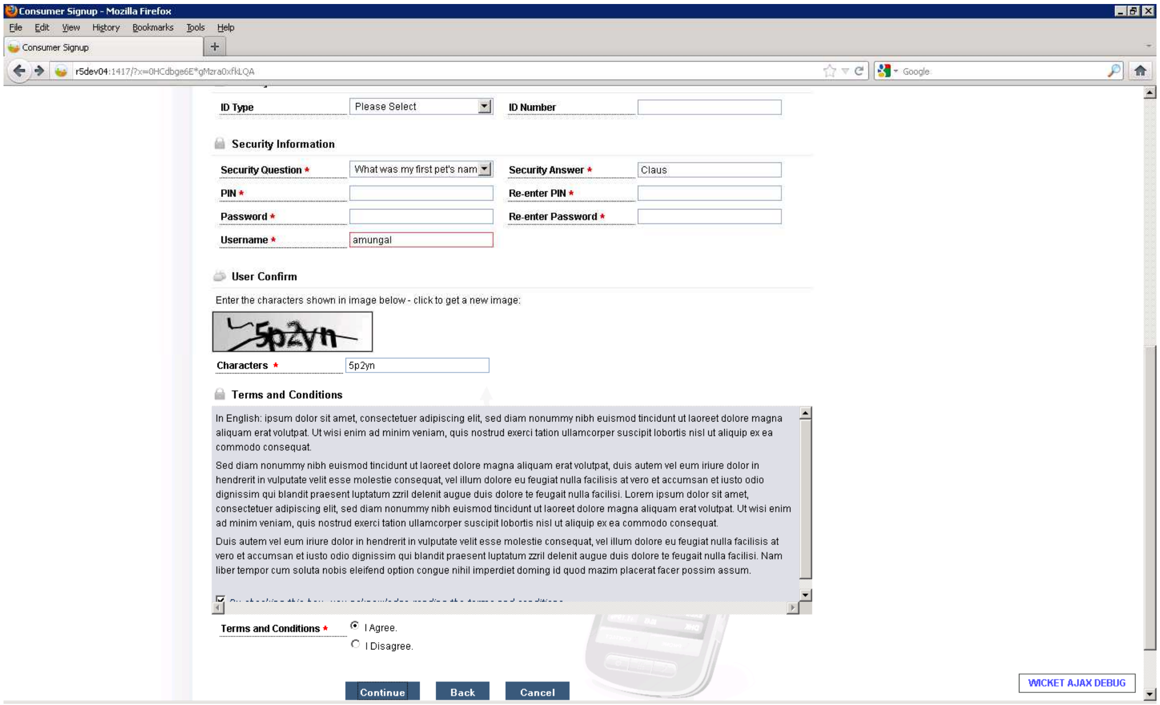
In the course of the signup process you will be asked information about yourself, such as;

- mobile number
- personal details
- your address, and
- bank account information

If you are not willing to provide us with this information you may not sign up to use this service.

Continue
Cancel
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 29:55 Minutes
SYBASE | An SAP Company

3. Fill in all required information fields, accept Terms and Conditions, and confirm the CAPTCHA image. Click Continue.


Consumer Signup - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Consumer Signup
r5dev04:1417/?x=0HCdbge6E*gMzra0xfkLQA
Google

ID Type	Please Select	ID Number	

Security Information

Security Question *	What was my first pet's nam	Security Answer *	Claus
PIN *		Re-enter PIN *	
Password *		Re-enter Password *	
Username *	amungal		

User Confirm

Enter the characters shown in image below - click to get a new image:

Characters * 5p2yn

Terms and Conditions

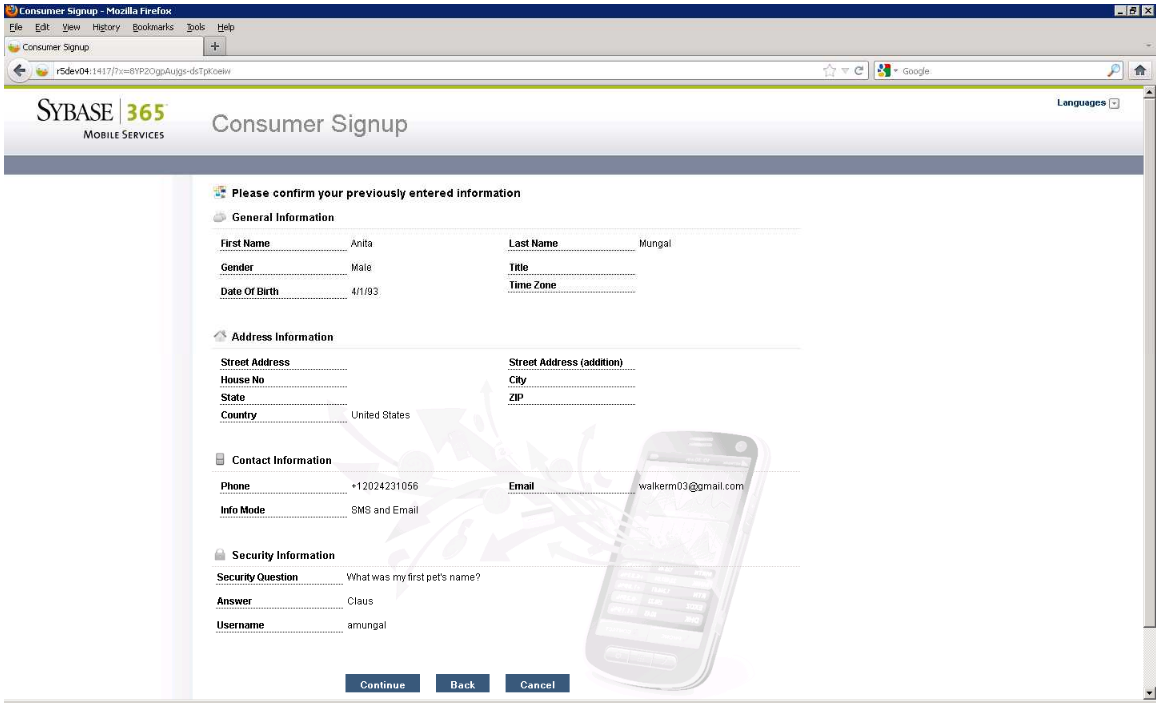
In English: ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat, duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum.

Terms and Conditions * ● I Agree. ○ I Disagree.

4. At the account summary page click Continue again


Consumer Signup - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Consumer Signup
r5dev04:1417/?x=8YP2OgpAujgs-dsTpKoeiw
Google
SYBASE 365 MOBILE SERVICES
Languages

Consumer Signup

Please confirm your previously entered information

General Information

First Name	Anita	Last Name	Mungal
Gender	Male	Title	
Date Of Birth	4/1/93	Time Zone	

Address Information

Street Address		Street Address (addition)	
House No		City	
State		ZIP	
Country	United States		

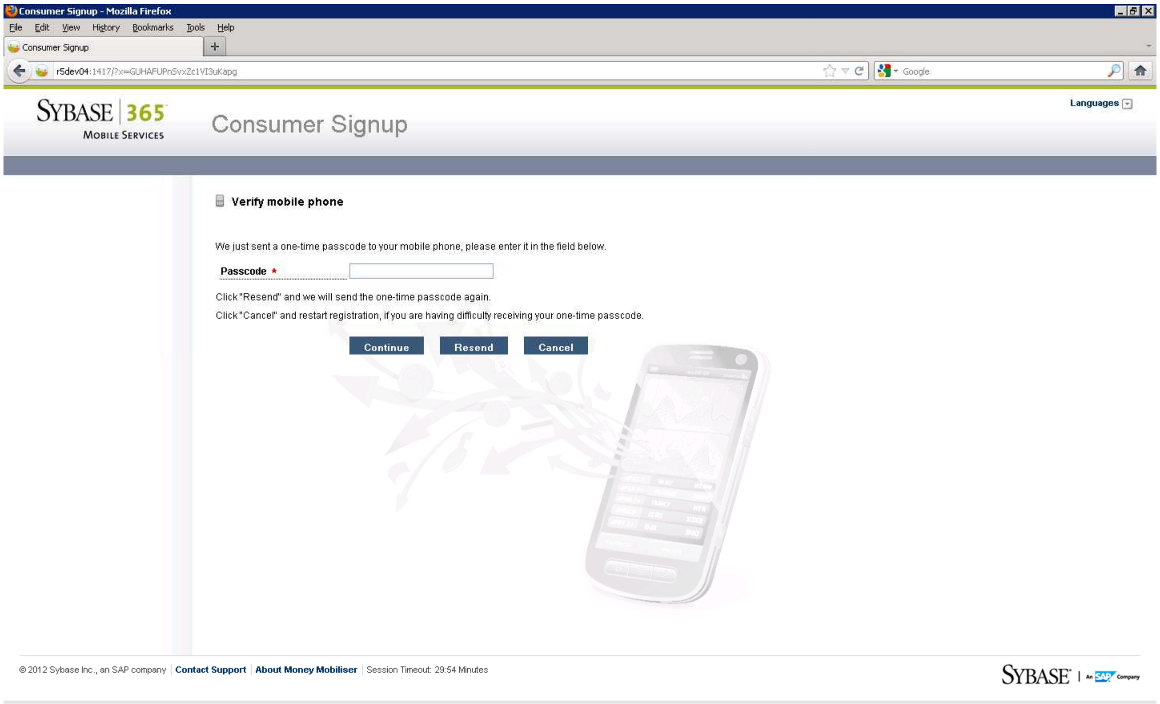
Contact Information

Phone	+12024231056	Email	walkerm03@gmail.com
Info Mode	SMS and Email		

Security Information

Security Question	What was my first pet's name?
Answer	Claus
Username	amungal

5. At the final part of the consumer signup, you will be asked for an OTP code to finalize the creation of the account.


Consumer Signup - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Consumer Signup
r5dev04:1417/?x=GUHAFUPnSvxZc1VI3uKapg
Google
SYBASE 365 MOBILE SERVICES
Languages

Consumer Signup

Verify mobile phone

We just sent a one-time passcode to your mobile phone, please enter it in the field below.

