

**Oracle® Communications Mobile
Synchronization Server**

Installation and Administration Guide

Release 1.0

July 2015

ORACLE®

Oracle Communications Mobile Synchronization Server Installation and Administration Guide, Release 1.0

Copyright © 2007, 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

- 1. Mobile Synchronization Server Technical Overview 4
- 2. Mobile Synchronization Server Release Notes 21
- 3. Mobile Synchronization Server Installation Guide 26
- 4. Mobile Synchronization Server Client Setup Guide for Palm OS 40
- 5. Mobile Synchronization Server Client Setup Guide for Windows Mobile 46
- 6. Mobile Synchronization Server Administration Guide 52
- 7. Setting Up and Managing Mobile Synchronization Server Security 65
- 8. Mobile Synchronization Server Glossary 68

Chapter 1. Mobile Synchronization Server Technical Overview

Oracle Communications Mobile Synchronization Server Technical Overview

This information introduces the architecture of the Oracle Communications Mobile Synchronization Server gateway server and the Oracle Communications Mobile Synchronization Server Clients for Pocket PC, Windows Mobile, and Palm devices. This information also details how these components communicate with each other to provide end users with a seamless data synchronization experience.

Topics:

- [Introduction](#)
- [Architectural Overview](#)
- [Oracle Communications Mobile Synchronization Server Synchronization Engine](#)
- [Oracle Communications Mobile Synchronization Server Clients](#)
- [Transport Layer](#)
- [Push Engine](#)
- [Administration](#)
- [Persistent Store \(Internal Data\) and Databases](#)
- [Universal Data Connector](#)

Introduction

About Industry Standards

The Open Mobile Alliance (OMA) is an umbrella standards organization formed to consolidate the various standards bodies of the mobile industry. Many leading industry consortiums such as the Wireless Village, also known as Instant Messaging and Presence Services (IMPS), the Wireless Access Protocol (WAP) Forum, and the SyncML Initiative have merged into OMA, making it the most important standards body responsible for many network protocols in the mobile industry.

When the SyncML Initiative merged into the OMA, it brought the SyncML-DS and SyncML-DM protocols now called OMA DS and OMA DM. Both OMA DS and OMA DM are based on the SyncML protocol, an Extensible Markup Language (XML) protocol designed for managing and synchronizing mobile devices.

OMA DS focuses on mobile data synchronization and provides a standard protocol for synchronizing Personal Information Manager (PIM) content, such as email, calendar, contacts, tasks, and notes between mobile devices and a server. OMA DS defines the protocol for synchronization, and uses standard data types (MIME types) such as vCard and iCalendar for data exchange. The use of standard data types enables vendor-independent synchronization.

All major device manufacturers are supporters of the OMA, and hundreds of devices on the market are shipping with built-in support for OMA DS.

Oracle Communications Mobile Synchronization Server provides a complete implementation of the OMA DS protocols, including full OMA DS 1.1.2 and 1.2 compatibility, and incorporates support for calendar, contacts and tasks data types. With the recent addition of the Universal Data Connector (UDC), Oracle Communications Mobile Synchronization Server is easily integrated with any third-party data repository, and includes out-of-the-box support for the Oracle Communications Unified Communications Suite.

Oracle Communications Mobile Synchronization Server was designed and built with a carrier-grade architecture, including support for load-balancing and failover, and has proven near-linear scalability.

Oracle makes every endeavor in the design of the application architecture to reduce integration effort. The gateway is based on industry standards widely adopted in the mobile industry, such as Lightweight Directory Access Protocol (LDAP) for interaction with user directories and OMA (Client Provisioning) CP for automatic over-the-air configuration of devices.

Architectural Overview

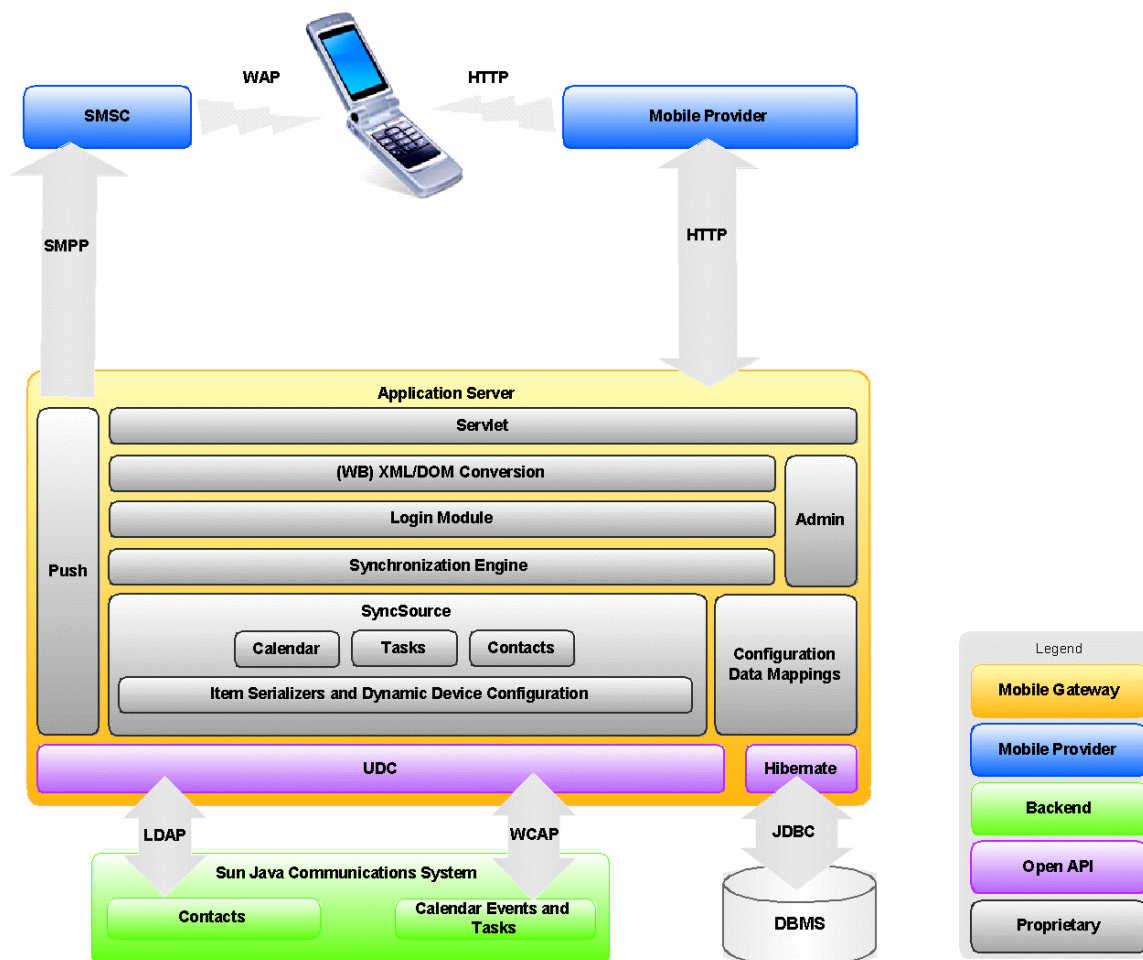
The Oracle Communications Mobile Synchronization Server gateway provides synchronization services for business users, acting as a gateway synchronizing their Oracle Communications Unified Communications Suite accounts with their mobile phone.

The gateway supports synchronization of contacts, calendar events and tasks between SyncML enabled mobile phones and the back-end server.

Because of its industry-standard approach, the gateway does not require additional client software to be installed on the device. While other solutions are limited to the small segment of Smartphones, Oracle Communications Mobile Synchronization Server is compatible with hundreds of SyncML enabled devices from all leading manufacturers. Oracle supplies clients for additional non-SyncML devices and platforms, including Windows Mobile and Palm OS.

The architecture of the gateway is based entirely on open industry standards and is designed to operate a highly scalable, fault-tolerant environment tightly integrated with the existing infrastructure. The gateway includes support for automatic failover and load-balancing, providing near-linear scalability. This architecture has been proven in carrier-grade deployments.

Figure 1 The Oracle Communications Mobile Synchronization Server Architectural Overview



Universal Data Connector (UDC)

On the back-end side, the gateway is based on a flexible plug-in Universal Data Connector (UDC) architecture. Oracle provides a plug-in for the Oracle Communications Unified Communications Suite. The UDC is provided as an open API component enabling easy integration of any third party Personal Information Management system without modification of the core gateway.

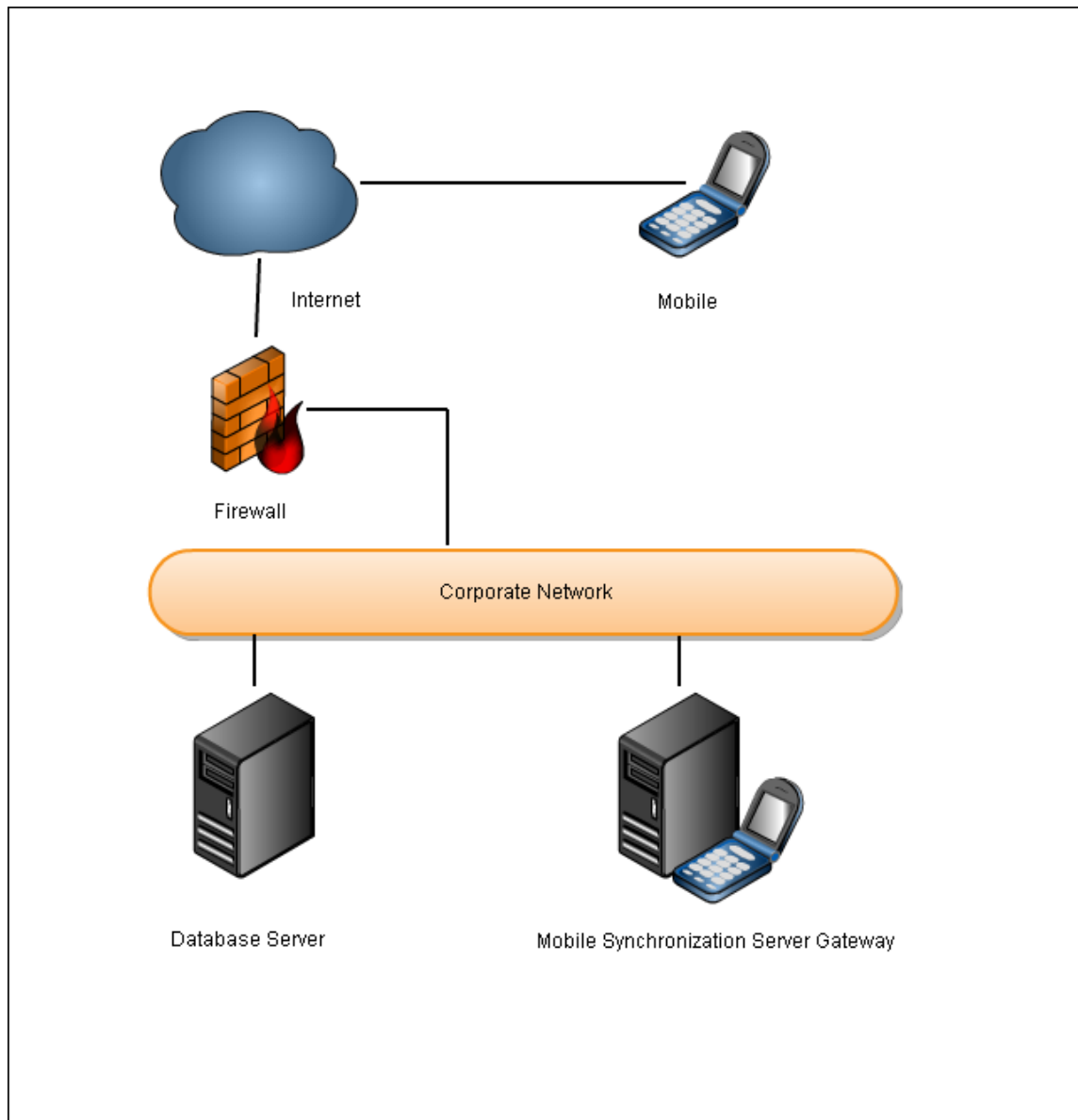
Item Serializers and Dynamic Device Configuration (DDC)

Serializers and deserializers convert a device item's byte array into a Java object (normally a JavaBeans object) and back again. The deserializer converts the byte array received from the client to a Java object for sending to the back-end server. The serializer converts the Java object back to a byte array when sending the item on to the back end server.

Most of the native clients follow the SyncML standard, with only a few device-specific deviations. However, the content of data items, such as a calendar events or contacts, differ sometimes substantially between manufacturers and models. For example, field lengths might differ or the event might use G.M.T. or local time only. To handle these differences, the serializers and deserializers must be device specific.

The gateway addresses the issue of device-specific variations of the SyncML protocol and data items with device specific configurations for the serializers and deserializers according to the phone manufacturer and model. Oracle's Dynamic Device Configuration (DDC) enables the gateway (through a live update mechanism) to stay constantly up to date with changes to these configurations.

Figure 2 Zero Footprint Architecture



Oracle Communications Mobile Synchronization Server features a unique zero footprint architecture that results in a faster adoption rate for mobile synchronization than competing solutions. Like a WAP gateway, which provides wireless access to WAP sites on the public Internet, the Oracle Communications Mobile Synchronization Server gateway provides synchronization services for personal information systems. Unlike other solutions, the Oracle Communications Mobile Synchronization Server gateway requires no installation of client applications on the mobile device. Users simply register at a web site and instantly synchronize their corporate data with mobile devices.

Security

Oracle makes every effort to ensure secure operation of the gateway, which was designed with security in mind. The gateway supports MD5 for encrypted authentication and all traffic flowing through the public Internet is encrypted with SSL (HTTPS), ensuring user data is at no time exposed to prying eyes. For security reasons, the gateway does not duplicate the user's data to a local database, but only meta data required during the synchronization process.

Oracle Communications Unified Communications Suite Integration

The Oracle Communications Mobile Synchronization Server gateway uses LDAP to authenticate users

according to their credentials with Oracle Communications Unified Communications Suite. Calendar items and tasks are synchronized by way of the WCAP adapter, and synchronization of contacts is performed through LDAP. Enhanced security is provided by the usage of the Web Calendar Access Protocol Secure (WCAPS) and Lightweight Directory Access Protocol Secure (LDAPS) protocols.

Network Elements

To provide flexibility, scalability, and high availability, the system architecture is based on a two-tier architecture separating the system into an application server tier (Oracle Communications Mobile Synchronization Server) and a database server tier.

Application Servers

The application server tier consists of one or many application servers running the gateway server application. The application server runs the SyncML Gateway application as well as the user and administration portals.

Oracle Communications Mobile Synchronization Server can be deployed on Oracle9i Application Server (formerly Application Server 9.0 and 9.1) on a variety of platforms including Solaris OS 9 or 10 and Red Hat Enterprise Linux.

Database Server

The database server stores log records created during SyncML sessions as well as user records mapping the user's credentials to the back-end server URL. Note that the database server does not store a replication of the actual user data such as calendar events or contacts. However, the database does act as a central repository for metadata required for synchronization, such as synchronization item IDs and the time and date that each mobile device was last synchronized. The following standard Structured Query Language (SQL) databases can be used: Postgres 8.1, MySQL 5, or Oracle 9.

Scalability and Resilience

Oracle Communications Mobile Synchronization Server has been designed to meet carrier-grade requirements for performance, scalability and stability. It has been demonstrated to support high levels of concurrency per server CPU and provides near-linear scalability in a load-balanced environment. Support for clustered deployments and automatic failover ensures continuous operation of the system in case of a hardware or software failure.

Oracle Communications Mobile Synchronization Server Synchronization Engine

There are two ways to initiate the synchronization process: the user can trigger it manually by selecting the appropriate menu item in the device's SyncML client, or the server can initiate the process (Push). As defined by the Open Mobile Alliance (OMA), for SyncML Push, the server sends a notification message to the device, causing the client to connect back to the server, which then transmits the changes to the device. To the end user, this process is completely transparent and can hardly be distinguished from a direct push where the notification itself contains the data.

During the synchronization session, the gateway receives either an XML byte array, or the compressed format WAP Binary XML (WBXML) which it then converts to XML. The XML or WBXML document is interpreted as a SyncML request that is part of the SyncML session. The synchronization core takes the SyncML requests and sends the client modifications to the back-end, through the Universal Data Connector (UDC), and collects any server modifications. After matching all the modifications (the main activity of synchronization), the server modifications are sent back to the client.