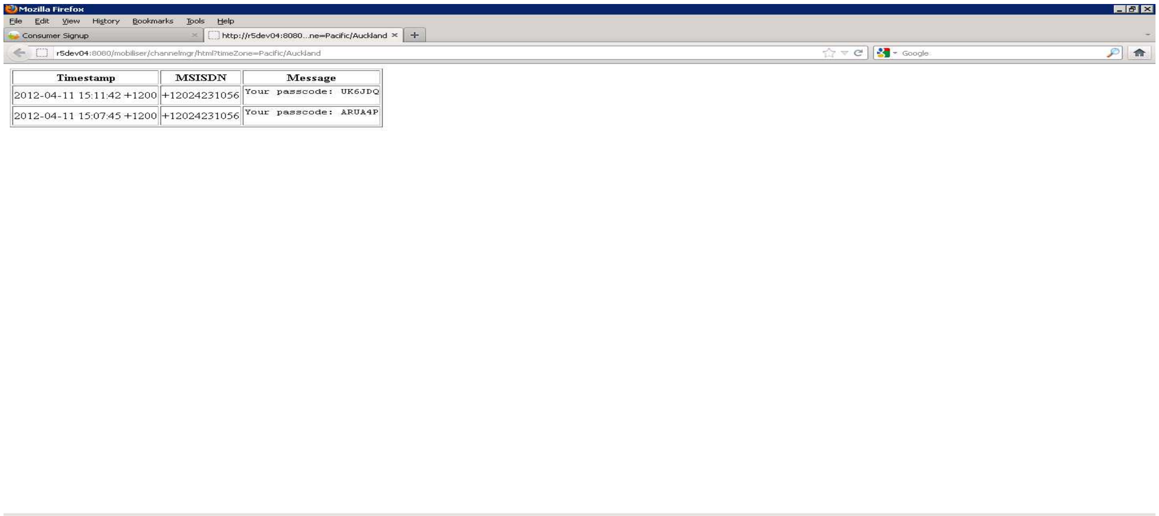
Passcode *

Click "Resend" and we will send the one-time passcode again.

Click "Cancel" and restart registration, if you are having difficulty receiving your one-time passcode.

Continue
Resend
Cancel
© 2012 Sybase Inc., an SAP company
Contact Support
About Money Mobiliser
Session Timeout: 29:54 Minutes
SYBASE An SAP Company

6. Go to the Channel Manager console to find the OTP information:
   a. http://<localhost>:8080/mobiliser/channelmgr/html?timeZone=Pacific/Auckland
   b. If asked for credentials to enter page use the following; Mobiliser:secret


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Consumer Signup
http://r5dev04:8080...ne=Pacific/Auckland
r5dev04:8080/mobiliser/channelmgr/html?timeZone=Pacific/Auckland
Google

Timestamp	MSISDN	Message
2012-04-11 15:11:42 +1200	+12024231056	Your passcode: UK6JDQ
2012-04-11 15:07:45 +1200	+12024231056	Your passcode: ARUA4P

7. Enter OTP specified on the page and click Continue
8. You will receive a confirmation page specifying a successful consumer signup, click continue and you will be redirected to the Web UI login page again where you can log in with the newly created Mobiliser account

Operations Dashboard

Overview

This document summarizes the information available from the Mobiliser Platform 5.1 container for managing and operating the Mobiliser 5.1 environment using the Operations Dashboard Web portal application and the interfaces of the Mobiliser Platform 5.1 server.

All information presented is presented as read-only and summarizes or visualizes information accessible through the JMX provided through Mobiliser Platform and the Java virtual machine.

This covers the Operations Dashboard pages for:

- System/Environment Information
- Mobiliser Requests Information
- Data Access Information
- Messaging/Channel Information
- Event Information
- Task Information
- Trackers

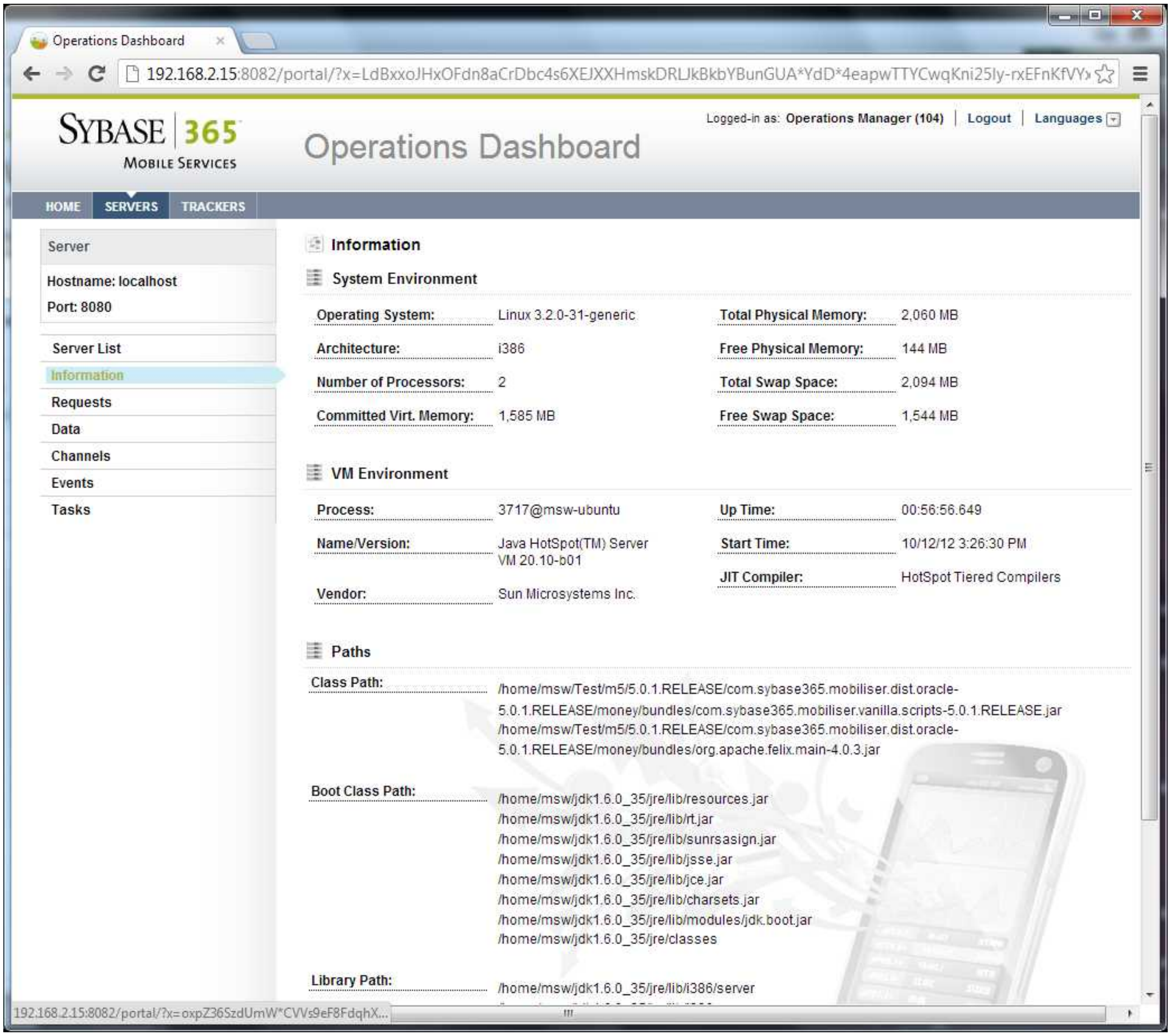
It also includes information on how to develop customized trackers for the Operations Dashboard and provides information on how other interfaces outside the Money Mobiliser Operations Dashboard Web Portal can access the same set of information through:

- Mobiliser Management SOAP/REST Interfaces
- JMX RMI

JVM/System Environment Pages

Summarizes the JVM and basic system environment the Mobiliser container is running in.
Key information:

- Up time
- Total/Free Physical Memory & Committed Virtual Memory
- Total Swap/Free Swap


Operations Dashboard
192.168.2.15:8082/portal/?x=LdBxxoJHxOFdn8aCrDbc4s6XEJXXHmskDRLJkBkbYBunGUA*YdD*4eapwTTYCwqKni25ly-rxEFnKfVY›
SYBASE 365
MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104)
Logout
Languages
HOME
SERVERS
TRACKERS
Server List
Information
Requests
Data
Channels
Events
Tasks
192.168.2.15:8082/portal/?x=oxpZ36SzdUmW*CVVs9eF8FdqhX...

Server

Hostname: localhost

Port: 8080

Information

System Environment

Operating System:	Linux 3.2.0-31-generic	Total Physical Memory:	2,060 MB
Architecture:	i386	Free Physical Memory:	144 MB
Number of Processors:	2	Total Swap Space:	2,094 MB
Committed Virt. Memory:	1,585 MB	Free Swap Space:	1,544 MB

VM Environment

Process:	3717@msw-ubuntu	Up Time:	00:56:56.649
Name/Version:	Java HotSpot(TM) Server VM 20.10-b01	Start Time:	10/12/12 3:26:30 PM
Vendor:	Sun Microsystems Inc.	JIT Compiler:	HotSpot Tiered Compilers

Paths

Class Path:

```
/home/msw/Test/m5/5.0.1.RELEASE/com.sybase365.mobiliser.dist.oracle-
5.0.1.RELEASE/money/bundles/com.sybase365.mobiliser.vanilla.scripts-5.0.1.RELEASE.jar
/home/msw/Test/m5/5.0.1.RELEASE/com.sybase365.mobiliser.dist.oracle-
5.0.1.RELEASE/money/bundles/org.apache.felix.main-4.0.3.jar
```

Boot Class Path:

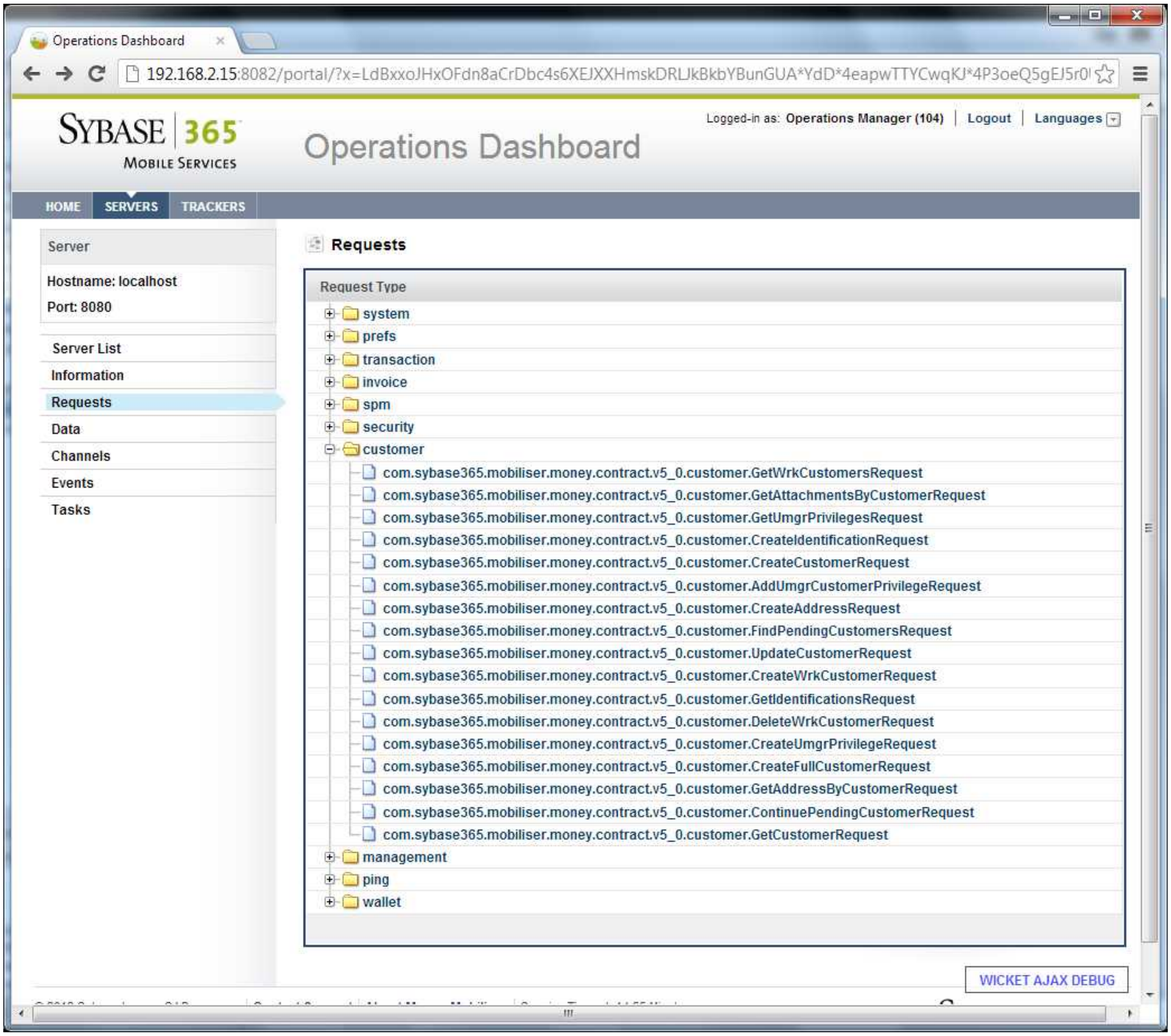
```
/home/msw/jdk1.6.0_35/jre/lib/resources.jar
/home/msw/jdk1.6.0_35/jre/lib/rt.jar
/home/msw/jdk1.6.0_35/jre/lib/sunrsasign.jar
/home/msw/jdk1.6.0_35/jre/lib/jsse.jar
/home/msw/jdk1.6.0_35/jre/lib/jce.jar
/home/msw/jdk1.6.0_35/jre/lib/charsets.jar
/home/msw/jdk1.6.0_35/jre/lib/modules/jdk.boot.jar
/home/msw/jdk1.6.0_35/jre/classes
```

Library Path:

```
/home/msw/jdk1.6.0_35/jre/lib/i386/server
```

Mobiliser Requests Information

Allows display and selection of any or all request made into the Mobiliser Platform server.



Operations Dashboard
192.168.2.15:8082/portal/?x=LdBxxoJHxOFdn8aCrDbc4s6XEJXXHmskDRLJkBkbYBunGUA*YdD*4eapwTTYCwqKJ*4P3oeQ5gEJ5r0!
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
Server List
Information
Requests
Data
Channels
Events
Tasks
WICKET AJAX DEBUG

Server

Hostname: localhost

Port: 8080

Requests

Request Type

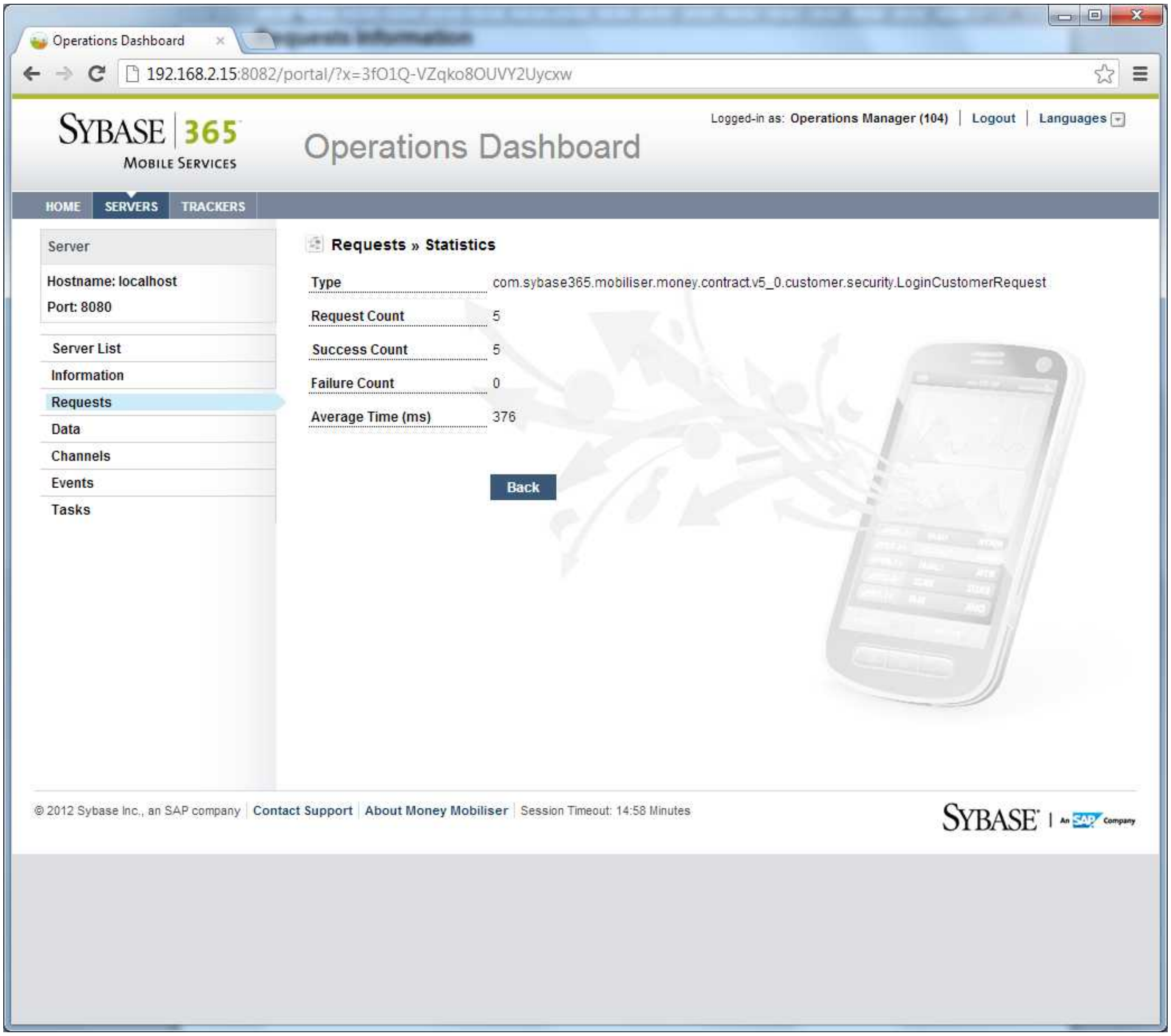
- system
- prefs
- transaction
- invoice
- spm
- security
- customer
  - com.sybase365.mobiliser.money.contract.v5_0.customer.GetWrkCustomersRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.GetAttachmentsByCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.GetUmgrPrivilegesRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.CreateIdentificationRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.CreateCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.AddUmgrCustomerPrivilegeRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.CreateAddressRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.FindPendingCustomersRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.UpdateCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.CreateWrkCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.GetIdentificationsRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.DeleteWrkCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.CreateUmgrPrivilegeRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.CreateFullCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.GetAddressByCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.ContinuePendingCustomerRequest
  - com.sybase365.mobiliser.money.contract.v5_0.customer.GetCustomerRequest
- management
- ping
- wallet

Mobiliser Requests Statistics

Allows drill down into statistics on each request made into the Mobiliser Platform server.

Key information:

- Total requests
- Requests succeeded/failed
- Average response time



Hostname: localhost

Port: 8080

Requests » Statistics

Type	com.sybase365.mobiliser.money.contract.v5_0.customer.security.LoginCustomerRequest
Request Count	5
Success Count	5
Failure Count	0
Average Time (ms)	376

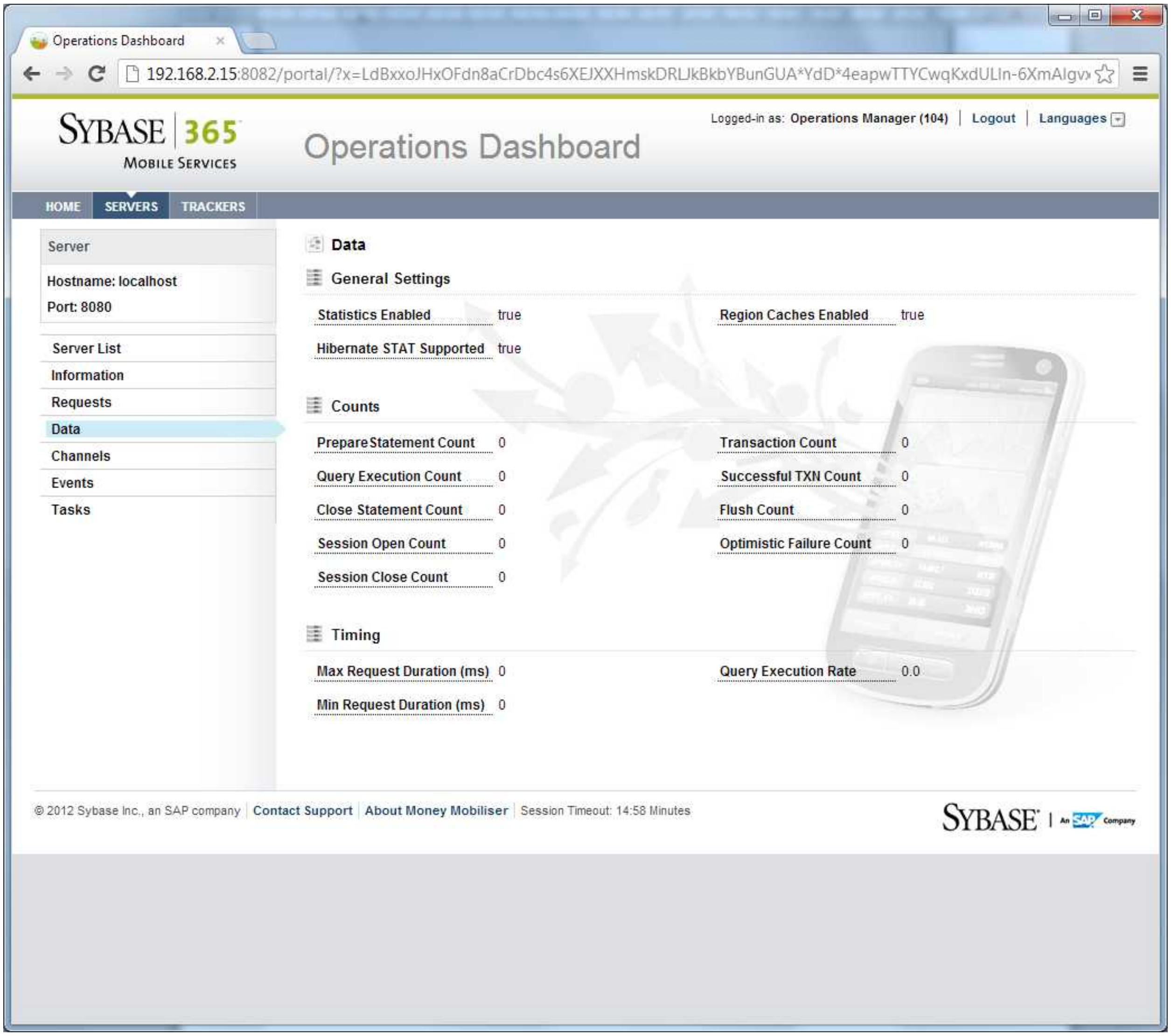
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:58 Minutes

Data Access Information

Reports on information made available from the database access and caching layer. (Is by default off and needs to be turned on/off manually due to extra load generated).