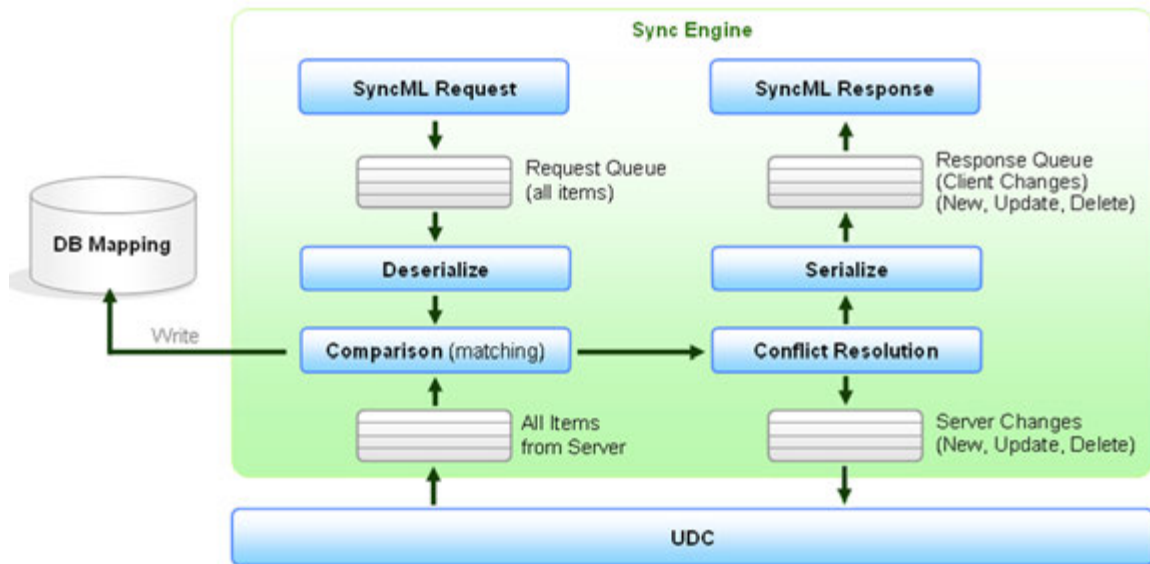
There are two main synchronization types:

- Fast sync. During a Fast Sync, the mobile device and gateway only update items modified since the previous synchronization. This is the standard synchronization type.
- Slow sync. During a Slow Sync the mobile device and gateway send all items belonging to a particular user; this is normally only required for the initial synchronization session between a mobile device and the gateway.

Client Mapping and Conflict Resolution (Slow Sync)

During a slow sync the client sends all its data to the gateway and the server sends all its data to the device. The server constructs a client mapping database that associates each client data entry with a corresponding server entry. A conflict is detected when the same item has a different value on the client and the server side. In the standard automatic conflict-resolution mode, the server value "wins" and is sent to the client, overriding the client value. The following figure shows a slow sync.

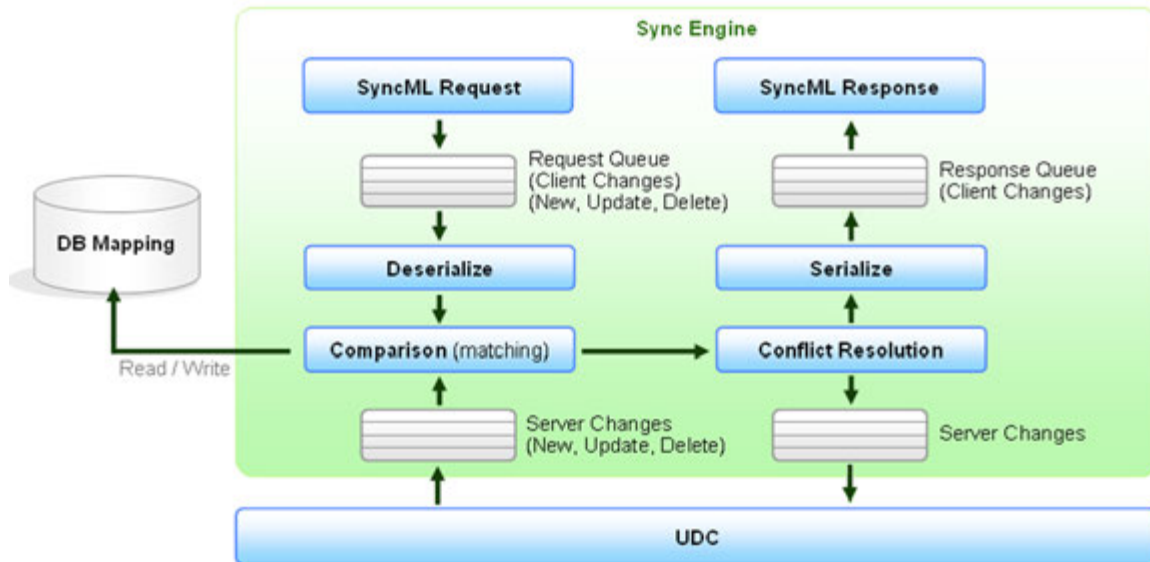
Slow Sync Schematic



Client Mapping and Conflict Resolution (Fast Sync)

Fast sync relies on the client-server mapping in the database, which contains the client and server data item IDs. Only the modifications are compared and synchronized between server and client, resulting in short synchronization sessions. A conflict is detected when the same item is modified on the client and the server side. In automatic conflict-resolution mode, the server modification "wins" and is sent to the client, overriding the client changes.

Fast Sync Schematic



Device-Specific Content Serializers

Serializers modify the sync data to best accommodate data incompatibility. For example, if the back-end repository has several different types of contact phone numbers and the mobile has only one, the serializer selects the phone number to send to the mobile device.

Request Queue

The request queue collects all the information from the client for the actual package. A request can contain the following:

- An alert for each data store that the client is to synchronize (Package #1)
- A put command for the client's device information (Package #1 or #3)
- A get command for the server's device information (Package #1 and #3)
- A status command for the server's response (Package #3 and #5)
- An add, replace, or delete command for data items (Package #3)

Response Queue

The response queue collects all information from the server for the actual package. A response can contain the following:

- An alert for each data store that the server is to synchronize (Package #2)
- A status command for the client's request (Package #2 and #4)
- A put command for the server's device information (Package #2 and #4)
- A get command for the client's device information (Package #2 and #4)
- An add, replace, or delete command for data items (Package #4)
- An optional, final acknowledgment (Package #6)

Incoming Client Changes

The incoming client changes are usually lazy loaded. First the identifying properties of all the items are requested. Then the whole content is requested, if needed.

Outgoing Server Changes

Outgoing server changes are distributed over multiple SyncML responses. If one item is too big to fit into

a single SyncML response and the mobile device supports "large objects" then the item is split over multiple SyncML responses.

Oracle Communications Mobile Synchronization Server Clients

While a large percentage of mobile devices are shipping with built-in clients, not all manufacturers have committed to SyncML support. Oracle offers a complete and homogenized end-to-end solution by providing support for the most important device platforms that are not shipping with a built-in SyncML Client: Palm OS and Microsoft Windows Mobile.

Palm OS - Oracle offers a SyncML client for the Palm OS based PDAs and Smartphones, enabling synchronization of contacts, calendar and tasks through the Oracle Communications Mobile Synchronization Server.

Windows Mobile - Oracle offers a SyncML client for Windows Pocket PCs and Windows Smartphones to enable wireless synchronization of contacts, calendar events, and tasks. The following Windows Mobile Operating Systems are supported: Windows Mobile 2003, Windows Mobile 5 and Windows Mobile 6.

Transport Layer

The transport layer for data synchronization between server and client can be HTTP or HTTPS. The Oracle Communications Mobile Synchronization Server gateway also includes support for MD5 encrypted authentication for other network elements. The gateway uses several industry-standard transport protocols, as shown in the following table.

Transport Protocols supported by Oracle Communications Mobile Synchronization Server

TransportProtocol	Usage
HTTP or HTTPS	Between application server and device. Also used to access the user and administration portals.
Java Database Connectivity (JDBC)	Between Hibernate and a persistent DB.
LDAP or LDAPS	Between client and Oracle Communications Unified Communications Suite contacts.
WCAP or WCAPS	Between client and Oracle Communications Unified Communications Suite calendar events.

Push Engine

The push engine notifies the client device if the user's data (contacts, calendar events, or tasks), stored on the back-end server, changes. If a change occurs, the push engine adds a corresponding event (new, delete, or update) to the event queue.

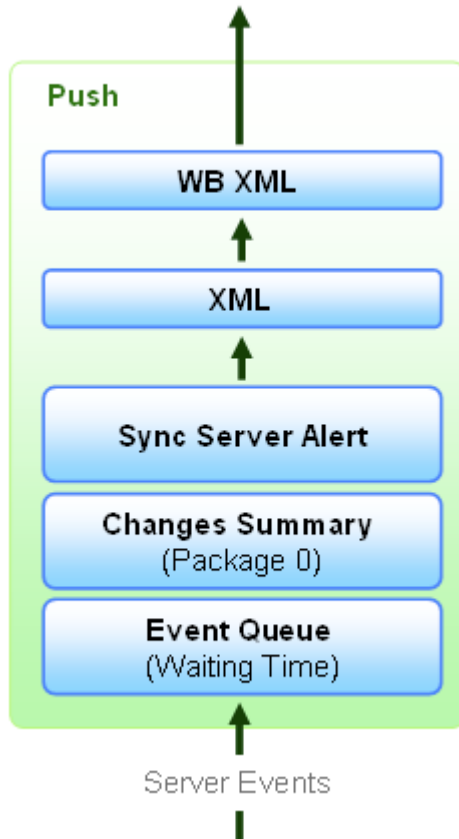
During the polling interval (configured by the user) the event is placed on hold, the event queue is emptied and processed if synchronization starts during this time. At the end of the polling interval the push engine checks if there are any items in the queue. If there are then it notifies the client device through a SyncML push, a Sync Server alert command.

The purpose of the polling interval is to summarize a series of back-end server changes that occur quickly, one after another. The length of the polling interval balances response time to changes against

bandwidth usage. If a change has occurred a SyncML Server alert is constructed and sent to the mobile client in WBXML format. The alert is sent as multiple binary SMS messages using the Short Message Peer to Peer (SMPP) protocol.

The following figure shows the push engine.

Push Engine



The gateway detects changes in the user's data by polling the back-end server frequently using a time interval specified by the administrator.

Administration

The Oracle Communications Mobile Synchronization Server administration console is accessed from the URL `http://domain/sync/admin`. The administration console provides a simple web-based interface for performing administrative tasks such as creating or deleting user accounts, changing the administrator's password, or inspecting gateway log files.

Administration Web Interface

Access to the administration interface of the gateway is controlled by the admin user name and password.

After successful authorization, the administration interface displays a tab to change the administrator's password, set the Oracle Communications Unified Communications Suite details, or reset the stored synchronization information.

User Settings Web Interface

User settings, such as calendar preferences, are set in the following ways:

- By the user, through the Oracle Communications Mobile Synchronization Server User Pages (http://domain/sync/user_).
- By the administrator, through the User Preferences section of the Administration Web Interface. For further details, see [General Database Tables](#).

Client Provisioning

The Oracle Communications Mobile Synchronization Server gateway provides a mechanism for configuring the native SyncML client on a target device. If the supported device requires the Oracle Communications Mobile Synchronization Server Client, the appropriate software is also installed over-the-air.

The user types the device type and telephone number and selects a four-digit PIN. The gateway refers to the Settings Database, which contains device configuration data for each of the supported device types. An XML package is sent to the device containing the gateway URL, database names, and user credentials. The user types the four-digit PIN, which applies the configuration to the handset.

This process ensures that the device configures correctly, reducing manual configuration errors and the related support overhead. The result is a fast and convenient experience for the device user.

Client provisioning is accessed through the User Settings or Administrator Web Interfaces.

Persistent Store (Internal Data) and Databases

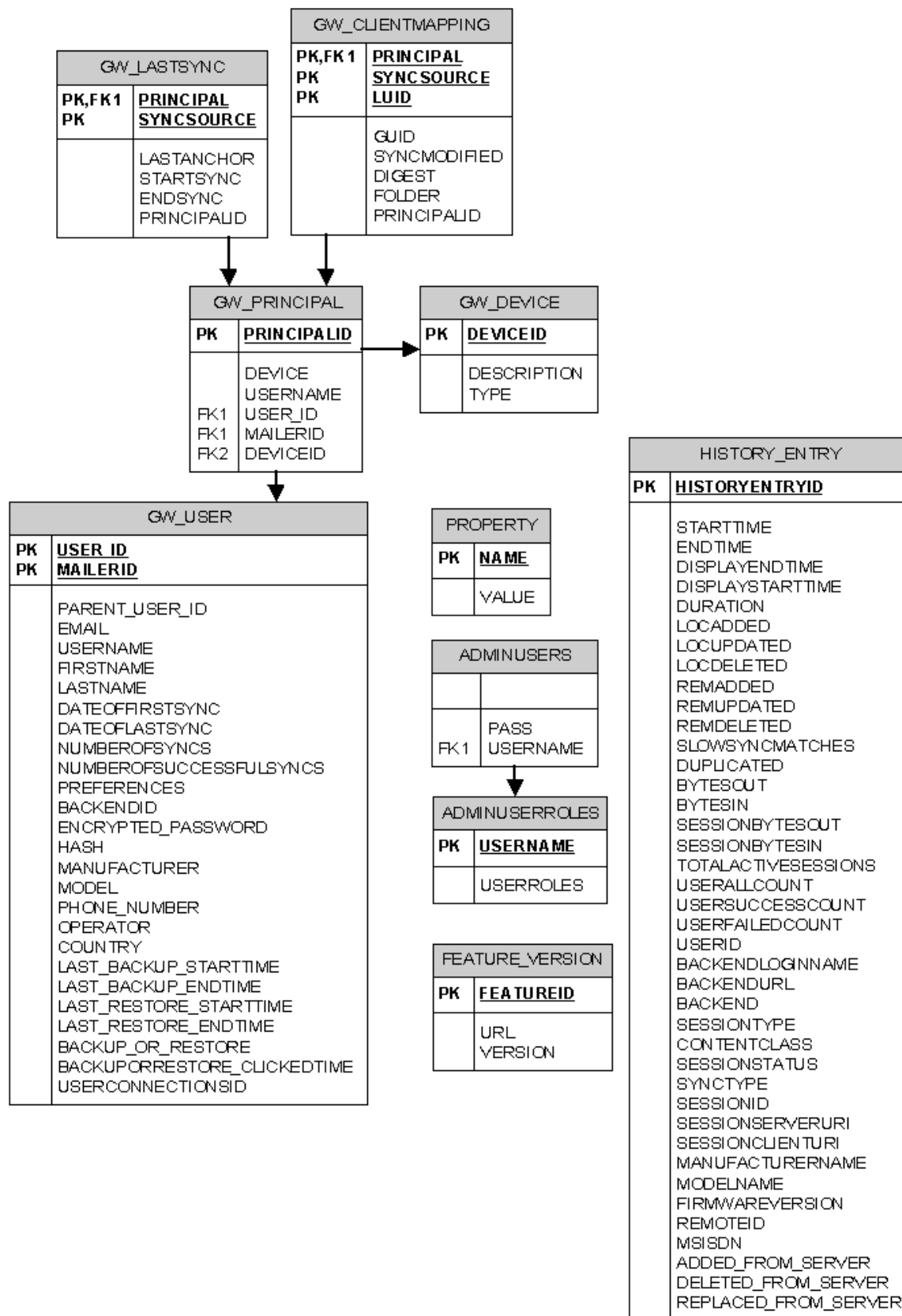
Oracle Communications Mobile Synchronization Server maintains synchronization timestamps for client devices and mappings between client and server items. This information is persistently stored in a database. One data store is provided for every supported content type; contacts, calendar events and tasks.

The server database contains a record of all synchronization activity for each user. Device specific configuration including special attributes mapping, is not part of this database.

General Database Tables

This section describes the Oracle Communications Mobile Synchronization Server gateway general database model. For more details, see the following figure.

Oracle Communications Mobile Synchronization Server General Database Model



The following table describes the General Database.