Key information:

- Counts of sessions opened/closed
- Transactions (database).
- Max/Min request duration
- Query execution rate


Operations Dashboard
192.168.2.15:8082/portal/?x=LdBxxoJHxOFdn8aCrDbc4s6XEJXXHmskDRLJkBkbYBunGUA*YdD*4eapwTTYCwqKxdULIn-6XmAlgv
SYBASE 365
MOBILE SERVICES
Logged-in as: Operations Manager (104)
Logout
Languages
HOME
SERVERS
TRACKERS
Server List
Information
Requests
Data
Channels
Events
Tasks

Operations Dashboard

Server

Hostname: localhost

Port: 8080

Data

General Settings

Statistics Enabled	true	Region Caches Enabled	true
Hibernate STAT Supported	true		

Counts

PrepareStatement Count	0	Transaction Count	0
Query Execution Count	0	Successful TXN Count	0
Close Statement Count	0	Flush Count	0
Session Open Count	0	Optimistic Failure Count	0
Session Close Count	0		

Timing

Max Request Duration (ms)	0	Query Execution Rate	0.0
Min Request Duration (ms)	0		

© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:58 Minutes

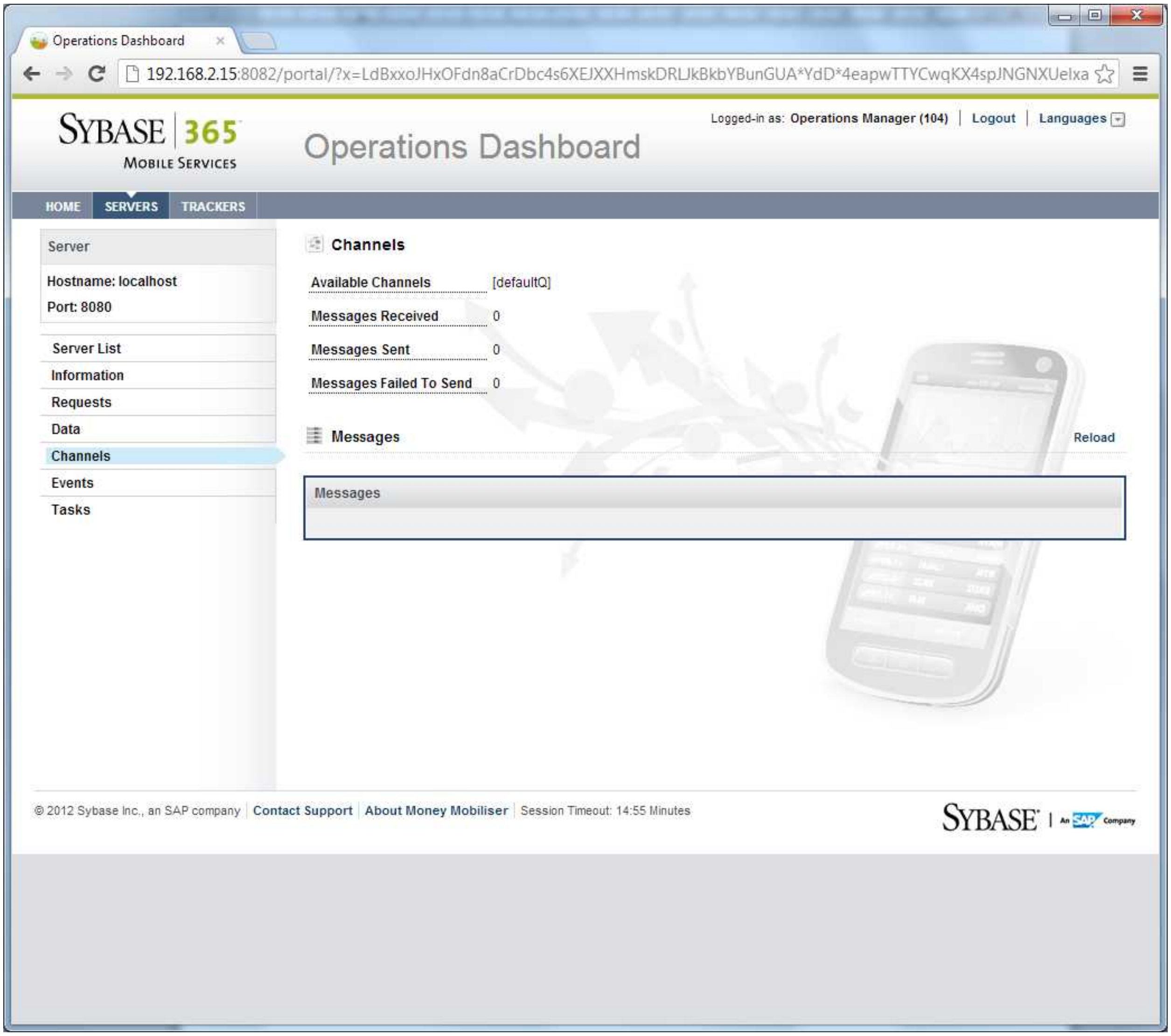
SYBASE | An SAP Company

Messaging/Channel Information

Reports statistics generated by the Mobiliser messaging services. Also shows information (contents encrypted of last 100 messages generated).

Key information:

- Messages Sent/Received
- Messages failed to send



Operations Dashboard
192.168.2.15:8082/portal/?x=LdBxxoJHxOFdn8aCrDbc4s6XEJXXHmskDRLJkBkbYBunGUA*YdD*4eapwTTYCwqKX4spJNGNXUelxa
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
Server
Server List
Information
Requests
Data
Channels
Events
Tasks
Channels
Messages
Reload
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:55 Minutes
SYBASE | An SAP Company

Hostname: localhost
Port: 8080

Available Channels	[defaultQ]
Messages Received	0
Messages Sent	0
Messages Failed To Send	0

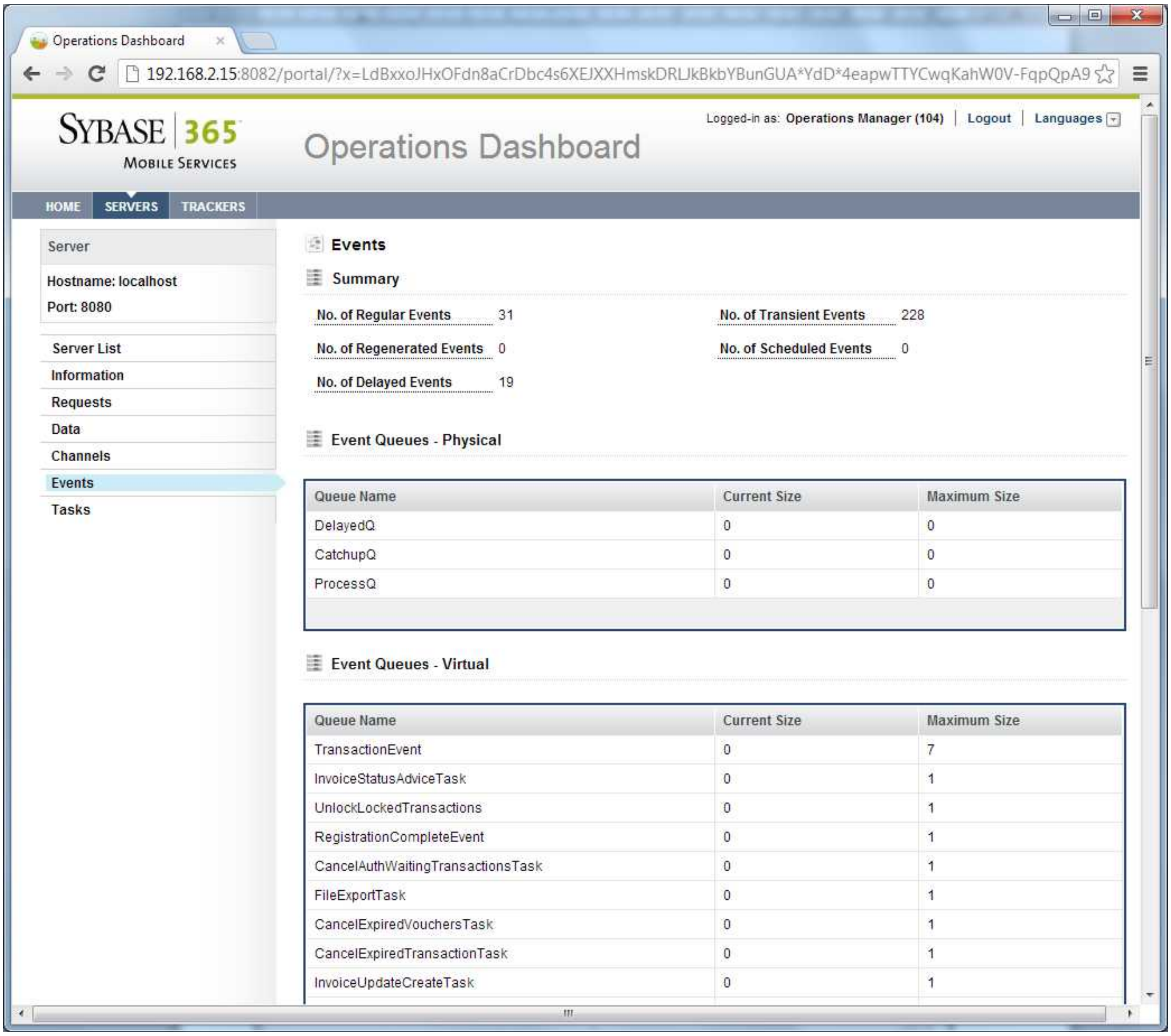
Messages

Event Information

Shows statistics generated by the Mobiliser event system. Events are internal actions that process independently of the originating. Allows drill down into Event Handler information and statistics.