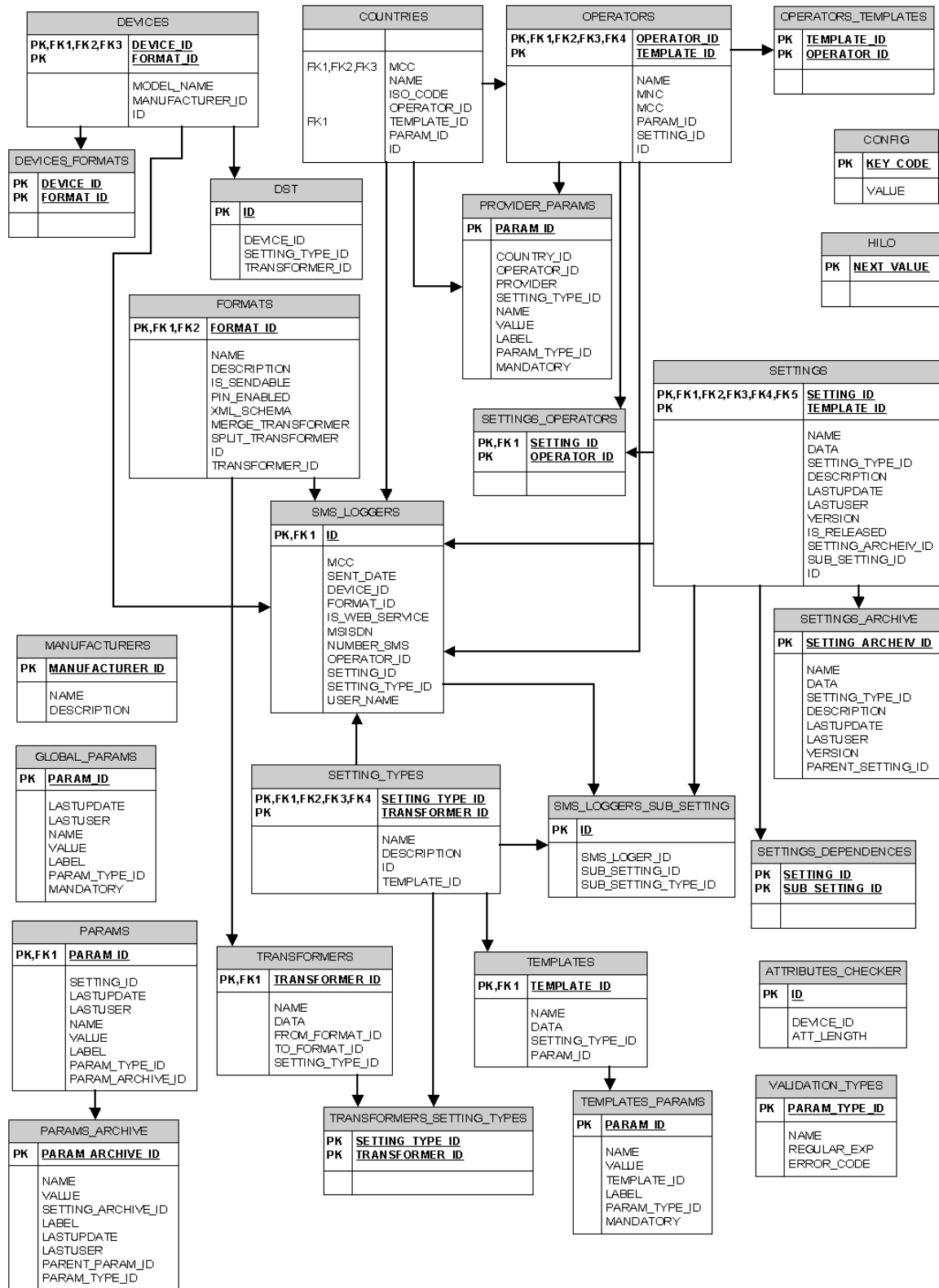
General Database

Table Name	Description
GW_LASTSYNC	Holds details of the last synchronization session per user and data types synchronized.
GW_CLIENTMAPPING	Maps device IDs (LUIDs) to server IDs (GUIDs).
GW_PRINCIPAL	Holds details of the pairing between user and device.
GW_USER	Holds user details.
GW_DEVICE	Holds device details.
PROPERTY	Holds properties set from the web UIs.
ADMINUSERS	Holds details of the administrator users.
ADMINUSERROLES	Holds roles of the administrator users.
FEATURE_VERSION	Holds the version numbers for each live update item.
HISTORY_ENTRY	Holds an overview by content type for each sync session.

Client-Provisioning Database Tables

This section describes the Oracle Communications Mobile Synchronization Server client-provisioning database model. The client-provisioning tables store configuration, data mappings, and user data. For further details, see the following figure.

Oracle Communications Mobile Synchronization Server Client-Provisioning Database Model



The following table describes the Client-Provisioning Database.

Client-Provisioning Database

Table	Name Description
ATTRIBUTES_CHECKER	Holds device and format specific limitations.
CONFIG	Holds configuration parameters for the settings database.
COUNTRIES	Holds details of each country.
DEVICES	Holds device information.
DEVICES_FORMATS	Holds relation information between devices and provisioning formats.
DST	Holds relation information between devices, setting types and setting transformers.
FORMATS	Holds list of client provisioning formats.
GLOBAL_PARAMS	Holds list of global settings parameters.
MANUFACTURERS	Holds details of device manufacturers.
OPERATORS	Holds information about the mobile operators.
OPERATORS_TEMPLATES	Holds settings templates for different operators.
PARAMS	Holds settings parameters.
PARAMS_ARCHIVE	Holds archive settings parameters for versioning.
PROVIDER_PARAMS	Holds provider, operator and country related settings parameters.
SETTINGS	Holds provisioning settings information.
SETTINGS_ARCHIVE	Holds archive of provisioning settings.
SETTINGS_DEPENDENCES	Holds information for the settings dependencies.
SETTINGS_OPERATORS	Holds information for the relation between settings and operators.
SETTING_TYPES	Holds settings type information: for example, SyncML-DS and GPRS.
SMS_LOGGERS	Holds details of sent SMSs.
SMS_LOGGERS_SUB_SETTING	Holds information of sent settings.
TEMPLATES_PARAMS	Holds parameters of settings templates.
TRANSFORMERS	Holds information for settings transformers from one format to another.
TRANSFORMERS_SETTING_TYPES	Holds information for relations between settings transformers and different setting types.
VALIDATION_TYPES	Holds information for settings parameter validators.
HILO	Holds key generator information.

Supported Databases

Oracle Communications Mobile Synchronization Server works with Postgres 8.0 and 8.1, Oracle 9, MySQL 4 and 5.

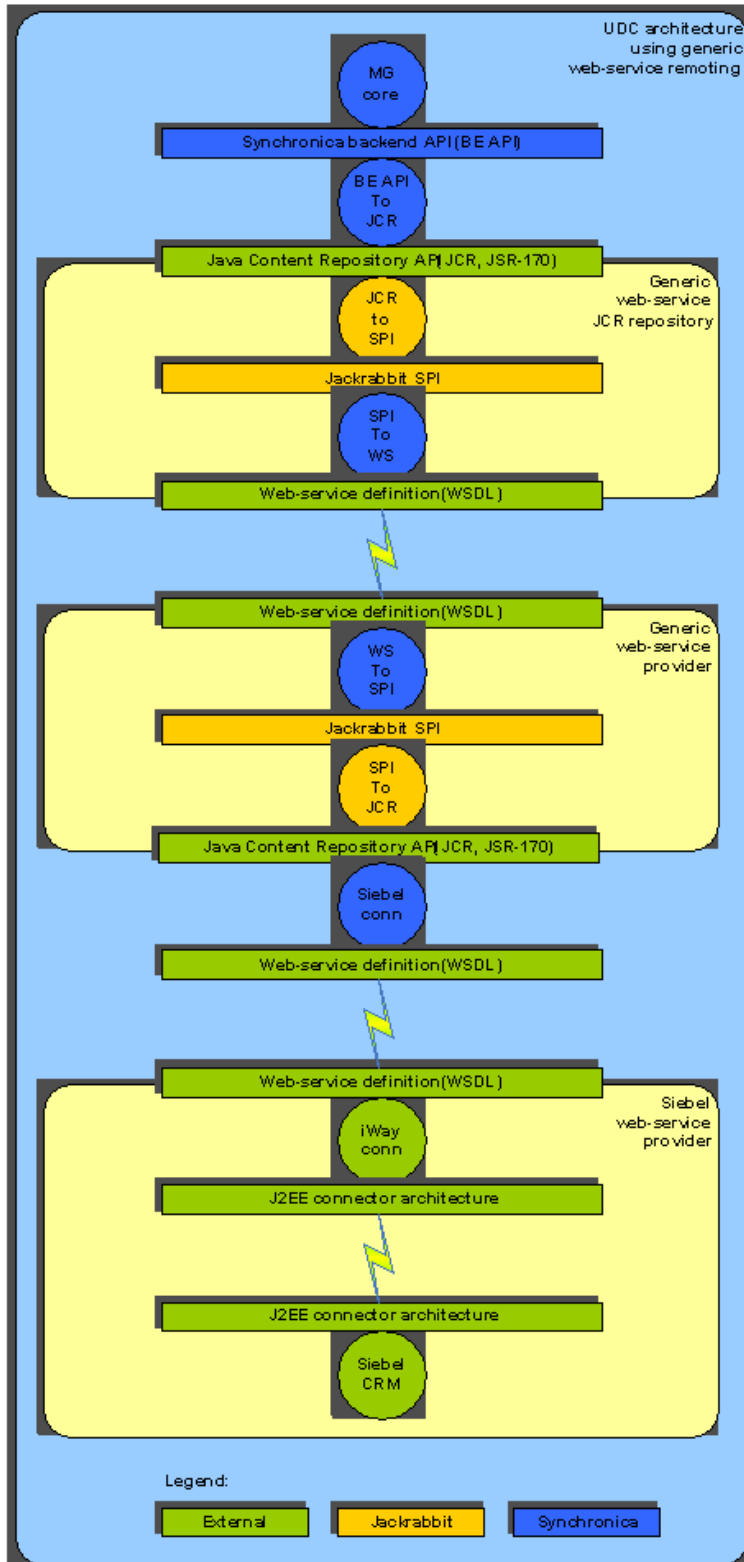
Universal Data Connector

The Universal Data Connector provides a "Data Modeling - Data Access" component that handles communications between the gateway and a back-end data store (or "data repository"). In simple terms, the UDC is a pluggable connector that enables distributive deployment, providing the gateway with the capability to access any data repository.

The UDC layer in Oracle Communications Mobile Synchronization Server uses JAX-WS Web Services interfaces to UDC Adapters providing access to any data store. JCR 170 was chosen because it is a well-defined protocol that provides generic methods for accessing hierarchical and structured data.

All future connectors will use the JAX-WS standard schema, as shown in the following figure.

UDC Architecture Using a Siebel Back-end Connector



UDC adapters are dynamically loaded by the gateway at runtime and do not need to be linked into the application. Providing additional scalability, the UDC adapters can even run on a separate server and can be load-balanced for horizontal scalability and failover at the data access layer.

UDCs are individually developed, mapping one native protocol to the data schema. Multiple adapters can

be grouped to provide customized access where needed.

Because each data repository is often considerably different, and accessing each requires consideration of these differences, the UDC encapsulates the nuances of various data repositories. As a result, the UDC provides a consistent data view to the gateway.

These features offer a number of benefits:

- **Scalability** - The number of connectors associated with a gateway installation is unlimited.
- **Maintainability** - The Oracle Communications Mobile Synchronization Server gateway requires no modification for any new data repository. The UDC communicates a defined syntax that provides the gateway with a consistent data view regardless of the underlying data structure.
- **Deployment** - Due to the distributive nature of the UDC, through the use of JAX-WS, connectors can be deployed in multiple situations. They are not dependent on either the gateway or their respective data repository.
- **Modularity** - Due to the modular approach used for connector development, any external organization can develop customized UDCs.

Chapter 2. Mobile Synchronization Server Release Notes

Oracle Communications Mobile Synchronization Server Release Notes Version 1.1

These Release Notes contain important information available at the time of the general release of Oracle Communications Mobile Synchronization Server 1.1 including:

- [About Mobile Synchronization Server 1.1](#)
- [Requirements for Mobile Synchronization Server 1.1](#)
- [Mobile Synchronization Server 1 Installation Notes](#)
- [Documentation Updates](#)
- [Problems Fixed in This Release of Mobile Synchronization Server 1.1](#)
- [Known Issues and Limitations in Oracle Communications Mobile Synchronization Server 1 \(formerly Sun Java Mobile Communications 1\)](#)

About Mobile Synchronization Server 1.1

Oracle Communications Mobile Synchronization Server provides synchronization services for business users, acting as a gateway synchronizing their Oracle Communications Unified Communications Suite accounts with their mobile phone.

The gateway supports synchronization of contacts, calendar events and tasks between SyncML enabled mobile phones and the back-end server.

For more information, see [Mobile Synchronization Server Technical Overview](#).

Requirements for Mobile Synchronization Server 1.1

This section describes the considerations, requirements, and settings that you must know about before beginning the Oracle Communications Mobile Synchronization Server installation.

Operating System Requirements

This release supports the following platforms:


Table 1 Operating System and Platform Support

Operating System	CPU	Comments
Solaris OS 10	SPARC, x86, x64	Not applicable.
Solaris OS 9	SPARC, x86, x64	Not applicable.
Red Hat Enterprise Linux 4 Advanced Server (32-bit and 64-bit versions) Enterprise Server (32-bit and 64-bit versions)	x86, x64	<ul style="list-style-type: none"> • Distinct 32-bit x86 and 64-bit AMD64/Intel EM64T distributions exist. • Advanced Server and Enterprise Server provide identical functionality. Essentially ES limits CPU/memory support.
Red Hat Enterprise Linux 3 Advanced Server (32-bit and 64-bit versions) Enterprise Server (32-bit and 64-bit versions)	x86, x64	<ul style="list-style-type: none"> • Distinct 32-bit x86 and 64-bit AMD64/Intel EM64T distributions exist. • Advanced Server and Enterprise Server provide identical functionality. Essentially ES limits CPU/memory support.

Product Requirements

The information in this section brings together all product requirements and minimum product versions for installing Mobile Synchronization Server:

Table 2 Product Requirements

Product	Minimum Version
Oracle Communications Unified Communications Suite Servers	At least Messaging Server 6.3, Oracle Communications Sun Calendar Server 6.3 <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> Note Mobile Synchronization Server is not currently supported on Oracle Communications Calendar Server (also known as Calendar Server 7).</p> </div>
Application Server	9.1
JDK	1.5 (included with Solaris 10 OS)
Database	Postgres 8.1.3 (included with Solaris 10 OS)

Considerations and System Requirements

As different scenarios apply to the Mobile Synchronization Server installation, you must first determine the most appropriate. Specifically, consider whether to enable standard HTTP access or only secure HTTPS connections to the Mobile Synchronization Server gateway.

The following table lists the system requirements and settings required for Mobile Synchronization Server deployment and operation.

Table 3 System Requirements

Item	Minimum	Recommended
Hard Disk Space	350 MB	1024 MB
Free Memory (RAM)	512 MB	Greater than 2 GB - Dependent on the number of instances to be created and application tuning.
Accounts	Root account: mandatory for installation procedure.	Application account: optional.
Product Licenses	A valid Oracle Communications Unified Communications Suite System license.	Not applicable.
Installation Directory	<code>/opt/SUNWappserver</code>	Not applicable.
TCP Ports	-	The following ports are required by Mobile Synchronization Server: HTTP: 80 or the port number that you configure during installation. This is the default value. HTTPS: 443 HTTPS/Admin: 443 or the port number that you configure during installation. This is the default value. JMX/Admin: 8686 IIOP: 3700, 3920, and 3820
Domain Name System (DNS)	DNS must be configured.	Not applicable.

Prerequisites

Before starting the Mobile Synchronization Server deployment, you must install the following:

- Solaris 10 OS
- JDK (supplied with Solaris 10 OS) with the path set to `JAVA_HOME` (`JAVA_HOME` is the default setting)
- Sun Java Application Server 9.1
- At least one Communications Suite server

Mobile Synchronization Server 1 Installation Notes

Deployment Scenarios

Mobile Synchronization Server fully supports deployment in global and non-global zones. For non-global zones, both sparse root and whole root zones setups are supported.

The Mobile Synchronization Server gateway server design also supports vertical and horizontal scalability. This scalability enables you to deploy the application in different scenarios. These scenarios include a dedicated single-server system running all infrastructure components or multiple servers with load balancing and failover.

Dedicated Mobile Synchronization Server

For live production environments, deploy the Mobile Synchronization Server gateway on a dedicated machine or Solaris zone. For increased security, consider deploying the dedicated Mobile Synchronization Server gateway in the DMZ of your corporate network. In these scenarios, you must configure your firewall to allow access from the Internet to the Mobile Synchronization Server gateway on HTTP (port 80) and/or HTTPS (port 443). In addition, the firewall needs to allow LDAP or LDAPS and WCAP or WCAPS connections from the Mobile Synchronization Server gateway to the Communications Suite servers.