Key information:

- Internal physical event queue sizes
- Internal virtual queue sizes for each different registered event type


Operations Dashboard
192.168.2.15:8082/portal/?x=LdBxxoJHxOFdn8aCrDbc4s6XEJXXHmskDRLJkBkbYBunGUA*YdD*4eapwTTYCwqKahW0V-FqpQpA9
SYBASE 365
MOBILE SERVICES
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
Server List
Information
Requests
Data
Channels
Events
Tasks

Operations Dashboard

Server

Hostname: localhost

Port: 8080

Events

Summary

No. of Regular Events	31	No. of Transient Events	228
No. of Regenerated Events	0	No. of Scheduled Events	0
No. of Delayed Events	19		

Event Queues - Physical

Queue Name	Current Size	Maximum Size
DelayedQ	0	0
CatchupQ	0	0
ProcessQ	0	0

Event Queues - Virtual

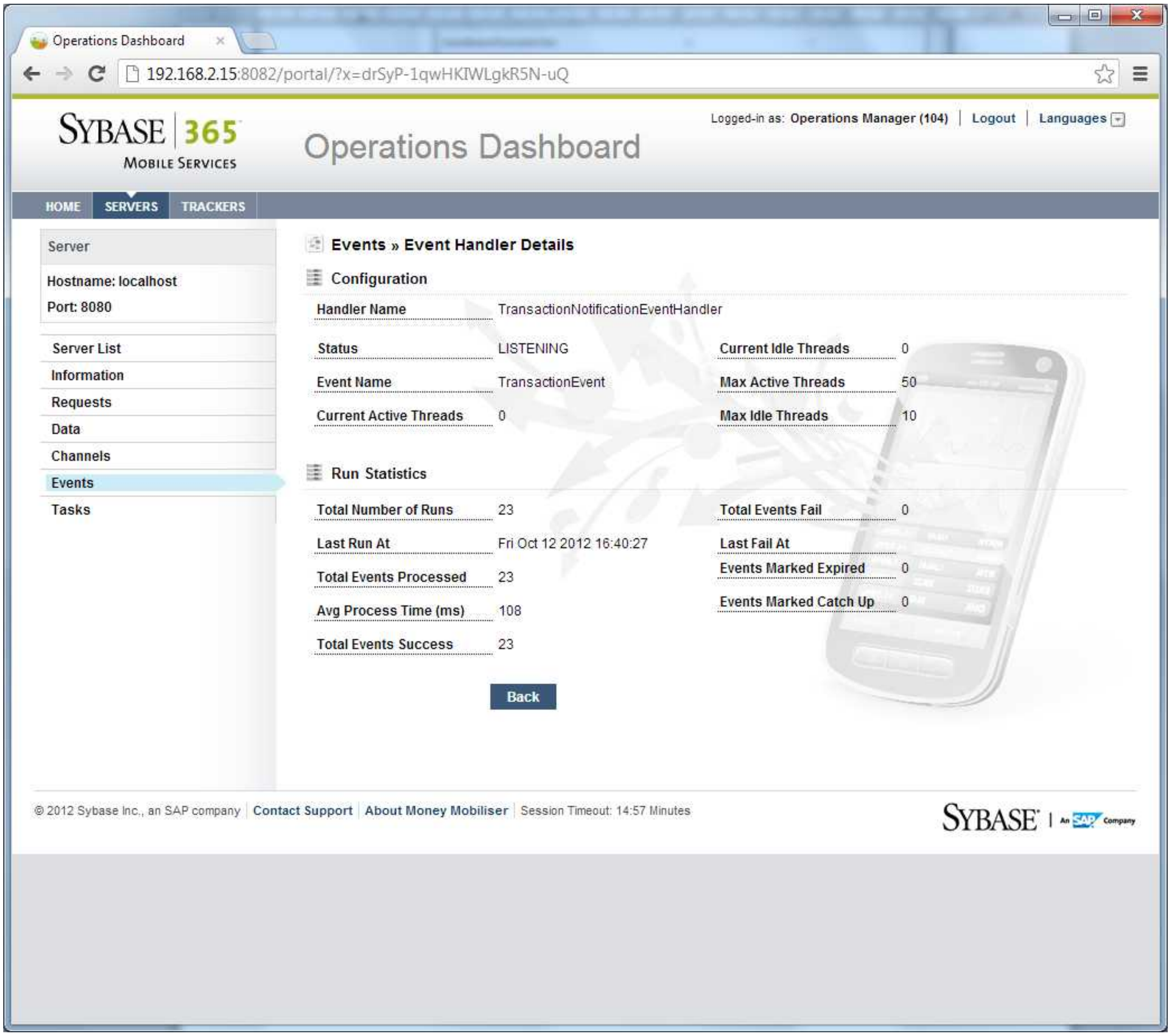
Queue Name	Current Size	Maximum Size
TransactionEvent	0	7
InvoiceStatusAdviceTask	0	1
UnlockLockedTransactions	0	1
RegistrationCompleteEvent	0	1
CancelAuthWaitingTransactionsTask	0	1
FileExportTask	0	1
CancelExpiredVouchersTask	0	1
CancelExpiredTransactionTask	0	1
InvoiceUpdateCreateTask	0	1

Event Handler Details

Allows drill down into Event Handler information and statistics.

Key information:

- Active/Idle Threads for this event handler
- Maximum Active/Idle Threads allocated for this event handler
- Handler run statistics; last run at date/time, last fail at date/time.
- Events processed successfully/failed/total
- Average process time



Operations Dashboard
192.168.2.15:8082/portal/?x=drSyP-1qwHKIWLgkR5N-uQ
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
Server
Server List
Information
Requests
Data
Channels
Events
Tasks
Back
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:57 Minutes
SYBASE | An SAP Company

Hostname: localhost

Port: 8080

Events » Event Handler Details

Configuration

Handler Name	TransactionNotificationEventHandler		
Status	LISTENING	Current Idle Threads	0
Event Name	TransactionEvent	Max Active Threads	50
Current Active Threads	0	Max Idle Threads	10

Run Statistics

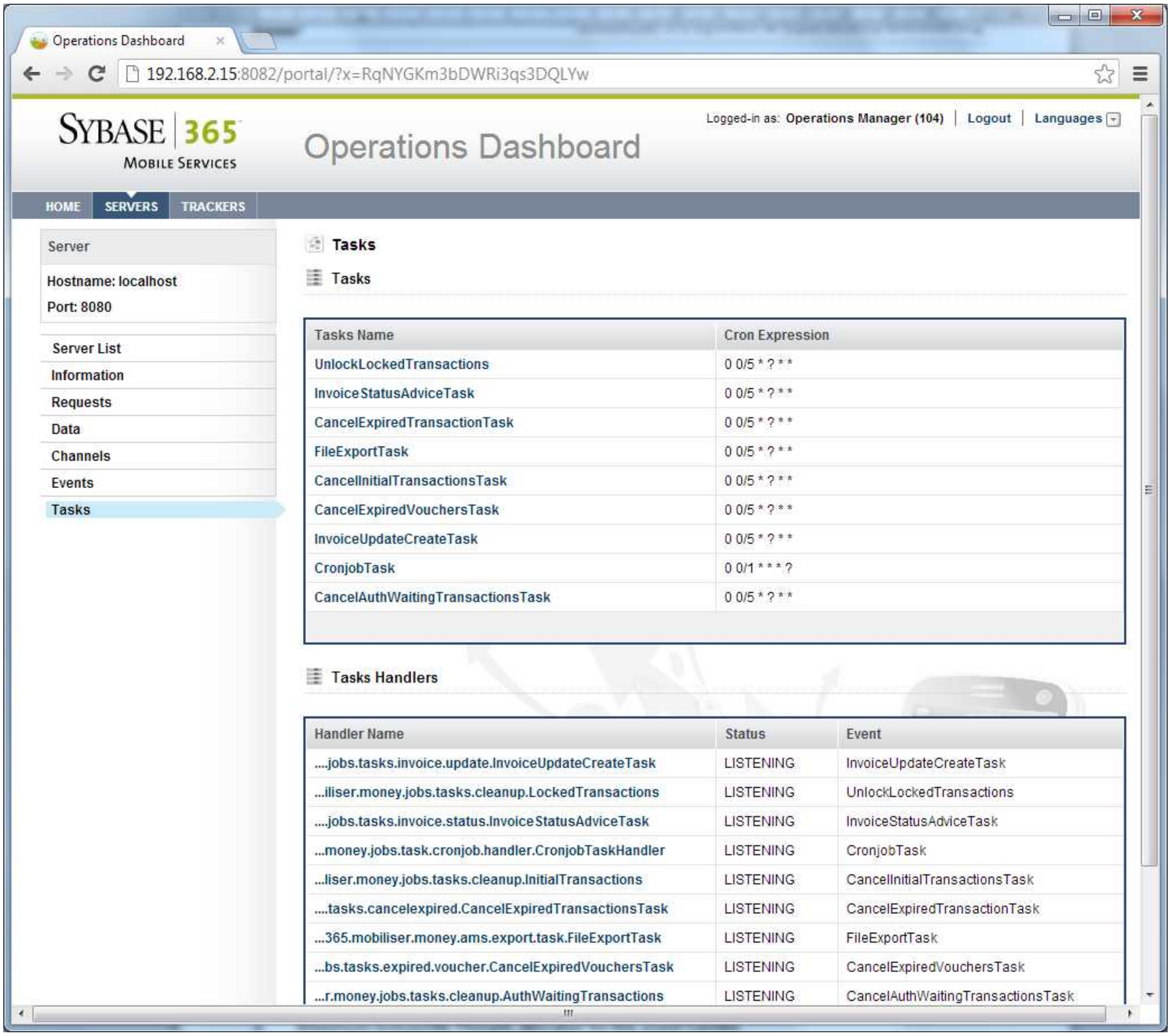
Total Number of Runs	23	Total Events Fail	0
Last Run At	Fri Oct 12 2012 16:40:27	Last Fail At	
Total Events Processed	23	Events Marked Expired	0
Avg Process Time (ms)	108	Events Marked Catch Up	0
Total Events Success	23		

Task Information

Shows statistics generated by the Mobiliser event system for tasks. Tasks are internal date/time scheduled actions. Allows drill down into Task Handler information and statistics.