Scalability

The Mobile Synchronization Server system architecture is scalable and, depending on the server hardware, supports thousands of concurrent sessions on a single-server system.

Larger installations might require horizontal scalability and failover that utilizes load-balancing mechanisms and multiple servers running Mobile Synchronization Server.

As a minimum for horizontal scalability and failover in the Application Server tier, at least two Application Servers are required. Depending on the expected amount of concurrent sessions, additional Application Servers can be introduced to share the load, without interruption of the service.

High Availability

The Mobile Synchronization Server architecture also supports failover, ensuring high availability in case of hardware or software failure.

Assuming a load-balanced installation as described previously, the Application Server already supports failover. The Application Server consists of multiple independent server systems running identical configurations of the Mobile Synchronization Server gateway server. If a single Application Server fails, the load balancer redirects incoming traffic to the surviving nodes in the Application Server tier. If you restore the failed system, it automatically reintegrates into the load-balancing and failover system.



Note

Deployment instructions for commercial clustering solutions are beyond the scope of this document. Refer to the installation instructions for these products.

Database Server

The expected load on the database (DB) server is very low, even with a large number of concurrent sessions. However, for large-scale carrier deployments, a DB clustering solution can provide additional scalability. Protect the database server from system failures by using database replication software, for example, the Oracle Solaris Cluster Manager for failover clustering. The Oracle Solaris Cluster Manager software requires at least two servers. Because the database server does not receive a heavy load, you can combine both the DB and OCMSS on the same system for smaller deployments.

Documentation Updates

The product name was rebranded to Oracle Communications Mobile Synchronization Server for release 1.1.

Problems Fixed in This Release of Mobile Synchronization Server 1.1

Secure Sockets Layer (SSL)

SSL is now supported.

Known Issues and Limitations in Oracle Communications Mobile Synchronization Server 1 (formerly Sun Java Mobile Communications 1)

Comms-Issue-S012

Installation Guide should describe how to uninstall Mobile Communications.

Event Time-shifts and Duplications

The time of events, appointments and reminders for all day events may shift during synchronization. Calendar entries may be duplicated as a result.

The synchronized events in the calendar are shifted from their original time, and are frequently duplicated on the device and the server as well. The time-shift can be the result of time-zone difference between the device and the back end, or daylight savings time adjustment.

Users whose mobile phones are set to a different time-zone than the server might have whole day events, such as birthdays duplicated, or reduced to one-hour events and shifted to the following of the previous day in their calendar. Appointments might be duplicated during each subsequent synchronization, populating the calendar with numerous duplicate entries. Reminders might be set to a time after the actual appointment. It is important to ensure that the device time-zone and server time-zone are in sync to avoid these issues

Exceptions to Recurring Events

Exceptions to recurring events are not supported

If a single occurrence of a recurring event is changed the change is ignored.

Synchronization Fails Because of Password Changes

Synchronization fails because a user's password has changed.

When the password to the back-end account is changed, it is not updated automatically in the gateway or on the user's device. Users must change the password manually on the device, or update it in the gateway and resend settings.

Chapter 3. Mobile Synchronization Server Installation Guide

Oracle Communications Mobile Synchronization Server Installation Guide Version 1 Update 1

This information describes how to install, configure, and run Oracle Communications Mobile Synchronization Server on Oracle Solaris 10 and Application Server for mobile synchronization of Oracle Communications Unified Communications Suite content, including calendar, tasks and contacts. This information also contains configuration information for required third-party components, including the Postgres database. It provides a detailed description of the commands to perform the installation. Finally, a section explains how to verify the installation.

Topics:

- [Installation Overview](#)
- [Installing Mobile Synchronization Server on Oracle Solaris 10 OS](#)
- [Verifying the Installation](#)
- [Debugging and Troubleshooting](#)
- [Uninstalling the Mobile Synchronization Server Gateway](#)

Installation Overview

Before You Begin

See [Mobile Synchronization Server Release Notes](#) for information on the considerations, requirements, and settings that you must know about before installing Mobile Synchronization Server.

Installing Mobile Synchronization Server on Oracle Solaris 10 OS

This section details the installation of Mobile Synchronization Server on Oracle Solaris 10 OS with a Postgres database server.

The installation process consists of the following steps:

1. Installing Mobile Synchronization Server
2. Configuring the Postgres Database
3. Creating Postgres database schemas and user accounts

Before installing Mobile Synchronization Server, meet the following requirements:

1. Complete the basic system setup, including installation of Solaris 10 OS and Postgres.
2. Have basic knowledge of the UNIX environment.
3. Be logged in as `root` user with administrative-level privileges.
4. Ensure that the Application Server is installed.

Installing the Application Server

To Install the Application Server

1. Download the latest binary file from the [Oracle Software Delivery Cloud](#).
In this example, the `sjsas-9_1-solaris-i586.bin` version is installed.
When the `.bin` file is run, it produces the following error if you have no graphical interface:

```
# ./sjsas-9_1-solaris-i586.bin
Connecting to X11 server ':0.0'.
Error: Cannot connect to X11 server ':0.0'.
Check that the DISPLAY environment variable is correctly set or try
rerunning this application with the following usage:
'sjsas-9_1-solaris-i586.bin' -console
```

2. To run the installer by using the command-line interface, run this command with the `-console` switch.

```
# ./sjsas-9_1-solaris-i586.bin -console
```

The `.bin` file first checks for available disk space, then checks for a Java 2 Runtime Environment. The `.bin` file extracts the installation files and starts the installation process. Next a welcome message appears.

3. Press Enter to continue installation.
4. Read the Software license agreement and press Enter.
The default installation directory for Application Server is `/opt/SUNWappserver`.
5. Either accept the default or type a location of your choice.
In this example, press Enter to accept the default.
6. The installation process detects whether this directory exists:
 - a. If the directory exists, press Enter to continue.
 - b. If the directory does not exist, type `1` to create the directory or type `2` to create another directory for the installation.
7. Next, the installation process tries to detect at minimum a Java 2 SDK version 5.0. To change this from the version that is detected, type the new location or just press the Enter key.
8. Type the administration user name and password.
The program asks you whether you want to store this information in `in.asadminpassfile` in the user's home directory.
9. Press Enter to confirm.
10. Provide the ports to use for Admin, HTTP, and HTTPS.
The defaults are 4848, 8080, and 8181 respectively. You can change these ports if you need to.
11. The installation program now asks if you want to enable the Update Center client.
The default response is `yes`. The Update Center client is for SAS self-updating and is not important for this installation.
12. Finally, the installation program asks whether this is a fresh installation or if you are upgrading from a previous version.
As this is a fresh installation, answer `no` to this question.
13. A list of the components of the installation is now displayed. Type `1` to install now.
14. The output from the installation process shows a progress bar.
15. When the installation completes, proceed with the next section.

Configuring the Postgres Database

To Configure the Postgres Database

1. Determine the version of Solaris OS that you are running.

```
cat /etc/release
```

Solaris 10 11/06 ships with PostgreSQL 8.1 and the default database location is `/var/lib/pgsql/data`. No Postgres user or group exists by default, so you need to create them.

Note
PostgreSQL cannot be run as `root`.

2. To create a user called `postgres` and assign it to a `postgres` group, execute the following commands as `root` user. Ensure that the directory `/export/home` exists.

Note
If you choose to use an existing user, you can skip this step and proceed to the next step. You can also skip this step if you are installing on Solaris 10 8/07, as this user already exists.

```
# groupadd postgres
# useradd -c 'PostgreSQL user' -d /export/home/postgres -g postgres
-m -s /bin/bash postgres
```

3. Choose a directory in which to create the database and ensure that the permissions are set correctly.
The default location in PostgreSQL 8.1 is `/var/lib/pgsql/data` but the database can be placed anywhere. In fact, in a production environment, you should place the database in its own file system partition, with consideration for space and growth, performance, and availability. To use the default directory with the Solaris OS user called `postgres`, execute the following commands to set the ownership and permissions.

```
# chown postgres:postgres /var/lib/pgsql/data
# chmod 700 /var/lib/pgsql/data
```

4. To create a database cluster:
 - a. Log in as `postgres`, or another user that you have selected to run the database.
 - b. Execute the `initdb` command to create the cluster in the `/var/lib/pgsql/data` directory:

```
$ initdb -D /var/lib/pgsql/data
```

- c. Start PostgreSQL by using the following command:

```
$ pg_ctl -D /var/lib/pgsql/data -l postmaster.log start
```

Note
You must either run this command from a directory that the Postgres user can write to or specify a directory location for the log file that the Postgres user can write to.

- d. To connect to the Postgres database running on a default port, execute the following

command:

```
$ psql postgres
```

Postgres Configuration

The default Postgres configuration rejects the TCP/IP connection from other machines (IP addresses).

To Allow External Connections

1. Log in to the Postgres server.
2. Locate and edit the configuration file `postgresql.conf`.
The file location varies depending on the version of Postgres installed. In the example installation it is found in the `/var/lib/postgres/data` directory.
3. Uncomment the lines beginning with `listen address` and `port =` to enable Postgres to accept incoming requests from other IP addresses on the default port 5432.

```
# - Connection Settings -
[+]listen_addresses = '*'          # what IP address(es) to listen on;
                                   # comma-separated list of addresses;
                                   # defaults to 'localhost', '*' = all

[+]port = 5432
```

4. To confirm that Postgres accepts incoming requests, execute the `telnet` command as follows. If the new setup is working, you can connect to the Postgres database on this port. A few seconds later the connection will end. You should see the following output:

```
telnet localhost 5432
```

5. If the new setup is working, you can connect to the Postgres database on this port. A few seconds later the connection ends. You should see the following output:

```
# telnet localhost 5432
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^\\]'.
```

6. If the Mobile Synchronization Server gateway is hosted on a different machine than the Postgres database, conduct a second test to check whether the gateway server can access the Postgres server.

This test ensures that no firewall or routing problems will ensue. Perform the following steps:

- a. Log in to the Mobile Synchronization Server host.
Use the `telnet` command to connect to the host name or IP address of the Postgres server.
- b. If the test succeeds you should see the following:

```
# telnet postgres 5432
Trying 127.0.0.1...
Connected to postgres.
Escape character is '^\\]'.
```

7. To enable other computers to authenticate to Postgres, the `pg_hba.conf` file must be edited in the Postgres data directory, `/var/lib/pgsql/data/`.
Locate the following section in this file:

```
# TYPE DATABASE USER CIDR-ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all trust
# IPv4 local connections:
host all all 127.0.0.1/32 trust
# IPv6 local connections:
host all all ::1/128 trust
```

8. Assuming that your Mobile Synchronization Server gateway servers are running in the 192.168.1.0/24 subnet, you need to add the following line to the IPV4 configuration:

```
host all all 192.168.1.0/24 trust
```

A more secure setup could look like the following, assuming that your gateway is installed on IP address 192.168.1.10:

```
# TYPE DATABASE USER CIDR-ADDRESS METHOD
host gwdb gwdbuser 192.168.1.10/32 trust
host settingsdb settingsdb 192.168.1.10/32 trust
```

Note
Make sure that the database and user name match the details that you use in the following section.

9. After you have completed the changes to this file, you must restart Postgres to apply the changes.

Creating Postgres Database Schemas and User Accounts

The Mobile Synchronization Server default setup has two different database schemas. Each schema has its own user account. The first schema, `gwdb`, is used to store gateway specific configuration, user provisioning and configuration data, and SyncML protocol-related metadata.

Command-Line Tools

When using Solaris OS 10 8/07 with Postgres 8.1, you need to use the command-line tools that belong to this version.

1. For Postgres 8.1, type the following:

```
/usr/bin/createdb
/usr/bin/createuser
```

Note
Using these commands with an incorrect version of Postgres produces errors.

2. Type the following commands on the Postgres server to create a database for the gateway named `gwdb`:

```
bash-3.00#/usr/bin/createdb gwdb
bash-3.00#/usr/bin/createuser -P gwdbuser
Output = you are prompted for the password
Type the password gwdbpass
Output = shall the user be a superuser? (y/n)
Type 'y'
```

3. The second schema and user `settingsdb` are used to store data for the Client provisioning module. Create a database for Client Provisioning named `settingsdb` as follows:

```
bash-3.00#/usr/bin/createdb settingsdb
bash-3.00#/usr/bin/createuser -P settingsdb
Output = you are prompted for the password
Type the password settingsdbpass
Output = shall the user be a superuser? (y/n)
Type 'y'&nbsp;
```

If you incorrectly create these users and need to remove them and start again, you can use the `dropuser` command.

Installing Mobile Synchronization Server on a New Domain on Application Server

This section describes how to run the Mobile Synchronization Server installation script. This script prompts for a number of settings before installing Mobile Synchronization Server, referred to as *gatewayserver* in a new Application Server domain, referred to as *domainname* from now on. Finally, the script starts the new domain and with it the gateway.

Note

The Application Server creates a default domain `domain1`. However, to avoid confusion, use the installation script to uninstall `domain1`.

1. Download the Mobile Synchronization zip file.
2. Unzip and verify the software.

```
unzip zipfile
cat README
md5sum *.bin *.CAB *.prc
```

Verify the accuracy of download and unzip operations by comparing the generated MD5 sums with those listed in the README file.
3. Start the installer as follows:

```
chmod 755 ./OCMSS-1.1.3.1.43-oracle-comms-sas.bin
./OCMSS-1.1.3.1.43-oracle-comms-sas.bin
```

Note

If an HTTP proxy is being used, run the following commands before running the script so that the Postgres driver can be downloaded.

```
http_proxy=http://username:password@host:port/
export http_proxy
```

The installation script produces the following output:

```
bash-3.2# ./OCMSS-1.1.3.1.43-oracle-comms-sas.bin
```

```

Verifying archive integrity... All good.
Uncompressing Oracle Communications Mobile Synchronization Server
(Mobile-Gateway-1.1.3.1.43-oracle-comms-sas).....
is the Oracle Communications Mobile Synchronization Server install
script for SAS
-----
© 2008,2011, Oracle and/or its affiliates. All rights reserved.
-----
your OS ...
Found a Solaris Operating system ...
SunOS coms-152x-206.in.oracle.com 5.10 Generic_144501-07 i86pc i386
i86pc

Do you want to continue with the installation? [y,n,?,q] y

Default domain, "domain1" found. Do you want to delete it? [y,n,?,q] y
Domain domain1 stopped.
All of a domain's node agents and server instances must be deleted
before the domain can be deleted.
CLI139 Could not delete domain, domain1.

Enter the name for the new SAS domain. [?,q] sync

Enter the instance port for the new domain [sync]. The default is 80
[?,q]

Enter the admin port for the new domain [sync]. The default is 4848
[?,q]

Enter the admin password for the new domain. The default is adminpass
[?,q]

Please select the Database you wish to connect to:
1) PostgreSQL
2) MySQL
3) Oracle
#? 1
This setup will connect to a PostgreSQL database.

Enter the hostname or IP address for the Database server. The default is
localhost. [?,q]

Enter the port for the Database server. The default is 5432 [?,q]
-----
chosen settings ...
-----
configuration
Domain name: sync
Admin port: 4848
Instance port: 80
-----
configuration
PostgreSQL database should be running on localhost:5432
PostgreSQL database schema and user:
schema:gwdb user:gwdbuser pass:*password*
schema:settingsdb user:settingsdb pass:*password*
-----
directory: /opt/SUNWappserver/domains/sync
-----
you want to accept these settings? [y,n,?,q]y
Using port 4848 for Admin.
Using port 80 for HTTP Instance.

```


Using default port 7676 for JMS.
Using default port 3700 for IIOP.
Using default port 8181 for HTTP_SSL.
Using default port 3820 for IIOP_SSL.
Using default port 3920 for IIOP_MUTUALAUTH.
Using default port 8686 for JMX_ADMIN.
On Unix platform, port numbers below 1024 may require special privileges.
Domain being created with profile:enterprise, as specified by variable AS_ADMIN_PROFILE in configuration file.
Security Store uses: NSS
Domain sync created.
Starting Domain sync, please wait.
Default Log location is /opt/SUNWappserver/domains/sync/logs/server.log.
Redirecting output to /opt/SUNWappserver/domains/sync/logs/server.log
Domain sync started.
Domain [sync] is running [Sun GlassFish Enterprise Server v2.1.1 Patch16 ((v2.1 Patch22)(9.1_02 Patch28)) (build b01-p16)] with its configuration and logs at: [/opt/SUNWappserver/domains].
Admin Console is available at [https://localhost:4848].
Use the same port [4848] for "asadmin" commands.
User web applications are available at these URLs:
[http://localhost:80 https://localhost:8181].
Following web-contexts are available:
[/web1 /__wstx-services].
Standard JMX Clients (like JConsole) can connect to JMXServiceURL:
[service:jmx:rmi:///jndi/rmi:///coms-152x-206.in.oracle.com:8686/jmxrmi]
for domain management purposes.
Domain listens on at least following ports for connections:
[80 8181 4848 3700 3820 3920 8686].
Domain supports application server clusters and other standalone instances.