Key information:

- Schedule of tasks
- Status of task handlers



Operations Dashboard

Server

Hostname: localhost

Port: 8080

Tasks

Tasks

Tasks Name	Cron Expression
UnlockLockedTransactions	0 0/5 * ? * *
InvoiceStatusAdviceTask	0 0/5 * ? * *
CancelExpiredTransactionTask	0 0/5 * ? * *
FileExportTask	0 0/5 * ? * *
CancelInitialTransactionsTask	0 0/5 * ? * *
CancelExpiredVouchersTask	0 0/5 * ? * *
InvoiceUpdateCreateTask	0 0/5 * ? * *
CronjobTask	0 0/1 * * * ?
CancelAuthWaitingTransactionsTask	0 0/5 * ? * *

Tasks Handlers

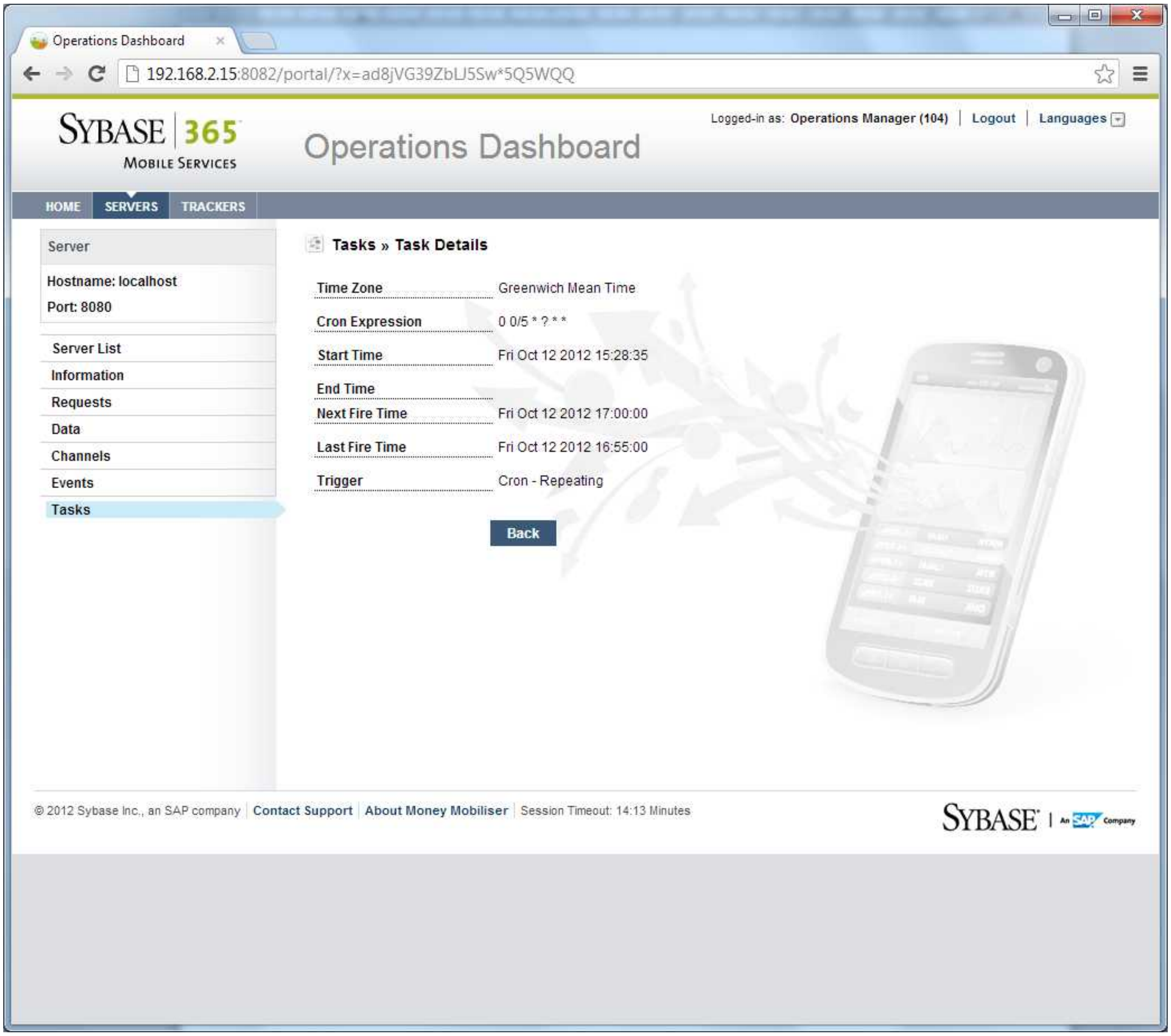
Handler Name	Status	Event
....jobs.tasks.invoice.update.InvoiceUpdateCreateTask	LISTENING	InvoiceUpdateCreateTask
...iliser.money.jobs.tasks.cleanup.LockedTransactions	LISTENING	UnlockLockedTransactions
....jobs.tasks.invoice.status.InvoiceStatusAdviceTask	LISTENING	InvoiceStatusAdviceTask
...money.jobs.task.cronjob.handler.CronjobTaskHandler	LISTENING	CronjobTask
...liser.money.jobs.tasks.cleanup.InitialTransactions	LISTENING	CancelInitialTransactionsTask
....tasks.cancelexpired.CancelExpiredTransactionsTask	LISTENING	CancelExpiredTransactionTask
...365.mobiliser.money.ams.export.task.FileExportTask	LISTENING	FileExportTask
...bs.tasks.expired.voucher.CancelExpiredVouchersTask	LISTENING	CancelExpiredVouchersTask
...r.money.jobs.tasks.cleanup.AuthWaitingTransactions	LISTENING	CancelAuthWaitingTransactionsTask

Task Details

Allows drill down into Task information and statistics.

Key information:

- Task fire (start) timings; last/next



Operations Dashboard
192.168.2.15:8082/portal/?x=ad8jVG39ZbLJ5Sw*5Q5WQQ
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
Server
Hostname: localhost
Port: 8080
Server List
Information
Requests
Data
Channels
Events
Tasks
Back
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:13 Minutes

Tasks » Task Details

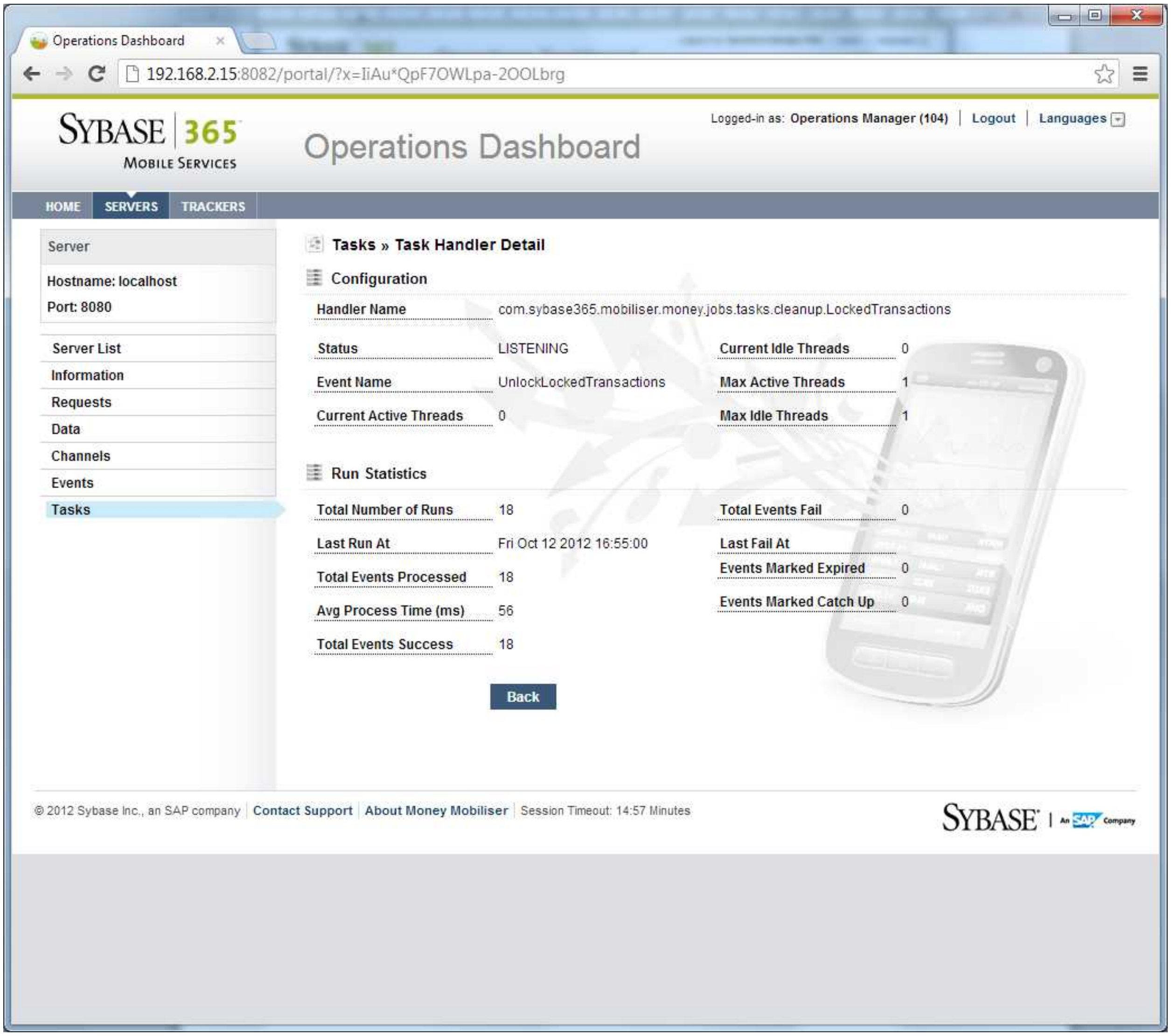
Time Zone	Greenwich Mean Time
Cron Expression	0 0/5 * ? * *
Start Time	Fri Oct 12 2012 15:28:35
End Time	
Next Fire Time	Fri Oct 12 2012 17:00:00
Last Fire Time	Fri Oct 12 2012 16:55:00
Trigger	Cron - Repeating

Task Handler Details

Also, allows drill down into Task Handler information and statistics.