This may take a few seconds ...

Please enter the alias password>
Please enter the alias password again>
Command create-password-alias executed successfully.

Please enter the alias password>
Please enter the alias password again>
Command create-password-alias executed successfully.
Extracting software ...
Copying files to installation directory ...
Configuring JPA with PostgreSQL ...
server.java-config.classpath-suffix =
/opt/SUNWappserver/domains/sync/ds/skin/user/messages/i18n:/opt/SUNWappse
create-jvm-options executed successfully.
Command create-jvm-options executed successfully.
Command create-jvm-options executed successfully.
Command create-jvm-options executed successfully.
Command create-jvm-options executed successfully.
Command create-jvm-options executed successfully.
Command create-jms-resource executed successfully.
Command create-jmsdest executed successfully.
Command create-jms-resource executed successfully.
Command create-jdbc-connection-pool executed successfully.
Command create-jdbc-connection-pool executed successfully.
Command create-jdbc-resource executed successfully.
Command create-jdbc-resource executed successfully.
Command create-auth-realm executed successfully.
Command deploy executed successfully with following warning messages:

```
Error occurred during application loading phase. The application will
not run properly. Please fix your application and redeploy.
WARNING: com.sun.enterprise.deployment.backend.IASDeploymentException:
Error while loading application [synchronica-server]. Please refer to
the server log for more details.
```

```
Stopping new domain [sync] now for a moment ...
Domain sync stopped.
```

```
Do you want to make this service restart if the server is rebooted?
[y,n,?,q]y
Use Solaris SMF to make the service failure tolerant
```

```
-----
Important note!
```

```
-----
start and stop a SMF managed domain, please use
svcadm enable svc:/application/SUNWappserver/sync:default
svcadm disable svc:/application/SUNWappserver/sync:default
```

```
Using /opt/SUNWappserver/bin/asadmin stop-domain causes the SMF manager
to restart the domain immediately.
```

```
-----
Service was created successfully. Here are the details:
Name of the service:application/SUNWappserver/sync
Type of the service:Domain
Configuration location of the service:/opt/SUNWappserver/domains
Manifest file location on the
system:/var/svc/manifest/application/SUNWappserver/sync_opt_SUNWappserver
service could be enabled using svcadm command.
Command create-service executed successfully.
Giving domain control to SMF now ...
starting now using SMF tools
svc:/application/SUNWappserver/sync:default (Appserver Domain
Administration Server)
  State: online since Thu Feb 23 10:44:30 2012
  See: man -M /opt/SUNWappserver/appserver/man -s 1 Appserver
  See: /var/svc/log/application-SUNWappserver-sync:default.log
Impact: None.
```

```
Mobile Gateway default administrator user is 'admin' and password is
'syncpass'. For security reasons log-in and change the password
Cleaning up temporary files created during the installation ...
Done!
bash-3.2#
```



Note

The installer can create a Solaris SMF manifest to make this service failure tolerant. For example, the service restarts if the server is rebooted or the service crashes.

```
Stop the domain with the following command:
svcadm disable svc:/application/SUNWappserver/domainname:default
```

Error Message Troubleshooting

When running the installer script you might receive the following error message:

```
Environment setting AS_HOME not set!
```

```
Please configure it accordingly (e.g. in /etc/profile) and restart this installation script.
```

```
On Solaris 10 and SAS 9.1 this is usually /opt/SUNWappserver
```

To Set the AS_HOME Value

1. Edit the `/etc/profile` file to include the following lines at the end. If you did not install Application Server in the default location, change the `AS_HOME` value to the location to which you installed it:

```
AS_HOME=/opt/SUNWappserver
export AS_HOME
```

2. Log out and then log in again for these changes to be applied, or you can use the following command to reload the profile:

```
. /etc/profile
```

Note the space between the dot and the forward slash.

3. Run the installation script again.
`./OCMSS-1.1.3.1.43-oracle-comms-sas.bin`

Updating MIME Types

After the script has finished, you need to update the MIME types in the default Application Server file `web.xml` to enable device client downloads.



Note

The `AS_HOME` environment variable must be set to the correct location for the Application Server on which the gateway is being installed.

To Update MIME Types

1. Locate the `default-web.xml` file in the directory:
`AS_HOME/domains/domainname/config`
2. Edit this file and add these lines to the MIME configuration section:

```
<mime-mapping>

<extension>cab</extension>

<mime-type>application/octet-stream</mime-type>

</mime-mapping>

<mime-mapping>

<extension>prc</extension>

<mime-type>application/x-pilot</mime-type>

</mime-mapping>
```

Configuring crontab

Create a `crontab` file on the gateway to perform the following tasks:

- Compressing the application log files.
- Optionally, synchronizing the machine clock with your company's NTP server, if available. This synchronization is essential if Postgres is set up on a different machine than the gateway.

To Synchronize the System Clock

1. Type `/usr/sbin/ntpdate location`. *location* refers to the NTP server.
2. If you are using `pool.ntp.org` as your NTP server, use the following command to update the time on the local system that is using the NTP server:

```
/usr/sbin/ntpdate pool.ntp.org
```

3. Configure a job to run this command nightly on the both the gateway and Postgres servers. Modify the `crontab` file on both systems to include the following line:

```
0 1 * * * /usr/sbin/ntpdate pool.ntp.org
```

4. Add the following line to the gateway `crontab` file to compress the log files every night to minimize storage space:

```
0 2 * * * gzip
/opt/SUNWappserver/domains/domainname/ds/log/synchronica.*.log
```

When you are using Solaris zones, the clock can only be set in the global zone, not in the non-global zone.

Verifying the Installation

The domain and database are now ready to test. Access the following pages to confirm that the gateway is working correctly:

- Accessing the Version Page
- Accessing the Administration Portal
- Accessing the User Self-Registration
- Accessing the User Portal

After the Mobile Synchronization Server administration pages are available, you can synchronize data with a mobile device. For information about using Mobile Synchronization Server, see the [Mobile Synchronization Server Administration Guide](#), the [Mobile Synchronization Server Client Setup Guide for Palm OS](#), and the [Mobile Synchronization Server Client Setup Guide for Windows Mobile](#).

Accessing the Version Page

To locate the Mobile Synchronization Server version and license information, see:

`http://gatewayserver:instanceport/sync`

where *instanceport* is the instance port set during the installation process.

Confirm that the version and license information is correct.

Accessing the Administration Portal

For more information about the operation of the Admin Portal, see the [Mobile Synchronization Server Administration Guide](#).

To Access the Mobile Synchronization Server Admin Portal

1. Type the URL: `http://gatewayserver:instanceport/sync/admin`
2. Type the default administrator user name `admin` and password `syncpass`.
3. Confirm that you can log in and see the login page like.

Accessing the User Self-Registration Page

Access the Mobile Synchronization Server registration page where users can register themselves at the following URL:

`http://gatewayserver:instanceport/sync/registration`

Confirm that this page loads.

Accessing the User Portal

To Access the User Portal

- Access the Mobile Synchronization Server User Portal at the following URL:
`http://gatewayserver:instanceport/sync/user`



Note

For more information about the operation of the User Portal, see the [Mobile Synchronization Server Client Setup Guide for Palm OS](#) and the [Mobile Synchronization Server Client Setup Guide for Windows Mobile](#).

Starting or Stopping Mobile Synchronization Server

- To start the server, type:

```
svcadm enable svc:/application/SUNWappserver/domainname:default
```

- To stop the server, type:

```
svcadm disable svc:/application/SUNWappserver/domainname:default
```

Debugging and Troubleshooting

This section provides log file information in case you encounter a problem or error while using Mobile Synchronization Server.

To debug or troubleshoot an error, you might need to one or more of the following files:

- Application Server log file: `/opt/SUNWappserver/domains/domainname/logs/server.log`
- Mobile Synchronization Server log file: `/opt/SUNWappserver/domains/domainname/ds/log/synchronica.log`
- SMF log file, which shows information about manual starts and stops, and unexpected restarts: `/var/svc/log/application-SUNWappserver-domainname:default.log`

To change the log level of Mobile Synchronization Server, edit the `/opt/SUNWappserver/domains/domainname/ds/conf/log4j.xml` file.

```
<!-- A time/date based rolling appender -->
  <appender name="FILE"
class="org.apache.log4j.DailyRollingFileAppender">
    <param name="File" value="../ds/log/synchronica.log"/>
    <param name="Append" value="false"/>
    <!-- Loglevel -->
    <param name="Threshold" value="DEBUG"/>
    <!-- Rollover at midnight each day -->
    <param name="DatePattern" value="'.'yyyy-MM-dd'.log'"/>
    <layout class="org.apache.log4j.PatternLayout">
    <!-- Synchronica pattern: Time Priority [Category] Message\n
-->
    <param name="ConversionPattern" value="%d{HH:mm:ss} [%t] %-5p
[%c{1}] %m%n"/>
    </layout>
  </appender>
```

The value of the threshold parameter can vary depending on the level of logging that you require. The following table describes the available options.

Log Levels

Log Level	Description
DEBUG	The DEBUG Level designates fine-grained informational events that are most useful to debug an application.
INFO	The INFO level designates informational messages that highlight the progress of the application at the coarse-grained level.
WARN	The WARN level designates potentially harmful situations.
ERROR	The ERROR level designates error events that might still enable the application to continue running.
FATAL	The FATAL level designates very severe error events that will usually lead the application to shut down.
ALL	All of the previous descriptions apply.
OFF	The OFF level has the highest possible rank and is intended to turn off logging.



Note

After changing this file to alter the log level, you must restart the server for the changes to occur.

Uninstalling the Mobile Synchronization Server Gateway

To remove the Mobile Synchronization Server gateway, use the `asadmin` commands to delete the Application Server domain.

1. Stop the domain:
`asadmin stop-domain domainname`
2. Delete the domain:
`asadmin delete-domain domainname`
3. Remove the `domainname` directory:
`rm -rf domainname`

Chapter 4. Mobile Synchronization Server Client Setup Guide for Palm OS

Oracle Communications Mobile Synchronization Server Client Setup Guide for Palm OS Version 1.1

The Mobile Synchronization Server Client for Palm OS enables your Palm device to synchronize your personal data items through the Mobile Synchronization Server.

This information describes the steps to set up your Palm device to work with your Mobile Synchronization Server synchronization service. The Mobile Synchronization Server Client is a small application that, when installed on your Palm device, connects to the Mobile Synchronization Server to provide automatic synchronization of contacts, calendar events, and tasks to and from your Personal Information Manager (PIM) Server and your Palm device.

Topics:

- [Mobile Synchronization Server for Palm Overview](#)
- [Device Setup](#)
- [Troubleshooting](#)

Mobile Synchronization Server for Palm Overview

This section describes the prerequisites for using the synchronization service on your Palm device.

Supported Palm Devices

The following Palm devices are compatible with the Mobile Synchronization Server Client:

- Treo 650
- Treo 680
- Treo 700p

Before You Start

You must have the following:

- A Mobile Synchronization Server account
- A compatible Palm device.
- A Data connection (CSD, GPRS, or UMTS) set up on your Palm device

Contact your mobile operator to set up a data plan or to confirm your mobile data access information.

Device Setup

This section describes how to set up your Palm device to synchronize with your Mobile Synchronization Server account. You learn how to install the Mobile Synchronization Server Client, add your account information, and eventually, synchronize your personal data items.

Mobile Synchronization Server Client Installation for Palm OS

To download the latest Mobile Synchronization Server Client for Palm OS, you must access the Mobile Synchronization Server User Portal. Contact your Mobile Synchronization Server service provider for more information.

To Download the Latest Client for Palm OS

- From the Mobile Synchronization Server User Portal, select the Downloads tab. The Palm OS options are displayed by default.

The Downloads/Palm OS screen has the options Send to Phone, Download to PC, and Download User Guide.

Sending to Phone

To Send to a Phone

1. Type your telephone number in the field provided.
You must use the international format. For example, **+441234567890**.
2. Click Send.
A provisioning message arrives on your device momentarily. Follow the onscreen instructions to install the Mobile Synchronization Server Client.

Downloading to PC

To Download to a PC

1. Click Download to PC to download the Mobile Synchronization Server client file to your desktop.



Note

You must have a data cable to connect your Palm device to your desktop. Alternatively, your desktop and your Palm device should be Bluetooth enabled to transfer files.

2. After the client installer downloads, transfer the file from the desktop to your Palm device and install the software on your Palm device. For more information, refer to the documentation provided with your device.

Downloading User Guide

To Download User Guide

- Click the Download User Guide link to download the Mobile Synchronization Server Client documentation to your desktop in PDF format.

Updating the Mobile Synchronization Server Client

Before updating the Mobile Synchronization Server Client, verify the version installed on your Palm device by accessing the About screen.

About Screen

The About screen displays the current version of the client installed on your device.

To Display the About Screen

1. Tap the tool bar in the upper left corner of the Mobile Synchronization Server Client screen.
The Options menu appears.
2. Choose About.
The About screen appears. The current version number is displayed here.
3. Click OK to exit and return to the Mobile Synchronization Server Client screen.
Regularly repeating the steps in [Mobile Synchronization Server Client Installation for Palm OS](#) ensures that you have the latest version of the Mobile Synchronization Server Client installed on your Palm device.

You must first ensure that you have removed the previous client from your device, as described next.

Removing Previous Client

To Remove the Previous Client

1. To remove the previous Mobile Synchronization Server Client from your Palm device, find the OCMSS icon in the list of applications installed on your device.
2. Tap the Menu key to display the Applications menu.
3. Choose Delete.
4. Choose OCMSS from the list of programs installed in your Palm device.
5. Confirm that you want to delete the Mobile Synchronization Server Client by tapping Yes
You can now install the latest Mobile Synchronization Server Client by following the steps in [Mobile Synchronization Server Client Installation for Palm OS](#).

Configuring Mobile Synchronization Server Client

The Mobile Synchronization Server Client needs to be configured before synchronization is possible. This section shows how to enter your Mobile Synchronization Server gateway account details on the device.

Locating the Mobile Synchronization Server Client Icon

To Start the Mobile Synchronization Server Client

1. The Mobile Synchronization Server Client icon is listed as one of the options in your Palm device screen identified by OCMSS.
2. Select the OCMSS icon.
The Mobile Synchronization Server Client screen appears.

Checking Server Settings

To Check your Server Settings

1. Tap the tool bar in the upper left corner of the Mobile Synchronization Server Client screen.
The Options menu pops up.
2. Choose Server.
The Server screen is displayed.
The three fields on the Server screen are used to specify the server address, port number, and option to use a secure connection (SSL). These settings enable your Palm device to communicate wirelessly with the Mobile Synchronization Server.
The fields on the Server screen are configured in one of the following ways:
 - Preconfigured by your Oracle Communications Mobile Synchronization Server service provider.
 - Configured manually on the Palm device.
3. If the Server screen fields are blank, contact your Mobile Synchronization Server service provider for assistance.
4. Tap Save to exit this screen and return to the Mobile Synchronization Server Client screen.

Entering Your Credentials

To Enter Your Credentials

1. Tap the tool bar in the upper left corner of the Mobile Synchronization Server Client screen.
2. Choose Login.
The Login screen appears.
3. Type the unique user name registered on your Mobile Synchronization Server account in the Login field, and your password in the Password field.
4. Tap Save to exit this screen and return to the Mobile Synchronization Server Client screen.

Selecting the Synchronization Type and Method

Before synchronization can occur, you must select the synchronization type and method.

Selecting the Synchronization Type

To Select a Synchronization Type

1. Tap the tool bar in the upper left corner of the Mobile Synchronization Server Client screen.
The Options menu pops up.
2. Choose Sync Options.
The Sync Options screen appears. Two types of synchronization can occur between your Palm device and the Mobile Synchronization Server, selectable from the Data menu:
 - Exchange Modified. The Mobile Synchronization Server compares all data items stored on your Palm device with data items stored in your PIM server, and synchronizes only new or changed data items.
 - Exchange All. The Mobile Synchronization Server compares all data items stored on your Palm device with those data items stored in your PIM server. During synchronization all items are refreshed.
3. To select the type of synchronization, tap the Data menu.

The option to display the Summary screen after each synchronization session is enabled by default. You can disable this option by clearing the Show summary checkbox.

Selecting Synchronization Method

To enable your Palm device to receive updates automatically from the Mobile Synchronization Server gateway server, the Automatic Synchronization box is selected by default.

Clear the Automatic Synchronization checkbox to disable automatic updates to your Palm device. After this feature is disabled, a manual synchronization is required to receive updates from the Mobile Synchronization Server.

To Select a Synchronization Method

1. Select one of the two automatic synchronization methods by tapping either field:
 - Data Push. The Mobile Synchronization Server sends an automatic request for your Palm device to start a synchronization session. This request must be configured by using the Mobile Synchronization Server User Portal.
 - Scheduled. The Mobile Synchronization Server Client is timed to initiate an automatic synchronization session with the Mobile Synchronization Server. If you choose this method, specify how often you want your Palm device to automatically query the Mobile Synchronization Server for updates by tapping the Interval field and typing your chosen number of minutes.
2. Optional. The Audible Alert feature makes the device chime when new items are received. This chime is enabled by default. Clear the checkbox to disable it.
The Enable Logging feature logs the diagnostic information to help identify issues. An

administrator can use some of the diagnostic data to troubleshoot issues with synchronization. By default, this option is not selected.

3. Tap Save to exit the Sync Options screen.

Beginning Synchronization

You are almost ready to begin synchronization. First, you must select which data items to synchronize between your Palm device and the Mobile Synchronization Server.

Selecting Data to Synchronize

To Select Data to Synchronize

- The Mobile Synchronization Server Client synchronizes contacts, calendar events, and tasks with the Mobile Synchronization Server. All data items are selected by default. To deselect any data item, clear the corresponding checkbox on the Mobile Synchronization Server Client screen.

Locating the Sync Button

To Start a Synchronization Session

1. Tap Sync located in the lower left corner of the Mobile Synchronization Server Client screen. The Summary screen appears with a progress bar indicating the status of the synchronization session.
2. Optional. If you want to stop synchronizing, tap Cancel. When the progress bar is completely filled in, the synchronization is finished. The message Synchronization Completed is displayed. The New, Updated and Removed rows display results of changes made on the Palm device as a result of the synchronization.
3. To view the results of the changes made, perform one of the following steps:
 - a. Tap Server to switch to results of changes made on the Server.
 - b. Tap Device to revert to the Device results.
 - c. Tap OK to exit the Sync Summary screen and return to the Mobile Synchronization Server Client screen.

Troubleshooting

This section contains descriptions of all the error messages generated by the Mobile Synchronization Server Client.

"Please Enter Username/Password"

If you left the Login or Password fields blank when entering your credentials, a Login Error is displayed when you attempt to synchronize.

To Enter Your Credentials

1. Click OK and return to the Login screen to enter your credentials. For more information, see [Entering Your Credentials](#).
2. Tap Sync to attempt synchronization again.

"Authentication Failure"

If you typed an email address or password different to the email address or password stored by the Mobile Synchronization Server, an error is displayed when you attempt to synchronize.

To Correct an "Authentication Failure"

1. Open the Server screen and delete, then reenter your email address and password.
2. Tap Save to return to the Mobile Synchronization Server Client screen.
3. Tap Sync to attempt synchronization again. If the credentials you entered this time were correct, the synchronization proceeds. The error occurs again if you attempt to synchronize without entering valid credentials.

"No Sync Item Is Selected"

On the Mobile Synchronization Server Client screen, if no data items are selected for synchronization, the error message "No Sync Item is Selected" appears when synchronization is attempted.

To Correct "No Sync Item Is Selected"

1. Click OK to return to the Mobile Synchronization Server Client screen.
2. Select the data item or items you want to synchronize by selecting the data item or items option checkbox.
3. Tap Sync to attempt synchronization again.



Note

At least one item must be selected to avoid this error when synchronizing.

"Connection Failure"

To Correct "Correction Failure"

1. If you receive a "Connection Failure" message, check for two possible reasons.
 - a. Ensure that a valid data service is correctly configured on your Palm device. Contact your operator for information about how to perform this configuration.
 - b. Check that you are in an area with data service. Check for the aerial and GPRS symbols on your Palm device home screen.
2. Contact your Oracle Communication Mobile Synchronization Server service provider to ensure the server is running.
3. Optional. If, after checking the previous items, you are still unable to synchronize, issue might be with the data service in your area or related to your account. Contact your operator for more information.

Chapter 5. Mobile Synchronization Server Client Setup Guide for Windows Mobile

Oracle Communications Mobile Synchronization Server Client Setup Guide for Windows Mobile Version 1.1

The Mobile Synchronization Server Client for Windows Mobile enables your Windows Mobile device to synchronize your personal data items through Mobile Synchronization Server.

This information describes how to set up your Windows Mobile device to work with your Mobile Synchronization Server synchronization service. The Mobile Synchronization Server Client is a small application that, when installed on your Windows Mobile device, connects to the Mobile Synchronization Server to provide automatic synchronization of contacts, calendar events, and tasks to and from your Personal Information Manager (PIM) Server and your Windows Mobile device.

Topics:

- [Mobile Synchronization Server for Windows Overview](#)
- [Device Setup](#)
- [Troubleshooting](#)

Mobile Synchronization Server for Windows Overview

This section describes the prerequisites for using the synchronization service on your Windows Mobile device.

Supported Windows Mobile Devices

The following Windows Mobile Devices are compatible with the Mobile Synchronization Server Client:

- Smartphone 2003 SE
- Pocket PC 2003 SE
- Windows Mobile 5.0 Smartphone
- Windows Mobile 5.0 Pocket PC
- Windows Mobile 6.0 Smartphone

Before You Start

You must have the following:

- A Mobile Synchronization Server account.
- A compatible Windows Mobile device.
- A Data connection (CSD, GPRS, or UMTS) set up on your Windows Mobile device.

Contact your mobile operator to set up a data plan or to confirm your mobile data access information.

Device Setup

This section describes how to set up your Windows Mobile device to synchronize with your Mobile Synchronization Server account. You learn how to install the Mobile Synchronization Server Client, add your account information, and eventually synchronize your personal data items.

Mobile Synchronization Server Client Installation for Windows Mobile

To download the latest Mobile Synchronization Server Client for Windows Mobile, you must access the Mobile Synchronization Server User Portal. For more information, contact your Mobile Synchronization Server service provider.

To Download the Latest Client for Windows Mobile

- From the Mobile Synchronization Server User Portal, select the Downloads tab.

The Downloads/Windows Mobile screen has the options Send to Phone, Download to PC, and Download User Guide.

Sending to Phone

To Send to a Phone

1. Type your telephone number into the field provided.
You must use the international format. For example, **+441234567890**.
2. Click Send.
A provisioning message arrives on your device momentarily.
3. Follow the on-screen instructions to install the Mobile Synchronization Server Client.

Downloading to PC

To Download to a PC

1. Click Download to PC to download the Mobile Synchronization Server client file to your desktop.



Note

You must have a data cable to connect your Windows Mobile device to your desktop. Alternatively, your desktop and your Windows Mobile device should be Bluetooth enabled to transfer files.

2. After the client installer downloads, transfer the file from the desktop to your Windows Mobile device and install the software on your Windows Mobile device.

For more information, refer to the documentation provided with your device.

Downloading the User Guide

To Download the User Guide

- Click the Download User Guide link to download the Mobile Synchronization Server Client documentation to your desktop in PDF format.

Updating the Mobile Synchronization Server Client

Regularly repeating the steps in [Mobile Synchronization Server Client Installation for Windows Mobile](#) ensures that you have the latest version of the Mobile Synchronization Server Client installed on your Windows Mobile device.

About Screen

The About Screen displays the current version of the client installed on your device.

To Display the About Screen

1. Choose the Settings menu in the lower right corner of the Mobile Synchronization Server Client screen.
The Settings Menu appears.
2. Choose About or tap number 4 on your key pad.
The About screen appears. The current version number is displayed.
3. Click Done to exit and return to the Mobile Synchronization Server Client screen.

Configuring Mobile Synchronization Server Client

The Mobile Synchronization Server Client needs to be configured before synchronization is possible. This section shows you how to enter your Mobile Synchronization Server account details on the device.

Locating the Mobile Synchronization Server Client Icon

To Start the Mobile Synchronization Server Client

1. The Mobile Synchronization Server Client icon is listed as one of the options in your Windows Mobile device screen identified by the OCMSS icon.
2. Select the OCMSS icon.
The Mobile Synchronization Server Client screen appears.

Checking Server Settings

To Check Server Settings

1. Choose Settings in the lower right corner of the Mobile Synchronization Server Client screen. The Settings Menu pops up.
2. Choose Server or tap number 2 on your keypad.
The Server screen is displayed.
The three fields on the Server screen are used to specify the server address, port number, and option to use a secure connection (SSL). These settings enable your Windows Mobile device to communicate wirelessly with the Mobile Synchronization Server.
The fields on the Server screen are configured in one of the following ways:
 - Preconfigured by your service provider.
 - Configured manually on the mobile device.
3. If the Server screen fields are blank, contact your Mobile Synchronization Server service provider for assistance.
4. Click Done to exit this screen and return to the Mobile Synchronization Server Client screen.

Entering Your Credentials

To Enter Your Credentials

1. Choose the Settings menu.
2. Choose Login or tap number 1 on your keypad.
The Login screen appears.
3. Type the unique email address registered on your Mobile Synchronization Server account in the Login Name field, and your password in the Password field. Select the Save Password checkbox to store your credentials.
4. Click Done to exit this screen and return to the Mobile Synchronization Server Client screen.

Selecting the Synchronization Type and Method

Before synchronization can occur, you must select the synchronization type and method.

Select Synchronization Type

1. Choose Settings located in the right corner of the Mobile Synchronization Server Client screen. The Settings menu pops up.
2. Choose Sync Options or tap number 3 on your keypad. The Sync Options screen appears. Two types of synchronization occur between your Windows Mobile device and the Mobile Synchronization Server gateway server:
 - Update only changed items. The Mobile Synchronization Server gateway server compares all data items stored on your Windows Mobile device with data items stored in your PIM server, and synchronizes only new or changed data items.
 - Update all items. The Mobile Synchronization Server compares all data items stored on your Windows Mobile device with those data items stored in your PIM server. During synchronization all items are refreshed.
3. To select the type of synchronization, select the left or right arrow on the list navigation box.

The option to display the Summary screen after each synchronization session is enabled by default. You can disable this option by clearing the checkbox, Show summary after a synchronization.

Selecting Synchronization Method

To enable your Windows Mobile device to receive updates automatically from the Mobile Synchronization Server, the Automatic Synchronization box is selected by default.

Clear the Automatic Synchronization checkbox to disable automatic updates to your Windows Mobile device. After this feature is disabled, a manual synchronization is required to receive updates from the Mobile Synchronization Server.

To Select a Synchronization Method

1. Select one of the two automatic synchronization methods by using either arrow on the list navigation box:
 - Scheduled. The Mobile Synchronization Server Client is timed to initiate an automatic synchronization session with the Mobile Synchronization Server gateway server. If you choose this method, specify how often you want your Windows Mobile device to automatically query the Mobile Synchronization Server for updates by selecting the Period in Mins field and typing your chosen number of minutes.
 - Push. The Mobile Synchronization Server sends an automatic request for your Windows Mobile device to start a synchronization session. This request must be configured by using the Mobile Synchronization Server User Portal.
2. Optional. The Audible Alert feature makes the device chime when new items are received. This chime is enabled by default. Clear the checkbox to disable it.
3. Click Done to exit the Sync Options screen.

The Enable Logging feature logs the diagnostic information to help identify issues. An administrator can use some of the diagnostic data to troubleshoot issues with synchronization. By default, this option is not selected.

Beginning Synchronization

You are almost ready to begin synchronization. First, you must select which data items to synchronize between your Windows Mobile device and the Mobile Synchronization Server.

Selecting Data to Synchronize

To Select Data to Synchronize

The Mobile Synchronization Server Client synchronizes contacts, calendar events, and tasks with the Mobile Synchronization Server.

1. Optional. All data items are selected by default.
2. To deselect any data item, clear the corresponding checkbox.

Locating the Sync Button

To Start a Synchronization Session

- Click Sync located in the left corner of the Mobile Synchronization Server Client screen. The Summary screen appears with a progress bar indicating the status of the Synchronization session.



Note

The New, Updated and Removed rows display details of the synchronization when it is finished.

Synchronization Results

When the progress bar is completely filled in, the Synchronization is finished. The New, Updated, and Removed rows are now populated with the results of changes made to the Mobile Synchronization Server Client as a result of the synchronization.

To View the Synchronization Results

1. To view the results of changes made, perform one of the following steps:
 - a. Click Server to switch to results of changes made on the Server side.
 - b. Click Client to revert to the Client results.
2. Click Done to exit the Summary screen and return to the Mobile Synchronization Server Client screen.

Troubleshooting

This section contains descriptions of all the error messages generated by the Mobile Synchronization Server Client.

After Selecting Sync, the Login Screen Appears

If you left the Login or Password fields blank when entering your credentials, the Login screen is displayed when you attempt to synchronize.

To Enter Your Credentials

1. Type your credentials into the Login Name and Password fields.
2. Select the Save Password checkbox and your credentials are stored in your device's memory.
3. Click Done to continue.
If the credentials you entered this time were correct, the synchronization proceeds. The error occurs again if you attempt to synchronize without entering your credentials.

"Synchronization Refused" Appears

If you typed an email address or password different from the email address or password stored by the Mobile Synchronization Server, a message box is displayed when you attempt to synchronize.

To Correct Synchronization Refused

1. Open the Login screen and delete, then reenter your email address and password.
2. Click Done to return to the Mobile Synchronization Server Client screen and try to synchronize again by selecting Sync. If the credentials you entered this time were correct, the synchronization proceeds. The error occurs again if you attempt to synchronize without entering valid credentials.

"Nothing Selected to Sync" Appears

On the Mobile Synchronization Server Client screen, if no data items are selected for synchronization, the error message "No data selected for Synchronization" appears when synchronization is attempted.

To Correct "Nothing Selected to Sync"

1. Click Done to go back to the Mobile Synchronization Server Client screen.
2. Select the data item or items you want to synchronize by selecting the data item or items option checkbox.



Note

At least one item must be selected to avoid this error when synchronizing.

"Communication Error" Appears

To Correct Communication Error

1. If you receive a "Communication Error" message, check for two possible causes:
 - a. Ensure that a valid data service is correctly configured on your Windows Mobile device. Contact your operator for information about how to perform this configuration.
 - b. Check that you are in an area with data service. Check for the aerial and GPRS symbols on your Windows Mobile device home screen.
2. Optional. If, after checking the previous items, you are still unable to synchronize, there might be an issue with the data service in your area or related to your account. Contact your operator for more information.

Chapter 6. Mobile Synchronization Server Administration Guide

Oracle Communications Mobile Synchronization Server Administration Guide

This information describes how to administer Mobile Synchronization Server. The Configuration section describes the steps necessary to configure Mobile Synchronization Server's general settings. The Administrator Tasks section describes how to create and delete user accounts, and modify user synchronization settings.

Topics:

- [Configuring Oracle Communications Mobile Synchronization Server](#)
- [Administration Tasks](#)

Configuring Oracle Communications Mobile Synchronization Server

This section describes how to configure the Mobile Synchronization Server gateway.

Logging in to the Administration Portal

To Log in to the Administration Portal

1. Type the administrator login page URL set during installation:
`http://servername:instanceport/sync/admin`
The server name, *servername*, and port, *instanceport*, were set during installation.
2. Confirm that you can see the login page.
3. Type the default user name **admin** and the password **syncpass** and click Login.

General Configuration

This section describes the global settings for the Mobile Synchronization gateway. You must complete these instructions before proceeding to [Administration Tasks](#).

The following steps are required for general configuration:

- [Changing the Administrator Password](#)
- [Configuring the Gateway Server](#)
- [Configuring the Gateway Back End](#)
- [Configuring the Communications Suite Back End](#)
- [Configuring Short Message Peer-to-Peer \(SMPP\) Protocol for Client Provisioning](#)

Changing the Administrator Password

To Change the Administrator Password

The default installation password is a security risk. You must change it.

1. Log in to the Administration portal.

2. Select the Gateway Tab.
3. Locate the Change Admin Password dialog box.
4. Type the old password, type the new password, and repeat the new password for confirmation.
5. Click Change Password to confirm the change.