Key information:

- Active/Idle Threads for this event handler
- Maximum Active/Idle Threads allocated for this event handler
- Handler run statistics; last run at date/time, last fail at date/time.
- Events processed successfully/failed/total
- Average process time



Operations Dashboard
192.168.2.15:8082/portal/?x=IiAu*QpF7OWLpa-2OOLbrg
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
Server
Server List
Information
Requests
Data
Channels
Events
Tasks
Back

Hostname: localhost

Port: 8080

Tasks » Task Handler Detail

Configuration

Handler Name	com.sybase365.mobiliser.money.jobs.tasks.cleanup.LockedTransactions		
Status	LISTENING	Current Idle Threads	0
Event Name	UnlockLockedTransactions	Max Active Threads	1
Current Active Threads	0	Max Idle Threads	1

Run Statistics

Total Number of Runs	18	Total Events Fail	0
Last Run At	Fri Oct 12 2012 16:55:00	Last Fail At	
Total Events Processed	18	Events Marked Expired	0
Avg Process Time (ms)	56	Events Marked Catch Up	0
Total Events Success	18		

© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:57 Minutes

SYBASE | An SAP Company

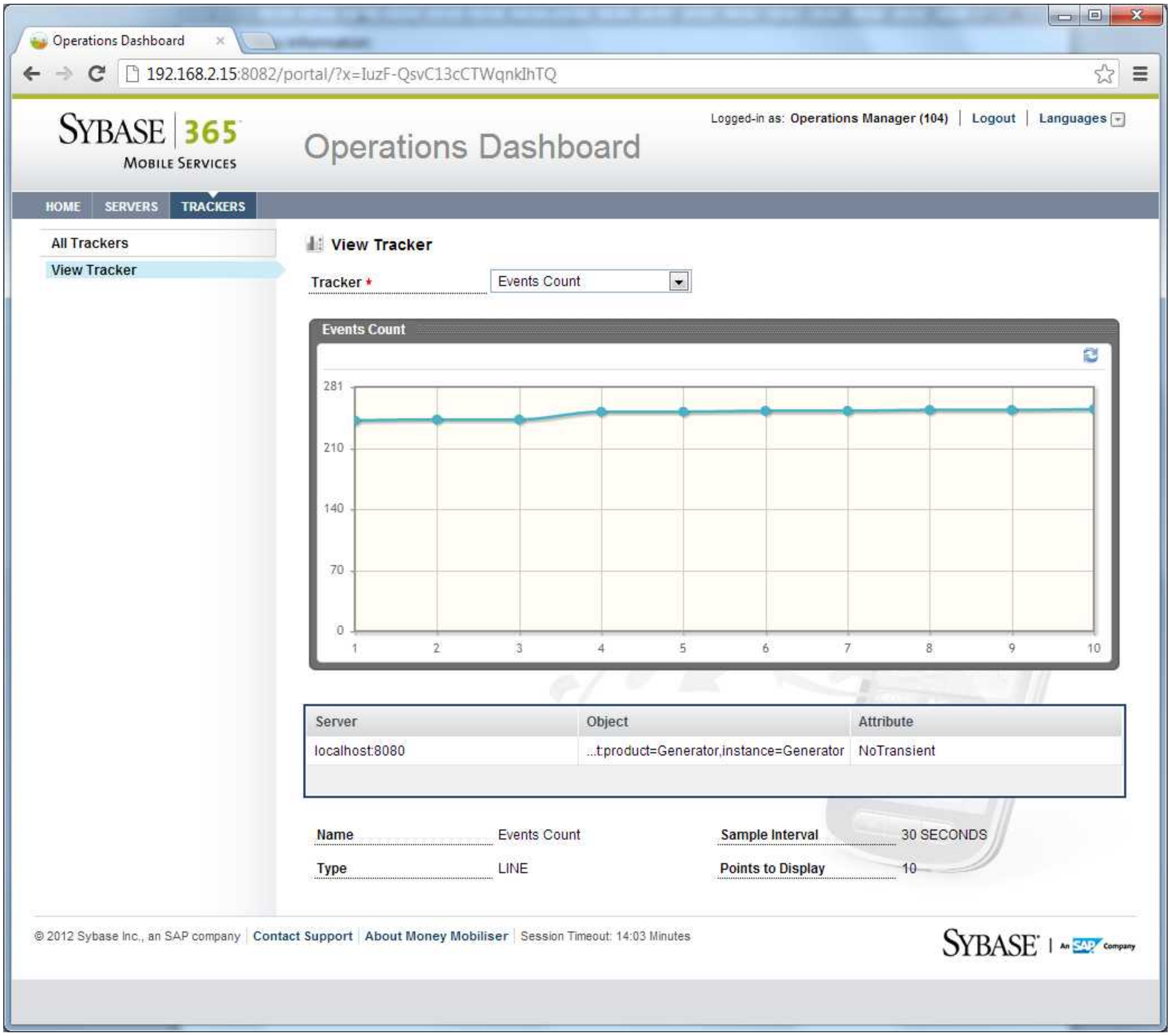
Trackers

Trackers provide a basic visualization of any JMX statistic-type attribute accessible from the Mobiliser JMX platform. (That includes any of the statistics shown above, plus other JMX attribute information available). Chart types are:

- Line
- Bar
- Gauge
- Candlestick

Sample trackers are provided to show visualization of:

- Total generated event count as a line chart

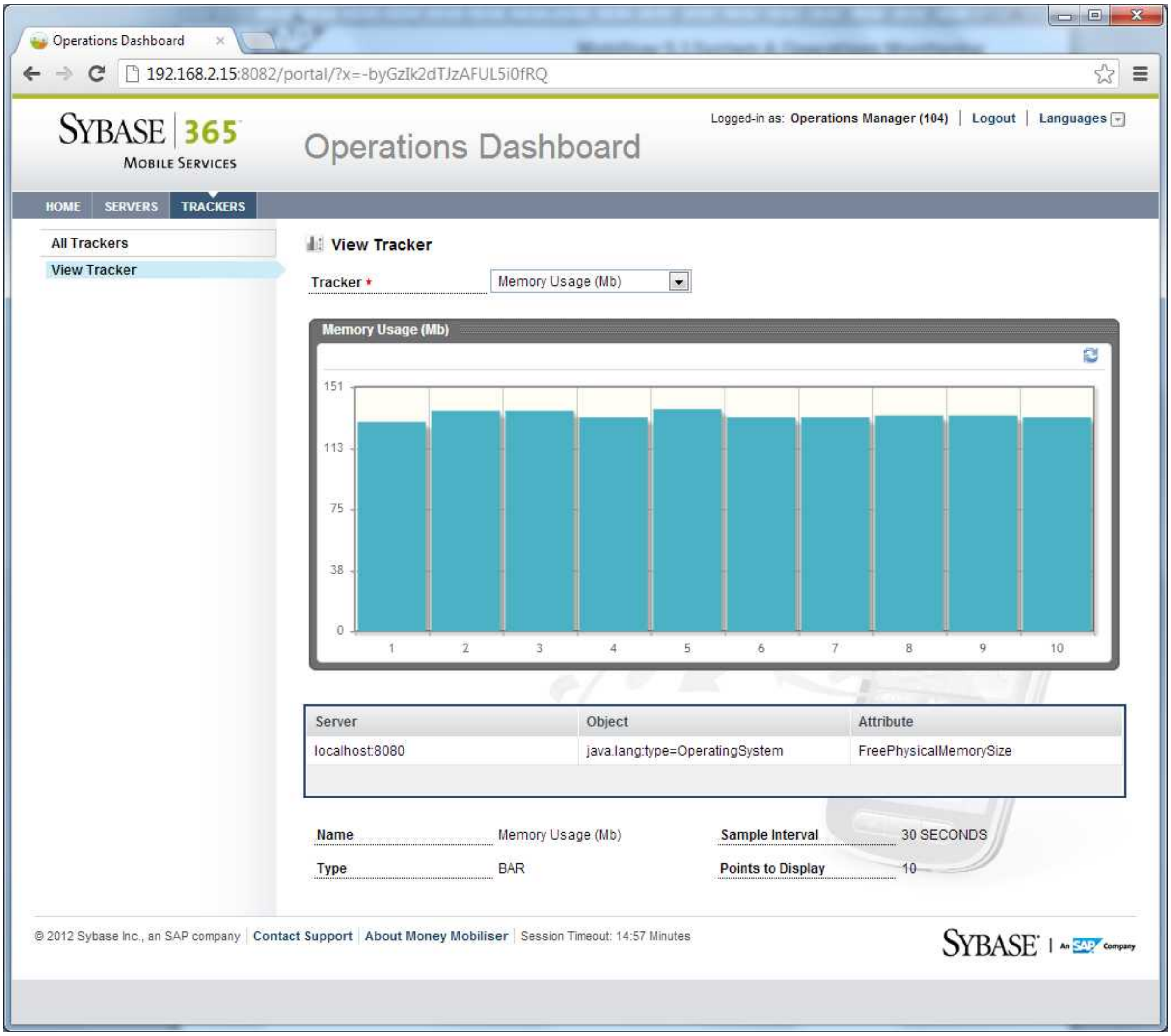

Operations Dashboard
192.168.2.15:8082/portal/?x=IuzF-QsvC13cCTWqnkIhTQ
SYBASE 365 MOBILE SERVICES
Operations Dashboard
Logged-in as: Operations Manager (104) | Logout | Languages
HOME
SERVERS
TRACKERS
All Trackers
View Tracker
View Tracker
Events Count
281
210
140
70
0
1
2
3
4
5
6
7
8
9
10
© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:03 Minutes
SYBASE | An SAP Company

Tracker * Events Count

Server	Object	Attribute
localhost:8080	...t:product=Generator,instance=Generator	NoTransient

Name	Events Count	Sample Interval	30 SECONDS
Type	LINE	Points to Display	10

Memory Usage as a Bar Chart



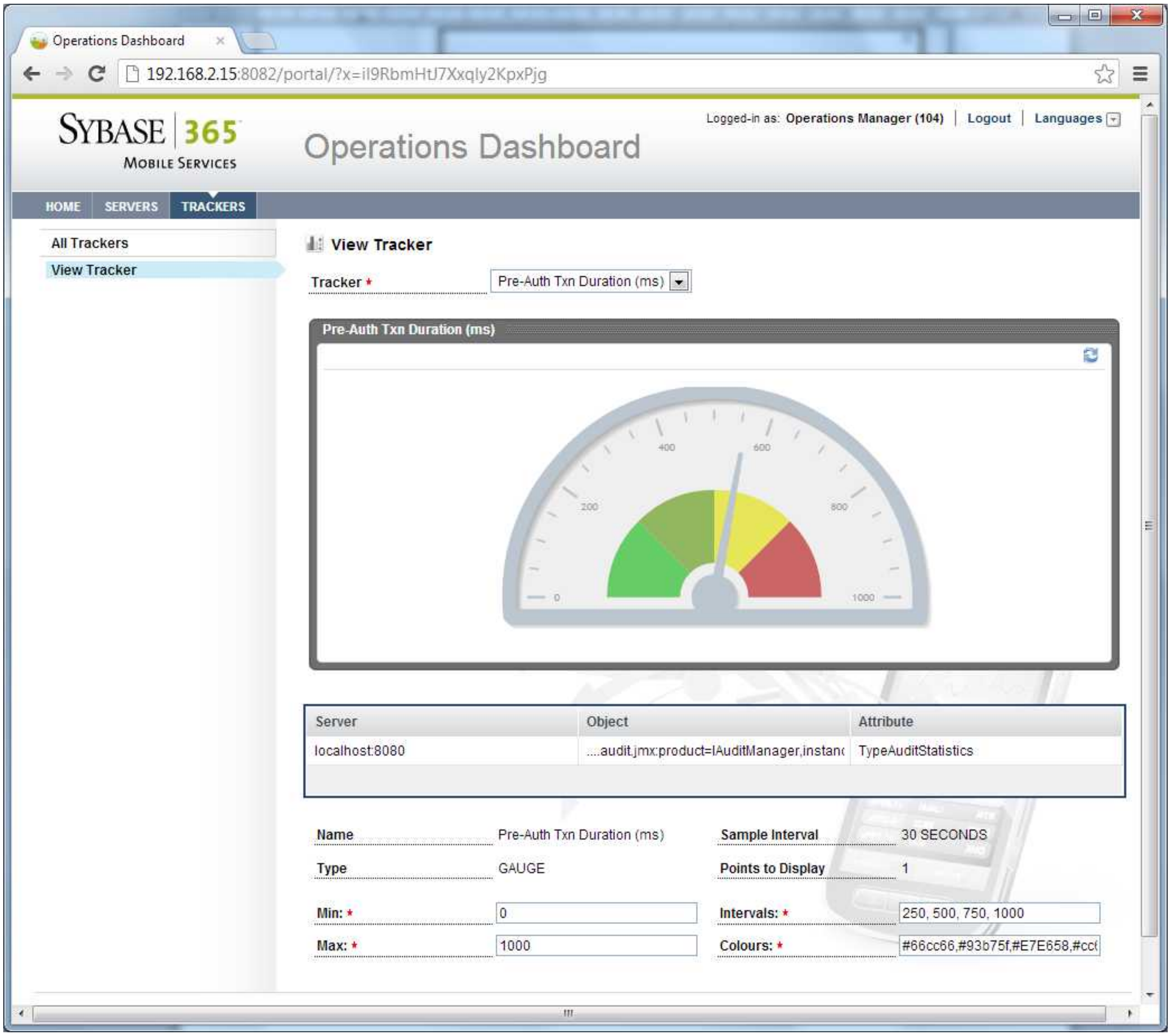
Tracker * Memory Usage (Mb)