Configuring the Gateway Server

To Configure the Gateway Server

1. Log in to the Administration portal.
2. Use the Gateway Tab to configure the Synchronization server settings.
3. Locate the Synchronization server dialog box.
4. Confirm that the server URL is correct.
The Server URL field specifies the location of the Mobile Synchronization Server gateway. This URL is sent to client devices during provisioning.
5. Type an appropriate application name.
The application name appears in Client Provisioning Short Message Service (SMS) messages sent to user devices. This is the name of the synchronization profile. A mobile device can have more than one synchronization profile. This name also acts as a "friendly name" to identify the sender to the end user. If the origin of the message is known, it is more likely to be accepted and the settings are more likely to be applied.
6. Click Save to store any changes.

Configuring the Gateway Back End

Currently only Communications Suite is supported as the back end for Mobile Synchronization Server.

To Configure the Gateway Back End

1. Log in to the Administration portal.
2. Click the Back-ends tab to specify the Communications Suite back-end details.
3. Click the Usage sub tab to view the available back ends.
These are listed in the Back-end usage dialog box.
4. Select the Use Communications Suite checkbox.
5. Click Save to apply any changes.

Configuring the Communications Suite Back End

To Configure Communications Suite

1. Log in to the Administration portal.
2. Click the Back-ends tab to change the back-end server settings.
3. Click the Communications Suite sub tab to define the Web Calendar Access Protocol (WCAP) and Lightweight Directory Access Protocol (LDAP) settings for Communications Suite.



Note

WCAP is used to communicate with Calendar Server 6.3. You must configure this setting correctly to enable calendar synchronization.

4. In the WCAP Settings dialog box, do the following:
 - a. Type the Calendar Server host name in the Host field.
 - b. To enable logging of WCAP activity, select the Logging Enabled checkbox and type a directory name in the Logging Directory field. By default this is `/tmp/wcapLogging`.
 - c. Click Save to use these settings.
5. In the LDAP User Identity Settings dialog box, do the following:
 - a. In the User identity host field, type the host ID of the LDAP server, that is, the IP address or domain name service (DNS) name of the LDAP server. For example:

11.22.33.44(IP address format)

LDAP.host.com(DNS format)

- b. In the User identity BaseDN field, type the host name of the LDAP User details server. For most installations type **ou=People,o=%D,dc=domainname1,dc=domainname2**
If users are located at `example.com`, for example, then *domainname1* is equal to `example` and *domainname2* is equal to `com`.
- c. In the Manager DN field, type the details of the LDAP domain manager:
 - For most installation, type **cn=Directory Manager** in the Manager DN field.
 - For installations where a less-privileged user is needed, type the DN of this user as the contact name, using the previous format.
- d. In the Manager Password field, type the password of the user in the previous step.
- e. In the Default Domain field, type the default domain of the user by using the format: **domainname1.domainname2**
for example: **example.com**
- f. In the UID Search field, type the UID Search text in the following format:
uid=%U
- g. In the Email Search field, type the UID Search text in the following format:
mail=%E



Note

You can also leave this field blank.

- h. Click Save to store and apply these settings.
6. Use the LDAP address book settings dialog box to synchronize contacts and tasks.
- a. Select the Using ComExpress checkbox if you are using Communications Express. Otherwise ensure that the checkbox is cleared.
 - b. In the Address Book Host field, type the host ID of the LDAP address book server, that is, the IP address or domain name service (DNS) name of the LDAP address book server. For example:
11.22.33.44 (IP address format)
ldapaddressbook.host.com (DNS format)
 - c. In the Address Book BaseDN, Type the correct format.
The expected format for this field is dependent on whether or not you are using Communications Express. If you are using Communications Express, the format for this field is the modern Communications Suite UI:
o=%D,o=PiServerDb
If neither %U nor %E appear in the configured value, this is automatically expanded internally to (using Communications Express):
`pipStoreOwner=%U,o=%D,o=PiServerDb`
When you are not using the standard address book schema, you can override it for example with:
`myOwnerAttribute=%E,o=%D,o=PiServerDb` or `ou=%E,o=%D,o=PiServerDb`
If you are not using Communications Express, the format for the Address Book BaseDN is the older Communications Suite UI:
ou=People,o=%D,o=isp,o=pab
If neither %U nor %E appear in the configured value, this is automatically expanded internally to (not using Communications Express):
ou=%U,ou=People,o=%D,o=isp,o=pab
When you are not using the standard address book schema, you can override it for example with:
`myOwnerAttribute=%U,ou=People,o=%D,o=isp,o=pab` or
`ou=%E,ou=People,o=%D,o=isp,o=pab`



Note

%U is substituted by the user ID, %E is substituted by the email address, and %D is substituted by the user-specific domain name.

- d. In the Manager DN field, type the details of the Domain Manager.
For most installations, type `cn=Directory Manager`.
For installations where a less-privileged user is needed, type the DN of this user instead.
- e. In the Manager Password field, type the password of the user in the previous step.
- f. Click Save to store and apply these settings.

Configuring Short Message Peer-to-Peer (SMPP) Protocol for Client Provisioning

To Configure SMPP for Client Provisioning:

1. Obtain your SMS service provider's SMPP details.
2. Click the SMS tab.
3. Locate the SMPP connection dialog box.
4. Type the SMPP server and port of your SMS service provider so that Mobile Synchronization Server can send provisioning messages to mobile devices.
5. Type the user name and password supplied by the SMS service provider.
6. Check that the details are correct
7. Click Save to store these values.

The Mobile Synchronization Server gateway is now fully configured.

Administration Tasks

This section contains tasks that you can perform by using the Mobile Synchronization Server Administration Portal.

Creating a User

The following methods are available for creating a user account on the gateway:

- The user creates the account through a mobile device.
- The administrator creates the account by using the Administration Portal on the gateway.
- The user creates an account by using the User Registration page on the gateway.

This information discusses creating a user account on the Administration Portal. Details of the other methods can be found in [Mobile Synchronization Server Client Setup Guide for Palm OS](#) and [Mobile Synchronization Server Client Setup Guide for Windows Mobile](#). See the sections on user setup and mobile device setup.

It is generally easier either for the administrator to create a user account by using the Administration Portal, or for users to register themselves through the User Registration page. In both methods the gateway server settings are sent to the device by SMS rather than typed manually by the end user, as required by device-based setup.

Create a user account by performing the following steps:

1. Entering user account details (carried out on the gateway)
2. Provisioning a mobile device (carried out on the gateway)
3. Accepting provisioning (carried out on the mobile device)

Entering User Account Data

To Enter a new user account data:

1. Click the Users tab.
2. Click the Create user sub tab.

The Create user dialog box contains the fields:

- User Email address
- Password
- User name
- Back-end server details, in this case, the details of the Communications Suite URL

To Create a new user account on the gateway:

1. In the Email address field, type the new user's email address.
The address must be the same as the email address for the user's account on the back-end server.
 2. In the Password field, type the user's password on the back-end server.
 3. In the User Name field, type the new user's Communications Suite user name.
 4. In the Mobile Device Number field, type the phone number of the user's mobile device.
 5. Click Register.
The Mobile Synchronization Server gateway verifies the user data with the back-end server.
- If successful, the message "User Successfully Created" appears. Proceed to the next stage: [Provisioning a Mobile Device](#).
 - If an error is displayed, check the new user details for errors.

Provisioning a Mobile Device

Now that the new user is registered with the gateway, you are ready to provision the user's mobile device with the synchronization settings. When you select the Edit Users tab, a list of user accounts on the gateway is displayed in table format.

Navigating the List of Users

To Navigate the list of registered users:

- Click the Prev and Next buttons.
- Click a column label to sort the list by that column.
- To search for a specific email address, user name or back-end URL, type the information in the Find field then click Search.

The following table describes the information contained in the list of registered users.

Description of the Columns in the List of Registered Users

Column	Description
Email	The user's email address.
User name	The user name used by the back-end server.
Back-End	The back-end server details, for example, the server URL.
First	The date of the first user synchronization session.
Last	The date of the last user synchronization session.
Syncs	The total number of synchronization sessions. For some mobile devices, a synchronization session may consist of multiple subsessions, with contacts, calendar events, and tasks as separate sessions.
Failures	Displays the number of failed synchronization sessions. Failure can be caused by a synchronization error or a wireless link interruption. Use the log file to determine the cause of failure.

To Access the Mobile Device Setup Page for the New User

- Navigate to the recently created user and click the Preferences button to the right of the row containing the user's details.
This action displays the Mobile Device Setup page for that user.

To Set up the User's Mobile Device

1. Set the following fields in the Mobile Device Configuration dialog box:
 - a. Choose the User's country from the Country drop-down list.
 - b. Choose the correct mobile operator from the Operator drop-down list.
 - c. Choose the mobile device manufacturer from the Make drop-down list.
 - d. Choose the model of the mobile device from the Model drop-down list. In the Mobile Device Number field, type the mobile device phone number. You must use international format, for example **+441234567890** for a UK mobile.
2. Click save to store these details.

To Send Configuration Settings to a User's Phone

1. Locate the Send configuration settings in the User's Mobile Device dialog box.
2. Note the User Pin.
Users must type this PIN on their device when the provisioning SMS arrives.
3. Click send.
The Mobile Synchronization Server gateway sends the provisioning information to the user's mobile device.

Accepting Provisioning (Mobile Device)

Shortly after clicking send, an SMS is sent to the mobile device. When users receive this SMS they must open the message and select the Save settings option.



Note

The exact option varies depending on the device make and model.

The user must type the agreed PIN. If the PIN is correct, the device is now ready to synchronize with the back-end server. The user can select synchronize on the device to start the first synchronization. The user is now fully setup.

Deleting a User

This section describes how to delete a Mobile Synchronization Server gateway user.

To Delete a User

1. From the Administration Portal select the Users tab.
Mobile Synchronization Server displays the Edit user dialog box.
2. Navigate to the correct user.
See [Navigating the List of Users](#) for details.
3. Click the user's corresponding Delete button.
This action deletes the user's gateway account. This action does not delete any data on the Communications Suite server or on the mobile device, but removes any information about previous synchronization sessions from the Mobile Synchronization Server gateway database.

The user's account is now deleted.

Viewing a User's Log

To View a User's Log

1. Navigate to the correct user.
See [Navigating the List of Users](#) for details.
2. Click Show Log to the right of this user.


This action displays a summary of all user sessions in a new browser window. Use this summary to troubleshoot synchronization problems.

Resetting a User

To Reset a User


1. Navigate to the correct user.
See [Navigating the List of Users](#) for details.
2. Click Reset to the right of this user.
This action resets the stored synchronization information mapping for the particular user, which will cause a complete synchronization of all data during the next synchronization. Use this function if a particular user has synchronization problems. Be aware that resetting a user significantly slows down the next synchronization.

Resetting Synchronization Mappings

 **Caution**
Resetting synchronization mappings is immediate (there is no confirmation dialog), and significantly affects system performance.

To Reset Synchronization Mappings

- Click Reset synchronization mappings to delete all ItemIDs (data mappings) stored on the gateway for all users. Synchronization mappings are used to map the relationship between data on the back-end Communications Server and the device.

 **Note**
Reset synchronization mappings only when experiencing persistent synchronization problems.

All synchronization information in the Mobile Synchronization Server gateway database is discarded. All users must perform a complete synchronization of all data, which is significantly slower than usual. Note that in all other respects synchronization behaves as normal from the users' viewpoint.

Setting the Mobile Communications Logging Level

For normal day to day operation the Info level should be sufficient. The following table shows the available options:

Logging Levels

Logging Level (highest to lowest)	Description
All	All messages are logged.
Fine	Message level providing tracing information.
Info	Message level for informational messages.
Warning	Message level indicating a potential problem.
Severe	Message level indicating a serious failure.

To Set the Logging Level

1. Use the drop down box within the Logging Configuration dialog to select the required level of logging.
2. Click Save to store the setting.

Setting a User's Synchronization Preferences

To Set a User's Synchronization Preferences

1. Navigate to the correct user as described in the Edit Tab Section.
2. Click Preferences to the right of this user.

The Preferences tab is used for specifying individual settings for the selected user.

The following Synchronization Preference subtabs are available from the Preferences tab:

- Synchronization
- Calendar Filter
- Account

These tabs are described in the following sections.

Synchronization

The Synchronization tab is used to specify data push options for the selected user. The Synchronization tab contains the dialog boxes: Data Items and Schedule.

Push requires that only one synchronization profile exists on the mobile device. If other synchronization profiles exist on the device and the user wants to use push synchronization, they must delete the other synchronization profiles.



Note

If the selected user's mobile device does not support push synchronization, the dialog boxes on this page are disabled.

To Set Which Data Items to Include in a Push Synchronization

1. Locate the Data items dialog box.
2. Select the checkboxes for the data types to be pushed to that user from the following list: calendar events, contacts, and tasks.
3. Click Save to store and apply these settings.

Scheduling Push Synchronization

To Schedule Push Synchronization:

1. Select the minimum interval in minutes between separate push synchronizations.
On each push synchronization, the Mobile Synchronization Server gateway pushes information about new, updated, or deleted data items on the back-end server to the user.
2. Click Save to store and apply these settings.

The selected interval is restricted by the Administrator settings. For more information, see [Schedule](#).

Calendar Events Filter

To Filter Which Calendar Events and Tasks the Selected User Receives

1. Click the Calendar Events Filter tab.
This tab can contain the following filter dialog boxes: Time Window for Calendar Events, Completion level of tasks, and Start date of tasks. The actual filter dialogs boxes displayed depend on the options chosen in the main Calendar Events Filter settings Tab. For more information, see [Set Calendar Filter Preferences](#).
2. Set the Synchronization Time Window for calendar events.
 - a. Select the checkbox none (sync all calendar events) to choose which calendar events to synchronize:
 - If **none** is checked, the system default values are used.
 - If **none** is unchecked, calendar events are synchronized as far back as the value entered in the Starting days in the past field and as far forward as the value entered in the Days in the Future field.



Caution

Calendar events that already exist on the device and that are older than the period entered in this field are deleted as part of the Synchronization process. This setting is used to save device memory. Tell the user if you plan to change this setting.

- b. Click Save to store and apply these settings, or Reset to return to the previously saved values.
3. Setting Task Filtering based on Task Completion Status.
To set task filtering based on task completion status:
 - a. Select or clear Incomplete only:
 - If Incomplete only is checked, only tasks that the user has not completed are synchronized by default.



Caution

Completed tasks on the device are deleted. This is used to save device memory. Warn the user if you change this setting.

- If Incomplete only is unchecked, completed tasks are synchronized up to the number of days specified in the field, Leave time for completed tasks.



Caution

Tasks completed prior to this date are removed from the device. This setting is used to save device memory. Warn the user if you plan to change this setting.

- b. Click Save to store and apply these settings, or Reset to return to the previously saved values.
4. Setting Task Filtering based on Task Start Date.
To set task filtering based on task start date:
 - a. Select either No filtering or Only tasks that start in the past.

- If No filtering is checked, all tasks (regardless of start date) are synchronized.
- If Only tasks that start in the past is checked, only those tasks with a start date in the past are synchronized.

**Caution**

Task items that already exist on the user's mobile device, with a start date in the future, are deleted as part of the synchronization process. This setting is used to save device memory. Warn the user if you plan to change this setting.

- b. Click Save to store and apply these settings, or Reset to return to the previously saved values.

Account

From the account tab it is possible for the system administrator to change a user's password or mobile device number.

1. Enter the user's old password in the Old Password field.
2. Enter the user's new password in the New Password field.
3. Confirm the new password by re-entering it in the Retype New Password field.
4. Click Save to store and apply the new password.

To Change the User's Mobile Device Number

1. Enter the new number in the Mobile Device Number field.
2. Click Save to store and apply the new number.

Set Synchronization Preferences for All Users

The Preferences tab is used to define both default and master synchronization settings for all users. For some settings it enables the administrator to control whether a value can be modified at the level of an individual user and if so, the range of settings available. Individual user preferences can be accessed by the users themselves on the user portal or by the administrator by using the preference option in the Users tab. See the [Mobile Synchronization Server Client Setup Guide for Palm OS](#) and the [Mobile Synchronization Server Client Setup Guide for Windows Mobile](#) for more information.