Server	Object	Attribute
localhost:8080	java.lang:type=OperatingSystem	FreePhysicalMemorySize

Name	Memory Usage (Mb)	Sample Interval	30 SECONDS
Type	BAR	Points to Display	10

© 2012 Sybase Inc., an SAP company | Contact Support | About Money Mobiliser | Session Timeout: 14:57 Minutes

Pre-Authorization of Transaction Request as a Gauge Chart



Tracker * Pre-Auth Txn Duration (ms)

Server	Object	Attribute
localhost:8080	....audit.jmx:product=IAuditManager,instanc	TypeAuditStatistics

Name	Pre-Auth Txn Duration (ms)	Sample Interval	30 SECONDS
Type	GAUGE	Points to Display	1
Min: *	0	Intervals: *	250, 500, 750, 1000
Max: *	1000	Colours: *	#66cc66,#93b75f,#E7E658,#cc(

Customized Trackers

New trackers can be added using simple configuration of the Web portal application.

- *Step 1: Specify the location of the data series for the tracker.*
- *Step 2: Specify the tracker type linking to the data series*
- *Step 3: Add to list of known trackers*

./webapps/portal/WEB-INF/trackers-context.xml:

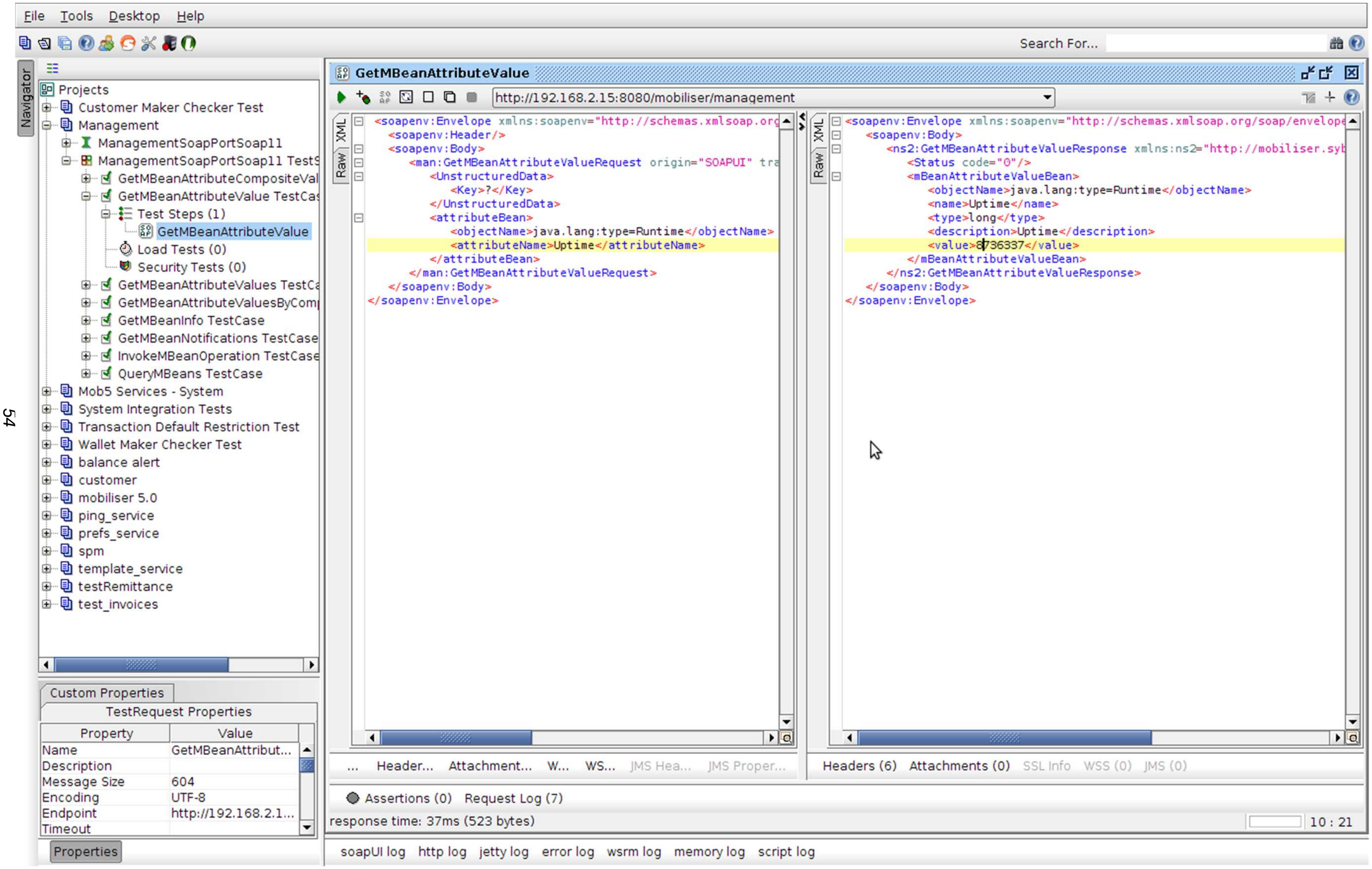
```
…
<!--
 DASHBOARD TRACKERS
  -->
<bean id="loginReqCntDataSeries"
class="com.sybase365.mobiliser.web.dashboard.pages.trackers.beans.TrackerDataSeriesBean">
  <property name="server" value="localhost:8080" />
  <property name="objectName"
value="com.sybase365.mobiliser.framework.service.audit.jmx:product=IAuditManager,instance=JmxAuditManager" />
  <property name="attribute" value="TypeAuditStatistics" />
  <property name="keyName" value="requestType" />
  <property name="keyValue"
value="com.sybase365.mobiliser.money.contract.v5_0.customer.security.LoginCustomerRequest" />
  <property name="valueName" value="successCount" />
  <property name="numberOfDataPoints" value="10" />
  <property name="dataSeriesDao" ref="trackersDataSeriesDao" />
</bean>
…
<bean id="loginReqCntTracker"
class="com.sybase365.mobiliser.web.dashboard.pages.trackers.beans.TrackerBean" init-method="init" destroy-method="destroy">
  <property name="name" value="Login Count" />
  <property name="type" ref="LINE" />
  <property name="sampleInterval" value="30" />
  <property name="sampleIntervalTimeUnit" ref="SECONDS" />
  <property name="pointsToDisplay" value="10" />
   <property name="dataSeries">
<util:list>
  <ref local="loginReqCntDataSeries" />
</util:list>
   </property>
</bean>
…
<!--
 DASHBOARD TRACKERS DAO
  -->
<bean id="trackersDao"
class="com.sybase365.mobiliser.web.dashboard.pages.trackers.dao.impl.TrackersSpringDaoImpl">
<property name="trackers">
<util:list>
…
  <ref local="loginReqCntTracker" />
…
  </util:list>
  </property>
</bean>
…
```

Management SOAP/REST Interface

The JMX information presented by the Web Operations Dashboard is accessed through the Mobiliser Management endpoint.

This end point translates SOAP requests in to requests for local JMX platform object and attributes information, and sends it back as a SOAP response.

This interface can also be accessed via REST returning XML or JSON data.
Example (from SOAP UI):


File
Tools
Desktop
Help
Search For...
Navigator
Projects
Customer Maker Checker Test
Management
ManagementSoapPortSoap11
ManagementSoapPortSoap11 TestS
GetMBeanAttributeCompositeVal
GetMBeanAttributeValue TestCas
Test Steps (1)
GetMBeanAttributeValue
Load Tests (0)
Security Tests (0)
GetMBeanAttributeValues TestCa
GetMBeanAttributeValuesByComp
GetMBeanInfo TestCase
GetMBeanNotifications TestCase
InvokeMBeanOperation TestCase
QueryMBeans TestCase
Mob5 Services - System
System Integration Tests
Transaction Default Restriction Test
Wallet Maker Checker Test
balance alert
customer
mobiliser 5.0
ping_service
prefs_service
spm
template_service
testRemittance
test_invoices
Custom Properties
TestRequest Properties
Properties
GetMBeanAttributeValue
http://192.168.2.15:8080/mobiliser/management
XML
Raw
... Header... Attachment... W... WS... JMS Hea... JMS Proper...
Headers (6) Attachments (0) SSL Info WSS (0) JMS (0)
Assertions (0) Request Log (7)
10 : 21
soapUI log http log jetty log error log wsrm log memory log script log

Property	Value
Name	GetMBeanAttribut...
Description	
Message Size	604
Encoding	UTF-8
Endpoint	http://192.168.2.1...
Timeout	

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org
  <soapenv:Header/>
  <soapenv:Body>
     <man:GetMBeanAttributeValueRequest origin="SOAPUI" tra
        <UnstructuredData>
           <Key>?</Key>
        </UnstructuredData>
        <attributeBean>
           <objectName>java.lang:type=Runtime</objectName>
           <attributeName>Uptime</attributeName>
        </attributeBean>
     </man:GetMBeanAttributeValueRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope
  <soapenv:Body>
     <ns2:GetMBeanAttributeValueResponse xmlns:ns2="http://mobiliser.syb
        <Status code="0"/>
        <mBeanAttributeValueBean>
           <objectName>java.lang:type=Runtime</objectName>
           <name>Uptime</name>
           <type>long</type>
           <description>Uptime</description>
           <value>8736337</value>
        </mBeanAttributeValueBean>
     </ns2:GetMBeanAttributeValueResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

response time: 37ms (523 bytes)