The Preferences tab contains two sub tabs, described later in this document:

- Synchronization
- Calendar Events Filter

Synchronization Preferences

The Synchronization tab is used to set the default push settings for all user accounts. It contains the following dialog boxes:

- Data Items
- Push Strategies
- Number of Alerts
- Schedule

Data Items**To Set the Data Items That Are Pushed to a User's Device**

1. Locate the Data Items dialog box.

2. For each data item, calendar events, contacts, and tasks, select one of the following checkboxes:
 - Default: If Default is checked, that data type is automatically pushed to each user's mobile device every time a push synchronization is triggered.
 - Users can define: If User can define is checked, users are able to change their individual synchronization setting for this item through the User Portal. See the [Mobile Synchronization Server Client Setup Guide for Palm OS](#) and the [Mobile Synchronization Server Client Setup Guide for Windows Mobile](#) for more details. If it is unchecked, the administrator preferences cannot be overridden by users.
3. Click Save to store and apply these settings.

Push Strategies

The Push Strategies dialog box contains a list of methods or strategies for carrying out push synchronization. Currently only one strategy is supported by the gateway. This is the OMA-DS Server Alert sent by SMS message.

To Enable a Push Strategy for All Users with Devices that Support This Strategy

- Select the checkbox which corresponds to the strategy.



Note

In the current version of Mobile Synchronization Server, only one strategy is available. Enabling it enables push synchronization for all supported user devices.

To Disable a Push Strategy for All Users with Devices that Support This Strategy

- Clear the checkbox that corresponds to the strategy.



Note

In the current version of Mobile Synchronization Server, only one strategy is available. Disabling it, disables push synchronization for all supported user devices.

Number of Alerts

The Number of Alerts tab is a throttle control. This tab enables the administrator to set the total maximum number of push synchronizations per day for all users (added together) and for each individual user. This feature is used to control the cost or bandwidth usage incurred by push synchronization.

To Set the Number of Alerts

1. Type the default maximum number of alerts per day for all users into the field.
Once this value is reached, push synchronization is disabled for all users until the next day.
2. Type the maximum number of alerts per day for a single user into the field, Max for a single user.
Once this value is reached, push synchronization is disabled for this user until the next day.
3. Click Save to store and apply these settings.

Schedule

The Schedule dialog box enables the administrator to sets the intervals for push synchronization for all users. The following fields are available:

- The interval (default) value sets the default number of minutes the Mobile Synchronization Server waits before checking the server for new items for a user. The default value is used automatically when a new user is created. Users can specify their own individual setting for this value in the User Portal.
- The interval (minimum) value sets the minimum interval value an individual user can specify using

the User Portal.

To Set the Schedule for Push Synchronizations

1. Type the desired values.
2. Click Save to store and apply these settings.

Calendar Filter Preferences

To Set Calendar and Task Filter Preferences

- Use the Main Calendar Filter tab to set the default synchronization options for calendar events and tasks for all users and to define what can be modified at the level of the individual user.

This page contains the following dialog boxes:

- Time Window for Calendar Events
- Completion Level of Tasks
- Start Date of Tasks

Time Window for Calendar Events

This dialog box enables the administrator to set the default filtering options for calendar events for all users.

To Set the Time Window for Past Calendar Events

1. If the Synchronize Calendar Events checkbox is unchecked, calendar events from up to one week in the past and up to one year in the future are synchronized by default. Select the check box to determine how far in the past events should be synchronized.



Note

Calendar events occurring up to one year in the future are synchronized by default and cannot be filtered.

2. You can also specify whether users can define their own filter for Calendar Events. To do this, select the Allow Users to Define a Filter check box and enter a maximum number of days in the past for events to be synchronized.
3. Click Save to store and apply these settings. Click Reset to return to the previously saved values.

Completion Level of Tasks

The Completion Status of Tasks dialog enables the administrator to set default filtering options for tasks (by completion level).

If Incomplete only is checked, then completed tasks are not synchronized.



Caution

All completed tasks on a user's mobile devices will be removed to save device memory. Warn users if you plan to change this setting.

To Synchronize Some Completed Tasks as Well as Incomplete Tasks:

1. Clear Incomplete only.
2. Select User can filter tasks by completion status to enable the user to filter tasks by completion status in the User Calendar Filter Preferences tab.
3. Type two values, default and max, to define the range of values the user can specify for the number of days completed tasks remain on the device.



Caution

Task items that already exist on the device, with a start date before the period entered in the field above will be deleted as part of the Synchronization process. This is to save device memory. Warn users if you plan to change this field.

4. Click Save to store these settings. Click Reset to return to the default value, incomplete only.

Start Date of Tasks

1. Use the Start Date of Tasks dialog box to filter Tasks by start date.
 - If User can filter tasks is checked, then the user can change the settings.
 - If No filtering is selected, then tasks are not filtered by start date.
 - If Only tasks that start in the past is selected, then only tasks that have already started are synchronized.



Caution

Task items that already exist on the device, with a start date before the period typed in the field above will be deleted as part of the Synchronization process. Items are deleted to save device memory. Warn users if you plan to change this field.

2. Click Save to store these settings. Click Reset to return to the default value, no filtering.

Updating Components

The Update tab is used to check for updates to Mobile Synchronization Server components and optionally install these updates.

Updating Configuration Files

To Update Configuration Files

1. Click Check for Updates.
Mobile Synchronization Server gateway contacts an external server to check for updates to configurations file for the following components:
 - Phone Setup Profiles
 - Type Allocation Code (TAC) List
 - Dynamic Device Configuration
 - Specific Device Clients for platforms that do not natively support SyncML for example, Windows Mobile and Palm OS.If any updates are found for these components, the appropriate update buttons are enabled.
2. Click the enabled Update buttons to install these updates.



Note

If no updates are found, a message is displayed advising the administrator.

Chapter 7. Setting Up and Managing Mobile Synchronization Server Security

Setting Up and Managing Oracle Communications Mobile Synchronization Server Security

This information provides an overview about security for the Oracle Communications Mobile Synchronization Server product. It also provides links to security topics that provide more indepth information for configuring and administering Mobile Synchronization Server security.

Topics:

- [Overview of Mobile Synchronization Server](#)
- [Secure Installation and Configuration](#)
- [Security Features](#)

Overview of Mobile Synchronization Server

For an overview of the product, see [Mobile Synchronization Server Technical Overview](#). For information on general security principals, such as security methods, common security threats, and analyzing your security needs, see [Designing for Security](#). For an overview of operating system security, see [Oracle Solaris Security for System Administrators](#).

Secure Installation and Configuration

Topics in this section:

- [Installation Overview](#)
- [Installing Infrastructure Components](#)
- [Installing Mobile Synchronization Server Components](#)
- [Post Installation Configuration](#)

Installation Overview

This section outlines the planning process for a secure installation and describes recommended deployment topologies for the systems.

Understanding Your Environment

To better understand your security needs, ask yourself the following questions:

1. Which resources am I protecting?
In a Mobile Synchronization Server production environment, consider which of the following resources you want to protect and what level of security you must provide:
 - Mobile Synchronization Server gateway
 - Mobile Synchronization Server back end (Postgres database)
 - Dependent resources, such as GlassFish Server, Directory Server, Calendar Server 6.3, and Messaging Server
 - Client security: SyncML clients on the device have the option of connecting to the Mobile Gateway using SSL to protect all data exchange and password exchanges between the

client and the gateway.

2. From whom am I protecting the resources?

In general, resources must be protected from everyone on the Internet. But should the Mobile Synchronization Server deployment be protected from employees on the intranet in your enterprise? Should your employees have access to all resources within the GlassFish Server environment? Should the system administrators have access to all resources? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators. On the other hand, perhaps it would be best to allow no system administrators access to the data or resources.

3. What will happen if the protections on strategic resources fail?

In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use Mobile Synchronization Server. Understanding the security ramifications of each resource help you protect it properly.

Deployment Topologies

You can deploy Mobile Synchronization Server on a single host or multiple hosts. If you want, you can deploy multiple front-end GlassFish Server hosts running the gateway application and then deploy the database on its own host as well. Typically, you deploy the Calendar Server and Messaging Server back ends, to which Mobile Synchronization Server provides access, on their own hosts.

For more information on deploying Mobile Synchronization Server, see the following information:

- [Mobile Synchronization Server Technical Overview](#)
- [Developing a Communications Suite Logical Architecture](#)

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture. For more information on addressing network infrastructure concerns, see [Determining Your Communications Suite Network Infrastructure Needs](#).

Installing Infrastructure Components

Mobile Synchronization Server is deployed within GlassFish Server. For information on how to install and configure GlassFish Server, see [Installing the Application Server](#). To operate GlassFish Server in secure mode, see [Secure Administration Overview](#). For information on how to configure GlassFish Server to use a certificate issued by a Certification Authority (CA) to establish secure sessions through secure sockets layer (SSL) technology, see [To Configure GlassFish Enterprise Server to Use a CA Signed Certificate for SSL](#). For more information, see the [Oracle GlassFish Security Guide](#).

Mobile Synchronization Server uses Postgres as the database for storing user records. For information on how to install and configure Postgres securely, see <http://wiki.postgresql.org>.

Installing Mobile Synchronization Server Components

See [Mobile Synchronization Server Installation Guide](#).

The installation of GlassFish Server, Postgres database, and Mobile Synchronization Server prompts for authentication credentials for the following:

- GlassFish Server administrator
- Postgres user
- Mobile Synchronization Server domain
- Gateway administrator

After installing the preceding software, when you configure the Mobile Synchronization Server gateway, you are prompted for authentication credentials for the Directory Server LDAP manager.

Post Installation Configuration

The high-level post-installation steps to configuring Mobile Synchronization Server for a secure deployment include:

1. Changing the default password for the Mobile Synchronization Server gateway administrator ID.
2. Configuring the gateway to communicate with the Calendar Server, Messaging Server, and LDAP server.

For instructions, see [Mobile Synchronization Server Administration Guide](#).

Security Features

Oracle makes every effort to ensure secure operation of the gateway, which was designed with security in mind. The gateway supports MD5 for encrypted authentication and all traffic flowing through the public Internet is encrypted with SSL (HTTPS), ensuring user data is at no time exposed to prying eyes. For security reasons, the gateway does not duplicate the user's data to a local database, but only meta data required during the synchronization process.

The Oracle Communications Mobile Synchronization Server gateway uses LDAP to authenticate users according to their credentials with Oracle Communications Unified Communications Suite. Calendar items and tasks are synchronized by way of the WCAP adapter, and synchronization of contacts is performed through LDAP. Enhanced security is provided by the usage of the Web Calendar Access Protocol Secure (WCAPS) and Lightweight Directory Access Protocol Secure (LDAPS) protocols.

Chapter 8. Mobile Synchronization Server Glossary

Oracle Communications Mobile Synchronization Server Glossary

Term	Definition
API	(Application Program Interface) A set of routines, protocols, and tools for building software applications.
ASP	(Application Service Provider) A set of routines, protocols, and tools for building software applications.
CSD	(Circuit Switched Data) It is the most basic mode of transferring data over a circuit-switched connection like GSM. The connection is established by dialing the number of an Internet service provider.
DBMS	Database Management System
DM	(Device Management Protocol) A part of the OMA/SyncML specification.
DNS	(Domain Name System) A System used to map human readable network names divided into fields separated by '.'s to the binary IP format.
DS	(Data Synchronization) A part of the OMA/SyncML specification.
ERP	Enterprise Resource Planning.
FOTA	Firmware Update Over-The-Air.
FUMO	(Firmware Update Management Object) enables mobile devices to be updated OTA by using the industry-standard protocol OMA DM.
GPRS	(General Packet Radio Service) Standardized as part of GSM Phase 2+, GPRS represents the first implementation of packet switching within GSM, which is a circuit-switched technology. GPRS offers theoretical data speeds of up to 115 Kbit/sec using multislot techniques. GPRS is an essential precursor for 3G, as it introduces the packet-switched core that UMTS requires.
GSM	(Global System for Mobile communications), The second-generation digital technology originally developed for Europe but which now has in excess of 71 per cent of the world market. Initially developed for operation in the 900-MHz band and subsequently modified for the 850-MHz, 1800-MHz, and 1900-MHz bands. GSM originally stood for Groupe Speciale Mobile, the CEPT committee that began the GSM standardization process.
HTTP	(Hypertext Transport Protocol) TCP/IP based Internet protocol that fetches hypertext objects from remote hosts.
HTTPS	(Hypertext Transport Protocol Secure) HTTP with an additional encryption and authentication SSL between HTTP and TCP.
IMEI	(International Mobile Equipment Identity) Each GSM mobile phone has a unique International Mobile Equipment Identity (IMEI), which identifies the mobile phone (not the GSM subscriber who is using the phone). Find a definition of the IMEI at http://umtslink.at/GSM/gsm_kennziffern.htm .

IMPS	Internet Messaging and Presence Service.
IP	Internet Protocol.
J2EE	(Java 2 Platform Enterprise Edition) J2EE is a platform-independent, Java-centric environment from Sun for developing, building, and deploying web-based enterprise applications online. The J2EE platform consists of a set of services, APIs, and protocols that provide the functionality for developing multi-tiered, web-based applications.
J2ME	(Java 2 Platform, Micro Edition) A collection of Java APIs that enables the device to run small, user-installable software applications written especially for mobile devices such as phones, developed by Sun Microsystems.
JDBC	(Java Database Connectivity) A set of APIs providing a standard to allow Java applets access to a database.
JMS	(Java Messaging Service) An API from Sun Microsystems for accessing enterprise messaging systems. Part of J2EE.
LAN	Local Area Network.
LDAP	(Lightweight Directory Access Protocol) Set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler.
LDAPS	(Lightweight Directory Access Protocol Secure) LDAP with an additional encryption/authentication SSL between LDAP and TCP.
LEMONADE	License to Enhanced Mobile Oriented And Diverse Endpoints.
OAP	(Over-the-Air Provisioning) The process of sending settings or commands wirelessly to a device through a mobile carrier, without the need for a data cable.
OMA	(Open Mobile Alliance) A standardization organization focused on the definition of industry standards for the mobile industry.
OSS/J	(Operational Support System) An initiative that produced a standard set of Java technology-based APIs to jump-start the implementation of end-to-end services on next-generation wireless networks. OSS/J leverages the convergence of telecommunications and Internet-based solutions.
OTA	(Over The Air) Activation method for services and tariff changes.
OTASU	(Over-the-Air Software Update) The process of applying a ROM update to a mobile device wirelessly, without the need for a data cable.
PAP	(Push Access Protocol) Provides an abstract protocol for sending WAP Push messages to devices. Removes the need for server-side applications to directly communicate with an SMSC.
PDA	(Personal Digital Assistant) A sophisticated handheld device with advanced display facilities and a range of business-oriented software programs.
PIM	(Personal Information Manager) A productivity tool that provides calendar, tasks and contact information.
SMPP	(Short Message Peer to Peer) An open, industry-standard protocol for sending SMS data over the Internet.
SMS	Short Message Service; a text message service which enables users to send short messages (160 characters) to other users. A very popular service, particularly amongst young people, with 400 billion SMS messages sent worldwide in 2002.

SMSC	(Short Message Service Center) A network element in the mobile telephone network that delivers SMS messages.
SMTP	(Simple Mail Transport Protocol) A simple text based protocol to send email over TCP/IP links.
SQL	Structured Query Language; standardized query language for requesting information from a database.
SSL	Secure Sockets Layer; a protocol developed by Netscape for transmitting private documents via the Internet.
STK	SIM ToolKit: specified within the GSM standard, this allows operators to add additional functions to the phone menu in order to provide new services such as mobile banking or email.
SyncML	Synchronization Markup Language; device-independent protocol for synchronization and device management defined by OMA.
TAC	Type Allocation Code; portion of the 15 IMEI code that is a unique identifier of wireless devices.
TCP	Transmission Control Protocol; enables two hosts to establish a connection and exchange streams of data.
TCP/IP	Transmission Control Protocol/Internet Protocol; suite of communications protocols used to connect hosts on the Internet.
UI	(User Interface) The interface to an application that a user can interact with to receive notifications or achieve tasks.
UMTS	One of the third-generation (3G) cell phone technologies.
URL	Uniform Resource Locator; the addressing system of the Internet. A set of URI schemes that have explicit instructions on how to access a resource on the Internet.
WAP	Wireless Application Protocol; a de facto standard for enabling mobile phones to access the Internet and advanced services. Users can access websites and pages which have been converted by the use of WML into stripped-down versions of the original more suitable for the limited display capabilities of mobile phones.
WBXML	WAP Binary Extensible Markup Language, allows XML documents to be transmitted in a compactly over mobile networks.
WCAP	Web Calendar Access Protocol; high level command-based protocol for communicating with the Calendar Server.
WCAPS	Web Calendar Access Protocol Secure; WCAP with an additional encryption/authentication SSL between WCAP and TCP.
WCDMA	Wideband CDMA; the technology created from a fusion of proposals to act as the European entrant for the ITU IMT-2000 family.
XML	Extensible Markup Language; a markup language for structured information.